Алгебраические расширения полей

Определение 1. Поле K называется *расширением* поля k, если $\mathsf{k} \subset K$.

Пример 2. $\mathbb{Q} \subset \mathbb{R}$, $\mathbb{Q} \subset \mathbb{Q}_p$, $\mathbb{R} \subset \mathbb{C}$, $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}]$.

Определение 3. Пусть $\mathsf{k} \subset K$ – расширение полей. Элемент $\alpha \in K$ называется *алгебраическим* над k, если существует многочлен $p(x) \in \mathsf{k}[x]$, не равный нулю такой, что $p(\alpha) = 0$. Иначе α называется *трансцендентным* над k.

Пример 4. Числа $\sqrt{2}, \sqrt{3} \in \mathbb{R}$ алгебраичны над $\mathbb{Q}$, они суть корни многочленов $x^2 - 2$ и $x^2 - 3$ соответственно. Число $\alpha = \sqrt{2} + \sqrt{3}$ также алгебраично. Чтобы это увидеть, заметим: $\alpha^2 = 2 + 2\sqrt{6} + 3 = 5 + 2\sqrt{6}$, $(\alpha^2 - 5)^2 = 24$, значит α обнуляет многочлен $(x^2 - 5)^2 - 24$.

Пример 5. Числа $\pi, e \in \mathbb{C}$ трансцендентны над $\mathbb{Q}$, однако доказать это непросто. Несложно доказать, что трансцендентно число $\sum_{k=1}^{\infty} 10^{-k!}$, однако ещё проще доказать, что трансцендентные числа существуют, не предъявляя явно примера. Дело в том, что множество алгебраических над $\mathbb{Q}$ чисел счётно, а множество всех комплексных чисел – несчётно.

В действительности, сумма, произведение и частное алгебраических чисел – тоже алгебраическое число. Как можно видеть из примера, построить многочлен, обнуляющий сумму двух алгебраических чисел по данным многочленам, обнуляющим сами числа, может быть непросто. Мы этого и не будем делать, а доказательство отложим на некоторое время.

Пусть $\mathsf{k} \subset K$ – расширение полей, а $\alpha \in K$ – элемент. Обозначим через $\mathsf{k}[\alpha]$ наименьшую подалгебру над k в K, содержащую α. Очевидно,

$$\mathsf{k}[\alpha] = \{p(\alpha) \mid p \in \mathsf{k}[\alpha]\}.$$

Аналогично, определим $\mathsf{k}(\alpha)$ как наименьшее подполе в K, содержащее k и α. Очевидно,

$$\mathsf{k}(\alpha) = \left\{ \frac{p(\alpha)}{q(\alpha)} \mid p, q \in \mathsf{k}[x] \right\}.$$

Как устроено $\mathsf{k}[\alpha]$? Имеется гомоморфизм колец $g\colon \mathsf{k}[x] \to \mathsf{k}[\alpha]$, переводящий x в α. Он сюръективен, пусть I – его ядро. Это идеал в $\mathsf{k}[x]$. Кольцо многочленов от одной переменной над полем – кольцо главных идеалов, поэтому I порождён некоторым многочленом $f(x)$. При этом фактор $\mathsf{k}[x]/I \cong \mathsf{k}[\alpha] \subset K$ не имеет делителей нуля, значит идеал I прост, а многочлен f неприводим. Возможны два случая: $f = 0$ и $f \neq 0$. Если $f = 0$, то $\mathsf{k}[\alpha] \cong \mathsf{k}[x]$, на элемент α нет алгебраических соотношений, это значит, что α трансцендентен над k. Во втором случае элемент α алгебраичен (так как обнуляется многочленом f) и все многочлены, обращающиеся в ноль на α, кратны f.

Определение 6. Пусть α – алгебраический над k элемент в K. *Минимальным многочленом* α над k называется ненулевой многочлен $f \in \mathsf{k}[x]$ минимальной степени такой, что $f(\alpha) = 0$. *Степенью* алгебраического элемента называется степень его минимального многочлена, обозначение: $\deg \alpha$ или $\deg_{\mathsf{k}} \alpha$.

Как доказано выше, все многочлены, равные нулю на α, кратны минимальному многочлену. В частности, минимальный многочлен определён однозначно с точностью до умножения на константы.

Пример 7. Пусть $\alpha \in \mathbb{C}$ – первообразный корень степени 6 из единицы. Тогда α обнуляет многочлен x^6-1. Раскладывая $x^6-1=(x^3-1)(x^3+1)=(x^3-1)(x+1)(x^2-x+1)$, видим, что α обнуляет x^2-x+1. Так как $\alpha \notin \mathbb{Q}$, это и есть минимальный многочлен, и $\deg \alpha = 2$.

Предложение 8. *Пусть $\mathsf{k} \subset K$ – расширение, $\alpha \in K$ – элемент. Тогда*
α алгебраический $\Rightarrow \mathsf{k}[\alpha] = \mathsf{k}(\alpha)$,
α трансцендентный $\Rightarrow \mathsf{k}[\alpha]$ – не поле.

Доказательство. Пусть α алгебраичен, а f – его минимальный многочлен, он прост. Если $p(\alpha) \neq 0 \in \mathsf{k}[\alpha]$, то p не делится на f, они взаимно просты. По алгоритму Евклида найдутся многочлены $u, v \in \mathsf{k}[x]$, для которых $pu + fv = 1$. Подставим α и получим: $p(\alpha)u(\alpha) = 1$, т.е. $p(\alpha)$ обратим в $\mathsf{k}[\alpha]$. Значит, $\mathsf{k}[\alpha]$ – поле и $\mathsf{k}[\alpha] = \mathsf{k}(\alpha)$. (Можно было также сказать, что $\mathsf{k}[\alpha] = \mathsf{k}[x]/(f)$ – поле как фактор по максимальному идеалу.)

Наоборот, если $\mathsf{k}[\alpha]$ – поле, то $1/\alpha \in \mathsf{k}[\alpha]$. Значит, найдётся $p \in \mathsf{k}[x]$ такой, что $1/\alpha = p(\alpha)$. Следовательно, α обнуляет многочлен $xp(x)-1$ и поэтому алгебраический над k. □

Предложение 9. *Пусть $\mathsf{k} \subset K$ – расширение, $\alpha \in K$ – элемент.*
α алгебраичен $\Rightarrow \dim_{\mathsf{k}} \mathsf{k}[\alpha] = \deg_{\mathsf{k}} \alpha$,
α трансцендентен $\Rightarrow \dim_{\mathsf{k}} \mathsf{k}[\alpha] = \infty$.

Доказательство. В первом случае пространство $\mathsf{k}[\alpha] = \mathsf{k}[x]/(f)$ имеет базис $\bar{1}, \bar{x}, \ldots, \overline{x^{d-1}}$, где $d = \deg \alpha = \deg f$. Во втором случае пространство $\mathsf{k}[\alpha] \cong \mathsf{k}[x]$ бесконечномерно. □

Как можно видеть, алгебраичность элемента измеряется размерностью подполя, которое он порождает.

Определение 10. Расширение полей $\mathsf{k} \subset K$ называется *конечным*, если K – конечномерное векторное пространство над k. В этом случае *степенью* расширения $[K : \mathsf{k}]$ называется размерность $\dim_{\mathsf{k}} K$.

Расширение полей $\mathsf{k} \subset K$ называется *алгебраическим*, если любой элемент $\alpha \in K$ алгебраичен над k.

Коротко говорят, что K конечно (алгебраично) над k, или что расширение K/k конечно (алгебраично).

Следующая простая лемма очень важна.

Лемма 11. *1. Элемент $\alpha \in K$ алгебраичен над подполем $\mathsf{k} \subset K$ тогда и только тогда найдётся промежуточное поле $\mathsf{k} \subset F \subset K$ такое, что $\alpha \in F$ и F конечно над k.*

2. Любое конечное расширение – алгебраическое.

3. Если $\mathsf{k} \subset F \subset K$ – расширения полей, то K конечно над k тогда и только тогда F конечно над k и K конечно над F, при этом $[K : \mathsf{k}] = [K : F] \cdot [F : \mathsf{k}]$.

Доказательство. 1. Пусть α алгебраичен над k, тогда в качестве F можно взять $\mathsf{k}[\alpha]$. Пусть, напротив, такое F существует. Тогда $\mathsf{k}(\alpha) \subset F$ из-за минимальности, значит пространство $\mathsf{k}[\alpha] \subset \mathsf{k}(\alpha) \subset F$ конечномерно над k, по предложению 9 α алгебраический.

2. Следует из 1. – можно взять $F = K$.

3. Пусть K/F и F/k конечны, докажем, что K/k конечно и размерности перемножаются. Выберем $y_1, \ldots, y_n$ – базис векторного пространства K над F, и $x_1, \ldots, x_m$ – базис векторного пространства F над k. Покажем, что попарные произведения $x_i y_j$ образуют базис K над k. Любой $y \in K$ разложим по базису $y = \sum c_i y_i$, где $c_i \in F$. Каждый c_i

разложим по базису F над k: $c_i = \sum_j c_{ij}x_j$, где $c_{ij} \in \mathsf{k}$. Объединяя, получим $y = \sum_{ij} c_{ij}x_j y_i$, т.е. $x_j y_i$ порождают K над k. Они линейно независимы: если $\sum_{ij} c_{ij}x_j y_i = 0$, то из линейной независимости y_i получаем, что $c_i = \sum_j c_{ij}x_j = 0$. А из линейной независимости x_j получаем, что $c_{ij} = 0$.

Для доказательства в другую сторону заметим: выше показано, что если в K над F или в F над k есть бесконечная линейно независимая система, то и в K над k она тоже есть. □

Пусть $\mathsf{k} \subset K$ – расширение, $\alpha_1 \dots, \alpha_n \in K$ – элементы. Определим $\mathsf{k}[\alpha_1, \dots, \alpha_n]$ как наименьшую k-подалгебру в K, содержащую все α_i.

Лемма 12. *Алгебра $\mathsf{k}[\alpha_1, \dots, \alpha_n]$ конечномерна над k тогда все α_i алгебраические над k. Если эти условия выполнены, то $\mathsf{k}[\alpha_1, \dots, \alpha_n]$ – конечное расширение k.*

Доказательство. Если $\mathsf{k}[\alpha_1, \dots, \alpha_n]$ конечномерна, то все α_i алгебраические по лемме 11. Обратно: заметим, что

$$\mathsf{k}[\alpha_1, \dots, \alpha_n] = \mathsf{k}[\alpha_1][\alpha_2] \dots [\alpha_n].$$

При этом каждый этаж башни

$$\mathsf{k} \subset \mathsf{k}[\alpha] \subset \mathsf{k}[\alpha_1][\alpha_2] \subset \dots \subset \mathsf{k}[\alpha_1][\alpha_2] \dots [\alpha_n]$$

порождён одним алгебраическим элементом и, значит, конечен по предложению 9 и является полем. По лемме 11 вся башня также конечна. □

Таким образом, конечные расширения – это конечно порождённые алгебраические. Теперь можно доказать основное свойство алгебраических чисел.

Предложение 13. *Пусть $\mathsf{k} \subset K$ – расширение полей, а $\alpha, \beta \in K$ алгебраичны над k. Тогда $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ также алгебраичны над k.*

Доказательство. По предыдущему, расширение $\mathsf{k}[\alpha, \beta] \supset \mathsf{k}$ конечно. Значит, по лемме 11 элементы $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in \mathsf{k}[\alpha, \beta]$ алгебраичны над k. □

Следствие 14. *Пусть $\mathsf{k} \subset K$ – расширение полей. Тогда множество элементов в K, алгебраичных над k, образует подполе.*

Напомним

Определение 15. Поле K называется *алгебраически замкнутым*, если любой многочлен в $K[x]$ степени, большей нуля, имеет в K корень.

Определение 16. Поле $K \supset \mathsf{k}$ называется *алгебраическим замыканием* поля k, если K алгебраично над k и алгебраически замкнуто.

Наша цель – доказать, что алгебраическое замыкание поля существует и единственно с точностью до изоморфизма. Сегодня мы докажем существование, проведём его в два шага: сначала по данному полю k построим содержащее его алгебраически замкнутое поле K, затем определим $\bar{\mathsf{k}} \subset K$ как множество алгебраических элементов в K над k и проверим, что $\bar{\mathsf{k}}$ – замыкание k.

Сделаем сначала второй шаг.

Лемма 17. *Пусть $\mathsf{k} \subset K$ – расширение, и поле K алгебраически замкнуто. Пусть $\bar{\mathsf{k}}$ – множество алгебраических элементов в K над k. Тогда $\bar{\mathsf{k}}$ – алгебраическое замыкание k.*

Доказательство. По построению, $\bar{\mathsf{k}}$ алгебраично над k, проверим алгебраическую замкнутость. Пусть $p \in \bar{\mathsf{k}}[x]$ – многочлен, $p(x) = p_n x^n + \ldots + p_1 x + p_0$. У p найдётся корень α в K. Рассмотрим башню расширений $\mathsf{k} \subset \mathsf{k}[p_0, \ldots, p_n] \subset \mathsf{k}[p_0, \ldots, p_n, \alpha]$. Первый её этаж конечен по лемме 12, второй этаж конечен, так как α алгебраический над $\mathsf{k}[p_0, \ldots, p_n]$. Значит, вся башня – конечное расширение и следовательно α алгебраичен над k, поэтому $\alpha \in \bar{\mathsf{k}}$ – корень p. □

Для построение алгебраически замкнутого поля нам понадобится понятие присоединения корня.

Определение 18. Пусть k – поле, а $f \in \mathsf{k}[x]$ – неприводимый многочлен. Говорят, что поле $K \supset \mathsf{k}$ *получено присоединением* к k *корня* многочлена f, если найдётся $\alpha \in K$ такой, что $f(\alpha) = 0$ и $K = \mathsf{k}[\alpha]$.

Лемма 19. *Присоединение корня существует и единственно.*

Доказательство. Существование: положим $K = \mathsf{k}[x]/(f)$. Это поле, так как многочлен f прост и идеал (f) максимален. Класс $\bar{x}$ в K является корнем f и порождает всё K, поэтому K получено присоединением к k корня f.

Единственность. Пусть $K' \supset \mathsf{k}$ получено присоединением к k корня α многочлена f. Определим гомоморфизм k-алгебр $g\colon \mathsf{k}[x] \to K'$, положив $g(x) = \alpha$. При этом $f(x) \mapsto f(\alpha) = 0$, поэтому g пропускается через гомоморфизм $\bar{g}\colon \mathsf{k}[x]/(f) \to K'$. Так как $\mathsf{k}[x]/(f)$ – поле, то $\bar{g}$ инъективен, а так как $\bar{g}(\bar{x}) = \alpha$ и α порождает K', то $\bar{g}$ сюръективен. □

Можно определить присоединение корня и для приводимого многочлена, но тогда результат не будет определён однозначно.

Определение 20. Пусть k – поле, а $p \in \mathsf{k}[x]$ – многочлен. Расширение $K \supset \mathsf{k}$ называется *полем разложения* многочлена f, если f раскладывается в K на линейные множители и K порождено над k корнями f.

Здесь многочлен f может быть приводимым. Несложно доказать, что поле разложения многочлена существует и единственно, но более удобно это будет делать после того, как мы построим алгебраическое замыкания поля.

Теперь мы можем сделать второй шаг в доказательстве существования алгебраического замыкания поля.

Лемма 21. *Пусть k – поле, тогда существует его алгебраически замкнутое расширение $K \supset \mathsf{k}$.*

Доказательство. При помощи конструкции присоединения корня можно построить поле, в котором любой заданный многочлен из $\mathsf{k}[x]$ имеет корень – достаточно взять неприводимый множитель. Итерируя конструкцию, можно построить расширение, в котором любое конечное (и даже счётное) число многочленов из $\mathsf{k}[x]$ имеют по корню. Однако если множество $\mathsf{k}[x]$ несчётно, нужна другая конструкция. А именно, присоединим корни всех многочленов сразу. Пусть M – множество всех многочленов положительной степени в $\mathsf{k}[x]$. Рассмотрим кольцо многочленов $\mathsf{k}[x_f]_{f \in M}$, где переменные соответствуют многочленам из M. Пусть $I \subset \mathsf{k}[x_f]$ – идеал, порождённый всеми многочленами $f(x_f)$. Покажем, что I не совпадает со всем кольцом. В противном случае получим соотношение $1 = \sum f_i(x_{f_i}) a_{f_i}$, где сумма конечна и $a_{f_i} \in \mathsf{k}[x_f]_{f \in M}$. Рассмотрим расширение k, в котором все многочлены f_i (их конечное число) имеют по корню α_i. Подставим в $1 = \sum f_i(x_{f_i}) a_{f_i}$ вместо x_{f_i} элемент α_i, получим $1 = 0$, противоречие.

Значит, I – собственный идеал, рассмотрим какой-нибудь максимальный идеал $I_m \supset I$. Фактор $\mathsf{k}[x_f]_{f\in M}/I_m$ и есть искомое поле. Действительно, в нём любой многочлен f имеет корень $\bar{x}_f$.

Таким образом, мы умеем строить расширение заданного поля, в котором у любого многочлена есть корень. Начиная с поля $\mathsf{k} = K_0$, построим последовательность расширений $K_0 \subset K_1 \subset K_2 \subset \ldots$, где K_i содержит корень любого многочлена из $K_{i-1}[x]$. Положим $K = \cup_i K_i$, очевидно, это поле. При этом для любого многочлена $p \in K[x]$ найдётся поле K_i, которое содержит все его коэффициенты. Тогда в K_{i+1} у p есть корень. Таким образом, K алгебраически замкнуто. □

Из лемм 21 и 17 следует

Предложение 22. *У любого поля существует алгебраическое замыкание.*