Сепарабельные и нормальные расширения

Для доказательства единственности алгебраического замыкания (и не только) нужно изучить, как устроены продолжения гомоморфизмов полей.

Определение 1. Пусть $\mathsf{k} \subset K$ – расширение полей, а $\sigma\colon \mathsf{k} \to L$ – вложение полей. Вложение $\bar\sigma\colon K \to L$ называется *продолжением* σ на K, если $\bar\sigma|_{\mathsf{k}} = \sigma$.

Наша ближайшая цель – доказать, что вложение в алгебраически замкнутое поле всегда можно продолжить на алгебраическое расширение. Простейший случай – продолжение на поле, порождённое одним элементом.

Лемма 2. *Пусть расширение $\mathsf{k} \subset K = \mathsf{k}[\alpha]$ порождено одним элементом, а $\sigma\colon \mathsf{k} \to L$ – вложение. Тогда количество продолжений σ на K равно числу различных корней многочлена $\sigma(f)$ в L, где $f \in \mathsf{k}[x]$ – минимальный многочлен α над k. В частности, если поле L алгебраически замкнуто, то продолжение существует.*

Доказательство. Пусть $\bar\sigma\colon \mathsf{k}[\alpha] \to L$ – продолжение. Тогда $0 = \bar\sigma(f(\alpha)) = \bar\sigma(f)(\bar\sigma(\alpha)) = \sigma(f)(\bar\sigma(\alpha))$ (т.к. коэффициенты f лежат в k), т.е. $\bar\sigma$ переводит α в корень $\sigma(f)$. Образом α гомоморфизм $\bar\sigma$ определён однозначно, т.к. α порождает K над k. Обратно, пусть $\beta \in L$ – корень $\sigma(f)$. Тогда существует вложение $\mathsf{k}[\alpha]$ в L, продолжающее σ и переводящее α в β. Чтобы его построить, рассмотрим гомоморфизм $\mathsf{k}[x] \to L$, равный σ на k и переводящий x в β. Он отправляет $f(x)$ в $\sigma(f)(\beta) = 0$ и поэтому пропускается через фактор $K = \mathsf{k}[x]/(f)$. □

Предложение 3. *Пусть расширение $\mathsf{k} \subset K$ алгебраическое, а поле L алгебраически замкнуто. Тогда для любого вложения $\sigma\colon \mathsf{k} \to L$ существует продолжение σ на K.*

При помощи предыдущей леммы можно по индукции построить продолжение вложения σ на любое подполе в K, порождённое конечным (и даже счётным) набором элементов. В общем случае идея та же – последовательно продолжать вложения на всё большие подполя, но при этом нужно использовать трансфинитную индукцию.

В алгебре для трансфинитных конструкций обычно применяется лемма Цорна – одна из эквивалентных формулировок аксиомы выбора. Напомним, что линейно упорядоченное множество – это частично упорядоченное множество, в котором любые два элемента сравнимы.

Лемма 4 (лемма Цорна). *Пусть X – частично упорядоченное множество. Предположим, что X обладает следующим свойством: у любого линейно упорядоченного подмножества $Y \subset X$ найдётся верхняя граница, т.е. такой $x \in X$, что для любого $y \in Y$ верно $y \leqslant x$. Тогда в X существует максимальный элемент, т.е. такой $x \in X$, для которого в X нет строго большего элемента.*

Доказательство леммы не приводится, потому что это аксиома. □

Доказательство предложения 3. Рассмотрим множество, образованное парами (F, σ_F), где $\mathsf{k} \subset F \subset K$ – промежуточное поле, а $\sigma_F\colon F \to L$ – вложение, для которого $\sigma_F|_{\mathsf{k}} = \sigma$. Определим на X порядок: $(F_1, \sigma_1) \leqslant (F_2, \sigma_2)$, если $F_1 \subset F_2$ и $\sigma_2|_{F_1} = \sigma_1$. Любое линейно упорядоченное множество $Y \subset X$ имеет в X верхнюю грань. А именно, рассмотрим поле $F_Y = \cup_{(F,\sigma_F)\in Y} F$ (это поле, так как из любых двух объединяемых полей одно вложено в другое) и вложение $\sigma_Y\colon F_Y \to L$, полученное склейкой всех σ_F. Очевидно, (F_Y, σ_Y) – верхняя граница Y. Значит, по лемме Цорна в X найдётся максимальный элемент (F, σ_F). Если $F = K$, то всё доказано. Иначе возьмём алгебраический $\alpha \in K \setminus F$ и продолжим σ_F на $F[\alpha]$ по лемме 2, получим элемент в X, строго больший (F, σ_F). Противоречие. □

Теперь, наконец, докажем единственность алгебраического замыкания.

Предложение 5. *Алгебраическое замыкание поля единственно. Т.е. для любых двух алгебраических замыканий K_1, K_2 поля k найдётся изоморфизм $K_1 \to K_2$, постоянный на k.*

Доказательство. Так как K_1 алгебраично над k, а K_2 алгебраически замкнуто, по предложению 3 найдётся вложение $\sigma\colon K_1 \to K_2$, постоянное на k. Докажем, что σ сюръективно. Пусть $\alpha \in K_2$, а $f \in \mathsf{k}[x]$ – многочлен со старшим коэффициентом 1, обнуляющий α. Тогда f раскладывается над алгебраически замкнутым полем K_1 на линейные множители: $f(x) = \prod(x-\beta_i) \in K_1[x]$. Применим σ, получим $f(x) = \sigma(f)(x) = \prod(x-\sigma(\beta_i))$. Подставим α: $0 = f(\alpha) = \prod(\alpha - \sigma(\beta_i))$. Значит, α равен одному из $\sigma(\beta_i)$ и следовательно, лежит в образе σ. □

Выясним более детально, как устроены продолжения вложений полей на конечные расширения.

Лемма 6. *Пусть $\mathsf{k} \subset K$ – конечное расширение, а L алгебраически замкнуто. Тогда количество продолжений вложения $\sigma\colon \mathsf{k} \to L$ на K не зависит от L и σ (и зависит только от $\mathsf{k} \subset K$).*

Доказательство. Пусть $\bar\sigma\colon K \to L$ – продолжение σ. Очевидно, $\bar\sigma(K)$ алгебраично над $\sigma(\mathsf{k})$. Поэтому, отождествляя k с $\sigma(\mathsf{k})$, можно сказать, что $\bar\sigma$ попадает в алгебраическое замыкание k. Таким образом, L можно считать алгебраическим замыканием k (а точнее говоря, $\sigma(\mathsf{k})$). Остаётся использовать единственность алгебраического замыкания. □

Определение 7. Количество продолжений вложения k в алгебраически замкнутое поле на конечное расширение $\mathsf{k} \subset K$ называется *сепарабельной степенью* расширения и обозначается $[K : \mathsf{k}]_s$.

Предложение 8. *Пусть $\mathsf{k} \subset K$ – конечное расширение. Тогда*

1. $[K : \mathsf{k}]_s \leqslant [K : \mathsf{k}]$,
2. *для промежуточного расширения $\mathsf{k} \subset F \subset K$ верно $[K : \mathsf{k}]_s = [K : F]_s \cdot [F : \mathsf{k}]_s$,*
3. $[\mathsf{k}[\alpha] : \mathsf{k}]_s \leqslant \deg_{\mathsf{k}} \alpha$, *равенство достигается тогда и только тогда минимальный многочлен для α не имеет кратных корней над $\bar{\mathsf{k}}$.*

Доказательство. 3. Было доказано: из леммы 2 следует, что $[\mathsf{k}[\alpha] : \mathsf{k}]_s$ равно количеству различных корней минимального многочлена α над k в $\bar{\mathsf{k}}$.

2. Очевидно: чтобы продолжить вложение $\sigma\colon \mathsf{k} \to L$ на K, необходимо и достаточно продолжить σ сначала на F (есть $[F : \mathsf{k}]_s$ способов), а затем на K (в каждом случае тут по $[K : F]_s$ способов).

1. Для расширения, порождённого одним элементом, это пункт 3. Общий случай получается по индукции по количеству порождающих элементов, с использованием того, что в башнях $[K : \mathsf{k}]_s = [K : F]_s \cdot [F : \mathsf{k}]_s$ и $[K : \mathsf{k}] = [K : F] \cdot [F : \mathsf{k}]$. □

Определение 9. Многочлен в $\mathsf{k}[x]$ называется *сепарабельным*, если он не имеет кратных корней в $\bar{\mathsf{k}}$. Конечное расширение полей $\mathsf{k} \subset K$ называется *сепарабельным*, если $[K : \mathsf{k}]_s = [K : \mathsf{k}]$. Элемент $\alpha \in K \supset \mathsf{k}$ называется *сепарабельным над* k, если $\mathsf{k}[\alpha]$ сепарабельно над k.

Из предыдущего предложения следует, что элемент сепарабелен тогда и только тогда его минимальный многочлен сепарабелен.

Предложение 10. *1. Конечное расширение $\mathsf{k} \subset K$ сепарабельно тогда и только тогда любой элемент $\alpha \in K$ сепарабелен над k.*

2. Расширение, порождённое конечным числом сепарабельных элементов, сепарабельно.

3. Если $\mathsf{k} \subset F \subset K$, то расширение K/k сепарабельно тогда и только тогда расширения K/F и F/k сепарабельны.

Доказательство. 3. $\Leftarrow$: если $[K : F]_s = [K : F]$ и $[F : \mathsf{k}]_s = [F : \mathsf{k}]$, то по мультипликативности получим $[K : \mathsf{k}]_s = [K : \mathsf{k}]$. $\Rightarrow$: от противного, если $[K : F]_s > [K : F]$ или $[F : \mathsf{k}]_s > [F : \mathsf{k}]$, то по мультипликативности получим $[K : \mathsf{k}]_s > [K : \mathsf{k}]$, противоречие.

2. Пусть $K = \mathsf{k}[\alpha_1, \ldots, \alpha_n]$ и все α_i сепарабельны над k. Заметим, что каждый α_i сепарабельный над $\mathsf{k}[\alpha_1, \ldots, \alpha_{i-1}]$, так как минимальный многочлен α_i над $\mathsf{k}[\alpha_1, \ldots, \alpha_{i-1}]$ делит минимальный многочлен α_i над k и поэтому не имеет кратных корней в $\bar{\mathsf{k}}$. Применим 3 к башне $\mathsf{k} \subset \mathsf{k}[\alpha_1] \subset \mathsf{k}[\alpha_1, \alpha_2] \subset \ldots \subset \mathsf{k}[\alpha_1, \ldots, \alpha_n] = K$ и получим, что K/k сепарабельно.

1. $\Rightarrow$: следует из 3, применённого к $\mathsf{k} \subset \mathsf{k}[\alpha] \subset K$. $\Leftarrow$: следует из 2 □

Первое утверждение этого предложения естественно взять за определение сепарабельности для бесконечных расширений.

Определение 11. Алгебраическое расширение $\mathsf{k} \subset K$ называется *сепарабельным*, если любой элемент в K сепарабелен над k.

Наконец, приведём пример несепарабельного расширения.

Пример 12. Пусть $K = \mathbb{F}_p(t)$ – поле рациональных функций, а $\mathsf{k} = \mathbb{F}(t^p)$ – его подполе. Тогда K порождено над k элементом t, он является корнем многочлена $x^p - t^p \in \mathsf{k}[x]$. Этот многочлен неприводим над k, и раскладывается на линейные множители в $K[x]$: $x^p - t^p = (x - t)^p$. Это не сепарабельный многочлен, его единственный корень в K есть t. Получаем: $[K : \mathsf{k}] = p$, $[K : \mathsf{k}]_s = 1$.

Как будет видно из следующего предложения, по существу этот пример несепарабельности – единственный.

Предложение 13. *Пусть $\mathsf{k} \subset K$ – расширение полей, $\alpha \in K$ – элемент, а f – его минимальный многочлен над k. Тогда*

1. *если $\operatorname{char} \mathsf{k} = 0$, то α сепарабелен. Следовательно, все алгебраические расширения в характеристике 0 сепарабельны.*

2. *если $\operatorname{char} \mathsf{k} = p$, то найдутся такое $m \geqslant 0$, что α^{p^m} сепарабелен над k, и такой сепарабельный многочлен $g(x)$, что $f(x) = g(x^{p^m})$. При этом $[\mathsf{k}[\alpha] : \mathsf{k}]_s = \deg g$, $[\mathsf{k}[\alpha] : \mathsf{k}] = p^m \cdot \deg g$.*

Доказательство. 1. Пусть $\operatorname{char} \mathsf{k} = 0$. Покажем, что f не имеет кратных корней в $\bar{\mathsf{k}}$. В противном случае у f и f' есть общий корень. Но $\deg f' = (\deg f) - 1$, значит $(f, f') \neq 1$ и f не неприводим.

2. В случае положительной характеристики возможно, что неприводимый многочлен имеет кратные корни в алгебраическом замыкании, при этом $f' = 0$. Так как $(x^n)' = nx^{n-1}$, то получаем, что все мономы, образующие f, имеют степень, кратную p. То есть, $f(x) = g(x^p)$ для некоторого многочлена g. Ясно, что g неприводим. Если он не сепарабелен, то повторяем те же рассуждения. В итоге найдём нужные g и m. Так как корень степени p в характеристике p единствен (если существует), то количество различный корней у f и g равны. Значит $[\mathsf{k}[\alpha] : \mathsf{k}]_s = \deg g$, $[\mathsf{k}[\alpha] : \mathsf{k}] = \deg f = p^m \deg g$. □

Другое важное и естественное свойство расширения полей – нормальность. Дадим три эквивалентных определения

Определение 14. Алгебраическое расширение $\mathsf{k} \subset K$ называется *нормальным*, если выполнено любое из трёх равносильных условий:

1. Если неприводимый многочлен в $\mathsf{k}[x]$ имеет корень в K, то он раскладывается в K на линейные множители.

2. K есть поле разложения некоторого семейства многочленов из $\mathsf{k}[x]$.

3. Для всех вложений $\sigma\colon K \to \bar{\mathsf{k}}$ над k образ $\sigma(K)$ один и тот же.

Доказательство равносильности условий. $1 \Rightarrow 2$. Возьмём семейство всех минимальных многочленов над k всех элементов в K. Очевидно, что его полем разложения будет K.

$2 \Rightarrow 3$. Фиксируем вложение $K \to \bar{\mathsf{k}}$ над k и отождествим K с его образом. Пусть $\sigma\colon K \to \bar{\mathsf{k}}$ – ещё одно вложение, постоянное на k. Покажем, что $\sigma(K) = K$. Пусть $\alpha \in K$ – произвольный элемент. Поле K порождено корнями некоторых многочленов, разлагающихся в K на линейные множители. Значит, можно найти конечно число таких многочленов, что их корни порождают α над k. Пусть f – их произведение, можно считать, что старший коэффициент f равен 1. Тогда $f(x) = \prod(x - \alpha_i)$, где $\alpha_i \in K$. Применим σ, получим $f(x) = \sigma(f)(x) = \prod(x - \sigma(\alpha_i))$. Т.е, σ переставляет α_i. Значит, $\sigma(\mathsf{k}[\alpha_1, \ldots, \alpha_n]) = \mathsf{k}[\alpha_1, \ldots, \alpha_n]$. Следовательно, $\sigma(K) = K$.

$3 \Rightarrow 1$. Пусть неприводимый многочлен $f \in \mathsf{k}[x]$ имеет корень $\alpha \in K$. Вложим K в $\bar{\mathsf{k}}$, и пусть β – ещё один корень f в $\bar{\mathsf{k}}$. По лемме 2, существует вложение $\mathsf{k}[\alpha]$ в $\bar{\mathsf{k}}$ над k, переводящее α в β. Продолжим его до вложения K в $\bar{\mathsf{k}}$. По условию, его образ есть K, значит $\beta \in K$. Таким образом, все корни f в $\bar{\mathsf{k}}$ лежат в K, следовательно f раскладывается в K на линейные множители. □

Пример 15.

1. Любое расширение степени 2 нормально: если поле K порождено корнем α многочлена $x^2 + px + q$, то оно содержит и другой его корень $-p - \alpha$.

2. Расширение $\mathbb{Q}[\sqrt[3]{2}] \supset \mathbb{Q}$ не нормально: неприводимый над $\mathbb{Q}$ многочлен $x^3 - 2$ раскладывается над $\mathbb{Q}[\sqrt[3]{2}]$ на два неприводимых множителя $(x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{2}^2)$.

3. Расширение $\mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{1}] \supset \mathbb{Q}$ нормально, так как это поле разложение многочлена $x^3 - 2$: оно содержит все кубические корни из 2.

4. Расширение $\mathbb{Q}[\sqrt[n]{1}] \supset \mathbb{Q}$, полученное присоединением первообразного корня, нормально: любой другой корень есть степень первообразного и потому лежит в $\mathbb{Q}[\sqrt[n]{1}]$.

Более удобно говорить о нормальных расширениях, если выбрано алгебраическое замыкание основного поля k и расширения предполагаются вложенными в него.

Определение 16. Пусть $\alpha \in \bar{\mathsf{k}}$ – элемент. *Сопряжёнными* с α называются корни минимального многочлена для α над k.

Для сепарабельного элемента α количество сопряжённых с ним равно степени α. Очевидно, сопряжённость – отношение эквивалентности. Сопряжённые с α элементы можно ещё описать как образы α при всевозможных вложениях $\mathsf{k}[\alpha]$ в $\bar{\mathsf{k}}$ над k. Также множество сопряжённых с α элементов совпадает с орбитой α относительно автоморфизмов поля $\bar{\mathsf{k}}$ над k.

Очевидно, определение 3 нормального расширения можно переформулировать так:

Предложение 17. *Пусть* $\mathsf{k} \subset K \subset \bar{\mathsf{k}}$ *– расширение. Поле* K *нормально над* k *тогда и только тогда* K *содержит вместе с любым элементом все сопряжённые с ним над* k*, а также тогда и только тогда* K *инвариантно относительно автоморфизмов* $\bar{\mathsf{k}}$ *над* k*.*

Напомним

Определение 18. Автоморфизмом поля K над подполем k называется биективный гомоморфизм полей $\sigma\colon K \to K$ такой, что $\sigma|_{\mathsf{k}} = \mathrm{id}$. Множество автоморфизмов K над k образует группу относительно композиции, которая называется *группой Галуа* расширения и обозначается $Gal(K, \mathsf{k})$

Как следует из доказанного на этой лекции, для конечного расширения $\mathsf{k} \subset K$

$$|Gal(K : \mathsf{k})| = |\operatorname{Hom}_{\mathsf{k}}(K, K)| \leqslant |\operatorname{Hom}_{\mathsf{k}}(K, \bar{\mathsf{k}})| = [K : \mathsf{k}]_s \leqslant [K : \mathsf{k}].$$

При этом в первом неравенстве достигается равенство в точности для нормальных расширений, а во втором – в точности для сепарабельных. Следовательно, порядок группы Галуа расширения равен его степени в том и только том случае, когда расширение нормально и сепарабельно.

Определение 19. Нормальное и сепарабельное расширение называется *расширением Галуа.*

Обычно группу Галуа рассматривают только для расширений Галуа, так как только для них она обладает хорошими свойствами.

Приведём несколько примеров группы Галуа.

Пример 20. Любое расширение степени 2 нормально. Если оно сепарабельно, то оно может быть получено добавлением двух различных квадратных корней $\pm\sqrt{a}$ из некоторого элемента a исходного поля. В таком случае группа Галуа изоморфна $\mathbb{Z}/2\mathbb{Z}$ и переставляет местами $\pm\sqrt{a}$.

Пример 21. Расширение $\mathbb{Q}[\sqrt{2}, \sqrt{3}] \supset \mathbb{Q}$ сепарабельно (т.к. характеристика ноль) и нормально (т.к. это поле разложения многочленов $x^2 - 2, x^2 - 3$). Оно имеет степень 4, в его группе Галуа G ровно 4 элемента. Они переставляют корни $\pm\sqrt{2}$ и $\pm\sqrt{3}$ друг с другом в каждой паре, следовательно, любой элемент $\sigma \in G$ имеет порядок 2. Значит, $G \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ и все перестановки реализуются.

Пример 22. Расширение $\mathbb{Q}[\sqrt[4]{2}] \supset \mathbb{Q}$ не нормально. Однако если присоединять $\sqrt[4]{2}$ к полю $\mathbb{Q}[i]$, получится нормальное расширение $\mathbb{Q}[\sqrt[4]{2}, i] \supset \mathbb{Q}[i]$. Действительно, все корни четвёртой степени из 2 отличаются умножением на i^m, поэтому добавив к $\mathbb{Q}[i]$ один корень, мы получим и все остальные. Степень расширения равна 4. Если $\sigma \in G = Gal(\mathbb{Q}[\sqrt[4]{2}, i], \mathbb{Q}[i])$, то $\sigma(\sqrt[4]{2}) = i^m\sqrt[4]{2}$, где $m \in \mathbb{Z}$ определено по модулю 4. При этом σ однозначно определяется по m. Получаем изоморфизм $G \to \mathbb{Z}/4\mathbb{Z}$: $\sigma \mapsto m$.

Иными словами, группа Галуа $\mathbb{Q}[\sqrt[4]{2}, i]$ над $\mathbb{Q}[i]$ реализует циклические перестановки на множестве из четырёх комплексных корней 4-й степени из 2. Можно показать, что группа Галуа $\mathbb{Q}[\sqrt[4]{2}, i]$ над $\mathbb{Q}$ действует на нём движениями квадрата.

Группа Галуа содержит много информации о расширении. Основной пример – замечательная теорема, которую мы докажем в следующий раз.

Теорема 23 (основная теорема теории Галуа). *Пусть* $\mathsf{k} \subset K$ *– конечное расширение Галуа. Тогда между множеством подгрупп в группе Галуа* $Gal(K, \mathsf{k})$ *и множеством промежуточных расширений* $\mathsf{k} \subset F \subset K$ *есть взаимно обратные биекции. А именно, подгруппе* $H \subset Gal(K, \mathsf{k})$ *отвечает поле инвариантов*

$$K^H = \{\alpha \in K | \forall \sigma \in H \ \sigma(\alpha) = \alpha\},$$

а подполю F *соответствует подгруппа*

$$Gal(K, F) = \{\sigma | \forall \alpha \in F \ \sigma(\alpha) = \alpha\} \subset Gal(K, \mathsf{k}).$$