Лекция 1.2. Теория Галуа.

Утверждение 1.1. Пусть L/K конечное расширение полей. Тогда число автоморфизмов L над K не превосходит степени расширения полей: $|\mathrm{Aut}_K L| \leq [L:K]$.

Доказательство. Представим расширение $K \subset L$, как композицию простых расширений: $K = K_0 \subset K_1 = K(\alpha_1) \subset K_2 = K(\alpha_1)(\alpha_2) \subset \ldots \subset K_m = K(\alpha_1)(\alpha_2)\ldots(\alpha_m) = L$. Каждый автоморфизм L над K индуцирует вложения $\varphi_i : K_i \to L$, причем φ_0 уже дано. φ_i можно продолжить до φ_{i+1} не более, чем $[K_{i+1} : K_i]$ способами. Значит, φ_0 можно продолжить до φ_m, являющегося автоморфизмом L над K, не более, чем $[K_1 : K_0][K_2 : K_1]\ldots[K_m : K_{m-1}] = [L : K]$ способами.

Утверждение 1.2.(Теорема о примитивном элементе) Пусть L/K конечное сепарабельное расширение полей. Тогда существует такой элемент $\gamma \in L$, что $L = K(\gamma)$, то есть расширение является простым.

Доказательство. Опять же, представим наше расширение, как композицию простых. Другими словами, выберем $\alpha_1, \ldots, \alpha_n \in L$ такие, что $L = K(\alpha_1, \ldots, \alpha_n)$. Будем вести индукцию по n. Из упражнения 1.8(е) следует, что достаточно доказать для $n = 2$. Пусть $L = K(\alpha, \beta)$. Случай, когда K конечное поле, является упражнением 1.7(в). Будем считать K бесконечным. Из упражнения 1.8(ж) следует, что существует ровно $[L : K]$ вложений $\sigma_i : L \to \overline{K}$ над K. Рассмотрим многочлен $P(x) = \prod_{i \neq j}(\sigma_i(\alpha) + x\sigma_i(\beta) - \sigma_j(\alpha) - x\sigma_j(\beta))$. Так как K бесконечно, и P ненулевой многочлен, то существует такое $c \in K$, что $P(c) \neq 0$. Тогда для $\gamma = \alpha + c\beta$ все $\sigma_i(\gamma)$ различны при различных i, и из соображения степени $L = K(\gamma)$.

Определение. Расширение L/K *нормально*, если минимальный многочлен любого элемента из L разлагается на линейные множители над L, то вместе с каждым элементом $\alpha \in L$ в L содержатся все остальные корни его минимального многочлена — *сопряженные* к α.

Теорема 1.3. Для конечного расширения L/K следующие условия равносильны:

(i) $|\mathrm{Aut}_K L| = [L : K]$;

(ii) $L^G = \{a \in L | \forall \varphi \in G \quad \varphi(a) = a\} = K$, где $G = \mathrm{Aut}_K L$;

(iii) расширение L/K нормально и сепарабельно.

Доказательство.

(i)$\Rightarrow$ (ii) Заметим, что L^G является полем. Так как $G = \mathrm{Aut}_K L = \mathrm{Aut}_{L^G} L$, то $|\mathrm{Aut}_K L| \leq [L : L^G]$. Далее все следует из соображения степени.

(ii)$\Rightarrow$ (iii) Пусть $\alpha \in L$, $\{\alpha = \alpha_1, \dots, \alpha_m\}$ — G-орбита α. Тогда $P(x) = \prod_{i=1}^m (x - \alpha_i) \in L^G[x] = K[x]$. Значит, минимальный многочлен элемента α делит $P(x)$ (на самом деле, как нетрудно видеть, совпадает с ним) и разлагается над L на линейные множители, то есть расширение L/K нормально. Поскольку все корни P различны, то расширение сепарабельно.

(iii)$\Rightarrow$ (i) По теореме о примитивном элементе, представим L как простое расширение $K(\gamma)$. Пусть P минимальный многочлен для α. Тогда из нормальности и сепарабельности у него ровно $\deg(P)$ корней в L. Из упражнения 1.2(г) следует, что существует ровно $\deg(P)$ вложений $\sigma_i : L \to L$ над K (являющихся автоматически изоморфизмами). В то же время, $\deg(P) = [L : K]$, и теорема доказана.

Замечание. Если подгруппа $H \subset G = \mathrm{Aut}_K L$ такая, что $L^H = K$, то $H = G$.

Доказательство. Для каждого элемента можно построить минимальный многочлен так, как это было сделано при доказательстве следствия (ii)$\Rightarrow$ (iii), но используя лишь H-орбиту. Так получается сепарабельность расширения, а значит, оно простое: $L = K(\gamma)$. Тогда $[L : K] = \deg(P) = |H|$, где P минимальный многочлен для γ. Отсюда следует требуемое.

Определение. Конечное расширение L/K, удовлетворяющее равносильным условиям из теоремы 1.3, называется *расширением Галуа*, а группа $\mathrm{Aut}_K L$ называется его *группой Галуа* $\mathrm{Gal}(L/K)$.

Следствие 1.4.

(i) Поле разложения L неприводимого сепарабельного многочлена $P \in K[x]$ является расширением Галуа L/K.

(ii) Композиция расширений Галуа является расширением Галуа. Если $K \subset L \subset F$ башня полей, и F/K является расширением Галуа, то и F/L тоже является расширением Галуа.

(iii) Любое сепарабельное расширение содержится в некотором расширении Галуа (для этого надо воспользоватся теоремой о примитивном элементе и рассмотреть соответствующее поле разложения).

Замечание. Расширение Галуа L/K является простым (по теореме о примитивном элементе), то есть $L = K(\gamma)$, а группа Галуа $\mathrm{Gal}(L/K)$ транзитивно действует на множестве элементов, сопряженных к γ. Значит, мы имеем вложение $\mathrm{Gal}(L/K) \subset S_n$, где $n = [L : K]$.

Пусть L/K расширение Галуа с группой G. Сопоставим каждому промежуточному полю $K \subset E \subset L$ группу Галуа G_E расширения L/E, а каждой подгруппе в $H \subset G$ сопоставим поле L^H.

Теорема 1.5.(Основная теорема теории Галуа) Отображения $E \mapsto G_E$ и $H \mapsto L^H$ взаимно обратны и, таким образом, устанавливают биекцию между подполями поля L, содержащими K, и подгруппами в G. При этом подполям E, являющимся нормальными расширениями поля K, соответствуют нормальные подгруппы $G_E \triangleleft G$ и $\mathrm{Gal}(E/K) = G_E$.

Доказательство. Из теоремы 1.3 следует, что $L^{G_E} = E$, а из замечания после нее вытекает то, что $H = \mathrm{Gal}(L/L^H)$.

Расширение E/K нормально тогда и только тогда, когда $\mathrm{Gal}(L/K)$ оставляет E на месте как множество, потому что $\mathrm{Gal}(L/K)$ транзитивно действует на сопряженных элементах. Заметим, что $gE = L^{gHg^{-1}}$, где $g \in G$. Следовательно, по доказанному, E/K нормально тогда и только тогда, когда подгруппа $H \subset G$ нормальна.

Пример. Докажем основную теорему алгебры, пользуясь теорией Галуа. Вложим произвольное конечное расширение $\mathbb{R}(i)$ в расширение Галуа с группой G, пользуясь тем, что характеристика нулевая. Рассмотрим в G силовскую 2-подгруппу. По основной теореме теории Галуа ей соответствует расширение поля $\mathbb{R}(i)$ нечетной степени. В то же время над $\mathbb{R}$, а значит, и над $\mathbb{R}(i)$, нет неприводимых многочленов нечетной степени, а стало быть, нет и нетривиальных расширений нечетной степени. Таким образом, группа G должна быть 2-группой. Но у каждой такой группы, если только она не тривиальна, есть подгруппа индекса 2, которой будет соответствовать квадратичное расширение $\mathbb{R}(i)$. Заметим, что у $\mathbb{R}(i)$ нет нетривиальных квадратичных расширений, так как из любого элемента в $\mathbb{R}(i)$ извлекается корень. Итак, получаем, что группа G тривиальная, что равносильно тривиальности изначального конечного расширения. Основная теорема алгебры доказана.