Часть 1. Теорема Галуа

Определение 1.1. Расширение L/K называется расширением Галуа, если L/K нормально и сепарабельно. Группа автоморфизмов $\mathrm{Aut}(L/K)$ называется группой Галуа поля L над K и обозначается $\mathrm{Gal}(L/K)$.

Всякой подгруппе $H \subset \mathrm{Gal}(L/K)$ можно сопоставить подполе $L^H = \{\, \alpha \in L \mid \forall \sigma \in \mathrm{Gal}(L/K)\ \alpha^\sigma = \alpha \,\}$. Аналогично, всякому подполю $F \subset L$ можно сопоставить подгруппу $\mathrm{Gal}(L/F) \subset \mathrm{Gal}(L/K)$. Основная теорема теории Галуа гласит:

Теорема 1.2. *Если L/K — конечное расширение Галуа, то сопоставления $H \mapsto L^H$, $F \mapsto \mathrm{Gal}(L/F)$ определяют взаимно однозначное соответствие между множеством $\{\, F \mid K \subset F \subset L \,\}$ промежуточных полей и множеством подгрупп $H \subset \mathrm{Gal}(L/K)$.*

Доказательство теоремы проведем в несколько этапов.

Лемма 1.3. *Если L/K — расширение Галуа, и $G = \mathrm{Gal}(L/K)$, то $L^G = K$.*

Доказательство: как было показано в прошлой лекции, если L/K нормально, то L^G/K — чисто несепарабельное расширение. Однако, если L/K сепарабельно, то и L^G/K сепарабельно, поэтому $L^G = K$. □

Лемма 1.4. *Если L/K — расширение Галуа и $K \subset F \subset L$, то L/F — расширение Галуа.*

Доказательство: L/F нормально, так как L/K нормально, и сепарабельно, так как L/K сепарабельно. □

Следствие 1.5. *Если L/K — расширение Галуа, то отображение $F \mapsto \mathrm{Gal}(L/F)$ — инъективно.*

Доказательство: если $K \subset F \subset L$, то L/F является расширением Галуа по лемме 1.4, поэтому из леммы 1.2 вытекает, что $F = L^{\mathrm{Gal}(L/F)}$. Значит, поле F восстанавливается по группе $\mathrm{Gal}(L/F)$, следовательно отображение $F \mapsto \mathrm{Gal}(L/F)$ инъективно. □

Замечание 1.6. В доказательстве инъективности конечность расширения L/K не используется. Поэтому этот результат верен и для бесконечных расширений Галуа.

Прежде чем заняться сюръективностью, докажем полезный результат.

Часть 2. Теорема о примитивном элементе

Определение 2.1. Пусть L/K — алгебраическое расширение полей. Элемент $\alpha \in L$ называется примитивным, если $L = K(\alpha)$.

Лемма 2.2. *Если для расширения полей L/K существует примитивный элемент, то L/K конечно и сущесвтует лишь конечное число различных промежуточных расширений $K \subset F \subset L$.*

Доказательство: первая часть очевидна, так как $[K(\alpha) : K] = \deg \mathrm{Irr}_\alpha^K(x)$. Докажем вторую часть. Пусть $p(x) = \mathrm{Irr}_\alpha^K(x)$. Предположим, что $K \subset F \subset L$ и рассмотрим многочлен $\mathrm{Irr}_\alpha^F(x) = x^k + a_1 x^{k-1} + \cdots + a_k$. Тогда, с одной стороны $K(a_1, \ldots, a_k) \subset F$, так как $a_1, \ldots, a_k \in F$, а с другой стороны $[K(\alpha) : K(a_1, \ldots, a_k)] \leqslant k = [K(\alpha) : F]$, значит $K(a_1, \ldots, a_k) = F$, то есть поле F восстанавливается по многочлену $\mathrm{Irr}_\alpha^F(x)$. С другой стороны, так как $p(\alpha) = 0$ и $p(x) \in K[x] \subset F[x]$, то $\mathrm{Irr}_\alpha^F(x) | p(x)$, так что достаточно показать, что многочлен $p(x)$ имеет лишь конечное число делителей в кольце $L[x]$. Однако ясно, что даже в кольце $\overline{L}[x]$ многочлен $p(x)$ имеет не больше, чем 2^n делителей, где $n = \deg p(x)$. □

Оказывается, верно и обратное утверждение.

Лемма 2.3. *Если L/K — конечное расширение и множество полей F, таких что $K \subset F \subset L$ конечно, то существует примитивный элемент.*

Доказательство: если поле K конечно, то L тоже конечно и в качестве примитивного элемента можно взять образующую группы L^*, которая, как мы знаем, циклична. Будем далее предполагать, что поле K бесконечно. Покажем, что если $L = K(\alpha, \beta)$, то найдется $\gamma \in L$, такое что $L = K(\gamma)$. Будем искать γ в виде $\gamma = \alpha + c\beta$, $c \in K$. Ясно, что в силу бесконечности поля K и конечности множества промежуточных полей, найдутся числа $c_1 \neq c_2 \in K$, такие что $K(\alpha + c_1\beta) = K(\alpha + c_2\beta)$. Но это поле содержит как $\beta = [(\alpha+c_1\beta) - (\alpha+c_2\beta)]/(c_1 - c_2)$, так и $\alpha = (\alpha + c_1\beta) - c_1\beta$, поэтому $K(\alpha+c_1\beta) = K(\alpha, \beta)$. Далее остается применить индукцию по количеству порождающих L над K. □

Еще одним важным классом расширений, для которого заведомо существует примитивный элемент, являются сепарабельные расширения.

Лемма 2.4. *Если L/K — конечное сепарабельное расширение, то существует примитивный элемент.*

Доказательство: как и выше, достаточно рассмотреть случай, когда K бесконечно, а $L = K(\alpha, \beta)$. Пусть $n = [L : K] = [L : K]_s$ и пусть $\sigma_1, \ldots, \sigma_n$ — различные гомоморфизмы $L \to \overline{K}$ над K. Заметим, что если $\sigma_i(\alpha) = \sigma_j(\alpha)$ и $\sigma_i(\beta) = \sigma_j(\beta)$, то $i = j$, так как $L = K(\alpha, \beta)$. Поэтому существует лишь конечное множество чисел $c \in K$, таких что $\sigma_i(\alpha+c\beta) = \sigma_j(\alpha+c\beta)$ при $i \neq j$. Выберем $c \in K$, так чтобы таких равенств при $i \neq j$ не было и рассмотрим $\gamma = \alpha + c\beta$. Тогда все числа $\sigma_i(\gamma) \in \overline{K}$ различны, следовательно σ_i — набор различных гомоморфизмов $K(\gamma) \to \overline{K}$. Значит $[K(\gamma) : K] \geqslant [K(\gamma) : K]_s \geqslant n = [L : K]$, следовательно $K(\gamma) = L$. □

Следствие 2.5. *Если L/K сепарабельно и $[K(\alpha) : K] \leqslant n$ для любого $\alpha \in L$, то $[L : K] \leqslant n$.*

Доказательство: пусть $\alpha \in L$ — таков, что $m = [K(\alpha) : K]$ — максимально возможное. Далее, если $\beta \notin K(\alpha)$, то по теореме о примитивном элементе существует γ, такое что $[K(\gamma) : K] = [K(\alpha, \beta) : K] > [K(\alpha) : K]$, что противоречит максимальности m. Значит $K(\alpha) = L$ и $[L : K] = [K(\alpha) : K] \leqslant n$. □

Часть 3. Окончание доказательства теоремы Галуа

Лемма 3.1. *Пусть L — поле и $G \subset \mathrm{Aut}(L)$ — конечная группа автоморфизмов, $|G| = n$, и $F = L^G$. Тогда L/F — конечное расширение Галуа, $G = \mathrm{Gal}(L/F)$ и $[L : F] = n$.*

Доказательство: пусть $\alpha \in L$ и $G\alpha = \{\alpha_1, \ldots, \alpha_m\}$. Ясно, что группа G переставляет числа α_i, поэтому многочлен $f(x) = \prod_{i=1}^m (x - \alpha_i)$ инвариантен относительно группы G, следовательно $f(x) \in F[x]$. С другой стороны, $f(\alpha) = 0$, следовательно $\mathrm{Irr}_\alpha^F(x) | f(x)$. Так как $f(x)$ раскладывается над полем L на линейные множители, и не имеет кратных корней, то то же верно и по отношению к многочлену $\mathrm{Irr}_\alpha^F(x)$. Так как α произвольно, то это означает, что расширение L/F нормально и сепарабельно, то есть является расширением Галуа. Более того, из приведенных выше рассуждений следует, что $\forall \alpha \in L$ имеем $[F(\alpha) : F] \leqslant n$, значит согласно 2.5 имеем $[L : F] \leqslant n$. С другой стороны $n = |G| \leqslant [L : F]_s \leqslant [L : F]$, значит $[L : F] = [L : F]_s = n$ и $G = \mathrm{Aut}(L/F) = \mathrm{Gal}(L/F)$. □

Теперь можно завершить доказательство теоремы Галуа. Действительно, если $H \subset \mathrm{Gal}(L/K)$ — подгруппа, то по лемме 3.1 имеем $H = \mathrm{Gal}(L/L^H)$, следовательно отображение $F \mapsto \mathrm{Gal}(L/F)$ — сюръективно.

Замечание 3.2. В доказательстве сюръективности существенным образом использована конечность расширения. Точнее говоря, использовалась конечность подшруппы $H \subset \mathrm{Gal}(L/K)$. Тем самым, даже если L/K бесконечное расширение Галуа, то образ отображения из множества подполей в множество подгрупп группы Галуа содержит все конечные подгруппы. В действительности, для бесконечных расширений отображение из множества подполей в множество подгрупп группы Галуа перестает быть сюръективным. Образ этого отображения состоит лишь из подгрупп, замкнутых относительно некоторой топологии на группе Галуа.

Теперь, закончив доказательство теоремы Галуа, займемся уточнениями. Пусть L/K — конечное расширение Галуа, и $G = \mathrm{Gal}(L/K)$. Заметим, что группа G действует как на множестве всех своих подгрупп (сопряжениями), так и на множестве всех промежуточных полей.

Лемма 3.3. *Изоморфизм теории Галуа является изоморфизмом G-множеств.*

Доказательство: пусть $\sigma \in G = \mathrm{Aut}(L/K)$ и $H \subset G$. Тогда $L^{\sigma H \sigma^{-1}} = \{\, \alpha \in L \mid \forall h \in H \ \sigma h \sigma^{-1}\alpha = \alpha \,\} = \{\, \alpha \in L \mid \forall h \in H \ h\sigma^{-1}\alpha = \sigma^{-1}\alpha \,\} = \{\, \alpha \in L \mid \sigma^{-1}\alpha \in L^H \,\} = \{\, \alpha = \sigma\beta \mid \beta \in L^H \,\} = (L^H)^\sigma$. □

Лемма 3.4. *Пусть L/K — конечное расширение Галуа, и $K \subset F \subset L$. Расширение F/K нормально $\Longleftrightarrow$ подгруппа $\mathrm{Gal}(L/F) \subset \mathrm{Gal}(L/K)$ — нормальна. В этом случае $\mathrm{Gal}(F/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/F)$.*

Доказательство: всякий гомоморфизм $F \to \overline{K}$ можно продолжить до гомоморфизма $L \to \overline{K}$ над K, который в силу нормальности L/K является автоморфизмом поля L. Следовательно, расширение F/K нормально $\Longleftrightarrow$ любой элемент группы $\mathrm{Gal}(L/K)$ оставляет F на месте, что в силу леммы 3.3 равносильно нормальности группы $\mathrm{Gal}(L/F)$.

Пусть теперь F/K нормально. Тогда всякий автоморфизм L/K оставляет F на месте, следовательно задает автоморфизм F/K. Тем самым, имеем гомоморфизм групп $\mathrm{Gal}(L/K) \to \mathrm{Gal}(F/K)$. Этот гомоморфизм сюръективен, так как всякий автоморфизм поля F над K можно продолжить до гомоморфизма из L в $\overline{K}$ над K, который является автоморфизмом L/K в силу нормальности L/K. В свою очередь, ядро гомоморфизма состоит из всех автоморфизмов L/K, тождественных на F, то есть по теореме Галуа совпадает с группой $\mathrm{Gal}(L/F)$. □

Лемма 3.5. *Если $K \subset F, F' \subset L$, то $F \subset F' \Longleftrightarrow \mathrm{Gal}(L/F') \subset \mathrm{Gal}(L/F)$. Иначе говоря, изоморфизм теории Галуа обращает отношение вложенности.*

Доказательство: если $F \subset F'$, то всякий автоморфизм поля L, тождественный на F' тождественнен и на F, поэтому $\mathrm{Gal}(L/F') \subset \mathrm{Gal}(L/F)$. Обратно, по теореме Галуа $L^{\mathrm{Gal}(L/F')} = F'$, поэтому вложение групп Галуа $\mathrm{Gal}(L/F') \subset \mathrm{Gal}(L/F)$ влечет вложение полей $F \subset F'$. □

Лемма 3.6. *Если $K \subset F \subset L$, то $[F:K] = (\mathrm{Gal}(L/K) : \mathrm{Gal}(L/F))$. В частности, полям, конечным над K соответствуют подгруппы конечного индекса.*

Доказательство: всякий гомоморфизм $F \to \overline{K}$ продолжается до автоморфизма поля L над K, так как L/K нормально. С другой стороны, автоморфизмы σ и σ' поля L над K задают один и тот же гомоморфизм $F \to \overline{K} \Longleftrightarrow \sigma^{-1}\sigma'$ тождественно на F, то есть лежит в $\mathrm{Gal}(L/F)$. Значит, множество гомоморфизмов $F \to \overline{K}$ совпадает с множеством смежных классов $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/F)$, следовательно $[F:K] = [F:K]_s = (\mathrm{Gal}(L/K) : \mathrm{Gal}(L/F))$. □

Замечание 3.7. Результаты 3.3–3.6 выполняются и для бесконечных расширений Галуа.

Замечание 3.8. Пусть $\overline{K}^{\mathrm{sep}}$ — сепарабельное замыкание поля K. Тогда $\overline{K}^{\mathrm{sep}}/K$ — максимальное сепарабельное расширение поля K. Его группа Галуа называется абсолютной группой Галуа поля K. Из теоремы Галуа следует, что сепарабельные расширения поля K находятся во взаимно однозначном соответствии с замкнутыми подгруппами абсолютной группы Галуа, при этом нормальные расширения соответствуют нормальным подгруппам, а конечные расширения соответствуют подгруппам конечного индекса.

Замечание 3.9. Изучение абсолютной группы Галуа поля рациональных чисел — одна из основных задач алгебраической теории чисел.

В завершение дадим еще одно определение.

Пусть $p(x) \in K[x]$ — неприводимый сепарабельный многочлен, а L — его поле разложения. Группа Галуа $\mathrm{Gal}(L/K)$ называется группой Галуа многочлена $p(x)$.