Теория Галуа, лекция 1: геометрический смысл теории Галуа

В этой лекции я расскажу вкратце, в чем состоит предмет теории Галуа. За определениями и разъяснением основных понятий лучше обращаться в следующие лекции, здесь только обзор. Доказательства тоже там.

1.1. Предмет теории Галуа

Сейчас я дам определение основных понятий теории Галуа, и перечислю главные теоремы. Теория Галуа содержит много других теорем, но если вы хорошо понимаете доказательство главных утверждений, все остальное будет уже нетрудно. Результатом изучения теории Галуа должно быть тесное знакомство с этими утверждениями и их доказательствами.

Определение 1.1. Пусть k – поле. **Расширение** k есть поле K, содержащее k; отношение «K является расширением k» обозначается $[K : k]$. **Конечное расширение** есть расширение $[K : k]$ такое, что K конечномерно как векторное пространство над k. **Степень** конечного расширения есть размерность K как векторного пространства над k. Элемент K называется **алгебраическим над** k, если он содержится в конечном расширении $[K' : k]$, то есть мультипликативно порождает поле K'', конечномерное над k. **Алгебраическое расширение** есть такое расширение $[K : k]$, что все элементы K алгебраичны над k.

Определение 1.2. Поле k называется **алгебраически замкнутым**, если любой многочлен $P(t) \in k[t]$ положительной степени имеет корень в k. Расширение $[\bar{k} : k]$ называется **алгебраическим замыканием** k, если $\bar{k}$ алгебраически замкнуто, а все элементы $\bar{k}$ алгебраичны над k.

Пример 1.3. Основная теорема алгебры утверждает, что поле $\mathbb{C}$ комплексных чисел алгебраически замкнуто.

Вопрос 1.4. Я знаю 4 доказательства этой теоремы: одно топологическое и использует свойства фундаментальной группы проколотого диска,

другое, тоже топологическое, использует теорему Брауэра о неподвижной точке, третье, аналитическое, использует разложение полинома в ряд Тэйлора в окрестности минимума, и четвертое, алгебраическое, утверждает, что поле, где любой многочлен нечетной степени имеет корень, можно алгебраически замкнуть, если добавить корни всех квадратных полиномов. А сколько доказательств основной теоремы алгебры знаете вы?

Пример 1.5. Рассмотрим множество всех элементов $\mathbb{C}$, алгебраических над $\mathbb{Q}$. Это множество образует поле, которое обозначается $\bar{\mathbb{Q}}$, и называется **алгебраическим замыканием** $\mathbb{Q}$.

Теорема 1.6. Пусть k – поле. Тогда алгебраическое замыкание $[\bar{k} : k]$ существует, и единственно с точностью до изоморфизма. Более того, любой автоморфизм k продолжается до автоморфизма $\bar{k}$, сохраняющего k.

Определение 1.7. Пусть $[K : k]$ – расширение полей. **Автоморфизм** K есть биективное отображение, сохраняющее сложение и умножение. **Автоморфизм** K **над** k есть автоморфизм K, действующий тождественно на $k \subset K$.

Замечание 1.8. Группа автоморфизмов K над k обозначается $\mathrm{Aut}_k(K)$. Это одно из основных понятий теории Галуа.

Определение 1.9. Пусть группа G действует на множестве S. Множество точек, которые сохраняются G, обозначается S^G. Когда S – векторное пространство, это множество называется **пространство инвариантов действия** G.

Главным предметом теории Галуа являются расширения Галуа. Расширения Галуа можно определить множеством разных способов. Вот некоторые из них. Чтобы не усложнять формулировки, я потребую характеристики 0.

Теорема 1.10. Пусть $[K : k]$ – конечное расширение полей характеристики 0. Тогда следующие условия равносильны.

(i) Пусть $G = \mathrm{Aut}_k K$. Тогда $k = K^G$.

(ii) Пусть $P(t) \in k[t]$ – неприводимый полином над k, имеющий хотя бы один корень в K. Тогда $P(t)$ разложим над K: $P(t) = \prod_i (t - \alpha_i)$, где все α_i лежат в K.

(iii) Тензорное произведение $K \otimes_k K$ изоморфно прямой сумме нескольких копий K.

(iv) Порядок группы $\operatorname{Aut}_k K$ равен степени расширения $[K : k]$.

Определение 1.11. Если верно одно из этих условий, $[K : k]$ называется **расширением Галуа**. Группа $\operatorname{Aut}_k K$ в такой ситуации называется **группой Галуа**.

Теорема 1.12. (основная теорема теории Галуа)
Пусть $[K : k]$ – расширение Галуа. Тогда существует биекция между подгруппами в $\operatorname{Aut}_k K$ и расширениями $[K' : k]$, лежащими в K. Эта биекция задается $G \mapsto K^G$. При этом, $[K^G : k]$ является расширением Галуа тогда и только тогда, когда подгруппа $G \subset \operatorname{Aut}_k K$ нормальна.

Важное следствие основной теоремы теории Галуа - «теорема о примитивном элементе».

Определение 1.13. Пусть $[K : k]$ – конечное расширение. Элемент $x \in K$ называется **примитивным**, если он порождает поле K, то есть если минимальное подполе K, содержащее x, равно K.

Теорема 1.14. (теорема о примитивном элементе)
Пусть $[K : k]$ – расширение Галуа. Тогда в K существует примитивный элемент.

Доказывать эту теорему проще, если поле k бесконечно. Понятно, что $x \in K$ примитивен, если он не лежит в собственном подполе $K' \subsetneq K$. Но таких подполей – конечное число, потому что группа Галуа имеет конечное число подгрупп, и они все являются конечномерными подпространствами в K.

Значит, теорема о примитивном элементе (для бесконечного поля) – следствие следующего простого утверждения, которое я оставлю в качестве упражнения.

Упражнение 1.15. Пусть V – конечномерное векторное пространство над бесконечным полем, а $V_1, ..., V_n \subset V$ – конечный набор пространств положительной коразмерности. Тогда дополнение $V \setminus \bigcup V_i$ непусто.

Большинство утверждений теории Галуа выводятся (обыкновенно - весьма просто) из основной теоремы.

Вот несколько полезных теорем, которые хорошо освоить (желательно помнить их вместе с доказательством).

Теорема 1.16. Пусть $[K : k]$ – расширение Галуа с циклической группой Галуа порядка n. Предположим, что k содержит все корни степени n из 1, то есть что многочлен $x^n - 1$ разлагается в K на линейные множители. Тогда $K = k[\sqrt[n]{a}]$: K получается из k добавлением корня n-й степени из a.

Замечание 1.17. Такое расширение называется **расширением Куммера**.

Определение 1.18. Коммутатор группы G есть подгруппа $[G, G] \subset G$, порожденная элементами вида $xyx^{-1}y^{-1}$. **Производный ряд** группы G_0 есть ряд вида $G_0 \supset G_1 \supset ...$, где $G_i = [G_{i-1}, G_{i-1}]$. **Разрешимая группа** есть группа, производный ряд который заканчивается тривиальной группой $\{e\}$.

Определение 1.19. Поле разложения неприводимого многочлена $P(t) \in k[t]$ положительной степени есть минимальное расширение $[K : k]$ такое, что многочлен $P(t)$ разлагается в K на линейные множители.

Замечание 1.20. Существование такого расширения не сразу очевидно; тем не менее, оно существует, единственно с точностью до изоморфизма, и является расширением Галуа. Это еще одно утверждение, которое надо уметь доказывать.

Определение 1.21. Группа Галуа неприводимого многочлена $P(t) \in k[t]$ есть группа Галуа его поля разложения.

Определение 1.22. Полиномиальное уравнение $P(t) = 0$, $P(t) \in k[t]$, называется **разрешимым в радикалах над** k, если оно имеет решение в поле $[K : k]$, которое получено последовательными расширениями $[K =$

$K_0 : K_1 : K_2 : ... : K_{N-1} : K_N = k]$, причем каждое $[K_i : K_{i+1}]$ есть поле разложения для многочлена $P(t) = t^n - a$.

Замечание 1.23. Иначе говоря, уравнение разрешимо в радикалах, если его решение можно выразить через алгебраические операции и операцию взятие корня.

Следующая теорема (доказанная Абелем) является одним из величайших достижений алгебры.

Теорема 1.24. Пусть $P(t)$ – неприводимый полином над полем k, а G – его группа Галуа. Уравнение $P(t) = 0$ разрешимо в радикалах тогда и только тогда, когда группа Галуа многочлена $P(t)$ разрешима.

Следствие 1.25. Существует полиномиальное уравнение степени 5 над $\mathbb{Q}$, которое не разрешимо в радикалах.

Действительно, можно без особенных усилий реализовать симметрическую группу S_5 в качестве группы Галуа некоторого уравнения степени 5; а эта группа не разрешима; доказательство этого чуть менее просто, но весьма элементарно.

1.2. Накрытия Галуа

Теория Галуа весьма мало отличается от теории накрытий, известной из топологии. Существует абстрактная (категорная) версия теории Галуа, в которой доказательство основной теоремы теории Галуа получается как следствие небольшого количества аксиоматических условий, которым удовлетворяют и расширения полей, и накрытия. Излагая теорию Галуа в этом курсе, я буду рассказывать такие версии доказательств, которые легко сводятся к абстрактной версии. Таким образом, внимательный читатель сможет заодно изучить основы теории Галуа для накрытий.

Все топологические пространства в этом разделе предполагаются хаусдорфовыми, локально линейно связными и локально односвязными. Это условия, которые нужны для применения принципа накрывающей гомотопии. Также, я буду считать, что пространство M (которое служит базой накрытий) связно.

Определение 1.26. Пусть M, $\tilde{M}$ — топологические пространства, а $\pi : \tilde{M} \longrightarrow M$ непрерывное отображение. π называется **этальным**, если у каждой точки $\tilde{x} \in \tilde{M}$ есть окрестность $\tilde{U} \ni \tilde{x}$ такая, что

$$\pi\big|_{\tilde{U}} : \tilde{U} \longrightarrow \pi(\tilde{U})$$

это гомеоморфизм. Это отображение называется **накрытием**, если у каждой точки $x \in M$, есть окрестность $U \ni x$ такая, что $\pi^{-1}(U)$ гомеоморфно $U \times S$, где S — топологическое пространство с дискретной топологией, а отображение $\pi\Big|_{\pi^{-1}(U)} : \pi^{-1}(U) \longrightarrow U$ при таком изоморфизме совпадает с проекцией $U \times S \longrightarrow U$. **Базой накрытия** называется M, а его **слоем** над точкой x — прообраз $\pi^{-1}(x)$. Накрытие $M_1 \longrightarrow M$ обозначается $[M_1 : M]$.

Замечание 1.27. Пусть $U \subset X$ — открытое подмножество, которое не является замкнутым. Отображение вложения $j : U \longrightarrow X$ этально, но не является накрытием (проверьте).

Пример 1.28. Отождествим окружность S^1 с одномерным тором $\mathbb{R}/2\pi\mathbb{Z}$. Естественная проекция $\mathbb{R} \longrightarrow S^1$ является накрытием (докажите). Проекция $\mathbb{R}^n$ на тор $T^n = \mathbb{R}^n/\mathbb{Z}^n$ также является накрытием (докажите это).

Определение 1.29. Пусть G — группа, действующая на топологическом пространстве M. Говорится, что действие G **вполне разрывно**, если у каждой точки $x \in M$ есть окрестность U такая, что $U \cap gU = \emptyset$ для любого $g \in G$ такого, что g действует не тождественно в окрестности U.

Пример 1.30. Пусть G — группа, вполне разрывно действующая на топологическом пространстве M. Тогда проекция $M \stackrel{\pi}{\longrightarrow} M/G$ является накрытием.

Определение 1.31. Автоморфизм накрытия $[M_1 : M]$ есть гомеоморфизм, коммутирующий с проекцией на M.

На накрытиях определены две операции, которые коммутативны и ассоциативны: это произведение и несвязная сумма, которую также называют копроизведением.

Определение 1.32. Пусть $[M_1 : M]$, $[M_2 : M]$ – накрытия M. Рассмотрим расслоенное произведение $M_1 \times_M M_2 \subset M_1 \times M_2$, состоящее из всех $(x, y) \in M_1 \times M_2$, которые проектируются в одну и ту же точку M. Тогда $M_1 \times_M M_2$ называется **произведением накрытий**.

Замечание 1.33. Произведение $M_1 \times_M M_2$ является накрытием M.

Определение 1.34. Пусть $[M_1 : M]$, $[M_2 : M]$ – накрытия M. Несвязное объединение $M_1 \coprod M_2$ называется **несвязной суммой**, или же **копроизведением** накрытий.

Легко видеть, что несвязная сумма дистрибутивна относительно умножения накрытий.

Упражнение 1.35. Пусть $[M_1 : M]$ – связное накрытие. Докажите, что следующие условия равносильны.

(i) Группа автоморфизмов накрытия $[M_1 : M]$ действует транзитивно на слоях (то есть прообразах точек M).

(ii) Произведение $M_1 \times_M M_1$ изоморфно (как накрытие) несвязной сумме нескольких копий M_1.

Определение 1.36. Накрытие, удовлетворяющее какому-то из условий предыдущего упражнение, называется **накрытием Галуа**, а группа $\mathrm{Aut}[M_1 : M]$ – его группой Галуа, или группой монодромии (по-английски: «deck transformation group»).

Основная теорема теории Галуа для накрытий формулируется так.

Теорема 1.37. Пусть $[M_1 : M]$ – накрытие Галуа, а $G = \mathrm{Aut}[M_1 : M]$ – его группа Галуа. Тогда существует биекция между подгруппами G и накрытиями $[M_1 : M_2 : M]$. При этой биекции подгруппа $G' \subset G$ соответствует накрытию M_1/G'.

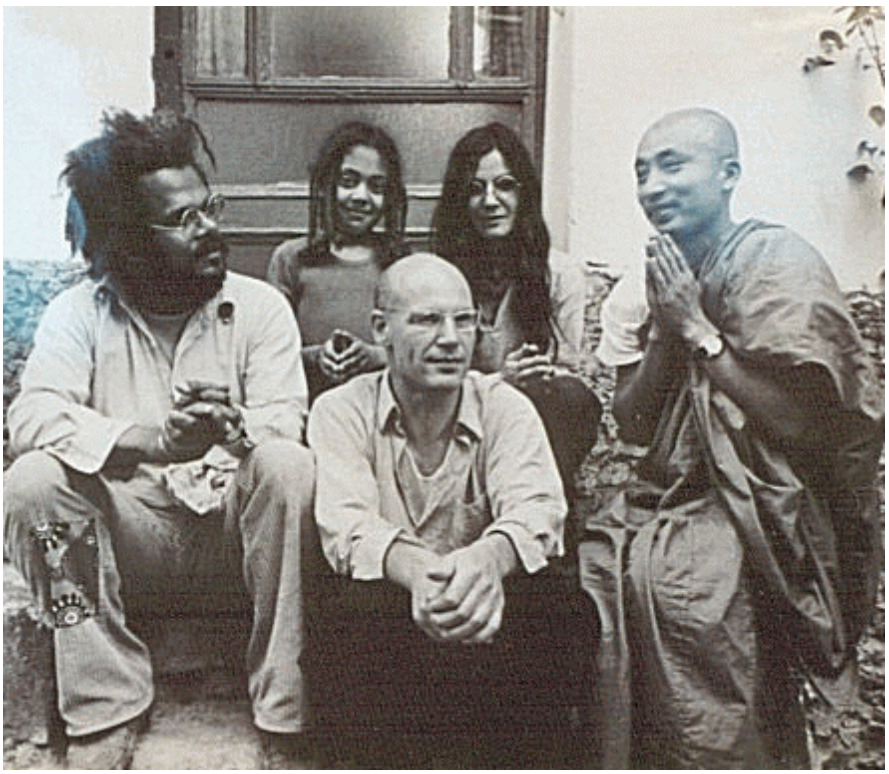
1.3. Теория Галуа в алгебре и геометрии: сравнительная табличка

Геометрия	**Алгебра**
Связное накрытие $[M_1 : M]$	Расширение полей $[K : k]$
Накрытие $[M_1 : M]$, которое не обязательно связно	Алгебра, изоморфная прямой сумме полей $[K_i : k]$
Несвязное объединение накрытий	Прямая сумма алгебр
Произведение накрытий	Тензорное произведение алгебр
Накрытие Галуа	Расширение Галуа
Универсальное накрытие	Алгебраическое замыкание
Накрытие Галуа есть такое накрытие $[M_1 : M]$, что $M' \times_M M' = \coprod^i M'$	Расширение Галуа есть такое расширение $[K : k]$, что $K \otimes_k K = \bigoplus^i K$
Взятие фактора M_1/G по подгруппе $G \subset \mathrm{Aut}[M_1 : M]$ группы автоморфизмов $[M_1 : M]$	Взятие пространства инвариантов K^G подгруппы $GH \subset \mathrm{Aut}[K : k]$ группы автоморфизмов $[K : k]$
Основная теорема теории Галуа	
$[M' : M]$ – накрытие Галуа. Тогда промежуточные накрытия $[M' : M'' : M]$ биективно соответствуют подгруппам в $\mathrm{Aut}[M' : M]$	$[K : k]$ – расширение Галуа. Тогда промежуточные расширения $[K : K' : k]$ биективно соответствуют подгруппам в $\mathrm{Aut}[K : k]$
подгруппа $G \subset \mathrm{Aut}[M' : M]$ соответствует фактору M'/G	подгруппа $G \subset \mathrm{Aut}[K : k]$ соответствует пространству инвариантов K^G.

1.4. Заключительные замечания

Аксиоматический подход к теории Галуа (включающей в себя обычную теорию Галуа и теорию Галуа накрытий) опубликован в SGA1 (Revêtements étales et groupe fondamental, Séminaire de Géométrie Algébrique 1),[1] за авторством Александра Гротендика и Мишель Рейно, которая была его студенткой.

[1] `http://arxiv.org/abs/math/0206203`



Alexander Grothendieck
(род. 28 марта 1928)

Гротендик определяет специальный класс категорий, которые он называет «категории Галуа», и доказывает, что в рамках этой теории можно определить все конструкции, которые определяются в обычной теории Галуа или теории Галуа для накрытий, и доказать основную теорему теории Галуа. Также он доказывает, что категория Галуа есть категория множеств с действием группы; это позволяет явно выписать фундаментальную группу или группу $\mathrm{Aut}[\bar{k} : k]$, исходя из данных соответствующей категории Галуа.

В следующих томах SGA этот же подход применялся для определения гомотопического класса многообразия (в частности, его когомологий), пользуясь конструкциями из коммутативной алгебры; эта наука называется «этальные когомологии». С помощью «этальных когомологий» можно говорить о топологическом устройстве многообразия над полем конечной характеристики, или, например, кольца $\mathbb{Z}$.