

ОСНОВНАЯ ТЕОРЕМА В КАТЕГОРНОЙ ТЕОРИИ ГАЛУА

С.Г. Далалян

Известия Национальной Академии Наук Армении. Математика,
том 27, № 4, 1992

Развивается "теория Галуа" для общих (абстрактных) категорий. В частности, на абстрактные категории переносится основная теорема классической теории Галуа.

§0. ВВЕДЕНИЕ

Полное и окончательное решение вопроса разрешимости полиномиального уравнения от одного неизвестного в радикалах, финально оформившееся в классическую теорию Галуа, базируется на трёх фундаментальных достижениях. Первым из них является введение понятия поля и переход от рассмотрения неприводимого многочлена к ассоциированному расширению поля коэффициентов этого многочлена. Во – вторых, это – введение понятия группы, рассмотрение группы автоморфизмов расширения полей и построение соответствия Галуа между промежуточными полями и подгруппами этой группы. Наконец, третий этап – перевод на язык полей и групп проблемы разрешимости полиномиального уравнения в радикалах и решение возникающей теоретико – групповой задачи. Сердцевиной и главным звеном этой программы является второй пункт, в рамках которого доказывается

Основная теорема классической теории Галуа.

Пусть поле K является расширением Галуа конечной степени поля k , G – группа Галуа этого расширения.

а) Соответствие Галуа устанавливает биекцию между промежуточными полями E рассматриваемого расширения и подгруппами H группы G .

б) Поле K является расширением Галуа поля E .

в) Поле E является расширением Галуа поля k в том и только в том случае, если подгруппа H нормальна в G ; группа Галуа этого расширения изоморфна факторгруппе G/H .

Главным первоисточником этих результатов является [1], современные изложения — [2], [3]. Здесь нас будут интересовать, главным образом, те результаты, которые связаны с обобщениями основной теоремы или доказательством её аналогов.

Прежде всего, основная теорема теории Галуа была перенесена на случай расширения полей бесконечной степени ([4]). Оказалось, что утверждения п.п. б) и в) справедливы и для бесконечных расширений Галуа. Однако в этом случае нарушается свойство п. а) : разным подгруппам группы G может соответствовать одно и то же промежуточное поле E . Для восстановления биективности надо рассматривать только "замкнутые" подгруппы группы G , каковыми являются наибольшие подгруппы, соответствующие промежуточным расширениям ([5]). Здесь замкнутость можно понимать как в смысле соответствия Галуа, так и, эквивалентно, относительно топологии на группе Галуа, имеющей в качестве базы окрестностей единицы все подгруппы группы G , являющиеся группами Галуа промежуточных расширений Галуа конечной степени над k .

Последний результат допускает максимальное в теории полей обобщение : при произвольном расширении K поля k с группой k -автоморфизмов G соответствием Галуа устанавливается биекция между множеством всех промежуточных полей E , над которыми K является расширением Галуа, и множеством всех компактных подгрупп группы G ([6]-[9]).

В [10] теория Галуа переносится на тела, точнее, доказывается утверждение п. а) основной теоремы в случае подтела k инвариантных элементов тела K относительно конечной группы внешних автоморфизмов G , действующих на тело K . Этот результат дополняется утверждением о равенстве степени верхнего подрасширения, определенного промежуточным телом E ,

порядку соответствующей подгруппы H , а степени нижнего подрасширения – индексу H в G .

Основную теорему удастся перенести и на некоммутативные кольца линейных преобразований векторного пространства над телом ([11]). При этом она претерпевает изменения, уже встречавшиеся в случае произвольного расширения полей и вызванные тем фактом, что как "замкнутые" подкольца, так и "замкнутые" подгруппы не совпадают с множествами, соответственно, всех промежуточных подколец и всех подгрупп уже в случае конечной группы Галуа. Основные технические трудности связаны именно с описанием "замкнутых" подколец и "замкнутых" подгрупп ([11]–[14]). Как частный результат разнотной теории получается полный аналог классической основной теоремы для случая подтела k данного тела K , образованного элементами, инвариантными относительно конечной группы его произвольных (а не только внешних) автоморфизмов. Однако "замкнутыми" оказываются все подтела, но не все подгруппы. Этот результат удастся распространить на случай бесконечной группы Галуа, только когда она состоит из внешних автоморфизмов ([11]).

Известны обобщения п. а) основной теоремы на случай, когда K – коммутативное кольцо без нетривиальных идемпотентов, являющееся конечно порожденным проективным модулем над подкольцом k элементов, инвариантных относительно группы Галуа G ([15]–[19]).

Весьма плодотворным оказалось приложение идей классической теории Галуа к обыкновенным дифференциальным уравнениям ([20]–[25]), обзорно [26]. Параллельная теория была развита для дифференциальных полей с аналогичной основной теоремой, подвергшейся двум модификациям.

Во-первых, место расширений Галуа обычных полей занимают расширения Пикара–Вессии (или, более общо, сильно нормальные расширения [15]) дифференциальных полей. В частности, это относится к исходному расширению K над k , причем предполагается, что k имеет алгебраически замкнутое поле констант характеристики нуль. Во-вторых, биекция множ-

ества промежуточных дифференциальных полей устанавливается, как и в случае расширения Галуа бесконечной степени для обычных полей, не со всеми подгруппами "дифференциальной" группы Галуа, а только с её "алгебраическими" (замкнутыми в смысле соответствия Галуа) подгруппами.

Группа Галуа расширения Пикара-Вессьо является алгебраической матричной группой. Венцом теории является результат о том, что разрешимости компоненты единицы дифференциальной группы Галуа соответствует разрешимость дифференциального уравнения в квадратурах ([26]).

В самое последнее время была развита теория Галуа для пучков множеств, доказан аналог основной теоремы (точнее п. а) этой теоремы) и полученные результаты были применены к предсхемам ([27]). Несколько особняком от общей канвы развития стоит, так называемая, треугольная теория Галуа ([28]).¹

Понятия и результаты, двойственные к тем, что составляют классическую теорию Галуа, а также её вышеприведенные модификации, возникают в тесно связанных друг с другом теориях римановых поверхностей, алгебраических функций и алгебраических кривых, и в общем виде в алгебраической геометрии (в частности, в связи с вопросами униформизации алгебраических многообразий (см. [8])).

Так в [29], определяется группа монодромии римановой поверхности (более точно, конечнолистного накрытия комплексной сферы, которое ассоциировано с римановой поверхностью по построению), являющаяся не чем иным, как группой Галуа соответствующего конечного расширения полей рациональных функций.

В [30] вводится понятие группы накрывающих преобразований накрытия $p: Y \rightarrow X$ топологических пространств и доказывается, что в случае

¹Рецензент привлёк внимание автора к статьям ([41]–[45]), которые содержат приложение идей классической теории Галуа к банаховым алгебрам. Согласно ([46]) имеется также небольшое число работ, посвященных теории Галуа общих алгебраических систем ([47], [48]).

когда X — риманова поверхность, а накрытие p индуцировано расширением L , получающимся присоединением к полю K мероморфных функций на X алгебраической функции, являющейся корнем целого многочлена с коэффициентами из K , группа накрывающих преобразований изоморфна группе автоморфизмов поля L над K . При этом накрытие Галуа можно определить либо требованием, чтобы соответствующее расширение полей мероморфных функций было расширением Галуа, либо эквивалентным условием транзитивности действия группы накрывающих преобразований на любом слое накрытия. Отметим, что, в частности, универсальное накрытие любого связного многообразия X есть накрытие Галуа и его группа Галуа изоморфна фундаментальной группе $\pi_1(X)$ ([30]). Именно такой подход, основанный на использовании групп Галуа, позволяет ввести понятие фундаментальной группы для произвольных схем ([31] и обзорно [32]).

Отображение

кривая $\longrightarrow$ поле рациональных функций на ней (*)

устанавливает двойственность между категориями полных неособых алгебраических кривых над фиксированным полем k и конечных расширений трансцендентного расширения $k(t)$ поля k . К сожалению, для многообразий высших размерностей такой двойственности не существует: гладкая полная модель соответствует полю степени трансцендентности ≥ 2 неоднозначно даже с точностью до бирегулярного изоморфизма ([33]). Тем не менее, нормальное накрытие алгебраического многообразия X имеет бирациональный характер, т.е. зависит только от (конечного сепарабельного) расширения L поля K рациональных функций многообразия X , верное для алгебраических многообразий произвольной размерности, позволяет перенести всю терминологию для расширений полей на конечные накрытия нормальных алгебраических многообразий вместе с некоторыми двойственными результатами ([34]).

В [15] "в наиболее общем смысле" теория Галуа трактуется как "теория, изучающая те или иные математические объекты на основе их группы

автоморфизмов". Значит естественно было ожидать развитие теории Галуа в рамках теории категорий. Однако автору такие попытки не известны. Первым шагом в этом направлении представляется настоящая работа. Под разрабатываемой "категорной теорией Галуа" подразумевается теория, которая ставит своей целью изучение зависимости между группой автоморфизмов (и более общо – полугруппой эндоморфизмов) объекта и его подобъектами (двойственно, факторобъектами) в абстрактной и по возможности максимально общей категории. При этом оказывается, что часто удобнее вместо подобъектов и факторобъектов данного объекта рассматривать морфизмы в него и из него или даже их семейства.

С одной стороны, категорная теория Галуа может быть рассмотрена как одна из параллелей классической теории Галуа наряду с её вышеприведенными аналогами и обобщениями. Вместе с тем, она занимает в этой цепи особое место в силу объемлющего, объединяющего и унифицирующего характера теоретико-категорного метода. Его специфика проявляется также в том, что в то время, как результаты категорной теории Галуа навеяны, а иногда просто скалькированы с классической или параллельных теорий Галуа, их доказательства полностью отличаются от известных, опирающихся на теоретико-множественный подход доказательств. Возможность категорного обобщения теории Галуа показывает её истинное место в математике.

Отметим, что частные теории Галуа служат не только эталоном для подражания для категорной теории, но и возможной областью приложения. Так, интерес автора к разрабатываемой тематике был обусловлен работами ([35], [36]) (в которых факторизацией по подгруппам группы Галуа строятся башни накрытий кривых и исследуются многообразия Прима этих накрытий), стремлением строго обосновать применение теории Галуа.

Статья состоит из трех параграфов. В §1 изучаются группы и полугруппы

еству его эндоморфизмов и исследуются их свойства. Здесь доказывается теорема 2, являющаяся обобщением п. (в) основной теоремы классической теории Галуа. В §3 приводится конструкция соответствия Галуа и ассоциированного с ним оператора замыкания, доказываются результаты, обобщающие утверждение п. (а) основной теоремы классической теории Галуа (теорема 3).

Сводка некоторых обозначений и соглашений

Морфизм φ из объекта A в объект B обозначается $A\varphi B$, множество всех морфизмов из объекта A в объект B — $\text{Mor}(A, B)$. Композиция морфизмов $A\varphi B$ и $B\psi C$ записывается слева направо: $\varphi\psi$. Полугруппа эндоморфизмов объекта A обозначается $\text{End}A$, группа автоморфизмов — $\text{Aut}A$, их единичный элемент — 1_A .

Класс всех подклассов класса A (в частности, множество всех подмножеств множества A) обозначается $B(A)$ и называется булианом A .

Если $A\varphi B$ — отображение множеств или классов, образ $A \subset A$ обозначается $A\varphi$, а прообраз $B \subset B$ — $B\varphi^{-1}$.

Частично упорядоченные множества и классы называются ординалами. Отображение $A\varphi A$ ординала A называется увеличивающим, если $a\var$

Формулировки двойственных понятий и свойств в тексте приводятся в исключительных случаях. Для названий двойственных понятий используется приставка "ко", ссылка на дуальные к сформулированным утверждения осуществляется с помощью верхнего индекса "звездочка".

Параграфы делятся на пункты, каждый из которых содержит не более одного утверждения, формулируемого как "предложение". При ссылке на него указывается номер соответствующего пункта. Значок $\diamond$ свидетельствует о конце доказательства (или его отсутствии в тривиальном случае). Отметим одно отличие в терминологии по сравнению с [38]. Расслоенные произведения называются коамальгами, двойственно, корасслоенные произведения - амальгами.

§1 ПОЛУГРУППЫ И ГРУППЫ, АССОЦИИРОВАННЫЕ С МОРФИЗМАМИ

1.1. Для произвольных объектов A и B рассмотрим тернарное отношение, определяемое равенством $\alpha\varphi = \varphi\beta$, где $\alpha \in \text{End}A$, $\beta \in \text{End}B$ и $\varphi \in \text{Mor}(A, B)$. Будем называть α перестановочным слева эндоморфизмом, β перестановочным справа эндоморфизмом, (α, β) парой ассоциированных перестановочных эндоморфизмов относительно морфизма φ . Множество всех пар ассоциированных перестановочных эндоморфизмов определяет соответствие $\mathcal{E}(\varphi)$ на $\text{End}A \times \text{End}B$, а множество всех пар ассоциированных перестановочных эндоморфизмов - соответствие $A(\varphi)$ на $\text{Aut}A \times \text{Aut}B$.

1.2. Предложение

1.3. Стандартным образом определяются правые и левые образы подмножеств относительно соответствий $\mathcal{E}(\varphi)$ и $A(\varphi)$. Правый образ $A\varphi_e$ подмножества $A \subseteq \text{End}A$ относительно соответствия $\mathcal{E}(\varphi)$ состоит из всех $\beta \in \text{End}B$, для которых существуют $\alpha \in A$ такие, что $(\alpha, \beta) \in \mathcal{E}(\varphi)$. Таким образом получаем отображения

$$B(\text{End}A)\varphi_e B(\text{End}B), \quad B(\text{End}B)\varphi^e B(\text{End}A).$$

$$B(\text{Aut}A)\varphi_a B(\text{Aut}B), \quad B(\text{Aut}B)\varphi^a B(\text{Aut}A).$$

1.4. Предложение. Отображения φ_e, φ^e и φ_a, φ^a удовлетворяют следующим свойствам.

(а) Все они изотонны.

(б) Композиции $\varphi_e\varphi^e, \varphi^e\varphi_e$ и $\varphi_a\varphi^a, \varphi^a\varphi_a$ — увеличивающие отображения.

(в) Отображения φ_e, φ^e и φ_a, φ^a квазиобратны друг к другу.

(г) Отображения φ_e и φ^e переводят подполугруппы с единицей в подполугруппы с единицей, а отображения φ_a и φ^a переводят подгруппы в подгруппы.

Доказательство. Утверждения (а) и (б) справедливы для отображений, ассоциированных с произвольным соответствием, а (г) — для произвольных полугрупповых и групповых соответствий ([37], гл.1, §2). На булианах множеств подразумевается естественный порядок по включению. Что касается утверждения (в), включение $A\varphi_e\varphi^e\varphi_e \supseteq A\varphi_e$ следует из (а), (б), а обратное включение вытекает из свойства транзитивности соответствия $\mathcal{E}(\varphi) \diamond$.

1.5. Применив свойство (г) к тривиальному и тотальному подполуг

$S^\varphi = \{1_A\}\varphi_e$ — полугруппа правых изотропных для φ эндоморфизмов или изотропная полугруппа морфизма φ ;

$G^\varphi = \{1_A\}\varphi_a$ — группа правых изотропных для φ автоморфизмов или изотропная группа морфизма φ ;

Двойственные коаллотропные и коизотропные полугруппы и группы обозначаются аналогично с помощью нижнего индекса.

1.6. Предложение. Если φ — мономорфизм, то

(а) $\mathcal{E}(\varphi)$ — график гомоморфизма полугрупп $S^{(\varphi)}\varphi_e \text{End} A$ с образом $S_{(\varphi)}$;

(б) $A(\varphi)$ — график гомоморфизма групп $G^{(\varphi)}\varphi_a \text{Aut} A$ с образом $G_{(\varphi)}$ и ядром G^φ .

Доказательство. Если $\alpha_1\varphi = \alpha_2\varphi = \varphi\beta$, то $\alpha_1 = \alpha_2$ ввиду мономорфности φ , поэтому φ_e и φ_a — отображения. Гомоморфность этих отображений следует из того, что соответствия $\mathcal{E}(\varphi)$ и $A(\varphi)$ замкнуты относительно покомпонентного умножения. Утверждения об образах очевидны, а $\ker \varphi_a = G^\varphi$, потому что равенство $\varphi\beta = 1\varphi$ по определению изотропной группы означает, что $\$

Доказательство. Для произвольных эндоморфизмов $\beta \in G^{(\varphi)}$ и $b \in S^\varphi$

$$\varphi\beta b = \alpha\varphi b = \alpha\varphi = \varphi\beta,$$

откуда следует, что $\beta b \beta^{-1} \in S^\varphi$. Поэтому $\beta S^\varphi \beta^{-1} \subset S^\varphi$. Поменяв β на β^{-1} , получим обратное включение. Если $b \in G^\varphi$, то точно так же получается равенство $\beta^{-1} G^\varphi \beta = G^\varphi$. $\diamond$

Следствие. Нормализаторы полугруппы изотропии S^φ и группы изотропии G^φ в группе $\text{Aut } B$ содержат аллотропную группу $G^{(\varphi)}$. $\diamond$

Как будет показано в следующем параграфе, для определенного класса морфизмов верно и обратное включение.

В следующих пунктах исследуем поведение полугрупп и групп, ассоциированных с морфизмами $A\varphi B$, $B\psi C$, $A\chi C$ в том случае, когда χ является композицией φ и ψ .

1.8. Предложение. Если $\chi = \varphi\psi$ и ψ изоморфизм, то

$$S^{(\chi)} = \psi^{-1} S^{(\varphi)} \psi, \quad S^\chi = \psi^{-1} S^\varphi \psi, \$$

(2) Правые образы $(S_{(\varphi)} \cap S_{(\chi)}) \varphi_e$ и $(S_{(\varphi)} \cap S_{\chi}) \varphi_e$ содержат подполугруппы $S^{(\varphi)} \cap S_{(\psi)}$ и $S^{(\varphi)} \cap S_{\psi}$ соответственно. Аналогично $(G_{(\varphi)} \cap G_{(\chi)}) \varphi_a \geq G^{(\varphi)} \cap G_{(\psi)}$, $(G_{(\varphi)} \cap G_{\chi}) \varphi_a \geq G^{(\varphi)} \cap G_{\psi}$.

(3) Если ψ - мономорфизм, то $S_{\chi} = S_{\varphi}$, $G_{\chi} = G_{\varphi}$;

$$S_{(\psi)} \cap S^{\varphi} = (S^{(\psi)} \cap S^{\chi}) \psi_e, \quad G_{(\psi)} \cap G^{\varphi} = (G^{(\psi)} \cap G^{\chi}) \psi_a,$$

$$(S_{(\psi)} \cap S^{\varphi}) \psi_e = S^{(\psi)} \cap S^{\chi}, \quad (G_{(\psi)} \cap G^{\varphi}) \psi_a = G^{(\psi)} \cap G^{\chi}.$$

Прежде, чем перейти к доказательству, сделаем два замечания. Только утверждение п. (а) из вышеприведенных является самодвойственным. При переходе к двойственным утверждениям включения не меняются на противоположные.

Доказательство. Проведем детальное доказательство только для п. (а). Прежде всего, произведение соответствий для φ и ψ лежит в одноименном соответствии для χ , потому что из равенств $\alpha\varphi = \varphi\beta$ и $\beta\psi = \psi\gamma$ следует равен

(д) Если $\alpha\varphi\psi = \alpha\chi = \chi = \varphi\psi$, то, сокращая на мономорфизм ψ , получаем $\alpha\varphi = \varphi$. Поэтому справедливы включения, обратные к включениям п. (б)*, что доказывает первые два равенства п. (д).

Из равенств $\beta\psi = \psi\gamma$ и $\chi\gamma = \chi$ следует равенство $\varphi\beta\psi = \varphi\psi\gamma = \varphi\psi$ и после сокращения на мономорфизм ψ получаем $\varphi\beta = \varphi$. Поэтому справедливы включения, обратные ко второму и четвертому включениям п. (г), что доказывает вторую пару равенств п. (д). Третья пара равенств получается из второй, если учесть, что при мономорфном ψ ψ^e является гомоморфным отображением, а ψ_e задает его полный прообраз. $\diamond$

1.10. Предложение. Если $\chi = \varphi\psi$, то $G^{(\psi)} \cap G^\chi$ является подгруппой нормализатора G^ψ в G^χ .

Доказательство. Если $\gamma \in G^{(\psi)} \cap G^\chi$, то $\gamma \in G^\chi$ и $\psi\gamma = \beta\psi$ для некоторого автоморфизма β . Используя свойства 1.9.(д)* и 1.8, получаем $G^\psi = G^{\beta\psi} = G^{\psi\gamma} = \gamma^{-1}G^\psi\gamma$. Это означает, что γ принадлежит нормализатору G^ψ в G^χ . $\diamond$

Замечание. Единственным препятствием для справедливости аналога доказанного предложения, получаемого заменой $S^{$

следующим дополнительным свойством : коконус K, σ, K , однозначно определяемый условием $\sigma, \kappa = \kappa, i \in I$, плотный в смысле ([38]), то есть если для морфизмов $K\varphi_1 B$ и $K\varphi_2 B$ все композиции κ, φ_1 и κ, φ_2 совпадают, то $\varphi_1 = \varphi_2$.

1.12. Предложение. Пусть $K, \kappa, A, i \in I$ — произвольное семейство подобъектов, $K_0 \kappa_0 A$ содержит все κ_i . Тогда $S^{\kappa_0} \leq \bigcap_{i \in I} S^{\kappa_i}$ а $G^{\kappa_0} \leq \bigcap_{i \in I} G^{\kappa_i}$. Если κ_0 — композит подобъектов $\kappa_i, i \in I$, то справедливы и обратные включения, т.е.

$$S^{\kappa_0} = \bigcap_{i \in I} S^{\kappa_i}, \quad G^{\kappa_0} = \bigcap_{i \in I} G^{\kappa_i}.$$

Доказательство. Поскольку $\kappa_i \leq \kappa_0$, то согласно 1.9 (б) $G^{\kappa_i} \geq G^{\kappa_0}$, $S^{\kappa_i} \geq S^{\kappa_0}$, следовательно $\bigcap_{i \in I} G^{\kappa_i} \geq G^{\kappa_0}$, $\bigcap_{i \in I} S^{\kappa_i} \geq S^{\kappa_0}$. Чтобы доказать обратное включение, заметим, что для любого α из $\bigcap_{i \in I} S^{\kappa_i}$ выполняются равенства $\kappa_i \alpha = \kappa_i 1$ при всех $i \in I$, поэтому по определению композита $\kappa \alpha = \kappa 1$, т.е. $\alpha \in S^{\kappa}$.

морфизмов в объект A является предординалом с отношением делимости морфизмов (которое, очевидно, рефлексивно, транзитивно, но не антисимметрично), однако класс $\mathcal{P}(A)$ подобъектов объекта A уже является ординалом.

Сопоставление морфизму или подобъекту его изотропных полугруппы и группы определяет отображения

$$\bar{A}e_0\mathcal{P}(\text{End } A), \quad \bar{A}a_0\mathcal{P}(\text{Aut } A), \quad \mathcal{P}(A)e\mathcal{P}(\text{End } A), \quad \mathcal{P}(A)a\mathcal{P}(\text{Aut } A),$$

которые согласно предложению 1.9 (б) антиизотонны.

Если морфизм $K \kappa A$ имеет кообраз $K \kappa_c K_c$, то дополнительный к нему морфизм $K_c \kappa'_c A$ равенством $\kappa_c \kappa'_c = \kappa$ определяется однозначно и согласно предложению 1.9 (д)* имеет те же изотропные полугруппу и группу, что и морфизм κ . Сам кообраз морфизма $K \kappa A$ определяется однозначно как факторобъект объекта K . Если дополнительный к кообразу морфизм κ'_c мономорфен, то он задает подобъект объекта A .

Предположим, что все морфизмы $\kappa \in \bar{A}$ имеют кообраз и дополнительные к кообразам морфизмы мономорфны (это условие, в частности, выполняется, если все $\kappa \in \bar{A}$ разлагаются в компози

