Метод вычисления группы Галуа многочлена с рациональными коэффициентами

Николай Дуров

Июнь 2005

Содержание

Введение

Задача вычисления группы Галуа конкретного многочлена с рациональными коэффициентами как подгруппы группы подстановок корней многочлена рассматривалась Жорданом еще в XIX веке. Предложенный тогда метод «абсолютной резольвенты» решал эту задачу в принципе и позволял доказывать определенные теоретические результаты о группах Галуа многочленов, однако был совершенно непригоден для практического использования. Затем в течение долгого времени эта проблема не привлекала внимания исследователей.

Ситуация изменилась в 70-х годах XX века, когда появление и широкое распространение электронных вычислительных машин сделало возможным практическую реализацию алгоритмов вычисления группы Галуа. Эти алгоритмы используются как и по отдельности (например, для изучения подполей данного простого расширения поля рациональных чисел, для вычисления зависимостей между корнями одного или нескольких неприводимых многочленов, для построения многочленов, обладающих заданной группой Галуа, что представляет собой теоретический интерес в связи с обратной задачей теории Галуа), так и в составе других алгоритмов (например, в системах компьютерной алгебры для упрощения выражений с радикалами и алгебраическими числами или функциями, а также для нахождения решений уравнений в радикалах, что исторически послужило одной из основных причин для создания теории Галуа).

Поскольку классический метод абсолютной резольвенты был совершенно непригоден для практического использования, даже на компьютерах, рядом авторов были предложены новые алгоритмы нахождения группы Галуа. Первым из этих методов был метод *относительных резольвент*, предложенный в 1973 году в работе [20]; практически все последующие предложенные и реализованные алгоритмы представляют собой либо модификации метода относительных резольвент, либо сочетают его с другими методами — чаще всего с методом *линейных резольвент*, предложенным в работе [21] уже в 80-х годах. В отличие от метода относительных резольвент, метод линейных резольвент дает только частичную информацию об искомой группе Галуа; однако он более эффективен, и полученная в результате его применения информация позволяет существенно ускорить последующее применение метода относительных резольвент в той или иной его модификации.

Многие авторы отмечают возможность применения теоремы плотности Чеботарева [17] (см., напр., [21] или обзор [19]). Тем не менее обычно обсуждение не выходит за рамки упоминания о том, что теорема плотности Чеботарева обычно позволяет быстро определить, что группа Галуа данного многочлена является симметрической или знакопеременной, и что практическое применение теоремы плотности Чеботарева для получения дальнейшей информации о группе Галуа, к сожалению, крайне неэффективно.

Целью данной работы является построение и обоснование некоторого эффективного метода вычисления группы Галуа многочлена с рациональными коэффициентами, основанного на теореме плотности Чеботарева. Такой метод естественным образом носит вероятностный характер; в связи с этим будет изучено, каким образом можно добиться того, чтобы вероятность ошибки была меньше любого наперед заданного числа. Впрочем, в предположении истинности обобщенной гипотезы Римана наш метод удается сделать в определенном смысле точным (см. 5.4).

Конечно же, теорема плотности Чеботарева может дать информацию только о количестве подстановок каждого из циклических типов, входящих в искомую группу Галуа G. Мы будем называть этот набор данных *виртуальной подгруппой*, соответствующей G. Во многих случаях виртуальная подгруппа однозначно определяет соответствующую подгруппу с точностью до сопряжения; даже если это не так, большое количество информации может быть извлечено из знания виртуальной подгруппы. Самым простым примером служит порядок искомой группы Галуа, однако мы получим хорошие *необходимые* условия для того, чтобы одна подгруппа содержалась в другой или чтобы подгруппа была разрешимой, в терминах соответствующих виртуальных подгрупп.

Кроме того, мы не хотим ограничиваться рассмотрением неприводимых многочленов (что соответствует рассмотрению только тех групп Галуа, которые являются транзитивными подгруппами симметрической группы $\mathfrak{S}_n$), как это делалось до сих пор: несмотря на то, что метод относительных резольвент формально годится для произвольных (сепарабельных) многочленов степени n, как это было отмечено еще в работе [20], его применение для приводимых многочленов требует предварительного знания решетки подгрупп симметрической группы $\mathfrak{S}_n$ и, как следствие, вычисления большого количества относительных резольвент. В связи с этим существующие реализации ограничиваются случаем неприводимого многочлена (т.е. транзитивных групп подстановок), поскольку классификация транзитивных подгрупп симметрической группы $\mathfrak{S}_n$ хорошо известна для $n \leq 31$.

Хочется подчеркнуть, что задача нахождения группы Галуа приводимого многочлена F представляет самостоятельный интерес и вовсе не сводится, как можно было бы предположить, исключительно к изучению групп Галуа неприводимых сомножителей многочлена F.

Расммотрим следующий пример. Предположим, что $F = F_1F_2$ является произведением различных неприводимых многочленов F_1 и F_2, и G_1, G_2, G — группы Галуа мночленов F_1, F_2 и F соответственно, а K_1 и K_2 — поля разложений многочленов F_1 и F_2 над полем рациональных чисел $\mathbb{Q}$ (рассматриваемые как подполя в $\bar{\mathbb{Q}}$). Тогда, как несложно видеть, порядок G равен произведению порядков G_1 и G_2 в том и только том случае, когда поля K_1 и K_2 линейно разделены над $\mathbb{Q}$ (и тогда $G \cong G_1 \times G_2$). С другой стороны, порядок G равен порядку G_1 в том и только том случае, если K_2 содержится в поле K_1, и знание G как группы подстановок корней позволяет определить гомоморфизм группы Галуа G_1 в группу G_2, определенный ограничением на подполе K_1. Кроме того, отсюда видно, что $K_1 = K_2$ в том и только том случае, если порядки групп G, G_1 и G_2 равны.

Приведенный выше пример показывает, что даже знание порядков групп Галуа приводимых многочленов дает много интересной информации о полях разложения многочленов. Отметим, что развиваемый в настоящей работе метод позволяет определять как минимум порядок группы Галуа многочленов степени ≤ 11 (даже если он оказывается не в состоянии полностью определить искомую группу Галуа) и в то же время очень эффективен, и потому он пригоден для практического решения задач, подобных описанным выше.

Как уже упоминалось ранее, метод относительных резольвент требует для своего использования знания решетки транзитивных подгрупп симметрической группы $\mathfrak{S}_n$; это в действительности послужило одной из основных причин для многочисленных исследований классификации транзитивных подгрупп $\mathfrak{S}_n$.

Оказывается, что для того, чтобы сделать эффективным метод, основанный на теореме плотности Чеботарева, необходимо заранее построить список всех виртуальных подгрупп симметрической группы $\mathfrak{S}_n$. В связи с этим существенная часть работы посвящена изложению и обоснованию эффективных методов перечисления виртуальных подгрупп симметрической группы. Эти методы были реализованы автором на компьютере, что в результате позволило построить списки всех виртуальных подгрупп $\mathfrak{S}_n$ при $n \leq 11$, для чего понадобилось 55 часов работы компьютера Pentium-IV (в полученном списке оказалось 11800 виртуальных подгрупп, из них 7213 соответствуют $n = 11$); при этом для вычисления таблиц при $n \leq 10$ потребовалось всего лишь семь минут работы. Поскольку эти таблицы требуется вычислить лишь однажды, нам представляется, что с помощью предлагаемых методов можно вычислить за приемлемое время эти таблицы для $n \leq 12$; для бóльших значений n, по всей видимости, потребуется дальнейшее развитие этих методов.

Итак, предлагаемая работа содержит:

1) Описание предлагаемого метода (названного нами *методом подсчета циклических типов*) вычисления группы Галуа как виртуальной подгруппы симметрической группы и необходимых подробностей его реализации, из которых наиболее существенными представляются эффективные методы нахождения степеней неприводимых сомножителей многочлена над простым полем, а также методы статистической обработки результатов.

2) Методы эффективного построения таблиц виртуальных подгрупп симметрической подгруппы. Для этого на кольце виртуальных характеров симметрической группы в дополнение к стандартным операциям мы вводим новые «τ-операции» и вводим τ-критерий, обычно позволяющий быстро отсекать «несущественные» виртуальные подгруппы, т.е. наборы данных, которые не соответствуют никакой «настоящей» подгруппе.

3) Методы получения информации о подгруппе по соответствующей виртуальной подгруппе. В частности, мы рассмотрим необходимые условия для того, чтобы подгруппа была разрешимой или содержалась в другой подгруппе. Здесь ключевую роль снова играет τ-критерий.

4) Краткий обзор существующих методов вычисления группы Галуа с целью их последующего сравнения с предлагаемым методом и обсуждения целесообразности их совместного применения.

Кроме того, в приложении приведены таблицы виртуальных подгрупп для $n \leq 6$ и примеры вычисления групп Галуа.

В связи с вышеизложенным работа построена следующим образом.

В первой главе приводится краткий обзор других методов в той мере, в какой это необходимо в дальнейшем для сравнения, а также излагается общая идея предлагаемого метода, который мы в дальнейшем называем *методом подсчета циклических типов*.

Во второй главе изучаются границы применимости методов, основанных на теореме плотности Чеботарева: следует ожидать, что в действительности поле рациональных чисел можно заменить любым полем, конечно порожденным над своим простым подполем. Кроме того, в этой главе приводится нужная нам формулировка теоремы плотности Чеботарева и объясняется, как она выводится из обычной.

В третьей главе систематически изучаются кольца характеров конечных и проконечных групп и вводятся τ-операции, а также τ-критерий, играющий ключевую роль во всей работе. Кроме того, в начальной части этой главы излагаются на языке теории категорий нужные в дальнейшем свойства операторных множеств и представлений групп. Это позволяет существенно упростить изложение последующего материала.

Затем в четвертой главе построенная общая теория применяется к симметрическим группам и развиваются три метода, совокупное применение которых позволяет эффективно строить таблицы виртуальных подгрупп симметрической группы. Кроме того, обсуждаются методы, позволяющие получать информацию о подгруппах, исходя из соответствующих виртуальных подгрупп.

В пятой главе обсуждаются моменты, существенные для эффективной реализации предлагаемого метода вычисления группы Галуа. В первых трех разделах этой главы мы рассматриваем два метода нахождения степеней неприводимых сомножителей многочлена над конечным полем. Интересным представляется тот факт, что предлагаемые методы не требуют нахождения самих неприводимых сомножителей и потому работают быстрее, чем обычные алгоритмы разложения многочленов на множители. В последнем разделе обсуждается метод статистического анализа результатов, основанный на сравнении нашей задачи с похожей статистической задачей, и даются практические рекомендации. Кроме того, при этом обсуждается, каким образом можно сделать наш метод точным в предположении истинности обобщенной гипотезы Римана.

В заключении производится сравнение нашего метода с другими методами и даются рекомендации об их возможном совместном применении.

Приложение содержит примеры вычисления группы Галуа, а также таблицы виртуальных подгрупп $\mathfrak{S}_n$ при $n \leq 6$, вычисленные методами, изложенными в основном тексте.

Новыми в настоящей работе представляются τ-критерий и все основанные на нем критерии и методы, включая методы перечисления виртуальных подгрупп симметрической группы, а также применение предложенного статистического анализа к данной задаче. Сами τ-операции, определенные нами на любом λ-кольце, также представляются новыми. Кроме того, автору не удалось обнаружить в литературе в явном виде изложенные методы определения степеней неприводимых сомножителей многочлена над простым полем, не требующие нахождения самого разложения на множители, хотя они, безусловно, являются вариациями на тему хорошо известного алгоритма Берлекэмпа разложения на множители многочленов над конечным полем.

Основные результаты, излагаемые в этой работе, опубликованы автором в [5] и [6].

1 Обзор методов вычисления группы Галуа

Предлагаемый далее обзор отмечает лишь основные идеи методов без обсуждения их возможных модификаций и оптимизаций в той мере, в какой это необходимо для последующего сравнения с нашим методом. Дополнительную информацию можно найти, например, в обзоре [19].

Задача нахождения группы Галуа G конкретного унитарного многочлена $F \in k[T]$ степени n с коэффициентами в поле k рассматривалась Жорданом еще в XIX веке. В его методе, как и во многих последующих, многочлен F обычно предполагался неприводимым; это следует иметь в виду при чтении дальнейшего, хотя большинство рассматриваемых методов в действительности годятся для произвольного сепарабельного F, не обязательно неприводимого.

1.1 Классический метод абсолютной резольвенты

В работах Жордана [18] появился первый метод вычисления группы Галуа G как подгруппы симметрической группы $\mathfrak{S}_n$; в течение очень долгого времени (до 70-х годов XX века) этот метод оставался единственным общим методом вычисления группы Галуа.

Основная идея этого метода заключается в сведении задачи нахождения подгруппы $G \subset \mathfrak{S}_n$ к задаче разложения на множители некоторой «резольвенты» R — многочлена степени $n!$ от $n+1$ переменной с коэффициентами в k. Если обозначить через α_1, α_2, …, α_n корни многочлена $F(T)$, то резольвенту можно определить формулой

$$R(T, X_1, \dots, X_n) = \prod_{\sigma \in \mathfrak{S}_n} \left(T - \sum_{i=1}^{n} \alpha_{\sigma_i} X_i \right) \quad . \tag{1.1.0.1}$$

Конечно же, нет необходимости для вычисления резольвенты R искать сами корни α_i: поскольку правая часть (1.1.0.1) является симметрическим многочленом от корней α_i, она выражается через основные симметрические функции от корней, т.е. через коэффициенты многочлена F. Уже на этом этапе видно, что на практике вычисление резольвенты при $n \geq 5$ довольно трудоемко.

Затем следует разложить $R(T, X_1, \dots, X_n)$ на неприводимые множители над полем k; если R_1 — один из них, то подгруппа $G \subset \mathfrak{S}_n$ определяется как множество тех подстановок переменных X_i, которые сохраняют многочлен R_1. Если нам дана какая-то нумерация корней α_i (например, заданием комплексных приближений), то мы можем определить G как группу подстановок корней, занумерованных указанным образом: достаточно взять в качестве R_1 неприводимый сомножитель R, в который входит $T - \sum_{1 \leq i \leq n} \alpha_i X_i$. В противном случае R_1 выбирается произвольно, что соответствует произвольной нумерации корней; тогда подгруппа $G \subset \mathfrak{S}_n$ определена с точностью до сопряжения.

Отметим, что тем самым в принципе задача нахождения группы Галуа многочлена с коэффициентами в поле k сведена к задаче разложения на множители многочлена от нескольких переменных с коэффициентами в k. Поскольку эта задача, в свою очередь, сводится к задаче разложения многочлена от одной переменной (вместо $H(X_1, X_2, \dots, X_n)$ достаточно разложить на множители $H(T, T^d, \dots, T^{d^n})$, где d — натуральное число, большее степени H; этот прием принадлежит Кронекеру), мы видим, что в принципе мы умеем находить группу Галуа многочленов в точности над теми полями, над которыми нам известен алгоритм разложения на множители многочленов от одной переменной.

В классическом варианте этого алгоритма предлагалось воспользоваться методом Кронекера разложения на множители многочленов от нескольких переменных с рациональными коэффициентами (см. изложение этого метода, равно как и описанного только что алгоритм вычисления группы Галуа, в книге [4]). Конечно же, это делало этот алгоритм совершенно непригодным для практического использования, хотя и давало возможность доказывать определенные теоретические факты о группе Галуа.

Один из первых таких фактов заключается в том, что группа Галуа редукции многочлена по простому модулю p, не делящему дискриминант многочлена F, вкладывается в группу подстановок G (см. [4], § 66). Иначе говоря, если редукция F_p раскладывается в произведение неприводимых многочленов степеней λ_1, λ_2, …, λ_r, то G содержит подстановку циклического типа $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_r)$ (т.е. подстановку с указанными длинами циклов).

Это позволяет строить примеры многочленов, группа Галуа которых является симметрической: так, в [4], § 66 рассматривается многочлен $F(T) = T^5 - T - 1$. Его редукция по модулю 3 неприводима, откуда следует неприводимость многочлена F и существование цикла длины 5 в его группе Галуа; редукция же F по модулю 2 раскладывается в произведение многочленов степеней 3 и 2, откуда следует наличие

подстановки циклического типа $3+2$. Несложно видеть, что единственной подгруппой $\mathfrak{S}_5$, содержащей подстановки циклических типов 5 и $3+2$, является вся $\mathfrak{S}_5$; тем самым доказано, что группа Галуа T^5-T-1 является симметрической.

В действительности в том случае, если группа Галуа неприводимого многочлена F является симметрической или знакопеременной, обычно достаточно рассмотрения редукций по модулю нескольких первых простых чисел, чтобы найти циклические типы подстановок, которые не могут встречаться ни в какой подгруппе $\mathfrak{S}_n$, отличной от $\mathfrak{S}_n$ и от $\mathfrak{A}_n$; поскольку необходимым и достаточным условием для того, чтобы G содержалась в знакопеременной группе $\mathfrak{A}_n$, является наличие в основном поле k квадратного корня из дискриминанта $\mathrm{disc}(F)$ многочлена F, это означает, что обычно мы можем довольно быстро определить, что группа Галуа данного многочлена является симметрической или знакопеременной.

Предыдущее утверждение можно сделать математически строгим, если воспользоваться теоремой плотности Чеботарева (см. [17]); это наблюдение делалось многими авторами, которые также отмечали, что для других групп Галуа теорема Чеботарева сама по себе, к сожалению, не дает нужной информации за приемлемое время, на чем обсуждение возможного применения теоремы плотности Чеботарева обычно и заканчивалось. Поскольку данная работа как раз и посвящена построению эффективного метода определения группы Галуа на основе теоремы плотности Чеботарева, мы не будем сейчас обсуждать подробнее эту проблему.

1.2 Метод относительных резольвент

Дальнейшее развитие проблема вычисления группы Галуа получила около тридцати-сорока лет назад, что было связано с появлением и распространением электронных компьютеров.

Одним из первых нововведений было использование появившихся в то время более эффективных алгоритмов разложения на множители многочленов с целыми коэффициентами, основанных на разложении редукции многочлена по простому модулю p с помощью алгоритма Берлекэмпа с последующим p-адическим подъемом полученного разложения до разложения по модулю p^N для достаточно большого N и группировкой сомножителей в полученном таким образом разложении. Однако даже эти методы разложения многочленов на множители были не в состоянии справиться с резольвентой (1.1.0.1) (которую мы теперь будем называть *классической* или *абсолютной*), не говоря уже о том, что по-прежнему оставалась проблема вычисления самой резольвенты.

В связи с этим в ряде работ (первой из которых, по всей видимости, была работа [20]) были предложены методы нахождения группы Галуа, основанные на нахождении *относительных резольвент*.

Ввиду важности этого понятия приведем основные определения (которые можно найти, например, в работе [20]). Для простоты мы будем предполагать, что $F(T)$ — унитарный многочлен с целыми коэффициентами, хотя в различных модификациях этого метода от этого ограничения часто можно избавиться.

Итак, зафиксируем степень n многочлена F, и будем предполагать, что F унитарен, неприводим и с целыми коэффициентами (последнего можно всегда добиться, заменив $F(T)$ на $F(dT)$ для подходящего целого $d>0$). Обозначим через α_1, α_2, …, α_n корни многочлена $F(T)$. В зависимости от варианта метода α_i рассматриваются либо как формальные корни $F(T)$ в поле $\bar{\mathbb{Q}}$, либо как комплексные корни (заданные с достаточно большой точностью), либо как элементы некоторого неразветвленного расширения поля p-адических чисел $\mathbb{Q}_p$ (тогда α_i задаются своими p-адическими приближениями). В последних двух случаях группа Галуа ищется как группа подстановок корней, упорядоченных указанным образом.

Пусть $A=\mathbb{Z}[X_1,\dots,X_n]$ — кольцо многочленов от n переменных с целыми коэффициентами, $K=\mathbb{Q}(X_1,\dots,X_n)$ — поле частных A. Определим (левое) действие симметрической группы $\mathfrak{S}_n$ на A и на K по правилу

$$(\sigma\cdot F)(X_1,\dots,X_n)=F(X_{\sigma^{-1}(1)},\dots,X_{\sigma^{-1}(n)}) \quad ,$$

где σ — произвольная подстановка из $\mathfrak{S}_n$, а F — произвольный многочлен (соотв. рациональная функция) из A (соотв. из K).

Для любой подгруппы $G\subset\mathfrak{S}_n$ обозначим, как обычно, через A^G (соотв. K^G) множество элементов A (соотв. K), сохраняемых всеми подстановками σ из G. Хорошо известно, что A^G — подкольцо в A, K^G — его поле частных, и степень $[K:K^G]$ равна порядку $|G|$ подгруппы G.

Отметим, что для любой подгруппы $G\subset\mathfrak{S}_n$ существует многочлен $P\in A$, стабилизатор которого равен в точности G: достаточно взять, например, $P=\sum_{\sigma\in G}\sigma\cdot(X_1X_2^2\cdots X_n^n)$.

Определение 1.2.1 *Пусть $F(T)$ — унитарный многочлен степени n с целыми коэффициентами, α_1, $\alpha_2, \ldots, \alpha_n$ — его корни. Пусть $H \subset G \subset \mathfrak{S}_n$ — подгруппы симметрической группы $\mathfrak{S}_n$, и пусть $P \in A$ — многочлен, стабилизатор которого в точности равен H. Тогда* относительная резольвента $Q_{(G,H)}(T)$ — *это многочлен степени $(G:H)$ с целыми алгебраическими коэффициентами, определенный формулой*

$$Q_{(G,H)}(T) = \prod_{\sigma \in G/H} \big(T - (\sigma \cdot P)(\alpha_1, \ldots, \alpha_n)\big) \quad .$$

Отметим, что относительная резольвента зависит от выбора многочлена P, хотя это обычно не отражается на записи.

Замечание 1.2.1.1 Несложно видеть, что если группа Галуа Γ многочлена F содержится в G, то коэффициенты $Q_{(G,H)}$ являются целыми рациональными числами.

Важность относительных резольвент обусловлена следующей несложной теоремой (см., напр., [20], 5):

Теорема 1.2.2 *В обозначениях предыдущего определения и замечания предположим, что Γ содержится в G. Предположим, кроме того, что $P(\alpha_1, \ldots, \alpha_n)$ является простым корнем $Q_{(G,H)}(T)$. Тогда $\Gamma \subset H$ в том и только том случае, если число $P(\alpha_1, \ldots, \alpha_n)$ является целым рациональным.*

Предположим, что мы умеем находить коэффициенты относительных резольвент $Q_{(G,H)}$ в случае $\Gamma \subset G$, и предположим, что у нас есть полная информация о решетке подгрупп симметрической группы $\mathfrak{S}_n$ (если, как это обычно делается, ограничиться случаем неприводимого F, то достаточно рассматривать транзитивные подгруппы $\mathfrak{S}_n$).

Далее все алгоритмы, основанные на рассмотрении относительных резольвент, поступают следующим образом. Перед очередным шагом алгоритма уже известна некоторая подгруппа $G \subset \mathfrak{S}_n$, заведомо содержащая искомую группу Галуа Γ (изначально можно взять $G = \mathfrak{S}_n$). Пусть $\{H_j\}$ — набор максимальных подгрупп в G, отличных от самой G (достаточно брать по одному представителю из класса G-сопряженных подгрупп; если F неприводим, рассматриваются только транзитивные H_j). Для каждой H_j вычислим относительную резольвенту $Q_{(H_j,G)}$ для подходящего многочлена P и проверим наличие у нее целых рациональных корней. Если $P(\alpha_{\sigma_1}, \ldots, \alpha_{\sigma_n})$ является простым целым рациональным корнем $Q_{(H_j,G)}$ для некоторой подстановки $\sigma \in G$, то Γ содержится в $\sigma^{-1} H_j \sigma$; перенумеровав корни, можно считать, что $\Gamma \subset H_j$, и на этом шаг алгоритма заканчивается. Если ни одна из резольвент $Q_{(H_j,G)}$ не имеет рациональных корней, то группа Γ должна совпадать с G, и на этом выполнение алгоритма заканчивается. Наконец, может так случиться, что у одной из резольвент $Q_{(H_j,G)}$ имеются кратные корни; в этом случае обычно предлагается сделать преобразование Чирнгаузена и попробовать снова.

Из приведенного выше описания видно, что методы, основанные на вычислении относительных резольвент, требуют знания решетки подгрупп в $\mathfrak{S}_n$. По этой причине все существующие реализации рассматривают только транзитивные подгруппы $\mathfrak{S}_n$ (что соответствует случаю неприводимого многочлена F), классификация которых известна вплоть до $n \leq 31$.

Разные варианты метода относительных резольвент отличаются в основном способом вычисления коэффициентов относительных резольвент и поиска их рациональных корней, а также набором используемых оптимизаций, которые позволяют уменьшить число рассматриваемых резольвент (например, если на одном из предыдущих этапов мы уже выяснили, что $\Gamma \not\subset H_j$, то на очередном этапе можно уже не проверять H'_k, содержащиеся в H_j).

Изначально в [20] был предложен метод вычисления относительных резольвент, основанный на подстановке в определение резольвенты численных значений комплексных корней α_i, вычисленных с высокой точностью, с последующим округлением полученных коэффициентов резольвенты до ближайших целых чисел. Этот же прием можно использовать для поиска целочисленных корней резольвент: надо округлять $P(\alpha_{\sigma_1}, \ldots, \alpha_{\sigma_n})$ до ближайших целых и подставлять полученные значения в резольвенту.

К сожалению, при таком подходе быстро накапливаются ошибки, и точность комплексных приближений к корням, необходимая для получения гарантированных результатов, оказывается слишком высокой. В связи с этим рядом авторов (см., например, [22], [23]) были предложены и изучены p-адические варианты метода относительных резольвент. В этом случае корни α_i ищутся в некотором конечном

неразветвленном расширении поля p-адических чисел $\mathbb{Q}_p$, где p — простое число, не делящее дискриминант многочлена F. Благодаря ультраметрическому неравенству треугольника ошибки округления поддаются точному учету, что позволяет заранее оценить необходимую точность и в дальнейшем производить все вычисления фактически в $\mathbb{Z}/p^N\mathbb{Z}$ (точнее, в некоторой конечной сепарабельной алгебре над этим кольцом); см. [22].

Кроме того, существует алгебраический подход к вычислению относительных резольвент, для применения которого для каждой подгруппы G строится некоторая фундаментальная система инвариантов (т.е. конечное множество многочленов, порождающих A^G как $\mathbb{Z}$-алгебру или, в других вариантах, порождающих $K^G/\mathbb{Q}$ как расширение полей) и затем коэффициенты резольвент выражаются через эти инварианты. Тогда на каждом шаге алгоритма можно найти коэффициенты нужных резольвент, если уже известны значения инвариантов группы G на корнях α_i; однако в том случае, когда мы находим подгруппу $H_j \subset G$, содержащую искомую группу Галуа, нам следует позаботиться о вычислении значений H_j-инвариантов исходя из уже известных значений G-инвариантов, а также из значения $F(\alpha_1, \ldots, \alpha_n)$.

В действительности этот подход требует большего объема вычислений, чем p-адические методы. Однако он заслуживает упоминания хотя бы потому, что он работает над произвольным полем k, над которым у нас есть алгоритм нахождения корней многочлена от одной переменной.

На этом мы завершим обзор метода относительных резольвент, поскольку его свойства нам нужны только для сравнения его с методом, развиваемым в настоящей работе. Дальнейшие подробности можно найти, например, в обзоре [19]. Укажем лишь, что на настоящий момент метод относительных резольвент является единственным методом, позволяющим гарантированно находить группу Галуа неприводимого многочлена степени $n \leq 20$ как группу подстановок корней, и потому все используемые на практике алгоритмы вычисления группы Галуа либо являются вариантами метода относительных резольвент (например, метод, используемый в системе `pari 2.0`), либо содержат его как одну из компонент (обычно вместе с методом линейных резольвент, как в системе `MAGMA`).

1.3 Метод линейных резольвент

Метод линейных резольвент был впервые предложен в работе [21]. Он заключается в рассмотрении разложений на множители линейных резольвент, определенных следующим образом.

Определение 1.3.1 *Пусть $F(T)$ — (неприводимый) унитарный многочлен степени n с коэффициентами в поле k, $\alpha_1, \ldots, \alpha_n$ — его корни. Пусть $e_1 \geq e_2 \geq \cdots e_r > 0$ — целые числа, $1 \leq r \leq n$. Обозначим через L линейный многочлен*

$$L(X_1, X_2, \ldots, X_n) = e_1X_1 + e_2X_2 + \cdots + e_rX_r \quad ,$$

и пусть $G := \mathrm{Stab}_{\mathfrak{S}_n}(L)$ — группа подстановок, сохраняющих L. Определим линейную резольвенту *$R(L, F)$ следующим образом:*

$$R(L, F) = \prod_{\sigma \in \mathfrak{S}_n/G} \big(T - (\sigma \cdot L)(\alpha_1, \ldots, \alpha_n)\big) \quad .$$

Иначе говоря, линейная резольвента — это относительная резольвента $Q_{(G,\mathfrak{S}_n)}$ (см. 1.2.1), построенная исходя из линейного многочлена L.

Отметим, что линейная резольвента, вообще говоря, не является многочленом первой степени, как это можно было бы предположить исходя из названия.

Предположим теперь, что все корни $R(L, F)$ различны (иначе, как и в предыдущем разделе, следует произвести преобразование Чирнгаузена).

Предложение 1.3.2 *Предположим, что все корни $R(L, F)$ различны. Тогда набор длин орбит множества $\mathfrak{S}_n/G$ относительно действия группы Галуа $\Gamma \subset \mathfrak{S}_n$ многочлена F совпадает с набором степеней неприводимых сомножителей линейной резольвенты $R(L, F)$. В частности, количество Γ-орбит на $\mathfrak{S}_n/G$ равно количеству неприводимых сомножителей $R(L, F)$.*

Пусть теперь X — n-элементное множество, на котором естественным образом действует наша группа $\mathfrak{S}_n$; можно считать, что $X = \{1, 2, \ldots, n\}$, или, что лучше, что X есть множество корней многочлена F: $X = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$.

Для любого $r \geq 1$ обозначим через $\binom{X}{r}$ или через $\tau^r(X)$ (последнее обозначение вводится далее в 3.5.2) множество r-элементных подмножеств множества X с естественным действием групп $\mathfrak{S}_n$ и $\Gamma \subset \mathfrak{S}_n$, а через $X^{\underline{r}}$ или через $\tau^{(1^r)}(X)$ (это обозначение вводится в 3.6.6.3) множество упорядоченных наборов из r различных элементов множества X с естественным действием $\mathfrak{S}_n$ и Γ.

Предыдущее предложение позволяет вычислить количество и длины Γ-орбит на множествах $\tau^r(X)$ и $\tau^{(1^r)}(X)$: достаточно положить в определении линейной резольвенты $e_1 = e_2 = \cdots = e_r = 1$ или взять все e_i попарно различными.

В работе [21] отмечается, что для неприводимых многочленов F степени $n \leq 7$ знание этой информации для $\tau^2(X)$, $\tau^3(X)$ и $\tau^{(1^2)}(X)$, вместе со знанием того, является ли $\mathrm{disc}(F)$ точным квадратом, позволяет различить (с точностью до сопряжения) все транзитивные подгруппы $\Gamma \subset \mathfrak{S}_n$, за исключением трех пар подгрупп в $\mathfrak{S}_6$; эти случаи в работе [21] предлагается различать построением дополнительной относительной резольвенты.

Вычисление и разложение на множители линейных резольвент сопряжено с теми же трудностями, что и вычисление относительных резольвент, рассмотренных в предыдущем разделе; применяются в основном те же классы методов. Поскольку для больших значений n и r линейные резольвенты являются многочленами очень высоких степеней, обычно стараются обойтись как можно меньшими значениями r.

На практике метод линейных резольвент обычно используется перед применением метода относительных резольвент для того, чтобы собрать предварительную информацию о возможных в данном случае группах Γ и тем самым сильно уменьшить количество относительных резольвент, необходимых для вычисления группы Галуа.

В дальнейшем мы покажем, что информацию, полученную по теореме плотности Чеботареве методом, предлагаемом в настоящей работе, можно использовать для определения количества Γ-орбит множеств $\tau^r(X)$ и $\tau^{(1^r)}(X)$, равно как и более общих множеств $\tau^{(\nu)}(X)$ (см. 3.6.6.3). Кроме того, наш метод позволяет получать и другую дополнительную информацию о подгруппе Γ и часто определять ее полностью (особенно если она транзитивна); тем самым наш метод может практически полностью заменить применение метода линейной резольвенты. Мы вернемся к этому вопросу в одном из заключительных разделов работы.

1.4 Метод подсчета циклических типов

Изложим теперь основную идею предлагаемого в настоящей работе метода определения группы Галуа, который мы будем для краткости называть *методом подсчета циклических типов*. Как и для остальных алгоритмов нахождения группы Галуа, основная идея крайне проста, однако для построения эффективной реализации требуется много дополнительных исследований.

Пусть $F \in \mathbb{Q}[T]$ — унитарный сепарабельный многочлен (не обязательно неприводимый) степени n. Возьмем произвольное простое число p. Может случиться, что p делит один из знаменателей коэффициентов F, или что p делит дискриминант F; мы будем называть такие простые числа *исключительными*. Поскольку множество исключительных простых чисел конечно, можно предполагать, что p не является исключительным (оно *регулярно*, как мы будем говорить), по крайней мере, если мы обладаем способом проверки исключительности простого числа p.

Итак, предположим, что p регулярно. Тогда редукция $F_p(T)$ многочлена $F(T)$ по модулю p является сепарабельным многочленом, и мы можем рассмотреть его разложение на неприводимые сомножители: $F_p = G_1 \cdot G_2 \cdots G_r$, где все G_i различны. Рассмотрим степени λ_i этих сомножителей. Можно предполагать, что $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r > 0$, так что мы получаем разбиение на слагаемые $\lambda^{(p)} = \lambda = (\lambda_1, \lambda_2, ...)$ натурального числа n (*разбиение* натурального числа n — это невозрастающая последовательность $\lambda = (\lambda_i)_{i \geq 1}$ целых неотрицательных чисел, такая, что $n = \sum_{i \geq 1} \lambda_i$; см. 4.1.2).

Возьмем теперь N различных регулярных простых чисел, вычислим для каждого из них разбиение $\lambda^{(p)}$ и положим $m_\lambda := \langle$число простых p, для которых $\lambda^{(p)} = \lambda\rangle$. Что можно сказать о распределении m_λ и о частотах m_λ/N при $N \to \infty$?

Ответ на этот вопрос доставляется следующей *теоремой плотности Чеботарева* (см. 2.2.4 и 2.3):

Теорема 1.4.1 *Пусть $\Gamma \subset \mathfrak{S}_n$ — группа Галуа многочлена $F(T)$ (для произвольно выбранной нумерации корней). Обозначим через $\mathcal{C}_\lambda$ множество подстановок $\sigma \in \mathfrak{S}_n$ циклического типа (т.е. со множеством длин циклов) λ. Тогда плотность множества простых p, для которых $\lambda^{(p)} = \lambda$, равна $|\Gamma \cap \mathcal{C}_\lambda|/|\Gamma|$, где через $|X|$ мы обозначаем количество элементов конечного множества X.*

Замечание 1.4.2 Множества $\mathcal{C}_\lambda$ являются в точности классами сопряженных элементов симметрической группы $\mathfrak{S}_n$.

Замечание 1.4.3 Эта теорема — не совсем теорема плотности Чеботарева, но легко из нее выводится. Этот вывод будет обсуждаться в следующей главе.

Итак, обозначим для каждой подгруппы $H \subset \mathfrak{S}_n$ через $p_H\colon \operatorname{part}_n \to [0,1]$ функцию, определенную формулой $p_H(\lambda) := |H \cap \mathcal{C}_\lambda|/|H|$ (здесь part_n — множество всех разбиений на слагаемые натурального числа n). Мы будем называть такие функции *виртуальными подгруппами* группы $\mathfrak{S}_n$. Сопряженным подгруппам соответствует одна и та же виртуальная подгруппа $\mathfrak{S}_n$; может случиться, что виртуальной подгруппе соответствует более одного класса сопряженных подгрупп. Наш алгоритм не будет различать такие подгруппы, так что мы ограничимся нахождением виртуальной подгруппы, определенной группой Галуа многочлена $F(T)$, и определением (по крайней мере, для небольших n) для каждой виртуальной подгруппы соответствующих «настоящих» подгрупп. Кроме того, мы покажем, что знание виртуальной подгруппы само по себе дает много информации о группе Галуа.

В разделе 5.4 будет обсуждаться, как определить эту виртуальную подгруппу с любым заданным «уровнем достоверности»; как обычно, при увеличении числа «экспериментов» (т.е. проанализированных простых чисел p) вероятность ошибки экспоненциально убывает. Кроме того, в том случае, если мы принимаем обобщенную гипотезу Римана, оказывается возможным *точное* определение интересующей нас виртуальной подгруппы.

Оказывается, что для эффективного применения этого метода необходимо предварительное построение таблицы виртуальных подгрупп — в противном случае метод оказывается практически неприменим уже для $n \geq 5$. Большая часть дальнейших рассмотрений будет как раз посвящена проблеме эффективного построения списка виртуальных подгрупп симметрической группы; здесь ключевую роль сыграют τ-операции и τ-критерий в его различных модификациях.

Кроме того, возникает проблема извлечения максимального количества информации из виртуальных подгрупп, соответствующих настоящим подгруппам. Так, хотелось бы определять, какие подгруппы содержатся в других, исходя из соответствующих виртуальных подгрупп, или проверять, является ли данная подгруппа разрешимой, исходя опять-таки исключительно из информации о соответствующей виртуальной подгруппе. Мы в дальнейшем увидим, что τ-критерий дает хорошие *необходимые* условия для разрешимости подгрупп, равно как и для проверки того, лежит ли одна подгруппа в другой.

Отметим еще раз, что сама возможность применения теоремы Чеботарева к задаче определения группы Галуа обсуждается многими авторами, однако обычно рассмотрение ограничивается упоминанием такой возможности и сожалением о том, что на практике такой метод крайне неэффективен. Главная цель настоящей работы заключается в том, чтобы опровергнуть это утверждение и построить очень эффективный алгоритм определения группы Галуа на основе теоремы плотности Чеботарева, причем для произвольных (не обязательно неприводимых) сепарабельных многочленов с рациональными коэффициентами.

2 Теорема плотности Чеботарева

В этой главе мы изучим область применимости методов, основанных на теореме плотности Чеботарева. Оказывается, что эти методы естественным образом переносятся на поля, конечно порожденные над простым подполем. Для иллюстрации этого мы формулируем общую теорему плотности Чеботарева в геометрической форме. Однако поскольку в дальнейшем мы ограничиваемся только рассмотрением поля рациональных чисел, а доказательство общей теоремы плотности Чеботарева увело бы нас далеко в сторону от заявленной темы работы, мы лишь намечаем его в серии замечаний и показываем, как можно вывести нужный нам вариант теоремы плотности Чеботарева из ее стандартного варианта для числовых полей.

Итак, в этой главе мы собираемся обсудить различные варианты теоремы плотности Чеботарева. Нам будет удобно при ее обсуждении использовать геометрический язык; это особенно полезно при рассмотрении ее обобщений. Однако перед этим нам понадобится напомнить основы теории этальной фундаментальной группы, которая одновременно является алгебраическим вариантом определения топологической фундаментальной группы гладкого алгебраического многообразия над $\mathbb{C}$ и обобщением понятия абсолютной группы Галуа поля.

2.1 Этальная фундаментальная группа

Напомним сначала определение и основные свойства этальных морфизмов схем. Все эти свойства можно найти в [11], 17, где этальные морфизмы изучаются в максимальной общности, или в [12], I, где даются определения для случая локально нетеровых схем. Поскольку для наших рассмотрений этого случая достаточно, приведем определения из [12].

Определение 2.1.1 *Пусть X, Y — локально нетеровы схемы, $f\colon X \to Y$ — морфизм локально конечного типа, $x \in X$, $y = f(x)$. Говорят, что морфизм f* неразветвлен *в точке x, если сужение диагонального отображения $\Delta_{X/Y} : X \to X \times_Y X$ на некоторую открытую окрестность точки x является открытым вложением, или, что равносильно, если слой $\Omega^1_{X/Y,x}$ в точке x пучка относительных дифференциалов $\Omega^1_{X/Y}$ тривиален. Если, кроме того, f является плоским в точке x, то говорят, что f* этален *в точке x.*

Определение 2.1.2 *Пусть X, Y — локально нетеровы схемы, $f\colon X \to Y$ — морфизм локально конечного типа. Морфизм f называется* неразветвленным, *если диагональное отображение $\Delta_{X/Y} : X \to X \times_Y X$ является открытым вложением, или, что равносильно, если пучок относительных дифференциалов $\Omega^1_{X/Y}$ тривиален. Если, кроме того, f является плоским, то f называется* этальным *морфизмом. Этальный конечный морфизм называется* этальным накрытием.

Замечание 2.1.3 Неразветвленность (соотв., этальность) морфизма f равносильна его неразветвленности (соотв., этальности) во всех точках $x \in X$.

Замечание 2.1.4 В первоначальном варианте [12] использовался термин “non ramifié” (неразветвленный); в окончательном варианте [12] и в [11] предлагается вместо этого использовать термин “net” (чистый).

Определение 2.1.5 *Пусть A, B — кольца (как всегда, коммутативные с единицей). Гомоморфизм колец $\varphi\colon A \to B$ называется* неразветвленным *(соотв.* этальным*), если соответствующий морфизм схем ${}^a\varphi\colon \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ неразветвлен (соотв. этален). В этом случае говорят также, что B является неразветвленной (соотв. этальной) A-алгеброй.*

Замечание 2.1.6 Несложно доказать, что всякий неразветвленный (и тем более этальный) морфизм квазиконечен (см. [12], I 3); если схема Y артинова (например, спектр поля), то всякий квазиконечный морфизм $f : X \to Y$ конечен ([10], 6.4.4), и потому всякая этальная схема над Y является этальным накрытием. Отсюда следует, в частности, что всякая этальная алгебра A над полем k конечна. В этом случае мы будем говорить также, что k-алгебра A сепарабельна; для конечномерных коммутативных алгебр над полем это определение согласуется с каким угодно определением сепарабельности, поскольку k-алгебра A этальна $\Leftrightarrow$ $\bar{k}$-алгебра $A \otimes_k \bar{k}$ этальна $\Leftrightarrow$ $\bar{k}$-алгебра $A \otimes_k \bar{k}$ изоморфна прямому произведению нескольких экземпляров $\bar{k}$ $\Leftrightarrow$ $A \simeq K_1 \times K_2 \times \cdots \times K_s$, где K_i — поля, конечные

сепарабельные расширения k. Этот пример показывает, что изучение всевозможных этальных накрытий $\operatorname{Spec} k$ по существу равносильно изучению всевозможных сепарабельных расширений поля k, т.е. подгрупп конечного индекса абсолютной группы Галуа поля k.

Следующее предложение дает большой набор примеров этальных накрытий.

Предложение 2.1.7 *(см. [12], I 7) Пусть A — кольцо, $f \in A[T]$ — унитарный многочлен степени n. Тогда A-алгебра $B := A[T]/f \cdot A[T]$ неразветвлена тогда и только тогда, когда многочлен F* сепарабелен, *т.е. $fA[T] + f'A[T] = A[T]$. В этом случае $\operatorname{Spec} B$ является этальным накрытием $\operatorname{Spec} A$; степень этого накрытия равна n. Более общо, если $s \in A[T]$ — еще один многочлен, то B_s является неразветвленной (или, что в данном случае одно и то же, этальной) A-алгеброй тогда и только тогда, когда $fA[T]_s + f'A[T]_s = A[T]_s$.*

Этальные морфизмы данного вида типичны в том смысле, что локально любой неразветвленный (соотв., этальный) морфизм раскладывается в композицию вложения (соотв., открытого вложения) с последующим этальным морфизмом вида, рассмотренного во второй части формулировки предложения.

Пусть теперь S — непустая связная нетерова схема, Ω — алгебраически замкнутое поле, $\bar{s} \in S(\Omega) = \operatorname{Hom}(\operatorname{Spec}\Omega, S)$ — геометрическая точка S; напомним, что задание такой точки равносильно заданию «обычной» точки s и вложения поля вычетов $\kappa(s) \to \Omega$.

Обозначим через $\mathcal{C} = \mathcal{C}_S$ полную подкатегорию категории S-схем $\mathbf{Sch}/S$, образованную этальными накрытиями схемы S. Любое плоское накрытие X/S определяется некоторым пучком $\mathcal{O}_S$-алгебр, который будет плоским и конечно представимым и потому локально свободным пучком $\mathcal{O}_S$-модулей. Это позволяет для любого этального (и даже плоского) накрытия X/S определить его степень — это ранг локально свободного $\mathcal{O}_S$-модуля $\mathcal{A}$.

Определим теперь функтор $F = F_{\bar{s}} \colon \mathcal{C}_S \to \mathbf{Set}$ следующим образом: $F(X)$ — это множество геометрических Ω-точек X, лежащих над $\bar{s}$, т.е. множество S-морфизмов $\bar{x} \colon \operatorname{Spec}\Omega \to X$. Это множество находится во взаимно однозначном соответствии с сечениями морфизма $X \times_S \operatorname{Spec}\Omega \to \operatorname{Spec}\Omega$, т.е. со множеством Ω-точек схемы $X_\Omega := X \times_S \operatorname{Spec}\Omega$. Если X/S — этальное накрытие степени n, то X_Ω — этальное накрытие $\operatorname{Spec}\Omega$ степени n, и потому X_Ω является суммой n экземпляров $\operatorname{Spec}\Omega$, а множество $F(X)$ состоит ровно из n элементов. Таким образом, в действительности функтор F принимает свои значения в категории конечных множеств **set**, и потому можно его рассматривать как функтор $F \colon \mathcal{C} \to \mathbf{set}$.

Оказывается, что пара $(\mathcal{C}, F)$ удовлетворяет *аксиоматическим условиям теории Галуа* (см. [12], V 4):

(G1) $\mathcal{C}$ обладает финальным объектом и расслоенными произведениями (иначе говоря, в $\mathcal{C}$ существуют конечные проективные пределы).

(G2) В $\mathcal{C}$ существуют конечные прямые суммы (в частности, существует инициальный объект $\varnothing_{\mathcal{C}}$), а также факторобъекты относительно произвольных конечных групп автоморфизмов.

(G3) Всякий морфизм $u \colon X \to Y$ раскладывается в композицию $X \xrightarrow{u'} Y' \xrightarrow{u''} Y$, где u' — строгий эпиморфизм, а u'' — мономорфизм, являющийся изоморфизмом на прямое слагаемое в Y.

(G4) Функтор F точен слева, т.е. сохраняет финальный объект и расслоенные произведения (иначе говоря, F перестановочен с конечными проективными пределами).

(G5) F перестановочен с конечными прямыми суммами, преобразует строгие эпиморфизмы в эпиморфизмы, и перестановочен с операцией взятия факторобъекта относительно конечной группы автоморфизмов.

(G6) Для всякого морфизма $u \colon X \to Y$, такого, что $F(u)$ — изоморфизм, u также является изоморфизмом (т.е. F *консервативен*).

Для любой проконечной группы π категория $\mathbf{b}_\pi$ конечных дискретных π-множеств вместе с забывающим функтором $I \colon \mathbf{b}_\pi \to \mathbf{set}$ удовлетворяет условиям аксиоматической теории Галуа (G1)–(G6). Оказывается, что верно и обратное ([12], V 4): для любой аксиоматической теории Галуа $(\mathcal{C}, F)$ существует проконечная группа π и эквивалентность категорий $G \colon \mathcal{C} \to \mathbf{b}_\pi$, такая, что $I \circ G = F$. При этом группа π определена однозначно с точностью до изоморфизма. В качестве π можно взять группу

$\mathrm{Aut}(F)$ автоморфизмов функтора F, наделенную топологией простой сходимости на всех $F(X)$; иначе говоря, для каждого $X \in \mathrm{Ob}\,\mathcal{C}$ и $\xi \in F(X)$ мы определяем $H_{X,\xi} := \{\sigma \in \mathrm{Aut}(F) : \sigma_X(\xi) = \xi\}$ и берем в качестве окрестностей единицы множества, содержащие конечное пересечение подгрупп указанного вида. Кроме того, даже если мы не фиксируем функтор-слой F, все равно любые два таких функтора (неканонически) изоморфны (для доказательства достаточно рассмотреть случай $\mathcal{C} = \mathbf{b}_\pi$), и потому группа π все равно определена однозначно с точностью до неединственного изоморфизма; любые два таких изоморфизма отличаются на внутренний автоморфизм группы π.

Таким образом, для связной (локально нетеровой) схемы S и геометрической точки $\bar{s}$ определена некоторая проконечная группа $\pi_1(S;\bar{s})$; при этом для каждого этального накрытия X/S на конечном множестве $F_{\bar{s}}(X)$ геометрических точек X, лежащих над $\bar{s}$, определяется непрерывное действие $\pi_1(S;\bar{s})$, такое, что сопоставление каждому X множества $F(X)$ с этим действием является эквивалентностью категории $\mathcal{C}_S$ этальных накрытий схемы S и категории конечных дискретных $\pi_1(S;\bar{s})$-операторных множеств.

Определение 2.1.8 *Определенная таким образом проконечная группа $\pi_1(S;\bar{s})$ называется* (этальной) фундаментальной группой *схемы S относительно геометрической точки $\bar{s}$.*

Важно, что при этой эквивалентности многие свойства X можно выразить в терминах π_1-множества $F(X)$: так, X связно тогда и только тогда, когда $F(X)$ связно (т.е. состоит из не более чем одной орбиты); X непусто тогда и только тогда, когда $F(X)$ непусто; разложению X на компоненты связности соответствует разложение $F(X)$ на орбиты; расслоенным произведениям соответствуют расслоенные произведения, и т.д.

Замечание 2.1.9 Пусть $S = \mathrm{Spec}\,k$ — спектр поля, $\Omega = \bar{k}$ — алгебраическое замыкание k, $\bar{s} \in S(\Omega)$ — геометрическая точка, определенная вложением $k \to \Omega$. Тогда для любого этального накрытия X/S схема X имеет вид $\mathrm{Spec}\,A$ для некоторой сепарабельной k-алгебры A, и $F_{\bar{s}}(X) = \mathrm{Hom}_S(\mathrm{Spec}\,\Omega, X) = \mathrm{Hom}_{k\text{-alg}}(A,\Omega)$. Заметим теперь, что группа Галуа $\mathrm{Gal}(\Omega/k)$ действует согласованным образом на всех $F_{\bar{s}}(X)$. Несложно видеть, что функтор $F_{\bar{s}}$, если рассмотреть его как функтор в категорию конечных дискретных $\mathrm{Gal}(\Omega/k)$-операторных множеств, является эквивалентностью категорий, и потому, ввиду единственности фундаментальной группы, в данном случае этальная фундаментальная группа совпадает с абсолютной группой Галуа.

Пример 2.1.10 В предположениях предыдущего замечания пусть $A = k[T]/f \cdot k[T]$, где f — сепарабельный многочлен. Тогда $F_{\bar{s}}(\mathrm{Spec}\,A) = \mathrm{Hom}_{k\text{-alg}}(A,\Omega) \cong \{\alpha \in \Omega : f(\alpha) = 0\}$, поскольку задание гомоморфизма k-алгебр $A \to \Omega$ эквивалентно заданию образа α класса T в A. Итак, $F_{\bar{s}}(\mathrm{Spec}\,A)$ есть множество корней $f(T)$ с естественным действием группы Галуа.

Замечание 2.1.11 Если $\bar{s}$ и $\bar{s}'$ — две различные геометрические точки S, то ввиду свойства единственности две фундаментальные группы $\pi_1(S;\bar{s})$ и $\pi_1(S;\bar{s}')$ изоморфны, однако канонического изоморфизма между ними не существует. В связи с этим вводится следующее определение: *множество путей* из $\bar{s}$ в $\bar{s}'$ есть множество изоморфизмов функтора $F_{\bar{s}}$ на $F_{\bar{s}'}$. Выбор какого-либо пути между $\bar{s}$ и $\bar{s}'$ позволяет определить изоморфизм между соответствующими фундаментальными группами.

Для любого непрерывного гомоморфизма проконечных групп $\varphi\colon H \to G$ можно определить функтор $\varphi^*\colon \mathbf{b}_G \to \mathbf{b}_H$ сужения группы операторов вдоль φ. Этот функтор точен; наоборот, несложно видеть (см. [12], V 6), что любой точный функтор R из $\mathbf{b}_G$ в $\mathbf{b}_H$ изоморфен функтору такого вида. Если, кроме того, $I_H \circ R = I_G$, где I_H и I_G — забывающие функторы в категорию конечных множеств, то $R = \varphi^*$ для однозначно определенного непрерывного гомоморфизма φ. Отсюда легко выводится следующее предложение (см. [12], V 7):

Предложение 2.1.12 *а) Пусть $f\colon T \to S$ — морфизм связных (локально нетеровых) схем, $\bar{t} \in T(\Omega)$ — геометрическая точка T, $\bar{s} := f(\bar{t}) \in S(\Omega)$ — ее образ в S. Рассмотрим точный функтор $f^* : \mathcal{C}_S \to \mathcal{C}_T$, сопоставляющий этальному накрытию X/S его обратный образ $X \times_S T/T$. Тогда существует единственный непрерывный гомоморфизм $\pi_1(f;\bar{t}) = \varphi\colon \pi_1(T;\bar{t}) \to \pi_1(S;\bar{s})$, такой, что при каноническом отождествлении множества $F_{\bar{t}}(f^*X)$ с $F_{\bar{s}}(X)$ функтор f^* совпадает с функтором сужения группы операторов φ^* (здесь мы также отождествляем $\mathcal{C}_S$ с $\mathbf{b}_{\pi_1(S;\bar{s})}$, и поступаем аналогично с $\mathcal{C}_T$).*

б) Если, кроме того, $f\colon T \to S$ является этальным накрытием, M — соответствующее $\pi_1(S;\bar{s})$-множество, H — стабилизатор элемента $\bar{t} \in M$ (напомним, что $M = F_{\bar{s}}(T)$ — это в точности множество

всех геометрических точек T, лежащих над $\bar{s}$), то $\pi_1(T;\bar{t})$ можно отождествить с открытой подгруппой H в $\pi_1(S;\bar{s})$; при этом гомоморфизм φ из пункта а) отождествляется с естественным вложением группы H.

Из пункта б) немедленно выводим

Следствие 2.1.13 *Для любого этального накрытия $p\colon X \to S$ степени n существует этальное накрытие $f\colon T \to S$, такое, что $f^*(X)$ есть сумма n экземпляров T.*

Это следствие нам нужно для доказательства следующей теоремы:

Теорема 2.1.14 *Пусть S — связная (локально нетерова) схема, $\bar{s}$ — некоторая геометрическая точка, $G := \pi_1(S;\bar{s})$ — этальная фундаментальная группа, $f\colon X \to S$ — этальное накрытие степени n, $M := F_{\bar{s}}(X)$ — соответствующее G-операторное множество и $\sigma \in \mathrm{Aut}_S(X)$ — произвольный автоморфизм накрытия X/S. Пусть $\mathcal{A} := f_*(\mathcal{O}_X)$ — пучок $\mathcal{O}_S$-алгебр, определяющий X. Поскольку $\mathcal{A}$ — локально свободный $\mathcal{O}_S$-модуль ранга n и σ^* — его автоморфизм, можно рассмотреть его характеристический многочлен $\chi_{\sigma^*}(T) := \det(T\cdot 1 - \sigma^*) \in \Gamma(S,\mathcal{O}_S)[T]$ и след $\mathrm{Tr}\,\sigma^* \in \Gamma(S,\mathcal{O}_S)$.*

Обозначим через E свободный $\mathbb{Z}$-модуль с базисом M и через $\widetilde{\sigma}$ его автоморфизм, действующий на базисные элементы как $F_{\bar{s}}(\sigma)$. Тогда $\chi_{\sigma^*}(T) = \chi_{\widetilde{\sigma}}(T)$ и $\mathrm{Tr}\,\sigma^* = \mathrm{Tr}\,\widetilde{\sigma} = \mathrm{card}\{x \in M : F(\sigma)(x) = x\}$. В частности, все коэффициенты характеристического многочлена σ^* целые.

Доказательство Ясно, что достаточно доказать утверждение про характеристический многочлен, так как след является одним из его коэффициентов. Пусть $g\colon S' \to S$ — существующее по следствию 2.1.13 этальное накрытие, такое, что $g^*(X)$ есть сумма n экземпляров S'. Положим $X' := g^*(X) = X \times_S S'$, $\sigma' := \sigma \times 1_{S'}$; тогда $\sigma'^* = \sigma^* \otimes_{\mathcal{O}_S} 1_{\mathcal{O}_{S'}}$, и потому $\chi_{\sigma'^*}(T)$ есть образ $\chi_{\sigma^*}(T)$ при гомоморфизме $\Gamma(S,\mathcal{O}_S)[T] \to \Gamma(S',\mathcal{O}_{S'})[T]$. Этот гомоморфизм инъективен, поскольку g — строго плоский морфизм. Поэтому достаточно доказать требуемое равенство для σ'. Поскольку, кроме того, можно считать, что X'/S' соответствует то же множество M, и при этом $F(\sigma')$ отождествляется с $F(\sigma)$, мы видим, что, заменив S, X и σ на S', X' и σ', можно считать, что X есть сумма n экземпляров S. При этом в каждом экземпляре S есть ровно одна геометрическая точка, лежащая над $\bar{s}$; сопоставив каждому экземпляру соответствующую точку, мы получим биекцию множества связных компонент X на множество M. Итак, X есть $S \times M = \coprod_{m\in M} S$, причем действия σ на X и $F(\sigma)$ на M при этом отождествлении согласованы. Отсюда $\mathcal{A} = \mathcal{O}_S^{(M)}$, и σ^* действует на базисных элементах как $F(\sigma)^{-1}$. Поэтому $\mathcal{A} \cong \mathcal{O}_S \otimes_{\mathbb{Z}} E^*$, а значит, $\chi_{\sigma^*}(T) = \chi_{{}^t\widetilde{\sigma}}(T) = \chi_{\widetilde{\sigma}}(T)$, что и требовалось доказать.

Кроме того, теперь мы можем определить *элемент Фробениуса*:

Определение 2.1.15 *Пусть S — связная (локально нетерова) схема, $s \in S$ — точка с конечным полем вычетов $\kappa(s) = \mathbb{F}_q$, $\Omega = \overline{\kappa(s)}$ и $\bar{s}$ — геометрическая точка S, определенная с помощью $\kappa(s) \to \Omega$. Обозначим через i_s морфизм $\mathrm{Spec}\,\kappa(s) \to S$; ясно, что $\bar{s}$ можно рассматривать как Ω-геометрическую точку $\mathrm{Spec}\,\kappa(s)$. Элемент Фробениуса $\mathrm{Frob}_s \in \pi_1(S;\bar{s})$, соответствующий геометрической точке $\bar{s}$ — это образ автоморфизма Фробениуса $(\varphi_q\colon x \mapsto x^q) \in \mathrm{Gal}(\Omega/\kappa(s)) = \pi_1(\mathrm{Spec}\,\kappa(s);\bar{s})$ относительно непрерывного гомоморфизма $\pi_1(i_s;\bar{s})$.*

Если $\bar{t}$ — другая геометрическая точка S и γ — путь из $\bar{s}$ в $\bar{t}$, устанавливающий некоторый изоморфизм $\theta : \pi_1(S;\bar{s}) \to \pi_1(S;\bar{t})$, то элемент Фробениуса $\mathrm{Frob}_{s,\gamma} \in \pi_1(S;\bar{t})$ *— это образ Frob_s относительно θ. Наконец, если заданы только s с конечным полем вычетов и геометрическая точка $\bar{t}$, можно определить $\mathrm{Frob}_s \in \pi_1(S;\bar{t})$, применив предыдущее определение к произвольно выбранной геометрической точке $\bar{s}$ с носителем в s и произвольному пути γ; полученный таким образом элемент определен с точностью до сопряжения, поскольку при выборе другого пути γ гомоморфизм θ изменяется на внутренний автоморфизм. Таким образом, в действительности в этом случае определен только* класс сопряженности элемента Фробениуса.

Наконец, если $s' \in S(\mathbb{F}_{q^r})$ — некоторая $\mathbb{F}_{q^r}$-значная точка с носителем s, положим $\mathrm{Frob}_{s'} := \mathrm{Frob}_s^r$; это есть образ автоморфизма Фробениуса $\varphi_{q^r} \in \pi_1(\mathrm{Spec}\,\mathbb{F}_{q^r};\bar{s})$ относительно $\pi_1(s';\bar{s})\colon \pi_1(\mathrm{Spec}\,\mathbb{F}_{q^r};\bar{s}) \to \pi_1(S;\bar{s})$. Аналогично тому, как это было проделано выше, определяется элемент $\mathrm{Frob}_{s',\gamma} \in \pi_1(S;\bar{t})$ и класс сопряженности $\mathrm{Frob}_{s'} \in \pi_1(S;\bar{t})$.

Следующее предложение дает удобное описание действия Frob_s на произвольном конечном π_1-операторном множестве.

Предложение 2.1.16 *Пусть S — связная (локально нетерова) схема, π_1 — ее фундаментальная группа (относительно некоторой геометрической точки), M — конечное π_1-операторное множество, X/S — соответствующее этальное накрытие, $s \in S$ — точка с конечным полем вычетов, $\mathrm{Frob}_s \in \pi_1$ — (произвольный) элемент Фробениуса, определенный s. Пусть $x_1, x_2, \ldots, x_r$ — все различные точки слоя X_s. Тогда набор длин циклов подстановки элементов M, определенной действием Frob_s на M, совпадает с набором $\left(\dim_{\kappa(s)} \kappa(x_i)\right)_{1 \le i \le r}$.*

Доказательство Пусть $\kappa(s) = \mathbb{F}_q$ — поле вычетов точки s, Ω — алгебраическое замыкание $\kappa(s)$, $\bar{s}$ — геометрическая точка s, определенная вложением $\kappa(s) \to \Omega$, $i_s\colon \operatorname{Spec}\kappa(s) \to S$ — естественный морфизм, $\varphi_q \in G := \mathrm{Gal}(\Omega/\mathbb{F}_q) \cong \pi_1(\operatorname{Spec}\kappa(s); \bar{s})$ — автоморфизм Фробениуса. Можно считать, что $\pi_1 = \pi_1(S; \bar{s})$ и что $\mathrm{Frob}_s = \pi_1(i_s)(\varphi_q)$, где $\pi_1(i_s)$ — гомоморфизм фундаментальных групп, индуцированный i_s: любой другой выбор заменяет Frob_s на сопряженный, а значит, и индуцированную этим элементов подстановку на M на сопряженную, что не изменяет набор длин циклов.

Рассмотрим этальное накрытие $X_s = X \times_S \operatorname{Spec}\kappa(s) \to \operatorname{Spec}\kappa(s)$; по определению $\pi_1(i_s)$ это накрытие задается множеством M, на котором G действует посредством сужения группы операторов относительно $\pi_1(i_s)$. Таким образом, элемент $\varphi_q \in G$ действует на M так же, как и $\mathrm{Frob}_s \in \pi_1$; поэтому можно, заменив X, S и π_1 на X_s, $\operatorname{Spec}\kappa(s)$ и G, считать, что $S = \operatorname{Spec}\kappa(s)$.

Итак, пусть $S = \operatorname{Spec}\mathbb{F}_q$; тогда $X = \coprod_{1 \le i \le r} \operatorname{Spec}\kappa(x_i)$ и потому G-операторное множество M есть сумма G-операторных множеств M_i, соответствующих каждому $\operatorname{Spec}\kappa(x_i)$. Если $d_i := \dim_{\mathbb{F}_q} \kappa(x_i)$, то $\kappa(x_i) = \mathbb{F}_{q^{d_i}}$, и подгруппа в $G \cong \widehat{\mathbb{Z}}$, оставляющая $\kappa(x_i)$ неподвижным, есть $d_i\widehat{\mathbb{Z}}$. Поэтому $M_i \cong \widehat{\mathbb{Z}}/d_i\widehat{\mathbb{Z}} \cong \mathbb{Z}/d_i\mathbb{Z}$, и образующая φ_q группы G циклически действует на M_i. Поскольку M есть сумма M_i, отсюда мы немедленно получаем, что набор длин циклов подстановки элементов M, определенной действием φ_q, в точности есть $(d_i)_{1 \le i \le r}$, что и требовалось доказать.

Нам понадобится еще следующий полезный факт (см. [12], V 8.2):

Теорема 2.1.17 *Пусть S — связная нормальная (локально нетерова) схема, ξ — ее общая точка, $K = \kappa(\xi)$ — поле рациональных функций на S, $\bar{s}$ — геометрическая точка, определенная вложением $K \to \overline{K}$. Тогда гомоморфизм групп $\mathrm{Gal}(\overline{K}/K) \cong \pi_1(\operatorname{Spec}K; \bar{s}) \to \pi_1(S; \bar{s})$, индуцированный морфизмом $\operatorname{Spec}K \to S$, сюръективен.*

2.2 Теорема плотности Чеботарева

Сначала сформулируем несколько вспомогательных утверждений.

Лемма 2.2.1 *Пусть G — проконечная группа, $U \subset G$ — произвольное подмножество. Следующие утверждения эквивалентны:*

(i) U открыто-замкнуто (т.е. одновременно открыто и замкнуто);

(ii) $U = XH$ для некоторого открытого нормального делителя H в G и конечного множества $X \subset G$;

(iii) U является объединением смежных классов G по некоторому открытому нормальному делителю $H \subset G$;

(iv) существует открытый нормальный делитель H в G и подмножество $U' \subset G/H$, такие, что U является прообразом U' относительно канонической проекции $\varphi\colon G \to G/H$.

Если эти условия выполнены, то для (лево- или правоинвариантной) меры Хаара μ на G, нормированной условием $\mu(G) = 1$, выполнено равенство $\mu(U) = |U'|/(G : H)$

Доказательство Импликации (ii)⇒(iii)⇒(iv)⇒(i) очевидны; докажем (i)⇒(ii). Для любого открытого нормального делителя H в G обозначим через U_H объединение всех смежных классов G по H, содержащихся в U. Тогда $U = \bigcup_H U_H$, где объединение берется по всем открытым нормальным делителям G, поскольку вместе с каждой точкой x открытое множество U содержит некоторую ее окрестность вида xH. Кроме того, семейство $\{U_H\}_H$ фильтруется по возрастанию, так как из $H' \subset H$ следует $U_{H'} \supset U_H$. Ввиду компактности U отсюда следует, что $U = U_H$ для некоторого H, т.е. существует открытое покрытие вида $U = \bigcup_{x \in X} xH$. Выбрав из него конечное подпокрытие, получим конечное множество X, удовлетворяющее (ii).

Осталось доказать последнее утверждение леммы. Для этого заметим, что мера $\mu(sH)$ любого смежного класса $sH = Hs$ совпадает с $\mu(H)$; поскольку G является дизъюнктным объединением $(G : H)$ таких классов, а U является дизъюнктным объединением $|U'|$ классов, получаем требуемое равенство.

Следствие 2.2.1.1 *Пусть G — проконечная группа, $f\colon G \to X$ — непрерывное отображение G во множество X, наделенное дискретной топологией. Тогда множество $f(G) \subset X$ конечно, и f представляется в виде $G \xrightarrow{\varphi} G/H \xrightarrow{f'} X$ для некоторого открытого нормального делителя H в G.*

Доказательство Множество $f(G)$ компактно и дискретно и потому конечно; пусть $(x_i)_{1\le i\le n}$ — все его различные элементы. Подмножество $f^{-1}(x_i) \subset G$ одновременно открыто и замкнуто в G, и потому, согласно лемме, является объединением смежных классов по некоторому открытому нормальному делителю H_i. Возьмем в качестве H пересечение всех H_i; тогда f постоянна на смежных классах по H и потому пропускается через $\varphi\colon G \to G/H$.

Определение 2.2.2 *(ср. [7]) Пусть Y — арифметическая схема (т.е. схема конечного типа над $\mathbb{Z}$) размерности d, $[Y]_0$ — множество ее замкнутых точек, $A \subset [Y]_0$ — произвольное подмножество этого множества. Для любой замкнутой точки $y \in [Y]_0$ определим ее* норму *равенством $N(y) := \operatorname{card}\kappa(y)$. Определим ζ-функцию множества A равенством $\zeta_A(s) := \prod_{y\in A}(1 - N(y)^{-s})^{-1}$. Эта функция равномерно сходится на компактах внутри области $\operatorname{Re} s > d$. По определению ζ-функция схемы Y — это ζ-функция множества всех ее замкнутых точек. Для некоторого $\varepsilon > 0$ она может быть продолжена до функции, мероморфной на $\operatorname{Re} s > d - \varepsilon$ и не имеющей никаких особенностей в этой области, кроме, возможно, простого полюса при $s = d$.*

Определим аналитическую плотность *множества A как предел отношения $\log\zeta_A(s)/\log\zeta_Y(s)$ при s, стремящемся сверху к d, если этот предел существует.*

Наконец, определим натуральную плотность *множества A как предел при $M \to \infty$ отношения количества точек $y \in A$ с нормами, не превосходящими M, к общему количеству точек $y \in [Y]_0$ с такими нормами.*

Замечание 2.2.3 Из общих свойств рядов Дирихле выводится, что если определена натуральная плотность множества A, то определена и аналитическая; наоборот, если функция $f(s) = \log\zeta_A(s) - \rho\log\zeta_Y(s)$ продолжается до функции, мероморфной в области $\operatorname{Re} s > d - \varepsilon$ и регулярной на прямой $\operatorname{Re} s = d$ для некоторых $\varepsilon > 0$ и $\rho \ge 0$, то определена и натуральная, и аналитическая плотность, причем обе они равны ρ (тауберова теорема Винера–Икеары; см., напр., [2]); если при этом функция $f(s)$ голоморфна в области $\operatorname{Re} s > d - \varepsilon$, то разность ρ и отношения, рассмотренного при определении натуральной плотности, есть $O(M^{-\varepsilon})$. Для всех множеств, которые мы будем рассматривать, эти условия выполнены, и потому безразлично, говорить ли о натуральной или об аналитической плотности. Кроме того, в числовом случае (X квазиконечна над $\operatorname{Spec}\mathbb{Z}$) можно взять $\varepsilon = 1/2$ (в усиленном варианте нашего утверждения), если выполнена обобщенная гипотеза Римана.

Теорема 2.2.4 *(теорема плотности Чеботарева) Пусть Y — связная нормальная арифметическая схема (т.е. схема конечного типа над $\mathbb{Z}$), $\bar y_0$ — ее геометрическая точка, $\pi_1 := \pi_1(Y; \bar y_0)$ — ее фундаментальная группа, $\mathcal{C} \subset \pi_1$ — открыто-замкнутое подмножество π_1, устойчивое относительно сопряжения. Тогда плотность замкнутых точек $y \in Y$, для которых $\operatorname{Frob}_y \in \mathcal{C}$, равна $\mu(\mathcal{C})$, где μ — мера Хаара на π_1, нормированная условием $\mu(\pi_1) = 1$, а Frob_y — какой-либо из элементов Фробениуса, соответствующих y (запись "$\operatorname{Frob}_y \in \mathcal{C}$" корректна, поскольку согласно определению 2.1.15 элемент Frob_y определен с точностью до сопряжения, а $\mathcal{C}$ устойчиво относительно сопряжения).*

Доказательство В действительности эта теорема нам будет нужна в одномерном случае, так что вместо доказательства мы покажем, как в этом случае теорема Чеботарева в нашей формулировке сводится к «обычной» теореме Чеботарева (см., напр., [2]). План общего доказательства будет затем намечен в серии замечаний.

Итак, предположим, что Y одномерна. По лемме 2.2.1 существует открытая нормальная подгруппа $H \subset \pi_1$ и подмножество $C' \subset G := \pi_1/H$, такое, что $\mathcal{C}$ есть прообраз C' относительно проекции $\varphi\colon \pi_1 \to G$. Пусть X/S — этальное «накрытие Галуа», определенное нормальной подгруппой H (т.е. соответствующее π_1-операторному множеству π_1/H при эквивалентности категорий, рассмотренной в предыдущем пункте). Пусть K и L — поля рациональных функций на Y и X соответственно; тогда K

— глобальное числовое поле и L/K — расширение Галуа с группой Галуа G. Замкнутые точки схемы Y соответствуют всем ненулевым простым идеалам кольца целых поля K, кроме конечного их числа; эти простые идеалы неразветвлены относительно L/K, так как X/Y — этальное накрытие. Для любой замкнутой точки $y \in Y$ элемент $\varphi(\mathrm{Frob}_y) \in G$ — это в точности «обычный» элемент Фробениуса; поскольку условия $\mathrm{Frob}_y \in \mathcal{C}$ и $\varphi(\mathrm{Frob}_y) \in C'$ эквивалентны и C' — подмножество в G, устойчивое относительно сопряжения, обычная теорема плотности Чеботарева утверждает, что плотность тех замкнутых точек y, для которых $\varphi(\mathrm{Frob}_y) \in C'$, равна $|C'|/|G|$, что по лемме 2.2.1 в точности равно $\mu(\mathcal{C})$.

Замечание 2.2.4.1 В общем случае теорема доказывается, как и в одномерном случае, с помощью L-функций. Пусть E — конечномерное векторное пространство, $\rho\colon \pi_1 \to \mathrm{Aut}_{\mathbb{C}} E$ — непрерывное комплексное представление проконечной группы π_1 (непрерывность здесь рассматривается относительно *дискретной топологии* на $\mathrm{Aut}_{\mathbb{C}} E$; согласно 2.2.1.1, такая непрерывность равносильна тому, что ρ пропускается через некоторую конечную факторгруппу π_1), и пусть $\chi\colon \pi_1 \to \mathbb{C}$ — соответствующий непрерывный характер (т.е. $\chi(g) = \mathrm{Tr}\,\rho(g)$). Для любого комплексного s с $\mathrm{Re}\, s > d = \dim S$ определим

$$L(s;\chi) = \prod_{y \in [Y]_0} \det(1 - N(y)^{-s}\rho(\mathrm{Frob}_y)) \quad .$$

По-другому можно определить $L(s;\chi)$ следующим образом:

$$\log L(s;\chi) = \sum_{y \in [Y]_0} \sum_{n \geq 1} \frac{1}{n} \chi(\mathrm{Frob}_y^n) N(y)^{-ns} \quad .$$

Последняя формула позволяет определить $\log L(s;\psi)$ для любой непрерывной *центральной* функции $\psi\colon \pi_1 \to \mathbb{C}$ (непрерывность, как обычно, понимается относительно дискретной топологии на $\mathbb{C}$, а центральность означает, что $\psi(hgh^{-1}) = \psi(g)$ для любых $g, h \in \pi_1$). Отметим следующие свойства L-функций:

a) Произведение для $L(s;\chi)$ и ряд для $\log L(s;\psi)$ равномерно сходятся на компактах, содержащихся в $\mathrm{Re}\, s > d$.

b) Если $\chi_0\colon \pi_1 \to \{1\} \subset \mathbb{C}$ — главный характер, то $L(s;\chi_0) = \zeta_Y(s)$.

c) Если $Y' \to Y$ — этальное накрытие, определенное некоторой открытой подгруппой $H \subset \pi_1$ (т.е. соответствующее π_1-операторному множеству π_1/H) и χ' — непрерывный характер группы H (которую можно отождествить с фундаментальной группой Y'), а $\chi = \mathrm{Ind}_H^{\pi_1}(\chi')$ — характер, индуцированный χ' на π_1, то $L_Y(s;\chi) = L_{Y'}(s;\chi')$. Аналогично, если $\psi'\colon H \to \mathbb{C}$ — непрерывная центральная функция и $\psi = \mathrm{Ind}_H^{\pi_1}(\psi')$, то $\log L_Y(s;\psi) = \log L_{Y'}(s;\psi')$ (доказательство этих фактов несложно, особенно если воспользоваться доказательством 2.1.16).

d) Линейность: $L(s;\chi_1+\chi_2) = L(s;\chi_1)\cdot L(s;\chi_2)$ и $\log L(s;a_1\psi_1+a_2\psi_2) = a_1 \log L(s;\psi_1) + a_2 \log L(s;\psi_2)$.

e) Если $\mathcal{C}$ — открыто-замкнутое подмножество в π_1, устойчивое относительно сопряжения, то его характеристическая функция $\varphi_A\colon \pi_1 \to \{0,1\} \subset \mathbb{C}$ является непрерывной центральной функцией, и $\log L_Y(s;\varphi_A) = \log \zeta_A(s)$.

f) Для любых двух непрерывных центральных функций ψ_1 и ψ_2 определим их скалярное произведение формулой

$$(\psi_1, \psi_2) := \int_{\pi_1} \psi_1(g)\overline{\psi_2(g)}\, d\mu(g) \quad .$$

Любая непрерывная центральная функция является комплексной линейной комбинацией конечного числа неприводимых непрерывных характеров, которые образуют ортонормированный базис в унитарном пространстве непрерывных центральных функций. Верно следующее утверждение («теорема Брауэра»): всякий непрерывный характер χ группы π_1 является целочисленной линейной комбинацией характеров, индуцированных неприводимыми характерами конечных циклических подфакторгрупп группы π_1 (т.е. циклических подгрупп конечных факторгрупп группы π_1). Если, кроме того, χ ортогонален главному характеру χ_0, можно обойтись характерами, индуцированными неглавными характерами циклических подфакторгрупп.

g) $\zeta_Y(s)$ может быть продолжена до мероморфной функции в области $\operatorname{Re} s > d - \varepsilon$ с единственным простым полюсом в $s = d$ на прямой $\operatorname{Re} s = d$ при некотором $\varepsilon > 0$. Если χ — непрерывный характер, ортогональный к χ_0, то $L_Y(s;\chi)$ и $\log L_Y(s;\chi)$ продолжаются до функций, голоморфных при $\operatorname{Re} s > d - 1$ (важная идея доказательства этого факта: свести к циклическому случаю с помощью теоремы Брауэра).

h) Если ψ — непрерывная центральная функция и $c := (\psi, \chi_0)$, то $\log L_Y(s;\psi) - c \cdot \log \zeta_Y(s)$ может быть продолжена до функции, мероморфной в области $\operatorname{Re} s > d - \varepsilon$ для некоторого $\varepsilon > 0$ и регулярной на прямой $\operatorname{Re} s = d$.

i) Если $\mathcal{C} \subset \pi_1$ — открыто-замкнутое множество, устойчивое относительно сопряжения, то $\log \zeta_{\mathcal{C}}(s) - \mu(\mathcal{C}) \cdot \log \zeta_Y(s)$ продолжается до функции, мероморфной в области $\operatorname{Re} s > d - \varepsilon$ для некоторого $\varepsilon > 0$ и регулярной на прямой $\operatorname{Re} s = d$.

Приведенный выше план доказательства показывает, каким образом осуществляется редукция к циклическому накрытию Галуа. В классическом случае необходимые свойства L-функций затем выводятся с помощью рассмотрения характеров аделей.

Замечание 2.2.4.2 Полностью избавиться от условия нормальности в формулировке теоремы Чеботарева нельзя, как показывает следующий пример. Пусть k — конечное поле характеристики $\neq 2$, $Y = \operatorname{Spec} k[X,Y]/(Y^2 - X^3 - X^2)$ — особая кубическая кривая, полученная склеиванием двух различных рациональных точек аффинной прямой $\mathbf{V}^1_k$. Тогда, как несложно видеть (см. [12]), фундаментальная группа Y изоморфна $\widehat{\mathbb{Z}} \times \operatorname{Gal}(\bar{k}/k) \cong \widehat{\mathbb{Z}}^2$, однако для любой замкнутой точки $y \in Y$ проекция соответствующего элемента Фробениуса на первую компоненту равна единице (т.е. нулю, если записывать $\widehat{\mathbb{Z}}$ аддитивно). Возьмем теперь $\mathcal{C} = (d\widehat{\mathbb{Z}}) \times \widehat{\mathbb{Z}}$ для произвольного $d > 1$; получим, что для всех замкнутых y имеет место $\operatorname{Frob}_y \in \mathcal{C}$ несмотря на то, что $\mu(\mathcal{C}) = 1/d$.

Можно построить аналогичным образом немного более сложный теоретико-числовой пример. Для этого надо взять $Y = \operatorname{Spec} \mathbb{Z}[2i]$; тогда Y — это схема, полученная склейкой замкнутых точек $(1+i)$ и $(1-i)$ нормальной схемы $\operatorname{Spec} \mathbb{Z}[i]$. Поскольку существует лишь конечное число числовых полей, неразветвленных над $\mathbb{Q}(i)$, фундаментальная группа $\operatorname{Spec} \mathbb{Z}[i]$ есть некоторая конечная группа H и потому фундаментальная группа Y есть полупрямое произведение H на $\widehat{\mathbb{Z}}$; далее пример завершается так же, как и раньше. (Проверки здесь довольно сложны, и потому мы их опускаем...)

Предложение 2.2.5 *Пусть Y — связная нормальная арифметическая схема (т.е. схема конечного типа над $\mathbb{Z}$), $\bar{y}_0$ — ее геометрическая точка, $\pi_1 := \pi_1(Y;\bar{y}_0)$ — ее фундаментальная группа, X/Y — этальное накрытие степени n, M — π_1-множество, соответствующее этому накрытию, $\theta\colon \pi_1 \to \mathfrak{S}_M \simeq \mathfrak{S}_n$ — непрерывный гомоморфизм π_1 в группу подстановок множества M, определенный действием π_1 на этом множестве. Пусть λ — разбиение натурального числа n и $\mathcal{C}_\lambda \subset \mathfrak{S}_M$ — множество подстановок циклического типа λ. Для любой замкнутой точки $y \in Y$ обозначим через $\lambda^{(y)}$ разбиение числа n, образованное степенями над $\kappa(y)$ полей вычетов $\kappa(x_i)$ точек слоя X_y.*

Тогда плотность множества тех $y \in [Y]_0$, для которых $\lambda^{(y)} = \lambda$, равна $|\mathcal{C}_\lambda \cap \theta(\pi_1)|/|\theta(\pi_1)|$.

Доказательство Согласно предложению 2.1.16 условие $\lambda^{(y)} = \lambda$ равносильно условию $\theta(\operatorname{Frob}_y) \in \mathcal{C}_\lambda$, т.е. $\operatorname{Frob}_y \in \theta^{-1}(\mathcal{C}_\lambda)$. Осталось применить ко множеству $\theta^{-1}(\mathcal{C}_\lambda)$ теорему 2.2.4 и заметить, что $\mu\big(\theta^{-1}(\mathcal{C}_\lambda)\big) = |\mathcal{C}_\lambda \cap \theta(\pi_1)|/|\theta(\pi_1)|$.

2.3 Обоснование метода

Пусть $F(T)$ — унитарный сепарабельный многочлен степени n с рациональными коэффициентами, m — произведение всех исключительных (относительно $F(T)$) простых чисел, $A = \mathbb{Z}[m^{-1}]$, $B = A[T]/(F(T))$, $S = \operatorname{Spec} A \subset \operatorname{Spec} \mathbb{Z}$, $X = \operatorname{Spec} B$; тогда S — открытая подсхема $\operatorname{Spec} \mathbb{Z}$, полученная выбрасыванием исключительных простых чисел, и согласно 2.1.7 X/S является этальным накрытием степени n.

Обозначим через $\bar{s}_0$ геометрическую общую точку S, определенную вложением поля рациональных функций $\mathbb{Q}$ схемы S в его алгебраическое замыкание $\overline{\mathbb{Q}}$. Тогда по 2.1.17 фундаментальную группу $\pi_1 := \pi_1(S;\bar{s}_0)$ можно отождествить с некоторой факторгруппой абсолютной группы Галуа $\pi_1(\operatorname{Spec} \mathbb{Q};\bar{s}_0) \cong G := \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Пусть M — n-элементное π_1-операторное множество, соответствующее накрытию X/S, и пусть $\theta\colon \pi_1 \to \mathfrak{S}_M$ — непрерывный гомоморфизм фундаментальной группы в группу подстановок множества M, индуцированный этим действием.

Мы знаем, что как G-операторное множество M можно отождествить со множеством корней многочлена $F(T)$ в $\overline{\mathbb{Q}}$ (см. 2.1.10). При этом образ группы G в $\mathfrak{S}_M$ совпадает с $H := \theta(\pi_1)$, поскольку гомоморфизм $G \to \mathfrak{S}_M$ раскладывается в композицию θ и *сюръективного* (согласно 2.1.17) гомоморфизма $G \to \pi_1$.

Теперь мы можем применить предложение 2.2.5, согласно которому плотность множества замкнутых точек $s \in S$, для которых $\lambda^{(s)}$ совпадает с заданным разбиением λ числа n, равна $|H \cap \mathcal{C}_\lambda|/|H|$.

Осталось заметить, что замкнутые точки $s \in S$ — это как раз точки, определенные регулярными простыми числами $p \in \mathbb{Z}$, и что соответствующее разбиение $\lambda^{(s)}$ — это в точности набор степеней неприводимых сомножителей редукции $F_p(T)$ многочлена $F(T)$ по модулю p, поскольку слой $X_s \cong X \otimes_{\mathbb{Z}} \kappa(s) \cong \operatorname{Spec} B \otimes_A \mathbb{F}_p \cong \operatorname{Spec} \mathbb{F}_p[T]/(F_p(T))$.

Таким образом, мы обосновали теорему 1.4.1, на которой основан наш метод.

Приведем полезную для дальнейшего эффективную форму теоремы плотности Чеботарева для числовых полей:

Теорема 2.3.1 *Пусть K — числовое поле, E/K — конечное расширение Галуа степени n, $G = \operatorname{Gal}(E/K)$, n_E — степень $E/\mathbb{Q}$ и d_E — дискриминант $E/\mathbb{Q}$. Для любого $x \geq 2$ и устойчивого относительно сопряжения подмножества $\mathcal{C} \subset G$ обозначим через $\pi_C(x)$ количество простых идеалов K с нормой, не превосходящей x, элемент Фробениуса относительно которых попадает в $\mathcal{C}$. Обозначим также через $\operatorname{Li}(x)$ интегральный логарифм:*

$$\operatorname{Li}(x) = \int_2^x \frac{dt}{\log t} \quad .$$

Тогда, если обобщенная гипотеза Римана верна, то существует константа $c > 0$, не зависящая от K, E и $\mathcal{C}$, такая, что для любого $x \geq 2$ выполнено неравенство

$$\left| \pi_{\mathcal{C}}(x) - \frac{|\mathcal{C}|}{|G|} \operatorname{Li}(x) \right| \leq c \cdot \frac{|\mathcal{C}|}{|G|} x^{1/2} (\log d_E + n_E \log x) \quad .$$

Более того, можно взять $c = 2$, а если ограничить x снизу некоторой абсолютной константой, то можно даже взять $c = 1/3$.

Доказательство Эта теорема была впервые доказана в несколько более слабой форме в [15] и затем уточнена в [9] и в [16]; наша формулировка совпадает с формулировкой из [9], 2.4 с учетом последующих замечаний.

3 Подгруппы, G-множества и линейные представления групп

3.1 Категория G-множеств

По существу все определения и многие факты, изложенные в этом пункте, можно найти в [13], IV. Мы хотим, однако, явно привести все возникающие конструкции и точные формулировки утверждений, а также изменения, необходимые для случая проконечных групп.

Определение 3.1.1 (см. [13], IV) *Пусть G — произвольная группа. Мы обозначим через $\mathbf{B}_G$ категорию G-множеств и будем называть ее* топосом G-множеств *или* классифицирующим топосом группы G. *Кроме того, обозначим через $\mathbf{b}_G$ категорию конечных G-операторных множеств и назовем его* (элементарным) топосом конечных G-множеств. *Для любых G-множеств X и Y мы обозначаем множество G-морфизмов из X в Y через $\mathrm{Hom}_{\mathbf{B}_G}(X,Y)$ или просто $\mathrm{Hom}_G(X,Y)$. Обозначим $e_{\mathbf{B}_G}$ финальный объект категорий $\mathbf{B}_G$ и $\mathbf{b}_G$: это одноточечное множество с единственным возможным действием G. Для определенности можно взять в качестве этого одноточечного множества $1 = \{\varnothing\}$. Инициальный объект $\varnothing_{\mathbf{B}_G} = \varnothing_G$ категорий $\mathbf{B}_G$ и $\mathbf{b}_G$ — это пустое множество с единственным возможным действием G. В категории $\mathbf{B}_G$ существуют произвольные (малые) проективные и индуктивные пределы, которые «можно вычислять в категории множеств». Морфизм в категории $\mathbf{B}_G$ является мономорфизмом (соотв., эпиморфизмом, изоморфизмом) тогда и только тогда, когда он инъективен (соотв., сюръективен, биективен) как отображение множеств.*

Неформально смысл предыдущего определения можно пояснить так: классифицирующий топос группы G — это «топологическое пространство», состоящее из одной точки с группой автоморфизмов G, а точнее, категория пучков множеств на таком пространстве. В связи с этим нам будет удобна терминология, вводимая в следующем определении:

Определение 3.1.2 Точечный топос $\mathbf{P}$ — *это категория множеств, или, что одно и то же, классифицирующий топос единичной группы.*

Определение 3.1.3 *Пусть $f\colon H \to G$ — гомоморфизм групп. Для любого G-операторного множества X определим H-операторное множество $f^*(X)$ следующим образом: $f^*(X)$ совпадает с X как множество, а действие H задается формулой $h \cdot x = f(h) \cdot x$. В этом случае мы будем говорить, что $f^*(X)$ получено из X* сужением группы операторов вдоль f. *Таким образом, мы определили функтор $f^*\colon \mathbf{B}_G \to \mathbf{B}_H$, который можно рассматривать также так функтор из $\mathbf{b}_G$ в $\mathbf{b}_H$. Мы будем обозначать этот функтор также через $\mathbf{B}_f^*$, а соответствующий функтор из $\mathbf{b}_G$ в $\mathbf{b}_H$ через $\mathbf{b}_f^*$. Обозначим через f_* или $\mathbf{B}_{f*}$ (соотв., $f_!$ или $\mathbf{B}_{f!}$) правый (соотв. левый) сопряженный функтор к $f^* = \mathbf{B}_f^*$. Если, кроме того, индекс $f(H)$ в G конечен, то функтор f_* (соотв. $f_!$) переводит конечные множества в конечные и потому определяет функтор $\mathbf{b}_{f*}$ (соотв. $\mathbf{b}_{f!}$), сопряженный справа (соотв. слева) к $\mathbf{b}_f^*$.*

Наконец, тройка $\mathbf{B}_f := (\mathbf{B}_f^*, \mathbf{B}_{f*}, \theta)$, где θ — изоморфизм сопряжения $\theta_{X,Y}\colon \mathrm{Hom}_H(\mathbf{B}_f^* X, Y) \cong \mathrm{Hom}_G(X, \mathbf{B}_{f*} Y)$, будет называться морфизмом топоса $\mathbf{B}_H$ в $\mathbf{B}_G$, определенным f. *Аналогично определяется морфизм элементарных топосов $\mathbf{b}_f$ в том случае, если индекс $f(H)$ в G конечен (см. 3.1.9 ниже).*

Напомним, каким образом строятся функторы f_* и $f_!$.

Лемма 3.1.4 *Пусть G, H — две произвольные группы, Q — (H,G)-множество, т.е. множество, на котором задано левое действие H и правое действие G, причем эти действия перестановочны в том смысле, что $(hq)g = h(qg)$ для любых $h \in H$, $g \in G$ и $q \in Q$. Пусть X — G-множество, Y — H-множество. Тогда имеет место канонический изоморфизм $\theta_{X,Y}\colon \mathrm{Hom}_H(Q \times^G X, Y) \to \mathrm{Hom}_G(X, \mathrm{Hom}_H(Q,Y))$, где $Q \times^G X$ — «сжатое произведение» Q и X, т.е. фактормножество множества $Q \times X$ относительно отношения эквивалентности $(qg, x) \sim (q, gx)$, левое действие H на $Q \times^G X$ индуцируется левым действием H на Q, а левое действие G на $\mathrm{Hom}_H(Q,Y)$ индуцировано правым действием G на Q.*

При этом $\theta_{X,Y}$ переводит H-отображение $f\colon Q \times^G X \to Y$ в отображение $\theta_{X,Y}(f)\colon x \mapsto \big(q \mapsto f([q,x])\big)$, где через $[q,x]$ обозначен класс пары $(q,x) \in Q \times X$ в сжатом произведении $Q \times^G X$.

Доказательство а) $\tilde{f}_x\colon q \mapsto f([q,x])$ является H-отображением: действительно, $\tilde{f}_x(hq) = f\big([hq,x]\big) = f\big(h[q,x]\big) = hf\big([q,x]\big) = h\tilde{f}_x(q)$, поскольку f — H-отображение;

b) $\tilde f\colon x \to \tilde f_x$ является G-отображением: $\tilde f_{gx}(q) = f\big([q,gx]\big) = f\big([qg,x]\big) = \tilde f_x(qg) = (g\tilde f_x)(g)$. Таким образом, $\theta_{X,Y}(f) = \tilde f$ действительно принадлежит $\mathrm{Hom}_G(X, \mathrm{Hom}_H(Q,Y))$, а значит, $\theta_{X,Y}$ корректно определено.

c) Наоборот, пусть дано $\tilde f \in \mathrm{Hom}_G(X, \mathrm{Hom}_H(Q,Y))$. Отметим, что если существует f, для которого $\tilde f = \theta_{X,Y}(f)$, то обязательно $f\big([q,x]\big) = \tilde f_x(q)$, где $\tilde f_x := \tilde f(x) \in \mathrm{Hom}_H(Q,Y)$. Таким образом, f определено однозначно; осталось проверить корректность. Прежде всего, $\tilde f_{gx} = \tilde f(gx) = g\tilde f_x$ и потому $\tilde f_{gx}(q) = (g\tilde f_x)(q) = \tilde f_x(qg)$, т.е. отображение $(q,x) \mapsto \tilde f_x(q)$ согласовано с отношением эквивалентности $(qg,x) \sim (q,gx)$, и, следовательно, определяет нужное отображение $f\colon Q \times^G X \to Y$; f будет H-отображением ввиду формул пункта a).

Следствие 3.1.4.1 *Пусть $f\colon H \to G$ — гомоморфизм групп. Функтор сужения группы операторов $f^*\colon \mathbf{B}_G \to \mathbf{B}_H$ обладает правым сопряженным f_*, который можно определить равенством $f_*(Y) := \mathrm{Hom}_H(G_d, Y)$, где G_d — это группа G, рассматриваемая как (H,G)-множество относительно действия $h \cdot g' \cdot g = f(h)g'g$. Кроме того, функтор f^* обладает левым сопряженным $f_!$, определенным формулой $f_!(Y) := G_s \times^H Y$, где на этот раз G_s — это G, рассматриваемая как (G,H)-множество.*

Доказательство Для доказательства первого факта применим лемму 3.1.4 для $Q = G_d$ и заметим, что H-множество $G_d \times^G X$ канонически изоморфно $f^*(X)$ для любого G-множества X. Второй факт доказывается еще одним применением леммы, где на этот раз нужно поменять ролями G и H, X и Y и взять в качестве Q множество G_s, рассматриваемое как (G,H)-множество: тогда получим, что $\mathrm{Hom}_G(G_s \times^H Y, X) \cong \mathrm{Hom}_H(Y, \mathrm{Hom}_G(G_s, X))$, после чего остается только заметить, что H-множество $\mathrm{Hom}_G(G_s, X)$ канонически изоморфно $f^*(X)$.

Замечание 3.1.4.2 Итак, для любого гомоморфизма групп $f\colon H \to G$ мы определили последовательность сопряженных функторов $f_!, f^*, f_*$. Из общих свойств сопряженных функторов следует, что $f_!$ сохраняет произвольные индуктивные пределы и, в частности, точен справа (под этим мы понимаем, что функтор сохраняет конечные индуктивные пределы), f^* сохраняет любые проективные и индуктивные пределы (и потому точен), а функтор f_* сохраняет проективные пределы (а значит, точен слева). Кроме того, если f инъективен, то $f_!$ переводит расслоенные произведения в расслоенные произведения, однако не сохраняет финальный объект, если только f не является изоморфизмом.

Замечание 3.1.4.3 Если $g\colon H' \to H$ — еще один гомоморфизм групп, то, очевидно, $(fg)^* = g^*f^*$; ввиду единственности сопряженных функторов отсюда получаем, что существуют канонические изоморфизмы $(fg)_* \cong f_*g_*$ и $(fg)_! \cong f_!g_!$. Впрочем, эти изоморфизмы легко построить, исходя непосредственно из 3.1.4.1.

Замечание 3.1.4.4 Пусть $f\colon H \to G$ — произвольный гомоморфизм групп. Сопряженность функторов $f_!$ и f^* позволяет определить естественные преобразования $\xi\colon f_!f^* \to 1_{\mathbf{B}_G}$ и $\eta\colon 1_{\mathbf{B}_H} \to f^*f_!$, которые можно описать явно с помощью 3.1.4.1 и 3.1.4. А именно, $\xi_X\colon f_!f^*X = G_s \times^H f^*X \to X$ переводит $[g,x] \in G_s \times^H f^*X$ в $gx \in X$, а $\eta_Y\colon Y \to f^*(G_s \times^H Y)$ переводит $y \in Y$ в $[e_G, y]$, где e_G — единица группы G. Аналогично, сопряженность функторов f^* и f_* определяет естественные преобразования $\xi'_Y\colon f^*f_*Y \to Y$ и $\eta'_X\colon X \to f_*f^*X$, которые мы сейчас явно опишем. А именно, $\xi'_Y\colon f^*\,\mathrm{Hom}_H(G_d, Y) \to Y$ переводит $\varphi \in \mathrm{Hom}_H(G_d,Y)$ в $\varphi(e_G)$, а $\eta'_X\colon X \to \mathrm{Hom}_H(G_d, f^*X)$ переводит $x \in X$ в функцию $\varphi_x\colon G_d \to f^*X$, определенную равенством $\varphi_x(g) = gx$.

Предложение 3.1.5 *Пусть $f\colon H \to G$ — гомоморфизм групп, ξ, η, ξ', η' — естественные преобразования, описанные в предыдущем замечании.*

a) *Следующие условия равносильны: (i) f инъективен; (ii) η_Y мономорфно (= инъективно) для любого $Y \in \mathrm{Ob}\,\mathbf{B}_H$; (iii) η_{H_s} мономорфно; (iv) функтор $f_!$ строг, т.е. инъективен на морфизмах; (v) функтор f_* строг; (vi) ξ'_Y эпиморфно (= сюръективно) для любого Y; (vii) ξ'_{H_s} эпиморфно.*

b) *Для любого f функтор f^* строг, ξ_X всегда эпиморфен, а η'_X мономорфен.*

c) *Следующие условия равносильны: (i) f сюръективен; (ii) ξ_X мономорфно для любого $X \in \mathrm{Ob}\,\mathbf{B}_G$; (ii') ξ_X биективно для любого $X \in \mathrm{Ob}\,\mathbf{B}_G$; (iii) ξ_{G_s} мономорфно; (iv') функтор f^* вполне строг, т.е. биективен на морфизмах; (v) η'_X биективно для любого X; (vi) η'_X эпиморфно для любого X.*

Если условия c) выполнены, то f^* индуцирует эквивалентность $\mathbf{B}_G$ и некоторой полной подкатегории в $\mathbf{B}_H$.

Доказательство a) (i)⇒(ii) очевидно, поскольку $\eta_Y(y) = \eta_Y(y') \Leftrightarrow y' = hy$ для некоторого $h \in \operatorname{Ker} f$; (ii)⇒(iii) тривиально; (iii)⇒(i): если $h \in \operatorname{Ker} f$, то $\eta_{H_s}(h) = \eta_{H_s}(e_H)$, откуда $h = e_H$. (ii)⇔(iv) — категорный факт, поскольку $(\eta_Y)_*\colon \operatorname{Hom}_H(Y', Y) \to \operatorname{Hom}_H(Y', f^*f_!Y) \cong \operatorname{Hom}_G(f_!Y', f_!Y)$ отождествляется с отображением, индуцированным $f_!$ на морфизмах; аналогично (v)⇔(vi). Поскольку $f_!$ и f_* являются вторыми сопряженными, из общей теории категорий (iv)⇔(v). Наконец, (vi)⇒(vii) очевидно, а для доказательства (vii)⇒(i) возьмем произвольный $h \in \operatorname{Ker} f$ и выберем $\varphi \in \operatorname{Hom}_H(G_d, H_s)$ так, чтобы $\varphi(e_G) = e_H$; тогда $h = h \cdot \varphi(e_G) = \varphi(h \cdot e_G) = \varphi(f(h)e_G) = \varphi(e_G) = e_H$.

b) Отображение $\xi_X\colon G_s \times^H X \to X$, переводящее $[g, x]$ в gx, очевидно, эпиморфно; остальные два утверждения пункта следуют отсюда по общекатегорным соображениям.

c) (i)⇒(ii'): заметим, что $f_!f^*X = G_s \times^H f^*X = G_s \times^G X \cong X$; (ii')⇒(ii)⇒(iii) очевидно ввиду b); (iii)⇒(i): для любого $g \in G$ $\xi_{G_s}([e_G, g]) = g = \xi_{G_s}([g, e_G])$, откуда $[e_G, g] = [g, e_G]$, т.е. существует $h \in H$, для которого $g = e_G \cdot h = f(h)$; (v)⇔(vi) ввиду b). Наконец, (ii')⇔(iv)⇔(v) снова из общих соображений, как и заключение предложения.

Пример 3.1.6 Пусть G — группа, 1 — единичная группа, $p\colon 1 \to G$ и $q\colon G \to 1$ — единственные возможные гомоморфизмы 1 в G и G в 1. Согласно определению 3.1.3, p и q индуцируют морфизмы топосов $\mathbf{B}_p\colon \mathbf{P} \to \mathbf{B}_G$ и $\mathbf{B}_q\colon \mathbf{B}_G \to \mathbf{P}$, которые мы для кратности обозначим p и q. Опишем явно возникающие при этом функторы. Функтор q^* сопоставляет каждому множеству Y его само, рассматриваемое как G-множество с тривиальным действием G. Функтор q_* переводит G-множество X во множество его неподвижных точек X^G, а функтор $q_!$ сопоставляет X множество его G-орбит X/G. Функтор p^* сопоставляет любому G-множеству X само это множество, лишенное действия G; $p_*(Y) \cong \operatorname{Hom}_G(G, Y) \cong Y^G$, где G действует, переставляя сомножители в Y^G, а $p_!(Y) \cong G \times Y$ с действием G, определенным формулой $g \cdot (g', y) = (gg', y)$.

Пример 3.1.7 Пусть G — группа, $H \subset G$ — подгруппа в G, $i\colon H \to G$ — гомоморфизм вложения. Опишем, как устроены функторы $i_!$ и i_*. Пусть Y — H-множество, $(s_\alpha)_{\alpha \in G/H}$ — множество представителей левых смежных классов G по H: $G = \coprod_\alpha s_\alpha H$. Тогда как множество $i_!Y = G \times^H Y = \coprod_\alpha (s_\alpha H \times^H Y) \simeq \coprod_\alpha Y \simeq G/H \times Y$. Этот изоморфизм зависит от выбора системы представителей (s_α). Действие G на $G/H \times Y$ задается так: если $\alpha \in G/H$ и $g \in G$, то $gs_\alpha = s_\beta h$ для однозначно определенных $\beta \in G/H$ и $h \in H$. Тогда $g \cdot (\alpha, y) = (\beta, hy)$ для любого $y \in Y$, как это немедленно следует из конструкции изоморфизма $i_!Y \simeq G/H \times Y$. Аналогично, $i_*Y = \operatorname{Hom}_H(G, Y) \simeq \prod_{G/H} Y$, поскольку всякое H-отображение $f\colon H \to Y$ однозначно восстанавливается по набору $\left(f(s_\alpha^{-1})\right)_{\alpha \in G/H}$ своих значений на системе представителей правых смежных классов G по H, и наоборот, всякий набор $a = (a_\alpha)_{\alpha \in G/H} \in \prod_{G/H} Y$ позволяет определить f по формуле $f(hs_\alpha^{-1}) = ha_\alpha$. При этом действие G задается так: $g \cdot a = b = (b_\alpha)_{\alpha \in G/H}$, где $b_\beta = ha_\alpha$, если, как и раньше, $gs_\alpha = s_\beta h$.

В частности, если $G = H \times K$, то $i_!Y \cong Y \times K$ с действием $hk \cdot (y, k') = (hy, kk')$, и $i_*Y \cong \prod_K Y$, где H действует покомпонентно, а K переставляет сомножители.

Пример 3.1.8 Пусть теперь $H \subset G$ — нормальная подгруппа и $f\colon G \to G/H$ — каноническая проекция. Опишем f_* и $f_!$ в этом случае. Для любого G-множества X $f_!X = G/H \times^G X \cong X/H$ — множество H-орбит X с естественным действием G/H и $f_*X = \operatorname{Hom}_G(G/H, X) \cong X^H$ — множество H-неподвижных элементов множества X с естественным действием G/H.

Замечание 3.1.9 Из предыдущих двух примеров следует, что для любого H-множества X и любого гомоморфизма групп $f\colon H \to G$ выполнено неравенство кардиналов $\operatorname{card} f_*X \leq (\operatorname{card} X)^{(G:f(H))}$. Разложив f в композицию сюръективного и инъективного гомоморфизмов групп, мы замечаем, что достаточно доказать утверждение для инъективного f, поскольку согласно предыдущему примеру для сюръективного f выполнено $\operatorname{card} f_*X \leq \operatorname{card} X$. Однако по 3.1.7 для инъективного f множество f_*X равномощно прямому произведению $\prod_{G/H} X$, откуда получаем требуемое неравенство.

В частности, если индекс $f(H)$ в G конечен, то f_* переводит конечные множества в конечные.

Предложение 3.1.10 *Пусть $f\colon H \to G$ — гомоморфизм групп. Рассмотрим функтор $f_!\colon \mathbf{B}_H \to \mathbf{B}_G$, сопряженный слева к функтору f^* сужения группы операторов. Тогда:*

a) *Функтор $f_!$ точен справа, переводит (произвольные) суммы объектов в суммы и сохраняет инициальный объект.*

b) *Функтор $f_!$ переводит непустые (т.е. не изоморфные инициальному) объекты в непустые и связные (т.е. не представляющиеся в виде суммы двух непустых объектов) объекты в связные. Кроме того, функтор $f_!$ индуцирует биекцию между множествами орбит $f_!X/G$ и X/H.*

c) *Пусть $Y \in \operatorname{Ob}\mathbf{B}_H$, $X := f_!Y$, $\eta_Y : Y \to f^*f_!Y = f^*X$ — морфизм, индуцированный сопряженностью функторов $f_!$ и f^*. Пусть $y_0 \in Y$ — произвольный элемент Y, и $x_0 := \eta_Y(y_0) \in X$ — его образ в X (напомним, что как множество $X = f^*X$). Тогда $\operatorname{Stab}_G(x_0) = f\big(\operatorname{Stab}_H(y_0)\big)$, где через $\operatorname{Stab}_G(x_0) = \{g \in G : gx_0 = x_0\}$ обозначен стабилизатор элемента x_0.*

d) *Если $K \subset H$ — произвольная подгруппа, то $f_!(H/K) \cong G/f(K)$, где H/K рассматривается как H-множество, а $G/f(K)$ — как G-множество.*

Доказательство a) Это утверждение формально следует из того, что $f_!$ обладает правым сопряженным и потому сохраняет произвольные индуктивные пределы.

b) Если объект $f_!X$ пуст, то множество $\operatorname{Hom}_G(f_!X, \varnothing_G) \cong \operatorname{Hom}_H(X, \varnothing_H)$ непусто, т.е. существует морфизм из X в пустой объект, откуда следует, что X пуст. Если $p\colon G \to 1$ — гомоморфизм в единичную группу, то, как мы знаем (см. 3.1.6), $p_!(f_!X) \cong f_!X/G$ и $(pf)_!X \cong X/H$, откуда получаем канонический изоморфизм между множествами орбит $f_!X/G \cong X/H$. В частности, если $f_!X$ состоит из не более одной орбиты, то и X тоже.

c) Можно считать, что функтор $f_!$ построен согласно 3.1.4.1, поскольку любые два левых сопряженных функтора к f^* канонически изоморфны. Тогда $X = f_!Y = G_s \times^H Y$, и по 3.1.4.4 $\eta_Y : Y \to f^*f_!Y$ — это H-отображение, переводящее $y \in Y$ в $[e_G, y] \in X$, где e_G — единица группы G. В частности, $x_0 = [e_G, y_0]$; отсюда для любого $g \in G$ получаем $gx_0 = x_0 \Leftrightarrow [g, y_0] = [e_G, y_0] \Leftrightarrow \exists h \in H : (g, hy_0) = (e_G \cdot h, y_0) \Leftrightarrow \exists h \in H : (g, hy_0) = (f(h), y_0) \Leftrightarrow \exists h \in \operatorname{Stab}_H(y_0) : g = f(h)$, откуда $\operatorname{Stab}_G(x_0) = f\big(\operatorname{Stab}_H(y_0)\big)$.

d) Пусть $Y := H/K$, $y_0 \in Y$ — образ единицы при отображении $H \to H/K$. Тогда по b) $X := f_!Y$ — связное непустое G-множество, т.е. G-множество, состоящее ровно из одной орбиты; следовательно, $X \cong G/\operatorname{Stab}_G(x_0)$ для любой точки $x_0 \in X$. Взяв $x_0 = \eta_Y(y_0)$, мы получим, согласно c), что $X \cong G/f(H)$.

Следствие 3.1.10.1 *Для любого H-множества X выполнено неравенство кардиналов $\operatorname{card} f_!X \leq \big(G : f(H)\big) \operatorname{card} X$, где $\big(G : f(H)\big)$ понимается как $\operatorname{card} G/f(H)$. В частности, если индекс $f(H)$ в G конечен, то $f_!$ переводит конечные множества в конечные. Кроме того, если f инъективен, то это неравенство всегда является равенством.*

Доказательство Разлагая X в сумму орбит, мы видим, что можно предполагать X связным, т.е. $X \simeq H/K$ для некоторой подгруппы $K \subset H$. Согласно пункту d) предложения $f_!X \simeq G/f(K)$, откуда $\operatorname{card} f_!X = \big(G : f(K)\big) = \big(G : f(H)\big)\big(f(H) : f(K)\big) \leq \big(G : f(H)\big)\big(H : K\big) = \big(G : f(H)\big) \operatorname{card} X$. Единственным неравенством в этой цепочке было $\big(f(H) : f(K)\big) \leq (H : K)$, которое превращается в равенство для инъективного f.

Предложение 3.1.11 *Пусть $i\colon H \to G$ — вложение подгруппы H в группу G. Обозначим $Z := i_!e_{\mathbf{B}_H} \cong G/H$ (напомним, что этот изоморфизм устанавливается с помощью элемента $z_0 \in X$, который является образом $\eta_{e_{\mathbf{B}_H}} : e_{\mathbf{B}_H} \to i^*i_!e_{\mathbf{B}_H}$). Для любого $Y \in \operatorname{Ob}\mathbf{B}_H$ обозначим через π_Y канонический морфизм Y в финальный объект $e_{\mathbf{B}_H}$.*

Определим функторы $A\colon \mathbf{B}_H \to \mathbf{B}_G/Z$ и $B\colon \mathbf{B}_G/Z \to \mathbf{B}_H$ следующим образом. Функтор A переводит Y в $i_!\pi_Y : i_!Y \to Z$, а B переводит $p\colon X \to Z$ в H-множество $p^{-1}(z_0)$, или, что одно и то же, в расслоенное произведение $i^*X \times_{i^*Z} e_{\mathbf{B}_H}$:

$$\begin{array}{ccc} i^*X \times_{i^*Z} e_{\mathbf{B}_H} & \longrightarrow & e_{\mathbf{B}_H} \\ \downarrow & & \downarrow{\scriptstyle \eta_{e_{\mathbf{B}_H}}} \\ i^*X & \xrightarrow{i^*p} & i^*Z \end{array} .$$

Тогда A и B являются квазиобратными эквивалентностями категорий.

Доказательство Прежде всего, отметим, что как множества i^*X и i^*Z совпадают с X и Z, а $\eta_{e_{\mathbf{B}_H}}$ можно отождествить со вложением $\{z_0\} \to Z$, и потому рассматриваемое расслоенное произведение действительно совпадает с $p^{-1}(z_0)$ как множество; кроме того, оно является подобъектом i^*X, и потому действие H на $p^{-1}(z_0)$ индуцировано действием G на X. Теперь предложение вытекает из следующего утверждения при $T = e_{\mathbf{B}_H}$:

Следствие 3.1.11.1 *Пусть $i\colon H \to G$ — вложение подгруппы H в группу G, T — объект $\mathbf{B}_H$. Рассмотрим функторы $A\colon \mathbf{B}_H/T \to \mathbf{B}_G/i_!T$ и $B\colon \mathbf{B}_G/i_!T \to \mathbf{B}_H/T$, определенные следующим образом. Функтор A переводит $p\colon Y \to T$ в $i_!p\colon i_!Y \to i_!T$, а B переводит $q\colon X \to i_!T$ в обратный образ $i^*q\colon i^*X \to i^*i_!T$ относительно канонического морфизма $\eta_T\colon T \to i^*i_!T$. Тогда A и B являются квазиобратными эквивалентностями категорий.*

Доказательство a) Отметим, что для любого $p\colon Y \to T$ следующий квадрат декартов:

$$\begin{array}{ccc} X & \xrightarrow{p} & T \\ \downarrow{\scriptstyle \eta_X} & & \downarrow{\scriptstyle \eta_T} \\ i^*i_!X & \xrightarrow{i^*i_!p} & i^*i_!T \end{array} .$$

Для доказательства этого факта отождествим согласно 3.1.4.1 и 3.1.4.4 $i_!X$ с $G_s \times^H X$, $i_!T$ с $G_s \times^H T$, η_X с отображением $x \mapsto [e, x]$ и η_T с $t \mapsto [e, t]$, где e — единичный элемент группы G; тогда $i_!p$ переводит $[e, x]$ в $[e, p(x)]$. Вертикальные стрелки этой диаграммы инъективны (см. 3.1.5), поэтому достаточно проверить, что для любых $[g, x] \in i^*i_!X$ и $t \in T$, для которых $[g, p(x)] = [e, t]$ существует $x' \in X$, такой, что $t = p(x')$ и $[g, x] = [e, x']$. В качестве такого x' можно взять gx. Действительно, $[g, p(x)] = [e, t] \Rightarrow \exists h \in H : (g, hp(x)) = (eh, t) \Rightarrow g \in H$ и $t = gp(x)$, откуда $[g, x] = [e, gx]$ и $t = gp(x) = p(gx)$, поскольку p — морфизм H-множеств.

b) Из декартовости этого квадрата немедленно следует, что существует функториальный изоморфизм $\alpha_p\colon p \to BA(p)$. Для того, чтобы построить морфизм $\beta_q\colon AB(q) \to q$, рассмотрим проекцию $\rho\colon Y := i^*X \times_{i^*i_!T} T \to i^*X$ и обозначим через $\rho'\colon i_!Y \to X$ морфизм, соответствующий ρ по сопряженности. Положим $\beta_q := \rho'$; надо еще проверить, что ρ' — это гомоморфизм $i_!T$-объектов, т.е. что $q\rho' = i_!(\sigma)$, где σ — проекция расслоенного произведения на T:

$$\begin{array}{ccc} Y & \xrightarrow{\rho} & i^*X \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle i^*q} \\ T & \xrightarrow{\eta_T} & i^*i_!T \end{array} \qquad \begin{array}{ccc} i_!Y & & \xrightarrow{\rho'} & & X \\ & {\scriptstyle i_!\sigma} \searrow & & \swarrow {\scriptstyle q} & \\ & & i_!T & & \end{array} .$$

Для доказательства равенства морфизмов $q\rho' = i_!\sigma$ достаточно доказать равенство их сопряженных морфизмов $\eta_T\sigma = i^*(q)\rho\colon Y \to i^*i_!T$, выполненное ввиду коммутативности декартового квадрата, изображенного выше.

c) Мы хотим проверить, что β_q — изоморфизм, т.е. что ρ' — изоморфизм. Для этого заметим, что Y есть множество пар (x, t), таких, что $q(x) = [e, t]$ в $i^*i_!T$, и потому $i_!Y = G_s \times^H Y$ есть множество троек (g, x, t), таких, что $q(x) = [e, t]$, отфакторизованное по отношению эквивалентности $(gh, x, t) \sim (g, hx, ht)$; будем обозначать класс такой тройки через $[g, x, t]$. Тогда $\rho'\colon i_!Y \to X$ — это отображение $[g, x, t] \mapsto gx$; обратное к нему задается формулой $\gamma\colon x \to [g, g^{-1}x, t]$, если $q(x) = [g, t]$; несложно видеть, что это отображение корректно определено и действительно обратно к ρ'.

d) Осталось проверить, что $\beta_{A(p)}A(\alpha_p) = 1$ и $B(\beta_q)\alpha_{B(q)} = 1$; мы опускаем эту проверку. Отметим, что доказательство сопряженности B и A использовало только сопряженность $i_!$ и i^*; специфика ситуации использовалась только при доказательстве того, что α и β — изоморфизмы.

Следствие 3.1.11.2 *Пусть $i\colon H \to G$ — инъективный гомоморфизм групп, Z — это G-объект $G/i(H)$.*

a) Категория $\mathbf{B}_H$ эквивалентна категории $\mathbf{B}_G/Z$; эта эквивалентность категорий позволяет отождествить i^* с функтором $X \mapsto (X \times Z \to Z)$ и $i_!$ с $(X \to Z) \mapsto X$.

b) Функтор $i_!$ сохраняет расслоенные произведения и ядра пар морфизмов, а также переводит мономорфизмы в мономорфизмы.

c) Для любого объекта $X \in \mathrm{Ob}\,\mathbf{B}_G$ объект $i_!i^*X$ канонически изоморфен $X \times Z$; при отождествлении $i_!i^*X$ с $X \times Z$ морфизм $\xi_X : i_!i^*X \to X$ отождествляется с проекцией $X \times Z \to Z$.

Замечание 3.1.12 Группа G однозначно определяется своим классифицирующим топосом $\mathbf{B}_G$. Действительно, объект $G_s \in \mathrm{Ob}\,\mathbf{B}_G$ можно охарактеризовать как максимальный связный непустой объект $\mathbf{B}_G$. *Непустота* объекта произвольной категории означает, что он не является инициальным объектом; *связность* означает, что он не представляется в виде суммы двух непустых объектов; наконец, максимальность в данном случае понимается так: для любого непустого связного X существует (неоднозначно определенный) эпиморфизм из G_s в X. Теперь G восстанавливается как группа, противоположная группе автоморфизмов этого объекта: $G = \mathrm{Aut}_{\mathbf{B}_G}(G_s)^{\mathrm{op}}$.

Обозначим через $\mathcal{A}b(\mathbf{B}_G)$ категорию абелевых групп в категории $\mathbf{B}_G$. Объекты этой категории — это четверки $(A, \mu, \sigma, \varepsilon)$, состоящие из объекта $A \in \mathrm{Ob}\,\mathbf{B}_G$ и морфизмов сложения $\mu\colon A \times A \to A$, взятия противоположного элемента $\sigma\colon A \to A$ и нулевого морфизма $\varepsilon\colon e_{\mathbf{B}_G} \to A$, удовлетворяющих обычным аксиомам абелевой группы. Ясно, что задание на G-множестве A структуры абелевой группы равносильно заданию на абелевой группе A действия группы G, согласованного со сложением; таким образом, $\mathcal{A}b(\mathbf{B}_G)$ — это категория G-абелевых групп, или, что одно и то же, левых $\mathbb{Z}[G]$-модулей. Аналогичным образом можно определить кольца (ассоциативные с единицей) в $\mathbf{B}_G$; объекты этой категории — это G-кольца, т.е. кольца с действием группы G, согласованным со сложением и умножением в кольце. Если K — такое кольцо, можно определить категорию (левых) K-модулей в категории $\mathbf{B}_G$, которая в данном случае будет категорией K-G-модулей, т.е. категорией, объекты которой — это «обычные» K-модули M, наделенные действием группы G, согласованным с умножением на скаляры из M, т.е. $g\lambda \cdot gx = g(\lambda \cdot x)$ для любых $g \in G$, $\lambda \in K$ и $x \in M$. Эти определения можно формально распространить на случай произвольной алгебраической структуры γ, определив тем самым категорию $\mathbf{B}_G^\gamma$; см. [13], III.

Обозначения 3.1.13 Для любой группы G обозначим через $\mathcal{A}b(\mathbf{B}_G) = \mathcal{A}b(G)$ категорию абелевых групп в $\mathbf{B}_G$, т.е. категорию G-абелевых групп. Для любой группы G и G-кольца K обозначим через $K\text{-}\mathcal{M}od(\mathbf{B}_G) = K\text{-}\mathcal{M}od(G)$ категорию (левых) K-модулей в $\mathbf{B}_G$, т.е. категорию (левых) K-G-модулей.

Замечание 3.1.14 Предположим, что $\mathcal{C}$ и $\mathcal{D}$ — категории, обладающие конечными проективными пределами (т.е. финальным элементом и расслоенными произведениями), $h\colon \mathcal{C} \to \mathcal{D}$ — точный слева функтор, и пусть, например, $A = (A, \mu, \sigma, \varepsilon)$ — абелева группа в $\mathcal{C}$, т.е. $A \in \mathrm{Ob}\,\mathcal{C}$, $\mu\colon A \times A \to A$, $\sigma\colon A \to A$ и $\varepsilon\colon e_{\mathcal{C}} \to A$, причем эти морфизмы удовлетворяют обычным условиям. Применив к этому набору h, мы получим абелеву группу $hA = (hA, h\mu, h\sigma, h\varepsilon)$, если мы отождествим $h(A \times A)$ с $hA \times hA$ и $he_{\mathcal{C}}$ с $e_{\mathcal{D}}$. Таким образом, любой точный слева функтор $h\colon \mathcal{C} \to \mathcal{D}$ определяет функтор $\mathcal{A}b(h)\colon \mathcal{A}b(\mathcal{C}) \to \mathcal{A}b(\mathcal{D})$, который мы часто будем обозначать той же буквой h. Это определение распространяется на произвольные алгебраические структуры. Например, для любого кольца K в $\mathcal{C}$ определен функтор $K\text{-}\mathcal{M}od(\mathcal{C}) \to hK\text{-}\mathcal{M}od(\mathcal{D})$.

В частности, для любого гомоморфизма групп $f\colon H \to G$ точные слева функторы $f^* = \mathbf{B}_f^*$ и $f_* = \mathbf{B}_{f_*}$ индуцируют функторы $\mathcal{A}b(\mathbf{B}_f^*) = \mathbf{B}_f^{*,ab} = f^{*,ab}\colon \mathcal{A}b(\mathbf{B}_G) \to \mathcal{A}b(\mathbf{B}_H)$ и $\mathcal{A}b(\mathbf{B}_{f_*}) = \mathbf{B}_{f_*}^{ab} = f_*^{ab}\colon \mathcal{A}b(\mathbf{B}_H) \to \mathcal{A}b(\mathbf{B}_G)$. Если мы обозначим через $I_G\colon \mathcal{A}b(\mathbf{B}_G) \to \mathbf{B}_G$ и I_H забывающие функторы, то из определения функторов $f^{*,ab}$ и f_*^{ab} немедленно следует, что $I_H f^{*,ab} = f^* I_G$ и $I_G f_*^{ab} = f_* I_H$, что позволяет часто обозначать функторы $f^{*,ab}$ и f_*^{ab} просто f^* и f_*. Кроме того, легко видеть, что изоморфизм сопряжения $\theta_{X,Y}\colon \mathrm{Hom}_H(f^*X, Y) \cong \mathrm{Hom}_G(X, f_*Y)$ переводит гомоморфизмы абелевых групп в гомоморфизмы абелевых групп (это на самом деле общий факт, при доказательстве которого, помимо сопряженности f^* и f_*, существенно используется точность слева f^*), и потому функторы $f^{*,ab}$ и f_*^{ab} по-прежнему сопряжены, причем изоморфизм сопряжения этих функторов «тот же», что и изоморфизм сопряжения f^* и f_*.

Как обычно, отсюда следует, что $f_*^{ab}\colon \mathcal{A}b(\mathbf{B}_H) \to \mathcal{A}b(\mathbf{B}_G)$ сохраняет произвольные проективные пределы и, в частности, точен слева, а $f^{*,ab}\colon \mathcal{A}b(\mathbf{B}_G) \to \mathcal{A}b(\mathbf{B}_H)$ сохраняет произвольные индуктивные пределы и, в частности, точен справа. Кроме того, $f^{*,ab}$ в данном случае сохраняет произвольные проективные пределы (поскольку проективные пределы G-абелевых групп вычисляются в категории множеств, а $f^{*,ab}$ есть функтор сужения группы операторов относительно $f\colon H \to G$).

Функтор $f_!$ *не* является точным слева и потому не может быть использован для построения функтора $f_!^{ab}$, сопряженного слева к $f^{*,ab}$. Тем не менее такой функтор существует; он может быть определен формулой $f_!^{ab}B = \mathbb{Z}[G] \otimes_H B$, где групповая алгебра $\mathbb{Z}[G]$ рассматривается как (G, H)-абелева группа,

а запись $\mathbb{Z}[G]\otimes_H B$ обозначает тензорное произведение над $\mathbb{Z}[H]$, или, что одно и то же, фактормодуль модуля $\mathbb{Z}[G]\otimes B$ по подмодулю, порожденному элементами вида $gh\otimes b - g\otimes hb$. Функтор f_*^{ab} также можно описать аналогичным образом: $f_*^{ab}(B) = \mathrm{Hom}_H(G_d, B) \cong \mathrm{Hom}_H(\mathbb{Z}[G], B) = \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], B)$, где $\mathbb{Z}[G]$ рассматривается как (H,G)-абелева группа. Конечно же, функтор $f_!^{ab}$ перестановочен с произвольными индуктивными пределами и, в частности, точен справа.

Пусть K — кольцо. Мы можем рассматривать его как G-кольцо с тривиальным действием G для любой группы G. Действуя как в случае абелевых групп, можно определить аналоги функторов $f^{*,ab}$, f_*^{ab} и $f_!^{ab}$ для категорий K-модулей на $\mathbf{B}_G$ и $\mathbf{B}_H$. Тем не менее ничего существенно нового здесь не получается, поскольку все эти функторы, включая соответствующий вариант $f_!$, согласуются с ранее построенными функторами категорий абелевых групп (т.е. выполнены очевидные условия коммутативности, включающие в себя забывающие функторы из категорий K-модулей в категории абелевых групп). Поэтому мы обозначаем эти функторы так же, как и соответствующие функторы категорий абелевых групп. Если B — это K-H-модуль, то формулы для f_*B и $f_!^{ab}B$, данные выше, можно переписать в виде $f_*B = \mathrm{Hom}_H(G_d, B) \cong \mathrm{Hom}_H(K[G], B) = \mathrm{Hom}_{K[H]}(K[G], B)$ и $f_!^{ab}B = K[G]\otimes_{KH} B$.

Замечание 3.1.15 Забывающий функтор $I\colon \mathcal{A}b(\mathbf{B}_G) \to \mathbf{B}_G$ обладает левым сопряженным $L\colon \mathbf{B}_G \to \mathcal{A}b(\mathbf{B}_G)$ — это функтор порождения свободной абелевой группы, переводящий G-множество X в свободную абелеву группу $L(X) = \mathbb{Z}^{(X)}$, на которой G действует, переставляя прямые слагаемые, т.е. $g\cdot[x] = [g\cdot x]$, где $g\in G$, $x\in X$, а $[x]\in\mathbb{Z}^{(X)}$ — соответствующая образующая. Если $f\colon H\to G$ — гомоморфизм групп, то, вычислив сопряженный слева функтор к $I_G f_*^{ab} = f_* I_H$, получаем канонический изоморфизм $f^{*,ab}L_G \cong L_H f^*$. Аналогично из $I_H f_{*,ab} = f_* I_G$ получаем $f_!^{ab} L_H \cong L_G f_!$.

Если K — G-кольцо, то забывающий функтор $I_K\colon K\text{-}\mathcal{M}od(\mathbf{B}_G) \to \mathbf{B}_G$ также обладает левым сопряженным $L_K\colon \mathbf{B}_G \to K\text{-}\mathcal{M}od(\mathbf{B}_G)$. Этот функтор переводит G-множество X в $L_K(X) = K^{(X)}$ с действием G, определенным формулой $g\cdot\sum_{x\in X}\lambda_x[x] = \sum_{x\in X}(g\cdot\lambda_x)[gx]$. Эти функторы перестановочны с $f^{*,ab}$ и $f_!^{ab}$, как и в случае абелевых групп.

Замечание 3.1.16 Практически все факты, доказанные ранее для функторов f^* и f_*, переносятся без изменений на функторы $f^{*,ab}$ и f_*^{ab}. С функтором $f_!^{ab}$ надо обращаться более аккуратно. Например, в ситуации примера 3.1.6 функтор $q^{*,ab} = q^*$ переводит абелеву группу B в соответствующую *постоянную* G-абелеву группу, т.е. в группу B с тривиальным действием G, функтор $q_*^{ab} = q_*$ сопоставляет G-абелевой группе A ее множество неподвижных элементов A^G, а функтор $q_!^{ab}$ переводит A в A_G — факторгруппу A по подгруппе, порожденной элементами вида $ga - a$. Таким образом, правые (соотв. левые) производные функторы функтора q_* (соотв. $q_!^{ab}$) дают в точности когомологии (соотв. гомологии) группы G. В обозначениях того же примера функтор p^* переводит G-абелеву группу A в ее саму, лишенную действия G, функтор p_* переводит абелеву группу B в $\mathrm{Hom}(G_d, B) \cong \prod_G B$, где G действует, переставляя сомножители, а $p_!^{ab}$ переводит B в $\mathbb{Z}^{(G_s)}\otimes B = B^{(G_s)}$, где G действует, переставляя прямые слагаемые.

В ситуации примера 3.1.8 для любой G-абелевой группы A G/H-абелева группа f_*A совпадает с A^H, а $f_!A$ — с A_H.

Замечание 3.1.16.1 Пусть, как и в примере 3.1.7, $i\colon H\to G$ — вложение подгруппы H в группу G, B — H-абелева группа, $(s_\alpha)_{\alpha\in G/H}$ — система представителей левых смежных классов G по H. Тогда, как и раньше, $i_*B = \mathrm{Hom}_H(G_d, B)$ отождествляется с абелевой группой $\prod_{G/H} B$ посредством сопоставления H-функции $f\colon G_d\to B$ набора $\big(f(s_\alpha^{-1})\big)_{\alpha\in G/H}$. Опишем теперь $i_!^{ab}B$: это $\mathbb{Z}[G]\otimes_H B \cong \bigoplus_\alpha s_\alpha\mathbb{Z}[H]\otimes_H B \cong \bigoplus_\alpha B \cong B^{(G/H)}$. Иначе говоря, $i_!^{ab}B$ изоморфно (как абелева группа) прямой сумме G/H экземпляров B; при этом всякий элемент $x = i_!^{ab}B = \mathbb{Z}[G]\otimes_H B$ однозначно записывается в виде $x = \sum_\alpha s_\alpha\otimes x_\alpha$, и этому элементу сопоставляется набор $(x_\alpha)\in B^{(G/H)}$. Опишем действие G на $i_!^{ab}B$ в терминах этого сопоставления. Несложно видеть, что если $gx = \sum_\alpha s_\alpha\otimes y_\alpha$, то $y_\beta = hx_\alpha$, если, как в примере 3.1.7, $gs_\alpha = s_\beta h$. Отметим, что i_*B есть множество наборов $(x_\alpha)\in\prod_{G/H}B$ с действием группы G, определенным той же формулой; тем самым мы определили мономорфизм G-абелевых групп $\sigma\colon i_!^{ab}B\to i_*B$, который является изоморфизмом, если множество G/H конечно. В действительности этот морфизм не зависит от выбора системы представителей (s_α), поскольку он совпадает с морфизмом $N_{f,B}$ из следующего определения.

Определение 3.1.17 *Пусть $f\colon H\to G$ — гомоморфизм групп с конечным ядром. Для любой H-абелевой группы определим гомоморфизм H-абелевых групп $N'_{f,B}\colon B\to f^*f_*B = \mathrm{Hom}_H(G_d, B)$ формулой $N'_{f,B}(b) = \varphi_b$, где $\varphi_b(g) = \sum_{h\in f^{-1}(g)} hb$. Обозначим также через $N_{f,B}\colon f_!^{ab}B\to f_*B$ морфизм*

G-абелевых групп, соответствующий морфизму $N'_{f,B}$ по сопряженности. Наконец, обозначим через $N'_f\colon 1_{\mathbf{B}_H} \to f^*f_*$ и $N_f\colon f_!^{ab} \to f_*$ соответствующие естественные преобразования функторов.

Проверка корректности этого определения сводится к проверке того, что $\varphi_b\bigl(f(h')g\bigr) = h'\varphi_b(g)$ и $\varphi_{h'b}(g) = \bigl(f(h')\varphi_b\bigr)(g)$; обе эти формулы проверяются непосредственно.

Предложение 3.1.18 *Сохраним обозначения предыдущего определения, и, кроме того, обозначим через n порядок ядра f. Тогда:*

a) *если f инъективен, то $N_{f,B}$ инъективен для любого B; если, кроме того, индекс $f(H)$ в G конечен, то все $N_{f,B}$ — изоморфизмы;*

b) *для любого H-модуля B, для которого гомотетия $n_{f_!B}$ умножения на n инъективна, гомоморфизм $N_{f,B}$ инъективен; если индекс $f(H)$ в G конечен, а гомотетия n_B биективна, то $N_{f,B}$ является изоморфизмом.*

Доказательство a) Это утверждение немедленно следует из рассуждений замечания 3.1.16.1 для $i = f$, если только мы проверим, что морфизм $\sigma\colon i_!B \to i_*B$, определенный в замечании, совпадает с $N_{f,B}$. Для этого достаточно проверить равенство соответствующих по сопряжению морфизмов $N'_{f,B}$ и $\sigma' = i^*(\sigma)\eta_B^{ab}\colon B \to i^*i_!B$, где $\eta_B^{ab}\colon B \to f^*f_!^{ab}B$ — канонический морфизм. При отождествлении из замечания 3.1.16.1 морфизм η_B^{ab} отождествляется с морфизмом, сопоставляющим $b \in B$ набор $(b_\alpha)_{\alpha\in G/H}$, такой, что $b_\varepsilon = s_\varepsilon^{-1}b$ и $b_\alpha = 0$ при $\alpha \neq \varepsilon$, где ε — класс единицы в G/H. Затем σ переводит этот набор в функцию $\varphi'_b\colon G_d \to B$, определенную этим же набором; согласно 3.1.7 получаем, что $\varphi'_b(h) = hb$ при $h \in H$ и $\varphi'_b(g) = 0$ при $g \notin H$, т.е. $\varphi'_b = \varphi_b$ и потому $\sigma' = N'_{f,B}$.

b) Рассмотрим сначала случай, когда $f\colon H \to G$ — сюръективный гомоморфизм с ядром K. Тогда $f_!^{ab}B$ отождествляется с B_K, а f_*B с B^K; при этом, как несложно видеть, канонический морфизм $\eta_B^{ab}\colon B \to f^*f_!^{ab}B$ отождествляется с каноническим эпиморфизмом $\pi\colon B \to B_K$, а $\eta'_B\colon f^*f_*B \to B$ отождествляется со вложением $\lambda\colon B \to B^K$; поэтому $N'_{f,B}$ отождествляется с морфизмом $N'\colon B \to B^K$, переводящим b в $\sum_{h\in K} hb$. Ввиду равенства $f^*(N_{f,B})\eta_B^{ab} = N'_{f,B}$ мы получаем, что $N = N_{f,B}\colon B_K \to B^K$ — это отображение, переводящее класс элемента $b \in B$ в элемент $\sum_{h\in K} hb \in B^K$. Теперь непосредственно видно, что $N\pi\lambda = n_{B^K}$ и $\pi\lambda N = n_{B_K}$; поэтому, если n_{B_K} инъективен, то и N инъективно; если же n_B биективен, то $N\mu = 1_{B^K}$ и $\mu N = 1_{B_K}$ при $\mu = \pi n_B^{-1}\lambda$, и потому N — изоморфизм.

В общем случае разложим $f\colon H \to G$ в композицию сюръективного гомоморфизма $p\colon H \to I$ и вложения $i\colon I \to G$, где $I = f(H)$. Отождествим $f_!^{ab}B$ с $i_!^{ab}p_!^{ab}B$ и f_*B с i_*p_*B; тогда морфизм $N_{f,B}\colon i_!^{ab}p_!^{ab}B \to i_*p_*B$ отождествляется с $N_{i,p_*B}i_!(N_{p,B})$. Проверка этого факта применением сначала сопряженности $p_!^{ab}$ и p^*, а затем $i_!^{ab}$ и i^* сводится к проверке того, что $N'_{f,B} = p^*(N'_{i,p_*B})N'_{p,B}\colon B \to p^*i^*i_*p_*B$. Это условие проверяется непосредственно исходя из определения 3.1.17 и из явной конструкции изоморфизма $i_*p_*B \cong f_*B$. Если гомотетия умножения на n в абелевой группе $f_!B \cong i_!p_!B$ инъективна, то и гомотетия $n_{p_!B}$ инъективна, поскольку $i_!p_!B$ изоморфна прямой сумме $(G : H)$ экземпляров $p_!B$. По доказанному для сюръективного случая $N_{p,B}$, а значит, и $i_!N_{p,B}$ инъективен, и к тому же N_{i,p_*B} инъективен по пункту a). Поэтому и $N_{f,B}$ инъективен. В том случае, если n_B биективна, а индекс $f(H)$ в G конечен, $N_{p,B}$ является изоморфизмом, а значит, $N_{f,B} = N_{i,p_*B}i_!(N_{p,B})$ тоже.

Следствие 3.1.18.1 *a) Для любого инъективного гомоморфизма групп $f\colon H \to G$, образ которого является подгруппой конечного индекса в G, естественное преобразование $N_f\colon f_!^{ab} \to f_*^{ab}$ является изоморфизмом, каждый из функторов $f_!^{ab}$ и f_*^{ab} обладает одновременно и левым, и правым сопряженным функтором, точен, строг и сохраняет произвольные индуктивные и проективные пределы.*

b) Для любого гомоморфизма групп $f\colon H \to G$ с конечным ядром порядка n и любого кольца K, в котором образ целого числа n обратим, утверждение пункта a) верно, если ограничиться рассмотрением категорий K-модулей, т.е. если рассмотреть функторы $f_!^{ab}$ и f_*^{ab} как функторы из K-$\mathcal{M}od(\mathbf{B}_H)$ в K-$\mathcal{M}od(\mathbf{B}_G)$.

Замечание 3.1.18.2 В частности, в условиях следствия функтор f_*^{ab} обладает правым сопряженным $f^! = f^{!,ab}$, а функтор $f_!^{ab}$ обладает левым сопряженным $f^? = f^{?,ab}$. Оба функтора $f^{!,ab}$ и $f^{?,ab}$ изоморфны функтору $f^{*,ab}$ и потому сохраняют какие угодно индуктивные и проективные пределы.

Определение 3.1.19 *Пусть G — группа. Для любых двух объектов $X, Y \in \mathbf{B}_G$ обозначим через $Hom_{\mathbf{B}_G}(X,Y)$ или просто $Hom(X,Y)$ множество отображений $\varphi\colon X \to Y$ с действием G, заданным формулой $(g\varphi)(x) = g\colon \varphi(g^{-1}x)$. Объект $Hom(X,Y)$ есть* Hom-объект *в категории $\mathbf{B}_G$, т.е. объект, представляющий функтор $S \mapsto \mathrm{Hom}_G(S \times X, Y)$; иначе говоря, имеет место канонический изоморфизм трифункторов $\mathrm{Hom}_G(S \times X, Y) \cong \mathrm{Hom}_G(S, Hom(X,Y))$.*

Если A и B — G-абелевы группы (соотв., K-G-модули, где K — G-кольцо), то через $Hom_G^{ab}(A,B)$ (соотв. $Hom_K(A,B)$) мы обозначим подобъект в $Hom_G(A,B)$, образованный гомоморфизмами абелевых групп (соотв. K-линейными отображениями), наделенный естественной структурой G-абелевой группы (соотв. G-абелевой группы и, в случае коммутативного K, K-G-модуля).

Наконец, для любых двух G-абелевых групп A и B (соотв. для правого K-G-модуля A и левого K-G-модуля B) обозначим через $A \otimes B$ (соотв. $A \otimes_K B$) обычное тензорное произведение, наделенное структурой G-абелевой группы (соотв., K-G-модуля в том случае, если K коммутативно) по правилу $g(a \otimes b) = ga \otimes gb$.

Замечание 3.1.19.1 Пусть $f\colon H \to G$ — гомоморфизм групп, X, X' — G-объекты. Тогда, как несложно видеть, $f^* Hom(X,X') \cong Hom(f^*X, f^*X')$.

3.2 Категория G-множеств: проконечный случай

Обсудим теперь изменения, необходимые для проконечного случая.

Определение 3.2.1 *Для любой проконечной группы G обозначим через $\mathbf{B}_G$ категорию* дискретных G-множеств, *т.е. G-множеств X, для которых действие $G \times X \to X$ непрерывно, если наделить X дискретной топологией. Будем называть $\mathbf{B}_G$* классифицирующим топосом *проконечной группы G. Аналогично определению 3.1.1 обозначим категорию конечных дискретных G-множеств через $\mathbf{b}_G$ и обозначим через $e_{\mathbf{B}_G}$ и $\varnothing_{\mathbf{B}_G} = \varnothing_G$ финальный и инициальный объекты категории $\mathbf{B}_G$ (и $\mathbf{b}_G$).*

В категории $\mathbf{B}_G$ существуют произвольные проективные и индуктивные пределы, причем конечные проективные и произвольные индуктивные пределы «можно вычислять в категории множеств».

Для любого непрерывного *гомоморфизма проконечных групп $f\colon H \to G$ обозначим через $f^*\colon \mathbf{B}_G \to \mathbf{B}_H$ функтор сужения группы операторов вдоль f. Обозначим (всегда существующий) правый сопряженный функтор к f^* через f_*, а левый сопряженный (если он существует) — через $f_!$. Функтор f_* перестановочен с произвольными проективными пределами (и потому точен слева); функтор f^* точен (слева и справа) и сохраняет произвольные индуктивные пределы. В том случае, если существует функтор $f_!$, он сохраняет произвольные индуктивные пределы, а f^* — произвольные проективные пределы.*

В дальнейшем для любой проконечной группы G мы будем рассматривать только дискретные G-множества, если не оговорено противное. Для того, чтобы указать, что на G-множестве X задана топология, отличная от дискретной, мы будем называть X топологическим G-множеством.

Аналогично 3.1.13 определим категории $\mathcal{A}b(\mathbf{B}_G) = \mathcal{A}b(G)$ и K-$\mathcal{M}od(\mathbf{B}_G) = K$-$\mathcal{M}od(G)$ и функторы $f^{*,ab} = f^*$, $f_*^{ab} = f_*$, а также функтор $f_!^{ab}$, сопряженный слева к $f^{*,ab}$, если такой функтор существует.

Замечание 3.2.1.1 Отметим, что любое G-множество X записывается в виде $X = \bigcup_U X^U$, где U пробегает множество всех открытых нормальных делителей G, а X^U, как обычно, обозначает множество U-неподвижных точек в X (напомним, что мы рассматриваем только дискретные G-множества). Эту же формулу можно записать в виде $X = \varinjlim_U X^U$, причем индуктивный предел берется по фильтрующемуся множеству индексов, и все морфизмы перехода $X^U \to X^V$ инъективны.

Опишем теперь, каким образом в категории $\mathbf{B}_G$ вычисляются проективные пределы. Для любого функтора $F\colon \mathcal{I} \to \mathbf{B}_G$ мы определим $\varprojlim F$ следующим образом: $\varprojlim_{\mathcal{I}} F_\iota = \varinjlim_U \varprojlim_{\mathcal{I}} F_\iota^U$. Другое возможное описание этого предела таково: вычислим сначала $X' = \varprojlim_{\mathcal{I}} F_\iota$ в категории топологических G-множеств, т.е. в категории топологических пространств с непрерывным действием G, и затем возьмем наибольшее дискретное G-подмножество X в X', т.е. множество точек из X', стабилизатор которых открыт, или, что одно и то же, объединение $X = \bigcup_U X'^U$. Тогда это G-множество X и будет искомым проективным пределом в категории $\mathbf{B}_G$.

Замечание 3.2.1.2 Пусть $f\colon H \to G$ — непрерывный гомоморфизм проконечных групп. Опишем, каким образом для данного H-множества Y строится $f_*(Y)$. Одна из возможных конструкций такова:

$f_*(Y) = \varinjlim_U f_{U*}\bigl(Y^{f^{-1}(U)}\bigr)$, где U пробегает множество всех открытых нормальных делителей группы G и $f_U\colon H/f^{-1}(U) \to G/U$ — гомоморфизм дискретных групп, индуцированный f, а f_{U*} — функтор, определенный в 3.1.3; согласно 3.1.4.1, $f_{U*}Y^{f^{-1}(U)} = \mathrm{Hom}_H\bigl(G/U, Y^{f^{-1}(U)}\bigr)$. Отсюда видно другое возможное описание $f_*(Y)$: это множество всех H-отображений $G \to Y$, пропускающихся через некоторую группу вида G/U (иначе говоря, $f_*(Y)$ состоит из всех *равномерно непрерывных* H-отображений $G \to Y$).

Предложение 3.2.2 *Пусть $f\colon H \to G$ — непрерывный гомоморфизм проконечных групп. Следующие условия равносильны:*

(*i*) *f открыт.*

(*ii*) *Существует функтор $f_!$, сопряженный слева к f^*.*

(*iii*) *Для любого открытого нормального делителя V в H существует G-множество $f_!(H/V)$, представляющее функтор $X \to \mathrm{Hom}_H(H/V, f^*X) \cong (f^*X)^V$.*

(*iii′*) *Для любого открытого нормального делителя V в H функтор $X \to (f^*X)^V$ перестановочен с фильтрующимися проективными пределами.*

(*iv*) *Функтор f^* перестановочен с произвольными проективными пределами.*

(*iv′*) *Функтор f^* перестановочен с фильтрующимися проективными пределами.*

Если эти условия выполнены, то $f_!$ можно определить равенством $f_!Y = G_s \times^H Y$ (см. 3.1.4.1), и, кроме того, определен функтор $f_!^{ab}\colon \mathcal{A}b(\mathbf{B}_H) \to \mathcal{A}b(\mathbf{B}_G)$, сопряженный слева к $f^{*,ab}$, причем $f_!^{ab}$ можно определить формулой $f_!^{ab}B = \mathbb{Z}[G] \otimes_H B$.

Доказательство (*i*)⇒(*ii*): Положим, как в 3.1.4.1, $f_!Y := G_s \times^H Y$; поскольку для любого элемента $[g, y] \in f_!Y$ выполнено равенство $\mathrm{Stab}_G([g, y]) = g\,\mathrm{Stab}_G([e_G, y])g^{-1} = gf\bigl(\mathrm{Stab}_H(y)\bigr)g^{-1}$ (см. 3.1.10) и f открыт, стабилизатор любого элемента $f_!Y$ открыт и потому $f_!Y$ является дискретным G-модулем. Тот факт, что $f_!$ сопряжен слева к f^*, следует теперь из 3.1.4.1.

Импликации (*ii*)⇒(*iii*) и (*ii*)⇒(*iv*)⇒(*iv′*) очевидны; кроме того, (*iii*)⇒(*iii′*), поскольку всякий представимый функтор перестановочен с произвольными проективными пределами. Импликация (*iii′*)⇒(*iv*) следует из того факта, что семейство функторов $(F_V\colon Y \mapsto Y^V)_V$ *консервативно*, т.е. всякий морфизм, одновременно переводимый всеми этими функторами в изоморфизм, является изоморфизмом; это утверждение немедленно следует из того, что для любого $Y \in \mathrm{Ob}\,\mathbf{B}_H$ выполнено $Y = \varinjlim_V Y^V$.

Докажем (*iv′*)⇒(*i*). Пусть V — произвольная открытая подгруппа в H. Обозначим через $\mathfrak{U}$ множество открытых подгрупп $U \subset G$, содержащих $f(V)$, и для каждого $U \in \mathfrak{U}$ обозначим $X_U := G/U$. Рассмотрим проективный предел $X := \varprojlim_{\mathfrak{U}} X_U$ в $\mathbf{B}_G$; по предположению f^*X отождествляется с $\varprojlim_{\mathfrak{U}} f^*X_U$. Кроме того, обозначим через X' проективный предел X_U в категории множеств (или топологических пространств); согласно 3.2.1.1, X (соотв. f^*X) отождествляется с подмножеством точек $x \in X'$, стабилизатор которых в G (соотв. в H) открыт. Рассмотрим точку $\xi \in X'$, являющуюся образом единицы группы G при канонической проекции $G \to X'$. Отметим, что $\mathrm{Stab}_H(\xi) \supset V$ и потому $\xi \in f^*X$, и, поскольку мы отождествили f^*X с X, $\xi \in X$, т.е. $\mathrm{Stab}_G(\xi) = \bigcap_{\mathfrak{U}} U$ открыт в G. Осталось заметить, что $\bigcap_{\mathfrak{U}} U = f(V)$, поскольку $f(V)$ — компактная подгруппа в G.

Нам осталось доказать, что функтор $f_!^{ab}B$, определенный равенством $f_!^{ab}B = \mathbb{Z}[G] \otimes_H B$, корректно определен для открытого f (тот факт, что $f_!^{ab}$ сопряжен слева к $f^{*,ab}$, будет следовать тогда из общих соображений). Для этого возьмем произвольный элемент $\alpha = \sum_{1 \le i \le n} g_i \otimes \alpha_i \in f_!^{ab}B$ и заметим, что стабилизатор $\mathrm{Stab}_G(\alpha) \supset \bigcap_{1 \le i \le n} g_i f\bigl(\mathrm{Stab}_H(\alpha_i)\bigr)g_i^{-1}$ открыт в G.

Замечание 3.2.2.1 Из общих свойств проконечных групп (например, из их характеризации как компактных вполне несвязных групп) следует, что условие (*i*) предложения 3.2.2 эквивалентно любому из следующих условий:

(*i′*) Образ $f(H)$ открыт в G.

(*i″*) $f(H)$ — подгруппа конечного индекса в G.

Замечание 3.2.3 Практически все результаты, доказанные в 3.1 для случая дискретных групп, переносятся без изменений на проконечный случай, если договориться рассматривать утверждения, касающиеся функторов $f_!$, только в том случае, если гомоморфизм групп f открыт, или, что согласно замечанию 3.2.2.1 одно и то же, если индекс $f(H)$ в G конечен. Так, 3.1.6 остается без изменений, за исключением утверждения про $p_!$, которое имеет смысл только в том случае, если G конечна. Аналогично, утверждение про $i_!$ из примера 3.1.7 имеет смысл только в том случае, если индекс $(G:H)$ конечен. Пример 3.1.8 не нуждается в изменениях, как и все утверждения про сюръективные гомоморфизмы групп, поскольку все сюръективные гомоморфизмы проконечных групп заведомо открыты.

Единственное принципиальное изменение, оставшееся неотмеченным, касается определения 3.1.19, в котором нужно теперь определять $Hom_G(X,Y)$ как наибольшее дискретное G-множество, содержащееся во множестве отображений $\varphi\colon X \to Y$ с действием G, определенным формулой $(g\varphi)(x) = g\cdot\varphi(g^{-1}x)$. Иначе говоря, $Hom_G(X,Y)$ есть множество отображений $\varphi\colon X \to Y$, являющихся U-отображениями для какой-нибудь открытой подгруппы U в G, т.е. $\varphi(gx) = g\varphi(x)$ для любых $g \in U$ и $x \in X$.

Замечание 3.2.4 Отметим, что для любой проконечной (и тем более конечной) группы G категории $\mathbf{b}_G$ и $\mathbf{B}_G$ полностью определяют друг друга. А именно, категорию $\mathbf{b}_G$ можно построить как полную подкатегорию в $\mathbf{B}_G$, образованную *локально конечными* объектами $\mathbf{B}_G$, т.е. такими $X \in \operatorname{Ob}\mathbf{B}_G$, для которых существует эпиморфизм $T \to e_{\mathbf{B}_G}$, такой, что T-объект $X \times T \to T$ изоморфен сумме объектов $T \to T$. Наоборот, можно восстановить категорию $\mathbf{B}_G$ по $\mathbf{b}_G$, рассмотрев категорию $\mathcal{I}nd(\mathbf{b}_G)$ Ind-объектов категории $\mathbf{b}_G$, т.е. категорию, объектами которой являются индуктивные системы "$\varinjlim$"$_\alpha X_\alpha = (I, X_\alpha, \varphi_{\alpha\beta})$, где I — малое фильтрующееся упорядоченное множество, $X_\alpha \in \operatorname{Ob}\mathbf{b}_G$, $\varphi_{\alpha\beta}\colon X_\alpha \to X_\beta$ при $\alpha \le \beta$ — морфизмы перехода; морфизмы в $\mathcal{I}nd(\mathbf{b}_G)$ определяются равенством $\operatorname{Hom}_{\mathcal{I}nd(\mathbf{b}_G)}(\text{"}\varinjlim\text{"}_\alpha X_\alpha, \text{"}\varinjlim\text{"}_\gamma Y_\gamma) := \varprojlim_\gamma \varinjlim_\alpha \operatorname{Hom}_{\mathbf{b}_G}(X_\alpha, Y_\gamma)$.

В действительности данная выше характеризация $\mathbf{b}_G$ как полной подкатегории в $\mathbf{B}_G$ верна и для произвольной дискретной группы G; однако для произвольной дискретной группы G категория $\mathcal{I}nd(\mathbf{b}_G)$ эквивалентна вовсе не категории $\mathbf{B}_G$, а категории $\mathbf{B}_{\widehat{G}}$, где через $\widehat{G}$ обозначено проконечное пополнение группы G.

Кроме того, несложно проверить, что любая из категорий $\mathbf{B}_G$ или $\mathbf{b}_G$ однозначно определяет проконечную группу G.

Определение 3.2.5 *Пусть R — кольцо (ассоциативное, с единицей), G — проконечная группа. Мы будем говорить, что* порядок группы G обратим в R, *если порядок любой дискретной факторгруппы группы G обратим в R. Мы будем говорить, что абелева группа A* однозначно делима на порядок G, *или что* порядок G обратим в A, *если порядок группы G обратим в кольце эндоморфизмов абелевой группы A.*

Отметим, что в том случае, если группа G конечна, терминология, введенная в этом определении, согласуется с обычным словоупотреблением.

Определение 3.2.6 *Пусть G — проконечная группа. Обозначим через μ_G (соотв. ν_G) левоинвариантную (соотв. правоинвариантную) меру Хаара на G, нормированную условием $\mu_G(G) = 1$ (соотв. $\nu_G(G) = 1$). Для любой (дискретной) абелевой группы A, в которой обратим порядок группы G, и любого* непрерывного *отображения $f\colon G \to A$ определим* интеграл *или* среднее значение *f на G и обозначим через $\int_G f\,d\mu$, $\int_G f\,d\mu_G$ или $\int_G f(g)\,d\mu_G(g)$ элемент группы A, определенный следующим образом:*

$$\int_G f(g)\,d\mu(g) = \frac{1}{(G:U)} \sum_{x \in G/U} f'(x)$$

где U — открытый нормальный делитель, для которого существует разложение $G \xrightarrow{\varphi} G/U \xrightarrow{f'} A$.

Это определение корректно, т.е. не зависит от выбора U; при этом если A — это множество вещественных чисел или локально выпуклое вещественное пространство, то определенный таким образом интеграл совпадает с обычным интегралом Лебега функции f по мере Хаара μ_G (или ν_G).

Если $M = g_0H$ (соотв. $M = Hg_0$) — левый (соотв. правый) смежный класс по замкнутой подгруппе H и $f\colon M \to A$ — непрерывная функция со значениями в абелевой группе A, в которой обратим порядок группы H, то определим интеграл $\int_M f(g)\,d\mu(g)$ как значение $\int_H f(g_0h)\,d\mu_H(h)$ (соотв.

$\int_H f(hg_0)\,d\mu_H(h)$). *Это определение корректно, т.е. не зависит от выбора g_0; если, кроме того, M является одновременно левым и правым смежным классом по H, то оба варианта данного определения дают одинаковый ответ.*

Если M пусто, положим $\int_M f(g)\,d\mu(g) = 0$.

Обобщим теперь определение 3.1.17:

Определение 3.2.7 *Пусть $f\colon H \to G$ — открытый непрерывный гомоморфизм проконечных групп, B — G-абелева группа, однозначно делимая на порядок ядра $K = \operatorname{Ker} f$. Определим $\widetilde{N}'_{f,B}\colon B \to f^*f_*B \subset \operatorname{Hom}_H(G_d, B)$ формулой $\widetilde{N}'_{f,B}(b) = \varphi_b$, где $\varphi_b(g) = \int_{f^{-1}(g)} hb\,d\mu(h)$. Определим $\widetilde{N}_{f,B}\colon f_!^{ab}B \to f_*^{ab}B$ как морфизм, соответствующий по сопряженности морфизму $\widetilde{N}'_{f,B}$. Обозначим через $\widetilde{N}_f\colon f_!^{ab} \dashrightarrow f_*^{ab}$ частично определенное таким образом естественное преобразование функторов.*

Корректность этого определения проверяется так же, как и корректность 3.1.17, за исключением проверки того, что φ_b действительно принадлежит $f^*f_*B \subset \operatorname{Hom}_H(G_d, B)$, т.е. (3.2.1.2) что для любого b отображение φ_b пропускается через факторгруппу G/U для некоторого открытого нормального делителя $U \subset G$; достаточно взять $U \subset f\big(\operatorname{Stab}_H(b)\big)$.

Отметим, что если ядро f конечно и состоит из m элементов, то $m\widetilde{N}'_{f,B} = N'_{f,B}$ и $m\widetilde{N}_{f,B} = N_{f,B}$, так что в этом случае мы снова получаем понятие из определения 3.1.17 с точностью до умножения на m. Следующее предложение является аналогом предложения 3.1.18:

Предложение 3.2.8 *В условиях определения 3.2.7 морфизм $\widetilde{N}_{f,B}\colon f_!^{ab}B \to f_*^{ab}B$ является изоморфизмом.*

Доказательство Доказательство совершенно аналогично доказательству 3.1.18, с тем отличием, что в сюръективном случае мы сразу получаем $\widetilde{N}\pi\lambda = 1_{B^K}$ и $\pi\lambda\widetilde{N} = 1_{B_K}$.

Следствие 3.2.8.1 *a) Для любого открытого вложения проконечных групп $f\colon H \to G$, естественное преобразование $N_f\colon f_!^{ab} \to f_*^{ab}$ является изоморфизмом, каждый из функторов $f_!^{ab}$ и f_*^{ab} обладает одновременно и левым, и правым сопряженным функтором, точен, строг и сохраняет произвольные индуктивные и проективные пределы.*

b) Для любого открытого гомоморфизма проконечных групп $f\colon H \to G$ и любого кольца K, в котором обратим порядок ядра f (см. 3.2.5), утверждение пункта a) верно, если ограничиться рассмотрением категорий K-модулей, т.е. если рассмотреть функторы $f_!^{ab}$ и f_*^{ab} как функторы из K-$\mathcal{M}od(\mathbf{B}_H)$ в K-$\mathcal{M}od(\mathbf{B}_G)$.

Замечание 3.2.9 В действительности в [13], IV определяется классифицирующий топос $\mathbf{B_G}$ для любой про-группы $\mathbf{G}$; это определение является одновременным обобщением определения классифицирующего топоса дискретной группы и проконечной группы, и потому можно было бы с самого начала излагать всю теорию сразу для про-групп. Нам, однако, такая общность не понадобится; поэтому мы ограничимся напоминанием определений.

Итак, пусть $\mathbf{G} = (G_\alpha, \varphi_{\alpha\beta})_{\alpha,\beta\in I}$ — (строгая) про-группа, т.е. проективная система групп $(G_\alpha)_{\alpha\in I}$, индексированная (малым) фильтрующимся упорядоченным множеством I, в которой все морфизмы перехода $\varphi_{\alpha\beta}\colon G_\beta \to G_\alpha$ *сюръективны* для любых $\alpha \le \beta$. Будем называть $\mathbf{G}$-множеством набор $\mathbf{A} = (A, A_\alpha, \mu_\alpha)_{\alpha\in I}$, где A — множество, $A_\alpha \subset A$, $\bigcup_\alpha A_\alpha = A$, и $\mu_\alpha\colon G_\alpha \times A_\alpha \to A_\alpha$ — действие G_α на A_α, причем эти действия согласованы следующим образом: для любых $\alpha \le \beta$ выполнено $A_\alpha \subset A_\beta$, и $\varphi_{\alpha\beta}(g_\beta)\cdot a_\alpha = g_\beta \cdot a_\alpha$ для любых $g_\beta \in G_\beta$ и $a_\alpha \in A_\alpha$. Кроме того, мы требуем, чтобы для любых $\alpha \le \beta$ было выполнено равенство $A_\beta^{\operatorname{Ker}\varphi_{\alpha\beta}} = A_\alpha$. Теперь можно определить *классифицирующий топос про-группы* $\mathbf{G}$ как категорию всевозможных $\mathbf{G}$-множеств (морфизмы в этой категории определяются естественным образом). Для любого морфизма про-групп $\mathbf{f}\colon \mathbf{H} \to \mathbf{G}$ можно определить функтор сужения про-группы операторов $\mathbf{f}^*$, его (всегда существующий) правый сопряженный $\mathbf{f}_*$ и (существующий только для «открытого» $\mathbf{f}$) левый сопряженный $\mathbf{f}_!$. Ясно, что взяв в качестве $\mathbf{G}$ проективную систему из одного элемента, мы снова получим определения классифицирующего топоса дискретной группы, а взяв в качестве $\mathbf{G}$ проективную систему, состоящую из конечных групп, мы получим определение классифицирующего топоса проконечной группы, являющейся проективным пределом этой системы.

3.3 λ-кольца

Напомним нужные нам положения теории λ-колец; подробное изложение этой теории можно найти, например, в [14], V.

На протяжении всего этого пункта через K обозначено основное кольцо, которое предполагается коммутативным с единицей. Все рассматриваемые кольца и алгебры мы также предполагаем коммутативными с единицей.

Определение 3.3.1 *Для любого (коммутативного) кольца A обозначим через $1+A[[t]]^+$, $\widehat{G}(A)$ или $\widehat{G}^t(A)$ множество формальных степенных рядов из $A[[t]]$, свободный член которых равен единице, рассматриваемое как абелева группа относительно умножения с фильтрацией, определенной следующим образом:* $\mathrm{Filt}^0\,\widehat{G}^t(A)=\widehat{G}^t(A)$ *и* $\mathrm{Filt}^n\,\widehat{G}^t(A)=1+t^nA[[t]]$ *при* $n\geq 1$. *В том случае, если для обозначения переменной вместо t используется другая буква, это соответствующим образом отражается в записи $\widehat{G}^t(A)$.*

Таким образом, мы определили функтор $\widehat{G}$ из категории колец в категорию фильтрованных абелевых групп, который можно также рассматривать как функтор, определенный на категории K-алгебр.

Отметим, что любое естественное преобразование функторов $\eta\colon \widehat{G}\to\widehat{G}$ однозначно определяется значением $\theta=\eta_{K[X]}(1+Xt)$ (см. [14], V 1.6). Приведем набросок доказательства этого факта:

a) Прежде всего, знание θ позволяет определить $\eta_A(1+at)$ для любой K-алгебры A и любого элемента $a\in A$. Действительно, если $f\colon K[X]\to A$ — гомоморфизм K-алгебр, переводящий X в a, то $\eta_A(1+at)=\eta_A\bigl(\widehat{G}^t(f)(1+Xt)\bigr)=\widehat{G}^t(f)\bigl(\eta_{K[X]}(1+Xt)\bigr)=\widehat{G}^t(f)(\theta)$.

b) В частности, можно взять $A=K[T_1,\ldots,T_n]$, $a=T_i$; мы уже знаем, что θ определяет $\eta_A(1+T_it)$, а потому и $\eta_A\bigl((1+T_1t)\cdots(1+T_nt)\bigr)=\eta_A(1+T_1t)\cdots\eta_A(1+T_nt)$ ввиду аддитивности η_A.

c) Обозначим через i вложение $A'=K[X_1,\ldots,X_n]$ в $A=K[T_1,\ldots,T_n]$, переводящее X_k в k-ый симметрический многочлен от переменных T_j. Тогда $\widehat{G}^t(i)$ переводит $\alpha_n:=1+X_1t+X_2t^2+\cdots+X_nt^n$ в $(1+T_1t)\cdots(1+T_nt)$, и потому $\widehat{G}^t(i)\bigl(\eta_{A'}(\alpha_n)\bigr)$ совпадает с $\eta_A(1+T_1t)\cdots\eta_A(1+T_nt)$. Все коэффициенты этого формального степенного ряда являются симметрическими функциями от T_j, и потому этот ряд однозначно представляется в виде $\widehat{G}^t(i)(\theta_n)$. Ввиду инъективности $\widehat{G}^t(i)$ отсюда получаем $\eta_{A'}(\alpha_n)=\theta_n$.

d) Знание $\theta_n:=\eta_{K[X_1,\ldots,X_n]}(1+X_1t+\cdots+X_nt)$ позволяет определить $\eta_A(1+a_1t+\cdots+a_nt^n)$ для любой K-алгебры A и любых $a_1,\ldots,a_n\in A$: надо, как в пункте a), рассмотреть гомоморфизм K-алгебр $f\colon K[X_1,\ldots,X_n]\to A$, переводящий X_i в a_i, и тогда $\eta_A(1+a_1t+\cdots+a_nt^n)=\widehat{G}(f)(\theta_n)$.

e) Поскольку η_A сохраняет фильтрацию, мы видим, что для произвольного ряда $\xi=1+a_1t+\cdots+a_nt^n+\cdots$ формальные ряды $\eta_A(\xi)$ и $\eta_A(1+a_1t+\cdots+a_nt^n)$ сравнимы по модулю t^{n+1}; переходя к пределу по n, мы видим, что значение $\eta_A(\xi)$ однозначно определено.

Отметим, что верно и обратное (см. [14], V 1.6): любой формальный ряд $\theta\in\widehat{G}^t(K[T])$ задает естественное преобразование функторов θ, если только выполнено следующее «условие непрерывности»: для любого $n\geq 2$ выполнено $\pi_n(\theta_n)\equiv\theta_{n-1}\pmod{t^n}$, где $\pi_n\colon K[X_1,\ldots,X_n]\to K[X_1,\ldots,X_{n-1}]$ — гомоморфизм K-алгебр, переводящий X_n в 0 и сохраняющий остальные X_i, а θ_{n-1} и θ_n — элементы, определенные исходя из θ в п. c) выше. Обычно это условие проверяется следующим образом: все рассматриваемые алгебры многочленов наделяются градуировкой, относительно которой T_i имеет степень 1, а X_i — степень i; затем проверяется, что, если в коэффициент при t^n в θ входят только одночлены степени $\geq n$, то аналогичным свойством обладают и все θ_n; поэтому X_n не входит в коэффициенты при t^i, $i<n$, в θ_n, что немедленно дает «условие непрерывности».

Аналогичные утверждения можно доказать про естественные преобразования $\eta\colon\widehat{G}\times\widehat{G}\to\widehat{G}$, аддитивные и согласующиеся с фильтрацией по каждой из переменных: любое такое η задается своим значением $\theta:=\eta_{K[X,Y]}(1+Xt,1+Yt)$. Более того, в действительности таким же образом доказывается, что любое естественное преобразование $\eta\colon\widehat{G}^n\to H$, аддитивное и согласованное с фильтрацией по каждому аргументу, задается своим значением на наборе $(1+Y_1t,\ldots,1+Y_nt)$, если предполагать, что H — это функтор из категории K-алгебр в категорию *полных* фильтрованных абелевых групп, перестановочный с операцией взятия инвариантов относительно конечной группы автоморфизмов (т.е. если

конечная группа G действует на K-алгебре A, то канонический морфизм $H(A^G) \to H(A)^G$ является автоморфизмом). Конечно же, функтор $\widehat{G}$ обладает этим свойством.

Определение 3.3.2 *Обозначим через $\circ$ естественное преобразование функторов $\widehat{G} \times \widehat{G} \to \widehat{G}$, определенное равенством $(1+Xt)\circ(1+Yt) = 1+XYt$ в $\widehat{G}^t(K[X,Y])$.*

Для любой K-алгебры A отображение $\circ_A \colon \widehat{G}^t(A) \times \widehat{G}^t(A) \to \widehat{G}^t(A)$ аддитивно по каждой из переменных и потому определяет на $\widehat{G}^t(A)$ структуру кольца. В дальнейшем мы будем всегда предполагать $\widehat{G}^t(A)$ наделенным этой структурой кольца.

Отметим, что $\widehat{G}^t(A)$ является коммутативным ассоциативным кольцом с единицей $1+t$, как немедленно следует из свойств единственности, рассмотренных выше. Например, для проверки ассоциативности надо заметить, что оба возникающих трифунктора принимают одно и то же значение $1+XYZt$ на наборе $(1+Xt, 1+Yt, 1+Zt)$.

Операцию $\circ$ можно задать с помощью универсальных многочленов:

$$(1+a_1t+\cdots+a_nt^n+\cdots)\circ(1+b_1t+\cdots+b_nt^n+\cdots) = 1+P_1t+\cdots+P_nt^n+\cdots$$

Здесь $P_n = P_n(a_1,\ldots,a_n;b_1,\ldots,b_n)$ — это многочлен с целыми коэффициентами, изобарный веса n по каждому из наборов переменных (a_i и b_i приписывается вес i) и симметричный относительно двух наборов переменных. Многочлен P_n можно вычислить, записав коэффициент при t^n в многочлене $\prod_{1\le i,j\le n}(1+\alpha_i\beta_it)$ через основные симметрические функции от (α_i) и (β_i); несколько менее трудоемкий способ нахождения P_n таков: надо заметить, что для любых $f \in \widehat{G}^t(A)$ и $\xi \in A$ верно $f\circ(1+\xi t) = f(\xi t)$ (как всегда, для проверки достаточно взять $f = 1+Xt$, $\xi = Y$), и потому P_n есть коэффициент при t^n в многочлене $f(\beta_1t)f(\beta_2t)\cdots f(\beta_nt)$, где $f = 1+a_1t+\cdots+a_nt^n$, если заменить в этом коэффициенте основные симметрические функции от (β_i) на b_i.

Например, $P_1(a_1;b_1) = a_1b_1$ и $P_2(a_1,a_2;b_1,b_2) = a_2b_1^2 + a_1^2b_2 - 2a_2b_2$.

Определение 3.3.3 Пред-λ-кольцом *называется коммутативное кольцо (с единицей) K, наделенное операциями $\lambda^i \colon K \to K$ для всех целых $i \ge 0$, такими, что $\lambda^0(x) = 1$, $\lambda^1(x) = x$ и $\lambda^n(x+y) = \sum_{i+j=n}\lambda^i(x)\lambda^j(y)$ для любых $x, y \in K$ и $n \ge 0$.*

Если K' — еще одно пред-λ-кольцо и $f \colon K \to K'$ — гомоморфизм колец, то мы будем говорить, что f является λ-гомоморфизмом, *если $\lambda^i(f(x)) = f(\lambda^i(x))$ для любого $i \ge 0$ и $x \in K$.*

Для любого $x \in K$ обозначим через $\lambda_t(x) = \lambda_t^K(x)$ формальный степенной ряд $\lambda^0(x)+\lambda^1(x)t+\cdots+\lambda^n(x)t^n+\cdots \in \widehat{G}^t(K)$. Таким образом, задание на кольце K структуры пред-λ-кольца равносильно заданию гомоморфизма абелевых групп $\lambda_t \colon K \to \widehat{G}^t(K)$, такого, что $\lambda_t(x) \equiv 1+xt \pmod{t^2}$ для любого $x \in K$. При этом $f \colon K \to K'$ является λ-гомоморфизмом в том и только том случае, если $\widehat{G}^t(f)\lambda_t^K = \lambda_t^{K'}f$.

Для любой K-алгебры A (или для любого кольца A) введем на $\widehat{G}^t(A)$ структуру пред-λ-кольца; тем самым мы фактически определим структуру пред-λ-кольца на функторе $\widehat{G}^t$. Для задания структуры пред-λ-кольца на $\widehat{G}^t(A)$ надо задать $\lambda_{u,A} \colon \widehat{G}^t(A) \to \widehat{G}^u(\widehat{G}^t(A))$ для каждого A, т.е. естественное преобразование функторов $\lambda_u \colon \widehat{G}^t \to \widehat{G}^u(\widehat{G}^t)$. Как обычно, достаточно определить $\lambda_{u,K[X]}(1+Xt)$; положим $\lambda_{u,K[X]}(1+Xt) = \{1+t\}+\{1+Xt\}u$. Несложно видеть, что «условие непрерывности» выполнено и что

$$\lambda^i(1+a_1t+\cdots+a_nt^n+\cdots) = 1+Q_{i,1}t+Q_{i,2}t^2+\cdots+Q_{i,j}t^j+\cdots \quad ,$$

где $Q_{i,j} = Q_{i,j}(a_1,a_2,\ldots,a_{ij})$ — некоторый универсальный многочлен с целыми коэффициентами, изобарный веса ij.

Определение 3.3.4 *Пред-λ-кольцо K называется* λ-кольцом, *если гомоморфизм абелевых групп λ_t, определенный выше, является λ-гомоморфизмом пред-λ-кольца K в пред-λ-кольцо $\widehat{G}(K)$.*

Иначе говоря, пред-λ-кольцо является λ-кольцом в том и только том случае, если $\lambda_t(1) = 1+t$, $\lambda_t(xy) = \lambda_t(x)\circ\lambda_t(y)$ и $\lambda_u(\lambda_t(x)) = \widehat{G}^u(\lambda_t)(\lambda_u(x))$ для любых $x, y \in K$. Эти же условия можно выразить поэлементно:

- $\lambda^i(1) = 0$ при $i \ge 2$;

- $\lambda^i(xy) = P_i\big(\lambda^1(x),\dots,\lambda^n(x);\lambda^1(y),\dots,\lambda^n(y)\big)$;
- $\lambda^j\big(\lambda^i(x)\big) = Q_{i,j}\big(\lambda^1(x),\dots,\lambda^{ij}(x)\big)$.

Пример 3.3.5 Пред-λ-кольцо $\widehat{G}^t(A)$ является λ-кольцом для любой K-алгебры A (и любого кольца A). Как обычно, для проверки этого факта достаточно сравнить возникающие естественные преобразования функторов на элементах вида $1+Xt$, для которых все проверки оказываются тривиальными.

Пример 3.3.6 Другой важный пример: на кольце $\mathbb{Z}$ есть единственная структура λ-кольца, заданная условием $\lambda_t(n) = (1+t)^n$ для любого $n \in \mathbb{Z}$. Иначе говоря, $\lambda^i(n) = \binom{n}{i}$. Для любого λ-кольца K единственный гомоморфизм колец $\mathbb{Z} \to K$ является λ-гомоморфизмом, откуда легко выводятся разнообразные формулы вроде $\lambda^k(x+n) = \sum_{0\le i\le k}\lambda^i(n)\lambda^{k-i}(x) = \sum_{0\le i\le k}\binom{n}{i}\lambda^{k-i}(x)$.

Замечание 3.3.7 Помимо λ-операций, на λ-кольцах определяются различные другие операции. Например, *γ-операции* вводятся равенством $\gamma^n(x) = \lambda^n(x+n-1)$ для любых $n \ge 0$ и $x \in K$. Если обозначить $\gamma_t(x) := \sum_{n\ge 0}\gamma^n(x)$, то, как несложно видеть, ряды $\gamma_t(x)$ и $\lambda_t(x)$ получаются друг из друга заменой переменных: $\gamma_s(x) = \lambda_{s/(1-s)}(x)$ и $\lambda_t(x) = \gamma_{t/(1+t)}(x)$.

Можно также определить «симметрические операции» $s^n(x)$ посредством равенства $s_t(x)\lambda_{-t}(x) = 1$, где, как обычно, $s_t(x) = \sum_{n\ge 0} s^n(x)t^n$; поэлементно эти операции задаются соотношениями $s^0(x) = 1$, $\sum_{0\le i\le n}(-1)^i s^{n-i}(x)\lambda^i(x) = 0$ при $n \ge 1$.

Кроме того, на λ-кольцах можно вводить многие другие операции. Так, в разделе 3.6 мы определим *τ-операции* τ^n (см. 3.6.2).

Замечание 3.3.8 Еще один важный класс операций, которые определяются на пред-λ-кольцах — это *операции Адамса* Ψ^k, определенные для $k \ge 1$ равенством

$$\frac{d}{dt}\big(\lambda_t(x)\big)\Big/\lambda_t(x) = \sum_{k\ge 1}(-1)^{k-1}\Psi^k(x)t^{k-1} \tag{3.3.8.1}$$

Основные свойства операций Адамса можно найти в приложении к [14], V. Здесь мы напомним, что всегда $\Psi^k(x+y) = \Psi^k(x)+\Psi^k(y)$, как это немедленно следует из равенства $\lambda_t(xy) = \lambda_t(x)\lambda_t(y)$ и общих свойств логарифмической производной; кроме того, $\Psi^1(x) = x$ для любого $x \in K$. Если пред-λ-кольцо K является λ-кольцом, то

$$\Psi^k(1) = 1; \quad \Psi^k(xy) = \Psi^k(x)\Psi^k(y); \quad \Psi^k \circ \Psi^{k'} = \Psi^{kk'} \quad . \tag{3.3.8.2}$$

Наоборот, если пред-λ-кольцо K свободно от $\mathbb{Z}$-кручения и в нем выполнены эти условия, то оно в действительности является λ-кольцом. На таком кольце λ-операции однозначно определяются операциями Адамса; если оно содержит $\mathbb{Q}$, то любое задание операций Адамса на K, удовлетворяющих перечисленным выше условиям, задает на K структуру λ-кольца.

Отметим, что в λ-кольце $\mathbb{Z}$ все операции Адамса являются тождественными отображениями, а в λ-кольце $\widehat{G}^t(A)$ выполнены соотношения $\Psi^k(1+at) = 1+a^kt$.

Позже нам понадобятся выражения, позволяющие определять λ-операции и симметрические операции исходя из операций Адамса. Для этого заметим, что из (3.3.8.1) и соотношения $s_t(x)\lambda_{-t}(x) = 1$ немедленно следует

$$\frac{d}{dt}\big(s_t(x)\big)\Big/s_t(x) = \sum_{k\ge 1}\Psi^k(x)t^{k-1} \quad . \tag{3.3.8.3}$$

Домножим теперь (3.3.8.1) на $\lambda_t(x)$, (3.3.8.1) на $s_t(x)$ и приравняем в полученных формальных степенных рядах коэффициенты при t^{n-1}, $n \ge 1$. В результате мы получим соотношения

$$\lambda^n(x) = \frac{1}{n}\sum_{k=1}^{n}(-1)^{k-1}\Psi^k(x)\lambda^{n-k}(x) \tag{3.3.8.4}$$

$$s^n(x) = \frac{1}{n}\sum_{k=1}^{n}\Psi^k(x)s^{n-k}(x) \quad . \tag{3.3.8.5}$$

Эти соотношения вместе с равенствами $\lambda^0(x) = s^0(x) = 1$ легко позволяют последовательно находить $\lambda^1(x), \lambda^2(x), \dots$ или $s^1(x), s^2(x), \dots$; для нахождения n-го члена одной из этих двух последовательностей используются все предыдущие, а также $\Psi^1(x),\dots,\Psi^n(x)$.

3.4 Кольцо характеров проконечной группы

Начнем этот раздел с нескольких общих определений.

Определение 3.4.1 *(см. [14], IV 1)* Группа Гротендика $\mathrm{K}(\mathcal{A})$ *(малой) абелевой категории* $\mathcal{A}$ *— это факторгруппа свободной абелевой группы, порожденной объектами* $\mathcal{A}$*, по подгруппе, порожденной элементами вида* $[\xi'] - [\xi] + [\xi'']$ *для всевозможных точных последовательностей* $0 \to \xi' \to \xi \to \xi'' \to 0$*. Образ элемента* $[\xi]$ *в* $\mathrm{K}(\mathcal{A})$ *мы будем называть* классом *объекта* ξ *и будем обозначать его* $\mathrm{cl}\,\xi$ *или* $\mathrm{cl}_{\mathcal{A}}\,\xi$*.*

Кроме того, если $\mathcal{A}'$ *— еще одна (малая) абелева категория,* $h\colon \mathcal{A} \to \mathcal{A}'$ *— точный функтор, то через* $\mathrm{K}(h)$*, а иногда и просто через* h*, мы будем обозначать (однозначно определенный) гомоморфизм абелевых групп, переводящий* $\mathrm{cl}_{\mathcal{A}}\,\xi$ *в* $\mathrm{cl}_{\mathcal{A}'}\,h(\xi)$*.*

Определение 3.4.2 *Пусть* $\mathcal{A}$ *— абелева категория,* B *— абелева группа. Отображение* $f\colon \mathrm{Ob}\,\mathcal{A} \to B$ *называется* аддитивным*, если для любой точной в* $\mathcal{A}$ *последовательности* $0 \to \xi' \to \xi \to \xi'' \to 0$ *выполнено равенство* $f(\xi) = f(\xi') + f(\xi'')$*.*

Пример 3.4.3 a) Ясно, что $\mathrm{cl}\colon \mathrm{Ob}\,\mathcal{A} \to \mathrm{K}(\mathcal{A})$ является аддитивным отображением, притом универсальным в следующем смысле: любое аддитивное отображение $f\colon \mathrm{Ob}\,\mathcal{A} \to B$ представляется в виде $f' \circ \mathrm{cl}$ для некоторого однозначно определенного гомоморфизма абелевых групп $f'\colon \mathrm{K}(\mathcal{A}) \to B$.

b) Функция, сопоставляющая конечномерному векторному пространству его размерность, является аддитивной; ясно, что она индуцирует изоморфизм между группой Гротендика категории конечномерных векторных пространств над некоторым фиксированным телом D и группой целых чисел $\mathbb{Z}$.

c) Если все объекты категории $\mathcal{A}$ имеют конечную длину, то функция $l\colon \mathrm{Ob}\,\mathcal{A} \to \mathbb{Z}$, сопоставляющая любому объекту его длину, является аддитивной. В этом случае мы можем, воспользовавшись теоремой Жордана—Гёльдера, описать структуру $\mathrm{K}(\mathcal{A})$: это есть свободная абелева группа, образующие которой — классы всевозможных простых объектов категории $\mathcal{A}$ (естественно, из каждого класса изоморфных простых объектов мы выбираем по одному представителю). Отсюда следует, что любая аддитивная функция на $\mathcal{A}$ однозначно определяется набором своих значений на классах изоморфности простых объектов, и наоборот, всякий такой набор значений определяет аддитивную функцию.

d) Если $\mathcal{A}$ — это категория конечно порожденных проективных модулей над (коммутативным) кольцом R, спектр которого связен (т.е. в кольце R нет нетривиальных идемпотентов), то функция, сопоставляющая проективному модулю его (однозначно определенный в данном случае) ранг, аддитивна.

Применим теперь эти определения к интересующему нас случаю.

Определение 3.4.4 *Пусть* G *— проконечная группа,* A *— (как обычно, коммутативное)* G*-кольцо. Обозначим через* $\mathrm{K}^{\cdot}(G, A)$ *или* $\mathrm{K}^{\cdot}(G)$*, если понятно, какое* G*-кольцо имеется в виду, группу Гротендика категории* локально проективных A*-*G*-*модулей*, т.е. A*-*G*-модулей, которые являются конечно порожденными проективными* A*-модулями в обычном смысле. Если, кроме того, кольцо* A *нетерово, то обозначим через* $\mathrm{K}_{\cdot}(G, A)$ *или* $\mathrm{K}_{\cdot}(G)$ *группу Гротендика категории* A*-*G*-*модулей конечного типа*, т.е. A*-*G*-модулей, которые являются конечно порожденными* A*-модулями. Наделим* $\mathrm{K}^{\cdot}(G, A)$ *структурой коммутативного кольца с единицей, определив умножение с помощью тензорного произведения:* $\mathrm{cl}\,P \cdot \mathrm{cl}\,Q = \mathrm{cl}(P \otimes_A Q)$*. Аналогично,* $\mathrm{K}_{\cdot}(G, A)$ *наделяется структурой* $\mathrm{K}^{\cdot}(G, A)$*-модуля; определен канонический гомоморфизм* $\mathrm{K}^{\cdot}(G, A)$*-модулей* $\mathrm{K}^{\cdot}(G, A) \to \mathrm{K}_{\cdot}(G, A)$*, переводящий класс в* $\mathrm{K}^{\cdot}(G, A)$ *локально проективного* A*-*G*-модуля в класс этого же модуля в* $\mathrm{K}_{\cdot}(G, A)$*.*

Кроме того, на $\mathrm{K}^{\cdot}(G, A)$ *есть структура пред-*λ*-кольца* (3.3.3)*, однозначно определенная условием* $\lambda^n(\mathrm{cl}\,P) = \mathrm{cl}(\bigwedge_A^n P)$*, где через* $\bigwedge_A^n P$ *обозначена* n*-ая внешняя степень* A*-модуля* P *с действием* G*, определенным формулой* $g \cdot (ax_1 \wedge x_2 \wedge \ldots \wedge x_n) = (ga)(gx_1) \wedge gx_2 \wedge \ldots \wedge gx_n$*.*

Определим на пред-λ*-кольце* $\mathrm{K}^{\cdot}(G, A)$ *инволюцию* $\xi \mapsto \check{\xi}$*, однозначно задаваемую условием* $(\mathrm{cl}\,P)^{\check{}} = \mathrm{cl}\,\check{P}$*, где* $\check{P} = \mathit{Hom}_A(P, A)$ *—* A*-*G*-модуль, двойственный к локально проективному* A*-*G*-модулю* P*.*

Замечание 3.4.4.1 Определение умножения в $\mathrm{K}^{\cdot}(G,A)$ и действия $\mathrm{K}^{\cdot}(G,A)$ на $\mathrm{K}_{\cdot}(G,A)$ корректно, поскольку для любого локально проективного P функтор $M \mapsto P \otimes_A M$ точен как и на категории локально проективных A-G-модулей, так и на категории A-G-модулей конечного типа. Ассоциативность и коммутативность определенного таким образом умножения — это ассоциативность и коммутативность тензорного произведения; единицей в $\mathrm{K}^{\cdot}(G,A)$ является $\mathrm{cl}\, A$.

Замечание 3.4.4.2 Заметим, что на $\mathrm{K}^{\cdot}(G,A)$ действительно есть структура пред-λ-кольца, удовлетворяющая условиям определения. Для доказательства отметим, что отображение λ'_t, переводящее локально проективный A-G-модуль P в ряд $1+\mathrm{cl}\, P\cdot t+\mathrm{cl}(\wedge^2 P)\cdot t^2+\cdots+\mathrm{cl}(\wedge^n P)\cdot t^n+\cdots \in 1+\mathrm{K}^{\cdot}(G,A)[[t]]^+ = \widehat{G}^t\big(\mathrm{K}^{\cdot}(G,A)\big)$, аддитивно, поскольку для любой точной последовательности локально проективных A-G-модулей $0 \to P' \to P \to P'' \to 0$ и для любого $n \geq 0$ на внешней степени $\wedge^n P$ существует каноническая фильтрация длины $n+1$, факторы которой изоморфны $\wedge^k P' \otimes \wedge^{n-k} P''$, где k принимает значения от 0 до n (см. [14], V 2.2.1). Из универсального свойства $\mathrm{K}^{\cdot}(G,A)$ теперь следует существование гомоморфизма абелевых групп $\lambda_t \colon \mathrm{K}^{\cdot}(G,A) \to \widehat{G}^t\big(\mathrm{K}^{\cdot}(G,A)\big)$, такого, что $\lambda'_t = \lambda_t \circ \mathrm{cl}$; согласно замечанию после определения 3.3.3, задание такого гомоморфизма абелевых групп равносильно заданию на $\mathrm{K}^{\cdot}(G,A)$ структуры пред-λ-кольца с нужными нам свойствами.

Замечание 3.4.4.3 Введем в $\mathrm{K}^{\cdot}(G,A)$ симметрические операции s^n с помощью 3.3.7. Тогда для любого локально проективного A-G-модуля M и любого целого $n \geq 0$ имеет место равенство $\mathrm{cl}\,\mathrm{S}^n M = s^n(\mathrm{cl}\, M)$. Для доказательства нужно заметить, что $\mathrm{cl}\,\mathrm{S}^n M$ и $s^n(\mathrm{cl}\, M)$ удовлетворяют одним и тем же рекуррентным соотношениям, поскольку $\mathrm{cl}\,\mathrm{S}^0 M = 1$ и $\sum_{0\leq k\leq n}(-1)^k \lambda^k(\mathrm{cl}\, M)\,\mathrm{cl}\,\mathrm{S}^{n-k} M = 0$ при $n \geq 1$. Последнее равенство следует из существования точной последовательности A-G-модулей (см. [3], X 9.3):

$$0 \to \bigwedge^n M \to \bigwedge^{n-1} M \otimes M \to \cdots \to \bigwedge^k M \otimes \mathrm{S}^{n-k} M \to \bigwedge^{k-1} M \otimes \mathrm{S}^{n-k+1} M \to \cdots \to \mathrm{S}^n M \to 0 \quad .$$

Замечание 3.4.4.4 В действительности пред-λ-кольцо $\mathrm{K}^{\cdot}(G,A)$ всегда является λ-кольцом (см. 3.3.4); общее доказательство этого факта довольно сложно, однако позже мы его легко докажем в нужном нам частном случае.

Замечание 3.4.4.5 Конечно же, можно обойтись без ограничений на нетеровость кольца A и на проконечность группы G; однако соответствующие конструкции, которые можно найти в [14], I–IV, несколько более сложны и существенно используют теорию триангулированных категорий. Кроме того, в этом случае λ-операции определяются гораздо сложнее.

Замечание 3.4.4.6 В том случае, если нетерово кольцо A регулярно и его размерность конечна, каноническое отображение $\mathrm{K}^{\cdot}(G,A) \to \mathrm{K}_{\cdot}(G,A)$ биективно, и потому позволяет определить на $\mathrm{K}_{\cdot}(G,A)$ структуру пред-λ-кольца и инволюцию. Проверка этого факта, как обычно, основана на теореме Гротендика о резольвенте: надо проверить, что любой A-G-модуль конечного типа M обладает резольвентой конечной длины, составленной из локально проективных A-G-модулей, и тогда обратное отображение $\mathrm{K}_{\cdot}(G,A) \to \mathrm{K}^{\cdot}(G,A)$ определяется тем, что оно переводит $\mathrm{cl}\, M$ в $\sum_{n\geq 0}(-1)^n \mathrm{cl}\, P_n$, где $(P_n)_{n\geq 0}$ — произвольная конечная резольвента A-G-модуля M, составленная из локально проективных A-G-модулей. Для доказательства существования такой резольвенты достаточно доказать, что для любого A-G-модуля конечного типа M существует локально проективный A-G-модуль P вместе с эпиморфизмом $\pi \colon P \to M$; отсюда легко строится бесконечная резольвента, которую можно оборвать через конечное число шагов из-за конечности когомологической размерности кольца A (по теореме Гильберта—Серра когомологическая размерность регулярного нетерова кольца равна его размерности Крулля). Построим P следующим образом. Выберем сначала эпиморфизм A-модулей $\pi' \colon L \to M$, где L — свободный A-модуль конечного ранга, и пусть $U \subset G$ — открытый нормальный делитель, оставляющий неподвижными все элементы M (такой есть, так как достаточно взять U, содержащийся в пересечении стабилизаторов элементов какой-либо конечной системы образующих A-модуля M). Теперь возьмем $P := A^{(G/U)} \otimes_A L$, $\pi \colon [gU] \otimes x \mapsto g\pi'(x)$, и определим действие G на P формулой $g \cdot (a[hU] \otimes x) = (ga)[ghU] \otimes x$.

Определение 3.4.5 *а) Пусть $f \colon H \to G$ — непрерывный гомоморфизм проконечных групп, A — G-кольцо. Обозначим через f^* гомоморфизмы абелевых групп $\mathrm{K}^{\cdot}(G,A) \to \mathrm{K}^{\cdot}(H, f^*A)$ и $\mathrm{K}_{\cdot}(G,A) \to \mathrm{K}_{\cdot}(H, f^*A)$, индуцированные точным функтором $f^{*,ab}$ (см. 3.4.1 и 3.1.14).*

b) Если, кроме того, кольцо A нетерово, гомоморфизм f открыт и порядок его ядра обратим в кольце A (см. 3.2.5), то обозначим через f_* гомоморфизм абелевых групп $\mathrm{K}.(H, f^*A) \to \mathrm{K}.(G, A)$, *определенный* точным *(согласно 3.2.8.1b) функтором f_*^{ab} из категории f^*A-H-модулей конечного типа в категорию A-G-модулей конечного типа. Если этот функтор переводит локально проективные модули в локально проективные, то обозначим также через f_* индуцированный этим функтором гомоморфизм* $\mathrm{K}^{\cdot}(H, f^*A) \to \mathrm{K}^{\cdot}(G, A)$.

Замечание 3.4.5.1 Для любого f^*A-H-модуля M на f_*M есть естественная структура f_*f^*A-G-модуля, поскольку функтор f_* точен слева (см. 3.1.14); если мы рассматриваем f_*M как A-G-модуль, это означает, что мы рассматриваем A-G-модуль, полученный из f_*f^*A-G-модуля f_*M сужением скаляров относительно канонического гомоморфизма G-колец $\eta'_A\colon A \to f_*f^*A$ (см. 3.1.4.4).

Замечание 3.4.5.2 Несложно проверить, что в действительности всякий раз, когда выполнены условия 3.4.5b), функтор f_*^{ab} *всегда* переводит локально проективные модули в локально проективные, и потому всегда можно определить $f_*\colon \mathrm{K}.(H, f^*A) \to \mathrm{K}.(G, A)$. Для проверки этого факта достаточно отдельно разобрать случай, когда f — открытое вложение (очевидный, поскольку тогда A-модуль f_*M неканонически изоморфен сумме $(G : H)$ экземпляров M) и случай, когда f сюръективен (в этом случае f_*M является прямым слагаемым в M; для доказательства достаточно проверить, что $\widetilde{N}'_{f,M}\colon M \to f^*f_*M$ из 3.2.7 является левым обратным к $\xi'_M\colon f^*f_*M \to M$ из 3.1.4.4).

Замечание 3.4.5.3 Гораздо интереснее определить гомоморфизм абелевых групп $f_*\colon \mathrm{K}.(H, f^*A) \to \mathrm{K}.(G, A)$ в том случае, когда функтор f_*^{ab} не является точным. По всей видимости, это возможно, по крайней мере, если тензорно домножить все абелевы группы на $\mathbb{Q}$, несмотря на то, что «обычный» способ $f_*(\mathrm{cl}\, M) = \sum_{n\geq 0}(-1)^n \mathrm{cl}(\mathbf{R}^n f_* M)$ не работает из-за того, что в этой сумме почти всегда оказывается бесконечное число ненулевых слагаемых.

Замечание 3.4.5.4 В условиях определения 3.4.5b) композиции $f_*f^*\colon \mathrm{K}.(G, A) \to \mathrm{K}.(G, A)$ и $f_*f^*\colon \mathrm{K}^{\cdot}(G, A) \to \mathrm{K}^{\cdot}(G, A)$ отождествляются с умножением на целое число $\big(G : f(H)\big)$. Для доказательства этого факта достаточно рассмотреть отдельно случай сюръективного f (тогда $\eta'_M\colon M \to f_*f^*M$ является изоморфизмом для любого M по 3.1.5c), и потому $f_*f^*(\mathrm{cl}\, M) = \mathrm{cl}\, M$), и случай, когда f является открытым вложением (тогда f_*f^*M неканонически изоморфен сумме $(G : H)$ экземпляров A-G-модуля M). Можно также вместо всего этого заметить, что согласно формуле проекции (3.4.6.1) $f_*(f^*(\xi)) = f_*(f^*(\xi)\cdot 1) = \xi \cdot f_*(1)$, и потому достаточно проверить, что $f_*(1) = \big(G : f(H)\big)$.

В частности, мы видим, что при выполнении этих условий для сюръективного f верно, что f^* инъективно, а f_* сюръективно; в частности, $\mathrm{K}^{\cdot}(G, A)$ можно отождествить с подпред-λ-кольцом в $\mathrm{K}^{\cdot}(H, f^*A)$.

Замечание 3.4.5.5 Несложно видеть, что для любой фильтрующейся проективной системы проконечных групп $(G_\alpha, f_{\alpha\beta})$ с сюръективными морфизмами перехода и любого постоянного кольца A верно, что $\mathrm{K}^{\cdot}(\varprojlim G_\alpha, A) = \varinjlim \mathrm{K}^{\cdot}(G_\alpha, A)$, где в правой части в качестве морфизмов перехода используются $f^*_{\alpha\beta}$, и аналогичное равенство верно и для $\mathrm{K}.(\varprojlim G_\alpha, A)$. Для доказательства нужно всего лишь заметить, что категория локально проективных A-G_α-модулей (соотв. A-G_α-модулей конечного типа) отождествляется с полной подкатегорией категории локально проективных A-G-модулей (соотв.\ldots), составленной из A-G-модулей, все элементы которых инвариантны под действием ядра канонического гомоморфизма $f_\alpha\colon G = \varprojlim G_\beta \to G_\alpha$, и что всякий объект категории локально проективных A-G-модулей изоморфен образу некоторого объекта из категории локально проективных A-G_α-модулей для подходящего α.

В частности, любую проконечную группу G можно записать как проективный предел ее дискретных факторгрупп G/U, откуда $\mathrm{K}^{\cdot}(G, A) = \varinjlim_U \mathrm{K}^{\cdot}(G/U, A)$ и аналогично для $\mathrm{K}.(G, A)$. Таким образом, вычисление $\mathrm{K}^{\cdot}$ и $\mathrm{K}.$ для проконечной группы G сводится к соответствующим вычислениям для конечных групп.

Замечание 3.4.5.6 Если кольцо A артиново, то категория A-G-модулей конечного типа артинова (т.е. длина каждого ее объекта конечна), и потому согласно 3.4.3c) $\mathrm{K}.(A, G)$ — свободная абелева группа, базисом которой служат классы простых A-G-модулей. В частности, это замечание применимо, если A — поле; кроме того, оно тогда применимо и к $\mathrm{K}^{\cdot}(A, G) \cong \mathrm{K}.(A, G)$.

Замечание 3.4.6 Несложно видеть, что $f^*\colon \mathrm{K}^{\cdot}(G,A) \to \mathrm{K}.(H, f^*A)$ является гомоморфизмом пред-λ-колец, сохраняющим инволюцию, поскольку функтор $f^{*,ab}$ сохраняет тензорные произведения, внешние степени и двойственные модули. Кроме того, $f^*\colon \mathrm{K}.(G,A) \to \mathrm{K}.(H, f^*A)$ является гомоморфизмом модулей, согласованным с гомоморфизмом колец $f^*\colon \mathrm{K}^{\cdot}(G,A) \to \mathrm{K}^{\cdot}(H, f^*A)$: это означает, что $f^*(\xi\eta) = f^*(\xi)f^*(\eta)$ для любых $\xi \in \mathrm{K}^{\cdot}(G,A)$ и $\eta \in \mathrm{K}.(G,A)$. Напротив, $f_*\colon \mathrm{K}^{\cdot}(H, f^*A) \to \mathrm{K}^{\cdot}(G,A)$ обладает этими свойствами только в исключительных случаях. Самое важное свойство, которым обладает f_* — это *формула проекции* (см. [14], IV 2.11.1.2): для любых $\xi \in \mathrm{K}^{\cdot}(G,A)$ и $\eta \in \mathrm{K}.(H, f^*A)$ верно

$$f_*(f^*(\xi)\eta) = \xi\, f_*(\eta) \quad . \tag{3.4.6.1}$$

Если определено отображение $f_*\colon \mathrm{K}^{\cdot}(H, f^*A) \to \mathrm{K}^{\cdot}(G,A)$, то эта формула верна и для $\eta \in \mathrm{K}^{\cdot}(H, f^*A)$.

Определение 3.4.7 *Для любой проконечной группы G и любой абелевой группы B обозначим через $\mathrm{Cen}(G,B)$ множество всех* центральных *функций $\varphi\colon G \to B$ (т.е. таких φ, что $\varphi(gh) = \varphi(hg)$ для любых $g, h \in G$), непрерывных относительно дискретной топологии на B (или, что равносильно, пропускающихся через дискретную факторгруппу G/U для некоторого U; см. 2.2.1.1). Ясно, что $\mathrm{Cen}(G,B)$ — абелева группа; если $B = \mathbb{C}$, то мы будем рассматривать $\mathrm{Cen}(G,\mathbb{C})$ как унитарное пространство относительно эрмитова скалярного произведения*

$$\big(\varphi_1, \varphi_2\big) := \int_G \varphi_1(g)\overline{\varphi_2(g)}\, d\mu(g) \quad . \tag{3.4.7.1}$$

Здесь интеграл понимается либо как обычный интеграл по мере Хаара, либо в смысле определения 3.2.6; см. также 2.2.4.1f).

Для любого непрерывного гомоморфизма проконечных групп $f\colon H \to G$ обозначим $\mathrm{Cen}(f,B)$: $\mathrm{Cen}(G,B) \to \mathrm{Cen}(H,B)$ или просто f^* отображение $\varphi \mapsto \varphi \circ f$. Ясно, что это гомоморфизм абелевых групп; если $B = \mathbb{C}$ и f сюръективно, то $\mathrm{Cen}(f,\mathbb{C})$ сохраняет скалярное произведение.

Если f — открытый непрерывный гомоморфизм проконечных групп, порядок ядра которого обратим в абелевой группе B (см. 3.2.5), то можно определить отображение $\mathrm{Ind}(f,B)$: $\mathrm{Cen}(H,B) \to \mathrm{Cen}(G,B)$, которое мы иногда будем также обозначать f_*, по формуле

$$\big(\mathrm{Ind}(f,B)(\varphi)\big)(g) = \big(G : f(H)\big) \int_G d\mu_G(\sigma) \int_{f^{-1}(\sigma g \sigma^{-1})} \varphi(h)\, d\mu(h) \tag{3.4.7.2}$$

Интеграл в этой формуле понимается в смысле определения 3.2.6, ровно так же, как это было в 3.2.7. Если обозначить через $\psi(\sigma)$ значение внутреннего интеграла, то, как несложно видеть, функция $\psi(\sigma)$ постоянна на левых смежных классах G по $f(H)$, и потому $\big(G : f(H)\big) \int_G \psi(\sigma)\, d\mu_G(\sigma) = \sum_{\alpha \in G/f(H)} \psi(\sigma_\alpha)$, где σ_α — произвольный представитель соответствующего левого смежного класса G по $f(H)$. Поэтому в определении $\mathrm{Ind}(f,B)$ не обязательно требовать, чтобы порядок G был обратим в B; кроме того, отсюда следует, что для сюръективного *ψ имеет место равенство*

$$\big(\mathrm{Ind}(f,B)(\varphi)\big)(g) = \int_{f^{-1}(g)} \varphi(h)\, d\mu(h) \quad .$$

Если B — кольцо, мы будем всегда рассматривать $\mathrm{Cen}(G,B)$ как кольцо относительно поэлементного умножения функций: $(\varphi_1\varphi_2)(g) = \varphi_1(g)\varphi_2(g)$. В этом случае $\mathrm{Cen}(f,B)$ является гомоморфизмом колец. Кроме того, если кольцо B содержит поле рациональных чисел, определим на $\mathrm{Cen}(G,B)$ операции Адамса Ψ^k следующим образом:

$$(\Psi^k\varphi)(g) = \varphi(g^k) \quad . \tag{3.4.7.3}$$

Несложно видеть, что это определение корректно (т.е. $\Psi^k\varphi$ является непрерывной центральной функцией) и что определенные таким образом операции Адамса Ψ^k аддитивны и удовлетворяют условиям (3.3.8.2), и потому, согласно 3.3.8, их можно использовать для задания на $\mathrm{Cen}(G,B)$ структуры λ-кольца (см. 3.3.4). При этом отображения $\mathrm{Cen}(f,B)$ сохраняют операции Адамса и потому являются λ-гомоморфизмами.

Кроме того, $\mathrm{Cen}(G,\mathbb{C})$ является λ-кольцом с инволюцией — эта инволюция есть комплексное сопряжение: $\bar\varphi(g) = \overline{\varphi(g)}$.

Определение 3.4.8 *Пусть G — проконечная группа, A —* постоянное *G-кольцо (как всегда, коммутативное с единицей), M — локально проективный A-G-модуль. Для любого $g \in G$ обозначим через $\chi_M(g)$ след автоморфизма g_M конечно порожденного проективного A-модуля M. Отображение $\chi_M\colon g \mapsto \chi_M(g)$ мы будем называть* характером *локально проективного A-G-модуля M. Несложно видеть, что для любого M характер $\chi_M \in \mathrm{Cen}(G, A)$, и что отображение $M \mapsto \chi_M$ аддитивно; обозначим определенное им отображение $\mathrm{K}^{\cdot}(G, A) \to \mathrm{Cen}(G, A)$ через χ_G или просто через χ. Для любого $\xi \in \mathrm{K}^{\cdot}(G, A)$ обозначим $\chi_G(\xi)$ также через χ_ξ.*

Замечание 3.4.8.1 Из общих свойств следов мы немедленно получаем, что для любых локально проективных A-G-модулей M и N и любого $g \in G$ верно равенство $\chi_{M\otimes N}(g) = \mathrm{Tr}\, g_{M\otimes N} = \mathrm{Tr}(g_M \otimes g_N) = \mathrm{Tr}\, g_M \cdot \mathrm{Tr}\, g_N = \chi_M(g)\chi_N(g)$, т.е. $\chi_{M\otimes N} = \chi_M\chi_N$. Отсюда и из определения умножения на $\mathrm{K}^{\cdot}(G, A)$ немедленно следует, что $\chi_G\colon \mathrm{K}^{\cdot}(G, A) \to \mathrm{Cen}(G, A)$ является гомоморфизмом колец. Можно проверить, что если A содержит поле рациональных чисел, то χ_G является λ-гомоморфизмом; мы позже докажем этот факт в случае $A = \mathbb{C}$.

Замечание 3.4.8.2 Несложно видеть, что для любого непрерывного гомоморфизма проконечных групп $f\colon G \to H$ и любого кольца A (как обычно, рассматриваемого как постоянное G-кольцо, т.е. кольцо с тривиальным действием G) следующая диаграмма коммутативна:

$$\begin{array}{ccc} \mathrm{K}^{\cdot}(G, A) & \xrightarrow{\chi_G} & \mathrm{Cen}(G, A) \\ \downarrow{\scriptstyle f^*} & & \downarrow{\scriptstyle \mathrm{Cen}(f,A)} \\ \mathrm{K}^{\cdot}(H, f^*A) & \xrightarrow{\chi_H} & \mathrm{Cen}(H, A) \end{array} .$$

Кроме того, если $G = \varprojlim G_\alpha$, где, как в замечании 3.4.5.5, $(G_\alpha, f_{\alpha\beta})$ — проективная система проконечных групп с сюръективными морфизмами перехода, то $\mathrm{K}^{\cdot}(G, A) \cong \varinjlim \mathrm{K}^{\cdot}(G_\alpha, A)$ согласно 3.4.5.5 и $\mathrm{Cen}(G, A) \cong \varinjlim \mathrm{Cen}(G_\alpha, A)$ по 2.2.1.1 (надо еще воспользоваться тем фактом, что всякая открытая подгруппа $U \subset G$ содержит ядро $f_\alpha\colon G \to G_\alpha$ для некоторого α). Поэтому, если для каждого индекса α гомоморфизм χ_{G_α} инъективен, то это же верно и для χ_G.

Определение 3.4.9 *Для любой проконечной группы G обозначим через $\mathrm{X}(G, \mathbb{C})$ или через $\mathrm{X}(G)$ образ $\mathrm{K}^{\cdot}(G, \mathbb{C})$ в $\mathrm{Cen}(G, \mathbb{C})$ относительно отображения χ_G, где $\mathbb{C}$ рассматривается как постоянное G-кольцо (т.е. с тривиальным действием G). Мы будем называть $\mathrm{X}(G)$* кольцом характеров *проконечной группы G. Элементы $\mathrm{X}(G)$ мы будем называть* виртуальными характерами *проконечной группы G.*

Замечание 3.4.9.1 Мы знаем, что категория конечномерных $\mathbb{C}$-G-модулей полупроста (действительно, всякий эпиморфизм $\pi\colon M \to N$ конечномерных $\mathbb{C}$-G-модулей расщепляется: чтобы увидеть это, возьмем $i' \in \mathit{Hom}(N, M)$, расщепляющий π как $\mathbb{C}$-линейное отображение, и положим $i := \int_G gi'\, d\mu(g)$; это и будет искомым расщеплением π), и потому $\mathrm{K}^{\cdot}(G, \mathbb{C})$, совпадающее в данном случае с $\mathrm{K}.(G, \mathbb{C})$ — это свободная абелева группа, порожденная классами $\mathrm{cl}\, S_\iota$ всевозможных (попарно неизоморфных) простых $\mathbb{C}$-G-модулей. Обозначим через $\chi_\iota \in \mathrm{Cen}(G, \mathbb{C})$ характер, соответствующий простому $\mathbb{C}$-G-модулю S_ι. Тогда по определению $\mathrm{X}(G)$ — это абелева группа, порожденная характерами χ_ι. Если G конечна, то известно (см. [8]), что *неприводимые характеры* χ_ι образуют ортонормированный базис в $\mathrm{Cen}(G, \mathbb{C})$; в частности, отображение χ_G инъективно, и потому можно отождествить $\mathrm{K}^{\cdot}(G, \mathbb{C})$ с его образом $\mathrm{X}(G)$.

Покажем, что если G — произвольная проконечная группа, то χ_ι по-прежнему образуют ортонормированный базис в $\mathrm{X}(G)$. Прежде всего, запишем $G = \varprojlim_U G/U$, где U пробегает множество всевозможных открытых нормальных делителей G. Для каждого U группа G/U конечна, и потому $\chi_{G/U}$ инъективно и $\chi_{G/U} \otimes 1_{\mathbb{C}}$ биективно; перейдем теперь к пределу, как в 3.4.8.2, и получим, что $\chi_G = \varinjlim_U \chi_{G/U}$ инъективно, а $\chi_G \otimes 1_{\mathbb{C}}$ биективно, т.е. образ $\mathrm{K}^{\cdot}(G, \mathbb{C})$ порождает $\mathbb{C}$-пространство $\mathrm{Cen}(G, \mathbb{C})$. Заметим теперь, что $\mathrm{K}^{\cdot}(G/U, \mathbb{C})$ отождествляется со свободной абелевой подгруппой в $\mathrm{K}^{\cdot}(G, \mathbb{C}) = \oplus_\iota \mathbb{Z}\, \mathrm{cl}\, S_\iota$, порожденной классами тех простых $\mathbb{C}$-G-модулей S_ι, все элементы которых остаются неподвижными под действием U, поскольку такие S_ι являются также простыми $\mathbb{C}$-G/U-модулями, и все простые $\mathbb{C}$-G/U-модули получаются таким образом. Возьмем два произвольных неизоморфных простых $\mathbb{C}$-G-модуля S_ι и S_κ и выберем U таким образом, чтобы оно оставляло неподвижными все элементы S_ι и S_κ; тогда

из ортогональности $\chi_{G/U}(\operatorname{cl} S_\iota)$ и $\chi_{G/U}(\operatorname{cl} S_\kappa)$ в $\operatorname{Cen}(G/U,\mathbb{C})$, коммутативности диаграммы из (3.4.8.2) и того факта, что $\operatorname{Cen}(f,\mathbb{C})$ сохраняет скалярное произведение для сюръективных f. Аналогично проверяется, что скалярный квадрат любого $\chi_\iota = \chi_G(\operatorname{cl} S_\iota)$ равен единице.

Предложение 3.4.10 *Пусть $f\colon H \to G$ — открытый непрерывный гомоморфизм проконечных групп. Тогда:*

a) *Отображения $\operatorname{Cen}(f,\mathbb{C})\colon \operatorname{Cen}(G,\mathbb{C}) \to \operatorname{Cen}(H,\mathbb{C})$ и $\operatorname{Ind}(f,\mathbb{C})\colon \operatorname{Cen}(H,\mathbb{C}) \to \operatorname{Cen}(G,\mathbb{C})$ сопряжены относительно эрмитова скалярного произведения на $\operatorname{Cen}(G,\mathbb{C})$ и $\operatorname{Cen}(H,\mathbb{C})$ («закон взаимности Фробениуса»).*

b) *Для любых конечномерных $\mathbb{C}$-G-модулей M и N выполнено равенство*

$$(\chi_M,\chi_N) = \dim_{\mathbb{C}} \operatorname{Hom}_G(N,M) = \dim_{\mathbb{C}}(M\otimes \check{N})^G \quad .$$

c) *Для любых $\xi,\eta \in \mathrm{K}^{\cdot}(G,\mathbb{C})$ выполнено равенство $\big(\chi_G(\xi),\chi_G(\eta)\big) = \varepsilon q_*(\xi\check{\eta})$, где $q\colon G \to 1$ — гомоморфизм G в единичную группу, а $\varepsilon\colon \mathrm{K}^{\cdot}(1,\mathbb{C}) \to \mathbb{Z}$ — канонический изоморфизм, определенный сопоставлением конечномерному векторному пространству его размерности (см. 3.4.3,b).*

d) *Для любых $\xi \in \mathrm{K}^{\cdot}(G,\mathbb{C})$ и $\eta \in \mathrm{K}^{\cdot}(H,\mathbb{C})$ выполнены равенства*

$$f_*\big(f^*(\xi)\eta\big) = \xi f_*(\eta) \quad \text{и} \quad \big(\chi_H(\eta),\chi_H(f^*(\xi))\big) = \big(\chi_G(f_*(\eta)),\chi_G(\xi)\big) \quad .$$

Доказательство a) Проверяется непосредственно исходя из определений $\operatorname{Cen}(f,\mathbb{C})$, $\operatorname{Ind}(f,\mathbb{C})$ и определения скалярного произведения на $\operatorname{Cen}(G,\mathbb{C})$ и $\operatorname{Cen}(H,\mathbb{C})$. При этом надо воспользоваться следующими двумя фактами, которые немедленно следуют из определения интеграла 3.2.6: $\int_H \varphi(h)\,d\mu_H(h) = \big(G : f(H)\big)\int_G d\mu_G(g)\int_{f^{-1}(g)} \varphi(h)\,d\mu(h)$ и $\int_{G\times G}\varphi(g,g')\,d\mu(g,g') = \int_{G\times G}\varphi(g,gg'g^{-1})\,d\mu(g,g')$.

b) Разложив M и N в суммы простых $\mathbb{C}$-G-модулей, мы видим, что достаточно доказать утверждение для простых M и N. Если M и N — изоморфные простые $\mathbb{C}$-G-модули, то по лемме Шура $\dim_{\mathbb{C}} \operatorname{Hom}_G(N,M) = 1$, откуда сразу следует нужное равенство; если же M и N неизоморфны, то $\operatorname{Hom}_G(N,M) = 0$, и тоже все сразу получается; нужно только воспользоваться каноническими изоморфизмами $\operatorname{Hom}_G(N,M) = \mathit{Hom}(N,M)^G \cong (M\otimes\check{N})^G$ и ортогональностью характеров (см. 3.4.9.1).

c) Достаточно доказать равенство для $\xi = \operatorname{cl} M$, $\eta = \operatorname{cl} N$, поскольку элементы такого вида порождают $\mathrm{K}^{\cdot}(G,\mathbb{C})$. Теперь заметим, что в этом случае по определению $\varepsilon q_*(\xi\check{\eta}) = \dim_{\mathbb{C}}(M\otimes\check{N})^G$, что по предыдущему пункту совпадает с (χ_M,χ_N).

d) Первое равенство — это в точности формула проекции (3.4.6.1); если теперь с обеим его частям применить εq_* и воспользоваться пунктом c), получим второе равенство.

Следствие 3.4.10.1 *Пусть $f\colon H \to G$ — открытый непрерывный гомоморфизм проконечных групп. Тогда следующая диаграмма коммутативна:*

$$\begin{array}{ccc} \mathrm{K}^{\cdot}(H,\mathbb{C}) & \xrightarrow{\chi_H} & \operatorname{Cen}(H,\mathbb{C}) \\ \big\downarrow{\scriptstyle f_*} & & \big\downarrow{\scriptstyle \operatorname{Ind}(f,\mathbb{C})} \\ \mathrm{K}^{\cdot}(G,\mathbb{C}) & \xrightarrow{\chi_G} & \operatorname{Cen}(G,\mathbb{C}) \end{array} \quad .$$

Доказательство Отождествим с помощью нижней горизонтальной стрелки этой диаграммы $\operatorname{Cen}(G,\mathbb{C})$ с $\mathrm{K}^{\cdot}(G,\mathbb{C})\otimes\mathbb{C}$; тогда согласно пункту c) предложения эрмитово скалярное произведение на $\operatorname{Cen}(G,\mathbb{C})$ отождествляется с эрмитовым продолжением скалярного произведения на $\mathrm{K}^{\cdot}(G,\mathbb{C})$, заданного формулой $(\xi,\eta) = \varepsilon q_*(\xi\check{\eta})$. Отождествим аналогичным образом $\operatorname{Cen}(H,\mathbb{C})$ с $\mathrm{K}^{\cdot}(G,\mathbb{C})\otimes\mathbb{C}$; тогда согласно (3.4.8.2) $\operatorname{Cen}(f,\mathbb{C})$ отождествляется с $f^*\otimes 1_{\mathbb{C}}$; при этом согласно пунктам a) и d) предложения отображения $\operatorname{Ind}(f,\mathbb{C})$ и $f_*\otimes 1_{\mathbb{C}}$ оба являются сопряженными к $\operatorname{Cen}(f,\mathbb{C}) = f^*\otimes 1_{\mathbb{C}}$. Отсюда и из невырожденности рассматриваемых эрмитовых скалярных произведений немедленно следует, что $\operatorname{Ind}(f,\mathbb{C}) = f_*\otimes 1_{\mathbb{C}}$, т.е. коммутативность диаграммы из формулировки следствия.

Определение 3.4.11 *Обозначим через $\widehat{\mathbb{Z}}$ проконечную группу, полученную из $\mathbb{Z}$ пополнением относительно проконечной топологии (т.е. топологии, базисом открытых окрестностей нуля которой являются всевозможные подгруппы конечного индекса). Ясно, что $\widehat{\mathbb{Z}} = \varprojlim_{n\geq 1}\mathbb{Z}/n\mathbb{Z}$ является коммутативным топологическим кольцом с единицей. Обозначим через $\widehat{C}$ аддитивную группу $\widehat{\mathbb{Z}}$, записываемую мультипликативно. Мы будем называть $\widehat{C}$* проциклической группой. *Обозначим также через C_n циклическую группу порядка n; ясно, что тогда $\widehat{C} = \varprojlim_{n\geq 1} C_n$. Обозначим через σ единицу кольца $\widehat{\mathbb{Z}}$, рассматриваемую как элемент проконечной группы $\widehat{C}$; мы будем называть σ* (топологической) образующей *проконечной группы $\widehat{C}$, поскольку множество ее степеней плотно в $\widehat{C}$. Кроме того, для любого $\alpha \in \widehat{\mathbb{Z}}$ обозначим через σ^α элемент α, рассматриваемый как элемент группы $\widehat{C}$; тогда по определению $\sigma^0 = e$, $\sigma^1 = \sigma$, $\sigma^{\alpha+\beta} = \sigma^\alpha\sigma^\beta$ для любых $\alpha, \beta \in \mathbb{Z}$.*

Определение 3.4.12 *Для любой проконечной группы G и любого ее элемента g обозначим через $f_g\colon \widehat{\mathbb{Z}} \to G$ непрерывный гомоморфизм проконечных групп, полученный продолжением по непрерывности из гомоморфизма $\mathbb{Z} \to G$, переводящего $n \in \mathbb{Z}$ в g^n (этот гомоморфизм непрерывен, так как для любого открытого нормального делителя $U \subset G$ индекса d все целые числа, кратные d, переводятся этим гомоморфизмом в элементы U). Мы будем рассматривать f_g и как гомоморфизм проконечных групп $\widehat{C} \to G$. Для любого $\alpha \in \mathbb{Z}$ положим $g^\alpha := f_g(\alpha)$; ясно, что если α — целое число, то это определение согласуется с обычным определением степени и что введенное таким образом понятие степеней элементов проконечной группы с показателями в $\mathbb{Z}$ обладает всеми обычными свойствами степеней.*

Замечание 3.4.13 Пусть G — произвольная проконечная группа. Рассмотрим следующую коммутативную диаграмму:

$$\begin{array}{ccc} \mathrm{K}^{\cdot}(G,\mathbb{C}) & \xrightarrow{(f_g^*)} & \prod_{g\in G}\mathrm{K}^{\cdot}(\widehat{C},\mathbb{C}) \\ \downarrow{\scriptstyle \chi_G} & & \downarrow{\scriptstyle \prod\chi_{\widehat{C}}} \\ \mathrm{Cen}(G,\mathbb{C}) & \xrightarrow{(\mathrm{Cen}(f_g,\mathbb{C}))} & \prod_{g\in G}\mathrm{Cen}(\widehat{C},\mathbb{C}) \end{array} .$$

Вертикальные стрелки этой диаграммы инъективны (см. 3.4.9.1). Нижняя стрелка также инъективна, поскольку для любой функции $\varphi \in \mathrm{Cen}(G,\mathbb{C})$ и любого элемента $g \in G$ выполнено равенство $\varphi(g) = \big(\mathrm{Cen}(f_g,\mathbb{C})(\varphi)\big)(\sigma)$. Отсюда следует инъективность оставшейся стрелки.

Отметим, кроме того, что вертикальные стрелки являются λ-гомоморфизмами (см. 3.4.4, 3.4.5a) и 3.4.7). Поэтому, если мы докажем, что $\chi_{\widehat{C}}$ является λ-гомоморфизмом, отсюда будет следовать, что и χ_G является λ-гомоморфизмом; поскольку нам уже известно, что $\mathrm{Cen}(G,\mathbb{C})$ является λ-кольцом (3.4.7), отсюда и из инъективности χ_G мы получим, что $\mathrm{K}^{\cdot}(G,\mathbb{C})$ является λ-кольцом.

Аналогично, горизонтальные стрелки сохраняют инволюции на рассматриваемых кольцах; поэтому, если мы докажем, что $\chi_{\widehat{C}}$ согласуется с инволюциями, то отсюда формальным образом мы немедленно получим, что χ_G тоже обладает этим свойством, т.е. $\chi_{\bar\xi} = \overline{\chi_\xi}$ для любого $\xi \in \mathrm{K}^{\cdot}(G,\mathbb{C})$.

Ясно, что этот список свойств, формально переносимых с $\chi_{\widehat{C}}$ на всевозможные χ_G, можно было бы продолжить...

Определение 3.4.14 *Для любого $c \in \mathbb{Q}/\mathbb{Z}$ обозначим через ζ^c корень из единицы $\exp(2\pi ic) \in \mathbb{C}$. Обозначим через S_c одномерный $\mathbb{C}$-$\widehat{C}$-модуль, определенный условием $\sigma^\alpha \cdot x = \zeta^{\alpha c}x$ для любого $x \in S_c$; соответствующий характер обозначим через χ_c. Обозначим через ξ_c элемент $\mathrm{cl}\,S_c \in \mathrm{K}^{\cdot}(\widehat{C},\mathbb{C})$.*

Замечание 3.4.14.1 Заметим, что для любого $\alpha \in \widehat{\mathbb{Z}}$ и $c \in \mathbb{Q}/\mathbb{Z}$ корректно определено произведение $\alpha c \in \mathbb{Q}/\mathbb{Z}$, которое, впрочем, можно определить для любого c, являющегося элементом кручения произвольной абелевой группы; именно в таком смысле и понимается произведение αc в предыдущем определении.

Замечание 3.4.14.2 Ясно, что $\chi_c(\sigma^\alpha) = \zeta^{\alpha c}$. Можно выписать разнообразные свойства $\mathbb{C}$-$\widehat{C}$-модулей S_c, их характеров χ_c и соответствующих элементов ξ_c. Вот некоторые из них:

- $S_c \otimes S_d = S_{c+d}$; $\quad \chi_c\chi_d = \chi_{c+d}$; $\quad \xi_c\xi_d = \xi_{c+d}$;

- S_0 есть одномерный $\mathbb{C}$-$\widehat{C}$-модуль с тривиальным действием $\widehat{C}$; $\chi_0 : \widehat{C} \to \mathbb{C}$ — это функция, тождественно равная единице; ξ_0 есть единица кольца $\mathrm{K}^{\cdot}(\widehat{C}, \mathbb{C})$;
- $\check{S}_c \cong S_{-c}$; $\quad \overline{\chi_c} = \chi_{-c}$; $\quad \check{\xi}_c = \xi_{-c}$;
- $\lambda_t(\chi_c) = 1 + \chi_c t$; $\quad \lambda_t(\xi_c) = 1 + \xi_c t$;
- $\Psi^k(\chi_c) = \chi_{kc}$; $\quad \Psi^k(\xi_c) = \xi_{kc}$.

Предложение 3.4.15 *Набор $(S_c)_{c\in\mathbb{Q}/\mathbb{Z}}$ представляет собой полный набор представителей классов изоморфности простых $\mathbb{C}$-$\widehat{C}$-модулей. Набор $(\xi_c)_{c\in\mathbb{Q}/\mathbb{Z}}$ представляет собой базис $\mathbb{Z}$-алгебры $\mathrm{K}^{\cdot}(\widehat{C}, \mathbb{C})$, а набор $(\chi_c)_{c\in\mathbb{Q}/\mathbb{Z}}$ — ортонормированный базис унитарного пространства $\mathrm{Cen}(\widehat{C}, \mathbb{C})$.*

Кроме того, если отождествить циклическую группу C_n порядка n с факторгруппой $\widehat{C}/\widehat{C}^n$, то множество простых $\mathbb{C}$-C_n-модулей отождествляется (с помощью π_n^*, где $\pi_n\colon \widehat{C} \to C_n$ — каноническая проекция) со множеством $(C_{p/n})_{0\le p<n}$.

Доказательство Докажем сначала последнее утверждение, для чего заметим, что все $C_{p/n}$ действительно являются $\mathbb{C}$-C_n-модулями, поскольку $\widehat{C}^n$ тривиально действует на каждом из них, причем эти $\mathbb{C}$-C_n-модули просты, поскольку они одномерны, и попарно неизоморфны, поскольку их характеры $\chi_{p/n}$ попарно различны. Осталось заметить, что их ровно n штук, и что согласно 3.4.9.1 общее количество попарно неизоморфных простых $\mathbb{C}$-C_n-модулей равно $\dim_{\mathbb{C}} \mathrm{Cen}(\widehat{C}, \mathbb{C}) = n$.

Запишем $\widehat{C} = \varprojlim_{n\ge 1} C_n$ и перейдем к пределу, как в 3.4.8.2; получим тогда первое утверждение предложения. Из него следуют все остальные по 3.4.9.1.

Обозначения 3.4.16 Обозначим через $\mathbb{Q}^{ab}$ максимальное абелево расширение $\mathbb{Q}$, т.е. поле, полученное из $\mathbb{Q}$ присоединением всевозможных корней из единицы $(\zeta^c)_{c\in\mathbb{Q}/\mathbb{Z}}$. Обозначим через $\mathbb{Z}^{ab}$ кольцо целых в $\mathbb{Q}^{ab}$; ясно, что $\mathbb{Z}^{ab}$ есть свободный $\mathbb{Z}$-модуль с базисом $(\zeta^c)_{c\in\mathbb{Q}/\mathbb{Z}}$. Кроме того, для любого $\alpha \in \widehat{\mathbb{Z}}^*$ обозначим через τ_α автоморфизм поля $\mathbb{Q}^{ab}$, переводящий ζ^c в $\zeta^{\alpha c}$. Обозначим через τ определенный таким образом гомоморфизм абелевых групп $\widehat{\mathbb{Z}}^* \to \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$; напомним, что τ является изоморфизмом (как это немедленно следует из неприводимости многочленов деления круга).

Предложение 3.4.17 *Пусть G — проконечная группа.*

a) Пред-λ-кольцо $\mathrm{K}^{\cdot}(G, \mathbb{C})$ является λ-кольцом.

b) $\chi_G\colon \mathrm{K}^{\cdot}(G, \mathbb{C}) \to \mathrm{Cen}(G, \mathbb{C})$ является инъективным λ-гомоморфизмом, сохраняющим инволюцию. Отображение χ_G индуцирует изоморфизм между $\mathrm{K}^{\cdot}(G, \mathbb{C})$ и кольцом характеров $\mathrm{X}(G)$. Этот изоморфизм является изоморфизмом λ-колец с инволюцией; в частности, для любого $\xi \in \mathrm{K}^{\cdot}(G, \mathbb{C})$ имеет место равенство $\chi_{\check{\xi}} = \overline{\chi}_\xi$.

c) Для любого виртуального характера χ и любого $g \in G$ значение $\chi(g)$ лежит в $\mathbb{Z}^{ab}$. Иначе говоря, $\mathrm{X}(G) \subset \mathrm{Cen}(G, \mathbb{Z}^{ab})$.

d) Для любого виртуального характера χ и любого $g \in G$ выполнено равенство $\chi(g^{-1}) = \overline{\chi(g)}$; кроме того, для любого $\alpha \in \widehat{\mathbb{Z}}^*$ выполнено равенство $\tau_\alpha\chi(g) = \chi(g^\alpha)$, где τ_α — автоморфизм поля $\mathbb{Q}^{ab}$, определенный в 3.4.16.

e) Все значения виртуального характера χ вещественны в том и только том случае, если $\chi(g) = \chi(g^{-1})$ при всех $g \in G$. Все значения χ принадлежат $\mathbb{Z}$ в том и только том случае, если $\chi(g^\alpha) = \chi(g)$ при всех $g \in G$ и $\alpha \in \widehat{\mathbb{Z}}^*$.

Доказательство Отметим сначала, что e) немедленно следует из c) и d), поскольку условие $\chi(g) = \chi(g^{-1})$ (соотв. $\chi(g^\alpha) = \chi(g)$) оказывается по d) равносильным условию $\chi(g) = \overline{\chi(g)}$ (соотв. $\tau_\alpha\chi(g) = \chi(g)$ для всех $\alpha \in \widehat{\mathbb{Z}}^*$), что по соображениям теории Галуа равносильно вещественности (соотв. рациональности) $\chi(g)$. Кроме того, согласно пункту c) значение $\chi(g)$ всегда является целым алгебраическим, и потому $\chi(g) \in \mathbb{Q} \Leftrightarrow \chi(g) \in \mathbb{Z}$.

Для того, чтобы доказать пункты a)–d), воспользуемся приемом из замечания 3.4.13, чтобы свести доказательство этих утверждений к случаю $G = \widehat{C}$. При этом согласно 3.4.13 в пунктах a) и b) достаточно проверить, что χ_G является λ-гомоморфизмом, т.е. что $\lambda_t \circ \chi_G = \widehat{G}^t(\chi_G) \circ \lambda_t : \mathrm{K}^{\cdot}(G, \mathbb{C}) \to \widehat{G}^t\big(\mathrm{Cen}(G, \mathbb{C})\big)$. Достаточно проверить, что эти отображения совпадают на элементах вида ξ_c, поскольку такие элементы порождают абелеву группу $\mathrm{K}^{\cdot}(\widehat{C}, \mathbb{C})$, а совпадение этих отображений на элементах

вида ξ_c немедленно следует из формул 3.4.14.2. Аналогично, проверка свойств c) и d) немедленно сводится к случаю $G = \widehat{C}$, $\chi = \chi_c$, который также легко разбирается с помощью формул из 3.4.14.2.

Следствие 3.4.18 *Пусть G — проконечная группа, M — конечномерный $\mathbb{C}$-G-модуль. Тогда для любого $n \geq 1$ и любого $g \in G$ выполнены равенства:*

$$\chi_{\wedge^n M}(g) = \frac{1}{n}\sum_{k=1}^{n}(-1)^{k-1}\chi_M(g^k)\chi_{\wedge^{n-k}M}(g) \quad , \tag{3.4.18.1}$$

$$\chi_{\mathrm{S}^n M}(g) = \frac{1}{n}\sum_{k=1}^{n}\chi_M(g^k)\chi_{\mathrm{S}^{n-k}M}(g) \quad . \tag{3.4.18.2}$$

Доказательство Согласно предыдущему предложению χ_G является λ-гомоморфизмом; осталось воспользоваться формулами (3.3.8.4), (3.3.8.5), определением (3.4.7.3) операций Адамса на $\mathrm{Cen}(G, \mathbb{C})$, определением 3.4.4 и замечанием 3.4.4.3.

3.5 Виртуальные подгруппы

Определение 3.5.1 *Пусть G — проконечная группа, A — G-кольцо, X — конечное G-множество. Обозначим через $L_{A,G}(X)$ или через $A^{(X)}$ свободный A-G-модуль, порожденный X (см. 3.1.15). Обозначим через $[X]$ класс $\mathrm{cl}\, A^{(X)}$ локально проективного A-G-модуля в $\mathrm{K}^{\cdot}(G, A)$ (см. 3.4.4). Если A — постоянное кольцо, то обозначим через $\chi_X \in \mathrm{Cen}(G, A)$ характер A-G-модуля $A^{(X)}$ (см. 3.4.8).*

Замечание 3.5.1.1 Значениями характера χ_X всегда являются целые неотрицательные числа в диапазоне от 0 до $\mathrm{card}\, X$ или образы этих целых чисел в простом подкольце кольца A. Для доказательства выберем в A-модуле $L = A^{(X)}$ стандартный базис $(e_x)_{x\in X}$ и заметим, что элемент $g \in G$ действует на элементах этого базиса по правилу $ge_x = e_{gx}$ (см. 3.1.15). Поэтому $\chi_X(g)$, т.е. след автоморфизма g_L, равен количеству элементов $x \in X$, остающихся неподвижными под действием g:

$$\chi_X(g) = \mathrm{card}\{x \in X : gx = x\} \quad .$$

Отсюда по 3.4.17e) следует, что для любого $g \in G$ и $\alpha \in \widehat{\mathbb{Z}}^*$ выполнено равенство $\chi_X(g^\alpha) = \chi_X(g)$.

Определение 3.5.2 *Пусть G — проконечная группа, X — G-множество. Для любого $n \geq 0$ определим n-ую симметрическую степень G-множества X следующим образом: $s^nX := X^n/\mathfrak{S}_n$, где симметрическая группа $\mathfrak{S}_n$ действует на X^n перестановками компонент, а действие G на s^nX индуцировано обычным покомпонентным действием G на X^n. Образ в s^nX элемента $(x_1, x_2, \ldots, x_n) \in X^n$ мы будем записывать в виде произведения $x_1x_2\cdots x_n$; таким образом, s^nX есть «множество одночленов степени n от переменных X». Обозначим через τ^nX G-подмножество в s^nX, образованное элементами вида $x_1x_2\cdots x_n$, у которых все компоненты x_i различны.*

Альтернативное описание τ^nX таково: это множество n-элементных подмножеств множества X с естественным действием группы G.

Следующее предложение суммирует основные свойства свободных A-G-модулей $A^{(X)}$, а также элементов $[X] \in \mathrm{K}^{\cdot}(G, A)$ и характеров χ_X.

Предложение 3.5.3 *Пусть G — проконечная группа, X, Y — конечные G-множества, $n \geq 0$ — целое число. Тогда:*

a) Существуют канонические изоморфизмы $A^{(X\times Y)} \cong A^{(X)} \otimes_A A^{(Y)}$, $A^{(X\sqcup Y)} \cong A^{(X)} \oplus A^{(Y)}$, а также $\mathrm{S}^n A^{(X)} \cong A^{(s^nX)}$.

b) В λ-кольце $\mathrm{K}^{\cdot}(G, A)$ выполнены равенства $[X \times Y] = [X]\cdot[Y]$, $[X \sqcup Y] = [X] + [Y]$, $[s^nX] = s^n[X]$. Если G-кольцо A постоянно и содержит поле рациональных чисел $\mathbb{Q}$ (например, $A = \mathbb{C}$), то выполнены равенства $\chi_{X\times Y} = \chi_X\chi_Y$, $\chi_{X\sqcup Y} = \chi_X + \chi_Y$, $\chi_{s^nX} = s^n\chi_X$.

c) Если $f\colon H \to G$ — непрерывный гомоморфизм проконечных групп, то существует канонический изоморфизм f^*A-H-модулей $(f^*A)^{(f^*X)} \cong f^*(A^{(X)})$, и в $\mathrm{K}^{\cdot}(H, f^*A)$ выполнено равенство $[f^*X] = f^*[X]$. Если A постоянно, то $\chi_{f^*X} = \mathrm{Cen}(f, A)(\chi_X)$.

d) Если $f\colon H \to G$ — открытый непрерывный гомоморфизм проконечных групп, то для любого конечного H-множества Z существует канонический изоморфизм $A^{(f_!Z)} \cong f_!^{ab}\big((f^*A)^{(Z)}\big)$. Если порядок

ядра f обратим в A (см. 3.2.5), то $A^{(f_!Z)} \cong f_!^{ab}\big((f^*A)^{(Z)}\big) \cong f_*\big((f^*A)^{(Z)}\big)$, и в $\mathrm{K}^{\cdot}(G,A)$ выполнено равенство $[f_!Z] = f_*[Z]$. Если, кроме того, A постоянно, то $\chi_{f_!Z} = \mathrm{Ind}(f,A)(\chi_Z)$ (см. 3.4.7).

Доказательство Пункт a) немедленно следует из определений; первая часть пункта b) следует из пункта a) и из определения операций на $\mathrm{K}^{\cdot}(G,A)$ (см. 3.4.4 и 3.4.4.3). Вторая часть пункта b) следует из первой и из того факта, что $\chi_G\colon \mathrm{K}^{\cdot}(G,A) \to \mathrm{Cen}(G,A)$ является гомоморфизмом λ-колец; этот факт верен всегда, однако мы его доказали только в нужном нам случае $A = \mathbb{C}$ (см. 3.4.17); поэтому мы можем пользоваться утверждением про симметрические степени только для $A = \mathbb{C}$; впрочем, согласно 3.5.1.1 значениями характеров χ_X и χ_{s^nX} являются целые числа, не зависящие от кольца A, и потому из равенства $\chi_{s^nX} = s^n\chi_X$ для $A = \mathbb{C}$ следует это же равенство для произвольного постоянного кольца A, содержащего $\mathbb{Q}$.

Далее, пункт c) следует из существования канонического изоморфизма $L_H \circ f^* \cong f^{*,ab} \circ L_G$ (см. 3.1.15) и из коммутативности диаграммы 3.4.8.2. Аналогично, пункт d) следует из существования канонического изоморфизма $L_G \circ f_! \cong f_!^{ab} \circ L_H$ (см. 3.1.15), из существования канонического изоморфизма $N_f\colon f_!^{ab} \to f_*^{ab}$ в случае обратимости порядка ядра f (см. 3.2.8.1) и из коммутативности диаграммы 3.4.10.1 в случае $A = \mathbb{C}$; для произвольного постоянного кольца A надо снова заметить, что все значения рассматриваемых характеров являются целыми числами, а все знаменатели, встречающиеся при вычислении $\mathrm{Ind}(f,A)$, лежат в A, поскольку мы предполагаем обратимость порядка ядра f в A, и поэтому общий случай следует из случая $A = \mathbb{C}$.

Замечание 3.5.3.1 Пункт d) предыдущего предложения показывает, что нет никаких шансов выразить $[f_*Z]$ через $[Z]$ или χ_{f^*Z} через χ_Z; еще одна операция, которую нельзя выразить таким образом — это $\mathit{Hom}(X,Y)$. Однако, как мы вскоре увидим, $[\tau^n X]$ выражается через $[X]$, как и χ_{τ^nX} через χ_X, хотя, конечно же, обычно $[\tau^n X] \neq \lambda^n[X]$, несмотря на равенство размерностей.

Замечание 3.5.3.2 Предыдущее предложение показывает, что мы можем производить многие операции с конечными G-множествами с помощью их характеров χ_X. К сожалению, могут быть неизоморфные G-множества с одинаковыми характерами; примеры этого будут приведены далее. Кроме того, возникают следующие вопросы:

- Как по χ_X восстановить (хотя бы частично) X?
- Как по виртуальному характеру $\chi \in \mathrm{X}(G)$ узнать, имеет ли он вид χ_X для какого-нибудь G-множества X?

Вскоре мы увидим, что на первый вопрос есть полный ответ в случае, когда G — проциклическая группа $\widehat{C}$ (см. 3.4.11). В следующем пункте мы дадим довольно хорошее *необходимое* условие того, чтобы виртуальный характер имел вид χ_X.

Замечание 3.5.3.3 Какая информация о конечном G-множестве X заведомо определяется по $[X] \in \mathrm{K}^{\cdot}(G,A)$ или по $\chi_X \in \mathrm{Cen}(G,A)$? Прежде всего, количество элементов $|X|$ множества X равно рангу локально проективного A-G-модуля $A^{(X)}$; поэтому $|X| = \mathrm{rank}\, A^{(X)} = \mathrm{rank}[X]$ (здесь через rank обозначена также аддитивная функция $\mathrm{K}^{\cdot}(G,A) \to \mathrm{H}^0(\mathrm{Spec}\, A, \mathbb{Z})$; если $\mathrm{Spec}\, A$ связен и непуст, то эта функция принимает свои значения в $\mathbb{Z}$). Если кольцо A постоянно, то $\chi_X(e) = \mathrm{rank}\, A^{(X)} \cdot 1 = |X| \cdot 1$, т.е. $\chi_X(e)$ есть образ $|X|$ в простом подкольце кольца A. Если характеристика кольца A равна нулю (например, $A = \mathbb{C}$), то A содержит кольцо целых чисел $\mathbb{Z}$, и потому χ_X однозначно определяет $|X|$.

Кроме того, количество компонент связности (т.е. G-орбит) G-множества X также однозначно определяется по χ_X, если A содержит $\mathbb{Q}$. Действительно, если обозначить через $\chi_0 : G \to A$ *главный характер* группы G, т.е. характер, тождественно равный единице, то $(\chi_X, \chi_0) = |X/G|$. Для доказательства этого факта рассмотрим гомоморфизм $q : G \to 1$, обозначим через χ_0' главный характер единичной группы и заметим, что согласно 3.1.6 $X/G \cong q_!X$, и по предложению 3.5.3d) $\chi_{X/G} = \chi_{q_!X} = q_*\chi_X$, где $q_* = \mathrm{Ind}(q,\mathbb{C})$. Отсюда $|X/G| = \chi_{X/G}(e) = (\chi_{X/G}, \chi_0') = (q_*\chi_X, \chi_0') = (\chi_X, q^*\chi_0') = (\chi_X, \chi_0)$. Здесь $q^* = \mathrm{Cen}(q,\mathbb{C})$, и мы воспользовались тем, что q_* и q^* сопряжены (см. 3.4.10,a), а также тем, что значения всех рассматриваемых характеров лежат в $\mathbb{Z}$, и потому можно считать, что $A = \mathbb{C}$.

Замечание 3.5.3.4 Произвольное G-множество X можно разложить в сумму орбит: $X = \coprod_{1\le i\le s} X_i$; выберем в каждом X_i какую-нибудь точку x_i и положим $U_i := \mathrm{Stab}_G(x_i)$. Тогда $G/U_i \cong X_i$, и согласно

3.5.3a) выполнено равенство $\chi_X = \sum_{1\le i\le s}\chi_{X_i} = \sum_{1\le i\le s}\chi_{G/U_i}$. Таким образом, для построения всевозможных характеров χ_X достаточно знать характеры $\chi_{G/U}$ для всевозможных открытых подгрупп $U\subset G$.

Определение 3.5.4 *Пусть G — проконечная группа, $U\subset G$ — открытая подгруппа в G. Назовем характер $\chi_{G/U}\in \mathrm{X}(G)\subset \mathrm{Cen}(G,\mathbb{C})$ виртуальной подгруппой G, определенной U. Иногда мы будем обозначать $\chi_{G/U}$ также через χ_U.*

Предложение 3.5.5 *Пусть G — проконечная группа, $U\subset G$ — открытая подгруппа в G. Тогда:*

a) Если $U'\subset G$ сопряжена с U, то $\chi_{G/U'}=\chi_{G/U}$.

b) $\chi_{G/U}(e)=(G:U)$, где e — единица группы G.

c) $(\chi_{G/U},\chi_0)=1$, где χ_0 — главный характер группы G, т.е. характер, тождественно равный единице.

d) Если $U=G$, то $\chi_{G/U}=\chi_0$.

e) Для любого неприводимого характера χ_λ группы G (см. 3.4.9.1) скалярное произведение характеров $(\chi_{G/U},\chi_\lambda)$ является целым неотрицательным числом. Все значения характера $\chi_{G/U}$ являются целыми неотрицательными числами, не превосходящими $(G:U)$. Для любого $g\in G$ и $\alpha\in\widehat{\mathbb{Z}}^*$ выполнено равенство $\chi_{G/U}(g^\alpha)=\chi_{G/U}(g)$.

f) Если группа G конечна, то $\chi_{G/1}$ — это функция, равная порядку группы G в точке e и нулю в остальных точках.

g) Если $f\colon H\to G$ — открытый непрерывный гомоморфизм проконечных групп и $V\subset H$ — открытая подгруппа, то $\chi_{G/f(V)}=f_*(\chi_{H/V})$, где $f_*=\mathrm{Ind}(f,\mathbb{C})$ (см. 3.4.7).

h) Если $i\colon U\to G$ — открытое вложение, χ_0' — главный характер группы U, то $\chi_{G/U}=i_*\chi_0'$. Для любого $g\in G$ значение $\chi_{G/U}(g)$ может быть вычислено по формуле

$$\chi_{G/U}(g)=(G:U)\,\mu_G\big(\{\sigma\in G:\sigma g\sigma^{-1}\in U\}\big)$$

i) Если группа G конечна, то для любого $g\in G$ имеет место равенство

$$\chi_{G/U}(g)=(G:U)\cdot\frac{|\mathcal{C}_\mu\cap U|}{|\mathcal{C}_\mu|}\quad,$$

где через $\mathcal{C}_\mu$ обозначен класс сопряженных элементов группы G, содержащий g.

Доказательство a) Если $U'=sUs^{-1}$, то отображение $g\mapsto sg$ индуцирует изоморфизм G-множеств G/U и G/U', и потому $\chi_{G/U}=\chi_{G/U'}$.

b) Согласно 3.5.3.3 $(G:U)=|G/U|=\chi_{G/U}(e)$.

c) Ясно, что G/U состоит ровно из одной орбиты; теперь воспользуемся 3.5.3.3.

d) Если $G=U$, то $\chi_{G/U}$ соответствует одномерному $\mathbb{C}$-G-модулю с тривиальным действием G; его характер и есть χ_0.

e) Согласно 3.4.9.1, скалярное произведение $(\chi_{G/U},\chi_\lambda)$ равно количеству простых $\mathbb{C}$-G-модулей с характером χ_λ в разложении полупростого $\mathbb{C}$-G-модуля в сумму простых. Поэтому это скалярное произведение является целым неотрицательным. Остальные утверждения — это частные случаи 3.5.1.1.

f) Ясно, что $G/1=G_s$; если $g\ne e$, то отображение $x\mapsto gx$ множества G в себя не имеет неподвижных точек, откуда согласно 3.5.1.1 $\chi_{G_s}(g)=0$.

g) Согласно 3.1.10d), существует канонический изоморфизм G-множеств $f_!(H/V)\cong G/f(V)$. Осталось применить 3.5.3d).

h) Применим g) к $V=H=U$ и $f=i$, а затем воспользуемся d). Для доказательства формулы воспользуемся определением $i_*=\mathrm{Ind}(i,\mathbb{C})$ из 3.4.7:

$$\chi_{G/U}(g)=(i_*\chi_0')(g)=(G:U)\int_G d\mu_G(\sigma)\int_{i^{-1}(\sigma g\sigma^{-1})}\chi_0'(h)\,d\mu(h)=(G:U)\mu_G\big(\{\sigma\in G:\sigma g\sigma^{-1}\}\big),$$

поскольку внутренний интеграл равен нулю или единице в зависимости от того, лежит ли элемент $\sigma g \sigma^{-1}$ в U или нет.

i) Обозначим через $p\colon G \to \mathcal{C}_\mu \subset G$ отображение, переводящее σ в $\sigma g \sigma^{-1}$. Согласно пункту h) $\chi_{G/U}(g) = (G:U)\mu_G\bigl(p^{-1}(U)\bigr)$, что по определению равно $(G:U)\cdot|p^{-1}(U)|/|G|$. Поскольку прообраз каждого элемента $\mathcal{C}_\mu$ относительно p состоит ровно из $|G|/|\mathcal{C}_\mu|$ элементов, мы видим, что $|p^{-1}(U)| = |U\cap\mathcal{C}_\mu|\cdot|G|/|\mathcal{C}_\mu|$, откуда $\chi_{G/U}(g) = (G:U)\cdot|\mathcal{C}_\mu\cap U|/|\mathcal{C}_\mu|$.

Замечание 3.5.6 Пусть G — конечная группа, $G = \coprod_{\mu\in M}\mathcal{C}_\mu$ — ее разложение на классы сопряженных элементов, H — подгруппа G. Выше мы определили виртуальную подгруппу, соответствующую H, как характер $\chi_{G/H}$. Однако в разделе 1.4 было дано другое определение: там виртуальной подгруппой называлось то, что мы теперь будем называть *функцией распределения*: это функция $p_H : M \to [0,1]\cap\mathbb{Q}$, определенная равенством $p_H(\mu) = |H\cap\mathcal{C}_\mu|/|H|$. Покажем, что $\chi_{G/H}$ и p_H однозначно определяют друг друга, что в какой-то мере оправдает появившееся противоречие в терминологии. Прежде всего, и $\chi_{G/H}$, и p_H позволяют определить порядок группы H, поскольку $\chi_{G/H}(e) = (G:H)$ (см. 3.5.5,b) и $p_H(\mu_0) = 1/|H|$, где $\mathcal{C}_{\mu_0}$ — класс единичного элемента. Далее, согласно 3.5.5,i) для любого $g\in\mathcal{C}_\mu$ выполнено равенство $\chi_{G/H}(g) = (G:H)\cdot|H\cap\mathcal{C}_\mu|/|\mathcal{C}_\mu|$, что по определению равно $p_H(\mu)\cdot|G|/|\mathcal{C}_\mu|$. Эта формула позволяет легко найти p_H по $\chi_{G/H}$, и наоборот.

Пример 3.5.7 Пусть $G = \widehat{C}$ — проциклическая группа, т.е. (см. 3.4.11) аддитивная группа $\widehat{\mathbb{Z}}$, записываемая мультипликативно. Для любого натурального n в $\widehat{C}$ есть ровно одна открытая подгруппа индекса n, а именно, $\widehat{C}^n$ (т.е. $n\widehat{\mathbb{Z}}$ в аддитивной записи). Обозначим через T_n соответствующее связное $\widehat{C}$-множество. Ясно, что T_n — это n-элементное множество, на котором топологическая образующая σ группы $\widehat{C}$ действует циклической перестановкой. Любое конечное $\widehat{C}$-множество X записывается в виде $X = \coprod_{1\le i\le s} T_{\lambda_i}$, однозначно с точностью до перестановки слагаемых; это разложение по существу есть разложение на непересекающиеся циклы подстановки, индуцированной на X действием топологической образующей σ. Таким образом, задание n-элементного G-множества X равносильно заданию разбиения $\lambda = (\lambda_i)_{i\ge1}$ числа n на слагаемые (напомним, что *разбиение на слагаемые* λ целого неотрицательного числа n — это невозрастающая последовательность целых неотрицательных чисел $(\lambda_i)_{i\ge1}$, сумма которых равна n).

Несложно описать характер χ_{T_d}: он равен d на элементах $\widehat{C}^d$ и равен 0 на всех остальных элементах $\widehat{C}$ (поскольку все такие элементы не имеют неподвижных точек на T_d; см. формулу 3.5.1.1). В частности, для любого целого n значение $\chi_{T_d}(\sigma^n)$ равно d или 0 в зависимости от того, делится ли n на d или нет.

Если X задается разбиением $\lambda = (\lambda_i)_{i\ge1}$, т.е. $X \cong \coprod_{i\ge1} T_{\lambda_i}$ (мы считаем $T_0 = \varnothing$, так что в действительности эта сумма конечна), то из предыдущего получаем, что $\chi_X(\sigma^n) = \sum_{\lambda_i|n}\lambda_i$.

Предложение 3.5.8 *Пусть $\widehat{C}$ — проциклическая группа (3.4.11). Тогда всякое конечное $\widehat{C}$-множество X однозначно с точностью до изоморфизма определяется значениями характера χ_X на элементах вида σ^n, где n пробегает множество целых чисел ≥1. Более точно, если $X \cong \coprod_{d\ge1} c_d T_d$, где T_d — это связное d-элементное $\widehat{C}$-множество из примера 3.5.7, $c_d \ge 0$ — целые числа, почти все равные нулю, а $c_d T_d$ означает сумму c_d экземпляров T_d, то для любого целого n выполнено равенство*

$$\chi_X(\sigma^n) = \sum_{d|n} c_d \quad .$$

Для любого $n\ge1$ выполнено равенство

$$c_n = \sum_{d|n}\mu\left(\frac{n}{d}\right)\chi_X(\sigma^d) \quad ,$$

где через μ обозначена функция Мебиуса.

Если заранее известно, что X состоит из $\le n$ элементов, то X однозначно определяется набором значений $\bigl(\chi_X(\sigma^k)\bigr)_{1\le k\le n}$.

Доказательство Первая формула по существу была доказана в 3.5.7; вторая формула немедленно следует из нее с помощью формулы обращения Мебиуса. Из второй формулы немедленно следует,

что набор $(c_k)_{1\le k\le n}$ однозначно определяется набором $\big(\chi_X(\sigma^k)\big)_{1\le k\le n}$; если заранее известно, что X состоит из не более чем n элементов, то заведомо $c_k = 0$ при всех $k > n$, и потому строение X однозначно определяется набором $\big(\chi_X(\sigma^k)\big)_{1\le k\le n}$.

Замечание 3.5.9 Пусть G — конечная группа, M — множество классов сопряженности элементов группы G, $(\mathcal{C}_\mu)_{\mu\in M}$ — сами эти классы, $d_\mu := |\mathcal{C}_\mu|$ — количество элементов в соответствующем классе, $(\chi_\lambda)_{\lambda\in\Lambda}$ — множество неприводимых характеров группы G. Обозначим через $\lambda_0 \in \Lambda$ индекс, соответствующий главному характеру группы G (т.е. характеру, тождественно равному единице), и пусть $\mu_0 \in M$ — класс сопряженности единичного элемента e группы G. Обозначим через $c = (c_{\lambda\mu})$ матрицу характеров группы G; таким образом, $c_{\lambda\mu} = \chi_\lambda(\mu)$.

Пусть H — произвольная подгруппа в G. Обозначим через x_λ коэффициент, с которым χ_λ входит в разложение $\chi_{G/H}$; из соотношений ортогональности характеров 3.4.9.1 немедленно получаем, что $x_\lambda = (\chi_{G/H}, \chi_\lambda)$. Положим $y_\mu := |H \cap \mathcal{C}_\mu|$, $y'_\mu = \chi_{G/H}(\mathcal{C}_\mu)$; пусть также $p_H : M \to [0,1] \cap \mathbb{Q}$ — функция распределения, соответствующая H, т.е. $p_H(\mu) = |H \cap \mathcal{C}_\mu|/|H|$. Выпишем известные нам соотношения между этими данными (см. 3.5.5 и 3.4.9.1):

1. $x_\lambda \ge 0; \quad x_\lambda \in \mathbb{Z}$;
2. $\sum_\lambda x_\lambda \cdot \deg\chi_\lambda = \chi_{G/H}(e) = \deg\chi_{G/H} = (G:H)$;
3. $x_{\lambda_0} = 1$;
4. $0 \le y_\mu \le d_\mu; \quad y_\mu \in \mathbb{Z}$;
5. $y_{\mu_0} = 1 = d_{\mu_0}$;
6. $\sum_\mu y_\mu = |H|$;
7. $y'_\mu = \chi_{G/H}(\mu) = (G:H)\cdot\frac{y_\mu}{d_\mu} \in \mathbb{Z}; \quad 0 \le y'_\mu \le (G:H)$;
8. $y'_\mu = \chi_{G/H}(\mu) = \sum_\lambda x_\lambda\chi_\lambda(\mu) = \sum_\lambda x_\lambda c_{\lambda\mu}$;
9. $y'_\mu = \chi_{G/H}(\mu)$ делится на $(G:H)/\operatorname{mcd}((G:H), d_\mu)$;
10. y_μ делится на $d_\mu/\operatorname{mcd}((G:H), d_\mu)$;
11. $x_\lambda = (\chi_{G/H}, \chi_\lambda) = \frac{1}{|G|}\sum_\mu d_\mu\chi_{G/H}(\mu)\overline{\chi_\lambda(\mu)} = \frac{1}{|H|}\sum_\mu \overline{c_{\lambda\mu}}y_\mu$;
12. $p_H(\mu) = y_\mu/|H| = y'_\mu d_\mu/|G|$.

Эти соотношения показывают, что $\chi_{G/H}$, p_H, $(x_\lambda)_{\lambda\in\Lambda}$, $(y_\mu)_{\mu\in M}$ и $(y'_\mu)_{\mu\in M}$ однозначно определяют друг друга, если только известна таблица характеров $(c_{\lambda\mu})$ и числа (d_λ). Кроме того, любой из этих наборов однозначно определяет порядок группы H и ее индекс (см. 3.5.6).

Замечание 3.5.10 Выписанные выше соотношения дают следующий способ построения списка всех виртуальных подгрупп данной группы G, таблица характеров которой известна. А именно, для «маленьких» групп H (точнее, порядков группы H) мы можем перебирать наборы целых неотрицательных чисел $(y_\mu)_{\mu\in M}$, удовлетворяющих условиям 4)–6) и 10), находить по каждому такому набору соответствующий набор (x_λ) по формуле 11), и проверять условия 1)–3); впрочем, достаточно проверять условие 1), поскольку условия 2) и 3) следуют из уже проверенных. Если же группа H «большая», то ее индекс мал, и можно перебирать наборы (x_λ), удовлетворяющие условиям 1)–3), находить для каждого такого набора (y'_μ) по формуле 8), и проверять условия 7) и 9); затем можно было бы найти (y_μ) из 7) и проверить условия 4)–6) и 10), однако в этом нет необходимости, поскольку эти условия окажутся выполненными автоматически.

Этот способ, в частности, позволяет (на компьютере) найти список, содержащий все виртуальные подгруппы групп $\mathfrak{S}_n$ при $n \le 7$; для бóльших n этот метод оказывается недостаточно эффективным и нужно применять методы из раздела 4.

Кроме того, построенный таким образом список может содержать «несущественные» виртуальные подгруппы, т.е. наборы данных, не соответствующие ни одной настоящей подгруппе группы G. Поскольку такие виртуальные подгруппы только замедляют работу нашего метода определения группы Галуа, нам нужно постараться избавиться от них. Один из критериев, позволяющих это делать — *τ-критерий*, — будет рассмотрен в следующем разделе (см. 3.6.6).

3.6 τ-операции и τ-критерий

Пусть G — проконечная группа. Напомним, что в 3.5.2 мы определили для любого G-множества X его n-ую симметрическую степень s^nX, которую можно неформально описать как множество «одночленов степени n от коммутирующих переменных X» с покомпонентным действием G. Мы также определили G-подмножество $\tau^nX \subset s^nX$, состоящее из одночленов $x_1 \cdots x_n$, таких, что элементы $x_1, \ldots, x_n \in X$ попарно различны. Наша ближайшая цель — для конечного G-множества X научиться выражать χ_{τ^nX} через χ_X (см. 3.5.1 и 3.5.3,a).

Лемма 3.6.1 *Пусть G — проконечная группа, X — G-множество.*

a) Симметрическая степень s^nX отождествляется со множеством функций $a\colon X \to \mathbb{N}_0$, сумма значений которых равна n. При этом функции a сопоставляется «одночлен» $\prod_{x\in X} x^{a(x)}$. Это отождествление согласуется с действием G, если, как обычно, определить действие G на функциях по правилу $(ga)(x) = a(g^{-1}x)$ (см. 3.1.19).

b) При этом отождествлении $\tau^nX \subset s^nX$ отождествляется со множеством функций $a\colon X \to \{0,1\}$, сумма значений которых равна n.

c) Для любого $n \geq 0$ существует канонический изоморфизм G-множеств

$$s^nX \cong \coprod_{k=0}^{\lfloor n/2 \rfloor} s^kX \times \tau^{n-2k}X \quad .$$

Доказательство Пункты a) и b) немедленно следуют из определения 3.5.2; надо только заметить, что одночлену $x_1 \cdots x_n$ сопоставляется функция a, значение которой $a(x)$ на произвольном элементе $x \in X$ равно количеству x_i, равных x.

Для доказательства пункта c) рассмотрим отображение θ, которое сопоставляет функции $a \in Hom(X, \mathbb{N}_0)$ пару функций $(b, c) \in Hom(X, \mathbb{N}_0) \times Hom(X, \{0,1\})$, определенных следующим образом: $b(x) = \lfloor a(x)/2 \rfloor$, $c(x) = a(x) - 2b(x)$ для всех $x \in X$, где через $\lfloor t \rfloor$ обозначена целая часть вещественного числа t. Отображение θ инъективно, поскольку $a = 2b + c$; его образом является как раз дизъюнктное объединение $\coprod_{0\leq k\leq n/2} s^kX \times \tau^{n-2k}X$ (здесь k — это сумма значений функции b). Наконец, ясно, что θ является G-отображением.

Определение 3.6.2 *Пусть K — пред-λ-кольцо (см. 3.3.3). Как обычно, для любого $x \in K$ положим $\lambda_t(x) := 1 + xt + \cdots + \lambda^n(x)t^n + \cdots$ (см. замечание после 3.3.3), и пусть $s_t(x) = 1 + xt + \cdots + s^n(x)t^n + \cdots = \lambda_{-t}(x)^{-1}$ — ряд, использованный в 3.3.7 для определения симметрических операций s^n. Введем новый ряд $\tau_t(x)$ с помощью равенства*

$$\tau_t(x) = s_t(x)/s_{t^2}(x) = \lambda_{-t^2}(x)/\lambda_{-t}(x) \tag{3.6.2.1}$$

и новые операции τ^n, $n \geq 0$, по формуле

$$\tau_t(x) = \sum_{n\geq 0} \tau^n(x)t^n \quad . \tag{3.6.2.2}$$

Замечание 3.6.3 Из определения немедленно следует, что $s_{t^2}(x)\tau_t(x) = s_t(x)$; из сравнения коэффициентов при t^n в этом равенстве мы немедленно получаем, что

$$s^n(x) = \sum_{k=0}^{\lfloor n/2 \rfloor} s^k(x)\tau^{n-2k}(x) \quad . \tag{3.6.3.1}$$

Отсюда мы получаем, что $\tau^0(x) = 1$, $\tau^1(x) = x$, $\tau^2(x) = s^2(x) - x$, $\tau^3(x) = s^3(x) - x^2$, $\tau^4(x) = s^4(x) - xs^2(x) + x^2 - s^2(x)$ ... В общем случае $\tau^n(x) = T_n\big(x, s^2(x), \ldots, s^n(x)\big)$, где T_n — некоторые универсальные многочлены с целыми коэффициентами. Аналогичным образом $\tau^n(x)$ выражается и через $x, \lambda^2(x), \ldots, \lambda^n(x)$. Наоборот, τ-операции однозначно определяют симметрические и λ-операции. Для этого достаточно заметить, что из (3.6.2.1) немедленно получается равенство

$$s_t(x) = \prod_{k\geq 0} \tau_{t^{2^k}}(x) = \tau_t(x)\tau_{t^2}(x)\tau_{t^4}(x)\cdots \quad . \tag{3.6.3.2}$$

Из этого равенства следует существование универсальных многочленов с целыми *неотрицательными* коэффициентами S_n, для которых $s^n(x) = S_n\bigl(x, \tau^2(x), \dots, \tau^n(x)\bigr)$.

Таким образом, на коммутативном кольце K можно определить структуру пред-λ-кольца, задав τ-операции. Для того, чтобы были выполнены условия определения пред-λ-кольца 3.3.3, необходимо и достаточно, чтобы $\tau^0(x) = 1$, $\tau^1(x) = x$ и $\tau^n(x+y) = \sum_{p+q=n} \tau^p(x)\tau^q(y)$ при всех $x, y \in K$, $n \geq 0$. Последнее равенство немедленно следует из равенства $\tau_t(x+y) = \tau_t(x)\tau_t(y)$, равносильного по формулам (3.6.2.1) и (3.6.3.2) равенству $\lambda_t(x+y) = \lambda_t(x)\lambda_t(y)$.

Если, кроме того, K является λ-кольцом, то из условий после определения 3.3.4, а также из возможности выразить $\tau^n(x)$ через $(\lambda^k(x))_{1\leq k\leq n}$ с помощью универсальных многочленов с целыми коэффициентами и возможности выразить $\lambda^n(x)$ через $\tau^k(x)$ при $1 \leq k \leq n$ аналогичным образом следует существование универсальных многочленов $Q'_{i,j} = Q'_{i,j}(X_1, X_2, \dots, X_{ij})$ с целыми коэффициентами, обладающих тем свойством, что $\tau^j\bigl(\tau^i(x)\bigr) = Q'_{i,j}\bigl(x, \tau^2(x), \dots, \tau^{ij}(x)\bigr)$ для любого $x \in K$ и $i, j \geq 1$. Выполнение этих условий в действительности необходимо и достаточно, чтобы пред-λ-кольцо было λ-кольцом.

Пример 3.6.4 Рассмотрим $\mathbb{Z}$ как λ-кольцо относительно единственно возможной на нем структуры λ-кольца (см. 3.3.6). Тогда $\lambda_t(n) = (1+t)^n$ для любого целого n, откуда по (3.6.2.1) получаем $\tau_t(n) = \lambda_{-t^2}(n)/\lambda_{-t}(n) = (1-t^2)^n/(1-t)^n = (1+t)^n = \lambda_t(n)$, что означает, что $\tau^k(n) = \lambda^k(n) = \binom{n}{k}$ при всех $k \geq 0$. В общем случае совпадение λ-операций и τ-операций крайне редко. Например, если в произвольном λ-кольце K выполнено равенство $\lambda_t(\xi) = 1 + \xi t$ для некоторого $\xi \in K$, то $\tau_t(\xi) = (1-\xi t^2)/(1-\xi t) = 1 + \xi t + (\xi^2 - 1)t^2 + (\xi^3 - \xi)t^3 + \dots + (\xi^n - \xi^{n-2})t^n + \dots$, т.е. $\tau^n(\xi) = \xi^n - \xi^{n-2}$ для всех $n \geq 2$.

Предложение 3.6.5 *Пусть G — проконечная группа, X — конечное G-множество, $n \geq 0$ — целое число, $\tau^n X$ — конечное G-множество, определенное в 3.5.2.*

a) Пусть A — произвольное G-кольцо. Введем на λ-кольце $\mathrm{K}^{\cdot}(G, A)$ (см. 3.4.4) τ-операции согласно определению 3.6.2. Тогда в кольце $\mathrm{K}^{\cdot}(G, A)$ имеет место равенство $[\tau^n X] = \tau^n[X]$ (см. 3.5.1).

b) Введем на λ-кольце характеров $\mathrm{X}(G) \subset \mathrm{Cen}(G, \mathbb{C})$ τ-операции согласно определению 3.6.2. Тогда $\chi_{\tau^n X} = \tau^n \chi_X$.

Доказательство a) Для доказательства заметим, что из 3.6.1c) и 3.5.3b) следует, что для любого $n \geq 0$ выполнено равенство $s^n[X] = \sum_{0\leq k\leq n/2} s^k[X] \cdot [\tau^{n-2k}X]$. Сравним это равенство с (3.6.3.1) для $x = [X]$ и заметим, что $[\tau^0 X] = 1 = \tau^0[X]$; из этих соотношений индукцией по n получаем $[\tau^n X] = \tau^n[X]$, поскольку $s^0[X] = 1$.

b) Доказательство совершенно аналогично — сначала заметим, что $s^n\chi_X = \sum_{0\leq k\leq n/2} s^k\chi_X \cdot \chi_{\tau^{n-2k}X}$, затем сравним это равенство с (3.6.3.1) для $x = \chi_X$; осталось провести индукцию по $n \geq 0$.

Замечание 3.6.5.1 Формулы (3.3.8.5), (3.4.7.3) и (3.6.3.1) дают возможность последовательно вычислять $s^0(x), \tau^0(x), s^1(x), \tau^1(x), \dots, s^n(x), \tau^n(x), \dots$; при вычислении очередного члена этой последовательности используются уже вычисленные предыдущие.

Теперь мы в состоянии сформулировать τ-критерий.

Предложение 3.6.6 *(«τ-критерий») Пусть G — конечная группа и $(\chi_\lambda)_{\lambda\in\Lambda}$ — множество ее неприводимых характеров. Для того, чтобы данная центральная функция $\chi \in \mathrm{Cen}(G, \mathbb{C})$ была характером вида χ_X для некоторого конечного G-множества X* необходимо *выполнение следующих условий:*

1. *Коэффициенты $x_\lambda = (\chi, \chi_\lambda)$ разложения функции χ по ортонормированному базису (χ_λ) являются целыми неотрицательными числами.*
2. *Все значения $\chi(g)$ являются целыми неотрицательными числами.*
3. *Условия 1) и 2) выполнены для всех $\tau^n\chi$ ($n \geq 1$), где τ-операции на $\mathrm{Cen}(G, \mathbb{C})$ определены с помощью* (3.6.2), (3.3.8.5) *и* (3.4.7.3).
4. *Если обозначить $d := \deg\chi = \chi(e)$, то $\tau^n\chi = \tau^{d-n}\chi$ для всех $0 \leq n \leq d$, и $\tau^n\chi = 0$ при $n > d$.*

Доказательство Нам надо доказать, что если $\chi = \chi_X$ для некоторого конечного G-множества X, то выполнены условия 1)–4). Условие 1) следует из того, что χ_X есть характер полупростого $\mathbb{C}$-G-модуля $\mathbb{C}^{(X)}$, и потому x_λ равно количеству простых $\mathbb{C}$-G-модулей с характером χ_λ в разложении $\mathbb{C}^{(X)}$ в сумму простых $\mathbb{C}$-G-модулей. Условие 2) следует из 3.5.1.1. Наконец, условие 3) следует из уже доказанного и из равенства $\tau^n \chi_X = \chi_{\tau^n X}$, установленного в 3.6.5,b). Условие 4) получается из описания $\tau^n X$ как множества n-элементных подмножеств множества X (см. 3.5.2), и из существования канонического изоморфизма $\tau^n X \cong \tau^{d-n} X$, определенного сопоставлением любому n-элементному подмножеству его дополнения.

Замечание 3.6.6.1 Заметим, что из условия 1) следует, что χ лежит в кольце характеров $\mathrm{X}(G)$; поскольку $\mathrm{X}(G)$ является λ-кольцом, все симметрические степени $s^n \chi$ также лежат в $\mathrm{X}(X)$, а значит, и $\tau^n \chi$ лежат в $\mathrm{X}(X)$, поскольку они выражаются через симметрические операции с помощью универсальных многочленов с целыми коэффициентами T_n (см. 3.6.3). В частности, все значения $(\tau^n \chi)(g)$ являются целыми алгебраическими числами (см. 3.4.17,c). Кроме того, из условия 2) следует, что все значения χ рациональны; воспользовавшись (3.4.7.3), (3.3.8.5) и (3.6.3.1), мы видим, что все значения $\Psi^n \chi$, $s^n \chi$ и $\tau^n \chi$ также рациональны; поскольку они являются к тому же целыми алгебраическими, можно заключить, что они являются целыми рациональными, т.е. принадлежат $\mathbb{Z}$.

Итак, из условий 1) и 2) следует, что все коэффициенты $(\tau^n \chi, \chi_\lambda)$ и все значения $(\tau^n \chi)(g)$ принадлежат $\mathbb{Z}$; поэтому при проверке условия 3) достаточно проверять неотрицательность этих чисел.

Замечание 3.6.6.2 Конечно же, на практике невозможно проверить условия 3) и 4) для всех $n \geq 0$; автор обычно ограничивался рассмотрением на компьютере случаев $0 \leq n \leq 128$.

Замечание 3.6.6.3 Как можно улучшить τ-критерий? Заметим, что попытка использовать условие, аналогичное условию 3), для симметрических операций $s^n \chi$ ничего нового не даст, поскольку симметрические операции выражаются через τ-операции с помощью универсальных многочленов S_n с *целыми неотрицательными* коэффициентами (см. 3.6.3). Еще один путь — пытаться применить τ-критерий к $\tau^n \chi$; может оказаться, что это также бессмысленно, если коэффициенты многочленов $Q'_{i,j}$ из 3.6.3 неотрицательны. Даже если это не так, такая разновидность τ-критерия кажется плохо приспособленной к применению на практике из-за очень быстрого роста коэффициентов и значений возникающих характеров.

Другой подход таков. Можно рассмотреть обобщение τ-операций, определенное следующим образом: для любого G-множества X и любого разбиения $\nu = (\nu_1, \nu_2, \ldots, \nu_l)$ мы определим G-множество $\tau^\nu X$ как G-подмножество в $s^{\nu_1} X \times \cdots \times s^{\nu_l} X$, образованное наборами из l «одночленов», такими, что элементы, входящие во все эти одночлены, попарно различны. Оказывается, что на произвольном λ-кольце можно определить обобщенные τ-операции τ^ν, так, чтобы $\chi_{\tau^\nu X} = \tau^\nu \chi_X$. После этого можно обобщить τ-критерий, рассматривая в условии 3) всевозможные $\tau^\nu \chi$.

Основной недостаток такого подхода — произвольные τ^ν довольно сложно вычислять, хотя они и задаются универсальными многочленами с целыми коэффициентами; кроме того, их слишком много. Автор пытался использовать операции $\tau^{(n,1)}$ в качестве дополнения к τ-критерию. Эти операции легко вычисляются, поскольку $\tau^n X \times X \cong \tau^{(n-1,1)} X \sqcup \tau^{(n,1)} X$, откуда $\sum_{n \geq 0} \tau^{(n,1)}(a) t^n = a \tau_t(a)/(1+t)$. Однако такие случаи, чтобы некоторый характер χ прошел обычный τ-критерий и не прошел после этого расширенный таким образом τ-критерий, крайне редки.

В дальнейшем нам, однако, понадобится явная формула для $\tau^{(1^n)}$:

Предложение 3.6.7 *Для произвольного G-множества X, где G — проконечная группа, и любого числа $n \geq 0$ определим G-множество $\tau^{(1^n)}(X) = \tau^{(1^n)} X$ как G-подмножество в X^n, образованное упорядоченными наборами $(x_1, x_2, \ldots, x_n)$, все компоненты которых попарно различны.*

Кроме того, для любого кольца K и любого $x \in K$ определим элемент $\tau^{(1^n)}(x)$ формулой

$$\tau^{(1^n)}(x) = \prod_{i=0}^{n-1} (x - i) \quad .$$

Тогда:

а) Для любого $n \geq 0$ существует канонический изоморфизм G-множеств $X \times \tau^{(1^n)} X \cong \tau^{(1^{n+1})} X \coprod n \cdot \tau^{(1^n)} X$, где через $n \cdot \tau^{(1^n)} X$ обозначена сумма n копий G-множества $\tau^{(1^n)} X$.

b) В кольце характеров $\mathrm{X}(G)$ *для всех* $n \geq 0$ *выполнено равенство* $\chi_{\tau^{(1^{n+1})}X} = (\chi_X - n) \cdot \chi_{\tau^{(1^n)}X}$.

c) В кольце характеров выполнено равенство $\chi_{\tau^{(1^n)}X} = \tau^{(1^n)}(\chi_X)$.

Доказательство Утверждение a) немедленно получается из комбинаторных соображений: в самом деле, G-подмножество $X \times \tau^{(1^n)}X \subset X^{n+1}$ состоит из наборов $(x_0, x_1, \ldots, x_n)$ элементов X, таких, что $x_1, \ldots, x_n$ попарно различны, и потому это подмножество разбивается в сумму G-подмножеств $A \coprod B_1 \coprod \ldots \coprod B_n$: в B_i попадают те наборы, у которых $x_0 = x_i$, а в A входят наборы, у которых x_0 отличен от всех других x_i. Осталось заметить, что A изоморфно $\tau^{(1^{n+1})}X$, а каждое из B_i изоморфно $\tau^{(1^n)}X$.

Отсюда и из 3.5.3b) немедленно получаем утверждение b); утверждение c) получается из b) индукцией по n.

Ясно, что τ-критерий может использоваться для проверки «виртуальных подгрупп», полученных методом замечания 3.5.10. Сейчас мы рассмотрим несколько других его применений.

Предложение 3.6.8 *Пусть* G *— конечная группа,* X *и* Y *— конечные* G*-множества,* χ_X *и* χ_Y *— соответствующие характеры. Тогда:*

a) Если существует G*-мономорфизм* $i\colon X \to Y$*, то характер* $\chi_Y - \chi_X$ *имеет вид* χ_Z *для некоторого конечного* G*-множества* Z *и, в частности, удовлетворяет условиям* τ*-критерия 3.6.6.*

b) Если существует G*-отображение* $f\colon X \to Y$*, то график* $\Gamma_f = (1_X, f)\colon X \to X \times Y$ *является* G*-мономорфизмом, характер* $\chi_X(\chi_Y - 1)$ *имеет вид* χ_Z *для некоторого конечного* G*-множества* Z *и потому удовлетворяет условиям* τ*-критерия.*

c) Если существует G*-эпиморфизм* $f\colon X \to Y$*, то для любого неприводимого характера* χ_λ *группы* G *выполнено неравенство* $(\chi_X, \chi_\lambda) \geq (\chi_Y, \chi_\lambda)$.

d) Если существует G*-эпиморфизм* $f\colon X \to Y$ *и степень* f *равна некоторому натуральному числу* d *(т.е.* $\operatorname{card} f^{-1}(y) = d$ *для любого* $y \in Y$*), то для любого* $k \geq 1$ *существует* G*-мономорфизм* $i\colon \tau^k Y \to \tau^{kd} X$*, характер* $\tau^{kd}\chi_X - \tau^k\chi_Y$ *имеет вид* χ_Z *для некоторого конечного* G*-множества* Z *и удовлетворяет условиям* τ*-критерия. В частности, характер* $\tau^d\chi_X - \chi_Y$ *имеет вид* χ_Z *и удовлетворяет условиям* τ*-критерия.*

Доказательство a) Возьмем $Z := Y - i(X)$; тогда $Y \cong X \sqcup Z$ и потому $\chi_Y = \chi_X + \chi_Z$.

b) Ясно, что график Γ_f является G-мономорфизмом; применим теперь пункт a) и заметим, что $\chi_{X\times Y} - \chi_X = \chi_X(\chi_Y - 1)$.

c) Действительно, f индуцирует эпиморфизм $\mathbb{C}$-G-модулей $L(f)\colon \mathbb{C}^{(X)} \to \mathbb{C}^{(Y)}$; поскольку они полупросты, это означает, что $\mathbb{C}^{(Y)}$ изоморфен прямому слагаемому в $\mathbb{C}^{(X)}$, и потому простой $\mathbb{C}$-G-модуль с характером χ_λ входит в разложение $\mathbb{C}^{(X)}$ не меньшее число раз, чем в разложение $\mathbb{C}^{(Y)}$.

d) Напомним, что $\tau^n X$ можно рассматривать как множество всех n-элементных подмножеств множества X с естественным действием G. Мономорфизм $i\colon \tau^k Y \to \tau^{kd} X$ можно теперь определить формулой $i(A) := f^{-1}(A)$ для любого k-элементного подмножества $A \subset Y$; ясно, что i действительно инъективно и является G-отображением, и потому можно применить пункт a). Второе утверждение пункта — частный случай первого при $k = 1$.

Лемма 3.6.9 *Пусть* G *— проконечная группа,* U*,* V *— открытые подгруппы в* G*,* $X := G/U$*,* $Y := G/V$*. Для того, чтобы подгруппа* U *содержалась в какой-либо из подгрупп* gVg^{-1}*, сопряженных с* V*, необходимо и достаточно, чтобы существовал* G*-морфизм* $f\colon X \to Y$*. Если такой* G*-морфизм* f *существует, то он обязательно является эпиморфизмом степени* $d = |X|/|Y| = (G : U)/(G : V)$ *(т.е.* $\operatorname{card} f^{-1}(y) = d$ *для любого* $y \in Y$*).*

Доказательство Пусть x_0 — выделенная точка $X = G/U$ (т.е. образ единицы группы G), y_0 — выделенная точка $Y = G/V$. Если существует G-морфизм $f\colon X \to Y$, то $f(x_0) = gy_0$ для некоторого $g \in G$, откуда $U = \mathrm{Stab}_G(x_0) \subset \mathrm{Stab}_G(f(x_0)) = gVg^{-1}$. Наоборот, если $U \subset gVg^{-1}$, то определим f как композицию отображения $X = G/U \to G/gVg^{-1}$ и канонического изоморфизма G-множеств $G/gVg^{-1} \to G/V$, индуцированного умножением справа на g^{-1}. Наконец, заметим, что любой G-морфизм $f\colon X \to Y$ является эпиморфизмом, поскольку $f(X)$ является непустым G-подмножеством

связного G-множества Y и потому совпадает с Y. Кроме того, пусть $d := \operatorname{card} f^{-1}(y_0)$; несложно видеть, что для любого $g \in G$ отображение $x \mapsto gx$ осуществляет биекцию между $f^{-1}(y_0)$ и $f^{-1}(gy_0)$ и потому $\operatorname{card} f^{-1}(y) = d$ для любого $y \in Y$, поскольку любой элемент $y \in Y$ имеет вид gy_0. Это означает, что $f\colon X \to Y$ является эпиморфизмом степени d. Ясно, что $\operatorname{card} X = \sum_{y\in Y} \operatorname{card} f^{-1}(y)$, т.е. $|X| = d|Y|$, откуда $d = |X|/|Y| = (G : U)/(G : V)$.

Предложение 3.6.10 *Пусть G — конечная группа, $(\chi_\lambda)_{\lambda\in\Lambda}$ — множество ее неприводимых характеров, U и V — подгруппы в G, $\chi = \chi_{G/U}$ и $\tilde\chi = \chi_{G/V}$ — соответствующие виртуальные подгруппы (см. 3.5.4). Для того, чтобы U содержалась в какой-либо из подгрупп gVg^{-1}, сопряженных с V,* необходимо *выполнение следующих условий:*

1. $d := \deg\chi/\deg\tilde\chi$ *является целым числом;*
2. $\chi(g) \le d\tilde\chi(g)$ *для всех $g \in G$;*
3. $(\chi, \chi_\lambda) \ge (\tilde\chi, \chi_\lambda)$ *для всех $\lambda \in \Lambda$;*
4. $\chi(\tilde\chi - 1)$ *удовлетворяет условиям τ-критерия;*
5. $\tau^{kd}\chi - \tau^k\tilde\chi$ *удовлетворяет условиям τ-критерия при всех $k \ge 1$.*

Доказательство Все эти условия, за исключением второго, следуют из леммы 3.6.9 и из предложения 3.6.8. Для доказательства второго пункта предположим, что $U \subset V$ (так можно считать, поскольку при замене подгруппы на сопряженную соответствующая виртуальная подгруппа не изменяется), и воспользуемся формулой из 3.5.5,i) для вычисления значений характеров χ и $\tilde\chi$; поскольку $U \subset V$, $|U \cap \mathcal{C}_\mu| \le |V \cap \mathcal{C}_\mu|$ для любого класса сопряженных элементов $\mathcal{C}_\mu \subset G$.

4 Виртуальные подгруппы симметрической группы

4.1 Характеры симметрической группы

Целью этого пункта является изложение основных свойств представлений симметрических групп $\mathfrak{S}_n$, свойств их характеров и изложение алгоритма вычисления таблицы характеров симметрической группы. В основном мы будем следовать книге Джеймса [1]. На протяжении этого пункта мы фиксируем основное кольцо $K = \mathbb{C}$, хотя практически для всех конструкций можно было бы использовать $K = \mathbb{Q}$ или даже $K = \mathbb{Z}$.

Определение 4.1.1 *Для любого множества X обозначим через $\mathfrak{S}_X$ группу, состоящую из биекций X на себя, оставляющих почти все (т.е. все, кроме конечного числа) элементы множества X неподвижными. Будем называть $\mathfrak{S}_X$* группой подстановок *или* симметрической группой *множества X. Для любого $Y \subset X$ мы будем отождествлять $\mathfrak{S}_Y$ с подгруппой в $\mathfrak{S}_X$. Для любого целого $n \geq 0$ обозначим через $[1, n]$ множество целых чисел от 1 до n и обозначим через $\mathfrak{S}_n$ группу подстановок $\mathfrak{S}_{[1,n]}$. Элементы группы подстановок мы будем называть* подстановками.

Для любых $m, n \geq 0$ мы будем отождествлять естественным образом $\mathfrak{S}_m \times \mathfrak{S}_n$ с подгруппой в $\mathfrak{S}_{m+n}$.

Определение 4.1.2 *Мы будем называть* разбиением *любую невозрастающую последовательность $\lambda = (\lambda_k)_{k \geq 1}$ целых неотрицательных чисел, все члены которой, начиная с некоторого, равны нулю. Если сумма $|\lambda|$ всех λ_k равна некоторому целому числу n, мы будем говорить, что λ является* разбиением (на слагаемые) числа n. *Если k — наибольший индекс, для которого $\lambda_k > 0$, мы будем записывать разбиение λ также в виде $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ или в виде $\lambda_1 + \lambda_2 + \cdots + \lambda_k$; тот факт, что λ является разбиением числа n, мы будем записывать также в виде $n = \lambda_1 + \lambda_2 + \cdots + \lambda_k$. Множество всех разбиений мы обозначим через* part, *множество разбиений целого неотрицательного числа n мы обозначим через* part_n, *а количество таких разбиений — через $p(n)$.*

Определение 4.1.3 *Пусть X — множество, $a_1, a_2, \ldots, a_n \in X$ — n различных элементов множества X ($n \geq 1$). Обозначим через $(a_1\ a_2\ \ldots\ a_n)$ подстановку $\sigma \in X$, определенную следующим образом: $\sigma(a_i) = a_{i+1}$ при $1 \leq i < n$, $\sigma(a_n) = a_1$ и $\sigma(x) = x$ для остальных $x \in X$. Мы будем говорить, что σ является* циклом длины n.

Замечание 4.1.4 Как известно, любая подстановка n-элементного множества X однозначно с точностью до порядка раскладывается в произведение непересекающихся циклов, причем каждый из элементов X входит ровно в один из этих циклов (допускаются циклы единичной длины). Набор длин этих циклов, упорядоченный по невозрастанию и дополненный бесконечным количеством нулей, образует некоторое разбиение λ числа n. Это разбиение называется *циклическим типом* данной подстановки. Для любого $\lambda \in \mathrm{part}_n$ обозначим через $\mathcal{C}_\lambda$ множество подстановок из $\mathfrak{S}_n$ циклического типа λ. Несложно видеть, что разбиение $\mathfrak{S}_n = \coprod_{\lambda \in \mathrm{part}_n} \mathcal{C}_\lambda$ представляет собой разложение $\mathfrak{S}_n$ на классы сопряженных элементов.

Определение 4.1.5 *Назовем* диаграммой Юнга *или просто* диаграммой *конечное подмножество $D \subset \mathbb{N} \times \mathbb{N}$, обладающее следующими свойствами:*

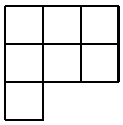
1. $(x + 1, y) \in D \Rightarrow (x, y) \in D$ *для любых* $x, y \in \mathbb{N}$;
2. $(x, y + 1) \in D \Rightarrow (x, y) \in D$ *для любых* $x, y \in \mathbb{N}$.

Пары (x, y) из D мы будем называть клетками диаграммы D *и будем говорить, что клетка (x, y) находится в строке y и в столбце x; мощность множества D мы будем называть* количеством клеток диаграммы D. *Множество всех диаграмм Юнга мы обозначим через* diag, *а множество диаграмм, состоящих из n клеток —* diag_n. *Для любой диаграммы Юнга D определим* двойственную диаграмму D' *следующим образом: $(x, y) \in D' \Leftrightarrow (y, x) \in D$.*

Определение 4.1.6 *Для любого разбиения $\lambda = (\lambda_i)_{i \leq 1}$ определим диаграмму Юнга $D(\lambda)$ следующим образом: $D(\lambda) = \{(x, y) \in \mathbb{N} \times \mathbb{N} : x \leq \lambda_y\}$. Мы будем говорить, что $D(\lambda)$ является* диаграммой, определенной разбиением λ. *Ясно, что $\lambda \mapsto D(\lambda)$ является биекцией* part *на* diag *и* part_n *на* diag_n,

обратная к которой задается формулой $\lambda_i := \min\{x \in \mathbb{N} : (x,i) \notin D\} - 1$. *Мы будем говорить, что разбиение* λ' двойственно к λ, *если диаграмма* $D(\lambda')$ *двойственна к* $D(\lambda)$.

Замечание 4.1.7 Обычно диаграммы Юнга изображают в виде диаграмм из клеток, направляя при этом ось абсцисс вправо, а ось ординат *вниз*. Вот, например, изображение диаграммы, соответствующей разбиению $7 = 3 + 3 + 1$:



Определение 4.1.8 *Для любого разбиения* $\lambda = (\lambda_1, \ldots, \lambda_k)$ *числа* n *обозначим через* $\mathfrak{S}_\lambda$ *группу* $\mathfrak{S}_{\lambda_1} \times \cdots \times \mathfrak{S}_{\lambda_k}$, *отождествленную обычным образом с подгруппой в* $\mathfrak{S}_n$.

Определение 4.1.9 *Пусть* λ *— разбиение числа* n, X *—* n*-элементное множество. Назовем* X-таблицей (Юнга) формы λ *любую биекцию* $t\colon D(\lambda) \to X$. *Если* $X = [1,n]$, *то будем называть* t *просто* таблицей (Юнга) формы λ. *Определим действие* $\mathfrak{S}_X$ *на множестве* X*-таблиц формы* λ *обычным образом:* $(\sigma t)(x,y) = \sigma\big(t(x,y)\big)$ *для любых* $\sigma \in \mathfrak{S}_X$, $(x,y) \in D(\lambda)$. *Мы будем говорить, что подстановка* $\sigma \in \mathfrak{S}_X$ сохраняет строки таблицы t, *если* $\mathrm{pr}_2 \circ t^{-1} \circ \sigma = \mathrm{pr}_2 \circ t^{-1}$, *где* $\mathrm{pr}_2\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ *— проекция на вторую компоненту; подгруппу* $R_t \subset \mathfrak{S}_X$, *образованную такими* σ, *мы будем называть* строчным стабилизатором таблицы t. *Аналогично, мы будем говорить, что* $\sigma \in \mathfrak{S}_X$ сохраняет столбцы таблицы t, *если* $\mathrm{pr}_1 \circ t^{-1} \circ \sigma = \mathrm{pr}_1 \circ t^{-1}$, *соответствующую подгруппу в* $\mathfrak{S}_X$ *мы обозначим через* C_t *и будем называть* столбцовым стабилизатором таблицы t. *Мы будем говорить, что две* X*-таблицы* t *и* t' *формы* λ строчно эквивалентны, *если* $t' = \sigma t$ *для некоторого* $\sigma \in R_t$. *Класс таблицы* t *относительно этого отношения эквивалентности мы будем называть* X-таблоидом формы λ, *определенным* t, *и будем обозначать его* $\{t\}$. *Если* $X = [1,n]$, *мы будем опускать упоминание об* X.

Замечание 4.1.9.1 Ясно, что две X-таблицы t и t' формы λ строчно эквивалентны в том и только том случае, если $\mathrm{pr}_2 \circ t^{-1} = \mathrm{pr}_2 \circ t'^{-1}$, так что строчная эквивалентность действительно является отношением эквивалентности, причем это отношение эквивалентности согласовано с действием $\mathfrak{S}_n$.

Предложение 4.1.10 *Пусть* $n \geq 0$, *и пусть* $\mathfrak{S}_n = \coprod_{\lambda \in \mathrm{part}_n} \mathcal{C}_\lambda$ *— разложение симметрической группы* $\mathfrak{S}_n$ *на классы сопряженных элементов (см. 4.1.4). Обозначим через* d_λ *количество подстановок циклического типа* λ, *т.е. количество элементов во множестве* $\mathcal{C}_\lambda$. *Значение* d_λ *может быть вычислено по формуле*

$$d_\lambda = \frac{n!}{\prod_{k=1}^n c_k! k^{c_k}} \tag{4.1.10.1}$$

где $c_k := \{i : \lambda_i = k\}$ *— количество слагаемых, равных* k, *в разбиении* λ.

Доказательство Прежде всего, рассмотрим разбиения множества $[1,n]$ на c_1 одноэлементных подмножеств, c_2 двухэлементных подмножеств и т. д. Таких разбиений $n!/\prod_k k!^{c_k}$; если мы не хотим различать в таком разбиении равномощные подмножества, эту величину надо еще разделить на $\prod_k c_k!$. Затем надо задать на каждом из множеств разбиения циклическую подстановку; на k-элементном множестве есть $(k-1)!$ различных циклических подстановок, и потому полученная величина умножается на $\prod_k (k-1)!^{c_k}$. В итоге получаем как раз выражение (4.1.10.1).

Определение 4.1.11 *Введем на множестве всех разбиений* part *два упорядочения. Пусть* λ *и* μ *— два разбиения. Мы будем говорить, что* μ мажорирует λ, *если для любого* $k \geq 1$ *выполнено неравенство* $\sum_{i=1}^k \lambda_i \leq \sum_{i=1}^k \mu_i$; *мы будем записывать это свойство в виде* $\lambda \preceq \mu$ *или* $\mu \succeq \lambda$. *Если, кроме того,* $\lambda \neq \mu$, *мы будем говорить, что* μ строго мажорирует λ, *и записывать это в виде* $\lambda \prec \mu$ *или* $\mu \succ \lambda$.

Определим на part лексикографический порядок *следующим образом:* $\lambda < \mu$ *(читается: «*λ *лексикографически меньше* μ*»), если* $\lambda \neq \mu$ *и первая ненулевая разность в последовательности* $(\mu_k - \lambda_k)_{k \geq 1}$ *положительна. Обычным образом вводятся обозначения* $\lambda \leq \mu$, $\mu > \lambda$ *и* $\mu \geq \lambda$.

Замечание 4.1.11.1 Ясно, что отношение мажорирования $\prec$ является отношением частичного порядка на part, а лексикографический порядок $<$ является линейным порядком на part. Кроме того, из определений немедленно следует, что $\lambda \prec \mu$ влечет за собой $\lambda < \mu$ (и $\lambda \preceq \mu$ влечет $\lambda \leq \mu$). На конечном множестве part_n также есть два отношения порядка, индуцированные $<$ и $\prec$; в частности, лексикографический порядок $<$ позволяет однозначно расположить элементы part_n по возрастанию. В дальнейшем, всякий раз, когда нам надо будет линейно упорядочить part_n (скажем, чтобы изобразить матрицы со множеством индексов part_n), мы будем использовать именно лексикографический порядок. Например, элементы part_5 упорядочиваются следующим образом: $(1,1,1,1,1) < (2,1,1,1) < (2,2,1) < (3,1,1) < (3,2) < (4,1) < (5)$.

Определение 4.1.12 *Для любого разбиения $\lambda \in \mathrm{part}_n$ определим следующим образом K-$\mathfrak{S}_n$-модуль M_λ: это свободный K-модуль, базисом которого являются всевозможные таблоиды $\{t\}$ формы λ, а $\mathfrak{S}_n$ действует на элементах этого базиса согласно 4.1.9. Обозначим через $\psi_\lambda \in \mathrm{X}(\mathfrak{S}_n)$ характер этого модуля.*

Замечание 4.1.12.1 Ясно, что $\mathfrak{S}_n$ транзитивно действует на множестве всех таблоидов формы λ и что стабилизатор любого таблоида сопряжен с подстановочной подгруппой $\mathfrak{S}_\lambda \subset \mathfrak{S}_n$ (см. 4.1.8 и 4.1.9). Таким образом, $M_\lambda \cong K^{(\mathfrak{S}_n/\mathfrak{S}_\lambda)}$ и $\psi_\lambda = \chi_{\mathfrak{S}_n/\mathfrak{S}_\lambda}$ (см. 3.5.1). Тем самым мы уже построили некоторые виртуальные подгруппы в $\mathfrak{S}_n$.

Укажем, каким образом можно вычислить значения характера ψ_λ на классе сопряженных элементов $\mathcal{C}_\mu$ для любых $\lambda, \mu \in \mathrm{part}_n$. Прежде всего, если $n = 0$, то $\lambda = \mu = ()$ (пустое разбиение, которое можно обозначить также (0) или $(0,0,\ldots)$), и $\psi_{(0)}(\mathcal{C}_{(0)}) = 1$. Для бóльших n значения $\psi_\lambda(\mathcal{C}_\mu)$ последовательно вычисляются с помощью следующего предложения:

Предложение 4.1.13 *Пусть $\lambda = (\lambda_1, \ldots, \lambda_k)$ и $\mu = (\mu_1, \ldots, \mu_l)$ — разбиения одного и того же числа $n > 0$. Тогда*

$$\psi_\lambda(\mathcal{C}_\mu) = \sum_{i=1}^{l} \psi_{\lambda_1,\ldots,\lambda_i-\mu_1,\ldots,\lambda_k}(\mathcal{C}_{\mu_2,\ldots,\mu_l}) \quad . \tag{4.1.13.1}$$

Запись $\psi_{\lambda_1,\ldots,\lambda_i-\mu_1,\ldots,\lambda_k}$ понимается следующим образом: если $\lambda_i - \mu_1 < 0$, то слагаемое, соответствующее данному индексу i, опускается в сумме (4.1.13.1)*; в противном случае мы упорядочиваем набор $(\lambda_1, \ldots, \lambda_i - \mu_1, \ldots, \lambda_k)$ в порядке невозрастания, дополняем бесконечным числом нулей, и рассматриваем $\psi_{\lambda'}$ для полученного таким образом разбиения $\lambda' \in \mathrm{part}_{n-\mu_1}$.*

Доказательство Выберем какую-нибудь подстановку σ циклического типа μ. Тогда $\psi_\lambda(\mathcal{C}_\mu) = \psi_\lambda(\sigma)$ есть число таблоидов формы λ, остающихся неподвижными под действием σ (см. 3.5.1.1), т.е. количество таблоидов $\{t\}$ формы λ, обладающих тем свойством, что любой цикл подстановки σ содержится в одной строке $\{t\}$. Иначе говоря, нам надо распределить циклы подстановки σ по строкам так, чтобы в i-ой строке оказалось ровно λ_i чисел. Рассмотрим первый цикл подстановки σ (т.е. тот самый цикл, которому соответствует слагаемое μ_1 циклического типа μ подстановки σ). Он стоит в какой-то строке $\{t\}$, например, в i-ой; если мы его выкинем из i-ой строки, мы получим в точности набор, количество которых задается i-ым слагаемым суммы (4.1.13.1); просуммировав по всем i от 1 до l, получаем формулу (4.1.13.1).

Следствие 4.1.14 *Если $\psi_\lambda(\mathcal{C}_\mu) \neq 0$, то $\mu \preceq \lambda$ и $\mu \leq \lambda$. Иначе говоря, матрица $\big(\psi_\lambda(\mathcal{C}_\mu)\big)_{\lambda,\mu\in\mathrm{part}_n}$ является нижнетреугольной матрицей, состоящей из целых неотрицательных чисел. При этом диагональные элементы этой матрицы не равны нулю.*

Доказательство Индукция по $n = |\lambda| = |\mu|$ с использованием формулы (4.1.13.1)

Определение 4.1.15 *Для любой таблицы t формы $\lambda \in \mathrm{part}_n$ обозначим через κ_t элемент групповой алгебры $\mathbb{Z}[\mathfrak{S}_n]$, определенный равенством $\kappa_t := \sum_{\sigma\in C_t}(\operatorname{sgn}\sigma)\sigma$, где C_t — столбцовый стабилизатор t (см. 4.1.9), а $\operatorname{sgn}\sigma = \pm 1$ — знак подстановки σ.*

Ясно, что для любой подстановки $\tau \in \mathfrak{S}_n$ $\kappa_{\tau t} = \sum_{\sigma\in C_{\tau t}}(\operatorname{sgn}\sigma)\sigma = \sum_{\sigma\in \tau C_t \tau^{-1}}(\operatorname{sgn}\sigma)\sigma = \tau\kappa_t\tau^{-1}$.

Определение 4.1.16 *Для любого разбиения $\lambda \in \mathrm{part}_n$ определим* модуль Шпехта $S_\lambda \subset M_\lambda$ *как K-$\mathfrak{S}_n$-подмодуль в M_λ, порожденный как K-модуль элементами вида $\kappa_t\{t\}$ для всевозможных таблиц t формы λ (это действительно K-$\mathfrak{S}_n$-модуль, поскольку $\tau\kappa_t\{t\} = \kappa_{\tau t}\{\tau t\}$). Обозначим через χ_λ характер K-$\mathfrak{S}_n$-модуля S_λ.*

Замечание 4.1.17 В действительности проверяется (см. [1]), что для любого поля K нулевой характеристики K-$\mathfrak{S}_n$-модуль S_λ прост, что модули Шпехта, соответствующие различным λ, попарно неизоморфны и потому (т.к. их количество равно количеству классов сопряженных элементов группы $\mathfrak{S}_n$) образуют полное семейство представителей классов простых K-$\mathfrak{S}_n$-модулей. Иначе говоря, $(\chi_\lambda)_{\lambda\in\mathrm{part}_n}$ — это в точности множество всех неприводимых характеров группы $\mathfrak{S}_n$. Кроме того, в разложении M_λ в сумму простых модулей встречаются только S_μ с $\mu \trianglerighteq \lambda$ (и, следовательно, $\mu \geq \lambda$), причем S_λ входит ровно один раз. Иначе говоря, матрица $M := (m_{\lambda\mu})_{\lambda,\mu\in\mathrm{part}_n}$, определенная равенством $\psi_\lambda = \sum_\mu m_{\lambda\mu}\chi_\lambda$, является верхней унитреугольной матрицей, состоящей из целых неотрицательных чисел. Отсюда немедленно следует, что все значения $\chi_\lambda(\mathcal{C}_\mu)$ являются целыми числами. Поскольку произвольный характер χ является целочисленной комбинацией (χ_λ), все его значения также являются целыми числами.

Замечание 4.1.18 Покажем, каким образом можно, пользуясь изложенными выше фактами, вычислить таблицу характеров группы $\mathfrak{S}_n$. Прежде всего, мы перечисляем в лексикографическом порядке все разбиения $\lambda \in \mathrm{part}_n$, и вычисляем для каждого из них $d_\lambda = |\mathcal{C}_\lambda|$ по формуле (4.1.10.1). Теперь мы можем вычислить скалярное произведение (φ_1, φ_2) двух произвольных характеров φ_1 и φ_2 по формуле $(\varphi_1, \varphi_2) = \frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n}\varphi_1(\sigma)\overline{\varphi_2(\sigma)} = \frac{1}{n!}\sum_{\mu\in\mathrm{part}_n} d_\mu\varphi_1(\mathcal{C}_\mu)\overline{\varphi_2(\mathcal{C}_\mu)} = \frac{1}{n!}\sum_{\mu\in\mathrm{part}_n} d_\mu\varphi_1(\mu)\varphi_2(\mu)$ (последнее равенство верно, поскольку все значения всех характеров $\mathfrak{S}_n$ лежат в $\mathbb{Z}$; кроме того, мы обозначили $\varphi_1(\mathcal{C}_\mu)$ через $\varphi_1(\mu)$ и аналогично для φ_2). Вычислим характеры (т.е. таблицу значений характеров) $(\psi_\lambda)_{\lambda\in\mathrm{part}_n}$ по формуле (4.1.13.1); замечание 4.1.17 показывает, что ортонормированный базис (χ_λ) унитарного пространства $\mathrm{Cen}(\mathfrak{S}_n, \mathbb{C})$ получается из базиса (ψ_λ) процессом ортогонализации Грама–Шмидта относительно порядка, противоположного лексикографическому. Иначе говоря, мы перебираем $\lambda \in \mathrm{part}_n$ в порядке, обратном лексикографическому, вычисляем коэффициенты $m_{\lambda\mu} := (\psi_\lambda, \chi_\mu)$ для всех $\mu > \lambda$ и затем полагаем $\chi_\lambda := \psi_\lambda - \sum_{\mu>\lambda} m_{\lambda\mu}\chi_\mu$. Помимо таблицы характеров $(\chi_\lambda(\mu))$, мы таким образом вычисляем верхнюю унитреугольную матрицу $(m_{\lambda\mu})$.

Изложенный выше метод (являющийся некоторым упрощением метода, изложенного в книге [1]) хорош тем, что он легко реализуется на компьютере.

Замечание 4.1.19 Пусть χ — произвольный виртуальный характер группы $\mathfrak{S}_n$ (т.е. элемент кольца характеров $\mathrm{X}(\mathfrak{S}_n)$). Мы можем задать χ с помощью любого из трех наборов целых чисел (x_λ), (y'_μ), (z_ν), определенных формулами $\chi = \sum_\lambda x_\lambda\chi_\lambda$, $y'_\mu = \chi(\mathcal{C}_\mu) = \chi(\mu)$, $\chi = \sum_\nu z_\nu\psi_\nu$. Укажем, каким образом переходить от одного такого задания к любому другому. Прежде всего, таблица характеров $(\chi_\lambda(\mu))$ позволяет переходить от (x_λ) к (y'_μ) и наоборот по формулам $y'_\mu = \sum_\lambda x_\lambda\chi_\lambda(\mu)$ и $x_\lambda = (\chi, \chi_\lambda) = \frac{1}{n!}\sum_\mu d_\mu y'_\mu\chi_\lambda(\mu)$. Мы можем также перейти от (x_λ) к (z_ν) и наоборот по формуле $x_\lambda = z_\lambda + \sum_{\nu<\lambda} m_{\nu\lambda}z_\nu$ и от (z_ν) к (y'_μ) и наоборот по формуле $y'_\mu = \sum_{\nu\geq\mu} z_\nu\psi_\nu(\mu)$ (здесь мы пользуемся треугольностью матриц $(m_\lambda\mu)$ и $(\psi_\lambda(\mu))$; см. 4.1.17 и 4.1.14).

4.2 Поиск виртуальных подгрупп в $\mathfrak{S}_n$: методы (a) и (c)

Пусть $G = \mathfrak{S}_n$ — симметрическая группа, $H \subset G$ — произвольная ее подгруппа, $\chi = \chi_{G/H}$ — соответствующая виртуальная подгруппа (см. 3.5.4). Согласно 3.5.9, виртуальная подгруппа χ полностью задается с помощью любого из наборов целых чисел $(x_\lambda)_{\lambda\in\Lambda}$, $(y_\mu)_{\mu\in M}$, $(y'_\mu)_{\mu\in M}$, или с помощью функции $p_H\colon M \to [0, 1]$, где Λ — множество, индексирующее неприводимые комплексные характеры $\mathfrak{S}_n$, а M — множество классов сопряженных элементов группы $\mathfrak{S}_n$. Согласно 4.1.4 и 4.1.17, мы можем взять $\Lambda = M = \mathrm{part}_n$, что мы и сделаем. Кроме того, у нас появляется еще один способ задания виртуальной подгруппы в $\mathfrak{S}_n$, а именно, с помощью набора целых чисел $(z_\nu)_{\nu\in\mathrm{part}_n}$, таких, что $\chi = \sum_\nu z_\nu\psi_\nu$; см. 4.1.19. Формулы 3.5.9 и 4.1.19 позволяют легко переходить от одного из этих описаний виртуальной подгруппы к любому другому.

Напомним, что нашей целью является построение для всех небольших n (скажем, $n \leq 12$) некоторых множеств характеров группы $\mathfrak{S}_n$, которые бы заведомо содержали всевозможные виртуальные подгруппы, т.е. характеры вида $\chi_{\mathfrak{S}_n/H}$ для некоторых подгрупп $H \subset \mathfrak{S}_n$. При этом мы хотим, чтобы эти множества характеров содержали как можно меньше «несущественных элементов», т.е. характеров,

не соответствующих никакой подгруппе. Мы введем следующую, несколько нелогичную, терминологию: эти характеры мы будем также называть виртуальными подгруппами, но будем говорить, что они *несущественны*, или что они не соответствуют ни одной «настоящей» подгруппе $\mathfrak{S}_n$.

Какие у нас есть критерии для определения несущественных виртуальных подгрупп? Помимо соотношений из 3.5.9, у нас есть τ-критерий 3.6.6 и его различные модификации (см. 3.6.6.3). Кроме того, можно придумать несколько теоретико-групповых тестов, основанных на том, что τ-критерий дает необходимое условие того, что одна подгруппа содержится в другой, в терминах соответствующих виртуальных подгрупп (см. 3.6.10). Так, всякая подгруппа порядка 48 в $\mathfrak{S}_6$ должна содержать некую подгруппу порядка 16 (а именно, свою силовскую 2-подгруппу); поэтому, если мы обнаруживаем виртуальную подгруппу порядка 48 (напомним, что порядок и индекс виртуальной подгруппы корректно определены; см. 3.5.6), которая не может содержать никакую виртуальную подгруппу порядка 16 (в смысле критерия 3.6.10), то эта виртуальная подгруппа порядка 48 является несущественной.

Основной идеей нашего построения списка виртуальных подгрупп $\mathfrak{S}_n$ является использование уже построенных списков для всех меньших значений n для построения списка для данного значения n — своего рода построение по индукции (база $n = 0$ тривиальна).

В данном разделе мы рассмотрим два метода построения виртуальных подгрупп $\mathfrak{S}_n$, которые мы назовем *методом (a)* и *методом (c)*. Грубо говоря, первый из этих методов заключается в том, что $\mathfrak{S}_{n-1}$ отождествляется с подгруппой в $\mathfrak{S}_n$, и потому всякая подгруппа $H \subset \mathfrak{S}_{n-1}$ может рассматриваться и как подгруппа $\mathfrak{S}_n$; надо только записать это в терминах соответствующих виртуальных подгрупп. Согласно 3.5.5,g), для любой подгруппы $H \subset \mathfrak{S}_{n-1}$ выполнено равенство $\chi_{\mathfrak{S}_n/H} = \mathrm{Ind}(i, \mathbb{C})(\chi_{\mathfrak{S}_{n-1}/H})$, где $i\colon \mathfrak{S}_{n-1} \to \mathfrak{S}_n$ — каноническое вложение, а $\mathrm{Ind}(i, \mathbb{C})\colon \mathrm{Cen}(\mathfrak{S}_{n-1}, \mathbb{C}) \to \mathrm{Cen}(\mathfrak{S}_n, \mathbb{C})$ — индуцированное им отображение центральных функций. Таким образом, для реализации метода (a) нам нужно научиться вычислять характер $\mathrm{Ind}(i, \mathbb{C})(\chi)$ по характеру χ; следующее предложение объясняет, как это можно сделать:

Предложение 4.2.1 *Пусть $f \in \mathrm{Cen}(\mathfrak{S}_{n-1}, \mathbb{C})$ — центральная функция, $i\colon \mathfrak{S}_{n-1} \to \mathfrak{S}_n$ — каноническое вложение, $f' := \mathrm{Ind}(i, \mathbb{C})(f) \in \mathrm{Cen}(\mathfrak{S}_n, \mathbb{C})$. Обозначим через Z $\mathfrak{S}_n$-множество $\{1, 2, \dots, n\}$ с естественным действием $\mathfrak{S}_n$, и пусть χ_Z — соответствующий характер (см. 3.5.1); таким образом, для любой подстановки $\sigma \in \mathfrak{S}_n$ значение $\chi_Z(\sigma)$ есть число неподвижных точек подстановки σ, а для любого разбиения $\lambda \in \mathrm{part}_n$ значение $\chi_Z(\mathcal{C}_\lambda)$ есть количество единичных слагаемых в разбиении λ.*

Тогда для любого разбиения $\lambda \in \mathrm{part}_n$ выполнено равенство

$$f'(\mathcal{C}_\lambda) = \begin{cases} 0, & \text{если } \chi_Z(\mathcal{C}_\lambda) = 0, \\ \chi_Z(\mathcal{C}_\lambda) f(\mathcal{C}_{\lambda'}), & \text{если } \lambda = \lambda' \vee (1) \text{ и } \chi_Z(\mathcal{C}_\lambda) > 0 \end{cases} . \tag{4.2.1.1}$$

Здесь через $\lambda' \vee (1)$ обозначено разбиение числа n, полученное добавлением единичного слагаемого к разбиению λ' числа $n - 1$. Отметим, что λ' однозначно определяется из равенства $\lambda = \lambda' \vee (1)$, и что существование такого λ' равносильно $\chi_Z(\mathcal{C}_\lambda) > 0$, т.е. наличию единичных слагаемых в λ; таким образом, формула, приведенная выше, корректна.

Доказательство Положим $\tau_k := (k\ n) \in \mathfrak{S}_n$ для всех k от 1 до n. Тогда τ_k образуют полную систему представителей $\mathfrak{S}_n/\mathfrak{S}_{n-1}$, и потому для любого $\sigma \in \mathcal{C}_\lambda \subset \mathfrak{S}_n$ выполнено равенство $f'(\sigma) = \sum_{\tau_k \sigma \tau_k^{-1} \in \mathfrak{S}_{n-1}} f(\tau_k \sigma \tau_k^{-1})$. Заметим, что $\tau_k \sigma \tau_k^{-1}$ попадает в $\mathfrak{S}_{n-1}$ тогда и только тогда, когда эта подстановка оставляет неподвижным элемент n, т.е. тогда и только тогда, когда $\sigma(k) = k$. Поэтому, если у σ нет неподвижных точек, т.е. если $\chi_Z(\sigma) = 0$, то и $f'(\sigma) = 0$; тем самым доказана первая часть формулы (4.2.1.1). Предположим теперь, что $\chi_Z(\sigma) > 0$, т.е. что $\lambda = \lambda' \vee (1)$ для некоторого $\lambda' \in \mathrm{part}_{n-1}$. Тогда количество тех k, для которых $\tau_k \sigma \tau_k^{-1} \in \mathfrak{S}_{n-1}$, равно числу неподвижных точек σ, т.е. $\chi_Z(\sigma)$; для всех этих k подстановка $\tau_k \sigma \tau_k^{-1} \in \mathfrak{S}_{n-1}$ имеет циклический тип λ', так что $f(\tau_k \sigma \tau_k^{-1}) = f(\mathcal{C}_{\lambda'})$; таким образом, мы получаем сумму $\chi_Z(\mathcal{C}_\lambda)$ слагаемых, равных $f(\mathcal{C}_{\lambda'})$, что и завершает проверку правильности формулы (4.2.1.1).

Обсудим теперь метод (c). Его суть заключается в том, что исходя из подгрупп $H \subset \mathfrak{S}_n$ и $K \subset \mathfrak{S}_m$ можно построить подгруппу $H \times K \subset \mathfrak{S}_n \times \mathfrak{S}_m \subset \mathfrak{S}_{n+m}$ (см. замечание после 4.1.1). Нам надо теперь изложить эту конструкцию в терминах соответствующих виртуальных подгрупп. Для этого мы введем следующую операцию: для любых двух конечных групп G и G' и любых двух центральных функций $f \in \mathrm{Cen}(G, \mathbb{C})$ и $f' \in \mathrm{Cen}(G', \mathbb{C})$ определим $f * f'$ формулой $(f * f')(g, g') = f(g) f'(g')$. Из определений немедленно следует, что если f и f' — характеры комплексных представлений групп G и G', то $f * f'$

есть характер их тензорного произведения, рассматриваемого как представление группы $G\times G'$. Кроме того, если Z — G-множество, Z' — G'-множество, то на $Z\times Z'$ есть естественно определенная структура $G\times G'$-множества, и $\chi_{Z\times Z'}=\chi_Z*\chi_{Z'}$. В частности, если $H\subset G$ и $H'\subset G'$ — произвольные подгруппы, то $(G\times G')/(H\times H')\cong G/H\times G'/H'$, и потому $\chi_{(G\times G')/(H\times H')}=\chi_{G/H}*\chi_{G'/H'}$.

Применительно к нашей ситуации все это означает, что $\chi_{\mathfrak{S}_{n+m}/(H\times K)}=\mathrm{Ind}(j,\mathbb{C})(\chi_{\mathfrak{S}_n/H}*\chi_{\mathfrak{S}_m/K})$, где $j\colon \mathfrak{S}_n\times\mathfrak{S}_m\to\mathfrak{S}_{n+m}$ — каноническое вложение. Оказывается, что этот характер легко вычисляется в терминах коэффициентов (z_ν), определенных в 4.1.19:

Предложение 4.2.2 *Пусть $j\colon \mathfrak{S}_n\times\mathfrak{S}_m\to\mathfrak{S}_{n+m}$ — каноническое вложение. Тогда:*

a) Для любых двух разбиений $\lambda\in\mathrm{part}_n$ и $\mu\in\mathrm{part}_m$ выполнено равенство $\mathrm{Ind}(j,\mathbb{C})(\psi_\lambda*\psi_\mu)=\psi_{\lambda\vee\mu}$, где ψ_λ, ψ_μ — характеры, определенные в 4.1.12, а $\lambda\vee\mu$ — разбиение числа $n+m$, полученное объединением разбиений λ и μ; иначе говоря, мы рассматриваем последовательность, образованную приписыванием к последовательности ненулевых компонент λ последовательности ненулевых компонент μ, затем упорядочиваем элементы получившейся последовательности в порядке невозрастания и дополняем бесконечным числом нулей.

b) Если $\chi_1=\sum_{\lambda\in\mathrm{part}_n}z^{(1)}_\lambda\psi_\lambda$ и $\chi_2=\sum_{\mu\in\mathrm{part}_m}z^{(2)}_\mu\psi_\mu$ — два характера групп $\mathfrak{S}_n$ и $\mathfrak{S}_m$ соответственно, то $\mathrm{Ind}(j,\mathbb{C})(\chi_1*\chi_2)=\sum_{\nu\in\mathrm{part}_{m+n}}z_\nu\psi_\nu$, где $z_\nu=\sum_{\lambda\vee\mu=\nu}z^{(1)}_\lambda z^{(2)}_\mu$.

Доказательство a) Мы знаем, что $\psi_\lambda=\chi_{\mathfrak{S}_n/\mathfrak{S}_\lambda}$, где $\mathfrak{S}_\lambda=\mathfrak{S}_{\lambda_1}\times\dots\times\mathfrak{S}_{\lambda_k}\subset\mathfrak{S}_n$ (см. 4.1.8 и 4.1.12.1). Кроме того, мы уже выяснили, что $\mathrm{Ind}(j,\mathbb{C})(\chi_{\mathfrak{S}_n/\mathfrak{S}_\lambda}*\chi_{\mathfrak{S}_m/\mathfrak{S}_\mu})=\chi_{\mathfrak{S}_{n+m}/(\mathfrak{S}_\lambda\times\mathfrak{S}_\mu)}$; осталось заметить, что подгруппа $\mathfrak{S}_\lambda\times\mathfrak{S}_\mu\subset\mathfrak{S}_{n+m}$ совпадает с подгруппой $\mathfrak{S}_{\lambda\vee\mu}$ с точностью до перенумерации элементов множества $\{1,2,\dots,n+m\}$, т.е. с точностью до сопряжения в $\mathfrak{S}_{n+m}$; поэтому их характеры совпадают.

b) Очевидное следствие пункта a) ввиду билинейности операции $(\chi_1,\chi_2)\mapsto\mathrm{Ind}(j,\mathbb{C})(\chi_1*\chi_2)$.

Замечание 4.2.3 Если проводить вычисления не для (y'_μ) (равных значениям виртуальной подгруппы $\chi_{\mathfrak{S}_n/H}$ на классах сопряженных элементов), а для набора $y_\mu=|\mathcal{C}_\mu\cap H|$ (см. 3.5.9), то вычисления еще упрощаются: несложно видеть, что если $H\subset\mathfrak{S}_{n-1}$ задается набором $(y^{(1)}_{\mu'})_{\mu'\in\mathrm{part}_{n-1}}$, то H как подгруппа $\mathfrak{S}_n$ задается набором $(y_\mu)_{\mu\in\mathrm{part}_n}$, таким, что $y_{\mu'\vee(1)}=y^{(1)}_{\mu'}$ и $y_\mu=0$, если $\chi_Z(\mu)=0$ (т.е. если μ не представляется в виде $\mu'\vee(1)$). Эти формулы сохраняют силу, если даже не предполагать, что рассматриваемые виртуальные подгруппы соответствуют каким-то «настоящим» подгруппам, а определять (y_μ) исходя из (y'_μ) по формулам 3.5.9.

4.3 Поиск виртуальных подгрупп в $\mathfrak{S}_n$: метод (b)

В этом пункте мы рассматриваем способ определения виртуальных подгрупп $\mathfrak{S}_n$, который мы назовем *методом (b)*. Сущность этого метода заключается примерно в следующем: для произвольной подгруппы $H\subset\mathfrak{S}_n$ мы можем рассмотреть связное $\mathfrak{S}_n$-множество $X:=\mathfrak{S}_n/H$; мы можем также рассмотреть X как $\mathfrak{S}_{n-1}$-множество, которое мы обозначим через i^*X (где $i\colon\mathfrak{S}_{n-1}\to\mathfrak{S}_n$ — каноническое вложение; см. 3.1.3). Тогда i^*X распадется в сумму не более чем n компонент связности (т.е. орбит), каждая из которых имеет вид $\mathfrak{S}_{n-1}/H_j$, т.е. $i^*X\cong\mathfrak{S}_{n-1}/H_1\sqcup\dots\sqcup\mathfrak{S}_{n-1}/H_s$. Отсюда $\mathrm{Cen}(i,\mathbb{C})(\chi_{\mathfrak{S}_n/H})=\mathrm{Cen}(i,\mathbb{C})(\chi_X)=\chi_{i^*X}=\sum_j\chi_{\mathfrak{S}_{n-1}/H_j}$ (см. 3.5.3,c) и b). Теперь можно предложить следующий план действий:

1. Перебрать всевозможные подходящие наборы виртуальных подгрупп $(\chi_{\mathfrak{S}_{n-1}/H_j})_{1\le j\le k}$ (мы уже построили все виртуальные подгруппы в $\mathfrak{S}_{n-1}$, так что нам это несложно сделать; кроме того, естественные ограничения на порядки и количество H_j таковы, что не придется перебирать слишком много вариантов).

2. Для каждого такого набора определить $\mathrm{Cen}(i,\mathbb{C})(\chi)$ как сумму всех $\chi_{\mathfrak{S}_{n-1}/H_j}$; определить отсюда $y_{\mu\vee(1)}=\chi\big(\mu\vee(1)\big)=\big(\mathrm{Cen}(i,\mathbb{C})(\chi)\big)(\mu)$ для всех $\mu\in\mathrm{part}_{n-1}$ (см. 3.4.7; мы пользуемся тем, что $i^{-1}(\mathcal{C}_{\mu\vee(1)})=\mathcal{C}_\mu$).

3. Произвести перебор возможных значений (y_μ) для тех $\mu\in\mathrm{part}_n$, которые не записываются в виде $\mu'\vee(1)$ (таких μ не очень много, а условия 1)–12) из 3.5.9 позволяют сильно сократить перебор).

4. Проверить условия 1)–12) из 3.5.9 (в действительности целочисленность коэффициентов (x_λ), или, что равносильно, (z_ν), можно проверять по ходу перебора, производимого в предыдущем пункте, поскольку согласно 4.1.19 z_ν зависит только от y_μ с $\mu \succeq \nu$; это позволяет отсекать по ходу заведомо неподходящие ветви перебора).

5. Проверить, удовлетворяет ли полученная виртуальная группа τ-критерию 3.6.6. Если да, то добавить ее в список виртуальных подгрупп $\mathfrak{S}_n$.

Для завершения описания метода (b) нам следует изучить, какие могут быть порядки подгрупп $H_j \subset \mathfrak{S}_{n-1}$, в зависимости от порядка $H \subset \mathfrak{S}_n$.

Предложение 4.3.1 *Пусть G — конечная группа, $G_0 \subset G$ — подгруппа, $i\colon G_0 \to G$ — каноническое вложение, $Z = G/G_0$ — G-операторное множество, $n := |Z| = (G : G_0)$. Пусть $H \subset G$ — еще одна подгруппа G, $X := G/H$, i^*X — G_0-операторное множество, полученное из X сужением группы операторов (см. 3.1.3). Тогда:*

a) *Существует естественная биекция между множеством компонент связности (т.е. G_0-орбит) G_0-множества i^*X и множеством компонент связности G-множества $i_!i^*X \cong X \times Z$ (см. 3.1.11.2). Точнее, если $i^*X = X'_1 \sqcup \ldots \sqcup X'_k$ является разложением i^*X на компоненты связности, то $X \times Z \cong i_!i^*X = i_!X'_1 \sqcup \ldots \sqcup i_!X'_k$ является разложением $X \times Z$ на компоненты связности.*

b) *Существует естественная биекция между множеством H-орбит Z и множеством G-орбит (т.е. компонент связности) $X \times Z$.*

c) *Пусть Z_j — H-орбита Z, соответствующая X'_j относительно композиции биекций, рассмотренных в пунктах a) и b). Положим $\nu_j := |Z_j|$. Тогда $(G : G_0)|X'_j| = |i_!X'_j| = (G : H)|Z_j|$ и $|X'_j| = (G : H)\nu_j/n$; кроме того, $\sum_{j=1}^k \nu_j = n$.*

d) *Выберем в каждом X'_j произвольный элемент x_j и положим $H_j := \mathrm{Stab}_{G_0}(x_j)$. Тогда $i^*(G/H) = i^*X \cong G_0/H_1 \sqcup \ldots \sqcup G_0/H_k$, $(G_0 : H_j) = |X'_j| = (G : H)\nu_j/n$ и $|H_j| = |H|/\nu_j$.*

e) *Выполнены соотношения $1 \leq \nu_j \leq n$ и $\sum_{j=1}^k \nu_j = n$, все ν_j делят порядок группы H и делятся на $n/\gcd\bigl(n, (G : H)\bigr)$.*

f) *Группа H транзитивно действует на Z тогда и только тогда, когда $k = 1$ и $\nu_1 = n$; в этом случае $|H_1| = |H|/n$ и $(G : H) = (G_0 : H_1)$.*

g) *Подгруппа $H \subset G$ содержится в некоторой подгруппе, сопряженной с G_0, в том и только том случае, если H имеет неподвижную точку на Z, т.е. если $\nu_j = 1$ для некоторого j.*

Доказательство a) Существование канонического изоморфизма G-множеств $i_!i^*X \cong X \times Z$ установлена в 3.1.11.2; кроме того, согласно 3.1.10,a),b) функтор $i_!$ сохраняет суммы и переводит непустые связные объекты в непустые связные объекты; отсюда немедленно получаем утверждение пункта a).

b) Этот пункт немедленно получается из пункта a), если поменять ролями G_0 с H (а значит, и Z с X).

c) Отображение $i\colon G_0 \to G$ инъективно, и потому согласно 3.1.10.1 $|i_!X'_j| = (G : G_0)|X'_j|$; меняя ролями G_0 и H, как в доказательстве пункта b), получаем $|i_!X'_j| = (G : H)|Z_j|$. Поскольку $(G : G_0) = n$ и $|Z_j| = \nu_j$, отсюда следует $|X'_j| = (G : H)\nu_j/n$. Кроме того, $n = |Z| = \sum_j |Z_j| = \sum_j \nu_j$.

d) Все, кроме последнего равенства, уже доказано в c), поскольку $|X'_j| = (G_0 : H_j)$. Осталось заметить, что $|H_j| = |G_0|/(G_0 : H_j) = n|G_0|/\bigl((G : H)\nu_j\bigr) = n|G_0||H|/(|G|\nu_j) = |H|/\nu_j$, поскольку $n = (G : H)$.

e) Мы уже знаем, что $\nu_j = |Z_j| \geq 1$ и что $\sum_j \nu_j = n$. Кроме того, согласно d), числа $(G : H)\nu_j/n$ и $|H|/\nu_j$ являются целыми; отсюда следуют последние два утверждения пункта.

f) Действительно, транзитивность действия H на Z как раз и означает, что Z состоит ровно из одной орбиты, т.е. что $k = 1$; остальные утверждения следуют тогда из d) и e).

g) Действительно, H оставляет неподвижной некоторую точку $gG_0 \in Z = G/G_0$ тогда и только тогда, когда H содержится в стабилизаторе $\mathrm{Stab}_G(gG_0) = gG_0g^{-1}$. С другой стороны, понятно, что H-неподвижные точки Z — это в точности одноэлементные H-орбиты Z_j, соответствующие $\nu_j = 1$.

Нам остается только применить это предложение в случае $G = \mathfrak{S}_n$, $G_0 = \mathfrak{S}_{n-1}$. Отметим, что мы можем сэкономить много усилий, рассматривая только те разбиения $\nu = (\nu_j)$ числа $n = (\mathfrak{S}_n : \mathfrak{S}_{n-1})$, в которых все $\nu_j \geq 2$, поскольку если некоторое $\nu_j = 1$, то по пункту g) только что доказанного предложения H сопряжена с некоторой подгруппой $\mathfrak{S}_{n-1}$, а все такие подгруппы уже найдены методом (a), изложенным в предыдущем разделе.

Кроме того, мы можем определить, какие из построенных виртуальных подгрупп $\mathfrak{S}_n$ могут соответствовать (или обязательно соответствуют) транзитивным (т.е. транзитивно действующим на $Z = \{1, 2, \ldots, n\} \cong \mathfrak{S}_n/\mathfrak{S}_{n-1}$) подгруппам $H \subset \mathfrak{S}_n$: это те виртуальные подгруппы, которые были получены методом (b) для разбиения $\nu = (n)$ хотя бы один раз (или были получены только методом (b) и только для такого разбиения).

Отметим, что некоторые виртуальные подгруппы могут быть получены методом (b) несколько раз для разных разбиений (ν_j) и виртуальных подгрупп $\chi_{\mathfrak{S}_{n-1}/H_j}$.

Читатель может поинтересоваться, а зачем вообще нужен метод (c)? Метод (b) и так позволяет получить все виртуальные подгруппы $\mathfrak{S}_n$, а метод (a) по существу используется только для оптимизации метода (b), чтобы не перебирать разбиения (ν_j), в которых $\nu_j = 1$ для некоторого j. Получается, что без метода (c) можно было бы совсем обойтись... Ответ здесь следующий: метод (c) дает возможность получить дополнительную информацию о получающихся виртуальных подгруппах. Так, если некоторая виртуальная подгруппа χ была получена методом (c) из виртуальных подгрупп χ' и χ'' и нам известно, что эти виртуальные подгруппы существенны (т.е. соответствуют каким-то реальным подгруппам $H' \subset \mathfrak{S}_n$ и $H'' \subset \mathfrak{S}_m$), то и χ является существенной, поскольку χ соответствует $H' \times H'' \subset \mathfrak{S}_{n+m}$. Метод (a) также строит из существенных виртуальных подгрупп существенные, чего нельзя сказать о методе (b).

4.4 Свойства виртуальных подгрупп

Для удобства дальнейших ссылок соберем теперь воедино полученные нами критерии, позволяющие извлекать информацию о свойствах подгрупп $H \subset G$ исходя из знания соответствующих виртуальных подгрупп $\chi_{G/H} \in \mathrm{X}(G)$. Для краткости мы будем обозначать $\chi_{G/H}$ просто через χ_H.

Здесь G — конечная группа, хотя многие результаты в действительности были нами доказаны для случая, когда H — открытая подгруппа проконечной группы G. Кроме того, некоторые критерии будут нами уточнены в случае $G = \mathfrak{S}_n$.

Итак:

1. *Порядок* и *индекс* группы H полностью определяется соответствующей виртуальной подгруппой, т.е. характером χ_H. Действительно, согласно 3.5.5,c) имеет место равенство $(G : H) = \chi_H(e)$, откуда $|H| = |G|/\chi_H(e)$. Это дает нам возможность говорить о порядке и об индексе виртуальной подгруппы как о величинах, формально определенных этими равенствами.

2. Количество элементов группы H, принадлежащих классу сопряженных элементов $\mathcal{C} \subset G$ (т.е. множеству подстановок $\mathcal{C}_\lambda$ фиксированного циклического типа λ в случае $G = \mathfrak{S}_n$), также полностью определяется χ_G (см. 3.5.5,i):

$$|H \cap \mathcal{C}| = \frac{|\mathcal{C}|}{(G : H)} \cdot \chi_H(g) \text{ для произвольного } g \in \mathcal{C}.$$

   Наоборот, числа $|H \cap \mathcal{C}|$ полностью определяют виртуальную подгруппу χ_H (см. 3.5.6).

3. Если подгруппы H_1 и H_2 *сопряжены*, то $\chi_{H_1} = \chi_{H_2}$ (см. 3.5.5,a). Отметим, что это условие является необходимым, но не достаточным: уже в группе $G = \mathfrak{S}_6$ есть несопряженные подгруппы $H_1 = \big\{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\big\}$ и $H_2 = \big\{e, (1\,2)(3\,4), (1\,2)(5\,6), (3\,4)(5\,6)\big\}$ с совпадающими виртуальными подгруппами. Интересно отметить, что в данном случае эти две группы обе изоморфны четверной группе Клейна V_4 и могут быть реализованы как группы Галуа двух многочленов шестой степени с одинаковыми полями разложения: H_1 есть группа Галуа многочлена $F_1(T) = (T^4 + 1)(T + 1)(T - 1) = T^6 - T^4 + T^2 - 1$, а H_2 — группа Галуа многочлена $F_2(T) = (T^2 + 1)(T^2 - 2)(T^2 + 2) = T^6 + T^4 - 4T^2 - 4$.

   Существование подобных примеров влечет за собой существование неизоморфных числовых полей с одинаковой ζ-функцией: достаточно рассмотреть поля K^{H_1} и K^{H_2}, где K — поле разложения какого-нибудь многочлена шестой степени над $\mathbb{Q}$, обладающего группой Галуа $\mathfrak{S}_6$.

4. *Нормальность* подгруппы H полностью определяется на уровне виртуальной подгруппы χ_H, поскольку нормальность H равносильна тому, что для любого класса сопряженных элементов $\mathcal{C}$ группы G либо $|H \cap \mathcal{C}| = 0$, либо $|H \cap \mathcal{C}| = |\mathcal{C}|$, а согласно п. 2) выше эти числа задаются χ_H.

5. Если H и N — две подгруппы в G, причем N нормальна, то H содержится в N в том и только том случае, если $|H \cap \mathcal{C}| \le |N \cap \mathcal{C}|$ для любого класса сопряженных элементов $\mathcal{C} \subset G$. Это условие равносильно также тому, что $\chi_N(g) = 0$ влечет $\chi_H(g) = 0$ для любого g из G. В частности, это замечание применимо в случае $G = \mathfrak{S}_n$, $N = \mathfrak{A}_n$, т.е. мы можем проверять четность подгруппы $H \subset \mathfrak{S}_n$ исходя из χ_H.

6. Аналогично сказанному в предыдущем пункте мы можем проверить, содержится ли нормальная подгруппа N в произвольной подгруппе $H \subset G$, поскольку это условие равносильно тому, что $|N \cap \mathcal{C}| \le |H \cap \mathcal{C}|$ для всех классов сопряженных элементов $\mathcal{C} \subset G$. Правда, в интересующем нас случае $G = \mathfrak{S}_n$ это замечание редко может быть полезным.

7. Если H_1 и H_2 — произвольные подгруппы G, то τ-критерий дает *необходимое* условие для того, чтобы H_1 содержалась в какой-либо подгруппе, сопряженной с H_2, в терминах соответствующих виртуальных подгрупп (см. 3.6.10).

8. Исходя из этого, мы можем получить необходимое условие для *разрешимости* H, если мы обладаем полным списком виртуальных подгрупп группы G (возможно, содержащим лишние элементы). Для этого достаточно заметить, что любая разрешимая подгруппа либо является единичной, либо содержит разрешимую подгруппу простого индекса. Поэтому мы можем упорядочить список виртуальных подгрупп по убыванию индекса и последовательно проверить, может ли очередная виртуальная подгруппа быть разрешимой, изучив ее возможные подгруппы простого индекса с помощью критерия из 7). Кроме того, если порядок виртуальной подгруппы χ_H является степенью простого числа, то мы знаем, что H является p-группой и потому заведомо разрешима.

9. Для любого G-множества X мы можем найти количество H-орбит множества X, исходя из χ_H и χ_X. В самом деле, рассуждая как при доказательстве 4.3.1,b), мы видим, что количество H-орбит X равно количеству G-орбит $X \times (G/H)$, которое согласно 3.5.3,b) и 3.5.3.3 равно $(\chi_X \chi_H, \chi_0)$, что в свою очередь равно (χ_X, χ_H). Итак, $|X/H| = (\chi_X, \chi_H)$.

   Отметим, что мы можем определить только количество орбит, но не их длины, как это видно из примера, приведенного в п. 3), если взять в качестве X множество чисел от 1 до 6 с естественным действием $G = \mathfrak{S}_6$: тогда набор длин H_1-орбит X есть $4+1+1$, а набор длин H_2-орбит — $2+2+2$.

10. С помощью τ-операций мы можем выразить $\chi_{\tau^r X}$ и $\chi_{\tau^{(1^r)} X}$ через χ_X (см. 3.6.5 и 3.6.7). Поскольку $\tau^r X$ и $\tau^{(1^r)} X$ — это множества r-элементных подмножеств и упорядоченных наборов из r различных элементов множества X соответственно, мы видим, что исходя из χ_H и χ_X мы можем вычислить количество H-орбит на каждом из этих множеств.

11. Все сказанное в предыдущих двух пунктах применимо, в частности, к случаю, когда $G = \mathfrak{S}_n$ и X — множество таблоидов формы ν для некоторого разбиения ν числа n (см. 4.1.9). Тогда χ_X — это в точности ψ_ν из 4.1.12, и потому количество H-орбит на множестве таблоидов формы ν равно (χ_H, ψ_ν). Напомним, что значения характера ψ_ν, равно как и коэффициенты его разложения по неприводимым характерам $\{\chi_\lambda\}$, могут быть легко вычислены (см. 4.1.18).

Все вышесказанное позволяет нам заключить, что знание виртуальной подгруппы дает нам довольно много информации о свойствах соответствующей подгруппы, и его самого по себе достаточно для решения многих задач.

5 Эффективная реализация метода

В этой главе мы обсудим существенные моменты реализации нашего метода вычисления группы Галуа, необходимые для того, чтобы эта реализация была эффективной. Как уже отмечалось во введении, одним из таких моментов является требование предварительного построения списка виртуальных подгрупп симметрической группы. Этот вопрос был подробно изучен в двух предыдущих главах. В этой же главе мы рассмотрим две другие проблемы, а именно, проблему эффективного нахождения разбиения $\lambda^{(p)}$, образованного степенями неприводимых сомножителей многочлена над конечным полем, и проблему статистической обработки результатов.

5.1 Нахождение разбиения $\lambda^{(p)}$: общие замечания

Итак, для любого многочлена $F \in \mathbb{Q}(T)$ степени n и любого простого числа $p \in \mathbb{P}$ мы хотим научиться быстро определять, является ли p исключительным для F (т.е. делителем знаменателя какого-либо из коэффициентов F или делителем дискриминанта F), и в случае отрицательного ответа (т.е. регулярности p) находить разбиение $\lambda = \lambda^{(p)} \in \mathrm{part}_n$, образованное степенями неприводимых сомножителей редукции F по модулю p.

Поскольку определить, входит или нет p в разложение знаменателей коэффициентов многочлена F, очень просто (по существу эта проверка происходит сама собой при вычислении редукции F по модулю p), мы можем предполагать, что p не делит ни один из знаменателей, так что определена редукция $\bar{F} \in \mathbb{F}_p[T]$ многочлена F по модулю p; кроме того, мы считаем, что p не делит старший коэффициент F, так что $\bar{F}$ также является многочленом степени F. Также можно считать, что $\bar{F}$ — унитарный многочлен степени n, при необходимости разделив $\bar{F}$ на старший коэффициент.

Таким образом, нам осталось решить следующую задачу: проверить сепарабельность данного унитарного многочлена $F \in k[T]$ степени n, и в случае положительного ответа найти разбиение λ, образованное степенями неприводимых сомножителей F. Здесь $k = \mathbb{F}_q$ — произвольное конечное поле характеристики p, $q = p^t$. Нас, конечно же, в первую очередь интересует случай $q = p$, однако все наши методы работают для произвольного конечного поля коэффициентов, что может пригодиться, например, для вычисления группы Галуа многочлена с коэффициентами в $\mathbb{F}_q(T)$.

Переформулируем поставленную задачу следующим образом. Рассмотрим n-мерную k-алгебру $A := k[T]/(F)$; ясно, что сепарабельность F равносильна сепарабельности, или, что в данном случае одно и то же, приведенности A. Кроме того, если A сепарабельна, то она представляется в виде $A \cong \mathbb{F}_{q^{\lambda_1}} \times \cdots \times \mathbb{F}_{q^{\lambda_s}}$, где $\lambda_1, \ldots, \lambda_s$ — это в точности степени неприводимых сомножителей многочлена F.

Мы рассмотрим два способа проверки сепарабельности A и нахождения разбиения $\lambda = (\lambda_1, \ldots, \lambda_s)$. Оба они основаны на рассмотрении степеней эндоморфизма Фробениуса Frob_A k-алгебры A, определенного, как обычно, формулой $\mathrm{Frob}_A\colon x \mapsto x^q$, поэтому мы опишем, каким образом вычислить матрицу эндоморфизма Фробениуса. Прежде всего, обозначим через θ образ T в $A = k[T]/(F)$; тогда элементы $(\theta^j)_{0 \le j \le n-1}$ образуют k-базис A, относительно которого мы будем вычислять матрицу Frob_A. Заметим, что сложение и вычитание элементов A, записанных в этом базисе, производится покомпонентно и требует $O(n)$ операций сложения и вычитания в конечном поле $k = \mathbb{F}_q$. Умножение элементов A производится посредством перемножения соответствующих многочленов из $k[T]$ степени $\le n-1$ с последующим взятием остатка от деления на F; все это требует $O(n^2)$ операций сложения, вычитания и умножения в k. Обычный «двоичный» алгоритм возведения в степень (основанный на равенствах $a^1 = a$, $a^{2k} = (a^k)^2$ и $a^{2k+1} = a^{2k} \cdot a$) позволяет вычислить θ^q за $O(\log q)$ операций умножения в A, т.е. за $O(n^2 \log q)$ арифметических операций в k. Затем можно, последовательно умножая на θ^q, найти все θ^{qj} при $0 \le j \le n-1$; все это потребует $O(n)$ операций умножения в A, т.е. $O(n^3)$ операций в поле k. Осталось заметить, что j-ый столбец матрицы Φ эндоморфизма Фробениуса Frob_A относительно рассматриваемого базиса состоит как раз из координат θ^{qj} относительно этого базиса. В итоге мы нашли матрицу Φ за $O(n^3 + n^2 \log q)$ операций в поле k.

Рассмотрим теперь по отдельности наши два метода.

5.2 Метод, основанный на вычислении рангов

Прежде всего, заметим, что сепарабельность, или, что одно и то же, приведенность A равносильна тривиальности ядра Frob_A, т.е. невырожденности матрицы Φ, или, что равносильно, условию $\operatorname{rank} \Phi = n$. Остается заметить, что ранг матрицы вычисляется методом Гаусса с помощью $O(n^3)$ операций в k, из них $O(n)$ операций деления.

Предположим теперь, что A сепарабельна и что $A \cong \mathbb{F}_{q^{\lambda_1}} \times \cdots \times \mathbb{F}_{q^{\lambda_s}}$; мы хотим определить $\lambda = (\lambda_1, \ldots, \lambda_s)$, или, что одно и то же, набор целых неотрицательных чисел $c_k = \operatorname{card}\{i : \lambda_i = k\}$. Ясно, что $\sum_{k\geq 1} kc_k = n$, так что $c_k = 0$ при $k > n$. Вычислим для произвольного $m \geq 1$ ранг матрицы $\Phi^m - E$, дополнение которого до n мы обозначим через a_m. Для этого мы рассмотрим базис A, составленный из нормальных базисов $\mathbb{F}_{q^{\lambda_i}}$ над $\mathbb{F}_q$, и заметим, что Frob_A переставляет элементы этого базиса как некоторая подстановка σ циклического типа λ. Отсюда немедленно следует, что $a_m = n - \operatorname{rank}(\Phi^m - E) = n - \operatorname{rank}(\mathrm{Frob}_A^m - 1_A)$ совпадает с количеством циклов в подстановке σ^m, т.е.

$$a_m = \sum_{i=1}^{s} \gcd(\lambda_i, m) = \sum_{k\geq 1} c_k \gcd(k, m) \quad .$$

Здесь мы воспользовались тем фактом, что цикл длины k после возведения в m-ую степень распадается на $\gcd(k, m)$ циклов одинаковой длины.

Для любого $m \geq 1$ положим $b_m := \sum_{k\geq 1} c_{km}$. Заметим, что в действительности эта сумма конечна, поскольку $c_k = 0$ при $k > n$, и $b_m = 0$ при $m > n$ по той же причине. Выразим теперь (a_m) через (b_m): $a_m = \sum_{k\geq 1} c_k \gcd(k, m) = \sum_{k\geq 1} c_k \sum_{d|\gcd(k,m)} \varphi(d) = \sum_{k\geq 1} \sum_{d|k,d|m} \varphi(d) c_k = \sum_{d|m} \varphi(d) \sum_{k'\geq 1} c_{k'd} = \sum_{d|m} \varphi(d) b_d$, где $\varphi(n)$ — функция Эйлера; в этой цепочке равенств мы воспользовались тем фактом, что $\sum_{d|n} \varphi(d) = n$ для любого $n \geq 1$. Заметим теперь, что равенства $a_m = \sum_{d|m} \varphi(d) b_d$ и $b_m = \sum_{k\geq 1} c_{km}$ позволяют однозначно определить $(c_k)_{1\leq k\leq n}$ по $(a_m)_{1\leq m\leq n}$; поскольку $c_k = 0$ при $k > n$, это означает, что λ однозначно определяется набором $(a_m)_{1\leq m\leq k}$. Мы можем явно выразить (b_m) через (a_m) и (c_k) через (b_m), воспользовавшись формулами обращения Мебиуса: получаем $b_m = \frac{1}{\varphi(m)} \sum_{d|m} \mu(m/d) a_d$ и $c_m = \sum_{k\geq 1} \mu(k) b_{km}$, где μ — функция Мебиуса. Эти формулы действительно определяют все (b_m), все (c_k) и λ по $a_1, a_2, \ldots, a_n$, поскольку мы знаем, что заведомо $b_m = 0$ и $c_m = 0$ при $m > n$.

Итак, мы видим, что первые n членов последовательности $a_m = n - \operatorname{rank}(\Phi^m - E)$ однозначно определяют λ, что дает нам возможность найти λ с помощью $O(n^4 + n^2 \log q)$ операций, поскольку для нахождения Φ нужно $O(n^3 + n^2 \log q)$ операций, и затем для последовательного вычисления $\Phi^2, \Phi^3, \ldots, \Phi^n$ и рангов матриц $\Phi^m - E$ нужно каждый раз еще $O(n^3)$ операций.

В действительности часто можно сэкономить часть этих операций, поскольку обычно λ уже определяется несколькими первыми членами последовательности (a_m). Это позволяет заранее построить «деревья распознавания» и использовать их для вычисления λ. Поясним сказанное примером для $n = 5$:

λ	$a = (a_1, a_2, \ldots)$	префикс распознавания
$(1,1,1,1,1)$	$(5,5,5,5,5,\ldots)$	$(5,\ldots)$
$(2,1,1,1)$	$(4,5,4,5,4,\ldots)$	$(4,\ldots)$
$(2,2,1)$	$(3,5,3,5,3,\ldots)$	$(3,5,\ldots)$
$(3,1,1)$	$(3,3,5,3,3,\ldots)$	$(3,3,\ldots)$
$(3,2)$	$(2,3,4,3,2,\ldots)$	$(2,*,4,\ldots)$
$(4,1)$	$(2,3,2,5,2,\ldots)$	$(2,*,2,\ldots)$
(5)	$(1,1,1,1,5,\ldots)$	$(1,\ldots)$

Укажем лишь, что при практической реализации на компьютере удобно хранить деревья поиска в структуре данных, которая называется *trie*.

5.3 Метод, основанный на вычислении следов

В отличие от предыдущего метода, этот метод применим только в том случае, если характеристика p поля коэффициентов больше степени n многочлена F. Это делает его особенно подходящим для разнохарактеристического случая (скажем, для вычисления группы Галуа многочлена с рациональными коэффициентами), поскольку мы можем выкинуть конечное число простых чисел, и почти полностью непригодным в равнохарактеристическом случае.

Суть предлагаемого метода заключается в определении λ по следам степеней эндоморфизма Фробениуса: $t_m := \operatorname{Tr} \mathrm{Frob}_A^m = \operatorname{Tr} \Phi^m$. Оказывается, что в случае $p > n$ набор $(t_m)_{1\leq m\leq n}$ однозначно определяет λ и к тому же позволяет установить, является ли алгебра A сепарабельной.

Пусть $\mathfrak{n}$ — нильрадикал k-алгебры A, $A_{\mathrm{red}} := A/\mathfrak{n}$ — приведенная алгебра, ассоциированная с A. Поскольку $p > n$, $\mathfrak{n}$ совпадает с ядром эндоморфизма Фробениуса; отсюда немедленно следует, что $\operatorname{Tr} \mathrm{Frob}_A^m = \operatorname{Tr} \mathrm{Frob}_{A_{\mathrm{red}}}^m$ для всех $m \geq 1$. Рассмотрим разложение приведенной алгебры $A_{\mathrm{red}} \cong \mathbb{F}_{q^{\lambda_1}} \times \cdots \times \mathbb{F}_{q^{\lambda_s}}$ для некоторого разбиения λ числа $n' = \dim A_{\mathrm{red}} \leq n$. Рассмотрим базис A_{red}, составленный из

нормальных базисов $\mathbb{F}_{q^{\lambda_i}}$ над $k = \mathbb{F}_q$; автоморфизм Фробениуса $\mathrm{Frob}_{A_{\mathrm{red}}}$ действует на этом базисе как некоторая подстановка $\sigma \in \mathfrak{S}_{n'}$ циклического типа λ; отсюда получаем, что $t_m = \mathrm{Tr}\,\mathrm{Frob}^m_{A_{\mathrm{red}}}$ совпадает с образом в простом подполе $\mathbb{F}_p \subset \mathbb{F}_q$ количества неподвижных точек t'_m подстановки σ^m. Поскольку $0 \le t'_m \le n' \le n < p$, мы можем однозначно восстановить t'_m по $t_m = t'_m \bmod p$.

Положим $c_k := \mathrm{card}\{i : \lambda_i = k\}$; тогда $\sum_{k\ge1} kc_k = |\lambda| = n' \le n$, так что $c_k = 0$ при $k > n$. Кроме того, $t'_m = \sum_{i:\lambda_i|m} \lambda_i = \sum_{d|m} dc_d$, откуда по формуле обращения Мебиуса получаем $c_m = \frac{1}{m}\sum_{d|m} \mu(m/d)t'_d$. Это показывает, что знание набора $(t'_m)_{1\le m\le n}$, или, что равносильно, знание набора $(t_m)_{1\le m\le n}$ позволяет определить все c_k (поскольку $c_k = 0$ при $k > m$), а значит, и λ, а также $n' = \sum_{k\ge1} kc_k$. При этом сепарабельность алгебры A также проверяется таким способом, поскольку эта сепарабельность равносильна равенству $n' = n$.

Это показывает, что данный метод более эффективен, чем предыдущий, поскольку он использует только умножение матриц $n \times n$ и вычисление их следов, хотя асимптотически число используемых операций есть $O(n^4 + n^2 \log q)$, как и для предыдущего метода.

Кроме того, как и для предыдущего метода, часто сепарабельность алгебры A и разбиение λ (которое нас интересует только в сепарабельном случае) определяются уже первыми несколькими членами последовательности следов (t'_m). Это позволяет строить деревья поиска, в которые включаются все разбиения λ числа n, а также все разбиения $\mu = (\mu_1, \ldots, \mu_s)$ чисел $n' < n$, такие, что $n = c_1\mu_1 + \cdots + c_s\mu_s$ для некоторого набора натуральных чисел (c_k) (можно обойтись только такими μ, поскольку μ — это набор степеней различных неприводимых сомножителей многочлена $F(T)$, и потому такие числа c_k должны существовать — можно взять кратности соответствующих сомножителей); при этом в дереве поиска такие μ не различаются, а только помечается, что они соответствуют несепарабельному случаю. Вот пример такого дерева поиска для $n = 5$:

$t' = (t'_1, t'_2, \ldots)$	v	λ
$(0, 0, \ldots)$	7	(5)
$(0, 2, \ldots)$	5	$(3, 2)$
$(1, 1, 1, 1, \ldots)$	-1	
$(1, 1, 1, 5, \ldots)$	6	$(4, 1)$
$(1, 1, 4, \ldots)$	-1	
$(1, 3, \ldots)$	-1	
$(1, 5, \ldots)$	3	$(2, 2, 1)$
$(2, 2, 2, \ldots)$	-1	
$(2, 2, 5, \ldots)$	4	$(3, 1, 1)$
$(2, 4, \ldots)$	-1	
$(3, 3, \ldots)$	-1	
$(3, 5, \ldots)$	2	$(2, 1, 1, 1)$
$(4, \ldots)$	-1	
$(5, \ldots)$	1	$(1, 1, 1, 1, 1)$

Здесь v — это -1 для несепарабельной алгебры A или номер разбиения λ при лексикографическом упорядочении всех разбиений числа n; ясно, что при работе на компьютере удобнее иметь дело не с λ, а с v.

Отметим, что существует также метод, который использует сначала метод Гаусса для проверки сепарабельности, как это делалось в методе, основанном на вычислении рангов, а затем вычисляет следы степеней автоморфизма Фробениуса для определения разбиения λ числа n; при этом нужно вычислять меньшее количество степеней автоморфизма Фробениуса, поскольку уже известна сепарабельность A. Вот возникающее дерево распознавания для $n = 5$:

$t' = (t'_1, t'_2, \ldots)$	v	λ
$(0, 0, \ldots)$	7	(5)
$(0, 2, \ldots)$	5	$(3, 2)$
$(1, 1, \ldots)$	6	$(4, 1)$
$(1, 5, \ldots)$	3	$(2, 2, 1)$
$(2, \ldots)$	4	$(3, 1, 1)$
$(3, \ldots)$	2	$(2, 1, 1, 1)$
$(5, \ldots)$	1	$(1, 1, 1, 1, 1)$

5.4 Статистический анализ результатов

Нам осталось теперь обсудить, после какого количества проанализированных простых чисел мы можем определить искомую группу Галуа (точнее, соответствующую виртуальную подгруппу $\mathfrak{S}_n$) с заранее указанным уровнем достоверности. Для этого мы рассмотрим следующую довольно близкую статистическую задачу. Предположим, что мы хотим определить некоторый неизвестный параметр η, принадлежащий некоторому заранее фиксированному конечному множеству H (в нашем случае H — множество всех виртуальных подгрупп $\mathfrak{S}_n$, а η соответствует искомой группе Галуа). Для этого мы проводим серию экспериментов $\xi_1, \xi_2, \ldots, \xi_j, \ldots$ (испытаний регулярных простых чисел), результат ξ_j каждого из которых принадлежит некоторому заранее известному конечному множеству Ξ (у нас $\Xi = \mathrm{part}_n$ — множество всех разбиений числа n, а ξ_j — это разбиение $\lambda^{(p)}$, соответствующее очередному простому числу p). Предположим, что для каждого $h \in H$ нам известна функция распределения вероятностей $p_h \colon \Xi \to [0,1]$ (т.е. такая функция, что $P(\xi_j = x | \eta = h) = p_h(x)$), и что различным h соответствуют различные p_h (иначе нам никак не различить такие $h \neq h'$, что $p_h = p_{h'}$). Кроме того, мы считаем, что если $p_h(x) = 0$, то ξ_j не может принимать значение x при $\eta = h$ (в нашем случае это условие выполнено, поскольку если подгруппа Галуа G симметрической группы $\mathfrak{S}_n$ не содержит подстановок некоторого циклического типа λ, то ни при каком регулярном p равенство $\lambda^{(p)} = \lambda$ невозможно, так как оно означало бы, что соответствующий элемент Фробениуса $\mathrm{Frob}_p \in G \subset \mathfrak{S}_n$ является подстановкой циклического типа λ). Еще одно предположение, которое мы делаем, заключается в том, что результаты различных экспериментов независимы (мы еще обсудим, что это означает в нашей ситуации).

Зафиксируем некоторое малое положительное ε (например, $\varepsilon = 10^{-6}$) и зададимся следующим вопросом: можем ли мы по N уже проделанным экспериментам определить η с вероятностью ошибки, меньшей ε, в случае положительного ответа определить η, а в случае отрицательного ответа найти примерное количество экспериментов, которые надо еще сделать для определения η.

Пусть N — количество уже проделанных экспериментов, $m_x := \mathrm{card}\{1 \leq j \leq N : \xi_j = x\}$ — количество экспериментов, в которых был получен результат $x \in \Xi$. Составим подмножество $H' \subset H$, образованное теми $h \in H$, для которых $p_h(x) > 0$ для всех $x \in \Xi$, таких, что $m_x > 0$. Ясно, что заведомо $\eta \in H'$ (напомним, что мы предполагаем, что при $\eta = h$ величина ξ_j не может принимать значения x, для которых $p_h(x) = 0$). Рассмотрим условные вероятности $P_h := P(A|\eta = h)$ получения данного набора (m_x) при условии $\eta = h$. Ясно, что $P_h = \prod_{x \in \Xi} p_h(x)^{m_x}$ и $\log P_h = \sum_{x \in \Xi} m_x \log p_h(x)$. Если $(Q_h)_{h \in H}$ — некоторое априорное распределение вероятностей того, что $\eta = h$ (т.е. $Q_h = P(\eta = h)$; мы предполагаем, что все $Q_h > 0$; конечно же, $\sum_{h \in H} Q_h = 1$), то по формуле Байеса

$$P(\eta = h_0 | A) = \frac{P(A|\eta = h_0) P(\eta = h_0)}{\sum_{h \in H} P(A|\eta = h) P(\eta = h)} = \frac{P_{h_0} Q_{h_0}}{\sum_{h \in H} P_h Q_h} \quad .$$

Мы хотели бы получить условие существования такого $h_0 \in H$, что $P(\eta = h_0|A) > 1 - \varepsilon$; вместо этого мы будем изучать почти равносильное условие $P(\eta = h|A)/P(\eta = h_0|A) < \varepsilon$ при всех $h \neq h_0$ (на самом деле из этого условия следует, что $P(\eta = h_0|A) > 1 - \varepsilon \cdot |H|$; мы считаем, что ε очень мало, а во множестве H гораздо меньше элементов, чем ε^{-1}). По формуле Байеса $P(\eta = h|A)/P(\eta = h_0|A) = P_h Q_h / (P_{h_0} Q_{h_0})$; логарифмируя, получаем условие

$$\sum_{x \in \Xi} m_x \log p_h(x) - \sum_{x \in \Xi} m_x \log p_{h_0}(x) < \log \varepsilon + \log Q_{h_0} - \log Q_h \quad .$$

Поскольку про значения Q_h нам ничего не известно, естественно в этом выражении заменить $\log Q_{h_0} - \log Q_h$ на нуль. Вот некоторое обоснование такого шага: если все $Q_h > \delta > 0$ (скажем, $\delta = 10^{-3}$), то заведомо $\log Q_h - \log Q_{h_0} < -\log \delta$, и потому, если левая часть рассмотренного неравенства меньше $\log \varepsilon + \log \delta$, то она меньше и $\log \varepsilon + \log Q_{h_0} - \log Q_h$; поэтому можно, заменив при необходимости ε на $\varepsilon\delta$, рассматривать условие

$$\sum_{x \in \Xi} m_x \log p_h(x) - \sum_{x \in \Xi} m_x \log p_{h_0}(x) < \log \varepsilon \quad .$$

Положим $V_h := \sum_x m_x \cdot \big(-\log p_h(x)\big)$, $M := -\log \varepsilon$; тогда полученное условие можно переписать в виде $V_{h_0} < V_h - M$.

Итак, предлагаемый метод решения поставленной задачи таков: вычисляем для всех $h \in H$ (а на самом деле только для $h \in H'$) $V_h := \sum_x m_x \cdot \big(-\log p_h(x)\big)$, $M := -\log \varepsilon$ (что-то вроде 20), выбираем

индексы h_0 и $h_1 \neq h_0$ из H, такие, что $V_{h_0} \leq V_{h_1} \leq V_h$ для всех $h \in H$, отличных от h_0 и h_1, и проверяем условие $V_{h_1} - V_{h_0} > M$. Если это условие выполнено, возвращаем h_0 в качестве значения η; если же нет, производим еще порядка $N \cdot \big(M/(V_{h_1} - V_{h_0}) - 1\big)$ экспериментов (лучше всего умножить это число на какую-нибудь константу, бóльшую единицы, скажем, 1.2, и добавить небольшое число вроде пяти; кроме того, если получается слишком много — скажем, больше $2N$ — то мы делаем только $2N$ экспериментов). Затем мы снова анализируем полученные данные, при необходимости снова делаем дополнительные эксперименты, и так до тех пор, пока мы не сможем определить η с нужной степенью уверенности.

Мы можем оценить число экспериментов, необходимое для определения η в случае $\eta = h_0$, следующим образом. Заменим m_x на его математическое ожидание $Np_{h_0}(x)$; тогда $V_h = N \sum_x p_{h_0}(x) \cdot (-\log p_h(x))$, и условие $V_{h_0} < V_h - M$ при всех $h \neq h_0$ оказывается равносильным условию $N > N_0 = \big(\min_{h \neq h_0} \sum_x p_{h_0}(x) \cdot (-\log p_h(x)) - \sum_x p_{h_0}(x) \cdot (-\log p_{h_0}(x))\big)^{-1}$.

Интересно, что оценки числа экспериментов (т.е. регулярных простых чисел), необходимых для определения группы Галуа многочлена степени $n \leq 10$ с вероятностью ошибки $\leq 10^{-6}$, вычисленные по указанной выше формуле с помощью уже построенной таблицы виртуальных подгрупп $\mathfrak{S}_n$, $n \leq 10$, оказываются на удивление небольшими — порядка 100–200, а наибольшее значение равно 513.7. Это показывает, насколько важно для рассматриваемого метода предварительное определение списка всех возможных виртуальных подгрупп, поскольку без такого списка потребовалось бы астрономическое количество экспериментов — порядка $50 \cdot (10^6)^2$.

Для применения рассмотренного метода анализа результатов к задаче определения группы Галуа следует сделать еще несколько дополнений. Во-первых, как лучше всего выбирать простые числа p для экспериментов? Предлагается выбирать их подряд, начиная с некоторой нижней границы, большей n (чтобы можно было пользоваться методом из раздела 5.3); такое предложение, помимо своей простоты, основано на известных свойствах аналитической плотности множеств простых чисел из теоремы плотности Чеботарева (см. [15], [9] и [16]).

Кроме того, предлагается следующая оптимизация. Всякий раз, когда мы получаем результат эксперимента (т.е. разбиение λ), никогда не получавшийся ранее, мы просматриваем список виртуальных подгрупп $\mathfrak{S}_n$, которые могут оказаться искомой группой Галуа, и выкидываем из него все элементы h с $p_h(\lambda) = 0$, поскольку такие виртуальные подгруппы заведомо не могут быть искомой группой Галуа. Если в какой-то момент в этом списке остается ровно один элемент (им может оказаться только симметрическая группа $\mathfrak{S}_n$), мы его сразу выдаем в качестве ответа. Кроме того, значения выражений V_h мы вычисляем только для h из этого списка, что позволяет сэкономить много усилий.

Еще один момент: может так получиться, что все рассматриваемые простые числа оказываются исключительными. Если произведение всех рассмотренных исключительных чисел больше некоторой оценки сверху модуля дискриминанта многочлена $F(T)$, это означает, что исходный многочлен F не был сепарабельным, на чем вычисление группы Галуа можно прекратить. Вместо этого автор считает, что если первые сто рассмотренных простых чисел оказались исключительными, то F несепарабелен; в том случае, если коэффициенты $F(T)$ относительно небольшие, такой подход оправдан; если же это не так, необходимую границу количества исключительных простых чисел следует определять исходя из размера коэффициентов многочлена.

Какое минимальное количество простых чисел следует рассмотреть? Иначе говоря, какова изначальная оценка на число экспериментов N? Рассуждения, аналогичные приведенным выше, показывают, что искомая граница зависит от размера коэффициентов многочлена примерно так же, как граница количества исключительных простых чисел, рассмотренная только что (при этом полезно рассмотреть многочлен $F(T) = T^2 - (p_1 p_2 \cdots p_N + 1)$, где $p_1, \ldots, p_N$ — первые N рассмотренных простых чисел). Поэтому автор предлагает изначально использовать $N = 100$ для многочленов с относительно небольшими коэффициентами, а количество дополнительных экспериментов рассчитывать по методике, изложенной выше (в действительности оценка из 2.3.1 показывает, что минимальное необходимое число экспериментов должно быть пропорционально логарифму дискриминанта многочлена $F(T)$).

Последний вопрос, который нам следует обсудить, таков: в какой степени статистическая модель, приведенная выше, соответствует ситуации, возникающей при нашем методе вычисления группы Галуа? Более тонкий статистический анализ показывает, что вместо независимости ξ_j достаточно требовать, чтобы дисперсия m_x оценивалась линейной функцией от N, т.е., грубо говоря, чтобы $m_x = Np_{h_0}(x) + O(N^{1/2})$. При этом теорема плотности Чеботарева на самом деле утверждает, что если ζ-функция Римана не имеет нулей в полосе $\operatorname{Re} z \geq 1 - \varepsilon$, то можно написать оценку вида $m_x = Np_{h_0}(x) + O(N^{1-\varepsilon})$; если гипотеза Римана верна, то можно брать ε сколь угодно близким к $1/2$

(см. оценку из [15], полученную в предположении верности обощенной гипотезы Римана; см. также [9], где эта оценка улучшена, и [16], где даны явные оценки возникающей константы; см. также 2.3.1, где мы привели результирующую формулировку теоремы плотности Чеботарева). Это практически полностью обосновывает произведенную выше замену исходной задачи на статистическую задачу.

Таким образом, произведенные оценки количества регулярных чисел, необходимых для определения группы Галуа, на самом деле верны, только если гипотеза Римана верна. Это не означает, что наш метод вычисления группы Галуа основан на гипотезе Римана: он будет работать и без гипотезы Римана, только гораздо дольше. Впрочем, практика показывает, что для определения группы Галуа многочлена степени ≤ 11 обычно действительно достаточно рассмотрения двухсот–трехсот простых чисел, что может рассматриваться как еще одно подтверждение (впрочем, довольно косвенное) истинности гипотезы Римана.

Кроме того, отметим, что эффективная версия теоремы плотности Чеботарева 2.3.1 дает возможность после определенного числа «экспериментов» *точно* выяснить виртуальную подгруппу, соответствующую группе Галуа: в какой-то момент все другие предположения о возможной виртуальной подгруппе начнут противоречить оценке 2.3.1, и при реализации нашего метода можно использовать это условие для проверки необходимости дополнительных экспериментов. Тем не менее приведенный выше приблизительный статистический анализ представляется полезным как минимум по двум причинам:

1) Мы получаем оценки на необходимое число экспериментов (по крайней мере, если у многочлена $F(T)$ относительно небольшие коэффициенты), а значит, и на время работы нашего алгоритма.

2) Этот упрощенный статистический анализ не зависит от дискриминанта многочлена $F(T)$, что позволяет использовать его на практике, по крайней мере для многочленов с небольшими коэффициентами, если мы готовы допустить некоторую «вероятность ошибки».

6 Заключение

Подведем общий итог.

- На основе теоремы плотности Чеботарева возможно построение эффективного метода вычисления группы Галуа многочлена с рациональными коэффициентами как подгруппы (точнее, соответствующей «виртуальной подгруппы») симметрической группы $\mathfrak{S}_n$.
- В настоящей работе предложен и подробно изучен один из таких методов. Были произведены также исследования, необходимые для его эффективной реализации на компьютере.
- Предложенный метод может быть эффективным, только если мы располагаем заранее вычисленной таблицей «виртуальных подгрупп» $\mathfrak{S}_n$, содержащей не слишком много «несущественных» (т.е. не соответствующих никакой реальной подгруппе) виртуальных подгрупп. В связи с этим нами был предложен, изучен и реализован при $n \leq 11$ метод перечисления всех виртуальных подгрупп симметрической группы.
- Этот метод перечисления виртуальных подгрупп существенно использует введенные и изученные в работе τ-операции на кольцах характеров конечных групп, а также основанный на них τ-критерий.
- Помимо этого, τ-операции и τ-критерий позволяют получать информацию о подгруппах симметрической группы, исходя из соответствующих виртуальных подгрупп. Например, мы располагаем хорошими необходимыми условиями для того, чтобы подгруппа была разрешимой или чтобы она содержалась в другой подгруппе.
- Из виртуальной подгруппы можно извлечь много информации о соответствующей подгруппе симметрической группы, даже если соответствующую подгруппу нельзя однозначно восстановить. Например, порядок, индекс, четность и транзитивность подгруппы, а также циклические типы входящих в нее подстановок всегда определяются виртуальной подгруппой. Кроме того, транзитивные подгруппы $\mathfrak{S}_n$ при $n \leq 7$ однозначно определяются соответствующими виртуальными подгруппами.
- Предложенный метод, в отличие от большинства других применяемых на практике методов, работает для произвольных сепарабельных многочленов, не обязательно неприводимых. Это позволяет использовать его для проверки совпадения, включения или линейной разделенности полей разложения нескольких многочленов.
- Предложенный метод позволяет вычислять количество (но не длины) орбит относительно действия группы Галуа многочлена $F(T)$ на различных $\mathfrak{S}_n$-множествах, например, на упорядоченных или неупорядоченных наборах, составленных из r различных корней многочлена $F(T)$. Поскольку это представляет собой бóльшую часть информации, обычно извлекаемой из метода линейных резольвент, а наш метод предоставляет и много другой информации о группе Галуа, представляется целесообразным его использование вместо метода линейных резольвент как и для получения частичной информации о группе Галуа, так и перед применением алгоритмов полного определения группы Галуа, основанных на методе относительных резольвент, для сокращения необходимого объема вычислений.

Список литературы

[1] Джеймс Г., *Теория представлений симметрических групп*, «Мир», М., 1982.

[2] Касселс Дж., Фрёлих А., *Алгебраическая теория чисел*, «Мир», М., 1969.

[3] Бурбаки Н., *Алгебра. Гл. X. Гомологическая алгебра*, «Наука», М., 1987.

[4] ван дер Варден Б.Л., *Алгебра*, 2-е изд., «Наука», М., 1979.

[5] Дуров Н.В., *Вычисление группы Галуа многочлена с рациональными коэффициентами I*, Зап. научн. семин. ПОМИ **319** (2004), 117–198.

[6] Дуров Н.В., *Вычисление группы Галуа многочлена с рациональными коэффициентами II*, Зап. научн. семин. ПОМИ **321** (2005), 90–135.

[7] Серр Ж.-П., *Дзета-функции и L-функции*, УМН **20** (1965), 19–26.

[8] Серр Ж.-П., *Линейные представления конечных групп*, «Мир», М., 1970.

[9] Serre J.P., *Quelques applications du théorème de densité de Chebotarev*, Publ. Math. IHES, **54** (1981), 123–201.

[10] Dieudonné J., Grothendieck A., *Eléments de Géométrie Algèbrique I: Le language des schémas*, Publ. Math. IHES, **4** (1960).

[11] Dieudonné J., Grothendieck A., *Eléments de Géométrie Algèbrique IV: Étude locale des schémas et des morphismes de schémas*, Publ. Math. IHES, **20** (1964), **24** (1965), **28** (1966), **32** (1967).

[12] Grothendieck A. et al., *Revêtements étales et Groupe Fondamental*, Lecture Notes in Math., 224, Springer-Verlag, Heidelberg, 1971.

[13] Artin M., Grothendieck A., Verdier J. L. et al., *Théorie des Topos et Cohomologie Étale des Schémas*, Lecture Notes in Math., 269, 270, 305, Springer-Verlag, Heidelberg, 1972–1973.

[14] Berthelot P., Illusie L. et al., *Théorie des Intersections et Théorème de Riemann–Roch*, Lecture Notes in Math., 225, Springer-Verlag, Heidelberg, 1971.

[15] Lagarias J.C., Odlyzko A.M., *Effective versions of the Chebotarev density theorem* // Frölich A. (ed.), *Algebraic Number Fields (L-functions and Galois properties)*, pp. 409–464, Academic Press, 1977.

[16] Œsterlé J., *Versions effectives du théorème de Chebotarev sous l'hypothèse de Riemann généralisée*, Astérisque, **61** (1979), 165–167.

[17] Tschebotareff N., *Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionklasse gehören*, Math. Ann. **95** (1926), 191–228.

[18] Jordan C., *Traité des substitutions et des équations algébriques*, Gauthier–Villars, 1870.

[19] Hulpke A., *Techniques for the Computation of Galois Groups* // *Algorithmic algebra and number theory (Heidelberg, 1997)*, pp. 65–77, Springer-Verlag, Berlin, 1999

[20] Stauduhar R.P., *The determination of Galois groups*, Math. Comp. **27** (1973), 981–996.

[21] McKay J., Soicher L.H., *Computing Galois groups over the rationals*, J. Number Theory **20** (1985), 273–281.

[22] Yokoyama K., *A modular method for computing the Galois group of polynomials*, J. Pure Appl. Algebra **117–118** (1997), 617–636.

[23] Geissler K., Klüners J., *Galois group computation for rational polynomials*, J. Symb. Comp. **30** (2000), no. 6, 653–674.

[24] Butler G., McKay J., *The transitive groups of degree up to eleven*, Comm. Alg. **11** (1983), no. 8, 863–911.

[25] Conway J., Hulpke A., McKay J., *On transitive permutation groups*, LMS J. Comput. Math., **1** (1998), 1–8.

[26] Darmon H., Ford D., *Computational verification of M_{11} and M_{12} as Galois groups over $\mathbb{Q}$*, Comm. Algebra **17** (1989), 2941–2943.

[27] Matzat B.H., *Konstruktive Galoistheorie*, Lecture Notes in Math., 1284, Springer-Verlag, Heidelberg, 1987.

A Примеры и таблицы

A.1 Примеры вычисления группы Галуа

Приведем несколько примеров вычисления группы Галуа.

Все приводимые нами результаты вычислений получены с помощью программы, реализующей наш метод. Во избежание повторений введем следующие обозначения: группу Галуа многочлена $F_j(T)$ обозначим через G_j, а его поле разложения над $\mathbb{Q}$ — через K_j. Кроме того, для каждого примера вычислений мы будем приводить в скобках затраченное время работы компьютера в миллисекундах (мс), количество рассмотренных простых s и максимальное рассмотренное простое число p_m, а также номер соответствующей виртуальной подгруппы в списке виртуальных подгрупп (для $n \leq 6$ эти списки приведены в конце приложения).

Некоторые из наших примеров основаны на многочленах, приведенных в работах [21], [26] и [27].

Первые несколько примеров призваны иллюстрировать, какого рода информацию мы можем получать, обладая алгоритмом вычисления группы Галуа приводимых многочленов (см. Введение). В частности, все полученные утверждения о полях разложения используют только порядки групп Галуа, которые всегда определяются нашим алгоритмом.

1) Рассмотрим многочлены $F_1(T) = T^5 - T - 1$, $F_2(T) = T^5 - 5T^4 + 8T^3 - 13T^2 + 12T - 4$ и $F_3(T) = F_1(T)F_2(T) = T^{10} - 5T^9 + 8T^8 - 13T^7 + 11T^6 - 3T^4 + 5T^3 + T^2 - 8T + 4$.

Тогда $G_1 = \mathfrak{S}_5$ (0 мс; $s = 2$; $p_m = 11$; $|G_1| = 120$; вирт. подгр. #39) и $G_2 = \mathfrak{S}_5$ (аналогично). При этом G_3 — подгруппа в $\mathfrak{S}_{10}$ порядка 120 (20 мс; $s = 122$; $p_m = 701$; $|G_3| = 120$; #3989).

Из этого мы можем заключить, что $G_1 \cong G_3 \cong G_2$, что $G_3 \cong \mathfrak{S}_5$ и что все три поля разложения K_1, K_2 и K_3 совпадают.

2) Рассмотрим $F_1(T) = T^5 - T - 1$, $F_2(T) = T^5 - T - 2$ и $F_3(T) = F_1(T)F_2(T) = T^{10} - 2T^6 - 3T^5 + T^2 + 3T + 2$.

Тогда $G_1 = \mathfrak{S}_5$ (см. выше), $G_2 = \mathfrak{S}_5$ (0 мс; $s = 3$; $p_m = 13$; $|G_2| = 120$; #39), а G_3 — группа порядка $14400 = 120^2$ (20 мс; $s = 62$; $p_m = 313$; $|G_3| = 14400$; #4570).

Поскольку $|G_3| = |G_1| \cdot |G_2|$, из этого следует, что $G_3 \cong G_1 \times G_2 = \mathfrak{S}_5 \times \mathfrak{S}_5 \subset \mathfrak{S}_{10}$ и что поля K_1 и K_2 линейно разделены над $\mathbb{Q}$.

3) Пусть $F_1(T) = T^5 - T - 1$, $F_2(T) = T^6 + 10T^5 + 55T^4 + 140T^3 + 175T^2 - 3019T + 25$ и $F_3(T) = F_1(T)F_2(T) = T^{11} + 10T^{10} + 55T^9 + 140T^8 + 174T^7 - 3030T^6 - 40T^5 - 195T^4 - 315T^3 + 2844T^2 + 2994T - 25$.

Тогда, как и в предыдущих примерах, $G_1 = \mathfrak{S}_5$; G_2 — нечетная (не содержащаяся в $\mathfrak{A}_6$) транзитивная подгруппа в $\mathfrak{S}_6$ порядка 120 (3 мс; $s = 62$; $p_m = 313$; $|G_2| = 120$; #96) и G_3 — также группа порядка 120 (32 мс; $s = 153$; $p_m = 929$; $|G_3| = 120$; #9957).

Отсюда мы, как и в примере 1), можем сделать вывод о том, что поля разложения K_1 и K_2 совпадают, что подгруппа $G_2 \subset \mathfrak{S}_6$ изоморфна $\mathfrak{S}_5$ и что многочлен $F_2(T)$ неприводим (поскольку G_2 транзитивна).

Кроме того, для $n \leq 7$ транзитивные подгруппы симметрической группы $\mathfrak{S}_n$ однозначно определяются соответствующими виртуальными подгруппами, и потому мы можем точно определить $G_2 \subset \mathfrak{S}_6$. Оказывается, что $G_2 \cong PGL_2(\mathbb{F}_5)$ (эта группа естественным образом действует на проективной прямой над $\mathbb{F}_5$, в которой как раз шесть $\mathbb{F}_5$-рациональных точек; тем самым определено вложение $PGL_2(\mathbb{F}_5) \subset \mathfrak{S}_6$).

4) Пусть $F_1(T) = T^6 + 6T^4 + 2T^3 + 9T^2 + 6T - 4$, $F_2(T) = T^2 - T - 1$ и $F_3(T) = F_1(T)F_2(T) = T^8 - T^7 + 5T^6 - 4T^5 + T^4 - 5T^3 - 19T^2 - 2T + 4$.

Тогда G_1 — четная транзитивная подгруппа $\mathfrak{S}_6$ порядка 36 (3 мс; $s = 60$; $p_m = 307$; $|G_1| = 36$; #89), $G_2 = \mathfrak{S}_2$ (0 мс; $s = 1$; $p_m = 3$; #4) и G_3 — нечетная подгруппа $\mathfrak{S}_8$ порядка 36 (9 мс; $s = 101$; $p_m = 571$; $|G_3| = 36$; #457).

Поскольку $|G_1| = |G_3|$, мы можем заключить, что $G_1 \cong G_3$ и что $K_1 = K_3 = K_1K_2$, т.е. что $K_2 \subset K_1$. Иначе говоря, поле K_1 содержит «золотое сечение» — корень многочлена $T^2 - T - 1$.

5) Пусть $F_1(T) = T^{11} - T - 1$. Тогда $G_1 = \mathfrak{S}_{11}$ (0 мс; $s = 3$; $p_m = 19$; $|G_1| = 11!$; #11800).

Этот пример демонстрирует тот факт, что для определения того, что группа Галуа данного многочлена является симметрической, обычно достаточно рассмотрения трех–четырех простых чисел. Этот эффект точно так же проявляется и для многочленов с «большими» коэффициентами; мы не будем приводить здесь соответствующие примеры.

6) Пусть $F_1(T) = T^{10}+T^9+\cdots+T^2+T+1$ — многочлен деления круга. Тогда G_1 — группа порядка 10, содержащая цикл длины 10, и потому изоморфная циклической группе $C_{10} = \mathbb{Z}/10\mathbb{Z}$ (12 мс; $s = 121$; $p_m = 691$; $|G_1| = 10$; #1604).

7) Пусть $F_1(T) = T^{11} + 105T^{10} + 4575T^9 + 106575T^8 + 1421850T^7 + 10754250T^6 + 43200750T^5 + 108840750T^4 + 645079125T^3 + 4357168125T^2 - 279006525T - 66430125$.

Тогда G_1 — четная транзитивная подгруппа в $\mathfrak{S}_{11}$ порядка 7920 (35 мс; $s = 152$; $p_m = 919$; $|G_1| = 7920$; #11731).

Многочлен $F_1(5T)/5^{11}$ получен в [27] подстановкой $X = 1$ в некоторый многочлен над $\mathbb{Q}(X)$, группа Галуа которого есть группа Матье M_{11}. Поскольку порядок M_{11} равен как раз 7920, мы видим, что G_1 также должна быть группой Матье M_{11}. Тем самым мы проверили утверждение из [27] о том, что группа Галуа G_1 многочлена $F_1(T)$ равна M_{11}.

Этот пример показывает, каким образом можно использовать наш метод в задачах обратной теории Галуа.

Приведенные выше примеры демонстрируют, что на практике для вычисления нашим методом группы Галуа (точнее, соответствующей виртуальной подгруппы) многочлена степени ≤ 11 обычно требуется рассмотреть менее двухсот простых модулей, для чего достаточно 40 мс вычислений.

A.2 Таблицы характеров $\mathfrak{S}_n$ при $n \leq 6$

Для каждого значения n от 1 до 6 мы приводим две таблицы, вычисленные с помощью метода, описанного в 4.1.18. Первая из них — это таблица характеров $\mathfrak{S}_n$. Ее строки соответствуют простым характерам χ_λ, а столбцы — классам сопряженных элементов $\mathcal{C}_\mu$, где λ и μ — разбиения числа n. Как обычно, мы располагаем все разбиения числа n в лексикографическом порядке. Помимо значений $\chi_\lambda(\mathcal{C}_\mu)$, для каждого класса сопряженных элементов указано количество элементов в нем — $d_\mu = \operatorname{card}\mathcal{C}_\mu$. Вторая таблица состоит из коэффициентов $m_{\lambda\mu} = (\psi_\lambda, \chi_\mu)$ (см. 4.1.18). Для $n = 5$ и 6 мы используем сокращенные обозначения для записи разбиений, соответствующих столбцам таблицы.

1.

d_μ	1
$\chi_\lambda(\mathcal{C}_\mu)$	(1)
(1)	1

$m_{\lambda\mu}$	(1)
(1)	1

2.

d_μ	1	1
$\chi_\lambda(\mathcal{C}_\mu)$	(1,1)	(2)
(1,1)	1	−1
(2)	1	1

$m_{\lambda\mu}$	(1,1)	(2)
(1,1)	1	1
(2)	0	1

3.

d_μ	1	3	2
$\chi_\lambda(\mathcal{C}_\mu)$	(1,1,1)	(2,1)	(3)
(1,1,1)	1	−1	1
(2,1)	2	0	−1
(3)	1	1	1

$m_{\lambda\mu}$	(1,1,1)	(2,1)	(3)
(1,1,1)	1	2	1
(2,1)	0	1	1
(3)	0	0	1

4.

d_μ	1	6	3	8	6
$\chi_\lambda(\mathcal{C}_\mu)$	(1,1,1,1)	(2,1,1)	(2,2)	(3,1)	(4)
(1,1,1,1)	1	−1	1	1	−1
(2,1,1)	3	−1	−1	0	1
(2,2)	2	0	2	−1	0
(3,1)	3	1	−1	0	−1
(4)	1	1	1	1	1

$m_{\lambda\mu}$	(1,1,1,1)	(2,1,1)	(2,2)	(3,1)	(4)
(1,1,1,1)	1	3	2	3	1
(2,1,1)	0	1	1	2	1
(2,2)	0	0	1	1	1
(3,1)	0	0	0	1	1
(4)	0	0	0	0	1

5.

d_μ	1	10	15	20	20	30	24
$\chi_\lambda(\mathcal{C}_\mu)$	(1^5)	$(2,1^3)$	$(2^2,1)$	$(3,1^2)$	$(3,2)$	$(4,1)$	(5)
$(1,1,1,1,1)$	1	−1	1	1	−1	−1	1
$(2,1,1,1)$	4	−2	0	1	1	0	−1
$(2,2,1)$	5	−1	1	−1	−1	1	0
$(3,1,1)$	6	0	−2	0	0	0	1
$(3,2)$	5	1	1	−1	1	−1	0
$(4,1)$	4	2	0	1	−1	0	−1
(5)	1	1	1	1	1	1	1

$m_{\lambda\mu}$	(1^5)	$(2,1^3)$	$(2^3,1)$	$(3,1^2)$	$(3,2)$	$(4,1)$	(5)
$(1,1,1,1,1)$	1	4	5	6	5	4	1
$(2,1,1,1)$	0	1	2	3	3	3	1
$(2,2,1)$	0	0	1	1	2	2	1
$(3,1,1)$	0	0	0	1	1	2	1
$(3,2)$	0	0	0	0	1	1	1
$(4,1)$	0	0	0	0	0	1	1
(5)	0	0	0	0	0	0	1

6.

d_μ	1	15	45	15	40	120	40	90	90	144	120
$\chi_\lambda(\mathcal{C}_\mu)$	(1^6)	$(2,1^4)$	$(2^2,1^2)$	(2^3)	$(3,1^3)$	$(3,2,1)$	(3^2)	$(4,1^2)$	$(4,2)$	$(5,1)$	(6)
$(1,1,1,1,1,1)$	1	−1	1	−1	1	−1	1	−1	1	1	−1
$(2,1,1,1,1)$	5	−3	1	1	2	0	−1	−1	−1	0	1
$(2,2,1,1)$	9	−3	1	−3	0	0	0	1	1	−1	0
$(2,2,2)$	5	−1	1	3	−1	−1	2	1	−1	0	0
$(3,1,1,1)$	10	−2	−2	2	1	1	1	0	0	0	−1
$(3,2,1)$	16	0	0	0	−2	0	−2	0	0	1	0
$(3,3)$	5	1	1	−3	−1	1	2	−1	−1	0	0
$(4,1,1)$	10	2	−2	−2	1	−1	1	0	0	0	1
$(4,2)$	9	3	1	3	0	0	0	−1	1	−1	0
$(5,1)$	5	3	1	−1	2	0	−1	1	−1	0	−1
(6)	1	1	1	1	1	1	1	1	1	1	1

$m_{\lambda\mu}$	(1^6)	$(2,1^4)$	$(2^2,1^2)$	(2^3)	$(3,1^3)$	$(3,2,1)$	(3^2)	$(4,1^2)$	$(4,2)$	$(5,1)$	(6)
$(1,1,1,1,1,1)$	1	5	9	5	10	16	5	10	9	5	1
$(2,1,1,1,1)$	0	1	3	2	4	8	3	6	6	4	1
$(2,2,1,1)$	0	0	1	1	1	4	2	3	4	3	1
$(2,2,2)$	0	0	0	1	0	2	1	1	3	2	1
$(3,1,1,1)$	0	0	0	0	1	2	1	3	3	3	1
$(3,2,1)$	0	0	0	0	0	1	1	1	2	2	1
$(3,3)$	0	0	0	0	0	0	1	0	1	1	1
$(4,1,1)$	0	0	0	0	0	0	0	1	1	2	1
$(4,2)$	0	0	0	0	0	0	0	0	1	1	1
$(5,1)$	0	0	0	0	0	0	0	0	0	1	1
(6)	0	0	0	0	0	0	0	0	0	0	1

A.3 Виртуальные подгруппы $\mathfrak{S}_n$ при $n \leq 6$

Мы приводим список всех виртуальных подгрупп $\mathfrak{S}_n$ при $n \leq 6$, вычисленный с помощью методов (a), (b) и (c) из разделов 4.2 и 4.3. Эти списки могут содержать лишние элементы, т.е. несущественные виртуальные подгруппы; автор намеренно оставил некоторые заведомо несущественные виртуальные подгруппы вроде виртуальной подгруппы #76, чтобы продемонстрировать существование таких виртуальных подгрупп. Теми же методами вычисляется список всех виртуальных подгрупп $\mathfrak{S}_n$ при $n \leq 11$. Этот список не приводится здесь только по причине своего большого размера — в него входит 11800 виртуальных подгрупп! Тем не менее, построенный автором список можно найти в электронном виде в сети Интернет по следующей ссылке: `http://acm.spbgu.ru/calcgal/`. Там же можно найти и программу для вычисления группы Галуа, основанную на нашем методе.

Приведем общие параметры полученных таблиц виртуальных подгрупп для $n \leq 11$. В следующей таблице V_n означает общее количество найденных виртуальных подгрупп симметрической группы $\mathfrak{S}_n$ (напомним, что среди них могут быть несущественные), а TV_n означает количество транзитивных виртуальных подгрупп. Кроме того, для сравнения приводится T_n — количество классов сопряженности транзитивных подгрупп $\mathfrak{S}_n$; эти данные взяты из работы [25]. Последний столбец означает время, за которое были вычислены таблицы для данного n на компьютере Pentium-IV.

n	V_n	TV_n	T_n	время
1	1	1	1	0 с
2	2	1	1	0 с
3	4	2	2	0 с
4	11	5	5	0 с
5	20	6	5	0 с
6	79	16	16	2 с
7	102	11	7	5 с
8	380	68	50	20 с
9	765	49	34	1 мин
10	3242	94	45	7 мин
11	7213	18	8	55 ч

Виртуальные подгруппы упорядочены по возрастанию n, а для одинаковых n — по возрастанию порядка. Виртуальные подгруппы $\mathfrak{S}_n$ одного и того же порядка упорядочиваются по лексикографическому убыванию вектора $y = (y_\mu)$.

Каждая виртуальная подгруппа H представлена таблицей следующего вида:

#33: порядок 12, индекс 10; − (30); свойства: `Ex`, `Pe`.

y_μ/d_μ	1/1	4/10	3/15	2/20	2/20	0/30	0/24
y'_μ	10	4	2	1	1	0	0
x_λ	0	0	0	0	1	1	1
разл. 1	⟨b⟩ $3(13)+2(16)$						
разл. 2	⟨c⟩ $3(8)+2(4)$						
подгр.	24, 28, 29, 30						

Сначала указывается порядковый номер виртуальной подгруппы в общем списке, ее порядок и индекс (напомним, что порядок и индекс виртуальной подгруппы корректно определены). Затем для положительных (т.е. содержащихся в знакопеременной группе $\mathfrak{A}_n \subset \mathfrak{S}_n$) виртуальных подгрупп записывается знак «+», а для отрицательных записывается «− (v)», где v — номер виртуальной подгруппы, соответствующей $H \cap \mathfrak{A}_n$. Первая строка завершается перечислением известных свойств данной виртуальной подгруппы, каждое из которых кодируется двумя буквами:

- `Ex` Виртуальная подгруппа существенна (т.е. соответствует какой-то настоящей подгруппе $\mathfrak{S}_n$).
- `Un` Виртуальная подгруппа соответствует не более одной настоящей подгруппе.
- `Cy` Виртуальная подгруппа соответствует циклической подгруппе (которая в этом случае однозначно определена).
- `Pe` Виртуальная подгруппа имеет вид $\mathfrak{S}_\lambda$ для некоторого разбиения $\lambda \in \mathrm{part}_n$ (см. 4.1.8).
- `Tr` Виртуальная подгруппа может соответствовать транзитивной подгруппе в $\mathfrak{S}_n$.
- `No` Виртуальная подгруппа соответствует нормальной подгруппе.

Следующие три строки содержат значения $y_\mu = |H \cap \mathcal{C}_\mu|$ (в виде y_μ/d_μ, где $d_\mu = |\mathcal{C}_\mu|$), $y'_\mu = \chi_{\mathfrak{S}_n/H}(\mathcal{C}_\mu)$ и $x_\lambda = (\chi_{\mathfrak{S}_n/H}, \chi_\lambda)$ (см. 3.5.9); при этом столбцы таблицы соответствуют разбиениям числа n, расположенным в лексикографическом порядке.

Далее следуют несколько строк, перечисляющие «разложения» H. По существу, каждая строка отражает один из путей построения данной подгруппы с помощью методов (a), (b) или (c). Для метода (a) запись выглядит так: ⟨a⟩ (v), где v — номер виртуальной подгруппы H' в $\mathfrak{S}_{n-1}$, из которой была получена H (см. описание метода (a) в 4.2). Для метода (b) запись устроена следующим образом: ⟨b⟩ $\nu_1(v_1) + \cdots + \nu_s(v_s)$, где ν — разбиение числа n, а v_j — номера соответствующих виртуальных подгрупп H_j в $\mathfrak{S}_{n-1}$ (см. описание метода (b) в 4.3). Наконец, для метода (c) запись устроена так: ⟨c⟩ $n_1(v_1)+n_2(v_2)$, где n_1 и n_2 — натуральные числа, такие, что $n_1+n_2 = n$, v_1 и v_2 — номера виртуальных подгрупп H_1 в $\mathfrak{S}_{n_1}$ и H_2 в $\mathfrak{S}_{n_2}$, таких, что $H = H_1 \times H_2$ (см. описание метода (c) в 4.2).

Последняя строка перечисляет все виртуальные подгруппы $H_j \neq H$, которые могут содержаться в H согласно τ-критерию 3.6.10. Поскольку этот список слишком велик, мы указываем только его

максимальные элементы; остальные подгруппы можно узнать, если просмотреть список подгрупп для каждой из H_j, для каждой из этих подгрупп снова просмотреть список подгрупп и т.д.

Виртуальные подгруппы $\mathfrak{S}_0$:

#1: порядок 1, индекс 1; +; свойства: Ex, Un, Cy, Pe, Tr, No.

y_μ/d_μ	1/1
y'_μ	1
x_λ	1

Виртуальные подгруппы $\mathfrak{S}_1$:

#2: порядок 1, индекс 1; +; свойства: Ex, Un, Cy, Pe, Tr, No.

y_μ/d_μ	1/1
y'_μ	1
x_λ	1

Виртуальные подгруппы $\mathfrak{S}_2$:

#3: порядок 1, индекс 2; +; свойства: Ex, Un, Cy, Pe, No.

y_μ/d_μ	1/1	0/1
y'_μ	2	0
x_λ	1	1

#4: порядок 2, индекс 1; − (3); свойства: Ex, Un, Cy, Pe, Tr, No.

y_μ/d_μ	1/1	1/1
y'_μ	1	1
x_λ	0	1
разл. 1	⟨b⟩ 2(2)	
подгр.	3	

Виртуальные подгруппы $\mathfrak{S}_3$:

#5: порядок 1, индекс 6; +; свойства: Ex, Un, Cy, Pe, No.

y_μ/d_μ	1/1	0/3	0/2
y'_μ	6	0	0
x_λ	1	2	1

#6: порядок 2, индекс 3; − (5); свойства: Ex, Un, Cy, Pe.

y_μ/d_μ	1/1	1/3	0/2
y'_μ	3	1	0
x_λ	0	1	1
разл. 1	⟨a⟩ 1(4)		
подгр.	5		

#7: порядок 3, индекс 2; +; свойства: Ex, Un, Cy, Tr, No.

y_μ/d_μ	1/1	0/3	2/2
y'_μ	2	0	2
x_λ	1	0	1
разл. 1	⟨b⟩ 3(3)		
подгр.	5		

#8: порядок 6, индекс 1; − (7); свойства: Ex, Un, Pe, Tr, No.

y_μ/d_μ	1/1	3/3	2/2
y'_μ	1	1	1
x_λ	0	0	1
разл. 1	⟨b⟩ 3(4)		
подгр.	6, 7		

Виртуальные подгруппы $\mathfrak{S}_4$:

#9: порядок 1, индекс 24; +; свойства: Ex, Un, Cy, Pe, No.

y_μ/d_μ	1/1	0/6	0/3	0/8	0/6
y'_μ	24	0	0	0	0
x_λ	1	3	2	3	1

#10: порядок 2, индекс 12; − (9); свойства: Ex, Un, Cy, Pe.

y_μ/d_μ	1/1	1/6	0/3	0/8	0/6
y'_μ	12	2	0	0	0
x_λ	0	1	1	2	1
разл. 1	⟨a⟩ 1(6)				
разл. 2	⟨c⟩ 2(4) + 2(3)				
подгр.	9				

#11: порядок 2, индекс 12; +; свойства: Ex, Un, Cy.

y_μ/d_μ	1/1	0/6	1/3	0/8	0/6
y'_μ	12	0	4	0	0
x_λ	1	1	2	1	1
разл. 1	⟨b⟩ 2(5) + 2(5)				
подгр.	9				

#12: порядок 3, индекс 8; +; свойства: Ex, Un, Cy.

y_μ/d_μ	1/1	0/6	0/3	2/8	0/6
y'_μ	8	0	0	2	0
x_λ	1	1	0	1	1
разл. 1	⟨a⟩ 1(7)				
подгр.	9				

#13: порядок 4, индекс 6; − (11); свойства: Ex, Pe.

y_μ/d_μ	1/1	2/6	1/3	0/8	0/6
y'_μ	6	2	2	0	0
x_λ	0	0	1	1	1
разл. 1	⟨b⟩ 2(6) + 2(6)				
разл. 2	⟨c⟩ 2(4) + 2(4)				
подгр.	10, 11				

#14: порядок 4, индекс 6; +; свойства: Ex, Un, Tr, No.

y_μ/d_μ	1/1	0/6	3/3	0/8	0/6
y'_μ	6	0	6	0	0
x_λ	1	0	2	0	1
разл. 1	⟨b⟩ 4(5)				
подгр.	11				

#15: порядок 4, индекс 6; − (11); свойства: Ex, Un, Cy, Tr.

y_μ/d_μ	1/1	0/6	1/3	0/8	2/6
y'_μ	6	0	2	0	2
x_λ	0	1	1	0	1
разл. 1	⟨b⟩ 4(5)				
подгр.	11				

#16: порядок 6, индекс 4; − (12); свойства: Ex, Pe.

y_μ/d_μ	1/1	3/6	0/3	2/8	0/6
y'_μ	4	2	0	1	0
x_λ	0	0	0	1	1
разл. 1	⟨a⟩ 1(8)				
подгр.	10, 12				

#17: порядок 8, индекс 3; − (14); свойства: Ex, Un, Tr.

y_μ/d_μ	1/1	2/6	3/3	0/8	2/6
y'_μ	3	1	3	0	1
x_λ	0	0	1	0	1
разл. 1	⟨b⟩ 4(6)				
подгр.	13, 14, 15				

#18: порядок 12, индекс 2; +; свойства: Ex, Un, Tr, No.

y_μ/d_μ	1/1	0/6	3/3	8/8	0/6
y'_μ	2	0	2	2	0
x_λ	1	0	0	0	1
разл. 1	⟨b⟩ 4(7)				
подгр.	12, 14				

#19: порядок 24, индекс 1; − (18); свойства: Ex, Un, Pe, Tr, No.

y_μ/d_μ	1/1	6/6	3/3	8/8	6/6
y'_μ	1	1	1	1	1
x_λ	0	0	0	0	1
разл. 1	⟨b⟩ 4(8)				
подгр.	16, 17, 18				

Виртуальные подгруппы $\mathfrak{S}_5$:

#20: порядок 1, индекс 120; +; свойства: Ex, Un, Cy, Pe, No.

y_μ/d_μ	1/1	0/10	0/15	0/20	0/20	0/30	0/24
y'_μ	120	0	0	0	0	0	0
x_λ	1	4	5	6	5	4	1

#21: порядок 2, индекс 60; − (20); свойства: Ex, Un, Cy, Pe.

y_μ/d_μ	1/1	1/10	0/15	0/20	0/20	0/30	0/24
y'_μ	60	6	0	0	0	0	0
x_λ	0	1	2	3	3	3	1
разл. 1	⟨a⟩ 1(10)						
подгр.	20						

#22: порядок 2, индекс 60; +; свойства: Ex, Un, Cy.

y_μ/d_μ	1/1	0/10	1/15	0/20	0/20	0/30	0/24
y'_μ	60	0	4	0	0	0	0
x_λ	1	2	3	2	3	2	1
разл. 1	⟨a⟩ 1(11)						
подгр.	20						

#23: порядок 3, индекс 40; +; свойства: Ex, Un, Cy.

y_μ/d_μ	1/1	0/10	0/15	2/20	0/20	0/30	0/24
y'_μ	40	0	0	4	0	0	0
x_λ	1	2	1	2	1	2	1
разл. 1	⟨a⟩ 1(12)						
разл. 2	⟨c⟩ 3(7) + 2(3)						
подгр.	20						

#24: порядок 4, индекс 30; − (22); свойства: Ex, Pe.

y_μ/d_μ	1/1	2/10	1/15	0/20	0/20	0/30	0/24
y'_μ	30	6	2	0	0	0	0
x_λ	0	0	1	1	2	2	1
разл. 1	⟨a⟩ 1(13)						
подгр.	21, 22						

#25: порядок 4, индекс 30; +; свойства: Ex.

y_μ/d_μ	1/1	0/10	3/15	0/20	0/20	0/30	0/24
y'_μ	30	0	6	0	0	0	0
x_λ	1	1	2	0	2	1	1
разл. 1	⟨a⟩ 1(14)						
подгр.	22						

#26: порядок 4, индекс 30; − (22); свойства: Ex, Un, Cy.

y_μ/d_μ	1/1	0/10	1/15	0/20	0/20	2/30	0/24
y'_μ	30	0	2	0	0	2	0
x_λ	0	1	2	1	1	1	1
разл. 1	⟨a⟩ 1(15)						
подгр.	22						

#27: порядок 5, индекс 24; +; свойства: Ex, Un, Cy, Tr.

y_μ/d_μ	1/1	0/10	0/15	0/20	0/20	0/30	4/24
y'_μ	24	0	0	0	0	0	4
x_λ	1	0	1	2	1	0	1
разл. 1	⟨b⟩ 5(9)						
подгр.	20						

#28: порядок 6, индекс 20; − (23); свойства: Ex, Pe.

y_μ/d_μ	1/1	3/10	0/15	2/20	0/20	0/30	0/24
y'_μ	20	6	0	2	0	0	0
x_λ	0	0	0	1	1	2	1
разл. 1	⟨a⟩ 1(16)						
разл. 2	⟨c⟩ 3(8) + 2(3)						
подгр.	21, 23						

#29: порядок 6, индекс 20; − (23); свойства: Ex, Un, Cy.

y_μ/d_μ	1/1	1/10	0/15	2/20	2/20	0/30	0/24
y'_μ	20	2	0	2	2	0	0
x_λ	0	1	0	1	1	1	1
разл. 1	⟨b⟩ 3(10) + 2(12)						
разл. 2	⟨c⟩ 3(7) + 2(4)						
подгр.	21, 23						

#30: порядок 6, индекс 20; +; свойства: Ex.

y_μ/d_μ	1/1	0/10	3/15	2/20	0/20	0/30	0/24
y'_μ	20	0	4	2	0	0	0
x_λ	1	1	1	0	1	1	1
разл. 1	⟨b⟩ 3(11) + 2(12)						
подгр.	22, 23						

#31: порядок 8, индекс 15; − (25); свойства: Ex, Un.

y_μ/d_μ	1/1	2/10	3/15	0/20	0/20	2/30	0/24
y'_μ	15	3	3	0	0	1	0
x_λ	0	0	1	0	1	1	1
разл. 1	⟨a⟩ 1(17)						
подгр.	24, 25, 26						

#32: порядок 10, индекс 12; +; свойства: Tr.

y_μ/d_μ	1/1	0/10	5/15	0/20	0/20	0/30	4/24
y'_μ	12	0	4	0	0	0	2
x_λ	1	0	1	0	1	0	1
разл. 1	⟨b⟩ 5(11)						
подгр.	22, 27						

#33: порядок 12, индекс 10; − (30); свойства: Ex, Pe.

y_μ/d_μ	1/1	4/10	3/15	2/20	2/20	0/30	0/24
y'_μ	10	4	2	1	1	0	0
x_λ	0	0	0	0	1	1	1
разл. 1	⟨b⟩ 3(13) + 2(16)						
разл. 2	⟨c⟩ 3(8) + 2(4)						
подгр.	24, 28, 29, 30						

#34: порядок 12, индекс 10; +; свойства: Ex.

y_μ/d_μ	1/1	0/10	3/15	8/20	0/20	0/30	0/24
y'_μ	10	0	2	4	0	0	0
x_λ	1	1	0	0	0	1	1
разл. 1	⟨a⟩ 1(18)						
подгр.	23, 25						

#35: порядок 15, индекс 8; +; свойства: Tr.

y_μ/d_μ	1/1	0/10	0/15	5/20	0/20	0/30	9/24
y'_μ	8	0	0	2	0	0	3
x_λ	1	0	0	1	0	0	1
разл. 1	⟨b⟩ 5(12)						
подгр.	23, 27						

#36: порядок 20, индекс 6; − (32); свойства: Tr.

y_μ/d_μ	1/1	0/10	5/15	0/20	0/20	10/30	4/24
y'_μ	6	0	2	0	0	2	1
x_λ	0	0	1	0	0	0	1
разл. 1	⟨b⟩ 5(15)						
подгр.	26, 32						

#37: порядок 24, индекс 5; − (34); свойства: Ex, Pe.

y_μ/d_μ	1/1	6/10	3/15	8/20	0/20	6/30	0/24
y'_μ	5	3	1	2	0	1	0
x_λ	0	0	0	0	0	1	1
разл. 1	⟨a⟩ 1(19)						
подгр.	28, 30, 31, 34						

#38: порядок 60, индекс 2; +; свойства: Ex, Un, Tr, No.

y_μ/d_μ	1/1	0/10	15/15	20/20	0/20	0/30	24/24
y'_μ	2	0	2	2	0	0	2
x_λ	1	0	0	0	0	0	1
разл. 1	⟨b⟩ 5(18)						
подгр.	30, 32, 34						

#39: порядок 120, индекс 1; − (38); свойства: Ex, Un, Pe, Tr, No.

y_μ/d_μ	1/1	10/10	15/15	20/20	20/20	30/30	24/24
y'_μ	1	1	1	1	1	1	1
x_λ	0	0	0	0	0	0	1
разл. 1	⟨b⟩ 5(19)						
подгр.	33, 35, 36, 37, 38						

Виртуальные подгруппы $\mathfrak{S}_6$:

#40: порядок 1, индекс 720; +; свойства: Ex, Un, Cy, Pe, No.

y_μ/d_μ	1/1	0/15	0/45	0/15	0/40	0/120	0/40	0/90	0/90	0/144	0/120
y'_μ	720	0	0	0	0	0	0	0	0	0	0
x_λ	1	5	9	5	10	16	5	10	9	5	1

#41: порядок 2, индекс 360; − (40); свойства: Ex, Un, Cy, Pe.

y_μ/d_μ	1/1	1/15	0/45	0/15	0/40	0/120	0/40	0/90	0/90	0/144	0/120
y'_μ	360	24	0	0	0	0	0	0	0	0	0
x_λ	0	1	3	2	4	8	3	6	6	4	1
разл. 1	⟨a⟩ 1(21)										
подгр.	40										

#42: порядок 2, индекс 360; +; свойства: Ex, Un, Cy.

y_μ/d_μ	1/1	0/15	1/45	0/15	0/40	0/120	0/40	0/90	0/90	0/144	0/120
y'_μ	360	0	8	0	0	0	0	0	0	0	0
x_λ	1	3	5	3	4	8	3	4	5	3	1
разл. 1	⟨a⟩ 1(22)										
подгр.	40										

#43: порядок 2, индекс 360; − (40); свойства: Ex, Un, Cy.

y_μ/d_μ	1/1	0/15	0/45	1/15	0/40	0/120	0/40	0/90	0/90	0/144	0/120
y'_μ	360	0	0	24	0	0	0	0	0	0	0
x_λ	0	3	3	4	6	8	1	4	6	2	1
разл. 1	⟨b⟩ 2(20) + 2(20) + 2(20)										
подгр.	40										

#44: порядок 3, индекс 240; +; свойства: Ex, Un, Cy.

y_μ/d_μ	1/1	0/15	0/45	0/15	2/40	0/120	0/40	0/90	0/90	0/144	0/120
y'_μ	240	0	0	0	12	0	0	0	0	0	0
x_λ	1	3	3	1	4	4	1	4	3	3	1
разл. 1	⟨a⟩ 1(23)										
разл. 2	⟨c⟩ 3(7) + 3(5)										
подгр.	40										

#45: порядок 3, индекс 240; +; свойства: Ex, Un, Cy.

y_μ/d_μ	1/1	0/15	0/45	0/15	0/40	0/120	2/40	0/90	0/90	0/144	0/120
y'_μ	240	0	0	0	0	0	12	0	0	0	0
x_λ	1	1	3	3	4	4	3	4	3	1	1
разл. 1	⟨b⟩ 3(20) + 3(20)										
подгр.	40										

#46: порядок 4, индекс 180; − (42); свойства: Ex, Pe.

y_μ/d_μ	1/1	2/15	1/45	0/15	0/40	0/120	0/40	0/90	0/90	0/144	0/120
y'_μ	180	24	4	0	0	0	0	0	0	0	0
x_λ	0	0	1	1	1	4	2	3	4	3	1
разл. 1	⟨a⟩ 1(24)										
подгр.	41, 42										

#47: порядок 4, индекс 180; − (42).

y_μ/d_μ	1/1	1/15	1/45	1/15	0/40	0/120	0/40	0/90	0/90	0/144	0/120
y'_μ	180	12	4	12	0	0	0	0	0	0	0
x_λ	0	1	1	2	2	4	1	2	4	2	1
разл. 1	⟨b⟩ 2(21) + 2(21) + 2(22)										
подгр.	41, 42, 43										

#48: порядок 4, индекс 180; +; свойства: Ex.

y_μ/d_μ	1/1	0/15	3/45	0/15	0/40	0/120	0/40	0/90	0/90	0/144	0/120
y'_μ	180	0	12	0	0	0	0	0	0	0	0
x_λ	1	2	3	2	1	4	2	1	3	2	1
разл. 1	⟨a⟩ 1(25)										
разл. 2	⟨b⟩ 2(22) + 2(22) + 2(22)										
разл. 3	⟨c⟩ 4(14) + 2(3)										
подгр.	42										

#49: порядок 4, индекс 180; − (42).

y_μ/d_μ	1/1	0/15	1/45	2/15	0/40	0/120	0/40	0/90	0/90	0/144	0/120
y'_μ	180	0	4	24	0	0	0	0	0	0	0
x_λ	0	2	1	3	3	4	0	1	4	1	1
разл. 1	$\langle$b$\rangle$ $4(20)+2(22)$										
подгр.	42, 43										

#50: порядок 4, индекс 180; − (42); свойства: `Ex`, `Un`, `Cy`.

y_μ/d_μ	1/1	0/15	1/45	0/15	0/40	0/120	0/40	2/90	0/90	0/144	0/120
y'_μ	180	0	4	0	0	0	0	4	0	0	0
x_λ	0	1	3	2	2	4	1	2	2	2	1
разл. 1	$\langle$a$\rangle$ 1(26)										
разл. 2	$\langle$c$\rangle$ $4(15)+2(3)$										
подгр.	42										

#51: порядок 4, индекс 180; +; свойства: `Ex`, `Un`, `Cy`.

y_μ/d_μ	1/1	0/15	1/45	0/15	0/40	0/120	0/40	0/90	2/90	0/144	0/120
y'_μ	180	0	4	0	0	0	0	0	4	0	0
x_λ	1	1	3	1	2	4	1	2	3	1	1
разл. 1	$\langle$b$\rangle$ $4(20)+2(22)$										
подгр.	42										

#52: порядок 5, индекс 144; +; свойства: `Ex`, `Un`, `Cy`.

y_μ/d_μ	1/1	0/15	0/45	0/15	0/40	0/120	0/40	0/90	0/90	4/144	0/120
y'_μ	144	0	0	0	0	0	0	0	0	4	0
x_λ	1	1	1	1	2	4	1	2	1	1	1
разл. 1	$\langle$a$\rangle$ 1(27)										
подгр.	40										

#53: порядок 6, индекс 120; − (44); свойства: `Ex`, `Pe`.

y_μ/d_μ	1/1	3/15	0/45	0/15	2/40	0/120	0/40	0/90	0/90	0/144	0/120
y'_μ	120	24	0	0	6	0	0	0	0	0	0
x_λ	0	0	0	0	1	2	1	3	3	3	1
разл. 1	$\langle$a$\rangle$ 1(28)										
разл. 2	$\langle$c$\rangle$ $3(8)+3(5)$										
подгр.	41, 44										

#54: порядок 6, индекс 120; − (44); свойства: `Ex`, `Un`, `Cy`.

y_μ/d_μ	1/1	1/15	0/45	0/15	2/40	2/120	0/40	0/90	0/90	0/144	0/120
y'_μ	120	8	0	0	6	2	0	0	0	0	0
x_λ	0	1	1	0	2	2	1	2	2	2	1
разл. 1	$\langle$a$\rangle$ 1(29)										
разл. 2	$\langle$c$\rangle$ $3(7)+3(6)$										
подгр.	41, 44										

#55: порядок 6, индекс 120; +; свойства: `Ex`.

y_μ/d_μ	1/1	0/15	3/45	0/15	2/40	0/120	0/40	0/90	0/90	0/144	0/120
y'_μ	120	0	8	0	6	0	0	0	0	0	0
x_λ	1	2	2	1	1	2	1	1	2	2	1
разл. 1	$\langle$a$\rangle$ 1(30)										
подгр.	42, 44										

#56: порядок 6, индекс 120; +.

y_μ/d_μ	1/1	0/15	3/45	0/15	0/40	0/120	2/40	0/90	0/90	0/144	0/120
y'_μ	120	0	8	0	0	0	6	0	0	0	0
x_λ	1	1	2	2	1	2	2	1	2	1	1
разл. 1	$\langle$b$\rangle$ $3(22)+3(22)$										
подгр.	42, 45										

#57: порядок 6, индекс 120; − (45); свойства: `Tr`.

y_μ/d_μ	1/1	0/15	0/45	3/15	0/40	0/120	2/40	0/90	0/90	0/144	0/120
y'_μ	120	0	0	24	0	0	6	0	0	0	0
x_λ	0	1	0	3	3	2	0	1	3	0	1
разл. 1	$\langle$b$\rangle$ 6(20)										
подгр.	43, 45										

#58: порядок 6, индекс 120; − (45); свойства: `Ex`, `Un`, `Cy`, `Tr`.

y_μ/d_μ	1/1	0/15	0/45	1/15	0/40	0/120	2/40	0/90	0/90	0/144	2/120
y'_μ	120	0	0	8	0	0	6	0	0	0	2
x_λ	0	1	1	2	2	2	1	2	2	0	1
разл. 1	$\langle$b$\rangle$ 6(20)										
подгр.	43, 45										

#59: порядок 8, индекс 90; − (48).

y_μ/d_μ	1/1	3/15	3/45	1/15	0/40	0/120	0/40	0/90	0/90	0/144	0/120
y'_μ	90	18	6	6	0	0	0	0	0	0	0
x_λ	0	0	0	1	0	2	1	1	3	2	1
разл. 1	$\langle$b$\rangle$ 2(24) + 2(24) + 2(24)										
подгр.	46, 47, 48										

#60: порядок 8, индекс 90; − (48); свойства: `Ex`.

y_μ/d_μ	1/1	2/15	3/45	0/15	0/40	0/120	0/40	2/90	0/90	0/144	0/120
y'_μ	90	12	6	0	0	0	0	2	0	0	0
x_λ	0	0	1	1	0	2	1	1	2	2	1
разл. 1	$\langle$a$\rangle$ 1(31)										
разл. 2	$\langle$b$\rangle$ 2(24) + 2(24) + 2(26)										
разл. 3	$\langle$c$\rangle$ 4(17) + 2(3)										
подгр.	46, 48, 50										

#61: порядок 8, индекс 90; − (51).

y_μ/d_μ	1/1	2/15	1/45	2/15	0/40	0/120	0/40	0/90	2/90	0/144	0/120
y'_μ	90	12	2	12	0	0	0	0	2	0	0
x_λ	0	0	0	1	1	2	0	1	3	1	1
разл. 1	$\langle$b$\rangle$ 4(21) + 2(24)										
подгр.	46, 47, 49, 51										

#62: порядок 8, индекс 90; − (48); свойства: `Ex`.

y_μ/d_μ	1/1	1/15	3/45	3/15	0/40	0/120	0/40	0/90	0/90	0/144	0/120
y'_μ	90	6	6	18	0	0	0	0	0	0	0
x_λ	0	1	0	2	1	2	0	0	3	1	1
разл. 1	$\langle$b$\rangle$ 4(21) + 2(25)										
разл. 2	$\langle$b$\rangle$ 4(22) + 2(24)										
разл. 3	$\langle$c$\rangle$ 4(14) + 2(4)										
подгр.	47, 48, 49										

#63: порядок 8, индекс 90; − (51); свойства: `Ex`.

y_μ/d_μ	1/1	1/15	1/45	1/15	0/40	0/120	0/40	2/90	2/90	0/144	0/120
y'_μ	90	6	2	6	0	0	0	2	2	0	0
x_λ	0	0	1	1	1	2	0	1	2	1	1
разл. 1	$\langle$b$\rangle$ 4(21) + 2(26)										
разл. 2	$\langle$c$\rangle$ 4(15) + 2(4)										
подгр.	47, 50, 51										

#64: порядок 8, индекс 90; +; свойства: `Ex`.

y_μ/d_μ	1/1	0/15	5/45	0/15	0/40	0/120	0/40	0/90	2/90	0/144	0/120
y'_μ	90	0	10	0	0	0	0	0	2	0	0
x_λ	1	1	2	1	0	2	1	0	2	1	1
разл. 1	$\langle$b$\rangle$ 4(22) + 2(25)										
подгр.	48, 51										

#65: порядок 8, индекс 90; − (48).

y_μ/d_μ	1/1	0/15	3/45	2/15	0/40	0/120	0/40	2/90	0/90	0/144	0/120
y'_μ	90	0	6	12	0	0	0	2	0	0	0
x_λ	0	1	1	2	1	2	0	0	2	1	1
разл. 1	⟨b⟩ $4(22)+2(26)$										
подгр.	48, 49, 50										

#66: порядок 9, индекс 80; +; свойства: `Ex`, `Un`.

y_μ/d_μ	1/1	0/15	0/45	0/15	4/40	0/120	4/40	0/90	0/90	0/144	0/120
y'_μ	80	0	0	0	8	0	8	0	0	0	0
x_λ	1	1	1	1	2	0	1	2	1	1	1
разл. 1	⟨b⟩ $3(23)+3(23)$										
разл. 2	⟨c⟩ $3(7)+3(7)$										
подгр.	44, 45										

#67: порядок 10, индекс 72; +.

y_μ/d_μ	1/1	0/15	5/45	0/15	0/40	0/120	0/40	0/90	0/90	4/144	0/120
y'_μ	72	0	8	0	0	0	0	0	0	2	0
x_λ	1	1	1	1	0	2	1	0	1	1	1
разл. 1	⟨a⟩ 1(32)										
подгр.	42, 52										

#68: порядок 12, индекс 60; − (55); свойства: `Ex`, `Pe`.

y_μ/d_μ	1/1	4/15	3/45	0/15	2/40	2/120	0/40	0/90	0/90	0/144	0/120
y'_μ	60	16	4	0	3	1	0	0	0	0	0
x_λ	0	0	0	0	0	1	1	1	2	2	1
разл. 1	⟨a⟩ 1(33)										
разл. 2	⟨c⟩ $3(8)+3(6)$										
подгр.	46, 53, 54, 55										

#69: порядок 12, индекс 60; − (56).

y_μ/d_μ	1/1	3/15	3/45	1/15	0/40	0/120	2/40	0/90	0/90	0/144	2/120
y'_μ	60	12	4	4	0	0	3	0	0	0	1
x_λ	0	0	0	1	0	1	1	1	2	1	1
разл. 1	⟨b⟩ $3(24)+3(24)$										
подгр.	47, 56										

#70: порядок 12, индекс 60; − (56); свойства: `Tr`.

y_μ/d_μ	1/1	0/15	3/45	4/15	0/40	0/120	2/40	0/90	0/90	0/144	2/120
y'_μ	60	0	4	16	0	0	3	0	0	0	1
x_λ	0	1	0	2	1	1	0	0	2	0	1
разл. 1	⟨b⟩ 6(22)										
подгр.	49, 56, 57, 58										

#71: порядок 12, индекс 60; +; свойства: `Ex`.

y_μ/d_μ	1/1	0/15	3/45	0/15	8/40	0/120	0/40	0/90	0/90	0/144	0/120
y'_μ	60	0	4	0	12	0	0	0	0	0	0
x_λ	1	2	1	0	1	0	0	1	1	2	1
разл. 1	⟨a⟩ 1(34)										
разл. 2	⟨c⟩ $4(18)+2(3)$										
подгр.	48, 55										

#72: порядок 12, индекс 60; +.

y_μ/d_μ	1/1	0/15	3/45	0/15	4/40	0/120	4/40	0/90	0/90	0/144	0/120
y'_μ	60	0	4	0	6	0	6	0	0	0	0
x_λ	1	1	1	1	1	0	1	1	1	1	1
разл. 1	⟨b⟩ $4(23)+2(30)$										
подгр.	48										

#73: порядок 12, индекс 60; +; свойства: `Tr`.

y_μ/d_μ	1/1	0/15	3/45	0/15	0/40	0/120	8/40	0/90	0/90	0/144	0/120
y'_μ	60	0	4	0	0	0	12	0	0	0	0
x_λ	1	0	1	2	1	0	2	1	1	0	1
разл. 1	⟨b⟩ 6(22)										
подгр.	48, 56										

#74: порядок 15, индекс 48; +.

y_μ/d_μ	1/1	0/15	0/45	0/15	5/40	0/120	0/40	0/90	0/90	9/144	0/120
y'_μ	48	0	0	0	6	0	0	0	0	3	0
x_λ	1	1	0	0	1	1	0	1	0	1	1
разл. 1	⟨a⟩ 1(35)										
подгр.	44, 52										

#75: порядок 16, индекс 45; − (64); свойства: `Ex`, `Un`.

y_μ/d_μ	1/1	3/15	5/45	3/15	0/40	0/120	0/40	2/90	2/90	0/144	0/120
y'_μ	45	9	5	9	0	0	0	1	1	0	0
x_λ	0	0	0	1	0	1	0	0	2	1	1
разл. 1	⟨b⟩ 4(24) + 2(31)										
разл. 2	⟨c⟩ 4(17) + 2(4)										
подгр.	59, 60, 61, 62, 63, 64, 65										

#76: порядок 16, индекс 45; − (64); свойства: `Un`.

y_μ/d_μ	1/1	1/15	5/45	1/15	0/40	0/120	0/40	6/90	2/90	0/144	0/120
y'_μ	45	3	5	3	0	0	0	3	1	0	0
x_λ	0	0	1	1	0	1	0	0	1	1	1
разл. 1	⟨b⟩ 4(26) + 2(31)										
подгр.	47, 50, 64										

#77: порядок 18, индекс 40; − (66); свойства: `Ex`.

y_μ/d_μ	1/1	3/15	0/45	0/15	4/40	6/120	4/40	0/90	0/90	0/144	0/120
y'_μ	40	8	0	0	4	2	4	0	0	0	0
x_λ	0	0	0	0	1	0	1	1	1	1	1
разл. 1	⟨b⟩ 3(28) + 3(29)										
разл. 2	⟨c⟩ 3(8) + 3(7)										
подгр.	53, 54, 66										

#78: порядок 18, индекс 40; +; свойства: `Ex`.

y_μ/d_μ	1/1	0/15	9/45	0/15	4/40	0/120	4/40	0/90	0/90	0/144	0/120
y'_μ	40	0	8	0	4	0	4	0	0	0	0
x_λ	1	1	1	1	0	0	1	0	1	1	1
разл. 1	⟨b⟩ 3(30) + 3(30)										
подгр.	55, 56, 66										

#79: порядок 18, индекс 40; − (66); свойства: `Tr`.

y_μ/d_μ	1/1	0/15	0/45	3/15	4/40	0/120	4/40	0/90	0/90	0/144	6/120
y'_μ	40	0	0	8	4	0	4	0	0	0	2
x_λ	0	1	0	1	1	0	0	1	1	0	1
разл. 1	⟨b⟩ 6(23)										
подгр.	57, 58, 66										

#80: порядок 20, индекс 36; − (67).

y_μ/d_μ	1/1	0/15	5/45	0/15	0/40	0/120	0/40	10/90	0/90	4/144	0/120
y'_μ	36	0	4	0	0	0	0	4	0	1	0
x_λ	0	0	1	1	0	1	0	0	0	1	1
разл. 1	⟨a⟩ 1(36)										
подгр.	50, 67										

#81: порядок 24, индекс 30; − (71); свойства: Ex, Pe.

y_μ/d_μ	1/1	6/15	3/45	0/15	8/40	0/120	0/40	6/90	0/90	0/144	0/120
y'_μ	30	12	2	0	6	0	0	2	0	0	0
x_λ	0	0	0	0	0	0	0	1	1	2	1
разл. 1	⟨a⟩ 1(37)										
разл. 2	⟨c⟩ 4(19) + 2(3)										
подгр.	53, 60, 71										

#82: порядок 24, индекс 30; − (73); свойства: Tr.

y_μ/d_μ	1/1	3/15	3/45	1/15	0/40	0/120	8/40	0/90	0/90	0/144	8/120
y'_μ	30	6	2	2	0	0	6	0	0	0	2
x_λ	0	0	0	1	0	0	1	1	1	0	1
разл. 1	⟨b⟩ 6(24)										
подгр.	58, 59, 73										

#83: порядок 24, индекс 30; − (71); свойства: Ex.

y_μ/d_μ	1/1	1/15	3/45	3/15	8/40	8/120	0/40	0/90	0/90	0/144	0/120
y'_μ	30	2	2	6	6	2	0	0	0	0	0
x_λ	0	1	0	0	1	0	0	0	1	1	1
разл. 1	⟨b⟩ 4(29) + 2(34)										
разл. 2	⟨c⟩ 4(18) + 2(4)										
подгр.	54, 62, 71										

#84: порядок 24, индекс 30; +; свойства: Ex.

y_μ/d_μ	1/1	0/15	9/45	0/15	8/40	0/120	0/40	0/90	6/90	0/144	0/120
y'_μ	30	0	6	0	6	0	0	0	2	0	0
x_λ	1	1	1	0	0	0	0	0	1	1	1
разл. 1	⟨b⟩ 4(30) + 2(34)										
подгр.	64, 71										

#85: порядок 24, индекс 30; +; свойства: Tr.

y_μ/d_μ	1/1	0/15	9/45	0/15	0/40	0/120	8/40	0/90	6/90	0/144	0/120
y'_μ	30	0	6	0	0	0	6	0	2	0	0
x_λ	1	0	1	1	0	0	1	0	1	0	1
разл. 1	⟨b⟩ 6(25)										
подгр.	64, 73										

#86: порядок 24, индекс 30; − (73); свойства: Tr.

y_μ/d_μ	1/1	0/15	3/45	6/15	0/40	0/120	8/40	6/90	0/90	0/144	0/120
y'_μ	30	0	2	12	0	0	6	2	0	0	0
x_λ	0	0	0	2	1	0	0	0	1	0	1
разл. 1	⟨b⟩ 6(26)										
подгр.	57, 65, 73										

#87: порядок 36, индекс 20; − (78); свойства: Ex, Pe.

y_μ/d_μ	1/1	6/15	9/45	0/15	4/40	12/120	4/40	0/90	0/90	0/144	0/120
y'_μ	20	8	4	0	2	2	2	0	0	0	0
x_λ	0	0	0	0	0	0	1	0	1	1	1
разл. 1	⟨b⟩ 3(33) + 3(33)										
разл. 2	⟨c⟩ 3(8) + 3(8)										
подгр.	68, 77, 78										

#88: порядок 36, индекс 20; − (78); свойства: Tr.

y_μ/d_μ	1/1	0/15	9/45	6/15	4/40	0/120	4/40	0/90	0/90	0/144	12/120
y'_μ	20	0	4	8	2	0	2	0	0	0	2
x_λ	0	1	0	1	0	0	0	0	1	0	1
разл. 1	⟨b⟩ 6(30)										
подгр.	70, 78, 79										

#89: порядок 36, индекс 20; +; свойства: Tr.

y_μ/d_μ	1/1	0/15	9/45	0/15	4/40	0/120	4/40	0/90	18/90	0/144	0/120
y'_μ	20	0	4	0	2	0	2	0	4	0	0
x_λ	1	0	1	0	0	0	0	0	1	0	1
разл. 1	⟨b⟩ 6(30)										
подгр.	51, 78										

#90: порядок 48, индекс 15; − (84); свойства: Ex, Pe.

y_μ/d_μ	1/1	7/15	9/45	3/15	8/40	8/120	0/40	6/90	6/90	0/144	0/120
y'_μ	15	7	3	3	3	1	0	1	1	0	0
x_λ	0	0	0	0	0	0	0	0	1	1	1
разл. 1	⟨b⟩ $4(33)+2(37)$										
разл. 2	⟨c⟩ $4(19)+2(4)$										
подгр.	68, 75, 76, 81, 83, 84										

#91: порядок 48, индекс 15; − (85); свойства: Tr.

y_μ/d_μ	1/1	3/15	9/45	7/15	0/40	0/120	8/40	6/90	6/90	0/144	8/120
y'_μ	15	3	3	7	0	0	3	1	1	0	1
x_λ	0	0	0	1	0	0	0	0	1	0	1
разл. 1	⟨b⟩ 6(31)										
подгр.	69, 70, 75, 76, 82, 85, 86										

#92: порядок 60, индекс 12; +; свойства: Ex.

y_μ/d_μ	1/1	0/15	15/45	0/15	20/40	0/120	0/40	0/90	0/90	24/144	0/120
y'_μ	12	0	4	0	6	0	0	0	0	2	0
x_λ	1	1	0	0	0	0	0	0	0	1	1
разл. 1	⟨a⟩ 1(38)										
подгр.	67, 71										

#93: порядок 60, индекс 12; +; свойства: Tr.

y_μ/d_μ	1/1	0/15	15/45	0/15	0/40	0/120	20/40	0/90	0/90	24/144	0/120
y'_μ	12	0	4	0	0	0	6	0	0	2	0
x_λ	1	0	0	1	0	0	1	0	0	0	1
разл. 1	⟨b⟩ 6(32)										
подгр.	67, 73										

#94: порядок 72, индекс 10; − (89); свойства: Tr.

y_μ/d_μ	1/1	6/15	9/45	6/15	4/40	12/120	4/40	0/90	18/90	0/144	12/120
y'_μ	10	4	2	4	1	1	1	0	2	0	1
x_λ	0	0	0	0	0	0	0	0	1	0	1
разл. 1	⟨b⟩ 6(33)										
подгр.	61, 69, 72, 87, 88, 89										

#95: порядок 120, индекс 6; − (92); свойства: Ex, Pe.

y_μ/d_μ	1/1	10/15	15/45	0/15	20/40	20/120	0/40	30/90	0/90	24/144	0/120
y'_μ	6	4	2	0	3	1	0	2	0	1	0
x_λ	0	0	0	0	0	0	0	0	0	1	1
разл. 1	⟨a⟩ 1(39)										
подгр.	68, 74, 80, 81, 92										

#96: порядок 120, индекс 6; − (93); свойства: Tr.

y_μ/d_μ	1/1	0/15	15/45	10/15	0/40	0/120	20/40	30/90	0/90	24/144	20/120
y'_μ	6	0	2	4	0	0	3	2	0	1	1
x_λ	0	0	0	1	0	0	0	0	0	0	1
разл. 1	⟨b⟩ 6(36)										
подгр.	70, 80, 86, 93										

#97: порядок 360, индекс 2; +; свойства: Ex, Un, Tr, No.

y_μ/d_μ	1/1	0/15	45/45	0/15	40/40	0/120	40/40	0/90	90/90	144/144	0/120
y'_μ	2	0	2	0	2	0	2	0	2	2	0
x_λ	1	0	0	0	0	0	0	0	0	0	1
разл. 1	⟨b⟩ 6(38)										
подгр.	72, 74, 84, 85, 89, 92, 93										

#98: порядок 720, индекс 1; − (97); свойства: Ex, Un, Pe, Tr, No.

y_μ/d_μ	1/1	15/15	45/45	15/15	40/40	120/120	40/40	90/90	90/90	144/144	120/120
y'_μ	1	1	1	1	1	1	1	1	1	1	1
x_λ	0	0	0	0	0	0	0	0	0	0	1
разл. 1	⟨b⟩ 6(39)										
подгр.	90, 91, 94, 95, 96, 97										