Записки научных
семинаров ПОМИ
Том 321, 2005 г.

**Н. В. Дуров**

# ВЫЧИСЛЕНИЕ ГРУППЫ ГАЛУА МНОГОЧЛЕНА С РАЦИОНАЛЬНЫМИ КОЭФФИЦИЕНТАМИ. II

Настоящая публикация завершает статью [10].

## 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 [2]. 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 $\lambda_k$ равна некоторому целому числу $n$, мы будем говорить, что $\lambda$ является разбиением (на слагаемые) числа $n$. Если*

---

Работа выполнена при поддержке Российского Фонда Фундаментальных исследований, грант 04-01-00082a.

*$k$ – наибольший индекс, для которого $\lambda_k > 0$, мы будем записывать разбиение $\lambda$ также в виде $(\lambda_1, \lambda_2, \ldots, \lambda_k)$ или в виде $\lambda_1+\lambda_2+\cdots+\lambda_k$; тот факт, что $\lambda$ является разбиением числа $n$, мы будем записывать также в виде $n = \lambda_1+\lambda_2+\cdots+\lambda_k$. Множество всех разбиений мы обозначим через* $\mathrm{part}$, *множество разбиений целого неотрицательного числа $n$ мы обозначим через* $\mathrm{part}_n$, *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 $\sigma$ 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 $\lambda$ 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 $\lambda$. 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.*

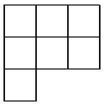
**Определение 4.1.5.** *Назовем диаграммой Юнга или просто диаграммой конечное подмножество $D \subset \mathbb{N} \times \mathbb{N}$, обладающее следующими свойствами:*

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* $\mathrm{diag}$, *а множество диаграмм, состоящих из $n$ клеток –* $\mathrm{diag}_n$. *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* $\lambda$. *Ясно, что* $\lambda \mapsto D(\lambda)$ *является биекцией* $\mathrm{part}$ *на* $\mathrm{diag}$ *и* $\mathrm{part}_n$ *на* $\mathrm{diag}_n$, *обратная к которой задается формулой* $\lambda_i := \min\{x \in \mathbb{N} : (x, i) \notin D\} - 1$. *Мы будем говорить, что разбиение* $\lambda'$ *двойственно к* $\lambda$, *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* $\lambda$ *– разбиение числа* $n$, $X$ *–* $n$*-элементное множество. Назовем* $X$*-таблицей (Юнга) формы* $\lambda$ *любую биекцию* $t\colon D(\lambda) \to X$. *Если* $X = [1, n]$, *то будем называть* $t$ *просто таблицей (Юнга) формы* $\lambda$. *Определим действие* $\mathfrak{S}_X$ *на множестве* $X$*-таблиц формы* $\lambda$ *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* $\sigma$, *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* $\lambda$ *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* $\lambda$, *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 $\lambda$ 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. 4.1.1). Обозначим через $d_\lambda$ количество подстановок циклического типа $\lambda$, т.е. количество элементов во множестве $\mathcal{C}_\lambda$. Значение $d_\lambda$ 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 $\lambda$.*

**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 $\lambda$ и $\mu$ – два разбиения. Мы будем говорить, что $\mu$ мажорирует $\lambda$, 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 $\mu$ строго мажорирует $\lambda$, и записывать это в виде $\lambda \prec \mu$ или $\mu \succ \lambda$.*

*Определим на* part *лексикографический порядок следующим образом: $\lambda < \mu$ (читается: "$\lambda$ лексикографически меньше $\mu$"), 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 $\mathrm{part}_n$ также есть два отношения порядка, индуцированные $<$ и $\prec$; в частности, лексикографический порядок $<$ позволяет однозначно расположить элементы $\mathrm{part}_n$ по возрастанию. В дальнейшем, всякий раз, когда нам надо будет линейно упорядочить $\mathrm{part}_n$ (скажем, чтобы изобразить матрицы со множеством индексов $\mathrm{part}_n$), мы будем использовать именно лексикографический порядок. Например, элементы $\mathrm{part}_5$ 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 $M_\lambda$: это свободный $K$-модуль, базисом которого являются всевозможные таблоиды $\{t\}$ формы $\lambda$, 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 $\lambda$ 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 $\psi_\lambda$ 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 бо́льших $n$ 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*

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

*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 $\sigma$ циклического типа $\mu$. Тогда $\psi_\lambda(\mathcal{C}_\mu) = \psi_\lambda(\sigma)$ есть число таблоидов формы $\lambda$, остающихся неподвижными под действием $\sigma$ (см. 3.5.1.1), т.е. количество таблоидов $\{t\}$ формы $\lambda$, обладающих тем свойством, что любой цикл подстановки $\sigma$ содержится в одной строке $\{t\}$. Иначе говоря, нам надо распределить циклы подстановки $\sigma$ по строкам так, чтобы в $i$-ой строке оказалось ровно $\lambda_i$ чисел. Рассмотрим первый цикл подстановки $\sigma$ (т.е. тот самый цикл, которому соответствует слагаемое $\mu_1$ циклического типа $\mu$ подстановки $\sigma$). 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 $\left(\psi_\lambda(\mathcal{C}_\mu)\right)_{\lambda,\mu\in \mathrm{part}_n}$ 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 $\kappa_t$ элемент групповой алгебры $\mathbb{Z}[\mathfrak{S}_n]$, определенный равенством $\kappa_t := \sum_{\sigma\in R_t}(\operatorname{sgn}\sigma)\sigma$, где $R_t$ – строчный стабилизатор $t$ (см. 4.1.9), а $\operatorname{sgn}\sigma = \pm 1$ – знак подстановки $\sigma$.*

Ясно, что для любой подстановки $\tau \in \mathfrak{S}_n$

$$\kappa_{\tau t} = \sum_{\sigma\in R_{\tau t}} (\operatorname{sgn}\sigma)\sigma = \sum_{\sigma\in \tau R_t \tau^{-1}} (\operatorname{sgn}\sigma)\sigma = \tau\kappa_t\tau^{-1}.$$

**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 $M_\lambda$, порожденный как $K$-модуль элементами вида $\kappa_t\{t\}$ для всевозможных таблиц $t$ формы $\lambda$ (это действительно $K$-$\mathfrak{S}_n$-модуль, поскольку $\tau\kappa_t\{t\} = \kappa_{\tau t}\{\tau t\}$). Обозначим через $\chi_\lambda$ характер $K$-$\mathfrak{S}_n$-модуля $S_\lambda$.*

**Замечание 4.1.17.** В действительности проверяется (см. [2]), что для любого поля $K$ нулевой характеристики $K$-$\mathfrak{S}_n$-модуль $S_\lambda$ прост, что модули Шпехта, соответствующие различным $\lambda$, 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 $M_\lambda$ в сумму простых модулей встречаются только $S_\mu$ с $\mu \succeq \lambda$ (и, следовательно, $\mu \geq \lambda$), причем $S_\lambda$ 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 $\chi$ является целочисленной комбинацией $(\chi_\lambda)$, 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 $(\varphi_1, \varphi_2)$ двух произвольных характеров $\varphi_1$ и $\varphi_2$ 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 $\varphi_2$). 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 $(\chi_\lambda)$ унитарного пространства $\mathrm{Cen}(\mathfrak{S}_n,\mathbb{C})$ получается из базиса $(\psi_\lambda)$ 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 [2]) хорош тем, что он легко реализуется на компьютере.

**Замечание 4.1.19.** Пусть $\chi$ – произвольный виртуальный характер группы $\mathfrak{S}_n$ (т.е. элемент кольца характеров $\mathrm{X}(\mathfrak{S}_n)$). Мы можем задать $\chi$ с помощью любого из трех наборов целых чисел $(x_\lambda)$, $(y'_\mu)$, $(z_\nu)$, 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 $(x_\lambda)$ к $(y'_\mu)$ 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 $(x_\lambda)$ к $(z_\nu)$ и наоборот по формуле $x_\lambda = z_\lambda + \sum_{\nu<\lambda} m_{\nu\lambda} z_\nu$ и от $(z_\nu)$ к $(y'_\mu)$ 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 $\chi$ 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 $\Lambda$ – 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, $n \leq 10$) 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 $\tau$-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 $\tau$-критерий дает необходимое условие того, что одна подгруппа содержится в другой, в терминах соответствующих виртуальных подгрупп (см. 3.6.9). 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 3.6.9), 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 подразделе 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 $\chi$; 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 $\chi_Z$ – 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 $\sigma$, а для любого разбиения $\lambda \in \mathrm{part}_n$ значение $\chi_Z(\mathcal{C}_\lambda)$ есть количество единичных слагаемых в разбиении $\lambda$.*

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

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

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

**Доказательство.** Положим $\tau_k := (k\ n) \in \mathfrak{S}_n$ для всех $k$ от 1 до $n$. Тогда $\tau_k$ 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 $\sigma$ 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 $\sigma$, т.е. $\chi_Z(\sigma)$; для всех этих $k$ подстановка $\tau_k\sigma\tau_k^{-1} \in \mathfrak{S}_{n-1}$ имеет циклический тип $\lambda'$, 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 $(z_\nu)$, 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 $\psi_\lambda$, $\psi_\mu$ – характеры, определенные в 4.1.12, а $\lambda\vee\mu$ – разбиение числа $n+m$, полученное объединением разбиений $\lambda$ и $\mu$; иначе говоря, мы рассматриваем последовательность, образованную приписыванием к последовательности ненулевых компонент $\lambda$ последовательности ненулевых компонент $\mu$, затем упорядочиваем элементы получившейся последовательности в порядке невозрастания и дополняем бесконечным числом нулей.*

b) *Если $\chi_1 = \sum_{\lambda\in\mathrm{part}_n} z_\lambda^{(1)}\psi_\lambda$ и $\chi_2 = \sum_{\mu\in\mathrm{part}_m} z_\mu^{(2)}\psi_\mu$ – два характера групп $\mathfrak{S}_n$ и $\mathfrak{S}_m$ соответственно, то*

$$\mathrm{Ind}(j,\mathbb{C})(\chi_1 * \chi_2) = \sum_{\nu\in\mathrm{part}_{m+n}} z_\nu\psi_\nu, \text{ где } z_\nu = \sum_{\lambda\vee\mu=\nu} z_\lambda^{(1)} z_\mu^{(2)}.$$

**Доказательство.** a) Мы знаем, что $\psi_\lambda = \chi_{\mathfrak{S}_n/\mathfrak{S}_\lambda}$, где $\mathfrak{S}_\lambda = \mathfrak{S}_{\lambda_1}\times\cdots\times\mathfrak{S}_{\lambda_k} \subset \mathfrak{S}_n$ (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 $\{1,2,\ldots,n+m\}$, 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 $(y'_\mu)$ (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 $\mu$ 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 $(y_\mu)$ исходя из $(y'_\mu)$ 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. $i^*X \cong \mathfrak{S}_{n-1}/H_1 \sqcup \ldots \sqcup \mathfrak{S}_{n-1}/H_s$. 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 $y_{\mu\vee(1)} = \chi\bigl(\mu \vee (1)\bigr) = \bigl(\mathrm{Cen}(i,\mathbb{C})(\chi)\bigr)(\mu)$ 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 $(y_\mu)$ для тех $\mu \in \mathrm{part}_n$, которые не записываются в виде $\mu' \vee (1)$ (таких $\mu$ 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 $(x_\lambda)$, или, что равносильно, $(z_\nu)$, можно проверять по ходу перебора, производимого в предыдущем пункте, поскольку согласно 4.1.19

$z_\nu$ зависит только от $y_\mu$ с $\mu \succeq \nu$; это позволяет отсекать по ходу заведомо неподходящие ветви перебора).

5. Проверить, удовлетворяет ли полученная виртуальная группа $\tau$-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, $i: G_0 \to G$ – 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 $\nu_j$ делят порядок группы $H$ и делятся на $n/\gcd(n, (G : H))$.*

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 $i_! i^* X \cong X \times Z$ установлено 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 $i: G_0 \to G$ 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 $|H_j| = |G_0|/(G_0 : H_j) = n|G_0|/\big((G : H)\nu_j\big) = n|G_0||H|/(|G|\nu_j) = |H|/\nu_j$, 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 подразделе.

Кроме того, мы можем определить, какие из построенных виртуальных подгрупп $\mathfrak{S}_n$ могут соответствовать (или обязательно соответствуют) транзитивным (т.е. транзитивно действующим на $Z = \{1, 2, \dots, n\} \cong \mathfrak{S}_n/\mathfrak{S}_{n-1}$) 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 $(\nu_j)$ 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 $(\nu_j)$, 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 $\chi$ была получена методом (c) из виртуальных подгрупп $\chi'$ и $\chi''$ 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 $\chi$ является существенной, поскольку $\chi$ соответствует $H' \times H'' \subset \mathfrak{S}_{n+m}$. Метод (a) также строит из существенных виртуальных подгрупп существенные, чего нельзя сказать о методе (b).

## 5. Нахождение разбиения $\lambda^{(p)}$

Теперь 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 $\lambda$, 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 $\mathrm{Frob}_A$ $k$-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 $\theta$ 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 $\mathrm{Frob}_A$. 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 $\theta^q$ 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 $\theta^q$, найти все $\theta^{qj}$ 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 $\Phi$ эндоморфизма Фробениуса $\mathrm{Frob}_A$ относительно рассматриваемого базиса состоит как раз из координат $\theta^{q^j}$ относительно этого базиса. В итоге мы нашли матрицу $\Phi$ за $O(n^3 + n^2 \log q)$ операций в поле $k$.

Рассмотрим теперь по отдельности наши два метода.

### 5.1. Метод, основанный на вычислении рангов

Прежде всего, заметим, что сепарабельность, или, что одно и то же, приведенность $A$ равносильна тривиальности ядра $\mathrm{Frob}_A$, т.е. невырожденности матрицы $\Phi$, 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 $\mathrm{Frob}_A$ переставляет элементы этого базиса как некоторая подстановка $\sigma$ циклического типа $\lambda$. 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 $\sigma^m$, т.е.

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

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 $(c_k)_{1\le k\le n}$ по $(a_m)_{1\le m\le n}$; поскольку $c_k = 0$ при $k > n$, это означает, что $\lambda$ однозначно определяется набором $(a_m)_{1\le m\le k}$. 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 $c_m = \sum_{k\ge 1}\mu(k)b_{km}$, где $\mu$ – функция Мебиуса. Эти формулы действительно определяют все $(b_m)$, все $(c_k)$ и $\lambda$ по $a_1, a_2, \dots, a_n$, поскольку мы знаем, что заведомо $b_m = 0$ и $c_m = 0$ при $m > n$.

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

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

| $\lambda$ | $a = (a_1, a_2, \dots)$ | префикс распознавания |
|---|---|---|
| $(1,1,1,1,1)$ | $(5,5,5,5,5,\dots)$ | $(5,\dots)$ |
| $(2,1,1,1)$ | $(4,5,4,5,4,\dots)$ | $(4,\dots)$ |
| $(2,2,1)$ | $(3,5,3,5,3,\dots)$ | $(3,5,\dots)$ |
| $(3,1,1)$ | $(3,3,5,3,3,\dots)$ | $(3,3,\dots)$ |
| $(3,2)$ | $(2,3,4,3,2,\dots)$ | $(2,*,4,\dots)$ |
| $(4,1)$ | $(2,3,2,5,2,\dots)$ | $(2,*,2,\dots)$ |
| $(5)$ | $(1,1,1,1,5,\dots)$ | $(1,\dots)$ |

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

### 5.2. 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 $\lambda$ по следам степеней эндоморфизма Фробениуса: $t_m := \operatorname{Tr}\operatorname{Frob}_A^m = \operatorname{Tr}\Phi^m$. Оказывается, что в случае $p > n$ набор $(t_m)_{1\leq m\leq n}$ однозначно определяет $\lambda$ 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 $\operatorname{Tr}\operatorname{Frob}_A^m = \operatorname{Tr}\operatorname{Frob}_{A_{\mathrm{red}}}^m$ 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 $\lambda$ числа $n' = \dim A_{\mathrm{red}} \leq n$. Рассмотрим базис $A_{\mathrm{red}}$, составленный из нормальных базисов $\mathbb{F}_{q^{\lambda_i}}$ над $k = \mathbb{F}_q$; автоморфизм Фробениуса $\operatorname{Frob}_{A_{\mathrm{red}}}$ действует на этом базисе как некоторая подстановка $\sigma \in \mathfrak{S}_{n'}$ циклического типа $\lambda$; отсюда получаем, что $t_m = \operatorname{Tr}\operatorname{Frob}_{A_{\mathrm{red}}}^m$ совпадает с образом в простом подполе $\mathbb{F}_p \subset \mathbb{F}_q$ количества неподвижных точек $t'_m$ подстановки $\sigma^m$. Поскольку $0 \leq t'_m \leq n' \leq n < p$, мы можем однозначно восстановить $t'_m$ по $t_m = t'_m \bmod p$.

Положим $c_k := \operatorname{card}\{i : \lambda_i = k\}$; тогда $\sum_{k\geq 1} kc_k = |\lambda| = n' \leq n$, 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 $(t'_m)_{1\leq m\leq n}$, или, что равносильно, знание набора $(t_m)_{1\leq m\leq n}$ позволяет определить все $c_k$ (поскольку $c_k = 0$ при $k > m$), а значит, и $\lambda$, а также $n' = \sum_{k\geq 1} kc_k$. 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 $\lambda$ (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 $\lambda$ 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 $\mu$, поскольку $\mu$ – 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 $\mu$ не различаются, а только помечается, что они соответствуют несепарабельному случаю. Вот пример такого дерева поиска для $n = 5$:

| $t' = (t'_1, t'_2, \ldots)$ | $v$ | $\lambda$ |
|---|---|---|
| $(0, 0, \ldots)$ | 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 $\lambda$ при лексикографическом упорядочении всех разбиений числа $n$; ясно, что при работе на компьютере удобнее иметь дело не с $\lambda$, 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 $\lambda$ числа $n$; при этом нужно вычислять меньшее количество степеней автоморфизма Фробениуса, поскольку уже известна сепарабельность $A$. Вот возникающее дерево распознавания для $n = 5$:

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

## 6. Статистический анализ результатов

Мы хотим теперь обсудить, после какого количества проанализированных простых чисел мы можем определить искомую группу Галуа (точнее, соответствующую виртуальную подгруппу $\mathfrak{S}_n$). Для этого мы рассмотрим следующую довольно близкую статистическую задачу. Предположим, что мы хотим определить некоторый неизвестный параметр $\eta$, принадлежащий некоторому заранее фиксированному конечному множеству $H$ (в нашем случае $H$ – множество всех виртуальных подгрупп $\mathfrak{S}_n$, а $\eta$ соответствует искомой группе Галуа). Для этого мы проводим серию экспериментов $\xi_1, \xi_2, \dots, \xi_j, \dots$ (испытаний регулярных простых чисел), результат $\xi_j$ каждого из которых принадлежит некоторому заранее известному конечному множеству $\Xi$ (у нас $\Xi = \mathrm{part}_n$ – множество всех разбиений числа $n$, а $\xi_j$ – 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 $\xi_j$ 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 $\lambda$, 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 $\lambda$). 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 $\varepsilon$ (например, $\varepsilon = 10^{-6}$) и зададимся следующим вопросом: можем ли мы по $N$ уже проделанным экспериментам определить $\eta$ с вероятностью ошибки, меньшей $\varepsilon$, в случае положительного ответа определить $\eta$, а в случае отрицательного ответа найти примерное количество экспериментов, которые надо еще сделать для определения $\eta$.

Пусть $N$ – количество уже проделанных экспериментов, $m_x := \operatorname{card}\{1 \le j \le N : \xi_j = x\}$ – 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 $\xi_j$ 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

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

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 $h \ne h_0$ (на самом деле из этого условия следует, что $P(\eta = h_0|A) > 1-\varepsilon\cdot|H|$; мы считаем, что $\varepsilon$ очень мало, а во множестве $H$ гораздо меньше элементов, чем $\varepsilon^{-1}$). 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

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

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 $\varepsilon$ на $\varepsilon\delta$, рассматривать условие

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

Положим $V_h := \sum_x m_x \cdot \bigl(-\log p_h(x)\bigr)$, $M := -\log\varepsilon$; 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 $h \in H'$) $V_h := \sum_x m_x \cdot \bigl(-\log p_h(x)\bigr)$, $M := -\log\varepsilon$ (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 $\eta$; если же нет, производим еще порядка $N \cdot \bigl(M/(V_{h_1} - V_{h_0}) - 1\bigr)$ экспериментов (лучше всего умножить это число на какую-нибудь константу, бо́льшую 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 $\eta$ с нужной степенью уверенности.

Мы можем оценить число экспериментов, необходимое для определения $\eta$ 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 $h$ оказывается равносильным условию $N > N_0 = \bigl(\min_{h\neq h_0} \sum_x p_{h_0}(x) \cdot (-\log p_h(x)) - \sum_x p_{h_0}(x) \cdot (-\log p_{h_0}(x))\bigr)^{-1}$.

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 $10! \cdot (10^6)^2$.

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 5.2); такое предложение, помимо своей простоты, основано на известных свойствах аналитической плотности множеств простых чисел из теоремы плотности Чеботарева.

Кроме того, предлагается следующая оптимизация. Всякий раз, когда мы получаем результат эксперимента (т.е. разбиение $\lambda$), 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.

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 анализ показывает, что вместо независимости $\xi_j$ 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 $\zeta$-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 $\varepsilon$ сколь угодно близким к $1/2$, что 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 $\leq 10$ обычно действительно достаточно рассмотрения двухсот простых чисел, что, в общем, может рассматриваться как еще одно подтверждение (впрочем, довольно косвенное) истинности гипотезы Римана.

## А. Таблицы

### А.1. 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 $\chi_\lambda$, а столбцы – классам сопряженных элементов $\mathcal{C}_\mu$, где $\lambda$ и $\mu$ – 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.

| $d_\mu$ <br> $\chi_\lambda(\mathcal{C}_\mu)$ | 1 <br> $(1)$ |
|---|---|
| $(1)$ | 1 |

| $m_{\lambda\mu}$ | $(1)$ |
|---|---|
| $(1)$ | 1 |

2.

| $d_\mu$ <br> $\chi_\lambda(\mathcal{C}_\mu)$ | 1 <br> $(1,1)$ | 1 <br> $(2)$ |
|---|---|---|
| $(1,1)$ | 1 | $-1$ |
| $(2)$ | 1 | 1 |

| $m_{\lambda\mu}$ | $(1,1)$ | $(2)$ |
|---|---|---|
| $(1,1)$ | 1 | 1 |
| $(2)$ | 0 | 1 |

3.

| $d_\mu$ <br> $\chi_\lambda(\mathcal{C}_\mu)$ | 1 <br> $(1,1,1)$ | 3 <br> $(2,1)$ | 2 <br> $(3)$ |
|---|---|---|---|
| $(1,1,1)$ | 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.

| $d_\mu$ <br> $\chi_\lambda(\mathcal{C}_\mu)$ | 1 <br> $(1,1,1,1)$ | 6 <br> $(2,1,1)$ | 3 <br> $(2,2)$ | 8 <br> $(3,1)$ | 6 <br> $(4)$ |
|---|---|---|---|---|---|
| $(1,1,1,1)$ | 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.

| $d_\mu$<br>$\chi_\lambda(\mathcal{C}_\mu)$ | 1<br>$(1^5)$ | 10<br>$(2,1^3)$ | 15<br>$(2^2,1)$ | 20<br>$(3,1^2)$ | 20<br>$(3,2)$ | 30<br>$(4,1)$ | 24<br>$(5)$ |
|---|---|---|---|---|---|---|---|
| $(1,1,1,1,1)$ | 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.

| $d_\mu$<br>$\chi_\lambda(\mathcal{C}_\mu)$ | 1<br>$(1^6)$ | 15<br>$(2,1^4)$ | 45<br>$(2^2,1^2)$ | 15<br>$(2^3)$ | 40<br>$(3,1^3)$ | 120<br>$(3,2,1)$ | 40<br>$(3^2)$ | 90<br>$(4,1^2)$ | 90<br>$(4,2)$ | 144<br>$(5,1)$ | 120<br>$(6)$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $(1,1,1,1,1,1)$ | 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.2. Виртуальные подгруппы $\mathfrak{S}_n$ при $n \le 6$**

Мы приводим список всех виртуальных подгрупп $\mathfrak{S}_n$ при $n \le 6$, 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 $n \le 10$, причем для вычисления потребовалось около 15 минут работы компьютера Pentium III-850. Этот список не приводится здесь только по причине своего большого размера – в него входит 4587 виртуальных подгрупп! Тем не менее, автор готов предоставить этот список в электронном виде.

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`.

| $y_\mu/d_\mu$ | 1/1 | 4/10 | 3/15 | 2/20 | 2/20 | 0/30 | 0/24 |
|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 10 | 4 | 2 | 1 | 1 | 0 | 0 |
| $x_\lambda$ | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| разл. 1 | $\langle$b$\rangle$ $3(13) + 2(16)$ | | | | | | |
| разл. 2 | $\langle$c$\rangle$ $3(8) + 2(4)$ | | | | | | |
| 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 $y_\mu/d_\mu$, 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: $\langle \mathrm{a}\rangle$ $(v)$, 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: $\langle \mathrm{b}\rangle$ $\nu_1(v_1)+\cdots+\nu_s(v_s)$, где $\nu$ – 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: $\langle \mathrm{c}\rangle$ $n_1(v_1)+n_2(v_2)$, 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 $\tau$-критерию 3.6.9. 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`.

| | |
|---|---|
| $y_\mu/d_\mu$ | 1/1 |
| $y'_\mu$ | 1 |
| $x_\lambda$ | 1 |

**Виртуальные подгруппы $\mathfrak{S}_1$:**

#2: порядок 1, индекс 1; +; свойства: `Ex`, `Un`, `Cy`, `Pe`, `Tr`, `No`.

| | |
|---|---|
| $y_\mu/d_\mu$ | 1/1 |
| $y'_\mu$ | 1 |
| $x_\lambda$ | 1 |

**Виртуальные подгруппы $\mathfrak{S}_2$:**

#3: порядок 1, индекс 2; +; свойства: `Ex`, `Un`, `Cy`, `Pe`, `No`.

| | | |
|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 0/1 |
| $y'_\mu$ | 2 | 0 |
| $x_\lambda$ | 1 | 1 |

#4: порядок 2, индекс 1; − (3); свойства: `Ex`, `Un`, `Cy`, `Pe`, `Tr`, `No`.

| | | |
|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 1/1 |
| $y'_\mu$ | 1 | 1 |
| $x_\lambda$ | 0 | 1 |
| разл. 1 | $\langle \mathrm{b} \rangle$ 2(2) | |
| подгр. | 3 | |

**Виртуальные подгруппы $\mathfrak{S}_3$:**

#5: порядок 1, индекс 6; +; свойства: `Ex`, `Un`, `Cy`, `Pe`, `No`.

| | | | |
|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 0/3 | 0/2 |
| $y'_\mu$ | 6 | 0 | 0 |
| $x_\lambda$ | 1 | 2 | 1 |

#6: порядок 2, индекс 3; $-$ (5); свойства: `Ex`, `Un`, `Cy`, `Pe`.

| $y_\mu/d_\mu$ | 1/1 | 1/3 | 0/2 |
|---|---|---|---|
| $y'_\mu$ | 3 | 1 | 0 |
| $x_\lambda$ | 0 | 1 | 1 |
| разл. 1 | $\langle$a$\rangle$ 1(4) | | |
| подгр. | 5 | | |

#7: порядок 3, индекс 2; $+$; свойства: `Ex`, `Un`, `Cy`, `Tr`, `No`.

| $y_\mu/d_\mu$ | 1/1 | 0/3 | 2/2 |
|---|---|---|---|
| $y'_\mu$ | 2 | 0 | 2 |
| $x_\lambda$ | 1 | 0 | 1 |
| разл. 1 | $\langle$b$\rangle$ 3(3) | | |
| подгр. | 5 | | |

#8: порядок 6, индекс 1; $-$ (7); свойства: `Ex`, `Un`, `Pe`, `Tr`, `No`.

| $y_\mu/d_\mu$ | 1/1 | 3/3 | 2/2 |
|---|---|---|---|
| $y'_\mu$ | 1 | 1 | 1 |
| $x_\lambda$ | 0 | 0 | 1 |
| разл. 1 | $\langle$b$\rangle$ 3(4) | | |
| подгр. | 6, 7 | | |

**Виртуальные подгруппы $\mathfrak{S}_4$:**

#9: порядок 1, индекс 24; $+$; свойства: `Ex`, `Un`, `Cy`, `Pe`, `No`.

| $y_\mu/d_\mu$ | 1/1 | 0/6 | 0/3 | 0/8 | 0/6 |
|---|---|---|---|---|---|
| $y'_\mu$ | 24 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 1 | 3 | 2 | 3 | 1 |

#10: порядок 2, индекс 12; $-$ (9); свойства: `Ex`, `Un`, `Cy`, `Pe`.

| $y_\mu/d_\mu$ | 1/1 | 1/6 | 0/3 | 0/8 | 0/6 |
|---|---|---|---|---|---|
| $y'_\mu$ | 12 | 2 | 0 | 0 | 0 |
| $x_\lambda$ | 0 | 1 | 1 | 2 | 1 |
| разл. 1 | $\langle$a$\rangle$ 1(6) | | | | |
| разл. 2 | $\langle$c$\rangle$ 2(4)+2(3) | | | | |
| подгр. | 9 | | | | |

#11: порядок 2, индекс 12; +; свойства: `Ex`, `Un`, `Cy`.

| $y_\mu/d_\mu$ | 1/1 | 0/6 | 1/3 | 0/8 | 0/6 |
|---|---|---|---|---|---|
| $y'_\mu$ | 12 | 0 | 4 | 0 | 0 |
| $x_\lambda$ | 1 | 1 | 2 | 1 | 1 |
| разл. 1 | $\langle$b$\rangle$ 2(5)+2(5) | | | | |
| подгр. | 9 | | | | |

#12: порядок 3, индекс 8; +; свойства: `Ex`, `Un`, `Cy`.

| $y_\mu/d_\mu$ | 1/1 | 0/6 | 0/3 | 2/8 | 0/6 |
|---|---|---|---|---|---|
| $y'_\mu$ | 8 | 0 | 0 | 2 | 0 |
| $x_\lambda$ | 1 | 1 | 0 | 1 | 1 |
| разл. 1 | $\langle$a$\rangle$ 1(7) | | | | |
| подгр. | 9 | | | | |

#13: порядок 4, индекс 6; − (11); свойства: `Ex`, `Pe`.

| $y_\mu/d_\mu$ | 1/1 | 2/6 | 1/3 | 0/8 | 0/6 |
|---|---|---|---|---|---|
| $y'_\mu$ | 6 | 2 | 2 | 0 | 0 |
| $x_\lambda$ | 0 | 0 | 1 | 1 | 1 |
| разл. 1 | $\langle$b$\rangle$ 2(6)+2(6) | | | | |
| разл. 2 | $\langle$c$\rangle$ 2(4)+2(4) | | | | |
| подгр. | 10, 11 | | | | |

#14: порядок 4, индекс 6; +; свойства: `Ex`, `Un`, `Tr`, `No`.

| $y_\mu/d_\mu$ | 1/1 | 0/6 | 3/3 | 0/8 | 0/6 |
|---|---|---|---|---|---|
| $y'_\mu$ | 6 | 0 | 6 | 0 | 0 |
| $x_\lambda$ | 1 | 0 | 2 | 0 | 1 |
| разл. 1 | $\langle$b$\rangle$ 4(5) | | | | |
| подгр. | 11 | | | | |

#15: порядок 4, индекс 6; − (11); свойства: `Ex`, `Un`, `Cy`, `Tr`.

| $y_\mu/d_\mu$ | 1/1 | 0/6 | 1/3 | 0/8 | 2/6 |
|---|---|---|---|---|---|
| $y'_\mu$ | 6 | 0 | 2 | 0 | 2 |
| $x_\lambda$ | 0 | 1 | 1 | 0 | 1 |
| разл. 1 | $\langle$b$\rangle$ 4(5) | | | | |
| | | | | | |

#16: порядок 6, индекс 4; $-$ (12); свойства: `Ex`, `Pe`.

| $y_\mu/d_\mu$ | 1/1 | 3/6 | 0/3 | 2/8 | 0/6 |
|---|---|---|---|---|---|
| $y'_\mu$ | 4 | 2 | 0 | 1 | 0 |
| $x_\lambda$ | 0 | 0 | 0 | 1 | 1 |
| разл. 1 | $\langle$a$\rangle$ 1(8) | | | | |
| подгр. | 10, 12 | | | | |

#17: порядок 8, индекс 3; $-$ (14); свойства: `Ex`, `Un`, `Tr`.

| $y_\mu/d_\mu$ | 1/1 | 2/6 | 3/3 | 0/8 | 2/6 |
|---|---|---|---|---|---|
| $y'_\mu$ | 3 | 1 | 3 | 0 | 1 |
| $x_\lambda$ | 0 | 0 | 1 | 0 | 1 |
| разл. 1 | $\langle$b$\rangle$ 4(6) | | | | |
| подгр. | 13, 14, 15 | | | | |

#18: порядок 12, индекс 2; $+$; свойства: `Ex`, `Un`, `Tr`, `No`.

| $y_\mu/d_\mu$ | 1/1 | 0/6 | 3/3 | 8/8 | 0/6 |
|---|---|---|---|---|---|
| $y'_\mu$ | 2 | 0 | 2 | 2 | 0 |
| $x_\lambda$ | 1 | 0 | 0 | 0 | 1 |
| разл. 1 | $\langle$b$\rangle$ 4(7) | | | | |
| подгр. | 12, 14 | | | | |

#19: порядок 24, индекс 1; $-$ (18); свойства: `Ex`, `Un`, `Pe`, `Tr`, `No`.

| $y_\mu/d_\mu$ | 1/1 | 6/6 | 3/3 | 8/8 | 6/6 |
|---|---|---|---|---|---|
| $y'_\mu$ | 1 | 1 | 1 | 1 | 1 |
| $x_\lambda$ | 0 | 0 | 0 | 0 | 1 |
| разл. 1 | $\langle$b$\rangle$ 4(8) | | | | |
| подгр. | 16, 17, 18 | | | | |

**Виртуальные подгруппы $\mathfrak{S}_5$:**

#20: порядок 1, индекс 120; $+$; свойства: `Ex`, `Un`, `Cy`, `Pe`, `No`.

| $y_\mu/d_\mu$ | 1/1 | 0/10 | 0/15 | 0/20 | 0/20 | 0/30 | 0/24 |
|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 120 | 0 | 0 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 1 | 4 | 5 | 6 | 5 | 4 | 1 |

#21: порядок 2, индекс 60; − (20); свойства: `Ex`, `Un`, `Cy`, `Pe`.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 1/10 | 0/15 | 0/20 | 0/20 | 0/30 | 0/24 |
| $y'_\mu$ | 60 | 6 | 0 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 0 | 1 | 2 | 3 | 3 | 3 | 1 |
| разл. 1 | ⟨a⟩ 1(10) | | | | | | |
| подгр. | 20 | | | | | | |

#22: порядок 2, индекс 60; +; свойства: `Ex`, `Un`, `Cy`.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 0/10 | 1/15 | 0/20 | 0/20 | 0/30 | 0/24 |
| $y'_\mu$ | 60 | 0 | 4 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 1 | 2 | 3 | 2 | 3 | 2 | 1 |
| разл. 1 | ⟨a⟩ 1(11) | | | | | | |
| подгр. | 20 | | | | | | |

#23: порядок 3, индекс 40; +; свойства: `Ex`, `Un`, `Cy`.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 0/10 | 0/15 | 2/20 | 0/20 | 0/30 | 0/24 |
| $y'_\mu$ | 40 | 0 | 0 | 4 | 0 | 0 | 0 |
| $x_\lambda$ | 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`.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 2/10 | 1/15 | 0/20 | 0/20 | 0/30 | 0/24 |
| $y'_\mu$ | 30 | 6 | 2 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 0 | 0 | 1 | 1 | 2 | 2 | 1 |
| разл. 1 | ⟨a⟩ 1(13) | | | | | | |
| подгр. | 21, 22 | | | | | | |

#25: порядок 4, индекс 30; +; свойства: `Ex`.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 0/10 | 3/15 | 0/20 | 0/20 | 0/30 | 0/24 |
| $y'_\mu$ | 30 | 0 | 6 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 1 | 1 | 2 | 0 | 2 | 1 | 1 |
| разл. 1 | ⟨a⟩ 1(14) | | | | | | |
| подгр. | 22 | | | | | | |

#26: порядок 4, индекс 30; − (22); свойства: `Ex`, `Un`, `Cy`.

| $y_\mu/d_\mu$ | 1/1 | 0/10 | 1/15 | 0/20 | 0/20 | 2/30 | 0/24 |
|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 30 | 0 | 2 | 0 | 0 | 2 | 0 |
| $x_\lambda$ | 0 | 1 | 2 | 1 | 1 | 1 | 1 |
| разл. 1 | ⟨a⟩ 1(15) | | | | | | |
| подгр. | 22 | | | | | | |

#27: порядок 5, индекс 24; +; свойства: `Ex`, `Un`, `Cy`, `Tr`.

| $y_\mu/d_\mu$ | 1/1 | 0/10 | 0/15 | 0/20 | 0/20 | 0/30 | 4/24 |
|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 24 | 0 | 0 | 0 | 0 | 0 | 4 |
| $x_\lambda$ | 1 | 0 | 1 | 2 | 1 | 0 | 1 |
| разл. 1 | ⟨b⟩ 5(9) | | | | | | |
| подгр. | 20 | | | | | | |

#28: порядок 6, индекс 20; − (23); свойства: `Ex`, `Pe`.

| $y_\mu/d_\mu$ | 1/1 | 3/10 | 0/15 | 2/20 | 0/20 | 0/30 | 0/24 |
|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 20 | 6 | 0 | 2 | 0 | 0 | 0 |
| $x_\lambda$ | 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`.

| $y_\mu/d_\mu$ | 1/1 | 1/10 | 0/15 | 2/20 | 2/20 | 0/30 | 0/24 |
|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 20 | 2 | 0 | 2 | 2 | 0 | 0 |
| $x_\lambda$ | 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`.

| $y_\mu/d_\mu$ | 1/1 | 0/10 | 3/15 | 2/20 | 0/20 | 0/30 | 0/24 |
|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 20 | 0 | 4 | 2 | 0 | 0 | 0 |
| $x_\lambda$ | 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`.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 2/10 | 3/15 | 0/20 | 0/20 | 2/30 | 0/24 |
| $y'_\mu$ | 15 | 3 | 3 | 0 | 0 | 1 | 0 |
| $x_\lambda$ | 0 | 0 | 1 | 0 | 1 | 1 | 1 |
| разл. 1 | $\langle$a$\rangle$ 1(17) | | | | | | |
| подгр. | 24, 25, 26 | | | | | | |

#32: порядок 10, индекс 12; +; свойства: `Tr`.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 0/10 | 5/15 | 0/20 | 0/20 | 0/30 | 4/24 |
| $y'_\mu$ | 12 | 0 | 4 | 0 | 0 | 0 | 2 |
| $x_\lambda$ | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| разл. 1 | $\langle$b$\rangle$ 5(11) | | | | | | |
| подгр. | 22, 27 | | | | | | |

#33: порядок 12, индекс 10; − (30); свойства: `Ex`, `Pe`.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 4/10 | 3/15 | 2/20 | 2/20 | 0/30 | 0/24 |
| $y'_\mu$ | 10 | 4 | 2 | 1 | 1 | 0 | 0 |
| $x_\lambda$ | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| разл. 1 | $\langle$b$\rangle$ $3(13)+2(16)$ | | | | | | |
| разл. 2 | $\langle$c$\rangle$ $3(8)+2(4)$ | | | | | | |
| подгр. | 24, 28, 29, 30 | | | | | | |

#34: порядок 12, индекс 10; +; свойства: `Ex`.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 0/10 | 3/15 | 8/20 | 0/20 | 0/30 | 0/24 |
| $y'_\mu$ | 10 | 0 | 2 | 4 | 0 | 0 | 0 |
| $x_\lambda$ | 1 | 1 | 0 | 0 | 0 | 1 | 1 |
| разл. 1 | $\langle$a$\rangle$ 1(18) | | | | | | |
| подгр. | 23, 25 | | | | | | |

#35: порядок 15, индекс 8; +; свойства: `Tr`.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 0/10 | 0/15 | 5/20 | 0/20 | 0/30 | 9/24 |
| $y'_\mu$ | 8 | 0 | 0 | 2 | 0 | 0 | 3 |
| $x_\lambda$ | 1 | 0 | 0 | 1 | 0 | 0 | 1 |
| разл. 1 | $\langle$b$\rangle$ 5(12) | | | | | | |
| подгр. | 23, 27 | | | | | | |

#36: порядок 20, индекс 6; − (32); свойства: `Tr`.

| $y_\mu/d_\mu$ | 1/1 | 0/10 | 5/15 | 0/20 | 0/20 | 10/30 | 4/24 |
|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 6 | 0 | 2 | 0 | 0 | 2 | 1 |
| $x_\lambda$ | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| разл. 1 | $\langle$b$\rangle$ 5(15) | | | | | | |
| подгр. | 26, 32 | | | | | | |

#37: порядок 24, индекс 5; − (34); свойства: `Ex`, `Pe`.

| $y_\mu/d_\mu$ | 1/1 | 6/10 | 3/15 | 8/20 | 0/20 | 6/30 | 0/24 |
|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 5 | 3 | 1 | 2 | 0 | 1 | 0 |
| $x_\lambda$ | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| разл. 1 | $\langle$a$\rangle$ 1(19) | | | | | | |
| подгр. | 28, 30, 31, 34 | | | | | | |

#38: порядок 60, индекс 2; +; свойства: `Ex`, `Un`, `Tr`, `No`.

| $y_\mu/d_\mu$ | 1/1 | 0/10 | 15/15 | 20/20 | 0/20 | 0/30 | 24/24 |
|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 2 | 0 | 2 | 2 | 0 | 0 | 2 |
| $x_\lambda$ | 1 | 0 | 0 | 0 | 0 | 0 | 1 |
| разл. 1 | $\langle$b$\rangle$ 5(18) | | | | | | |
| подгр. | 30, 32, 34 | | | | | | |

#39: порядок 120, индекс 1; − (38); свойства: `Ex`, `Un`, `Pe`, `Tr`, `No`.

| $y_\mu/d_\mu$ | 1/1 | 10/10 | 15/15 | 20/20 | 20/20 | 30/30 | 24/24 |
|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $x_\lambda$ | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| разл. 1 | $\langle$b$\rangle$ 5(19) | | | | | | |
| подгр. | 33, 35, 36, 37, 38 | | | | | | |

**Виртуальные подгруппы $\mathfrak{S}_6$:**

#40: порядок 1, индекс 720; +; свойства: Ex, Un, Cy, Pe, No.

| $y_\mu/d_\mu$ | 1/1 | 0/15 | 0/45 | 0/15 | 0/40 | 0/120 | 0/40 | 0/90 | 0/90 | 0/144 | 0/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 720 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 1 | 5 | 9 | 5 | 10 | 16 | 5 | 10 | 9 | 5 | 1 |

#41: порядок 2, индекс 360; − (40); свойства: Ex, Un, Cy, Pe.

| $y_\mu/d_\mu$ | 1/1 | 1/15 | 0/45 | 0/15 | 0/40 | 0/120 | 0/40 | 0/90 | 0/90 | 0/144 | 0/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 360 | 24 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 0 | 1 | 3 | 2 | 4 | 8 | 3 | 6 | 6 | 4 | 1 |
| разл. 1 | $\langle a\rangle$ 1(21) | | | | | | | | | | |
| подгр. | 40 | | | | | | | | | | |

#42: порядок 2, индекс 360; +; свойства: Ex, Un, Cy.

| $y_\mu/d_\mu$ | 1/1 | 0/15 | 1/45 | 0/15 | 0/40 | 0/120 | 0/40 | 0/90 | 0/90 | 0/144 | 0/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 360 | 0 | 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 1 | 3 | 5 | 3 | 4 | 8 | 3 | 4 | 5 | 3 | 1 |
| разл. 1 | $\langle a\rangle$ 1(22) | | | | | | | | | | |
| подгр. | 40 | | | | | | | | | | |

#43: порядок 2, индекс 360; − (40); свойства: Ex, Un, Cy.

| $y_\mu/d_\mu$ | 1/1 | 0/15 | 0/45 | 1/15 | 0/40 | 0/120 | 0/40 | 0/90 | 0/90 | 0/144 | 0/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 360 | 0 | 0 | 24 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 0 | 3 | 3 | 4 | 6 | 8 | 1 | 4 | 6 | 2 | 1 |
| разл. 1 | $\langle b\rangle$ 2(20) + 2(20) + 2(20) | | | | | | | | | | |
| подгр. | 40 | | | | | | | | | | |

#44: порядок 3, индекс 240; +; свойства: Ex, Un, Cy.

| $y_\mu/d_\mu$ | 1/1 | 0/15 | 0/45 | 0/15 | 2/40 | 0/120 | 0/40 | 0/90 | 0/90 | 0/144 | 0/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 240 | 0 | 0 | 0 | 12 | 0 | 0 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 1 | 3 | 3 | 1 | 4 | 4 | 1 | 4 | 3 | 3 | 1 |
| разл. 1 | $\langle a\rangle$ 1(23) | | | | | | | | | | |
| разл. 2 | $\langle c\rangle$ 3(7) + 3(5) | | | | | | | | | | |
| подгр. | 40 | | | | | | | | | | |

#45: порядок 3, индекс 240; +; свойства: Ex, Un, Cy.

| $y_\mu/d_\mu$ | 1/1 | 0/15 | 0/45 | 0/15 | 0/40 | 0/120 | 2/40 | 0/90 | 0/90 | 0/144 | 0/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 240 | 0 | 0 | 0 | 0 | 0 | 12 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 1 | 1 | 3 | 3 | 4 | 4 | 3 | 4 | 3 | 1 | 1 |
| разл. 1 | $\langle b\rangle$ 3(20) + 3(20) | | | | | | | | | | |
| подгр. | 40 | | | | | | | | | | |

#46: порядок 4, индекс 180; − (42); свойства: Ex, Pe.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 2/15 | 1/45 | 0/15 | 0/40 | 0/120 | 0/40 | 0/90 | 0/90 | 0/144 | 0/120 |
| $y'_\mu$ | 180 | 24 | 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 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).

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 1/15 | 1/45 | 1/15 | 0/40 | 0/120 | 0/40 | 0/90 | 0/90 | 0/144 | 0/120 |
| $y'_\mu$ | 180 | 12 | 4 | 12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 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.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 0/15 | 3/45 | 0/15 | 0/40 | 0/120 | 0/40 | 0/90 | 0/90 | 0/144 | 0/120 |
| $y'_\mu$ | 180 | 0 | 12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 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).

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 0/15 | 1/45 | 2/15 | 0/40 | 0/120 | 0/40 | 0/90 | 0/90 | 0/144 | 0/120 |
| $y'_\mu$ | 180 | 0 | 4 | 24 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 0 | 2 | 1 | 3 | 3 | 4 | 0 | 1 | 4 | 1 | 1 |
| разл. 1 | ⟨b⟩ 4(20) + 2(22) | | | | | | | | | | |
| подгр. | 42, 43 | | | | | | | | | | |

#50: порядок 4, индекс 180; − (42); свойства: Ex, Un, Cy.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 0/15 | 1/45 | 0/15 | 0/40 | 0/120 | 0/40 | 2/90 | 0/90 | 0/144 | 0/120 |
| $y'_\mu$ | 180 | 0 | 4 | 0 | 0 | 0 | 0 | 4 | 0 | 0 | 0 |
| $x_\lambda$ | 0 | 1 | 3 | 2 | 2 | 4 | 1 | 2 | 2 | 2 | 1 |
| разл. 1 | ⟨a⟩ 1(26) | | | | | | | | | | |
| разл. 2 | ⟨c⟩ 4(15) + 2(3) | | | | | | | | | | |
| подгр. | 42 | | | | | | | | | | |

#51: порядок 4, индекс 180; +; свойства: Ex, Un, Cy.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 0/15 | 1/45 | 0/15 | 0/40 | 0/120 | 0/40 | 0/90 | 2/90 | 0/144 | 0/120 |
| $y'_\mu$ | 180 | 0 | 4 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 0 |
| $x_\lambda$ | 1 | 1 | 3 | 1 | 2 | 4 | 1 | 2 | 3 | 1 | 1 |
| разл. 1 | ⟨b⟩ 4(20) + 2(22) | | | | | | | | | | |
| подгр. | 42 | | | | | | | | | | |

#52: порядок 5, индекс 144; +; свойства: Ex, Un, Cy.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 0/15 | 0/45 | 0/15 | 0/40 | 0/120 | 0/40 | 0/90 | 0/90 | 4/144 | 0/120 |
| $y'_\mu$ | 144 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 4 | 0 |
| $x_\lambda$ | 1 | 1 | 1 | 1 | 2 | 4 | 1 | 2 | 1 | 1 | 1 |
| разл. 1 | ⟨a⟩ 1(27) | | | | | | | | | | |
| подгр. | 40 | | | | | | | | | | |

#53: порядок 6, индекс 120; − (44); свойства: Ex, Pe.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 3/15 | 0/45 | 0/15 | 2/40 | 0/120 | 0/40 | 0/90 | 0/90 | 0/144 | 0/120 |
| $y'_\mu$ | 120 | 24 | 0 | 0 | 6 | 0 | 0 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 0 | 0 | 0 | 0 | 1 | 2 | 1 | 3 | 3 | 3 | 1 |
| разл. 1 | ⟨a⟩ 1(28) | | | | | | | | | | |
| разл. 2 | ⟨c⟩ 3(8) + 3(5) | | | | | | | | | | |
| подгр. | 41, 44 | | | | | | | | | | |

$\#54$: порядок 6, индекс 120; $-$ (44); свойства: Ex, Un, Cy.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 1/15 | 0/45 | 0/15 | 2/40 | 2/120 | 0/40 | 0/90 | 0/90 | 0/144 | 0/120 |
| $y'_\mu$ | 120 | 8 | 0 | 0 | 6 | 2 | 0 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 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.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 0/15 | 3/45 | 0/15 | 2/40 | 0/120 | 0/40 | 0/90 | 0/90 | 0/144 | 0/120 |
| $y'_\mu$ | 120 | 0 | 8 | 0 | 6 | 0 | 0 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 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; $+$.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 0/15 | 3/45 | 0/15 | 0/40 | 0/120 | 2/40 | 0/90 | 0/90 | 0/144 | 0/120 |
| $y'_\mu$ | 120 | 0 | 8 | 0 | 0 | 0 | 6 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 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.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 0/15 | 0/45 | 3/15 | 0/40 | 0/120 | 2/40 | 0/90 | 0/90 | 0/144 | 0/120 |
| $y'_\mu$ | 120 | 0 | 0 | 24 | 0 | 0 | 6 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 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.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 0/15 | 0/45 | 1/15 | 0/40 | 0/120 | 2/40 | 0/90 | 0/90 | 0/144 | 2/120 |
| $y'_\mu$ | 120 | 0 | 0 | 8 | 0 | 0 | 6 | 0 | 0 | 0 | 2 |
| $x_\lambda$ | 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).

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 3/15 | 3/45 | 1/15 | 0/40 | 0/120 | 0/40 | 0/90 | 0/90 | 0/144 | 0/120 |
| $y'_\mu$ | 90 | 18 | 6 | 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 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.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 2/15 | 3/45 | 0/15 | 0/40 | 0/120 | 0/40 | 2/90 | 0/90 | 0/144 | 0/120 |
| $y'_\mu$ | 90 | 12 | 6 | 0 | 0 | 0 | 0 | 2 | 0 | 0 | 0 |
| $x_\lambda$ | 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).

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 2/15 | 1/45 | 2/15 | 0/40 | 0/120 | 0/40 | 0/90 | 2/90 | 0/144 | 0/120 |
| $y'_\mu$ | 90 | 12 | 2 | 12 | 0 | 0 | 0 | 0 | 2 | 0 | 0 |
| $x_\lambda$ | 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.

| $y_\mu/d_\mu$ | 1/1 | 1/15 | 3/45 | 3/15 | 0/40 | 0/120 | 0/40 | 0/90 | 0/90 | 0/144 | 0/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 90 | 6 | 6 | 18 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 0 | 1 | 0 | 2 | 1 | 2 | 0 | 0 | 3 | 1 | 1 |
| разл. 1 | ⟨b⟩ 4(21) + 2(25) | | | | | | | | | | |
| разл. 2 | ⟨b⟩ 4(22) + 2(24) | | | | | | | | | | |
| разл. 3 | ⟨c⟩ 4(14) + 2(4) | | | | | | | | | | |
| подгр. | 47, 48, 49 | | | | | | | | | | |

#63: порядок 8, индекс 90; − (51); свойства: Ex.

| $y_\mu/d_\mu$ | 1/1 | 1/15 | 1/45 | 1/15 | 0/40 | 0/120 | 0/40 | 2/90 | 2/90 | 0/144 | 0/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 90 | 6 | 2 | 6 | 0 | 0 | 0 | 2 | 2 | 0 | 0 |
| $x_\lambda$ | 0 | 0 | 1 | 1 | 1 | 2 | 0 | 1 | 2 | 1 | 1 |
| разл. 1 | ⟨b⟩ 4(21) + 2(26) | | | | | | | | | | |
| разл. 2 | ⟨c⟩ 4(15) + 2(4) | | | | | | | | | | |
| подгр. | 47, 50, 51 | | | | | | | | | | |

#64: порядок 8, индекс 90; +; свойства: Ex.

| $y_\mu/d_\mu$ | 1/1 | 0/15 | 5/45 | 0/15 | 0/40 | 0/120 | 0/40 | 0/90 | 2/90 | 0/144 | 0/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 90 | 0 | 10 | 0 | 0 | 0 | 0 | 0 | 2 | 0 | 0 |
| $x_\lambda$ | 1 | 1 | 2 | 1 | 0 | 2 | 1 | 0 | 2 | 1 | 1 |
| разл. 1 | ⟨b⟩ 4(22) + 2(25) | | | | | | | | | | |
| подгр. | 48, 51 | | | | | | | | | | |

#65: порядок 8, индекс 90; − (48).

| $y_\mu/d_\mu$ | 1/1 | 0/15 | 3/45 | 2/15 | 0/40 | 0/120 | 0/40 | 2/90 | 0/90 | 0/144 | 0/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 90 | 0 | 6 | 12 | 0 | 0 | 0 | 2 | 0 | 0 | 0 |
| $x_\lambda$ | 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.

| $y_\mu/d_\mu$ | 1/1 | 0/15 | 0/45 | 0/15 | 4/40 | 0/120 | 4/40 | 0/90 | 0/90 | 0/144 | 0/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 80 | 0 | 0 | 0 | 8 | 0 | 8 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 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; +.

| $y_\mu/d_\mu$ | 1/1 | 0/15 | 5/45 | 0/15 | 0/40 | 0/120 | 0/40 | 0/90 | 0/90 | 4/144 | 0/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 72 | 0 | 8 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 0 |
| $x_\lambda$ | 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.

| $y_\mu/d_\mu$ | 1/1 | 4/15 | 3/45 | 0/15 | 2/40 | 2/120 | 0/40 | 0/90 | 0/90 | 0/144 | 0/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 60 | 16 | 4 | 0 | 3 | 1 | 0 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 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).

| $y_\mu/d_\mu$ | 1/1 | 3/15 | 3/45 | 1/15 | 0/40 | 0/120 | 2/40 | 0/90 | 0/90 | 0/144 | 2/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 60 | 12 | 4 | 4 | 0 | 0 | 3 | 0 | 0 | 0 | 1 |
| $x_\lambda$ | 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.

| $y_\mu/d_\mu$ | 1/1 | 0/15 | 3/45 | 4/15 | 0/40 | 0/120 | 2/40 | 0/90 | 0/90 | 0/144 | 2/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 60 | 0 | 4 | 16 | 0 | 0 | 3 | 0 | 0 | 0 | 1 |
| $x_\lambda$ | 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.

| $y_\mu/d_\mu$ | 1/1 | 0/15 | 3/45 | 0/15 | 8/40 | 0/120 | 0/40 | 0/90 | 0/90 | 0/144 | 0/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 60 | 0 | 4 | 0 | 12 | 0 | 0 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 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; +.

| $y_\mu/d_\mu$ | 1/1 | 0/15 | 3/45 | 0/15 | 4/40 | 0/120 | 4/40 | 0/90 | 0/90 | 0/144 | 0/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 60 | 0 | 4 | 0 | 6 | 0 | 6 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 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.

| $y_\mu/d_\mu$ | 1/1 | 0/15 | 3/45 | 0/15 | 0/40 | 0/120 | 8/40 | 0/90 | 0/90 | 0/144 | 0/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 60 | 0 | 4 | 0 | 0 | 0 | 12 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 1 | 0 | 1 | 2 | 1 | 0 | 2 | 1 | 1 | 0 | 1 |
| разл. 1 | ⟨b⟩ 6(22) | | | | | | | | | | |
| подгр. | 48, 56 | | | | | | | | | | |

#74: порядок 15, индекс 48; +.

| $y_\mu/d_\mu$ | 1/1 | 0/15 | 0/45 | 0/15 | 5/40 | 0/120 | 0/40 | 0/90 | 0/90 | 9/144 | 0/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 48 | 0 | 0 | 0 | 6 | 0 | 0 | 0 | 0 | 3 | 0 |
| $x_\lambda$ | 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.

| $y_\mu/d_\mu$ | 1/1 | 3/15 | 5/45 | 3/15 | 0/40 | 0/120 | 0/40 | 2/90 | 2/90 | 0/144 | 0/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 45 | 9 | 5 | 9 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |
| $x_\lambda$ | 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.

| $y_\mu/d_\mu$ | 1/1 | 1/15 | 5/45 | 1/15 | 0/40 | 0/120 | 0/40 | 6/90 | 2/90 | 0/144 | 0/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 45 | 3 | 5 | 3 | 0 | 0 | 0 | 3 | 1 | 0 | 0 |
| $x_\lambda$ | 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.

| $y_\mu/d_\mu$ | 1/1 | 3/15 | 0/45 | 0/15 | 4/40 | 6/120 | 4/40 | 0/90 | 0/90 | 0/144 | 0/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 40 | 8 | 0 | 0 | 4 | 2 | 4 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 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.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 0/15 | 9/45 | 0/15 | 4/40 | 0/120 | 4/40 | 0/90 | 0/90 | 0/144 | 0/120 |
| $y'_\mu$ | 40 | 0 | 8 | 0 | 4 | 0 | 4 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 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.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 0/15 | 0/45 | 3/15 | 4/40 | 0/120 | 4/40 | 0/90 | 0/90 | 0/144 | 6/120 |
| $y'_\mu$ | 40 | 0 | 0 | 8 | 4 | 0 | 4 | 0 | 0 | 0 | 2 |
| $x_\lambda$ | 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).

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 0/15 | 5/45 | 0/15 | 0/40 | 0/120 | 0/40 | 10/90 | 0/90 | 4/144 | 0/120 |
| $y'_\mu$ | 36 | 0 | 4 | 0 | 0 | 0 | 0 | 4 | 0 | 1 | 0 |
| $x_\lambda$ | 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.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 6/15 | 3/45 | 0/15 | 8/40 | 0/120 | 0/40 | 6/90 | 0/90 | 0/144 | 0/120 |
| $y'_\mu$ | 30 | 12 | 2 | 0 | 6 | 0 | 0 | 2 | 0 | 0 | 0 |
| $x_\lambda$ | 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.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 3/15 | 3/45 | 1/15 | 0/40 | 0/120 | 8/40 | 0/90 | 0/90 | 0/144 | 8/120 |
| $y'_\mu$ | 30 | 6 | 2 | 2 | 0 | 0 | 6 | 0 | 0 | 0 | 2 |
| $x_\lambda$ | 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.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 1/15 | 3/45 | 3/15 | 8/40 | 8/120 | 0/40 | 0/90 | 0/90 | 0/144 | 0/120 |
| $y'_\mu$ | 30 | 2 | 2 | 6 | 6 | 2 | 0 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 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.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 0/15 | 9/45 | 0/15 | 8/40 | 0/120 | 0/40 | 0/90 | 6/90 | 0/144 | 0/120 |
| $y'_\mu$ | 30 | 0 | 6 | 0 | 6 | 0 | 0 | 0 | 2 | 0 | 0 |
| $x_\lambda$ | 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.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y_\mu/d_\mu$ | 1/1 | 0/15 | 9/45 | 0/15 | 0/40 | 0/120 | 8/40 | 0/90 | 6/90 | 0/144 | 0/120 |
| $y'_\mu$ | 30 | 0 | 6 | 0 | 0 | 0 | 6 | 0 | 2 | 0 | 0 |
| $x_\lambda$ | 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.

| $y_\mu/d_\mu$ | 1/1 | 0/15 | 3/45 | 6/15 | 0/40 | 0/120 | 8/40 | 6/90 | 0/90 | 0/144 | 0/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 30 | 0 | 2 | 12 | 0 | 0 | 6 | 2 | 0 | 0 | 0 |
| $x_\lambda$ | 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.

| $y_\mu/d_\mu$ | 1/1 | 6/15 | 9/45 | 0/15 | 4/40 | 12/120 | 4/40 | 0/90 | 0/90 | 0/144 | 0/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 20 | 8 | 4 | 0 | 2 | 2 | 2 | 0 | 0 | 0 | 0 |
| $x_\lambda$ | 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.

| $y_\mu/d_\mu$ | 1/1 | 0/15 | 9/45 | 6/15 | 4/40 | 0/120 | 4/40 | 0/90 | 0/90 | 0/144 | 12/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 20 | 0 | 4 | 8 | 2 | 0 | 2 | 0 | 0 | 0 | 2 |
| $x_\lambda$ | 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.

| $y_\mu/d_\mu$ | 1/1 | 0/15 | 9/45 | 0/15 | 4/40 | 0/120 | 4/40 | 0/90 | 18/90 | 0/144 | 0/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 20 | 0 | 4 | 0 | 2 | 0 | 2 | 0 | 4 | 0 | 0 |
| $x_\lambda$ | 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.

| $y_\mu/d_\mu$ | 1/1 | 7/15 | 9/45 | 3/15 | 8/40 | 8/120 | 0/40 | 6/90 | 6/90 | 0/144 | 0/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 15 | 7 | 3 | 3 | 3 | 1 | 0 | 1 | 1 | 0 | 0 |
| $x_\lambda$ | 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.

| $y_\mu/d_\mu$ | 1/1 | 3/15 | 9/45 | 7/15 | 0/40 | 0/120 | 8/40 | 6/90 | 6/90 | 0/144 | 8/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 15 | 3 | 3 | 7 | 0 | 0 | 3 | 1 | 1 | 0 | 1 |
| $x_\lambda$ | 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.

| $y_\mu/d_\mu$ | 1/1 | 0/15 | 15/45 | 0/15 | 20/40 | 0/120 | 0/40 | 0/90 | 0/90 | 24/144 | 0/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 12 | 0 | 4 | 0 | 6 | 0 | 0 | 0 | 0 | 2 | 0 |
| $x_\lambda$ | 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.

| $y_\mu/d_\mu$ | 1/1 | 0/15 | 15/45 | 0/15 | 0/40 | 0/120 | 20/40 | 0/90 | 0/90 | 24/144 | 0/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 12 | 0 | 4 | 0 | 0 | 0 | 6 | 0 | 0 | 2 | 0 |
| $x_\lambda$ | 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`.

| $y_\mu/d_\mu$ | 1/1 | 6/15 | 9/45 | 6/15 | 4/40 | 12/120 | 4/40 | 0/90 | 18/90 | 0/144 | 12/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 10 | 4 | 2 | 4 | 1 | 1 | 1 | 0 | 2 | 0 | 1 |
| $x_\lambda$ | 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`.

| $y_\mu/d_\mu$ | 1/1 | 10/15 | 15/45 | 0/15 | 20/40 | 20/120 | 0/40 | 30/90 | 0/90 | 24/144 | 0/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 6 | 4 | 2 | 0 | 3 | 1 | 0 | 2 | 0 | 1 | 0 |
| $x_\lambda$ | 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`.

| $y_\mu/d_\mu$ | 1/1 | 0/15 | 15/45 | 10/15 | 0/40 | 0/120 | 20/40 | 30/90 | 0/90 | 24/144 | 20/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 6 | 0 | 2 | 4 | 0 | 0 | 3 | 2 | 0 | 1 | 1 |
| $x_\lambda$ | 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`.

| $y_\mu/d_\mu$ | 1/1 | 0/15 | 45/45 | 0/15 | 40/40 | 0/120 | 40/40 | 0/90 | 90/90 | 144/144 | 0/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 0 | 2 | 2 | 0 |
| $x_\lambda$ | 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`.

| $y_\mu/d_\mu$ | 1/1 | 15/15 | 45/45 | 15/15 | 40/40 | 120/120 | 40/40 | 90/90 | 90/90 | 144/144 | 120/120 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y'_\mu$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $x_\lambda$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| разл. 1 | ⟨b⟩ 6(39) | | | | | | | | | | |
| подгр. | 90, 91, 94, 95, 96, 97 | | | | | | | | | | |

## Литература


1. Ж.-П. Серр, *Линейные представления конечных групп.* — Мир, М. (1970).
2. Г. Джеймс, *Теория представлений симметрических групп.* — Мир, М. (1982).
3. Дж. Касселс, А. Фрёлих, *Алгебраическая теория чисел.* — Мир, М. (1969).
4. J. Dieudonné, A. Grothendieck, *Eléments de Géométrie Algèbrique: Le language des schémas.* — Publ. Math. IHES, No. 4 (1960).
5. J. Dieudonné, A. Grothendieck, *Eléments de Géométrie Algèbrique: Étude locale des schémas et des morphismes de schémas.* — Publ. Math. IHES, No. 20 (1964), No. 24 (1965), No. 28 (1966), No. 32 (1967).
6. A. Grothendieck et al., *Revêtements étales et Groupe Fondamental.* — Lecture Notes in Math., 224, Springer-Verlag, Heidelberg (1971).
7. M. Artin, A. Grothendieck, J. L. Verdier et al., *Théorie des Topos et Cohomologie Étale des Schémas.* — Lecture Notes in Math., 269, 270, 305, Springer-Verlag, Heidelberg (1972–1973).
8. P. Berthelot, L. Illusie et al., *Théorie des Intersections et Théorème de Riemann–Roch.* — Lecture Notes in Math., 225, Springer-Verlag, Heidelberg (1971).
9. Н. Бурбаки, *Алгебра. Гл. X. Гомологическая алгебра.* Наука, М. (1987).
10. Н. В. Дуров, *Вычисление группы Галуа многочлена с рациональными коэффициентами.* I. — Зап. научн. семин. ПОМИ **319** (2004), 117–198.



Durov N. V. Computation of the Galois group of a polynomial with rational coefficients, II.

A new method, which enables us to compute rather efficiently the Galois group of a polynomial over $\mathbb{Q}$, respectively, over $\mathbb{Z}$ is presented. Reductions of this polynomial with respect different prime modules are studied, and the information obtained is used for the calculation of the Galois group of the initial polynomial. This method uses an original modification of the Chebotarev density theorem and it is in essence a probability method. The irreducibility of the polynomial under consideration is not assumed. The appendix to this paper contains tables which enable one to find the Galois group of polynomials of degree less than or equal to 10 as a subgroup of the symmetric group.

Here the final part of the paper is published. The first part is contained in the previous issue (see Vol. 319 (2004)).



С.-Петербургский государственный университет



Поступило 25 июня 2004 г.