М. В. Игнатьев, Квантовая комбинаторика, *Матем. просв.*, 2014, выпуск 18, 66–111

Квантовая комбинаторика

М. В. Игнатьев

Предисловие

Очень часто серьёзная математическая проблема есть, в конечном счёте, проблема классификации тех или иных объектов, а главная трудность обычно заключается в изобретении адекватного языка, адекватных терминов, в которых эта классификация должна быть дана. В то же время удачная система терминов обычно позволяет продвинуться в решении поставленных задач гораздо дальше, чем предполагалось. Ярчайшим примером здесь являются диаграммы Дынкина — они классифицируют, пожалуй, не один *десяток* математических конструкций: простые алгебры Ли, простые алгебраические группы, особенности волновых фронтов, колчаны конечного типа...

В самом широком смысле комбинаторика и есть набор разнообразных методов, приспособленных для классификации математических объектов той или иной природы. Статус комбинаторики как единой науки до сих пор вызывает самые оживлённые дискуссии, но систематическое использование комбинаторных методов в алгебре, геометрии, анализе очень часто приводит к первоклассным результатам.

Числа сочетаний и размещений являются комбинаторной классикой; с изучения их свойств почти всегда начинается знакомство с комбинаторикой. Известно огромное количество тождеств, связывающих между собой числа сочетаний и размещений и обладающих как изящными алгебраическими доказательствами, так и яркой комбинаторной трактовкой. Пожалуй, один из наиболее эффектных подходов к изучению широкого класса таких тождеств приведён в книге [16].

Оказывается, эти абсолютно классические объекты допускают чрезвычайно широкое обобщение. А именно, их можно рассматривать как значения некоторых многочленов от переменной q с целыми коэффициентами в точке $q = 1$. Эти многочлены называются *квантовыми числами сочетаний* и *размещений* соответственно. Термин объясняется сходством

с квантовой механикой, где буквой q часто обозначают число $e^{\hbar}$ ($\hbar$ — постоянная Планка): некоторые формулы классической механики могут быть получены предельным переходом при $\hbar \to 0$, то есть при $q \to 1$.

Более того, выяснилось, что все классические комбинаторные тождества тоже допускают свои квантовые аналоги, которые при $q = 1$ превращаются в исходные, так что «обычная» комбинаторика может рассматриваться как очень частный случай «квантовой». Есть у квантовых аналогов и чисто комбинаторная интерпретация, которая при $q = 1$ даёт исходное комбинаторное определение классических чисел сочетаний и размещений. Но и это ещё не всё. На самом деле, квантовые числа сочетаний и размещений допускают совершенно неожиданную геометрическую трактовку в терминах векторных пространств над конечными полями, а именно, они перечисляют определённые конфигурации подпространств.

Цель этой статьи — изложить начальные понятия и результаты теории квантовых аналогов. В первом параграфе мы напоминаем определения чисел сочетаний и размещений, выводим явную формулу для них и доказываем те тождества, которые потом будем квантовать (в том числе, конечно, треугольник Паскаля и бином Ньютона). Второй параграф содержит определения квантовых чисел сочетаний и размещений, их элементарные свойства и квантовые аналоги тождеств, доказанных в параграфе 1.

Третий параграф посвящён комбинаторной интерпретации квантовых аналогов. А именно, мы показываем, что квантовое число сочетаний из n по k можно представить как сумму одночленов вида q в какой-то степени, причём каждый одночлен соответствует неупорядоченной выборке k предметов из n предметов. Таким образом, при $q = 1$ мы имеем классическое комбинаторное определение чисел сочетаний. Аналогичная формула доказывается и для квантовых чисел размещений.

В четвёртом параграфе мы весьма кратко напоминаем базовые сведения из линейной алгебры: определения поля, векторного пространства, линейно зависимых и независимых векторов, базиса и размерности пространства. Всё это нужно для ключевого, пятого параграфа, в котором доказано, что квантовые аналоги перечисляют флаги (цепочки подпространств фиксированных размерностей) в конечномерных векторных пространствах над конечным полем из q элементов. Более того, оказывается, что квантовые тождества, полученные ранее чисто алгебраически, могут быть передоказаны с использованием этой геометрической интерпретации!

В шестом параграфе мы приводим ещё один, теоретико-групповой взгляд на квантовые числа сочетаний и размещений. После быстрого напоминания важнейших определений из теории групп мы определяем группу невырожденных матриц и доказываем, что квантовые аналоги — это

в точности индексы $\mathrm{GL}_n(\mathbb{F}_q)$ по параболическим подгруппам (подгруппам блочно-треугольных матриц) специального вида. На самом деле, после геометрической интерпретации в этом нет уже ничего удивительного или загадочного. Причина в том, что эти параболические подгруппы являются стабилизаторами флагов специального вида при естественном действии полной линейной группы на множестве всех флагов данного типа. Объяснению этого факта и посвящён последний, седьмой параграф.

Теперь скажем о том, чего в этой статье *нет*. Дело в том, что квантовые аналоги — очень содержательная теория, которая сейчас быстро развивается и имеет массу красивых приложений, рассказать о которых у нас не было никакой возможности. Во-первых, с помощью квантовых чисел сочетаний и размещений могут быть доказаны вполне классические тождества, известные ещё Эйлеру и Гауссу. Подробно этот аспект разбирается, например, в книге [7], посвящённой квантовой версии математического анализа.

Во-вторых, квантовые аналоги являются мощным вычислительным средством при работе с так называемыми *квантовыми группами*. Эти объекты, лежащие на стыке математики и теоретической физики, возникли в 1980-е годы в работах В. Г. Дринфельда и М. Джимбо и быстро стали очень популярными как среди алгебраистов, так и среди специалистов по квантовой теории поля. Грубо говоря, квантовые группы — это специфические «деформации» классических конечномерных алгебр Ли, к примеру алгебры $\mathfrak{sl}_n(\mathbb{C})$. Подробности можно найти в книге [15].

Далее, существует масса квантовых аналогов других замечательных комбинаторных объектов — чисел Стирлинга, чисел Белла, чисел Каталана... Мы не можем перечислять здесь десятки статей, посвящённых весьма красивым тождествам, связывающим квантовые версии этих объектов. Интересующийся читатель может вбить в любой поисковой системе запрос вроде `q-Catalan numbers` и посмотреть, сколько ссылок будет получено в ответ. Другой вариант — сделать такой же запрос на странице Международного математического архива `http://front.math.ucdavis.edu`.

Наконец, даже те сюжеты, о которых идёт речь в статье, чаще всего далеко не исчерпываются изложенным здесь материалом. Так, мы не приводим геометрического доказательства формулы треугольника Паскаля: оно хотя и не слишком сложно, требует определения аффинного пространства и аффинных плоскостей, см. [7]. Интерпретация квантовых аналогов в терминах параболических подгрупп даёт возможность получать далеко идущие обобщения всей этой теории, если брать вместо группы $\mathrm{GL}_n(\mathbb{F}_q)$ другие редуктивные матричные группы над конечными полями — к примеру $\mathrm{SO}_n(\mathbb{F}_q)$ или $\mathrm{Sp}_{2n}(\mathbb{F}_q)$. Впрочем, мы и стремились не столько дать

полный обзор теории квантовых аналогов, сколько изложить несколько ярких и вместе с тем простых сюжетов, способных заинтересовать продвинутого старшеклассника или студента младших курсов.

Статья представляет собой очень расширенную версию лекции, прочитанной мной на Малом мехмате МГУ 11 ноября 2006 года. Я благодарю Александра Васильевича Спивака за приглашение прочесть эту лекцию. Я очень признателен Владимиру Доценко, который на летней школе «Современная математика» в Дубне в 2005 году впервые познакомил меня с квантовыми аналогами чисел сочетаний и размещений.

Я благодарен Владиславу Дружинину, который, будучи тогда школьником, рассказал мне придуманное им геометрическое доказательство теоремы 5.8. Я также выражаю благодарность Ивану Лишаеву, который (тоже будучи школьником) обратил моё внимание на комбинаторную интерпретацию чисел размещений (предложение 3.2).

Многие из сформулированных в тексте упражнений разбирались на учебно-исследовательском семинаре, которым я руководил в 2010 году, на кафедре алгебры и геометрии Самарского государственного университета. Это помогло исправить некоторые ошибки и, я надеюсь, порой улучшить способ изложения. Я выражаю признательность Сергею Бронникову, Ксении Вяткиной, Дмитрию Елисееву, Елене Кукариной, Павлу Никулину, Фёдору Череватенко и другим участникам семинара.

Отдельная благодарность — Михаилу Панову, чудесные TEXнические познания которого сильно способствовали улучшению оформления текста.

§ 1. Классическая комбинаторика

Читатель, скорее всего, уже сталкивался с элементарными комбинаторными понятиями и фактами. Тем не менее, мы считаем нужным напомнить некоторые базовые вещи — хотя бы для того, чтобы зафиксировать обозначения. Пусть n — любое целое неотрицательное число, а k — произвольное целое число от 0 до n.

Число размещений из n по k — это количество строк длины k, заполненных числами от 1 до n. Другими словами, это количество способов выбрать k предметов из n разных предметов, причём важен порядок, в котором эти предметы выбираются. Действительно, если занумеровать предметы числами от 1 до n и затем записывать в строку номера выбираемых предметов, то мы как раз получим строку длины k, заполненную числами от 1 до n. Обозначается число размещений из n по k через $(n)_k$.

Некоторое смущение может вызвать это определение при $n = 0$ или $k = 0$. Принято считать, что $(n)_0 = 1$ для всех n, включая 0. Объяснение

таково: есть ровно один способ взять нуль предметов — не взять ничего. Также формально полагают, что $(n)_k = 0$ при $k > n$: нельзя выбрать десять предметов из пяти! Часто вместо $(n)_k$ пишут через A_n^k, но мы предпочитаем указанное выше обозначение; оно сейчас становится всё более популярным.

Это определение не даёт возможности быстро посчитать, чему равно, например, $(2013)_{500}$. Вообще, для любого комбинаторного объекта естественный вопрос — как его «посчитать». Иногда, для некоторых объектов, получение явной формулы — очень непростая задача, но для чисел размещений это совсем не сложно.

Действительно, $(n)_1 = n$ — можно взять любой предмет, $(n)_2 = n(n-1)$, так как первый предмет можно выбрать n способами (взять любой), а если первый предмет уже выбран, то второй можно выбрать $n-1$ способом — взять любой из оставшихся. Аналогично

$$(n)_k = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n-k+1)$$

для любого k. Заметим, что если для любого натурального m обозначить $m! = 1 \cdot 2 \cdot \ldots \cdot m$ (читается «эм факториал») и положить $0! = 1$, то

$$(n)_k = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1) \cdot (n-k) \cdot (n-k-1) \cdot \ldots \cdot 1}{(n-k) \cdot (n-k-1) \cdot \ldots \cdot 1} = \frac{n!}{(n-k)!}.$$

Упражнение 1.1. i) Докажите, что $n \cdot (n)_k = (n)_{k+1} + k \cdot (n)_k$.

ii) Покажите, что

$$(0)_m + (1)_m + \ldots + (n-1)_m = \frac{(n)_{m+1}}{m+1}.$$

Число сочетаний из n по k — это количество способов выбрать k предметов из n разных предметов, если нам не важен порядок, в котором они выбираются. Обозначение: $\binom{n}{k}$.

Как и для чисел размещений, $\binom{n}{0} = 1$, ибо есть только один способ взять нуль предметов — не взять ничего; кроме того, $\binom{n}{k} = 0$ при $k > n$. Часто для чисел сочетаний используется обозначение C_n^k.

Понятно, что

$$\binom{n}{n} = \binom{n}{0} = 1,$$

так как есть один способ выбрать n предметов из n предметов — взять всё. Далее,

$$\binom{n}{1} = \binom{n}{n-1} = n.$$

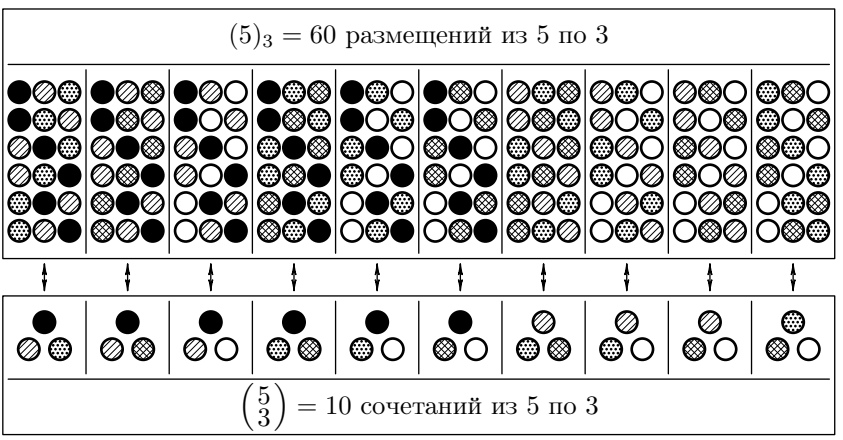
В самом деле, есть ровно n способов выбрать один предмет из n: взять любой. Но выбрать $n-1$ предмет из n предметов — это то же самое, что

не выбрать один, откуда и получаем требуемое равенство. Вообще,

$$\binom{n}{k} = \binom{n}{n-k}$$

для любого k, так как выбрать k предметов — это то же самое, что не выбрать $n-k$ оставшихся.

Числа сочетаний тоже несложно посчитать явно. Действительно, мы уже знаем, сколько способов выбрать k предметов из n предметов, если нам важен порядок — это как раз число размещений из n по k. Разные размещения могут задавать одно и то же сочетание, если они отличаются лишь порядком следования выбранных предметов. Точнее, если у нас есть какое-то фиксированное размещение, то оно будет задавать такое же сочетание, как и все, которые получаются из него любой перестановкой выбранных предметов. Пусть, например, $n=5$, $k=3$. На рисунке показано, какие размещения соответствуют одним и тем же сочетаниям.



Но есть всего $k!$ способов переставить k выбранных разных предметов (почему?), так что

$$\binom{n}{k} = \frac{(n)_k}{k!} = \frac{n\cdot(n-1)\cdot\ldots\cdot(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}. \qquad (1)$$

Обратим внимание, что из этой формулы тоже сразу получается равенство $\binom{n}{k} = \binom{n}{n-k}$ (почему?).

Упражнение 1.2 (треугольник Паскаля). i) Докажите, что для любого $n \geqslant 1$ и для любого k от 1 до $n-1$

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

ii) Докажите эту формулу ещё раз, не прибегая к явной формуле для чисел сочетаний, а используя лишь их первоначальное комбинаторное определение.

Эта формула называется формулой треугольника Паскаля по следующим причинам. Будем строить бесконечный треугольник из чисел по такому правилу: в самой верхней строке поставим единицу, в следующей — две единицы. В каждой следующей строке будет на одно число больше, чем в предыдущей; числа будем располагать симметрично относительно середины строки. По краям будем ставить единицы, а каждое число, кроме крайних, будет равно сумме двух стоящих над ним. Несколько первых строк треугольника выглядят так:

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}$$

Занумеруем строки этого треугольника неотрицательными целыми числами сверху вниз, тогда в n-й строке будет $n+1$ число; занумеруем их слева направо числами от 0 до n. Крайние числа равны единице; для любого $n \geqslant 0$ и любого k от 0 до n число, стоящее в этом треугольнике в n-й строке на k-й позиции, равно числу сочетаний из n по k. К примеру, $\binom{5}{2} = 10$. Этот бесконечный треугольник называется треугольником Паскаля.

Упражнение 1.3 (бином Ньютона). Докажите, что для $n \geqslant 0$

$$(x+y)^n = \binom{n}{0}x^n y^0 + \binom{n}{1}x^{n-1}y^1 + \binom{n}{2}x^{n-2}y^2 + \ldots + \binom{n}{n}x^0 y^n.$$

Указание. Используйте комбинаторное определение чисел сочетаний.

При небольших n формула бинома Ньютона называется «формулой сокращённого умножения»; к примеру, при $n = 2$ она гласит, что

$$(x+y)^2 = \binom{2}{0}x^2y^0 + \binom{2}{1}x^1y^1 + \binom{2}{2}x^0y^2 = x^2 + 2xy + y^2.$$

Вместе с треугольником Паскаля это даёт довольно быстрый алгоритм возведения в степень; например,

$$(x+y)^5 = x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5.$$

Из-за важности бинома Ньютона числа сочетаний иногда называют даже биномиальными коэффициентами. Мы сейчас рассмотрим чисто алгебра-

ическое доказательство, использующее лишь формулу (1) и треугольник Паскаля — это нужно будет нам в следующем параграфе.

Утверждение 1.4. *Формула бинома Ньютона верна.*

Доказательство. Используем индукцию по n. База индукции $n = 0$ очевидна: любой многочлен в нулевой степени равен единице, так что формула принимает вид $1 = 1$. Если это кажется «трюком», то можно стартовать с $n = 1$, где формула тоже очевидна: $x + y = x + y$.

Предположим теперь, что для $n - 1$ формула уже доказана. Тогда

$$\begin{aligned}(x+y)^n &= (x+y)\cdot(x+y)^{n-1} = (x+y)\times\\ &\times\left(\binom{n-1}{0}x^{n-1}y^0 + \binom{n-1}{1}x^{n-2}y^1 + \ldots + \binom{n-1}{n-1}x^0y^{n-1}\right) =\\ &= \binom{n-1}{0}x^ny^0 + \binom{n-1}{1}x^{n-1}y^1 + \ldots + \binom{n-1}{n-1}x^1y^{n-1} +\\ &+ \binom{n-1}{0}x^{n-1}y^1 + \binom{n-1}{1}x^{n-2}y^2 + \ldots + \binom{n-1}{n-1}x^0y^n =\\ &= x^n + \left(\binom{n-1}{1} + \binom{n-1}{0}\right)x^{n-1}y^1 + \ldots +\\ &+ \left(\binom{n-1}{n-1} + \binom{n-1}{n-2}\right)x^1y^{n-1} + y^n.\end{aligned}$$

Остаётся использовать треугольник Паскаля. □

Упражнение 1.5. i) Покажите, что

$$\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n} = 2^n.$$

ii) Докажите это, используя только комбинаторное определение чисел сочетаний. Подсказка: сколько всего существует последовательностей из плюсов и минусов длины n?

iii) Проверьте, что

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \ldots = 0.$$

iv) Убедитесь в верности равенства

$$1\cdot\binom{n}{1} + 2\cdot\binom{n}{2} + \ldots + n\cdot\binom{n}{n} = n\cdot 2^{n-1}.$$

v) Докажите, что

$$\binom{n}{0}\binom{m}{k} + \binom{n}{1}\binom{m}{k-1} + \ldots + \binom{n}{k}\binom{m}{0} = \binom{n+m}{k}.$$

Конечно, всё это только верхушка айсберга. Комбинаторика развивается невероятно быстро и имеет огромное количество эффектных приложений в современной алгебре, геометрии, анализе, теории графов и в ряде других областей современной математики. У нас нет никакой возможности изложить здесь даже все элементарные и абсолютно классические сведения про числа сочетаний и размещений. (Так, мы совершенно не касаемся красивейшей и очень полезной интерпретации в терминах путей на клетчатой бумаге.) Ограничимся лишь ссылками на несколько учебников. Элементарные комбинаторные методы чётко изложены в книге [1]. Полезное обсуждение алгоритмических аспектов основных комбинаторных понятий содержится в [13]. Мы горячо рекомендуем всем *великолепную* книгу [3], в которой комбинаторика предстаёт чрезвычайно эффективным орудием решения самых разнообразных алгебраических и геометрических проблем.

На более высоком уровне комбинаторные аспекты алгебры освещаются в фундаментальном учебнике [14] — разумеется, *не* предназначенном для первого знакомства с предметом. Отдельного восхищения заслуживает глава про «каталанову болезнь», в которой собрано несколько *сотен* интерпретаций знаменитых чисел Каталана; см. по этому поводу также статью [5, 6]. Наконец, очень понятное и быстрое введение в теорию производящих функций приведено в [11]. Все эти книги мы непременно советуем прочесть (пусть не сразу!) тем, кто действительно хочет овладеть современными комбинаторными и алгоритмическими методами.

§ 2. Квантовые аналоги

Перейдём к определению интересующих нас объектов. Термин «квантовый» действительно связан с квантовой физикой. Дело в том, что в классической механике может существовать любая, сколь угодно малая порция энергии. Напротив, с точки зрения квантовой теории, электрон на данной длине волны не может излучать энергии порциями, которые меньше известной константы, которая обозначается $\hbar$ и называется *постоянной Планка*. В ряде формул удобно использовать обозначение $q = e^{\hbar}$.

Часть классической механики может быть получена из квантовой «предельным переходом» при $\hbar \to 0$; при этом $q \to 1$. Таким образом, в первом приближении квантовый объект можно понимать как некую «деформацию» классического объекта, так зависящую от параметра q, что при $q = 1$ мы получаем исходный классический объект.

Все эти невнятные объяснения мы сейчас наполним вполне прозрачным смыслом в конкретных случаях. Больше мы не станем вдаваться в причины использования «квантовой» терминологии; краткие коммента-

рии по поводу связи квантовой комбинаторики с глубокими разделами современной теоретической физики приведены в предисловии.

Определение 2.1. *Квантовым аналогом* натурального числа n называется многочлен от переменной q вида

$$[n] = 1 + q + q^2 + \ldots + q^{n-1}.$$

Синонимы: квантовое число n, q-аналог числа n. Используются также обозначения n_q и $[n]_q$, но у нас q всегда будет просто переменной, так что мы не будем указывать его в обозначениях. Положим также $[0] = 1$.

Отметим, что $[n] = n$ при $q = 1$, то есть 1-аналог равен обычному числу n. Многочлен $[n]$ можно представить в более компактной форме:

$$[n] = \frac{q^n - 1}{q - 1}.$$

Также его легко вычислить для небольших n: $[1] = 1$, $[2] = 1 + q$, и так далее. Теперь — ключевой момент: мы можем «имитировать» определение обычного факториала, используя квантовые числа вместо обычных.

Определение 2.2. Пусть n — любое натуральное число. *Квантовым факториалом* называется многочлен от переменной q вида

$$[n]! = [1] \cdot [2] \cdot \ldots \cdot [n].$$

Синонимы: квантовый аналог факториала, q-факториал. Формально определим $[0]! = 1$.

Подчеркнём, что, вообще говоря, $[n!] \neq [n]!$. К примеру, $[3!] = [6]$ — многочлен пятой степени, в то время как $[3]! = [1] \cdot [2] \cdot [3]$ — многочлен всего лишь третьей степени.

Упражнение 2.3. i) Для каких чисел a и b будет верно равенство

$$[a] \cdot [b] = [ab]?$$

ii) Докажите, что для любых n, k

$$[n] = [k] + q^k \cdot [n-k] = [n-k] + q^{n-k} \cdot [k].$$

Обратите внимание на последнюю формулу. Ясно, что при $q = 1$ она превращается в два очевидных равенства:

$$n = k + (n-k) = (n-k) + k.$$

При этом квантовая формула отличается от классической добавлением «квантовых поправок» — степеней q — к некоторым слагаемым.

Определение 2.4. Для $n \geqslant 0$, $0 \leqslant k \leqslant n$ *квантовым числом размещений из* n *по* k называется многочлен от переменной q вида

$$[n]_k = [n] \cdot [n-1] \cdot \ldots \cdot [n-k+1] = \frac{[n]!}{[n-k]!}.$$

Определим также *квантовое число сочетаний из* n *по* k как частное двух многочленов вида

$$\begin{bmatrix} n \\ k \end{bmatrix} = \frac{[n]_k}{[k]!} = \frac{[n] \cdot [n-1] \cdot \ldots \cdot [n-k+1]}{[k]!} = \frac{[n]!}{[k]![n-k]!}.$$

Пока непонятно, делится ли числитель на знаменатель, то есть является ли квантовое число сочетаний настоящим многочленом с целыми коэффициентами. Впрочем, если изначально определить обычное число сочетаний формулой (1), то доказать, что это целое число, тоже не так-то просто. Отметим пока, что при $q = 1$ квантовые числа сочетаний и размещений превращаются в обычные. Кроме того, выполняются очевидные равенства

$$\begin{bmatrix} n \\ 0 \end{bmatrix} = \begin{bmatrix} n \\ n \end{bmatrix} = 1$$

и, шире, для любого k

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n \\ n-k \end{bmatrix}.$$

Собственно, пафос квантовой науки заключается в следующем: теперь, когда мы определили квантовые аналоги классических комбинаторных объектов, оказывается, что *все* классические тождества допускают квантовые аналоги! Другими словами, для классического тождества всегда можно придумать тождество с квантовыми числами сочетаний и размещений, которое отличается от обычного квантовыми поправками и превращается в обычное при подстановке $q = 1$. Таким образом, вся классическая комбинаторика, имеющая дело с числами сочетаний и размещений, включается в грандиозную программу квантовой комбинаторики как очень частный случай. Перейдём к конкретным фактам.

Упражнение 2.5. i) Докажите квантовый аналог формулы из упражнения 1.1 (i):

$$[n] \cdot [n]_k = [n]_{k+1} + q^{n-k} \cdot [k] \cdot [n]_k.$$

ii) (Квантовый треугольник Паскаля.) Докажите, что для любого k от 1 до $n-1$

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k \end{bmatrix} + q^{n-k} \cdot \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} = q^k \cdot \begin{bmatrix} n-1 \\ k \end{bmatrix} + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}.$$

Следствие 2.6. *Квантовое число сочетаний является многочленом от переменной q с целыми коэффициентами.*

Доказательство. Вытекает из формулы для квантового треугольника Паскаля. □

Чтобы квантовать второе важнейшее тождество с числами сочетаний и размещений — бином Ньютона, — требуется ещё пара определений.

Определение 2.7. Определим *n-ю квантовую степень* как многочлен с целыми коэффициентами от переменных x, y, q вида

$$[x+y]^n = (x+y)\cdot(x+qy)\cdot(x+q^2y)\cdot\ldots\cdot(x+q^{n-1}y)$$

(обратите внимание, что $[x+y]^n \neq [y+x]^n$). Положим формально

$$[x+y]^0 = 1.$$

Упражнение 2.8 (квантовый бином Ньютона). Покажите, что для любого $n \geqslant 0$

$$[x+y]^n = q^{0\cdot(-1)/2}\begin{bmatrix} n \\ 0 \end{bmatrix} x^n y^0 + q^{1\cdot 0/2}\begin{bmatrix} n \\ 1 \end{bmatrix} x^{n-1}y^1 + q^{2\cdot 1/2}\begin{bmatrix} n \\ 2 \end{bmatrix} x^{n-2}y^2 + \\ + \ldots + q^{k\cdot(k-1)/2}\begin{bmatrix} n \\ k \end{bmatrix} x^{n-k}y^k + \ldots + q^{n\cdot(n-1)/2}\begin{bmatrix} n \\ n \end{bmatrix} x^0 y^n.$$

Указание. Действуйте, как в доказательстве утверждения 1.4.

Есть и другой способ квантовать бином Ньютона, связанный ещё с одной фундаментальной идеей квантовой физики — идеей некоммутативности (подробности см. в последнем параграфе). А именно, будем считать, что x и y — это не обычные переменные, связанные соотношением $xy = yx$, а «буквы» в «алфавите» некоего нового «языка», слова которого записаны этими буквами. Тогда $x^2y = xxy$ и $yx^2 = yxx$ — это, конечно, разные слова.

Будем предполагать, что грамматические правила этого «языка» позволяют в любом слове две подряд идущие буквы yx заменить на буквы xy, но при этом «умножить» слово на q, то есть просто приписать перед словом букву q. Если считать, что букву q можно свободно «протаскивать» через все остальные буквы, то кратко это правило можно выразить так:

$$yx = qxy.$$

Например,

$$y^2x^3 = q^6x^3y^2.$$

Можно определить «сложение» и «умножение» слов более или менее очевидными формальными правилами (вдаваться в детали мы сейчас не станем). К примеру,

$$(x+y)^2 = (x+y)\cdot(x+y) = x^2 + xy + yx + y^2 = x^2 + (1+q)xy + y^2.$$

Упражнение 2.9 (квантовый бином Ньютона, некоммутативная версия). Докажите, что при таком определении

$$(x+y)^n = \begin{bmatrix} n \\ 0 \end{bmatrix} x^n y^0 + \begin{bmatrix} n \\ 1 \end{bmatrix} x^{n-1} y^1 + \ldots + \begin{bmatrix} n \\ n \end{bmatrix} x^0 y^n.$$

Таким образом, можно обойтись даже без квантовых поправок, если пожертвовать коммутативностью умножения переменных.

§ 3. Комбинаторная интерпретация

Мы только что видели, что два важнейших тождества — треугольник Паскаля и бином Ньютона — допускают изящные квантовые переформулировки. Неприятным моментом является то, что квантовые числа сочетаний и размещений пока определяются чисто алгебраически, в то время как в классической ситуации числа сочетаний и размещений перечисляют некоторые объекты. Как мы сейчас увидим, квантовым аналогам тоже можно дать весьма изящную комбинаторную трактовку, которая в каком-то смысле является квантованием классического комбинаторного определения.

Обозначим через $\mathcal{A}_{n,k}$ множество k-элементных подмножеств множества $\{1, 2, \ldots, n\}$; таким образом, просто по определению, $|\mathcal{A}_{n,k}| = \binom{n}{k}$. Для каждого подмножества $S \subset \{1, 2, \ldots, n\}$ будем через $w(S)$ обозначать сумму чисел, входящих в это подмножество. Например,

$$w(\{2, 4, 5\}) = 11, \quad w(\varnothing) = 0.$$

Предложение 3.1. *Имеет место формула*

$$\begin{bmatrix} n \\ k \end{bmatrix} = \sum_{S \in \mathcal{A}_{n,k}} q^{w(S) - \frac{k(k+1)}{2}}.$$

Доказательство. Будем доказывать формулу индукцией по n. База индукции $n = 0$ проверяется тривиально: при единственном возможном значении $k = 0$ формула имеет вид $1 = 1$, так как $w(\varnothing) = 0$. Предположим, что для $n - 1$ формула уже доказана. При $k = 0$ она очевидно верна (ибо имеет вид $1 = 1$), так что дальше можно считать, что $k > 0$.

Разобьём все подмножества из $\mathcal{A}_{n,k}$ на две части, $\mathcal{A}_1$ и $\mathcal{A}_2$. В первую поместим те, в которых содержится n, а во вторую — те, в которых n не содержится. Например, при $n = 4$, $k = 2$ эти части устроены так:

$$\mathcal{A}_1 = \{\{1, 4\}\ , \{2, 4\},\ \{3, 4\}\},$$
$$\mathcal{A}_2 = \{\{1, 2\},\ \{1, 3\},\ \{2, 3\}\}.$$

Вторая часть пуста при $k = n$; в этом случае формула проверяется очень легко. Действительно, при $k = n$ левая часть формулы равна $\begin{bmatrix} n \\ n \end{bmatrix} = 1$, а правая часть равна

$$q^{w(\{1,\ldots,n\})-\frac{n(n+1)}{2}} = q^0 = 1.$$

Итак, дальше можно считать, что $k < n$.

Если из любого подмножества S из $\mathcal{A}_1$ выкинуть n, то получится $(k-1)$-элементное подмножество S' множества $\{1, \ldots, n-1\}$. Ясно, что это задаёт взаимно однозначное соответствие между $\mathcal{A}_1$ и $\mathcal{A}_{n-1,\,k-1}$, причём $w(S) = w(S') + n$. С другой стороны, множество $\mathcal{A}_2$ просто совпадает с $\mathcal{A}_{n-1,\,k}$. Таким образом, правая часть доказываемого равенства имеет вид

$$\sum_{S\in\mathcal{A}_{n,k}} q^{w(S)-\frac{k(k+1)}{2}} = \sum_{S\in\mathcal{A}_1} q^{w(S)-\frac{k(k+1)}{2}} + \sum_{S\in\mathcal{A}_2} q^{w(S)-\frac{k(k+1)}{2}} =$$

$$= \sum_{S'\in\mathcal{A}_{n-1,\,k-1}} q^{w(S')+n-\frac{k(k+1)}{2}} + \sum_{S\in\mathcal{A}_{n-1,\,k}} q^{w(S)-\frac{k(k+1)}{2}}.$$

Заметим, что

$$\frac{k(k+1)}{2} = \frac{k(k-1)}{2} + k,$$

поэтому

$$q^{w(S')+n-\frac{k(k+1)}{2}} = q^{n-k}\cdot q^{w(S')-\frac{k(k-1)}{2}}.$$

Значит, правая часть доказываемого равенства переписывается в виде

$$q^{n-k}\sum_{S'\in\mathcal{A}_{n-1,\,k-1}} q^{w(S')-\frac{k(k-1)}{2}} + \sum_{S\in\mathcal{A}_{n-1,\,k}} q^{w(S)-\frac{k(k+1)}{2}}.$$

По предположению индукции, первое и второе слагаемые равны соответственно $q^{n-k}\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}$ и $\begin{bmatrix} n-1 \\ k \end{bmatrix}$. Для завершения доказательства осталось использовать квантовый треугольник Паскаля. □

Обратим внимание, что при $q = 1$ левая часть будет равна просто $\binom{n}{k}$. В то же время правая часть будет иметь вид

$$\sum_{\mathcal{A}_{n,k}} q^0 = \sum_{\mathcal{A}_{n,k}} 1 = |\mathcal{A}_{n,k}|$$

— и мы видим, что это комбинаторное определение чисел сочетаний!

Пусть, далее, $\mathcal{B}_{n,k}$ — множество строк длины k, заполненных числами от 1 до n, то есть, в частности, $|\mathcal{B}_{n,k}| = (n)_k$. Для каждой строки T, заполненной числами от 1 до n, будем через $w(T)$ обозначать сумму чисел

в ней, а через $N(T)$ — количество инверсий в T. Напомним, что *инверсией* в строке T называется такая пара чисел i, j, встречающаяся в ней, что $i > j$, но при этом число i появляется в T раньше, чем число j. К примеру, полный список инверсий в строке $T = (3, 4, 1, 5, 2)$ выглядит так: $(3, 1)$, $(3, 2)$, $(4, 1)$, $(4, 2)$, $(5, 2)$, поэтому $N(T) = 5$.

Предложение 3.2. *Имеет место формула*

$$[n]_k = \sum_{T \in \mathcal{B}_{n,k}} q^{w(T)+N(T)-\frac{k(k+1)}{2}}.$$

Доказательство. Опять используем индукцию по n (база $n = 0$ очевидна). Предположим, что формула уже доказана для $n - 1$. Как и в прошлом доказательстве, поделим все строки из $\mathcal{B}_{n,k}$ на две части, $\mathcal{B}_1$ и $\mathcal{B}_2$. В первую часть поместим те, в которых встречается число n, а во вторую — те, в которых оно не встречается. К примеру, при $n = 3$, $k = 2$ эти части будут выглядеть так:

$$\mathcal{B}_1 = \{\{1, 3\}, \{3, 1\},\ \{2, 3\},\ \{3, 2\}\}, \quad \mathcal{B}_2 = \{\{1, 2\},\ \{2, 1\}\}.$$

При $k = n$ во второй части нет ни одной строки, но это никак не отразится на ходе рассуждений.

Если из любой строки из $\mathcal{B}_1$ удалить число n, то получится строка из $\mathcal{B}_{n-1,\,k-1}$. Обозначим полученное отображение через

$$r\colon \mathcal{B}_1 \to \mathcal{B}_{n-1,\,k-1}.$$

Ясно, что таким образом можно получить любую строку из $\mathcal{B}_{n-1,\,k-1}$.

Более того, пусть T' — какая-то фиксированная строка длины $k - 1$. Какие строки переходят в неё под действием отображения r? Мы можем добавить n перед всей строкой T', после первого её символа, после второго, и так далее, вплоть до последней возможности — добавить n после всей строки T. Значит, есть всего k строк T длины k таких, что $r(T) = T'$. Обозначим их $T_0, T_1, \ldots, T_{k-1}$ в зависимости от того, после какой позиции строки T' добавляется n.

Заметим, что сумма чисел в любой из этих строк на n больше, чем в строке T. Кроме того, в строке T_0 на $k - 1$ инверсию больше, чем в строке T', потому что число n образует инверсию с любым числом, идущим после него. В строке T_1 на $k - 2$ инверсии больше, чем в строке T' по тем же причинам (число n не образует инверсию ни с одним числом, идущим раньше него). Рассуждая аналогично, получим, что

$$\sum_{\substack{T \in \mathcal{B}_1 \\ r(T)=T'}} q^{w(T)+N(T)} = q^{w(T_0)+N(T_0)} + q^{w(T_1)+N(T_1)} + \ldots + q^{w(T_{k-1})+N(T_{k-1})} =$$

$$= q^{w(T')+n+N(T')+(k-1)} + q^{w(T')+n+N(T')+(k-2)} + \ldots + q^{w(T')+n+N(T')+0} =$$
$$= q^n \cdot (q^{k-1} + q^{k-2} + \ldots + 1) \cdot q^{w(T')+N(T')} = q^n \cdot [k] \cdot q^{w(T')+N(T')}.$$

Осталось заметить, что $\mathcal{B}_2$ — это в точности множество $\mathcal{B}_{n-1,\,k}$. С учётом сделанных выше замечаний и предположения индукции правая часть доказываемого равенства переписывается в виде

$$\sum_{T\in\mathcal{B}_{n,k}} q^{w(T)+N(T)-\frac{k(k+1)}{2}} =$$
$$= \sum_{T\in\mathcal{B}_1} q^{w(T)+N(T)-\frac{k(k+1)}{2}} + \sum_{T\in\mathcal{B}_2} q^{w(T)+N(T)-\frac{k(k+1)}{2}} =$$
$$= q^{-\frac{k(k+1)}{2}} \sum_{T\in\mathcal{B}_1} q^{w(T)+N(T)} + \sum_{T\in\mathcal{B}_{n-1,\,k}} q^{w(T)+N(T)-\frac{k(k+1)}{2}} =$$
$$= q^{-\frac{k(k-1)+2k}{2}} \sum_{T'\in\mathcal{B}_{n-1,\,k-1}} \left(\sum_{T\in\mathcal{B}_1,\ r(T)=T'} q^{w(T)+N(T)} \right) + [n-1]_k =$$
$$= q^{-k} \cdot q^{-\frac{k(k-1)}{2}} \sum_{T'\in\mathcal{B}_{n-1,\,k-1}} \left(q^n \cdot [k] \cdot q^{w(T')+N(T')}\right) + [n-1]_k =$$
$$= q^{n-k} \cdot [k] \sum_{T'\in\mathcal{B}_{n-1,\,k-1}} q^{w(T')+N(T')-\frac{k(k-1)}{2}} + [n-1]_k =$$
$$= q^{n-k}[k][n-1]_{k-1} + [n-1]_k =$$
$$= [n-1]_{k-1} \cdot (q^{n-k}[k] + [n-k]) = [n][n-1]_k = [n]_k,$$

что и требовалось доказать. Предпоследнее равенство вытекает из упражнения 2.5 (ii). □

§ 4. Векторные пространства над конечными полями

Как мы позже увидим, квантовые числа сочетаний и размещений допускают очень красивую и полезную *геометрическую* интерпретацию при правильном понимании термина «геометрическая». Эта интерпретация позволяет доказывать квантовые аналоги классических тождеств с помощью подсчёта тех или иных конфигураций подпространств в векторных пространствах над конечными полями, к определению которых мы и переходим.

Определение 4.1. *Полем* называется произвольное непустое множество $\mathbb{F}$ вместе с двумя *бинарными операциями*, удовлетворяющими некоторым условиям. Каждая бинарная операция — это отображение из $\mathbb{F} \times \mathbb{F}$

в $\mathbb{F}$. Другими словами, это правило, которое каждой упорядоченной паре элементов (x, y) из $\mathbb{F}$ ставит в соответствие какой-то новый элемент из $\mathbb{F}$. Будем обозначать этот элемент через $x + y$ для первой операции и через xy — для второй. Вот свойства, которым должны удовлетворять эти бинарные операции:

1) $(x + y) + z = x + (y + z)$ для любых $x, y, z \in \mathbb{F}$;
2) существует элемент $0 \in \mathbb{F}$ такой, что $0 + x = x$ для любого $x \in \mathbb{F}$;
3) для любого $x \in \mathbb{F}$ существует элемент $-x \in \mathbb{F}$ такой, что $x + (-x) = 0$;
4) $x + y = y + x$ для любых $x, y \in \mathbb{F}$;
5) $(xy)z = x(yz)$ для любых $x, y, z \in \mathbb{F}$;
6) существует элемент $1 \neq 0$ такой, что $1x = x$ для любого $x \in \mathbb{F}$;
7) для любого $x \neq 0$ существует элемент $x^{-1} \in \mathbb{F}$ такой, что $xx^{-1} = 1$;
8) $xy = yx$ для любых $x, y \in \mathbb{F}$;
9) $x(y + z) = xy + xz$ для любых $x, y, z \in \mathbb{F}$.

Скобки обозначают порядок выполнения операций — сначала выполняется действие в скобках. Первая бинарная операция называется *сложением*, а вторая — *умножением*. Первое и пятое свойства называют *ассоциативностью* сложения и умножения соответственно; элементы 0 и 1 называются *нулём* и *единицей* соответственно. Для любого $x \in \mathbb{F}$ элементы $-x$ и x^{-1} называются *противоположным* и *обратным* к x соответственно.

Упражнение 4.2. Докажите, что $0x = 0$ и $(-1)x = -x$ для любого $x \in \mathbb{F}$.

Пример 4.3. i) Множество рациональных чисел $\mathbb{Q}$ и множество вещественных чисел $\mathbb{R}$ являются полями. Обратим внимание, что строгое определение этих множеств весьма нетривиально; интересующегося читателя отсылаем к книге [4].

ii) Рассмотрим произвольное простое число p. Для любого целого a будем через $a \bmod p$ обозначать остаток от деления a на p. Пусть

$$\mathbb{F}_p = \{0, 1, \ldots, p - 1\}.$$

Введём на этом множестве бинарные операции следующим правилом:

$$x + y = x + y \mod p, \qquad xy = xy \mod p.$$

Упражнение 4.4. i) Докажите, что эти бинарные операции превращают $\mathbb{F}_p$ в поле.

ii) Постройте таблицы умножения для $\mathbb{F}_5$ и $\mathbb{F}_7$.

Таким образом, поля не обязаны состоять из бесконечного числа элементов, как $\mathbb{Q}$ и $\mathbb{R}$. Более тонкий вопрос — сколько элементов может быть

в конечном поле? Оказывается, число элементов в нём всегда является степенью простого числа [10, гл. 5, § 2, предложение 2], но мы для простоты ограничимся случаем, когда количество элементов поля — простое число.

Упражнение 4.5. Введите на множестве из четырёх элементов две бинарные операции, которые превратят его в поле.

Определение 4.6. Пусть $\mathbb{F}$ — любое поле. Договоримся называть его элементы *числами*. Векторным пространством над полем $\mathbb{F}$ называется непустое множество V вместе с отображениями

$$V \times V \to V\colon (\bar{x}, \bar{y}) \mapsto \bar{x} + \bar{y},$$
$$\mathbb{F} \times V \to V\colon (\alpha, \bar{x}) \mapsto \alpha\bar{x}.$$

Они называются соответственно *сложением* и *умножением на числа* и должны удовлетворять следующим свойствам:

1) $(\bar{x} + \bar{y}) + \bar{z} = \bar{x} + (\bar{y} + \bar{z})$ для любых $\bar{x}, \bar{y}, \bar{z} \in V$;
2) существует $\overline{0} \in V$ такой, что $\bar{x} + \overline{0} = \bar{x}$ для любого $\bar{x} \in V$;
3) для любого $\bar{x} \in V$ существует $-\bar{x} \in V$, для которого $\bar{x} + (-\bar{x}) = \overline{0}$;
4) $\bar{x} + \bar{y} = \bar{y} + \bar{x}$ для любых $\bar{x}, \bar{y} \in V$;
5) $\alpha(\beta\bar{x}) = (\alpha\beta)\bar{x}$ для любых $\bar{x} \in V$, $\alpha, \beta \in \mathbb{F}$;
6) $(\alpha + \beta)\bar{x} = \alpha\bar{x} + \beta\bar{x}$ для любых $\bar{x} \in V$, $\alpha, \beta \in \mathbb{F}$;
7) $\alpha(\bar{x} + \bar{y}) = \alpha\bar{x} + \alpha\bar{y}$ для любых $\bar{x}, \bar{y} \in V$, $\alpha \in \mathbb{F}$;
8) $1\bar{x} = \bar{x}$ для любого $\bar{x} \in V$.

Мы будем называть элементы множества V *векторами* и писать над ними чёрточки, чтобы отличать их от чисел из поля $\mathbb{F}$. Вектор $\overline{0}$ называется *нулевым*. Для любого $\bar{x} \in V$ вектор $-\bar{x}$ называется *противоположным* к $\bar{x}$.

Упражнение 4.7. Докажите, что $0\bar{x} = \overline{0}$ и $(-1)\bar{x} = -\bar{x}$ для любого вектора $\bar{x} \in V$.

Пример 4.8. i) Пусть $\mathbb{F} = \mathbb{R}$, V — множество обычных (*геометрических*) векторов на плоскости E^2 или в пространстве E^3, отложенных от какой-то фиксированной точки O. Сложение и умножение на числа определяются так же, как в школьном курсе геометрии.

ii) Пусть $\mathbb{F}$ — любое поле,

$$V = \mathbb{F}^n = \left\{ \bar{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix},\ x_i \in \mathbb{F} \right\}$$

— *n-мерное координатное пространство*, то есть просто множество упорядоченных наборов из n элементов поля $\mathbb{F}$. Сложение векторов и умножение

на числа определяются покоординатно:

$$\bar{x}+\bar{y}=\begin{pmatrix} x_1+y_1 \\ \vdots \\ x_n+y_n \end{pmatrix}, \quad \lambda\bar{x}=\begin{pmatrix} \lambda x_1 \\ \vdots \\ \lambda x_n \end{pmatrix}, \quad \bar{x},\bar{y}\in V,\ \lambda\in\mathbb{F}.$$

iii) Множество многочленов от переменной x с коэффициентами из поля $\mathbb{F}$ является векторным пространством; оно обозначается $\mathbb{F}[x]$. Сложение многочленов и умножение их на числа определяются очевидным образом. Можно также рассмотреть пространство $\mathbb{F}_n[x]$ многочленов степени не выше n.

iv) Рассмотрим множество *квадратных матриц* — таблиц размера $n\times n$, заполненных числами из поля $\mathbb{F}$:

$$V=\operatorname{Mat}_n(\mathbb{F})=\left\{ A=\begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \dots & a_{n,n} \end{pmatrix},\ a_{i,j}\in\mathbb{F} \right\}.$$

Оно является векторным пространством относительно поэлементного сложения и умножения на числа.

Векторы $\bar{v}_1,\dots,\bar{v}_n\in V$ называются *линейно независимыми*, если из того, что $\alpha_1\bar{v}_1+\ldots+\alpha_n\bar{v}_n=\bar{0}$ для каких-то $\alpha_1,\dots\alpha_n\in\mathbb{F}$, следует, что все α_i равны нулю. В противном случае векторы называются *линейно зависимыми*.

Пример 4.9. Один вектор является линейно зависимым тогда и только тогда, когда он нулевой. Два вектора будут линейно зависимыми в том и только в том случае, когда они пропорциональны, то есть один получается из другого умножением на какое-то число из поля $\mathbb{F}$. Если V — это пространство геометрических векторов на плоскости E^2, то это равносильно коллинеарности векторов. Любые три вектора на плоскости линейно зависимы (почему?). Если же V — пространство геометрических векторов в E^3, то три вектора будут линейно независимыми тогда и только тогда, когда они не лежат в одной плоскости, а четыре вектора линейно зависимы всегда (почему?).

Набор линейно независимых векторов $e=\{\bar{e}_1,\dots,\bar{e}_n\}\subset V$ называется *базисом* в V, если любой вектор можно однозначно представить в виде линейной комбинации векторов из e, то есть для любого $\bar{x}\in V$ существуют единственные $x_1,\dots,x_n\in\mathbb{F}$ такие, что $\bar{x}=x_1\bar{e}_1+\ldots+x_n\bar{e}_n$; числа x_i называются *координатами* вектора $\bar{x}$ в базисе e. Если в V существует хоть один базис, состоящий из конечного числа векторов, то все базисы состоят из одного и того же числа векторов [9, гл. 1, § 2], которое обозначается $\dim V$ и называется *размерностью* V; само пространство V называется в этом случае *конечномерным*.

Можно показать, что размерность равна количеству векторов в любом максимальном по включению линейно независимом наборе векторов из V, причём любой такой набор является базисом V. (Термин «максимальный по включению» означает, что сам набор состоит из линейно независимых векторов, а при добавлении к нему любого вектора из V становится линейно зависимым.) Таким образом, размерность пространства — это максимально возможное количество линейно независимых векторов в нём.

Пример 4.10. Векторы $\bar{e}_i$, у которых на i-м месте стоит единица, а остальные координаты равны нулю, образуют базис $\mathbb{F}^n$, называемый *стандартным*. Таким образом, $\dim \mathbb{F}^n = n$. Матрицы $E_{i,j}$, у которых (i, j)-й элемент равен единице, а остальные — нулю (они называются *матричными единицами*), образуют базис $\mathrm{Mat}_n(\mathbb{F})$; тем самым, $\dim \mathrm{Mat}_n(\mathbb{F}) = n^2$. В пространстве $\mathbb{F}_n[x]$ есть *степенной* базис $\{1, x, x^2, \ldots, x^n\}$, поэтому $\dim \mathbb{F}_n[x] = n+1$. Напротив, в пространстве $\mathbb{F}[x]$ нельзя построить базис из конечного числа векторов, то есть это пространство бесконечномерно. Дальше мы везде будем рассматривать только конечномерные пространства.

Непустое подмножество $U \subset V$ называется *подпространством*, если оно замкнуто относительно операций сложения и умножения на числа, то есть $\bar{x} + \bar{y} \in U$ и $\alpha\bar{x} \in U$ для любых $\bar{x}, \bar{y} \in U$, $\alpha \in \mathbb{F}$. Любое подпространство само является векторным пространством относительно тех же операций, что и V. *Линейной оболочкой* набора векторов $S = \{\bar{a}_1, \ldots, \bar{a}_n\} \subset V$ называется минимальное по размерности подпространство $\langle S \rangle$, содержащее S; другими словами, это множество всех линейных комбинаций векторов из S:

$$\langle S \rangle = \{\alpha_1\bar{a}_1 + \ldots + \alpha_n\bar{a}_n, \alpha_i \in \mathbb{F}\}.$$

Говорят также, что линейная оболочка *натянута* на векторы $\bar{a}_1, \ldots, \bar{a}_n$. Имеет место *теорема о дополнении до базиса* [9, гл. 1, § 2, теорема 3(ii)]: базис любого подпространства $U \subset V$ всегда можно дополнить до базиса всего пространства V. В частности, $\dim U \leqslant \dim V$. Отметим, что если $\dim U = \dim V$, то $U = V$.

Здесь мы прерываем перечисление начальных фактов из теории векторных пространств. Мы не будем определять линейные отображения и операторы, потому что они нам нигде не будут нужны явно. По сути, геометрическая интерпретация q-аналогов квантовых тождеств основана на том простом факте, что в любом n-мерном пространстве над полем $\mathbb{F} = \mathbb{F}_q$ из q элементов ровно q^n векторов — это сразу вытекает из определения базиса и размерности. Мы увидим, что квантовые аналоги равны количеству подпространств определённой размерности, удовлетворяющих тем или иным дополнительным условиям.

§ 5. Геометрическая интерпретация

С этого момента и до конца статьи мы будем рассматривать векторные пространства только над конечным полем $\mathbb{F} = \mathbb{F}_q$ из q элементов. Сначала мы докажем простую, но очень полезную лемму, которая будет не раз использована дальше.

Лемма 5.1. *В n-мерном пространстве над $\mathbb{F}_q$ существует*

$$(q^n - 1) \cdot (q^n - q) \cdot (q^n - q^2) \cdot \ldots \cdot (q^n - q^{k-1})$$

наборов из k линейно независимых векторов.

Доказательство. Первый вектор можно выбрать любым, кроме нулевого, то есть для него есть $q^n - 1$ вариантов. Второй вектор можно взять любым, лишь бы он не лежал в одномерном подпространстве, натянутом на первый вектор, то есть для второго вектора есть $q^n - q$ вариантов. Аналогично третий вектор может быть любым вектором, не лежащим в двумерном подпространстве, натянутом на первые два вектора, то есть для него есть $q^n - q^2$ вариантов, и так далее. □

Теорема 5.2. *Квантовое число сочетаний $\begin{bmatrix} n \\ k \end{bmatrix}$ совпадает с количеством k-мерных подпространств в n-мерном пространстве над полем $\mathbb{F}_q$.*

Доказательство. Любое k-мерное подпространство однозначно определяется своим базисом, состоящим из k линейно независимых векторов. По только что доказанной лемме, количество таких базисов равно

$$(q^n - 1) \cdot (q^n - q) \cdot (q^n - q^2) \cdot \ldots \cdot (q^n - q^{k-1}).$$

С другой стороны, разные базисы могут задавать одно и то же подпространство. Точнее, чтобы получить число подпространств, нужно поделить записанное выше выражение на количество базисов в k-мерном пространстве, которое по той же самой лемме равно

$$(q^k - 1) \cdot (q^k - q) \cdot (q^k - q^2) \cdot \ldots \cdot (q^k - q^{k-1}).$$

Окончательно, всего k-мерных подпространств в n-мерном пространстве будет

$$\begin{aligned}
&\frac{(q^n - 1) \cdot (q^n - q) \cdot (q^n - q^2) \cdot \ldots \cdot (q^n - q^{k-1})}{(q^k - 1) \cdot (q^k - q) \cdot (q^k - q^2) \cdot \ldots \cdot (q^k - q^{k-1})} = \\
&\quad = \frac{(q^n - 1) \cdot q \cdot (q^{n-1} - 1) \cdot q^2 \cdot (q^{n-2} - 1) \cdot \ldots \cdot q^{k-1} \cdot (q^{n-k+1} - 1)}{(q^k - 1) \cdot q \cdot (q^{k-1} - 1) \cdot q^2 \cdot (q^{k-2} - 1) \cdot \ldots \cdot q^{k-1} \cdot (q - 1)} = \\
&\quad = \frac{(q^n - 1) \cdot (q^{n-1} - 1) \cdot (q^{n-2} - 1) \cdot \ldots \cdot (q^{n-k+1} - 1)}{(q^k - 1) \cdot (q^{k-1} - 1) \cdot (q^{k-2} - 1) \cdot \ldots \cdot (q - 1)} =
\end{aligned}$$

$$= \frac{\frac{q^n-1}{q-1}\cdot\frac{q^{n-1}-1}{q-1}\cdot\frac{q^{n-2}-1}{q-1}\cdot\ldots\cdot\frac{q^{n-k+1}-1}{q-1}}{\frac{q^k-1}{q-1}\cdot\frac{q^{k-1}-1}{q-1}\cdot\frac{q^{k-2}-1}{q-1}\cdot\ldots\cdot\frac{q-1}{q-1}} =$$

$$= \frac{[n]\cdot[n-1]\cdot[n-2]\cdot\ldots\cdot[n-k+1]}{[k]!} = \frac{[n]!}{[k]![n-k]!} = \begin{bmatrix} n \\ k \end{bmatrix},$$

что и требовалось доказать. □

Множество k-мерных подпространств в n-мерном пространстве V над полем $\mathbb{F}$ часто обозначается $\mathrm{Gr}_k(V)$ и называется *грассманианом*. Таким образом, мы только что доказали, что

$$|\mathrm{Gr}_k(\mathbb{F}_q^n)| = \begin{bmatrix} n \\ k \end{bmatrix}.$$

Чтобы дать аналогичную трактовку квантовым числам размещений, нам нужно будет ещё одно важнейшее понятие из линейной алгебры.

Определение 5.3. Пусть $0 < d_1 < d_2 < \ldots < d_r < n$. *Флагом типа* $d = (d_1, d_2, \ldots, d_r)$ в пространстве V называется цепочка вложенных друг в друга подпространств

$$U_1 \subset U_2 \subset \ldots \subset U_r$$

в V таких, что

$$\dim U_1 = d_1, \quad \dim U_2 = d_2, \quad \ldots, \quad \dim U_r = d_r.$$

Флаг типа $(1, 2, \ldots, n-1)$ называется *полным*. Будем обозначать множество всех флагов типа d через $\mathcal{F}_d(V)$; множество полных флагов обозначим через $\mathcal{F}(V)$.

Предложение 5.4. i) *Количество полных флагов в n-мерном пространстве над $\mathbb{F}_q$ равно $[n]!$.* ii) *Количество флагов типа $(1, 2, \ldots, k)$ в n-мерном пространстве над $\mathbb{F}_q$ равно $[n]_k$.*

Доказательство. Первый пункт является частным случаем второго (при $k = n-1$), так что докажем сразу второй пункт. Число способов выбрать последнее k-мерное подпространство флага равно $\begin{bmatrix} n \\ k \end{bmatrix}$ по доказанной выше теореме. В нём мы можем выбрать $(k-1)$-мерное подпространство $\begin{bmatrix} k \\ k-1 \end{bmatrix} = [k]$ способами. В этом $(k-1)$-мерном подпространстве есть всего $\begin{bmatrix} k-1 \\ k-2 \end{bmatrix} = [k-1]$ подпространств размерности $k-2$, и так далее. В конечном счёте число способов выбрать флаг типа $(1, 2, \ldots, k)$ будет равно

$$\begin{bmatrix} n \\ k \end{bmatrix}\cdot[k]\cdot[k-1]\cdot\ldots\cdot[1] = \frac{[n]!}{[k]![n-k]!}\cdot[k]! = \frac{[n]!}{[n-k]!} = [n]_k,$$

что и требовалось показать. □

Таким образом, если V — n-мерное пространство над полем $\mathbb{F}_q$ из q элементов и $d = (1, 2, \ldots, k)$, то

$$|\mathcal{F}(V)| = [n]!, \quad |\mathcal{F}_d(V)| = [n]_k.$$

Всё это можно ещё немножко обобщить.

Определение 5.5. Пусть $0 < l_1 < l_2 < \ldots < l_r$, $l_1 + l_2 + \ldots + l_r = n$. *Квантовым мультиномиальным коэффициентом* называется отношение двух многочленов с целыми коэффициентами от переменной q вида

$$\begin{bmatrix} n \\ l_1, \ldots, l_r \end{bmatrix} = \frac{[n]!}{[l_1]! \cdot \ldots \cdot [l_r]!}.$$

Обратим внимание, что, как и в случае с квантовыми числами сочетаний, заранее непонятно, будет ли это выражение многочленом от q, то есть поделится ли числитель на знаменатель.

Упражнение 5.6. Докажите, что квантовый мультиномиальный коэффициент $\begin{bmatrix} n \\ l_1, \ldots, l_r \end{bmatrix}$ равен количеству флагов в n-мерном пространстве над полем $\mathbb{F}_q$, имеющих тип $(l_1, l_1 + l_2, \ldots, l_1 + \ldots + l_{r-1})$. Проверьте, что этот коэффициент действительно является многочленом от q с целыми коэффициентами.

Мы переходим к кульминации этого параграфа — геометрическому доказательству квантовых аналогов тождеств, рассмотренных в параграфе 1. Сначала докажем геометрически квантовый аналог тождества из упражнения 1.1 (i), сформулированный ранее в упражнении 2.5 (i).

Теорема 5.7. *Для любых $n \geqslant 0$, $0 \leqslant k \leqslant n$ выполняется тождество*

$$[n] \cdot [n]_k = [n]_{k+1} + q^{n-k} \cdot [k] \cdot [n]_k.$$

Доказательство. Пусть V — n-мерное пространство над полем $\mathbb{F}_q$. Посчитаем количество пар вида (L, F), где L — одномерное подпространство в V, а F — флаг в V типа $(n-k, n-k+1, \ldots, n-1)$. С одной стороны, согласно теореме 5.2, одномерное пространство L можно выбрать $\begin{bmatrix} n \\ 1 \end{bmatrix} = [n]$ способами. По упражнению 5.6, флаг F можно выбрать

$$\begin{bmatrix} n \\ n-k, 1, \ldots, n-1 \end{bmatrix} = \frac{[n]!}{[n-k]! \cdot [1]! \cdot \ldots \cdot [1]!} = [n]_k$$

способами. Таким образом, число пар (L, F) равно $[n] \cdot [n]_k$, то есть левой части доказываемого тождества.

С другой стороны, посчитаем отдельно количество тех пар (L, F), в которых одномерное пространство L содержится в $(n-k)$-мерном подпространстве флага F. Сам флаг можно выбрать $[n]_k$ способами, а одномерное подпространство в его $(n-k)$-мерном подпространстве $\begin{bmatrix} n-k \\ 1 \end{bmatrix} = [n-k]$ способами. Значит, количество пар (L, F) указанного вида равно

$$[n-k] \cdot [n]_k = [n]_{k+1},$$

то есть первому слагаемому в правой части доказываемого тождества.

Найдём теперь количество тех пар (L, F), в которых пространство L содержится в $(n-k+1)$-мерном, но не в $(n-k)$-мерном подпространстве флага F. Оно будет равно $([n-k+1]-[n-k]) \cdot [n]_k$. Аналогично число пар (L, F), в которых L содержится в $(n-k+1)$-мерном, но не в $(n-k+1)$-мерном подпространстве флага F, равно $([n-k+2]-[n-k+1]) \cdot [n]_k$, и так далее. Значит, с учётом упражнения 2.3 (ii), число пар (L, F) равняется

$$[n]_{k+1} + ([n-k+1]-[n-k]) \cdot [n]_k + ([n-k+2]-[n-k+1]) \cdot [n]_k + \ldots + \\ + ([n]-[n-1]) \cdot [n]_k = [n]_{k+1} + (n-[n-k]) \cdot [n]_k = [n]_{k+1} + q^{n-k} \cdot [k] \cdot [n]_k,$$

то есть в точности правой части доказываемого тождества. □

Квантуем теперь тождество из упражнения 1.5 (v), которое, будучи записанным с использованием знака суммы, принимает вид

$$\sum_{i=0}^{k} \binom{n}{k-i} \cdot \binom{m}{i} = \binom{m+n}{k}.$$

Теорема 5.8. *Имеет место тождество*

$$\sum_{i=0}^{k} q^{(m-i)(k-i)} \cdot \begin{bmatrix} n \\ k-i \end{bmatrix} \cdot \begin{bmatrix} m \\ i \end{bmatrix} = \begin{bmatrix} m+n \\ k \end{bmatrix}.$$

Доказательство. Пусть V — $(m+n)$-мерное пространство над $\mathbb{F}_q$. По теореме 5.2, количество k-мерных подпространств в нём равно $\begin{bmatrix} m+n \\ k \end{bmatrix}$, то есть правой части доказываемого тождества.

Зафиксируем теперь какое-то m-мерное подпространство U в V. Пусть W — произвольное k-мерное подпространство пространства V. Тогда его пересечение $\widetilde{W}$ с U тоже будет подпространством (проверьте!) размерности i, где $0 \leqslant i \leqslant m$. Подпространство $\widetilde{W}$ можно выбрать в пространстве U всего $\begin{bmatrix} m \\ i \end{bmatrix}$ способами. Пусть оно уже выбрано. Выберем и зафиксируем в нём какой-нибудь базис. Дополним его векторами $\bar{v}_1, \ldots, \bar{v}_{k-i}$ до базиса k-мерного пространства W так, чтобы $W \cap U = \widetilde{W}$.

Первый вектор можно выбрать любым, не лежащим в U, это можно сделать $q^{m+n} - q^m$ способами. Второй вектор может быть любым, не лежащим в $(m+1)$-мерном подпространстве, натянутом на U и вектор $\bar{v}_1$. Значит, всего есть $q^{m+n} - q^{m+1}$ вариантов для вектора $\bar{v}_2$, и так далее. Получаем, что векторы $\bar{v}_1, \ldots, \bar{v}_{k-i}$ можно выбрать

$$(q^{m+n} - q^m) \cdot (q^{m+n} - q^{m+1}) \cdot \ldots \cdot (q^{m+n} - q^{m+k-i-1})$$

способами.

Как мы уже не раз видели, некоторые из таких наборов будут задавать одно и то же подпространство W. А именно, количество k-мерных подпространств, пересечение которых с U есть фиксированное i-мерное подпространство $\widetilde{W}$, равно

$$\frac{(q^{m+n} - q^m) \cdot (q^{m+n} - q^{m+1}) \cdot \ldots \cdot (q^{m+n} - q^{m+k-i-1})}{(q^k - q^i) \cdot (q^k - q^{i+1}) \cdot \ldots \cdot (q^k - q^{k-1})} =$$

$$= \frac{q^{m+(m+1)+\ldots+(m+k-i-1)} \cdot (q^n - 1) \cdot (q^{n-1} - 1) \cdot \ldots \cdot (q^{n-k+i+1} - 1)}{q^{i+(i+1)+\ldots+(k-i)} \cdot (q^{k-1} - 1) \cdot (q^{k-i-1} - 1) \cdot \ldots \cdot (q - 1)} =$$

$$= \frac{q^{(m-i)(k-i)} \cdot [n] \cdot [n-1] \cdot \ldots \cdot [n-k+i+1]}{[k-i]!} = q^{(m-i)(k-i)} \cdot \begin{bmatrix} n \\ k-i \end{bmatrix}.$$

Получаем, что общее количество k-мерных подпространств в V, пересечение которых с подпространством U имеет размерность i, равно $q^{(m-i)(k-i)} \cdot \begin{bmatrix} n \\ k-i \end{bmatrix} \cdot \begin{bmatrix} m \\ i \end{bmatrix}$. Складывая эти выражения по всем i от 0 до k, получим левую часть доказываемого тождества. □

§ 6. Группы матриц

Как и в параграфе 4, мы не можем здесь, конечно, дать хоть сколь-нибудь полное введение в теорию групп — поэтому ограничиваемся лишь теми определениями и примерами, которые нужны будут нам дальше, отсылая заинтересованного читателя к прекрасным книгам [2, 8, 10].

Определение 6.1. Группа — это непустое множество G вместе с бинарной операцией $x, y \in G \mapsto x \circ y \in G$, удовлетворяющей следующим трём свойствам.

1) $(x \circ y) \circ z = x \circ (y \circ z)$ для любых $x, y, z \in G$;
2) существует $e \in G$ такой, что $x \circ e = e \circ x = x$ для любого $x \in G$;
3) для любого $x \in G$ существует $\widetilde{x} \in G$ такой, что $x \circ \widetilde{x} = \widetilde{x} \circ x = e$.

Первое свойство, как всегда, называется *ассоциативностью* бинарной операции. Элемент e называется *нейтральным*, а элемент $\widetilde{x}$ — *обратным* к элементу x.

Упражнение 6.2. Докажите, что нейтральный элемент ровно один. Покажите также, что для любого элемента есть ровно один обратный.

Пример 6.3. i) Любое поле $\mathbb{F}$ является группой относительно операции сложения. Множество $\mathbb{F}^\times$ ненулевых элементов поля также образует группу относительно операции умножения.

ii) Любое векторное пространство является группой относительно сложения векторов.

iii) Целые числа образуют группу относительно операции сложения, но не образуют группу относительно операции умножения.

Нам потребуется определить ещё одну группу — группу матриц. Будем называть *матрицей n-го порядка* квадратную табличку размера $n \times n$, заполненную числами из какого-то фиксированного поля $\mathbb{F}$. (Можно рассматривать также и прямоугольные, но не обязательно квадратные матрицы.) Множество всех матриц n-го порядка с элементами из $\mathbb{F}$ обозначим через $\mathrm{Mat}_n(\mathbb{F})$. Будем через $a_{i,j}$ обозначать (i,j)-й элемент матрицы A, то есть число, стоящее в этой матрице в i-й строке и в j-м столбце.

Определим произведение матриц $A, B \in \mathrm{Mat}_n(\mathbb{F})$ правилом $C = AB$, где

$$c_{i,j} = \sum_{k=1}^{n} a_{i,k} b_{k,j}.$$

Упражнение 6.4. Докажите, что умножение матриц ассоциативно, то есть что $(AB)C = A(BC)$ для любых $A, B, C \in \mathrm{Mat}_n(\mathbb{F})$. Проверьте, что единичная матрица

$$E = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

является нейтральным элементом.

Определителем матрицы A называется число, обозначаемое $\det A$, которое вычисляется по следующему правилу. Если $n = 1$, то $\det A = a_{11}$, а для любого $n \geqslant 2$

$$\det A = (-1)^{i+1} \cdot a_{i,1} \cdot M_{i,1} + \ldots + (-1)^{i+n} \cdot a_{i,n} \cdot M_{i,n}.$$

Здесь i — произвольное число от 1 до n, а через $M_{i,j}$ обозначается определитель матрицы $(n-1)$-го порядка, получающейся из матрицы A вычёркиванием i-й строки и j-го столбца (он называется *дополнительным минором*). Эта формула для вычисления определителя часто называется формулой

разложения по строке. Верна также аналогичная формула *разложения по столбцу*: для любого j от 1 до n

$$\det A = (-1)^{1+j} \cdot a_{1,j} \cdot M_{1,j} + \ldots + (-1)^{n+j} \cdot a_{n,j} \cdot M_{n,j}.$$

Определитель матрицы A обозначают ещё так:

$$\det A = \begin{vmatrix} a_{1,1} & a_{1,2} & \ldots & a_{1,n} \\ a_{2,1} & a_{2,2} & \ldots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \ldots & a_{n,n} \end{vmatrix}.$$

Пример 6.5. Для $n = 2$ и $n = 3$ соответственно

$$\begin{vmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{vmatrix} = (-1)^{1+1} \cdot a_{1,1} \cdot M_{1,1} + (-1)^{1+2} \cdot a_{1,2} \cdot M_{1,2} = a_{1,1}a_{2,2} - a_{1,2}a_{2,1},$$

$$\begin{vmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{vmatrix} = (-1)^{1+1} \cdot a_{1,1} \cdot M_{1,1} + (-1)^{1+2} \cdot a_{1,2} \cdot M_{1,2} +$$

$$+ (-1)^{1+3} \cdot a_{1,3} \cdot M_{1,3} =$$

$$= a_{1,1} \cdot (a_{2,2}a_{3,3} - a_{2,3}a_{3,2}) - a_{1,2} \cdot (a_{2,1}a_{3,3} - a_{2,3}a_{3,1}) +$$

$$+ a_{1,3} \cdot (a_{2,1}a_{3,2} - a_{2,2}a_{3,1}) = a_{1,1}a_{2,2}a_{3,3} + a_{1,2}a_{2,3}a_{3,1} +$$

$$+ a_{1,3}a_{2,1}a_{3,2} - a_{1,3}a_{2,2}a_{3,1} - a_{1,2}a_{2,1}a_{3,3} - a_{1,1}a_{2,3}a_{3,2}.$$

Если определитель матрицы A равен нулю, то она называется *вырожденной* (а если не равен нулю — *невырожденной*). Множество всех невырожденных матриц n-го порядка с элементами из поля $\mathbb{F}$ будем обозначать через $\mathrm{GL}_n(\mathbb{F})$. Самое главное свойство определителя, которое нам потребуется, — это то, что матрица является невырожденной тогда и только тогда, когда её столбцы являются линейно независимыми (другими словами, образуют базис) в пространстве $\mathbb{F}^n$ [8, гл. 3, § 3, следствие из теоремы 1]. Кроме того, определитель произведения матриц равен произведению определителей:

$$\det(AB) = \det A \cdot \det B$$

(см., к примеру, [8, гл. 3, § 2, теорема 3]).

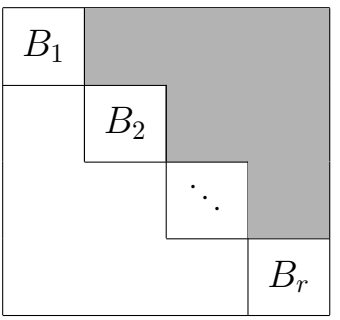
Упражнение 6.6. i) Матрица $A \in \mathrm{Mat}_n(\mathbb{F})$ называется *верхнетреугольной*, если $a_{i,j} = 0$ при $i > j$. Другими словами, матрица A имеет такой вид:

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \ldots & a_{1,n} \\ 0 & a_{2,2} & \ldots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & a_{n,n} \end{pmatrix}.$$

Докажите, что определитель верхнетреугольной матрицы равен произведению её диагональных элементов, то есть

$$\det A = a_{1,1} \cdot a_{2,2} \cdot \ldots \cdot a_{n,n}.$$

ii) Матрица называется *блочно-треугольной*, если существуют такие числа $b_1, \ldots, b_r$, в сумме равные n, что $a_{i,j} = 0$, если $j \leqslant b_1 + \ldots + b_k$ и $i > b_1 + \ldots + b_k$ для любого $1 \leqslant k \leqslant r$. Проще говоря, матрица A имеет такой вид:



Здесь диагональные «блоки» матрицы A — это матрицы $B_1, B_2, \ldots, B_r$ размеров $b_1 \times b_1$, $b_2 \times b_2$, $\ldots$, $b_r \times b_r$ соответственно. На «серых» позициях, то есть в верхней части матрицы, могут стоять любые числа, а в нижней части матрицы стоят нули. Набор чисел $(b_1, \ldots, b_r)$ назовём *типом* блочно-треугольной матрицы A. Покажите, что произведение двух блочно-треугольных матриц одного типа снова будет блочно-треугольной матрицей того же типа. Проверьте также, что $\det A = \det B_1 \cdot \ldots \cdot \det B_r$.

Далее, матрица $B \in \mathrm{Mat}_n(\mathbb{F})$ называется *обратной* к данной матрице $A \in \mathrm{Mat}_n(\mathbb{F})$, если $AB = BA = E$. Если такая матрица существует, то ровно одна (см. упражнение 6.2). В этом случае она обозначается A^{-1}, а матрица A называется *обратимой*. Можно показать [8, гл. 3, § 3, теорема 1], что матрица обратима тогда и только тогда, когда её определитель отличен от нуля.

Один из способов нахождения обратной матрицы заключается в следующем. Разрешим делать со строками произвольной прямоугольной матрицы такие преобразования: прибавлять к любой строке любую другую строку, умноженную на любое число, умножать любую строку на любое ненулевое число и менять местами любые две строки. Пусть A — невырожденная квадратная матрица n-го порядка. Припишем к матрице A справа единичную матрицу и, проводя описанные выше преобразования со строками полученной матрицы размера $n \times 2n$, добьёмся, чтобы в «левой части» этой матрицы получилась единичная матрица (если A обратима, то это возможно). Тогда в «правой части» получится A^{-1}. Вот пример

нахождения обратной матрицы:

$$\left(\begin{array}{ccc|ccc} 10 & -4 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 2 & -1 & 0 & 0 & 0 & 1 \end{array}\right) \begin{array}{l}\leftarrow\\ \leftarrow\end{array} \sim \left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 0 & 1 & 0 \\ 10 & -4 & 1 & 1 & 0 & 0 \\ 2 & -1 & 0 & 0 & 0 & 1 \end{array}\right) \begin{array}{l} \\ -10\mathrm{I} \\ -2\mathrm{I}\end{array} \sim$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & -14 & -9 & 1 & -10 & 0 \\ 0 & -3 & -2 & 0 & -2 & 1 \end{array}\right) \begin{array}{l} \\ -5\mathrm{III} \\ \end{array} \sim$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & -5 \\ 0 & -3 & -2 & 0 & -2 & 1 \end{array}\right) \begin{array}{l} \\ \\ +3\mathrm{II}\end{array} \sim$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & -5 \\ 0 & 0 & 1 & 3 & -2 & -14 \end{array}\right) \begin{array}{l} -\mathrm{III} \\ -\mathrm{III} \\ \end{array} \sim$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & 1 & 0 & -3 & 3 & 14 \\ 0 & 1 & 0 & -2 & 2 & 9 \\ 0 & 0 & 1 & 3 & -2 & -14 \end{array}\right) \begin{array}{l} -\mathrm{II} \\ \\ \end{array} \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -1 & 1 & 5 \\ 0 & 1 & 0 & -2 & 2 & 9 \\ 0 & 0 & 1 & 3 & -2 & -14 \end{array}\right).$$

Из всего сказанное выше следует, что множество невырожденных матриц $\mathrm{GL}_n(\mathbb{F})$ является группой относительно операции умножения матриц. Эта группа иногда называется *полной линейной* группой или *общей линейной* группой (по-английски `general linear`, отсюда и обозначение).

Определение 6.7. Группа G, состоящая из конечного числа элементов, называется *конечной*; $|G|$ называется *порядком* группы G.

Пример 6.8. Любое конечное поле $\mathbb{F}_q$ относительно сложения является конечной группой порядка q. Кроме того, n-мерное векторное пространство V над полем $\mathbb{F}_q$ относительно сложения векторов является конечной группой порядка q^n (почему?).

Упражнение 6.9. Докажите, что порядок группы $\mathrm{GL}_n(\mathbb{F}_q)$ равен

$$(q^n - 1) \cdot (q^n - q) \cdot \ldots \cdot (q^n - q^{n-1}).$$

Определение 6.10. Непустое подмножество H группы G называется *подгруппой*, если выполняются два условия:

1) $x \circ y \in H$ для любых $x, y \in H$;
2) $\widetilde{x} \in H$ для любого $x \in H$ (см. определение 6.1).

Пример 6.11. i) Любая группа является подгруппой в самой себе. Множество, состоящее только из нейтрального элемента группы, является подгруппой.

ii) Поле рациональных чисел $\mathbb{Q}$ является подгруппой в поле вещественных чисел $\mathbb{R}$ относительно сложения.

iii) Положительные числа образуют подгруппу в $\mathbb{R}^\times$ относительно умножения.

iv) Любое подпространство является подгруппой в векторном пространстве относительно сложения векторов.

v) Числа, кратные фиксированному натуральному числу n, образуют подгруппу в группе целых чисел $\mathbb{Z}$ относительно сложения.

Упражнение 6.12. i) Докажите, что любая подгруппа содержит нейтральный элемент группы.

ii) Проверьте, что непустое подмножество H группы G является подгруппой тогда и только тогда, когда из того, что x, y лежат в H, следует, что $x \circ \widetilde{y}$ тоже лежит в H.

Обратим внимание, что любую подгруппу H в группе G можно рассматривать как самостоятельную группу относительно той же операции $\circ$: нужно просто «забыть», что эта операция определена на всей группе G, и применять её только к элементам из H. Первое свойство подгруппы гарантирует, что результат применения операции всегда лежит в H, поэтому мы получаем корректно определённую бинарную операцию на H. (Почему будут выполняться аксиомы группы?)

Упражнение 6.13. i) Обозначим через B множество всех верхнетреугольных матриц из $\mathrm{GL}_n(\mathbb{F})$. Докажите, что это подгруппа в $\mathrm{GL}_n(\mathbb{F})$. Она называется *борелевской* подгруппой. Чему равен её порядок при $\mathbb{F} = \mathbb{F}_q$?

ii) Обозначим через P множество всех блочно-треугольных матриц из $\mathrm{GL}_n(\mathbb{F})$ данного типа $(b_1, \ldots, b_r)$. Докажите, что это подгруппа в $\mathrm{GL}_n(\mathbb{F})$. Она называется *параболической* подгруппой. Чему равен порядок этой подгруппы при $\mathbb{F} = \mathbb{F}_q$?

iii) Обозначим через $\mathrm{SL}_n(\mathbb{F})$ множество всех матриц из $\mathrm{GL}_n(\mathbb{F})$, определитель которых равен 1. Покажите, что это подгруппа в $\mathrm{GL}_n(\mathbb{F})$. Она называется *специальной линейной* группой (по-английски `special linear`).

Определение 6.14. Пусть G — любая группа, H — любая подгруппа в ней, $g \in G$ — произвольный элемент. *Левым смежным классом* элемента g по подгруппе H называется множество $gH = \{g \circ h,\ h \in H\}$.

Пример 6.15. i) Пусть G — любая группа, $H = G$. Тогда левый смежный класс любого элемента совпадает со всей группой G (почему?). Напротив, если $H = \{e\}$, то $gH = \{g\}$ для любого $g \in G$.

ii) Если G — группа целых чисел с операцией сложения, H — подгруппа, состоящая из чисел, кратных фиксированному натуральному числу n, то

смежный класс числа g состоит из всех целых чисел, дающих при делении на n такой же остаток, как число g.

iii) Пусть $G = \mathbb{R}^\times$, $H = \mathbb{R}_{>0}$ — множество положительных чисел. Тогда смежный класс любого положительного числа совпадает с H, то есть с множеством положительных чисел, а смежный класс любого отрицательного числа — с множеством отрицательных чисел.

Упражнение 6.16. i) Проверьте, что $gH = H$ тогда и только тогда, когда элемент g лежит в H.

ii) Пусть $g \in G$ — произвольный элемент. Постройте взаимно однозначное отображение из H в gH. Из существования такого отображения вытекает, в частности, что если H — конечная группа, то все смежные классы состоят из одного и того же числа элементов, равного порядку группы H.

iii) Покажите, что смежные классы либо не пересекаются, либо совпадают, то есть если $g_1, g_2 \in G$ и $g_1H \cap g_2H \neq \varnothing$, то $g_1H = g_2H$.

iv) (*Теорема Лагранжа.*) Если G — конечная группа, H — подгруппа в ней, то число различных левых смежных классов по подгруппе H равно $|G|/|H|$. Это число обозначается $[G : H]$ и называется *индексом* группы G по подгруппе H. В частности, порядок G делится на порядок H.

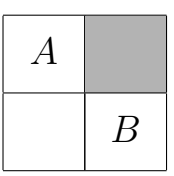
iv) Пусть $G = \mathrm{GL}_n(\mathbb{F})$, $H = \mathrm{SL}_n(\mathbb{F})$. Докажите, что две невырожденные матрицы A и B лежат в одном смежном классе по подгруппе H тогда и только тогда, когда их определители совпадают. Чему равен порядок $\mathrm{SL}_n(\mathbb{F}_q)$?

Оказывается, квантовые аналоги — это в точности индексы $\mathrm{GL}_n(\mathbb{F}_q)$ по подгруппам специального вида.

Упражнение 6.17. i) Покажите, что индекс $\mathrm{GL}_n(\mathbb{F}_q)$ по борелевской подгруппе равен $[n]!$.

ii) Докажите, что индекс $\mathrm{GL}_n(\mathbb{F}_q)$ по параболической подгруппе, состоящей из блочно-треугольных матриц типа $(b_1, \ldots, b_r)$, где $b_1 + \ldots + b_r = n$, равен квантовому мультиномиальному коэффициенту $\begin{bmatrix} n \\ b_1, \ldots, b_r \end{bmatrix}$.

В частности, если матрицы имеют тип $(k, n-k)$, то индекс по соответствующей параболической подгруппе равен квантовому числу сочетаний $\begin{bmatrix} n \\ k \end{bmatrix}$. С другой стороны, пусть матрицы имеют тип $(n-k, 1, \ldots, 1)$ (k единиц). Другими словами, параболическая подгруппа состоит из матриц такого вида:



Здесь A — любая невырожденная матрица размера $(n-k)\times(n-k)$, а B — любая невырожденная верхнетреугольная матрица размера $k\times k$. На «серых» позициях стоят любые числа, а в нижней части матрицы — нули. Тогда индекс группы $\mathrm{GL}_n(\mathbb{F}_q)$ по подгруппе P равен

$$\begin{bmatrix} n \\ n-k, 1, \ldots, 1 \end{bmatrix} = \frac{[n]!}{[n-k]!} = [n]_k,$$

то есть квантовому числу размещений.

Итак, мы видим, что, как и в классической комбинаторике, квантовые аналоги на самом деле перечисляют многие объекты весьма различной природы. В заключение мы объясним, почему трактовка квантовых аналогов в терминах матричных групп на самом деле вытекает из геометрической интерпретации. Для этого нам понадобится ещё одно важное понятие — действие группы на множестве.

§ 7. Действие групп матриц на флагах

Определение 7.1. Пусть G — любая группа, а X — какое-то непустое множество. *Действие* группы G на множестве X — это правило, которое каждой паре $g\in G$, $x\in X$ ставит в соответствие какой-то элемент множества X, обозначаемый $g.x$. При этом должны выполняться два условия:

1) $g.(h.x) = (g\circ h).x$ для любых $g, h\in G$, $x\in X$;
2) $e.x = x$ для любого $x\in X$.

Если задано действие группы G на множестве X, то говорят, что G *действует* на X и пишут $G : X$ или $G \curvearrowright X$.

Пример 7.2. i) Если G — любая группа, а X — любое множество, то правило $g.x = x$ для любых $g\in G$, $x\in X$ задаёт на X действие, называемое *тождественным*.

ii) Пусть $G=\mathbb{Z}$, $X=\mathbb{R}$. Правило $g.x = g+x$ определяет действие группы целых чисел (по сложению) на множестве вещественных чисел.

iii) Любая группа действует на самой себе следующим образом:

$$g.x = gxg^{-1}, \quad g, x\in G.$$

Проверьте, что это действительно действие. Оно называется *действием внутренними автоморфизмами*.

iv) Пусть H — любая подгруппа в группе G. Тогда H действует на G так: $h.x = hx$, $h\in H$, $x\in G$. Убедитесь, что это и в самом деле является действием. Оно называется *действием левыми сдвигами*.

v) Обозначим через G группу $\mathrm{GL}_n(\mathbb{F})$, а через X — n-мерное координатное пространство $\mathbb{F}^n$. Тогда $G \curvearrowright X$ по правилу $A.\bar{x} = A\bar{x}$ (имеется в виду умножение матрицы $n \times n$ на вектор, рассматриваемый как матрица $n \times 1$). То, что это действие, вытекает из ассоциативности умножения матриц и из того, что $E.\bar{x} = \bar{x}$ для любого вектора $\bar{x}$.

Определение 7.3. Пусть G — группа, действующая на множестве X, а x — произвольный элемент из X. *Орбитой* этого элемента под действием группы G называется множество Ω_x, состоящее из всех элементов $g.x$, когда g пробегает группу G, то есть

$$\Omega_x = \{g.x,\ g \in G\}.$$

Обратим внимание, что сам элемент всегда лежит в своей орбите, так как по второй аксиоме действия группы $e.x = x$.

Посмотрим, как выглядят орбиты в каждом из указанных выше примеров.

Пример 7.4. i) G, X — любые, $g.x = x$. Ясно, что орбита каждого элемента состоит только из этого элемента: $\Omega_x = \{x\}$ для любого $x \in X$.

ii) $G = \mathbb{Z}$, $X = \mathbb{R}$, $g.x = g + x$. Здесь орбита числа $x \in \mathbb{R}$ состоит из всех чисел, которые имеют такую же дробную часть, что и x.

iii) $X = G$, $g.x = gxg^{-1}$. Описание орбит здесь зависит от того, о какой группе идёт речь. Отметим лишь, что орбита в этом случае называется *классом сопряжённости* элемента x. Как будет устроен класс сопряжённости элемента x, если $G = \mathbb{Z}$?

iv) H — подгруппа в группе G, $H \curvearrowright G$ по правилу $h.x = hx$. Здесь орбита элемента x — это в точности его левый смежный класс по подгруппе H, то есть $\Omega_x = xH$.

v) $G = \mathrm{GL}_n(\mathbb{F})$, $X = \mathbb{F}^n$, $A.\bar{x} = A\bar{x}$. Конечно, в орбите нулевого вектора лежит только он сам: $\Omega_{\overline{0}} = \{\overline{0}\}$. На самом деле орбита любого ненулевого вектора совпадает с множеством всех ненулевых векторов. Действительно, в параграфе 4 была сформулирована теорема о дополнении до базиса, которая, напомним, гласит, что базис любого подпространства можно дополнить до базиса пространства. Отсюда сразу следует, что любой ненулевой вектор из $\mathbb{F}^n$ можно включить в базис пространства $\mathbb{F}^n$ (почему?).

Пусть теперь $\bar{x} \in \mathbb{F}^n$ — любой ненулевой вектор. Дополним его до базиса $\bar{f}_1 = \bar{x}, \bar{f}_2, \ldots, \bar{f}_n$ и рассмотрим матрицу A, j-й столбец которой совпадает со столбцом $\bar{f}_j$. Легко проверить, что если $\bar{e}_1$ — первый вектор стандартного базиса $\mathbb{F}^n$ (вектор, у которого первая координата равна единице, а остальные — нулю), то $A.\bar{e}_1 = A\bar{e}_1 = \bar{x}$. Значит, каждый ненулевой вектор лежит в орбите вектора $\bar{e}_1$. Из пункта (i) следующего упражнения вытекает, что

тогда орбита каждого ненулевого вектора совпадает с орбитой вектора $\bar{e}_1$, которая, в свою очередь, совпадает с множеством ненулевых векторов.

Упражнение 7.5. Пусть группа G действует на множестве X.

i) Докажите, что орбиты двух элементов либо не пересекаются, либо совпадают, то есть если $x, y \in X$ и $\Omega_x \cap \Omega_y \neq \varnothing$, то $\Omega_x = \Omega_y$.

ii) *Стабилизатором* элемента x называется множество тех элементов группы G, под действием которых элемент x переходит сам в себя. Обозначается стабилизатор так:

$$\mathrm{Stab}(x) = \{g \in G \mid g.x = x\}.$$

Покажите, что он всегда является подгруппой в группе G.

iii) Постройте взаимно однозначное соответствие между множеством левых смежных классов группы G по подгруппе $\mathrm{Stab}(x)$ и орбитой Ω_x.

Из последнего пункта вытекает замечательное следствие: если группа G конечна, то количество элементов в орбите элемента x равно индексу G по $\mathrm{Stab}(x)$, то есть

$$|\Omega_x| = [G : \mathrm{Stab}(x)] = \frac{|G|}{|\mathrm{Stab}(x)|}.$$

Теперь уже легко объяснить, как получить групповую интерпретацию квантовых аналогов из геометрической.

Упражнение 7.6. i) Напомним, что через $\mathcal{F}_d(\mathbb{F}^n)$ мы обозначали в параграфе 5 множество всех флагов типа $d = (d_1, \ldots, d_{r-1})$ в пространстве $\mathbb{F}^n$. Обозначим $b_1 = d_1$, $b_2 = d_2 - d_1$, $b_3 = d_3 - d_2$, $\ldots$, $b_{r-1} = d_{r-1} - d_{r-2}$, $b_r = n - d_{r-1}$. Пусть F — флаг типа d, $U_1 \subset \ldots \subset U_{r-1}$ — подпространства, его образующие, а A — любая невырожденная матрица. Рассмотрим множества

$$AU_i = \{A\bar{x},\ \bar{x} \in U_i\}, \quad 1 \leqslant i \leqslant r-1.$$

Докажите, что это подпространства, причём $AU_1 \subset \ldots \subset AU_r$ и $\dim(AU_i) = \dim U_i$ для всех i. Другими словами, цепочка вложенных подпространств $AU_1 \subset \ldots \subset AU_{r-1}$ образует флаг того же типа, что и F; обозначим этот флаг через $A.F$. Тем самым мы определили действие группы $\mathrm{GL}_n(\mathbb{F})$ на множестве флагов $\mathcal{F}_d(\mathbb{F}^n)$.

ii) Покажите, что это действие *транзитивно*, то есть всё множество $\mathcal{F}_d(\mathbb{F}^n)$ представляет из себя одну орбиту.

iii) Обозначим через F_0 так называемый *координатный* флаг. По определению, в нём подпространство U_i натянуто на первые i векторов стандартного базиса, то есть

$$U_i = \langle \bar{e}_1, \ldots, \bar{e}_i \rangle, \quad 1 \leqslant i \leqslant r.$$

Проверьте, что его стабилизатор — это в точности параболическая подгруппа P, состоящая из блочно-треугольных матриц типа $(b_1, \ldots, b_r)$.

Пусть теперь $\mathbb{F} = \mathbb{F}_q$. Тогда индекс $\mathrm{GL}_n(\mathbb{F}^n)$ по подгруппе P будет совпадать с количеством элементов множества $\mathcal{F}_d(\mathbb{F}^n)$, которое, в силу упражнения 5.6, равно квантовому мультиномиальному коэффициенту $\begin{bmatrix} n \\ b_1, \ldots, b_r \end{bmatrix}$, как и было показано в упражнении 6.17.

Ответы, указания, решения

1.1. Решение. i) Нужно просто привести дроби к общему знаменателю:

$$(n)_{k+1} + k \cdot (n)_k = \frac{n!}{(n-k-1)!} + \frac{k \cdot n!}{(n-k)!} = \frac{(n-k) \cdot n!}{(n-k) \cdot (n-k-1)!} + \frac{k \cdot n!}{(n-k)!} =$$
$$= \frac{(n-k) \cdot n!}{(n-k)!} + \frac{k \cdot n!}{(n-k)!} = \frac{n \cdot n!}{(n-k)!} = n \cdot (n)_k.$$

ii) Докажем индукцией по n. База индукции: пусть $n = 1$. Если $m = 0$, то левая часть имеет вид $(0)_0 = 1$, а правая равна $\dfrac{(1)_1}{1} = 1$, как и должно быть. Если же $m \geqslant 1$, то и левая, и правая части равны нулю.

Предположим теперь, что для какого-то натурального числа n формула уже доказана. Преобразуем левую часть для $n+1$, применив к ней сначала предположение индукции, а затем формулу из пункта (i):

$$(0)_m + (1)_m + \ldots + (n-1)_m + (n)_m = \frac{n_{m+1}}{m+1} + (n)_m =$$
$$= \frac{n_{m+1} + (m+1) \cdot (n)_m}{m+1} = \frac{(n_{m+1} + m \cdot (n)_m) + (n)_m}{m+1} =$$
$$= \frac{n \cdot (n)_m + (n)_m}{m+1} = \frac{(n+1) \cdot (n)_m}{m+1} = \frac{(n+1)_m}{m+1},$$

что и требовалось доказать.

1.2. i) Решение. Приведём правую часть к общему знаменателю:

$$\binom{n-1}{k} + \binom{n-1}{k-1} = \frac{(n-1)!}{k! \cdot (n-k-1)!} + \frac{(n-1)!}{(k-1)! \cdot (n-k)!} =$$
$$= \frac{(n-k) \cdot (n-1)!}{k! \cdot (n-k) \cdot (n-k-1)!} + \frac{k \cdot (n-1)!}{k \cdot (k-1)! \cdot (n-k)!} =$$
$$= \frac{(n-k) \cdot (n-1)!}{k! \cdot (n-k)!} + \frac{k \cdot (n-1)!}{k! \cdot (n-k)!} = \frac{n \cdot (n-1)!}{k! \cdot (n-k)!} = \frac{n!}{k! \cdot (n-k)!},$$

но это и есть число сочетаний из n по k.

ii) Указание. Предположим, что нужно набрать команду из k игроков, причём у нас всего n претендентов. Посчитайте отдельно способы сформировать команду, взяв первого претендента, а отдельно — не взяв первого претендента.

1.3. Решение. В левой части стоит произведение n скобок, в каждой из которых написано $x+y$. Раскроем скобки, но пока не будем приводить подобные слагаемые. Каждое слагаемое в получившейся сумме формируется так: мы перемножаем сколько-то переменных x и сколько-то переменных y, причём если y мы взяли из k скобок, то x берётся из оставшихся $n-k$ скобок. Значит, каждое слагаемое равно $x^{n-k}y^k$ для какого-то k от 0 до n.

Если мы теперь приведём подобные, то коэффициент перед слагаемым вида $x^{n-k}y^k$ будет равен количеству таких слагаемых до приведения подобных, то есть количеству способов выбрать k скобок из n скобок (это те скобки, из которых мы выбрали переменную y). Но это в точности число сочетаний из n по k, как и написано в правой части.

1.5. i) Решение. Подставим в бином Ньютона $x=y=1$.

ii) Решение. Посчитаем, чему равно количество последовательностей из плюсов и минусов длины n. С одной стороны, на каждой позиции может стоять либо плюс, либо минус (всего два варианта), причём каждая позиция заполняется независимо от остальных, поэтому число таких последовательностей равно $2\cdot 2\cdot\ldots\cdot 2$ (n сомножителей), то есть 2^n.

С другой стороны, посчитаем количество тех последовательностей, в которых ровно k плюсов. Эти плюсы могут стоять на любых k позициях из n (на остальных автоматически стоят минусы), а количество способов выбрать эти позиции равно, по определению, числу сочетаний $\binom{n}{k}$. Осталось заметить, что k может быть любым числом от нуля до n.

iii) Решение. Подставим в бином Ньютона $x=1$, $y=-1$.

iv) Указание. Предположите, что имеется n депутатов, из которых нужно выбрать одного президента, а из оставшихся сформировать правительство, в которое входит любое число депутатов от 0 до $n-1$.

v) Решение. Пусть нам надо выбрать k предметов из $n+m$ предметов. Поделим эти $n+m$ предметов на две кучки по n и m предметов. Сперва выберем из первой кучки j предметов; это можно сделать $\binom{n}{j}$ способами. Теперь из второй кучки осталось выбрать $\binom{m}{k-j}$ предметов; это, в свою очередь, можно сделать $\binom{m}{k-j}$ способами. Значит, общее число способов выбрать k предметов так, чтобы из первой кучки было взято j предметов, равно $\binom{n}{j}\cdot\binom{m}{k-j}$. Теперь заметим, что j может быть любым от 0 до k — и так получатся все способы выбрать k предметов из $n+m$ предметов.

2.3. Решение. i) Если это равенство верно, то степени многочленов в левой и в правой частях равны. Степень многочлена слева равна

$$(a-1)+(b-1)=a+b-2.$$

Степень многочлена справа равна $ab-1$. Значит,

$$ab-1=a+b-2,$$

то есть $(a-1)\cdot(b-1)=0$, откуда хотя бы одно из чисел a или b равно единице. Очевидно, что в таком случае второе число может быть любым.

ii) Докажем первое равенство; второе доказывается аналогично. Преобразуем правую часть:

$$[k]+q^k\cdot[n-k]=\frac{q^k-1}{q-1}+\frac{q^k\cdot(q^{n-k}-1)}{q-1}=\frac{q^k-1+q^n-q^k}{q-1}=\frac{q^n-1}{q-1}=[n].$$

2.5. Решение. i) Преобразуем правую часть:

$$\begin{aligned}[n]_{k+1}+q^{n-k}\cdot[k]\cdot[n]_k&=\frac{[n]!}{[n-k-1]!}+\frac{q^{n-k}\cdot[k]\cdot[n]!}{[n-k]!}=\\&=\frac{[n-k]\cdot[n]!}{[n-k]\cdot[n-k-1]!}+\frac{q^{n-k}\cdot[k]\cdot[n]!}{[n-k]!}=\\&=\frac{[n-k]\cdot[n]!}{[n-k]!}+\frac{q^{n-k}\cdot[k]\cdot[n]!}{[n-k]!}=\\&=\frac{([n-k]+q^{n-k}\cdot[k])\cdot[n]!}{[n-k]!}=\frac{[n]\cdot[n]!}{[n-k]!}=[n]\cdot[n]_k.\end{aligned}$$

Переход от третьей строки к четвёртой основан на втором равенстве из пункта (ii) предыдущего упражнения.

ii) Докажем первое равенство; второе доказывается аналогично. Преобразуем правую часть:

$$\begin{aligned}\begin{bmatrix}n-1\\k\end{bmatrix}+q^{n-k}\cdot\begin{bmatrix}n-1\\k-1\end{bmatrix}&=\frac{[n-1]!}{[k]!\cdot[n-k-1]!}+\frac{q^{n-k}\cdot[n-1]!}{[k-1]!\cdot[n-k!]}=\\&=\frac{[n-k]\cdot[n-1]!}{[k]!\cdot[n-k]!}+\frac{q^{n-k}\cdot[k]\cdot[n-1]!}{[k]!\cdot[n-k]!}=\\&=\frac{([n-k]+q^{n-k}\cdot[k])\cdot[n-1]!}{[k]!\cdot[n-k]!}=\frac{[n]\cdot[n-1]!}{[k]!\cdot[n-k]!}=\\&=\frac{[n]!}{[k]!\cdot[n-k]!}=\begin{bmatrix}n\\k\end{bmatrix}.\end{aligned}$$

Здесь мы опять пользовались пунктом (ii) предыдущего упражнения.

2.8. Решение. Применим индукцию по n. База индукции $n = 0$ очевидна. Предположим, что для $n-1$ утверждение уже доказано. Тогда, с учётом предположения индукции,

$$\begin{aligned}
[x+y]^n &= [x+y]^{n-1}\cdot(x+q^{n-1}y) = (x+q^{n-1}y)\times\\
&\quad\times\Big(q^{0\cdot(-1)/2}\cdot\begin{bmatrix}n-1\\0\end{bmatrix}x^{n-1}y^0 + q^{1\cdot0/2}\cdot\begin{bmatrix}n-1\\1\end{bmatrix}x^{n-2}y^1+\ldots+\\
&\quad+q^{k(k-1)/2}\cdot\begin{bmatrix}n-1\\k\end{bmatrix}x^{n-1-k}y^k+\ldots+q^{(n-1)(n-2)/2}\cdot\begin{bmatrix}n-1\\n-1\end{bmatrix}x^0y^{n-1}\Big) =\\
&=\Big(q^{0\cdot(-1)/2}\cdot\begin{bmatrix}n-1\\0\end{bmatrix}x^{n}y^0 + q^{1\cdot0/2}\cdot\begin{bmatrix}n-1\\1\end{bmatrix}x^{n-1}y^1+\ldots+\\
&\quad+q^{k(k-1)/2}\cdot\begin{bmatrix}n-1\\k\end{bmatrix}x^{n-k}y^k+\ldots+q^{(n-1)(n-2)/2}\cdot\begin{bmatrix}n-1\\n-1\end{bmatrix}x^1y^{n-1}\Big)+\\
&\quad+q^{n-1}\cdot\Big(q^{0\cdot(-1)/2}\cdot\begin{bmatrix}n-1\\0\end{bmatrix}x^{n-1}y^1 + q^{1\cdot0/2}\cdot\begin{bmatrix}n-1\\1\end{bmatrix}x^{n-2}y^2+\ldots+\\
&\quad+q^{k(k-1)/2}\cdot\begin{bmatrix}n-1\\k\end{bmatrix}x^{n-1-k}y^{k+1}+\ldots+q^{(n-1)(n-2)/2}\cdot\begin{bmatrix}n-1\\n-1\end{bmatrix}x^0y^{n}\Big).
\end{aligned}$$

Последнюю сумму мы разбили на две группы слагаемых, взятых в скобки. Уберём из первой скобки самое первое слагаемое (оно равно x^n), а из второй скобки — самое последнее слагаемое (оно равно y^n).

Оставшиеся слагаемые разобьём на пары так, чтобы в каждую пару вошло по одному слагаемому из каждой скобки. А именно, в пару к слагаемому

$$q^{k(k-1)/2}\cdot\begin{bmatrix}n-1\\k\end{bmatrix}x^{n-k}y^k$$

из первой скобки возьмём слагаемое

$$q^{(k-1)(k-2)/2}\cdot\begin{bmatrix}n-1\\k-1\end{bmatrix}x^{n-k}y^k$$

из второй скобки. Тогда сумма в каждой паре равна

$$q^{k(k-1)/2}\cdot\begin{bmatrix}n-1\\k\end{bmatrix}x^{n-k}y^k + q^{(n-1)+(k-1)(k-2)/2}\cdot\begin{bmatrix}n-1\\k-1\end{bmatrix}x^{n-k}y^k.$$

Поскольку $k(k-1)/2 = (k-1)(k-2)/2 + (k-1)$, сумму в каждой паре можно переписать в виде

$$\begin{aligned}
&q^{k(k-1)/2}\cdot\Big(\begin{bmatrix}n-1\\k\end{bmatrix}x^{n-k}y^k + q^{(n-1)-(k-1)}\cdot\begin{bmatrix}n-1\\k-1\end{bmatrix}x^{n-k}y^k\Big) =\\
&=q^{k(k-1)/2}\cdot\Big(\begin{bmatrix}n-1\\k\end{bmatrix}+q^{n-k}\cdot\begin{bmatrix}n-1\\k-1\end{bmatrix}\Big)\cdot x^{n-k}y^k = q^{k(k-1)/2}\cdot\begin{bmatrix}n\\k\end{bmatrix}x^{n-k}y^k
\end{aligned}$$

(мы воспользовались квантовым треугольником Паскаля).

Окончательно:

$$[x+y]^n = x^n + q^{1\cdot 0/2}\cdot\begin{bmatrix} n \\ 1 \end{bmatrix} x^{n-1}y^1 + q^{2\cdot 1/2}\cdot\begin{bmatrix} n \\ 1 \end{bmatrix} x^{n-2}y^2 + \\ + q^{k(k-1)/2}\cdot\begin{bmatrix} n \\ k \end{bmatrix} x^{n-k}y^k + \ldots + q^{(n-1)(n-2)/2}\cdot\begin{bmatrix} n \\ n-1 \end{bmatrix} x^1y^{n-1} + y^n,$$

что и требовалось доказать.

2.9. Указание. Докажите сначала, что $yx^m = q^m x^m y$. Теперь примените индукцию по n (база индукции $n = 0$ очевидна). Если утверждение уже доказано при $n-1$, то предположение индукции показывает, что

$$(x+y)^n = (x+y)\cdot(x+y)^{n-1} = (x+y)\times \\ \times\left(\begin{bmatrix} n-1 \\ 0 \end{bmatrix} x^{n-1}y^0 + \begin{bmatrix} n-1 \\ 1 \end{bmatrix} x^{n-2}y^1 + \ldots + \right. \\ \left. + \begin{bmatrix} n-1 \\ k \end{bmatrix} x^{n-1-k}y^k + \ldots + \begin{bmatrix} n-1 \\ n-1 \end{bmatrix} x^0y^{n-1}\right) = \\ = x^n + \begin{bmatrix} n-1 \\ 1 \end{bmatrix} x^n y^1 + \ldots + \begin{bmatrix} n-1 \\ k \end{bmatrix} x^{n-k}y^k + \ldots + \begin{bmatrix} n-1 \\ n-1 \end{bmatrix} x^1y^{n-1} + \\ + \begin{bmatrix} n-1 \\ 0 \end{bmatrix} yx^{n-1}y^1 + \ldots + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} yx^{n-1-k}y^k + \ldots + \begin{bmatrix} n-1 \\ n-2 \end{bmatrix} yx^1y^{n-2} + y^n.$$

Теперь рассуждайте так же, как в решении предыдущего упражнения; в частности, используйте треугольник Паскаля.

4.2. Решение. Покажем сначала, что $0^2 = 0$. В самом деле,

$$0^2 = 00 = 0(0+0) = 0^2 + 0^2.$$

Прибавив к обеим частям этого равенства -0^2, получим, что

$$0 = 0^2 + (-0^2) = (0^2 + 0^2) + (-0^2) = 0^2 + (0^2 + (-0^2)) = 0^2 + 0 = 0^2,$$

как мы и хотели.

Обозначим теперь $0x$ через a и заметим, что

$$a0 = (0x)0 = 0(x0) = 0(0x) = 0^2x = 0x = a.$$

Если предположить, что $a \neq 0$, то существует a^{-1} и тогда

$$1 = a^{-1}a = a^{-1}(a0) = (a^{-1}a)0 = 1\cdot 0 = 0$$

по определению элемента 1. Но это противоречит условию $1 \neq 0$, поэтому $a = 0$.

Обозначим теперь $(-1)x$ через b. Тогда

$$x + b = 1x + (-1)x = (1 + (-1))x = 0x = 0.$$

А раз так, то

$$-x = -x + 0 = -x + (x + b) = (-x + x) + b = 0 + b = b,$$

как и было обещано.

4.4. i) Указание. Обратите внимание, что даже проверка ассоциативности нетривиальна! Для доказательства существования обратного элемента используйте тот факт, что для любых целых чисел a, b найдутся такие целые числа c, d, что

$$ac + bd = \text{НОД}(a, b).$$

Доказательство этого факта вытекает из алгоритма Евклида нахождения наибольшего общего делителя. Это доказательство можно найти, к примеру, в [12, гл. 4].

ii) Ответ. Вот эти таблицы для $\mathbb{F}_5$ и $\mathbb{F}_7$:

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\cdot$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

4.5. Ответ. Пусть это множество состоит из элементов a, b, c, d. Зададим сложение и умножение так:

$+$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	d	b
d	a	d	b	c

4.7. Решение. Пусть $0\overline{x} = \overline{a}$, тогда

$$\overline{a} = 0\overline{x} = (0 + 0)\overline{x} = 0\overline{x} + 0\overline{x} = \overline{a} + \overline{a}.$$

Прибавим к обеим частям этого равенства вектор $-\bar{a}$:

$$\overline{0} = \bar{a} + (-\bar{a}) = (\bar{a} + \bar{a}) + (-\bar{a}) = \bar{a} + (\bar{a} + (-\bar{a})) = \bar{a} + \overline{0} = \bar{a},$$

как мы и хотели.

С другой стороны, пусть $(-1)\bar{x} = \bar{b}$, тогда

$$\overline{0} = 0\bar{x} = (1 + (-1))\bar{x} = 1\bar{x} + (-1\bar{x}) = \bar{x} + \bar{b}.$$

Прибавим к обеим частям этого равенства вектор $-\bar{x}$:

$$-\bar{x} = -\bar{x} + \overline{0} = -\bar{x} + (\bar{x} + \bar{b}) = (-\bar{x} + \bar{x}) + \bar{b} = \overline{0} + \bar{b} = \bar{b}.$$

5.6. Решение. Пусть F — флаг типа $(l_1, l_1 + l_2, \ldots, l_1 + \ldots + l_{r-1})$, образованный цепочкой подпространств

$$U_1 \subset U_2 \subset \ldots \subset U_{r-1}$$

в n-мерном пространстве V. Подпространство U_{r-1}, согласно теореме 5.2, можно выбрать

$$\begin{bmatrix} n \\ l_1 + \ldots + l_{r-1} \end{bmatrix} = \frac{[n]!}{[l_1 + \ldots + l_{r-1}]![n - l_1 - \ldots - l_{r-1}]!} = \frac{[n]!}{[l_1 + \ldots + l_{r-1}]![l_r]!}$$

способами.

Аналогично число способов выбрать подпространство U_{r-2} в пространстве U_{r-1} равно

$$\begin{bmatrix} [l_1+\ldots+l_{r-1}] \\ l_1+\ldots+l_{r-2} \end{bmatrix} = \frac{[l_1+\ldots+l_{r-1}]!}{[l_1+\ldots+l_{r-2}]![l_1+\ldots+l_{r-1}-\ldots-l_{r-2}]!} = \frac{[l_1+\ldots+l_{r-1}]!}{[l_1+\ldots+l_{r-2}]![l_{r-1}]!}.$$

Значит, количество способов выбрать в V пару подпространств $U_{r-2} \subset U_{r-1}$ нужных размерностей равно

$$\frac{[n]!}{[l_1 + \ldots + l_{r-1}]![l_r]!} \cdot \frac{[l_1 + \ldots + l_{r-1}]!}{[l_1 + \ldots + l_{r-2}]![l_{r-1}]!} = \frac{[n]!}{[l_1 + \ldots + l_{r-2}]![l_{r-1}]![l_r]!}.$$

Продолжая этот процесс, получим в конце концов, что количество способов выбрать флаг F в пространстве V в точности равно квантовому мультиномиальному коэффициенту $\begin{bmatrix} n \\ l_1, \ldots, l_r \end{bmatrix}$.

Покажем теперь, что он является многочленом от q с целыми коэффициентами. Для этого используем индукцию по $r \geqslant 2$. База индукции $r = 2$ очевидна: это в точности утверждение о том, что квантовое число сочетаний является многочленом от q с целыми коэффициентами. Предположим теперь, что утверждение доказано для $r - 1$. Тогда, по предположению индукции, $\begin{bmatrix} n \\ l_1, \ldots, l_{r-2}, l_{r-1} + l_r \end{bmatrix}$ является многочленом от q

с целыми коэффициентами. Но $\begin{bmatrix} l_{r-1}+l_r \\ l_{r-1} \end{bmatrix}$ — тоже многочлен от q с целыми коэффициентами, поэтому таковым будет и

$$\begin{bmatrix} n \\ l_1,\ldots,l_{r-2},l_{r-1}+l_r \end{bmatrix}\cdot\begin{bmatrix} l_{r-1}+l_r \\ l_{r-1} \end{bmatrix}=\frac{[n]!}{[l_1]!\ldots[l_{r-2}]![l_{r-1}+l_r]!}\cdot\frac{[l_{r-1}+l_r]!}{[l_{r-1}]![l_r]!}=\begin{bmatrix} n \\ l_1,\ldots,l_r \end{bmatrix}.$$

6.2. Решение. Если e_1, e_2 — нейтральные элементы, то

$$e_1 = e_1 \circ e_2 = e_2.$$

Первое равенство вытекает из того, что e_2 нейтрален, а второе — из нейтральности e_1.

Если теперь y, z — обратные элементы к какому-то элементу $x \in G$, то с учётом ассоциативности бинарной операции в группе

$$y = y \circ e = y \circ (x \circ z) = (y \circ x) \circ z = e \circ z = z.$$

6.4. Решение. По определению, (i,j)-й элемент левой части равен

$$\sum_{k=1}^{n}(AB)_{i,k}c_{k,j} = \sum_{k=1}^{n}\left(\sum_{l=1}^{n}a_{i,l}b_{l,k}\right)\cdot c_{k,j} = \sum_{k,l=1}^{n}a_{i,l}b_{l,k}c_{k,j}.$$

Последняя запись означает, что слагаемые в сумме нумеруются двумя индексами, k и l, каждый из которых может независимо от другого принимать любое значение от 1 до n.

Аналогично (i,j)-й элемент правой части равен

$$\sum_{l=1}^{n}a_{i,l}(BC)_{l,j} = \sum_{l=1}^{n}a_{i,l}\left(\sum_{k=1}^{n}b_{l,k}c_{k,j}\right) = \sum_{l,k=1}^{n}a_{i,l}b_{l,k}c_{k,j}.$$

Получаем, что это один и тот же элемент!

Проверка того, что E — нейтральный элемент, тривиальна.

6.6. i) Указание. Примените формулу разложения по последней строке (или по первому столбцу) несколько раз.

ii) Решение. Пусть X, Y — блочно-треугольные матрицы, имеющие тип $b_1,\ldots,b_r$, $Z = XY$. Пусть k — любое число от 1 до r. Обозначим $v = b_1 + \ldots + b_k$. Надо показать, что $c_{i,j} = 0$ при $j \leqslant v$ и $i > v$. Но

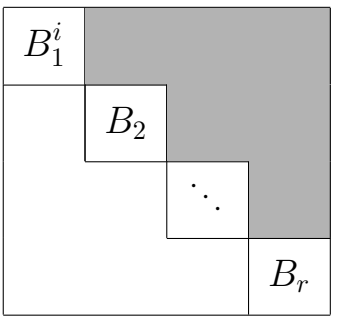
$$z_{i,j} = (x_{i,1}y_{1,j} + \ldots + x_{i,v}y_{v,j}) + (x_{i,v+1}y_{v+1,j} + \ldots + x_{i,n}y_{n,j}).$$

В первой группе слагаемых равны нулю элементы матрицы X, а во второй — элементы матрицы Y.

Для доказательства факта про определители используем индукцию по n. База индукции $n = 1$ очевидна. Предположим, что для блочно-треугольных матриц размера $n-1$ утверждение уже доказано. Применим к матрице A формулу разложения по первому столбцу. Если через B_1^i обозначить матрицу, получающуюся из матрицы B_1 удалением i-й строки и первого столбца, то мы получим, что

$$\det A = \sum_{i=1}^{n} (-1)^{i+1} a_{i,1} M_{i,1} = \sum_{i=1}^{b_1} (-1)^{i+1} a_{i,1} M_{i,1},$$

где $M_{i,1}$ — определитель матрицы вида



Он, по предположению индукции, равен $\det B_1^i \cdot \det B_2 \cdot \ldots \cdot \det B_r$, поэтому

$$\det A = \left(\sum_{i=1}^{b_1} (-1)^{i+1} a_{i,1} \det B_1^i \right) \cdot \det B_2 \cdot \ldots \cdot \det B_r = \det B_1 \cdot \det B_2 \cdot \ldots \cdot \det B_r.$$

6.9. Указание. Воспользуйтесь тем, что определитель матрицы отличен от нуля тогда и только тогда, когда её столбцы образуют базис в $\mathbb{F}_q^n$.

6.12. ii) Указание. Для доказательства достаточности не забудьте, что в H есть хотя бы один элемент. Покажите сначала, что в H лежит нейтральный элемент, потом — что если $x \in H$, то и $\widetilde{x} \in H$, и, наконец, что если $x, y \in H$, то и $x \circ y \in H$.

6.13. Ответ. i) Если $\mathbb{F} = \mathbb{F}_q$, то $|B| = (q-1)^n \cdot q^{n(n-1)/2}$.

ii) При $\mathbb{F} = \mathbb{F}_q$

$$\begin{aligned} |P| = {} & (q^{b_1} - 1) \cdot (q^{b_1} - q) \cdot \ldots \cdot (q^{b_1} - q^{b_1 - 1}) \times \\ & \times (q^{b_2} - 1) \cdot (q^{b_2} - q) \cdot \ldots \cdot (q^{b_2} - q^{b_2 - 1}) \times \ldots \times \\ & \times (q^{b_r} - 1) \cdot (q^{b_r} - q) \cdot \ldots \cdot (q^{b_r} - q^{b_r - 1}) \times q^a, \end{aligned}$$

где $a = \frac{1}{2} \cdot \big(n(n-1) - b_1(b_1-1) - b_2(b_2-1) - \ldots - b_r(b_r-1) \big)$.

6.16. i) Решение. Если $gH = H$, то, поскольку $e \in H$, мы видим, что $g = g \circ e \in gH = H$.

Обратно, пусть $g \in H$, тогда для любого элемента $h \in H$ выполняется $g \circ h \in H$, потому что H — подгруппа. Значит, $gH \subset H$. Наконец, каким бы ни был $x \in H$, элемент $h = \widetilde{g} \circ x$ лежит в H, так как H — подгруппа и $g, x \in H$. А тогда $x = e \circ x = (g \circ \widetilde{g}) \circ x = g \circ (\widetilde{g} \circ x) = g \circ h$ лежит в gH, поэтому $H \subset gH$. Вывод: $gH = H$.

ii) Указание. Взаимно однозначное отображение из H в gH устроено очень просто: оно переводит $h \in H$ в $g \circ h$.

iii) Решение. Покажем, что $g_1 H \subset g_2 H$ (обратное включение показывается точно так же). Для этого заметим сначала, что $g_1 \in g_2 H$. В самом деле, по условию существует такой $z \in G$, что $z \in g_1 H \cap g_2 H$. Другими словами, найдутся такие $h_1, h_2 \in H$, что $z = g_1 \circ h_1 = g_2 \circ h_2$. Но тогда

$$g_1 = z \circ \widetilde{h}_1 = (g_2 \circ h_2) \circ \widetilde{h}_1 = g_2 \circ (h_2 \circ \widetilde{h}_1) = g_2 \circ h'$$

лежит в $g_2 H$, так как $h' = h_2 \circ \widetilde{h}_1 \in H$.

Если теперь $g_1 \circ h$ — произвольный элемент из $g_1 H$, то

$$g_1 \circ h = (g_2 \circ h') \circ h = g_2 \circ (h' \circ h)$$

тоже лежит в $g_2 H$, ибо $h' \circ h \in H$.

iv) Указание. Воспользуйтесь двумя предыдущими пунктами.

v) Ответ. $|\mathrm{SL}_n(\mathbb{F}_q)| = \dfrac{(q^n - 1) \cdot (q^n - q) \cdot \ldots \cdot (q^n - q^{n-1})}{q - 1}$.

6.17. Указание. i) Воспользуйтесь упражнениями 6.9 и 6.13 (i).

ii) Воспользуйтесь упражнениями 6.9 и 6.13 (ii).

7.5. i) Указание. Доказательство должно быть очень похоже на доказательство упражнения 6.16 (iii).

iii) Указание. Это отображение переводит левый смежный класс элемента $g \in G$ в $g.x$.

7.6. Решение. i) Если $A\bar{x}$, $A\bar{y}$ лежат в AU_i для каких-то $\bar{x}, \bar{y} \in U_i$, то $\bar{x} + \bar{y} \in U_i$, поскольку U_i — подпространство, поэтому

$$A\bar{x} + A\bar{y} = A(\bar{x} + \bar{y}) \in AU_i.$$

Второе свойство подпространства проверяется аналогично. Итак, AU_i — подпространство. Включения $AU_i \subset AU_{i+1}$ очевидны: для любого $A\bar{x} \in U_i$ имеем $\bar{x} \in U_i \subset U_{i+1}$, а значит, $A\bar{x} \in AU_{i+1}$.

Покажем, что $\dim AU_i = \dim U_i$. Ясно, что $\dim AU_i \leqslant \dim U_i$. Действительно, предположим, что векторы $A\bar{x}_1, \ldots, A\bar{x}_k \in AU_i$ линейно независимы.

Тогда линейно независимы и векторы $\bar{x}_1, \ldots, \bar{x}_k \in U_i$ (докажите это от противного). Значит, в AU_i не может быть больше линейно независимых векторов, чем в U_i, откуда и вытекает требуемое неравенство.

Осталось заметить, что в предыдущем рассуждении A — любая невырожденная матрица, а U_i — любое подпространство. Легко понять, что $U_i = A^{-1}(AU_i)$ (проверьте!), поэтому

$$\dim U_i = \dim A^{-1}(AU_i) \leqslant \dim AU_i,$$

а значит, они равны.

ii) Достаточно доказать, что любой флаг F типа d лежит в орбите координатного флага F_0 (почему этого достаточно?). Чтобы это доказать, выберем в U_1 базис, затем дополним его до базиса U_2, полученный набор векторов дополним до базиса U_3, и так далее. В конце концов, получим базис U_{r-1}, который дополним до базиса всего $\mathbb{F}^n$. Обозначим через A матрицу, столбцы которой состоят из координат векторов этого базиса. Легко проверить (проверьте!), что $A.F_0 = F$.

iii) Докажем, что $\mathrm{Stab}(F_0) \subset P$. Выберем произвольную матрицу A из стабилизатора флага F_0. Пусть k — какое-то число от 1 до r. Нужно показать, что $a_{i,j} = 0$ при $j \leqslant b_1 + \ldots + b_k$ и $i > b_1 + \ldots + b_k$. Но условие $A.F_0 = F_0$ означает, в частности, что $AU_k = U_k$. Это равносильно тому, что $A\bar{e}_j \in U_k$ для любого $j \leqslant d_k = b_1 + \ldots + b_k$.

Среди прочего, $A\bar{e}_j \in U_k$ для $j \leqslant b_1 + \ldots + b_k$. Но условие $A\bar{e}_j \in U_k$ означает, что вектор $A\bar{e}_j$ (а это в точности j-й столбец матрицы A) может быть представлен в виде линейной комбинации первых d_k векторов стандартного базиса, то есть его координаты $a_{i,j}$ равны нулю при $i > d_k$, как мы и хотели. Итак, $\mathrm{Stab}(F_0) \subset P$. Обратное включение проверяется похоже и совсем просто.

Список литературы

[1] *Виленкин Н. Я., Виленкин А. Н., Виленкин П. А.* Комбинаторика. М.: МЦНМО, 2013.

[2] *Винберг Э. Б.* Курс алгебры. М.: МЦНМО, 2013.

[3] *Грэхем Р., Кнут Д., Паташник О.* Конкретная математика. Основание информатики. М.: Мир, Бином, 2009.

[4] *Давидович Б. М., Пушкарь П. Е., Чеканов Ю. В.* Математический анализ в 57-й школе. Четырёхгодичный курс. М.: МЦНМО, 2008.

[5] *Доценко В. В.* Числа Каталана и естественные отображения / С. В. Иванов, К. П. Кохась, А. И. Храбров и др., сост. Петербургские олимпиады школьников по математике 2003–2005. СПб.: Невский диалект, БХВ–Петербург, 2006. С. 328–360.

[6] *Доценко В. В.* Числа Каталана и естественные отображения. Летние конференции Турнира городов. Избранные материалы. Вып. 1. М.: МЦНМО, 2009. С. 139–165.

[7] *Кац В. Г., Чен П.* Квантовый анализ. М.: МЦНМО, 2005.

[8] *Кострикин А. И.* Введение в алгебру. Часть 1: Основы алгебры. М.: МЦНМО, 2009.

[9] *Кострикин А. И.* Введение в алгебру. Часть 2: Линейная алгебра. М.: МЦНМО, 2009.

[10] *Кострикин А. И.* Введение в алгебру. Часть 3: Основные структуры алгебры. М.: МЦНМО, 2009.

[11] *Ландо С. К.* Лекции о производящих функциях. М.: МЦНМО, 2007. Электронная версия `http://www.mccme.ru/free-books/lando/lando-genfunc.pdf`.

[12] *Прасолов В. В.* Задачи по алгебре, арифметике и анализу. М.: МЦНМО, 2011.

[13] *Окулов С. М.* Дискретная математика. Теория и практика решения задач по информатике. М.: Бином. Лаборатория знаний, 2008.

[14] *Стенли Р.* Перечислительная комбинаторика. Деревья, производящие функции и симметрические функции. М.: Мир, 2013.

[15] *Jantzen J. C.* Lectures on quantum groups // Grad. Staud. in Math. V. 6. AMS, 1996.

[16] *Petkovšek M., Wilf H. S., Zeilberger D.* $A{=}B$. A K Peters, Wellesley, Massachusetts, 1996. Электронная версия `http://www.math.upenn.edu/~wilf/AeqB.html`.

М. В. Игнатьев, Самарский государственный университет
`mihail.ignatev@gmail.com`