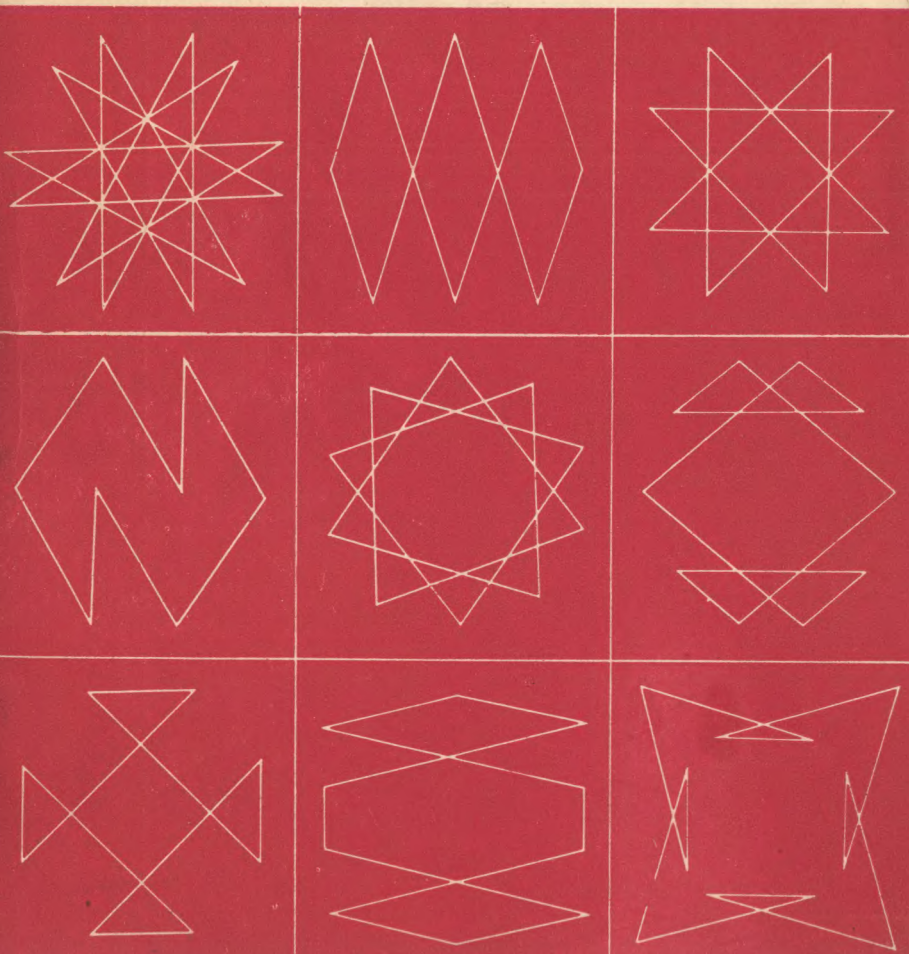
Ф. БАХМАН
Э. ШМИДТ

СОВРЕМЕННАЯ МАТЕМАТИКА
ПОПУЛЯРНАЯ СЕРИЯ

n-УГОЛЬНИКИ




ИЗДАТЕЛЬСТВО
МИР

n-ECKE

von

FRIEDRICH BACHMANN
Dr. Phil., O. Professor an der Universitä Kiel

und

ECKART SCHMIDT
Studienassessor, Kiel

BIBLIOGRAPHISCHES INSTITUT MANNHEIM/WIEN/ZÜRICH
Hochschultaschenbücher-Verlag
1970

«СОВРЕМЕННАЯ МАТЕМАТИКА»

Популярная серия

Ф. БАХМАН, Э. ШМИДТ

n-УГОЛЬНИКИ

Перевод с немецкого
А. И. Сироты

Под редакцией
И. М. Яглома

ИЗДАТЕЛЬСТВО «МИР»

Москва 1973

УДК 512:513.19

В этой книге на вполне элементарном материале, начинающемся с простейших геометрических истин (середины сторон произвольного четырехугольника являются вершинами параллелограмма и т. д.), развита весьма изящная теория, устанавливающая зачастую совершенно неожиданные связи между геометрией и важными концепциями и понятиями современной алгебры. Большое достоинство книги — сопровождающие изложение задачи, которые позволяют читателю все время контролировать степень овладения материалом.

Книга рассчитана на любителей математики самых разных категорий, начиная от старшеклассников, интересующихся этой наукой (например, учащихся школ с математической специализацией).

Редакция литературы по математическим наукам

Б $\frac{0223\text{-}040}{041(01)\text{-}73}$

ОТ РЕДАКТОРА

Имя первого из авторов — профессора университета в Киле Фридриха Бахмана — знакомо советскому читателю по переводу его обстоятельной монографии, в которой излагаются развиваемые кильской школой идеи в области оснований (евклидовой и неевклидовой) геометрии [1]).

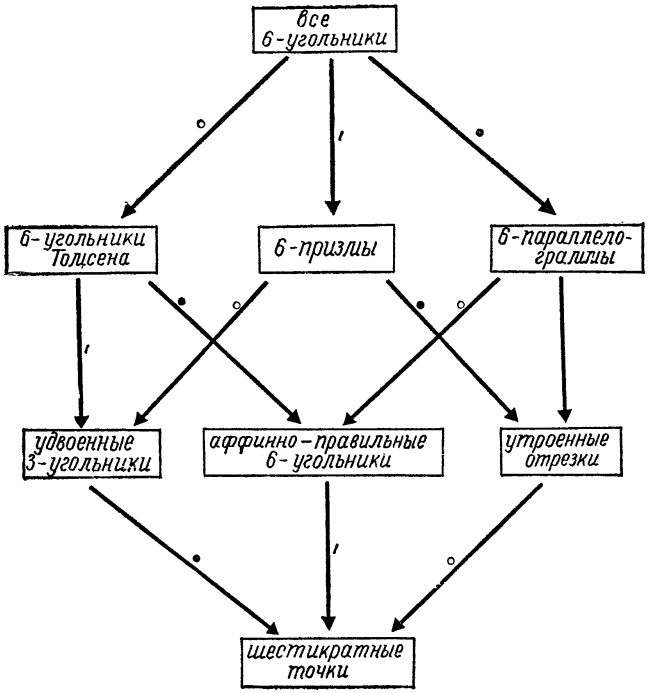
Настоящая книга носит совсем другой характер. Она начинается с достаточно поверхностной (и широко известной) теоремы: *середины сторон любого четырехугольника являются вершинами параллелограмма.* (У авторов вершины четырехугольника могут принадлежать любому — конечномерному или бесконечномерному — векторному пространству, построенному над почти любым полем; читателю, однако, мы рекомендуем рассматривать построения авторов на обычной плоскости или в трехмерном пространстве.) С этого простого предложения начинает раскручиваться цепь теорем — и как далеко эта цепь ведет! Вначале каждому n-угольнику сопоставляются три других n-угольника: вершинами одного из них являются середины сторон исходного n-угольника (отображение °); вершинами второго — точки пересечения медиан (центры тяжести) треугольников, образованных тройками соседних вершин исходного n-угольника (отображение •); вершинами третьего — четвертые вершины параллелограммов, построенных на трех соседних вершинах исходного n-угольника (отображение ′). Эти «циклические операции» отображают множество всех n-угольников в себя, но, вообще говоря, не на себя: «полное» множество всех n-угольников они могут

---

[1]) Ф. Бахман, Построение геометрии на основе понятия симметрии, «Наука», М., 1969.

перевести в его подмножество, в определенный «циклический класс» n-угольников.

Так, отображение $^\circ$ переводит множество всех 4-угольников в класс параллелограммов; три отображения $^\circ$, $\bullet$ и $'$, взятые в любом порядке, «сжимают» множество всех 6-угольников в класс шестикратных точек (6-угольников $A_1A_1A_1A_1A_1A_1$), как видно из следующей «коммутативной диаграммы»:



Далее понятия циклической операции (отображающей множество всех n-угольников в себя) и циклического класса n-угольников обобщаются; рассматриваются всевозможные циклические классы n-угольников — цепочка таких классов ведет от множества всех n-угольников к «нулевому классу», содержащему единственный (вырож-

денный!) n-угольник, все вершины которого совпадают с началом координат. Впрочем, выражение «цепочка классов» может создать у читателя неправильное впечатление: структура циклических классов оказывается достаточно сложной и разветвленной; в ней устанавливается определенный «порядок» и вводятся алгебраические операции, превращающие эту структуру в булеву алгебру классов n-угольников, на всем протяжении книги служащую одним из основных инструментов исследования.

Постепенно изложение обогащается новыми алгебраическими и геометрическими деталями. Число рассматриваемых классов n-угольников растет; рассматриваемые свойства систем n-угольников становятся более глубокими. Меняются и сопровождающие изложение задачи (которыми мы настоятельно советуем не пренебрегать): сначала это несложные упражнения; затем среди них появляются и некоторые «большие темы», которые могут послужить трамплином для самостоятельной исследовательской работы читателя. На ранней стадии исследования большую роль приобретает алгебра многочленов, в частности «многочлены деления круга» (делители многочленов $x^n - 1$); затем неожиданно возникают мотивы, навеянные теорией чисел. Используемые алгебраические средства становятся более глубокими: наряду с булевой алгеброй применяются некоторые понятия теории структур (перечисленные в приложении II); специально анализируются случаи того или иного основного поля, над которым строится «пространство n-угольников» (в частности, специально рассматриваются многоугольники над полем вещественных или комплексных чисел). И при этом все построения остаются совершенно прозрачными и элементарными.

Автор настоящих строк надеется, что эта своеобразная и очень красивая «микротеория», выразительно демонстрирующая на сравнительно элементарном уровне некоторые типичные черты «больших» математических теорий, вызовет интерес читателей. Кажется только, что авторы несколько перегрузили изложение не особенно существенными алгебраическими деталями, и преподавателю, который захотел бы использовать материал этой книги в занятиях с начинающими математиками, следует позаботиться о том, чтобы раскрыть «ядро» развиваемых здесь

конструкций, не слишком углубляясь в частности, составляющие «оболочку» этого ядра (см. также авторский обзор содержания на стр. 12).

Немногочисленные подстрочные примечания переводчика и редактора книги обозначаются звездочками в отличие от нумерованных сносок авторов; звездочками же отмечены названия тех фигурирующих в списке литературы работ, ссылки на которые отсутствуют в немецком оригинале. Мы также изменили порядок приложений, поскольку то из них, которое посвящено многочленам деления круга, более тесно, чем второе, примыкает к основному тексту книги.

И. М. Яглом

ИЗ ПРЕДИСЛОВИЯ АВТОРОВ

Математика обладает способностью открывать в окружающих нас вещах новые стороны и неожиданным образом расширять наши представления.

П. С. АЛЕКСАНДРОВ

Это книга об n-угольниках, классах n-угольников и отображениях множества n-угольников в себя.

n-угольники относятся к изначальным геометрическим объектам. Каждый знаком с какими-либо классами n-угольников, и геометрические наблюдения, на которых основывается эта книга, настолько элементарны, что будут понятны всем (см. введение). Однако трактовка более общих вопросов уже опирается на определенный алгебраический аппарат.

Для удобства использования этого аппарата мы определяем n-угольник как набор

$$(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n)$$

n элементов некоторого векторного пространства над полем, в котором $n \cdot 1 \neq 0$. Перефразируя Г. Шоке[1]), можно сказать, что понятие векторного n-набора открывает нам «царский путь» в геометрию — путь линейной алгебры *).

Основным объектом нашего исследования являются определенные множества n-угольников, которые называются циклическими классами. Прототип этого понятия (при $n=4$) — класс параллелограммов, т. е. множество 4-угольников $(\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3, \boldsymbol{a}_4)$, для которых $\boldsymbol{a}_1 - \boldsymbol{a}_2 + \boldsymbol{a}_3 - \boldsymbol{a}_4 = \boldsymbol{o}$. В общем случае циклический класс состоит из всех n-угольников, удовлетворяющих некоторой «циклической» системе однородных линейных уравнений с коэффициентами из данного поля.

Основная теорема о циклических классах утверждает, что число циклических классов для каждого n конечно,

---

[1]) Г. Шоке, Геометрия, «Мир», М., 1970.

*) Имеются в виду приписываемые Евклиду слова: «В геометрию нет царского пути».

точнее, что циклические классы образуют некоторую конечную булеву алгебру. Произвольный n-угольник однозначно разлагается в «сумму» n-угольников из «атомарных» циклических классов. Таким образом, n-угольники обладают некоторой атомарной структурой. Краеугольные камни — n-угольники из атомарных классов — отличаются определенными свойствами правильности.

Алгебраические средства, которыми мы пользуемся, лежат в основном русле алгебры [1]), и одна из целей этой книги состоит в том, чтобы описать очень красивые, на наш взгляд, связи между геометрией n-угольников и алгеброй.

Мы предполагаем, что читатель знаком с основными фактами линейной алгебры и такими алгебраическими понятиями, как группа, кольцо, поле, векторное пространство, гомоморфизм [2]). Необходимые понятия и результаты теории структур, а также основные свойства многочленов деления круга изложены в двух приложениях.

Мы весьма признательны Г. Киндеру (написавшему приложение о структурах), нашему постоянному собеседнику, одному из авторов развиваемой здесь теории, а также У. Шпенглеру, прорешавшему 126 упражнений. За помощь при корректуре мы благодарим Л. Бреккера и П. Клопша.

Киль

Ф. Б.
Э. Ш.

[1]) Однако попытки сообщить эту теорию могут встретить алгебраические трудности.

[2]) См., например, [3], [6], [9], [10], [12].

ПРЕДЫСТОРИЯ КНИГИ

Осенью 1964 г. во время конференции Общества усовершенствования преподавания естественных наук я задался вопросом, нельзя ли для оживления курса геометрии предложить тему, доступную студентам, связанную с систематической теорией, но не слишком отягощенную элементарно-геометрическими рассмотрениями. Я занялся тогда исследованием n-угольников на основе некоторого аксиоматического точечного исчисления. Основную роль при этом играет подходящим образом специализированная диэдральная группа (абелева группа, расширенная присоединением смежного класса некоторого инволютивного элемента). Этот подход, который лег в основу статьи [21], опубликованной в Grundzügen der Mathematik *), и был более подробно развит в курсе лекций в январе—феврале 1966 г., использовал Э. Шмидт, который доказал уже известную к тому времени основную теорему для рационального и вещественного числовых полей с помощью диагонализации циклической матрицы.

Летом 1966 г. Г. Киндер, побуждаемый к тому В. Пейасом, предложил новый подход к этой теории на языке векторных пространств. Он показал, что связь между циклическими классами n-угольников и многочленами проясняет касающиеся циклических классов закономерности.

Эта книга излагает содержание двухчасовой лекции, которую я прочитал осенью 1966 г. в Мичиганском университете и, в развернутом виде, зимой 1967/68 г.— в Кильском университете.

При подготовке настоящего издания я часто с благодарностью думал о математиках, которые во время докладов и в личных беседах со мной проявляли интерес к этой небольшой теории и рекомендовали опубликовать ее изложение.

Ф. Б.

---

*) «Основы математики»—многотомное издание, по своим установкам близкое к выпускаемым издательством Гостехиздат—Физматгиз—«Наука» книгам «Энциклопедии элементарной математики».

ОБЗОР СОДЕРЖАНИЯ

В конце введения и в гл. 1 и 2 определяются понятия циклического класса n-угольников и циклического отображения. Главы 1—4 посвящены в первую очередь примерам[1]).

В гл. 5 и в § 1 гл. 6 развиваются алгебраические методы, с помощью которых в § 2 гл. 6 доказывается основная теорема о циклических классах.

После алгебраической подготовки, которой отведены гл. 7 и § 1—2 гл. 9, мы в гл. 8 и 9 переходим к систематическому рассмотрению булевой алгебры циклических классов n-угольников. Результаты сведены в основную диаграмму (рис. 61, стр. 157).

В гл. 10—12 рассматривается разложение n-угольников в сумму n-угольников из атомарных циклических классов для случаев, когда основным полем является поле рациональных, комплексных или действительных чисел.

Можно сократить чтение этой книги, ограничившись лишь гл. 1, § 1—5 гл. 2, § 1—4 гл. 5 и гл. 6.

---

[1]) При чтении этих глав можно оставаться на наивной точке зрения, в стиле введения, и рассматривать специальные классы отображений n-угольников, не задумываясь о скрытых за ними общих понятиях.

ВВЕДЕНИЕ

Во введении мы будем пользоваться нестрогими соображениями наглядности. Все геометрические образы предполагаются вложенными в некоторое евклидово пространство произвольной размерности [1]).

Вспомним простую теорему: *во всяком четырехугольнике середины сторон образуют параллелограмм* (рис. 1). В этой

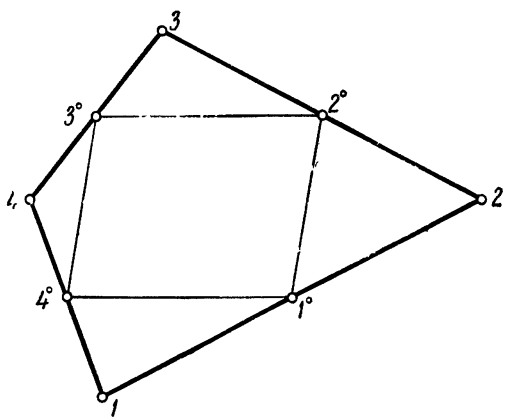


Рис. 1.

теореме всякому четырехугольнику A ставится в соответствие новый четырехугольник A°, образованный серединами сторон A. Тем самым задано некоторое отображение множества четырехугольников в себя. В результате этого отображения получается не все множество четырехуголь-

[1]) При этом мы используем лишь аффинные, но не метрические понятия и результаты.

ников, а некоторый его подкласс — класс параллелограммов: отображение «специализирует» множество четырехугольников. Специализация проявляется также в понижении размерности: ведь произвольный четырехугольник, вообще говоря, имеет размерность 3, в то время как параллелограмм самое большее двумерен.

Итак,

1°. *Если* $\boldsymbol{A}$ *— четырехугольник, то* $\boldsymbol{A}^\circ$ *— параллелограмм.*

Естественно возникает общий вопрос: для всякого ли n множество n-угольников специализируется при подобном отображении? Для нечетных n ответ оказывается отрицательным (для $n=3$ это очевидно). Для $n=6$ специализация существует [1]), но она не так наглядна, как при $n=4$. Вообще, справедливо такое утверждение:

2°. *Середины сторон произвольного* $2m$*-угольника* $\boldsymbol{A}$ *образуют* $2m$*-угольник* $\boldsymbol{A}^\circ$*, стороны которого, взятые через одну, образуют замкнутые векторные многоугольники.*

Последнее утверждение можно уточнить следующим образом. Если мы условимся обозначать стороны многоугольника $\boldsymbol{A}^\circ$ попеременно через a и b, то a-стороны, взятые отдельно, образуют замкнутый векторный многоугольник [2]) и то же самое верно для b-сторон. Так, стороны изображенного на рис. 2 шестиугольника Томсена (см. [25], рис. 3, или [22], рис. 28) обладают указанным свойством. Этим же свойством обладает изображенная на рис. 3 пятиконечная звезда.

К сожалению, термин «параллелограмм» не охватывает никаких n-угольников, где $n>4$. Чтобы исправить положение, введем новое понятие, обобщающее понятие параллелограмма и имеющее смысл для каждого четного $n=2m$. А именно, $2m$-угольник назовем $2m$*-параллелограммом*, если каждая из его сторон образует с противоположной стороной обычный параллелограмм. К числу 6-параллелограммов принадлежат, например, контуры обычно употребляемых параллельных проекций (параллелепипедов

---

[1]) См. Яглом [27], стр. 31.

[2]) Иными словами, если мы сдвинем параллельно a-стороны (взятые в любом порядке) так, чтобы конец каждой стороны совпал с началом следующей, то конец самой последней a-стороны совпадает с началом первой.

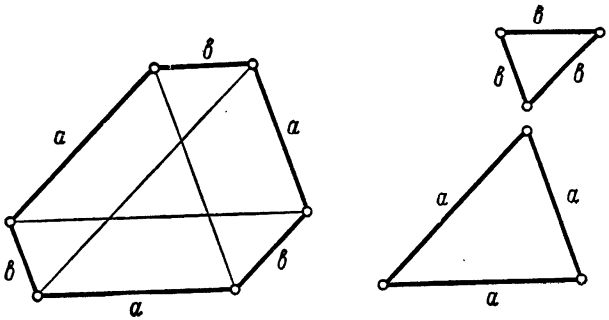


Рис. 2.

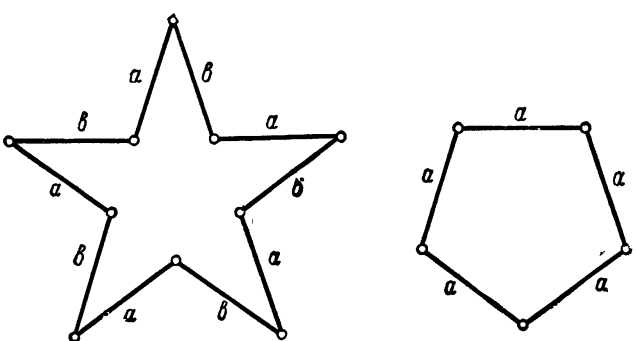


Рис. 3.

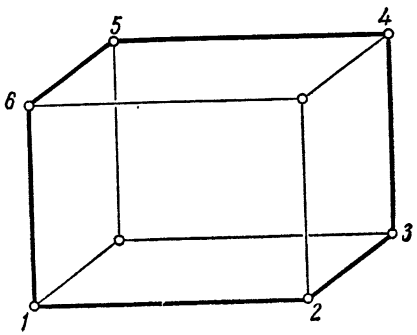


Рис. 4.

(см. рис. 4)); однако, разумеется, 6-параллелограмм может и не быть плоским.

Если A — некоторый 6-угольник, то A° не обязан быть 6-параллелограммом. Можно, однако, поставить вопрос о том, нельзя ли указать отображение, которое переводит множество всех 6-угольников в класс 6-параллелограммов.

Чтобы дать ответ на этот вопрос, модифицируем использованное ранее отображение. Середины сторон n-угольника являются центрами тяжести двух последовательных его вершин. Отсюда возникает естественное видоизменение этой конструкции: вместо середин сторон условимся рассматривать центры тяжести трех последовательных вершин n-угольника. Полученные центры тяжести образуют новый n-угольник $A^\bullet$, который мы и поставим в соответствие исходному n-угольнику A. На рис. 5 приведен пример указанного построения: точка $1^\bullet$ является центром тяжести вершин 1, 2, 3; точка $2^\bullet$ — вершин 2, 3, 4 и т. д.; все полученные точки $1^\bullet, 2^\bullet, \ldots, n^\bullet$ являются вершинами n-угольника $A^\bullet$, при этом имеет место такое предложение:

3°. *Для любого* 6*-угольника* A 6*-угольник* $A^\bullet$ *является* 6*-параллелограммом.*

Рассмотрим, наконец, еще одно отображение. Любые три последовательные вершины n-угольника дополним четвертой точкой до параллелограмма. (На рис. 6 точка $1'$ является четвертой вершиной параллелограмма 1, 2, 3, $1'$; точка $2'$ — параллелограмма 2, 3, 1, $2'$; точка $3'$ — параллелограмма 3, 1, 2, $3'$.) Множество четвертых вершин параллелограммов образует n-угольник, который мы обозначим через A'. Наше новое отображение — это отображение $A \to A'$. При этом справедливо следующее утверждение:

4°. *Для всякого* 6*-угольника* A *шестиугольник* A' *является призмой.*

Под *призмой* мы понимаем то, что наглядно изображено на рис. 8, *а* и *б*. (Обратите внимание на нумерацию вершин!) Утверждение 4° тем более замечательно, что для $n = 1, 2, 3, 4, 5, 7, 8, 9, 10, 11$ отображение $A \to A'$ невырожденно, т. е. никак не специализирует множество всех n-угольников.

Вот еще одно утверждение, в котором сам исходный n-угольник принадлежит специальному классу:

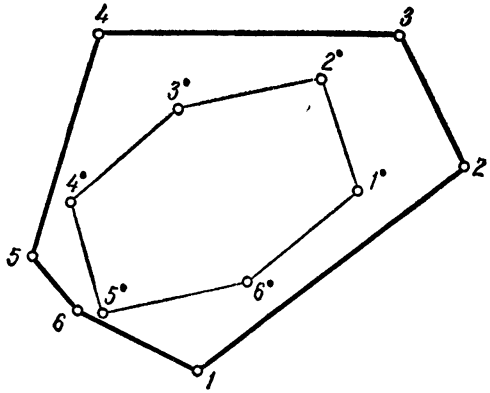


Рис. 5.

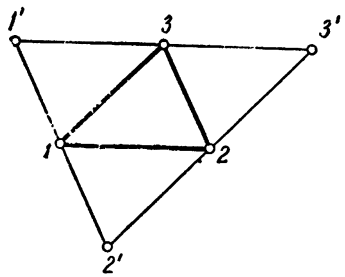


Рис. 6.

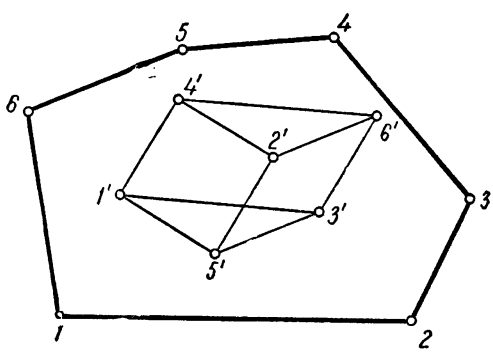
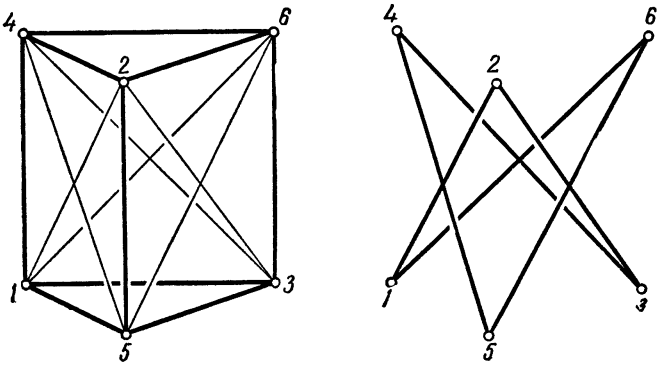


Рис. 7.

5°. *Если* A *есть* 8*-угольник, в котором вершины, взятые через одну, образуют параллелограммы, то* A° *есть* 8*-параллелограмм* (рис. 9).



а *б*

Рис. 8.

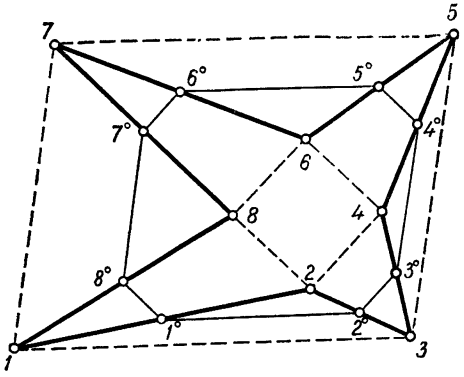


Рис. 9.

Фигурирующий в 5° 8-угольник A может быть построен следующим образом. Возьмем два произвольных параллелограмма и перенумеруем их вершины соответственно только нечетными и только четными числами (1, 3, 5, 7) и (2, 4, 6, 8). Тогда искомый 8-угольник A есть 8-угольник (1, 2, 3, ..., 8).

Множество 6-угольников специализируется при любом из рассмотренных отображений (см. утверждения 2°, 3° и 4°). Последовательное выполнение этих отображений все более и более сужает специализацию:

6°. *Для любого* 6-*угольника* A 6-*угольник* $A^{\circ\bullet}$ *является аффинно-правильным* (см. рис. 10), *а* $A^{\circ\bullet\prime}$ *— тривиальным* 6-*угольником, т. е.* 6-*кратно взятой точкой.*

При этом снижается максимально возможная размерность 6-угольников: если исходный 6-угольник может быть пятимерным, то аффинно-правильный 6-угольник не более чем двумерен, а тривиальный имеет размерность 0.

Как можно доказать сформулированные утверждения?

Первый возможный для этого путь основан на элементарной геометрии. Например, утверждения 1° и 5° следуют из теоремы: *средняя линия треугольника параллельна основанию и равна его половине* (см. рис. 11 и 12). Далее, пусть в четырехугольнике (1, 2, 3, 4) точки 1 •, 2 • являются центрами тяжести соответственно вершин 1, 2, 3 и 2, 3, 4. Тогда отрезок (1 •, 2 •) *параллелен стороне* (1, 4) *и равен ее трети* (рис. 13). Шестикратное применение этого факта доказывает утверждение 3°.

Второй путь основан на векторной алгебре. Выберем произвольно в пространстве начало координат. Тогда точка пространства задается своим радиусом-вектором, а n-угольник — набором n радиусов-векторов — вершин n-угольника:

$$(a_1, a_2, \ldots, a_n).$$

При этом мы далее не будем различать точку и отвечающий ей вектор, а также n-угольник и отвечающий ему набор n-векторов. Все свойства (1°—6°) легко перевести на язык векторной алгебры, после чего их доказательство сведется к простым выкладкам.

Доказательство 1°. Заметим, что *четырехугольник* (a_1, a_2, a_3, a_4) *является параллелограммом тогда и только тогда, когда* $a_2 - a_1 = a_3 - a_4$, или

$$a_1 - a_2 + a_3 - a_4 = o, \qquad (*)$$

т. е. когда знакопеременная сумма его вершин равна нулевому вектору o. Пусть теперь $A = (a_1, a_2, a_3, a_4)$. Тогда,

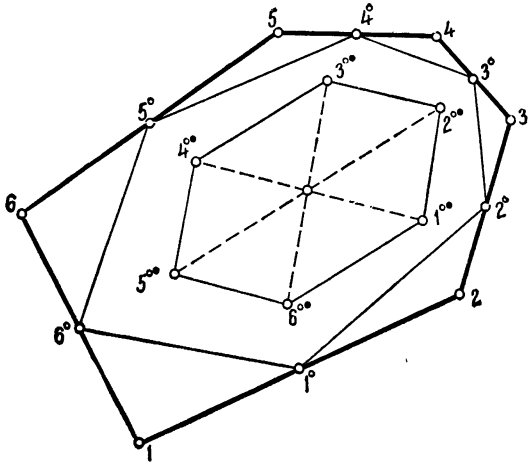


Рис. 10.

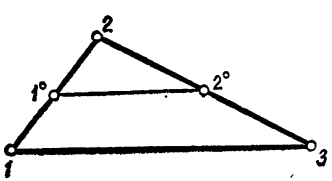


Рис. 11.

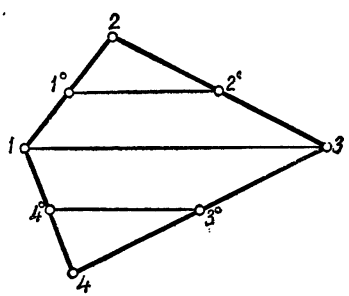


Рис. 12.

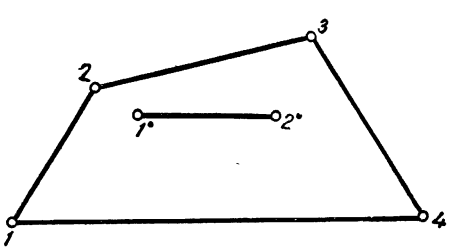


Рис. 13.

очевидно,

$$A^\circ = \left(\tfrac{1}{2}(a_1+a_2),\ \tfrac{1}{2}(a_2+a_3),\ \tfrac{1}{2}(a_3+a_4),\ \tfrac{1}{2}(a_4+a_1)\right).$$

Легко проверить, что знакопеременная сумма вершин четырехугольника A° всегда равна o.

Доказательство 2°. В $2m$-угольнике стороны, взятые через одну, образуют два замкнутых векторных m-угольника тогда и только тогда, когда

$$(a_2-a_1)+(a_4-a_3)+\ldots+(a_{2m}-a_{2m-1})=o,$$
$$(a_3-a_2)+(a_5-a_4)+\ldots+(a_1-a_{2m})=o.$$

(В каждом из равенств в скобках стоят векторы сторон, взятых через одну.) Но каждое из этих равенств можно переписать так: $a_1-a_2+a_3-a_4+\ldots+a_{2m-1}-a_{2m}=o$; таким образом, *знакопеременная сумма вершин $2m$-угольника должна равняться нулю.*

Если теперь $A=(a_1,\ \ldots,\ a_{2m})$—произвольный $2m$-угольник, то

$$A^\circ = \left(\tfrac{1}{2}(a_1+a_2),\ \tfrac{1}{2}(a_2+a_3),\ \ldots,\ \tfrac{1}{2}(a_{2m}+a_1)\right).$$

Легко проверить, что знакопеременная сумма вершин $2m$-угольника A° всегда равна o.

Доказательство 4°. Нетрудно видеть, что 6-угольник является призмой тогда и только тогда, когда

$$a_1-a_4=a_3-a_6=a_5-a_2$$

(см. рис. 8, *а*, *б*). Пусть $A=(a_1,\ \ldots,\ a_6)$—произвольный 6-угольник. Через a_1', a_2', ... обозначим четвертые вершины соответствующих параллелограммов: $(a_1,\ a_2,\ a_3,\ a_1')$, $(a_2,\ a_3,\ a_4,\ a_2')$, ... Тогда из (*) находим

$$a_1'=a_1-a_2+a_3,\ a_2'=a_2-a_3+a_4,\ \ldots,\ a_6'=a_6-a_1+a_2.$$

Легко проверить, что всегда

$$a_1'-a_4'=a_3'-a_6'=a_5'-a_2',$$

так как каждая из этих разностей равна $a_1 - a_2 + a_3 - a_4 + a_5 - a_6$. Итак, $A' = (a'_1, \ldots, a'_6)$ — призма.

Доказательство утверждений 3°, 5°, 6° предоставляется читателю.

Утверждения 1°—6° возникли из рассмотрения естественных геометрических отображений; они показывают, как специализируются при тех или иных отображениях определенные классы n-угольников, где n фиксировано. Существует много других теорем такого типа. Чтобы очертить общие рамки наших исследований, необходимо строго установить, какие множества n-угольников мы называем «классами» и какие отображения n-угольников нас интересуют, т. е. дать основные определения. Простейшие примеры, разобранные выше, позволяют надеяться, что мы напали на след глубоких закономерностей, связывающих классы n-угольников и определенные отображения.

Теперь от примеров мы перейдем к общим понятиям *циклического класса* и *циклического отображения*. Определениям этих понятий посвящены гл. 1 и 2 нашей книги.

ГЛАВА 1

ЦИКЛИЧЕСКИЕ КЛАССЫ n-УГОЛЬНИКОВ

§ 1. n-угольники, пространство n-угольников

Пусть n — натуральное число и K — (коммутативное) поле, характеристика которого взаимно проста с n. Элементы этого поля будем обозначать буквами a, b, ..., нулевой элемент — символом 0, единичный — 1. Обратный к n элемент (он существует в силу требования, наложенного на характеристику поля) обозначим $1/n$. [Для поля характеристики 0, в частности для поля рациональных чисел $\mathbf{Q}$, это требование выполняется при любом n.]

Обозначим через V векторное пространство над K; элементы $\boldsymbol{a}$, $\boldsymbol{b}$, ... из V назовем его *точками*, нулевой вектор $\boldsymbol{o}$ — его *началом*. Размерность V может быть какой угодно, конечной или бесконечной, но она не должна равняться нулю (т. е. V не должно сводиться к одному лишь началу $\boldsymbol{o}$).

n-угольником назовем любой упорядоченный набор n элементов из V: $(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n)$; n-угольники мы будем обозначать также заглавными буквами $\boldsymbol{A}, \boldsymbol{B}, \ldots$; буквой $\boldsymbol{O}$ мы обозначим нулевой n-угольник $(\boldsymbol{o}, \boldsymbol{o}, \ldots, \boldsymbol{o})$. Множество всех n-угольников обозначим $\mathcal{A}_n$.

Сложение n-угольников и *умножение* их *на элементы поля* K определим равенствами

$$(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n) + (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n) = \\ = (\boldsymbol{a}_1 + \boldsymbol{b}_1, \boldsymbol{a}_2 + \boldsymbol{b}_2, \ldots, \boldsymbol{a}_n + \boldsymbol{b}_n),$$

$$c(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n) = (c\boldsymbol{a}_1, \ldots, c\boldsymbol{a}_n)$$

(см. рис. 14 и 15). При этом множество всех n-угольников становится векторным пространством над K, а именно

$$\mathcal{A}_n = V^n = V \oplus V \oplus \ldots \oplus V.$$

Это пространство $\mathcal{A}_n$ мы будем называть *пространством n-угольников*.

Наряду с формальным определением n-угольника мы будем использовать и геометрическую терминологию. Точки $a_1, \ldots, a_n$ мы назовем *вершинами* n-угольника; упорядоченные пары последовательных вершин (a_i, a_{i+1}) — его *сторонами* (где натуральные числа i берутся $\bmod n$; таким образом, (a_n, a_1) — тоже сторона n-угольника); разности $a_{i+1} - a_i$ — *векторами сторон*. Если $n = 2m$ четно,

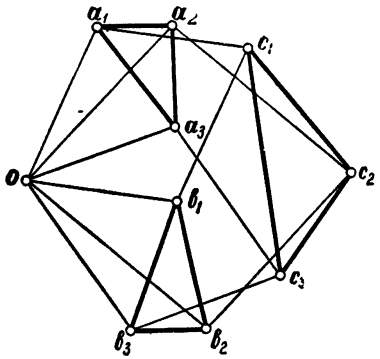


Рис. 14. Сумма двух треугольников.

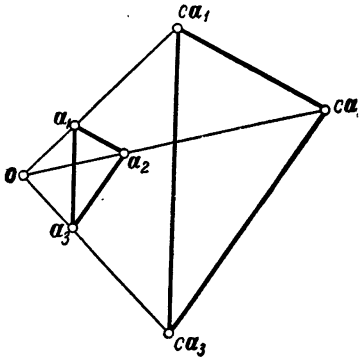


Рис. 15. Умножение 3-угольника на число.

то a_i и a_{i+m} назовем *противоположными вершинами* n-угольника, а (a_i, a_{i+1}) и (a_{i+m}, a_{i+m+1}) — его *противоположными сторонами*. Однако при этом не следует забывать, что на n-угольники можно также смотреть как на элементы векторного пространства V^n.

В определении n-угольника не предполагается, что его вершины обязательно различны. *Тривиальным* мы будем называть n-угольник $(a, a, \ldots, a)$, т. е. n раз повторенный 1-угольник. Множество тривиальных n-угольников мы будем обозначать символом $\mathcal{A}_{1,n}$. Легко проверить, что $\mathcal{A}_{1,n}$ — подпространство пространства $\mathcal{A}_n$.

§ 2. Циклические классы

К индексам n-угольника $(a_1, \ldots, a_n)$ применим n раз циклическую подстановку. Мы получим n-угольники

$$(a_2, \ldots, a_n, a_1), (a_3, \ldots, a_n, a_1, a_2), \ldots, (a_n, a_1, \ldots, a_{n-1}) \quad (1)$$

с тем же набором вершин и сторон. Будем считать, что все они задают один геометрический n-угольник.

Если исходный n-угольник удовлетворяет уравнению

$$c_0\boldsymbol{a}_1 + c_1\boldsymbol{a}_2 + \ldots + c_{n-1}\boldsymbol{a}_n = \boldsymbol{o}$$

с произвольными коэффициентами $c_0, c_1, \ldots, c_{n-1} \in K$, то этому уравнению вовсе не должны удовлетворять все n-угольники (1). Поэтому мы ограничимся рассмотрением лишь *циклических систем* уравнений, т. е. однородных систем

$$\begin{aligned} c_0\boldsymbol{a}_1 + c_1\boldsymbol{a}_2 + \ldots + c_{n-1}\boldsymbol{a}_n &= \boldsymbol{o}, \\ c_0\boldsymbol{a}_2 + c_1\boldsymbol{a}_3 + \ldots + c_{n-1}\boldsymbol{a}_1 &= \boldsymbol{o}, \\ \ldots\ldots\ldots\ldots\ldots\ldots & \\ c_0\boldsymbol{a}_n + c_1\boldsymbol{a}_1 + \ldots + c_{n-1}\boldsymbol{a}_{n-1} &= \boldsymbol{o} \end{aligned} \qquad (2)$$

с заданным набором коэффициентов $c_0, c_1, \ldots, c_{n-1} \in K$. Множество решений такой системы обладает тем свойством, что *вместе с n-угольником $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)$ ему принадлежит и вся последовательность* (1).

Множество решений циклической системы мы назовем *циклическим классом n-угольников*. Из теории систем однородных уравнений следует, что *циклический класс является подпространством пространства $\mathcal{A}_n$*.

В связи с тем что вся циклическая система (2) однозначно определяется одним из своих уравнений, мы введем сокращенную запись системы (2):

$$c_0\boldsymbol{a}_1 + c_1\boldsymbol{a}_2 + \ldots + c_{n-1}\boldsymbol{a}_n = \boldsymbol{o}, \ldots. \qquad (2')$$

Набор n элементов $(c_0, \ldots, c_{n-1})$ из K будем называть *коэффициентами* циклической системы, а элемент $\sum c_i$ — ее *суммой коэффициентов*.

Всякий n-набор элементов из K определяет единственную систему (2), а следовательно, и единственный циклический класс. Однако разные n-наборы могут определять один и тот же циклический класс. Таковы, например, наборы, различающиеся лишь общим множителем $c \neq 0$. Поэтому в случае $K = \mathbf{Q}$ всякий циклический класс может быть описан целочисленным n-набором.

Циклическая система с набором коэффициентов (0, ..., 0) определяет множество $\mathcal{A}_n$ всех n-угольников. Ци-

клическая система

$$a_1 - a_2 = o, \ \ldots$$

определяет множество $\mathcal{A}_{1,n}$ тривиальных n-угольников [1]). Множество решений циклической системы

$$a_1 = o, \ \ldots$$

состоит из одного n-угольника $O = (o, \ldots, o)$. Итак, $\mathcal{A}_n$, $\mathcal{A}_{1,n}$, $\{O\}$ — циклические классы.

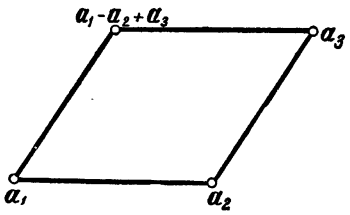


Рис. 16.

Пример. Пусть $n = 4$. Четырехугольник (a_1, a_2, a_3, a_4) называется *параллелограммом*, если векторная сумма противоположных сторон равна o: $(a_2 - a_1) + (a_4 - a_3) = o, \ldots$. Полученную циклическую систему запишем в форме

$$a_1 - a_2 + a_3 - a_4 = o, \ \ldots \ . \qquad (3)$$

Здесь первое равенство означает, что знакопеременная сумма вершин равна o, а остальные три равенства следуют из первого. Итак, *множество параллелограммов образует циклический класс.*

Для всяких трех точек $a_1, a_2, a_3 \in V$ точку $a_1 - a_2 + a_3$ (см. рис. 16) мы назовем *четвертой вершиной параллелограмма тройки* (a_1, a_2, a_3) или, короче, просто *четвертой вершиной тройки* (a_1, a_2, a_3).

---

[1]) При $n = 1$ оба эти класса совпадают: всякий 1-угольник, разумеется, тривиален.

Упражнения*)

1. Всякий циклический класс $\mathcal{C}$ инвариантен относительно линейных преобразований α пространства V: из $(a_1, \ldots, a_n) \in \mathcal{C}$ следует, что $(\alpha a_1, \ldots, \alpha a_n) \in \mathcal{C}$.

2. Всякое ли подпространство пространства $\mathcal{A}_n = V^n$, которое с каждым n-угольником $(a_1, a_2, \ldots, a_n)$ содержит всю последовательность (1), является циклическим классом?

3. Обязательно ли каждый циклический класс вместе с n-угольником $(a_1, \ldots, a_n)$ содержит также и n-угольник $(a_n, \ldots, a_2, a_1)$?

4. Всякий набор, полученный из $(c_0, c_1, \ldots, c_{n-1})$ циклической подстановкой, определяет тот же циклический класс, что и $(c_0, \ldots, c_{n-1})$.

5. Если $(c_0, c_1, \ldots, c_{n-1})$ и $(d_0, d_1, \ldots, d_{n-1})$ определяют один и тот же циклический класс, то $(c_0 - d_0, c_1 - d_1, \ldots, c_{n-1} - d_{n-1})$ определяет циклический класс, охватывающий первый.

§ 3. Центр тяжести n-угольника. Нуль-изобарический класс

Под *центром тяжести* n-угольника $(a_1, a_2, \ldots, a_n)$ мы будем понимать точку $\frac{1}{n}\sum a_i$ из V, т. е. среднее арифметическое вершин n-угольника. При $n = 2$ центр тяжести называется также *серединой* 2-угольника (отрезка).

Каждому n-угольнику $(a_1, \ldots, a_n) \in V^n$ поставим в соответствие тривиальный n-угольник, *каждая вершина которого является центром тяжести исходного*. Полученное отображение обозначим через σ:

$$\sigma\colon (a_1, \ldots, a_n) \longrightarrow \left(\frac{1}{n}\sum a_i, \ldots, \frac{1}{n}\sum a_i\right).$$

Образ $\sigma(a_1, \ldots, a_n)$ *n-угольника* при нашем отображении мы будем называть *n-угольником центра тяжести*, или просто *центром тяжести* исходного n-угольника **). Ясно, что σ есть линейное отображение пространства $\mathcal{A}_n$, переводящее $\mathcal{A}_n$ в класс $\mathcal{A}_{1,n}$ тривиальных n-угольников; для всякого тривиального n-угольника имеем $\sigma(a, \ldots, a) =$

*) В тех случаях, когда условие упражнения имеет вид формулировки некоторой теоремы, требуется доказать эту теорему.

**) Таким образом, термин «центр тяжести» будет иметь у нас два значения: точки и n-угольника; из контекста всегда будет ясно, о чем идет речь.

$= (\boldsymbol{a}, \ldots, \boldsymbol{a})$. Отсюда вытекает следующее свойство отображения σ:

$$\sigma\sigma(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n) = \sigma(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n) \tag{4}$$

— центр тяжести центра тяжести n-угольника совпадает с (первым) центром тяжести. (Отсюда видно, что отображение σ является проекцией: $\sigma^2 = \sigma$; см. § 4 гл. 2.)

Многоугольники $(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n)$ с центром тяжести $\boldsymbol{O}$, т. е. такие, что

$$\sigma(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n) = (\boldsymbol{o}, \ldots, \boldsymbol{o}), \tag{5}$$

образуют циклический класс, так как равенство (5) есть иная форма записи циклической системы

$$\frac{1}{n}\sum \boldsymbol{a}_i = \boldsymbol{o}, \ldots$$

(все уравнения этой системы совпадают). Этот циклический класс является ядром линейного отображения σ; он обозначается через $\mathring{\mathcal{A}}_{1,n}$ и состоит — если вернуться в исходное пространство V — из всех n-угольников, (обычный) центр тяжести которых совпадает с началом $\boldsymbol{o}$ пространства V.

Изобаричными мы будем называть два n-угольника $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)$, $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$, имеющие один и тот же центр тяжести:

$$\sigma(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n) = \sigma(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n). \tag{6}$$

Условие (6), очевидно, эквивалентно равенству

$$\frac{1}{n}\sum \boldsymbol{a}_i = \frac{1}{n}\sum \boldsymbol{b}_i \text{ или } \sum \boldsymbol{a}_i = \sum \boldsymbol{b}_i.$$

Свойство «изобаричности» есть отношение эквивалентности в множестве $\mathcal{A}_n$ всех n-угольников, совместимое с линейными операциями в $\mathcal{A}_n$*); оно задает разбиение множества всех n-угольников на *изобарические классы*. Всякий n-угольник изобаричен своему центру тяжести [см. (4)].

*) Другими словами, если $\boldsymbol{A} \sim \boldsymbol{A}_1$ и $\boldsymbol{B} \sim \boldsymbol{B}_1$, где $\sim$ — знак отношения изобаричности n-угольников, то

$$\boldsymbol{A} + \boldsymbol{B} \sim \boldsymbol{A}_1 + \boldsymbol{B}_1 \quad \text{и} \quad c\boldsymbol{A} \sim c\boldsymbol{A}_1.$$

Два тривиальных n-угольника изобаричны тогда и только тогда, когда они совпадают. Отсюда следует, что *всякий изобарический класс содержит ровно один тривиальный n-угольник*, являющийся общим центром тяжести всех n-угольников этого класса. Этот тривиальный n-угольник является представителем изобарического класса.

$\overset{\circ}{\mathcal{A}}_n$ является изобарическим классом, содержащим $(\boldsymbol{o}, \ldots, \boldsymbol{o})$; назовем его *нуль-изобарическим классом*. [Всякий изобарический класс является смежным классом $\overset{\circ}{\mathcal{A}}_n + (\boldsymbol{a}, \ldots, \boldsymbol{a})$. Если $\boldsymbol{a} \neq \boldsymbol{o}$, то смежный класс не является подпространством V^n, а значит, циклическим классом; $\overset{\circ}{\mathcal{A}}_n$ — единственный циклический класс, являющийся изобарическим классом.]

§ 4. Два типа циклических классов

Всякий циклический класс содержит тривиальный n-угольник $\boldsymbol{O} = (\boldsymbol{o}, \ldots, \boldsymbol{o})$.

1°. *Если циклический класс содержит тривиальный n-угольник, отличный от $\boldsymbol{O}$, то он содержит все тривиальные n-угольники.*

Доказательство. Предположим, что данный циклический класс определяется набором коэффициентов $(c_0, \ldots, c_{n-1}) \in K$. Тривиальный n-угольник $(\boldsymbol{a}, \ldots, \boldsymbol{a})$, $\boldsymbol{a} \neq \boldsymbol{o}$, принадлежит этому циклическому классу. Это означает, что он удовлетворяет системе уравнений (2):

$$c_0\boldsymbol{a} + c_1\boldsymbol{a} + \ldots + c_{n-1}\boldsymbol{a} = \boldsymbol{o} \text{ или } \left(\sum c_i\right)\boldsymbol{a} = \boldsymbol{o}. \qquad (7)$$

Так как по условию $\boldsymbol{a} \neq \boldsymbol{o}$, то $\sum c_i = 0$. Но если $\sum c_i = 0$, то (7) удовлетворяется при любом $\boldsymbol{a}$.

2°. *Всякий циклический класс вместе с каждым n-угольником $\boldsymbol{A}$ содержит и его центр тяжести $\sigma\boldsymbol{A}$.*

Доказательство. n-угольник $\sigma\boldsymbol{A}$ является средним арифметическим n-угольников последовательности (1), включая исходный. Поэтому он является решением однородной циклической системы как линейная комбинация n ее решений.

Из 1° следует, что существует два типа циклических классов:

А. Циклические классы, *охватывающие класс* $\mathcal{A}_{1,n}$ *тривиальных* n*-угольников*. Класс такого типа вместе с n-угольником $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)$ содержит все n-угольники

$$(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)+(\boldsymbol{a}, \ldots, \boldsymbol{a})=(\boldsymbol{a}_1+\boldsymbol{a}, \ldots, \boldsymbol{a}_n+\boldsymbol{a}),$$

получаемые из $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)$ всевозможными параллельными переносами. Другими словами, этот класс *инвариантен относительно параллельных переносов*. Такие циклические классы мы назовем *свободными*.

В. Циклические классы, которые из тривиальных n-угольников содержат только n-угольник $\boldsymbol{O}$. Из 2° следует, что всякий такой циклический класс содержится в нуль-изобарическом классе $\overset{\circ}{\mathcal{A}}_n$. Эти циклические классы назовем *центральными*.

Сформулируем окончательный результат:

Теорема 1. *Существует два типа циклических классов: свободные, т. е. те, которые содержат класс тривиальных* n*-угольников, и центральные, содержащиеся в нуль-изобарическом классе. Свободные циклические классы являются пространствами решений циклических систем с нулевой суммой коэффициентов, центральные — пространствами решений систем с суммой коэффициентов, отличной от нуля.*

$\mathcal{A}_n$ — максимальный, $\mathcal{A}_{1,n}$ — минимальный свободные циклические классы; $\overset{\circ}{\mathcal{A}}_n$ — максимальный, $\{\boldsymbol{O}\}$ — минимальный центральные циклические классы. На приведенной диаграмме (рис. 17) связь между этими четырьмя основными классами изображена наглядно: циклические классы отмечаются точками, а соединяющие эти точки наклонные или вертикальные отрезки обозначают включение ниже расположенного класса в класс, расположенный выше на том же отрезке. При этом свободные циклические классы можно представлять себе расположенными где-то на отрезке, соединяющем $\mathcal{A}_{1,n}$ и $\mathcal{A}_n$, а центральные классы — на отрезке, соединяющем $\{\boldsymbol{O}\}$ и $\overset{\circ}{\mathcal{A}}_n$.

Пример. Пусть $n=4$. Тогда свободный циклический класс образуют *параллелограммы*, а центральный циклический класс, определяемый системой $\boldsymbol{a}_1+\boldsymbol{a}_3=\boldsymbol{o}, \ldots,$ — *параллелограммы с центром тяжести в начале* $\boldsymbol{o}$.

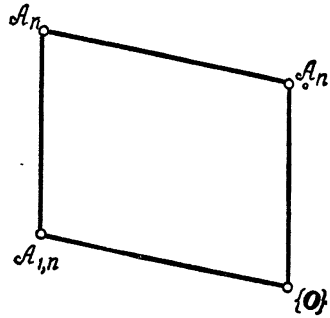


Рис. 17.

Для любого n-угольника $\boldsymbol{A}$ n-угольник $\boldsymbol{A}-\sigma\boldsymbol{A}$ принадлежит $\mathring{\mathcal{A}}_n$. Действительно, в силу (4)

$$\sigma(\boldsymbol{A}-\sigma\boldsymbol{A})=\sigma\boldsymbol{A}-\sigma\boldsymbol{A}=\boldsymbol{O}.$$

Геометрически n-угольник $\boldsymbol{A}-\sigma\boldsymbol{A}$ получается из $\boldsymbol{A}$ таким параллельным переносом, что его новый центр тяжести совпадает с началом $\boldsymbol{o}$.

Если $\boldsymbol{A}$ принадлежит некоторому циклическому классу, то, согласно 2°, ему же принадлежит $\sigma\boldsymbol{A}$, а следовательно, и $\boldsymbol{A}-\sigma\boldsymbol{A}$. Позднее мы докажем, что отображение

$$\boldsymbol{A}\longrightarrow\boldsymbol{A}-\sigma\boldsymbol{A},$$

как и следует ожидать, ставит в соответствие каждому свободному циклическому классу содержащийся в нем центральный класс и что это соответствие взаимно однозначно.

Итак, два типа классов естественным образом связаны друг с другом; поэтому мы не потеряем никаких геометрических свойств n-угольников, если ограничимся лишь одним из этих типов. В наших примерах мы будем предпочитать свободные циклические классы.

Упражнения

1. При $n \neq 1$ четыре основных циклических класса попарно различны. При $n=2$ никаких других циклических классов нет.

2. Пусть некоторый свободный циклический класс $\mathscr{C}$ определен набором $(c_0, \ldots, c_{n-1})$, где $\sum c_i = 0$. Тогда набор $\left(c_0+\frac{1}{n}, c_1+\frac{1}{n}, \ldots, \ldots, c_{n-1}+\frac{1}{n}\right)$ определяет класс n-угольников из $\mathscr{C}$ с центром тяжести в начале O.

3. Пусть центральный класс определен набором $(c_0, \ldots, c_{n-1})$. Тогда набор $(c_0-c, c_1-c, \ldots, c_{n-1}-c)$, где c — любой элемент поля, не равный $\frac{1}{n}\sum c_i$, определяет тот же циклический класс.

§ 5. Периодические классы

Пусть d — делитель n: $n = d \cdot \bar{d}$.

Рассмотрим циклическую систему уравнений

$$a_1 = a_{d+1}, \ldots, \tag{8}$$

определяющую циклический класс, состоящий из n-угольников

$$(a_1, \ldots, a_d, a_1, \ldots, a_d, \ldots, a_1, \ldots, a_d),$$

т. е. из $\bar{d}$ раз пройденных d-угольников (рассматриваемых, разумеется, как $(d \cdot \bar{d})$-угольники). Назовем такие n-угольники *периодическими* с периодом d; рассматриваемый класс назовем тоже *периодическим* и обозначим через $\mathscr{A}_{d,\bar{d}}$. Ясно, что $\mathscr{A}_{d,\bar{d}}$ — свободный циклический класс.

Каждому делителю d числа n соответствует свой периодический класс $\mathscr{A}_{d,\bar{d}}$. Крайние случаи: $\mathscr{A}_{n,1}$ — класс всех n-угольников $\mathscr{A}_n$; $\mathscr{A}_{1,n}$ — класс тривиальных n-угольников.

В связи с этим приведем следующую таблицу. Расположим вершины n-угольника в $\bar{d}$ столбцов из d вершин каждый:

$$\begin{array}{cccc} a_1 & a_{d+1} & \ldots & a_{n-d+1} \\ a_2 & a_{d+2} & \ldots & a_{n-d+2} \\ \ldots & \ldots & \ldots & \ldots \\ a_d & a_{2d} & \ldots & a_n \end{array}$$

Строки этой таблицы содержат $\bar{d}$ элементов. Каждую из них назовем *d-шаговым* $\bar{d}$*-угольником* многоугольника $\boldsymbol{A} = (\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n)$, или, короче, *хордовым* $\bar{d}$*-угольником*. Позже мы неоднократно воспользуемся возможностью выделения тех или иных новых циклических классов с помощью наложения определенных ограничений на хордо-

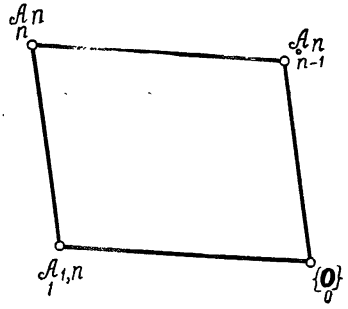


Рис. 18.

вые $\bar{d}$-угольники. В частности, класс $\mathcal{A}_{d,\bar{d}}$ состоит из тех n-угольников, для которых все хордовые $\bar{d}$-угольники тривиальны.

§ 6. Степень свободы циклического класса

Как мы уже отмечали, циклический класс параллелограммов обладает следующим свойством: всякие три точки $\boldsymbol{a}_1$, $\boldsymbol{a}_2$, $\boldsymbol{a}_3$ могут быть единственным образом дополнены до параллелограмма: $\boldsymbol{a}_4 = \boldsymbol{a}_1 - \boldsymbol{a}_2 + \boldsymbol{a}_3$. Можно сказать, что этот циклический класс обладает *тремя степенями свободы* (или что его степень свободы равна 3).

Дадим общее определение. Циклический класс $\mathcal{C}$ n-угольников имеет *степень (свободы)* f, если f — максимальное число произвольно взятых точек $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_f$, которые могут быть единственным образом дополнены до n-угольника $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_f, \boldsymbol{a}_{f+1}, \ldots, \boldsymbol{a}_n)$ класса $\mathcal{C}$. Степень циклического класса $\mathcal{C}$ обозначается $\mathrm{Grad}\,\mathcal{C}$.

На рис. 18 числа под циклическими классами обозначают их степени свободы. Для периодических классов,

очевидно, $\operatorname{Grad} \mathcal{A}_{d,\bar{d}} = d$, ибо при многократном прохождении одного и того же многоугольника его степень, очевидно, не меняется.

Рассмотрим теперь циклическую систему (2), задаваемую набором коэффициентов $(c_0, \ldots, c_{n-1})$. Запись (2) для линейной системы необычна; перепишем ее в более привычной форме:

$$\begin{aligned} c_0\boldsymbol{a}_1 + c_1\boldsymbol{a}_2 + \ldots + c_{n-1}\boldsymbol{a}_n &= \boldsymbol{o}, \\ c_{n-1}\boldsymbol{a}_1 + c_0\boldsymbol{a}_2 + \ldots + c_{n-2}\boldsymbol{a}_n &= \boldsymbol{o}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ c_1\boldsymbol{a}_1 + c_2\boldsymbol{a}_2 + \ldots + c_0\boldsymbol{a}_n &= \boldsymbol{o}. \end{aligned}$$

Теперь легко выписать матрицу коэффициентов этой системы:

$$M(c_0, c_1, \ldots, c_{n-1}) = \begin{pmatrix} c_0 & c_1 & \ldots & c_{n-1} \\ c_{n-1} & c_0 & \ldots & c_{n-2} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ c_1 & c_2 & \ldots & c_0 \end{pmatrix}.$$

Каждая строка матрицы содержит одни и те же элементы, только от строки к строке их совокупность циклически сдвигается на один элемент вправо. Такие матрицы называются *циклическими*.

Предположим, что первые r строк этой матрицы линейно независимы, а $(r+1)$-я строка является их линейной комбинацией. Тогда всякая следующая строка является той же линейной комбинацией r предыдущих. Итак, r последовательных строк матрицы являются максимальной линейно независимой системой, следовательно, ранг матрицы равен r. Из теории систем линейных однородных уравнений следует, что в этом случае $n-r$ произвольно заданных последовательных точек могут быть единственным образом дополнены до решения системы. Отсюда следует

Теорема 2. *Степень свободы циклического класса, заданного набором* $(c_0, \ldots, c_{n-1})$, *равна*

$$n - \operatorname{Rang} M(c_0, \ldots, c_{n-1}).$$

Упражнение. Пусть $\dim V = m$. Тогда $\dim V^n = n \cdot m$, и если $\mathcal{C} \subseteq V^n$ — циклический класс, такой, что $\operatorname{Grad} \mathcal{C} = f$, то $\dim \mathcal{C} = fm$.

§ 7. Размерность n-угольника

Определим *размерность* $\dim \boldsymbol{A}$ n-угольника $\boldsymbol{A}$, понимаемого как система из n точек векторного пространства V. Для n-угольника с центром тяжести $\boldsymbol{o}$ естественно положить

$$\dim(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n) = \dim\langle \boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n\rangle,$$

где $\langle \boldsymbol{a}_1, \ldots, \boldsymbol{a}_n\rangle$ — подпространство, натянутое на векторы $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$. Так как $\frac{1}{n}\sum \boldsymbol{a}_i = \boldsymbol{o}$, то размерность этого подпространства не превышает $n-1$. Для произвольного n-угольника $\boldsymbol{A}$ положим

$$\dim \boldsymbol{A} = \dim(\boldsymbol{A} - \sigma\boldsymbol{A}),$$

так что n-угольники, полученные один из другого параллельным переносом, имеют по определению одинаковую размерность. Размерность n-угольника не превосходит $n-1$, всякий тривиальный n-угольник имеет размерность 0, размерность треугольника и параллелограмма не превосходит 2.

Размерность n-угольника есть размерность минимального содержащего его линейного многообразия в V. [По определению, все линейные многообразия в V суть смежные классы $T+\boldsymbol{a}$, где T — подпространство V и $\dim(T+\boldsymbol{a}) = \dim T$.]

Замечание. Пусть размерность V равна n. Рассмотрим максимальную размерность, которую могут иметь n-угольники, принадлежащие заданному циклическому классу. Это число будет одним и тем же для свободного циклического класса и для отвечающего ему центрального класса[1]); оно равно степени свободы центрального класса, в то время как степень свободного класса будет на 1 выше.

---

[1]) Это введенное в § 4 понятие будет еще уточнено в § 2 гл. 3.

§ 8. Примеры циклических классов

Здесь мы ограничимся лишь примерами *свободных* циклических классов, выделяемых в множествах n-угольников при тех или иных фиксированных значениях n. Отношение принадлежности между этими классами, которое будет нас особенно интересовать, мы условимся схематически изображать на графических схемах или диаграммах следующим образом: если в диаграмме два

Рис. 19.

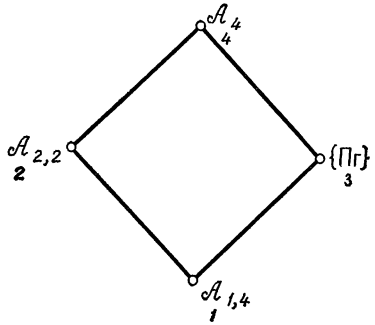


Рис. 20.

циклических класса соединены наклонным или вертикальным отрезком, то класс, находящийся ниже, включается в верхний, принадлежащий тому же отрезку. Число под классом обозначает степень свободы этого класса.

Заметим, что мы не стремимся указать здесь полный набор всех циклических классов, даже для малых n. Вопросами полноты мы будем заниматься несколько позднее.

a) $n=p$ (простое число). Нам уже известны свободные циклические классы $\mathcal{A}_p$, $\mathcal{A}_{1,p}$ (рис. 19). Этим исчерпывается множество периодических классов p-угольников, так как p имеет только тривиальные делители p и 1.

b) $n=4$. Существуют три периодических класса: $\mathcal{A}_4$, $\mathcal{A}_{2,2}$ (класс дважды пройденных отрезков), $\mathcal{A}_{1,4}$; прибавим к ним еще циклический класс параллелограммов,

при этом мы придем к диаграмме, изображенной на рис. 20.

c) $n=2m$. Во введении уже упоминались $2m$-*параллелограммы*, для которых векторная сумма противоположных пар сторон равна нулю; они, очевидно, определяются циклической системой

$$\boldsymbol{a}_1-\boldsymbol{a}_2+\boldsymbol{a}_{m+1}-\boldsymbol{a}_{m+2}=\boldsymbol{o},\ \ldots .$$

Эквивалентным является требование совпадения середин отрезков, соединяющих пары противоположных вершин:

$$\tfrac{1}{2}(\boldsymbol{a}_1+\boldsymbol{a}_{m+1})=\tfrac{1}{2}(\boldsymbol{a}_2+\boldsymbol{a}_{m+2}),\ \ldots .$$

Класс $2m$-параллелограммов имеет степень $m+1$. На рис. 21 изображен один специальный 12-параллелограмм.

4-параллелограммы являются также 4-угольниками, знакопеременная сумма вершин которых равна $\boldsymbol{o}$ (см. равенство (*) на стр. 19). Это условие позволяет также выделить определенный циклический класс $2m$-угольников, задаваемый циклической системой

$$\boldsymbol{a}_1-\boldsymbol{a}_2+\boldsymbol{a}_3-\boldsymbol{a}_4+\ldots+\boldsymbol{a}_{2m-1}-\boldsymbol{a}_{2m}=\boldsymbol{o},\ \ldots .$$

Все уравнения этой системы совпадают с первым уравнением, откуда следует, что рассматриваемый класс имеет степень $2m-1$. Этот циклический класс мы будем называть *АСО-классом* (буквы АСО напоминают нам, что здесь «Альтернированная (знакопеременная) Сумма (вершин) — Нуль»). Таким образом, получена

Теорема 3. *Множество $2m$-параллелограммов и множество $2m$-угольников класса АСО суть циклические классы $2m$-угольников.*

При $n=4$ оба эти циклических класса совпадают. Это совпадение имеет место только при $n=2m=4$, так как лишь при $m+1=2m-1$ степени этих классов одинаковы: из $m+1=2m-1$ следует, что $m=2$.

При $n=4m$ справедлива

Теорема 4. *Всякий $4m$-параллелограмм одновременно является АСО-многоугольником.*

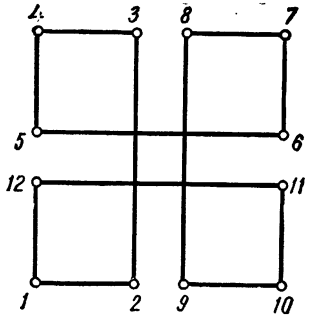


Рис. 21.

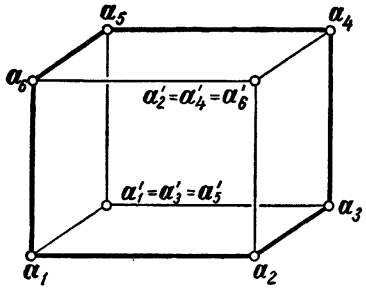


Рис. 22. 6-параллелограмм.

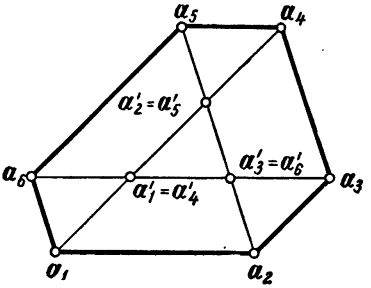


Рис. 23. АСО-6-угольник.

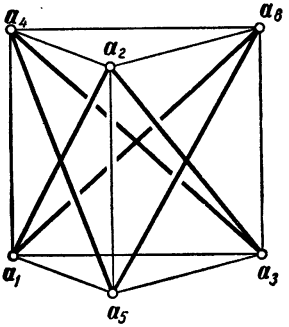


Рис. 24. Призма.

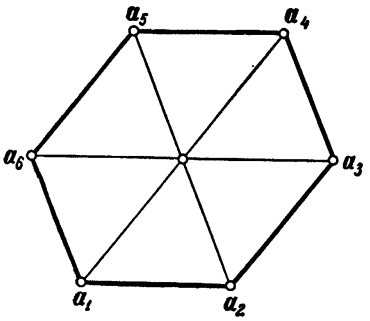


Рис. 25. Аффинно-правильный 6-угольник.

Доказательство. Если $(a_1, a_2, \ldots, a_8)$ есть 8-параллелограмм, то (a_1, a_2, a_5, a_6) и (a_3, a_4, a_7, a_8) — параллелограммы, откуда уже следует его принадлежность классу АСО. То же рассуждение проходит и в общем случае.

d) $n=6$. Имеется четыре периодических класса: $\mathcal{A}_6$, $\mathcal{A}_{3,2}$ (класс дважды пройденных треугольников), $\mathcal{A}_{2,3}$ (класс трижды пройденных отрезков), $\mathcal{A}_{1,6}$, а также, согласно теореме 3, класс 6-параллелограммов (рис. 22) и АСО-класс (рис. 23).

Во введении указан еще один вид 6-угольников — *призмы* (рис. 24). Расположим вершины произвольного 6-угольника в таблицу

$$\begin{matrix} a_1 & a_3 & a_5 \\ a_4 & a_6 & a_2 \end{matrix}$$

в которой индексы по строкам отличаются на две, а по столбцам — на три единицы. Тогда призму можно будет определить как такой 6-угольник, для которого в V существует параллельный перенос, переводящий точки первой строки таблицы в соответствующие точки второй строки. Циклическая система $a_1 - a_4 = a_3 - a_6, \ldots$ показывает, что множество призм является циклическим классом.

6-угольник называется *аффинно-правильным*, если в V существует такая точка, которая дополняет каждые три последовательные вершины 6-угольника до параллелограмма (рис. 25). Множество аффинно-правильных 6-угольников (обозначим его через $\mathcal{R}_6$) также является циклическим классом, так как оно может быть задано циклической системой

$$a_1 - a_2 + a_3 = a_2 - a_3 + a_4, \ldots .$$

В диаграмме (см. рис. 26) указаны включения, существующие между восемью циклическими классами 6-угольников. Если из одного класса диаграммы исходят два поднимающихся вверх отрезка, то каждый раз можно убедиться, что соответствующий класс является пересечением вышестоящих. В качестве примера покажем, что справедлива

Теорема 5. *Аффинно-правильные 6-угольники суть 6-параллелограммы с нулевой знакопеременной суммой вершин.*

Для доказательства заметим, что АСО-6-угольник, 6-параллелограмм и аффинно-правильный 6-угольник слу-

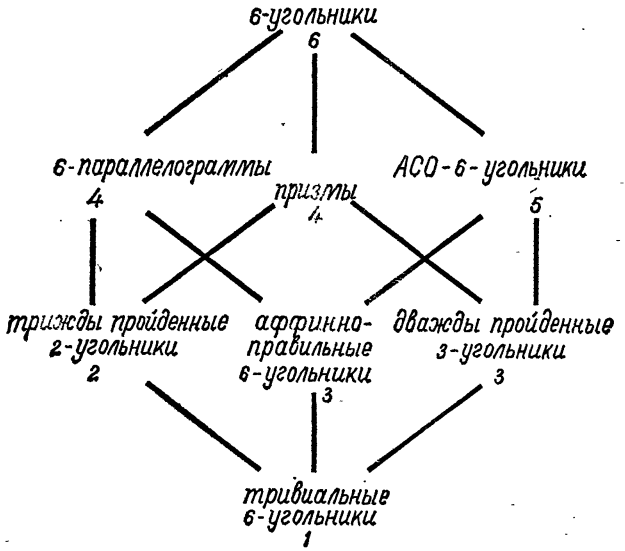


Рис. 26.

дующим образом определяются с помощью четвертой вершины $a_i' = a_i - a_{i+1} + a_{i+2}$ трех последовательных вершин a_i, a_{i+1}, a_{i+2}:

АСО-6-угольники суть 6-угольники, для которых

$$a_1' = a_4',\ a_2' = a_5',\ a_3' = a_6';$$

6-параллелограммы суть 6-угольники, для которых

$$a_1' = a_3' = a_5',\ a_2' = a_4' = a_6';$$

аффинно-правильные 6-угольники суть 6-угольники, для которых

$$a_1' = a_2' = a_3' = a_4' = a_5' = a_6'.$$

Отсюда сразу вытекает справедливость нашего предложения.

Отметим еще одно свойство степеней свободы: в изображенной на рис. 26 диаграмме имеются отрезки трех разных направлений, и вдоль отрезков каждого фиксированного направления разность степеней постоянна, причем сумма этих трех разностей равна разности между максимальной и минимальной степенями классов диаграммы.

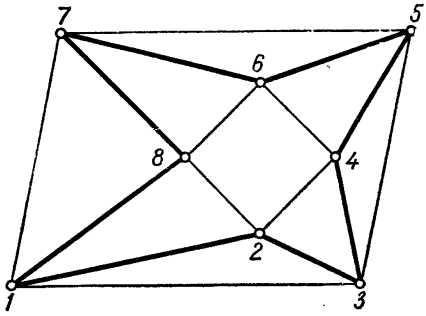


Рис. 27.

Случай $n=6$ есть первый действительно интересный пример развиваемой нами теории, и мы рекомендуем его читателю в качестве «самого главного» примера.

е) $n=8$. Наряду с четырьмя периодическими классами $\mathcal{A}_8$, $\mathcal{A}_{4,2}$ (класс дважды пройденных 4-угольников), $\mathcal{A}_{2,4}$ (класс четырежды пройденных отрезков) и $\mathcal{A}_{1,8}$ здесь имеются также (теорема 3) класс *8-параллелограммов* и *АСО-класс*. Из теоремы 4 следует, что АСО-класс охватывает класс 8-параллелограммов.

Далее, дважды пройденные параллелограммы составляют циклический класс, входящий в $\mathcal{A}_{4,2}$; он определяется системой

$$a_1-a_2+a_3-a_4=0, \ldots.$$

Кроме того, отметим множество 8-угольников, для которых оба хордовых четырехугольника (образованных вершинами, взятыми через одну) являются параллелограммами (рис. 27); это множество также является циклическим

классом, определенным системой

$$a_1 - a_3 + a_5 - a_7 = 0, \ldots .$$

В диаграмме (рис. 28) этот класс не назван, а лишь отмечен точкой, под которой стоит цифра 6—степень рассматриваемого класса.

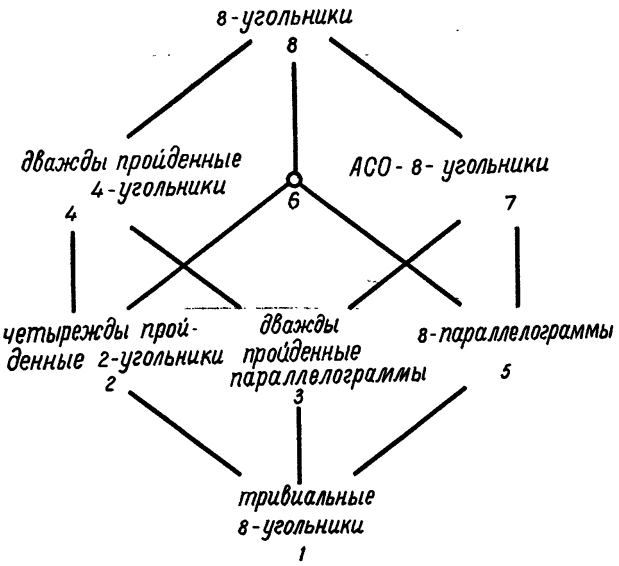


Рис. 28.

Диаграмма классов 8-угольников отличается от диаграммы восьми классов 6-угольников: периодические классы образуют в ней цепочку, призмы и аффинно-правильные 8-угольники отсутствуют. Классы дважды пройденных 4-угольников образуют поддиаграмму нашей диаграммы, совпадающую с диаграммой 4-угольников.

f) $n = 10$. Легко указать восемь циклических классов, аналогичных классам 6-угольников.

Вместо аффинно-правильных 6-угольников здесь появляется класс, определенный системой

$$a_1 - a_2 + a_3 - a_4 + a_5 = a_2 - a_3 + a_4 - a_5 + a_6, \ldots, .$$

Этой системе удовлетворяют обыкновенные правильные 10-угольники евклидовой плоскости и их аффинные образы (докажите!). Однако на рис. 29 показан 10-угольник этого класса, отнюдь не являющийся аффинно-правильным. Этот циклический класс имеет степень 5; максимальная размерность входящих в него 10-угольников равна 4 (если размерность V не менее 4).

Общим свойством для 6, 8, 10 является то, что эти числа имеют по 4 делителя.

g) $n=12$. Число 12 имеет 6 делителей; этот факт сильно увеличивает число свободных циклических классов.

1)—6) суть периодические классы 12-угольников, отвечающие делителям $d=12$, 6, 4, 3, 2, 1.

7)—11). Класс трижды пройденных параллелограммов определяется набором 12 чисел (1, —1, 1, —1, 0, ..., 0). Дважды пройденные 6-угольники классов АСО-6-параллелограммов, призм и аффинно-правильных 6-угольников образуют еще четыре циклических класса, отличных от вышеуказанных. Если $(c_0, c_1, \ldots, c_5)$ — набор коэффициентов, определяющих один из классов 6-угольников, то соответствующий класс 12-угольников определяется набором $(c_0, c_1, \ldots, c_5, 0, \ldots, 0)$.

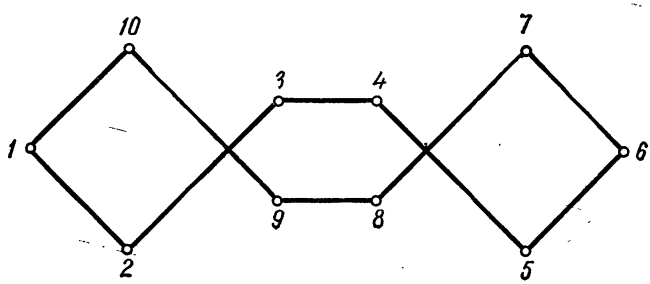


Рис. 29.

12)—16). Дальнейшие циклические классы получим путем наложения условий на хордовые d-угольники (см. § 5). Те 12-угольники, у которых три хордовых 4-угольника являются параллелограммами, образуют циклический класс, определяемый набором (1, 0, 0, —1, 0, 0, 1, 0, 0, —1, 0, 0). Аналогично 12-угольники,

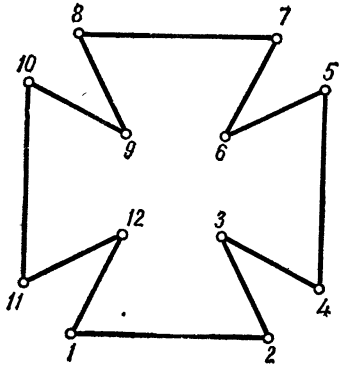


Рис. 30.

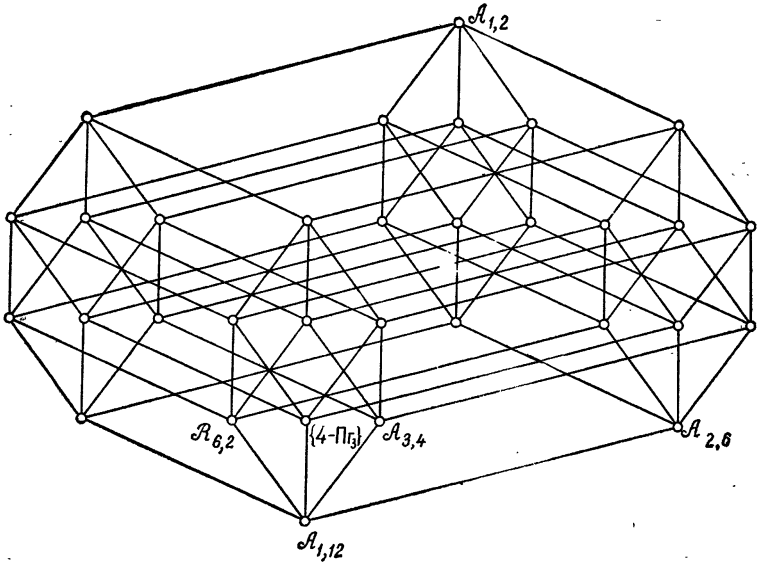


Рис. 31. 32 свободных циклических класса 12-угольников; $\mathcal{R}_{6,2}$ — класс дважды пройденных аффинно-правильных 6-угольников; {4-Пг$_3$} — класс трижды пройденных параллелограммов.

у которых хордовые 6-угольники принадлежат циклическим классам АСО, 6-параллелограммов, призм и аффинно-правильных 6-угольников, образуют циклические классы. Если $(c_0, \ldots, c_5)$ — набор, определяющий рассматриваемый класс 6-угольников [1]), то соответствующий класс 12-угольников определяется набором $(c_0, 0, c_1, 0, \ldots, c_5, 0)$. «Мальтийский крест», изображенный на рис. 30, есть 12-угольник, в котором оба хордовых 6-угольника аффинно-правильны.

17)—20). Другое требование, которое можно наложить на хордовые d-угольники,— это требование их *изобаричности*. Для $d=2, 3, 4, 6$ получается четыре циклических класса 12-угольников. Если изобаричны хордовые 2-угольники (пары противоположных вершин), то получаем 12-параллелограммы; если изобаричны хордовые 6-угольники, то получаем АСО-12-угольники.

В мальтийском кресте оба аффинно-правильных хордовых 6-угольника — и даже вообще все хордовые d-угольники — изобаричны.

21). Расположим вершины 12-угольника в таблицу

$$\begin{matrix} a_1 & a_4 & a_7 & a_{10} \\ a_5 & a_8 & a_{11} & a_2 \\ a_9 & a_{12} & a_3 & a_6 \end{matrix}$$

где индексы по горизонтали возрастают на три, а по вертикали — на четыре единицы (по модулю 12). Потребуем, чтобы существовали параллельные переносы, переводящие точки одной строки в соответствующие точки любой другой. Легко видеть, что это требование совпадает с аналогичным требованием для столбцов; 12-угольники, удовлетворяющие этому требованию, назовем (3, 4)-*призмами*. Очевидно, множество (3, 4)-призм определяется циклической системой

$$a_1 - a_5 = a_4 - a_8, \quad \ldots$$

и потому является циклическим классом.

Читателю предоставляется возможность определить дальнейшие циклические классы 12-угольников и расположить их в диаграмму (рис. 31).

[1]) Эти 6-наборы были таковы: (1, —1, 1, —1, 1, —1), (1, —1, 0, 1, —1, 0), (1, 0, —1, —1, 0, 1) и (1, —2, 2, —1, 0, 0).

Упражнения

1. Каждую вершину треугольника $a, b, c \in V$ отразим относительно каждой другой вершины (рис. 32). Полученный 6-угольник $(2a-b, 2a-c, 2b-c, 2b-a, 2c-a, 2c-b)$ имеет знакопеременную сумму, равную o.

2. Пусть $a, b, c, p \in V$. Построим отражение точки p относительно a, полученной точки — относительно b, затем относительно c и затем повторно относительно a, b и c. Полученная замкнутая фигура есть призма (рис. 33).

3. Пусть $a, b, c, p \in V$. Построим четвертые вершины параллелограммов $a-p+b$, $b-p+c$, $c-p+a$. Многоугольник $A=(a, a-p+b, b, b-p+c, c, c-p+a)$ есть 6-параллелограмм. Всякий ли 6-параллелограмм описывается таким образом?

Вершины шестиугольника $\frac{1}{2}(A+P)$, где $P=(p, \ldots, p)$, являются серединами ребер «тетраэдра» a, b, c, p. Многоугольник $\frac{1}{2}(A+P)$ также является 6-параллелограммом (рис. 34). Таким образом, три пары середин противоположных ребер тетраэдра имеют общую середину, являющуюся центром тяжести тетраэдра. Что мы получим, если p — центр тяжести (a, b, c)?

4. Пусть $n=d\cdot\bar{d}$ и $\mathscr{C}_d$ — циклический класс d-угольников. Множество n-угольников, в которых все хордовые d-угольники принадлежат классу $\mathscr{C}_d$, является циклическим классом. Набор n чисел, определяющий этот циклический класс, получается из d-набора $(c_0, \ldots, c_{d-1})$, если между каждыми двумя числами последнего поставить $\bar{d}-1$ нулей.

5. Пусть $n=d\bar{d}$ — разложение числа n на взаимно простые делители. Циклическая система

$$a_1' - a_{d+1} - a_{\bar{d}+1} + a_{d+\bar{d}+1} = o, \ldots$$

определяет циклический класс n-угольников. Назовем их $(d, \bar{d})$-*призмами*; $(d, \bar{d})$-призма состоит из $\bar{d}$ совместимых параллельными переносами d-угольников, или из d совместимых параллельными переносами $\bar{d}$-угольников; (2, 3)-призмы — это обычные 6-призмы. Всякий n-угольник есть $(n, 1)$-призма. Для каких n не существует больше никаких классов призм?

6. Пусть $n=d\cdot\bar{d}$. Если $\mathscr{C}_d$ — циклический класс d-угольников, то множество $\mathscr{C}_{d,\,\bar{d}}$ всех n-угольников, являющихся $\bar{d}$ раз пройденными d-угольниками из $\mathscr{C}_d$, т. е. множество n-угольников

$$(a_1, \ldots, a_d, a_1, \ldots, a_d, \ldots, a_1, \ldots, a_d),$$

где $(a_1, \ldots, a_d) \in \mathscr{C}_d$, является циклическим классом. Утверждение «если $(c_0, \ldots, c_{d-1})$ — определяющий набор для $\mathscr{C}_d$, то $\mathscr{C}_{d,\,\bar{d}}$ определяется набором $(c_0, \ldots, c_{d-1}, 0, \ldots, 0)$», вообще говоря, неверно.

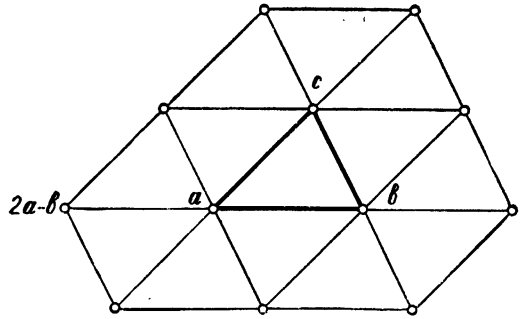


Рис. 32.

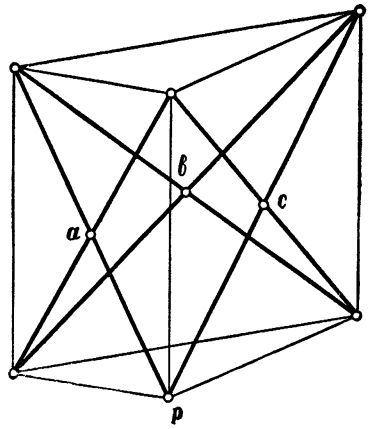


Рис. 33.

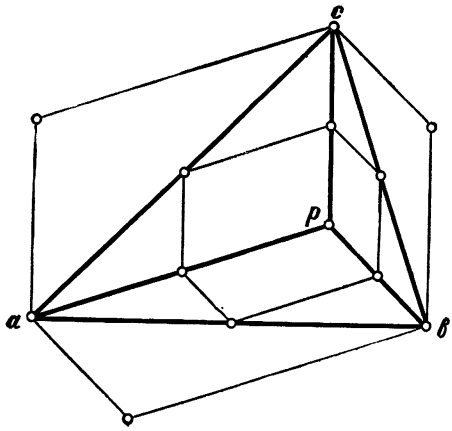


Рис. 34.

ГЛАВА 2

ЦИКЛИЧЕСКИЕ ОТОБРАЖЕНИЯ n-УГОЛЬНИКОВ

§ 1. Циклические отображения

Во введении приведены примеры отображений множества n-угольников в специальные подмножества, которые оказываются циклическими классами. Например, каждому n-угольнику ставится в соответствие n-угольник, образованный серединами сторон:

$$(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n) \to (\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n),$$

где

$$\boldsymbol{b}_1 = \frac{1}{2}(\boldsymbol{a}_1 + \boldsymbol{a}_2), \quad \boldsymbol{b}_2 = \frac{1}{2}(\boldsymbol{a}_2 + \boldsymbol{a}_3), \quad \ldots, \quad \boldsymbol{b}_n = \frac{1}{2}(\boldsymbol{a}_n + \boldsymbol{a}_1).$$

Система, определяющая это отображение, носит явно циклический характер: всякое последующее уравнение получается из предыдущего циклической подстановкой индексов 1, 2, ...

Дадим теперь общее определение. Линейное отображение множества всех n-угольников $\mathcal{A}_n$ в себя называется *циклическим*, если оно задается системой

$$\begin{aligned}
\boldsymbol{b}_1 &= c_0\boldsymbol{a}_1 + c_1\boldsymbol{a}_2 + \ldots + c_{n-1}\boldsymbol{a}_n,\\
\boldsymbol{b}_2 &= c_0\boldsymbol{a}_2 + c_1\boldsymbol{a}_3 + \ldots + c_{n-1}\boldsymbol{a}_1,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
\boldsymbol{b}_n &= c_0\boldsymbol{a}_n + c_1\boldsymbol{a}_1 + \ldots + c_{n-1}\boldsymbol{a}_{n-1},
\end{aligned} \tag{1}$$

где $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ — образ n-угольника $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)$ при данном отображении. Коэффициенты $(c_0, \ldots, c_{n-1})$ назовем *n-набором коэффициентов* циклического отображения. Ядро этого отображения (множество n-угольников, переходящих в $\boldsymbol{O}(\boldsymbol{o}, \boldsymbol{o}, \ldots, \boldsymbol{o})$) определяется однородной системой, получающейся, если в (1) положить $\boldsymbol{b}_i = \boldsymbol{o}$. Она совпадает с системой (2) гл. 1 (стр. 25) и, следовательно, определяет *циклический класс* (задаваемый тем же n-набором $(c_0, c_1, \ldots, c_{n-1})$). Итак, получена

Теорема 1. *Циклический класс является ядром циклического отображения с тем же набором коэффициентов.*

Эта определяющая связь между циклическими классами и циклическими отображениями является основанием для дальнейшего изучения циклических классов.

Теорема 2. *Различные n-наборы элементов из K определяют различные отображения.*

Доказательство. Надо доказать, что если два отображения совпадают, то совпадают также определяющие их n-наборы $(c_0, c_1, \ldots, c_{n-1})$ и $(d_0, d_1, \ldots, d_{n-1})$. Как и раньше, предположим, что пространство V состоит не из одного только нуль-вектора; итак, пусть $\boldsymbol{a} \neq \boldsymbol{o}$. По предположению оба циклических отображения переводят n-угольник $(\boldsymbol{a}, \boldsymbol{o}, \ldots, \boldsymbol{o})$ в один и тот же n-угольник, т. е.

$$(c_0\boldsymbol{a}, c_{n-1}\boldsymbol{a}, \ldots, c_1\boldsymbol{a}) = (d_0\boldsymbol{a}, d_{n-1}\boldsymbol{a}, \ldots, d_1\boldsymbol{a}).$$

Так как $\boldsymbol{a} \neq \boldsymbol{o}$, отсюда следует, что $c_i = d_i$ для всех $i = 0, 1, \ldots, n-1$.

Итак, *число циклических отображений равно числу n-наборов элементов из K.* Различные циклические отображения могут иметь один и тот же циклический класс в качестве ядра. К числу стоящих перед нами задач относится и задача определения количества циклических классов.

Примеры из введения приводят к близкому вопросу: *всякое ли циклическое отображение переводит множество всех n-угольников в циклический класс?* В этой и следующей главах будут найдены образы геометрически наглядных циклических отображений. Ответ на общий вопрос будет дан в гл. 6 и далее.

§ 2. Алгебра циклических отображений

Прежде чем перейти к примерам, мы хотим очертить общие рамки наших исследований.

Пусть φ — отображение множества $\mathcal{A}_n$ в себя. Через $\varphi\boldsymbol{A}$ обозначим образ n-угольника $\boldsymbol{A}$ при этом отображе-

нии. Полный образ и ядро отображения φ обозначим так:

$$\operatorname{Ker}\varphi=\{\boldsymbol{A}:\varphi\boldsymbol{A}=\boldsymbol{O}\},\quad \operatorname{Im}\varphi=\varphi\mathcal{A}_n=\{\varphi\boldsymbol{A}:\boldsymbol{A}\in\mathcal{A}_n\}.$$

Пусть φ, ψ, ...—эндоморфизмы векторного пространства $\mathcal{A}_n$ (линейные отображения $\mathcal{A}_n$ в себя). Сложение, умножение на число $c\in K$ и произведение эндоморфизмов определяются равенствами

$$(\varphi+\psi)\boldsymbol{A}=\varphi\boldsymbol{A}+\psi\boldsymbol{A},\qquad (c\varphi)\boldsymbol{A}=c(\varphi\boldsymbol{A}),\qquad (\psi\varphi)\boldsymbol{A}=\psi(\varphi\boldsymbol{A}),$$

так что умножение эндоморфизмов — это их последовательное выполнение. Обозначим через 0 нулевой эндоморфизм φ, для которого $\operatorname{Im}\varphi=\boldsymbol{O}$, и через 1—единичный эндоморфизм ψ, для которого $\psi\boldsymbol{A}=\boldsymbol{A}$ для всех $\boldsymbol{A}$. По отношению к названным операциям множество эндоморфизмов образует алгебру над K, которую мы обозначим через $\operatorname{End}(\mathcal{A}_n)$; 0 и 1—нулевой и единичный элементы этой алгебры.

Циклические отображения являются частными случаями эндоморфизмов. Отображение

$$\zeta\colon (\boldsymbol{a}_1,\ \boldsymbol{a}_2,\ \ldots,\ \boldsymbol{a}_n)\to(\boldsymbol{a}_2,\ \ldots,\ \boldsymbol{a}_n,\ \boldsymbol{a}_1)$$

является циклическим и определяется n-набором коэффициентов (0, 1, 0, ..., 0). [При $n=1$ имеем $\zeta=1$.] Очевидно, что $\zeta^n=1$. Степени

$$1,\ \zeta,\ \zeta^2,\ \ldots,\ \zeta^{n-1} \tag{2}$$

эндоморфизма ζ образуют циклическую группу порядка n и переводят каждый n-угольник $\boldsymbol{A}$ в множество n-угольников, получающихся из $\boldsymbol{A}$ циклическими подстановками вершин. Очевидно, что *всякий циклический класс инвариантен относительно* ζ.

Пусть теперь φ—циклическое отображение, определяемое n-набором $(c_0,\ c_1,\ \ldots,\ c_{n-1})$. Тогда систему (1) можно переписать так:

$$\begin{aligned}
&(\boldsymbol{b}_1,\ \boldsymbol{b}_2,\ \ldots,\ \boldsymbol{b}_n)=\\
&=(c_0\boldsymbol{a}_1,\ c_0\boldsymbol{a}_2,\ \ldots,\ c_0\boldsymbol{a}_n)+ &&=c_0\mathrm{1}\,(\boldsymbol{a}_1,\ \boldsymbol{a}_2,\ \ldots,\ \boldsymbol{a}_n)+\\
&+(c_1\boldsymbol{a}_2,\ c_1\boldsymbol{a}_3,\ \ldots,\ c_1\boldsymbol{a}_1)+ &&+c_1\zeta\,(\boldsymbol{a}_1,\ \boldsymbol{a}_2,\ \ldots,\ \boldsymbol{a}_n)+\\
&\ldots\ldots\ldots\ldots\ldots &&\ldots\ldots\ldots\ldots\ldots\\
&+(c_{n-1}\boldsymbol{a}_n,\ \ldots,\ c_{n-1}\boldsymbol{a}_{n-1})= &&+c_{n-1}\zeta^{n-1}(\boldsymbol{a}_1,\ \boldsymbol{a}_2,\ \ldots,\ \boldsymbol{a}_n)=\\
&=\sum_{i=0}^{n-1}c_i\zeta^i(\boldsymbol{a}_1,\ \boldsymbol{a}_2,\ \ldots,\ \boldsymbol{a}_n).
\end{aligned}$$

Поскольку $(a_1, \ldots, a_n)$ — любой n-угольник, получена

Теорема 3. *Циклическое отображение с набором коэффициентов* $(c_0, c_1, \ldots, c_{n-1})$ *представимо в алгебре* $\mathrm{End}(\mathcal{A}_n)$ *в виде*

$$\sum_{i=0}^{n-1} c_i \zeta^i. \tag{3}$$

Разумеется, само отображение ζ не представляет никакого геометрического интереса; однако всякое циклическое отображение оказывается представимым в виде линейной комбинации степеней (2), которые в силу теоремы 2 линейно независимы. Действия с этими линейными комбинациями полностью определяются операциями в алгебре $\mathrm{End}(\mathcal{A}_n)$. Равенства

$$\sum c_i \zeta^i + \sum d_i \zeta^i = \sum (c_i + d_i)\zeta^i, \quad c \cdot \sum c_i \zeta^i = \sum (cc_i)\zeta^i$$

показывают, как производится *сложение* циклических отображений и *умножение на число* $c \in K$. При перемножении двух линейных комбинаций степеней ζ^i следует учитывать, что $\zeta^n = 1$; поэтому

$$\sum d_i \zeta^i \cdot \sum c_i \zeta^i = \sum e_i \zeta^i,$$

где

$$\begin{aligned} e_0 &= d_0c_0 + d_1c_{n-1} + \ldots + d_{n-1}c_1, \\ e_1 &= d_0c_1 + d_1c_0 + \ldots + d_{n-1}c_2, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ e_{n-1} &= d_0c_{n-1} + d_1c_{n-2} + \ldots + d_{n-1}c_0. \end{aligned} \tag{4}$$

Таким образом, *произведение циклических отображений снова является циклическим отображением.*

Коэффициенты произведения не меняются при замене c_i на d_i, и наоборот. Отсюда следует, что произведение циклических отображений коммутативно:

Теорема 4. *Циклические отображения образуют коммутативную алгебру над* K, *подалгебру алгебры* $\mathrm{End}(\mathcal{A}_n)$, *с базисом* $1, \zeta, \ldots, \zeta^{n-1}$.

Эта алгебра является одновременно *групповой алгеброй* (над K) *циклической группы, порожденной элементом* ζ.

Мы будем обозначать ее через $K[\zeta]$ и более подробно рассмотрим в § 1 гл. 8.

Из коммутативности циклических отображений в силу теоремы 1 вытекает, что *циклические классы инвариантны относительно всех циклических отображений.*

Теорема 5. *Если ψ — циклическое отображение, а $\mathscr{C}$ — произвольный циклический класс, то $\psi\mathscr{C} \subset \mathscr{C}$.*

Доказательство. В силу теоремы 1, $\mathscr{C}$ является ядром некоторого циклического отображения φ: $\mathscr{C} = \operatorname{Ker}\varphi$. Если $\boldsymbol{A} \in \operatorname{Ker}\varphi$, то $\varphi\boldsymbol{A} = \boldsymbol{O}$; поэтому тем более $\psi\varphi\boldsymbol{A} = \psi\boldsymbol{O} = \boldsymbol{O}$. Но так как $\psi\varphi = \varphi\psi$, то $\varphi\psi\boldsymbol{A} = \boldsymbol{O}$, откуда следует, что $\psi\boldsymbol{A} \in \operatorname{Ker}\varphi$.

§ 3. Сумма коэффициентов циклического отображения

Некоторые свойства циклического отображения $\varphi = \sum c_i\zeta^i$ связаны с числом $s(\varphi) \in K$ — *суммой коэффициентов* этого отображения. Соответствие

$$\varphi = \sum c_i\zeta^i \longrightarrow s(\varphi) = \sum c_i \tag{5}$$

является гомоморфизмом алгебры $K[\zeta]$ в K: действительно, равенство

$$s(\varphi\psi) = s(\varphi)\cdot s(\psi)$$

непосредственно следует из (4).

Аналогично, из определения (1) циклического отображения следует, что

$$\sum \boldsymbol{b}_i = \sum c_i \cdot \sum \boldsymbol{a}_i, \quad \text{или} \quad \frac{1}{n}\sum \boldsymbol{b}_i = \sum c_i \cdot \frac{1}{n}\sum \boldsymbol{a}_i. \tag{6}$$

Отсюда вытекает:

Если сумма коэффициентов $s(\varphi)$ циклического отображения φ равна 0, то φ переводит каждый n-угольник в n-угольник с центром тяжести $\boldsymbol{O}$, а все множество $\mathscr{A}_n$ в нуль-изобарический класс $\mathscr{A}_n^{\circ}$. Такие отображения составляют ядро гомоморфизма (5) и, следовательно, идеал алгебры $K[\zeta]$.

Циклические отображения φ с суммой коэффициентов $s(\varphi) = 1$ — это те отображения, которые сохраняют центр

тяжести любого n-угольника и, следовательно, изобарические классы. Такие циклические отображения мы будем называть *изобарическими циклическими отображениями.* Произведение таких отображений является изобарическим циклическим отображением.

Пример. Отображение σ из § 3 гл. 1, сопоставляющее каждому n-угольнику его центр тяжести, есть изобарическое циклическое отображение с набором коэффициентов $\left(\frac{1}{n}, \frac{1}{n}, \ldots, \frac{1}{n}\right)$:

$$\sigma = \frac{1}{n}(1 + \zeta + \zeta^2 + \ldots + \zeta^{n-1}).$$

Очевидно, что

$$\operatorname{Im} \sigma = \mathcal{A}_{1,n}, \quad \operatorname{Ker} \sigma = \mathring{\mathcal{A}}_n.$$

Теорема 1 допускает уточнение. Всякий циклический класс служит ядром циклического отображения, либо имеющего нулевую сумму коэффициентов, либо изобарического. Действительно, если $s(\varphi) \neq 0$, то $\frac{1}{s(\varphi)}\varphi$ — изобарическое отображение с тем же ядром, что и φ. Отсюда и из теоремы 1 гл. 1 следует

Теорема 6. *Свободные циклические классы являются ядрами циклических отображений с нулевой суммой коэффициентов; центральные классы — ядрами изобарических отображений.*

Упражнения

1. Пусть $\boldsymbol{A} = (a_1, a_2, \ldots, a_n)$. Вершины n-угольника $(\zeta - 1)\boldsymbol{A}$ являются «векторами сторон» $a_{j+1} - a_j$ для $\boldsymbol{A}$; при этом

$$\operatorname{Im}(\zeta - 1) = \mathring{\mathcal{A}}_n, \quad \operatorname{Ker}(\zeta - 1) = \mathcal{A}_{1,n}.$$

2. Обратимые циклические отображения образуют группу относительно умножения в $K[\zeta]$. Всякое обратимое циклическое отображение взаимно однозначно переводит в себя любой циклический класс. Примеры: *растяжение* (или *гомотетия*) $c \cdot 1$, где $c \neq 0$ — элемент из K; *отражение n-угольника относительно его центра тяжести* $2\sigma - 1$; ζ; $\zeta - c$, где $c^n \neq 1$. Какие из этих отображений являются изобарическими?

Циклические отображения с суммой коэффициентов 0 необратимы.

3. Пусть φ — циклическое отображение. Множество $\operatorname{Fix}\varphi = \{A : \varphi A = A\}$ есть циклический класс. Если φ изобарично, то $\operatorname{Fix}\varphi$ — свободный класс. Пример: если d — делитель n, то $\operatorname{Fix}\zeta^d = \mathcal{A}_{d,\overline{d}}$; при $n=4$ класс $\operatorname{Fix}(\zeta - \zeta^2 + \zeta^3)$ — это класс параллелограммов.

Для всякого циклического класса $\mathscr{C}$ существует циклическое отображение, для которого $\mathscr{C} = \operatorname{Fix}\varphi$. Исследуйте соотношение $\operatorname{Fix}\varphi = \operatorname{Fix}\psi$; например, если $\operatorname{Char} K \neq 2$, то $\operatorname{Fix}\varphi = \operatorname{Fix}(2\varphi - 1)$.

§ 4. Проекции

Пусть M — любое множество элементов a, b, ..., а φ, ψ, ... — отображения M в себя. Будем обозначать через $\operatorname{Im}\varphi$ *образ* M, а через $\operatorname{Fix}\varphi$ множество *неподвижных элементов* отображения φ:

$$\operatorname{Im}\varphi = \{\varphi a : a \in M\}, \quad \operatorname{Fix}\varphi = \{a : \varphi a = a\}.$$

($\operatorname{Fix}\varphi$ есть максимальное подмножество M, на котором φ тождественно.) Очевидно, что $\operatorname{Fix}\varphi \subseteq \operatorname{Im}\varphi$.

Отображение φ, такое, что $\varphi\varphi = \varphi$, называется *идемпотентным* отображением *(идемпотентом)*, или *проекцией (проектированием)* M в себя. Утверждение, что φ есть проекция, эквивалентно каждому из трех следующих утверждений:

1) сужение φ на $\operatorname{Im}\varphi$ является тождественным отображением;

2) $\operatorname{Im}\varphi = \operatorname{Fix}\varphi$;

3) $\operatorname{Im}\varphi \subseteq \operatorname{Fix}\varphi$.

Различные проекции могут иметь один и тот же образ. Замечательно, однако, что если проекции коммутируют, то из совпадения образов следует совпадение самих проекций:

Теорема 7. *Если* φ *и* ψ *— коммутирующие проекции* (т. е. $\varphi\psi = \psi\varphi$) *и* $\operatorname{Im}\varphi = \operatorname{Im}\psi$, *то* $\varphi = \psi$.

Доказательство. Пусть a — любой элемент из M. По условию теоремы $\operatorname{Im}\varphi = \operatorname{Im}\psi \subseteq \operatorname{Fix}\psi$. Таким образом, $\varphi a \in \operatorname{Fix}\psi$, т. е. $\psi\varphi a = \varphi a$. Аналогично $\varphi\psi a = \psi a$, но так как $\varphi\psi = \psi\varphi$, то $\varphi a = \psi a$ (для всех a).

Квазипроекцией будем называть такое отображение M в себя, которое на образе M действует взаимно одно-

значно (другими словами, сужение $\varphi|_{\mathrm{Im}\,\varphi}$ которого на образ $\mathrm{Im}\,\varphi$ множества M взаимно однозначно).

Введем обозначение $\hat{\varphi} = \varphi|_{\mathrm{Im}\,\varphi}$. Тогда если φ — квазипроекция, то $\hat{\varphi}^{-1}\varphi$ — проекция M на $\mathrm{Im}\,\varphi$.

Пусть теперь $(\mathcal{A}, +)$ — абелева группа с элементами $\boldsymbol{o}, \boldsymbol{a}, \ldots$; $\varphi, \psi, \ldots$ — эндоморфизмы $\mathcal{A}$. Ясно, что $\mathrm{Im}\,\varphi$ и $\mathrm{Fix}\,\varphi$ являются подгруппами в $\mathcal{A}$. Наряду с ними φ задает еще одну подгруппу — *ядро* φ:

$$\mathrm{Ker}\,\varphi = \{\boldsymbol{a} : \varphi\boldsymbol{a} = \boldsymbol{o}\}.$$

Множество эндоморфизмов $\mathcal{A}$ является *кольцом* по отношению к операциям сложения $((\varphi + \psi)\,\boldsymbol{a} = \varphi\boldsymbol{a} + \psi\boldsymbol{a})$ и умножения (т. е. последовательного выполнения эндоморфизмов); нулем этого кольца является эндоморфизм 0, переводящий каждый элемент $\mathcal{A}$ в $\boldsymbol{o}$; единицей — тождественный эндоморфизм 1. Если φ — эндоморфизм, то $1 - \varphi$ — тоже эндоморфизм. Положим $1 - \varphi = \varphi'$; тогда $\varphi'' = \varphi$, т. е. $\varphi \longrightarrow 1 - \varphi$ есть инволютивное соответствие в кольце эндоморфизмов $\mathcal{A}$. Очевидно, справедливы соотношения

$$\mathrm{Fix}\,\varphi = \mathrm{Ker}\,(1 - \varphi); \quad \mathrm{Ker}\,\varphi = \mathrm{Fix}\,(1 - \varphi).$$

Пусть теперь φ — идемпотентный эндоморфизм, или проекция в $\mathcal{A}$. Тогда $1 - \varphi$ — тоже проекция и выполняются равенства

$$1 = \varphi + (1 - \varphi), \quad \varphi(1 - \varphi) = (1 - \varphi)\varphi = 0.$$

Два отображения, удовлетворяющие последним равенствам, называются *взаимно дополнительными*. Имеем также

$$\mathrm{Im}\,\varphi = \mathrm{Ker}\,(1 - \varphi), \quad \mathrm{Ker}\,\varphi = \mathrm{Im}\,(1 - \varphi). \tag{7}$$

Теорема 8. *Если φ — идемпотентный эндоморфизм абелевой группы $\mathcal{A}$, то*

$$\mathcal{A} = \mathrm{Im}\,\varphi \oplus \mathrm{Ker}\,\varphi. \tag{8}$$

[Последнее равенство означает, что

$$\mathcal{A} = \mathrm{Im}\,\varphi + \mathrm{Ker}\,\varphi \text{ и } \mathrm{Im}\,\varphi \cap \mathrm{Ker}\,\varphi = \{\boldsymbol{o}\}.$$

Говорят также, что $\mathrm{Im}\,\varphi$ и $\mathrm{Ker}\,\varphi$ — дополняющие друг друга подгруппы группы $\mathcal{A}$.]

Доказательство. Для всех $\boldsymbol{a} \in \mathcal{A}$ имеем

$$\boldsymbol{a} = \boldsymbol{a} \cdot 1 = \varphi\boldsymbol{a} + (1-\varphi)\,\boldsymbol{a} \in \operatorname{Im}\varphi + \operatorname{Im}(1-\varphi) = \\ = \operatorname{Im}\varphi + \operatorname{Ker}\varphi.$$

Если $\boldsymbol{a} \in \operatorname{Im}\varphi \cap \operatorname{Ker}\varphi$, то (поскольку $\operatorname{Im}\varphi = \operatorname{Fix}\varphi$)

$$\varphi\boldsymbol{a} = \boldsymbol{a} \text{ и } \varphi\boldsymbol{a} = \boldsymbol{o}, \text{ откуда } \boldsymbol{a} = \boldsymbol{o}.$$

Эндоморфизм φ группы $\mathcal{A}$ тогда и только тогда есть квазипроекция, когда

$$\operatorname{Im}\varphi^2 = \operatorname{Im}\varphi \quad \text{и} \quad \operatorname{Ker}\varphi^2 = \operatorname{Ker}\varphi. \tag{9}$$

Действительно, φ — квазипроекция тогда и только тогда, когда всякий элемент из $\operatorname{Im}\varphi$ имеет свой прообраз в $\operatorname{Im}\varphi$:

$$\operatorname{Im}\varphi \in \varphi \operatorname{Im}\varphi,$$

или, поскольку $\varphi \operatorname{Im}\varphi = \operatorname{Im}\varphi^2$,

$$\operatorname{Im}\varphi \subseteq \operatorname{Im}\varphi^2, \quad \text{т. е.} \quad \operatorname{Im}\varphi = \operatorname{Im}\varphi^2$$

(обратное включение очевидно). Далее, утверждение: «φ действует на $\operatorname{Im}\varphi$ взаимно однозначно» эквивалентно утверждению: «из $\varphi\varphi\boldsymbol{a} = \boldsymbol{o}$ следует $\varphi\boldsymbol{a} = \boldsymbol{o}$», т. е. эквивалентно включению

$$\operatorname{Ker}\varphi^2 \subseteq \operatorname{Ker}\varphi.$$

Таким образом, φ есть квазипроекция тогда и только тогда, когда

$$\operatorname{Im}\varphi \subseteq \operatorname{Im}\varphi^2, \quad \operatorname{Ker}\varphi^2 \subseteq \operatorname{Ker}\varphi,$$

т. е. когда (9) имеют место (поскольку обратные включения тривиальны).

Теорема 8′. *Для того чтобы эндоморфизм φ абелевой группы $\mathcal{A}$ удовлетворял условию* (8), *необходимо и достаточно, чтобы φ был квазипроекцией.*

Доказательство. Следующие высказывания эквивалентны между собой:

1) для всякого $\varphi\boldsymbol{a}$ существует $\varphi\boldsymbol{b}$, такой, что $\varphi\boldsymbol{a} = \varphi\varphi\boldsymbol{b}$;

2) для всякого a существует b, такой, что $\varphi a = \varphi\varphi b$, или $\varphi(a - \varphi b) = o$, или $a - \varphi b \in \operatorname{Ker}\varphi$, или $a = \varphi b + (a - \varphi b)$, где $a - \varphi b \in \operatorname{Ker}\varphi$;

3) $\mathcal{A} \in \operatorname{Im}\varphi + \operatorname{Ker}\varphi$.

Кроме того, эквивалентны высказывания: из $\varphi\varphi a = o$ следует $\varphi a = o$; из $\varphi a \in \operatorname{Ker}\varphi$ следует $\varphi a = o$; $\operatorname{Im}\varphi \cap \operatorname{Ker}\varphi = \{o\}$.

Проекции существуют и среди циклических отображений множества всех n-угольников $\mathcal{A}_n$ в себя; будем называть их *циклическими проекциями*. Так, 0 и 1 — циклические проекции. В § 1 этой главы был поставлен вопрос об образах циклических отображений. Следующая теорема дает на него частичный ответ:

Теорема 9. *Если* φ *— циклическая проекция, то* $\operatorname{Im}\varphi$ *— циклический класс.*

Доказательство. Если φ — циклическая проекция, то $1 - \varphi$ — тоже циклическая проекция. Тогда $\operatorname{Im}\varphi = \operatorname{Ker}(1 - \varphi)$; но $\operatorname{Ker}(1 - \varphi)$ является циклическим классом (теорема 1).

Сумма коэффициентов $s(\varphi)$ циклической проекции φ равна 0 или 1. Действительно, отображение $\varphi \to s(\varphi)$ является гомоморфизмом $K[\zeta]$ на K. Если φ — идемпотент, то $s(\varphi)$ — тоже идемпотент в K, но поле не имеет идемпотентных элементов, отличных от 0 и 1. Если $s(\varphi) = 1$, то $s(1 - \varphi) = 0$ (и наоборот). Отсюда и из теоремы 6 следует, что *если* φ *— изобарическая циклическая проекция, то* $\operatorname{Im}\varphi$ *— свободный циклический класс. Если же* $s(\varphi) = 0$, *то* $\operatorname{Im}\varphi$ *— центральный циклический класс.*

Образ и ядро любой циклической проекции являются взаимно дополнительными подпространствами векторного пространства $\mathcal{A}_n$ (см. теорему 8).

Суммируем полученные результаты:

Теорема 9′. *Если* φ *— циклическая проекция, то* $\operatorname{Im}\varphi$ *и* $\operatorname{Ker}\varphi$ *— взаимно дополнительные циклические классы. Если при этом* φ *изобарично, то* $\operatorname{Im}\varphi$ *— свободный, а* $\operatorname{Ker}\varphi$ *— центральный циклические классы; если же* $s(\varphi) = 0$,

то, напротив, $\operatorname{Ker}\varphi$ — *свободный, а* $\operatorname{Im}\varphi$ — *центральный классы.*

Пример: σ есть изобарическая циклическая проекция, $\operatorname{Im}\sigma = \mathcal{A}_{1,n}$ — класс тривиальных n-угольников, $\operatorname{Ker}\sigma$ — нуль-изобарический класс $\overset{\circ}{\mathcal{A}}_n$ (см. § 3 гл. 1 и § 3 этой главы). Далее, $1-\sigma$ есть циклическая проекция с нулевой суммой коэффициентов. Итак,

$$\mathcal{A}_n = \mathcal{A}_{1,n} \oplus \overset{\circ}{\mathcal{A}}_n, \quad \text{где} \quad \operatorname{Im}\sigma = \mathcal{A}_{1,n} = \operatorname{Ker}(1-\sigma),$$

$$\operatorname{Ker}\sigma = \overset{\circ}{\mathcal{A}}_n = \operatorname{Im}(1-\sigma).$$

Пусть $\boldsymbol{A}$ — произвольный n-угольник. Разложение

$$\boldsymbol{A} = \sigma\boldsymbol{A} + (1-\sigma)\boldsymbol{A}$$

является представлением $\boldsymbol{A}$ в виде суммы тривиального n-угольника — центра тяжести $\boldsymbol{A}$ — и n-угольника, полученного из $\boldsymbol{A}$ таким параллельным переносом, чтобы его новый центр тяжести совпал с $\boldsymbol{o}$. Это представление $\boldsymbol{A}$ в виде суммы тривиального и нуль-изобарического n-угольников единственно.

Упражнение. Эндоморфизм абелевой группы тогда и только тогда является квазипроекцией, когда существует некоторая проекция, имеющая с данным эндоморфизмом одинаковые образ и ядро. Так как проекция полностью определяется своими образом и ядром, то для заданной квазипроекции φ искомая проекция единственна и равна $\widehat{\varphi}^{-1}\varphi$.

§ 5. Примеры

Мы укажем примеры изобарических циклических отображений для $n=4$ и $n=6$.

а) $n=4$. *Циклическое отображение* $(\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3, \boldsymbol{a}_4) \longrightarrow (\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, \boldsymbol{b}_4)$:

$$\boldsymbol{b}_1 = \tfrac{1}{2}(\boldsymbol{a}_1 + \boldsymbol{a}_2), \ \ldots$$

ставит в соответствие каждому 4-угольнику 4-угольник середин его сторон. Обозначим это отображение через $\varkappa_2$:

$$\varkappa_2(\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3, \boldsymbol{a}_4) = \left(\tfrac{1}{2}(\boldsymbol{a}_1+\boldsymbol{a}_2), \ \tfrac{1}{2}(\boldsymbol{a}_2+\boldsymbol{a}_3), \ \tfrac{1}{2}(\boldsymbol{a}_3+\boldsymbol{a}_4), \ \tfrac{1}{2}(\boldsymbol{a}_4+\boldsymbol{a}_1)\right).$$

Образ всякого 4-угольника при этом отображении имеет знакопеременную сумму вершин нуль и, следовательно, является параллелограммом; $\operatorname{Im} \varkappa_2$ является циклическим классом параллелограммов. При этом $\varkappa_2$ переводит в множество тривиальных 4-угольников класс дважды пройденных отрезков (a_1, a_2, a_1, a_2), т. е. $\mathcal{A}_{2,2}$ в $\mathcal{A}_{1,4}$.

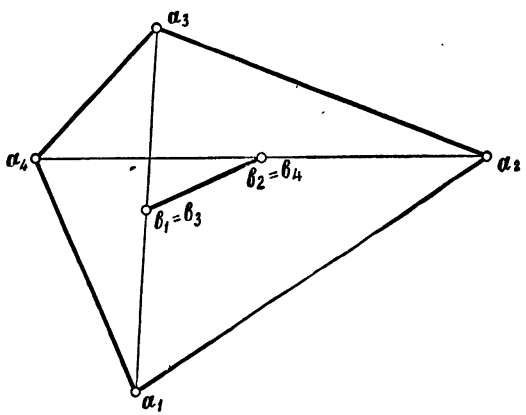


Рис. 35.

Перейдем теперь к *изобарическим циклическим отображениям* $\mathcal{A}_4$ в $\mathcal{A}_{2,2}$. Очевидно, что таким является отображение

$$b_1 = \frac{1}{2}(a_1 + a_3), \ \ldots,$$

которое каждому 4-угольнику ставит в соответствие дважды пройденный 2-угольник середин диагоналей исходного 4-угольника (рис. 35). Прообразами тривиальных 4-угольников являются здесь параллелограммы. Это отображение обозначим через μ_2.

Итак, для всех отрезков диаграммы свободных классов 4-угольников из § 8 гл. 1 мы имеем циклическое отображение, которое переводит верхний класс в нижний

(рис. 36). Последовательное выполнение $\varkappa_2\mu_2$ тривиализирует все 4-угольники.

Как элементы $K[\zeta]$, $\varkappa_2$ и μ_2 можно записать так:

$$\varkappa_2 = \frac{1}{2}(1+\zeta), \quad \mu_2 = \frac{1}{2}(1+\zeta^2),$$

откуда

$$\varkappa_2\mu_2 = \frac{1}{2}(1+\zeta)\cdot\frac{1}{2}(1+\zeta^2) = \frac{1}{4}(1+\zeta+\zeta^2+\zeta^3) = \sigma.$$

Отображение μ_2 является циклической проекцией (идемпотентом). Действительно,

$$\left(\frac{1}{2}(1+\zeta^2)\right)^2 = \frac{1}{4}(1+2\zeta^2+\zeta^4) = \frac{1}{2}(1+\zeta^2), \text{ так как } \zeta^4 = 1.$$

Примечание. Буква $\varkappa$ с индексом всегда обозначает отображение, сопоставляющее каждому n-угольнику

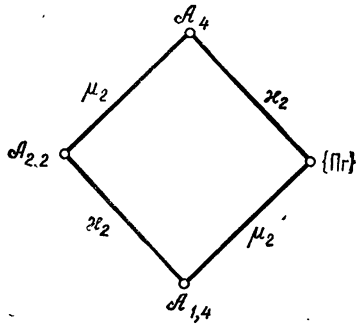


Рис. 36.

n-угольник центров тяжести нескольких последовательных вершин исходного; μ с индексом обозначает отображение, сопоставляющее каждому n-угольнику n-угольник центров тяжести хордовых многоугольников. Это так называемые *последовательные* и *хордовые усреднения* (см. гл. 4).

b) $n = 6$. Через $\varkappa_2$, $\varkappa_3$, α_3 обозначим циклические отображения $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_6) \to (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_6)$, заданные посред-

ством циклических систем

$$\varkappa_2\colon \quad \boldsymbol{b}_1=\frac{1}{2}(\boldsymbol{a}_1+\boldsymbol{a}_2),\ \ldots,$$

$$\varkappa_3\colon \quad \boldsymbol{b}_1=\frac{1}{3}(\boldsymbol{a}_1+\boldsymbol{a}_2+\boldsymbol{a}_3),\ \ldots,$$

$$\alpha_3\colon \quad \boldsymbol{b}_1=\boldsymbol{a}_1-\boldsymbol{a}_2+\boldsymbol{a}_3,\ \ldots;$$

$\varkappa_2$ — знакомое нам отображение, сопоставляющее каждому 6-угольнику 6-угольник середин его сторон; $\varkappa_2$ и $\varkappa_3$ — отображения в 6-угольники центров тяжести соответственно двух и трех последовательно взятых вершин исходного 6-угольника; α_3 переводит 6-угольник в 6-угольник, состоящий из четвертых вершин последовательных троек вершин исходного 6-угольника. Для этих трех отображений справедливы следующие предложения введения:

1°. $\varkappa_2$ *отображает* $\mathcal{A}_6$ *в класс* 6*-угольников с нулевой знакопеременной суммой вершин*;

2°. $\varkappa_3$ *отображает* $\mathcal{A}_6$ *в класс* 6*-параллелограммов*;

3°. α_3 *отображает* $\mathcal{A}_6$ *в класс призм* (см. рис. 37—40).

В их справедливости мы убеждаемся элементарным подсчетом:

1°. $\sum(\pm\boldsymbol{b}_i)=\boldsymbol{o}$ [$\sum(\pm\boldsymbol{b}_i)$ — знакопеременная сумма вершин].

2°. Из системы, определяющей $\varkappa_3$, следует, что

$$\frac{1}{2}(\boldsymbol{b}_1+\boldsymbol{b}_4)=\frac{1}{2}(\boldsymbol{b}_2+\boldsymbol{b}_5)=\frac{1}{2}(\boldsymbol{b}_3+\boldsymbol{b}_6)=\frac{1}{6}\sum\boldsymbol{a}_i.$$

Это означает, что во всяком 6-угольнике — образе середины диагоналей совпадают между собой и с центром тяжести исходного 6-угольника (он же — центр тяжести полученного 6-угольника).

3°. Из системы, определяющей α_3, следует, что

$$\boldsymbol{b}_1-\boldsymbol{b}_4=\boldsymbol{b}_3-\boldsymbol{b}_6=\boldsymbol{b}_5-\boldsymbol{b}_2=\sum(\pm\boldsymbol{a}_i),$$

т. е. в 6-угольнике — образе тройки вершин $(\boldsymbol{b}_1, \boldsymbol{b}_3, \boldsymbol{b}_5)$ и $(\boldsymbol{b}_4, \boldsymbol{b}_6, \boldsymbol{b}_2)$ различаются на вектор параллельного переноса $\sum(\pm\boldsymbol{a}_i)$ (призмы). Кроме того, $\sum(\pm\boldsymbol{a}_i)=$ $=\frac{1}{3}\sum(\pm\boldsymbol{b}_i)$.

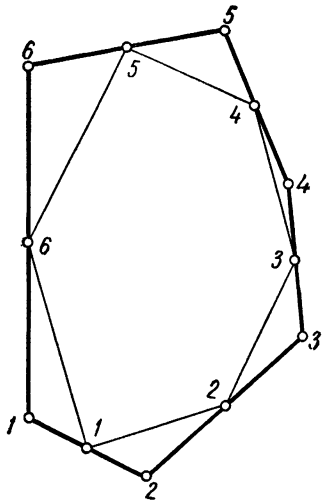


Рис. 37. $\varkappa_2$.

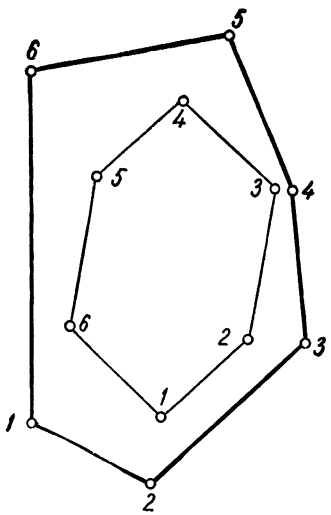


Рис. 38. $\varkappa_3$.

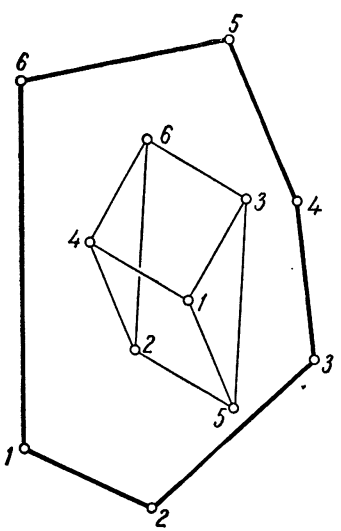


Рис. 39. α_3.

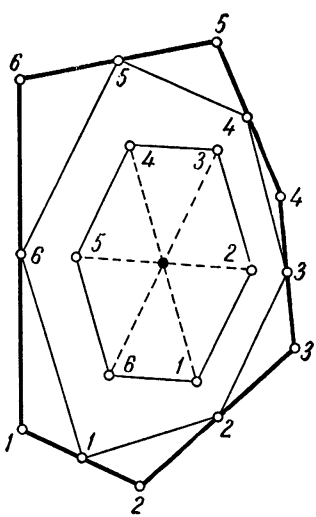


Рис. 40. $\alpha_3\varkappa_3\varkappa_2$.

В диаграмме восьми свободных классов 6-угольников (§ 8 гл. 1) $\varkappa_2$ действует в направлении NW—SO (северо-запад—юго-восток), $\varkappa_3$ — в направлении NO—SW, α_3 — в направлении N—S, на каждом отрезке вышестоящий класс отображается в нижестоящий (рис. 41).

Тот факт, что $\varkappa_2$ переводит класс 6-параллелограммов в класс аффинно-правильных 6-угольников (рис. 42), можно обнаружить и без подсчетов следующим образом.

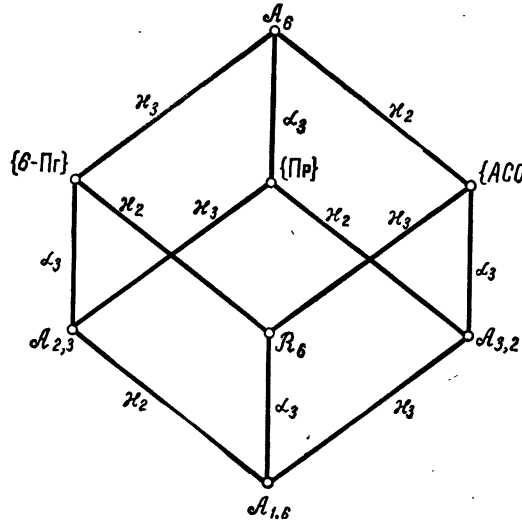


Рис. 41.

Пусть A есть 6-параллелограмм; тогда $\varkappa_2 A$ по теореме 5 — тоже 6-параллелограмм, а, согласно 1°, знакопеременная сумма его вершин равна 0; таким образом, в силу теоремы 5 гл. 1, $\varkappa_2 A$ — аффинно-правильный 6-угольник.

Возьмем произвольный 6-угольник и применим к нему последовательно в любом порядке три отображения $\varkappa_2$, $\varkappa_3$, α_3; в результате получится тривиальный 6-угольник, а именно 6 раз повторенный центр тяжести исходного 6-угольника (см. рис. 40).

В $K[\zeta]$ рассматриваемые отображения записываются в виде

$$\varkappa_2 = \frac{1}{2}(1+\zeta),\ \varkappa_3 = \frac{1}{3}(1+\zeta+\zeta^2),\ \alpha_3 = 1-\zeta+\zeta^2,$$

откуда

$$\varkappa_2\varkappa_3\alpha_3 = \frac{1}{2}(1+\zeta)\cdot\frac{1}{3}(1+\zeta+\zeta^2)\cdot(1-\zeta+\zeta^2) =$$

$$= \frac{1}{6}(1+\zeta+\zeta^2+\zeta^3+\zeta^4+\zeta^5) = \sigma.$$

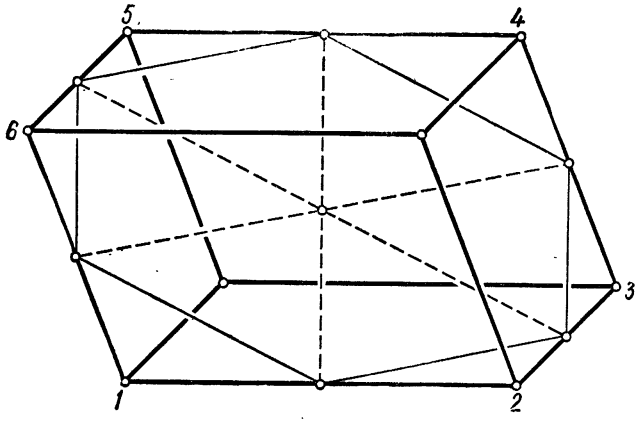


Рис. 42.

Упражнения

1. Отразим каждую вершину 5-угольника $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_5)$ относительно середины противоположной стороны. Тем самым определяется циклическое отображение β множества 5-угольников в себя. Применим отображение α_3 к $\beta(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_5)$; в результате получим $(\boldsymbol{a}_2, \ldots, \boldsymbol{a}_5, \boldsymbol{a}_1)$; поэтому β — обратимое отображение.

2. Обобщением α_3 являются изобарические циклические отображения, определенные для нечетных u, а именно:

$$\alpha_u : (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n) \longrightarrow (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n), \text{ где } \boldsymbol{b}_1 = \boldsymbol{a}_1 - \boldsymbol{a}_2 + \boldsymbol{a}_3 - \ldots + \boldsymbol{a}_u, \ldots;$$

при этом $\alpha_u = 1-\zeta+\zeta^2-\ldots+\zeta^{u-1}$. При нечетных n и $\mathrm{Char}\, K \neq 2$ отображения α_n и $\varkappa_2$ взаимно обратны.

§ 6. Циклическая квазипроекция

Примеры предыдущего параграфа показывают, что при $n=4$ и 6 многие циклические отображения переводят множество всех n-угольников в циклические классы. Между тем нас интересует вопрос о том, являются ли все циклические отображения отображениями на циклические классы, т. е. переводят ли они все пространство $\mathcal{A}_n$ в (те или иные) циклические классы.

В качестве примера приведем дальнейшее исследование этого вопроса для отображения $\varkappa_2$ при $n=4$.

Пусть $\boldsymbol{A}$ — произвольный 4-угольник; тогда $\varkappa_2\boldsymbol{A}$, т. е. 4-угольник середин сторон, является параллелограммом. Обратно, пусть $\boldsymbol{B}$ — заданный параллелограмм. Существует ли «описанный вокруг него» 4-угольник, т. е. существует ли 4-угольник $\boldsymbol{A}$, такой, что $\boldsymbol{B}=\varkappa_2\boldsymbol{A}$? Если да, то что можно сказать о множестве описанных 4-угольников? Существуют ли среди них параллелограммы, и если да, то сколько именно параллелограммов?

Мы утверждаем следующее:

1°. $\varkappa_2\boldsymbol{A}$ — *всегда параллелограмм.* 2°. *Для всякого параллелограмма* $\boldsymbol{B}$ *существует такой* 4*-угольник* $\boldsymbol{A}$, *что* $\boldsymbol{B}=\varkappa_2\boldsymbol{A}$. 3°. *Для всякого параллелограмма* $\boldsymbol{B}$ *существует единственный параллелограмм* $\boldsymbol{A}$, *такой, что* $\boldsymbol{B}=\varkappa_2\boldsymbol{A}$.

Прежде чем доказывать эти предложения, объединим их:

Теорема 10. *Пусть* $n=4$; *тогда* $\varkappa_2$ *отображает множество всех* 4*-угольников на циклический класс параллелограммов*; *в множестве параллелограммов* $\varkappa_2$ *действует взаимно однозначно.*

Теорема 10 утверждает, что $\varkappa_2$ есть квазипроекция. [Очевидно, что проекцией $\varkappa_2$ не является: $\operatorname{Im}\varkappa_2 \neq \operatorname{Fix}\varkappa_2$ и $\varkappa_2=\frac{1}{2}(1+\zeta)$ не совпадает со своим квадратом.]

Доказательство 2° и 3°. Пусть $\boldsymbol{B}=(\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, \boldsymbol{b}_4)$ — параллелограмм, так что

$$\boldsymbol{b}_1-\boldsymbol{b}_2+\boldsymbol{b}_3-\boldsymbol{b}_4=\boldsymbol{o}. \tag{10}$$

Найдем решение неоднородной системы

$$\begin{aligned} b_1 &= \tfrac{1}{2}(a_1 + a_2), \quad b_2 = \tfrac{1}{2}(a_2 + a_3), \\ b_3 &= \tfrac{1}{2}(a_3 + a_4), \quad b_4 = \tfrac{1}{2}(a_4 + a_1), \end{aligned} \tag{11}$$

где четвертое уравнение представляет собой знакопеременную сумму первых трех и поэтому является их следствием. Положим $a_1 = o$; тогда остальные три вектора найдутся однозначно и мы получим частное решение системы (11):

$$(o,\ 2b_1,\ -2b_1 + 2b_2,\ 2b_1 - 2b_2 + 2b_3). \tag{12}$$

Общее решение соответствующей *однородной* системы есть циклический класс $\operatorname{Ker} \varkappa_2$; он состоит из дважды пройденных отрезков с центром тяжести o, т. е. из 4-угольников $(c,\ -c,\ c,\ -c)$. Общее решение исходной системы (11) есть сумма частного решения (12) и общего решения однородной системы

$$(c,\ -c + 2b_1,\ c - 2b_1 + 2b_2,\ -c + 2b_1 - 2b_2 + 2b_3), \tag{13}$$

где c произвольно.

Множество решений (13) всегда содержит *параллелограмм*, ибо требование, чтобы «знакопеременная сумма вершин равнялась нулю», приводит к единственному значению $c = \frac{1}{2}(3b_1 - 2b_2 + b_3)$. Согласно (10),

$$c = b_1 - b + b_4, \text{ где } b = \tfrac{1}{4}\sum b_i. \tag{14}$$

Решение (13) данной системы имеет следующий геометрический смысл: чтобы получить четырехугольник, описанный вокруг параллелограмма $(b_1,\ b_2,\ b_3,\ b_4)$, достаточно, выбрав любую точку c, отразить ее относительно точки b_1; полученную точку отразить относительно b_2, затем относительно b_3. Так как формула (13) дает все решения системы, то всякий описанный 4-угольник можно получить таким образом. Описанный параллелограмм, как следует из (14), получится в том случае,

когда c — четвертая вершина параллелограмма, натянутого на точки b_1, b, b_4 (где b — центр тяжести заданного параллелограмма; рис. 43).

Приведенный разбор примеров циклических отображений ставит ряд дополнительных общих вопросов. Например, *всякое ли циклическое отображение является квазипроекцией*, т. е., согласно теореме 8′, для всякого ли

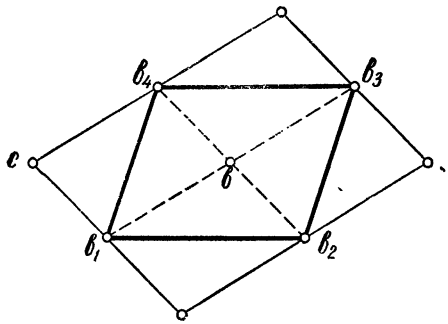


Рис. 43.

циклического отображения образ и ядро — взаимно дополнительные подпространства пространства V^n?

Упражнения

1. (Шоке [26], стр. 68.) Пусть $\operatorname{Char} K \neq 2$. Для произвольного n-угольника B определите все n-угольники A, для которых B является n-угольником середин сторон, т. е. $\varkappa_2 A = B$. (Из упр. 5 § 2 следует, что при нечетном n для всякого n-угольника A существует единственный «описанный» n-угольник, вершины которого являются знакопеременными суммами n последовательных вершин исходного n-угольника A.)

2. Пусть $n=6$. Всякий ACO-6-угольник есть $\varkappa_2$-образ точно одного ACO-6-угольника. Всякий 6-параллелограмм есть $\varkappa_3$-образ точно одного 6-параллелограмма. Всякая призма есть α_3-образ точно одной призмы.

3. Пусть $n=4$, $\operatorname{Char} K \neq 3$. Тогда α_3, $\varkappa_3$ взаимно однозначно отображают $\mathcal{A}_4$ на себя. Одинаковы ли параллелограммы середин сторон 4-угольников A и $\alpha_3 A$? Если $A \in \mathring{\mathcal{A}}_4$, то $\varkappa_3 A = -\frac{1}{3}\zeta^{-1}A$.

4. Пусть $n=5$, $\operatorname{Char} K \neq 2, 3$. Тогда $\varkappa_2$, $\varkappa_3$, α_3 взаимно однозначно отображают $\mathcal{A}_5$ на себя. Если $A \in \mathring{\mathcal{A}}_5$, то $\varkappa_2\varkappa_3\alpha_3 A = \frac{1}{6}A$.

§ 7. Изобарические циклические проекции для $n=4$

Пусть $n=4$. Для каждого из трех периодических классов 4-угольников изобарическими проекциями, переводящими в эти классы все пространство $\mathcal{A}_4$, являются соответственно 1, μ_2, σ. Больше никаких циклических проекций с этими классами в качестве образов не существует. Это следует из теоремы 7 и коммутативности циклических отображений.

Найдем циклическую проекцию, переводящую $\mathcal{A}_4$ в класс *параллелограммов*. Поскольку $\varkappa_2$ — квазипроекция (теорема 10), искомой проекцией является $\hat{\varkappa}_2^{-1}\varkappa_2$, где $\hat{\varkappa}_2$ — ограничение $\varkappa_2$ на множестве параллелограммов (см. § 4 этой главы).

Пусть $\boldsymbol{A}$ — произвольный 4-угольник, и пусть $\varkappa_2\boldsymbol{A}=\boldsymbol{B}$, $\hat{\varkappa}_2^{-1}\varkappa_2\boldsymbol{A}=\hat{\varkappa}_2^{-1}\boldsymbol{B}=\boldsymbol{A}^*$. Тогда $\varkappa_2\boldsymbol{A}=\varkappa_2\boldsymbol{A}^*=\boldsymbol{B}$, т. е. $\boldsymbol{A}^*$ — параллелограмм, имеющий с $\boldsymbol{A}$ одинаковые середины сторон, и $\boldsymbol{A}\to\boldsymbol{A}^*$ — искомая проекция:

Теорема 11. *Пусть* $n=4$; *отображение, сопоставляющее каждому* 4*-угольнику такой параллелограмм, что середины сторон образа и исходного* 4*-угольника совпадают, является циклической проекцией множества* $\mathcal{A}_4$ *на класс параллелограммов; оно изобарично и равно* $1-\mu_2+\sigma$.

Доказательство. Пусть $\boldsymbol{A}=(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_4)$, $\boldsymbol{B}$ и $\boldsymbol{A}^*$ определены, как выше, $\boldsymbol{A}^*=(\boldsymbol{a}_1^*, \ldots, \boldsymbol{a}_4^*)$. Чтобы получить явное выражение $\boldsymbol{a}_i^*$ через $\boldsymbol{a}_i$, необходимо, положив

$$\boldsymbol{B}=\varkappa_2\boldsymbol{A}=\left(\tfrac{1}{2}(\boldsymbol{a}_1+\boldsymbol{a}_2), \ \ldots, \ \tfrac{1}{2}(\boldsymbol{a}_4+\boldsymbol{a}_1)\right),$$

подставить в формулу (13) из § 6 значение $\boldsymbol{c}$, задаваемое равенством (14). При этом мы получим циклическую систему

$$\boldsymbol{a}_1^*=\tfrac{1}{4}(3\boldsymbol{a}_1+\boldsymbol{a}_2-\boldsymbol{a}_3+\boldsymbol{a}_4), \ \ldots \ .$$

Таким образом, $\boldsymbol{A}\to\boldsymbol{A}^*$ — циклическое отображение с коэффициентами $\frac{1}{4}$ (3, 1, —1, 1), сумма которых равна 1;

в $K[\zeta]$ это отображение задается так:

$$\frac{1}{4}(3+\zeta-\zeta^2+\zeta^3)=1-\frac{1}{2}(1+\zeta^2)+\frac{1}{4}(1+\zeta+\zeta^2+\zeta^3)=$$
$$=1-\mu_2+\sigma.$$

Последнее выражение, записанное в форме

$$A^*=A-\mu_2 A+\sigma A,$$

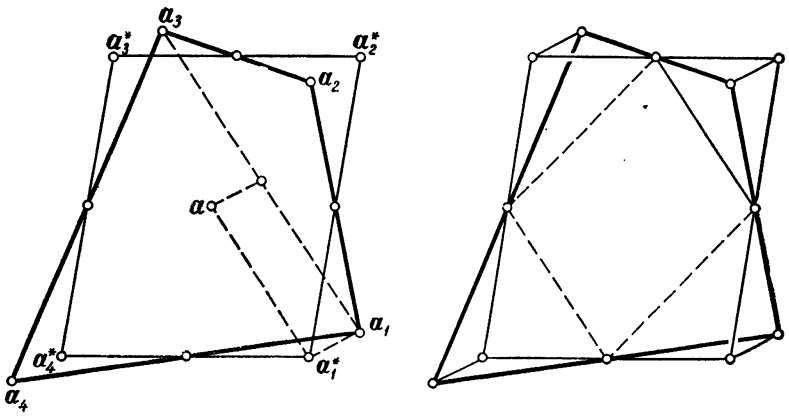


Рис. 44.

дает способ построения параллелограмма A^*, если задан 4-угольник A: a_i^* есть четвертая вершина параллелограмма, натянутого на точку a_i, середину диагонали (a_i, a_{i+2}) и центр тяжести A (рис. 44; центр тяжести A есть середина отрезка, соединяющего середины диагоналей в A).

Итак, для каждого из четырех свободных циклических классов (см. § 8 гл. 1) существует изобарическая циклическая проекция, переводящая в этот класс все пространство $\mathcal{A}_4$.

Теперь снова возникает общий вопрос: *для всякого ли циклического класса n-угольников существует циклическая проекция, переводящая в него все пространство* $\mathcal{A}_n$?

Упражнения

1. Пусть $n=4$. Для каждого из операторов 1, μ_2, $1-\mu_2+\sigma$, σ введем новый оператор, полученный вычитанием его из тождественного оператора 1. Мы получим циклические проекции, которые переводят $\mathcal{A}_4$ соответственно в $\{O\}$, в класс параллелограммов с центром тяжести O, в класс дважды пройденных 2-угольников с центром тяжести O, в класс $\overset{\circ}{\mathcal{A}}_4$.

В силу теоремы 8′, $A=A^*+(\mu_2-\sigma)A$ есть однозначное разложение A на 4-угольник из $\operatorname{Im}\varkappa_2$ и 4-угольник из $\operatorname{Ker}\varkappa_2$.

2. $\operatorname{Im}(\zeta-1)=\overset{\circ}{\mathcal{A}}_n=\operatorname{Im}(1-\sigma)$. Пусть $n\neq 1$. Тогда $\zeta-1$ есть квазипроекция: для $\chi=\frac{1}{n}(\zeta+2\zeta^2+\ldots+(n-1)\zeta^{n-1})$ имеем $(\zeta-1)\chi=1-\sigma$, а на $\overset{\circ}{\mathcal{A}}_n$ отображение $1-\sigma$, а следовательно, и $(\zeta-1)\chi$ являются тождественными. Таким образом, $\zeta-1$ и χ обратны друг другу. Элемент χ является обратимым: даже в $K[\zeta]$ можно найти $\psi\in K[\zeta]$, такое, что $\psi\chi=1$ (сделайте это!).

3. Пусть $n=4$. Определим циклическое отображение χ равенством $\varkappa_2\chi=1-\mu_2+\sigma$. Обратимо ли χ в $K[\zeta]$?

§ 8. Циклические матрицы

Запишем в обычной форме систему (1), определяющую циклическое отображение с набором коэффициентов $(c_0, c_1, \ldots, c_{n-1})$:

$$\begin{aligned}
b_1 &= c_0a_1+c_1a_2+\ldots+c_{n-1}a_n,\\
b_2 &= c_{n-1}a_1+c_0a_2+\ldots+c_{n-2}a_n,\\
&\cdots\cdots\cdots\cdots\\
b_n &= c_1a_1+c_2a_2+\ldots+c_0a_n.
\end{aligned}$$

Коэффициенты этого отображения образуют циклическую матрицу $M(c_0, c_1, \ldots, c_{n-1})$, определенную в § 6 гл. 1.

Циклическому отображению ζ соответствует циклическая матрица $Z=M(0, 1, 0, \ldots, 0)$ — *матрица некоторой подстановки* *); $Z^n=E$ (где E — единичная матрица). Имеет место разложение

$$M(c_0, c_1, \ldots, c_{n-1})=\sum c_iZ^i.$$

Соответствие

$$\sum c_i\zeta^i \longrightarrow \sum c_iZ^i$$

*) То есть такая матрица, все элементы которой равны 0 или 1 и в каждой строке и в каждом столбце которой имеется ровно одна единица.

есть изоморфизм алгебры $K[\zeta]$ на *алгебру* $K[Z]$ *циклических матриц порядка* n *над* K. Последовательному выполнению циклических отображений соответствует умножение циклических матриц; отсюда следует, что это умножение коммутативно.

Таким образом, мы получаем еще одну интерпретацию теории циклических отображений n-угольников в виде теории циклических матриц порядка n. Циклический класс n-угольников можно теперь охарактеризовать как множество тех n-угольников, которые циклическая матрица переводит в нуль.

Представление циклических отображений на языке алгебры матриц открывает новый доступный и привлекательный подход к изучению циклических отображений и циклических классов n-угольников.

Упражнения

1. Неособые циклические матрицы порядка n образуют абелеву группу относительно матричного умножения.

2. Неособые диагональные матрицы D порядка n, которые преобразуют каждую циклическую матрицу T снова в циклическую [т. е. такие, что $D^{-1}TD$ — снова циклическая матрица], суть те матрицы, диагональные элементы которых имеют вид

$$c,\ c\omega,\ c\omega^2,\ \ldots,\ c\omega^{n-1},$$

где $c \neq 0$, а $\omega = \sqrt[n]{1}$ в K. Найти такие матрицы D над полем рациональных и действительных чисел (см. § 5 гл. 9, упр 3).

3. Пусть K — поле, содержащее все корни n-й степени из 1, а $\omega = \sqrt[n]{1}$ — первообразный корень. Неособая матрица порядка n

$$U = (u_{i,j}), \quad \text{где} \quad u_{i,j} = \omega^{i \cdot j},$$

преобразует всякую циклическую матрицу в диагональную. Пусть T — циклическая матрица, соответствующая набору $(c_0, c_1, \ldots, c_{n-1})$. Тогда диагональная матрица $D = U^{-1}TU$ состоит из элементов $d_i = c_0 + c_1\omega^i + c_2\omega^{2i} + \ldots + c_{n-1}\omega^{(n-1)i}$, где $i = 1, 2, \ldots, n$. Какие следствия можно вывести отсюда для идемпотентных циклических матриц?

ГЛАВА 3

ОБ ИЗОБАРИЧЕСКИХ ЦИКЛИЧЕСКИХ ОТОБРАЖЕНИЯХ

§ 1. σ-ядро

Здесь мы будем заниматься отображениями, которые являются одновременно циклическими и изобарическими; к их числу относятся, например, отображения 1, σ, ζ. Вапомним, что *изобарическим* называется отображение φ, переводящее в себя каждый изобарический класс, т. е. такое, что $\sigma\varphi \boldsymbol{A} = \sigma \boldsymbol{A}$ для всякого n-угольника $\boldsymbol{A}$, что можно также записать в виде равенства

$$\sigma\varphi = \sigma. \tag{1}$$

Если φ — *циклическое* отображение, то формуле (1) эквивалентны следующие утверждения:

$$(1 - \sigma)\,\varphi = \varphi - \sigma; \tag{2}$$

$$s(\varphi) = 1; \tag{3}$$

$$\mathcal{A}_{1,\,n} \subseteq \operatorname{Fix} \varphi. \tag{4}$$

По поводу эквивалентности равенств (1) и (3) см. § 3 гл. 2. Эта эквивалентность вытекает также из следующей леммы:

Лемма. *Для всякого циклического отображения* ψ

$$\psi\sigma = s(\psi)\sigma.$$

Доказательство нетрудно получить, вспомнив свойства произведения циклических отображений; см. § 2 гл. 2.

Обратимся теперь к эквивалентности (1) и (4). Ясно, что (1) эквивалентно равенству $\varphi\sigma = \sigma$ (ибо циклические отображения коммутативны); последнее же означает, что для всякого n-угольника $\boldsymbol{A}$

$$\varphi(\sigma \boldsymbol{A}) = \sigma \boldsymbol{A}, \quad \text{т. е.} \quad \mathcal{A}_{1,\,n} \subseteq \operatorname{Fix} \varphi.$$

Итак, пусть φ — *изобарическое отображение*. Ядро φ есть центральный класс (см. теорему 6 гл. 2). Наряду с множеством n-угольников, которые отображение φ обращает в нуль, рассмотрим множество n-угольников, которые φ переводит в тривиальные n-угольники (т. е. в их центры тяжести). Это множество $\operatorname{Ker}\varphi$ назовем σ-*ядром* отображения φ:

$$\underset{\sigma}{\operatorname{Ker}}\varphi := \{\boldsymbol{A} : \varphi\boldsymbol{A} = \sigma\boldsymbol{A}\} = \operatorname{Ker}(\varphi - \sigma)\ ^*).$$

σ-ядро φ также является циклическим классом (теорема 1 гл. 2); он содержит все тривиальные n-угольники [ибо $\sigma\boldsymbol{A} = \boldsymbol{A}$ для каждого тривиального n-угольника $\boldsymbol{A}$ и в силу (4) $\varphi\boldsymbol{A} = \boldsymbol{A}$, а следовательно, $\varphi\boldsymbol{A} = \sigma\boldsymbol{A}$] и, значит, является свободным циклическим классом. Это следует также из теоремы 6 гл. 2, если учесть, что

$$s(\varphi - \sigma) = s(\varphi) - s(\sigma) = 1 - 1 = 0.$$

Упражнение. Справедливо равенство $\zeta\sigma = \sigma$. Пользуясь им, докажите лемму.

§ 2. Два типа циклических классов

Теорема 1. *Всякий циклический класс является или σ-ядром, или ядром некоторого изобарического циклического отображения. Свободные циклические классы являются σ-ядрами, а центральные — ядрами изобарических циклических отображений.*

Доказательство. В силу теоремы 6 гл. 2 достаточно показать, что *ядро циклического отображения ψ, для которого $s(\psi) = 0$, является также σ-ядром некоторого изобарического циклического отображения.* Обозначим $\psi + \sigma = \varphi$; тогда $s(\varphi) = 1$ и $\operatorname{Ker}\psi = \underset{\sigma}{\operatorname{Ker}}\varphi$.

Мы хотим установить связь между свободными и центральными циклическими классами. Предварительно установим следующие соотношения (в которых φ — цик-

*) Знак $:=$ (в нашей литературе чаще используется в том же смысле символ $\overset{\text{def}}{=}$; def — сокращение латинского слова definitio — определение) означает «равно по определению».

лическое изобарическое отображение):

$$\underset{\sigma}{\operatorname{Ker}}\,\varphi \cap \operatorname{Ker}\sigma = \operatorname{Ker}\varphi; \tag{5}$$

$$\underset{\sigma}{\operatorname{Ker}}\,\varphi = \operatorname{Im}\sigma + \operatorname{Ker}\varphi; \tag{6}$$

$$(1-\sigma)\underset{\sigma}{\operatorname{Ker}}\,\varphi = \operatorname{Ker}\varphi. \tag{7}$$

$\operatorname{Ker}\sigma$ — нуль-изобарический класс, $\operatorname{Im}\sigma = \operatorname{Fix}\sigma$ — класс тривиальных n-угольников (см. § 3 гл. 2).

Доказательство (5) и (7). Пусть $\boldsymbol{A}$ — произвольный n-угольник. Три следующих утверждения эквивалентны между собой: a) $\varphi\boldsymbol{A} = \boldsymbol{O}$; b) $\varphi\boldsymbol{A} = \sigma\boldsymbol{A} = \boldsymbol{O}$; c) существует такой n-угольник $\boldsymbol{B}$, что $\boldsymbol{A} = (1-\sigma)\boldsymbol{B}$ и $\varphi\boldsymbol{B} = \sigma\boldsymbol{B}$.

Из a) следует $\sigma\varphi\boldsymbol{A} = \sigma\boldsymbol{O} = \boldsymbol{O}$, а значит, в силу (1), $\sigma\boldsymbol{A} = \boldsymbol{O}$, т. е. равенства b). Если выполняется b), то $\boldsymbol{A} = (1-\sigma)\boldsymbol{A}$ и $\varphi\boldsymbol{A} = \sigma\boldsymbol{A}$, следовательно, верно и c). Из c) в силу (2) следует $\varphi\boldsymbol{A} = \varphi(1-\sigma)\boldsymbol{B} = (\varphi-\sigma)\boldsymbol{B} = \varphi\boldsymbol{B} - \sigma\boldsymbol{B} = \boldsymbol{O}$, т. е. a).

Эквивалентность b) и a) видна из равенства (5), эквивалентность c) и a) — из равенства (7).

Равенство (6) можно доказать аналогично, но мы воспользуемся свойствами модулей. Если $\mathscr{B}$, $\mathscr{C}$, $\mathscr{D}$ — подпространства некоторого векторного пространства (а циклические классы являются ими), то

$$\text{из } \mathscr{B} \subseteq \mathscr{D} \text{ следует } (\mathscr{B}+\mathscr{C}) \cap \mathscr{D} = \mathscr{B} + (\mathscr{C} \cap \mathscr{D})$$

(см. приложение II). Далее, σ-ядро отображения φ является свободным циклическим классом; поэтому $\operatorname{Im}\sigma \subseteq \underset{\sigma}{\operatorname{Ker}}\,\varphi$ и

$$\underset{\sigma}{\operatorname{Ker}}\,\varphi = \mathcal{A}_n \cap \underset{\sigma}{\operatorname{Ker}}\,\varphi = (\operatorname{Im}\sigma + \operatorname{Ker}\sigma) \cap \underset{\sigma}{\operatorname{Ker}}\,\varphi =$$
$$= \operatorname{Im}\sigma + (\operatorname{Ker}\sigma \cap \underset{\sigma}{\operatorname{Ker}}\,\varphi) = \operatorname{Im}\sigma + \underset{\sigma}{\operatorname{Ker}}\,\varphi.$$

Из теоремы 1, (5) и (6) следует, что отображение

$$\underset{\sigma}{\operatorname{Ker}}\,\varphi \longrightarrow \operatorname{Ker}\varphi \quad (\varphi\text{ — изобарическое})$$

является *взаимно однозначным отображением множества свободных циклических классов на множество центральных*

классов. Таким образом, каждому свободному циклическому классу $\mathscr{C}$ соответствует единственный центральный класс, который мы обозначим $\overset{\circ}{\mathscr{C}}$. Результат сформулируем в виде следующего правила и теоремы 2:

Правило. *Если* φ *изобарично и* $\mathscr{C} = \underset{\sigma}{\mathrm{Ker}}\,\varphi$, *то* $\overset{\circ}{\mathscr{C}} = \underset{\circ}{\mathrm{Ker}}\,\varphi$.

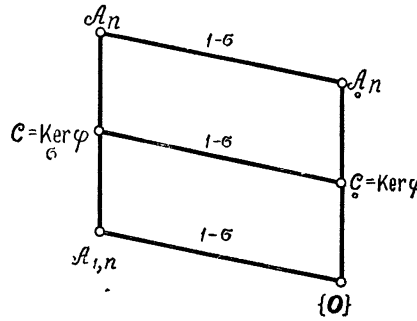


Рис. 45.

Теорема 2. *Соответствие* $\mathscr{C} \to \overset{\circ}{\mathscr{C}}$, *где* $\mathscr{C}$ *— свободный, а* $\overset{\circ}{\mathscr{C}}$ *— отвечающий ему центральный циклический класс, является взаимно однозначным отображением множества всех свободных циклических классов на множество центральных циклических классов. При этом справедливы равенства*

$$\mathscr{C} \cap \overset{\circ}{\mathcal{A}}_n = \overset{\circ}{\mathscr{C}}, \quad \mathscr{C} = \mathcal{A}_{1,n} + \overset{\circ}{\mathscr{C}}, \quad (1-\sigma)\,\mathscr{C} = \overset{\circ}{\mathscr{C}}.$$

Циклическая проекция $1-\sigma$ (см. § 4 гл. 2) сопоставляет каждому n-угольнику $\boldsymbol{A}$ n-угольник с центром тяжести $\boldsymbol{o}$, получаемый из $\boldsymbol{A}$ параллельным переносом. Теорема 2 утверждает, что эта проекция устанавливает взаимно однозначное соответствие между обоими типами классов.

Рассматриваемое соответствие (см. рис. 45) очень естественно. Достаточно ограничиться одним из этих типов, поскольку привлечение второго типа не может до-

ставить нам никаких новых геометрически содержательных фактов. Однако подобное ограничение (скажем, свободными циклическими классами) может оказаться затруднительным из-за чисто алгебраических осложнений. Следующий параграф содержит некоторые указания по этому поводу.

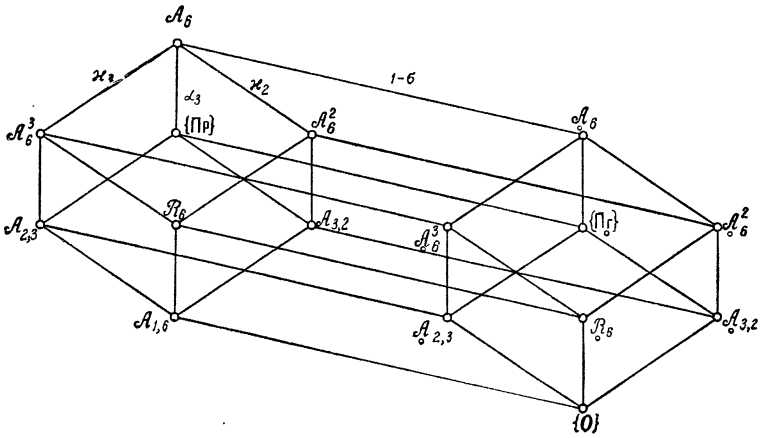


Рис. 46.

Иногда мы будем пользоваться этими ограничениями, например в § 1 и 2 гл. 4, но для того, чтобы сформулировать и доказать основную теорему нашей теории, и для выяснения связи между циклическими классами и циклическими отображениями нам потребуются оба эти понятия в их естественной алгебраической общности.

На изображенной на рис. 46 диаграмме указаны все включения 16 циклических классов 6-угольников, которые получаются, если к 8 свободным циклическим классам присоединить соответствующие им центральные классы (по поводу обозначений см. § 1 гл. 4).

Замечание 1. Пусть снова φ — изобарическое циклическое отображение. Как следует из (4), $\operatorname{Im}\varphi$ содержит класс тривиальных n-угольников $[\mathcal{A}_{1,n} \subseteq \operatorname{Fix}\varphi \subseteq \operatorname{Im}\varphi]$. Значит, если $\operatorname{Im}\varphi$ является циклическим классом, то обязательно свободным. Равенство $\psi \operatorname{Im}\varphi = \operatorname{Im}\psi\cdot\varphi$ выполняется уже для всякого отображения множества в

себя; для $\psi = 1 - \sigma$ оно имеет вид

$$(1 - \sigma)\,\mathrm{Im}\,\varphi = \mathrm{Im}\,(\varphi - \sigma)$$

[см. формулу (2)]. Из теоремы 2 следует такое

Правило. *Если* φ *— изобарическое отображение и* $\mathscr{C} = \mathrm{Im}\,\varphi$, *то* $\mathscr{C} = \mathrm{Im}\,(\varphi - \sigma)$. (Здесь $\mathscr{C}$ — свободный циклический класс.)

Замечание 2. Два подпространства $\mathscr{B}$ и $\mathscr{C}$ векторного пространства $\mathscr{A}_n$ называются *взаимно дополнительными*, если

$$\mathscr{A}_n = \mathscr{B} + \mathscr{C},\ \mathscr{B} \cap \mathscr{C} = \{O\},\ \text{т. е. } \mathscr{A}_n = \mathscr{B} \oplus \mathscr{C}.$$

Из двух взаимно дополнительных циклических классов один всегда свободный, другой — центральный. Действительно, два свободных циклических класса не могут быть взаимно дополнительными, так как их пересечение содержит по меньшей мере класс тривиальных n-угольников; два центральных класса также не могут быть взаимно дополнительными, так как их сумма не выходит за пределы нуль-изобарического класса.

Упражнения

1. Циклическое отображение $\zeta - 1$ взаимно однозначно отображает множество свободных циклических классов на множество центральных классов (см. упражнения к § 3 и 7 гл. 2).

2. Пусть в множестве 6-угольников одно за другим действуют циклические отображения $\varkappa_2$, $\varkappa_3$, α_3, $1 - \sigma$. Проследите по изображенной на рис. 46 диаграмме, как с каждым отображением мы будем спускаться к все более узкому классу 6-угольников и в конце концов дойдем до нулевого класса $\{O\}$; таким образом, $\varkappa_2\varkappa_3\alpha_3(1 - \sigma) = 0$.

§ 3. Об изобарических циклических отображениях

Мы сделаем несколько замечаний, которые будут полезны при о ерировании с изобарическими циклическими отображениями.

Напомним, что $K[\zeta]$ — коммутативная алгебра циклических отображений; $\varphi \longrightarrow s(\varphi)$ — гомоморфизм этой алгебры на K. Ядро этого гомоморфизма (множество отобра-

жений, для которых $s(\varphi)=0$) является идеалом I_0 в $K[\zeta]$, $K[\zeta]/I_0\cong K$ и, следовательно, I_0—максимальный идеал в $K[\zeta]$. Для любого $c\in K$ множество I_c циклических отображений φ, таких, что $s(\varphi)=c$, является смежным классом по идеалу I_0; I_1—множество изобарических циклических отображений (для которых $s(\varphi)=1$)—представимо в виде

$$I_1=I_0+\sigma, \tag{8}$$

так как $\sigma\in I_1$. Если φ, $\psi\in I_1$, то $\varphi\psi\in I_1$, но $-\varphi$, $\varphi+\psi\notin I_1$; всякая знакопеременная сумма нечетного числа элементов из I_1 снова принадлежит I_1. Отображение $\varphi\longrightarrow 1-\varphi$ переводит I_1 и I_0 друг в друга, а

$$\varphi\longrightarrow 1-\varphi+\sigma \tag{9}$$

является инволютивным отображением I_1 в себя. Если φ—идемпотентный элемент I_1, то $1-\varphi+\sigma$—тоже идемпотент. Их произведение равно σ, а «булева сумма» (сумма минус произведение, см. § 1 гл. 5) равна 1; поэтому эти две изобарические циклические проекции называются взаимно σ-*дополнительными*.

Правило. *Если* φ—*изобарическая циклическая проекция, то это справедливо и для* $1-\varphi+\sigma$, *причем*

$$\operatorname{Im}(1-\varphi+\sigma)=\operatorname*{Ker}_{\sigma}\varphi,\quad \operatorname*{Ker}_{\sigma}(1-\varphi+\sigma)=\operatorname{Im}\varphi. \tag{10}$$

Равенства (10) следуют из очевидного равенства $\operatorname{Im}\varphi=\operatorname{Ker}(1-\varphi)$ и определения σ-ядра. Оба множества в (10) являются свободными циклическими классами (теорема 1).

Пример. 1, σ—взаимно σ-дополнительны. При $n=4$ множество четырех изобарических циклических проекций из § 7 гл. 2 распадается на две пары взаимно σ-дополнительных: 1, σ и μ_2, $1-\mu_2+\sigma$; при этом $\operatorname{Im}(1-\mu_2+\sigma)=\operatorname*{Ker}_{\sigma}\mu_2$ есть класс параллелограммов.

Упражнение. В $K[\zeta]$ главный идеал (σ), порожденный σ, есть $K\sigma$; следовательно, он состоит из циклических отображений $\sum c_i\zeta^i$, где $c_0=c_1=\ldots=c_{n-1}$. Главный идеал $(1-\sigma)=I_0$ и $K[\zeta]=K\sigma\oplus I_0$.

Заметка о сложении n-угольников

1. Сложение n-угольников. Напомним, что под n-угольником мы понимаем произвольный набор n точек из V. Пусть $\boldsymbol{A}=(a_1, \ldots, a_n)$ и $\boldsymbol{B}=(b_1, \ldots, b_n)$—два таких n-угольника.

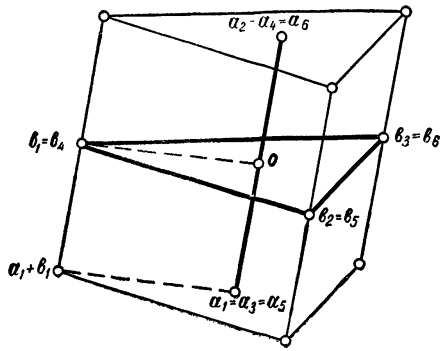


Рис. 47.

Если $\boldsymbol{A}$ и $\boldsymbol{B}$ принадлежат нуль-изобарическому классу (имеют центр тяжести o), то их сумма имеет ясный геометрический смысл: i-я вершина $\boldsymbol{A}+\boldsymbol{B}$ является четвертой вершиной параллелограмма, натянутого на точки a_i, o—общий центр тяжести для $\boldsymbol{A}$ и $\boldsymbol{B}$ и b_i; при этом центр тяжести $\boldsymbol{A}+\boldsymbol{B}$ также совпадает с o. На рис. 47 построена сумма трижды пройденного 2-угольника и дважды пройденного 3-угольника с общим центром тяжести o; здесь $n=6$ и сумма $\boldsymbol{A}+\boldsymbol{B}$ есть ризма.

Пусть теперь $\boldsymbol{A}$, $\boldsymbol{B}$—произвольные n-угольники. По-прежнему i-я вершина $\boldsymbol{A}+\boldsymbol{B}$ есть четвертая вершина параллелограмма (a_i, o, b_i), но теперь o—обычная точка, геометрически не связанная с n-угольниками $\boldsymbol{A}$ и $\boldsymbol{B}$, а лежащая «где попало». Однако геометрические свойства суммы все-таки сохраняются и в этом случае. Так, сумма $(c_1, c_2, \ldots, c_6)$ трижды пройденного отрезка $(a_1, a_2, a_1, a_2, a_1, a_2)$ и дважды пройденного 3-угольника $(b_1, b_2, b_3, b_1, b_2, b_3)$ по-прежнему является призмой; легко про-

верить, что $c_1 - c_4 = c_3 - c_6$, ... (ибо $(a_1 + b_1) - (a_2 + b_1) = (a_1 + b_3) - (a_2 + b_3)$, ...).

Для центров тяжести A, B и $A + B$ имеет место соотношение

$$\sigma(A + B) = \sigma A + \sigma B.$$

Однако если A и B изобаричны: $\sigma A = \sigma B = S(s, s, \ldots, s)$, то $A + B$ только в том случае принадлежит тому же изобарическому классу, что A и B, когда $S = O$.

Для изобарических n-угольников можно ввести новую операцию *сложения из центра тяжести*, не выводящую из их изобарического класса. Определим новую сумму A и B как n-угольник, i-я вершина которого является четвертой вершиной для тройки (a_i, s, b_i), где s — общий центр тяжести A и B. Очевидна связь между новой суммой (обозначим ее через $A \underset{\sigma}{+} B$) и старой:

$$A \underset{\sigma}{+} B = A + B - S.$$

Эта связь позволяет чисто алгебраическим путем установить формальные свойства новой суммы.

Упражнение. Множество всех 4-угольников евклидовой плоскости с произвольно выбранным началом образует группу относительно сложения. Параллелограммы образуют подгруппу этой группы. Образуют ли подгруппу квадраты?

2. Сдвиг сложения в абелевой группе. Пусть $(\mathcal{A}, +)$ — абелева группа и $s \in \mathcal{A}$. Введем новую операцию, которую будем называть *сдвигом сложения на элемент* s:

$$a \underset{s}{+} b = a + b - s. \tag{1}$$

Будем говорить также, что эта операция получена *параллельным переносом на элемент* s:

$$x \longrightarrow x + s \tag{2}$$

обычного группового сложения, в том смысле, что к ней приводит цепочка отображений

$$(a, b) \longrightarrow (a - s, b - s) \longrightarrow (a - s) + (b - s) \longrightarrow$$
$$\longrightarrow ((a - s) + (b - s)) + s = a + b - s.$$

Так как $(x+s)\underset{s}{+}(y+s)=(x+y)+s$, то перенос (2) устанавливает изоморфизм между $(\mathcal{A}, +)$ и $(\mathcal{A}, \underset{s}{+})$. Отсюда следует, что $(\mathcal{A}, \underset{s}{+})$ — *тоже абелева группа с нулевым элементом* s.

Пусть $(\mathcal{U}, +)$ — подгруппа группы $(\mathcal{A}, +)$. Подгруппой, изоморфной $(\mathcal{U}, +)$ относительно сдвига сложения $\underset{s}{+}$, является смежный класс $(\mathcal{U}+s, \underset{s}{+})$. Наоборот, *каждый смежный класс можно превратить в группу, заменив групповое сложение сдвигом сложения на элемент* s, *принадлежащий этому классу.*

Если φ — эндоморфизм группы $(\mathcal{A}, +)$ и $s \in \operatorname{Fix}\varphi$, то множество φ-прообразов элемента s:

$$\{c \in \mathcal{A} : \varphi c = s\} = \operatorname{Ker}\varphi + s \tag{3}$$

является абелевой группой по отношению к операции $\underset{s}{+}$.

Наконец, пусть $(R, +, \cdot)$ — коммутативное кольцо с элементами $a, b, \ldots$ и s — идемпотентный элемент в R. Отображение $x \longrightarrow sx$ (умножение на s) есть идемпотентный эндоморфизм кольца R, при котором s переходит в себя. Ядро $\{x \in R : sx = 0\}$ этого эндоморфизма обозначим через I; при этом снова

$$\{c \in R : sc = s\} = I + s. \tag{4}$$

Так как $(x+s)(y+s) = xy + s$ для всех $x, y \in I$, то перенос (2) устанавливает изоморфизм колец $(I, +, \cdot)$ и $(I+s, \underset{s}{+}, \cdot)$; в последнем s — нулевой элемент.

Упражнения

1. Пусть $(\mathcal{A}, +)$ — векторное пространство над полем K и $s \in \mathcal{A}$; тогда $(\mathcal{A}, \underset{s}{+})$ с обычным умножением $(c, a) \longrightarrow ca$ $(c \in K,\ a \in \mathcal{A})$ в том и только в том случае является векторным пространством, когда $s = o$.

2. Пусть $(R, +, \cdot)$ — кольцо, $s \in R$ и T — подкольцо; $(T+s, \underset{s}{+}, \cdot)$ является кольцом тогда и только тогда, когда $s^2 = s$ и $sT = \{0\} \underset{s}{=} Ts$.

3. Сложение изобарических n-угольников из центра тяжести. В векторном пространстве $\mathcal{A}_n$ всякий изобарический класс (множество n-угольников с общим центром

тяжести S) является смежным классом $\mathcal{A}_n + S$ по $\overset{\circ}{\mathcal{A}}_n$ — нуль-изобарическому классу; здесь $S = (s, s, \ldots, s)$ — тривиальный n-угольник, общий центр тяжести этого класса. *Поэтому изобарический класс относительно следующим образом определенной операции сложения*[1]) *(сложение из центра тяжести):*

$$A \underset{\sigma}{+} B = A + B - S$$

образует абелеву группу с нулем S. Очевидно, что $A \underset{\sigma}{-} B = A - B + S$.

Мы далее не будем пользоваться этим «сдвинутым» сложением. Отметим, однако, два случая, когда обычная сумма n-угольников совпадает с нововведенной, и поэтому ее можно понимать в смысле «сложения из центра тяжести»:

1) сумма n-угольников из нуль-изобарического класса;

2) знакопеременная сумма нечетного числа изобарических n-угольников [к 2) заметим, что для изобарических A, B, C имеем $A \underset{\sigma}{-} B + C = A - B \underset{\sigma}{+} C$].

Примеры. К случаю 1). Циклический класс n-угольников назовем *атомарным*, если он отличен от нулевого класса $\{O\}$ и не содержит никакого отличного от $\{O\}$ циклического класса. Из теоремы 1 гл. 1 следует, что *класс* $\mathcal{A}_{1,n}$ *тривиальных* n*-угольников является атомарным* (минимальный свободный циклический класс); *все остальные атомарные классы* — центральные (почему?).

В дальнейшем мы покажем, что *всякий* n*-угольник может быть единственным образом представлен в виде суммы* n*-угольников из атомарных циклических классов.*

Любая сумма n-угольников из атомарных классов $\neq \mathcal{A}_{1,n}$ относится к случаю 1); прибавление тривиального n-угольника означает только параллельный перенос (в V) полученного ранее n-угольника. Отсюда следует, что искомое разложение на атомарные классы имеет внутренний геометрический смысл.

---

[1]) В выражении $A \underset{\sigma}{+} B$ индекс σ сокращенно обозначает общий центр тяжести $\sigma A = \sigma B$.

К случаю 2). Всякая знакопеременная сумма нечетного числа изобарических образов заданного n-угольника $\boldsymbol{A}$ есть сумма 2). В самом деле, если, например, φ, ψ, χ — изобарические циклические отображения, то $(\varphi-\psi+\chi)\boldsymbol{A}=\varphi\boldsymbol{A}-\psi\boldsymbol{A}+\chi\boldsymbol{A}$ есть сумма 2). Если φ есть изобарическая циклическая проекция, то $1-\varphi+\sigma$ — ее σ-дополнение и

$$(1-\varphi+\sigma)\boldsymbol{A}=\boldsymbol{A}-\varphi\boldsymbol{A}+\sigma\boldsymbol{A}=\boldsymbol{A}\underset{\sigma}{-}\varphi\boldsymbol{A};$$

i-й вершиной этого n-угольника является четвертая вершина параллелограмма, у которого остальные три вершины — это i-я вершина $\boldsymbol{A}$, i-я вершина $\varphi\boldsymbol{A}$ и центр тяжести $\boldsymbol{A}$. Для $n=4$ с этим построением совпадает данная в § 7 гл. 2 конструкция параллелограмма $(1-\mu_2+\sigma)\boldsymbol{A}$, который имеет одинаковый параллелограмм середин сторон с данным 4-угольником $\boldsymbol{A}$.

Внутри изобарического класса, являющегося абелевой группой относительно сдвига сложения $\boldsymbol{A}\underset{\sigma}{+}\boldsymbol{B}$, всякое изобарическое отображение действует как эндоморфизм; иначе говоря,

$$\varphi(\boldsymbol{A}\underset{\sigma}{+}\boldsymbol{B})=\varphi\boldsymbol{A}\underset{\sigma}{+}\varphi\boldsymbol{B}$$

[ср. формулу (1) гл. 3].

Можно сделать еще один шаг в рассмотрении связанных со сдвигом сложения конструкций, определив следующим образом *сдвиг сложения в множестве изобарических циклических отображений* $\{\varphi\in K[\zeta]:\sigma\varphi=\sigma\}$:

$$\varphi\underset{\sigma}{+}\psi=\varphi+\psi-\sigma.$$

Относительно так определенного σ-сложения это множество становится абелевой группой; присоединив же сюда ранее определенную операцию умножения (последовательное выполнение отображений), мы получим коммутативное кольцо эндоморфизмов изобарического класса, нулевым элементом которого является эндоморфизм σ. При этом, например, $1\underset{\sigma}{-}\varphi=1-\varphi+\sigma$ и для каждого n-угольника $\boldsymbol{A}$

$$(\varphi\underset{\sigma}{+}\psi)\boldsymbol{A}=\varphi\boldsymbol{A}\underset{\sigma}{+}\psi\boldsymbol{A}.$$

Таким образом, по отношению к операциям $(\underset{\sigma}{+}, \cdot)$ множество изобарических циклических отображений образует кольцо эндоморфизмов любого циклического класса, в котором сложение понимается в смысле сложения из центра тяжести.

Итак, мы выяснили, что с геометрической точки зрения достаточно ограничиться свободными циклическими классами, поскольку положение начала $\boldsymbol{o}$ является для нас несущественным. В дальнейшем, имея это в виду, мы нигде не будем добиваться формулировок, не зависящих от выбора начала.

ГЛАВА 4

ОТОБРАЖЕНИЯ УСРЕДНЕНИЯ

§ 1. Изобарически распадающиеся n-угольники

Обозначим через $\tau(n)$ число делителей n. Как известно, оно зависит от показателей степени, с которыми входят простые делители в «каноническое разложение» числа n *).

Пусть d — делитель n и $n = d\bar{d}$. Вершины n-угольника $(a_1, \ldots, a_n)$ расположим в таблицу по модулю d:

$$\begin{matrix} a_1 & a_{d+1} & \ldots & a_{n-d+1} \\ a_2 & a_{d+2} & \ldots & a_{n-d+2} \\ \cdot & \cdot & \cdot & \cdot \\ a_d & a_{2d} & \ldots & a_n \end{matrix} \qquad (1)$$

В строках этой таблицы стоят $\bar{d}$-наборы, определяющие хордовые $\bar{d}$-угольники заданного n-угольника (см. § 5 гл. 1); число их равно d.

Различные циклические классы можно определять наложением условий на эти хордовые многоугольники. Если потребовать, чтобы все хордовые $\bar{d}$-угольники из (1) были тривиальными, то получится *периодический класс* $\mathcal{A}_{d,\bar{d}}$. Существует $\tau(n)$ периодических классов; их можно расположить в диаграмму включений, аналогичную диаграмме делителей числа n.

Будем говорить, что n-угольник $(a_1, \ldots, a_n)$ *d-кратно изобарически распадается*, если d хордовых многоугольников из (1) имеют общий центр тяжести. Легко проверить, что он совпадает с центром тяжести исходного n-угольника. Все d-кратно распадающиеся n-угольники

*) Если $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$, то $\tau(n) = (\alpha_1+1)(\alpha_2+1)\ldots(\alpha_n+1)$ (эта формула доказывается легко и имеется во многих учебниках теории чисел).

образуют свободный циклический класс $\mathcal{A}_n^d$, определяемый циклической системой

$$\frac{d}{n}(\boldsymbol{a}_1+\boldsymbol{a}_{d+1}+\ldots+\boldsymbol{a}_{n-d+1})=\frac{1}{n}\sum \boldsymbol{a}_i, \quad \ldots . \qquad (2)$$

Крайние случаи здесь таковы: $\mathcal{A}_n^1=\mathcal{A}_n$, $\mathcal{A}_n^n=\mathcal{A}_{1,n}$.

Примеры для $n=2m$: $\mathcal{A}_{2m}^2$ — класс $2m$-угольников с равной нулю знакопеременной суммой вершин; $\mathcal{A}_{2m}^m$ — класс $2m$-параллелограммов.

Для всякого делителя d числа n существует свой класс $\mathcal{A}_n^d$. Следовательно, всего имеется $\tau(n)$ классов изобарически распадающихся n-угольников; их можно расположить в диаграмму включений соответственно диаграмме делителей числа n.

При $n=6$ класс $\mathcal{A}_{2,3}+\mathcal{A}_{3,2}$ есть класс призм (см. заметку о сложении n-угольников), а $\mathcal{A}_6^2\cap\mathcal{A}_6^3$ — множество 6-угольников, распадающихся как на 2 изобарических 3-угольника, так и на 3 изобарических 2-угольника, т. е. класс аффинно-правильных 6-угольников (теорема 5 гл. 1). Примеры показывают, что сумма двух периодических классов в общем случае не является периодическим классом и пересечение двух классов типа $\mathcal{A}_n^d$ также не является классом того же типа. Таким образом, с помощью взятия сумм периодических классов и пересечений классов типа $\mathcal{A}_n^d$ можно получать новые циклические классы.

Замечание по поводу обозначений. Для того чтобы оттенить разницу между делителем d числа n и «дополнительным» делителем $\bar{d}$, подчеркнем, что в обозначении $\mathcal{A}_n^d$ верхний индекс указывает число изобаричных хордовых многоугольников, на которые распадаются n-угольники рассматриваемого класса, а не количество вершин в каждом из этих многоугольников. Это замечание будет важно ниже, при определении отображения μ_d.

Упражнения

1. $\operatorname{Grad}\mathcal{A}_n^d=n-d+1$.

2. Пусть $\boldsymbol{A}=(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)$. Вершинами n-угольника $(\zeta^d-1)\boldsymbol{A}$ являются «хорды порядка d», т. е. векторы $\boldsymbol{a}_{i+d}-\boldsymbol{a}_i$. Если $d\mid n$, то $\operatorname{Im}(\zeta^d-1)=\mathring{\mathcal{A}}_n^d$, $\operatorname{Ker}(\zeta^d-1)=\operatorname{Fix}\zeta^d=\mathcal{A}_{d,\bar{d}}$.

3. Множество периодических классов $\mathcal{A}_{d,\bar{d}}$ (где $d|n$) является «$\bigcap$-подсвязкой», а множество классов $\mathcal{A}_n^d$ — «$+$-подсвязкой» структуры подпространств пространства $\mathcal{A}_n$. Сравните их со структурой делителей числа n.

§ 2. Хордовые усреднения

Пусть снова $d|n$. *Хордовым d-усреднением* мы назовем циклическое отображение $(a_1, \ldots, a_n) \to (b_1, \ldots, b_n)$:

$$b_1 = \frac{d}{n}(a_1 + a_{d+1} + \ldots + a_{n-d+1}), \quad \ldots, \tag{3}$$

которое далее будет обозначаться символом μ_d. Ясно, что μ_d — изобарическое циклическое отображение, переводящее вершины n-угольника $\boldsymbol{A}$ в центры тяжести $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_d$ строк таблицы (1), т. е. хордовых $\bar{d}$-угольников. Очевидно, что $\boldsymbol{b}_1 = \boldsymbol{b}_{d+1}, \ldots$, т. е. что $\mu_d(a_1, \ldots, a_n)$ *есть $\bar{d}$ раз пройденный d-угольник.*

Теорема 1. μ_d *является проекцией*; $\operatorname{Im}\mu_d = \mathcal{A}_{d,\bar{d}}$, $\operatorname{Ker}_{\sigma}\mu_d = \mathcal{A}_n^d$.

Доказательство. Мы только что показали, что $\operatorname{Im}\mu_d \subseteq \mathcal{A}_{d,\bar{d}}$. Очевидно, $\mathcal{A}_{d,\bar{d}} \subseteq \operatorname{Fix}\mu_d$. [Если $a_1 = a_{d+1}, \ldots$, то $b_1 = a_1, \ldots$.] Отсюда следуют первые два утверждения нашей теоремы. Третье утверждение по существу совпадает с определением класса $\mathcal{A}_n^d$: равенство

$$\mu_d(a_1, a_2, \ldots, a_n) = \sigma(a_1, a_2, \ldots, a_n)$$

— это лишь иная запись циклической системы (2), задающей $\mathcal{A}_n^d$.

В алгебре $K[\zeta]$

$$\mu_d = \frac{d}{n}(1 + \zeta^d + \zeta^{2d} + \ldots + \zeta^{n-d}),$$ в частности $\mu_1 = \sigma$, $\mu_n = 1$.

Множество всех $\tau(n)$ проекций μ_d для заданного n *замкнуто относительно умножения*, точнее, имеет место

Правило. $\mu_r \cdot \mu_s = \mu_{(r,s)}$, *где* $(r, s) = \text{НОД}$ *чисел* $r, s \mid n$.

Доказательство мы оставляем читателю в качестве упражнения.

Отображение $1-\mu_d+\sigma$ является σ-дополнительной к μ_d циклической проекцией. Оно изобарично; кроме того, из теоремы 1 § 3 гл. 3 следует

Теорема 2. $\operatorname{Im}(1-\mu_d+\sigma)=\mathcal{A}_n^d$, $\underset{\sigma}{\operatorname{Ker}}(1-\mu_d+\sigma)=\mathcal{A}_{d,\bar{d}}$.

Упражнение. Каждый из восьми свободных циклических классов 8-угольников (см. § 8 гл. 1) является образом класса $\mathcal{A}_8$ соответственно при следующих циклических проекциях: $\mu_8=1$, μ_4, μ_2, $\mu_1=\sigma$, $\mu_8-\mu_4+\mu_2$, $\mu_8-\mu_4+\mu_1$, $\mu_8-\mu_2+\mu_1$, $\mu_4-\mu_2+\mu_1$.

§ 3. Дополнительные проекции

Две циклические проекции мы назовем *взаимно дополнительными* (ср. § 4 гл. 2), если они переводятся друг в друга инволютивным оператором $1-$. Таким образом, каждой циклической проекции φ отвечает единственная дополнительная проекция $1-\varphi$.

Проекциями, дополнительными к μ_d и $1-\mu_d+\sigma$, являются $1-\mu_d$ и $\mu_d-\sigma$. Покажем, что образы и ядра этих четырех отображений определяются следующей диаграммой:

$$\boxed{\begin{matrix} 1-\mu_d+\sigma & 1-\mu_d \\ \mu_d & \mu_d-\sigma \end{matrix}} \underset{\rightarrow}{\operatorname{Im}} \boxed{\begin{matrix} \mathcal{A}_n^d & \mathcal{A}_n^d \\ \mathcal{A}_{d,\bar{d}} & \mathcal{A}_{d,\bar{d}} \end{matrix}} \underset{\leftarrow}{\operatorname{Ker}} \boxed{\begin{matrix} \mu_d-\sigma & \mu_d \\ 1-\mu_d & 1-\mu_d+\sigma \end{matrix}}$$

Доказательство. $\operatorname{Im}(1-\mu_d+\sigma)$ и $\operatorname{Im}\mu_d$ известны (см. теоремы 1 и 2 из § 2). В силу второго правила из § 2 гл. 3 соответствующие им центральные классы — это $\operatorname{Im}(1-\mu_d)$ и $\operatorname{Im}(\mu_d-\sigma)$. Ядра этих проекций получаются из формулы $\operatorname{Ker}\varphi=\operatorname{Im}(1-\varphi)$, где φ — циклическая проекция.

Применение теоремы 9′ гл. 2 к проекциям μ_d и $1-\mu_d+\sigma$ приводит к следующему результату:

Теорема 3. $\mathcal{A}_n=\mathcal{A}_{d,\bar{d}}\oplus\underset{\circ}{\mathcal{A}_n^d}$, $\mathcal{A}_n=\mathcal{A}_n^d\oplus\underset{\circ}{\mathcal{A}_{d,\bar{d}}}$.

Ее первое утверждение равносильно *однозначности представления каждого n-угольника в виде суммы $\bar{d}$ раз пройденного d-угольника и n-угольника, все хордовые $\bar{d}$-угольники которого имеют центр тяжести* O. Это разложение

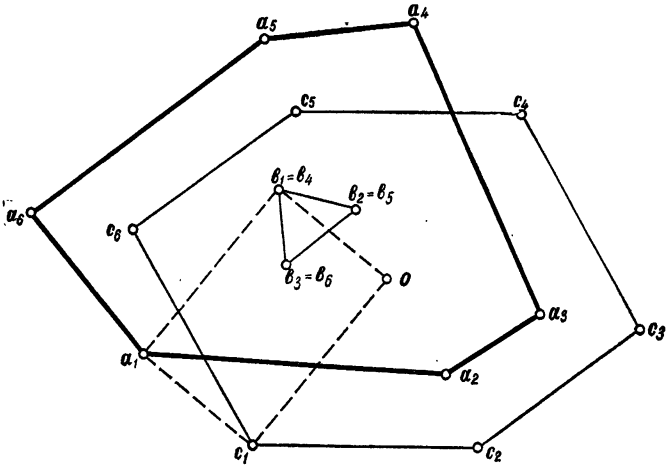


Рис. 48.

легко получить геометрически. Обозначим через $\boldsymbol{B}$ периодический n-угольник — $\bar{d}$ раз пройденный d-угольник центров тяжести последовательно взятых хордовых $\bar{d}$-угольников n-угольника $\boldsymbol{A}$. Тогда равенство $\boldsymbol{A}=\boldsymbol{B}+(\boldsymbol{A}-\boldsymbol{B})$ и будет искомым разложением. В частности, при $n=2m$ и $d=m$ многоугольник $\boldsymbol{B}$ есть дважды пройденный m-угольник, вершины которого являются серединами «главных диагоналей» $\boldsymbol{A}$ (т. е. средними арифметическими пар противоположных вершин), а $\boldsymbol{A}-\boldsymbol{B}$ есть $2m$-параллелограмм с центром тяжести O (т. е. $2m$-угольник, середины всех диагоналей которого совпадают с O, см. рис. 48). Максимальная размерность многоугольников $\boldsymbol{B}$ и $\boldsymbol{A}-\boldsymbol{B}$ в этом случае равна $m-1$ и m.

На рис. 49 изображена диаграмма включений четырех циклических классов теоремы 3 и четырех основных классов (см. § 4 гл. 1). Отрезки, соединяющие два класса

этой диаграммы, означают существование проекции (одной из проекций μ_d, $1-\mu_d+\sigma$ или $1-\sigma$), отображающей верхний класс на нижний. Параллельные отрезки означают одинаковые проекции.

Упражнения

1. Всякий 4-угольник однозначно представим в виде суммы дважды пройденного 2-угольника и параллелограмма с центром тяжести o. Всякий 6-угольник однозначно представим в виде суммы

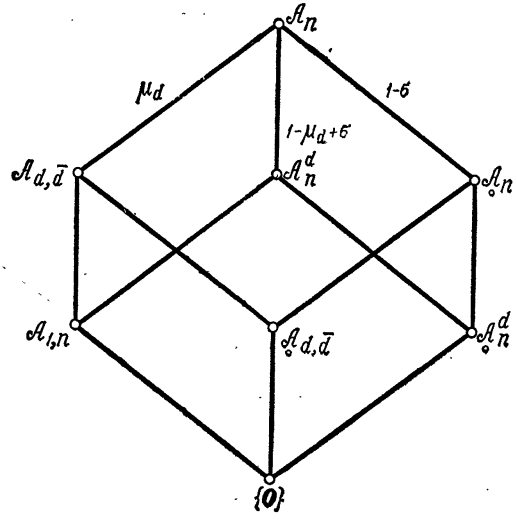


Рис. 49.

дважды пройденного треугольника и 6-параллелограмма с центром тяжести o. Всякий 6-угольник однозначно представим также в виде суммы трижды пройденного 2-угольника и ACO-6-угольника с центром тяжести o.

2. Если φ — изобарическая циклическая проекция, то проекции $\varphi-\sigma$ и $1-\varphi$ не являются изобарическими. Их сумма равна $1-\sigma$, а произведение 0. При этом

$$\mathcal{A}_n = \operatorname{Im}(\varphi-\sigma) \oplus \operatorname{Im}(1-\varphi) = \operatorname{Im}(\varphi-\sigma) \oplus \operatorname{Ker}\varphi,$$

а при $\varphi=\mu_d$ имеем

$$\mathcal{A}_n = \mathcal{A}_{d,\bar{d}} \oplus \mathcal{A}_n^d.$$

§ 4. Последовательные усреднения

Ради полноты изложения рассмотрим здесь обобщения введенных ранее отображений $\varkappa_2$ и $\varkappa_3$, которые для нас будут менее важны, чем отображения, введенные в предыдущих параграфах.

Циклическое отображение $(a_1, \ldots, a_n) \to (b_1, \ldots, b_n)$, определенное системой

$$b_1 = \frac{1}{d}(a_1 + \ldots + a_d), \quad \ldots, \tag{4}$$

будем называть *последовательным d-усреднением* и обозначать через $\varkappa_d$; отображение $\varkappa_d$ изобарично.

При $n = 4$ имеем: $\operatorname{Im}\varkappa_2 = \underset{\sigma}{\operatorname{Ker}}\,\mu_2$ — класс параллелограммов $\mathcal{A}_4^2$, а $\operatorname{Im}\mu_2 = \underset{\sigma}{\operatorname{Ker}}\,\varkappa_2$ — класс дважды пройденных 2-угольников $\mathcal{A}_{2,2}$. При $d \mid n$ справедлива общая

Теорема 4. $\operatorname{Im}\varkappa_d = \mathcal{A}_n^d$, $\underset{\sigma}{\operatorname{Ker}}\,\varkappa_d = \mathcal{A}_{d,\overline{d}}$.

Доказательство. 1) Рассмотрим таблицу (1) для n-угольника $(b_1, \ldots, b_n)$. Сумма элементов любой ее строки равна $\frac{1}{d}\sum a_i$, откуда следует, что $\operatorname{Im}\varkappa_d \subseteq \mathcal{A}_n^d$.

2) σ-ядро отображения — это множество n-угольников, удовлетворяющих условию $\varkappa_d(a_1, \ldots, a_n) = \sigma(a_1, \ldots, a_n)$, которое можно также записать в виде циклической системы

$$\frac{1}{d}(a_1 + \ldots + a_d) = \frac{1}{n}\sum a_i, \ \ldots . \tag{5}$$

Из первых двух равенств системы (5) следует, что $a_1 = a_{d+1}, \ldots$. Отсюда в силу цикличности (5) $\underset{\sigma}{\operatorname{Ker}}\,\varkappa_d \subseteq \mathcal{A}_{d,\overline{d}}$. Обратно, если $a_1 = a_{d+1}, \ldots$, то система (5), очевидно, удовлетворяется.

3) Заметим, что $\varkappa_d = \frac{1}{d}(1 + \zeta + \zeta^2 + \ldots + \zeta^{d-1})$ и $\varkappa_d\mu_d = \sigma$.

Для завершения доказательства теоремы 4 остается показать, что $\mathcal{A}_n^d \subseteq \operatorname{Im}\varkappa_d$, т. е. что для всякого d-кратно изобарически распадающегося n-угольника существует его $\varkappa_d$-прообраз. Мы докажем даже большее:

Для всякого n-угольника из $\mathcal{A}_n^d$ в $\mathcal{A}_n^d$ существует точно один его $\varkappa_d$-прообраз. (*)

Доказательство. В $K[\zeta]$ существует элемент λ_d, удовлетворяющий уравнению

$$1=\varkappa_d\lambda_d+\mu_d \tag{6}$$

[между прочим, отсюда следует, что $\varkappa_d\cdot\lambda_d\cdot\mu_d=0$]. Легко проверить, что этим элементом является

$$-(1-\zeta)\cdot\frac{d}{n}(d\zeta^d+2d\zeta^{2d}+\ldots+(n-d)\zeta^{n-d}).$$

Напомним основные тождества, которыми необходимо пользоваться при подсчете:

$$\varkappa_d(1-\zeta)=\frac{1}{d}(1-\zeta^d);\quad \zeta^n=1;\quad \mu_d=\frac{d}{n}(1+\zeta^d+\ldots+\zeta^{n-d}).$$

Рассмотрим циклическое отображение $\bar{\varkappa}_d=\lambda_d+\sigma$. Так как $\varkappa_d\sigma=\sigma$ [см. формулы (1) гл. 3], то $\varkappa_d\cdot\bar{\varkappa}_d=\varkappa_d\cdot\lambda_d+\sigma$, и из (6) следует, что

$$\varkappa_d\bar{\varkappa}_d=1-\mu_d+\sigma. \tag{7}$$

Но, по теореме 2, $\mathcal{A}_n^d=\mathrm{Fix}\,(1-\mu_d+\sigma)$. Таким образом,

$$\mathcal{A}_n^d=\mathrm{Fix}\,\varkappa_d\cdot\bar{\varkappa}_d. \tag{8}$$

Итак, для всякого n-угольника $\boldsymbol{B}$ из $\mathcal{A}_n^d$ его $\varkappa_d$-прообраз равен $\bar{\varkappa}_d\boldsymbol{B}$; по теореме 5 гл. 2 он принадлежит $\mathcal{A}_n^d$. Однозначность прообраза также следует из (8): если $\boldsymbol{A}_1, \boldsymbol{A}_2\in\mathcal{A}_n^d$ и $\varkappa_d\boldsymbol{A}_1=\varkappa_d\boldsymbol{A}_2$, то $\bar{\varkappa}_d\varkappa_d\boldsymbol{A}_1=\bar{\varkappa}_d\varkappa_d\boldsymbol{A}_2$; в силу коммутативности циклических отображений и из (8) получаем, что $\boldsymbol{A}_1=\boldsymbol{A}_2$. Итак, утверждение (*) и теорема 4 доказаны.

На классе d-кратно изобарически распадающихся n-угольников сужение отображения $\bar{\varkappa}_d$ есть отображение, обратное сужению $\varkappa_d$.

Следствие. *Отображение $\varkappa_d$ есть квазипроекция, имеющая с циклической проекцией $1-\mu_d+\sigma$ одинаковые образ и ядро.*

Это следует из теорем 2, 4, утверждения (*) и первого правила из § 2 гл. 3.

Упражнения

1. $\varkappa_d$ является обратимым элементом в $K[\zeta]$; укажите обратный ему элемент.

2. На классе $2m$-параллелограммов $\varkappa_m$ взаимно однозначно; $\frac{m}{2}(1-\zeta)+\sigma$ обратно к $\varkappa_m$. Пример для $n=4$: отображение $1-\zeta+\sigma$ каждому параллелограмму ставит в соответствие «описанный вокруг него» параллелограмм (см. § 6 гл. 2 и упр. 3 к § 7 гл. 2).

3. Если $n=d\bar{d}$ — разложение n на взаимно простые множители, то

$$\operatorname{Ker}(\zeta^d-1)(\zeta^{\bar{d}}-1)=\operatorname*{Ker}_{\sigma}\varkappa_d\varkappa_{\bar{d}}=\operatorname{Im}\mu_d+\operatorname{Im}\mu_{\bar{d}}=\mathcal{A}_{d,\bar{d}}+\mathcal{A}_{\bar{d},d}$$

— класс $(d, \bar{d})$-призм (см. упр. 5 к § 8 гл. 1).

ГЛАВА 5

ИДЕМПОТЕНТНЫЕ ЭЛЕМЕНТЫ И БУЛЕВЫ АЛГЕБРЫ

Понятие булевой алгебры и остальные необходимые нам понятия из теории структур содержатся в приложении II, которое и рекомендуется просмотреть, прежде чем приступить к этой главе.

§ 1. Идемпотентные элементы кольца

Пусть $(R, +, \cdot)$ — коммутативное кольцо с элементами $0, a, b, \ldots$. Элемент a называется *идемпотентным*, если $a \cdot a = a$. Множество идемпотентных элементов из R обозначим через $E(R)$. Оно содержит нулевой элемент и вместе с элементами a, b всегда содержит ab, но не обязательно $a+b$.

Для любых элементов из R определим *присоединенное произведение*[1]):

$$a \circ b = a + b - ab. \tag{1}$$

Введенное таким образом умножение элементов кольца R коммутативно и ассоциативно, его единицей является 0 кольца. Два элемента называются взаимно *ортогональными*, если их (обычное!) произведение равно 0. Для взаимно ортогональных элементов $a \circ b = a + b$. Если $a, b \in E(R)$, то и $a \circ b \in E(R)$; в частности, в этом случае $a \circ a = a$.

$(E(R), \circ, \cdot)$ является дистрибутивной структурой. Действительно, легко проверить, что для этих операций справедливы законы дистрибутивности и поглощения (остальные аксиомы структуры очевидны).

---

[1]) Ван-дер-Варден ([6], II, стр. 57) обозначает его звездочкой и называет «звездчатым умножением», а Джекобсон ([8], стр. 20) — как и мы, кружочком (и называет «круговой коммутацией»).

С помощью операций $\circ$ и $\cdot$ в множестве элементов $E(R)$ можно ввести отношение $\leqslant$: мы будем писать $a \leqslant b$, если $ab = a$, или, что эквивалентно, $a \circ b = b$. При этом 0 оказывается наименьшим элементом $E(R)$. Таким образом, операции $\circ$, $\cdot$ можно понимать как структурные максимум и минимум (см. приложение II).

Если кольцо R содержит единицу, то она является наибольшим элементом в $E(R)$. Отображение $a \longrightarrow 1-a$ кольца R в R взаимно однозначно и инволютивно. Если $a \in E(R)$, то $1-a \in E(R)$; при этом справедливы равенства

$$1 = a \circ (1-a), \quad a(1-a) = 0, \tag{2}$$

т. е. a и $1-a$ суть *взаимно дополнительные* элементы структуры $E(R)$.

Итак, $(E(R), \circ, \cdot)$ — *дистрибутивная структура с дополнениями, т. е. булева алгебра.*

Теорема 1. *Идемпотентные элементы коммутативного кольца с единицей образуют булеву алгебру по отношению к операциям* $\circ$ *и* $\cdot$.

Далее присоединенное умножение $\circ$ мы будем называть *булевым сложением.*

Заметим, что отображение $1-$ переставляет операции $\circ$ и $\cdot$. Действительно, для любых $a, b \in R$

$$1-(a \circ b) = (1-a)(1-b), \quad 1-ab = (1-a) \circ (1-b). \tag{3}$$

Положим $1-a = a'$; тогда равенства (3) примут вид

$$(a \circ b)' = a' \cdot b', \quad (a \cdot b)' = a' \circ b', \quad a, b \in R.$$

Примеры к теореме 1.

1. В области целостности R с 1 (в частности, в поле) 0 и 1 — единственные идемпотентные элементы. Действительно, из $a^2 = a$ следует $a(1-a) = 0$, а так как R не имеет делителей нуля, то $a = 0$ или $1-a = 0$.

2. Идемпотентами кольца классов вычетов $\mathbf{Z}/(30)$ являются 0, 1, 6, 10, 15, 16, 21, 25. На рис. 50 наглядно изображена булева алгебра $E(\mathbf{Z}/(30))$.

3. Пусть $K_1, K_2, \ldots, K_k$ — поля; $R = \sum \oplus K_i$, т. е. R есть множество k-наборов

$$(a_1, a_2, \ldots, a_k), \quad \text{где} \quad a_i \in K_i, \tag{4}$$

в котором сложение и умножение определяются покомпонентно. Здесь $E(R)$ состоит из 2^k элементов вида (4), где все $a_i \in \{0, 1\}$. Элементы

$$(1, 0, \ldots, 0), \quad (0, 1, \ldots, 0), \quad \ldots, \quad (0, \ldots, 0, 1) \qquad (5)$$

(их число равно k) атомарны в $E(R)$. Произведение двух различных элементов из них равно нулевому элементу $(0, 0, \ldots, 0)$; следовательно, они «взаимно ортогональны».

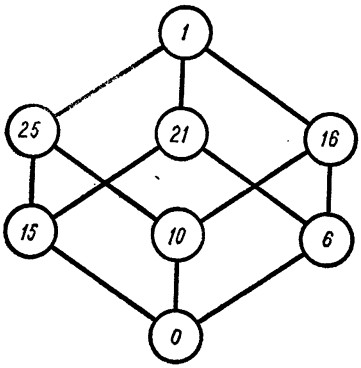


Рис. 50.

Булева сумма элементов (5) является обычной суммой и равна единичному элементу $(1, 1, \ldots, 1)$ кольца R. [Пример 2 можно рассматривать как частный случай этого примера.]

Упражнения

1. Пусть R — коммутативное кольцо с 1. Если $a \in E(R)$ и $b \in E(R)$, то $E(R)$ принадлежит также и элемент

$$a \oplus b := a + b - 2ab = a \circ b - ab = ab' + a'b.$$

$(E(R), \oplus, \cdot)$ является *булевым кольцом* с единицей, т. е. кольцом с 1, в котором каждый элемент идемпотентен.

2. Пусть R — коммутативное кольцо с 1, в котором существует $\frac{1}{2}$. Обозначим через $I(R)$ множество *инволютивных элементов* R, т. е. элементов, квадрат которых равен единице; $I(R)$ — подгруппа группы обратимых элементов.

Рассмотрим взаимно однозначное отображение

$$e \to 2e-1 \qquad (*)$$

множества $E(R)$ на $I(R)$. Посредством этого отображения перенесем операции $(\circ, \cdot)$ из $E(R)$ в $I(R)$. Тогда получим, что $I(R)$ является булевой алгеброй относительно операций

$$a \sqcup b := \frac{1}{2}(1+a+b-ab), \quad a \sqcap b := \frac{1}{2}(-1+a+b+ab)$$

с максимальным элементом 1 и минимальным элементом -1; a и $-a$ являются в этой алгебре взаимно дополнительными. Операции $\sqcup$ и $\sqcap$ можно понимать как максимум и минимум относительно введенного условием $1+a=(1+a)\,b$ отношения $a \leqslant b$.

Если e, $f \in E(R)$, причем посредством отображения $(*)$ элементы e, f переходят соответственно в a, b, то $ef \circ e'f'$ переходит в ab ($e'=1-e$, $f'=1-f$). Элементы ef и $e'f'$ взаимно ортогональны.

3. Если R — прямая сумма k полей K_i, $\operatorname{Char} K_i \neq 2$, то $I(R)$ содержит 2^k элементов (4), где $a_i \in \{1, -1\}$.

§ 2. Булевы алгебры, порожденные конечным числом элементов

Примеры предыдущего пункта служат иллюстрацией также к следующей теореме, которая основывается на представлении единицы в виде суммы попарно ортогональных элементов.

Теорема 2. *Пусть в коммутативном кольце R с единицей элементы $e_1, \ldots, e_k$ отличны от 0 и таковы, что*

$$1 = e_1 + e_2 + \ldots + e_k, \qquad (6)$$

$$e_i e_j = 0, \quad i \neq j. \qquad (7)$$

Тогда все «частичные суммы» выражения $e_1 + \ldots + e_k$ образуют булеву алгебру по отношению к операциям $\circ$, $\cdot$, содержащую 2^k элементов, причем элементы e_i в ней атомарны.

Под «частичными суммами» выражения

$$e_1 + \ldots + e_k \qquad (8)$$

подразумевается само это выражение и все те, которые получаются из него, если отбросить любое число слагаемых. Таких частичных сумм можно построить 2^k, включая пустую сумму, равную 0.

Перейдем теперь к доказательству этой теоремы.

1) *Все e_i идемпотентны.* Действительно, умножим обе части равенства (6) на e_i. В силу (7) получаем $e_i = e_i^2$.

2) Для попарно ортогональных элементов операции $\circ$ и $+$ совпадают. А так как все e_i попарно ортогональны, то частичные суммы выражения (8) являются также булевыми суммами. В частности, *всякая частичная сумма идемпотентна.*

3) *Произведение двух частичных сумм снова является частичной суммой*; она состоит из тех слагаемых e_i, которые входят в оба сомножителя («пересечение» частичных сумм).

4) *Булева сумма двух частичных сумм также является частичной суммой*; в нее входят те e_i, которые содержатся хотя бы в одном из сомножителей («объединение» частичных сумм). Так,

$$(e_1 + e_2) \circ (e_2 + e_3) = e_1 \circ e_2 \circ e_2 \circ e_3 = e_1 \circ e_2 \circ e_3 = e_1 + e_2 + e_3.$$

5) Дополнение к данной частичной сумме есть сумма всех тех e_i, которые в нее не вошли.

Из 1) и 2) следует, что *частичные суммы выражения* (8) *являются элементами* $E(R)$; согласно 3), 4), 5), *они образуют булеву подалгебру алгебры* $(E(R), \circ, \cdot)$.

6) Две частичные суммы совпадают тогда и только тогда, когда в них входят в точности одни и те же слагаемые. (Пусть, например, $e_1 + e_2 + e_3 = e_2 + e_3 + e_4$; умножив это равенство на e_1, получим $e_1 = 0$ в противоречии с тем, что $e_i \neq 0$.) В частности, $e_i \neq e_j$, если $i \neq j$.

Таким образом, наша подалгебра состоит из 2^k элементов.

7) Произведение e_i на частичную сумму равно e_i или 0, смотря по тому, входит e_i в эту частичную сумму или нет. Отсюда следует, что e_i атомарны (см. приложение II).

Наконец, очевидно, что частичные суммы более чем с одним слагаемым не атомарны, чем и завершается доказательство теоремы.

Дополнение 1. *Если в теореме 2 отказаться от предположения $e_i \neq 0$ для всех i, то частичные суммы выражения $e_1 + \ldots + e_k$ по-прежнему будут составлять булеву подалгебру $(E(R), \circ, \cdot)$ с атомарными элементами $e_i \neq 0$.*

Если l — число элементов $e_i \neq 0$, то эта подалгебра содержит 2^l элементов.

Дополнение 2. *Для элементов $e_1, \ldots, e_k \in R$ (6) и (7) эквивалентны равенствам*

$$1 = e_1 \circ e_2 \circ \ldots \circ e_k \tag{6'}$$

и

$$e_i (e_1 \circ e_2 \circ \ldots \circ e_{i-1} \circ e_{i+1} \circ \ldots \circ e_k) = 0. \tag{7'}$$

Таким образом, утверждение, что $e_1, \ldots, e_k$ — попарно ортогональные элементы, в сумме дающие 1, эквивалентно следующему: любой из элементов $e_1, \ldots, e_k$ дополнителен к булевой сумме остальных, и их «прямая» булева сумма равна 1.

Доказательство. В доказательстве теоремы 2 мы уже перешли от (6), (7) к (6'), (7') [см. 1), 2), 3)]. Обратно, пусть элементы $e_1, \ldots, e_k \in R$ удовлетворяют (6'), (7'). Обозначим $e_1 \circ \ldots \circ e_{i-1} \circ e_{i+1} \circ \ldots \circ e_k = e_i^*$; тогда равенства (6'), (7') принимают вид

$$1 = e_i \circ e_i^* \quad \text{и} \quad e_i e_i^* = 0.$$

Это означает, что $1 = e_i + e_i^*$. Умножив последнее равенство на e_i, получим $e_i = e_i^2$; значит, e_i идемпотентны и, следовательно, идемпотентна любая их булева сумма. Далее, если $i \neq j$, то $e_i^* \cdot e_j = (\ldots \circ e_j) \cdot e_j = e_j$, в силу закона поглощения (см. приложение II, аксиома 3). Умножим теперь полученное равенство на e_i; мы получим $0 = e_i e_j$, что доказывает (7). Равенство (6) следует из (6') и (7).

Пусть теперь $e_1, \ldots, e_k$ — произвольные элементы $E(R)$ [так что равенства (6) и (7) не обязаны выполняться]. Определим так называемые *минимальные булевы многочлены* от $e_1, \ldots, e_k$, к числу которых относятся выражение

$$e_1 \cdot e_2 \ldots e_k \quad . \tag{9}$$

и все многочлены, которые могут быть получены из (9) заменой любого числа элементов e_i на $e_i' = 1 - e_i$. Формально число этих многочленов равно 2^k; мы обозначим их через $M_1, M_2, \ldots, M_{2^k}$. Справедливы равенства

$$1 = M_1 + M_2 + \ldots + M_{2^k} \tag{10}$$

и

$$M_iM_j=0 \quad \text{при} \quad i\neq j. \tag{11}$$

[Равенство (10) доказывается индукцией по k; (11), очевидно, следует из того, что $e_i\cdot e_i'=0$.]

Суммы минимальных многочленов, т. е. частичные суммы

$$M_1+M_2+\ldots+M_{2^k}, \tag{12}$$

образуют булеву подалгебру алгебры $(E(R), \circ, \cdot)$ (дополнение 1 к теореме 2); эта подалгебра содержит элементы $e_1, e_2, \ldots, e_k$. (Действительно, запишем, например, равенство $e_1=e_1\cdot 1$ и представим 1 в виде суммы всех минимальных многочленов от $e_2, \ldots, e_k$.) Это есть минимальная булева подалгебра $E(R)$, содержащая заданные элементы $e_1, e_2, \ldots, e_k$; будем говорить, что она порождена ими.

Отличные от нуля минимальные многочлены атомарны в этой подалгебре. Если их количество равно l, то подалгебра содержит 2^l элементов. Очевидно, $l\leqslant 2^k$. В случае $l=2^k$ будем называть порожденную элементами $e_1, \ldots, e_k$ подалгебру *свободной* подалгеброй.

Примеры

1. Пусть $e\in E(R)$ и $e\neq 0, 1$. Минимальные многочлены от e—это e и e'; остальные суммы минимальных многочленов 0 и $e+e'=1$. Булева алгебра, порожденная элементом e, состоит из 4 элементов: 0, 1, e, e' (рис. 51).

2. Пусть $e_1, e_2\in E(R)$, $e_1, e_2\neq 0$, $e_1e_2=0$, $e_1+e_2\neq 1$. Минимальные многочлены от e_1, e_2 суть следующие: $e_1\cdot e_2=0$, $e_1e_2'=e_1$, $e_1'e_2=e_2$, $e_1'e_2'=1-e_1-e_2$. Три последних отличны от нуля. Все отличные от нуля суммы минимальных многочленов сводятся к e_1+e_2, e_1', e_2', 1. Таким образом, булева алгебра, порожденная элементами e_1, e_2, состоит из 8 элементов (рис. 52).

§ 3. Идемпотентные эндоморфизмы абелевой группы; Im-вложения

Под *вложением* мы будем понимать изоморфизм или антиизоморфизм структуры L_1 на подструктуру структуры L_2, т. е. взаимно однозначное отображение L_1 в L_2,

сохраняющее структурные операции «максимум» и «минимум» или меняющее их местами.

В теоремах, связанных с этим понятием (теоремы вложения), речь идет о вложениях некоторых «малых» структур с определенными свойствами (как, например, булевых алгебр) в «большие», которые, вообще говоря, даже не являются дистрибутивными.

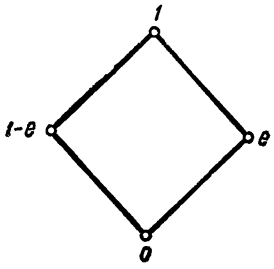


Рис. 51.

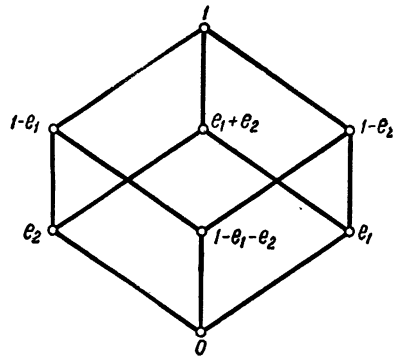


Рис. 52.

Пусть $(\mathcal{A}, +)$ — абелева группа, $(\mathrm{End}(\mathcal{A}), +, \cdot)$ — кольцо эндоморфизмов группы $\mathcal{A}$, $(L(\mathcal{A}), +, \cap)$ — структура подгрупп группы $\mathcal{A}$. Если φ — идемпотентный эндоморфизм $\mathcal{A}$, то

$$(\{0, 1, \varphi, 1-\varphi\}, \circ, \cdot) \tag{13}$$

является булевой алгеброй эндоморфизмов группы $\mathcal{A}$. Образы отображений (13) являются подгруппами в $\mathcal{A}$. При переходе к образам операциям $\circ$ и $\cdot$ соответствуют операции $+$ и $\cap$. Поэтому отображение Im является изоморфизмом булевой алгебры (13) на следующую подструктуру структуры $(L(\mathcal{A}), +, \cap)$:

$$(\{\{0\}, \mathcal{A}, \mathrm{Im}\,\varphi, \mathrm{Im}\,(1-\varphi)\}, +, \cap), \tag{14}$$

которая тем самым тоже является булевой алгеброй (рис. 53). Результатом этого вложения является теорема 8 из § 4 гл. 2. Двойственные рассуждения приводят к выводу, что Ker — антиизоморфизм структур (13) и (14).

Это утверждение можно обобщить. Пусть $(E, \circ, \cdot)$ — произвольная булева алгебра эндоморфизмов $\mathcal{A}$. Заметим, что элементами E являются попарно коммутирующие идемпотентные эндоморфизмы. Если $\varphi\psi = \varphi$ (или $\varphi \circ \psi = \psi$), то говорят, что $\varphi \leqslant \psi$.

Теорема 3 (теорема об Im-вложении). *Пусть* $(E, \circ, \cdot)$ — *булева алгебра эндоморфизмов абелевой группы* $\mathcal{A}$, *тогда* Im (*т. е. отображение* $\varphi \longrightarrow \operatorname{Im}\varphi$) *является изоморфизмом*

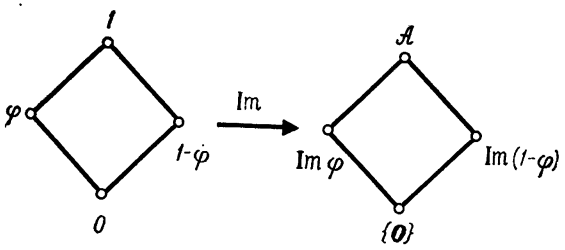


Рис. 53.

$(E, \circ, \cdot)$ *на подструктуру структуры подгрупп* $(L(\mathcal{A}), +, \cap)$.

Эта подструктура, естественно, также является булевой алгеброй; обозначим ее $L_E(\mathcal{A})$.

Доказательство. В силу теоремы 7 гл. 2 отображение Im взаимно однозначно. Поэтому остается доказать, что для коммутирующих идемпотентных эндоморфизмов φ и ψ справедливы равенства

$$\operatorname{Im}(\varphi \circ \psi) = \operatorname{Im}\varphi + \operatorname{Im}\psi; \tag{15}$$

$$\operatorname{Im}(\varphi \cdot \psi) = \operatorname{Im}\varphi \cap \operatorname{Im}\psi. \tag{16}$$

Если $\varphi, \psi \in \operatorname{End}(\mathcal{A})$ и $\varphi\psi = \psi\varphi$, то

$$\operatorname{Fix}\varphi + \operatorname{Fix}\psi \subseteq \operatorname{Fix}(\varphi \circ \psi) \subseteq \operatorname{Im}(\varphi \circ \psi) \subseteq \operatorname{Im}\varphi + \operatorname{Im}\psi; \tag{15'}$$

$$\operatorname{Fix}\varphi \cap \operatorname{Im}\psi \subseteq \operatorname{Im}\varphi\psi \subseteq \operatorname{Im}\varphi \cap \operatorname{Im}\psi. \tag{16'}$$

Действительно, для первого включения (15′) имеем: если $\varphi a = a$, то $(\varphi \circ \psi)a = (\varphi + \psi - \psi\varphi)a = a$ и $\operatorname{Fix}\varphi \subseteq \subseteq \operatorname{Fix}(\varphi \circ \psi)$. Второе включение очевидно (см. § 4 гл. 2).

Третье включение проверяется легко: $(\varphi \circ \psi)\, a = (\varphi + \psi - \psi\varphi)\, a = \varphi a + \psi(a - \varphi a)$.

Для первого включения (16′) имеем: если $\psi a \in \operatorname{Fix}\varphi$, то $\varphi\psi a = \psi a$, т. е. $\psi a \in \operatorname{Im}\varphi\psi$. Второе включение: $\varphi\psi a = \varphi(\psi a) = \psi(\varphi a)$.

Если φ и ψ, кроме того, идемпотентны, то $\operatorname{Fix}\varphi = \operatorname{Im}\varphi$, $\operatorname{Fix}\psi = \operatorname{Im}\psi$ и (15′) и (16′) превращаются в (15), (16). [(16) выполняется даже для таких коммутирующих отображений φ и ψ, из которых по крайней мере одно идемпотентно.]

Для коммутирующих идемпотентных эндоморфизмов φ, ψ выполняются также правила

$$\operatorname{Ker}\varphi\psi = \operatorname{Ker}\varphi + \operatorname{Ker}\psi; \tag{17}$$

$$\operatorname{Ker}(\varphi \circ \psi) = \operatorname{Ker}\varphi \cap \operatorname{Ker}\psi, \tag{18}$$

которые выводятся из (15) и (16) с помощью равенства $\operatorname{Ker}\varphi = \operatorname{Im}(1-\varphi)$ и законов де Моргана. Три следующих соотношения эквивалентны:

1) $\varphi \leqslant \psi$, 2) $\operatorname{Im}\varphi \subseteq \operatorname{Im}\psi$, 3) $\operatorname{Ker}\varphi \supseteq \operatorname{Ker}\psi$.

Для нас теорема 3 представляет интерес в том случае, когда $0,\ 1 \in E$. Тогда $\{0\}$ и $\mathcal{A}$ принадлежат $L_E(\mathcal{A})$; для всякого элемента φ из E существует дополнительный элемент $1-\varphi \in E$; взаимно дополнительные элементы из E переходят при Im-вложении во взаимно дополнительные подгруппы в $\mathcal{A}$, и произведение отображений $\varphi \to 1-\varphi \to \operatorname{Im}(1-\varphi) = \operatorname{Ker}\varphi$ (т. е. отображение Ker) является антиизоморфизмом E на $L_E(\mathcal{A})$.

Дополнение. *Если* $\varphi_1, \ldots, \varphi_k$ *— эндоморфизмы* $\mathcal{A}$, *удовлетворяющие условиям*

$$1 = \varphi_1 + \varphi_2 + \ldots + \varphi_k \tag{19}$$

и

$$\varphi_i \varphi_j = 0,\ i \neq j, \tag{20}$$

то $\mathcal{A} = \sum \oplus \operatorname{Im}\varphi_i$.

Доказательство. В силу (20) $\varphi_1, \ldots, \varphi_k$ попарно коммутируют. В порожденном ими подкольце кольца $\operatorname{End}(\mathcal{A})$ выполнены теорема 2 и ее дополнения; частич-

ные суммы выражения $\varphi_1 + \ldots + \varphi_k$ образуют булеву алгебру, атомарными элементами которой являются $\varphi_i \neq 0$. Заменим (19), (20) эквивалентными равенствами второго дополнения. Доказываемое утверждение следует теперь из теоремы 3.

Упражнения

1. Найдите булеву алгебру идемпотентных эндоморфизмов для циклических групп порядка 6, 30, 105.

2. Если φ — идемпотентный эндоморфизм векторного пространства над полем, характеристика которого не равна двум, то $1+\varphi$ — автоморфизм. Найдите обратный к нему.

§ 4. Булева алгебра циклических проекций

Основная ценность материала этой главы для теории n-угольников состоит в возможности применения теоремы 1 к алгебре $K[\zeta]$ циклических отображений, что приводит к $(E(K[\zeta]), \circ, \cdot)$ — *булевой алгебре циклических проекций*.

Посредством Im-вложения эта булева алгебра отображается в структуру подпространств векторного пространства n-угольников $\mathcal{A}_n$. Так получается булева алгебра циклических классов (теорема 9 гл. 2). Позже (гл. 6) мы докажем, что эта алгебра содержит все циклические классы.

Из § 4 гл. 2 мы знаем, что из двух взаимно дополнительных проекций в $E(K[\zeta])$ одна всегда изобарична, а другая имеет нулевую сумму коэффициентов. Обе они при Im-вложении переходят во взаимно дополнительные циклические классы; один из них свободный, другой — центральный (см. теорему 9′ гл. 2).

σ *является атомарным элементом в* $E(K[\zeta])$. [Действительно, $s(\varphi)=0$ или 1 для всякой циклической проекции φ; следовательно, в силу леммы из § 1 гл. 3 $\varphi\sigma=0$ или $\varphi\sigma=\sigma$; поэтому если $\varphi \leqslant \sigma$, т. е. $\varphi\sigma=\varphi$, то $\varphi=0$ или $\varphi=\sigma$.] Так как σ — наименьшая изобарическая циклическая проекция (см. равенство (1) гл. 3), то остальные атомарные элементы из $E(K[\zeta])$ имеют нулевую сумму коэффициентов. В булевой алгебре циклических классов, полученной посредством Im-вложения алгебры $E(K[\zeta])$, класс $\operatorname{Im}\sigma = \mathcal{A}_{1,n}$ тривиальных n-угольников — минималь-

ный свободный циклический класс — является атомарным; остальные атомарные классы — центральные.

Булева алгебра $E(K[\zeta])$ содержит по меньшей мере $\tau(n)$ хордовых усреднений $\mu_d(d\,|\,n)$ (см. теорему 1 гл. 4), а значит, и порожденную ими подалгебру. [Напоминаем, что $\mu_1=\sigma$; $\mu_n=1$.]

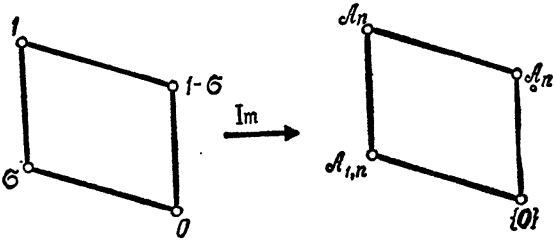


Рис. 54.

§ 5. Примеры Im-вложений

Булева подалгебра алгебры $E(K[\zeta])$, порожденная одним элементом σ, состоит из элементов 0, 1, σ, $1-\sigma$. Посредством Im-вложения получаются четыре основных циклических класса (рис. 54; см. § 4 гл. 1).

Построим *булеву подалгебру* $E(\mu_d, \sigma)$ *алгебры* $E(K[\zeta])$, *порожденную двумя элементами* μ_d *и* σ, где $d\,|\,n$, $d\neq 1$. Булевы минимальные многочлены от μ_d и σ суть

$$\mu_d\sigma=\sigma,\quad (1-\mu_d)\,\sigma=0,\quad \mu_d(1-\sigma)=\mu_d-\sigma,$$
$$(1-\mu_d)(1-\sigma)=1-\mu_d. \tag{21}$$

Многочлены σ, $\mu_d-\sigma$ и $1-\mu_d$ являются системой атомарных элементов подалгебры $E(\mu_d, \sigma)$. Следовательно, она содержит $2^3=8$ элементов — сумм минимальных многочленов; ими являются 0, атомарные элементы, дополнительные к ним элементы и 1. [Это верно для любой подалгебры $E(\varphi, \sigma)$, где φ — произвольная изобарическая циклическая проекция $\neq 1, \sigma$.]

На рис. 55 изображена диаграмма булевой алгебры $E(\mu_d, \sigma)$. Диаграмма циклических классов, полученная посредством Im-вложения, знакома нам по § 3 гл. 4

(см. рис. 49). Теперь мы знаем, что эти восемь циклических классов образуют булеву алгебру относительно операций суммы и пересечения.

Интересно исследовать *булеву подалгебру* E_μ *алгебры* $E(K[\zeta])$, *порожденную всеми циклическими проекциями* μ_d (где $d \mid n$; n — фиксировано). При $n=4$ и вообще при $n=p^2$, где p — простое число, она имеет тип рассмотренной выше алгебры.

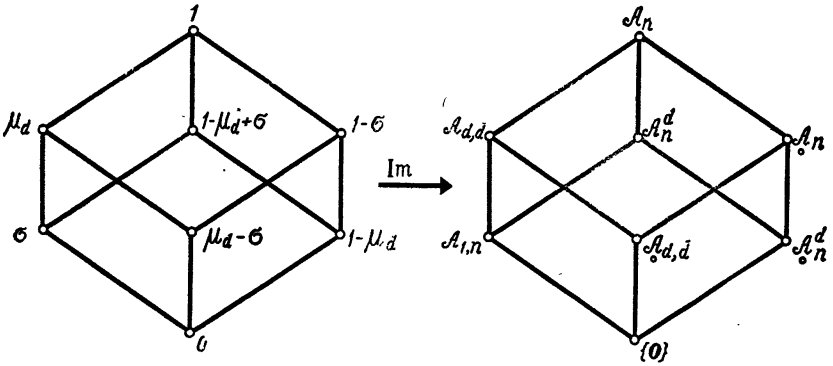


Рис. 55.

Пусть теперь $n=6$. Подалгебра E_μ порождена проекциями $\mu_1=\sigma$, μ_2, μ_3, $\mu_6=1$. Можно считать, что она порождена только элементами μ_2 и μ_3. Минимальные многочлены от μ_2 и μ_3:

$$\mu_2\mu_3=\sigma,\ \mu_2(1-\mu_3)=\mu_2-\sigma,\quad (1-\mu_2)\mu_3=\mu_3-\sigma,\quad (1-\mu_2)(1-\mu_3) \tag{22}$$

отличны от нуля, а следовательно, являются системой атомарных элементов подалгебры E_μ, состоящей из $2^4=16$ элементов — сумм минимальных многочленов. Это восемь изобарических отображений

$$\begin{matrix} 1, & 1-\mu_2+\sigma, & 1-\mu_3+\sigma, & (1-\mu_2+\sigma)(1-\mu_3+\sigma), \\ \sigma, & \mu_2, & \mu_3, & \mu_2+\mu_3-\sigma \end{matrix} \tag{23}$$

(они разбиты на пары σ-дополнительных, записанных в 4 столбцах) и восемь отображений с нулевой суммой

коэффициентов, которые получаются из (23) вычитанием элемента σ, или, что то же самое, умножением на $(1-\sigma)$ [см. формулу (2) гл. 3].

Теорема 4. *Пусть* $n=6$. *Булева алгебра, порожденная четырьмя хордовыми усреднениями* (*здесь* $\tau(6)=4$), *содержит* 16 *циклических проекций. Образами этих проекций в* $\mathcal{A}_6$ *являются восемь свободных циклических классов из* § 8 гл. 1 *и соответствующие им центральные классы. Эти* 16 *циклических классов* 6-*угольников образуют булеву алгебру в структуре, являющейся подпространством* $\mathcal{A}_6$— *векторного пространства* 6-*угольников.*

Доказательство. Достаточно установить справедливость второго утверждения теоремы, так как первое уже было доказано выше, а третье следует из второго на основании теоремы 3. Осталось найти образы $\mathcal{A}_6$ при проекциях (23) и соответствующих им неизобарических проекциях. Образы первых трех пар из (23) получены в теоремах 1 и 2 гл. 4. Далее, согласно § 1 гл. 4,

$$\operatorname{Im}(1-\mu_2+\sigma)(1-\mu_3+\sigma)=$$
$$=\operatorname{Im}(1-\mu_2+\sigma)\cap\operatorname{Im}(1-\mu_3+\sigma)=\mathcal{A}_6^2\cap\mathcal{A}_6^3$$

— класс аффинно-правильных 6-угольников и

$$\operatorname{Im}(\mu_2+\mu_3-\sigma)=\operatorname{Im}(\mu_2\circ\mu_3)=\operatorname{Im}\mu_2+\operatorname{Im}\mu_3=\mathcal{A}_{2,3}+\mathcal{A}_{3,2}$$

— класс призм. Образами $\mathcal{A}_6$ при неизобарических циклических проекциях из E_μ являются центральные классы, соответствующие перечисленным свободным (второе правило из § 2 гл. 3), что и доказывает теорему.

Как известно, единица представима в виде суммы атомарных элементов (22) из E_μ:

$$1=\sigma+(\mu_2-\sigma)+(\mu_3-\sigma)+(1-(\mu_2+\mu_3-\sigma)). \quad (24)$$

Посредством Im-вложения (дополнение к теореме 3) получаем разложение

$$\mathcal{A}_6=\mathcal{A}_{1,6}\overset{\circ}{\oplus}\mathcal{A}_{2,3}\overset{\circ}{\oplus}\mathcal{A}_{3,2}\overset{\circ}{\oplus}\mathcal{R}_6. \quad (25)$$

Справа стоят атомарные классы булевой алгебры, состоящей из 16 циклических классов 6-угольников (см. рис. 46). Из (25) следует

Теорема 5. *Всякий* 6*-угольник однозначно представим в виде суммы тривиального* 6*-угольника, трижды пройденного* 2*-угольника с центром тяжести* o*, дважды пройденного* 3*-угольника с центром тяжести* o *и аффинно-правильного* 6*-угольника с центром тяжести* o.

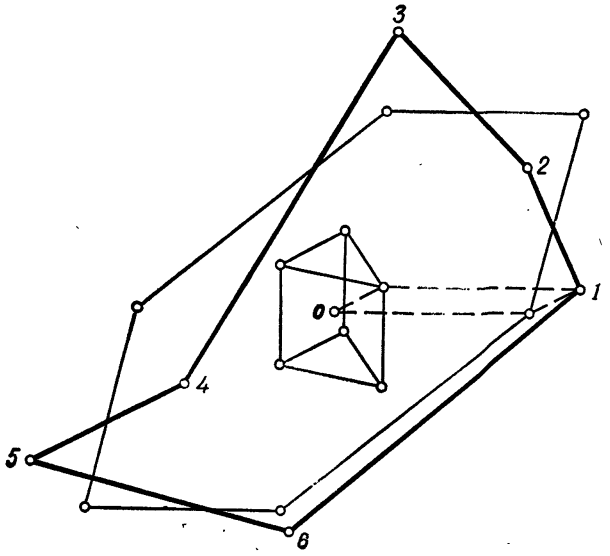


Рис. 56. Разложение 6-угольника с центром тяжести o в сумму призмы с центром тяжести o и аффинно-правильного 6-угольника с центром тяжести o.

Применим (24) к 6-угольнику A:

$$A = \sigma A + (\mu_2 - \sigma) A + (\mu_3 - \sigma) A + (1 - (\mu_2 + \mu_3 - \sigma)) A. \quad (26)$$

Это и есть искомое разложение A: первая компонента σA — это тривиальный шестиугольник — центр тяжести A; $\mu_2 A$ — трижды пройденный 2-угольник, состоящий из центров тяжести хордовых 3-угольников 6-угольника A; аналогично, $\mu_3 A$ — дважды пройденный 3-угольник середин диагоналей A. Вторая и третья компоненты (26) получаются таким сдвигом $\mu_2 A$ и $\mu_3 A$, чтобы их центр тяжести совпал с нулевой точкой.

6-угольник $A^* = (\mu_2 + \mu_3 - \sigma) A$ является призмой. Опишем ее построение: i-я вершина A^* является четвертой вершиной параллелограмма для тройки (i-я вершина $\mu_2 A$, центр тяжести A, i-я вершина $\mu_3 A$). Будем говорить, что призма A^* *натянута на центры тяжести хордовых многоугольников многоугольника* A. Очевидно, что если A — призма, то $A^* = A$.

Четвертая компонента A — многоугольник $(1 - (\mu_2 + \mu_3 - \sigma)) A = A - A^*$ — есть аффинно-правильный 6-угольник с центром тяжести o; мы назовем его *аффинно-правильной компонентой* 6-угольника A.

Просуммируем полученные результаты.

Теорема 6. *Пусть* A — *произвольный 6-угольник и* A^* — *призма, натянутая на центры тяжести его хордовых многоугольников. Тогда* $A - A^*$ *является аффинно-правильным 6-угольником с центром тяжести* o (см. рис. 56).

Замечательно соотношение размерностей A, A^* и $A - A^*$: многоугольник A, вообще говоря, пятимерен, призма A^* не более чем трехмерна, аффинно-правильный 6-угольник $A - A^*$ не более чем двумерен.

Упражнения

1. Проведите аналогичные исследования для $n = 8$.

2. Булева алгебра, порожденная всеми μ_d (где $d \mid n$), имеет $\tau(n)$ атомарных элементов.

3. Пусть $K = \mathbf{Q}$, $V = \mathbf{Q}^2$. Разложите 6-угольник $[(-5, 6), (7, 7), (10, 2), (0, -7), (-5, -5), (-7, -3)]$ в соответствии с теоремой 5.

4. Всякий 4-угольник однозначно представим в виде суммы тривиального 4-угольника, дважды пройденного 2-угольника с центром тяжести o и параллелограмма с центром тяжести o. Разложите таким образом 4-угольник $[(0, 0), (7, 1), (6, 6), (3, 7)]$; здесь $K = \mathbf{Q}$, $V = \mathbf{Q}^2$.

ГЛАВА 6

ОСНОВНАЯ ТЕОРЕМА О ЦИКЛИЧЕСКИХ КЛАССАХ

§ 1. Сравнения в кольце главных идеалов

Пусть R — коммутативное кольцо с 1. Единицы (или обратимые элементы) кольца R образуют по умножению абелеву группу U. Элементы $a, b \in R$ называются *ассоциированными*, если существует такой элемент $u \in U$, что $a = ub$ (в таком случае мы пишем $a \sim b$). Ассоциированность является отношением эквивалентности в R. Класс ассоциированных с a элементов обозначим через Ua.

Порожденный элементом a главный идеал Ra мы будем, как обычно, обозначать через (a). Очевидно, что из $a \sim b$ следует $(a) = (b)$ (но не наоборот!).

Лемма. *Пусть e_1 и e^* — идемпотентные элементы коммутативного кольца с 1. Тогда следующие утверждения эквивалентны:*

$$1)\ e \sim e^*; \quad 2)\ (e) = (e^*); \quad 3)\ e = e^*.$$

Отсюда следует, что класс ассоциированных элементов содержит не более одного идемпотентного элемента.

Доказательство. Очевидно, что 1) $\Rightarrow$ 2) и 3) $\Rightarrow$ 1); таким образом, остается доказать, что 2) $\Rightarrow$ 3).

Множество (e) состоит из элементов ae, где $a \in R$. Так как e — идемпотент, то $ae \cdot e = ae$: умножение на e не меняет элементов из (e). В частности, если $e^* \in (e)$, то $e^*e = e^*$. Аналогично $ee^* = e$. Отсюда в силу коммутативности кольца следует, что $e^* = e$.

Кольцом главных идеалов называется область целостности с 1, в которой всякий идеал является главным[1]). Известные примеры колец главных идеалов: кольцо целых чисел, кольцо многочленов над произвольным телом.

---

[1]) См., например, [9], § 49; [5], ч, I, § 17, 18; [11], § 8, 9.

В кольце главных идеалов всякий отличный от нуля элемент, не являющийся единицей кольца, представим в виде произведения простых элементов — и это представление единственно с точностью до порядка сомножителей и замены их ассоциированными.

Пусть теперь R — кольцо главных идеалов, и пусть задан элемент $m \in R$. Будем говорить, что *a сравним с b по модулю m*:

$$a \equiv b \bmod (m), \text{ если } a - b \in (m).$$

Сравнение является отношением эквивалентности в R, согласованным со сложением и умножением элементов R.

Элемент $e \in R$ назовем *идемпотентным по модулю* (m), если $e^2 \equiv e \bmod (m)$, или, что то же самое, $e(1-e) \equiv 0 \bmod (m)$. Если e идемпотентен $\bmod (m)$, то $e' = 1 - e$ — тоже идемпотентен $\bmod (m)$. Произведение и булева сумма двух элементов, идемпотентных $\bmod (m)$, тоже идемпотентны $\bmod (m)$.

Элемент m из R назовем *свободным от квадратов*, если он представим в виде произведения попарно неассоциированных простых элементов:

$$m = p_1 p_2 \ldots p_k \quad (k \geqslant 1). \qquad (*)$$

Для случая, когда m свободен от квадратов, мы докажем две теоремы об идемпотентных $\bmod (m)$ элементах. При этом мы будем пользоваться простейшими свойствами сравнений, знакомыми читателю из элементарной теории чисел и справедливыми для любого кольца главных идеалов [1]).

Итак, пусть m имеет вид $(*)$ и $i \in \{1, 2, \ldots, k\}$. Нам понадобятся следующие утверждения:

1°. *$a \equiv b \bmod (m)$ тогда и только тогда, когда $a \equiv b \bmod (p_i)$ для всех p_i.*

2°. *Элемент e тогда и только тогда идемпотентен $\bmod (m)$, когда для каждого p_i он сравним $\bmod (p_i)$ либо с 0, либо с 1.*

---

[1]) Для доказательства основной теоремы теории циклических классов n-угольников нам понадобится тот случай, когда R — кольцо многочленов над полем K.

Доказательство. Следующие соотношения эквивалентны:
$e(1-e) \equiv 0 \bmod (m)$; $e(1-e) \equiv 0 \bmod (p_i)$ для всех p_i; для каждого p_i либо $e \equiv 0 \bmod (p_i)$, либо $e \equiv 1 \bmod (p_i)$.

3°. («Китайская конструкция».) *Для всякого p_i в R существует элемент e_i, такой, что*

$$e_i \equiv 1 \bmod (p_i); \tag{1}$$

$$e_i \equiv 0 \bmod \left(\frac{m}{p_i}\right). \tag{2}$$

Из (2) следует

$$e_i \equiv 0 \bmod (p_j) \text{ при } j \neq i. \tag{2'}$$

В силу 2°, e_i *идемпотентен* $\bmod (m)$, а в силу 1°, e_i *однозначно определен* $\bmod (m)$. *Справедливы равенства*

$$1 \equiv e_1 + e_2 + \ldots + e_k \bmod (m); \tag{3}$$

$$e_i e_j \equiv 0 \bmod (m), \quad i \neq j. \tag{4}$$

Доказательство. Так как p_i и $\frac{m}{p_i}$ взаимно просты, то сравнение $\frac{m}{p_i} x_i \equiv 1 \bmod (p_i)$ разрешимо. Обозначим через e_i левую часть этого сравнения, в котором вместо x_i стоит некоторое его решение. Очевидно, e_i удовлетворяет сравнениям (1), (2), а следовательно, и (2'). Сравнения (3), (4) удовлетворяются по модулю всех (p_i), а в силу 1° и $\bmod (m)$.

4°. 2^k *частичных сумм выражения $e_1 + \ldots + e_k$ идемпотентны и попарно не сравнимы* $\bmod (m)$. *Всякий идемпотентный* $\bmod (m)$ *элемент сравним с одной из этих частичных сумм.*

Доказательство. Если I—подмножество множества $\{1, 2, \ldots, k\}$, то, согласно (1) и (2'),

$$\sum_{j \in I} e_j \equiv \begin{cases} 1 \bmod (p_i) & \text{для } i \in I, \\ 0 \bmod (p_i) & \text{для } i \notin I. \end{cases}$$

Это означает, что частичные суммы $e_1 + \ldots + e_k$ идемпотентны $\bmod (m)$ (утверждение 2°). Всякие две формально различные частичные суммы несравнимы $\bmod (m)$: если e_1, например, присутствует в одной из них и отсутствует

в другой, то первая сумма сравнима с единицей, вторая — с нулем $\bmod(p_i)$. Если e — произвольный идемпотентный $\bmod(m)$ элемент, то в силу 2° существует подмножество I множества $\{1, 2, \ldots, k\}$, такое, что $e \equiv 1 \bmod(p_i)$ для $i \in I$ и $e \equiv 0 \bmod(p_i)$ для $i \notin I$. Отсюда следует, что $e \equiv \sum_{i \in I} e_i \bmod(p_j)$ для всех p_j, а значит, $e \equiv \sum_{i \in I} e_i \bmod(m)$.

Итак, доказана

Теорема 1. *Пусть R — кольцо главных идеалов и m — свободный от квадратов элемент вида (*). В R существует ровно 2^k идемпотентных по модулю (m) элементов, попарно не сравнимых $\bmod(m)$ между собой и таких, что каждый идемпотентный $\bmod(m)$ элемент сравним $\bmod(m)$ ровно с одним из этих 2^k элементов.*

Теорема 2. *Пусть R — кольцо главных идеалов и m свободен от квадратов. Всякий элемент из R ассоциирован по модулю (m) с некоторым идемпотентным по модулю (m) элементом.*

Скажем точнее: *для всякого $a \in R$ существуют идемпотентный по модулю (m) элемент e и элемент u, такие, что*

$$a \equiv ue' \bmod(m) \quad [e' = 1 - e], \tag{5}$$

сравнение их $x \equiv 1 \bmod(m)$ *разрешимо.* (6)

Доказательство. Пусть m имеет вид (*) и $e_1, \ldots, e_k$ — идемпотентные по модулю (m) элементы «китайской конструкции». Разобьем все простые элементы $p_1, p_2, \ldots, p_k$ на две группы: те, которые делят a, и те, которые a не делят. Пусть $I = \{i\colon p_i \mid a\}$. Положим

$$\sum_{j \in I} e_j = e.$$

Элемент e идемпотентен по модулю (m). Как и в доказательстве 4°,

$$e \equiv \begin{cases} 1 \bmod(p_i), & \text{если } p_i \mid a, \\ 0 \bmod(p_i), & \text{если } p_i \nmid a. \end{cases}$$

Отсюда следует, что $ae \equiv 0 \bmod (p_i)$ для всех p_i (при $p_i \mid a$ первый сомножитель, а при $p_i \nmid a$ второй сравнимы с нулем $\bmod (p_i)$). Таким образом, $ae \equiv 0 \bmod (m)$, или

$$a \equiv ae' \bmod (m) \quad \text{и} \quad a \equiv (a+e)\,e' \bmod (m).$$

[Последнее сравнение следует из того, что $ee' \equiv 0 \bmod (m)$.] Положим $a+e=u$. Тогда справедливо сравнение (5) и

$$u = a+e \equiv \begin{cases} 0+1 \equiv 1 \not\equiv 0 \bmod (p_i), & \text{если } p_i \mid a, \\ a+0 \equiv a \not\equiv 0 \bmod (p_i), & \text{если } p_i \nmid a. \end{cases}$$

Это означает, что ни один из простых p_i не делит u. Следовательно, u и m взаимно просты и сравнение (6) разрешимо. Теорема доказана.

Замечание. Идемпотентным и ассоциированным с $a \bmod (m)$ элементом является e', а не e. Такие обозначения выбраны потому, что, как показано в доказательстве, элемент p_i ассоциирован $\bmod (m)$ с $e_i' = 1 - e_i$, а не с e_i.

§ 2. Основные теоремы о циклических отображениях и циклических классах

Вернемся к теории n-угольников. Пусть выполнены все условия § 1 гл. 1. Через $K[x]$ обозначим *кольцо многочленов* над K. Оно является кольцом главных идеалов, а также алгеброй над полем K. Если в произвольный многочлен $f(x)$ вместо x подставить ζ, то получим циклическое отображение $f(\zeta)$ — элемент коммутативной алгебры $K[\zeta]$ циклических отображений. Подстановка $x \longrightarrow \zeta$ задает гомоморфизм $K[x]$ на $K[\zeta]$. В силу теоремы 4 гл. 2 ядром этого гомоморфизма является идеал, порожденный многочленом $x^n - 1$:

$$f(x) \equiv 0 \bmod (x^n - 1) \text{ эквивалентно } f(\zeta) = 0.$$

Сравнение $\bmod (x^n - 1)$ в $K[x]$ эквивалентно равенству в $K[\zeta]$:

$$f(x) \equiv g(x) \bmod (x^n - 1) \text{ эквивалентно } f(\zeta) = g(\zeta).$$

Теорема 3. *Многочлен $x^n - 1$ в $K[x]$ свободен от квадратов.*

Доказательство. Многочлен x^n-1 не является ни нулем, ни единицей кольца $K[x]$. Хорошо известно, что многочлен, не свободный от квадратов, должен иметь со своей производной общий множитель, отличный от единицы. Но нетривиальный общий множитель у многочленов $f(x)=x^n-1$ и nx^{n-1} может существовать только в том случае, когда многочлен nx^{n-1} нулевой, т. е. если $n=0$ в поле K, что противоречит предположению гл. 1 о характеристике поля K.

Пусть число простых делителей многочлена x^n-1 в кольце $K[x]$ равно k и

$$x^n-1=p_1(x)\ p_2(x)\ \ldots\ p_k(x), \tag{7}$$

где $p_i(x)$ — попарно не ассоциированные в силу теоремы 3 простые делители x^n-1.

Обозначим через $F_d(x)$ d-й многочлен деления круга из $K[x]$ (см. приложение I). Тогда x^n-1 может быть представлен в виде произведения

$$x^n-1=\prod_{d|n} F_d(x). \tag{8}$$

Поэтому k не меньше числа сомножителей в правой части (8), т. е. числа $\tau(n)$ делителей n. С другой стороны, k, конечно, не больше, чем n, поэтому

$$\tau(n)\leqslant k\leqslant n. \tag{9}$$

Если $K=\mathbf{Q}$ ($\mathbf{Q}$ — поле рациональных чисел), то многочлены деления круга, как известно, неприводимы и (8) является разложением x^n-1 на простые множители. В этом случае $\tau(n)=k$. Второе равенство в (9) ($k=n$) выполняется, если поле K содержит все корни n-й степени из 1 (например, если $K=\mathbf{C}$ — поле комплексных чисел). Многочлен $x-1$ всегда является простым делителем x^n-1 независимо от поля K и числа n.

Циклические проекции являются образами *идемпотентных* $\bmod(x^n-1)$ элементов из $K[x]$ при гомоморфизме $K[x]\to K[\zeta]$. Из теорем 1, 2 и 3 следует

Теорема 4. *Существует ровно 2^k циклических проекций. Всякое циклическое отображение ассоциировано с некоторой циклической проекцией, т. е. для всякого цикличе-*

ского отображения φ *существует циклическая проекция* π *и обратимое циклическое отображение* χ, *такие, что* $\varphi = \chi\pi$.

В силу леммы, циклическая проекция, ассоциированная с циклическим отображением φ, определена однозначно; обозначим ее через π_φ. Из теоремы 4 следует, что множество всех циклических отображений распадается на конечное число классов ассоциированных элементов. Вот еще одна формулировка теоремы 4:

Теорема 4′. *Алгебра* $K[\zeta]$ *состоит из* 2^k *классов ассоциированных элементов; циклические проекции образуют полную систему представителей этих классов.*

Теперь можно вернуться к рассмотрению циклических классов n-угольников. Здесь нам будет полезна

Теорема 5. *Для циклических отображений* φ, ψ *следующие утверждения эквивалентны:*
1) $\varphi \sim \psi$, 2) $(\varphi) = (\psi)$, 3) $\operatorname{Ker}\varphi = \operatorname{Ker}\psi$, 4) $\operatorname{Im}\varphi = \operatorname{Im}\psi$.
В частности, для всякого циклического отображения φ:

$$\operatorname{Ker}\varphi = \operatorname{Ker}\pi_\varphi, \tag{10}$$

$$\operatorname{Im}\varphi = \operatorname{Im}\pi_\varphi. \tag{11}$$

Доказательство. Очевидно, что 1) $\Rightarrow$ 2). Если $(\varphi) \subseteq (\psi)$, то $\operatorname{Ker}\varphi \supseteq \operatorname{Ker}\psi$ и $\operatorname{Im}\varphi \subseteq \operatorname{Im}\psi$ (действительно, если $\varphi = \chi\psi$, то $\operatorname{Ker}\varphi = \operatorname{Ker}\chi\psi \supseteq \operatorname{Ker}\psi$ и $\operatorname{Im}\varphi = \operatorname{Im}\chi\psi = \operatorname{Im}\psi\chi \subseteq \operatorname{Im}\psi$); из $(\varphi) \supseteq (\psi)$ следуют обратные включения. Значит, 2) $\Rightarrow$ 3) и 2) $\Rightarrow$ 4).

В частности, положим $\psi = \pi_\varphi$; тогда, так как 1° $\varphi \sim \pi_\varphi$, то также 2° $(\varphi) = (\pi_\varphi)$, и утверждения 3) и 4) превращаются в равенства (10) и (11).

Далее, рассмотрим утверждения:

1′) $\pi_\varphi \sim \pi_\psi$, 2′) $(\pi_\varphi) = (\pi_\psi)$, 3′) $\operatorname{Ker}\pi_\varphi = \operatorname{Ker}\pi_\psi$,
4′) $\operatorname{Im}\pi_\varphi = \operatorname{Im}\pi_\psi$.

Учитывая, что 1°, 2°, (10), (11) справедливы также и для ψ, легко получить эквивалентность 1) и 1′); 2) и 2′); 3) и 3′); 4) и 4′). Но каждое из утверждений 1′) —4′) эквивалентно равенству $\pi_\varphi = \pi_\psi$. [В самом деле, для 1′) и 2′)

это следует из леммы; для 4′)—из теоремы 7 гл. 2.] В силу формул (7) гл. 2, 3′) эквивалентно равенству $\operatorname{Im}(1-\pi_\varphi)=\operatorname{Im}(1-\pi_\psi)$, а последнее в силу теоремы 7 гл. 2 эквивалентно тому, что $1-\pi_\varphi=1-\pi_\psi$, или $\pi_\varphi=\pi_\psi$ на основании равенства (7) и теоремы 7 из гл. 2.

Следствием теорем 4 и 5 является

Теорема 6. *Всякое циклическое отображение является квазипроекцией.*

Первое доказательство. В каждом коммутативном кольце с единицей из $a\sim b$ следует $a^2\sim b^2$. Если элемент a ассоциирован с идемпотентным элементом e, то $a^2\sim e$; следовательно, $a^2\sim a$. Это утверждение в силу теоремы 4 применимо к каждому циклическому отображению φ; но по теореме 5 из $\varphi^2\sim\varphi$ следует, что $\operatorname{Im}\varphi^2=\operatorname{Im}\varphi$ и $\operatorname{Ker}\varphi^2=\operatorname{Ker}\varphi$, т. е. что φ—квазипроекция.

Второе доказательство. Пусть φ—циклическое отображение. По теореме 8 гл. 2 $\mathcal{A}_n=\operatorname{Im}\pi_\varphi\oplus\operatorname{Ker}\pi_\varphi$, а, согласно (10) и (11), $\mathcal{A}_n=\operatorname{Im}\varphi\oplus\operatorname{Ker}\varphi$. Из теоремы 8′ гл. 2 теперь вытекает, что φ—квазипроекция.

В силу теоремы 1 гл. 2 циклические классы n-угольников определяются как *ядра циклических отображений*. В силу теоремы 5 два циклических отображения имеют одинаковые ядра тогда и только тогда, когда они ассоциированы. По теореме 4′ существует ровно 2^k классов ассоциированных элементов. Отсюда следует, что *существует ровно 2^k циклических классов n-угольников*.

Тот факт, что (при заданном n) существует только конечное число (а именно 2^k) циклических классов n-угольников, составляет внушительную часть основной теоремы о циклических классах.

Чтобы разобраться детальнее в строении циклических классов, полезно подробнее ознакомиться с циклическими проекциями.

В силу (10) и (11) всякому циклическому отображению φ отвечает единственная циклическая проекция π_φ, имеющая то же самое ядро и тот же образ, что и φ. Рассмотрим циклическую проекцию $\varepsilon_\varphi=1-\pi_\varphi$. Она на-

зывается *дополнительной* к π_φ и удовлетворяет «обратным» (по сравнению с (10), (11)) условиям

$$\operatorname{Ker}\varphi = \operatorname{Ker}\pi_{\check{\varphi}} = \operatorname{Im}\varepsilon_{\check{\varphi}}, \tag{12}$$

$$\operatorname{Im}\varphi = \operatorname{Im}\pi_{\check{\varphi}} = \operatorname{Ker}\varepsilon_{\check{\varphi}}. \tag{13}$$

Множество $\{\pi_{\check{\varphi}}\colon \varphi \in K[\zeta]\}$ содержит все циклические проекции (действительно, каждая циклическая проекция ассоциирована сама с собой) и совпадает с множеством дополнительных проекций $\varepsilon_{\check{\varphi}}$. В силу (12) и (13) *совпадают множества*:

1) *ядер циклических отображений*,
2) *ядер циклических проекций*,
3) *образов* $\mathcal{A}_n$ *при циклических проекциях*,
4) *образов* $\mathcal{A}_n$ *при циклических отображениях*.

Но первое из них (а значит, и все четыре) является множеством циклических классов (теорема 1 гл. 2). Подчеркнем еще следующий факт:

Теорема 7. *Всякий циклический класс является образом* $\mathcal{A}_n$ *при некоторой циклической проекции.*

Мы ответили теперь на все поставленные в гл. 2 вопросы, касающиеся циклических классов и циклических отображений.

Булева алгебра $(E(K[\zeta]), \circ, \cdot)$ циклических проекций (см. § 4 гл. 5) содержит 0 и 1 и состоит, согласно теореме 4, из 2^k элементов. С помощью Im-вложения (см. теорему 3 гл. 5) ее можно отобразить в структуру подпространств $\mathcal{A}_n$. В результате в множестве (в булевой алгебре) 2^k циклических классов (см. теорему 9 гл. 2) индуцируется структура исходной булевой алгебры (теорема 7). Итак, имеет место

Основная теорема. *Циклические классы n-угольников образуют конечную булеву алгебру.*

Эта булева алгебра является подструктурой структуры подпространств векторного пространства $\mathcal{A}_n$. *Если* k — *число простых делителей многочлена* $x^n - 1$ *в* $K[x]$, *то число циклических классов n-угольников равно* 2^k.

При всей необозримости структуры подпространств $\mathcal{A}_n$ понятие циклического класса n-угольников выделяет в ней конечную булеву решетку.

Выводы из основной теоремы таковы:

Сумма и пересечение двух циклических классов n-угольников снова являются циклическими классами;

$\mathcal{A}_n$ является прямой суммой атомарных циклических классов — атомарных элементов булевой алгебры циклических классов;

всякий n-угольник однозначно представим в виде суммы n-угольников из атомарных циклических классов.

Понятие атомарных циклических классов, как и число этих классов, зависит от поля K. Грубо говоря, n-угольники атомарных классов обладают определенными свойствами регулярности. В гл. 10—12 мы рассмотрим этот вопрос более подробно.

Пример: $n=6$, $K=\mathbf{Q}$. Так как $\tau(6)=4$, то существует $2^4=16$ циклических классов 6-угольников. Следовательно, в § 5 гл. 5 перечислены все циклические классы 6-угольников и полученное там разложение (рис. 46) является разложением на «атомарные 6-угольники».

Процедура нахождения атомарных циклических классов или атомарных компонент пространства n-угольников может быть следующей. В соответствии с «китайской конструкцией» для всякого делителя $p_i(x)$ двучлена x^n-1 определим многочлен $e_i(x)\in K[x]$, удовлетворяющий условиям

$$e_i(x)\equiv 1 \bmod (p_i(x)), \tag{14}$$

$$e_i(x)\equiv 0 \bmod \left(\frac{x^n-1}{p_i(x)}\right). \tag{15}$$

Тогда $e_1(\zeta), \ldots, e_k(\zeta)$ — отличные от нуля попарно ортогональные циклические проекции, сумма которых равна 1; они являются атомарными циклическими проекциями в $E(K[\zeta])$ (теорема 2 гл. 5); $\operatorname{Im} e_1(\zeta), \ldots, \operatorname{Im} e_k(\zeta)$ — атомарные циклические классы n-угольников, и *разложение $\boldsymbol{A}$ на атомарные компоненты* имеет вид

$$\boldsymbol{A}=e_1(\zeta)\,\boldsymbol{A}+e_2(\zeta)\,\boldsymbol{A}+\ldots+e_k(\zeta)\,\boldsymbol{A}. \tag{16}$$

n-угольники, для которых заданные атомарные компоненты обращаются в нуль, образуют циклический класс, и каждый из 2^k циклических классов можно получить

этим способом. Например, если $K=\mathbf{Q}$, то 6-угольники, у которых отсутствует аффинно-правильная компонента, являются призмами (см. § 5 гл. 5).

Упражнения

1. Пусть φ — циклическое отображение. Если $\mathscr{C}$ — циклический класс, то $\varphi\mathscr{C}$ — тоже циклический класс, причем $\varphi\mathscr{C}\subset\mathscr{C}$ (усиление теоремы 5 гл. 2). Справедливо равенство $\varphi\mathscr{C}=\pi_{\varphi}\mathscr{C}$. В булевой алгебре циклических классов рассмотрим интервалы $[\operatorname{Ker}\varphi,\ \mathscr{A}_n]$ и $[\{0\},\ \operatorname{Im}\varphi]$. Если $\mathscr{C}$ пробегает элементы первого интервала, то $\mathscr{C}\longrightarrow\varphi\mathscr{C}$ — изоморфизм первого интервала на второй (рис. 57). Какие

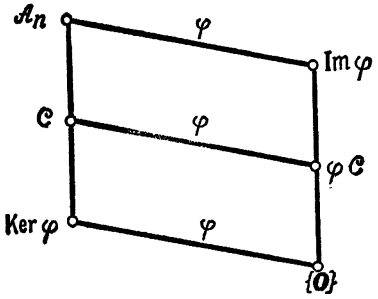


Рис. 57.

циклические отображения обладают следующим свойством: всякий циклический класс принадлежит точно одному из этих двух интервалов? (См. приложение II; § 5 гл. 2; § 2 гл. 3.)

2. Инволютивные циклические отображения называются *циклическими симметриями*. Они составляют подгруппу группы единиц кольца $K[\zeta]$ и имеют сумму коэффициентов ± 1. Пусть теперь $\operatorname{Char}K\neq 2$. Циклические симметрии образуют также булеву алгебру по отношению к композициям, введенным в упр. 2 из § 1 гл. 5; $\varepsilon\longrightarrow 2\varepsilon-1$ есть изоморфизм булевой алгебры циклических проекций на булеву алгебру циклических симметрий; при этом[1]) $\operatorname{Fix}\varepsilon=\operatorname{Fix}(2\varepsilon-1)$, $\operatorname{Bahn}\varepsilon=\operatorname{Bahn}(2\varepsilon-1)$. Существует точно 2^k циклических симметрий.

Отображение

$$\varphi\longrightarrow\operatorname{Fix}\varphi$$

есть изоморфизм булевой алгебры циклических симметрий на булеву алгебру циклических классов. Циклические симметрии φ, для которых $\operatorname{Fix}\varphi=\mathscr{C}$, являются «отражениями относительно $\mathscr{C}$», т. е. эндоморфизмами V^n, которые $\mathscr{C}$ поэлементно оставляют на месте, а всякий n-угольник $\boldsymbol{A}$ из дополнительного к $\mathscr{C}$ класса переводят

[1]) $\operatorname{Bahn}\psi$ (траектория, орбита) определяется как $\operatorname{Im}(1-\psi)$.

в $-A$. [Если $\varphi=2\varepsilon-1$, то можно сказать, что под действием φ всякий n-угольник отражается от своего ε-образа.]

В группе циклических симметрий изобарические симметрии образуют подгруппу индекса 2; неизобарические можно получить из них умножением на -1.

Структурный минимум попарно различных антиатомарных элементов булевой алгебры циклических симметрий равен произведению этих элементов. Циклические симметрии являются частичными произведениями произведения всех антиатомарных элементов.

3. Если $n=2m$, то ζ^m есть изобарическая циклическая симметрия. Пусть $K=\mathbf{Q}$. При $n=4$ изобарические циклические симметрии образуют «четверную группу Клейна», состоящую из четырех элементов: 1, ζ^2, $\frac{1}{2}(-1+\zeta+\zeta^2+\zeta^3)$, $\frac{1}{2}(1+\zeta-\zeta^2+\zeta^3)$. Определите все изобарические циклические симметрии при $n=6$.

§ 3. Простые делители многочлена x^n-1 и атомарные циклические классы

Пусть $p_i(x)$ — произвольный простой делитель x^n-1. Тогда $p_i(\zeta)$ — циклическое отображение, с которым ассоциирована циклическая проекция $1-e_i(\zeta)$ (см. замечание в конце § 1). Равенство (12) принимает вид

$$\operatorname{Ker} p_i(\zeta)=\operatorname{Im} e_i(\zeta). \tag{17}$$

Отсюда следует, что *ядро циклического отображения* $p_i(\zeta)$ *является атомарным циклическим классом.*

Так как вообще ядро циклического отображения $c_0+c_1\zeta+\ldots+c_{n-1}\zeta^{n-1}$ является пространством решений циклической системы $c_0\boldsymbol{a}_1+c_1\boldsymbol{a}_2+\ldots+c_{n-1}\boldsymbol{a}_n=\boldsymbol{o}$, ... (см. § 2 гл. 2), то наш вывод можно переформулировать следующим образом:

Теорема 8. *Циклическая система уравнений, n-набор коэффициентов которой совпадает с n-набором коэффициентов простого делителя многочлена* x^n-1 *в* $K[x]$, *описывает атомарный циклический класс n-угольников.*

Под *n-набором коэффициентов собственного делителя* $\sum c_i x^i$ *многочлена* x^n-1 подразумевается набор $(c_0, \ldots, c_{n-1})$. Положим по определению, что отвечающий многочлену x^n-1 как делителю самого себя n-набор есть $(0, 0, \ldots, 0)$. Последнее соглашение надо учитывать только в простом случае $n=1$.

Как говорилось ранее, существует единственный свободный атомарный циклический класс — класс тривиальных n-угольников; все же остальные атомарные классы — *центральные* (ср. с заметкой о сложении n-угольников в конце гл. 3).

Класс тривиальных n-угольников соответствует простому делителю $x-1$ многочлена x^n-1. Действительно, при $n \neq 1$ набор коэффициентов $x-1$ имеет вид $(-1, 1, 0, \ldots, 0)$; соответствующая циклическая система

$$-\boldsymbol{a}_1+\boldsymbol{a}_2=\boldsymbol{o}, \ \ldots, \text{ или } \boldsymbol{a}_1=\boldsymbol{a}_2=\ldots=\boldsymbol{a}_n$$

определяет класс тривиальных n-угольников. [При $n=1$ многочлен $x-1$ не является *собственным* делителем; в силу соглашения его 1-набор коэффициентов является «нулевым набором» (0); здесь каждый 1-угольник удовлетворяет соответствующей системе $0\boldsymbol{a}_1=\boldsymbol{o}$, которая определяет класс всех 1-угольников, совпадающий с классом тривиальных 1-угольников.]

Положим $p_1(x)=x-1$. Тот факт, что остальные $p_i(x)$ определяют *центральные* классы, легко усмотреть также из следующих соображений: имеем $p_2(x) \ldots p_k(x) = x^{n-1}+\ldots+x+1$; при $x=1$ получаем

$$p_2(1) \ldots p_k(1)=n, \text{ т. е. } p_i(1) \neq 0, \ i=2, \ldots, n.$$

Но $p_i(1)$ — это *сумма коэффициентов* многочлена $p_i(x)$. Итак, сумма коэффициентов циклического отображения $p_i(\zeta)$ отлична от нуля, и задаваемая этим набором коэффициентов циклическая система определяет *центральный* класс (см. теорему 1 гл. 1).

Если пронормировать все многочлены $p_i(x)$, где $i \neq 1$, умножив их на $\frac{1}{p_i(1)}$, то подстановка $x \longrightarrow \zeta$ приведет к *изобарическим* циклическим отображениям с теми же ядрами, что и $p_i(\zeta)$.

Если $K=\mathbf{Q}$ ($\mathbf{Q}$ — поле рациональных чисел), то простыми делителями x^n-1 являются *многочлены деления круга* $F_d(x)$, где $d|n$ и $F_1(x)=x-1$; они и определяют атомарные циклические классы.

Пример: $K=\mathbf{Q}$, $n=6$. В этом случае

$$x^6-1=F_1(x)F_2(x)F_3(x)F_6(x)=$$
$$=(x-1)(x+1)(x^2+x+1)(x^2-x+1)$$

и $F_2(1)=2$, $F_3(1)=3$, $F_6(1)=1$. Циклические системы с нормированными наборами коэффициентов для $d=2, 3, 6$ имеют вид

$$d=2:\ \frac{1}{2}(\boldsymbol{a}_1+\boldsymbol{a}_2)=\boldsymbol{o},\ \ldots;\quad d=3:\ \frac{1}{3}(\boldsymbol{a}_1+\boldsymbol{a}_2+\boldsymbol{a}_3)=\boldsymbol{o},\ \ldots;$$

$$d=6:\ \boldsymbol{a}_1-\boldsymbol{a}_2+\boldsymbol{a}_3=\boldsymbol{o},\ \ldots\ .$$

Они определяют (как видно непосредственно из уравнений) соответственно класс $\mathcal{A}_{2,3}$ трижды пройденных 2-угольников с центром тяжести $\boldsymbol{o}$, класс $\mathcal{A}_{3,2}$ дважды пройденных 3-угольников с центром тяжести $\boldsymbol{o}$ и класс $\mathcal{R}_6$ аффинно-правильных 6-угольников с центром тяжести $\boldsymbol{o}$. Вместе с классом тривиальных 6-угольников эти классы образуют полный набор атомарных циклических классов. Циклическими отображениями, которые получаются подстановкой $x\longrightarrow\zeta$ в нормированные многочлены $F_d(x)$, $d=2, 3, 6$, являются

$$\frac{1}{2}F_2(\zeta)=\varkappa_2,\quad \frac{1}{3}F_3(\zeta)=\varkappa_3,\quad F_6(\zeta)=\alpha_3,$$

т. е. в точности те отображения, которые рассматривались в гл. 2 в связи с изучением возможных классов 6-угольников.

Упражнения

1. Для любого n и любого допустимого K «n-угольник — центр тяжести» n-угольника $\boldsymbol{A}$ является атомарной компонентой $\boldsymbol{A}$.

2. Пусть $n=4$ и элемент -1 не является квадратом в K. Пусть $\boldsymbol{A}$ — некоторый 4-угольник и $\boldsymbol{A}-\sigma\boldsymbol{A}=\boldsymbol{A}_0$ (см. § 4 гл. 2). Атомарными компонентами $\boldsymbol{A}$ являются $\sigma\boldsymbol{A}$, дважды пройденный 2-угольник середин диагоналей 4-угольника $\boldsymbol{A}_0$ и параллелограмм, который имеет тот же параллелограмм середин сторон, что и $\boldsymbol{A}_0$.

Если элемент -1 является квадратом в K, то этот параллелограмм не будет атомарной компонентой: его можно будет разложить на два квадрата (ср. гл. 11).

ГЛАВА 7

ИДЕМПОТЕНТ-ВЛОЖЕНИЕ. ФАКТОРКОЛЬЦО КОЛЬЦА ГЛАВНЫХ ИДЕАЛОВ

В настоящей главе мы рассмотрим с некоторой общей точки зрения те развитые в § 1 гл. 6 конструкции, которые совместно с понятием Im-вложения послужили алгебраическим фундаментом доказательства основной теоремы о циклических классах n-угольников.

Эта глава является чисто алгебраической. Мы изучим здесь соотношения между делителями элемента m, принадлежащего кольцу главных идеалов R; идеалами кольца R, порожденными этими делителями; идеалами факторкольца $R/(m)$; идемпотентными элементами кольца $R/(m)$. Нас особенно будет интересовать случай, когда m свободен от квадратов.

Эти алгебраические результаты в гл. 8 будут применены к теории n-угольников. При этом в гл. 8 роль R будет играть кольцо многочленов $K[x]$, а роль элемента $m \in R$ — свободный от квадратов многочлен $x^n - 1$; факторкольцо $K[x]/(m)$ с точностью до изоморфизма совпадает с алгеброй циклических отображений векторного пространства n-угольников $\mathcal{A}_n$.

В § 2 гл. 8 будет рассмотрена в общем виде фундаментальная связь между делителями $x^n - 1$, циклическими классами n-угольников и циклическими проекциями (см. изображенную на рис. 60 схему). В § 3 гл. 6 эта связь была рассмотрена лишь для простых делителей $x^n - 1$ и атомарных циклических классов.

В начале настоящей главы мы придадим новую форму второй теореме о Im-вложении, рассматривая ее как теорему о R-модулях. Это позволит нам ввести понятие идемпотент-вложения.

Теореме об идемпотент-вложении в гл. 9 мы противопоставим теорему об идеал-вложении. Она описывает общую

ситуацию, из которой, минуя циклические проекции, следует теорема о циклических классах и устанавливается связь между делителями $x^n - 1$ и циклическими классами n-угольников.

§ 1. R-модули

Пусть $(R, +, \cdot)$—кольцо с 1 и $(\mathcal{A}, +)$—абелева группа. Элементы R мы будем обозначать через $a, b, \ldots, r, s \ldots$, а элементы $\mathcal{A}$—через $\boldsymbol{a}, \boldsymbol{b}, \ldots$.

$\mathcal{A}$ называется *R-модулем*, если определено отображение $R \times \mathcal{A}$ в $\mathcal{A}$:

$$(r, \boldsymbol{a}) \to r\boldsymbol{a}, \tag{1}$$

называемое *умножением*, такое, что выполняются следующие правила:

1) $r(\boldsymbol{a}+\boldsymbol{b}) = r\boldsymbol{a} + r\boldsymbol{b}$; 2) $(r+s)\boldsymbol{a} = r\boldsymbol{a} + s\boldsymbol{a}$;

3) $(rs)\boldsymbol{a} = r(s\boldsymbol{a})$; 4) $1\boldsymbol{a} = \boldsymbol{a}$.

Для всякого $r \in R$ множество $r\mathcal{A}$ есть подгруппа в $\mathcal{A}$. Говорят, что r *аннулирует* a, если

$$r\boldsymbol{a} = \boldsymbol{o}. \tag{2}$$

Множество тех r, для которых равенство (2) выполняется при любом $\boldsymbol{a}$, называется *аннулятором* $\mathcal{A}$ (обозначается $\operatorname{an}\mathcal{A}$):

$$\operatorname{an}\mathcal{A} = \{r : r\boldsymbol{a} = \boldsymbol{o} \text{ для всех } \boldsymbol{a}\} = \{r : r\mathcal{A} = \{\boldsymbol{o}\}\}.$$

Множество $\operatorname{an}\mathcal{A}$ является (двусторонним) идеалом в R. (Разумеется, правильнее было бы писать $\operatorname{an}_R \mathcal{A}$.)

Пример 1. Пусть $R = \operatorname{End}(\mathcal{A})$. Умножение (1) определим как применение эндоморфизма к элементу из $\mathcal{A}$. Тогда $\operatorname{an}\mathcal{A} = (0)$.

Пример 2. Кольцо $(R, +, \cdot)$ является R-модулем, если в качестве умножения (1) взять умножение в R. Так как единицу аннулирует только 0, то $\operatorname{an} R = (0)$.

§ 2. Идемпотент-вложение

Пусть R коммутативно. Тогда $r\mathcal{A}$ является R-подмодулем $\mathcal{A}$ для любого r. Пусть, как и выше, $(E(R), \circ, \cdot)$ — булева алгебра идемпотентных элементов из R (теорема 1 гл. 5). Если e, $f \in E(R)$, то

$$\text{из } e\mathcal{A} = f\mathcal{A} \text{ следует } e \equiv f \pmod{\operatorname{an}\mathcal{A}}, \tag{3}$$

$$(e \circ f)\,\mathcal{A} = e\mathcal{A} + f\mathcal{A}, \tag{4}$$

$$ef\mathcal{A} = e\mathcal{A} \cap f\mathcal{A}. \tag{5}$$

Свойство (3) доказывается так же, как теорема 7 гл. 2, а (4) и (5) — как правила (15) и (16) из § 3 гл. 5. Обозначим через $L(\mathcal{A})$ структуру R-подмодулей $\mathcal{A}$. Пользуясь свойствами (3)—(5), мы по-новому сформулируем теорему 3 гл. 5:

Теорема 1 (идемпотент-вложение). *Пусть R — коммутативное кольцо с единицей, $\mathcal{A}$ есть R-модуль,* $\operatorname{an}\mathcal{A} = (0)$. *Тогда отображение*

$$e \longrightarrow e\mathcal{A} \quad (e \in E(R)) \tag{6}$$

является изоморфизмом булевой алгебры $(E(R), \circ, \cdot)$ на подструктуру структуры $(L(\mathcal{A}), +, \cap)$.

Рассматриваемое вложение выделяет в $L(\mathcal{A})$ булеву алгебру R-подмодулей $\mathcal{A}$.

§ 3. Частный случай идемпотент-вложения

Рассмотрим частный случай R-модуля — само (коммутативное) кольцо R (см. в § 1 пример 2). Подмодулями в нем являются его идеалы. В частности, $rR = (r)$ есть главный идеал, порожденный элементом r. Через $L(R)$ обозначим структуру идеалов кольца R. По теореме 1 отображение

$$e \longrightarrow eR = (e) \tag{7}$$

является изоморфизмом булевой алгебры $(E(R), \circ, \cdot)$ на подструктуру структуры идеалов $(L(R), +, \cap)$.

Особенно проста связь между идемпотентами и идеалами R, если R представляет собой *прямую сумму полей*

$$R = K_1 \oplus K_2 \oplus \ldots \oplus K_k.$$

Единица 1_R этого кольца имеет вид

$$1_R = e_1 + e_2 + \ldots + e_k, \tag{8}$$

где $e_1, e_2, \ldots, e_k$ — попарно ортогональные идемпотентные элементы

$$e_1 = (1, 0, \ldots, 0), \quad e_2 = (0, 1, \ldots, 0), \ldots$$
$$\ldots, e_k = (0, 0, \ldots, 1). \tag{9}$$

Элементы $e_1, \ldots, e_k$ атомарны в булевой алгебре $(E(R), \circ, \cdot)$; всякий элемент в $E(R)$ представляет собой частичную сумму выражения $e_1 + \ldots + e_k$ (см. пример 3 из § 1 гл. 5 и теорему 2 гл. 5).

Вложение (7) переводит единицу (8) кольца R в

$$R = (e_1) + (e_2) + \ldots + (e_k), \tag{10}$$

а всякую частичную сумму — в соответствующую частичную сумму выражения $(e_1) + (e_2) + \ldots + (e_k)$. При этом идеал (e_i) состоит из всех элементов кольца вида $(0, \ldots, 0, a_i, 0, \ldots, 0)$ и, следовательно, изоморфен K_i.

Более того, справедливо утверждение: *каждый идеал M кольца R является частичной суммой выражения* $(e_1) + (e_2) + \ldots + (e_k)$.

Доказательство. Имеем $M = e_1M + e_2M + \ldots + e_kM$ [вложение $\subseteq$ следует из того, что $M = 1_R \cdot M$, и из (8); вложение $\supseteq$ — из того, что $M \supseteq e_iM$]. Всякий идеал e_iM или равен нулевому идеалу, или совпадает с (e_i) [ясно, что $(e_i) \supseteq e_iM$; с другой стороны, так как идеал (e_i) изоморфен полю, то он содержит только нулевой идеал (0) и самого себя].

Теорема 2. *Если R — (конечная) прямая сумма полей, то отображение* (7) *является изоморфизмом $E(R)$ на (полную!) структуру идеалов кольца R.*

Таким образом, в прямой сумме k полей всякий идеал есть главный идеал, порожденный некоторым идемпотентным элементом; структура идеалов является булевой алгеброй из 2^k элементов.

§ 4. Идеалы и делимость в кольце главных идеалов

Пусть R—кольцо главных идеалов. Включение $(r) \supseteq (s)$ эквивалентно утверждению, что r делит s: $r \mid s$. Если $r \mid s$, то все ассоциированные с r элементы делят любой элемент, ассоциированный с s. В частности, утверждению 1) $(r) = (s)$ эквивалентно 2) $r \mid s$ и $s \mid r$, а если R—область целостности, то и 3) $r \sim s$.

Сумма идеалов (a) и (b) есть идеал, порожденный НОД (a, b) элементов a и b: $(a) + (b) = ((a, b))$; пересечение идеалов (a) и (b) есть идеал, порожденный НОК $[a, b]$ элементов a и b: $(a) \cap (b) = ([a, b])$. НОД и НОК элементов a, b определяются этими свойствами с точностью до ассоциированности.

Отношение «делит» и понятия НОД и НОК переносятся на классы ассоциированных элементов. *Множество классов ассоциированных элементов является структурой L с операциями* НОК *и* НОД *в качестве (структурных) максимума и минимума.* Отношение «делит» является в этой структуре отношением частичной упорядоченности. Соответствие $r \longrightarrow (r)$ является антиизоморфизмом структуры L на структуру $L(R)$ идеалов кольца R. Обе эти структуры обладают свойством дистрибутивности (см. приложение II).

В кольце главных идеалов разложение на простые множители однозначно (точная формулировка приведена в § 1 гл. 6). Отсюда следует важное свойство колец главных идеалов: в них *всякая возрастающая цепочка идеалов обрывается.*

Пусть $m \in R$. Классы элементов, ассоциированных с делителями m, образуют подструктуру $L(m) \subseteq L$; назовем ее *m-подструктурой* структуры L. Структура $L(m)$ также дистрибутивна и при $m \neq 0$ конечна.

Если m свободен от квадратов, т. е. допускает представление

$$m = p_1 p_2 \ldots p_k, \qquad (*)$$

где p_i—попарно не ассоциированные простые элементы $(k \geqslant 1)$, то 2^k частичных произведений из $p_1 p_2 \ldots p_k$ попарно не ассоциированы и представляют собой все делители числа m (пустое частичное произведение считаем

равным 1). Очевидно, что m-подструктура является структурой с дополнениями, даже булевой алгеброй с 2^k элементами и с простыми элементами $p_1, p_2, \ldots, p_k$ в качестве атомарных.

Идеал (m) будем называть *свободным от квадратов*, если m имеет вид (*).

§ 5. Факторкольцо кольца главных идеалов

Пусть заданы кольцо главных идеалов R и элемент $m \neq 0$ из R; далее, пусть $R/(m)$ — *факторкольцо по главному идеалу* (m). Рассмотрим следующие структуры:

L_1: *m-подструктура*,
L_2: *интервал* $[(m), R]$ *структуры идеалов* R,
L_3: *структура идеалов кольца* $R/(m)$,
L_4: $(E(R/(m)), \circ, \cdot)$ — *булева алгебра идемпотентов кольца* $R/(m)$.

Делители m обозначим через t. Соответствие

$$t \longrightarrow (t)$$

является антиизоморфизмом i_{12} структур L_1 и L_2.

Далее, канонический гомоморфизм $a \longrightarrow a + (m)$, отображающий R на $R/(m)$, индуцирует изоморфизм структуры идеалов, содержащих (m), на структуру идеалов кольца $R/(m)$. Так как идеалы, содержащие m, суть не что иное, как идеалы, порожденные делителями m, то отображение

$$i_{23}\colon\ (t) \longrightarrow (t + (m))$$

является изоморфизмом L_2 на L_3. Очевидно, справедлива

Теорема 3. *Произведение отображений* i_{12}, i_{23} *является антиизоморфизмом* m-*подструктуры на структуру идеалов кольца* $R/(m)$. *Всякий идеал из* $R/(m)$ *имеет вид* $(t + (m))$, *где* $t \mid m$. *Если* $t_1, t_2 \mid m$, *то* $(t_1 + (m)) = (t_2 + (m))$ *тогда и только тогда, когда* $(t_1) = (t_2)$.

Из теоремы 3 следует, что всякий идеал кольца $R/(m)$ является главным. Однако $R/(m)$ может содержать делители нуля, и тогда его нельзя назвать кольцом главных идеалов.

Пусть a — произвольный элемент из R; тогда $(a+(m))$ — идеал в $R/(m)$ и справедлива

Лемма. a) *Если* $(a, m)=(t)$, *то* $(a+(m))=(t+(m))$; b) *равенство* $(a_1+(m))=(a_2+(m))$ *эквивалентно* $(a_1, m)=(a_2, m)$.

Доказательство. a) Если $a\in(t)$, то $a+(m)\in(t+(m))$. С другой стороны, так как $t\in(a, m)$, то t допускает представление $t=ua+vm$; отсюда следует, что

$$t+(m)=ua+vm+(m)=ua+(m)\in(a+(m)).$$

b) Пусть $(a_i, m)=(t_i)$, $i=1, 2$. Тогда из a) следует, что $(a_i+(m))=(t_i+(m))$, и, в силу теоремы 3, $(t_1+(m))=(t_2+(m))$ эквивалентно $(t_1)=(t_2)$.

Напомним, что элемент $e\in R$ тогда и только тогда идемпотентен $\bmod(m)$, когда смежный класс $e+(m)$ идемпотентен в кольце $R/(m)$. Согласно § 3, существует изоморфизм

$$i_{43}: e+(m)\longrightarrow(e+(m))$$

L_4 на булеву подалгебру структуры L_3.

Произведение отображений $i_{12}i_{23}$ дает возможность получить все идеалы кольца $R/(m)$, а отображение i_{43} — по крайней мере один из них. Естественно, возникает вопрос: является ли отображение i_{43} отображением *на*, или, что то же самое, всякий ли идеал в $R/(m)$, который может быть записан в виде $(t+(m))$, где $t\mid m$, порождается идемпотентным смежным классом? Ответ на этот вопрос дает «китайская теорема об остатках» (см. теорему 4′).

Теорема 4 («китайская теорема об остатках»). *Пусть элемент* $m\neq 0$ *кольца главных идеалов* R *представим в виде произведения попарно взаимно простых элементов:* $m=t_1t_2\ \ldots\ t_k$. *Тогда существуют смежные классы*

$$e_1+(m),\ e_2+(m),\ \ldots,\ e_k+(m) \tag{11}$$

со следующими свойствами:

a) *смежные классы* (11) *попарно ортогональны, а их сумма является смежным классом единицы;*

b) $(t_i+(m))=(1-e_i+(m))$.

Доказательство. а) Пусть $m/t_i = \bar{t}_i$. Так как t_i, $\bar{t}_i$ взаимно просты, сравнение $\bar{t}_i x_i \equiv 1 \bmod (t_i)$ разрешимо в R. Обозначим через e_i левую часть сравнения, в котором x_i есть некоторое его решение. Тогда

$$e_i \equiv 1 \bmod (t_i), \tag{12}$$

$$e_i \equiv 0 \bmod (\bar{t}_i). \tag{13}$$

Следовательно, $e_i \equiv 0 \bmod (t_j)$, $j \neq i$, и

$$1 \equiv e_1 + e_2 + \ldots + e_k \bmod (m), \tag{14}$$

$$e_i e_j \equiv 0 \bmod (m), \quad i \neq j. \tag{15}$$

Последние два сравнения справедливы потому, что они выполняются для попарно взаимно простых t_i, $i = 1, 2, \ldots, k$. В факторкольце $R/(m)$ сравнения (14) и (15) переходят в равенства. Утверждение а) доказано.

Из сравнений (14), (15) следует, что e_i идемпотентны $\bmod (m)$ [достаточно (14) умножить на e_i]. Значит, $1 - e_i$ тоже идемпотентны $\bmod (m)$.

b) $1 - e_i \in (t_i)$ [см. (12)]; $m \in (t_i)$, следовательно, $(1 - e_i, m) \subseteq (t_i)$. С другой стороны, в силу (13) существуют $u_i \in R$, такие, что $e_i = u_i \bar{t}_i$; следовательно, $1 = 1 - e_i + u_i \bar{t}_i$. Умножив последнее равенство на t_i, получим $t_i \in (1 - e_i, m)$. Таким образом, $(t_i) = (1 - e_i, m)$ и утверждение b) следует из леммы.

Теорема 4′ (частный случай «китайской теоремы об остатках»). *Пусть $m \neq 0$ — элемент кольца главных идеалов R и t — делитель m, взаимно простой с m/t. Тогда система сравнений*

$$e \equiv 1 \bmod (t), \tag{16}$$

$$e \equiv 0 \bmod \left(\frac{m}{t}\right) \tag{17}$$

разрешима в R [однозначно $\bmod (m)$], причем e и $1 - e$ идемпотентны $\bmod (m)$ и

$$(t + (m)) = (1 - e + (m)). \tag{18}$$

Следствие. *Пусть, как всегда, R — кольцо главных идеалов, m свободно от квадратов и $R/(m)$ — факторкольцо по*

(m). *Всякий идеал в* $R/(m)$ *является главным, порожденным некоторым идемпотентным элементом* (см. теорему 2 гл. 6).

Доказательство. Из теоремы 3 следует, что всякий идеал в $R/(m)$ может быть записан в виде $(t+(m))$, где $t \mid m$, а из теоремы 4′ — что при свободном от квадратов m он порождается идемпотентным смежным классом.

Теорема 5. *Если* R *— кольцо главных идеалов и* m *— свободный от квадратов элемент вида* (*), *то структуры* L_1, L_2, L_3, L_4 *являются булевыми алгебрами из* 2^k *элементов. Произведение* $i_{12}i_{23}$ *антиизоморфно отображает* L_1 *через* L_2 *на* L_3, *а отображение* i_{43} *является изоморфизмом* L_4 *на* L_3.

Доказательство. 1) L_1 является булевой алгеброй из 2^k элементов (см. § 4); значит, L_2 и L_3 — тоже булевы алгебры с этим же количеством элементов (так как i_{12} и i_{23} — антиизоморфизм и изоморфизм).

2) i_{43} является изоморфизмом L_4 на L_3 (см. только что доказанное следствие). Поэтому булева алгебра L_4 тоже содержит 2^k элементов.

Условимся обозначать через e_t решение системы сравнений (16), (17). В силу (18) имеет место

Правило. $(t+(m)) = (1-e_t+(m))$.

Так как $1-e_t+(m)$ и $e_t+(m)$ – взаимно дополнительные элементы из L_4, то, применяя i_{43} и пользуясь правилом, получим

$(t+(m))$ и $(e_t+(m))$ — *взаимно дополнительные идеалы в* $R/(m)$.

Теорема 6 («китайский изоморфизм»). *Если* R *— кольцо главных идеалов и* $m \in R$ *свободно от квадратов, то отображение*

$$t \longrightarrow e_t+(m) \tag{19}$$

является изоморфизмом m*-подструктуры на булеву алгебру идемпотентных элементов кольца* $R/(m)$.

Доказательство. Рассмотрим произведение следующих отображений: 1) антиизоморфизма i_{12} структуры

L_1 на L_2; 2) изоморфизма i_{23} структуры L_2 на L_3; 3) «дополнительного» отображения L_3 на L_3: $x \to 1-x$ (оно является инволютивным антиизоморфизмом L_3 на L_3); 4) изоморфизма i_{43}^{-1} структуры L_3 на L_4. Последовательность указанных отображений действует следующим образом:

$$t \to (t) \to (t+(m)) \to (e_t+(m)) \to e_t+(m)$$

и является изоморфизмом.

Имея в виду специально теорию n-угольников, придадим связи между рассматриваемыми булевыми алгебрами более удобный для нас вид. При этом, чтобы избежать антиизоморфизмов, заменим булевы алгебры L_2, L_3 и L_4 двойственными к ним алгебрами L_2', L_3' и L_4'.

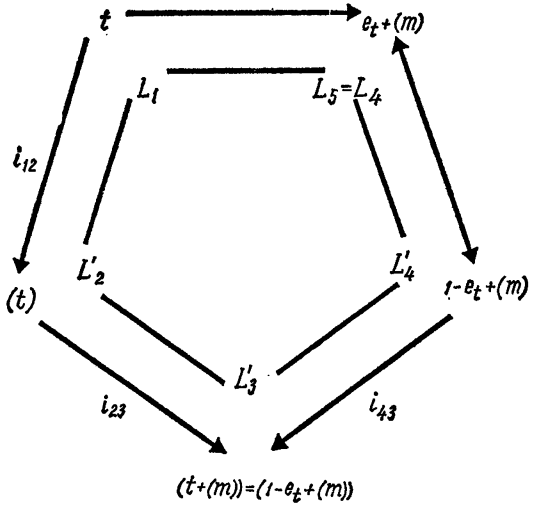


Рис. 58.

Теорема 5′. *При условиях теоремы* 5 L_1, L_2', L_3', L_4' *являются булевыми алгебрами из* 2^k *элементов, связанными естественными изоморфизмами* i_{12}, i_{23} *и* i_{43}, *отображающими соответственно* L_1 *на* L_2', L_2' *на* L_3', L_4' *на* L_3'.

Обозначим через L_5 второй экземпляр L_4 и рассмотрим булевы алгебры

$$L_1,\ L_2',\ L_3',\ L_4',\ L_5, \text{ где } L_5 = L_4 = E(R/(m), \circ, \cdot).$$

Тогда «дополнительное» отображение в $E(R/(m))$ является инволютивным антиизоморфизмом булевой алгебры L_5, т. е. изоморфизмом L_4' на L_5; «китайский изоморфизм» отображает L_1 на L_5.

Остается указать следующую интерпретацию сформулированного в этом параграфе правила. Пусть $t \mid m$; построим две цепочки отображений

$$t \longrightarrow (t) \longrightarrow (t + (m))$$

и

$$t \longrightarrow e_t + (m) \longrightarrow 1 - e_t + (m) \longrightarrow (1 - e_t + (m)),$$

переводящих t в идеал из $R/(m)$ (отдельные шаги этих цепочек — это изоморфизмы L_1 на L_2' и L_2' на L_3'; L_1 на L_5, L_5 на L_4' и L_4' на L_3' (см. рис. 58)). В силу правила результирующие отображения являются одним и тем же изоморфизмом L_1 на L_3'.

§ 6. Факторкольцо как сумма факторколец

Теорема 4″ (дополнение к «китайской теореме об остатках»). *Пусть выполнены условия теоремы* 4. *Тогда*

$$R/(m) \cong \sum \oplus R/(t_i).$$

Доказательство. Обозначим через φ_i: $a \longrightarrow a + (t_i)$ канонический гомоморфизм R на $R/(t_i)$. Тогда

$$\varphi\colon\ a \longrightarrow (\varphi_1 a,\ \varphi_2 a,\ \ldots,\ \varphi_k a)$$

— гомоморфизм R в прямую сумму колец $R/(t_i)$. Ядром этого гомоморфизма является идеал (m). Далее, $a \in \operatorname{Ker}\varphi$ тогда и только тогда, когда $a \equiv 0 \bmod (t_i)$ для всех i, т. е. когда $a \equiv 0 \bmod (m)$. Если $a_1,\ a_2,\ \ldots,\ a_k$ — заданные элементы из R, а $e_1,\ \ldots,\ e_k$ — элементы, рассматриваемые в доказательстве теоремы 4, а), то в силу (12) и (13)

$$a_1 e_1 + a_2 e_2 + \ldots + a_k e_k \equiv a_i \bmod (t_i),\ i = 1,\ 2,\ \ldots,\ k.$$

Отсюда следует, что φ есть отображение R *на* прямую сумму, что и доказывает теорему.

Разложение теоремы 4″ можно несколько уточнить:

$$R/(m) = \sum \oplus (e_i + (m)) \tag{20}$$

и

$$(e_i + (m)) \cong R/(t_i). \tag{21}$$

Действительно, частичные суммы суммы всех смежных классов (11) образуют булеву подалгебру алгебры L_4. [Это следует из теоремы 4, а) и дополнения 1 к теореме 2 гл. 5.] Посредством i_{43} (идемпотент-вложение) эта подалгебра отображается в структуру идеалов L_3, при этом сумма всех смежных классов (11) отображается в разложение (20). Изоморфизм (21) доказывается следующим образом: индуцированный φ изоморфизм $R/(m)$ на прямую сумму $R/(t_i)$ переводит $ae_i + (m)$ в $(0, \ldots, 0, \varphi_i a, 0, \ldots, 0)$, но

$$\{ae_i + (m) : a \in R\} = (e_i + (m)).$$

Следствие из теоремы 4″. *Если m — свободный от квадратов элемент вида* (*), *то* $R/(m) = \sum \oplus R/(p_i)$, *причем* $R/(p_i)$ — *поля.*

Для доказательства достаточно применить теорему 4″ к взаимно простым делителям p_i и вспомнить, что идеал, порожденный простым элементом, максимальный. Это означает, что факторкольцо по нему является полем.

Итак, если R — кольцо главных идеалов, а m свободен от квадратов, то $R/(m)$ является *прямой суммой полей.* Структура идеалов кольца $R/(m)$ изоморфна булевой алгебре его идемпотентных элементов (ср. теорему 5).

ГЛАВА 8

БУЛЕВЫ АЛГЕБРЫ n-УГОЛЬНИКОВ (ТЕОРИЯ I)

§ 1. Булевы алгебры $L_1 — L_5$

Пусть выполнены все предположения § 1 гл. 1. Напомним, что через $K[x]$ обозначается кольцо многочленов над полем K; многочлен $x^n — 1$ свободен от квадратов, k — число простых делителей многочлена $x^n — 1$ в $K[x]$, $L(x^n — 1)$ — структура делителей $x^n — 1$ — является булевой алгеброй с 2^k элементами (см. § 2 гл. 6).

Подстановка $x \longrightarrow \zeta$ индуцирует гомоморфизм $K[x]$ на алгебру циклических отображений $K[\zeta]$:

$$f(x) \longrightarrow f(\zeta). \tag{1}$$

Ядро этого гомоморфизма есть идеал, порожденный многочленом $x^n — 1$. [Действительно, $\zeta^n — 1 = 0$; но если $t(x) \mid x^n — 1$, то $t(\zeta) \neq 0$, так как $1, \zeta, \ldots, \zeta^{n-1}$ независимы (см. теорему 4 гл. 2).] Отсюда следует, что

$$K[x]/(x^n — 1) \cong K[\zeta]. \tag{2}$$

При этом изоморфизме

$$f(x) + (x^n — 1) \longrightarrow f(\zeta); \tag{3}$$

в частности, смежный класс x переходит в ζ. Итак, имеет место

Теорема 1. *Алгебра $K[\zeta]$ циклических отображений изоморфна факторкольцу кольца главных идеалов $K[x]$ по свободному от квадратов идеалу $(x^n — 1)$.*

Если разложение многочлена $x^n — 1$ на простые множители в $K[x]$ имеет вид

$$x^n — 1 = p_1(x)\, p_2(x) \ldots p_k(x), \tag{4}$$

то

$$K[x]/(x^n — 1) \cong \sum \bigoplus K[x]/(p_i(x)) \tag{5}$$

(см. следствие из теоремы 4″ гл. 7); слагаемые в правой части являются полями.

Теорема 1′. *$K[\zeta]$ является прямой суммой k полей.*

Напомним важные следствия из этих теорем: 1) булева алгебра $E(K[\zeta])$ циклических проекций имеет точно 2^k элементов; 2) всякий идеал в $K[\zeta]$ является главным, порожденным некоторой циклической проекцией (см. § 3 гл. 7).

Структуры L_1—L_5 (§ 5 гл. 7) в нашем случае принимают вид

L_1: *структура делителей многочлена* $x^n - 1$;
L_2: *интервал* $[(x^n - 1), K[x]]$ *из структуры идеалов кольца* $K[x]$;
L_3: *структура идеалов кольца* $K[\zeta]$;
L_4: $(E(K[\zeta]), \circ, \cdot)$—*булева алгебра циклических проекций*;
L_5: $(E(K[\zeta]), \circ, \cdot)$—*булева алгебра циклических проекций.*

(Напомним, что L_5—это просто второй экземпляр L_4.) Все эти структуры являются булевыми алгебрами. Между ними существуют изоморфизмы или антиизоморфизмы (теоремы 5 и 6 гл. 7), переводящие каждый элемент одной из этих алгебр в единственный соответствующий ему элемент любой другой из них.

Мы хотим описать действие этих отображений. Для этого введем следующие обозначения: $t(x)$—произвольный делитель многочлена $x^n - 1$; $\overline{t}(x)$—дополнительный к нему делитель, так что $x^n - 1 = t(x)\,\overline{t}(x)$; $e(x)$—многочлен, идемпотентный по модулю $(x^n - 1)$; $e(\zeta)$—отвечающая $e(x)$ циклическая проекция.

Система сравнений

$$e(x) \equiv 1 \bmod (t(x)), \tag{6}$$

$$e(x) \equiv 0 \bmod (\overline{t}(x)) \tag{7}$$

имеет единственное по модулю $(x^n - 1)$ решение, т. е. существует единственный многочлен степени $< n$ [1]), удовлетворяющий этой системе. Это решение идемпотентно

[1]) К числу многочленов степени $< n$ присоединяем и нулевой многочлен.

по модулю $(x^n - 1)$ (теорема 4′ гл. 7); обозначим его через $e_t(x)$.

Как и раньше, чтобы избежать антиизоморфизмов, заменим булевы алгебры L_2, L_3, L_4 двойственными к ним алгебрами L_2', L_3', L_4'. Итак, мы будем рассматривать булевы алгебры

$$L_1,\ L_2',\ L_3',\ L_4',\ L_5 \qquad (*)$$

и отображения

i_{12}: $t(x) \longrightarrow (t(x))$ — антиизоморфизм L_1 на L_2 и, следовательно, изоморфизм L_1 на L_2';

i_{23}: $(t(x)) \longrightarrow (t(\zeta))$ — канонический изоморфизм L_2 на L_3 и, следовательно, изоморфизм L_2' на L_3' (подстановка $x \longrightarrow \zeta$);

i_{43}: $e(\zeta) \longrightarrow (e(\zeta))$ — изоморфизм L_4 на L_3, следовательно, также L_4' на L_3' (идемпотент-вложение; см. теорему 2 гл. 7);

i_{45}: $e(\zeta) \longrightarrow 1 - e(\zeta)$ — «дополнительное» отображение (инволютивный антиизоморфизм) в $E(K[\zeta])$, следовательно, изоморфизм L_4' на L_5 или совпадающий с ним изоморфизм i_{54} L_5' на L_4';

i_{15}: $t(x) \longrightarrow e_t(\zeta)$ — изоморфизм L_1 на L_5 (теорема 6 гл. 7).

[Обозначения L_1, L_2, ..., L_5, i_{12}, i_{23}, i_{43} будут в дальнейшем употребляться именно в этом, специализированном по сравнению с гл. 7 смысле.] Согласно теоремам 5′ и 6 гл. 7, имеет место

Теорема 2. *Структуры L_1, L_2', L_3', L_4', L_5 являются булевыми алгебрами из 2^k элементов; они связаны указанными выше изоморфизмами.*

Произведения отображений $i_{12}i_{23}$: $t(x) \longrightarrow (t(x)) \longrightarrow (t(\zeta))$ и $i_{15}i_{54}i_{43}$: $t(x) \longrightarrow e_t(\zeta) \longrightarrow 1 - e_t(\zeta) \longrightarrow (1 - e_t(\zeta))$ совпадают в силу правила из § 5 гл. 7:

$$(t(\zeta)) = (1 - e_t(\zeta)). \qquad (8)$$

Таким образом, отображения i_{12}, i_{23}, i_{43}^{-1}, i_{45}, i_{15}^{-1} образуют цикл изоморфизмов: их произведение является тождественным автоморфизмом L_1 (рис. 59).

Нахождение образа нетривиально лишь для последнего из отображений теоремы 2. Для заданного делителя $t(x)$ многочлена $x^n - 1$ здесь требуется найти многочлен $e_t(x)$. Мы укажем явное выражение для $e_t(x)$ через производную $t'(x)$.

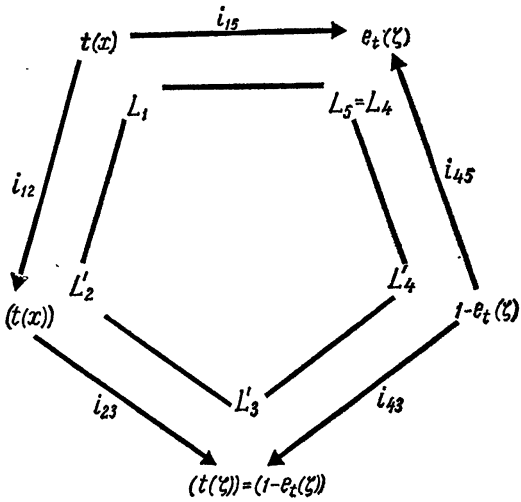


Рис. 59.

Теорема 3 [дифференциальное выражение для $e_t(x)$]. *Если* $t(x)$ *—делитель* $x^n - 1$, *то многочлен*

$$\frac{1}{n}\,\overline{t}\,(x)\,x\,t'(x) \tag{9}$$

удовлетворяет сравнениям (6) *и* (7), *так же как многочлен* [1])

$$\frac{1}{n}\left[\overline{t}\,(x)\,xt'(x) - \operatorname{Grad} t \cdot (x^n - 1)\right] \tag{10}$$

степени $< n$.

---

[1]) $\operatorname{Grad} f(x)$ — степень многочлена $f(x)$.

Доказательство. Очевидно, многочлен (9) удовлетворяет сравнению (7). Для проверки сравнения (6) продифференцируем обе части равенства $\bar{t}(x)\,t(x) = x^n - 1$ и умножим результат на $\frac{x}{n}$:

$$\frac{1}{n}\bar{t}'(x)\,xt(x) + \frac{1}{n}\bar{t}(x)\,xt'(x) = x^n.$$

Первое слагаемое $\equiv 0 \bmod (t(x))$, а правая часть $\equiv 1 \bmod (t(x))$ [поскольку $x^n \equiv 1 \bmod (t(x))$, ибо $t(x) \mid x^n - 1$]. Отсюда следует (6).

Старший член многочлена (9) равен $\frac{1}{n}\operatorname{Grad} t \cdot x^n$. Поэтому степень многочлена (10), сравнимого с (9) $\bmod (x^n - 1)$, будет $< n$, что и доказывает теорему.

В силу теоремы 3

$$e_t(\zeta) = \frac{1}{n}\bar{t}(\zeta)\,\zeta t'(\zeta). \tag{11}$$

Пример. Для делителей $t(x)$: 1, $x-1$, $x^{n-1}+\ldots$ $\ldots + x + 1$, $x^n - 1$, циклическими проекциями $e_t(\zeta)$ являются 0, σ, $1-\sigma$, 1.

Теперь мы можем указать решение следующей задачи: *для данного циклического отображения $f(\zeta)$ найти циклическую проекцию, порождающую в $K[\zeta]$ тот же идеал, что и $f(\zeta)$.*

Во-первых, найдем, хотя бы с помощью алгоритма Евклида, НОД многочленов $f(x)$ и $x^n - 1$. Обозначим его через $t(x)$. По лемме § 5 гл. 7 $(f(\zeta)) = (t(\zeta))$. Искомая циклическая проекция, согласно (8), находится по теореме 3. Из теоремы 5 гл. 6 следует

Теорема 4. *Если $f(\zeta)$ — циклическое отображение и $t(x) = \text{НОД}\,(f(x), x^n - 1)$ в $K[x]$, то*

$$(f(\zeta)) = (t(\zeta)) = (1 - e_t(\zeta)); \tag{12}$$

$1 - e_t(\zeta)$ является циклической проекцией, имеющей с отображениями $f(\zeta)$ и $t(\zeta)$ одинаковые образ и ядро.

Отображение i_{1_5} является изоморфизмом. Поэтому элементу $\bar{t}(x)$, дополнительному в структуре L_1 к $t(x)$, оно

ставит в соответствие циклическую проекцию $1-e_t(\zeta)$, дополнительную в структуре L_5 к $e_t(\zeta)$: $e_{\bar{t}}(\zeta)=1-e_t(\zeta)$.

Следовательно, в силу (11)

$$1-e_t(\zeta)=\frac{1}{n}t(\zeta)\,\zeta\bar{t}'(\zeta). \tag{13}$$

Упражнение. Определите идемпотентные по модулю (x^n-1) многочлены степени $<n$ из $\mathbf{Q}[x]$ для $n=4$ и 6.

§ 2. Делители многочлена x^n-1 и циклические классы

Как известно, Im-вложение является изоморфизмом булевой алгебры циклических проекций $L_5:(E(K[\zeta]),\mathbf{o},\cdot)$ на L_6: булеву алгебру циклических классов n-угольников (см. § 2 гл. 6). С другой стороны, если $t(x)\mid x^n-1$, то $\operatorname{Ker} t(\zeta)$ — ядро циклического отображения $t(\zeta)$ — является циклическим классом (теорема 1 гл. 2). Мы будем называть его *циклическим классом, определенным многочленом* $t(x)$. Точнее говоря, этот класс определяется циклической системой уравнений, n-набор коэффициентов которой совпадает с n-набором коэффициентов многочлена $t(x)$ (ср. § 3 гл. 6).

Теорема 5. *Отображение*

$$t(x)\longrightarrow \operatorname{Ker} t(\zeta) \tag{14}$$

задает изоморфизм структуры делителей многочлена x^n-1 *на булеву алгебру циклических классов* n*-угольников.*

Докажем теорему последовательным применением уже известных изоморфизмов.

Циклическая проекция, переводящая множество всех n*-угольников в циклический класс* n*-угольников, определенный многочленом* $t(x)$, *есть* $e_t(\zeta)$:

$$\operatorname{Ker} t(\zeta)=\operatorname{Im} e_t(\zeta). \tag{15}$$

Действительно, $t(\zeta)$ и циклическая проекция $1-e_t(\zeta)$ имеют совпадающие ядра (теорема 4); поэтому

$$\operatorname{Ker} t(\zeta)=\operatorname{Ker}(1-e_t(\zeta))=\operatorname{Im} e_t(\zeta)$$

[см. формулы (7) гл. 2 и равенство (12) гл. 6, где роль $e_t(\zeta)$ играет $\varepsilon_{t(\zeta)}$].

Доказательство теоремы 5. Произведение отображений $i_{15}\,\mathrm{Im}$: $t(x) \longrightarrow \mathrm{Im}\, e_t(\zeta)$ является изоморфизмом $L_1 = L(x^n - 1)$ на L_8. В силу формулы (15) он совпадает с отображением (14).

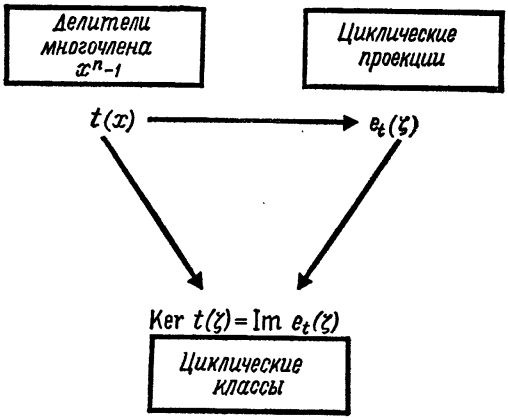


Рис. 60.

Предположим, что выбрана система 2^k попарно не ассоциированных делителей $x^n - 1$; тогда из теоремы 5 следует

Теорема 6. *Любой из 2^k циклических классов n-угольников описывается циклической системой уравнений, n-набор коэффициентов которой совпадает с n-набором коэффициентов одного из 2^k делителей многочлена $x^n - 1$* (ср. теорему 8 гл. 6).

Теорема 7. *Две циклические системы уравнений с n-наборами коэффициентов $(c_0, c_1, \ldots, c_{n-1})$ и $(d_0, d_1, \ldots, d_{n-1})$ тогда и только тогда определяют один и тот же циклический класс, когда многочлены $\sum c_i x^i$ и $\sum d_i x^i$ имеют один и тот же* НОД *с многочленом $x^n - 1$.*

Таким образом, вопрос о том, определяют ли две циклические системы один и тот же класс, можно решить с помощью алгоритма Евклида.

Доказательство теоремы 7. Равенство $\operatorname{Ker} f(\zeta) = \operatorname{Ker} g(\zeta)$ эквивалентно равенству $(f(\zeta)) = (g(\zeta))$ (теорема 5 гл. 6); по лемме из § 5 гл. 7 последнее равенство эквивалентно утверждению, что $f(x)$ и $g(x)$ имеют с $x^n - 1$ один и тот же НОД.

Изоморфизмы теоремы 2 позволяют отобразить каждую из алгебр L_1, L_2', L_3', L_4' на L_5, тогда как Im отображает L_5 на L_6. Таким образом, для каждой из алгебр

$$L_1,\ L_2',\ L_3',\ L_4',\ L_5 \qquad (*)$$

имеется изоморфизм, отображающий ее на булеву алгебру циклических классов L_6. При этом элементам алгебр (*), отвечающим друг другу в силу теоремы 2, сопоставляется один и тот же циклический класс.

Каждый из изоморфизмов алгебр (*) на L_6 указывает свой путь к изучению циклических классов. Для изоморфизма L_1 на L_6 он изложен в теоремах 5 и 6. Чаще всего мы будем пользоваться этим изоморфизмом и изоморфизмом Im алгебры L_5 на L_6. Изоморфизм L_4' на L_6 является отображением Ker; он ставит в соответствие каждому элементу $e(\zeta) \in L_4'$ циклический класс $\operatorname{Im}(1 - e(\zeta)) = \operatorname{Ker} e(\zeta)$ и представляет самостоятельный интерес (см. § 3 гл. 5). Изоморфизмы L_2' и L_3' на L_6 ставят в соответствие каждому идеалу циклический класс и будут рассмотрены в гл. 9.

Упражнение. Если $x^n - 1 = t(x)\,\bar{t}(x)$, то $\operatorname{Im} t(\zeta) = \operatorname{Ker} \bar{t}(\zeta)$. Отображение $t(x) \to \operatorname{Im} t(\zeta)$ задает антиизоморфизм структуры делителей $x^n - 1$ на булеву алгебру циклических классов.

§ 3. Спектр

Пусть N — поле разложения многочлена $x^n - 1$ над K и w — первообразный корень n-й степени из единицы: $N = K(w)$. Под *спектром* многочлена $x^n - 1$ мы будем понимать множество всех корней n-й степени из единицы:

$$w,\ w^2,\ \ldots,\ w^{n-1},\ w^n = 1. \qquad (16)$$

Оно распадается на k классов, каждый из которых состоит из корней, принадлежащих одному простому в $K[x]$ делителю x^n-1. Каждый такой класс мы будем называть *точкой* спектра.

Функция, определенная на множестве (16), с областью значений $\{0, 1\}$, принимающая равные значения на сопряженных корнях, называется заданной на спектре *характеристической функцией*. Если e, f — характеристические функции, то функция ef равна 1 в точках, где обе функции принимают значение 1, и 0 во всех остальных точках; $e \circ f$ равна 1 в точках, где *хотя бы одна* из функций e или f принимает значение 1, и 0 в остальных точках. Характеристические функции с операциями $\circ$, $\cdot$ образуют булеву алгебру из 2^k элементов. Ее атомарными элементами являются функции, принимающие значение 1 ровно в одной точке и 0 в остальных точках.

Понятие многочлена, идемпотентного по модулю (x^n-1) в $K[x]$, тесно связано с понятием характеристической функции.

Сравнение по модулю (x^n-1) означает равенство на спектре:

1°. $f(x) \equiv g(x) \bmod (x^n-1)$ *эквивалентно утверждению* $f(w^l) = g(w^l)$ *для всех* w^l.

Действительно, $h(x) \equiv 0 \bmod (x^n-1)$ эквивалентно утверждению $x^n-1 \mid h(x)$, а оно в свою очередь эквивалентно утверждению $x-w^l \mid h(x)$ для всех w^l, т. е. $h(w^l) = 0$ для всех w^l.

2°. $e^2(x) \equiv e(x) \bmod (x^n-1)$ *эквивалентно утверждению* $e(w^l) \in \{0, 1\}$ *для всех* w^l.

Другими словами, многочлен из $K[x]$ идемпотентен тогда и только тогда, когда он принимает на спектре лишь значения 0 и 1.

Доказательство. Согласно 1°, данное сравнение эквивалентно утверждению $e^2(w^l) = e(w^l)$ для всех w^l, а так как $e(w^l)$ — элементы поля N, то последнее равенство выполняется только тогда, когда $e(w^l) = 0$ или 1.

Если многочлен $f(x) \in K[x]$ равен нулю на одном из корней n-й степени из 1, то он обращается в 0 также на всех сопряженных к нему корнях; если $f(x)$ принимает

значение 1 на некотором корне n-й степени из 1, то он принимает то же значение на всех сопряженных к нему корнях [достаточно применить предыдущее утверждение к $1-f(x)$]. Отсюда и из 2° следует, что

Многочлены из $K[x]$, *идемпотентные по модулю* (x^n-1), *являются характеристическими функциями на спектре многочлена* x^n-1. Несравнимые по модулю (x^n-1) многочлены, согласно 1°, на спектре различаются.

Мы получили новую интерпретацию идемпотентов факторкольца $K[x]/(x^n-1)$, а следовательно, и циклических проекций. Построение циклических проекций сводится к решению интерполяционной задачи в $K[x]$:

Теорема 8. *Пусть* $t(x)$ *— делитель* x^n-1. а) *Если*

$$e(x)=\begin{cases}1 & \text{на корнях многочлена } t(x),\\ 0 & \text{на остальных корнях } n\text{-й степени из } 1,\end{cases}$$

то $\operatorname{Ker} t(\zeta)=\operatorname{Im} e(\zeta)$, *т. е. циклическая проекция* $e(\zeta)$ *отображает множество всех* n*-угольников на циклический класс, определенный многочленом* $t(x)$. b) *Если*

$$e(x)=\begin{cases}0 & \text{на корнях многочлена } t(x),\\ 1 & \text{на остальных корнях } n\text{-й степени из } 1,\end{cases}$$

то $\operatorname{Ker} t(\zeta)=\operatorname{Ker} e(\zeta)$.

Доказательство. а) Условия для $e(x)$ эквивалентны сравнениям (6) и (7). Следовательно, $e(x)=e_t(x)$ и справедливо (15).

[Замечание. Многочлен (10) теоремы 3 решает следующую интерполяционную задачу: *для делителя* $t(x)$ *многочлена* x^n-1 *найти многочлен степени* $<n$, *принимающий на корнях* $t(x)$ *значение* 1, *а на остальных корнях* n*-й степени из единицы значение* 0.]

b) Наложенные на $e(x)$ условия эквивалентны тому, что $1-e(x)$ удовлетворяет сравнениям (6) и (7); поэтому $1-e(x)$ есть многочлен $e_t(x)$. Таким образом, $e(\zeta)=1-e_t(\zeta)$, и наше утверждение вытекает из теоремы 4.

Упражнение. Циклическое отображение $f(\zeta)$ тогда и только тогда обратимо, когда $f(x)$ и x^n-1 в $K[x]$ взаимно просты, т. е. когда в поле разложения x^n-1 ни один из корней n-й степени из 1 не является нулем $f(x)$.

§ 4. Примеры определения циклических классов по делителям многочлена $x^n - 1$

Простой делитель $x-1$ многочлена x^n-1 определяет циклическое отображение $\zeta-1$ и, следовательно, циклический класс

$$\operatorname{Ker}(\zeta-1)=\{\boldsymbol{A}:(\zeta-1)\boldsymbol{A}=\boldsymbol{O}\}=\{\boldsymbol{A}:\zeta\boldsymbol{A}=\boldsymbol{A}\}$$

— класс $\mathcal{A}_{1,n}$ тривиальных n-угольников. Дополнительному к $x-1$ делителю

$$m_1(x):=\frac{1}{n}(1+x+x^2+\ldots+x^{n-1})$$

(нормированному так, чтобы сумма его коэффициентов равнялась 1) соответствует циклическое отображение $m_1(\zeta)=\sigma$, и, следовательно, циклический класс $\operatorname{Ker}\sigma=\overset{\circ}{\mathcal{A}}_n$ — нуль-изобарический класс (как известно, он дополнителен к классу тривиальных n-угольников).

Будем различать два типа делителей $t(x)$ многочлена x^n-1:

I) $x-1 \mid t(x)$, или, что то же самое, $t(1)=0$;
II) $x-1 \nmid t(x)$, что эквивалентно $t(x) \mid m_1(x)$, или $t(1)\neq 0$.
[$t(1)$ есть сумма коэффициентов $t(x)$.]

Всякий делитель типа I) *определяет некоторый свободный циклический класс, а всякий делитель типа* II) *— центральный класс.*

Действительно, по теореме 5 условие $x-1 \mid t(x)$ эквивалентно включению $\mathcal{A}_{1,n}=\operatorname{Ker}(\zeta-1)\subseteq\operatorname{Ker}t(\zeta)$.

Если делитель $t(x)$ типа I) определяет свободный циклический класс $\mathcal{C}$, то $t(x)/(x-1)$ определяет соответствующий центральный класс $\overset{\circ}{\mathcal{C}}$. Действительно, $t(x)/(x-1)$ есть НОД $t(x)$, $m_1(x)$; он определяет $\mathcal{C}\cap\overset{\circ}{\mathcal{A}}_n=\overset{\circ}{\mathcal{C}}$.

Всякий делитель $t(x)$ типа II) можно, умножив его на $1/t(1)$, нормировать так, чтобы его сумма коэффициентов была $=1$ [1]); тогда соответствующая получаемая

[1]) Идемпотентный по модулю (x^n-1) делитель типа II) должен быть нормирован так: поскольку его значение в точке 1 спектра $\neq 0$, следует потребовать, чтобы оно было $=1$.

подстановкой $x \to \zeta$ циклическая проекция будет *изобарической*. Делитель $t(x)$ типа II) можно нормировать так, чтобы равнялась 1 сумма коэффициентов многочлена $t(x)/(x-1)$.

Пусть $d \mid n$ и $n = d\bar{d}$. Многочлен x^d-1 является делителем x^n-1 типа I). Ему соответствует циклическое отображение ζ^d-1, и циклический класс

$$\operatorname{Ker}(\zeta^d-1) = \{\boldsymbol{A} : (\zeta^d-1)\,\boldsymbol{A} = \boldsymbol{O}\} = \{\boldsymbol{A} : \zeta^d \boldsymbol{A} = \boldsymbol{A}\}$$

— это класс $\mathcal{A}_{d,\bar{d}}$ $\bar{d}$ раз пройденных d-угольников.

Делителю типа II)

$$k_d(x) := \frac{1}{d}(1 + x + \ldots + x^{d-1}) = \frac{1}{d}\frac{x^d-1}{x-1}$$

соответствует центральный класс $\overset{\circ}{\mathcal{A}}_{d,\bar{d}}$.

Делитель типа II)

$$m_d(x) := \frac{d}{n}(1 + x^d + \ldots + x^{n-d}) = \frac{d}{n}\frac{x^n-1}{x^d-1}$$

дополнителен к x^d-1. Он определяет дополнительный к $\mathcal{A}_{d,\bar{d}}$ класс $\overset{\circ}{\mathcal{A}}{}^d_n$ — класс d-кратно изобарически распадающихся n-угольников с центром тяжести $\boldsymbol{o}$ (см. теорему 3 гл. 4).

Многочлен $m_d(x)$ идемпотентен по модулю (x^n-1), так как он принимает значение 1 *на корнях* d-*й степени из* 1 *и значение* 0 *в остальных точках спектра.* Действительно, если w^l — корень d-й степени из 1, то $w^{ld}=1$ и

$$m_d(w^l) = \frac{d}{n}(1 + w^{ld} + w^{2ld} + \ldots + w^{l(n-d)}) = 1,$$

а если w^l не является корнем d-й степени из 1, т. е. $w^{ld} \neq 1$, то

$$m_d(w^l) = \frac{d}{n}\frac{1-1}{w^{ld}-1} = 0.$$

Отображения $m_d(\zeta)$ и $k_d(\zeta)$ суть не что иное, как *хордовое* и *последовательное* d-усреднения. Их ядра известны из теорем 1 и 4 гл. 4 и первого правила § 2 гл. 3.

Частичные произведения выражения $(x-1)\,k_d(x)\,m_d(x)$ являются нормированными представителями элементов булевой подалгебры алгебры делителей многочлена x^n-1. Если $d \neq 1, n$, то 8 формально различных частичных произведений действительно различны. Частичные произведения, состоящие из $k_d(x)$ и $m_d(x)$, определяют центральные классы $\{\boldsymbol{O}\}$, $\mathcal{A}_{d,\bar{d}}$, $\overset{\circ}{\mathcal{A}}{}^{d}_{n}$, $\overset{\circ}{\mathcal{A}}_{n}$, а эти же многочлены, умноженные на $(x-1)$,— соответствующие свободные циклические классы.

Делители многочлена x^d-1 определяют циклические классы n-угольников, содержащиеся в классе $\bar{d}$ раз пройденных d-угольников. [Действительно, условие $t(x) \mid x^d-1$ эквивалентно включению $\operatorname{Ker} t(\zeta) \subseteq \operatorname{Ker}(\zeta^d-1) = \mathcal{A}_{d,\bar{d}}$.] В булевой алгебре циклических классов n-угольников они образуют подструктуру, которая изоморфна булевой алгебре d-угольников; n-угольники этих классов получаются $\bar{d}$-кратным прохождением d-угольников соответствующих классов.

Введем следующие обозначения: если $\mathcal{C}_d$ — некоторый циклический класс d-угольников, то через $\mathcal{C}_{d,\bar{d}}$ будем обозначать класс $\bar{d}$ раз пройденных d-угольников из $\mathcal{C}_d$:

$$(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_d, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_d, \ldots, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_d), \quad \text{где } (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_d) \in \mathcal{C}_d. \tag{17}$$

$\mathcal{C}_{d,\bar{d}}$ является циклическим классом n-угольников.

Лемма. *Пусть $d \mid n$, $t(x) \mid x^d-1$ и $\mathcal{C}_d$ — циклический класс d-угольников, определенный многочленом $t(x)$. Тогда $\mathcal{C}_{d,\bar{d}}$ есть циклический класс n-угольников, определенный этим же многочленом.*

Доказательство. *Класс d-угольников, определенный многочленом x^d-1, есть $\mathcal{A}_d$ — множество всех d-угольников; класс n-угольников, определенный этим же многочленом, есть $\mathcal{A}_{d,\bar{d}}$.*

Пусть теперь $t(x) = \sum_{i=0}^{d-1} c_i x^i$ — собственный делитель x^d-1. Тогда $\mathcal{C}_d$ является пространством решений циклической системы

$$c_0\boldsymbol{a}_1 + \ldots + c_{d-1}\boldsymbol{a}_d = \boldsymbol{o},\ c_0\boldsymbol{a}_2 + \ldots + c_{d-1}\boldsymbol{a}_1 = \boldsymbol{o},\ \ldots \quad (d \text{ уравнений}). \tag{18}$$

Так как $t(x) \mid x^d-1 \mid x^n-1$, то циклический класс $\mathscr{C}_n$, определенный многочленом $t(x)$, содержится в $\mathscr{A}_{d,\bar{a}}$: $\mathscr{C}_n \subseteq \subseteq \mathscr{A}_{d,\bar{a}}$. С другой стороны, он является пространством решений системы

$$c_0\boldsymbol{a}_1+\ldots+c_{d-1}\boldsymbol{a}_d=\boldsymbol{o},\ c_0\boldsymbol{a}_2+\ldots+c_{d-1}\boldsymbol{a}_{d+1}=\boldsymbol{o},\ \ldots \quad (n \text{ уравнений}). \tag{19}$$

Если $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_d)$ удовлетворяет системе (18), то $(\boldsymbol{a}_1 \ldots, \boldsymbol{a}_d, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_d, \ldots, \boldsymbol{a}_1, \ldots, \boldsymbol{a}_d)$ удовлетворяет системе (19); поэтому $\mathscr{C}_{d,\bar{a}} \subseteq \mathscr{C}_n$. Обратно, пусть $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n) \subseteq \mathscr{C}_n$. Поскольку $\mathscr{C}_n \subseteq \mathscr{A}_{d,\bar{a}}$, имеем $\boldsymbol{a}_{d+1}=\boldsymbol{a}_1, \ldots$; следовательно, система (19) совпадает с (18), т. е. $\mathscr{C}_n \subseteq \mathscr{C}_{d,\bar{a}}$.

Теорема 9. *Из атомарных циклических классов n-угольников не являются подклассами периодических классов лишь те, которые определены делителями многочлена $F_n(x)$. Остальные атомарные циклические классы n-угольников получаются из атомарных циклических классов d-угольников $(d \parallel n)$ с помощью $\frac{n}{d}$-кратного прохождения этих d-угольников.*

Здесь $d \parallel n$ обозначает, что d — собственный делитель n, т. е. $d \mid n$ и $d \neq n$.

Доказательство. Атомарные циклические классы определяются посредством простых делителей x^n-1, следовательно, простых делителей многочленов деления круга $F_d(x)$ при $d \mid n$. Различные многочлены деления круга имеют различные простые делители. Если циклический класс $\mathscr{C}$ определен простым делителем $p(x)$ многочлена $F_d(x)$ при $d \parallel n$, то, согласно лемме, $\mathscr{C}_n=\mathscr{C}_{d,\bar{a}}$, поскольку $F_d(x) \mid x^d-1$. Таким образом, при $d \parallel n$ класс $\mathscr{C}_n$ содержится в периодическом классе $\mathscr{A}_{d,\bar{a}}$. Простые делители многочлена $F_n(x)$ не делят x^d-1 при $d \parallel n$ Поэтому определяемые ими классы не содержатся в собственно периодических классах.

Если $K=\mathbf{Q}$, то для каждого n имеется точно один «типичный» атомарный класс n-угольников, а именно тот, который определяется многочленом $F_n(x)$. Все остальные атомарные циклические классы n-угольников получаются из «типичных» атомарных классов d-угольников $(d \mid n)$ их

многократным прохождением. «Типичный» атомарный класс 6-угольников состоит из аффинно-правильных 6-угольников с центром тяжести O. Для произвольного n «типичные» атомарные классы описаны в гл. 10.

Упражнения

1. Делитель $t(x)$ многочлена x^n-1 тогда и только тогда идемпотентен по модулю (x^n-1), когда дополнительный делитель делит многочлен $1-t(x)$ Многочлен

$$1-m_d(x)=\frac{d}{n}((1-x^d)+(1-x^{2d})+\ldots+(1-x^{n-d})), \text{ где } d \mid n,$$

делится на x^d-1; поэтому $m_d(x)$ идемпотентен по модулю (x^n-1).

2. Пусть $d \mid n$ и $m'_d(x)$ — производная $m_d(x)$. Тогда

$$1-m_d(x) \equiv \frac{1}{d}(x^d-1)\,xm'_d(x) \bmod (x^n-1)$$

(см. (6), гл. 4).

3. Пусть $n=d\bar{d}$. Если $e(x)$ — многочлен из $K[x]$, идемпотентный по модулю $(x^{\bar{d}}-1)$, то $e(x^d)$ идемпотентен по модулю (x^n-1). Пользуясь этим, докажите, что $m_d(x)$ идемпотентен по модулю (x^n-1).

4. Если $n=d\bar{d}$ и w — корень $\bar{d}$-й степени из 1 в K, то многочлен

$$\frac{d}{n}w\frac{x^n-1}{x^d-w}=\frac{d}{n}(1+w^{-1}x^d+(w^{-1}x^d)^2+\ldots+(w^{-1}x^d)^{\bar{d}-1})$$

является идемпотентным по модулю (x^n-1) собственным делителем x^n-1 из $K[x]$. Могут ли быть в $K[x]$ другие многочлены с этим свойством?

ГЛАВА 9

БУЛЕВЫ АЛГЕБРЫ n-УГОЛЬНИКОВ (ТЕОРИЯ II)

§ 1. Соответствие Галуа между аннуляторами и ядрами

Прежде всего напомним известные факты.

Лемма. *Пусть* M, N — *множества*; φ — *отображение* M *в* N, *а* ψ — *отображение* N *в* M, *такие, что*

1) $\psi\varphi x = x$ *для всех* $x \in M$, 2) $\varphi\psi y = y$ *для всех* $y \in N$.

Тогда φ *есть взаимно однозначное отображение* M *на* N *и* ψ *обратно к* φ.

Действительно, φ взаимно однозначно: если $\varphi x_1 = \varphi x_2$, то $\psi\varphi x_1 = \psi\varphi x_2$ и, согласно 1), $x_1 = x_2$. Кроме того, φ является отображением *на*: в силу 2) любой элемент $y \in N$ является φ-образом элемента $\psi y \in M$.

Пусть, как и раньше, R — кольцо с единицей, $\mathcal{A}$ — некоторый R-модуль (см. § 1 гл. 7). Говорят, что $r \in R$ *аннулирует* $a \in \mathcal{A}$, если

$$ra = o.$$

Аннулятором подмножества из $\mathcal{A}$ называется множество элементов кольца R, аннулирующих любой элемент этого подмножества.

Если $\mathcal{B}$ — некоторый r-подмодуль $\mathcal{A}$, то его аннулятор

$$\operatorname{an}\mathcal{B} = \{r : r\mathcal{B} = \{o\}\}$$

является идеалом в R. Обратно, пусть S — идеал в R. *Ядром* этого идеала называется множество элементов из $\mathcal{A}$, аннулирующихся всеми элементами из S:

$$\ker S = \{a : Sa = \{o\}\};$$

оно является R-подмодулем в $\mathcal{A}$.

Если S, T суть идеалы из R, а $\mathcal{B}$, $\mathcal{C}$ суть R-подмодули $\mathcal{A}$, то

$$\text{из } S \subseteq T \text{ следует } \ker S \supseteq \ker T, \tag{1}$$

$$\text{из } \mathcal{B} \subseteq \mathcal{C} \text{ следует } \operatorname{an}\mathcal{B} \supseteq \operatorname{an}\mathcal{C}, \tag{2}$$

$$\operatorname{an}\ker S \supseteq S, \tag{3}$$

$$\ker \operatorname{an} \mathcal{B} \supseteq \mathcal{B}, \tag{4}$$

$$\operatorname{an}\ker \operatorname{an} \mathcal{B} = \operatorname{an} \mathcal{B}, \tag{5}$$

$$\ker \operatorname{an}\ker S = \ker S. \tag{6}$$

Утверждения (1)—(4) очевидны. Докажем (5): здесь включение $\supseteq$ получается, если в (3) положить $S = \operatorname{an} \mathcal{B}$, обратное включение следует из (4) и (2). Утверждение (6) доказывается аналогично.

Множество идеалов кольца R, которые являются аннуляторами R-подмодулей $\mathcal{A}$, обозначим $L^{\operatorname{an}}(R)$:

$$L^{\operatorname{an}}(R) = \{\operatorname{an} \mathcal{B} : \mathcal{B} \text{ есть } R\text{-подмодуль } \mathcal{A}\},$$

а множество R-подмодулей $\mathcal{A}$, являющихся ядрами идеалов кольца R, обозначим $L^{\ker}(\mathcal{A})$:

$$L^{\ker}(\mathcal{A}) = \{\ker S : S \text{— идеал в } R\}.$$

Для всякого идеала $S \subset R$ идеал $\operatorname{an}\ker S$ есть минимальный охватывающий S аннулятор. [Действительно, $\operatorname{an}\ker S$ является аннулятором; в силу (3) он содержит S; если $S \subseteq T$ и T — некоторый аннулятор, то в силу (1), (2), (5) $\operatorname{an}\ker S \subseteq \operatorname{an}\ker T = T$.] Если M — множество идеалов в R и $\langle M\rangle$ — идеал, порожденный их объединением, то $\operatorname{an}\ker\langle M\rangle$ — минимальный аннулятор, охватывающий все идеалы из M.

Для всякого R-подмодуля $\mathcal{B} \subseteq \mathcal{A}$ множество $\ker \operatorname{an} \mathcal{B}$ есть минимальное охватывающее $\mathcal{B}$ ядро. Если $\mathcal{M}$ — множество R-подмодулей из $\mathcal{A}$ и $\langle \mathcal{M}\rangle$ — подмодуль, порожденный их объединением, то $\ker \operatorname{an}\langle \mathcal{M}\rangle$ — минимальное ядро, охватывающее все R-подмодули из $\mathcal{M}$.

Пересечение аннуляторов является аннулятором, пересечение ядер — ядром:

$$\bigcap_{\mathcal{B} \in \mathcal{M}} \operatorname{an} \mathcal{B} = \operatorname{an}\langle \mathcal{M}\rangle, \tag{7}$$

$$\bigcap_{S \in M} \ker S = \ker\langle M\rangle. \tag{8}$$

Доказательство (8). Вместо $\bigcap\limits_{S \in M}$ будем писать просто $\bigcap$. Включение $\supseteq$: из $S \subseteq \langle M\rangle$ и (1) следует, что

$\ker S \supseteq \ker \langle M \rangle$. Отсюда $\bigcap \ker S \supseteq \ker \langle M \rangle$. Обратное включение $\subseteq$: для любого $S \in M$ имеем $\bigcap \ker S \subseteq \ker S$. В силу (2) и (3) $\operatorname{an}(\bigcap \ker S) \supseteq \operatorname{an} \ker S \supseteq S \supseteq \langle M \rangle$. Применим (1) к крайним членам этой цепочки: $\ker \operatorname{an}(\bigcap \ker S) \subseteq \subseteq \ker \langle M \rangle$. В силу (4) $\bigcap \ker S \subseteq \ker \operatorname{an}(\bigcap \ker S) \subseteq \ker \langle M \rangle$. Утверждение доказано.

Из формул (7) и (8) следует, что $L^{\operatorname{an}}(R)$ и $L^{\ker}(\mathcal{A})$ являются полными структурами с включением в качестве отношения частичной упорядоченности и со следующими операциями «минимум» соответственно: $\inf M = \bigcap\limits_{S \in M} S$ для всякого подмножества M из $L^{\operatorname{an}}(R)$ и $\inf \mathscr{M} = \bigcap\limits_{\mathscr{B} \in \mathscr{M}} \mathscr{B}$ для всякого подмножества $\mathscr{M}$ из $L^{\ker}(\mathcal{A})$. Операции «максимум» определяются отсюда следующим образом: $\sup M = \operatorname{an} \ker \langle M \rangle$ для $L^{\operatorname{an}}(R)$ и $\sup \mathscr{M} = \ker \operatorname{an} \langle \mathscr{M} \rangle$ для $L^{\ker}(\mathcal{A})$.

Теорема 1. *Пусть R — кольцо с 1 и $\mathcal{A}$ — некоторый R-модуль. Ограничения операций* ker *и* an *соответственно на множества $L^{\operatorname{an}}(R)$ и $L^{\ker}(\mathcal{A})$ являются парой взаимно обратных антиизоморфизмов структур $L^{\operatorname{an}}(R)$ и $L^{\ker}(\mathcal{A})$.*

Доказательство. Из (5) и (6), согласно лемме, следует, что ограничения ker и an являются взаимно однозначными и взаимно обратными отображениями *на*. Из (1) и (2) следует, что они являются антиизоморфизмами [1]).

§ 2. Идеал-вложение

Потребуем теперь, чтобы R было кольцом главных идеалов; $\mathcal{A}$ — по-прежнему R-модуль. Справедливы следующие три утверждения:

1°. $\ker(r) \cap \ker(s) = \ker[(r) + (s)]$,

2°. $\ker(r) + \ker(s) = \ker[(r) \cap (s)]$,

3°. *Из* $(0) \neq r \subseteq (s)$ *и* $(r) \in L^{\operatorname{an}}(R)$ *следует, что* $(s) \in L^{\operatorname{an}}(R)$.

---

[1]) По поводу общего соответствия Галуа, индуцированного некоторым отношением между двумя множествами, см., например, [2].

Они означают, что *пересечение и сумма двух ядер — снова ядро и что всякий идеал, содержащий отличный от нуля аннулятор, сам является аннулятором.*

Доказательство. 1° следует из (8). Докажем 2°. Включение $\subseteq$ очевидно. Пусть

$$(r)+(s)=(t). \tag{9}$$

Если $t=0$, то утверждение тривиально. Если $t\neq 0$, то существуют элементы r_1, s_1, u и v, такие, что $r=r_1t$, $s=s_1t$ и $t=ur+vs$. [Действительно, t есть общий делитель r и s, и потому представим в виде их линейной комбинации.] Итак, $t=ur_1t+vs_1t$, откуда, поскольку $t\neq 0$, имеем $1=ur_1+vs_1$. Кроме того, $rs_1=r_1ts_1=r_1s\in(r)\cap(s)$.

Пусть теперь $\boldsymbol{a}\in\ker[(r)\cap(s)]$. Тогда $rs_1\boldsymbol{a}=r_1s\boldsymbol{a}=\boldsymbol{o}$; следовательно, $s_1\boldsymbol{a}\in\ker(r)$, $r_1\boldsymbol{a}\in\ker(s)$. С другой стороны,

$$\boldsymbol{a}=1\cdot\boldsymbol{a}=(ur_1+vs_1)\,\boldsymbol{a}=ur_1\boldsymbol{a}+vs_1\boldsymbol{a}\in\ker(s)+\ker(r).$$

Включение $\supseteq$ доказано.

Докажем 3°. Это утверждение эквивалентно следующему: из $(0)\neq(r)\subseteq(s)$ и $\operatorname{an}\ker(r)=(r)$ следует, что $\operatorname{an}\ker(s)=(s)$. Положим $\operatorname{an}\ker(s)=(t)$. В силу (3) $(s)\subseteq(t)$, а в силу (6) $\ker(s)=\ker\operatorname{an}\ker(s)=\ker(t)$. Так как $(r)\subseteq(s)$, то существует такой r_1, что

$$r=r_1s. \tag{10}$$

Для всякого $\boldsymbol{a}\in\ker(r)$ имеем $r_1s\boldsymbol{a}=\boldsymbol{o}$; следовательно, $r_1\boldsymbol{a}\in\ker(s)=\ker(t)$, поэтому $tr_1\boldsymbol{a}=\boldsymbol{o}$. Итак, tr_1 аннулирует $\ker(r)$: $tr_1\in\operatorname{an}\ker(r)=(r)$. Существует такой u, что $tr_1=ur=ur_1s$. Так как $r\neq 0$, то из (10) следует, что $r_1\neq 0$, следовательно, $t=us$, т. е. $(t)\subseteq(s)$. Из двух взаимно обратных включений вытекает, что $(t)=(s)$, и $\operatorname{an}\ker(s)=(s)$.

Следствием теоремы 1 и утверждений 1°—3° является

Теорема 2 (идеал-вложение). *Если R — кольцо главных идеалов и $\mathcal{A}$ — некоторый R-модуль, то $L^{\mathrm{an}}(R)$ и $L^{\ker}(\mathcal{A})$ являются подструктурами соответственно структуры идеалов кольца R и структуры подмодулей модуля $\mathcal{A}$; отображение* ker *является антиизоморфизмом $L^{\mathrm{an}}(R)$ на $L^{\ker}(\mathcal{A})$.*

Если $\operatorname{an}\mathcal{A} \neq (0)$, *то* $L^{\operatorname{an}}(R)$ *есть конечный интервал* $[\operatorname{an}\mathcal{A}, R]$ *структуры идеалов из* R.

Таким образом, если $\operatorname{an}\mathcal{A} \neq (0)$ и $\operatorname{an}\mathcal{A} = (m)$, то структура $L^{\operatorname{an}}(R)$ изоморфна интервалу $[(m), R]$, который в свою очередь антиизоморфен структуре делителей элемента m (см. § 4 гл. 7). Следовательно, существует изоморфизм структуры $L(m)$ — делителей элемента m на структуру $L^{\ker}(\mathcal{A})$: $t \longrightarrow (t) \longrightarrow \ker(t)$.

В частности, если идеал $\operatorname{an}\mathcal{A} = (m)$ свободен от квадратов и k — число простых делителей элемента m, то $L(m)$, $[(m), R]$, $L^{\ker}(\mathcal{A})$ — конечные булевы алгебры из 2^k элементов.

§ 3. Второе доказательство основной теоремы. Основная диаграмма

Вернемся к теории n-угольников. Пусть выполнены все условия § 1 гл. 1. Если $f(\zeta)$ — циклическое отображение, то через

$$f(\zeta)\boldsymbol{A} \tag{11}$$

обозначается образ n-угольника $\boldsymbol{A}$ при отображении $f(\zeta)$. Легко проверить, что относительно этого «умножения» на $f(\zeta)$ пространство всех n-угольников $\mathcal{A}_n = V^n$ является $K[\zeta]$-модулем.

Однако при $n \neq 1$ кольцо $K[\zeta]$ не является кольцом главных идеалов. Чтобы иметь возможность применить теорему об идеал-вложении, придется перейти к кольцу главных идеалов $K[x]$. Для этого определим умножение многочлена $f(x) \in K[x]$ и n-угольника $\boldsymbol{A} \in \mathcal{A}_n$ формулой

$$f(x) \cdot \boldsymbol{A} = f(\zeta)\boldsymbol{A}. \tag{12}$$

Теперь $\mathcal{A}_n$ является $K[x]$-модулем и

$$\operatorname{an}\mathcal{A}_n = (x^n - 1) \neq (0). \tag{13}$$

По теореме 3 гл. 6 идеал $x^n - 1$ свободен от квадратов. Поэтому структура

L_2: интервал $[(x^n - 1), K[x]]$ структуры идеалов кольца $K[x]$

является конечной булевой алгеброй. По теореме 2 отображение ker является антиизоморфизмом L_2 на структуру $L^{\ker}(\mathcal{A}_n)$. Значит, и эта структура является конечной булевой алгеброй в структуре подпространств векторного пространства $\mathcal{A}_n$.

Для произвольного идеала $(f(x)) = K[x] \cdot f(x)$ имеем

$$\ker(f(x)) = \operatorname{Ker} f(\zeta). \tag{14}$$

Действительно,

$$\ker(f(x)) = \{\boldsymbol{A} : K[x] \cdot f(x) \cdot \boldsymbol{A} = \{\boldsymbol{O}\}\} = \{\boldsymbol{A} : f(x) \cdot \boldsymbol{A} = \boldsymbol{O}\} = \\ = \{\boldsymbol{A} : f(\zeta) \cdot \boldsymbol{A} = \boldsymbol{O}\} = \operatorname{Ker} f(\zeta).$$

Но по теореме 1 гл. 2 ядра циклических отображений являются циклическими классами, и равенство (14) доказывает справедливость следующего утверждения:

Структура $L^{\ker}(\mathcal{A}_n)$ состоит из циклических классов n-угольников.

Итак, снова получена

Основная теорема. *Циклические классы n-угольников образуют конечную булеву алгебру; она является подструктурой структуры подпространств векторного пространства $\mathcal{A}_n$* (ср. § 2 гл. 6.)

Первое доказательство основной теоремы опиралось на идемпотенты, конструкцию китайской теоремы об остатках и идемпотент-вложение (в специальной форме Im-вложения). Второе доказательство обходится без этих вспомогательных средств и основывается только на понятии R-модуля и идеал-вложении.

Замечание. При этом получено, очевидно, и новое не использующее циклических проекций доказательство теоремы 5 гл. 8 о связи между делителями $t(x)$ многочлена $x^n - 1$ и циклическими классами. Действительно, в конце § 2 мы установили изоморфизм $t(x) \to (t(x)) \to \\ \to \ker(t(x))$ структуры делителей $x^n - 1$ на булеву алгебру $L^{\ker}(\mathcal{A}_n)$, которая, как показывает (14), состоит из циклических классов n-угольников: $\ker(t(x)) = \operatorname{Ker} t(\zeta)$.

$\mathcal{A}_n$ является также $K[\zeta]$-модулем. Из определения (12) следует, что $\ker(f(x)) = \ker(f(\zeta))$, а в силу (14)

$$\ker(f(x)) = \operatorname{Ker} f(\zeta) = \ker(f(\zeta)). \tag{15}$$

Следовательно, отображение ker является также антиизоморфизмом структуры идеалов кольца $K[\zeta]$ на булеву алгебру циклических классов (ср. доказательство теоремы 5 гл. 8).

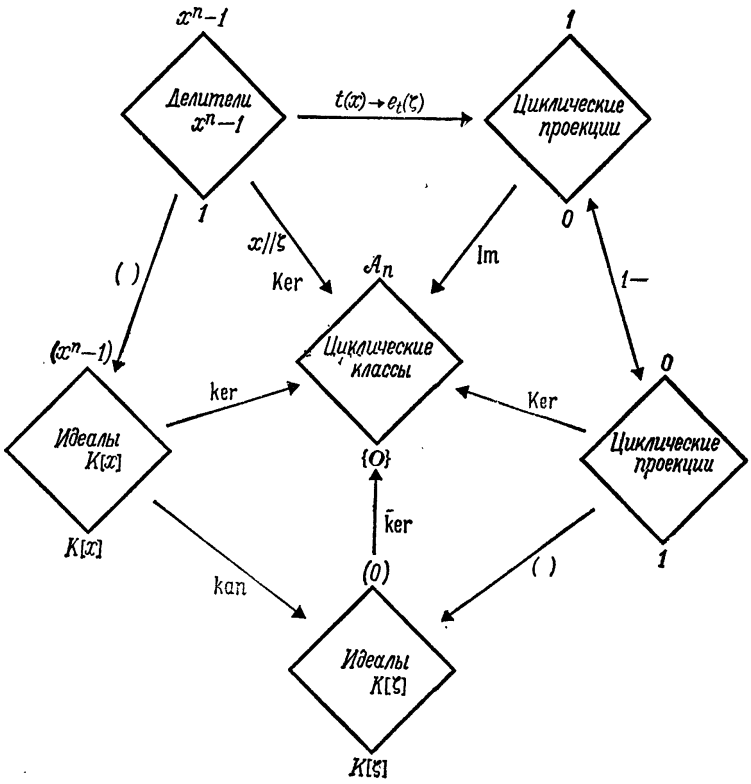


Рис. 61. Основная диаграмма.
[$x//\zeta$ обозначает подстановку $x \to \zeta$.]

Таким образом, цель, поставленная нами в гл. 8, достигнута, и мы можем сформулировать заключительную теорему об изоморфизме между рассматриваемыми булевыми алгебрами (см. также изображенную на рис. 61 основную диаграмму, где просуммированы полученные результаты). Отображение $t(x) \longrightarrow \operatorname{Ker} t(\zeta)$ (теорема 5 гл. 8),

являющееся результатом последовательного выполнения отображений $x \longrightarrow \zeta$ и Ker, обозначим $\mathrm{Ker}\cdot(x) \longrightarrow \zeta$.

Теорема 3. *Отображения* $\mathrm{Ker}\cdot(x) \longrightarrow \zeta$, ker, ker, Ker, Im *являются изоморфизмами булевых алгебр*

$$L_1,\ L_2',\ L_3',\ L_4',\ L_5 \qquad (*)$$

на булеву алгебру циклических классов n-угольников L_6. Элементам булевых алгебр (*), *соответствующим друг другу при изоморфизмах теоремы* 2 *гл.* 8, *они ставят в соответствие один и тот же циклический класс.*

Доказательство. Запишем набор из пяти соответствующих друг другу элементов булевых алгебр (*). Если $t(x) \mid x^n - 1$ и $\dot{K}$ — мультипликативная группа поля K, то

$$\dot{K}\cdot t(x),\quad (t(x)),\quad (t(\zeta)) = (e_t'(\zeta)),\quad e_t'(\zeta),\quad e_t(\zeta),$$

где $e_t'(\zeta) = 1 - e_t(\zeta)$, и есть искомый набор. Этим элементам соответствуют циклические классы

$$\mathrm{Ker}\, t(\zeta) = \ker(t(x)) = \ker(t(\zeta)) =$$
$$= \ker(e_t'(\zeta)) = \mathrm{Ker}\, e_t'(\zeta) = \mathrm{Im}\, e_t(\zeta).$$

Первое, второе и четвертое равенства справедливы в силу (15), пятое — в силу равенств (7) гл. 2.

Упражнения

1. Если φ — эндоморфизм векторного пространства над K и $m(x)$ — минимальный многочлен для φ, то $K[\varphi] \cong K[x]/(m(x))$.

2. Пусть Char $K \neq 2$. Тогда $K[\zeta] = K[\varkappa_2]$: всякое циклическое отображение может быть записано как линейная комбинация степеней отображения $\varkappa_2$. Приведите пример. Каков минимальный многочлен для $\varkappa_2$?

§ 4. Градуировка. Степень свободы циклического класса

Такие понятия, как степень, размерность, ранг, позволяют поставить в соответствие каждому элементу булевых алгебр L_1, L_3, $L_4 = L_5$, L_6 некоторое число из множества $\{0, 1, \ldots, n\}$. А именно:

(L_1) Делителю x^n-1, а также классу ассоциированных делителей сопоставим *степень* многочлена

$$t(x) \longrightarrow \operatorname{Grad} t(x).$$

(L_3) Идеалу из $K[\zeta]$ сопоставим *размерность* идеала

$$(f(\zeta)) \longrightarrow \dim (f(\zeta)).$$

[Алгебра $K[\zeta]$ по теореме 4 гл. 2 является n-мерным векторным пространством над K; всякий идеал как подпространство $K[\zeta]$ имеет свою размерность.]

(L_5) Циклической проекции сопоставим ее ранг

$$e(\zeta) \longrightarrow \operatorname{Rang} e(\zeta)$$

[под *рангом циклического отображения* $f(\zeta)=\sum c_i\zeta^i$ понимается ранг циклической матрицы $M(c_0, c_1, \ldots, c_{n-1})$].

(L_6) Циклическому классу сопоставим его *степень свободы*

$$\mathscr{C} \longrightarrow \operatorname{Grad} \mathscr{C} \qquad \text{(см. § 6 гл. 1).}$$

При этом справедливы соотношения

$$\operatorname{Rang} f(\zeta) = \dim (f(\zeta)), \tag{16}$$

$$n - \operatorname{Grad} t = \dim (t(\zeta)) \text{ для } t(x) \mid x^n-1. \tag{17}$$

Несколько отложив доказательство этих равенств, выведем из них важные следствия.

Если $t(x)$ — делитель x^n-1 и $(f(\zeta))=(t(\zeta))$, то

$$\operatorname{Grad}\operatorname{Ker} f(\zeta) = n - \operatorname{Rang} f(\zeta) = n - \dim (f(\zeta)) = \operatorname{Grad} t. \tag{18}$$

Первое равенство выполняется в силу теоремы 2 гл. 1, второе и третье следуют из (16), (17).

Снова заменим структуру идеалов из $K[\zeta]$ двойственной ей структурой L_3' и поставим в соответствие идеалам их коразмерность:

$$(L_3') \qquad (f(\zeta)) \longrightarrow \operatorname{codim} (f(\zeta)) = n - \dim (f(\zeta)).$$

Тогда происходит одновременная *градуировка* алгебр L_1, L_3', L_5, L_6.

Теорема 4. *Элементам булевых алгебр* L_1, L_3', L_5, L_6, *переводимым друг в друга изоморфизмами теоремы* 2 *гл.* 8, *соответствует одно и то же число.*

Доказательство. Четыре переходящих друг в друга элемента из L_1, L_3', L_5, L_6 можно записать так:

$$K \cdot t\,[x],\ (t\,(\zeta)),\ e_t\,(\zeta),\ \operatorname{Ker} t\,(\zeta),\ \text{где } t\,(x) \mid x^n - 1$$

(см. теоремы 2 и 5 гл. 8). Им соответствуют числа

$$\operatorname{Grad} t,\ n - \dim\,(t\,(\zeta)),\ \operatorname{Rang} e_t\,(\zeta),\ \operatorname{Grad} \operatorname{Ker} t\,(\zeta).$$

Первое, второе и четвертое числа одинаковы в силу (18). Далее, $(e_t\,(\zeta)) = (\overline{t}\,(\zeta))$ (см. равенство (8) гл. 8 и конец § 1 той же главы), а из (16) и (17) следует, что

$$\operatorname{Rang} e_t\,(\zeta) = \dim\,(e_t\,(\zeta)) = \dim\,(\overline{t}\,(\zeta)) = n - \operatorname{Grad} \overline{t} = \operatorname{Grad} t.$$

Теорема доказана.

Следствием из теоремы 4 является

Теорема 5. *Степень свободы циклического класса, определенного делителем* $t\,(x)$ *многочлена* $x^n - 1$, *равна степени многочлена* $t\,(x)$; *степень свободы циклического класса, определенного циклической системой с коэффициентами* $c_0, c_1, \ldots, c_{n-1}$, *равна степени* НОД (*в* $K\,[x]$) *многочленов* $\sum c_i x^i$ *и* $x^n - 1$.

Так как сумма степеней простых делителей многочлена $x^n - 1$ равна n, то сумма степеней свободы атомарных циклических классов n-угольников всегда равна n. Этот факт следует также из того, что справедлива

Теорема 6. *Для любых циклических классов* $\mathcal{B}$ *и* $\mathcal{C}$

$$\operatorname{Grad}\,(\mathcal{B} + \mathcal{C}) + \operatorname{Grad}\,(\mathcal{B} \cap \mathcal{C}) = \operatorname{Grad} \mathcal{B} + \operatorname{Grad} \mathcal{C}.$$

Действительно, аналогичная формула справедлива для размерностей любых двух подпространств векторного пространства; нам достаточно лишь применить ее к пространству $K\,[\zeta]$ [идеалы $(f\,(\zeta))$ являются в нем подпространствами] и воспользоваться тем, что $\operatorname{Grad} \operatorname{Ker} f\,(\zeta) = n - \dim\,(f\,(\zeta))$.

Предоставляем читателю обобщить на булевы алгебры циклических классов n-угольников утверждение о разностях степеней свободы соседних классов в диаграмме циклических классов 6-угольников (см. § 8 гл. 1).

Перейдем, наконец, к доказательству равенств (16) и (17). Рассмотрим изоморфное кольцу $K[\zeta]$ факторкольцо $K[x]/(x^n-1)$. Его элементы — смежные классы $f(x)+(x^n-1)$, где $f(x)\in K[x]$, мы условимся обозначать $[f(x)]$; классы $[c]$, где $c\in K$, образуют изоморфное K подкольцо кольца $K[x]/(x^n-1)$. Если положить по определению

$$c[f(x)]:=[cf(x)],\quad c\in K,$$

то $K[x]/(x^n-1)$ превратится в алгебру над K, каждый элемент которой имеет вид $[f(x)]$, где $f(x)=c_0+c_1x+\ldots+c_{n-1}x^{n-1}$, $c_i\in K$. Как векторное пространство над K эта алгебра имеет размерность n; ее базис образуют элементы

$$[1],\ [x],\ \ldots,\ [x^{n-1}]. \tag{19}$$

Всякий идеал в $K[x]/(x^n-1)$ является главным идеалом $([f(x)])$ (см. теорему 3 гл. 7), его размерность как подпространства векторного пространства мы обозначим через $\dim([f(x)])$.

Докажем следующие формулы:

$$\operatorname{Rang} M(c_0,\ c_1,\ \ldots,\ c_{n-1})=\dim([\textstyle\sum c_ix^i]), \tag{16'}$$

$$n-\operatorname{Grad} t=\dim([t(x)])\ \text{для}\ t(x)\mid x^n-1. \tag{17'}$$

В силу изоморфизма $[f(x)]\longrightarrow f(\zeta)$ они совпадают с формулами (16) и (17).

Доказательство (16'). Положим $c_0+c_1x+\ldots+c_{n-1}x^{n-1}=f(x)$. Смежные классы

$$[f(x)],\ [xf(x)],\ \ldots,\ [x^{n-1}f(x)] \tag{20}$$

образуют систему, порождающую подпространство $([f(x)])$. Согласно равенствам

$$[f(x)]=c_0[1]+c_1[x]+\ldots+c_{n-1}[x^{n-1}],$$

$$[xf(x)] = c_{n-1}[1] + c_0[x] + \ldots + c_{n-2}[x^{n-1}],$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$[x^{n-1}f(x)] = c_1[1] + c_2[x] + \ldots + c_0[x^{n-1}],$$

максимальное число линейно независимых классов системы (20) равно рангу матрицы $M(c_0, c_1, \ldots, c_{n-1})$, что и требовалось доказать.

Доказательство (17′). Для $t(x) = x^n - 1$ утверждение справедливо. Пусть теперь $\operatorname{Grad} t = m < n$. Смежные классы

$$[t(x)], \quad [xt(x)], \quad \ldots, \quad [x^{n-m-1}t(x)] \tag{21}$$

линейно независимы. Действительно, если бы линейная комбинация смежных классов (21) с коэффициентами a_0, a_1, $\ldots$, $a_{n-m-1} \in K$ равнялась $[0]$, то мы имели бы $[(a_0 + a_1x + \ldots + a_{n-m-1}x^{n-m-1})\,t(x)] = [0]$; однако это возможно лишь в том случае, когда $a_0 + a_1x + \ldots + a_{n-m-1}x^{n-m-1} \equiv 0$.

Обозначим через $s(x)$ многочлен степени $< n$, сравнимый с $x^{n-m}t(x)$ по модулю $(x^n - 1)$. Так как $t(x) \mid x^n - 1$, то также $s(x) \equiv x^{n-m}\,t(x) \bmod (t_n(x))$. Отсюда следует, что $t(x) \mid s(x)$, или $s(x) = s_1(x)\,t(x)$. Очевидно, что $\operatorname{Grad} s_1(x) < n - m$; поэтому смежный класс

$$[x^{n-m}t(x)] = [s_1(x)\,t(x)]$$

лежит в подпространстве T, порожденном классами (21). Следовательно, $[x]\,T \subseteq T$.

Итак, $[t(x)] \in T \subseteq ([t(x)])$ и $[x]\,T \subseteq T$. Отсюда следует, что $T = ([t(x)])$. Базис T, состоящий из $n - m$ смежных классов (21), является также базисом $([t(x)])$, что и доказывает формулу (17′).

Упражнения

1. Выведите неравенство $\operatorname{Grad} \operatorname{Ker} f(\xi) \leqslant \operatorname{Grad} f$ для $f(x) = \sum_{i=0}^{m} c_i x^i$ $(c_m \neq 0,\ m < n)$ непосредственно из циклической системы уравнений $c_0\boldsymbol{a}_1 + c_1\boldsymbol{a}_2 + \ldots + c_m\boldsymbol{a}_{m+1} = \boldsymbol{o}$, $\ldots$.

2. Более абстрактное доказательство равенства (17) получается из соотношения

$$n - \dim(t(\zeta)) = \dim K[\zeta]/(t(\zeta)) = \dim K[x]/(t(x)) = \operatorname{Grad} t$$

для $t(x) \mid x^n - 1$.

3. Пусть $K = \mathbf{Q}$. Какие из чисел 0, 1, ..., n являются степенями свободы циклических классов n-угольников? Для каких n к а ж д о е из этих чисел может быть степенью свободы некоторого циклического класса?

§ 5. Смешанные задачи

1. Пусть $\mathscr{C}$ — циклический класс степени m, определенный делителем $t(x) = c_0 + c_1 x + \ldots + c_m x^m$ (где $t(x) \mid x^n - 1$). Произвольный n-угольник из $\mathscr{C}$ можно получить следующим образом: $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ выберем произвольно, $\boldsymbol{a}_{m+1}, \ldots, \boldsymbol{a}_n$ найдутся единственным образом из рекуррентной системы

$$c_0\boldsymbol{a}_1 + \ldots + c_m\boldsymbol{a}_{m+1} = \boldsymbol{o}, \quad \ldots, \quad c_0\boldsymbol{a}_{n-m} + \ldots + c_m\boldsymbol{a}_n = \boldsymbol{o}.$$

Полученное представление циклического класса $\mathscr{C}$ назовем *нормальным*. При этом представлении $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ — параметры. [$t(x)$ можно еще нормировать так, чтобы $c_m = 1$.]

2. Пусть γ — автоморфизм, а φ — эндоморфизм некоторой абелевой группы. Обозначим $\gamma\varphi\gamma^{-1}$ через φ^γ; тогда $\gamma(\operatorname{Ker}\varphi) = \operatorname{Ker}\varphi^\gamma$, $\gamma(\operatorname{Im}\varphi) = \operatorname{Im}\varphi^\gamma$.

3. Пусть $n = 2m$; отображение α: $(\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3, \ldots, \boldsymbol{a}_{2m}) \to (\boldsymbol{a}_1, -\boldsymbol{a}_2, \boldsymbol{a}_3, \ldots, -\boldsymbol{a}_{2m})$ является инволютивным автоморфизмом $\mathscr{A}_n$, но не циклическим отображением. Для всякого циклического отображения $f(\zeta)$ имеем $f(\zeta)^\alpha = f(-\zeta)$. Отображение

$$f(\zeta) \longrightarrow f(-\zeta) \qquad (*)$$

является инволюгивным автоморфизмом в $K[\zeta]$, а также в $E(K[\zeta])$. Справедливо равенство $\alpha(\operatorname{Ker} t(\zeta)) = \operatorname{Ker} t(\zeta)^\alpha = \operatorname{Ker} t(-\zeta)$. Отображение

$$\operatorname{Ker} t(\zeta) \longrightarrow \operatorname{Ker} t(-\zeta) \qquad (**)$$

является инволютивным автоморфизмом булевой алгебры циклических классов, сохраняющим степень класса. Оно меняет местами АСО-класс и нуль-изобарический класс, класс тривиальных $2m$-угольников и класс m раз пройденных 2-угольников с центром тяжести $\boldsymbol{o}$.

При $K = \mathbf{Q}$, $n = 4$ и $n = 6$ исследуйте, как отображение (*) преобразует циклические проекции, а отображение (**) — циклические классы.

4. Пусть n четно и $d \mid n$. Вместе с $m_d(x)$ (§ 4 гл. 8) многочлен $m_d(-x)$ является идемпотентным $\bmod(x^n - 1)$ делителем многочлена $x^n - 1$. Если d четно, то $m_d(x) = m_d(-x)$. Пусть d нечетно. Установите связь между $m_d(x)$ и $m_d(-x)$ и опишите ее в терминах булевой алгебры циклических проекций и циклических классов. На-

пример,

$$m_d(x)+m_d(-x)=m_{2d}(x),\quad m_d(x)\,m_d(-x)\equiv 0 \bmod (x^n-1), \qquad (*)$$

$$1-m_d(-x)+m_1(-x)=1-(m_{2d}(x)-m_d(x))+ \\ +(m_2(x)-m_1(x)). \qquad (**)$$

Заменяя x на ζ в (**), получим циклическую проекцию, которая имеет одинаковые образ и ядро с $\alpha_d=1-\zeta+\zeta^2-\ldots+\zeta^{d-1}$; ее можно записать так: $\mu_2 \circ \mu_d \circ (1-\mu_{2d})$.

5. Пусть $\operatorname{Char} K \neq 2$. При нечетном n отображение α_d $(d \mid n)$ обратимо; обратным элементом является $\varkappa_2(1-\zeta^d+\zeta^{2d}-\ldots+\zeta^{n-d})$.

6. Отображение $\alpha_3=1-\zeta+\zeta^2$ специализирует множество n-угольников только при $n=6, 12, 18, \ldots$.

7. Действие α_3 на параллелограмм, а также многократно пройденный параллелограмм сводится к циклической перестановке его вершин. Существуют ли еще нетривиальные n-угольники, обладающие тем же свойством?

8. Пусть $\operatorname{Char} K=0$. Рассмотрим отображение $\varkappa_r=\frac{1}{r}(1+\zeta+\zeta^2+\ldots+\zeta^{r-1})$ для любого $r=1, 2, \ldots$. Если d есть НОД чисел r и n, то $\varkappa_r$ и $\varkappa_d$ имеют одинаковые образ и ядро.

Если u нечетно и $d=\text{НОД}(u, n)$, то α_u, α_d имеют одинаковые образ и ядро.

9. Отображение $\zeta \longrightarrow \zeta^{-1}$ является автоморфизмом кольца $K[\zeta]$, переводящим $f(\zeta)=c_0+c_1\zeta+\ldots+c_{n-1}\zeta^{n-1}$ в $f(\zeta^{-1})=c_0+c_{n-1}\zeta+\ldots+c_1\zeta^{n-1}$. Пусть $t(x)$ — делитель x^n-1. Если $t(x)$ симметричен или антисимметричен (см. § 1 гл. 12; при $K=\mathbf{Q}$ это предположение выполняется всегда), то отображения $t(\zeta)$ и $t(\zeta^{-1})$ имеют одинаковые образ и ядро.

10 *(циклические классы циклических отображений)*. Циклическое отображение пространства V^n задается n-набором коэффициентов $(c_0, c_1, \ldots, c_{n-1})$, $c_i \in K$, следовательно, «n-угольником» из векторного пространства K^n (здесь $V=K$, $\mathcal{A}_n=K^n$). Все понятия теории n-угольников посредством изоморфизма $(c_0, c_1, \ldots, c_{n-1}) \longrightarrow \sum c_i \cdot \zeta^i$ переносятся из K^n на $K[\zeta]$. Идеалы в $K[\zeta]$ можно истолковать теперь как «циклические классы циклических отображений».

Пример. Идеал (σ) состоит из «тривиальных» циклических отображений, т. е. отображений $\sum c_i\zeta^i$, где $c_0=c_1=\ldots=c_{n-1}$; идеал $(1-\sigma)$ — из циклических отображений «с центром тяжести 0», т. е. из циклических отображений $\sum c_i\zeta^i$, где $\frac{1}{n}\sum c_i=0$ (ср. упражнение к § 3 гл. 3).

11 *(циклические отображения циклического класса)*. По теореме 5 гл. 2 циклический класс $\mathscr{C}$ остается на месте под действием любого циклического отображения. Но, вообще говоря, внутри $\mathscr{C}$ некоторые отображения действуют одинаково Мы хотим выделить в $K[\zeta]$ подмножество, содержащее все различные циклические отображения класса $\mathscr{C}$.

Пусть многочлен $t(x) \mid x^n - 1$ определяет класс $\mathscr{C}: \mathscr{C} = \operatorname{Ker} t(\zeta) = \operatorname{Im} e_t(\zeta)$. Два циклических отображения одинаково действуют на $\mathscr{C}$, когда они сравнимы $\bmod (t(\zeta))$. Всевозможные различные циклические отображения $\mathscr{C}$ представляются элементами идеала $(e_t(\zeta))$. Справедливы равенства

$$K[\zeta] = (t(\zeta)) \oplus (e_t(\zeta)) \text{ и } (e_t(\zeta)) \cong K[\zeta]/(t(\zeta)) \cong K[x]/(t(x)).$$

Идеал $(e_t(\zeta))$ состоит из циклических отображений, которые переводят $\mathscr{A}_n$ в $\mathscr{C}$.

12. Пусть $n = 4$. Системой представителей всех циклических отображений на классе параллелограммов

$$(\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3, \boldsymbol{a}_4), \quad \boldsymbol{a}_1 - \boldsymbol{a}_2 + \boldsymbol{a}_3 - \boldsymbol{a}_4 = \boldsymbol{o}$$

являются циклические отображения с набором коэффициентов

$$(c_0, c_1, c_2, c_3), \text{ где } c_0 - c_1 + c_2 - c_3 = 0,$$

т. е. класс «параллелограммов» циклических отображений (в смысле задачи 10). В частности, к ним принадлежат циклические отображения, переводящие множество всех 4-угольников в множество параллелограммов, такие, как $\varkappa_2$ и проекция $1 - \mu_2 + \sigma$ с наборами коэффициентов $\frac{1}{2}(1, 1, 0, 0)$ и $\frac{1}{4}(3, 1, -1, 1)$.

Руководствуясь этими примерами, установите общую теорему относительно различных циклических отображений циклического класса n-угольников.

13 (Киндер). Из всякой подстановки π множества $\{1, \ldots, n\}$ можно получить автоморфизм $\bar{\pi}$ векторного пространства n-угольников $\mathscr{A}_n = V^n$ над K:

$$\bar{\pi}: (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n) \longrightarrow (\boldsymbol{a}_{\pi(1)}, \ldots, \boldsymbol{a}_{\pi(n)});$$

$\pi \longrightarrow \bar{\pi}$ есть мономорфизм группы $\mathfrak{S}_n$ всех подстановок чисел $\{1, \ldots, n\}$ в группу автоморфизмов $\mathscr{A}_n$. Например, циклическое отображение ζ есть образ подстановки $\begin{pmatrix} 1 & 2 & \ldots & n \\ 2 & 3 & \ldots & 1 \end{pmatrix} = (1, 2, \ldots, n)$. Вообще говоря, $\bar{\pi}$ не является циклическим отображением. Покажите, что для всякого $\pi \in \mathfrak{S}_n$ следующие утверждения попарно эквивалентны:

1°. $\bar{\pi} \in K[\zeta]$; 2°. $\bar{\pi}\zeta = \zeta\bar{\pi}$; 3°. $\pi(1 \ \ldots \ n) = (1 \ \ldots \ n)\pi$;

4°. $(\pi(1) \ \ldots \ \pi(n)) = (1 \ \ldots \ n)$; 5°. $\pi = (1 \ \ldots \ n)^j$ для некоторого $j \in \{0, 1, \ldots, n-1\}$; 6°. $\bar{\pi} = \zeta^j$ для некоторого $j \in \{0, 1, \ldots, n-1\}$.

Отсюда следует, что $\bar{\pi}$ является циклическим отображением тогда и только тогда, когда оно имеет вид некоторой степени ζ.

14 (Киндер). Согласно задаче 2, автоморфизм пространства $\mathscr{A}_n$ отображает всякий циклический класс на циклический класс, если он принадлежит нормализатору $N(K[\zeta])$ кольца $K[\zeta]$ в $\operatorname{End}(\mathscr{A}_n)$. Покажите, что для всякой подстановки π чисел $\{1, \ldots, n\}$

следующие утверждения попарно эквивалентны:

1°. $\bar{\pi} \in N(K[\zeta])$; 2°. $\bar{\pi}\zeta\bar{\pi}^{-1} \in K[\zeta]$; 3°. $\overline{(\pi(1) \ldots \pi(n))} \in K[\zeta]$; 4°. $(\pi(1) \ldots \pi(n)) = (1 \ldots n)^j$, где $j \in \{0, 1, \ldots, n-1\}$; 5°. Существуют j, взаимно простое с n, и $k \in \{0, 1, \ldots, n-1\}$, такие, что для $i = 1, 2, \ldots, n$

$$\pi(i) \equiv i \cdot j + k \bmod n. \qquad (*)$$

Группу подстановок со свойствами 1°—5° обозначим через G_n. Пусть F_n — подгруппа подстановок $\pi \in G_n$, таких, что автоморфизмы $\bar{\pi}$ отображают на себя всякий циклический класс. Подстановка $(1 \ldots n) \in F_n$ ($j = k = 1$) порождает группу Z_n порядка n, которая в G_n (и тем самым в F_n) является нормальным делителем.

Покажите, что факторгруппа F_n/Z_n изоморфна группе Галуа многочлена $x^n - 1$ над полем K. Смежный класс πZ_n подстановки π, удовлетворяющей сравнению (*), соответствует K-автоморфизму $\sum c_i w^i \longrightarrow \sum c_i w^{ij}$ ($c_i \in K$) поля $K(w)$. Здесь w — первообразный корень n-й степени из 1 в поле разложения $K(w)$ многочлена $x^n - 1$ над K.

15. Пусть K_p — простое поле характеристики p и $p \mid n$. Если $n = p^l m$ и $(p, m) = 1$, то $x^n - 1 = (x^m - 1)^{p^l}$. Существует по меньшей мере $(p^l + 1)^{\tau(m)}$ циклических классов. Определите циклические классы 6-угольников над K_3 (они образуют дистрибутивную структуру, но не булеву алгебру).

ГЛАВА 10

РАЦИОНАЛЬНЫЕ КОМПОНЕНТЫ n-УГОЛЬНИКА

§ 1. Q-правильные n-угольники

n-угольник $\boldsymbol{A}$ называется **Q**-*правильным*, если *все его хордовые* d-*угольники*[1]) *изобаричны* (здесь d — любой нетривиальный делитель числа n). Множество **Q**-правильных n-угольников обозначим через $\mathcal{R}_n$.

Всякий 1-угольник и всякий p-угольник (p — простое число) **Q**-правильны: $\mathcal{R}_1 = \mathcal{A}_1$, $\mathcal{R}_p = \mathcal{A}_p$; таким образом, для $n = 1$, p понятие **Q**-правильности бессодержательно. Чтобы оценить, насколько оно ограничительно в случае составного n, полезно разобрать несколько частных случаев (см. рис. 62—85).

В гл. 4 были рассмотрены классы изобарически распадающихся n-угольников: если $d \mid n$ и $n = d\bar{d}$, то n-угольник, все хордовые d-угольники которого изобаричны, называется $\bar{d}$-*кратно изобарически распадающимся*. Множество таких n-угольников образует циклический класс $\mathcal{A}_n^d$; $\mathcal{A}_n^1$ есть класс n-угольников; $\mathcal{A}_n^n$ — класс тривиальных n-угольников.

Очевидно, что $\mathcal{R}_n$ является пересечением всех классов A_n^d, где $d \neq n$:

$$\mathcal{R}_n = \bigcap_{\substack{d \mid n \\ d \neq 1, n}} \mathcal{A}_n^{n/d} = \bigcap_{\substack{d \mid n \\ d \neq n, 1}} \mathcal{A}_n^d. \qquad (1)$$

$\mathcal{R}_n$ является свободным циклическим классом (как пересечение свободных циклических классов).

Примеры. $\mathcal{R}_4$ совпадает с классом параллелограммов $\mathcal{A}_4^2$; $\mathcal{R}_6 = \mathcal{A}_6^2 \cap \mathcal{A}_6^3$ — класс аффинно-правильных 6-угольников (§ 1 гл. 4). Вообще, **Q**-правильными $2p$-угольниками

---

[1]) Хордовые d-угольники n-угольника $\boldsymbol{A}$ — это строки таблицы вершин этого многоугольника, записанной mod $\frac{n}{d}$.

(p — простое нечетное число) являются $2p$-параллелограммы, имеющие равную нулю знакопеременную сумму вершин. Это такие $2p$-угольники, в которых все p-наборы последовательных вершин имеют одну и ту же знакопеременную сумму. Их «параметрическим представлением» является

$$(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_p, -\boldsymbol{a}_1 + 2\boldsymbol{s}, \ldots, -\boldsymbol{a}_p + 2\boldsymbol{s}),$$
$$\text{где } \boldsymbol{s} = \boldsymbol{a}_1 - \boldsymbol{a}_2 + \boldsymbol{a}_3 - \ldots + \boldsymbol{a}_p.$$

Итак, **Q**-правильный $2p$-угольник можно построить следующим образом: выберем произвольно p точек, построим их знакопеременную сумму (хотя бы путем последовательного достраивания четвертой вершины параллелограмма) и затем отразим выбранные точки относительно $\boldsymbol{s}$.

Теорема 1. *Пусть $n \neq 1$; n-угольник $\boldsymbol{A}$ тогда и только тогда* **Q**-*правилен, когда для каждого простого делителя p числа n все его хордовые p-угольники изобаричны.*

Доказательство. Если $t \mid d \mid n$, то $\mathcal{A}_n^{n/t} \subseteq \mathcal{A}_n^{n/d}$. Так как для всякого делителя $d \neq 1$ числа n существует простой делитель p, такой, что $p \mid d$, то для всякого класса, входящего в первое пересечение (1), найдется содержащийся в нем класс $\mathcal{A}_n^{n/p}$. Этими меньшими классами и можно ограничиться в пересечении:

$$\mathcal{R}_n = \bigcap_{p \mid n} \mathcal{A}_n^{n/p} \text{ для } n \neq 1. \qquad (2)$$

Пример. $\mathcal{R}_8 = \mathcal{A}_8^4$ — класс 8-параллелограммов (см. теорему 4 гл. 1).

Все *хордовые* d-угольники **Q**-правильного n-угольника (где $d \mid n$) **Q**-правильны. Действительно, при $t \mid d \mid n$ все хордовые t-угольники хордового d-угольника для $\boldsymbol{A}$ сами являются хордовыми t-угольниками для $\boldsymbol{A}$ и потому изобаричны. Можно задать обратный вопрос: как влияет **Q**-правильность и изобаричность хордовых многоугольников на **Q**-правильность всего n-угольника? Например, если выбрать два аффинно-правильных 6-угольника и перенумеровать их вершины так: $(\boldsymbol{a}_1, \boldsymbol{a}_3, \ldots, \boldsymbol{a}_{11})$, $(\boldsymbol{a}_2, \boldsymbol{a}_4, \ldots, \boldsymbol{a}_{12})$, то 12-угольник $(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_{12})$ является **Q**-правильным. В частности, при специальном выборе аффинно-правиль-

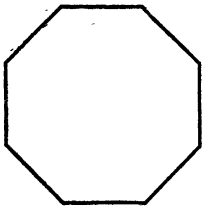


Рис. 62.

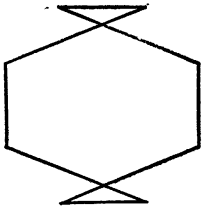


Рис. 63.

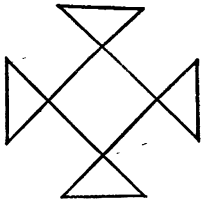


Рис. 64.

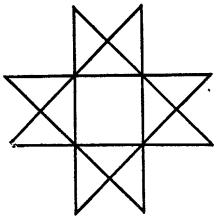


Рис. 65.

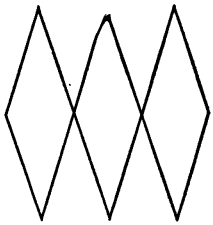


Рис. 66.

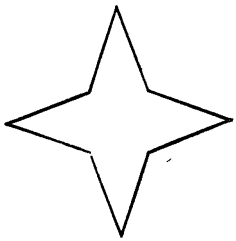


Рис. 67.

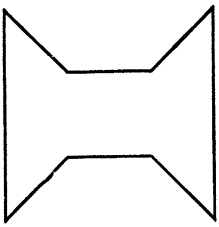


Рис. 68.

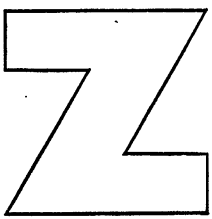


Рис. 69.

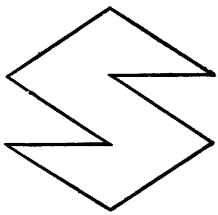


Рис. 70.

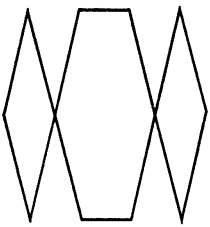


Рис. 71.

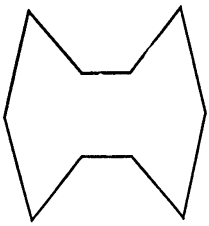


Рис. 72.

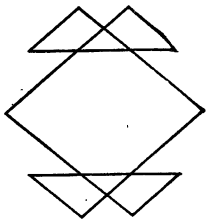


Рис. 73.

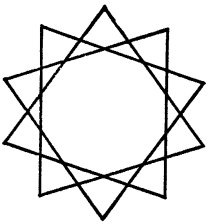


Рис. 74.

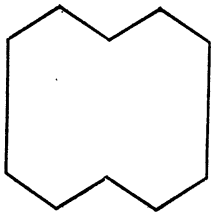


Рис. 75.

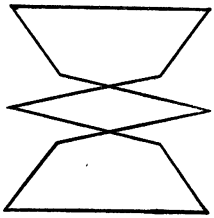


Рис. 76.

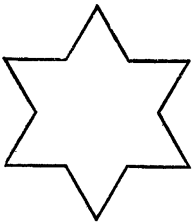


Рис. 77.

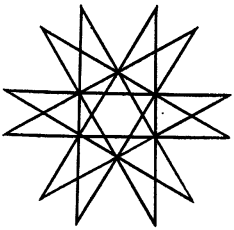


Рис. 78.

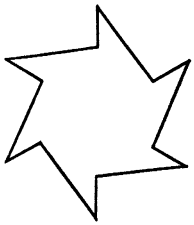


Рис. 79.

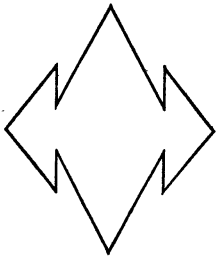


Рис. 80.

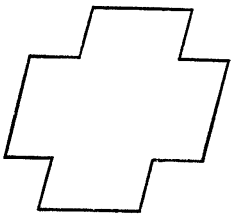


Рис. 81.

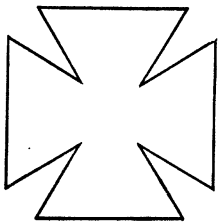


Рис. 82.

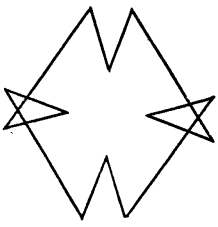


Рис. 83.

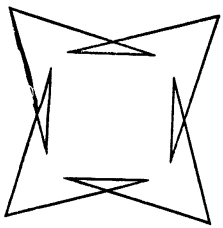


Рис. 84.

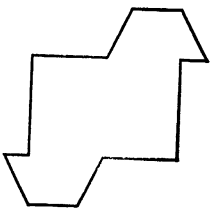


Рис. 85.

ных 6-угольников получаются «мальтийский крест» и «звезда Давида» (рис. 82, 77).

Q-правильные n-угольники с центром тяжести o образуют центральный циклический класс $\overset{\circ}{\mathcal{R}}_n$. Для него также справедливы формулы (1) и (2), если в них все свободные классы $\mathcal{A}_n^d$ заменить соответствующими центральными классами $\overset{\circ}{\mathcal{A}}_n^d$.

Упражнения

1. При $n=p^\nu$, где p — простое число, n-угольники, хордовые p-угольники которых изобаричны, являются **Q**-правильными.

2. Если $n \neq 1$ и n^* — свободное от квадратов *ядро* n (максимальный свободный от квадратов делитель n), то **Q**-правильными являются те n-угольники, все хордовые n^*-угольники которых **Q**-правильны и изобаричны.

§ 2. Циклические классы, определенные многочленами деления круга

В гл. 8 мы говорили о циклических классах n-угольников, определенных многочленами деления круга $F_d(x)$, где $d \mid n$, и прежде всего о классе, определенном многочленом $F_n(x)$. При $n=1$ это есть класс всех 1-угольников.

Теорема 2. *Пусть* $n \neq 1$. *Циклический класс* n*-угольников, определенный многочленом* $F_n(x)$, *состоит из* **Q***-правильных* n*-угольников с центром тяжести* o:

$$\operatorname{Ker} F_n(\zeta) = \overset{\circ}{\mathcal{R}}_n. \tag{3}$$

Доказательство. Из многочленов $m_d(x)$ (см. § 4 гл. 8) образуем булеву сумму (см. § 1 гл. 5)

$$\sum_{d \parallel n} \circ m_d(x). \tag{4}$$

На первообразных корнях n-й степени из единицы многочлен (4) принимает значение 0, а на остальных 1. Действительно, на первообразных корнях каждое слагаемое равно 0, а на корнях d-й степени из единицы, где $d \parallel n$, слагаемое $m_d(x)$ равно 1, следовательно, и булева сумма равна 1.

Рассмотрим систему равенств

$$\operatorname{Ker} F_n(\zeta) = \operatorname{Ker} \sum_{d\|n} \circ\, \mu_d = \bigcap_{d\|n} \operatorname{Ker} \mu_d = \bigcap_{d\|n} \mathcal{A}_n^d = \overset{\circ}{\mathcal{R}}_n.$$

Справедливость первого равенства следует из того, что $m_d(\zeta) = \mu_d$ и из теоремы 8b гл. 8; справедливость второго — из правила (18) гл. 5 и, наконец, третьего — из § 3 гл. 4.

Теорема 3. *$F_1(x)$ определяет класс тривиальных n-угольников; $F_d(x)$, где $d \mid n$, $d \neq 1$, — класс $\bar{d}$ раз пройденных $\mathbf{Q}$-правильных d-угольников с центром тяжести o:*

$$\operatorname{Ker} F_1(\zeta) = \mathcal{A}_{1,n},\ \operatorname{Ker} F_d(\zeta) = \overset{\circ}{\mathcal{R}}_{d,\bar{d}} \text{ для } d \mid n,\ d \neq 1. \quad (5)$$

Доказательство. Первая из формул (5) нам уже известна (см. § 3 гл. 6). Пусть теперь $d \mid n$, $d \neq 1$. В силу теоремы 2, $F_d(x)$ определяет класс $\mathbf{Q}$-правильных d-угольников $\overset{\circ}{\mathcal{R}}_d$; по лемме из § 4 гл. 8 тот же многочлен определяет класс n-угольников $\overset{\circ}{\mathcal{R}}_{d,\bar{d}}$.

Каждому делителю d соответствует свой класс $\overset{\circ}{\mathcal{R}}_{d,\bar{d}}$; его степень свободы равна (см. теорему 5 гл. 9) степени определяющего многочлена $F_d(x)$, следовательно, значению функции Эйлера $\varphi(d)$. Отсюда следует, между прочим, что класс $\mathbf{Q}$-правильных n-угольников при $n \neq 1$ имеет степень свободы $\varphi(n) + 1$.

Поскольку произведение многочленов деления круга $F_d(x)$ (при $d \mid n$) равно $x^n - 1$ и они попарно взаимно просты, то, согласно теореме 5 гл. 8, $\mathcal{A}_n$ является прямой суммой циклических классов (5).

Если $K = \mathbf{Q}$, то многочлены $F_d(x)$ ($d \mid n$, старшие коэффициенты равны 1) являются простыми делителями $x^n - 1$. Поэтому классы (5) являются атомарными циклическими классами (теорема 5 гл. 8; ср. § 3 гл. 6).

Теорема 4. *При $K = \mathbf{Q}$ атомарными циклическими классами n-угольников являются класс $\mathcal{A}_{1,n}$ тривиальных n-угольников и классы $\overset{\circ}{\mathcal{R}}_{d\bar{d}}$ $\bar{d}$ раз пройденных $\mathbf{Q}$-правильных d-угольников с центром тяжести o ($d \mid n$, $d \neq 1$), включая (при*

$d=n, n\neq 1$) *класс* $\mathcal{R}_n^{\circ}$ **Q**-*правильных* n-*угольников с центром тяжести* $\boldsymbol{o}$.

Пример: $K=\mathbf{Q}$, $n=12$. Существует шесть атомарных циклических классов 12-угольников:

тривиальные 12-угольники,
шестикратно пройденные 2-угольники с центром тяжести $\boldsymbol{o}$,
четырехкратно пройденные 3-угольники с центром тяжести $\boldsymbol{o}$,
трижды пройденные параллелограммы с центром тяжести $\boldsymbol{o}$,
дважды пройденные аффинно-правильные 6-угольники с центром тяжести $\boldsymbol{o}$,
Q-правильные 12-угольники с центром тяжести $\boldsymbol{o}$.

Выясним, что представляют собой **Q**-правильные 12-угольники. Многочлену $F_{12}(x)=x^4-x^2+1$ соответствует циклическая система $\boldsymbol{a}_1-\boldsymbol{a}_3+\boldsymbol{a}_5=\boldsymbol{o}, \ldots$. Она распадается на две системы — с нечетными и четными индексами, — каждая из которых определяет аффинно-правильные 6-угольники. Итак, **Q**-правильными являются 12-угольники, оба хордовых 6-угольника которых аффинно-правильны и изобаричны.

§ 3. Рациональные компоненты n-угольника

Как и для всякого делителя x^n-1, для многочлена деления круга $F_d(x)$, где $d\,|\,n$, существует однозначно определенная циклическая проекция, отображающая множество всех n-угольников на циклический класс, определенный многочленом $F_d(x)$ (см. § 2 гл. 8). Обозначим ее через ε_d:

$$\operatorname{Ker} F_d(\xi)=\operatorname{Im}\varepsilon_d. \tag{6}$$

Проекция ε_d соответствует многочлену $F_d(x)$ при изоморфизме структур i_{15}: L_1 на L_5 (см. § 1 гл. 8). При этом произведению делителей из L_1 изоморфна булева сумма соответствующих проекций и взаимно простым делителям соответствуют ортогональные проекции. Поскольку многочлены $F_d(x)$ для всех $d\,|\,n$ попарно взаимно просты и их

произведение равно $x^n - 1$, проекции ε_d для всех $d \mid n$ попарно взаимно ортогональны и их сумма равна 1.

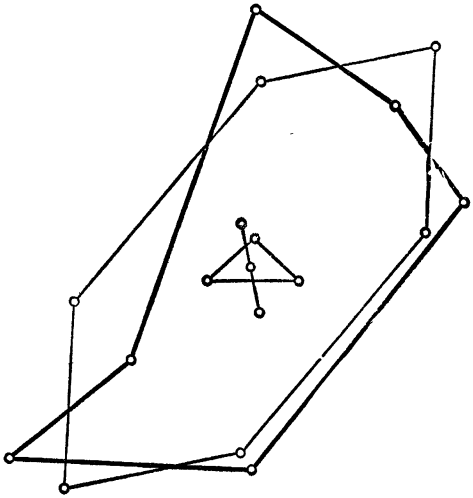


Рис. 86. Разложение 6-угольника с центром тяжести $\boldsymbol{o}$ на его рациональные компоненты.

Отсюда получается однозначное разложение произвольного n-угольника $\boldsymbol{A}$ на n-угольники из циклических классов (5):

$$\boldsymbol{A} = \sum_{d \mid n} \varepsilon_d \boldsymbol{A}. \tag{7}$$

Циклическая проекция ε_1, отображающая множество всех n-угольников на класс тривиальных, совпадает с σ; следовательно, $\varepsilon_1 \boldsymbol{A}$ — центр тяжести n-угольника $\boldsymbol{A}$. При $d \neq 1$ многоугольник $\varepsilon_d \boldsymbol{A}$ есть $\bar{d}$ раз пройденный $\mathbf{Q}$-правильный d-угольник с центром тяжести $\boldsymbol{o}$.

Эти n-угольники $\varepsilon_d \boldsymbol{A}$ мы будем называть *рациональными компонентами* $\boldsymbol{A}$, а n-угольник $\varepsilon_n \boldsymbol{A}$ — *рациональной* $\mathbf{Q}$-*правильной компонентой* $\boldsymbol{A}$. Если $K = \mathbf{Q}$, то разложение (7) является атомарным (см. рис. 86).

Для всякого делителя d циклическую проекцию ε_d можно получить из $F_d(x)$ и его производной с помощью формулы (11) гл. 8. Существует еще одно интересное представление ε_d:

Теорема 5.

$$\varepsilon_d = \mu_d \prod_{t \parallel d} (1 - \mu_t).$$

Доказательство. Пусть $d \mid n$. Рассмотрим многочлен

$$f_d(x) := m_d(x) \prod_{t \parallel d} (1 - m_t(x)).$$

Он равен 1 на первообразных корнях степени d из 1 и 0 на остальных корнях степени n из 1. Действительно, на первообразных корнях степени d из 1 все сомножители произведения $f_d(x)$ равны 1 (на каждом из таких корней $m_d(x)$ равен 1, а $m_d(x)$ равен 0, $t \parallel d$). Остальные корни из 1 либо являются корнями степени t ($t \parallel d$), либо вообще не являются корнями степени d из 1. На первых из них $m_t(x)$ равен 1, а $1 - m_t(x)$ равен 0; на последних $m_d(x)$ равен 0.

Отсюда следует, что $f_d(\zeta)$ является циклической проекцией, отображающей множество всех n-угольников на циклический класс, определенный многочленом $F_d(x)$ (см. теорему 8а гл. 8). Поэтому $f_d(\zeta) = \varepsilon_d$. Теорема доказана.

Приведем формулу, обратную к доказанной в теореме 5:

$$\mu_d = \sum_{t \mid d} \varepsilon_t. \tag{8}$$

[Поскольку ε_d попарно ортогональны, в формуле (8) можно вместо простой суммы писать также булеву сумму.]

Доказательство. Многочлены $m_d(x)$ и $f_d(x)$ связаны следующим сравнением:

$$m_d(x) \equiv \sum_{t \mid d} f_t(x) \mod (x^n - 1). \tag{9}$$

Действительно, поскольку многочлен $f_t(x)$ равен 1 на первообразных корнях t-й степени из 1 и 0 на остальных

корнях n-й степени из 1, то стоящая справа в (9) сумма равна 1 на всех корнях степени d из 1 и 0 на всех остальных корнях n-й степени из 1. Таким образом, эта сумма совпадает с $m_d(x)$ на спектре многочлена x^n-1. Если в (9) вместо x подставить ζ, получим (8).

Упражнение. Вывести непосредственно из формулы (8) мультипликативное правило для μ_d (§ 2 гл. 4).

§ 4. Булева алгебра, порожденная хордовыми усреднениями, и ее атомарные элементы

Как известно, хордовые усреднения μ_d, где $d|n$, являются циклическими проекциями и как элементы булевой алгебры $(E(K[\zeta]), \circ, \cdot)$ порождают некоторую подалгебру E_μ (§ 5 гл. 5). Элементы μ_d не являются свободными образующими алгебры E_μ, т. е. не все μ_d атомарны в E_μ. Справедлива

Теорема 6. *Циклические проекции ε_d (где $d|n$) образуют систему атомарных элементов алгебры E_μ. Эта алгебра содержит $2^{\tau(n)}$ элементов и в случае $K=\mathbf{Q}$ состоит из всех циклических проекций.*

Доказательство. По теореме 5, ε_d (где $d|n$) *принадлежат* E_μ; они отличны от нуля, попарно ортогональны и их сумма равна 1. Отсюда (в силу теоремы 2 гл. 5) следует, что ε_d атомарны в некоторой подалгебре, принадлежащей E_μ и содержащей $2^{\tau(n)}$ элементов. Из формулы (8) вытекает, что эта подалгебра совпадает с E_μ. При $K=\mathbf{Q}$ количество простых делителей x^n-1 равно $\tau(n)$ (§ 2 гл. 6), а количество циклических проекций равно $2^{\tau(n)}$ (теоремы 1′ и 2 гл. 8); следовательно, все они содержатся в E_μ. Теорема доказана.

Фигурирующее в теореме 5 произведение можно сократить: при $d\neq 1$ можно ограничиться максимальным собственным делителем t числа d. Запись комбинаций из μ_d с помощью операций $\circ$, $\cdot$, $1-$ [как, например, в теореме 5 или в формуле (4)] удобна тем, что изоморфизмом Im (или антиизоморфизмом Ker) она непосредственно переносится на соответствующие комбинации циклических классов. С другой стороны, раскроем скобки

в произведении теоремы 5 и воспользуемся правилом из § 2 гл. 4. Тогда мы и представим ε_d в виде целочисленной линейной комбинации из элементов μ_t, где $t|d$.

Пример: $n=12$, $\varepsilon_1=\mu_1$, $\varepsilon_2=\mu_2-\mu_1$, $\varepsilon_3=\mu_3-\mu_1$, $\varepsilon_4=\mu_4-\mu_2$, $\varepsilon_6=\mu_6-\mu_3-\mu_2+\mu_1$, $\varepsilon_{12}=\mu_{12}-\mu_6-\mu_4+\mu_2$ (причем всегда $\mu_1=\sigma$, а при $n=12$ еще $\mu_{12}=1$).

В этом примере коэффициенты при μ_t в представлениях для ε_d равны 1, —1, 0 и сумма их равна нулю при $d\neq 1$. Эта закономерность имеет общий характер. Действительно, на основании формулы обращения Мёбиуса [1]) из (8) следует

Теорема 7.

$$\varepsilon_d=\sum_{t|d}\mu\left(\frac{d}{t}\right)\mu_t.$$

Здесь $\mu(m)$ — *функция Мёбиуса* натурального аргумента m, определенная следующим образом: $\mu(1)=1$; $\mu(m)=(-1)^r$, если m есть произведение r попарно различных простых делителей; $\mu(m)=0$, если $m\neq 1$ и не свободно от квадратов; при этом $\sum_{t|m}\mu(t)=0$ при всех $m\neq 1$.

Итак, мы получили два представления ε_n (теоремы 5 и 7). Применяя законы де Моргана к формуле теоремы 5 и учитывая, что $\mu_n=1$, эти представления можно переписать так:

$$1-\varepsilon_n=\sum_{d|\,|n}\circ\mu_d; \tag{10}$$

$$1-\varepsilon_n=-\sum_{d|\,|n}\mu\left(\frac{n}{d}\right)\mu_d. \tag{11}$$

Упражнение. Проекция ε_d (где $d|n$) допускает следующее представление с помощью функции Мёбиуса:

$$\varepsilon_d=\sum_{i=0}^{n-1}c_i\xi^i, \quad \text{где} \quad c_i=\frac{1}{n}\sum_{t|(d,\,i)}\mu\left(\frac{d}{t}\right)t$$

[1]) См., например, Хассе [18], § 4, 7 [или Виноградов [7]. — *Прим. ред.*]

$[(d, i)$ обозначает НОД чисел d и $i]$. Если число d свободно от квадратов, то справедливы также формулы

$$c_i = \frac{1}{n}\,\mu\left(\frac{d}{(d, i)}\right)\varphi\,((d, i)),$$

где $\varphi(m)$ — функция Эйлера.

§ 5. К построению рациональных компонент n-угольника

1-угольник имеет единственную рациональную компоненту — самого себя. Пусть теперь $n \neq 1$.

Класс $\overset{\circ}{\mathcal{R}}_n$ **Q**-правильных n-угольников является пересечением классов $\overset{\circ}{\mathcal{A}}{}_n^d$, где $d \| n$. В булевой алгебре циклических классов n-угольников дополнительными к $\overset{\circ}{\mathcal{A}}{}_n^d$ являются классы $\mathcal{A}_{d,\,\bar{d}}$ (теорема 3 гл. 4); поэтому *дополнительным к центральному классу* $\overset{\circ}{\mathcal{R}}_n$ **Q**-*правильных* n-*угольников является класс*

$$\mathcal{A}_n^* = \sum_{d \| n} \mathcal{A}_{d,\,\bar{d}}, \tag{12}$$

сумма всех собственно периодических классов. Для него справедлива теорема, аналогичная теореме 1. С другой стороны, поскольку $\mathcal{A}_n$ разлагается в прямую сумму циклических классов из теоремы 3, то $\mathcal{A}_n^*$ есть сумма всех этих классов, кроме $\overset{\circ}{\mathcal{R}}_n$.

Из $\operatorname{Im}\varepsilon_n = \overset{\circ}{\mathcal{R}}_n$ вытекает, что $\operatorname{Im}(1-\varepsilon_n) = \mathcal{A}_n^*$.

Примеры. $\mathcal{A}_6^*$ — класс призм (см. § 5 гл. 5); $\mathcal{A}_{12}^*$ — класс 12-угольников, оба хордовых 6-угольника которых являются призмами.

Теперь рассмотрим разложение n-угольника $\boldsymbol{A}$ на его рациональные компоненты. Запишем $\boldsymbol{A}$ следующим образом:

$$\boldsymbol{A} = \sum_{d \| n} \varepsilon_d \boldsymbol{A} + \varepsilon_n \boldsymbol{A} = \boldsymbol{A}^* + \varepsilon_n \boldsymbol{A},$$

$$\text{где } \boldsymbol{A}^* = \sum_{d \| n} \varepsilon_d(\boldsymbol{A}) = (1-\varepsilon_n)\,\boldsymbol{A}. \tag{13}$$

Прежде всего представим себе, что для всякого собственного делителя d числа n построен периодический n-угольник $\mu_d \boldsymbol{A}$, вершинами которого являются центры тяжести хордовых d-угольников ($d\bar{d} = n$; теорема 1 гл. 4).

Компонента $\varepsilon_d \boldsymbol{A}$ при $d \neq n$ строится из таких собственно периодических n-угольников, а именно из $\mu_d \boldsymbol{A}$ и $\mu_t \boldsymbol{A}$, где t — собственный делитель d, для которого $\frac{d}{t}$ свободно от квадратов (см. теорему 7). Подобным же образом на основании формулы (11) строится n-угольник $\boldsymbol{A}^*$; $\boldsymbol{A}^*$ и его слагаемые $\varepsilon_d \boldsymbol{A}$ $(d \| n)$ принадлежат классу $\mathcal{A}_n^*$.

$\mathbf{Q}$-правильная компонента $\varepsilon_n \boldsymbol{A}$ не принадлежит классу $\mathcal{A}_n^*$ (если $\boldsymbol{A} \in \mathcal{A}_n^*$, то $\varepsilon_n \boldsymbol{A} = \boldsymbol{O}$) и не строится из собственных периодических n-угольников. Ее можно представить в виде разности $\boldsymbol{A} - \boldsymbol{A}^*$, что уже было сделано для $n = 6$ в теореме 6 гл. 5; $\boldsymbol{A}$ и $\boldsymbol{A}^*$ изобаричны, поэтому $\boldsymbol{A} - \boldsymbol{A}^*$ есть $\mathbf{Q}$-правильный n-угольник с центром тяжести $\boldsymbol{o}$.

Упражнения

1. Если n равно степени простого числа p, то дополнительным к центральному $\mathbf{Q}$-правильному классу является периодический класс, а именно класс p раз пройденных $\frac{n}{p}$-угольников.

2. Всякому свободному циклическому классу p^l-угольников $\mathcal{C}$ можно поставить в соответствие два свободных класса p^{l+1}-угольников: 1) класс p^{l+1}-угольников, хордовые p^l-угольники которых принадлежат $\mathcal{C}$, 2) класс p^{l+1}-угольников, хордовые p^l-угольники которых изобаричны и принадлежат $\mathcal{C}$. Всякий ли свободный циклический класс p^{l+1}-угольников можно при $K = \mathbf{Q}$ получить таким образом?

ГЛАВА 11

КОМПЛЕКСНЫЕ КОМПОНЕНТЫ n-УГОЛЬНИКА

§ 1. ω-n-угольники, правильные n-угольники

Пусть ω — некоторый корень n-й степени из 1, принадлежащий полю K ($\omega = 1$ всегда принадлежит полю K). Назовем *ω-n-угольником* такой n-угольник, в котором каждая следующая вершина получается из предыдущей умножением на ω:

$$(\boldsymbol{a},\ \omega\boldsymbol{a},\ \omega^2\boldsymbol{a},\ \ldots,\ \omega^{n-1}\boldsymbol{a}),\ \boldsymbol{a}\in V. \tag{1}$$

Если $\boldsymbol{a}\neq\boldsymbol{o}$, то все вершины n-угольника (1) принадлежат одномерному подпространству $K\boldsymbol{a}$ пространства V.

Если $\omega = 1$, то множество ω-n-угольников совпадает с классом тривиальных n-угольников. Если $\omega\neq 1$, то ω — корень многочлена $(x^n-1)/(x-1) = 1+x+x^2+\ldots$ $\ldots+x^{n-1}$, следовательно,

$$1+\omega+\omega^2+\ldots+\omega^{n-1}=0. \tag{2}$$

Отсюда видно, что при $\omega\neq 1$ всякий ω-n-угольник векторного пространства V имеет центр тяжести $\boldsymbol{o}$; действительно,

$$\frac{1}{n}(\boldsymbol{a}+\omega\boldsymbol{a}+\omega^2\boldsymbol{a}+\ldots+\omega^{n-1}\boldsymbol{a})=\boldsymbol{o} \tag{3}$$

для всех $\omega\neq 1$ и всех $\boldsymbol{a}\in V$.

Вместе с ω полю K принадлежит также ω^{-1}. Если вершины n-угольника (1) переписать в обратном порядке, то получится ω^{-1}-n-угольник и так можно получить каждый ω^{-1}-n-угольник. При $\omega\neq\pm 1$ только нулевой n-угольник $\boldsymbol{O}$ является одновременно ω-n-угольником и ω^{-1}-n-угольником.

ω-n-угольники образуют циклический класс, число степеней свободы которого равно 1. Он является атомарным классом, определенным простым делителем $x-\omega$.

Действительно, при $n \neq 1$ n-угольники (1) являются решениями циклической системы $\boldsymbol{a}_2 = w\boldsymbol{a}_1, \ldots$. При $n = 1$ множество w-n-угольников совпадает с множеством всех 1-угольников и утверждение остается справедливым (ср. § 3 гл. 6).

Если K содержит все корни n-й степени из 1, т. е. если $x^n - 1$ разлагается в $K[x]$ на линейные множители, то для всякого корня n-й степени из 1 имеется свой класс w-n-угольников и справедлива

Теорема 1. *Если поле K содержит все корни n-й степени из* 1, *то атомарными циклическими классами n-угольников являются классы w-n-угольников, где w пробегает все корни n-й степени из* 1 (см. § 3 гл. 6 или теорему 5 гл. 8).

Если к w-n-угольнику (1) прибавить произвольный тривиальный n-угольник, получим

$$(\boldsymbol{a} + \boldsymbol{b},\ w\boldsymbol{a} + \boldsymbol{b},\ \ldots,\ w^{n-1}\boldsymbol{a} + \boldsymbol{b}), \quad \boldsymbol{a},\ \boldsymbol{b} \in V. \tag{4}$$

Множество n-угольников вида (4) обозначим через $\mathscr{C}_w$. Тогда $\mathscr{C}_1$ — класс тривиальных n-угольников. При $w \neq 1$ класс $\mathscr{C}_w$ является свободным классом, соответствующим центральному классу w-n-угольников; он имеет степень свободы 2, определяется многочленом $(x-1)(x-w)$ и в булевой алгебре циклических классов является верхним соседним к классу тривиальных n-угольников.

Пусть теперь K содержит все корни n-й степени из 1. Тогда существует $\varphi(n)$ классов

$$\mathscr{C}_w, \text{ где } w \text{ — первообразный корень } n\text{-й степени из } 1. \tag{5}$$

Все n-угольники, принадлежащие классам (5), т. е. все n-угольники (4), мы назовем *правильными n-угольниками**). Правильными будем также называть все тривиальные n-угольники[1]). В нетривиальном правильном n-угольнике все вершины различны.

---

*) Ясно, что при $K = \mathscr{C}$ и $\dim V = 1$ (комплексная плоскость) $\mathscr{C}_w$ — это класс правильных n-угольников (в элементарно-геометрическом смысле; см. стр. 184, в частности, рис. 87).

[1]) Поскольку класс тривиальных n-угольников существует при любых n и K, имеет смысл называть их правильными также и в том случае, когда K не содержит всех корней n-й степени из 1.

Класс (5) единствен только в случае $\varphi(n)=1$, т. е. при $n=1$, 2. Класс $\mathscr{C}_1$ ($n=1$), соответственно $\mathscr{C}_{-1}$ ($n=2$), содержит все 1-угольники, соответственно 2-угольники, поэтому для всякого допустимого поля K любой 1- или 2-угольник является правильным. При этом случай $n=1$ является несколько особым, ибо из всех классов (5) только $\mathscr{C}_1$ при $n=1$ является атомарным; все остальные классы (5) при $n\neq 1$ содержат класс тривиальных n-угольников.

Множество правильных n-угольников, т. е. объединение циклических классов (5), вообще говоря, циклическим классом не является: действительно, сумма двух n-угольников из различных классов (5) не является правильным n-угольником. Оно является классом только при $n=1$, 2.

Сумма всех классов (5) определяется при $n\neq 1$ многочленом $(x-1)F_n(x)$ (теорема 5 гл. 8), а при $n=1$ — многочленом $x-1$. Отсюда следует, что сумма классов (5) является классом **Q**-правильных n-угольников; однако только при $n=1$, 2 всякий **Q**-правильный n-угольник является правильным n-угольником.

Следствие из теоремы 1. *Пусть K содержит все корни n-й степени из* 1. *Атомарными циклическими классами являются: класс тривиальных n-угольников* (при $n=1$ — единственный) *и, кроме того, при $n\neq 1$, $\varphi(n)$ классов правильных n-угольников с центром тяжести* $\boldsymbol{o}$ (в сумме они составляют центральный класс $\overset{\circ}{\mathscr{R}}_n$ **Q**-правильных n-угольников) *и классы $\frac{n}{d}$-кратно пройденных правильных d-угольников с центром тяжести* $\boldsymbol{o}$ (где d — *всевозможные нетривиальные* делители числа n).

Это следствие обосновывается следующими рассуждениями.

В любом из классов w-n-угольников для всякой точки $\boldsymbol{a}$ можно указать единственный n-угольник с началом $\boldsymbol{a}$. Если w — первообразный корень n-й степени из 1, то все классы теоремы 1 суть классы w^l-n-угольников, где $l\in\{1, 2, \ldots, n\}$.

Обозначим w^l-n-угольник с началом $\boldsymbol{a}$ через $\boldsymbol{A}_l(\boldsymbol{a})$ (так что $\boldsymbol{A}_1(\boldsymbol{a})$ — это исходящий из точки $\boldsymbol{a}$ w-n-угольник).

Тогда $\boldsymbol{A}_1(\boldsymbol{a})$ — правильный n-угольник. Если l взаимно просто с n, то w^l — тоже первообразный корень и $\boldsymbol{A}_l(\boldsymbol{a})$ — тоже правильный n-угольник; множество его вершин совпадает с $\boldsymbol{A}_1(\boldsymbol{a})$, только нумерация будет иной: условимся говорить, что $\boldsymbol{A}_l(\boldsymbol{a})$ получен из $\boldsymbol{A}_1(\boldsymbol{a})$ *l-хордовым обходом*[1]), где l взаимно просто с n. В общем же случае если w^l — первообразный корень d-й степени из 1 (где $d \mid n$), то $\boldsymbol{A}_l(\boldsymbol{a})$ есть $\frac{n}{d}$-кратно пройденный правильный d-угольник [т. е. w^l-d-угольник с началом $\boldsymbol{a}$]; при $d \neq n$ многоугольник $\boldsymbol{A}_l(\boldsymbol{a})$ будет собственно периодическим.

Многоугольник $\boldsymbol{A}_n(\boldsymbol{a}) = (\boldsymbol{a}, \boldsymbol{a}, \ldots, \boldsymbol{a})$ имеет центр тяжести $\boldsymbol{a}$. При $n \neq 1$ все n-угольники $\boldsymbol{A}_1(\boldsymbol{a}), \ldots, \boldsymbol{A}_{n-1}(\boldsymbol{a})$ (в том числе и многократно пройденные d-угольники) в силу (3) имеют центр тяжести $\boldsymbol{o}$.

Подведем итог сказанному:

Теорема 2. *Если $\boldsymbol{A}$ — правильный n-угольник, то всякий n-угольник, полученный из него l-хордовым обходом (где l взаимно просто с n), также является правильным. Если d — делитель n, то хордовый d-угольник правильного n-угольника $\boldsymbol{A}$ является правильным d-угольником; при $d \neq 1$ он имеет тот же центр тяжести, что и исходный $\boldsymbol{A}$.*

Упражнения

1. Среднее арифметическое n-угольников $\boldsymbol{A}_1(\boldsymbol{a}), \ldots, \boldsymbol{A}_n(\boldsymbol{a})$ есть n-угольник $(\boldsymbol{a}, \boldsymbol{o}, \ldots, \boldsymbol{o})$.

2. Обладают ли $\mathbf{Q}$-правильные n-угольники свойством, сформулированным в теореме 2?

3. Простое поле характеристики p, $p \nmid n$, содержит все корни n-й степени из 1 тогда и только тогда, когда $p \equiv 1 \bmod n$.

§ 2. Случай поля комплексных чисел

Если $K = \mathbf{C}$ — поле комплексных чисел, то для всякого n корни n-й степени из 1 имеют вид

$$w = e^{i\theta} = \cos\theta + i\sin\theta, \text{ где } \theta = \frac{2\pi}{n} l \quad (l = 1, 2, \ldots, n).$$

[1]) Пусть $\boldsymbol{A} = (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)$ и l — произвольное число. Образуем n-угольник $(\boldsymbol{a}_1, \boldsymbol{a}_{1+l}, \ldots, \boldsymbol{a}_{1+(n-1)l})$, где индексы у $\boldsymbol{a}_i$ берутся $\bmod n$, — именно этот n-угольник мы будем называть полученным из $\boldsymbol{A}$ *l-хордовым обходом*.

Всякое одномерное подпространство $\mathbf{C}\boldsymbol{a}$ в V, где $\boldsymbol{a} \neq \boldsymbol{o}$, представляет собой гауссову числовую плоскость. Отображение

$$\boldsymbol{x} \longrightarrow w\boldsymbol{x}$$

здесь представляет собой поворот вокруг нулевой точки $\boldsymbol{o}$ на угол θ. Каждая вершина w-n-угольника (1) получается из предыдущей вершины с помощью этого поворота. Следовательно, *правильные в нашем смысле n-угольники на гауссовой плоскости являются правильными n-угольниками в обычном* (евклидовом) *смысле* (рис. 87).

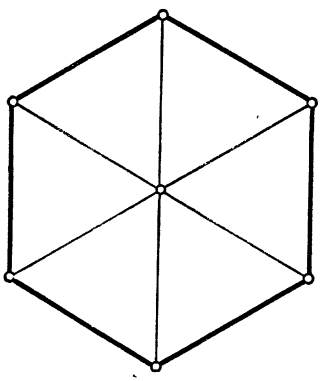


Рис. 87.

При $w = e^{i\theta}$, где $\theta = \frac{2\pi}{n}$, w-n-угольники суть обыкновенные правильные выпуклые n-угольники с положительным обходом вершин и центром тяжести $\boldsymbol{o}$ (см. рис. 88); w^{-1}-n-угольники — это те же n-угольники с обратным порядком обхода вершин. Они образуют новый циклический класс: при $n > 2$ оба эти класса правильных n-угольников различны; общим для них является только нулевой n-угольник. Если $\varphi(n) > 2$, то существуют еще и другие правильные n-угольники с центром тяжести $\boldsymbol{o}$, например при $n = 5$ класс пройденных в положительном (соответственно в отрицательном) направлении правильных пятиконечных звезд с центром тяжести $\boldsymbol{o}$ (рис. 89).

Всего над полем комплексных чисел существует n атомарных циклических классов n-угольников. Ими являются:

При $n=4$ — тривиальные 4-угольники; дважды пройденные 2-угольники $(a, -a, a, -a)$; квадраты $(a, ia,$

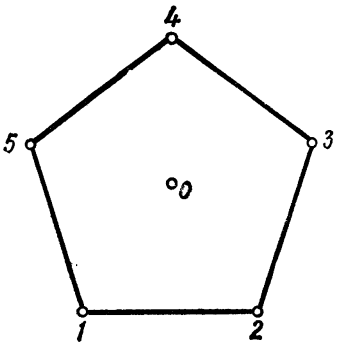


Рис. 88.

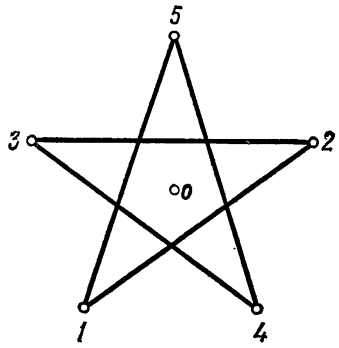


Рис. 89.

$-a, -ia)$; квадраты, пройденные в противоположном направлении.

При $n=5\left(\theta=\frac{2\pi}{5},\ w=e^{i\theta}\right)$ — тривиальные 5-угольники; правильные 5-угольники $(a, wa, \ldots, w^4a)$; правильные 5-угольники, пройденные в противоположном направлении; правильные звезды $(a, w^2a, w^4a, wa, w^3a)$; правильные звезды, пройденные в противоположном направлении.

При $n=6\left(\theta=\frac{2\pi}{6},\ w=e^{i\theta}\right)$ — тривиальные 6-угольники; трижды пройденные 2-угольники $(a, -a, \ldots, -a)$; дважды пройденные правильные 3-угольники $(a, w^2a, w^4a, a, w^2a, w^4a)$; правильные треугольники, дважды пройденные в противоположном направлении; правильные 6-угольники $(a, wa, \ldots, w^5a)$; правильные 6-угольники, пройденные в противоположном направлении.

§ 3. Комплексные компоненты n-угольника

Пусть, как и раньше, поле K содержит все корни n-й степени из 1. Всякий n-угольник $\boldsymbol{A}$ однозначно разлагается в сумму n-угольников из атомарных циклических классов, т. е. в силу теоремы 1 в сумму ω-n-угольников, где ω пробегает все корни n-й степени из 1. Слагаемое, соответствующее заданному корню ω, назовем *ω-компонентой* $\boldsymbol{A}$, а все эти слагаемые — *комплексными компонентами* $\boldsymbol{A}$.

Наша задача — найти комплексные компоненты n-угольника $\boldsymbol{A}=(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n)$. Запишем прежде всего очевидное равенство

$$(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n)=(\boldsymbol{a}_1, \boldsymbol{o}, \ldots, \boldsymbol{o})+(\boldsymbol{o}, \boldsymbol{a}_2, \ldots, \boldsymbol{o})+ \\ +(\boldsymbol{o}, \ldots, \boldsymbol{o}, \boldsymbol{a}_n). \qquad (6)$$

Поскольку сумма всех корней n-й степени из 1 при $n \neq 1$ равна 0 [см. (2)], имеем

$$(\boldsymbol{a}_1, \boldsymbol{o}, \ldots, \boldsymbol{o})=\sum_{\text{по всем } \omega} \frac{1}{n}(\boldsymbol{a}_1, \omega\boldsymbol{a}_1, \omega^2\boldsymbol{a}_1, \ldots, \omega^{n-1}\boldsymbol{a}_1). \qquad (7)$$

Тем самым n-угольник $(\boldsymbol{a}_1, \boldsymbol{o}, \ldots, \boldsymbol{o})$ представлен в виде суммы n-угольников из атомарных классов теоремы 1, а именно в виде суммы ω-n-угольников с началом в точке $\frac{1}{n}\boldsymbol{a}_1$; в силу однозначности атомарного разложения мы получили комплексные компоненты n-угольника $(\boldsymbol{a}_1, \boldsymbol{o}, \ldots, \boldsymbol{o})$. Аналогично

$$(\boldsymbol{o}, \boldsymbol{a}_2, \boldsymbol{o}, \ldots, \boldsymbol{o})=\sum_{\text{по всем } \omega} \frac{1}{n}(\omega^{n-1}\boldsymbol{a}_2, \boldsymbol{a}_2, \omega\boldsymbol{a}_2, \ldots, \omega^{n-2}\boldsymbol{a}_2),$$

где справа стоят комплексные компоненты n-угольника $(\boldsymbol{o}, \boldsymbol{a}_2, \boldsymbol{o}, \ldots, \boldsymbol{o})$, и т. д. В силу (6) достаточно сложить все эти разложения; при этом мы соберем все компоненты, относящиеся к одному корню ω; их сумма даст ω-n-угольник, а именно ω-n-угольник с началом

$$\frac{1}{n}(\omega^n\boldsymbol{a}_1+\omega^{n-1}\boldsymbol{a}_2+\ldots+\omega\boldsymbol{a}_n)=\frac{1}{n}\sum_{i=0}^{n-1}\omega^{-i}\boldsymbol{a}_{1+i}. \qquad (8)$$

Как известно, все остальные вершины этого ω-n-угольника получаются из его начала умножением соответственно на

w, w^2, ..., w^{n-1}. Тем самым мы полностью решили поставленную задачу. [Этот результат можно описать следующим образом. Запишем один под другим w^{-1}-n-угольники с началом $\boldsymbol{a}_i$, где $i=1, 2, \ldots, n$. Тогда центр тяжести точек, лежащих на главной диагонали этой таблицы, является первой вершиной (8) w-компоненты n-угольника $\boldsymbol{A}$. Остальные вершины этой компоненты получаются умножением первой последовательно на w, w^2, ..., w^{n-1}; они являются также центрами тяжести систем точек, лежащих на параллелях к главной диагонали.]

w-n-угольник с началом (8) является образом n-угольника $(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n)$ при циклическом отображении с n-набором коэффициентов $\frac{1}{n}(1, w^{-1}, w^{-2}, \ldots, w^{-(n-1)})$, т. е. (см. теорему 3 гл. 2) при циклическом отображении

$$e_w(\zeta) := \frac{1}{n}(1 + w^{-1}\zeta + w^{-2}\zeta^2 + \ldots + w^{-(n-1)}\zeta^{n-1}) = \frac{1}{n}\sum_{i=0}^{n-1} w^{-i}\zeta^i.$$

Сформулируем полученный результат:

Теорема 3. *Если поле K содержит все корни n-й степени из 1, то*

$$\boldsymbol{A} = \sum_{\text{по всем } w} e_w(\zeta)\,\boldsymbol{A}, \text{ где } e_w(\zeta) = \frac{1}{n}\sum_{i=0}^{n-1} w^{-i}\zeta^i,$$

является однозначным разложением произвольного n-угольника $\boldsymbol{A}$ на n-угольники из атомарных циклических классов.

Слагаемое $e_w(\zeta)\,\boldsymbol{A}$ является w-n-угольником, а $e_w(\zeta)$ — проекцией $\mathcal{A}_n$ на множество w-n-угольников.

Следствие. *Отображение $e_w(\zeta)$ проектирует множество всех n-угольников на класс w-n-угольников, являющийся атомарным циклическим классом, определенным многочленом $x-w$.*

Другими словами, $e_w(\zeta)$ являются атомарными циклическими проекциями. Это следствие можно взять за основу, проверив его непосредственным подсчетом (подобно двум первым утверждениям теоремы 1 гл. 4). Тогда из него

будет вытекать теорема 3. Однако, поскольку строение отображений $e_w(\zeta)$ само по себе представляет интерес, мы получим наше следствие из общих теорем гл. 8.

В гл. 8 указаны два пути нахождения циклической проекции, отображающей $\mathcal{A}_n$ на циклический класс, определенный многочленом $x-w$:

1) Для $t(x)=x-w$ отображение $e_t(\zeta)$ есть нужная нам проекция (см. формулу (15) гл. 8). Вычисление с помощью формулы, содержащей производную $t(x)$ (теорема 3 гл. 8), приводит к следующему результату:

$$e_w(x)=\frac{1}{n}\left(1+w^{-1}x+(w^{-1}x)^2+\ldots+(w^{-1}x)^{n-1}\right)=\frac{1}{n}\sum_{i=0}^{n-1}w^{-i}x^i.$$

Подстановка $x\longrightarrow\zeta$ дает искомую проекцию $e_w(\zeta)$.

2) По теореме 8а гл. 8 нужная нам проекция получается подстановкой ζ в многочлен из $K[x]$, равный 1 на w и 0 на остальных корнях n-й степени из 1.

Рассмотрим делитель многочлена x^n-1, дополнительный к $x-w$:

$$\frac{x^n-1}{x-w}=w^{-1}\left(1+(w^{-1}x)+(w^{-1}x)^2+\ldots+(w^{-1}x)^{n-1}\right).$$

Он равен нулю на всех корнях n-й степени из 1, отличных от w; если же подставить в него $x=w$, то он обращается в $w^{-1}n$. Поэтому достаточно поделить рассматриваемый многочлен на $w^{-1}n$ и произвести подстановку $x\longrightarrow\zeta$.

Заметим еще раз, что ненулевыми комплексными компонентами $\mathbf{Q}$-правильных n-угольников с центром тяжести $\boldsymbol{o}$ могут быть только правильные n-угольники с центром тяжести $\boldsymbol{o}$.

Пример. На гауссовой числовой плоскости (случай $V=K=\mathbf{C}$) *всякий параллелограмм с центром тяжести* $\boldsymbol{o}$ *однозначно представим в виде суммы двух квадратов с центром тяжести* $\boldsymbol{o}$, *проходимых в противоположных направлениях*. На рис. 90 $\boldsymbol{A}=(\boldsymbol{a}_1,\ \boldsymbol{a}_2,\ -\boldsymbol{a}_1,-\boldsymbol{a}_2)$ разлагается на i-компоненту $\boldsymbol{A}$:

$$\frac{1}{2}(\boldsymbol{a}_1-i\boldsymbol{a}_2,\ i\boldsymbol{a}_1+\boldsymbol{a}_2,\ -\boldsymbol{a}_1+i\boldsymbol{a}_2,\ -i\boldsymbol{a}_1-\boldsymbol{a}_2)$$

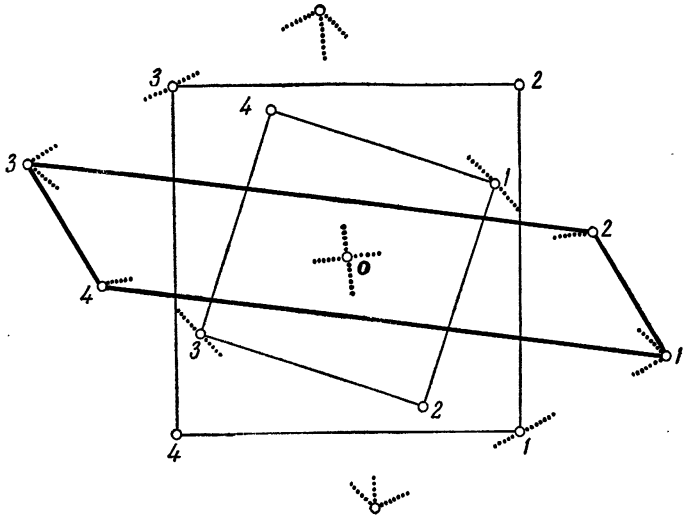


Рис. 90.

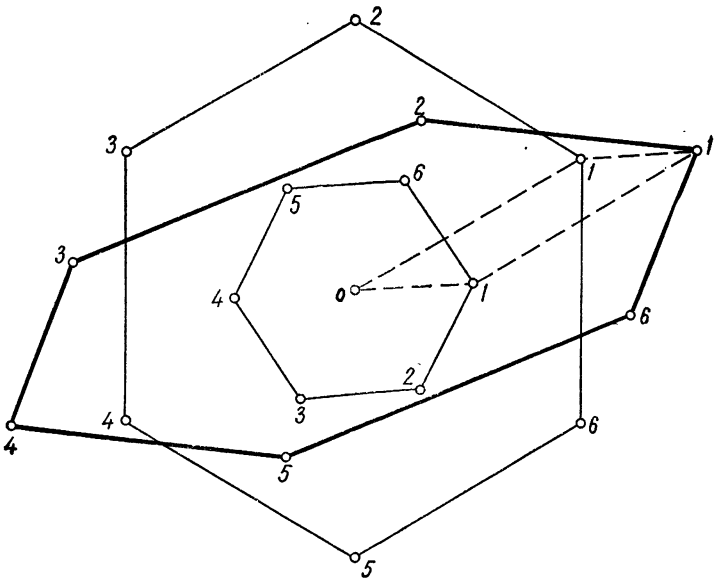


Рис. 91.

и $(-i)$-компоненту $\boldsymbol{A}$:

$$\frac{1}{2}(\boldsymbol{a}_1+i\boldsymbol{a}_2,\ -i\boldsymbol{a}_1+\boldsymbol{a}_2,\ -\boldsymbol{a}_1-i\boldsymbol{a}_2,\ i\boldsymbol{a}_1-\boldsymbol{a}_2).$$

Аналогично всякий 3-угольник с центром тяжести $\boldsymbol{o}$ однозначно представим в виде суммы двух проходимых в противоположных направлениях правильных 3-угольников с центром тяжести $\boldsymbol{o}$; всякий аффинно-правильный 6-угольник с центром тяжести $\boldsymbol{o}$ — в виде суммы двух проходимых в противоположных направлениях правильных 6-угольников с центром тяжести $\boldsymbol{o}$ (рис. 91).

Упражнения

1. Как специализируется разложение параллелограмма на два квадрата с тем же центром тяжести, если этот параллелограмм является ромбом?

2. Для каких n все комплексные компоненты n-угольника на гауссовой числовой плоскости можно построить циркулем и линейкой?

3. Пусть K содержит все корни n-й степени из 1. Эти корни являются собственными значениями эндоморфизма ζ пространства $\mathcal{A}_n$; класс w-n-угольников — собственным подпространством, отвечающим собственному значению w (множеством n-угольников $\boldsymbol{A}$, для которых $\zeta\boldsymbol{A}=w\boldsymbol{A}$); атомарное разложение $\mathcal{A}_n$ — разложением на собственные подпространства эндоморфизма ζ; $e_w(\zeta)$ является проекцией $\mathcal{A}_n$ на соответствующее корню w собственное подпространство.

4. Всякое циклическое отображение $f(\zeta)$ действует на классы w-n-угольников как растяжение (гомотетия) с коэффициентом $f(w)$.

ГЛАВА 12

ВЕЩЕСТВЕННЫЕ КОМПОНЕНТЫ n-УГОЛЬНИКА

§ 1. Симметрические циклические классы

В векторном пространстве n-угольников рассмотрим отображение

$$\boldsymbol{A}=(\boldsymbol{a}_1,\ \boldsymbol{a}_2,\ \ldots,\ \boldsymbol{a}_n)\to\boldsymbol{A}^*=(\boldsymbol{a}_1,\ \boldsymbol{a}_n,\ \ldots,\ \boldsymbol{a}_2), \qquad (1)$$

которое всякому n-угольнику $\boldsymbol{A}$ ставит в соответствие n-угольник $\boldsymbol{A}^*$ с тем же началом, но с противоположным порядком обхода вершин.

Очевидно, что отображение (1) является инволютивным линейным отображением $\mathcal{A}_n$ на себя:

$$\boldsymbol{A}^{**}=\boldsymbol{A},\ (\boldsymbol{A}+\boldsymbol{B})^*=\boldsymbol{A}^*+\boldsymbol{B}^*,\ (c\boldsymbol{A})^*=c\boldsymbol{A}^*.$$

Далее, $(\zeta\boldsymbol{A})^*=\zeta^{-1}\boldsymbol{A}^*$, откуда следует, что для любого циклического отображения $f(\zeta)$

$$(f(\zeta)\,\boldsymbol{A})^*=f(\zeta^{-1})\,\boldsymbol{A}^*. \qquad (2)$$

Если $\boldsymbol{A}$ принадлежит циклическому классу, являющемуся ядром отображения $f(\zeta)$, то $\boldsymbol{A}^*\in\operatorname{Ker}f(\zeta^{-1})$ (и обратно), т. е. отображение (1) переводит всякий циклический класс снова на циклический класс.

Условимся называть *симметрическими* [1]) те циклические классы, которые переводятся в себя отображением (1); другими словами, циклический класс является симметрическим, если вместе с каждым n-угольником $\boldsymbol{A}$ он содержит также и n-угольник $\boldsymbol{A}^*$.

Имеет место

---

[1]) Симметрические циклические классы известны также под названием *циклических-антициклических* классов, так как вместе с n-угольником $\boldsymbol{A}$ каждый из них содержит все n-угольники, полученные из $\boldsymbol{A}$ как циклической, так и антициклической подстановкой.

Теорема 1. *Симметрические циклические классы n-угольников образуют булеву подалгебру булевой алгебры всех циклических классов n-угольников. Эта подалгебра содержит четыре основных класса; вместе с каждым свободным циклическим классом она содержит соответствующий ему центральный класс, и обратно.*

Последнее утверждение следует из теоремы 2 гл. 3.

Рассмотрим следующее отображение кольца $K[x]$ (определенное для многочленов $\neq 0$):

$$f(x) \longrightarrow f^*(x) = x^{\operatorname{Grad} f} f(x^{-1}). \tag{3}$$

Ясно, что $c^* = c$ для каждого $c \neq 0$ из K; $(f(x)\,g(x))^* = f^*(x)\,g^*(x)$. Многочлен $f(x)$ называется *симметрическим*, если $f^*(x) = f(x)$, и *кососимметрическим*, если $f^*(x) = -f(x)$.

1°. *Если $f^*(x)$ ассоциирован с $f(x)$, то $f(x)$ — симметрический или кососимметрический многочлен (и обратно).*

Доказательство. Пусть $f^*(x) = cf(x)$, где $c \neq 0$ и $c \in K$. Если $c_m \neq 0$ — старший коэффициент $f(x)$ и c_0 — его свободный член, то $c_0 = cc_m$, $c_m = cc_0$; следовательно, $c_m = c^2 c_m$ и $c = \pm 1$.

2°. *Отображение* (1) *переводит циклический класс* $\operatorname{Ker} f(\zeta)$ *на циклический класс* $\operatorname{Ker} f^*(\zeta)$.

Доказательство. Так как все степени ζ обратимы в $K[\zeta]$, то $f(\zeta^{-1})$ и $\zeta^{\operatorname{Grad} f} f(\zeta^{-1}) = f^*(\zeta)$ ассоциированы в $K[\zeta]$, а значит, имеют одинаковые ядра (см. теорему 5 гл. 6):

$$\operatorname{Ker} f(\zeta^{-1}) = \operatorname{Ker} f^*(\zeta).$$

Для доказательства следующей теоремы напомним о существовании изоморфизма структуры делителей многочлена $x^n - 1$ на булеву алгебру циклических классов n-угольников (теорема 5 гл. 8):

$$t(x) \longrightarrow \operatorname{Ker} t(\zeta). \tag{4}$$

Теорема 2. *Пусть $t(x) \mid x^n - 1$. Если многочлен $t(x)$ симметричен или кососимметричен, то класс* $\operatorname{Ker} t(\zeta)$ *симметричен, и обратно.*

Прежде всего заметим, что из $t(x) \mid x^n - 1$ следует $t^*(x) \mid x^n - 1$; в самом деле, если $x^n - 1 = t(x)\,\bar{t}(x)$, то $-(x^n-1) = (x^n-1)^* = t^*(x)\,\bar{t}^*(x)$.

Доказательство теоремы 2. В силу изоморфизма (4) $t(x)$ и $t^*(x)$ ассоциированы тогда и только тогда, когда $\operatorname{Ker} t(\zeta) = \operatorname{Ker} t^*(\zeta)$ (по поводу «только тогда» см. замечание выше), после чего теорема 2 следует из 1° и 2°.

Многочлен $x-1$ кососимметричен, и если $f(x)$ симметричен, то произведение $(x-1)f(x)$ кососимметрично. Если $\operatorname{Char} K \neq 2$, то каждый кососимметрический многочлен можно получить из симметрического умножением на $x-1$.

3°. *Если* $\operatorname{Char} K \neq 2$, *то множество кососимметрических многочленов совпадает с множеством многочленов вида* $(x-1)f(x)$, *где* $f(x)$ *—симметрический многочлен.*

Доказательство. Для любого многочлена $g(x)$ имеем $g^*(1) = g(1)$. Если $g(x)$ кососимметричен, то, кроме того, $g(1) = -g(1)$; следовательно, $g(1) = 0$ при $\operatorname{Char} K \neq 2$, т. е. $g(x)$ делится на $x-1$: $g(x) = (x-1)f(x)$. Из $g^*(x) = -g(x)$ следует, что $(x-1)^* f^*(x) = -(x-1)f(x)$, откуда $f^*(x) = f(x)$.

4°. *Многочлен*

$$P_n(x) = \frac{x^n - 1}{x-1} = 1 + x + \ldots + x^{n-1}$$

не имеет кососимметрических делителей.

Доказательство. $P_n(1) = n \cdot 1 \neq 0$. Отсюда следует, что ни $P_n(x)$, ни его делители не делятся на $x-1$. Если $\operatorname{Char} K \neq 2$, то в силу 3° $P_n(x)$ не имеет кососимметрических делителей. Если же $\operatorname{Char} K = 2$, то всякий кососимметрический многочлен одновременно является симметрическим, что тоже позволяет условно считать наше утверждение справедливым.

Следствие теоремы 2. *Симметрические делители многочлена* $P_n(x)$ *определяют симметрические центральные классы; они же, умноженные на* $x-1$, *определяют свободные симметрические классы.*

Доказательство. Симметрические центральные классы содержатся в нуль-изобарическом классе. Так как последний определяется многочленом $P_n(x)$ (см. § 4 гл. 8), то симметрические центральные классы определяются симметрическими или кососимметрическими делителями $P_n(x)$ (теорема 2). В силу 4° можно считать эти делители симметрическими.

Если многочлен $t(x)$ — симметрический делитель $P_n(x)$ и $\mathscr{C}$ — определенный им симметрический центральный класс, то $(x-1)\,t(x)$ — многочлен, определяющий соответствующий свободный класс $\mathscr{C}$ (§ 4 гл. 8). По теореме 1 класс $\mathscr{C}$ тоже симметричен.

Пример. Многочлены деления круга $F_d(x)$, где $d \mid n$, симметричны при $d \neq 1$ (см. приложение I); многочлен $F_1(x)$ кососимметричен. Над полем рациональных чисел $\mathbf{Q}$ эти многочлены определяют атомарные циклические классы. В силу теоремы 2 они симметричны. Отсюда следует (теорема 1), что симметричны все циклические классы над $\mathbf{Q}$.

Упражнения

1. Пусть $n \neq 1, 2$ и w — принадлежащий K первообразный корень n-й степени из 1. Класс w-n-угольников отображением (1) переводится в класс w^{-1}-n-угольников; при $n \neq 1, 2$ классы правильных n-угольников не являются симметрическими.

2. На гауссовой числовой плоскости $\mathbf{Q}(i)$ из 16 циклических классов 4-угольников только 8 симметрических; эти классы определены и над $\mathbf{Q}$.

3. Если Char $K \neq 2$, то симметрические делители $x^n - 1$ определяют центральные симметрические классы, кососимметрические делители $x^n - 1$ определяют свободные симметрические классы.

§ 2. Специальный тип циклических систем уравнений

Имея в виду возможность разложения векторного пространства n-угольников на симметрические циклические классы (в общем случае такая возможность существует только над специальными полями), рассмотрим в этом и следующем параграфах симметрические циклические

классы n-угольников минимальной степени, а именно:

Класс тривиальных n-угольников и симметрические центральные классы степеней 1 и 2. (5)

Класс тривиальных n-угольников — это единственный свободный циклический класс степени 1; он симметричен. При четном $n=2m$ существует центральный симметрический класс степени 1; это $\mathcal{A}_{2,m}^{\circ}$ — класс m-кратно пройденных 2-угольников с центром тяжести $\boldsymbol{o}$. Этот класс определяется многочленом $x+1$. Других симметрических классов степени 1 не существует.

Из классов (5) подробного изучения заслуживают только симметрические центральные классы степени 2. Они могут существовать лишь при $n \geqslant 3$ и определяются квадратичными симметрическими делителями многочлена $P_n(x)$, т. е. многочленами из $K[x]$ вида

$$x^2 - cx + 1 \mid P_n(x) \tag{6}$$

(см. следствие теоремы 2 и теорему 5 гл. 9).

В булевой алгебре симметрических циклических классов n-угольников все классы (5) атомарны [1]).

Пусть $n \geqslant 3$ и $x^2 - cx + 1$ — квадратичный симметрический многочлен в $K[x]$; пока не будем предполагать, что он делит $P_n(x)$. Его коэффициенты $(1, -c, 1, 0, \ldots, 0)$ определяют циклическую систему уравнений

$$\boldsymbol{a}_1 - c\boldsymbol{a}_2 + \boldsymbol{a}_3 = \boldsymbol{o}, \ldots. \tag{7}$$

Симметрический циклический класс, являющийся ее решением, обозначим через $\mathscr{C}(c)$: $\mathscr{C}(c) = \operatorname{Ker}(\zeta^2 - c\zeta + 1)$. Степень свободы этого класса $\leqslant 2$, принадлежащие ему n-угольники не более чем двумерны.

Система (7) имеет следующий геометрический смысл: *существует такое $c \in K$, что сумма $\boldsymbol{a}_1$ и $\boldsymbol{a}_3$ равна c-кратной вершине $\boldsymbol{a}_2$, сумма $\boldsymbol{a}_2$ и $\boldsymbol{a}_4$ равна c-кратной вершине $\boldsymbol{a}_3$*

[1]) Симметрический центральный класс степени 1 существует, как мы уже отмечали, лишь при $n=2m$; он определяется двучленом $x+1$ и не содержится ни в каком симметрическом центральном классе степени 2. Действительно, соотношение $x+1 \mid x^2 - cx + 1 \mid P_n(x)$ невозможно [из $x+1 \mid x^2 - cx + 1$ следует, что $c = -2$, но $x^2 + 2x + 1 = (x+1)^2$ не является делителем $P_n(x)$].

и т. д. Из нее следует, что все вершины n-угольника $(\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n) \in \mathscr{C}(c)$, начиная с третьей, можно выразить в виде линейной комбинации вершин $\boldsymbol{a}_1$ и $\boldsymbol{a}_2$. Для этого построим по числу c последовательность $\hat{c}_0, \hat{c}_1, \hat{c}_2, \ldots \in K$:

$$\hat{c}_0 = -1, \quad \hat{c}_1 = 0, \quad \hat{c}_{k+2} = -\hat{c}_k + c\hat{c}_{k+1} \quad (k \geqslant 0). \tag{8}$$

Из первых $n-2$ уравнений системы (7) вытекает, что

$$\boldsymbol{a}_k = -\hat{c}_{k-1}\boldsymbol{a}_1 + \hat{c}_k\boldsymbol{a}_2 \text{ для } k = 1, 2, \ldots, n. \tag{9}$$

Выразив $\boldsymbol{a}_{n-1}$ и $\boldsymbol{a}_n$ из (9), запишем два последних уравнения системы (7) в виде

$$\boldsymbol{a}_1 = -\hat{c}_n\boldsymbol{a}_1 + \hat{c}_{n+1}\boldsymbol{a}_2, \quad \boldsymbol{a}_2 = (\hat{c}_{n-1} + c)\boldsymbol{a}_1 - \hat{c}_n\boldsymbol{a}_2. \tag{10}$$

Если $\hat{c}_n = -1$ и $\hat{c}_{n+1} = 0$, то $\hat{c}_{n+k} = \hat{c}_k$ для всех $k \geqslant 0$. В этом случае мы будем говорить, что последовательность (8) является *периодической с периодом* n. Заметим, что при этом $\hat{c}_{n-1} = -c$.

Примеры последовательностей (8) для различных c:

$c = 2$: $-1, 0, 1, 2, 3, 4, \ldots$;
$c = -2$: $-1, 0, 1, -2, 3, -4, \ldots$;
$c = -1$: $-1, 0, 1, -1, 0, \ldots$;
$c = 0$: $-1, 0, 1, 0, -1, 0, \ldots$;
$c = 1$: $-1, 0, 1, 1, 0, -1, 0, \ldots$;

$\mathscr{C}(2)$ — класс тривиальных n-угольников;
$\mathscr{C}(-2)$ при $n = 2m$ — класс $\overset{\circ}{\mathscr{A}}_{2,m}$;
$\mathscr{C}(-1)$ при $n = 3$ — класс 3-угольников с центром тяжести $\boldsymbol{o}$;
$\mathscr{C}(0)$ при $n = 4$ — класс параллелограммов с центром тяжести $\boldsymbol{o}$;
$\mathscr{C}(1)$ при $n = 6$ — класс аффинно-правильных 6-угольников с центром тяжести $\boldsymbol{o}$.

Теорема 3. *Пусть* $n \geqslant 3$. *Система вида* (7) *может определять из ненулевых классов лишь класс тривиальных* n*-угольников и центральные симметрические классы степеней* 1 *и* 2. *Система* (7) *определяет центральный сим-*

метрический класс степени 2 *тогда и только тогда, когда последовательность* (8) *периодическая с периодом* n.

Доказательство. Свободный симметрический класс степени 2 существует только при четном $n=2m$ — это класс $\mathcal{A}_{2,m}$, определенный многочленом $(x-1)(x+1)$ (см. теорему 1). Очевидно, что он не может быть представлен циклической системой (7). Центральный симметрический класс степени 2 является классом $\mathcal{C}(c)$ тогда и только тогда, когда c удовлетворяет условию (6). Если (6) не выполняется, то $\mathcal{C}(c)$ — симметрический циклический класс степени <2, т. е. или нулевой класс $\mathcal{A}_{1,n}=\mathcal{C}$ (2) тривиальных n-угольников, или, при $n=2m$, класс $\mathcal{A}_{2,m}=\mathcal{C}$ (—2).

Второе утверждение теоремы 3: $\operatorname{Crad}\mathcal{C}(c)=2$ означает, что при любом выборе $\boldsymbol{a}_1$ и $\boldsymbol{a}_2$ система (7) разрешима. Так как $\boldsymbol{a}_3,\ldots,\boldsymbol{a}_n$ из первых $n-2$ уравнений выражаются через $\boldsymbol{a}_1$ и $\boldsymbol{a}_2$ по формуле (9), то с учетом этих уравнений последние два уравнения системы, т. е. уравнения (10), должны тождественно удовлетворяться при любых $\boldsymbol{a}_1$ и $\boldsymbol{a}_2$. Для этого необходимо и достаточно, чтобы в обеих частях этих уравнений коэффициенты при $\boldsymbol{a}_1$ и $\boldsymbol{a}_2$ совпадали, т. е. чтобы

$$1=-\hat{c}_n,\quad 0=\hat{c}_{n+1},\quad 0=\hat{c}_{n-1}+c,\quad 1=-\hat{c}_n. \tag{11}$$

[Если уравнения (10) выполняются при любых $\boldsymbol{a}_1$, $\boldsymbol{a}_2$, то они выполняются, в частности, при $\boldsymbol{a}_1\neq\boldsymbol{o}$, $\boldsymbol{a}_2=\boldsymbol{o}$ и при $\boldsymbol{a}_1=\boldsymbol{o}$, $\boldsymbol{a}_2\neq\boldsymbol{o}$, что приводит к равенствам (11); с другой стороны, если выполняются (11), то система (10) удовлетворяется при любых $\boldsymbol{a}_1$ и $\boldsymbol{a}_2$.] Равенства (11) означают, что последовательность (8) периодическая с периодом n.

Итак, утверждение, что c определяет симметрический центральный класс степени 2, эквивалентно условию (6), а оно в свою очередь — утверждению, что *элементу с соответствует периодическая последовательность* (8) *с периодом* n.

Таким образом, подобные периодические последовательности элементов из K оказываются тесно связанными с центральными симметрическими классами степени 2.

Упражнения

1. Пусть условие (6) выполняется. В поле разложения многочлена x^n-1 над K корнями x^2-cx+1 являются два взаимно обратных корня n-й степени из 1: w и w^{-1}; при этом $c=w+w^{-1}$ и $w\neq\pm 1$. Исходя из этого, докажите, что последовательность (8) — периодическая с периодом n.

2. Если последовательность (8) — периодическая с периодом n, то $\hat{c}_0+\hat{c}_1+\hat{c}_2+\ldots+\hat{c}_{n-1}=0$.

3. Для каких рациональных чисел c и для каких вещественных c последовательность (8) является периодической?

4. Пусть $c\in K$, пусть $\boldsymbol{a}_1$, $\boldsymbol{a}_2$ — линейно независимые элементы из V ($\dim V\geqslant 2$) и имеется рекуррентная последовательность $\boldsymbol{a}_k=-\boldsymbol{a}_{k-2}+c\boldsymbol{a}_{k-1}$ для $k=3, 4, \ldots$. Последовательность точек $\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3, \ldots$ является периодической с периодом n тогда и только тогда, когда такова же последовательность (8).

§ 3. Аффинно-правильные n-угольники

Аффинно-правильными центральными классами мы будем называть симметрические центральные классы степени $\leqslant 2$, содержащиеся в **Q**-правильном центральном классе $\mathring{\mathcal{R}}_n$. [Единственный аффинно-правильный центральный класс степени 0 — это нулевой класс; аффинно-правильный центральный класс степени 1 существует только при $n=2$: это $\mathring{\mathcal{A}}_2=\mathring{\mathcal{R}}_2$ — класс 2-угольников с центром тяжести $\boldsymbol{o}$.] Свободные классы, соответствующие аффинно-правильным центральным классам, назовем *свободными аффинно-правильными классами*. Назовем n-угольник *аффинно-правильным*, если он принадлежит аффинно-правильному классу.

Все аффинно-правильные n-угольники являются **Q**-*правильными*. Каждый такой n-угольник самое большее двумерен (т. е. расположен в плоскости). Все тривиальные n-угольники и все 1-, 2-, 3-угольники аффинно-правильны.

Поскольку **Q**-правильный центральный класс при $n\neq 1$ определяется n-м многочленом деления круга $F_n(x)$ (теорема 2 гл. 10), справедлива

Теорема 4. *Для $n\geqslant 3$ отличные от $\{\boldsymbol{O}\}$ аффинно-правильные центральные классы определяются квадратичными симметрическими делителями многочлена $F_n(x)$.*

Аффинно-правильными 4-угольниками являются параллелограммы; при $n=6$ наше новое определение совпадает

с введенным в гл. 1. В случаях $n=1, 2, 3, 4, 6$ всякий $\mathbf{Q}$-правильный n-угольник является аффинно-правильным.

Теорема 5. *Нетривиальные аффинно-правильные n-угольники над произвольным полем K (таким, что* Char $K \nmid n$) *существуют только при* $n=2, 3, 4, 6$.

Действительно, уже над полем рациональных чисел многочлен деления круга $F_n(x)$ неприводим и, следовательно, имеет квадратичные делители только тогда, когда он сам квадратичен, т. е. когда $\varphi(n)=2$.

Если K содержит все корни n-й степени из 1, то квадратичный симметрический делитель $F_n(x)$ со старшим коэффициентом 1 имеет вид

$$x^2-(w+w^{-1})x+1=(x-w)(x-w^{-1}) \tag{12}$$

(w — первообразный корень n-й степени из 1).

Отсюда с учетом изоморфизма (4) следует

Теорема 6. *Если K содержит все корни n-й степени из* 1, *то при $n \geqslant 3$ всякий аффинно-правильный n-угольник с центром тяжести $\mathbf{o}$ однозначно представим в виде суммы правильного w-n-угольника и правильного w^{-1}-n-угольника, где w — некоторый первообразный корень n-й степени из* 1.

Иллюстрацией к этой теореме может служить пример из § 3 гл. 11.

Лемма. *Пусть $n \geqslant 3$, $x^2-cx+1 \in K[x]$ — квадратичный симметрический делитель многочлена $F_n(x)$:*

$$x^2-cx+1 \mid F_n(x) \tag{13}$$

и $c_0, c_1, c_2, \ldots$ — последовательность элементов из K, определенная формулами

$$c_0=2,\ c_1=c,\ c_{k+2}=-c_k+cc_{k+1}\ (k \geqslant 0). \tag{14}$$

Тогда в $K[x]$

$$F_n(x)=\prod_{\substack{(k,\,n)=1,\\ k<n/2}}(x^2-c_k x+1). \tag{15}$$

Доказательство. В поле разложения x^n-1 над K элемент c имеет вид $c=w+w^{-1}$, где w — первообразный

корень n-й степени из 1. Положим

$$c'_k = w^k + w^{-k} \text{ при } k = 0,\ 1,\ 2,\ \ldots\ .$$

Тогда $c'_0 = 2$, $c'_1 = c$ и справедлива рекуррентная формула $c'_{k+2} = -c'_k + cc'_{k+1}$. Отсюда следует, что $c'_k = c_k$. Многочлен $F_n(x)$ равен произведению двучленов $x - w^k$, где $(k, n) = 1$. Так как $w^{-k} = w^{n-k}$ и из $(k, n) = 1$ следует $(n-k, n) = 1$, то сомножители $x - w^k$ и $x - w^{-k}$ входят в разложение многочлена $F_n(x)$ попарно. Лемма доказана.

Как показывает доказательство леммы, *последовательность* (14) *не может иметь меньший чем n период*, и если n четно ($n = 2m$), то $c_m = -2$. Кроме того, $c_k = c_{n-k}$. Из леммы следует

Теорема 7. *Пусть $n \geqslant 3$. Если многочлен $F_n(x)$ имеет один квадратичный симметрический делитель в $K[x]$, то он в этом кольце полностью разлагается в произведение квадратичных симметрических делителей. Таким образом, нетривиальные аффинно-правильные n-угольники над K существуют тогда и только тогда, когда $F_n(x)$ разлагается в $K[x]$ на квадратичные симметрические делители.*

Итак, при заданных $n \geqslant 3$ и K из существования одного ненулевого аффинно-правильного центрального класса следует существование $\frac{1}{2}\varphi(n)$ таких классов. Их сумма является центральным классом **Q**-правильных n-угольников.

Кроме того, из существования разложения (15) многочлена $F_n(x)$ следует существование аналогичного разложения многочленов $F_d(x)$ для всех делителей $d \neq 1$ числа n:

$$F_d(x) = \prod_{\substack{(k,\ n) = \frac{n}{d} \\ k < \frac{n}{2}}} (x^2 - c_k x + 1) \text{ для } d \mid n,\ d \geqslant 3 \qquad (16)$$

(случай $d = 2$ в доказательстве не нуждается), или, что то же самое, существование нетривиальных аффинно-правильных d-угольников (где $d \mid n$, $d \neq 1$).

Из сказанного следует, что лемма описывает способ, с помощью которого одному аффинно-правильному классу

ставится в соответствие некоторая последовательность циклических классов. Остановимся на этом подробнее.

Пусть $n \geqslant 3$ и $\mathscr{C}(c)$ — аффинно-правильный центральный класс, определенный квадратичным симметрическим делителем $x^2 - cx + 1$ многочлена $F_n(x)$. Построим последовательность циклических классов n-угольников

$$\mathscr{C}(c) = \mathscr{C}(c_1),\ \mathscr{C}(c_2),\ \ldots,\ \mathscr{C}(c_n), \tag{17}$$

где c_k удовлетворяют соотношениям (14). Здесь $\mathscr{C}(c_n) = \mathscr{C}(2) = \mathscr{A}_{1,n}$ — класс тривиальных n-угольников; при $n = 2m$ имеем $\mathscr{C}(c_m) = \mathscr{C}(-2) = \overset{\circ}{\mathscr{A}}_{2,m}$. За исключением этих двух случаев, $x^2 - c_k x + 1$ являются делителями многочлена $P_n(x) = \dfrac{x^n - 1}{x - 1}$ (см. доказательство леммы), и, следовательно, соответствующие классы $\mathscr{C}(c_k)$ являются симметрическими центральными классами степени 2. Так как $\mathscr{C}(c_k) = \mathscr{C}(c_{n-k})$, то при нечетном n различные классы (17) представлены набором $\mathscr{C}(c_1)$, $\mathscr{C}(c_2)$, ..., $\mathscr{C}(c_{(n-1)/2})$, $\mathscr{C}(c_n)$, а при четном n ($n = 2m$) — набором $\mathscr{C}(c_1)$, ..., $\mathscr{C}(c_m)$, $\mathscr{C}(c_n)$.

В силу теоремы 4 и леммы, *если* $(k, n) = 1$ (*и только в этом случае*), $\mathscr{C}(c_k)$ — *аффинно-правильный центральный класс.*

Если $k \neq n$ *и* $\dfrac{n}{(n, k)} = d$, *то класс* $\mathscr{C}(c_k)$ *состоит из* $\dfrac{n}{d}$*-кратно пройденных аффинно-правильных* d*-угольников с центром тяжести* $\boldsymbol{O}$ (действительно, $x^2 - c_k x + 1$ является делителем $F_d(x)$; см. (16) и лемму из § 4 гл. 8).

Для случаев $k = n$ и $k = m$, $n = 2m$ соответствующие классы уже указаны.

Выясним, какие геометрические соотношения существуют между классами (17). С этой целью рассмотрим n отображений $\mathscr{A}_n$ в себя:

$$\boldsymbol{A} = (\boldsymbol{a}_1,\ \boldsymbol{a}_2,\ \ldots,\ \boldsymbol{a}_n) \longrightarrow \boldsymbol{A}_k = (\boldsymbol{a}_1,\ \boldsymbol{a}_{1+k},\ \boldsymbol{a}_{1+2k},\ \ldots,\ \boldsymbol{a}_{1+n-k}), \tag{18}$$

где $k = 1, 2, \ldots, n$. Здесь $\boldsymbol{A}_1 = \boldsymbol{A}$, $\boldsymbol{A}_n = (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_1)$ — тривиальный n-угольник; все $\boldsymbol{A}_k$ имеют своим началом $\boldsymbol{a}_1$; $\boldsymbol{A}_k$ и $\boldsymbol{A}_{n-k}$ различаются между собой только направлением обхода: $\boldsymbol{A}_{n-k} = \boldsymbol{A}_k^*$. Многоугольник $\boldsymbol{A}_k$ получается из $\boldsymbol{A}$

k-хордовым обходом (см. примечание на стр. 183). Если k взаимно просто с n, то множество вершин n-угольника $\boldsymbol{A}_k$ совпадает с $\boldsymbol{A}$; если $(k, n) = \frac{n}{d}$, то $\boldsymbol{A}_k$ есть $\frac{n}{d}$-кратно пройденный хордовый d-угольник n-угольника $\boldsymbol{A}$.

Мы хотим показать, что *отображения* (18) *n-угольники аффинно-правильного центрального класса $\mathscr{C}(c)$ переводят в n-угольники класса $\mathscr{C}(c_k)$*. Предварительно докажем

Предложение. *Если выполнены все условия леммы, то*

$$x^2 - cx + 1 \mid x^{2k} - c_k x^k + 1 \text{ для всех } k = 1, 2, \ldots, n.$$

Доказательство. В поле разложения многочлена $x^n - 1$ над K квадратный трехчлен $x^2 - cx + 1$ имеет вид (12); $c_k = w^k + w^{-k}$; поэтому $w^{2k} - c_k w^k + 1 = 0$ и $w^{-2k} - c_k w^{-k} + 1 = 0$: корни w и w^{-1} многочлена $x^2 - cx + 1$ являются также корнями многочлена $x^{2k} - c_k x^k + 1$. Следовательно, наше предложение справедливо над некоторым расширением поля K; поэтому оно справедливо и в $K[x]$.

Из этого предложения следует, что класс $\mathscr{C}(c) = \operatorname{Ker}(\zeta^2 - c\zeta + 1)$ содержится в классе $\operatorname{Ker}(\zeta^{2k} - c_k\zeta^k + 1)$. Если $\boldsymbol{A} = (\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_n) \in \mathscr{C}(c)$, то $\boldsymbol{a}_1 - c_k\boldsymbol{a}_{1+k} + \boldsymbol{a}_{1+2k} = \boldsymbol{o}, \ldots$, а это означает, что $\boldsymbol{A}_k \in \mathscr{C}(c_k)$, что и требовалось доказать.

Итак, отображения $\boldsymbol{A} \longrightarrow \boldsymbol{A}_k$ ставят в соответствие аффинно-правильному n-угольнику $\boldsymbol{A}$ с центром тяжести $\boldsymbol{o}$ аффинно-правильные n-угольники с центром тяжести $\boldsymbol{o}$, многократно пройденные аффинно-правильные d-угольники с центром тяжести $\boldsymbol{o}$ (где d — нетривиальный делитель числа n) и (для $k = n$) тривиальный n-угольник. Если $\boldsymbol{A}$ принадлежит классу $\mathscr{C}(c)$, то его образы распределяются по классам $\mathscr{C}(c_k)$. В симметрическом классе $\mathscr{C}(c_k)$ вместе с $\boldsymbol{A}_k$ лежит также $\boldsymbol{A}_{n-k} = \boldsymbol{A}_k^*$.

Сформулируем полученные результаты в виде теоремы, аналогичной теореме 2 из гл. 11:

Теорема 8. *Если $\boldsymbol{A}$ — аффинно-правильный n-угольник, то все n-угольники, которые получаются из $\boldsymbol{A}$ k-хордовым обходом, где k взаимно просто с n, также являются аффинно-правильными. Если d — делитель n, то хордовые d-уголь-*

ники n-угольника $\boldsymbol{A}$ являются аффинно-правильными d-угольниками, которые при $d \neq 1$ имеют тот же центр тяжести[1]), *что и* $\boldsymbol{A}$.

Вернемся к разложению многочленов $F_n(x)$ на квадратичные симметрические делители. Если при $n \geqslant 3$ в $K[x]$ существует один квадратичный симметрический делитель $x^2 - cx + 1$ многочлена $F_n(x)$, то имеет место разложение

$$x^n - 1 = \begin{cases} (x-1) \prod\limits_{k=1}^{(n-1)/2} (x^2 - c_k x + 1) & \text{для нечетных } n; \\ (x-1)(x+1) \prod\limits_{k=1}^{m-1} (x^2 - c_k x + 1) & \text{для четных } n = 2m, \end{cases} \tag{19}$$

где c_k удовлетворяют соотношениям (14) [см. (15), (16) и формулу (8) из гл. 6; при $n = 1$, 2 разложение (19) тривиально; сомножители $x^2 - c_k x + 1$ определены только при $n \geqslant 3$]. Структурный изоморфизм (4) переводит (19) в следующее разложение пространства n-угольников $\mathcal{A}_n$:

$$\mathcal{A}_n = \begin{cases} \mathcal{A}_{1,n} \oplus \mathscr{C}(c_1) \oplus \mathscr{C}(c_2) \oplus \ldots \oplus \mathscr{C}(c_{(n-1)/2}) & \text{для нечетных } n; \\ \mathcal{A}_{1,n} \oplus \mathcal{A}_{2,m} \oplus \mathscr{C}(c_1) \oplus \mathscr{C}(c_2) \oplus \ldots \oplus \mathscr{C}(c_{m-1}) & \text{для четных } n = 2m. \end{cases} \tag{20}$$

Здесь все классы $\mathscr{C}(c_k)$ $\left(k = 1, 2, \ldots, \frac{n-1}{2}\right.$, соответственно $\left.\frac{n}{2} - 1\right)$ являются симметрическими центральными классами степени 2.

Итак, *в разложение* (20) *входят класс тривиальных n-угольников и симметрические центральные классы степеней* 1 *и* 2; *все они при* $n \geqslant 3$ *описываются системой типа* (7) (теорема 3).

Упражнение. Пусть $n \geqslant 3$ и $\mathscr{C}(c)$ — аффинно-правильный центральный класс. Образом $\mathscr{C}(c)$ при отображении $\boldsymbol{A} \to \boldsymbol{A}_k$ (соответственно $\boldsymbol{A} \to \boldsymbol{A}_{n-k}$) является $\mathscr{C}(c_k)$, $k = 1, 2, \ldots, n$.

[1]) Совпадение центров тяжести следует из $\mathbf{Q}$-правильности $\boldsymbol{A}$.

§ 4. Три крайних случая булевых алгебр циклических классов n-угольников

Пусть, как и прежде, n — натуральное число, K — некоторое поле и V — векторное пространство над ним, удовлетворяющее требованиям § 1 гл. 1. Обозначим через $L_n(K, V)$ булеву алгебру n-угольников из V [см. основную теорему § 2 гл. 6]; она изоморфна структуре делителей многочлена $x^n - 1$ в $K[x]$ [фундаментальный изоморфизм (4)]. Отсюда следует, что при фиксированном K все булевы алгебры $L_n(K, V)$ независимо от V изоморфны между собой. В частности, только от K зависит число атомарных классов алгебры $L_n(K, V)$, равное числу простых делителей $x^n - 1$ в $K[x]$. Обозначим его через $k_n(K)$. Тогда число циклических классов в $L_n(K, V)$ (тоже независимо от выбора V) равно $2^{k_n(K)}$.

Обозначим через $n_1, n_2, \ldots, n_{k_n(K)}$ степени простых делителей $x^n - 1$ в $K[x]$. Тогда

$$n = n_1 + n_2 + \ldots + n_{k_n(K)}. \tag{21}$$

[Так как $x - 1$ всегда делит $x^n - 1$, будем считать, что $n_1 = 1$, а при четном n, поскольку $x + 1 \mid x^n - 1$, и $n_2 = 1$.] В силу изоморфизма (4) и теоремы 5 гл. 9 числа $n_1, n_2, \ldots, n_{k_n(K)}$ являются также степенями свободы атомарных циклических классов в $L_n(K, V)$.

Для любого поля K $2^{\tau(n)}$ циклических классов, определенных всеми частичными произведениями, входящими в произведение

$$\prod_{d \mid n} F_d(x), \tag{22}$$

образуют булеву подалгебру $\overset{\circ}{L}_n(K, V) \subseteq L_n(K, V)$ (*всегда присутствующие циклические классы n-угольников*). Случай совпадения $\overset{\circ}{L}_n(K, V) = L_n(K, V)$ (минимальный случай) имеет место тогда и только тогда, когда (22) является разложением $x^n - 1$ на простые множители, т. е. когда

1) $k_n(K) = \tau(n)$.

Вообще,

$$\tau(n) \leqslant k_n(K) \leqslant n, \tag{23}$$

и максимальный случай

2) $k_n(K) = n$

имеет место тогда и только тогда, когда $x^n - 1$ в $K[x]$ разлагается на линейные множители. Равенство (21) принимает в случае 1) вид $n = \sum_{d \mid n} \varphi(d)$, а в случае 2) вид $n = 1 + 1 + \ldots + 1$. Вопрос о том, как выглядят в обоих случаях атомарные циклические классы, обсуждался в гл. 10 и 11.

Теперь появляется еще одна булева подалгебра $L_n^*(K, V)$ — подалгебра *симметрических циклических классов* n-угольников (теорема 1). Эти классы определяются симметрическими или кососимметрическими делителями многочлена $x^n - 1$ в $K[x]$ (теорема 2); поэтому их число не зависит от V. Если через $k_n^*(K)$ обозначить число атомарных циклических классов в $L_n^*(K, V)$, то общее число классов в этой подалгебре будет равно $2^{k_n^*(K)}$.

«Всегда присутствующие» циклические классы n-угольников симметричны (см. конец § 1): $\overset{\circ}{L_n}(K, V) \subseteq L_n^*(K, V)$. Отсюда следует, что $\tau(n) \leqslant k_n^*(K)$. Если k_n^* принимает наименьшее возможное значение $k_n^*(K) = \tau(n)$, то это означает, что многочлены деления круга $F_d(x)$ (где $d \mid n$) не имеют в $K[x]$ ни одного нетривиального симметрического или кососимметрического делителя. В этом случае $L_n^*(K, V) = \overset{\circ}{L_n}(K, V)$.

Число $k_n^*(K)$ принимает наибольшее возможное значение тогда и только тогда, когда $x^n - 1$ разлагается в $K[x]$ на симметрические и кососимметрические множители степеней 1 и 2. В этом случае равенство (21) принимает вид

$$n = \begin{cases} 1 + 2 + 2 + \ldots + 2 & \text{для нечетных } n; \\ 1 + 1 + 2 + \ldots + 2 & \text{для четных } n; \end{cases}$$

следовательно, $k_n^*(K) = 1 + \left[\frac{n}{2}\right]$. Это тот случай, о котором говорилось в конце § 3. В общем случае справедливо неравенство

$$\tau(n) \leqslant k_n^*(K) \leqslant 1 + \left[\frac{n}{2}\right]. \qquad (24)$$

При этом $L_n^*(K, V)$ является булевой подалгеброй алгебры $L_n(K, V)$, следовательно, $k_n^*(K) \leqslant k_n(K)$. Остановимся на случаях, когда $k_n^* = k_n$, т. е. когда *всякий циклический класс является симметрическим*. Очевидно, что для этого достаточно потребовать, чтобы симметрическими были атомарные классы в L_n. [В структуре делителей многочлена из $K[x]$ эквивалентным является условие, чтобы всякий делитель был симметрическим или кососимметрическим; для этого достаточно потребовать, чтобы такими были простые делители $x^n - 1$.]

Здесь мы также рассмотрим два крайних случая. Первый:

$$\tau(n) = k_n^*(K) = k_n(K) \text{ означает, что}$$

$$L_n^\circ(K, V) = L_n^*(K, V) = L_n(K, V)$$

и, следовательно, совпадает с уже знакомым случаем 1). Остается

3) $k_n(K) = k_n^*(K) = 1 + \left[\frac{n}{2}\right]$.

Если при любом n имеет место случай 1), то соответствующее поле K обладает следующим свойством: *всякий многочлен деления круга в нем неприводим*. Если при любом n имеет место случай 2), то *поле K содержит все корни любой степени из* 1. Если при любом n имеет место случай 3), то *поле K таково, что всякий многочлен деления круга, за исключением $F_1(x)$ и $F_2(x)$, разлагается на неприводимые квадратичные симметрические множители*. Мы хотим показать, что этим свойством обладают максимальные упорядоченные поля.

§ 5. Вещественные компоненты n-угольника

Лемма. *Упорядоченное поле не содержит никаких других корней из* 1, *кроме* 1 *и* -1.

Доказательство. Пусть K — упорядоченное поле. Нужно показать, что никакой многочлен $x^n - 1$ не имеет в K корней, отличных от 1 и -1. Пусть сначала n четно. Так как в разложении

$$x^n - 1 = (x-1)(x+1)(1 + x^2 + x^4 + \ldots + x^{n-2})$$

третий сомножитель положительно определен, то корнями x^n-1 в K являются только $+1$ и -1. Если n нечетно, то x^n-1 является делителем $x^{2n}-1$ и потому имеет не больше чем два корня: $+1$ и -1; но так как $(-1)^n-1=-1-1\neq 0$, то остается один корень $+1$.

Пусть теперь K — *максимальное упорядоченное поле*[1]). Тогда неприводимыми многочленами в $K[x]$ являются, как известно, линейные и знакоопределенные квадратичные многочлены. При $n\geqslant 3$ многочлены деления круга $F_n(x)$ не имеют делителей $x-1$ и $x+1$, поэтому в силу леммы разлагаются только на знакоопределенные квадратичные множители. Покажем, что они симметричны.

Пусть x^2-cx+d — такой делитель; тогда d является корнем n-й степени из 1. В силу леммы $d=1$ или -1. Если $d=-1$, то x^2-cx+d при $x=\pm 1$ принимает значения разных знаков ($\pm c$; очевидно, что $c\neq 0$), что противоречит знакоопределенности многочлена x^2-cx+d. Итак, $d=+1$ и x^2-cx+d симметричен. Отсюда следует, что разложение многочлена x^n-1 на простые множители имеет вид (19) (в обозначениях леммы из § 3), а разложение $\mathcal{A}_n$ на атомарные циклические классы имеет вид (20).

Сформулируем полученные результаты:

Теорема 9. *Пусть K — максимальное упорядоченное поле. Для заданного n над K, кроме класса тривиальных n-угольников, существует $\frac{n-1}{2}$, если n нечетно, и $\frac{n}{2}$, если n четно, атомарных циклических классов n-угольников. Эти классы состоят или из аффинно-правильных n-угольников с центром тяжести $\mathbf{o}$, или из $\frac{n}{d}$-кратно пройденных аффинно-правильных d-угольников с центром тяжести $\mathbf{o}$, где d пробегает множество всех нетривиальных делителей n. Все циклические классы n-угольников симметричны.*

Если K является полем вещественных чисел $\mathbf{R}$, то число c из леммы § 3 равно сумме двух взаимно обратных

[1]) См. Бурбаки [4]. Максимальные упорядоченные поля иначе называются вещественно-замкнутыми полями с их однозначно определенным упорядочением (см., например, Ван дер-Варден [5], ч I, гл. 9).

первообразных корней n-й степени из 1:

$$2\cos\frac{2\pi}{n}=e^{i\frac{2\pi}{n}}+e^{-i\frac{2\pi}{n}},$$

а c_k вычисляются по формуле

$$c_k=2\cos k\frac{2\pi}{n}\quad(k=0,\ 1,\ 2,\ \ldots).$$

Для $n=1,\ 2,\ 3,\ 4,\ 6$ разложение x^n-1 на простые множители, а значит, и разложение $\mathcal{A}_n$ на атомарные циклические классы над $\mathbf{R}$ и над $\mathbf{Q}$ совпадают. В этих случаях над $\mathbf{R}$ существуют только те циклические классы,

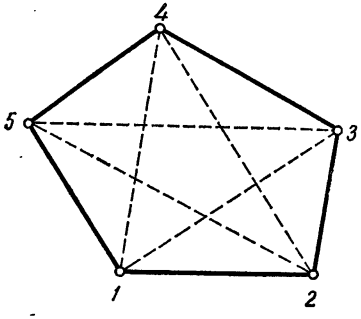


Рис. 92.

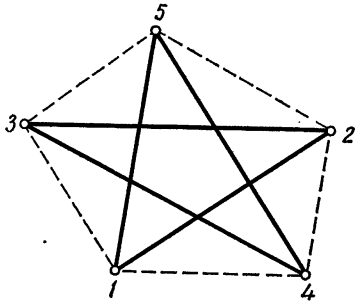


Рис. 93.

которые существуют над $\mathbf{Q}$. Для $n=5$ атомарными над $\mathbf{Q}$ являются класс тривиальных 5-угольников и класс всех 5-угольников с центром тяжести $\boldsymbol{o}$. Над $\mathbf{R}$ последний класс разлагается в прямую сумму двух атомарных аффинно-правильных центральных классов, определенных циклическими системами

$$\boldsymbol{a}_1-2\cos\frac{2\pi}{5}\boldsymbol{a}_2+\boldsymbol{a}_3=\boldsymbol{o},\ \ldots;\ \boldsymbol{a}_1-2\cos\frac{4\pi}{5}\boldsymbol{a}_2+\boldsymbol{a}_3=\boldsymbol{o},\ \ldots \tag{25}$$

(см. рис. 92 и 93).

В частности, *на вещественной аффинной плоскости* ($V=\mathbf{R}^2$) *всякий 5-угольник с центром тяжести* $\boldsymbol{o}$ *однозначно разлагается в сумму аффинно-правильного 5-уголь-*

ника с центром тяжести $\boldsymbol{o}$ *и аффинно-правильной 5-угольной звезды с центром тяжести* $\boldsymbol{o}$ (рис. 94).

Разложение (19), тривиальное при $n=1, 2$, при $n \geqslant 3$ существует над всяким полем K, удовлетворяющим условиям: $\operatorname{Char} K \nmid n$ и $F_n(x)$ разлагается в $K[x]$ на квадратичные симметрические множители x^2-cx+d, не обязательно простые. Тогда существует и разложение (20);

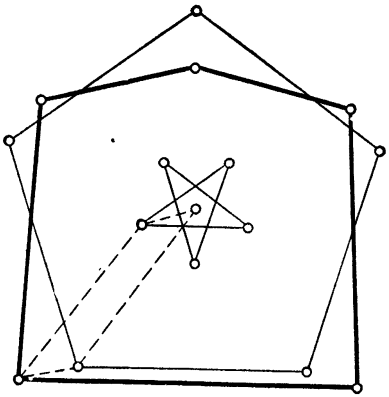


Рис. 94.

при этом слагаемые — класс тривиальных n-угольников и центральные симметрические классы степеней 1 и 2 — являются атомарными, вообще говоря только в булевой алгебре *симметрических* циклических классов n-угольников.

Назовем *вещественными компонентами* n-угольника $\boldsymbol{A}$ компоненты, входящие в классы разложения (20). При $n=1, 2$ рациональные, вещественные и комплексные компоненты n-угольника совпадают. При $n=3, 4, 6$ совпадают рациональные и вещественные компоненты.

Итак, *вещественными компонентами n-угольника являются аффинно-правильные n-угольники или многократно пройденные аффинно-правильные d-угольники, где* d *— собственный делитель* n; *кроме тривиального n-угольника центра тяжести, все остальные компоненты имеют центр тяжести* $\boldsymbol{o}$.

В связи с введенными в этой главе понятиями возникает ряд проблем. Например, было бы интересно выяснить соотношение между понятием аффинно-правильных n-угольников, введенным в § 3, и обычными аффинными образами правильных n-угольников. Но у всякой книги должен быть конец, и мы считаем возможным здесь остановиться.

Упражнения

1. Циклической проекцией, отображающей пространство $\mathcal{A}_n$ на циклический класс, определенный делителем x^2-cx+1 многочлена $F_n(x)$, является

$$\frac{1}{n}\sum_{k=0}^{n-1} c_k \zeta^k$$

(в предположениях леммы из § 3). Найдите циклические проекции, отображающие $\mathcal{A}_n$ на циклические классы, определенные делителями x^2-c_kx+1 многочлена x^n-1 $\left(\text{где } k=1, 2, \ldots, \left[\frac{n-1}{2}\right]\right)$.

2 (*косинус-многочлены*). Пусть K — поле, характеристика которого не делит n, и ω — первообразный корень n-й степени из 1, принадлежащий полю разложения многочлена x^n-1 над K. Если $K=\mathbf{R}$, то суммы

$$\omega^k+\omega^{-k}, \quad k=0, 1, \ldots, \left[\frac{n}{2}\right], \qquad (*)$$

равны $2\cos k\frac{2\pi}{n}$. Определим n-й косинус-многочлен $C_n(x)$ как многочлен со старшим коэффициентом 1, имеющий корнями значения (*). Легко проверить, что

$C_1(x)=x-2$, $C_2(x)=(x-2)(x+2)$,
$C_3(x)=(x-2)(x+1)$, $C_4(x)=(x-2)(x+2)x$,
$C_5(x)=(x-2)(x^2+x-1)$, $C_6(x)=(x-2)(x+2)(x+1)(x-1)$.

Вообще, n-й косинус-многочлен $C_n(x)$ для нечетных n представим в виде

$$C_n(x)=$$

$$=\frac{1}{2^{(n-1)/2}}(x-2)^{\left[\frac{j}{2}\right]}\sum_{j=0}^{(n-1)/2}\binom{\frac{n-1}{2}}{j}x^{\frac{n-1}{2}-j}(x+2)^{\left[\frac{j+1}{2}\right]},$$

а для четных n — в виде

$$C_n(x)=\frac{1}{2^{(n-2)/2}}(x-2)(x+2)\sum_{j=0}^{[(n-2)/4]}\binom{\frac{n}{2}}{2j+1}x^{\frac{n-2}{2}-2j}(x-2)^j\times$$

$$\times(x+2)^j.$$

Коэффициенты n-го косинус-многочлена $C_n(x)$ лежат в простом подполе поля K и в случае $\mathrm{Char}\,K=0$ целочисленны.

3 (Киндер). a) Отображение $f(\zeta)\to f(\zeta^{-1})$ является инволютивным автоморфизмом K-алгебры $K[\zeta]$.

b) Фиксированные элементы этого автоморфизма — назовем их *симметрическими циклическими отображениями* — образуют подалгебру $K[\eta]$ в $K[\zeta]$ ($\eta:=\zeta+\zeta^{-1}$). Ее ранг равен $1+\left[\frac{n}{2}\right]$.

c) Минимальный многочлен эндоморфизма η пространства V^n есть n-й косинус-многочлен $C_n(x)$: $K[\eta]\cong K[x]/(C_n(x))$.

d) Булева алгебра $(E(K[\eta]), 0, \cdot)$ идемпотентов из $K[\eta]$ является булевой подалгеброй булевой алгебры циклических проекций $(E(K[\zeta]), 0, \cdot)$.

e) Симметрические циклические классы n-угольников являются ядрами симметрических циклических отображений. Требование симметричности $\mathrm{Ker}\,f(\zeta)$ эквивалентно условию $f(\zeta)\sim f(\zeta^{-1})$ (теорема 5 гл. 6); идемпотентность $f(\zeta)$ эквивалентна идемпотентности $f(\zeta^{-1})$ (см. a)); ассоциированные идемпотенты равны (лемма из § 1 гл. 6).

f) Булева алгебра симметрических циклических классов n-угольников изоморфна структуре делителей многочлена $C_n(x)$.

Нетривиальные аффинно-правильные n-угольники существуют (при $n\neq 1$) тогда и только тогда, когда $C_n(x)$ разлагается на линейные множители.

4 (Киндер) (см. упр. 14 в гл. 9). Пусть w — первообразный корень n-й степени из 1 в некотором расширении поля K. Покажите, что

a) все циклические классы n-угольников симметричны тогда и только тогда, когда w и w^{-1} сопряжены над K. [Это не всегда так; например, это не так при $n=8$ и $K=\mathbf{Q}(i)$]

b) Если n есть степень некоторого нечетного простого числа, то все циклические классы n-угольников симметричны тогда и только тогда, когда $[w:K]$ четно (см. приложение I, § 1, упр. 2).

5 (α-n-угольники). Пусть n, K и V — натуральное число, поле и векторное пространство над ним, удовлетворяющие требованиям § 1 гл. 1. Будем интерпретировать $\mathcal{A}_n$ как $\mathrm{End}(V)$-модуль. Всякий эндоморфизм β пространства V индуцирует линейное отображение $\mathcal{A}_n$ в себя:

$$\beta(a_1, a_2, \ldots, a_n)=(\beta a_1, \beta a_2, \ldots, \beta a_n).$$

Если $\mathcal{C}$ — циклический класс n-угольников, то

$$\mathrm{End}(V)\,\mathcal{C}=\mathcal{C}.$$

Если $\dim V \geqslant \operatorname{Grad} \mathscr{C}$, то существует n-угольник $\boldsymbol{A} \in \mathscr{C}$, такой, что

$$\operatorname{End}(V)\,\boldsymbol{A} = \mathscr{C}.$$

Ограничимся автоморфизмами α порядка n пространства V: $\alpha^n = 1$. Фиксируем такой автоморфизм и рассмотрим множество α-n-угольников

$$\mathscr{A}_\alpha = \{(a, \alpha a, \ldots, \alpha^{n-1}a) : a \in V\}.$$

Если $m(x) \in K[x]$ — минимальный многочлен автоморфизма α, то $m(x) \mid x^n - 1$ и

1°. $\mathscr{A}_\alpha \subseteq \operatorname{Ker} m(\zeta)$,

2°. $\operatorname{End}(V)\,\mathscr{A}_\alpha = \operatorname{Ker} m(\zeta)$.

Вообще говоря, не всякий циклический класс $\mathscr{C} = \operatorname{Ker} t(\zeta)$, где $t(x) \mid x^n - 1$, представим в виде 2°. Однако если $\dim V \geqslant n$ и $\mathscr{C}$ — свободный циклический класс, то существует автоморфизм α порядка n пространства V на себя, такой, что $\mathscr{C} = \operatorname{End}(V)\,\mathscr{A}_\alpha$. Можно ли в представлении 2° ограничиться идемпотентными эндоморфизмами V?

По аффинно-правильным n-угольникам см. Боттема [23]; по поводу содержания гл. 10—12 см. Киндер [24].

ПРИЛОЖЕНИЕ I

МНОГОЧЛЕНЫ ДЕЛЕНИЯ КРУГА

Э. Шмидт

§ 1. Корни из единицы

Пусть заданы натуральное число n и поле K, характеристика которого не делит n.

Элемент w некоторого расширения поля K называется *корнем n-й степени из* 1, если он является корнем многочлена $x^n - 1$.

В силу предположения относительно характеристики поля K многочлен $x^n - 1$ и его производная $n \cdot x^{n-1}$ взаимно просты. Отсюда следует, что многочлен $x^n - 1$ свободен от квадратов и не имеет кратных корней ни в каком расширении поля K (ср. с теоремой 3 гл. 6.)

Таким образом, поле разложения $x^n - 1$ над K имеет ровно n различных корней n-й степени из 1. Они образуют группу относительно умножения. Эта группа как конечная подгруппа мультипликативной группы поля является циклической [1]). Каждый порождающий ее элемент называется *первообразным* корнем n-й степени из 1. Если w — первообразный корень n-й степени из 1, то все элементы

$$w,\ w^2,\ \ldots,\ w^{n-1},\ w^n = 1$$

являются корнями n-й степени из 1; при этом w^l тогда и только тогда является первообразным корнем, когда $(l, n) = 1$. Число первообразных корней n-й степени из 1 равно значению функции Эйлера $\varphi(n)$, которая определяется как *число взаимно простых* с n *натуральных чисел, меньших* n.

В циклической группе корней n-й степени из 1 всякий элемент имеет порядок, равный некоторому делителю d числа n, и, следовательно, является первообразным корнем

---

[1]) См. Артин [1], теорема 26.

d-й степени из 1. Таким образом, и множество корней n-й степени из 1 состоит из первообразных корней d-й степени из 1, где d пробегает все делители числа n.

Поле разложения $x^n - 1$ над простым полем характеристики 0 (или характеристики p, где p — простое число, не делящее n) называется n-м *полем деления круга* характеристики 0 (соответственно характеристики p).

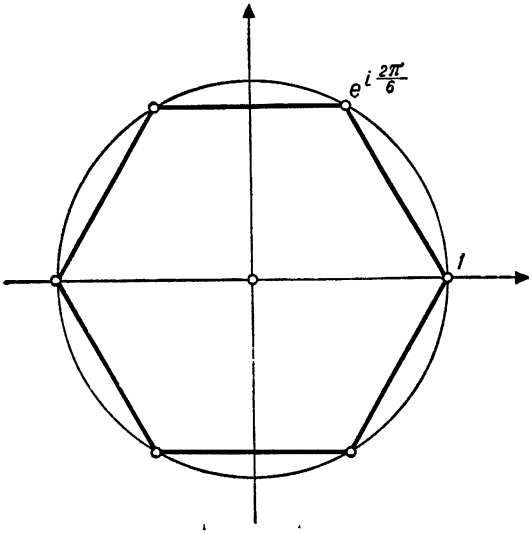


Рис. 95.

Оно получается из исходного простого поля присоединением к нему первообразных корней n-й степени из 1.

Поле *комплексных* чисел при любом n содержит все корни n-й степени из 1. Первообразным корнем n-й степени из 1 является число

$$w = e^{\frac{2\pi i}{n}}.$$

На гауссовой числовой плоскости все корни n-й степени из 1: w, w^2, ..., w^{n-1}, $w^n = 1$ располагаются в вершинах правильного n-угольника, вписанного в окружность радиуса 1 (рис. 95).

Упражнения

1. Сумма всех корней n-й степени из 1 при $n \neq 1$ равна 0; сумма первообразных корней n-й степени из 1 равна $-\mu(n)$, где μ — *функция Мёбиуса* (см. стр. 216). Произведение корней n-й степени из 1 равно $(-1)^{n+1}$, произведение первообразных корней n-й степени из 1 равно -1 при $n=2$ и $+1$ при $n \neq 2$.

2. Если простое число p является характеристикой поля K и $n=mp$, то $x^n-1=(x^m-1)^p$ и всякий корень n-й степени из 1 является корнем m-й степени из 1.

§ 2. Многочлены деления круга

Сохраним предположение о том, что $\operatorname{Char} K \nmid n$. Под *$n$-м многочленом деления круга* мы будем понимать многочлен со старшим коэффициентом 1, корнями которого являются первообразные корни n-й степени из 1, т. е. многочлен

$$F_n(x)=\prod_{w}(x-w)$$ (w пробегает множество всех первообразных корней n-й степени из 1).

Степень n-го многочлена деления круга равна $\varphi(n)$, и пока он определен лишь над полем разложения многочлена x^n-1.

Так как множество всех корней из 1 состоит из первообразных корней степени d, где d пробегает множество всех делителей n, а первообразные корни d-й степени являются корнями d-го многочлена деления круга, то

$$x^n-1=\prod_{d \mid n} F_d(x). \qquad (1)$$

Формула (1) однозначно определяет $F_n(x)$. Из нее прежде всего следует, что $F_1(x)=x-1$. Если известны $F_d(x)$ для всех $d \| n$, то многочлен $F_n(x)$ можно получить из этой формулы, применяя обычный алгоритм деления целочисленных многочленов. Отсюда следует, что коэффициенты $F_n(x)$ при любом n принадлежат простому подполю поля K и целочисленны, если $\operatorname{Char} K=0$. Поэтому эти многочлены можно рассматривать над простыми полями.

Над полем рациональных чисел многочлены деления круга неприводимы[1]: представление (1) является разложением многочлена x^n-1 на неприводимые сомножители.

[1]) См., например, Ван-дер-Варден [5], ч. I, § 53.

Примеры.

$$F_1(x) = x - 1, \qquad F_2(x) = x + 1,$$
$$F_3(x) = x^2 + x + 1, \qquad F_4(x) = x^2 + 1,$$
$$F_5(x) = x^4 + x^3 + x^2 + x + 1, \qquad F_6(x) = x^2 - x + 1.$$

Гомоморфизм $\mathbf{Z}$ на $\mathbf{Z}/(p)$ (p — простое число, не делящее n), продолженный на соответствующие этим полям кольца многочленов, переводит n-й многочлен деления круга над полем рациональных чисел в n-й многочлен деления круга над простым полем характеристики p.

Пользуясь формулами обращения Мёбиуса[1]), можно получить из формул (1) следующее выражение для $F_n(x)$:

$$F_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}. \tag{2}$$

Здесь μ — функция Мёбиуса натурального аргумента, определенная следующим образом:

$$\mu(m) = \begin{cases} 1, & \text{если } m = 1, \\ (-1)^r, & \text{если } m \text{ есть произведение } r \text{ попарно} \\ & \text{различных простых делителей;} \\ 0, & \text{если } m \neq 1 \text{ не свободно от квадратов.} \end{cases}$$

Пример. Если p — простое число, то

$$x^p - 1 = F_p(x) F_1(x)$$

и, значит,

$$F_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1.$$

Если n^* — свободное от квадратов ядро n (см. стр. 171; $1^* = 1$), то

$$F_n(x) = F_{n^*}(x^{n/n^*}). \tag{3}$$

Этот результат можно получить из формулы (2), приняв во внимание, что функция Мёбиуса не свободного от квадратов аргумента равна 0. Следовательно, многочлены деления круга достаточно определить для свободных от квадратов индексов.

---

[1]) Ср. выше, стр. 177; см., например, Хассе [18], § 4, 7 [или Виноградов [7]. — *Прим. ред.*].

Многочлены деления круга удовлетворяют следующим *рекуррентным соотношениям*:

$$F_{np}(x) = F_n(x^p), \text{ если } p \text{ — простое число и } p|n,$$
$$F_{np}(x) = \frac{F_n(x^p)}{F_n(x)}, \text{ если } p \text{ — простое число и } p \nmid n. \tag{4}$$

Доказательство. Запишем равенства (4) без дробей:
$F_{np}(x) = F_n(x^p)$ при $p|n$, $F_{np}(x) F_n(x) = F_n(x^p)$ при $p \nmid n$.
Левые и правые части этих равенств являются нормированными многочленами одинаковых степеней, имеющими одинаковые корни, а значит, совпадают.

Формулы (4) позволяют вычислять многочлены деления круга для любого n. Исходными в этих вычислениях являются многочлены

$$F_1(x) = x - 1, \quad F_p(x) = x^{p-1} + x^{p+2} + \ldots + x + 1.$$

Многочлен $F_1(x)$ кососимметричен, все остальные многочлены деления круга $F_n(x)$, $n \neq 1$, симметричны (см. § 1 гл. 12):

$$F_n(x) = x^{\varphi(n)} F_n(x^{-1}) \text{ при } n \neq 1. \tag{5}$$

Из (3) следует, что достаточно доказать (5) для свободных от квадратов n. Для простых p многочлены $F_p(x)$, очевидно, симметричны. Если $F_n(x)$ симметричен ($n \neq 1$) и p — простое число, не делящее n, то $F_{np}(x)$ симметричен как частное симметрических многочленов (см. (4)).

Значение n-го многочлена деления круга при $x = 1$ (сумма коэффициентов многочлена) *равно*

$$F_n(1) = \begin{cases} 0 \text{ при } n = 1, \\ p \text{ при } n = p^k \ (p \text{ простое}, \ k \neq 0), \\ 1 \text{ в остальных случаях.} \end{cases} \tag{6}$$

Согласно (3), достаточно ограничиться случаем свободного от квадратов n. При $n = 1$ и $n = p$ утверждение (6) очевидно. Далее, если (6) верно для $n \neq 1$, то в силу (4) при простом $q \nmid n$ имеем

$$F_{nq}(1) = \frac{F_n(1^q)}{F_n(1)} = 1,$$

что и требовалось доказать.

Вот еще одно соотношение для нечетных $n \neq 1$:

$$F_{2n}(x) = F_n(-x). \tag{7}$$

Согласно (3) и (4), это соотношение достаточно доказать для нечетных простых p:

$$F_{2p}(x) = \frac{(x^{2p}-1)(x-1)}{(x^p-1)(x^2-1)} = \frac{x^p+1}{x+1} =$$
$$= x^{p-1} - x^{p-2} + \ldots - x + 1 = F_p(-x).$$

Упражнения

1. Формулы (2) и (4) являются частными случаями соотношения

$$F_n(x) = \prod_{t|d} F_{n/d}^{\mu(d/t)}(x^t) \text{ для } d|n.$$

2. Докажите формулу (5), пользуясь представлением (2).

3. Вычислите значение n-го полинома деления круга $F_n(x)$ в точке $x = -1$.

4. n-й многочлен деления круга над m-м полем деления круга характеристики нуль неприводим тогда и только тогда, когда $(n, m)|2$.

§ 3. Теорема Редеи

Как всякий целочисленный многочлен, n-й многочлен деления круга порождает главный идеал в кольце $\mathbf{Z}[x]$. Справедлива следующая

Теорема[1]). *В кольце* $\mathbf{Z}[x]$ *главный идеал* $(F_n(x))$ *при* $n \neq 1$ *порождается многочленами* $F_p(x^{n/p})$, *где* p *пробегает все простые делители числа* n.

Ограничимся свободным от квадратов n [см. (3)]. Теорема доказывается индукцией по числу простых делителей числа n. Для простого n утверждение справедливо. Пусть $n = mp$, где $m \neq 1$ и p — простое число, не делящее m. Положим

$$f(x) = F_m(x^p) F_{mp}^{-1}(x) \text{ и } g(x) = F_p(x^m) F_{mp}^{-1}(x).$$

В силу (4), $f(x) = F_m(x) \in \mathbf{Z}[x]$ и

$$g(x) = \frac{x^{mp}-1}{(x^m-1) F_{mp}(x)} = \prod_{t \| m} F_{tp}(x) \in \mathbf{Z}[x].$$

[1]) См. Редеи [14]; Шёнберг [20].

Корнями многочлена $f(x)$ являются первообразные корни m-й степени из 1 u; корнями $g(x)$ — первообразные корни tp-й степени из 1 v; t пробегает все собственные делители числа m. Результант R многочленов $f(x)$ и $g(x)$ равен

$$R=\prod_{u,\,v}(v-u)=\prod_{u,\,v}(1-v^{-1}u).$$

R является единицей в кольце целых алгебраических чисел. Действительно, единицами являются v, $w=v^{-1}u$, как первообразные корни некоторой степени $d\neq 1$ из 1, и $1-w=1-v^{-1}u$, как показывает соотношение

$$(1-w)\prod_{\substack{(j,\,d)=1\\ j\neq 1}}(1-w^j)=F_d(1)=1.$$

С другой стороны, результант многочленов $f(x)$ и $g(x)$, как известно, представим в виде

$$R=F(x)f(x)+G(x)g(x),$$

причем коэффициенты многочленов $F(x)$ и $G(x)$ принадлежат тому же кольцу, что и коэффициенты $f(x)$ и $g(x)$ [1]). В нашем случае все многочлены целочисленны, поэтому $R\in\mathbf{Z}$, а из его обратимости следует, что $R=\pm 1$. Итак, в кольце $\mathbf{Z}[x]$

$$(1)=(f(x),\ g(x))$$

и, следовательно,

$$(F_{mp}(x))=(F_m(x^p),\ F_p(x^m)).$$

Отсюда по индукции доказывается окончательное утверждение теоремы.

Пример. Представление $F_n(x)$, соответствующее теореме Редеи, легко указать при $n=pq$, где p, q — различные простые числа. Найдутся числа $0<a<q$ и $0<b<p$, такие, что $1=ap-bq$. Тогда

$$F_{pq}(x)=\frac{x^{ap}-1}{x-1}F_{pq}(x)-\frac{x^{bq}-1}{x-1}xF_{pq}(x)=$$
$$=\frac{x^{ap}-1}{x^p-1}F_p(x^q)-\frac{x^{bq}-1}{x^q-1}xF_q(x^p).$$

Сомножители, стоящие перед многочленами деления круга, являются целочисленными многочленами.

[1]) См., например, Ван-дер-Варден [5], ч. I, § 27.

Упражнения

1. $F_6(x) = F_3(x^2) - xF_2(x^3)$, $F_{15}(x) = (x^3+1)F_3(x^5) - xF_5(x^3)$.

2. Коэффициенты многочлена $F_{pq}(x)$ (p, q — простые числа) равны 0 или ± 1. Определите число положительных и отрицательных коэффициентов этого многочлена.

3. Многочлен $F_{105}(x)$ является многочленом деления круга минимального индекса, в котором не все коэффициенты равны 0 или ± 1.

§ 4. Многочлены деления круга над простыми конечными полями

Пусть заданы натуральное число n и простое p, не делящее n. *Порядком числа p по модулю n* называется минимальное натуральное число l, для которого $p^l \equiv 1 \bmod n$ [обозначается $\operatorname{Ord}(p, n)$]. Согласно малой теореме Ферма, $\operatorname{Ord}(p, n) \mid \varphi(n)$.

Многочлены деления круга, неприводимые над простым полем характеристики 0, могут не обладать этим свойством над полями конечной характеристики.

Пример. Все $p-1$ отличных от нуля элементов простого поля характеристики p являются корнями $(p-1)$-й степени из 1. Отсюда следует, что над простым полем характеристики p всякий многочлен деления круга с индексом n, делящим $p-1$, разлагается на линейные множители. Так, для $p=7$

$$F_1(x) = x-1, \qquad F_2(x) = x-6,$$
$$F_3(x) = (x-2)(x-4), \qquad F_6(x) = (x-3)(x-5).$$

Условие «n делит $p-1$» означает, что $\operatorname{Ord}(p, n) = 1$. Вообще, справедлива

Теорема. *n-е поле деления круга характеристики p имеет над своим простым полем*[1]) *степень* $\operatorname{Ord}(p, n)$.

Доказательство. Пусть K есть n-е поле деления круга характеристики p и e — степень K над его простым подполем. Тогда K — конечное поле, содержащее p^e элементов. Мультипликативная группа любого поля из p^l элементов (l — натуральное число) является циклической

[1]) Ср. Редеи [15], § 135.

группой порядка p^l-1. Поле K является минимальным конечным расширением простого поля, таким, что его мультипликативная группа содержит подгруппу корней n-й степени из 1, имеющую порядок n. Известно, что конечная циклическая группа содержит подгруппу порядка n тогда и только тогда, когда ее порядок делится на n. Итак, p^e-1 — минимальное из чисел p^l-1, которые делятся на n, или e — минимальное из чисел l, таких, что $n \mid (p^l-1)$, т. е. $p^l \equiv 1 \bmod n$, а это означает, что $e = \operatorname{Ord}(p, n)$.

Из этой теоремы следует, что всякий первообразный корень n-й степени из 1 является алгебраическим элементом порядка $\operatorname{Ord}(p, n)$ над простым полем.

Следствие. *Над простым полем характеристики p n-й многочлен деления круга $F_n(x)$ является произведением попарно не ассоциированных неприводимых многочленов степени* $\operatorname{Ord}(p, n)$. *Число неприводимых сомножителей в разложении $F_n(x)$ равно* $\varphi(n)/\operatorname{Ord}(p, n)$.

Упражнения (Здесь рассматриваются многочлены деления круга над конечным простым полем характеристики p.)

1. $F_n(x)$ неприводим тогда и только тогда, когда $n=4$, q^k, $2q^k$ ($k \geqslant 0$; q — нечетное простое число) и p — первообразное *) по модулю n число.

2. При $p=2$: $F_7(x) = (x^3+x+1)(x^3+x^2+1)$,
при $p=13$: $F_7(x) = (x^2+3x+1)(x^2+5x+1)(x^2+6x+1)$,
при $p=17$: $F_9(x) = (x^2+3x+1)(x^2+4x+1)(x^2-7x+1)$,
при $p=3$: $F_8(x) = (x^2+x-1)(x^2-x-1)$,
при $p=11$: $F_{15}(x) = (x^2-2x+4)(x^2+4x+5)(x^2+5x+3) \times (x^2+3x-2)$.

3. Определите число неприводимых множителей многочлена $x^{12}-1$ при $p=5$, 7, 11.

*) То есть является по модулю n первообразным корнем из 1 степени $\varphi(n)$.

ПРИЛОЖЕНИЕ II

СТРУКТУРЫ

Г. Киндер

Множество L называется *структурой*[1]), если в нем определены две бинарные операции $\sqcup$ и $\sqcap$ (отображения $L\times L\longrightarrow L$) и бинарное отношение $\leqslant$ (подмножество $L\times L$), удовлетворяющие следующим аксиомам:

Аксиома 1 (*ассоциативность*): $(a\sqcup b)\sqcup c=a\sqcup(b\sqcup c)$, $(a\sqcap b)\sqcap c=a\sqcap(b\sqcap c)$.

Аксиома 2 (*коммутативность*): $a\sqcup b=b\sqcup a$, $a\sqcap b=b\sqcap a$.

Аксиома 3 (*поглощение*): $a\sqcup(a\sqcap b)=a$, $a\sqcap(a\sqcup b)=a$.

Аксиома 4: $a\leqslant b\langle\!=\!\rangle a\sqcap b=a$.

Примечание к аксиоме 4. Если для двух операций $\sqcup$ и $\sqcap$ в множестве L выполнены аксиомы 1, 2 и 3, то отношение $\leqslant$ можно определить при помощи аксиомы 4.

Аксиомам 1—4 эквивалентны следующие аксиомы:

Аксиома 1′ (*рефлексивность*): $a\leqslant a$.

Аксиома 2′ (*транзитивность*): $a\leqslant b\wedge b\leqslant c\Rightarrow a\leqslant c$.

Аксиома 3′ (*антисимметрия*): $a\leqslant b\wedge b\leqslant a\Rightarrow a=b$.

Аксиома 4′ (*максимум*): $a,\ b\leqslant c\langle\!=\!\rangle a\sqcup b\leqslant c$.

Аксиома 5′ (*минимум*): $c\leqslant a,\ b\langle\!=\!\rangle c\leqslant a\sqcap b$.

Мы приведем примеры структур и некоторые методы получения новых структур из заданных. Начнем с важнейшего примера, являющегося до некоторой степени прототипом всех структур:

1. Множество $\mathfrak{P}(M)$ всех подмножеств множества M с операциями $\cup$ и $\cap$ и отношением $\subseteq$.

---

[1]) Английское lattice, немецкое Verband.

2. Пусть $\mathfrak{C}$ — некоторое множество подмножеств из M ($\mathfrak{C} \subseteq \mathfrak{P}(M)$), замкнутое относительно операции пересечения, т. е. такое, что для всякого подмножества $\mathfrak{M} \subseteq \mathfrak{C}$

$$\bigcap \mathfrak{M} = \bigcap_{T \in \mathfrak{M}} T \in \mathfrak{C}.$$

Всякому подмножеству $A \subset M$ поставим в соответствие подмножество $\langle A \rangle \in \mathfrak{C}$ — пересечение всех подмножеств из $\mathfrak{C}$, содержащих A. Тогда $(\mathfrak{C}, \langle \cup \rangle, \cap, \subseteq)$ является структурой ($\langle \cup \rangle$ означает операцию $(T, U) \to \langle T \cup U \rangle$).

Следующие четыре примера 3—6 являются частными случаями примера 2.

3. Множество всех подгрупп некоторой группы.

4. Множество всех нормальных делителей некоторой группы. (В этой структуре $T \sqcup U = \langle T \cup U \rangle = T \cdot U$.)

5. Множество всех R-подмодулей некоторого R-модуля (R — кольцо). (Здесь $\langle T \cup U \rangle = T + U$.)

6. Множество $L(R)$ всех двусторонних идеалов некоторого кольца R. (Здесь $\langle T \cup U \rangle = T + U$.)

7. Множество $L(R) \setminus \{(0)\}$ всех отличных от нуля идеалов области целостности R с операциями $+$, $\cap$ и $\subseteq$.

8. Пусть R — кольцо главных идеалов, $L(R)$ — структура идеалов кольца R (пример 6). Рассмотрим отображение $a \to (a)$. Полным прообразом идеала $(a) = Ra$ является класс ассоциированных с a элементов Ua; через U обозначается группа обратимых элементов («единиц») кольца R. Соответствие $Ra \to Ua$ взаимно однозначно отображает структуру $L(R)$ на множество классов ассоциированных элементов. В последнем можно следующим образом ввести операции $\sqcup$, $\sqcap$, $\leqslant$: для произвольных a, $b \in R$ пусть $Ua \sqcup Ub$ — класс наибольшего общего делителя a и b; $Ua \sqcap Ub$ — класс наименьшего общего кратного a и b; $Ua \leqslant Ub$ означает, что a делится на b. Тогда указанное выше соответствие станет изоморфизмом структур.

9. Пусть $(K, \leqslant)$ — произвольное линейно упорядоченное множество, т. е. такое, что в нем выполняются аксиомы 1′, 2′, 3′ и для всяких двух элементов a, $b \in K$ справедливо одно из отношений $a \leqslant b$, $b \leqslant a$. Относительно операции $a \sqcup b = \max(a, b)$, $a \sqcap b = \min(a, b)$ и отношения $\leqslant$ множество K является структурой.

10. Структурой является множество $E(R)$ всех идемпотентных элементов коммутативного кольца R с операциями $a \sqcup b = a \circ b\,(= a+b-a\cdot b)$ и $a \sqcap b = ab$ (см. примечание к аксиоме 4; см. также § 1 гл. 5).

Пусть задана структура $(L, \sqcup, \sqcap, \leqslant)$. Определим отношение $\geqslant$ следующим образом:

$$a \geqslant b \langle\!=\!\rangle\, b \leqslant a.$$

Тогда $(L, \sqcap, \sqcup, \geqslant)$ также является структурой; она называется *двойственной* к исходной. Сформулируем *принцип двойственности* теории структур:

Если некоторое утверждение $\mathfrak{S}$ теории структур справедливо для всех структур, то справедливо также и двойственное к нему утверждение $\mathfrak{S}^*$, полученное из $\mathfrak{S}$ заменой $\sqcup$, $\sqcap$, $\leqslant$ соответственно на $\sqcap$, $\sqcup$, $\geqslant$.

Действительно, $\mathfrak{S}^*$ справедливо для всякой структуры $(L, \sqcup, \sqcap, \leqslant)$, так как $\mathfrak{S}$ справедливо для всякой структуры, в том числе и для $(L, \sqcap, \sqcup, \geqslant)$.

Пример.

11. Структура, двойственная к структуре примера 8, состоит из классов ассоциированных элементов с операциями НОК и НОД и отношением $|$ («делит»).

Пусть задано *семейство структур* $\mathfrak{C}$, т. е. отображение $i \longrightarrow \mathfrak{C}_i = (L_i, \sqcup_i, \sqcap_i, \leqslant_i)$ множества «индексов» I в множество структур. *Произведением структур* $\prod \mathfrak{C} = \prod\limits_{i \in I} \mathfrak{C}_i$ называется множество всевозможных отображений a множества I в объединение множеств $\bigcup\limits_{i \in I} L_i$, при которых $i \longrightarrow a_i \in L_i$. Произведение $\prod \mathfrak{C}$ является структурой относительно операций $\sqcup$, $\sqcap$ и отношения $\leqslant$, определенных следующим образом:

$$(a \sqcup b)_i = a_i \sqcup_i b_i,$$
$$(a \sqcap b)_i = a_i \sqcap_i b_i,$$
$$a \leqslant b \langle\!=\!\rangle\, \forall i \in I\colon a_i \leqslant_i b_i.$$

[Если I пусто $(I = \varnothing)$, то $\mathfrak{C} = \varnothing$; очевидно, что и $\bigcup\limits_{i \in I} L_i = \varnothing$, так что $\prod \mathfrak{C}$ состоит только из пустого отображения пустого множества в себя, и $\varnothing \sqcup \varnothing = \varnothing = \varnothing \sqcap \varnothing$, $\varnothing \leqslant \varnothing$.]

Пример.

12. Пусть $\mathfrak{R}$ — семейство коммутативных колец с множеством индексов $I=\{1, 2, \ldots, n\}$. Отображение $i \longrightarrow (E(\mathfrak{R}_i), \circ, \cdot)$ определяет семейство структур. Их произведением является структура $(E(\mathfrak{R}_1 \oplus \ldots \oplus \mathfrak{R}_n), \circ, \cdot)$ идемпотентных элементов прямой суммы $\mathfrak{R}_1 \oplus \ldots \oplus \mathfrak{R}_n$.

Будем говорить, что структура $(T, \sqcup', \sqcap', \leqslant')$ является соответственно *подсвязкой*, *$\sqcup$-подсвязкой*, *$\sqcap$-подсвязкой* и *подструктурой структуры* $(L, \sqcup, \sqcap, \leqslant)$, если она удовлетворяет условиям, собранным в следующую таблицу:

$(T, \sqcup', \sqcap', \leqslant')$ называется	структуры $(L, \sqcup, \sqcap, \leqslant)$, если $T \subseteq L$ и для всех $a, b \in T$ выполняется
подсвязкой	$a \leqslant' b \Longleftrightarrow a \leqslant b$
$\sqcup$-подсвязкой	$a \sqcup' b = a \sqcup b$
$\sqcap$-подсвязкой	$a \sqcap' b = a \sqcap b$
подструктурой	$a \sqcup' b = a \sqcup b \wedge a \sqcap' b = a \sqcap b$

Примеры.

13. В структуре $(\mathfrak{P}(\{1, 2, 3, 4\}), \cup, \cap, \subseteq)$ (см. пример 1) подсвязкой является $\{\varnothing, \{1, 2\}, \{1, 3\}, \{1, 2, 3, 4\}\}$.

14. В структуре классов ассоциированных элементов кольца целых чисел $\mathbf{Z}$ с операциями НОК, НОД и отношением $|$ подсвязкой является $\{U, U3, U4, U6, U24\}$ (см. пример 11 (и 8); здесь $U=\{1, -1\}$).

15. Структура $(\mathfrak{C}, \langle \cup \rangle, \cap, \subseteq)$ примера 2 является $\cap$-подсвязкой структуры подмножеств $(\mathfrak{P}(M), \cup, \cap, \subseteq)$ (пример 1).

16. Структура R-подмодулей R-модуля M (пример 5) является подструктурой структуры подгрупп аддитивной группы M (примеры 3 и 4):

17. Всякое подмножество, замкнутое относительно операций $\sqcup$ и $\sqcap$, структуры $(L, \sqcup, \sqcap, \leqslant)$ образует подструктуру относительно ограничения этих операций. Специальные подструктуры в $(L, \sqcup, \sqcap, \leqslant)$ можно получить,

выбрав для элементов a, b из L следующие подмножества:

$(a)_{\leqslant} := \{x : a \leqslant x\}$ *(верхний (главный) идеал),*
$(b)_{\geqslant} := \{x : b \geqslant x\}$ *(нижний (главный) идеал),*
$[a, b] := \{x : a \leqslant x \leqslant b\}$ *(интервал, или промежуточная структура b/a).*

К этим специальным случаям относится следующий пример:

18. В структуре классов ассоциированных элементов кольца главных идеалов с операциями НОК и НОД и отношением $|$ (пример 11 (и 8)) классы, состоящие из делителей заданного элемента m, образуют интервал $[U, Um]$. В § 4 гл. 7 он обозначался через $L(m)$.

Пусть теперь задана произвольная структура $(L, \sqcup, \sqcap, \leqslant)$. Если $a \leqslant b$ и $a \neq b$, будем писать $a < b$:

$$a < b :\langle\!=\!\rangle\, a \leqslant b \wedge a \neq b.$$

Отношение, двойственное к $<$, обозначим $>$.

Определение.

Элемент a из L называется	в $(L, \sqcup, \sqcap, \leqslant)$, если
нулевым элементом	$a \leqslant x$ для всех $x \in L$
единичным элементом	$x \leqslant a$ для всех $x \in L$
атомом (атомарным элементом)	существует единственный $x \in L$, такой, что $x < a$
антиатомом	существует единственный $x \in L$, такой, что $a < x$

Будем обозначать через 0 нулевой, а через 1 единичный элемент структуры (если они существуют). Их единственность следует из аксиомы 3′.

Если существует атомарный элемент a, то существует и нулевой элемент структуры, причем это единственный элемент, меньший a. Действительно, пусть $n < a$. Для всех $x \in L$ имеем $x \sqcap a \leqslant a$, поэтому или $x \sqcap a = a$, или $x \sqcap a = n$. Итак, $n \leqslant x$ для всех $x \in L$. Это означает, что $n = 0$. Атомарные элементы будем обозначать буквами p,

$q, \ldots$. Множество всех атомарных элементов обозначим через $\mathfrak{A}(L, \sqcup, \sqcap, \leqslant)$.

Высказанное утверждение допускает двойственное.

Примеры.

19. В структуре $(\mathfrak{P}(M), \cup, \cap, \subseteq)$ (см. пример 1) пустое множество $\varnothing$ является нулевым элементом, M — единичным. Одноэлементные подмножества атомарны; их дополнения до M антиатомарны.

20. В структурах, встречающихся в алгебре, атомарные элементы часто называют минимальными, антиатомарные — максимальными элементами (подгруппами, идеалами, ...).

21. В структуре, состоящей из множества действительных чисел отрезка [0, 1], операций max, min и отношения $\leqslant$ (см. пример 9), нулевым элементом является число 0, единичным — число 1. Ни атомов, ни антиатомов в ней нет.

22. В структуре $(\{Ua : a \in R\}, \text{НОК}, \text{НОД}, |)$ (пример 11) нулевым элементом является $U = U1$, единичным — $\{0\} = U0$. Атомарными являются классы, состоящие из простых элементов, антиатомов не существует (если R не является полем).

Пусть снова задана произвольная структура $(L, \sqcup, \sqcap, \leqslant)$. Обозначим через $[a]$ множество атомарных элементов $p \in L$, таких, что $p \leqslant a$:

$$[a] := \{p : p \in \mathfrak{A}(L, \sqcup, \sqcap, \leqslant) \wedge p \leqslant a\}.$$

Отображение

$$a \to [a] \qquad (*)$$

переводит исходную структуру $(L, \sqcup, \sqcap, \leqslant)$ в структуру всех подмножеств множества атомарных элементов $(\mathfrak{P}(\mathfrak{A}(L, \sqcup, \sqcap, \leqslant)), \cup, \cap, \subseteq)$. Это отображение может быть сильно вырожденным (структура примера 21 не имеет атомарных элементов: $[a] = \varnothing$ для любого a), но может быть также изоморфизмом. Так, в примере 1 (и 19) отображение $x \to \{x\}$ является, очевидно, взаимно однозначным отображением M на $\mathfrak{A}(\mathfrak{P}(M), \cup, \cap, \subseteq)$. Поэтому $(*)$ является изоморфизмом структур $(\mathfrak{P}(M), \cup, \cap, \subseteq)$ и $(\mathfrak{P}(\mathfrak{A}(\mathfrak{P}(M)), \cup, \cap, \subseteq)), \cup, \cap, \subseteq))$.

Отсюда следует

Теорема 1. *Если структура* $(L, \sqcup, \sqcap, \leqslant)$ *изоморфна некоторой структуре* $(\mathfrak{P}(M), \cup, \cap, \subseteq)$, *то в качестве множества* M *может быть взято* $\mathfrak{A}(L, \sqcup, \sqcap, \leqslant)$; *тогда данный изоморфизм структур есть не что иное, как отображение* (*). *Для того чтобы структура* $(L, \sqcup, \sqcap, \leqslant)$ *была изоморфна структуре всех подмножеств некоторого множества, необходимо и достаточно, чтобы выполнялись следующие два требования:*

(1) *для любых* $a, b \in L$

$$[a] \subseteq [b] \Rightarrow a \leqslant b;$$

(2) *для любого множества* A *атомарных элементов структуры* $(L, \sqcup, \sqcap, \leqslant)$ *существует элемент* $a \in L$, *такой, что* $A = [a]$.

Мы хотим теперь показать, что для того чтобы структура $(L, \sqcup, \sqcap, \leqslant)$ удовлетворяла этим требованиям, необходимо и достаточно, чтобы она была полной, атомарной, дистрибутивной структурой с дополнениями; другими словами, чтобы она была *полной булевой алгеброй*.

Дадим необходимые определения.

Элемент s структуры $(L, \sqcup, \sqcap, \leqslant)$ называется *верхней границей* множества $A \subseteq L$, если $a \leqslant s$ для всех $a \in A$. Обозначение:

$$A \leqslant s.$$

Элемент $g \in L$ называется *точной верхней границей*, или *структурным максимумом* множества $A \subseteq L$, если

$$A \leqslant s \langle\Rightarrow\rangle g \leqslant s,$$

т. е. если g является нулевым элементом в структуре всех верхних границ множества A (см. пример 17). Отсюда, в частности, следует единственность точной верхней границы. Ее обозначение:

$$\bigsqcup A.$$

Используя это обозначение, требование (1) в теореме 1 можно записать более сжато: *для любого элемента* $a \in L$

$$a = \bigsqcup [a]. \qquad (1')$$

Двойственные понятия: *нижняя граница множества* A

$$s \leqslant A$$

и *точная нижняя граница* (или минимум) множества A

$$\sqcap A.$$

В силу аксиомы 4′ всякое двухэлементное подмножество $A = \{a, b\}$ в L имеет точную верхнюю границу, а именно

$$a \sqcup b = \bigsqcup \{a, b\}.$$

Структура называется *полной*, если любое ее подмножество имеет точную верхнюю границу. В полной структуре *всякое подмножество A имеет также и нижнюю границу*:

$$\sqcap A = \bigsqcup \{x : x \leqslant A\}.$$

Действительно, если $a \in A$, то $\{x : x \leqslant A\} \leqslant a$. Отсюда следует, что $\bigsqcup \{x : x \leqslant A\} \leqslant a$ и $\bigsqcup \{x : x \leqslant A\}$ является нижней границей множества A, очевидно, превосходящей все остальные нижние границы.

Структура, двойственная к полной структуре, тоже полна.

Всякая полная структура $(L, \sqcup, \sqcap, \leqslant)$ *имеет нулевой элемент, а именно* $\bigsqcup \varnothing \ (= \sqcap L)$, *и единичный элемент* $\bigsqcup L \ (= \sqcap \varnothing)$.

Примеры.

23. Структура $(\mathfrak{P}(M), \cup, \cap, \subseteq)$ примера 1 [и, следовательно, всякая структура со свойствами (1) и (2)] полна. Точной верхней границей множества подмножеств из M является объединение этих множеств, точной нижней границей — их пересечение.

24. Полны также структуры примеров 2—6, 8, 11 и 21.

25. Произведение семейства полных структур полно.

26. *Всякая непустая конечная структура полна.*

27. Неполной структурой является, например, множество рациональных чисел $\mathbf{Q}$ с операциями max, min и отношением $\leqslant$ (пример 9).

Элемент y называется *дополнением* к x, если

$$x \sqcap y = 0 \quad \text{и} \quad x \sqcup y = 1.$$

Структура с нулем и единицей называется *структурой с дополнениями*, если каждый ее элемент имеет по крайней мере одно дополнение.

Структура, двойственная к структуре с дополнениями, сама является структурой с дополнениями. Чтобы доказать, что произведение структур с дополнениями является структурой с дополнениями, необходимо использовать аксиому выбора.

Примеры.

28. Структура $(\mathfrak{P}(M), \cup, \cap, \subseteq)$ [а также всякая структура, удовлетворяющая требованиям (1) и (2)] является структурой с дополнениями. Всякое подмножество A из M имеет единственное дополнение, а именно множество, дополняющее A до M:

$$M \setminus A = \{x : x \in M \wedge x \notin A\}.$$

29. Структура K-подмодулей некоторого K-модуля (K — поле, см. пример 5), а следовательно, структура подпространств векторного пространства являются структурами с дополнениями, так как всякий базис подпространства может быть дополнен до базиса всего пространства.

30. В структуре $(\{Ua : a \in R\}, \text{НОК}, \text{НОД}, |)$ примера 11 (и 22) интервал $[Ua, Ub]$, где $a|b$ и $a \neq 0$, является структурой с дополнениями тогда и только тогда, когда элемент $\frac{b}{a} \in R$ свободен от квадратов. В этом случае класс $Ut \in [Ua, Ub]$ обладает единственным дополнением — классом $U\frac{ab}{t}$. В частности, *структура* $L(m) = [U, Um]$ *делителей элемента* $m \in R$ (см. пример 18) *является структурой с дополнениями тогда и только тогда, когда* m *свободно от квадратов* (обратимые элементы относятся к свободным от квадратов).

31. В структуре $(E(R), \circ, \cdot)$ идемпотентов коммутативного кольца R (см. пример 10) всякий непустой отрезок $[a, b]$ есть структура с дополнениями; однозначно определенным дополнением к $x \in [a, b]$ является $a - x + b$. Если кольцо R имеет единичный элемент 1, то 0 и 1 в R соответствуют 0 и 1 в $(E(R), \circ, \cdot)$; в этом случае вся структура $E(R) = [0, 1]$ есть структура с дополнениями.

[Если в кольце R всякий делитель нуля нильпотентен, как, например, в факторкольце $\mathbf{Z}/(p^n)$ или в области целостности, то идемпотентными элементами являются только 0 и 1. Действительно, из $a^2=a$ или $a(a-1)=0$ следует, что $a=1$ или a—делитель нуля; но тогда он нильпотентен, а нильпотентный идемпотент равен нулю.]

Выясним теперь, что означает требование (2).

Теорема 2. *Если любой элемент x полной структуры имеет точно одно дополнение x', то для всякого множества A атомов структуры*

$$A=[\bigsqcup A]. \tag{2'}$$

Доказательство. Очевидно, что $A\subseteq[\bigsqcup A]$. Докажем обратное включение. Пусть $p\in[\bigsqcup A]$. Так как $p\leqslant\bigsqcup A$ и $p\sqcap p'=0$, то соотношение $\bigsqcup A\leqslant p'$ выполняться не может; следовательно, не может выполняться и соотношение $A\leqslant p'$. Это означает, что существует элемент $q\in A$, такой, что $q\not\leqslant p'$. Осталось показать, что $p=q\in A$. С одной стороны, так как $p'\sqcap q\neq q$, то $p'\sqcap q=0$. С другой стороны, $p\sqcup(p'\sqcup q)=1$. Так как p атомарен, то $p\sqcap(p'\sqcup q)$ равен либо нулю, либо p. Если $p\sqcap(p'\sqcup q)=0$, то в силу единственности дополнения $p'\sqcup q=p'$ и $q\leqslant p'$, чего не может быть. Таким образом, $p\sqcap(p'\sqcup q)=p$. Тогда $p'\sqcup q=p\sqcup(p'\sqcup q)=1$.

Итак, q—элемент, дополнительный к p', значит, $q=p$.

Структура $(L, \sqcup, \sqcap, \leqslant)$ называется *дистрибутивной*, если в ней выполняется дистрибутивный закон

$$(\mathrm{D}_\sqcup) \qquad a\sqcup(b\sqcap c)=(a\sqcup b)\sqcap(a\sqcup c).$$

Двойственным к нему является закон

$$(\mathrm{D}_\sqcap) \qquad a\sqcap(b\sqcup c)=(a\sqcap b)\sqcup(a\sqcap c).$$

Докажем, что в *дистрибутивной структуре закон* $(\mathrm{D}_\sqcap)$ *тоже справедлив, т. е. структура, двойственная к дистрибутивной структуре, тоже дистрибутивна.*

Доказательство.

$$a\sqcap(b\sqcup c)=a\sqcap(a\sqcup c)\sqcap(b\sqcup c)=$$
$$=((a\sqcap b)\sqcup a)\sqcap((a\sqcap b)\sqcup c)=(a\sqcap b)\sqcup(a\sqcap c).$$

Обратное утверждение совпадает с двойственным к только что доказанному и справедливо в силу принципа двойственности.

Подструктура дистрибутивной структуры дистрибутивна. Произведение дистрибутивных структур дистрибутивно.

Примеры.

32. Сруктура $(\mathfrak{P}(M), \cup, \cap, \subseteq)$ [и, следовательно, всякая структура, удовлетворяющая требованиям (1) и (2)] дистрибутивна.

33. *Структура* $(L(R), +, \cap, \subseteq)$ *идеалов кольца главных идеалов* R *дистрибутивна.* Действительно, достаточно показать, что

$$Ra \cap (Rb + Rc) \subseteq (Ra \cap Rb) + (Ra \cap Rc)$$

(противоположное включение очевидно во всякой структуре). Пусть $Rb + Rc = Rd$, тогда $d = bu + cv$, $b = db'$, $c = dc'$. Всякий элемент из $Ra \cap (Rb + Rc)$ представим как в виде xa, так и в виде $yd = ybu + ycv$. Первое слагаемое $ybu = ydb'u = xab'u \in Ra \cap Rb$; второе слагаемое $ycv = ydc'v = xac'v \in Ra \cap Rc$, что и требовалось доказать.

34. Дистрибутивны следующие структуры: структура примера 8, изоморфная структура примера 33, и двойственная к ней структура $(\{Ua : a \in R\}$, НОК, НОД, $|)$ примера 11.

35. Дистрибутивна структура всякого линейно упорядоченного множества (пример 9).

36. Структура $(E(R), \circ, \cdot)$ (пример 10) дистрибутивна. Действительно, если a, b, c — идемпотентные элементы коммутативного кольца R, то $a(b \circ c) = ab + ac - abc = ab + ac - abac = (ab) \circ (ac)$ (см. § 1 гл. 5).

Теорема 3. *Если в некоторой дистрибутивной структуре с* 0 *и* 1 *как элементы* x_1, y_1, *так и элементы* x_2, y_2 *взаимно дополнительны, то из* $x_1 \leqslant x_2$ *следует* $y_2 \leqslant y_1$.

Доказательство.

$$y_2 \leqslant (y_1 \sqcup x_1) \sqcap (y_1 \sqcup y_2) = y_1 \sqcup (x_1 \sqcap y_2) \leqslant y_1 \sqcup (x_2 \sqcap y_2) = y_1.$$

Из этой теоремы следует, что элементы *дистрибутивной структуры с* 0 *и* 1 *имеют не более одного дополнения.*

Дистрибутивные структуры с дополнениями называются *булевыми структурами*[1]) (или *булевыми алгебрами*). Дополнение элемента x (однозначно определенное в силу теоремы 3) обозначим через x'. *Отображение*

$$x \longrightarrow x'$$

является — снова в силу теоремы 3 — *изоморфизмом булевой алгебры* $(L, \sqcup, \sqcap, \leqslant, 0, 1, ')$ *на двойственную к ней булеву алгебру* $(L, \sqcap, \sqcup, \geqslant, 1, 0, ')$. Итак, булева алгебра двойственна сама себе. Легко проверить, что в ней справедливы *законы де Моргана*

$$(a \sqcup b)' = a' \sqcap b' \quad \text{и} \quad (a \sqcap b)' = a' \sqcup b'.$$

Булевой подалгеброй булевой алгебры $(L, \sqcup, \sqcap, \leqslant, 0, 1, ')$ называется подструктура структуры $(L, \sqcup, \sqcap, \leqslant)$, содержащая 0, 1 и вместе с каждым элементом x дополнительный к нему элемент x', другими словами, подмножество, содержащее 0, 1 и замкнутое относительно операций $\sqcup$, $\sqcap$, $'$, вместе с ограничением на него этих операций.

Примеры.

37. $(\mathfrak{P}(M), \cup, \cap, \subseteq)$ и, следовательно, всякая структура со свойствами (1) и (2) является булевой алгеброй (см. примеры 28 и 32).

38. *Интервал* $[Ua, Ub]$, *описанный в примере* 30, *в частности подструктура* $L(m)$, *если* m *свободно от квадратов, являются булевыми алгебрами* (см. пример 34).

39. Булевы алгебры, состоящие из идемпотентных элементов кольца, указаны в примерах 31 и 36.

40. В дистрибутивной структуре с 0 и 1 множество элементов, имеющих дополнение, является подструктурой (пример 17) и даже булевой алгеброй.

41. Булевой алгеброй является множество всех открытых подмножеств M некоторого топологического пространства с операциями: $M \sqcup N$ — множество внутренних точек множества $\overline{M \cup N}$, $M \sqcap N = M \cap N$ и отношением: $M \leqslant N$ означает $M \subseteq N$ (черта означает замыкание множества).

Следствием дистрибутивного закона $(D_{\sqcup})$ является *модулярный закон*

$$(M) \qquad a \leqslant c \Rightarrow a \sqcup (b \sqcap c) = (a \sqcup b) \sqcap c.$$

[1]) George Boole, 1815—1864.

Для доказательства достаточно применить ($D_{\sqcup}$) к левой части равенства в (M). Структура, удовлетворяющая этому закону, называется *модулярной*. Очевидно, структура, двойственная к модулярной, модулярна. Всякая подструктура и произведения модулярных структур модулярны.

Для модулярных структур очевидным образом справедлива следующая *теорема об изоморфизме* (см. рис. 96):

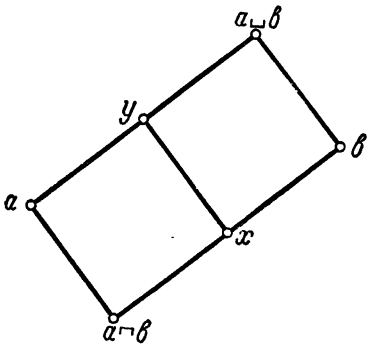


Рис. 96.

Для произвольных a, b $\sqcup$*-отображение*

$$x \longrightarrow a \sqcup x \text{ («объединение с } a\text{»)}$$

интервала $[a \sqcap b, b]$ *в интервал* $[a, a \sqcup b]$ *и* $\sqcap$*-отображение*

$$y \longrightarrow y \sqcap b \text{ («пересечение с } b\text{»)}$$

интервала $[a, a \sqcup b]$ *в* $[a \sqcap b, b]$ *являются взаимно обратными изоморфизмами структур, т. е.*

$$a \sqcap b \leqslant x \leqslant b \Rightarrow (x \sqcup a) \sqcap b = x, \tag{3}$$

и, по принципу двойственности,

$$a \leqslant y \leqslant a \sqcup b \Rightarrow a \sqcup (b \sqcap y) = y. \tag{4}$$

Обратно, закон (M) является следствием как утверждения (3), так и утверждения (4). В этом можно убедиться, положив, например, в (4) $y = (a \sqcup b) \sqcap c$.

Примеры.

42. Структура нормальных делителей группы G (пример 4) модулярна. Справедливо даже более общее утверждение: для всяких трех множеств $A, B, C \subseteq G$, таких, что $A^{-1} \subseteq A$ и $C \cdot C \subseteq C$,

$$A \subseteq C \Rightarrow A \cdot (B \cap C) = (A \cdot B) \cap C.$$

(Доказательство тривиально; оно использует включения $A^{-1}C \subseteq AC \subseteq CC \subseteq C$.) В частности, структура подгрупп абелевой группы модулярна и, следовательно, модулярна структура подмодулей некоторого R-модуля (пример 16). (Отсюда название «модулярный».)

43. Подсвязка примера 14 из пяти элементов не является модулярной.

44. Структура подгрупп группы обратимых элементов факторкольца $\mathbf{Z}/(8)$ модулярна (см. пример 42), но не дистрибутивна.

Мы хотим теперь установить достаточные условия для того, чтобы структура удовлетворяла требованию (1). Назовем *атомарной* структуру, в которой требование

$$[a] \subseteq [b] \Rightarrow a \leqslant b \tag{1}$$

выполняется по крайней мере для случая $[a] = \varnothing$, т. е. в которой из $[a] = \varnothing$ следует, что $a = 0$. Всякая непустая атомарная структура имеет нулевой элемент.

Теорема 4. *Всякая атомарная модулярная структура с дополнениями удовлетворяет требованию* (1).

Доказательство. Пусть $[a] \subseteq [b]$. Дополнение к $a \sqcap b$ обозначим через c. Имеем

$$[c \sqcap a] = [c \sqcap a] \cap [b] = [c \sqcap a \sqcap b] = [0] = \varnothing.$$

В силу атомарности структуры $c \sqcap a = 0$. Далее,

$$b \geqslant a \sqcap b \sqcup (c \sqcap a) = ((a \sqcap b) \sqcup c) \sqcap a = 1 \sqcap a = a.$$

(Здесь во втором равенстве мы воспользовались законом модулярности.)

Примеры.

45. $(\mathfrak{P}(M), \cup, \cap, \subseteq)$, как и всякая структура со свойством (1), атомарна (см. пример 19).

46. Структура $(\{Ua : a \in R\}$, НОК, НОД, $|\,)$ классов ассоциированных элементов кольца главных идеалов R атомарна (см. пример 22).

47. Всякая конечная структура атомарна.

48. Структура подпространств векторного пространства (см. пример 29) атомарна. Ее атомарными элементами являются одномерные подпространства.

49. Структура $(L(R), +, \cap, \subseteq)$ идеалов кольца R с единицей в общем случае неатомарна, но всегда антиатомарна (т. е. в ней выполняется свойство, двойственное к атомарности).

В заключение соберем в одной теореме факты, установленные в теоремах 1—4:

Теорема 5. *Для того чтобы структура была изоморфна структуре всех подмножеств некоторого множества, необходимо и достаточно, чтобы она была полной атомарной булевой алгеброй.*

Следствие. *Для того чтобы структура была изоморфна структуре всех подмножеств некоторого конечного множества, необходимо и достаточно, чтобы она была конечной булевой алгеброй.*

Литература к приложению II: Биркгоф [2], Хермес [19], Маклейн и Биркгоф [13], Резерфорд [16]. [См. также Скорняков [17].— *Ред.*]

СПИСОК ЛИТЕРАТУРЫ

Алгебра

1. Артин (Artin E.), Galoissche Theorie, Leipzig, 1959.
2. Биркгоф (Birkhoff G.), Теория структур, М., 1952.
3. Биркгоф (Birkhoff G.) и Маклейн (MacLane S.), A survey of modern algebra, New York, 1965.
4. Бурбаки (Bourbaki N.), Элементы математики. Алгебра (многочлены и поля, упорядоченные группы), М., 1965.
5. Ван-дер-Варден (Van der Waerden B. L.), Современная алгебра, ч. I, II, М., 1947.
6. —Algebra, I—II, Berlin, 1966—67.
7*. Виноградов И. М., Основы теории чисел, М., 1972.
8. Джекобсон Н., Строение колец, М., ИЛ, 1961.
9. Кохендёрфер (Kochendörffer R.), Einführung in die Algebra, Berlin, 1955.
10. Ковальский (Kowalsky H. J.), Lineare algebra, Berlin, 1965.
11. Курош А. Г., Лекции по общей алгебре, М., 1962.
12. Ленг С., Алгебра, М., 1968.
13. Маклейн (MacLane S.) и Биркгоф (Birkhoff G.), Algebra, New York, 1967.
14. Редеи (Redei L.), Über das Kreisteilungspolynom, *Acta Math. Acad. Sci. Hung.*, 5 (1954), 27—28.
15. —Algebra I, Leipzig, 1959.
16. Резерфорд (Rutherford D. E.), Introduction to Lattice theory, Edinburgh, London, 1965.
17*. Скорняков Л. А., Элементы теории структур, М., 1970.
18. Хассе (Hasse H.), Лекции по теории чисел, М., 1953.
19. Хермес (Hermes H.), Einführung in die Verbandtheorie, Berlin, 1967.
20. Шёнберг (Schoenberg I. J.), Note on the cyclotomic polynomial *Mathematika*, **11** (1964), 131—136.

Геометрия

21. Бахман (Bachmann F.) и Бочек (Boczeck I.), Punkte, Vektoren, Spiegelungen, Grundzüge der Math., Band II A. Kap. 2, Göttingen, 1967.
22. Бляшке (Blaschke W.) и Боль (Bol G.), Geometrie der Gewebe, Berlin, 1938.
23. Боттема (Bottema O.), De elementaire meetkunde van het platte vlak, Groningen, 1938.
24. Киндер (Kinder H.), Eine geometrische interpretation der Galoisgruppe von x^n-1, Vortrag in Oberwolfach, 29.5.1969.
25. Томсен (Thomsen G.), Schnittpunktsätze in ebenen Geweben, *Abh. Math. Sem. Univ. Hamburg*, **7** (1930), 99—106.
26. Шоке Г., Геометрия, М., 1970.
27. Яглом И. М., Геометрические преобразования, ч. I, II, М., 1955—56.

ОБОЗНАЧЕНИЯ

$A, B, \ldots$ — n-угольники, $O=(o, \ldots, o)$ — нулевой n-угольник, стр. 23

Циклические классы n-угольников:

$\mathcal{A}_n$ — множество всех n-угольников, стр. 23

$\mathcal{A}_{1,n}$ — класс тривиальных n-угольников, стр. 24

$\mathcal{A}_n$ — нуль-изобарический класс, стр. 29

$\mathring{\mathcal{C}}$ — центральный класс, соответствующий свободному циклическому классу $\mathcal{C}$, стр. 75

$\mathcal{A}_{d,\bar{d}}$ — периодический класс ($n=d\bar{d}$), стр. 32

$\mathcal{A}_n^d$ — класс d-кратно изобарически распадающихся n-угольников ($d \mid n$), стр. 85

$\mathcal{R}n$ — класс $\mathbf{Q}$-правильных n-угольников, стр. 167

$\mathcal{R}_6$ — класс аффинно-правильных 6-угольников, стр. 39

Специальные циклические отображения:

ζ — $(a_1, a_2, \ldots, a_n) \to (a_2, \ldots, a_n, a_1)$, стр. 50

σ — проекция; каждому n-угольнику $(a_1, a_2, \ldots, a_n)$ ставит в соответствие n-угольник центра тяжести, т. е. n-угольник $(a, a, \ldots, a)$, где $a=\frac{1}{n}\sum a_i$, стр. 27

μ_d — (для $d \mid n$) хордовое усреднение, проекция, каждому n-угольнику $(a_1, a_2, \ldots, a_n)$ ставит в соответствие $\frac{n}{d}$-кратно пройденный d-угольник с вершинами $\frac{d}{n}(a_1+a_{d+1}+\ldots+a_{n-d+1}), \ldots$; эти точки яв-

	ляются центрами тяжести хордовых $\frac{n}{d}$-угольников n-угольника $(a_1, a_2, \ldots, a_n)$, стр. 87
$\varkappa_d$	последовательное усреднение; каждому n-угольнику $(a_1, a_2, \ldots, a_n)$ ставит в соответствие n-угольник с вершинами $\frac{1}{d}(a_1+a_2+\ldots+a_d)$, ...; эти точки являются центрами тяжести d последовательных вершин n-угольника $(a_1, a_2, \ldots, a_n)$, стр. 91
$s(\varphi)$	сумма коэффициентов циклического отображения φ, стр. 52
$K[\zeta]$	алгебра циклических отображений, стр. 51, 52
$E(K[\zeta])$	булева алгебра циклических проекций, стр. 104
Grad $\mathscr{C}$	степень (свободы) циклического класса $\mathscr{C}$, стр. 33
Ker φ	ядро отображения φ, Im φ — образ φ, Fix φ — множество неподвижных элементов отображения φ, стр. 50, 54
End $(\mathscr{A})$	кольцо эндоморфизмов абелевой группы A, стр. 50
an $\mathscr{A}$	аннулятор R-модуля $\mathscr{A}$, стр. 151
ker S	ядро идеала S, стр. 151
$a \circ b := a+b-ab$,	стр. 94
$\tau(n)$	число делителей числа n, стр. 85
$\varphi(n)$	функция Эйлера, стр. 213
$\mu(n)$	функция Мёбиуса, стр. 177
$d \mid\mid n$	d является собственным делителем n: $d \mid n$ и $d \neq n$, стр. 149

Специальные полиномы:

$F_n(x)$	n-й полином деления круга, стр. 215
$m_d(x)$	$=\frac{d}{n}(1+x^d+x^{2d}+\ldots+x^{n-d})=\frac{d}{n}\frac{x^n-1}{x^d-1}$ $(d \mid n)$, стр. 147

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

ОГЛАВЛЕНИЕ

УВАЖАЕМЫЙ ЧИТАТЕЛЬ!

Ваши замечания о содержании книги, ее оформлении, качестве перевода и другие просим присылать по адресу: 129820, Москва, И-110, ГСП, 1-й Рижский пер., д. 2, издательство «Мир».

Ф. Бахман, Э. Шмидт

n-угольники

Редактор Н. И. Плужникова
Художник А. В. Шипов
Художественный редактор В. И. Шаповалов
Технический редактор Е. С. Потапенкова
Корректор К. Л. Водяницкая

Сдано в набор 17/X 1972 г. Подписано к печати 14/III 1973 г. Бумага № 2 $84\times108^{1}/_{32}=3{,}88$ бум. л. Усл. печ. л. 13,02. Уч.-изд. л. 11,12. Изд. № 1/6784. Цена 77 коп. Заказ № 588.

ИЗДАТЕЛЬСТВО «МИР»
Москва, 1-й Рижский пер., 2

Набрано и сматрицировано
в ордена Трудового Красного Знамени
Первой Образцовой типографии
имени А. А. Жданова «Союзполиграфпрома»
при Государственном комитете
Совета Министров СССР по делам издательств,
полиграфии и книжной торговли
Москва, М-54, Валовая, 28

Отпечатано в ордена Трудового Красного Знамени
Ленинградской типографии № 2
имени Евгении Соколовой «Союзполиграфпрома»
при Государственном комитете Совета Министров
СССР по делам издательств, полиграфии
и книжной торговли
г. Ленинград, Л-52, Измайловский проспект, 29

77 коп.

В популярной серии

«СОВРЕМЕННАЯ МАТЕМАТИКА»

вышли в свет следующие книги:

БЕККЕНБАХ Э., БЕЛЛМАН Р. **Введение в неравенства**

ОРЕ О. **Графы и их применение**

НИВЕН А. **Числа рациональные и иррациональные**

НЕВАНЛИННА Р. **Пространство, время и относительность**

СТИНРОД Н., ЧИНН У. **Первые понятия топологии**

ЛИНДОН Р. **Заметки по логике**

МОСТЕЛЛЕР Ф., РУРКЕ Р., ТОМАС ДЖ. **Вероятность**

ШОКЕ Г. **Геометрия**

ХАРТСХОРН Р. **Основы проективной геометрии**

КАЦ М., УЛАМ С. **Математика и логика. Ретроспектива и перспективы**

ГРОССМАН И., МАГНУС В. **Группы и их графы**

МИЛНОР ДЖ., УОЛЛЕС А. **Дифференциальная топология (начальный курс)**

ЭББИНХАУЗ Г.-Д., ЯКОБС К., МАН Ф.-К., ХЕРМЕС Г. **Машины Тьюринга и рекурсивные функции**

ИЗДАТЕЛЬСТВО «МИР»