

Ф. Картеси

ВВЕДЕНИЕ В КОНЕЧНЫЕ ГЕОМЕТРИИ

Перевод с английского
Ф. Л. Варпаховского и А. С. Солодовникова



Москва «Наука»
Главная редакция
физико-математической литературы
1980

22.151

К 27

УДК 51³

F. Kárteszi

*Introduction to
Finite Geometries*

Akadémiai Kiadó
Budapest

1976

Картези Ф. Введение в конечные геометрии: Пер. с англ. — М.: Наука. Главная редакция физико-математической литературы, 1980. — 320 с.

Основной объект книги — конечные проективные плоскости. Рассматриваются и другие виды конечных плоскостей: аффинные, гиперболические, мёбиусовы и т. д. Дается развернутая теория плоскостей Галуа — основного класса конечных проективных плоскостей. Рассмотрен ряд приложений конечных плоскостей к комбинаторике и теории графов.

Предназначается для научных работников, аспирантов и студентов математических отделений университетов и пединститутов, а также лиц, занимающихся приложениями конечных геометрий.

© Akadémiai Kiadó, Budapest 1976

© Перевод на русский язык,
Издательство «Наука».
Главная редакция
физико-математической
литературы, 1980

К $\frac{20203+021}{053(02)-80}$ 42-80.1702040000

*Моему дорогому учителю
профессору БЕНИАМИНО СЕГРЕ*

ПРЕДИСЛОВИЕ

Настоящая книга построена на основе курса лекций, которые я читаю в Будапештском университете под общим названием «Проективная геометрия» начиная с 1948 года. Первое время я лишь кратко упоминал о понятии конечной проективной плоскости в общем контексте классической проективной геометрии. С годами я постепенно увеличивал долю конечных геометрий за счет классических разделов.

Учитывая, что предварительная подготовка моих слушателей была неодинаковой, я вынужден был начинать изложение на совершенно элементарном уровне.

Более чем двадцатилетний опыт преподавания, а также успехи теории за последние тридцать лет выработали у меня определенный дидактический подход, нашедший свое отражение в моих лекциях. По настоянию некоторых моих бывших студентов я представил эти лекции в форме учебника.

По своему подходу эта книга несколько непохожа на традиционные учебники подобного рода. Прежде всего, я не стремился к всестороннему освещению предмета, включая последние достижения; меня скорее интересовали те средства и методы, которые определяли ход его развития. Я считаю эту книгу в известной мере экспериментальной, как и сами мои лекции, и с интересом ожидаю отзывов читателей, которые пожелают пользоваться ею для знакомства с теорией конечных геометрий.

Что касается терминологии, я часто бывал вынужден — главным образом из-за скудости соответствующих публикаций на венгерском языке — вводить новые термины или

же отклоняться от общепринятых; разумеется, во всех таких случаях я объяснял точное значение приводимого термина. Несколько необычны также и некоторые иллюстрации, например таблицы, условные изображения фигур и т. п.

Я хотел бы подчеркнуть, что весьма обязан профессорам Д. Строммеру и Г. Сасу за их полезные советы и внимательный просмотр рукописи, а также М. Фридьеши и Г. Видеки за ясные и аккуратные рисунки.

Наконец, я считаю своим долгом выразить мою признательность издательству Венгерской академии наук за публикацию этой книги.

Ф. Картеси

СИМВОЛЫ И ОБОЗНАЧЕНИЯ

$ N $	число элементов в множестве N .
$\{a, b, \dots, h\}$	множество, состоящее из элементов a, b, \dots, \dots, h .
$\{x \mid P\}$	множество элементов x , обладающих свойством P (например, $\{x \in G \mid x^2 = 1\}$).
$x \in N$	элемент x принадлежит множеству N .
$x \notin N$	x не принадлежит N .
$U \subseteq N$	каждый элемент множества U принадлежит N .
$U \subset N$	каждый элемент U принадлежит N , но не всякий элемент N принадлежит U .
$A \cap B$	$\{x \mid x \in A \text{ и } x \in B\}$, максимальная общая часть, пересечение.
$A \cup B$	$\{x \mid x \in A \text{ или } x \in B\}$, объединение A и B .
$A \otimes B$	множество всех упорядоченных пар (a, b) , где $a \in A$ и $b \in B$.
$A \setminus B, A \setminus B$	$\{x \mid x \in A \text{ и } x \notin B\}$.
$\circ, *, \perp, \wedge$	знаки операций (определяемых особо в каждом случае).
(A, \circ)	система с одной операцией (в случае операций сложения и умножения пишется соответственно $(A, +)$ и (A, \times)).
$(A, +, \cdot), (A, \perp, \wedge)$	системы с двумя операциями.
$F(x, m, b)$	тернарная операция.
$GF(q)$	поле Галуа из q элементов.
(x_1, x_2, x_3)	координаты точки.
$[u_1, u_2, u_3]$	координаты прямой.
●	знак инцидентности (в таблице инцидентности).
Σ	(произвольная) таблица инцидентности.
Ω	циклическая таблица инцидентности.
$C^{m, x}$	квадрат Γ -таблицы инцидентности.

$\Gamma(q), \Gamma$	таблица инцидентности, разбитая на квадраты.
$\overrightarrow{AB}; a, \dots, x$	векторы.
λx	произведение вектора и скаляра.
$(x), [u]$	точка и прямая, заданные своими координатами.
$[u](x)$	$u_1x_1 + u_2x_2 + u_3x_3$.
$S_{n,q}$	n -мерное (арифметическое) пространство над полем Галуа $GF(q)$; пространство Галуа.
$t-(v, k, \lambda)$	система блоков $t-(v, k, \lambda)$.
I	система аксиом, состоящая из аксиом I_1, I_2, I_3, I_4 .
D, P, R	теоремы Дезарга, Паскаля, Рейдемейстера.
MD, MP, MR	микро-теоремы Дезарга, Паскаля, Рейдемейстера.

Глава 1

ОСНОВНЫЕ ПОНЯТИЯ, ОТНОСЯЩИЕСЯ К КОНЕЧНЫМ ГЕОМЕТРИЯМ

В этой главе будет дано простое и элементарное изложение основных понятий, задач и методов теории конечных геометрий. Мы начнем с описания того, в чем состоит предмет этого нового раздела математики и как он возник из нескольких классических дисциплин.

1.1. Конечная плоскость

Проективная плоскость, получаемая путем добавления к евклидовой плоскости идеальных точек и идеальной прямой, называется *классической проективной плоскостью*. Для этой плоскости известны следующие основные факты, касающиеся отношения инцидентности точек и прямых:

(1) *Для любых двух различных точек существует единственная инцидентная им прямая* (называемая прямой, соединяющей эти две точки).

(2) *Для любых двух различных прямых существует единственная инцидентная им точка* (называемая точкой пересечения этих двух прямых).

(3) *Существуют такие четыре точки, что прямая, инцидентная любым двум из них, не инцидентна ни одной из двух других.* (Желая выразить этот факт, мы будем говорить, что существует собственный четырехугольник.)

Примем теперь указанные выше основные утверждения за аксиомы. Всякая теорема, являющаяся следствием этих аксиом, выполняется и для классической проективной плоскости. Существуют, однако, и другие системы объектов, называемых точками и прямыми, которые вместе с некоторым отношением инцидентности — выполняющимся или нет для каждой пары из одной точки и одной прямой — удовлетворяют требованиям (1), (2), (3). Одним из наиболее давних и простых примеров таких систем служит *фигура Фано* (см. рис. 2).

Рассмотрим нераскрашенную шахматную доску размером 7 на 7, на которой фигуры расставлены так, как показано на рис. 1. Назовем вертикали $P_1, P_2, P_3, P_4, P_5, P_6$ и P_7 доски «точками», а горизонтали $l_1, l_2, l_3, l_4, l_5, l_6$ и l_7 — «прямыми». Будем понимать «инцидентность» точки и прямой как тот факт, что клетка пересечения соответствующей вертикали с соответствующей горизонталью занята фигурой (на рисунке такая клетка обозначена кружком), и пусть незанятая клетка означает «неинцидентность». Нетрудно проверить, что такая модель действительно удовлетворяет требованиям (1), (2), (3).

	P_1	P_2	P_3	P_4	P_5	P_6	P_7
l_7	●			●			●
l_6			●	●		●	
l_5	●	●				●	
l_4					●	●	●
l_3		●		●	●		
l_2	●		●		●		
l_1		●	●				●

Рис. 1.]

Так, например, единственная прямая, соединяющая точки P_4 и P_6 , есть l_2 . Единственная точка, инцидентная прямым l_3 и l_5 , есть P_2 . Собственным четырехугольником является $P_1P_2P_3P_4$, причем $l_1, l_2, l_3, l_5, l_6, l_7$ — это шесть прямых, соединяющих различные пары его точек, так что система удовлетворяет условию (3). В дальнейшем данная система будет именоваться *плоскостью Фано*.

Мы будем изучать в основном конечные плоскости, которые будут трактоваться как конечные множества точек (что имеет ряд преимуществ). Прямая при этом понимается как точечное подмножество, выделяемое некоторыми свойствами. Итак, плоскость есть множество точек, скажем $\Sigma = \{P_1, P_2, \dots\}$, а прямые на плоскости суть определенные подмножества этого множества Σ . Точки и прямые будем обозначать соответственно большими и малыми латинскими буквами. Проективная плоскость задается следующей системой аксиом:

I_1 . Если $P \in \Sigma$, $Q \in \Sigma$ и $P \neq Q$, то существует единственная прямая l , для которой $P \in l$ и $Q \in l$.

I_2 . Если $g \subset \Sigma$, $l \subset \Sigma$ и $g \neq l$, то существует точка P такая, что $P \in g$ и $P \in l$.

I_3 . Существуют четыре точки такие, что всевозможные пары из них определяют в соответствии с I_1 шесть различных прямых,

Мы уже знаем, что абстрактная проективная плоскость, определяемая этими аксиомами, не является противоречивым понятием: мы располагаем примерами классической проективной плоскости и плоскости Фано.

(а) Из аксиом I_1 и I_2 следует, что любые две различные прямые имеют одну и только одну общую точку.

Именно, в силу I_2 существует одна, а в силу I_1 — не более одной общей точки для двух различных прямых.

(б) Существуют четыре прямых, из которых никакие три не имеют общей точки. (То есть существуют собственные четырехсторонники.)

В самом деле, если для точек P_1, P_2, P_3 и P_4 выполняется аксиома I_3 , то прямые P_1P_2, P_2P_3, P_3P_4 и P_4P_1 удовлетворяют утверждению (б).

Как и в классической проективной геометрии, для абстрактной проективной плоскости имеет место принцип двойственности. Это следует из того, что I_1 и I_2 , а также I_3 и теорема (б) двойственны друг другу.

(с) Всякая прямая имеет по меньшей мере три точки; всякая точка принадлежит по меньшей мере трем прямым.

Поскольку вторая часть утверждения двойственна первой, то достаточно доказать лишь первую часть.

Существуют собственные четырехугольники; пусть $P_1P_2P_3P_4$ — один из них. Произвольной прямой l могут принадлежать две, одна или ни одной вершины этого четырехугольника. В первом случае пусть $P_3 \in l$ и $P_4 \in l$. Прямые P_1P_2 и P_3P_4 имеют единственную общую точку, которая не является вершиной данного четырехугольника. Она вместе с тем является третьей точкой прямой l . Во втором случае пусть l проходит только через вершину P_4 , тогда каждая из прямых P_1P_2 и P_2P_3 пересекает l в одной точке. В третьем случае каждая из прямых P_4P_1, P_4P_2 и P_4P_3 пересекает l в одной точке. Следовательно, утверждение (с) верно.

Эти теоремы, выражающие основные свойства классической проективной плоскости, будучи принятыми в качестве аксиом, определяют значительно более общее понятие абстрактной проективной плоскости. Чтобы ограничить это понятие и получить понятие конечной проективной плоскости порядка q , мы вводим четвертую аксиому.

I_4 . Существует прямая, состоящая из $q + 1$ точек, где q ($q > 1$) — некоторое (подходящее) целое положительное число.

Эту аксиому можно считать естественной, поскольку ей удовлетворяет плоскость Фано (при $q = 2$). Далее, из трех предыдущих аксиом вытекает, что $q > 1$. (Теорема (с).)

Систему аксиом I_1, I_2, I_3 и I_4 будем обозначать символом I . Рассмотрим некоторые простые, но важные следствия системы аксиом I .

(d) Каждая прямая состоит из $q + 1$ точек.

(e) Через каждую точку проходит $q + 1$ прямых.

! (f) Плоскость состоит из $q^2 + q + 1$ точек.

(g) Плоскость содержит $q^2 + q + 1$ прямых.

В примере на рис. 1 ($q = 2$) эти теоремы выражаются следующими свойствами:

$2 + 1 = 3$ кружка содержатся в каждой строке таблицы.

3 кружка содержатся в каждом столбце таблицы.

Таблица состоит из $2^2 + 2 + 1$ (непустых) столбцов.

Таблица состоит из $2^2 + 2 + 1$ (непустых) строк.

Докажем последовательно все утверждения от (d) до (g). При этом воспользуемся обычной конструкцией перспективного соответствия, которая, очевидно, распространяется на случай плоскости, определяемой системой аксиом I .

(d) Пусть $l = \{P_1, P_2, \dots, P_{q+1}\}$ — прямая, удовлетворяющая аксиоме I_4 , а l' — произвольная прямая, отличная от l , $l' \neq l$. В силу I_2 прямые l и l' имеют общую точку; пусть это будет точка P_j . Прямая l' содержит, согласно теореме (с), точку Q_1 , отличную от P_j ; кроме того, прямая, соединяющая точку P_k прямой l , отличную от точки P_j , с точкой Q_1 , содержит точку Q_2 , отличную как от Q_1 , так и от P_k . Далее, совокупность прямых, соединяющих Q_2 с точками прямой l , исчерпывает множество всех прямых, проходящих через Q_2 , как это легко следует из аксиом I_1 и I_2 ; при этом каждая из этих прямых пересекает l' в некоторой точке, поэтому прямая l' содержит $q + 1$ точек. Ясно, что l' не может иметь более $q + 1$ точек — иначе, соединяя эти точки с Q_2 , мы получили бы, что в пучке прямых, проходящих через Q_2 , содержится более чем $q + 1$ прямых.

(e) Доказательство теоремы (e) получается двойственным образом из доказательства теоремы (d), поскольку,

как мы уже показали, существует точка Q_2 , через которую проходит ровно $q+1$ прямых.

(f) Каждая точка плоскости лежит, согласно I_1 , на некоторой прямой пучка прямых с центром Q_2 . На каждой из $q+1$ прямых этого пучка имеется, согласно (d), q точек, отличных от Q_2 . Поэтому общее число точек равно $(q+1)q+1 = q^2+q+1$.

(g) Доказательство теоремы (g) получается двойственным образом из доказательства теоремы (f).

О п р е д е л е н и е. Структура, удовлетворяющая системе аксиом I, называется конечной проективной «плоскостью порядка q ».

Когда это не даст повода к недоразумениям, мы будем говорить просто о «плоскости порядка q ».

Для многих q остается открытым вопрос: существует ли плоскость порядка q , где q — целое, большее 2?

1.2. Изоморфные плоскости, таблицы инцидентности

Рассмотрим две конечные проективные плоскости порядка q , т. е. два множества с одним и тем же числом элементов $n = q^2 + q + 1$, в которых можно указать n подмножеств по $q+1$ элементов в каждом таким образом, что структуры этих множеств, порождаемые данными подмножествами, — мы будем называть их *комбинаторными структурами* — удовлетворяют системе аксиом I. Поскольку оба множества состоят из одинакового числа элементов, для обозначения элементов обоих множеств можно использовать одни и те же названия или же один и тот же набор индексов.

Рассмотрим, например, рис. 1 и 2. Обе таблицы удовлетворяют системе аксиом I, что легко проверяется (таблица рис. 1 была уже проверена ранее). Пользуясь одним и тем же набором индексов, мы тем самым установили взаимно однозначное соответствие между двумя различными плоскостями порядка 2. По этому соот-

	P_1	P_2	P_3	P_4	P_5	P_6	P_7
I_1	•	•		•			
I_2	•		•				•
I_3		•				•	•
I_4	•				•	•	
I_5				•	•		•
I_6			•	•		•	
I_7		•	•		•		

Рис. 2.

ветствию, однако, трудно судить о структурном подобии двух способов распределения знаков инцидентности.

Более показательную информацию можно получить, если ввести следующие простые операции. Мы будем ниже называть рис. 1 « Σ_1 -таблицей», а рис. 2 — « Σ_2 -таблицей».

1° Разложим таблицу Σ_1 на столбцы. После этого сделаем перестановки по схеме

$$\omega = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 7 & 2 & 4 & 3 & 5 & 6 \end{pmatrix},$$

в которой даются номера столбцов. Эта схема означает, что мы оставляем первый столбец на месте, второй столбец заменяем седьмым, третий — вторым и т. д.; разумеется, столбцы переставляются вместе с содержащимися в них знаками. Объединяем теперь переставленные столбцы. Операцию, выполненную согласно такому предписанию, будем называть ω -преобразованием.

2° Разлагаем далее таблицу на строки и, выполнив перестановки строк, скажем, по схеме

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 4 & 6 & 2 & 5 & 7 \end{pmatrix},$$

объединяем переставленные строки. Подобную операцию будем называть σ -преобразованием.

3° Исходя из некоторой таблицы, выполним сначала ω -преобразование, а затем над получившейся таблицей — σ -преобразование. Обратно, выполним сначала σ -преобразование, а затем ω -преобразование. В обоих случаях каждая клетка таблицы (вместе с заключенным в ней знаком) переместится на одно и то же место. Мы образовали композицию двух перемещений во взаимно перпендикулярных направлениях, причем результат композиции этих перемещений не зависит от порядка данных перемещений. Этот факт выражается записью $\omega\sigma = \sigma\omega = \tau$; композицию перемещений (преобразований) будем называть τ -преобразованием. Ясно, что ω -преобразование можно считать τ -преобразованием, рассматривая его как композицию самого себя с σ -преобразованием, оставляющим все столбцы на месте. Аналогично, всякое σ -преобразование также является τ -преобразованием.

Если теперь применить те именно ω - и σ -преобразования, которые приведены выше, к нашей таблице Σ_1 , то

легко заметить, что расстановка знаков в таблице Σ_1 перейдет в расстановку знаков таблицы Σ_2 . Это можно выразить, записав, что

$$\omega(\Sigma_1) = \sigma\omega(\Sigma_1) = \tau(\Sigma_1) = \Sigma_2.$$

Таким образом, мы получаем, что таблицы рис. 1 и 2, по существу, являются двумя различными формами (реализациями) одной и той же комбинаторной структуры, т.е. таблица рис. 1 то же задает плоскость Фано.

О п р е д е л е н и е. Если две таблицы инцидентности удовлетворяют системе аксиом I и одна из них получается из другой τ -преобразованием, то будем говорить, что эти две таблицы (две плоскости) изоморфны; неизоморфные таблицы (плоскости) будем называть гетероморфными.

В определении говорится о таблицах инцидентности, удовлетворяющих системе I. Вообще, таблица инцидентности есть любая таблица $m \times n$, каждая клетка которой либо пуста, либо содержит знак. В дальнейшем будут рассматриваться и такие таблицы инцидентности (например, таблицы на рис. 72 и 73, стр. 205—207), которые не представляют конечных плоскостей. Подобные таблицы мы также будем называть изоморфными, если одна из них переводится в другую посредством τ -преобразования (например, две таблицы инцидентности на рис. 71, стр. 204). Мы приведем также и примеры гетероморфных таблиц (например, две таблицы, изображенные на рис. 17, 72 и 73, стр. 60, 205—207).

Ясно, что таблицы инцидентности, задающие конечные плоскости, могут быть изоморфны только тогда, когда они имеют один и тот же порядок q . Две плоскости одного и того же порядка могут быть и гетероморфны друг другу — на этом в дальнейшем мы остановимся подробнее, пока отметим только, что это возможно лишь для таблиц размером минимум 91 на 91 с 7371 пустыми клетками и 910 клетками, содержащими знак инцидентности. Если даны две такие таблицы, то установить их гетероморфность отнюдь не просто.

Существуют ли две гетероморфные плоскости порядка 2? Прежде чем исследовать этот вопрос, дополним список теорем, перечисленных в 1.1.

(h) *Таблица инцидентности, задающая конечную плоскость, не может содержать знаков инцидентности в каждой из 4 клеток, стоящих в пересечении каких-либо двух строк и двух столбцов* (т. е. в такой таблице нельзя выделить часть, показанную на рис. 3).

В противном случае таблица не удовлетворяла бы аксиоме I_1 — через две точки проходили бы две различные прямые.

Рассмотрим теперь таблицу Σ , задающую плоскость порядка 2. Расположение знаков в первой строке этой таблицы либо такое же, как в первой строке рис. 4, либо может быть сделано таким же за счет подходящего ω -пре-

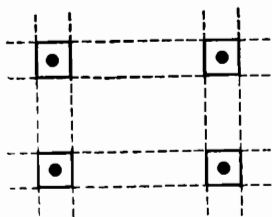


Рис. 3.

	1	2	3	4	5	6	7
1	●	●		●			
2	●		●				●
3		●				●	●
4	●				●	●	
5				○	○		○
6			○	○		○	
7		○	○	○			
	C_1	C_2	C_3		C_4		

Рис. 4.

образования. Выделим в преобразованной таблице $\omega(\Sigma) = \Sigma_1$ строку, в первой клетке которой стоит знак \bullet . Либо эта строка — вторая, либо может быть сделана второй с помощью подходящего σ -преобразования, оставляющего первую строку на месте. Применяя подходящее ω -преобразование к таблице $\sigma(\Sigma_1) = \Sigma_2$, мы можем, в силу теоремы (h), получить таблицу Σ_3 , у которой знаки в первых двух строках расставлены так же, как на рис. 4. Точно так же легко убедиться, что с помощью ω -и σ -преобразований можно перевести исходную таблицу в таблицу, первые четыре строки которой такие же, как на рис. 4. При этом знаки в последних трех строках каким-то образом переместятся. Отделим верхнюю часть с темными и кружками \bullet от нижней части, состоящей из 7×3 клеток, и разделим последнюю — так, как показано на рисунке — на части C_1 , C_2 , C_3 и C_4 . В нижней части

таблицы для обозначения инцидентности будем пользоваться светлым кружком \circ .

В верхней части первого столбца таблицы имеются три знака \bullet , поэтому C_1 , будучи нижней частью столбца, не может содержать знака \circ . В части C_2 имеется только один знак \circ , и его можно с помощью подходящего σ -преобразования, не затрагивающего первых четырех строк, перевести в последнюю строку. В этой строке имеются еще два знака \circ , которые, в силу теоремы (h), могут располагаться лишь так, как на рис. 4. Зачерним теперь знаки последней строки, считая их расположение зафиксированным.

Теперь остается исследовать расположение $7 \cdot 3 - 5 \cdot 3 = 6$ знаков, распределенных в $2 \cdot 5 = 10$ клетках в 5-й и 6-й строках, приходящихся на C_3 и C_4 . В силу теоремы (h) в C_4 не может быть знаков в двух соседних клетках, но в каждом столбце должно содержаться по одному знаку \circ , поскольку по два знака \bullet в этих столбцах зафиксировано. Эти знаки \circ либо расположены так же, как на рис. 4, либо могут быть переведены в это положение перестановкой 5-й и 6-й строк. Зачерним и эти знаки.

Нам остается еще определить расположение 4 знаков, попадающих в 6 клеток 5-й и 6-й строк из C_3 . Легко видеть, однако, что — в силу теоремы (h) и расположения уже фиксированных знаков — эти 4 знака могут быть распределены лишь так, как на рис. 4.

Таким образом, любая таблица инцидентности, представляющая плоскость порядка 2, действительно может быть переведена в таблицу рис. 2 посредством перестановок строк и столбцов. Иными словами, справедлива следующая

Т е о р е м а. *Плоскости порядка 2 совпадают с точностью до изоморфизма (т. е., по существу, имеется лишь один вид плоскости второго порядка).*

1.3. Конструирование конечных плоскостей. Циклические плоскости

До сих пор мы ознакомились лишь с реализацией классической проективной плоскости и плоскости порядка 2; действительно, мы умеем доказывать существование только этих двух видов плоскостей — путем конструирования

ния моделей, удовлетворяющих аксиомам I_1, I_2, I_3 или системе аксиом I. Плоскости порядка q известны для некоторых целых значений q (больших 1); однако в общем виде вопрос существования и представления конечных плоскостей произвольного порядка не решен. Это, быть может, одна из наиболее трудных нерешенных проблем современной математики.

Ниже мы рассмотрим некоторые простые конструкции, позволяющие получить те или иные конечные плоскости. Мы проиллюстрируем наш метод на случае $q = 4$, но сделаем это так, чтобы, следуя данному примеру, легко можно было сконструировать конечные плоскости также и для $q = 2, 3, 5$. (Больше того, некоторая алгебраическая процедура позволит применить этот метод для бесконечного множества натуральных q .)

Пусть

$$n = q^2 + q + 1 = 2C_{q+1}^2 + 1$$

и окружность k с центром O делится n точками на равные части; эти n точек будут вершинами правильного n -угольника, скажем $P_1 P_2 \dots P_n = \Sigma(n)$. Пусть φ означает центральный угол, опирающийся на сторону n -угольника, так что $n\varphi = 2\pi$. На рис. 5 показан 21-угольник, $\Sigma(21)$, отвечающий $q = 4$. Число хорд разной длины, соединяющих различные вершины многоугольника, есть C_{q+1}^2 , поскольку таково число хорд разной длины, исходящих из одной вершины. Число различных пар, составленных из $q + 1$ точек, также равно C_{q+1}^2 . Возникает следующий естественный вопрос:

Можно ли так выбрать $q + 1$ вершин многоугольника $\Sigma(n)$, чтобы все хорды, соединяющие различные пары вершин, были разной длины?

Ясно, что это невозможно, если вершин берется больше чем $q + 1$: в этом случае среди хорд, соединяющих различные пары этих вершин, найдутся две хорды равной длины. Если выбор $q + 1$ вершин, удовлетворяющих нашему условию, возможен, то определяемый ими выпуклый $(q + 1)$ -угольник будем обозначать через Λ . Исходя из определения и сделанного выше замечания, мы будем называть подмногоугольник Λ , если он существует, *максимальным вполне неправильным подмногоугольником правильного многоугольника $\Sigma(n)$* .

На рис. 5 приведен пример, показывающий, что многоугольники Λ существуют. В качестве Λ на рисунке из многоугольника $\Sigma(21)$ выделен пятиугольник $P_1P_2P_5P_{15}P_{17}$; 10 хорд разной длины соединяют различные пары вершин этого пятиугольника. Известно, что подмногоугольник Λ ,

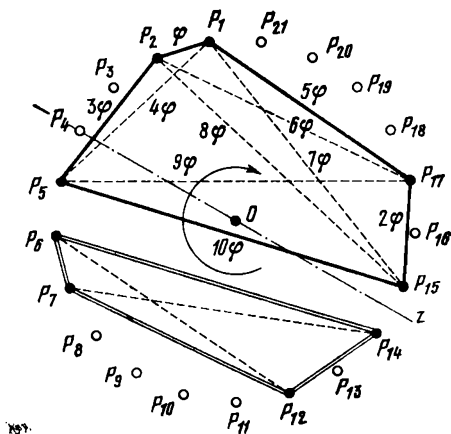


Рис. 5.

отвечающий данному выше определению, существует не для всякого натурального q ; на самом деле, наименьшее значение q , для которого подобный подмногоугольник не существует, есть 6. В случае $q = 6$ мы можем выразить этот факт следующим образом: *Во всяком множестве из двадцати одной хорды, которые соединяют всевозможные пары вершин произвольного подсемиугольника правильного 43-угольника, содержатся две хорды равной длины.* Доказательства этого утверждения мы здесь не приводим. Сравнительно нетрудно найти подмногоугольник Λ в $\Sigma(n)$, если $q = 2, 3, 4, 5$; при этих значениях q для определения вершин искомого подмногоугольника проще всего воспользоваться методом проб и ошибок. Но с ростом q число подлежащих проверке случаев растет настолько быстро, что этот метод оказывается практически неприемлемым. Перебор можно заменить некоторыми алгебраическими процедурами, которые, однако, неуместно было бы излагать в рамках вводной главы.

Пусть для некоторого n подмногоугольник Λ в $\Sigma(n)$ существует. Рассмотрим последовательность многоугольников $\Lambda_1, \Lambda_2, \dots, \Lambda_n$, в которой $\Lambda_1 = \Lambda$, а Λ_k получается из Λ_1 поворотом вокруг точки O на угол $(k-1)\varphi$ (при этом, как и на рис. 5, направление вращения соответствует убыванию номеров вершин). Связь между n -элементным точечным множеством $\{P_1, P_2, \dots, P_n\}$ и множеством многоугольников $\{\Lambda_1, \Lambda_2, \dots, \Lambda_n\}$ с тем же числом элементов может быть охарактеризована следующими утверждениями:

A_1 . Для любых j и k , $1 \leq j, k \leq n$, $j \neq k$, существует единственный многоугольник Λ_r , в котором обе точки P_j и P_k являются вершинами.

A_2 . Для любых j и k , $1 \leq j, k \leq n$, $j \neq k$, существует единственная точка P_s , являющаяся вершиной каждого из подмногоугольников Λ_j и Λ_k .

A_3 . Существует подчетыреугольник $\Pi = P_i P_j P_h P_k$ многоугольника $\Sigma(n)$, с которым каждый из подмногоугольников $\Lambda_1, \Lambda_2, \dots, \Lambda_n$ имеет не более двух общих вершин.

В основе доказательства этих утверждений лежит тот факт, что каждая из длин хорд многоугольника $\Sigma(n)$ встречается ровно один раз среди длин хорд каждого многоугольника Λ_k ; поскольку

$$n = q^2 + q + 1 = q(q+1) + 1$$

— число нечетное, то угол поворота (в указанном выше направлении), переводящего вершину P_j в вершину P_k , $j \neq k$, будет отличен от угла поворота, переводящего вершину P_k в вершину P_j . Не умаляя общности, можно считать, что первый меньше второго.

Чтобы доказать утверждение A_1 , рассмотрим хорду многоугольника Λ_1 , длина которой равна длине хорды $P_j P_k$. Легко видеть, что эта хорда переводится в хорду $P_j P_k$ поворотом, в данном направлении, на угол $l\varphi < 2\pi$, где $0 \leq l \leq n-1$. Следовательно, Λ_{l+1} и есть единственный требуемый многоугольник.

Для доказательства A_2 рассмотрим угол поворота $l\varphi$, переводящего Λ_j в Λ_k . Многоугольник Λ_j имеет единственную хорду, на которую опирается центральный угол (с вершиной в точке O), равный $l\varphi$. Поворот на угол $l\varphi$ переводит один конец этой хорды в другой, но

этот другой конец — ввиду равенства угла поворота углу (с вершиной O), на который опирается хорда, — является также вершиной Λ_k , т. е. общей вершиной Λ_j и Λ_k *).

Для доказательства утверждения A_3 выберем один из многоугольников Λ_s и отразим его относительно диаметра, проходящего через одну из точек P_i . Любой подтреугольник полученного таким способом образа Λ'_s многоугольника Λ_s имеет ориентацию, противоположную ориентации треугольника, зеркальным отражением которого он является; следовательно, только одна сторона исходного треугольника может при вращении перейти в сторону его зеркального образа. Отсюда вытекает, что всякий подчетыреугольник многоугольника Λ'_s удовлетворяет утверждению A_3 . Разумеется, при $q = 2$ многоугольник Λ_s будет всего лишь треугольником и наше доказательство теряет силу. Но в этом случае, приняв $\Lambda_s = \{P_1 P_2 P_4\}$, мы получим, что $\Pi = \{P_1 P_2 P_5 P_7\}$ удовлетворяет утверждению A_3 .

Будем теперь считать многоугольник $\Sigma(n)$ «плоскостью». Вершины P_1, P_2, \dots, P_n этого многоугольника пусть будут «точками», а подмногоугольники $\Lambda_1, \Lambda_2,$

..., Λ_n — «прямыми» плоскости. Для такой модели утверждения A_1, A_2, A_3 переходят в аксиомы I_1, I_2, I_3 . Таким образом, получается, что построенная комбинаторно-геометрическая конструкция служит реализацией конечной плоскости порядка q . Значение данного метода не умаляется тем фактом, что при больших q требуемый перебор оказывается громоздким, даже практически неосуществимым; это, впрочем, побуждает нас искать дополнительные математические соображения, которые сделали бы такой перебор ненужным. В дальнейшем мы еще вернемся к этой задаче.

Мы приведем здесь списки вершин многоугольников Λ_1 , отвечающие некоторым значениям q (для краткости мы

*) Доказательство единственности общей вершины у многоугольников Λ_j и Λ_k автором не приводится. Его можно провести следующим образом. Пусть Λ_j и Λ_k имеют две общие вершины P и Q . Поскольку P и Q принадлежат Λ_k , то они получаются поворотом на угол $1/q$ каких-то двух вершин P' и Q' многоугольника Λ_j . Но тогда этот многоугольник имеет две равные хорды $P'Q'$ и PQ . — *Прим. перев.*

пишем 1, 2, 4 вместо P_1, P_2, P_4 и т. д.):

$$q=2, \quad n=7, \quad \Lambda_1=\{1, 2, 4\};$$

$$q=3, \quad n=13, \quad \Lambda_1=\{1, 2, 5, 7\};$$

$$q=4, \quad n=21, \quad \Lambda_1=\{1, 2, 5, 15, 17\};$$

$$q=5, \quad n=31, \quad \Lambda_1=\{1, 2, 4, 9, 13, 19\};$$

$$q=6, \quad n=43 \quad \text{— не существует};$$

$$q=7, \quad n=57, \quad \Lambda_1=\{1, 2, 4, 14, 33, 37, 44, 53\};$$

$$q=8, \quad n=73, \quad \Lambda_1=\{1, 2, 4, 8, 16, 32, 37, 55, 64\};$$

$$q=9, \quad n=91, \quad \Lambda_1=\{1, 2, 4, 10, 28, 50, 57, 62, 78, 82\}.$$

Таким образом, располагая этим перечнем, мы можем получить семь различных конечных плоскостей. В каждом из этих случаев легко составить таблицу инцидентности. Если, например, взять случай $q=4$ (см. рис. 5), то получится таблица, приведенная на рис. 6.

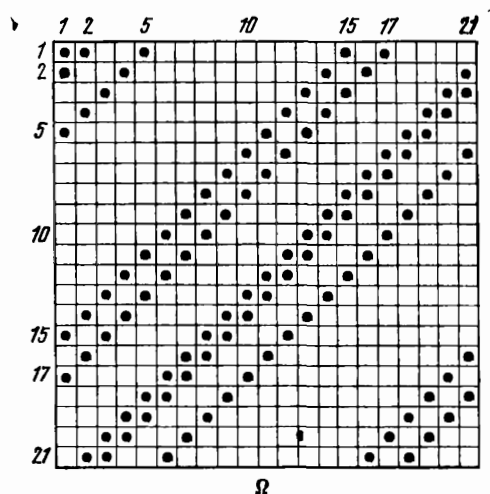


Рис. 6.

Эта таблица — по терминологии, заимствованной из теории матриц, — *циклическая и симметрическая* (по отношению к главной диагонали). Циклическая таблица

инцидентности, задающая конечную плоскость, будет называться впредь Ω -таблицей или, короче, $\Omega(q)$. Таким образом, таблица на рис. 2 есть не что иное, как $\Omega(2)$.

1.4. Г-таблица конечной проективной плоскости

Среди (изоморфных) таблиц инцидентности, задающих конечную плоскость, имеются такие, которые дают более ясное представление об отношении инцидентности, чем другие таблицы, что легко, например, заметить, сравнивая рис. 1 и 2, и это особенно сильно проявляется при больших q . В случае $q = 2$ мы показали, что всякую таблицу инцидентности можно преобразовать в циклическую таблицу (см. рис. 2). Однако существуют и такие таблицы инцидентности, которые не преобразуются в циклические. Мы не приводим здесь соответствующего примера, поскольку наименьший размер такой таблицы есть 91×91 . Имеются, впрочем, таблицы других видов, в которые можно перевести любую таблицу инцидентности путем ω - и σ -преобразований и которые наглядно выражают структурные свойства плоскости.

Возьмем пустую таблицу $n \times n$, где $n = 1 + q + q^2$. Разобьем эту таблицу на части с помощью нескольких жирных линий, как показано на рис. 7. Две такие линии отделяют первую строку и первый столбец таблицы от остальной ее части. В результате образуется узкий крюк в форме буквы Г. Рассмотрим ту часть таблицы инцидентности, которая заполняет «внутренность» этого Г-крюка и которая состоит из $(n - 1)^2$ квадратов; ее можно разбить на $q + 1$ вертикальных полос шириной в q клеток каждая, называемых *столбцевыми полосами*. Аналогично, эту же часть таблицы можно разбить на $q + 1$ горизонтальных полос высотой в q клеток каждая, называемых *строчными полосами*. В пересечении всех столбцевых и строчных полос получается $(q + 1)^2$ квадратов по q^2 клеток каждый (выделенных на рисунке жирными линиями). Теперь из первой столбцевой и первой строчной полос мы образуем широкий Г-образный крюк и подобным же образом во внутренности этого крюка строим еще один Г-образный крюк. На нашем рисунке 3 гнездовых крюка, отделенных друг от друга жирными линиями, образуют вместе *полный Г-крюк* шириной в $2q + 1$ клеток. Подтаблица,

заполняющая внутренность полного Γ -крюка и состоящая из $(q - 1)^2$ квадратов, будет обозначаться через Θ . Двигаясь снаружи вовнутрь, мы будем говорить соответственно о *внешнем, среднем и внутреннем Γ -крюках* и о *Θ -внутренности*; часть, образованная внутренним Γ -крюком и Θ -внутренностью, будет называться *$\Gamma\Theta$ -внутренностью*.

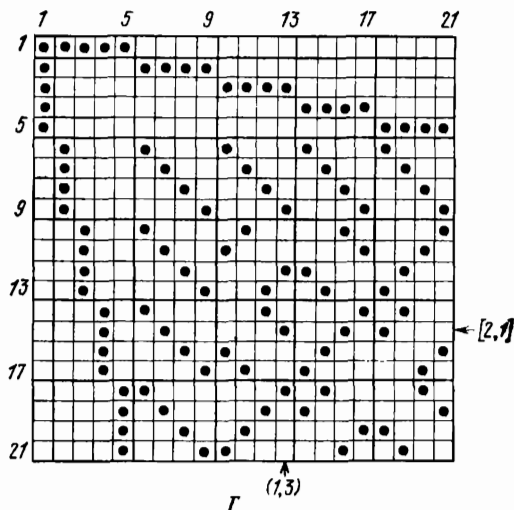


Рис. 7.

Пустую таблицу, разбитую указанным образом на части, будем называть Γ -*решеткой*. Эта решетка соответствует разбиению числа n на слагаемые по формуле $n = 1 + q + q + (q - 1)q$.

Преобразуем теперь таблицу инцидентности Ω (4) на рис. 6 с помощью следующих ω - и σ -преобразований:

$$\omega = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 \\ 1 & 2 & 5 & 15 & 17 & 21 & 16 & 14 & 4 & 7 & 6 & 20 & 10 & 11 & 18 & 19 & 13 & 8 & 3 & 12 & 9 \end{pmatrix}$$

и

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 \\ 1 & 2 & 17 & 5 & 15 & 16 & 21 & 4 & 14 & 18 & 11 & 13 & 19 & 3 & 8 & 9 & 12 & 6 & 7 & 10 & 20 \end{pmatrix};$$

легко проверить, что при этом получится таблица, заполняющая Γ -решетку рис. 7. Проследим по рисунку, как распределены знаки инцидентности в этой Γ -решетке.

В левом верхнем углу внешнего крюка $2q + 1$ знаков образуют Г-фигуру. В силу этого левый верхний квадрат среднего Г-крюка пуст, в остальной же его части знаки располагаются лестничным образом — так, как это показано на рисунке. В каждом квадрате внутреннего крюка знаки инцидентности стоят по главной диагонали. Каждый квадрат, принадлежащий Θ , имеет диагональное распределение знаков, и внутри Θ насчитывается $q - 1$ различных таких распределений. Под «диагональным распределением» понимается такое расположение знаков, при котором в каждой строке и каждом столбце встречается ровно один знак.

Таблица, устроенная подобным образом, называется Г-таблицей и обозначается через $\Gamma(q)$.

Разумеется, данное здесь описание не заменяет определения, а приводится лишь с целью проиллюстрировать его на конкретном примере. Определяется же Г-таблица следующими условиями:

1° Расположение знаков во внешнем и среднем крюках (секционно) ступенчатое, соответствующее данной Г-решетке.

2° Распределение знаков во всех квадратах внутреннего крюка одинаково и является одним из $q!$ различных диагональных распределений.

Ясно, что если, например, переставить одинаковым образом столбцы, проходящие через каждый квадрат внутреннего Г-крюка какой-либо Г-таблицы, то условия 1°, 2° не нарушатся и в результате получится новая Г-таблица. Выше мы привели пример преобразования таблицы $\Omega(q)$ в таблицу $\Gamma(q)$. Такое преобразование всегда возможно, однако не всякую таблицу $\Gamma(q)$ можно преобразовать в таблицу $\Omega(q)$. Справедлива следующая

Т е о р е м а. Любую таблицу инцидентности, представляющую конечную плоскость, можно с помощью подходящих ω - и σ -преобразований (т. е. с помощью подходящего τ -преобразования) перевести в таблицу $\Gamma(q)$.

Наше доказательство основывается главным образом на том факте, что в таблице инцидентности конечной плоскости знаки инцидентности не могут располагаться во всех вершинах какого-либо прямоугольника, т. е. так, как показано на рис. 3. В целях краткости эту запрещенную конфигурацию будем называть *прямоугольником знаков*.

Сначала, с помощью подходящих ω - и σ -преобразований, перераспределим знаки во внешнем и среднем Г-крюках таким образом, чтобы получалось (секционно)

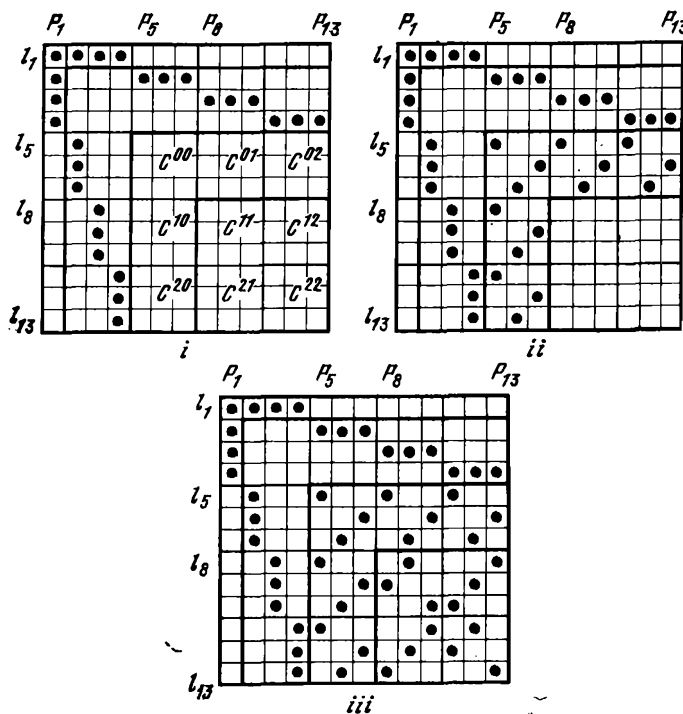


Рис. 8.

ступенчатое распределение, — по образцу, представленному на рис. 7 и 8, *i*. Осуществимость такого перераспределения легко вытекает из свойств I_1 , (d) и (e) конечной плоскости, а также из следствия аксиомы I_1 об отсутствии в таблице инцидентности прямоугольника знаков.

Условимся здесь и в дальнейшем пользоваться символами

$$\begin{array}{lll} C^{00}, & C^{01}, & C^{0, q-1}, \\ C^{10}, & C^{11}, & C^{1, q-1}, \\ C^{q-1, 0}, & C^{q-1, 1}, & \dots, C^{q-1, q-1} \end{array}$$

для обозначения q^2 квадратов, заполняющих внутренность среднего Г-крюка, т. е. Г Θ -внутренность.

На рис. 8, *i* мы оставили незаполненными все квадраты C^{rs} , чтобы выделить первую фазу перераспределения. Конечно, на первой фазе знаки инцидентности распределяются каким-то образом и во всех этих незаполненных квадратах C^{rs} . В действительности после первой фазы упорядочения в каждом квадрате C^{rs} распределение знаков будет диагональным, т. е. в каждой строке и каждом столбце квадрата будет ровно по одному знаку. Для доказательства этого заметим, что два знака инцидентности не могут встретиться в одной строке, (соответственно столбце) квадрата, так как иначе эти знаки вместе со знаками соответствующей строки (столбца) среднего Г-крюка образовывали бы прямоугольник знаков, что невозможно. С другой стороны, всякая строка (столбец) квадрата содержит хотя бы один знак, иначе эта строка (столбец) и одна из строк (столбцов) среднего Г-крюка не удовлетворяли бы аксиоме I_2 (соответственно I_1). Таким образом, любая строка и любой столбец квадрата C^{rs} действительно содержит ровно по одному знаку.

Теперь, сохраняя распределение знаков в среднем Г-крюке, продолжим упорядочение таблицы с целью добиться выполнения условия 2° для внутреннего крюка.

После выполнения первой фазы преобразований распределения знаков в квадратах внутреннего Г-крюка (см. рис. 8, *i*) будут, вообще говоря, различными; но мы можем произвести такое перераспределение, чтобы все они стали одинаковыми и, более того, совпадали с наперед выбранным из $q!$ различных диагональных распределений.

В самом деле, пусть, например, выбрано распределение, показанное на рис. 8, *ii*. Рассмотрим сначала какой-либо квадрат из последовательности

$$C^{00}, C^{01}, C^{0, q-1},$$

скажем квадрат C^{0s} . Требуемое диагональное распределение в этом квадрате получается с помощью подходящих ω -преобразований, действующих только на те столбцы всей таблицы, которые проходят через данный квадрат. Так мы добиваемся нужного диагонального распределения во всех квадратах верхней части внутреннего Г-крюка,

Теперь остается получить такое же распределение в квадратах

$$C^{10}, C^{20}, \quad C^{q-1,0}.$$

Рассмотрим квадрат C^{00} . Для этого квадрата требуемое распределение достигается с помощью σ -преобразований, действующих только на те строки, которые проходят через данный квадрат; аналогично перестраиваются все остальные указанные выше квадраты. Таким образом, проведение второй фазы преобразований завершает доказательство нашей теоремы.

После выполнения второго цикла преобразований в квадратах Θ -внутренности также получаются некоторые

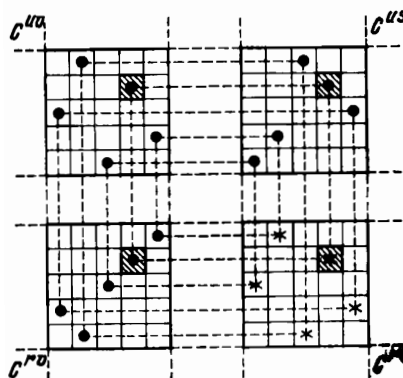


Рис. 9.

диагональные распределения. Относительно этих распределений мы можем сделать только несколько общих замечаний. Сначала, однако, снабдим одним комментарием рис. 9.

Гомологичными элементами (гомологично ассоциированными) будем называть такие клетки $\Gamma\Theta$ -внутренности таблицы инцидентности, которые совмещаются при совмещении — путем сдвига — содержащих их квадратов.

Так, например, клетки, заштрихованные на рис. 9, — гомологично ассоциированные. Фигура из четырех квадратов $\Gamma\Theta$ -внутренности, образованная пересечением двух столбцовых и двух строчных полос, будет называться *прямоугольником квадратов* — по аналогии с прямоугольником знаков. Пусть в квадратах C^{uv} , C^{us} и C^{rv} даны какие-нибудь диагональные распределения; тогда, пользуясь отсутствием в таблице прямоугольников знаков, в квадрате C^{rs} можно указать q клеток, не содержащих знака инцидентности. На рис. 9 эти q пустых клеток помечены символом *.

Мы докажем теперь следующие общие утверждения о квадратах $\Gamma\Theta$ -внутренности:

D_1 . Распределение знаков в каждом из квадратов C^{rs} — диагональное.

D_2 . Если первые или вторые индексы двух квадратов совпадают и не равны нулю, то распределения знаков в этих квадратах различны.

D_3 . Если совместить в одном квадрате знаки всех квадратов одной строчной или столбцовой полосы, не проходящей через квадрат C^{00} , то получится точное заполнение одного квадрата.

Утверждение D_1 уже было доказано ранее, а утверждения D_2 и D_3 легко следуют из нашего комментария к рис. 9.

Поскольку всего имеется q^2 квадратов C^{rs} , то число δ различных диагональных распределений, встречающихся в этих q^2 квадратах, меньше $q^2 + 1$. Возникает естественный вопрос: что еще можно сказать о соотношении между δ и q ? Мы знаем, что случай $q = \delta$ возможен — примерами служат рис. 7 и рис. 8, *iii*. Ясно, что δ не может быть меньше q , иначе одно и то же распределение встречалось бы в каждой строчной полосе, а это противоречит D_2 . Можно указать пример, в котором $\delta > q$ ($q = 9$, $\delta = 27$); мы не приводим здесь этого примера, поскольку соответствующая таблица инцидентности имеет размер 91×91 . Учитывая, что в квадратах внутреннего Г-крюка можно получить одинаковые распределения, мы приходим к следующей оценке:

$$D_4. \quad q \leq \delta \leq (q-1)^2 + 1.$$

В качестве примера на применение Г(q)-таблиц нами будет установлена следующая

Т е о р е м а. *Существует единственная плоскость порядка 3.*

Доказательство заключается в приведении таблиц инцидентности произвольных плоскостей порядка 3 к одному и тому же виду. Сначала добиваемся, чтобы знаки во внешнем, среднем и внутреннем Г-крюках распределялись так, как показано на рис. 8, *ii*. Согласно замечанию к рис. 9 в каждом из квадратов C^{11} , C^{12} , C^{22} и C^{21} три клетки обязательно пусты, а три знака в остальных шести клетках составляют, в силу D_1 , диагональное распределение. Но возможны только два диагональных распределения трех знаков в шести клетках — обозначим их через A и B . Эти распределения встречаются в четырех квадратах в

одном из следующих двух видов:

$$\begin{pmatrix} A & B \\ B & A \end{pmatrix} \text{ или } \begin{pmatrix} B & A \\ A & B \end{pmatrix}.$$

Второе из них переводится в первое с помощью преобразований

$$\omega: 8, 9, 10, 11, 12, 13 \rightarrow 11, 12, 13, 8, 9, 10$$

и

$$\sigma: 3, 4 \rightarrow 4, 3,$$

относящихся соответственно к столбцам и строкам всей таблицы *). Таким образом, мы видим, что таблица инцидентности, представляющая какую-либо плоскость порядка 3, может быть приведена τ -преобразованием к виду, показанному на рис. 8, iii.

1.5. Системы координат на конечной плоскости

Мы введем теперь новые обозначения для клеток $\Gamma\Theta$ -внутренности, состоящей из внутреннего Γ -крюка и Θ -внутренности таблицы инцидентности $\Gamma(q)$; эти обозначения служат для идентификации как отдельных клеток, так и содержащих их квадратов.

Ранее мы пользовались обозначениями l_1, l_2, \dots, l_n для строк и P_1, P_2, \dots, P_n для столбцов Γ -таблицы ($n = 1, 2, \dots, q^2 + q + 1$). Дальнейшее будет относиться только к строкам l_{q+2}, \dots, l_n и столбцам P_{q+2}, \dots, P_n . Строки, проходящие через некоторый квадрат, будем нумеровать (начиная с верхней) цифрами $0, 1, \dots, q-1$ и b -ю строку, проходящую через квадрат C^{m0} , будем обозначать символом $[m, b]$. Аналогично, столбцы квадрата нумеруются (слева направо) цифрами $0, 1, \dots, q-1$ и y -й столбец квадрата C^{0x} обозначается символом (x, y) . Клетку в пересечении строки $[m, b]$ со столбцом (x, y) обозначим

$$\langle m, b; x, y \rangle.$$

Γ -таблица конечной плоскости задает *тернарную операцию* на множестве $Q = \{0, 1, \dots, q-1\}$ следующим

*) Запись $(a, b, c, \dots) \rightsquigarrow (k, l, m, \dots)$ означает то же, что и запись

$$\begin{pmatrix} a & b & c & \dots \\ k & l & m & \dots \end{pmatrix}.$$

образом. Пусть (x, m, b) — произвольная упорядоченная тройка чисел из Q . Тогда в той части строки $[m, b]$ из $\Gamma\Theta$, которая содержится в квадрате C^{mx} , найдется, в силу D_1 , ровно один знак инцидентности — допустим, в y -м столбце. Номер y этого столбца мы и сопоставляем тройке (x, m, b) . Тем самым на Q определяется тернарная операция

$$F(x, m, b) = y.$$

Например, для таблицы рис. 7 имеем

$$F(1, 2, 1) = 3,$$

так как знак инцидентности оказывается в пересечении строки $[2, 1]$ и столбца $(1, 3)$.

Поскольку строки таблицы задают прямые, а столбцы — точки, то можно говорить о *координатах точки* x, y (или о точке (x, y)) и о *координатах прямой* m, b (или о прямой $[m, b]$). Понятно, что точки P_1, \dots, P_{q+1} и прямые l_1, \dots, l_{q+1} оказываются вне этой системы координат. Однако эта система остается все же вполне целесообразной, что подтверждается следующим сравнением.

Проведем аналогию между декартовыми координатами точки на евклидовой плоскости и введенными выше координатами точки на конечной плоскости. На евклидовой плоскости любой прямой (не параллельной оси y), имеющей угловой коэффициент m и проходящей через точку $(0, -b)$, можно приписать пару координат $[m, b]$. При этом семейство прямых евклидовой плоскости, не параллельных оси y , задает тернарную арифметическую операцию на множестве действительных чисел

$$xm - b = y,$$

которая играет роль тернарной операции

$$F(x, m, b) = y$$

(множество действительных чисел играет роль множества индексов Q). Геометрически мы приписываем тройке чисел (x, m, b) ординату y точки прямой $[m, b]$ с абсциссой x . Прямую, параллельную оси y , можно описывать как геометрическое место точек, удовлетворяющих условию $x = c$. Евклидова плоскость может быть расширена до проективной плоскости путем присоединения к ней идеаль-

ных точек, образующих идеальную прямую. К каждой прямой добавляется единственная идеальная точка, причем к каждой из двух параллельных прямых добавляется одна и та же идеальная точка.

Аналитическая геометрия конечной плоскости, получаемая с помощью множества индексов Q , в значительной степени аналогична аналитической геометрии евклидовой плоскости. Мы можем теперь продолжить эту аналогию, включив в нее не учитывавшиеся ранее точки P_1, P_2, P_{q+1} и прямые l_1, l_2, \dots, l_{q+1} .

На конечной плоскости роль идеальных точек играют точки P_1, P_2, \dots, P_{q+1} , т. е. точки, которым не приписывалось никаких координат. Множество этих точек $l_1 = \{P_1, P_2, \dots, P_{q+1}\}$ играет роль идеальной прямой. Из этой аналогии вытекают такие следствия:

1° Прямая $l_2 = \{P_1, P_{q+2}, P_{q+3}, \dots, P_{2q+1}\}$ играет роль оси y .

2° Роль параллельных прямых, пересекающихся в идеальной точке P_r , на конечной плоскости играют прямые, которые изображаются строками, проходящими через квадрат $C^{r-2,0}$ ($r = 1, 2, \dots, q+1$) *).

3° Прямая $l_{q+2} = \{P_2, P_{q+2}, P_{2q+2}, \dots, P_{qq+2}\}$ играет роль оси x .

4° Точки P_{q+2} и P_{2q+3} играют роль начала координат и точки $(1, 1)$ соответственно.

На евклидовой плоскости мы можем задать множество (неидеальных) точек, инцидентных прямой $[m, b]$, с помощью линейного уравнения

$$y = mx - b.$$

На конечной плоскости этому уравнению **соответствует** уравнение

$$y = F(x, m, b),$$

определяемое тернарной операцией F на Q .

Данная аналогия приводит к некоторой графической модели конечной плоскости, которая часто встречается в литературе (обычно без какого-либо ее содержательного истолкования).

*) Мы распространяем обозначение C^{rs} на квадраты ~~среднего~~ Γ -крюка, допуская для индексов r и s значение -1 .

Мы воспользуемся рассмотренной аналогией для построения модели, соответствующей таблице рис. 7. Эта модель представлена на рис. 10 (изображение неполное). На этом рисунке q^2 (неидеальных) точек конечной плоскости, помеченных парами своих координат (x, y) , изображены в виде точек решетки на евклидовой плоскости. Указанные точки получаются в пересечении равноотстоящих

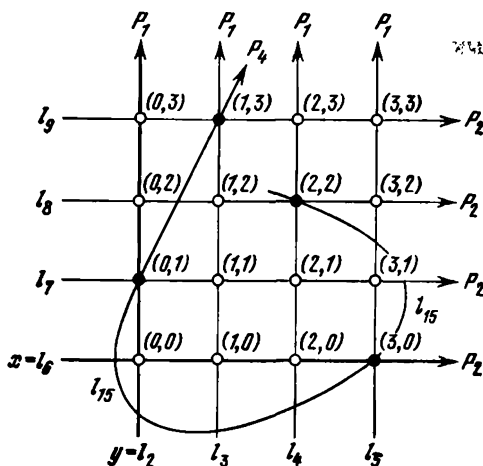


Рис. 10.

прямых l_2, l_3, \dots, l_{q+1} с перпендикулярными им равноотстоящими прямыми $l_{q+2}, l_{q+3}, \dots, l_{2q+1}$. Эти прямые изображают на евклидовой плоскости $2q$ прямых конечной плоскости. Однако остальные прямые конечной плоскости не изображаются, вообще говоря, в виде прямых евклидовой плоскости. Так, например, строка l_{15} рис. 7 представлена на нашем рисунке в виде кривой l_{15} , причем указанная в конце стрелки буква P_4 означает идеальную точку P_4 , которая должна быть добавлена к этой кривой.

Если мы добавим к двум изображенным на рисунке семействам прямых, соответствующих идеальным точкам P_1 и P_2 , в качестве третьего семейства все кривые с общей идеальной точкой P_{k+1} , представляющие строки

$$l_{kq+2}, l_{kq+3}, l_{(k+1)q+1},$$

то мы получим фигуру, напоминающую криволинейную сеть. Если теперь рассматривать только те точки кривых, которые изображают точки конечной плоскости, то получится фигура из q^2 точек — «криволинейная номограмма» семейства функций $y = F(x, k - 1, b)$, в которой каждому значению параметра b из Q отвечает одна функция (вообще, в двухпараметрическом семействе функций $y = F(x, m, b)$ каждой паре значений m и b из Q отвечает своя функция). Если нанести на рисунок изображения всех прямых конечной плоскости, то мы совместим на нем $q - 1$ различных криволинейных сетей.

Полная картина даже в случае $q = 4$ оказывается чрезвычайно сложной. Мы поэтому будем предпочитать пользоваться Γ -таблицами, которые более наглядны.

1.6. Понятие о плоскостях Галуа и полях Галуа

Тесная связь между аналитической геометрией конечной плоскости и обычной аналитической геометрией приводит к понятию об одной специальной разновидности конечных плоскостей. Нам потребуется прежде всего ряд понятий, касающихся полей и групп. Поле с конечным числом элементов будем называть *конечным полем* или *полем Галуа* *). Рассмотрим следующий пример конечного поля.

Пусть поле Галуа состоит из 4 элементов; обозначим его $GF(4)$. Мы зададим конкретное поле из 4 элементов с помощью таблиц для операций. Условимся элементы поля обозначать буквами a_0, a_1, a_2 и a_3 ; далее, a_0 будем считать нейтральным элементом относительно сложения (нулем поля), а a_1 — нейтральным элементом относительно умножения (единицей поля). Таблицы сложения (A) и умножения (M) зададим следующим образом (вместо a_i везде пишется i):

$+$	0	1	2	3	\times	0	1	2	3
0	0	1	2	3	0	0	0	0	0
1	1	0	3	2	1	0	1	2	3
2	2	3	0	1	2	0	2	3	1
3	3	2	1	0	3	0	3	1	2
A					M				

*) См. Приложение: 7.1. 4° в основную теорему в 7.2,

По этим таблицам легко проверить, что задаваемые ими операции сложения и умножения удовлетворяют всем аксиомам поля. Конечно, такая проверка довольно утомительна даже для поля со столь небольшим числом элементов. Например, чтобы убедиться в справедливости закона дистрибутивности в одном только случае $(2 + 3) \cdot 3 = 2 \cdot 3 + 3 \cdot 3$, мы должны проделать следующее. По таблице A находим $2 + 3 = 1$, а по таблице M — $1 \cdot 3 = 3$, поэтому в левой части равенства получается элемент a_3 . По таблице M находим $2 \cdot 3 = 1$ и $3 \cdot 3 = 2$, а по таблице A — $1 + 2 = 3$, значит, и в правой части равенства получается элемент a_3 . Таким образом, дистрибутивный закон выполняется для тройки элементов (a_2, a_3, a_3) .

Позднее мы займемся вопросом о том, как строить таблицы A и M для произвольного поля Галуа. Сейчас отметим только, что число элементов поля Галуа является степенью простого числа и что для всякой такой степени q имеется, по существу, только одно поле. (В нашем примере имеет место случай $q = 2^2$.)

Вернемся к примеру конечной плоскости, указанной на рис. 7. Заменим во всех квадратах

$$C^{10}, C^{11}, C^{12}, C^{13}$$

все знаки инцидентности вторыми индексами содержащих их квадратов. Если затем совместить все квадраты в одном, то получится таблица индексов размером 4×4 , которая будет не чем иным, как таблицей A поля Галуа $GF(4)$.

Рассмотрим на рис. 7 все 4×4 квадратов, на которые разбита $\Gamma\Theta$ -внутренность. Каждый квадрат C^{ii} второго ряда обозначим индексом i , $i = 0, 1, 2, 3$. Пусть C^{rs} — произвольный квадрат из $\Gamma\Theta$; как видно из таблицы, распределение знаков инцидентности в C^{rs} совпадает с распределением знаков в одном из квадратов второго ряда; сопоставим квадрату C^{rs} индекс указанного квадрата. В результате получится таблица индексов размером 4×4 , первая строка и первый столбец которой состоят из нулей. На самом деле эта таблица будет не чем иным, как таблицей M поля $GF(4)$.

В связи с этим примером возникает следующий вопрос: можно ли по таблицам сложения и умножения произвольного поля $GF(q)$ построить $\Gamma(q)$ -таблицу конечной пло-

скости, точнее, ее $\Gamma\Theta$ -внутренность? Положительный ответ на этот вопрос позволил бы построить столько конечных геометрий, сколько имеется полей Галуа (или степеней простых чисел).

Пусть $q = p^r$ — данная простая степень, и пусть даны таблицы операций соответствующего поля $GF(q)$. Пусть элементы поля обозначены индексами $0, 1, 2, \dots, q-1$. Существенно только, чтобы цифры 0 и 1 обозначали нуль и единицу; выбор же индексов для остальных элементов поля произволен. Расставим знаки в Γ -решетке, соответствующей данному q , следующим образом:

1° Внешний и средний Γ -крюки заполним (секционно) ступенчатым образом в соответствии с определением Γ -таблицы.

2° Каждому квадрату C^{rs} из $\Gamma\Theta$ поставим в соответствие индекс t , стоящий в пересечении строки индекса r и столбца индекса s таблицы M ($t = rs$). После этого расставим знаки в тех клетках квадрата C^{rs} , которые соответствуют клеткам таблицы A , содержащим индекс t .

Таблицу инцидентности, полученную указанным путем, обозначим Γ ($GF(q)$). Распределение знаков в этой таблице симметрично относительно главной диагонали. Это непосредственно очевидно для знаков во внешнем и среднем Γ -крюках, а для знаков в $\Gamma\Theta$ -внутренности вытекает из симметрии таблиц A и M , имеющей место в силу коммутативности обеих операций.

Нам теперь предстоит доказать, что таблица Γ ($GF(q)$) действительно задает конечную плоскость порядка q .

Ясно, что аксиома I_4 выполняется, поскольку в первой строке таблицы имеется $q+1$ знаков инцидентности.

Чтобы проверить аксиому I_3 , достаточно взять столбцы $P_2, P_3, P_{q+2}, P_{q+3}$ и убедиться, что найдется шесть строк, каждая из которых пересекает два из них в клетках, содержащих знак инцидентности. Этому условию удовлетворяют строки

$$l_1, l_2, l_{q+2}, l_{q+s+2}, l_{2q+2}, l_{2q+s+2}^*).$$

Ввиду симметрии таблицы инцидентности Γ ($GF(q)$) достаточно проверить какую-нибудь одну из аксиом I_1, I_2 .

*) Здесь не указано значение параметра s . В качестве s следует брать номер той строки таблицы A , в пересечении которой со столбцом, соответствующим единице, стоит нуль. — Прим. перев.

Мы поэтому докажем, что для двух произвольных строк найдется один и только один столбец, который пересекает эти строки в клетках, содержащих знак инцидентности.

Вернувшись к рис. 7 и 8, iii, мы видим, что для некоторых пар строк единственный искомым столбец находится непосредственно.

1° Если $r \leq q + 1$, $s \leq q + 1$ и $r \neq s$, то для строк l_r и l_s искомым будет столбец P_1 . Если $r = 1$ и $s > q + 1$, то для строк l_r и l_s искомым будет один из столбцов P_2, \dots, P_{q+1} (а именно столбец P_{k+1} , когда $kq + 1 < s \leq (k + 1)q + 1$).

2° Если $1 < r \leq q + 1$ и $s > q + 1$ ($kq + 1 < s \leq (k + 1)q + 1$), то искомым столбец должен проходить через квадрат $C^{k-1, r-2}$, поскольку сегмент из q знаков инцидентности строки l_r (т. е. всех ее знаков, за исключением знака в столбце P_1) приходится на столбцы этого квадрата. Далее, строка l_s проходит через квадрат $C^{k-1, r-2}$, а так как распределение знаков в этом квадрате диагональное, то в нем найдется единственная клетка строки l_s , содержащая знак инцидентности. Искомым будет столбец, проходящий через эту клетку.

Если обе строки l_r и l_s проходят через $\Gamma\Theta$, т. е. если $r > q + 1$ и $s > q + 1$, то найти столбец, удовлетворяющий нашему условию, не столь просто. В этом случае выясним сначала следующий вопрос: если строка и столбец квадрата C^{mx} ($0 \leq m, x \leq q - 1$) с индексами b и y соответственно пересекаются в клетке, содержащей знак инцидентности, то каково отношение между числами m, b, x, y с точки зрения арифметики поля $GF(q)$? (Еще один пример определения операций с помощью таблиц A и M для поля из $q = 3^2 = 9$ элементов приведен на рис. 44.) Мы докажем, что выполняется равенство

$$y = mx - b.$$

В нашей конструкции квадрат C^{mx} соответствует клетке таблицы M , определяемой строкой индекса m и столбцом индекса x ; в этой клетке стоит число $mx = t$ — в смысле умножения в поле $GF(q)$. То же самое число t будет находиться в тех клетках таблицы A , которым отвечают строчный и столбцовый индексы b и y , удовлетворяющие равенству $b + y = t$, — в смысле сложения в поле $GF(q)$. Таким образом, клетка квадрата C^{mx} со строчным и столб-

цевым индексами b и y тогда и только тогда содержит знак инцидентности, когда $b + y = t = tx$, т. е. когда $y = tx - b$.

Пусть строки l_r и l_s проходят через $\Gamma\Theta$; используя отношение $y = tx - b$, мы можем найти те клетки обеих строк, в которых содержится знак инцидентности. Допустим, прямые l_r и l_s имеют соответственно координаты $[m, b]$ и $[m', b']$. Мы видим, что l_r и l_s содержат знак инцидентности в одном и том же столбце (x, y) в точности тогда, когда одновременно выполняются соотношения

$$y = tx - b \quad \text{и} \quad y = m'x - b'.$$

Решение этой системы уравнений в поле $GF(q)$ получается по правилам обычной арифметики (основывающейся только на аксиомах поля).

Найдем это решение. Очевидно, возможны три случая:

- а) $m \neq m'$, $b \neq b'$, тогда $x = (b' - b)(m' - m)^{-1}$, $y = (mb' - m'b)(m' - m)^{-1}$;
- б) $m \neq m'$, $b = b'$, тогда $x = 0$, $y = -b$;
- с) $m = m'$, $b \neq b'$, тогда решение не существует.

Последнее означает, что столбец, который пересекает обе прямые l_r и l_s в клетках, содержащих знак инцидентности, не может проходить через $\Gamma\Theta$. Но в случае с) обе прямые l_r и l_s проходят через один и тот же квадрат C^{m_0} , а все такие прямые содержат знак инцидентности в $(m+2)$ -м столбце. Значит, и в случае с) искомый столбец существует.

Этим завершается доказательство того, что таблица инцидентности $\Gamma(GF(q))$ удовлетворяет аксиоме I_2 .

Таким образом, наша конструкция позволяет по каждому полю $GF(q)$ построить таблицу инцидентности $\Gamma(GF(q))$, представляющую конечную проективную плоскость порядка q .

Отметим еще следующий попутно установленный результат.

Инцидентность прямой (строки) $[m, b]$ и точки (столбца) (x, y) эквивалентна равенству

$$y = tx - b,$$

в котором операции понимаются как операции поля $GF(q)$.

Конечная плоскость, задаваемая таблицей инцидентности $\Gamma(GF(q))$ (короче $\Gamma(q)$) и определяемая алгебраической структурой поля $GF(q)$, будет обозначаться символом $S_{2,q}$.

и называться *плоскостью Галуа*; поле $GF(q)$ будет называться *координатным полем плоскости* $S_{2,q}$.

Понятно, что упорядоченные пары (x, y) элементов x, y поля определяют только q^2 точек плоскости $S_{2,q}$, а именно точки, соответствующие столбцам $P_{q+2}, P_{q+3}, \dots, P_n$ ($n = q^2 + q + 1$) таблицы $\Gamma(q)$. Не существует упорядоченных пар (x, y) — иначе говоря, *пар неоднородных координат*, соответствующих столбцам P_1, P_2, \dots, P_{q+1} таблицы; распределения знаков в этих столбцах получены не из поля $GF(q)$, а были заранее определены как стандартные распределения во внешнем и среднем Γ -крюках. Соответствующие этим столбцам $q + 1$ точек называются *идеальными точками* плоскости $S_{2,q}$.

Аналогично, упорядоченные пары $[m, b]$ элементов поля определяют только q^2 прямых плоскости, а именно прямые, соответствующие строкам $l_{q+2}, l_{q+3}, \dots, l_n$ таблицы. Никакая упорядоченная пара $[m, b]$ не отвечает ни одной из строк l_1, l_2, \dots, l_{q+1} , представляющих те прямые плоскости $S_{2,q}$, которые пересекаются в идеальной точке P_1 . Строка l_1 представляет прямую, содержащую все идеальные точки плоскости $S_{2,q}$; эта прямая называется *идеальной прямой* плоскости $S_{2,q}$.

Мы уже видели, что прямые, задаваемые уравнениями $y = mx - b_1$ и $y = mx - b_2$, пересекаются в точке P_{m+2} , которая является идеальной. В этом смысле мы говорим, что две указанные прямые *параллельны*. Аналогично, среди прямых l_2, l_3, \dots, l_{q+1} любые две считаются параллельными.

В аналитической геометрии евклидовой плоскости, расширенной путем присоединения идеальных элементов, уравнение

$$y = mx - b$$

выражает прямую, пересекающую ось y ; причем m есть угловой коэффициент прямой, а число b (взятое с подходящим знаком) есть расстояние от точки пересечения прямой с осью y до начала координат. Таким образом, обнаруживается тесная аналогия между классической проективной плоскостью и плоскостью Галуа. Данное уравнение выражает прямую на евклидовой плоскости или на плоскости Галуа соответственно тому, является

ли координатное поле полем действительных чисел или одним из полей $GF(q)$.

На плоскости $S_{2,q}$ можно ввести и однородные координаты; это позволит включить в координатную систему точки P_1, P_2, \dots, P_{q+1} и прямые l_1, l_2, \dots, l_{q+1} . Рассмотренная выше аналогия позволяет, по существу, ввести однородные координаты обычным образом. Мы, однако, не будем здесь входить в подробности, а отметим только основные моменты.

Пусть дано координатное поле $K = GF(q)$, и пусть его элементы обозначены цифрами $0, 1, 2, \dots, q-1$ (с принятыми ранее соглашениями).

Для точки с (неоднородными) координатами (x, y) тройка (x_1, x_2, x_3) однородных координат определяется равенством $(x_1, x_2, x_3) = (\lambda x, \lambda y, \lambda)$, где $\lambda \in K$ и $\lambda \neq 0$.

Для точек P_{m+1} ($m = 0, 1, \dots, q-1$) однородные координаты определяются как тройки $(1, m, 0)$, где элементы m считаются элементами из K .

Точке P_1 приписывается тройка однородных координат $(0, 1, 0)$.

Аналогично, для прямой с (неоднородными) координатами $[m, b]$ тройка $[u_1, u_2, u_3]$ однородных координат определяется равенством $[u_1, u_2, u_3] = [\mu m, -\mu, -\mu b]$, где $\mu \in K$ и $\mu \neq 0$.

Для прямых l_{r+1} ($r = 0, 1, \dots, q-1$) однородные координаты определяются как тройки $[1, 0, -r]$, где элементы r считаются элементами из K . Прямой l_1 приписывается тройка однородных координат $[0, 0, 1]$.

Из этих определений следует, что тройка $(0, 0, 0)$ не задает никакой точки, а тройка $[0, 0, 0]$ не задает никакой прямой; далее, инцидентность точки (x_1, x_2, x_3) и прямой $[u_1, u_2, u_3]$ имеет место тогда и только тогда, когда выполняется равенство

$$u_1 x_1 + u_2 x_2 + u_3 x_3 = 0.$$

Бурное развитие геометрии Галуа обязано, безусловно, тесной аналогии между геометрией на плоскости Галуа и аналитической геометрией на классической проективной плоскости, а также далеко продвинутой теорией конечных полей. Теорию плоскостей Галуа можно к настоящему времени считать завершенной главой в теории конечных геометрий.

1.7. Замкнутые подплоскости конечной проективной плоскости

Сделаем теперь некоторые замечания об особой роли аксиомы I_3 . Из истории развития проективной геометрии видно, что аксиомы I_1 и I_2 хотя и выражают наиболее важные структурные свойства проективной плоскости, однако, взятые сами по себе, определяют слишком общую структуру. В процессе развития проективной геометрии предпринимались попытки сузить понятие проективной плоскости путем введения дополнительных аксиом, с тем чтобы теория не исчерпывалась бедными по содержанию — в силу их чрезмерной общности — теоремами. В действительности иногда случалось, что добавление новых аксиом только усложняло теорию и вместе с тем приводило к понятию, ненамного более общему, чем понятие классической проективной плоскости.

Приведем здесь две модели — в качестве примеров плоскостей, определяемых только аксиомами I_1 и I_2 .

1° «Точками» и «прямыми» являются соответственно вершины и стороны треугольника на евклидовой плоскости с их отношением инцидентности.

2° «Точками» являются точки P_1, P_2, \dots, P_k ($k > 2$) прямой l_0 на евклидовой плоскости и точка P_0 , лежащая вне этой прямой, а «прямыми» — прямые $P_0P_1, P_0P_2, \dots, P_0P_k, l_0$; отношение инцидентности то же, что и на евклидовой плоскости.

В модели 1° теоремы (d) и (e) из 1.1 остаются верными, а в модели 2° — нет.

Таким образом, естественно ввести дальнейшие аксиомы, ограничивающие понятие проективной плоскости.

Роль аксиомы, эквивалентной I_3 — *прямая имеет по меньшей мере три точки*, — впервые изучалась Фано. Система аксиом I была введена с целью выделения из общего понятия проективной плоскости понятия конечной проективной плоскости.

Исследуем теперь одну простую геометрическую модель.

На рис. 11 представлен правильный 21-угольник P, в котором с помощью знаков \circ , \odot , \bullet выделены три правильных семиугольника A, B и C:

$$P = P_1P_2 \dots P_{21} = A_1B_1C_1 \dots A_7B_7C_7 = A \cup B \cup C.$$



Рассмотрим подпятиугольник

$$P_1 P_4 P_5 P_{10} P_{12} = A_1 A_2 B_2 A_4 C_4 = \Lambda_1$$

многоугольника Р. Все 10 хорд, соединяющие всевозможные пары вершин этого пятиугольника, имеют разные длины. Поэтому пятиугольник Λ можно рассматривать

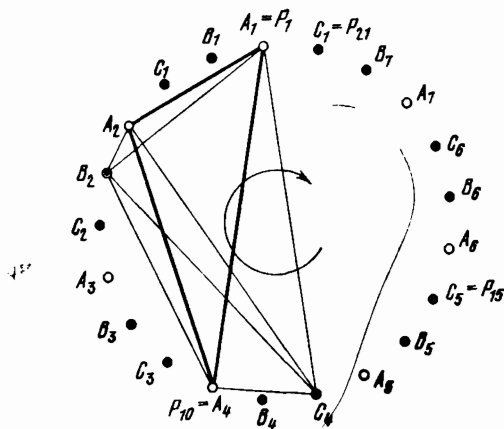


Рис. 11.

как прямую плоскости порядка 4, задаваемой многоугольником Р. (Остальные прямые получаются из Λ_1 вращением в направлении, показанном на рисунке стрелкой.)

Возьмем теперь подтреугольник

$$A_1 A_2 A_4 = P_1 P_4 P_{10} = \Lambda_1^A$$

семиугольника А. Стороны этого треугольника имеют разные длины; следовательно, Λ_1^A можно рассматривать как прямую плоскости порядка 2, задаваемую многоугольником А. Остальные прямые этой плоскости получаются из Λ_1^A поворотами вокруг центра многоугольника А на углы $2k\pi/7$ ($k=1, 2, \dots, 6$) в направлении, указанном стрелкой.

Считая, что все многоугольники Р, А, В, С, Λ_1 и Λ_1^A суть точечные множества своих вершин, мы видим, что справедливы следующие утверждения:

$$P = A \cup B \cup C, \quad A \cap B = B \cap C = C \cap A = \emptyset,$$

$$A \cap \Lambda_1 = \Lambda_1^A \subset \Lambda_1, \quad B \cap \Lambda_1 = B_2, \quad C \cap \Lambda_1 = C_4.$$

Вращением на угол $2\pi/21$ (на угол $4\pi/21$) многоугольник A переводится в многоугольник B (в многоугольник C); при этом треугольники, представляющие прямые плоскости порядка 2, задаваемой многоугольником A , переводятся в треугольники, представляющие прямые плоскости порядка 2, задаваемой многоугольником B (многоугольником C).

Этот пример подсказывает следующее определение.

Подплоскостью конечной проективной плоскости называется конечная проективная плоскость, точки которой составляют правильную часть множества точек исходной плоскости и каждая прямая которой есть подмножество некоторой прямой исходной плоскости.

Термин «подплоскость» используется в литературе также и в других случаях. С целью отличить приведенное определение будем иногда предпосылать этому термину термин «замкнутая» и говорить о замкнутой подплоскости. Пока что, однако, нам предстоит иметь дело только с пятым подплоскости в указанном здесь смысле.

Пусть S — конечная плоскость порядка n , а S^* — ее подплоскость порядка m . Из нашего определения следует, что $m < n$. Пусть $P_1 \in S^*$ и $P_2 \in S^*$. Если l^* — прямая плоскости S^* , соединяющая точки P_1 и P_2 , то $l^* \subset l$, где l — некоторая прямая на S . Поскольку l состоит из $n + 1$, а l^* из $m + 1$ точек, то прямая l содержит $n - m$ точек, не принадлежащих l^* . Мы будем говорить, что прямая l^* *дополняется* этими $n - m$ точками до прямой l . Аналогично, плоскость S^* дополняется до плоскости S ; мы будем выражать это обстоятельство, называя S *расширением* S^* .

В примере, приведенном на рис. 11, получилось, что $n = 4$ и $m = 2$. Впоследствии мы увидим, что плоскость Галуа порядка 9 имеет подплоскость порядка 3. Таким образом, в некоторых случаях $n = m^2$. Известен также пример плоскости, не являющейся плоскостью Галуа и имеющей подплоскость порядка 2, так что в этом случае $n > m^2$.

Т е о р е м а. *Если проективная плоскость порядка n имеет подплоскость порядка m , то либо $n = m^2$, либо $n \geq m^2 + m$ (теорема Брука).*

Д о к а з а т е л ь с т в о. Пусть S^* и S имеют прежний смысл. Пусть, далее, l^* — прямая из S^* , а $l \subset S$ — ее расширение. Рассмотрим точку $Y \in l$, не содержащуюся

в l^* , а следовательно, и в S^* . Множество $P^* = S^* - l^*$ содержит $(m^2 + m + 1) - (m + 1) = m^2$ точек. Удалив прямую l из пучка прямых плоскости S , проходящих через точку Y , мы получим множество L из n прямых. Исследуем отношение инцидентности для множеств L и P^* .

Пусть x^* — прямая плоскости S^* , соединяющая две точки из P^* , а x — соединяющая те же точки прямая плоскости S , так что $x^* \subset x$. Прямые x^* и l^* пересекаются в точке плоскости S^* , не принадлежащей P^* и отличной от Y . А так как $x^* \cap l^* = x \cap l$, то никакая прямая из L не может содержать двух точек из P^* . С другой стороны, всякая точка из P^* лежит на одной из прямых множества L (а именно на прямой плоскости S , соединяющей данную точку с точкой Y), т. е. m^2 прямых из L содержат по одной точке из P^* . Если иных прямых в L нет, то $n = m^2$.

Допустим теперь, что L содержит более m^2 прямых и y — прямая из L , не имеющая общих точек с P^* . Каждая из $m^2 + m + 1$ прямых плоскости S , являющихся расширениями прямых плоскости S^* , пересекает прямую y ; однако никакие две из них не могут пересекаться с y в одной точке, поскольку общая точка этих двух прямых должна принадлежать S^* , а y не содержит точек из S^* . Таким образом, число точек прямой y не может быть меньше числа прямых на плоскости S^* , т. е. $n + 1 \geq m^2 + m + 1$. Значит, если $n \neq m^2$, то $n \geq m^2 + m$.

Позднее мы увидим, какую важную роль играет понятие подплоскости при изучении строения конечных проективных плоскостей. Мы также дадим исчерпывающее описание подплоскостей плоскости порядка 4, приведенной на рис. 11.

1.8. Понятие конечной аффинной плоскости

С точки зрения аксиоматики понятие аффинной плоскости проще понятия евклидовой плоскости. Однако по традиции сначала строится теория евклидовой плоскости, а затем на основе этой теории вводится понятие аффинной плоскости. Более того, возможен и такой подход, при котором сначала из евклидовой плоскости получается проективная плоскость, а затем уже от проективной плоскости путем удаления из нее одной прямой (и, конечно, всех точек этой прямой) приходят к аффинной плоскости.

В получившейся плоскости аксиома I_2 уже не выполняется, поскольку две прямые, пересекавшиеся в изъятой точке, становятся непересекающимися. Кроме того, эта плоскость обладает тем свойством, что через всякую точку, не лежащую на какой-либо прямой, проходит единственная прямая, не пересекающая этой прямой. Две непересекающиеся прямые называются параллельными. Удаляя то одну, то другую прямую, мы будем получать различные аффинные плоскости, но все они изоморфны друг другу *).

Прежде чем определить аффинную плоскость аксиоматически, мы рассмотрим классическую схему на конкретном примере.

Возьмем конечную проективную плоскость, заданную таблицей рис. 7. Вычеркнем из таблицы строку (прямую) l_1 и вместе с нею столбцы (точки) P_1, P_2, P_3, P_4 и P_5 . Оставшуюся часть таблицы обозначим символом $\Gamma^1_1(4)$. Полученную структуру будем называть *аффинной плоскостью (порядка 4), ассоциированной с проективной плоскостью порядка 4*.

По таблице непосредственно проверяем следующие свойства $\Gamma^1_1(4)$.

Аффинная плоскость состоит из $4^2 = 16$ точек и $4^2 + 4 = 20$ прямых; каждая прямая состоит из 4 точек, и через каждую точку проходят 5 прямых. Множество всех прямых можно разбить на 5 классов по 4 прямых в каждом классе так, что любые две прямые одного класса параллельны, а любые две прямые разных классов пересекаются; через каждые две точки проходит единственная прямая; через точку, лежащую вне какой-либо прямой, проходит единственная прямая, не пересекающаяся с первой прямой; точки P_9, P_{10} и P_{11} не коллинеарны.

В случае произвольной таблицы $\Gamma(q)$ ассоциированная таблица $\Gamma^1_1(q)$ обладает теми же свойствами — с точностью до числовых значений параметров.

Однако изоморфизм таблиц $\Gamma^1_1(4)$ и $\Gamma^1_s(4)$ ($s \neq 1$) сразу не очевиден. Чтобы убедиться в том, что изоморфизм имеет место, заметим, что перестановками строк и столбцов таблицу $\Gamma(4)$ можно снова превратить в циклическую

*) Две аффинные плоскости S и S' *изоморфны*, если существует взаимно однозначное отображение $\alpha: S \rightarrow S'$, сохраняющее коллинеарность точек.

таблицу $\Omega(4)$, приведенную на рис. 6, и что с помощью циклических перестановок можно, не нарушая распределения знаков в таблице $\Omega(4)$, любую ее строку сделать первой.

Таблица инцидентности любой плоскости Галуа приводится к циклическому виду (теорема Зингера). Таким образом, в случае плоскости Галуа классический способ построения аффинной плоскости из проективной реализуется в полном своем объеме.

Известны, однако, такие конечные проективные плоскости, которые, при устранении из них разных прямых, приводят к неизоморфным аффинным плоскостям *). Поэтому в символе S^l верхний индекс, обозначающий устраняемую прямую, существен.

Обратимся теперь к аксиоматическому определению конечной аффинной плоскости. *Параллельность* двух прямых будем понимать как их совпадение либо как отсутствие у них общих точек; при таком определении отношение параллельности становится отношением эквивалентности. Абстрагируя свойства плоскости $\Gamma^l(4)$, мы определим *аффинную плоскость порядка q* с помощью следующей системы аксиом А:

A_1 . Любые две различные точки инцидентны ровно одной прямой.

A_2 . Существует одна и только одна прямая, инцидентная данной точке и параллельная данной прямой, не содержащей эту точку.

A_3 . Существует треугольник (три точки, не инцидентные одной и той же прямой).

A_4 . Существует прямая, состоящая из q ($q > 1$) точек.

Множество всех прямых, параллельных какой-либо одной прямой, называется классом. Считая такие классы *идеальными точками*, мы — следуя традиционному подходу — получаем проективную плоскость порядка q , ассоциированную с данной аффинной плоскостью. Однако аффинная плоскость, полученная из этой проективной плоскости устранением какой-либо прямой, не обязательно изоморфна исходной аффинной плоскости.

*) Примером такой плоскости является плоскость порядка 9, представленная на рис. 45 и 46.

1.9. Различные виды конечных гиперболических плоскостей

Пусть дана конечная плоскость *); если для всякой пары $[l, P]$, состоящей из прямой l и точки P вне этой прямой, число прямых, проходящих через P и не пересекающих l , равно нулю, то конечная плоскость проективная; если это число равно единице, то она аффинная.

От этих частных случаев перейдем к общей ситуации: для каждой неинцидентной пары $[l, P]$ множество прямых, проходящих через точку P , разобьем на два подмножества — подмножество μ прямых, пересекающих l , и подмножество ν прямых, не пересекающих l . Число элементов множеств μ и ν обозначим соответственно через $|\mu|$ и $|\nu|$. Если для каждой пары $[l, P]$ выполняется условие $|\nu| > 1$, то плоскость будем называть *гиперболической*. Если найдутся такие целые неотрицательные числа $M (> 1)$ и m , что для всякой пары $[l, P]$ выполняются условия $|\nu| = M$ и $|\mu| = m$, то мы будем говорить о *регулярной гиперболической плоскости*.

В последнее десятилетие появилось несколько исследований по гиперболическим плоскостям, и теперь известно, что существуют нерегулярные конечные гиперболические плоскости. Мы здесь ограничимся изучением регулярных конечных гиперболических плоскостей.

Ряд авторов определяет гиперболическую плоскость, называемую иначе $\langle m, n \rangle$ -плоскостью, следующей системой аксиом H^* :

H_1^* . Для любых двух различных точек существует единственная инцидентная им прямая.

H_2^* . Для любой прямой существует не инцидентная ей точка.

H_3^* . Существует такое число $n > 1$, что для любой $[l, P]$ -пары $|\nu| = n$.

H_4^* . Существует прямая, состоящая из $m > 0$ точек.

Из этих аксиом читатель без труда выведет следующие теоремы:

*) Под конечной плоскостью здесь, по-видимому, подразумевается система, удовлетворяющая аксиомам I_1, I_2, I_4 . — Прим. перес.

1° Число всех точек и число всех прямых плоскости равны соответственно

$$(m+n)(m-1)+1 \quad \text{и} \quad \frac{m+n}{m} [(m+n)(m-1)+1]^*).$$

2° Число m является делителем числа $n(n-1)$.

3° При $m > 2$ плоскость $\langle m, 2 \rangle$ не существует.

К сожалению, система H^* приводит, как мы увидим, к излишне широкому попятно гиперболической плоскости, охватывая и такие фигуры, которые тривиальны и не выражают существа дела. Определим минимальное число элементов в модели H^* и укажем такую минимальную модель в евклидовом пространстве.

Из аксиом системы H^* и теоремы 1° вытекает, что минимальной $\langle m, n \rangle$ -плоскостью должна быть $\langle 2, 2 \rangle$ -плоскость, если она существует. Но она, как мы сейчас увидим, действительно существует и состоит из 5 точек и 10 прямых.

Пусть в трехмерном евклидовом пространстве выбрано 5 точек P_1, P_2, P_3, P_4 и P_5 , никакие три из которых не лежат на одной прямой и никакие четыре не лежат в одной плоскости. Обозначим через l_{rs} прямую, соединяющую точки P_r и P_s ($r \neq s$; $r, s = 1, \dots, 5$), — всего имеется десять таких прямых. Эти точки и прямые будем считать «точками» и «прямыми» $\langle 2, 2 \rangle$ -плоскости. Мы получим модель, удовлетворяющую всем аксиомам системы H^* (рис. 12).

Будем пока искать другие модели также в евклидовом пространстве. Обозначим найденную фигуру из 5 точек через $\nabla(5)$ и укажем следующее обобщение: пусть $\nabla(k)$

*) Теорему 1° нельзя считать вполне очевидной. Наметим вкратце ее доказательство.

В силу H_1^* существует прямая l_0 из m точек. Поэтому через всякую точку P вне l_0 проходит m прямых, пересекающих l_0 , и n прямых, не пересекающих l_0 (согласно H_2^*), т. е. в общей сложности $m+n$ прямых. Пусть l — произвольная прямая, отличная от l_0 , и P — точка вне l и l_0 . Из $m+n$ прямых, проходящих через P , ровно n прямых не пересекает l (аксиома H_3^*), поэтому l содержит в точности m точек. Отсюда легко определяется число точек плоскости. Если умножить число точек плоскости на число $m+n$ прямых, проходящих через каждую точку, и учесть, что каждая прямая плоскости считается при этом m раз, то мы получим вторую из доказываемых формул. — Прим. перес.

означает фигуру из точек P_1, P_2, \dots, P_k , никакие три из которых не лежат на одной прямой и никакие четыре не принадлежат одной плоскости. Число прямых $P_r P_s = l_{rs}$ ($r \neq s$; $r, s = 1, 2, \dots, k$) в фигуре $\nabla(k)$ есть $(k-1)k/2$. Легко видеть, что модель $\nabla(k)$ удовлетворяет определению $\langle 2, k-3 \rangle$ -плоскости. На рис. 13 изображена модель $\nabla(6)$, т. е. $\langle 2, 3 \rangle$ -плоскость.

Таким образом, имея дело с системой аксиом H^* , мы получаем бесконечную последовательность тривиальных фигур $\nabla(5)$, $\nabla(6)$, $\nabla(7)$, в качестве моделей конечной регулярной гиперболической плоскости. Постараемся поэтому усовершенствовать систему H^* , с тем чтобы исключить из числа моделей все ∇ -фигуры.

В сущности, достаточно заменить требование $m > 0$ в H_4^* несколько более сильным требованием $m > 2$, из которого, в силу теоремы 3°, будет следовать, что случай $n = 2$ невозможен, т. е. условие $n > 1$ в H_3^* можно заменить условием $n > 2$. Однако эта видоизмененная система аксиом также будет допускать некоторые тривиальные модели. Для преодоления этих трудностей мы воспользуемся иным подходом к определению гиперболической плоскости, предложенным Кроузом.

Мы введем понятие, роль которого раскрывается в одном замечательном свойстве обычного пространства. Рассмотрим подмножество T плоскости, содержащее по меньшей мере две точки и не являющееся прямой, но обладающее следующим свойством: всякая прямая, соединяющая две точки из T , содержится в T .

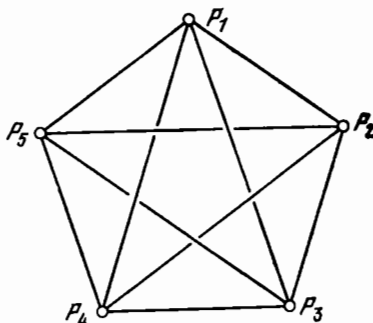


Рис. 12.

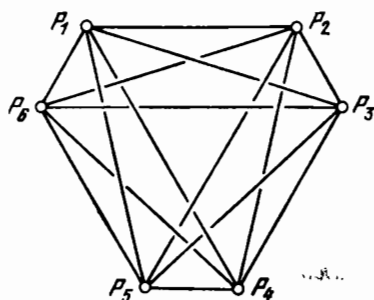


Рис. 13.

На обычной евклидовой плоскости подобного собственного подмножества T не существует. Аналогично, если взять конечную проективную плоскость, то подмножество T должно содержать какие-нибудь две точки A и B , а значит, и все $q + 1$ точек прямой AB . Далее, в T должна найтись точка C , отличная от точек прямой AB . Но тогда все прямые, соединяющие точку C с точками прямой AB , также принадлежат T , т. е. T совпадает со всей плоскостью. Однако каждая фигура $\nabla(k)$, являющаяся, согласно H^* , гиперболической плоскостью, содержит правильное подмножество T с указанным выше свойством. В самом деле, в качестве T можно взять любой подтреугольник фигуры $\nabla(k)$. Если плоскость содержит правильное подмножество T , то будем называть это подмножество *трактом* плоскости. Таким образом, евклидова, а также классическая и конечная проективная плоскости не имеют трактов.

Для определения гиперболической плоскости Кроув предложил систему аксиом, которая обеспечивает отсутствие трактов на плоскости. Рассмотрим следующую систему аксиом H :

H_1 . Для любых двух точек существует единственная инцидентная им прямая.

H_2 . Существуют такие числа m и n , что, какова бы ни была прямая l , через любую точку P , не лежащую на l , проходит m прямых, пересекающих l , и n прямых, не пересекающих l .

H_3 . Существуют три точки, не лежащие на одной прямой.

H_4 . $(m - 1)^2 > n > 2$.

Фигуру, удовлетворяющую системе H , снова будем называть $\langle m, n \rangle$ -плоскостью.

Нетрудно доказать, что для числа точек и числа прямых $\langle m, n \rangle$ -плоскости остаются верными выражения, указанные в теореме 1°.

Т е о р е м а К р о у в а. В плоскости, определяемой системой H , не существует трактов.

Д о к а з а т е л ь с т в о. Допустим, что плоскость S , удовлетворяющая системе H , содержит тракт T . В тракте T найдутся три точки, не лежащие на одной прямой, скажем точки A , B и C . Возьмем произвольную точку $P \in S \setminus T$; через нее проходят $\lambda = m + n$ прямых, причем, в силу H_4 ,

$\lambda < m + (m - 1)^2 = m(m - 1) + 1$. Соединим точку C со всеми точками прямой AB — получится m прямых, содержащих в общей сложности $m(m - 1) + 1$ точек плоскости, которые все принадлежат T . Соединив все эти точки с точкой P , мы получим $m(m - 1) + 1$ различных прямых, проходящих через P , поскольку точка P не может лежать ни на какой прямой, проходящей через две точки из T . Таким образом, мы пришли к противоречию, и теорема доказана.

Теорема. *Фигура, удовлетворяющая системе аксиом H , существует.*

Доказательство. В силу H_4 плоскость с минимальным числом элементов, удовлетворяющая системе аксиом H , должна быть $\langle 3, 3 \rangle$ -плоскостью, если таковая существует. В силу теоремы 1° $\langle 3, 3 \rangle$ -плоскость должна состоять из 13 точек и 26 прямых. Такая плоскость действительно существует, ее таблица инцидентности приведена на рис. 14. Множество точек этой $\langle 3, 3 \rangle$ -плоскости можно разбить следующими двумя способами:

$$l_5 \cup l_9 \cup l_{11} \cup l_{25} \cup P_9 \quad \text{и} \quad l_1 \cup l_{18} \cup l_{22} \cup l_{24} \cup P_2;$$

при этом каждая точка плоскости, отличная от P_2 и P_9 , может быть представлена единственным образом как точка пересечения некоторой прямой из первого разбиения с некоторой прямой из второго разбиения.

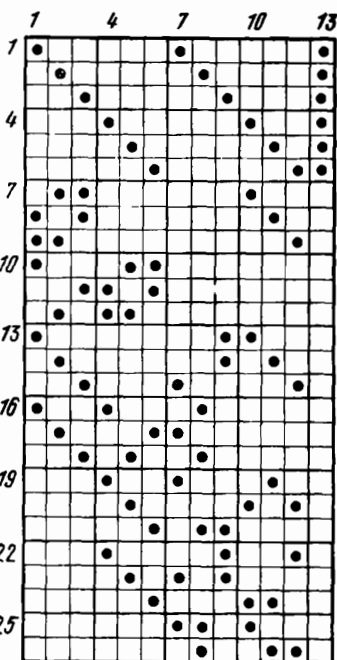


Рис. 14.

1.10. Плоскости Галуа и теорема Декарта

Когда проективная геометрия была впервые построена как обобщение евклидовой геометрии, теорема Декарта о перспективных треугольниках выступала лишь в каче-

стве следствия других, более простых теорем. Позднее, в поисках путей для независимого обоснования проективной геометрии, теорема Дезарга приобрела фундаментальное значение. В последующем изложении теорему Дезарга будем иногда для краткости называть D-теоремой или теоремой D.

Исследуя возможности введения координат на проективной плоскости без привлечения евклидовой метрики, Гильберт показал, что этой цели можно достигнуть с помощью теоремы Дезарга.

Гильберт фиксирует три точки O , U и V на прямой и, опираясь на аксиомы инцидентности и D-теорему, указывает две конструкции, каждая из которых по любой паре точек прямой, отличных от V , позволяет найти определенную точку прямой, также отличную от V . Эти геометрические операции зависят только от выбора тройки точек O , U , V . Одну из операций Гильберт называет сложением, другую — умножением и доказывает, что для этих операций выполняются все аксиомы поля, кроме аксиомы о коммутативности умножения. Для коммутативности умножения необходимо и достаточно, чтобы выполнялась еще теорема Паскаля (сокращенно: P-теорема) о шести точках, располагающихся по три на каждой из двух данных прямых. Эти факты легли в основу построения координатной системы без использования метрики.

Таким образом, стремясь получить аксиоматическое определение проективной плоскости, Гильберт сосредоточил свое внимание на D-теореме и P-теореме. Он доказал, что теорема Дезарга не выводится из аксиом инцидентности для плоскости. Поэтому теорему Дезарга следует присоединить в качестве четвертой аксиомы к трем аксиомам инцидентности, определяющим проективную плоскость. Гильберт доказал, что в этой расширенной системе аксиом теорема Паскаля недоказуема. Напротив, как было показано Гессенбергом, при добавлении к аксиомам инцидентности в качестве еще одной аксиомы теорема Паскаля получается система — обозначаемая IP , — в которой теорема Дезарга выводится.

Если проективная плоскость задается системой аксиом IP , то ее аналитическая геометрия, как было показано Гессенбергом, почти не отличается от аналитической геометрии классической проективной плоскости; разница

лишь в том, что в первом случае координатное поле обязательно является полем действительных чисел.

Придерживаясь намеченной здесь схемы, мы получаем бесконечно много проективных плоскостей, включая плоскости Галуа, рассмотренные ранее.

Завершим это краткое изложение истории вопроса построением плоскостей Галуа и рассмотрением некоторых теорем геометрии этих плоскостей.

1° Пусть $K = GF(q)$, $q = p^r$ (p — простое, а r — целое положительное число). Рассмотрим множество всех последовательностей (x_1, x_2, x_3) из трех элементов поля K (короче — троек элементов из K), за исключением последовательности $(0, 0, 0)$. Это множество разобьем на классы следующим образом: две тройки (x_1, x_2, x_3) и (y_1, y_2, y_3) тогда и только тогда принадлежат одному классу, когда найдется такой элемент $\lambda \in K$, $\lambda \neq 0$, для которого

$$y_1 = \lambda x_1, \quad y_2 = \lambda x_2, \quad y_3 = \lambda x_3.$$

Эти классы будем называть *точками*. Всякий класс однозначно определяется одной из своих троек (x_1, x_2, x_3) . Всякую тройку будем называть *однородной координатной тройкой* точки, которой эта тройка принадлежит.

Поскольку $GF(q)$ содержит q элементов, то множество всех троек — исключая тройку $(0, 0, 0)$ — состоит из $q^3 - 1$ элементов. Далее, λ может принимать $q - 1$ значений, поэтому в любом классе содержится $q - 1$ элементов, откуда получается, что число точек (классов) равно $q^2 + q + 1$.

Подмножество множества всех точек, определяемое уравнением

$$a_1x_1 + a_2x_2 + a_3x_3 = 0,$$

где элементы a_1, a_2, a_3 принадлежат K и не все равны нулю, будем называть *прямой*. Ясно, что если

$$b_1 = \lambda a_1, \quad b_2 = \lambda a_2, \quad b_3 = \lambda a_3 \quad (\lambda \in K, \lambda \neq 0),$$

то уравнение

$$b_1x_1 + b_2x_2 + b_3x_3 = 0$$

определяет то же подмножество, что и первое уравнение. Как мы вскоре убедимся, верно и обратное: если эти два уравнения определяют одно и то же множество точек,

то их коэффициенты удовлетворяют приведенному выше условию.

Для каждого поля K справедливы следующие теоремы:

A. Если тройки (x_1, x_2, x_3) и (y_1, y_2, y_3) определяют две различные точки, то существует единственная, с точностью до множителя λ , ненулевая тройка $[a_1, a_2, a_3]$, удовлетворяющая условиям

$$a_1x_1 + a_2x_2 + a_3x_3 = 0,$$

$$a_1y_1 + a_2y_2 + a_3y_3 = 0.$$

B. Если не существует такого $\lambda \in K$, что одно из уравнений

$$a_1x_1 + a_2x_2 + a_3x_3 = 0,$$

$$b_1x_1 + b_2x_2 + b_3x_3 = 0$$

получается из другого умножением на λ , то найдется единственная, с точностью до множителя μ , ненулевая тройка (x_1, x_2, x_3) , удовлетворяющая каждому из этих уравнений.

Но эти две теоремы как раз и означают, что для точек и прямых — как они здесь определены — выполняются соответственно аксиомы I_1 и I_2 .

Из теоремы A следует, что тройки $[a_1, a_2, a_3]$ и $[b_1, b_2, b_3]$ определяют одну и ту же прямую тогда и только тогда, когда существует $\lambda \neq 0$ такое, что $b_j = \lambda a_j$ ($j = 1, 2, 3$). Поэтому ненулевая тройка $[a_1, a_2, a_3]$ называется *координатной тройкой прямой*; элементы этой тройки называются *однородными координатами прямой*.

Аксиоме I_3 удовлетворяют следующие четыре точки:

$$(1, 0, 0), \quad (0, 1, 0) \quad (0, 0, 1), \quad (1, 1, 1).$$

Наконец, определим число точек на каждой прямой. Для этого рассмотрим, например, прямую $[1, 0, 0]$, т. е. прямую, заданную уравнением

$$1 \cdot x_1 + 0 \cdot x_2 + 0 \cdot x_3 = 0.$$

Ясно, что этому уравнению удовлетворяют те и только те тройки, которые имеют вид $(0, x_2, x_3)$. Из элементов поля K можно составить q^2 различных пар; поэтому, если не считать тройки $(0, 0, 0)$, которой не отвечает никакая точка, то получится $q^2 - 1$ троек указанного вида — по $q - 1$ троек в $q + 1$ различных классах. Следовательно,

данная прямая, а значит и всякая другая прямая, содержит $q + 1$ точек, т. е. плоскость имеет порядок q .

Определенная таким образом плоскость называется *плоскостью Галуа* над координатным полем $GF(q)$ и обозначается символом $S_{2,q}$.

2° Взаимозаменяемость точек и прямых по принципу двойственности выражается во взаимозаменяемости знаков (...) и [...] в принятых выше определениях.

Во избежание недоразумений следует с осторожностью пользоваться в проективных пространствах терминологией и понятиями векторных пространств. Можно, например, считать тройку (z_1, z_2, z_3) линейной комбинацией троек (x_1, x_2, x_3) и (y_1, y_2, y_3) с коэффициентами из K и писать

$$\lambda(x_1, x_2, x_3) + \mu(y_1, y_2, y_3) = (z_1, z_2, z_3),$$

если $\lambda, \mu \in K$ и выполняются равенства

$$z_1 = \lambda x_1 + \mu y_1, \quad z_2 = \lambda x_2 + \mu y_2, \quad z_3 = \lambda x_3 + \mu y_3.$$

Тройки (x_1, x_2, x_3) , (y_1, y_2, y_3) и (z_1, z_2, z_3) определяют три точки, скажем X, Y и Z ; однако запись $\lambda X + \mu Y = Z$, равно как и выражение «линейная комбинация точек» некорректны ввиду их неоднозначности.

В самом деле, буквы X и Y обозначают классы, состоящие из $q - 1$ троек; выбирая в качестве представителей этих классов различные тройки, мы, очевидно, будем получать различные линейные комбинации (z_1, z_2, z_3) . Если при этом $X \neq Y$, то среди полученных линейных комбинаций найдутся такие, которые принадлежат разным классам.

Проиллюстрируем эту ситуацию на следующем примере.

Пусть K есть поле классов вычетов по модулю 3, т. е. $K = GF(3)$. Таблицы операций для этого поля будут

+	0	1	2	×	0	1	2
0	0	1	2	0	0	0	0
1	1	2	0	1	0	1	2
2	2	0	1	2	0	2	1
	A				M		

Выпишем множество всех координатных троек, разбив его на классы:

$$\begin{aligned}
 P_1: & \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} \right\}; & P_2: & \left\{ \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix} \right\}; & P_3: & \left\{ \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 2 \end{pmatrix} \right\}; \\
 P_4: & \left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \\ 0 \end{pmatrix} \right\}; & P_5: & \left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 2 \end{pmatrix} \right\}; & P_6: & \left\{ \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 2 \end{pmatrix} \right\}; \\
 P_7: & \left\{ \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \\ 2 \end{pmatrix} \right\}; & P_8: & \left\{ \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} \right\}; & P_9: & \left\{ \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix} \right\}; \\
 P_{10}: & \left\{ \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix} \right\}; & P_{11}: & \left\{ \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix} \right\}; \\
 P_{12}: & \left\{ \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 2 \end{pmatrix} \right\}; & P_{13}: & \left\{ \begin{pmatrix} 2 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix} \right\}.
 \end{aligned}$$

Каждый класс состоит из двух троек. В каждом классе можно выбрать в качестве представителя ту тройку, у которой *последний ненулевой элемент является единичным элементом поля K*. Такой выбор представителей вскоре нам пригодится.

Возвращаясь к интересующему нас вопросу, выясним, что может означать выражение «линейная комбинация точек» $P_8 + 2P_{13}$. Возможны следующие выборы представителей для пары точек P_8, P_{13} :

$$\begin{aligned}
 & (2, 1, 0), (2, 2, 1); (2, 1, 0), (1, 1, 2); \\
 & (1, 2, 0), (2, 2, 1); (1, 2, 0), (1, 1, 2).
 \end{aligned}$$

Комбинация $P_8 + 2P_{13}$ означает при этом поочередно тройки $(0, 2, 2), (1, 0, 1), (2, 0, 2), (0, 1, 1)$, иначе говоря, точки P_6, P_5, P_5, P_6 , т. е. получается две, а не одна точка, как было бы в случае векторного пространства. Легко проверить, что получившиеся две точки P_5 и P_6 лежат на прямой

$$x_1 + x_2 + 2x_3 = 0,$$

соединяющей точки P_8 и P_{13} ; более того, эти четыре точки исчерпывают множество точек данной прямой.

Вообще, для ненулевых элементов $\lambda, \mu \in K = GF(q)$ и $P_j, P_k \in S_{2,q}$ комбинация $\lambda P_j + \mu P_k$, как можно про-

верить, неоднозначна и включает в себе $q - 1$ точек, получающихся при различных выборах троек в качестве представителей точек P_j и P_k . И опять-таки указанные $q - 1$ точек вместе с двумя исходными точками исчерпывают множество всех точек прямой, соединяющей P_j и P_k .

Однако можно устранить неоднозначность линейной комбинации точек путем подходящей нормализации соответствующих однородных координатных троек. Выше уже был указан один способ нормализации: из $q - 1$ эквивалентных координатных троек, определяющих точку, выбирается тройка, последний ненулевой элемент которой является единичным; эта тройка будет называться *нормированной координатной тройкой точки*.

Теперь мы следующим образом определим точку C , которая будет считаться линейной комбинацией $\lambda A + \mu B$ точек A и B с коэффициентами λ и μ : пусть точки A и B имеют нормированные координатные тройки (a_1, a_2, a_3) и (b_1, b_2, b_3) соответственно; тогда за точку C принимается точка, определяемая однородной координатной тройкой

$$(\lambda a_1 + \mu b_1, \lambda a_2 + \mu b_2, \lambda a_3 + \mu b_3).$$

Конечно, указанная тройка не обязательно будет нормированной.

Ясно, что если $\lambda = \mu = 0$, то линейная комбинация $\lambda A + \mu B$ не является точкой, ибо тройка $(0, 0, 0)$ не определяет никакой точки. Далее, если $\lambda \neq 0$, но $\mu = 0$, то точка C совпадает с A ; аналогично, при $\lambda = 0$, но $\mu \neq 0$ точка C совпадает с B . Очевидно, что если $\lambda' = \sigma\lambda$ и $\mu' = \sigma\mu$, то линейные комбинации $\lambda A + \mu B$ и $\lambda' A + \mu' B$ либо задают одну и ту же точку, либо обе равны тройке $(0, 0, 0)$. Таким образом, если $\mu \neq 0$ и комбинация $\lambda A + \mu B$ отлична от тройки $(0, 0, 0)$, то она определяет ту же точку, что и комбинация $\nu A + B$, где $\nu = \lambda\mu^{-1}$. Следовательно, общее число точек, определяемых всевозможными комбинациями вида $\lambda A + \mu B$, можно найти, перебирая все комбинации вида $\nu A + B$ для различных $\nu \in K$ и присоединяя к ним точку A , которую нельзя представить в последней форме (если она отлична от точки B).

Легко видеть, что если $A \neq B$, то $\lambda A + \mu B = (0, 0, 0)$ тогда и только тогда, когда $(\lambda, \mu) = (0, 0)$.

Далее, если $v \neq v'$, то точка $vA + B$ отлична от точки $v'A + B$, иначе мы имели бы

$$(v' - \sigma v)A + (1 - \sigma)B = (0, 0, 0),$$

откуда, согласно сделанному замечанию, следовало бы $v' - \sigma v = 0$ и $1 - \sigma = 0$, т. е. $v = v'$ — вопреки предположению.

Таким образом, получается q различных точек, отвечающих q значениям v , и поэтому общее число точек, определяемых комбинациями вида $\lambda A + \mu B$, равно $q + 1$.

Пусть $u_1x_1 + u_2x_2 + u_3x_3 = 0$ есть уравнение прямой, соединяющей точки A и B . Поскольку

$$u_1a_1 + u_2a_2 + u_3a_3 = 0, \quad u_1b_1 + u_2b_2 + u_3b_3 = 0,$$

то

$$u_1(\lambda a_1 + \mu b_1) + u_2(\lambda a_2 + \mu b_2) + u_3(\lambda a_3 + \mu b_3) = 0,$$

т. е. всякая точка, являющаяся линейной комбинацией исходных точек, принадлежит данной прямой; более того, указанными точками исчерпывается множество всех точек этой прямой, ибо всякая прямая плоскости Галуа порядка q содержит в точности $q + 1$ точек.

3° Воспользуемся теперь полученными результатами и докажем, что *теорема Дезарга верна на любой плоскости Галуа*.

Т е о р е м а. Пусть шесть различных точек образуют два собственных треугольника $A_1A_2A_3$ и $B_1B_2B_3$. Если прямые A_1B_1 , A_2B_2 , A_3B_3 имеют общую точку D , то точки

$$C_1 = A_2A_3 \cap B_2B_3, \quad C_2 = A_3A_1 \cap B_3B_1, \\ C_3 = A_1A_2 \cap B_1B_2$$

все различны и лежат на одной прямой d .

Д о к а з а т е л ь с т в о. Рассмотрим сначала частный случай, когда точка D совпадает с одной из шести данных точек. Пусть, например, $D = A_1$. Тогда точки A_1 , A_2 и B_2 лежат на одной прямой, и то же верно для точек A_1 , A_3 и B_3 . Поэтому $C_3 = A_1A_2 \cap B_1B_2 = B_2$ и $C_2 = A_3A_1 \cap B_3B_1 = B_3$. Далее, точка $A_2A_3 \cap B_2B_3 = C_1$ не может совпасть ни с B_2 , ни с B_3 (иначе получилось бы $A_2 = B_2$ или $A_3 = B_3$, что противоречит условию

теоремы). Таким образом, точки $C_1, C_2 = B_3$ и $C_3 = B_2$ все различны и лежат на одной прямой $d = B_2B_3$.

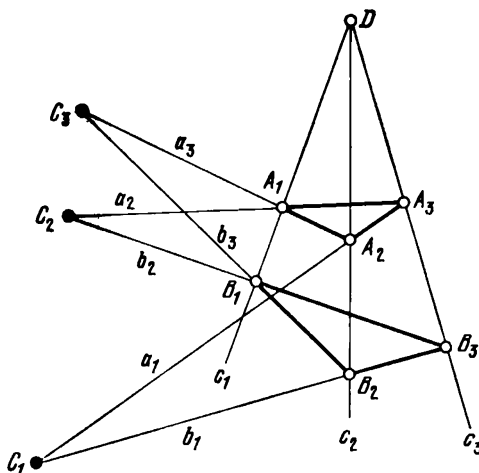


Рис. 15.

Перейдем теперь к общему случаю (рис. 15). Точки B_1, B_2 и B_3 можно представить (необязательно в нормированном виде) как линейные комбинации

$$B_1 = \lambda A_1 + D, \quad B_2 = \mu A_2 + D, \quad B_3 = \nu A_3 + D$$

$$(\lambda \neq 0, \quad \mu \neq 0, \quad \nu \neq 0),$$

где для точек A_1, A_2, A_3 и D берутся нормированные координатные тройки. Отсюда получаем

$$B_1 - B_2 = \lambda A_1 - \mu A_2, \quad B_2 - B_3 = \mu A_2 - \nu A_3,$$

$$B_3 - B_1 = \nu A_3 - \lambda A_1.$$

Комбинация $B_1 - B_2$ есть некоторая точка C_3 прямой B_1B_2 , а комбинация $\lambda A_1 - \mu A_2$ есть точка прямой A_1A_2 . Следовательно, $C_3 = A_1A_2 \cap B_1B_2$. Рассуждая аналогично, получаем, что точками пересечения соответственных сторон треугольников являются точки

$C_1 = \mu A_2 - \nu A_3$, $C_2 = \nu A_3 - \lambda A_1$, $C_3 = \lambda A_1 - \mu A_2$. Эти точки различны. Действительно, если бы две из них, скажем C_1 и C_2 , совпадали, то для некоторого $\sigma \neq 0$

выполнялось бы равенство $\mu A_2 - \nu A_3 = \sigma (\nu A_3 - \lambda A_1)$. Отсюда следовало бы

$$\mu A_2 + \sigma \lambda A_1 = (1 + \sigma) \nu A_3, \quad \lambda \mu \nu \neq 0,$$

т. е. точки A_1 , A_2 и A_3 лежали бы на одной прямой, вопреки условию теоремы.

Пользуясь приведенными выше выражениями, задающими точки C_1 , C_2 , C_3 в виде линейных комбинаций, находим

$$C_1 + C_2 = (-1) \cdot C_3.$$

Таким образом, точки C_1 , C_2 и C_3 лежат на одной прямой. Теорема доказана.

Т е о р е м а. *Проективная плоскость порядка q , определенная аксиомами I_1 , I_2 , I_3 , D, изоморфна плоскости Галуа.*

Доказательство этой теоремы будет дано в главе 2, посвященной детальному изучению геометрии плоскостей Галуа.

1.11. Недезаргова плоскость

В первых примерах (моделях), показывающих невыводимость теоремы Дезарга из аксиом I_1 , I_2 , I_3 , прямые содержали континуум точек (примеры Гильберта и Моултона). Затем были указаны примеры конечных плоскостей, в которых теорема Дезарга неверна (примеры Веблена и Веддербарна). Четыре с половиной десятилетия спустя Холлом был найден особенно поучительный пример. Плоскость Холла содержит лишь счетное множество точек на каждой прямой. Хотя модель Холла бесконечна, мы рассмотрим ее здесь, поскольку из нее можно извлечь примеры конечных недезарговых плоскостей.

На рис. 16' представлено несколько первых таблиц из последовательности таблиц инцидентности T^1 , T^2 , T^3 , ... Члены этой последовательности называются *ступенями* определяемой нами плоскости (столбцы, как обычно, считаются точками, а строки — прямыми ступени). Первая ступень представляет собственный четырехугольник, для которого выполняется аксиома I_3 . Поскольку каждая ступень является расширением предыдущей ступени, то аксиома I_3 выполняется для всех ступеней.

Последовательность ступеней построена таким образом, что I_1 выполняется для нечетных ступеней, а I_2 — для четных. Рассмотрим новую последовательность таблиц:

$$T_1 = T^1, \quad T_2 = T^2 - T^1, \quad T_3 = T^3 - T^2,$$

Это таблицы, состоящие поочередно из «прямых» и «точек», добавляются к таблицам последовательных ступеней — к каждой ступени присоединяются либо недостающие в ней «точки пересечения», либо недостающие «соединяющие прямые».

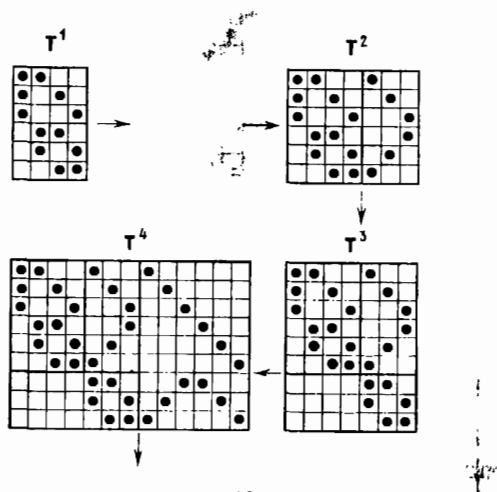


Рис. 16.

Для каждой пары строк (столбцов), не содержащих двух знаков \bullet в двух клетках какого-либо одного столбца (одной строки), добавляется столбец (строка) с двумя знаками в соответствующих клетках. Разумеется, на каждой стадии число добавляемых столбцов (строк) конечно, так как подлежащая расширению таблица инцидентности имеет только конечное число различных пар строк (пар столбцов).

Этот процесс попеременного добавления строк и столбцов продолжается неограниченно. В самом деле, если бы на некотором этапе очередную ступень нельзя было бы расширить ни за счет новых строк, ни за счет новых столбцов, то выполнялись бы обе аксиомы I_1 и I_2 (а также

и аксиома I_3 , поскольку она выполняется для T^1); следовательно, мы получили бы конечную плоскость. Однако таблица инцидентности конечной плоскости имеет по

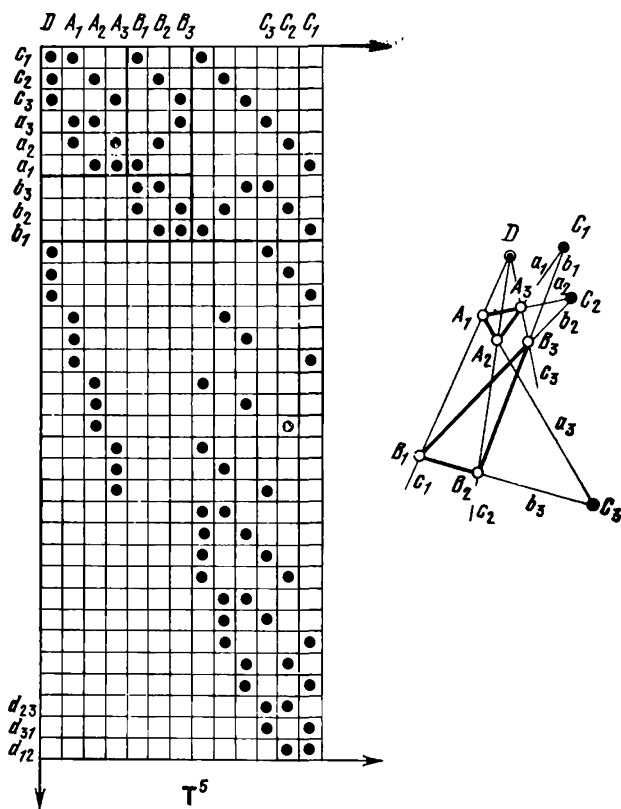


Рис. 17.

крайней мере три знака инцидентности в каждой строке и каждом столбце. Между тем полученная нами таблица инцидентности содержала бы строки или столбцы, добавленные на последнем этапе расширения, а в них было бы только два знака инцидентности, и мы пришли бы к противоречию.

Из способа построения таблиц вытекает, что фигура

$$H = T_1 \cup T_2 \cup T_3 \cup$$

удовлетворяет аксиомам I_1, I_2, I_3 и поэтому является проективной плоскостью, однако не конечной.

На рис. 17 показана часть T^5 таблицы Н. Уже по этой части можно проверить, что плоскость Н недезаргова. Рассмотрим таблицу T^5 и изображенную рядом с ней графическую схему. Треугольники $A_1A_2A_3$ и $B_1B_2B_3$ образуют перспективную пару относительно центра D . Однако это перспективное соответствие не является осевым: точки C_1, C_2, C_3 определяют попарно три прямые d_{12}, d_{23}, d_{31} и, значит, не лежат на одной прямой.

Рассмотрим последовательность ступеней плоскости и найдем для каждой ступени число точек и число прямых. Мы получим последовательность пар чисел, в которых первое число есть число точек, а второе — число прямых:

$$(4, 6), (7, 6), (7, 9), (9, 13), (13, 33),$$

Выпишем аналогичную последовательность пар чисел для конечных плоскостей порядков 2, 3, 4, ...:

$$(7, 7), (13, 13), (21, 21), (31, 31), (57, 57),$$

Сопоставление этих двух последовательностей наводит на один любопытный вопрос: можно ли дополнить таблицы T^2 и T^4 соответственно одной и четырьмя строками с таким распределением знаков, чтобы получились таблицы инцидентности конечных плоскостей соответственно порядков 2 и 3?

Положительный ответ на этот вопрос вытекает из рис. 18 и 19. Совмещая в одной строке распределения знаков в строках l_7, l_8, l_9 , дополняющих T^2 до T^3 , мы получим некоторую новую строку l^7 . В результате присоединения строки $l^7 = l_7 \cup l_8 \cup l_9$ к таблице T^2 получается таблица рис. 18. Далее, если строки, дополняющие T^4 до T^5 , объединить последовательно по три, то получатся четыре новых строки:

$$\begin{aligned} l^{10} &= l_{10} \cup l_{11} \cup l_{12}, & l^{11} &= l_{13} \cup l_{14} \cup l_{15}, \\ l^{12} &= l_{16} \cup l_{17} \cup l_{18}, & l^{13} &= l_{19} \cup l_{20} \cup l_{21}. \end{aligned}$$

Присоединение этих четырех строк к таблице T^4 дает таблицу рис. 19. Легко убедиться, что таблицы рис. 18 и 19

Рис. 18.

	P_1	P_4	P_7
L_1	•	•	
L_4	•		•
L_7		•	•

Рис. 19.

	P_1	P_4	P_6	P_{13}
L_1	•	•		•
L_6		•	•	
L_{10}	•			•
L_{13}		•	•	•

Рис. 18.

Рис. 19.

являются таблицами инцидентности конечных **плоскостей** порядков 2 и 3 соответственно.

1.12. Коллинеации и группы коллинеаций конечной плоскости

Как нетрудно догадаться по названию, в этом параграфе мы намерены распространить на конечные геометрии некоторые хорошо известные понятия классической проективной геометрии. Все факты, не являющиеся следствиями аксиом I_1, I_2, I_3 , мы исключим из нашей геометрии, а остающиеся факты будут специализированы в соответствии с аксиомой I_4 . Это и есть путь, ведущий к построению конечной проективной геометрии.

Прежде всего нам придется иметь дело с такими *взаимно однозначными отображениями плоскости в себя*, которые сохраняют коллинеарность точек (плоскость при этом рассматривается как точечное множество). Эти отображения характеризуются следующими условиями:

(1) *Каждой точке плоскости сопоставляется единственная точка, называемая ее образом.*

(2) Любая точка плоскости является образом единственной точки, называемой ее прообразом.

(3) Образы любых трех точек тогда и только тогда принадлежат одной прямой, когда сами эти точки принадлежат одной прямой.

Рассмотрим в качестве иллюстрации рис. 20 и 21. На обоих рисунках представлены конечные плоскости порядка 3. Между этими плоскостями установлено взаимно однозначное соответствие — соответствующие друг другу элементы обозначены одной и той же буквой. Оставим пока в стороне три вида обозначений для знаков инцидентности. На рис. 21 три идеальные точки указаны стрелками и три прямые изображены в виде кривых; «прямая» $\{P_1, P_2, P_3, P_4\} = l_1$ на рисунке не представлена.

В случае конечной плоскости отображения, удовлетворяющие условиям (1), (2), задаются подстановками (так же как и отображения множества прямых, если выполняются условия, двойственные условиям (1), (2)). Подстановки точек и прямых будут записываться в круглых и квадратных скобках соответственно. Рассмотрим в нашем примере два отображения: отображение точек

$$\omega = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 12 & 8 & 5 & 11 & 10 & 1 & 2 & 3 & 13 & 9 & 4 & 6 & 7 \end{pmatrix}$$

и отображение прямых

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 4 & 6 & 9 & 2 & 5 & 1 & 3 & 11 & 8 & 7 & 12 & 13 & 10 \end{bmatrix}.$$

Здесь выражение $(\dots \overset{j}{k} \dots)$ пишется вместо $(\dots \overset{P_j}{P_k} \dots)$ и означает, что образом точки P_j является точка P_k или, что то же самое, P_j есть прообраз P_k ; аналогично для прямых.

Условия, двойственные условиям (1), (2), (3), будем обозначать соответственно (1*), (2*), (3*). Очевидно, ω удовлетворяет условиям (1), (2), а σ — условиям (1*), (2*). Вообще, любая из $13!$ подстановок точек (прямых) удовлетворяет условиям (1), (2) (соответственно условиям (1*), (2*)). Но отнюдь не для каждой подстановки точек выполняется условие (3) (для подстановки прямых — условие (3*)).

Например, отображение ω переводит точки P_2, P_3, P_4 , лежащие на одной прямой, в точки P_8, P_5, P_{11} , также

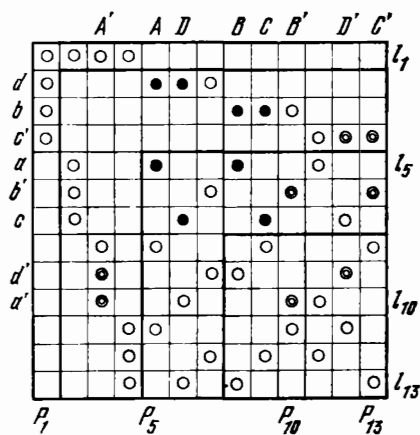


Рис. 20.

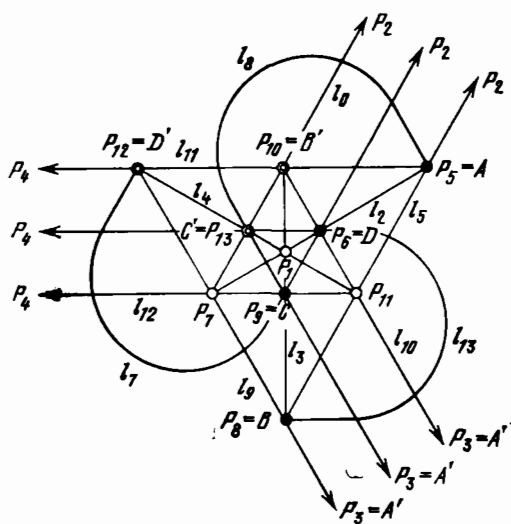


Рис. 21.

лежащие на одной прямой; неколлинеарные точки P_7, P_8, P_9 переводятся в неколлинеарные точки P_2, P_3, P_{13} ; точки P_1, P_2, P_3 лежат на одной прямой, а их образы P_{12}, P_8, P_5 — нет; неколлинеарные точки P_5, P_6, P_{10} переводятся в коллинеарные точки P_{10}, P_1, P_9 . Итак, отображение ω не удовлетворяет условию (3). Подобным же образом σ не удовлетворяет (3*).

На самом деле из $13!$ подстановок точек лишь $2^4 \cdot 3^3 \cdot 13 = 5616$ удовлетворяют условию (3); мы опускаем здесь доказательство этого факта. Ясно, что если отображение (подстановка) π точек удовлетворяет условию (3), то подмножество точек тогда и только тогда составляет прямую, когда образ этого подмножества при отображении π есть прямая. По этой причине отображение, удовлетворяющее условиям (1), (2), (3), называется *коллинеацией*. Например, для плоскости, представленной на рис. 20, подстановка

$$(1.12.1) \quad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 7 & 11 & 9 & 4 & 3 & 12 & 8 & 10 & 13 & 2 & 6 & 1 & 5 \end{pmatrix}$$

является коллинеацией. С помощью таблицы инцидентности этой плоскости и ее графической схемы (на рис. 21) легко найти подстановку λ прямых, индуцированную подстановкой π :

$$(1.12.2) \quad \lambda = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 12 & 9 & 6 & 2 & 10 & 5 & 4 & 8 & 3 & 7 & 1 & 13 & 11 \end{bmatrix}.$$

Из того, что условия (1), (2), (3) выполняются для отображения π , вытекает, что для λ выполняются условия (1*), (2*), (3*). Аналогично, исходя из отображения λ , удовлетворяющего условиям (1*), (2*), (3*), мы получаем отображение π , индуцированное λ , для которого выполняются условия (1), (2), (3). Таким образом, хотя следовало бы говорить о коллинеации $\langle \pi, \lambda \rangle$ или $\langle \lambda, \pi \rangle$, можно ограничиваться указанием лишь π или λ , ибо π однозначно определяет λ и наоборот.

В нашем примере точки P_4 и прямая l_8 совпадают со своими образами, т. е.

$$P_4 \xrightarrow{\pi} P_4 \quad \text{и} \quad l_8 \xrightarrow{\lambda} l_8.$$

Точки и прямые, обладающие этим свойством, называются *неподвижными (инвариантными) точками и прямыми коллинеации*.

Однако из того, что прямая l_8 неподвижна, не вытекает, что какие-либо ее точки также неподвижны, как это видно из подстановки

$$\begin{pmatrix} 3 & 5 & 9 & 13 \\ 9 & 3 & 13 & 5 \end{pmatrix},$$

являющейся ограничением отображения π на множество

$$l_8 = \{P_3, P_5, P_9, P_{13}\}.$$

Аналогично, прямые, проходящие через неподвижную точку, не обязательно неподвижны, как показывает, например, подстановка

$$\begin{bmatrix} 1 & 11 & 12 & 13 \\ 12 & 1 & 13 & 11 \end{bmatrix},$$

являющаяся ограничением отображения λ на пучок прямых $\{l_1, l_{11}, l_{12}, l_{13}\}$ с центром в точке P_4 . Вообще говоря, можно только утверждать, что неподвижная прямая и пучок прямых с неподвижным центром отображаются при коллинеации в самих себя.

Существует, однако, коллинеация, имеющая неподвижную точку и неподвижную прямую, которые обладают одним замечательным свойством. Чтобы проиллюстрировать это свойство на примере, рассмотрим на плоскости, представленной на рис. 20 и 21, отображение точек

$$(1.12.3) \quad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 1 & 3 & 2 & 4 & 12 & 13 & 11 & 8 & 9 & 10 & 7 & 5 & 6 \end{pmatrix}$$

и индуцированное им отображение прямых

$$(1.12.4) \quad \lambda = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 1 & 4 & 3 & 2 & 9 & 10 & 8 & 7 & 5 & 6 & 11 & 12 & 13 \end{bmatrix}.$$

В этой коллинеации *все четыре прямые $l_1, l_{11}, l_{12}, l_{13}$, проходящие через неподвижную точку P_4 , неподвижны*. Точку, обладающую указанным свойством, называют *центром коллинеации*. Аналогичное свойство выполняется для неподвижной прямой l_3 : *все четыре точки P_1, P_8, P_9, P_{10} , лежащие на неподвижной прямой l_3 , неподвижны*; прямая с таким свойством называется *осью коллинеации*. Естественным образом возникают следующие два вопроса:

1° Всегда ли коллинеация, обладающая центром, обладает и осью, и обратно?

2° Может ли коллинеация, отличная от тождественной, иметь несколько центров, или несколько осей?

Ответы на эти вопросы будут даны позднее. Заметим только, что тождественная коллинеация представляет собой отображение, в котором каждая точка и каждая прямая неподвижны, более того, каждая точка является центром, а каждая прямая — осью.

В приведенном выше примере центр P_4 коллинеации не лежит на оси коллинеации l_3 . Свяжем теперь каждую точку, отличную от неподвижных точек $P_1, P_4, P_8, P_9, P_{10}$, с образом этой точки. Аналогично, каждую прямую, отличную от неподвижных прямых $l_1, l_3, l_{11}, l_{12}, l_{13}$, свяжем с образом этой прямой. Мы получим следующие пары:

$$\begin{aligned} & (P_2, P_3), (P_3, P_2), (P_5, P_{12}), (P_6, P_{13}), \\ & (P_7, P_{11}), (P_{11}, P_7), (P_{12}, P_5), (P_{13}, P_6), \\ & [l_2, l_4], [l_4, l_2], [l_5, l_9], [l_6, l_{10}], \\ & [l_7, l_8], [l_8, l_7], [l_9, l_5], [l_{10}, l_6], \end{aligned}$$

в каждой из которых второй элемент является образом первого. Легко видеть, что всякая прямая, соединяющая точки какой-либо пары, неподвижна; *прямые, отвечающие всем указанным парам точек, пересекаются в центре P_4* . Коллинеация, обладающая подобным свойством, называется *перспективой относительно точки* (перспективой из точки). Аналогично, точка пересечения любых двух прямых, составляющих какую-либо из перечисленных выше пар прямых, лежит на оси l_3 . Коллинеация с таким свойством называется *перспективным соответствием относительно прямой*. В нашем примере мы получили *центрально-осевую коллинеацию*.

Приведем еще один пример центрально-осевой коллинеации, а именно рассмотрим отображение

$$(1.12.5) \quad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 1 & 2 & 3 & 4 & 7 & 5 & 6 & 10 & 8 & 9 & 13 & 11 & 12 \end{pmatrix}$$

и индуцированное им отображение

$$(1.12.6) \quad \lambda = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 1 & 2 & 3 & 4 & 6 & 7 & 5 & 9 & 10 & 8 & 12 & 13 & 11 \end{bmatrix}.$$

Неподвижная точка P_1 этой коллинеации является ее центром, а неподвижная прямая l_1 — осью, причем на этот раз $P_1 \in l_1$.

Если центр лежит на оси, то коллинеацию называют *элацией* *), в противном случае коллинеация называется *гомологией*. Таким образом, первый пример был примером гомологии, а второй — примером элации.

Из элементарной комбинаторики известно, что все подстановки n -элементного множества образуют группу — *полную группу подстановок данного множества*. Коллинеации конечной плоскости составляют подгруппу полной группы подстановок, действующих на множестве точек плоскости, поскольку, как легко видеть, произведение двух коллинеаций и обратный элемент для всякой коллинеации также являются коллинеациями. Эта подгруппа называется *группой коллинеаций* конечной проективной плоскости. Согласно *Эрлангенской программе* Ф. Клейна конечная проективная геометрия сводится к изучению группы коллинеаций. С этой точки зрения можно объяснить, например, тот факт, что в книге М. Холла «Теория групп» большая глава посвящена в основном геометрии конечных проективных плоскостей. Важную роль в изучении групп коллинеаций играют гомологии и элации.

Все степени какой-либо коллинеации образуют *циклическую группу*. Так, в примере рис. 2 степени коллинеации

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 5 & 6 & 7 & 1 \end{pmatrix}$$

составляют группу порядка 7. При этом коллинеация π не имеет неподвижных точек. Задача о приведении таблицы инцидентности конечной плоскости к циклическому виду сводится к отысканию подобной подгруппы в группе всех коллинеаций плоскости.

Коллинеации, квадраты которых совпадают с тождественной коллинеацией, имеют глубокий геометрический смысл. Такие коллинеации называются *инволюциями*. Коллинеация π , заданная подстановкой (1.12.3), является инволюцией. Поскольку эта инволюция представляет собой центрально-осевую коллинеацию, то ее можно считать аналогом осевой симметрии на евклидовой плоскости.

*) Или *проективным сдвигом*. — *Прим. перев.*

Роль оси симметрии играет здесь ось коллинеации — прямая l_3 , а прямым, перпендикулярным к оси симметрии, соответствуют прямые, проходящие через центр P_4 .

Порядком коллинеации π называется наименьшее целое положительное число r такое, что π^r есть тождественная коллинеация. Для полноты изложения отметим, что порядок коллинеации (1.12.1) равен 8, а коллинеации (1.12.5) — 3.

Связь между центрально-осевыми коллинеациями и теоремой Дезарга будет изучена позднее, но уже сейчас из рис. 21 непосредственно видно, что любой треугольник, составленный из инвариантных точек, и его образ при центрально-осевой коллинеации находятся в перспективном соответствии как относительно центра, так и относительно оси коллинеации. Например, в случае коллинеации (1.12.3) с центром P_4 и осью l_3 образом треугольника $P_5P_6P_{11}$ является треугольник $P_{12}P_{13}P_7$.

Как мы видим, между понятиями коллинеации на конечной плоскости и коллинеации на классической проективной плоскости существует значительная аналогия; используя эту аналогию, можно доказать многие теоремы конечной геометрии. Имеются, однако, и такие свойства конечной плоскости, которые существенно отличаются от свойств классической проективной плоскости и поэтому не могут быть доказаны по аналогии. Например, для классической проективной плоскости справедлива следующая теорема: для всякого отображения

$$\pi_0 = \begin{pmatrix} A & B & C & D \\ A' & B' & C' & D' \end{pmatrix}$$

четверки вершин собственного четырехугольника $ABCD$ на четверку вершин собственного четырехугольника $A'B'C'D'$ существует единственная коллинеация π , ограничение которой на множество $\{A, B, C, D\}$ совпадает с π_0 . Эта теорема выполняется также и для плоскостей Галуа, но не для всякой конечной плоскости. Первую часть этого утверждения мы только проиллюстрируем на примере, вторую же докажем.

В силу свойства (3) любая коллинеация переводит собственный четырехугольник снова в собственный четырехугольник. Четырехугольник $ABCD = P_5P_8P_9P_6$ рис. 20 переводится в четырехугольник $A'B'C'D' = P_3P_{10}P_{13}P_{12}$

того же рисунка отображением

$$\pi_0 = \begin{pmatrix} 5 & 8 & 9 & 6 \\ 3 & 10 & 13 & 12 \end{pmatrix},$$

которое реализуется коллинеацией π , заданной подстановкой (1.12.1).

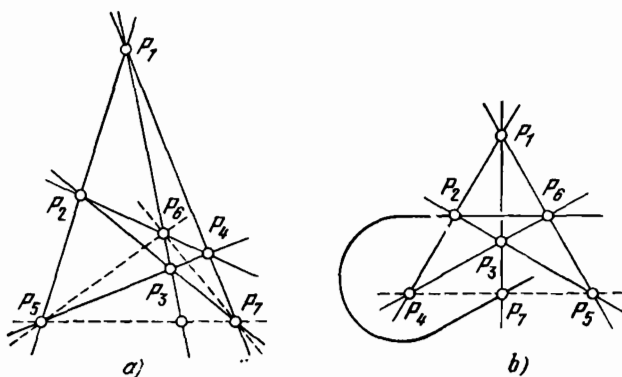


Рис. 22.

Прежде чем доказывать вторую часть нашего утверждения, сделаем несколько замечаний относительно плоскости Фано (рис. 22).

На классической проективной плоскости диагональные точки собственного четырехугольника составляют собственный треугольник, как показано на рис. 22, а. Диагональные точки, т. е. точки пересечения противоположных сторон четырехугольника, — это в данном случае точки P_5, P_6, P_7 :

$$P_5 = P_1P_2 \cap P_3P_4, \quad P_6 = P_1P_3 \cap P_2P_4,$$

$$P_7 = P_1P_4 \cap P_2P_3.$$

Треугольник $P_5P_6P_7$ — собственный.

Однако некоторые конечные плоскости допускают собственные четырехугольники с диагональными точками, лежащими на одной прямой. Рассмотрим, например, плоскость Фано, представленную на рис. 22, б. На этой плоскости все диагональные точки четырехугольника

$P_1P_2P_3P_6$, т. е. точки

$$P_4 = P_1P_2 \cap P_3P_6, \quad P_7 = P_1P_3 \cap P_2P_6,$$

$$P_5 = P_1P_6 \cap P_2P_3,$$

лежат на прямой l_5 . Всего на данной плоскости имеется семь собственных четырехугольников. Каждый из них получается удалением из плоскости точек какой-либо прямой, которые как раз и являются диагональными точками остающегося собственного четырехугольника.

Таким образом, на каждой плоскости следует различать два вида собственных четырехугольников:

1° Четырехугольники, диагональные точки которых образуют собственный треугольник, — *обыкновенные четырехугольники*.

2° Четырехугольники, диагональные точки которых лежат на одной прямой, — *четырехугольники Фано*. В случае плоскости Фано это такие четырехугольники, множество вершин и диагональных точек которых совпадает с множеством всех точек плоскости.

Отметим без доказательства, что на плоскости Галуа либо все четырехугольники обыкновенные, либо все они — четырехугольники Фано. Вторая возможность осуществляется, например, в случае плоскости Фано и в случае плоскости порядка 4, представленной на рис. 7. Существует плоскость порядка 9 (не являющаяся плоскостью Галуа), которая содержит как обыкновенные четырехугольники, так и четырехугольники Фано. Ясно, что, в силу свойства (3) (стр. 63), *всякий четырехугольник Фано переходит при коллинеации в четырехугольник Фано, а обыкновенный четырехугольник — в обыкновенный*.

После этого отступления вернемся к доказательству нашего утверждения относительно отображения π_0 , переводящего четырехугольник $ABCD$ в четырехугольник $A'B'C'D'$. Согласно сделанному выше замечанию имеется конечная плоскость, не являющаяся плоскостью Галуа, которая содержит как обыкновенные четырехугольники, так и четырехугольники Фано. Если в качестве одного из рассматриваемых четырехугольников выбрать четырехугольник Фано, а в качестве другого — обыкновенный, то отображение π_0 нельзя будет, очевидно, продолжить до коллинеации.

В дальнейшем *плоскостью Фано* будет называться всякая плоскость, не содержащая обыкновенных четырехугольников (т. е. плоскость, все собственные четырехугольники которой являются четырехугольниками Фано).

1.13. Сохраняющие коллинеарность отображения аффинной и регулярной гиперболической конечной плоскости

Рассмотрим аффинную плоскость порядка q , определяемую системой аксиом А. Эта плоскость состоит из q^2 точек и $q(q+1)$ прямых. Выделим из множества всех подстановок q^2 -элементного множества точек подмножество подстановок, которые удовлетворяют условию (3), сформулированному в начале параграфа 1.12. Легко проверить, что указанное подмножество подстановок есть подгруппа в группе всех подстановок. Эта подгруппа называется *группой коллинеаций аффинной плоскости*.

Из определения сразу же следует, что *при аффинных коллинеациях сохраняется параллельность прямых*. Действительно, если $a \parallel b$ и $a \neq b$, то множество $a' \cap b'$, где a' и b' — образы прямых a и b при аффинной коллинеации, пусто. В противном случае существовала бы точка P' такая, что $P' \in a'$ и $P' \in b'$, и для ее прообраза P выполнялись бы условия $P \in a$ и $P \in b$, а это противоречит исходному предположению.

Пусть S_0 — аффинная плоскость и G_0 — ее группа коллинеаций. Дополним плоскость идеальными точками, определяемыми как общие точки параллельных прямых, и идеальной прямой l , состоящей из этих точек. В результате получится новая плоскость S с группой коллинеаций G . На самом деле, группа G_0 изоморфна подгруппе $G(l)$ тех коллинеаций группы G , которые оставляют неподвижной прямую l . Мы уже знаем, что аффинные плоскости, полученные из S удалением различных прямых, могут быть неизоморфны между собой; это находит свое отражение в том факте, что группы $G_0(l_1)$ и $G_0(l_2)$, отвечающие каким-нибудь прямым l_1 и l_2 из S , необязательно изоморфны друг другу.

При изучении строения аффинных плоскостей важное значение имеют следующие виды центрально-осевых кол-

линеаций, различаемые по той роли, которую играют в них идеальные элементы:

(а) Если центр коллинеации не является идеальной точкой, но ее ось совпадает с идеальной прямой, то коллинеация называется *гомотетией*, а центр коллинеации — *центром гомотетии*.

(б) Если центр и ось коллинеации являются соответственно идеальной точкой и идеальной прямой, то коллинеация называется *переносом*. Гомотетия и перенос аналогичны одноименным преобразованиям в классической геометрии.

(с) Если центр коллинеации — идеальная точка, а ее ось не является идеальной прямой, то коллинеация называется *осевым аффинным преобразованием*.

(д) Если центр коллинеации — идеальная точка и лежит на оси коллинеации, которая, однако, не является идеальной прямой, то такую коллинеацию естественно было бы называть *аффинным сдвигом*. Общепринятого термина для обозначения этого понятия не существует, в немецкой литературе используется термин «Scherung».

Приведем следующий пример аффинного сдвига. На рис. 21 аффинная плоскость порядка 3 задается точками P_5, P_6, \dots, P_{12} и прямыми l_2, l_3, \dots, l_{13} (некоторые из них изображены на рисунке в виде кривых). Отображение точек

$$\pi = \begin{pmatrix} 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 7 & 5 & 6 & 8 & 9 & 10 & 12 & 13 & 11 \end{pmatrix}$$

и индуцированное им отображение прямых

$$\lambda = \begin{bmatrix} 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 2 & 3 & 4 & 9 & 10 & 8 & 12 & 13 & 11 & 6 & 7 & 5 \end{bmatrix}$$

отвечают всем требованиям определения (д).

Кроме проективной и аффинной плоскостей мы уже имели дело еще с одной фигурой, также именуемой конечной плоскостью. Речь идет о регулярной конечной гиперболической плоскости. Ясно, что и в этом случае можно было бы исследовать группу сохраняющих коллинеарность отображений плоскости на себя. Поскольку в дальнейшем мы не будем заниматься гиперболическими плоскостями, проанализируем подробно пример гиперболической плоскости, приведенный на рис. 14. Прежде всего

отметим следующий удивительный факт: в то время как порядок группы коллинеаций проективной плоскости порядка 3 равен 5616, порядок группы коллинеаций нашей плоскости, хотя эта плоскость также состоит из 13 точек, равен всего лишь 6. В обоих случаях из общего числа 13! подстановок берутся только те подстановки, которые сохраняют принадлежность любых трех точек одной прямой. Общее число троек точек, принадлежащих одной прямой, для проективной плоскости из 13 точек составляет 52, а для нашей гиперболической плоскости из 13 точек — 26. Таким образом, в последнем случае на выполнение условия (3) (стр. 63) налагается вдвое меньше ограничений. Но несмотря на это число допустимых подстановок получается в данном случае значительно меньше. Отбор подстановок, сохраняющих коллинеарность, является, по-видимому, трудной комбинаторной задачей; эта задача, однако, упрощается, если принять во внимание свойства некоторых указанных ниже фигур.

Рассмотрим две непересекающиеся прямые a и b на плоскости рис. 14 и точку C , не лежащую ни на одной из них. Каждая прямая плоскости содержит три точки; через каждую точку проходит 6 прямых, и если взять какую-либо прямую и точку вне ее, то из 6 прямых, проходящих через эту точку, 3 пересекают данную прямую, а 3 не пересекают. Следовательно, может случиться, что в фигуре Cab не всякая точка прямой a проектируется из C на прямую b ; более того, существует такая фигура Cab , что ни одна точка прямой a не проектируется на прямую b и ни одна точка прямой b не проектируется на прямую a ; например, можно взять

$$C = P_1, \quad a = l_3, \quad b = l_{12}.$$

Если каждая точка прямой a проектируется из C на b , то семерка точек, состоящая из точки C и точек прямых a и b , называется *перспективной семеркой точек* (рис. 23, i). На плоскости рис. 14 мы имеем следующую перспективную семерку:

$$C = P_{11}, \quad a = l_{15} = \{P_3, P_7, P_{12}\}, \quad b = l_{16} = \{P_1, P_4, P_8\}.$$

Точка P_{11} считается *центром* этой семерки. Укажем еще две перспективные семерки:

$$C = P_{13}, \quad a = l_8 = \{P_1, P_3, P_{11}\}, \quad b = l_{23} = \{P_7, P_9, P_5\}$$

и

$$C = P_{13}, \quad a = l_{14} = \{P_2, P_9, P_{11}\}, \quad b = l_{18} = \{P_8, P_3, P_5\}.$$

Отметим, что точка P_{13} является общим центром этих двух семерок. Точка P_1 не является центром никакой перспективной семерки точек. В соответствии с этими примерами

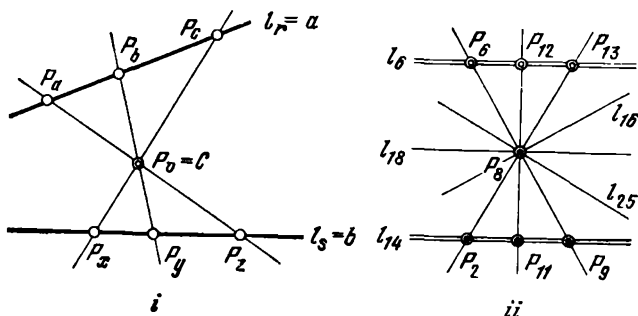


Рис. 23.

можно дать следующую классификацию точек нашей гиперболической плоскости: *двойные центры* (точки P_2, P_8, P_9, P_{11}), *простые центры* (точки P_6, P_{12}, P_{13}) и *обыкновенные точки*, т. е. точки, не являющиеся центрами (точки $P_1, P_3, P_4, P_5, P_7, P_{10}$).

Все $7 = 4 + 3$ центров образуют весьма замечательную фигуру (рис. 23, ii). Все простые центры лежат на одной прямой $l_6 = \{P_6, P_{12}, P_{13}\}$; назовем ее *простой осью*. Три из четырех двойных центров также лежат на одной прямой $l_{14} = \{P_2, P_9, P_{11}\}$; эту прямую будем называть *двойной осью*. Четвертый двойной центр — точка P_8 — не лежит ни на одной из этих осей, но три простых центра проектируются из этой точки в двойные центры, при этом каждая из трех проектирующих прямых называется *смешанной осью*.

По свойству (3) отображений, сохраняющих коллинеарность, образы перспективных семерок точек и только они снова являются перспективными семерками точек. Отсюда следует, что при этих отображениях двойные центры переходят в двойные центры, простые центры — в простые центры, обыкновенные точки — в обыкновенные

точки. Более того, точка P_8 всегда должна быть неподвижной, поскольку остальные три двойных центра лежат на одной прямой. Таким образом, эта точка обладает свойствами, выделяющими ее среди всех других точек плоскости; ее поэтому можно было бы назвать *главной* точкой плоскости. Из наших утверждений относительно сохранения типов точек вытекает, что образы простых, двойных и смешанных осей также являются осями тех же типов.

Теперь нетрудно убедиться, что сохраняющие коллинеарность преобразования гиперболической плоскости исчерпываются следующими шестью преобразованиями:

	1	2	3	4	5	6	7	8	9	10	11	12	13
π_1	1	2	3	4	5	6	7	8	9	10	11	12	13
π_2	7	2	5	10	3	12	1	8	11	4	9	6	13
π_3	4	9	7	1	10	13	3	8	2	5	11	12	6
π_4	3	9	10	5	7	12	4	8	11	1	2	13	6
π_5	10	11	1	7	4	13	5	8	2	3	9	6	12
π_6	5	11	4	3	1	6	10	8	9	7	2	13	12

Таблица Кэли этой группы подстановок имеет следующий вид (вместо каждого элемента π_k пишется его индекс k):

\times	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	4	3	6	5
3	3	5	1	6	2	4
4	4	6	2	5	1	3
5	5	3	6	1	4	2
6	6	4	5	2	3	1

Если сопоставить элементам $\pi_1, \pi_2, \pi_3, \pi_4, \pi_5, \pi_6$ соответственно перестановки $abc, acb, bac, bca, cab, cba$, то окажется, что эта таблица есть таблица умножения для полной группы подстановок трехэлементного множества $\{a, b, c\}$.

Полученными здесь результатами, дополняющими результаты параграфа 1.9, мы завершаем исследование $(3,3)$ -плоскости.

1.14. Конечные проективные плоскости и полные ортогональные системы латинских квадратов

В этом параграфе мы будем заниматься комбинаторными задачами, с которыми в настоящее время имеет дело математическая статистика. Но первая такая задача была рассмотрена еще Эйлером в 1782 году.

Знаменитая задача Эйлера, так называемая «задача о 36 офицерах», состоит в следующем. На военном параде 36 офицеров нужно выстроить в каре из шести перенг по шесть офицеров в каждой, причем известно, что от каждого из шести родов войск в параде участвует шесть офицеров шести различных рангов и в каждой перенге и в каждом ряду должно быть по одному офицеру каждого рода войск и каждого ранга. Эйлер пришел к выводу, что эта задача не имеет решения; весьма сложное доказательство этого факта было найдено Тарри лишь в 1900 году.

Из неразрешимости задачи Эйлера вытекает, как будет доказано впоследствии, невозможность конечной проективной плоскости порядка 6.

Прежде чем ввести некоторые понятия комбинаторики, нам потребуется определить одну алгебраическую структуру. Пусть Q — конечное множество из q элементов, и пусть операция на Q (которую мы будем называть умножением) удовлетворяет следующим аксиомам:

- (1) Если $a \in Q$ и $b \in Q$, то $ab = c \in Q$.
- (2) Если $a, b, c \in Q$ и $a \neq b$, то $ac \neq bc$ и $ca \neq cb$.

Примером, реализующим такую структуру, является четырехэлементное множество $Q = \{a, b, c, d\}$ с операцией, которая задана таблицей на рис. 24.

В качестве примера можно было бы взять таблицу Кэли любой группы, поскольку групповая операция удовлетворяет указанным выше аксиомам, однако рассматриваемая структура не обязана быть группой. Действительно, в нашем примере $(bc)d = ad = c$ и $b(cd) = ba = b$, т. е. операция не ассоциативна.

Конечную структуру, определяемую условиями (1), (2), будем называть конечной *квазигруппой*.

В таблице умножения конечной квазигруппы каждая строка и каждый столбец представляют собой некоторую перестановку элементов множества Q ; следовательно,

всякий элемент из Q встречается ровно один раз в каждой строке и в каждом столбце, т. е. клетки, занятые каким-либо элементом, распределены диагональным образом. Диагональные распределения, соответствующие разным элементам, не перекрываются, их называют *параллельными*. Так, параллельными будут распределения цифр 5 и 7 в таблице на рис. 25.

	a	b	c	d
a	a	b	d	c
b	b	c	a	d
c	c	d	b	a
d	d	a	c	b

Рис. 24.

0	7	5	8	3	1	4	2	6
1	8	3	6	4	2	5	0	7
2	6	4	7	5	0	3	1	8
3	1	8	5	0	7	2	6	4
4	2	6	3	1	8	0	7	5
5	0	7	4	2	6	1	8	3
6	4	2	1	8	3	7	5	0
7	5	0	2	6	4	8	3	1
8	3	1	0	7	5	6	4	2

Рис. 25.

Таблица размером $q \times q$, заполненная элементами q различных видов таким образом, что всякая строка и всякий столбец таблицы содержат ровно по одному элементу каждого вида, называется *латинским квадратом порядка q* . Ясно, что всякий латинский квадрат задает операцию некоторой квазигруппы. Элементы основного множества Q латинского квадрата будут обычно обозначаться как индексы $0, 1, 2, \dots, q-1$.

Рассмотрим класс всех латинских квадратов с основным множеством $Q = \{0, 1, 2, \dots, q-1\}$. Введем важное понятие ортогональности двух квадратов этого класса.

Сначала, однако, определим операцию, сопоставляющую каждой паре (L_1, L_2) латинских квадратов порядка q таблицу размером $q \times q$, каждая клетка которой содержит упорядоченную пару элементов — первый элемент пары берется из гомологичной *) клетки квадрата L_1 ,

*) Две клетки двух таблиц одного размера называются *гомологичными*, если клетка одной таблицы расположена в строке и столбце с теми же номерами, что и клетка другой таблицы.

а второй — из гомологичной клетки квадрата L_2 . Эту таблицу будем обозначать буквой U и записывать: $U = L_1 \cap L_2$ (см. примеры на рис. 26 и 27).

Если все q^2 упорядоченных пар элементов из Q содержатся в таблице $U = L_1 \cap L_2$, то пару (L_1, L_2) будем называть *ортогональной*. Ясно, что если пара (L_1, L_2)

0	1	2	\cap	$=$	02	11	20
1	2	0			11	20	02
2	0	1			20	02	11
L_1					U		

Рис. 26.

2	1	0	\cap	$=$	22	10	01
1	0	2			11	02	20
0	2	1			00	21	12
L_1					U		

Рис. 27.

ортогональна, то такой же будет и пара (L_2, L_1) . Таким образом, определенное выше отношение симметрично. Оно называется *отношением ортогональности*. Заметим, что не для всякой таблицы V размером $q \times q$, содержащей все упорядоченные пары элементов из Q , существуют латинские квадраты L_1 и L_2 такие, что $L_1 \cap L_2 = V$. Например, в случае $q = 3$ таблица

$$V = \begin{pmatrix} (0,0) & (0,1) & (0,2) \\ (1,0) & (1,1) & (1,2) \\ (2,0) & (2,1) & (2,2) \end{pmatrix}$$

не может быть получена из латинских квадратов с помощью операции \cap . На рис. 26 квадраты L_1 и L_2 не ортогональны, тогда как на рис. 27 изображены ортогональные квадраты. Ясно, что никакой латинский квадрат порядка $q > 1$ не ортогонален самому себе.

Теперь мы можем сформулировать упомянутую в начале параграфа теорему Эйлера — Тарри в следующем

виде: не существует ортогональной пары квадратов порядка шесть.

Нетрудно проверить, что квадраты L_1 и L_2 , представленные на рис. 28, образуют ортогональную пару. Квадрат L'_2 , полученный из квадрата L_2 применением к его элементам подстановки $0, 1, 2, 3 \rightarrow 2, 0, 3, 1$, также ортогонален L_1 . Легко видеть, что и вообще всякая подстановка элементов основного множества переводит латинский квадрат снова в латинский квадрат и что при таком

L_1	<table><tr><td>0</td><td>1</td><td>2</td><td>3</td></tr><tr><td>1</td><td>0</td><td>3</td><td>2</td></tr><tr><td>2</td><td>3</td><td>0</td><td>1</td></tr><tr><td>3</td><td>2</td><td>1</td><td>0</td></tr></table>	0	1	2	3	1	0	3	2	2	3	0	1	3	2	1	0	L_2	<table><tr><td>1</td><td>0</td><td>2</td><td>3</td></tr><tr><td>3</td><td>2</td><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td><td>3</td><td>2</td></tr><tr><td>2</td><td>3</td><td>1</td><td>0</td></tr></table>	1	0	2	3	3	2	0	1	0	1	3	2	2	3	1	0	L'_2	<table><tr><td>0</td><td>2</td><td>3</td><td>1</td></tr><tr><td>1</td><td>3</td><td>2</td><td>0</td></tr><tr><td>2</td><td>0</td><td>1</td><td>3</td></tr><tr><td>3</td><td>1</td><td>0</td><td>2</td></tr></table>	0	2	3	1	1	3	2	0	2	0	1	3	3	1	0	2
0	1	2	3																																																		
1	0	3	2																																																		
2	3	0	1																																																		
3	2	1	0																																																		
1	0	2	3																																																		
3	2	0	1																																																		
0	1	3	2																																																		
2	3	1	0																																																		
0	2	3	1																																																		
1	3	2	0																																																		
2	0	1	3																																																		
3	1	0	2																																																		

Рис. 28.

преобразовании одного из квадратов пары (L_1 , L_2) отношение ортогональности между квадратами этой пары сохраняется.

Предположим теперь, что мы построили из элементов множества $Q = \{0, 1, 2, \dots, q-1\}$ всевозможные латинские квадраты порядка q и хотим выбрать из них r попарно ортогональных. Чтобы узнать, существуют ли такие r квадратов, достаточно, в силу сделанного замечания, рассмотреть квадраты, первые столбцы которых одинаковы; можно даже считать, что первый столбец каждого квадрата, читаемый сверху вниз, в точности совпадает с перестановкой $0, 1, 2, \dots, q-1$. Если из множества латинских квадратов можно выбрать подмножество r попарно ортогональных, то это подмножество называется r -элементной ортогональной системой латинских квадратов порядка q .

Т е о р е м а. Если r -элементная ортогональная система латинских квадратов порядка q существует, то $r \leq q$.

Д о к а з а т е л ь с т в о. Пусть L_1, L_2, \dots, L_r — ортогональная система квадратов и первый столбец каждого квадрата совпадает с перестановкой $0, 1, 2, \dots, q-1$.

Предположим, что $r > q$. Второй элемент первой строки каждого квадрата L_i ($i = 1, 2, \dots, r$) можно выбрать $q-1$ способами. Поскольку имеется

по меньшей мере q латинских квадратов, то у каких-то двух из них, скажем L_s и L_t , на втором месте первой строки окажется один и тот же элемент k . Но тогда пара (k, k) встретится в таблице $L_s \cap L_t$ и на k -м месте в первом

0	1	2	3
1	0	3	2
2	3	0	1
3	2	1	0

L_1

0	2	3	1
1	3	2	0
2	0	1	3
3	1	0	2

L_2

0	3	1	2
1	2	0	3
2	1	3	0
3	0	2	1

L_3

Рис. 29.

столбце, и на втором месте в первой строке, что противоречит ортогональности квадратов L_s и L_t . Теорема доказана.

На рис. 29 представлены три латинских квадрата порядка 4, их первые столбцы одинаковы. Легко убедиться, что эти квадраты попарно ортогональны. Отсюда видно, что для некоторых значений q выполняется соотношение $r = q - 1$. Однако если $q = 6$, то по теореме Эйлера — Тарри $r < 2$.

Ортогональная система, для которой $r = q - 1$, называется *полной ортогональной системой*.

В некоторых вопросах, особенно в математической статистике, важно уметь строить ортогональную систему латинских квадратов заданного порядка q , содержащую максимально возможное число квадратов. Это очень трудная задача, в общем виде она не решена. Достаточно сказать, что только несколько лет назад было доказано существование ортогональных квадратов порядка 10, причем доказательство основывалось на явной конструкции. Если $q = p^r$ (где p — простое), то существует полная ортогональная система латинских квадратов порядка q . Мы докажем это утверждение, используя некоторые рассмотренные ранее свойства конечных проективных плоскостей.

Пусть $q = p^r$. Рассмотрим таблицу $\Gamma(q)$ плоскости $S_{2,q}$. Рисунок 30 соответствует случаю $q = 2^2$. Мы отделяем в таблице часть, состоящую из $q \times (q - 1)$ квадратов, а именно прямоугольник шириной в q и высотой

в $q - 1$ квадратов, расположенный в нижнем правом углу таблицы. Каждый знак инцидентности в этой части заменяем номером столбца квадрата, который этот знак содержит. Таким образом, каждая строка выделенного прямоугольника будет содержать перестановку номеров $0, 1, \dots, q - 1$ (рис. 30, *i*). Если все столбцы каждой

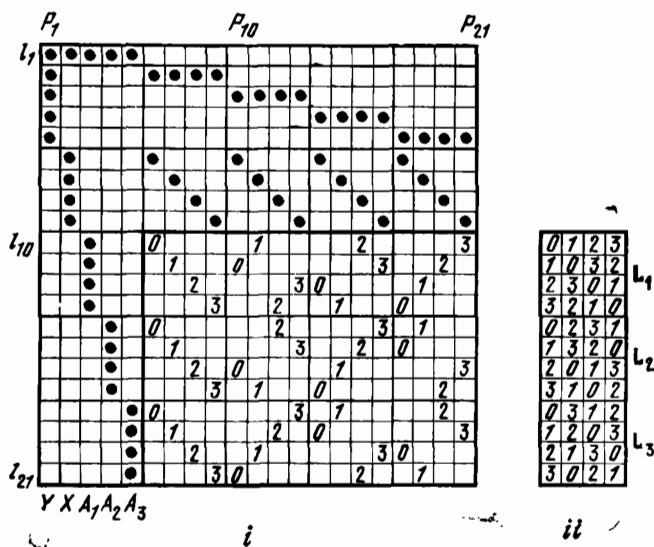


Рис. 30.

столбцовой полосы совместить в одном столбце, то получится столбцовая полоса из $q - 1$ квадратов (рис. 30, *ii*). Обозначим квадраты этой полосы через L_1, L_2, \dots, L_{q-1} . Построение указанным способом системы квадратов по таблице $\Gamma(q)$ плоскости $S_{2,q}$ будем называть λ -процедурой и записывать в виде $\Gamma(q) \rightarrow (L_1, L_2, \dots, L_{q-1})$.

В примере на рис. 30 процесс $\Gamma(q) \rightarrow (L_1, L_2, L_3)$ приводит к полной ортогональной системе латинских квадратов, поскольку получившиеся квадраты L_1, L_2, L_3 совпадают с квадратами, представленными на рис. 29. Мы утверждаем, что при любом q λ -процедура, примененная к таблице $\Gamma(q)$ плоскости $S_{2,q}$, дает полную ортогональную систему латинских квадратов порядка q .

То, что каждая из таблиц L_1, L_2, \dots, L_{q-1} является латинским квадратом, легко вытекает из свойств D_1, D_2, D_3 таблицы $\Gamma(q)$, указанных в параграфе 1.4. Докажем теперь, пользуясь геометрическими соображениями, что всякая пара (L_s, L_t) ($s \neq t$; $s, t = 1, 2, \dots, q-1$) — ортогональная.

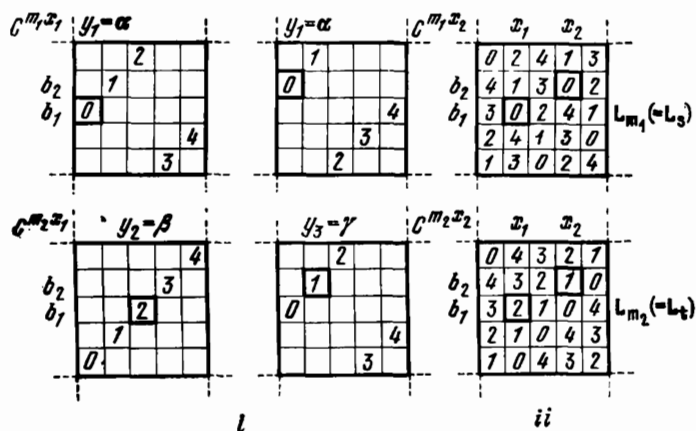


Рис. 31.

Допустим, что для некоторых s и t , $s \neq t$, пара (L_s, L_t) — не ортогональная. Это означает, что в таблице L_s можно указать такие две клетки, содержащие одно и то же число α , что числа β и γ , содержащиеся в гомологичных им клетках таблицы L_t , равны: $\beta = \gamma$.

Воспользуемся обозначениями, которые применялись в параграфе 1.5. Пусть $s = m_1$ и $t = m_2$, и пусть две клетки, выбранные в таблице L_s (и гомологичные им клетки в таблице L_t), будут (b_1, x_1) и (b_2, x_2) (рис. 31). Положим $\alpha = y_1$, $\beta = y_2$, $\gamma = y_3$. Из описания λ -процедуры и устройства таблицы $\Gamma(q)$ (см. параграф 1.5) видно, что пары (α, β) и (α, γ) в таблице $U_{st} = L_s \cap L_t$ получаются переносом соответствующих чисел из квадратов $C^{m_1 x_1}$, $C^{m_1 x_2}$, $C^{m_2 x_1}$, $C^{m_2 x_2}$, т. е. в клетках (b_1, y_1) , (b_2, y_1) , (b_1, y_2) , (b_2, y_3) этих квадратов находятся соответственно числа $\alpha, \alpha, \beta, \gamma$. Это можно следующим образом записать с помощью уравнения $y = F(x, m, b)$,

выражающего инцидентность точки (x, y) и прямой $[m, b]$:

$$\begin{aligned} y_1 &= F(x_1, m_1, b_1), & y_1 &= F(x_2, m_1, b_2), \\ y_2 &= F(x_1, m_2, b_1), & y_3 &= F(x_2, m_2, b_2). \end{aligned}$$

Учитывая условие $\beta = \gamma$, мы получаем

$$F(x_1, m_1, b_1) = F(x_2, m_1, b_2), \quad F(x_1, m_2, b_1) = F(x_2, m_2, b_2).$$

Покажем, что эти равенства несовместны. С этой целью воспользуемся моделью, изображенной на рис. 32, в которой уравнение $y = F(x, m, b)$ интерпретируется так же,

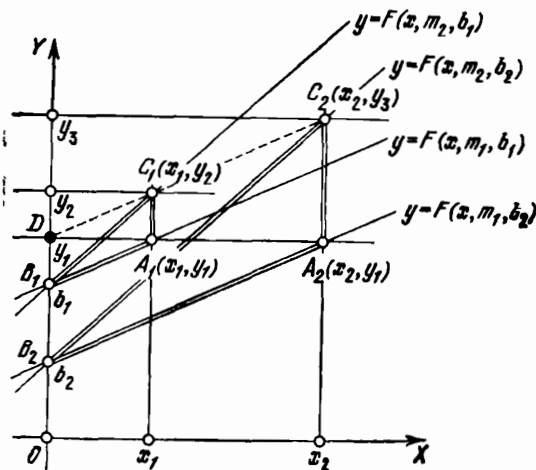


Рис. 32.

как и на рис. 10 параграфа 1.5. Из условий $m_1 \neq m_2$, $b_1 \neq b_2$ и $x_1 \neq x_2$ следует, что для фигуры, изображенной на рис. 32, имеет место

$$B_1 \neq B_2, \quad A_1 \neq A_2, \quad C_1 \neq C_2.$$

Кроме того, $A_1A_2 \parallel OX$, так как $y_1 = F(x_1, m_1, b_1) = F(x_2, m_1, b_2)$. Следовательно, точка $D = A_1A_2 \cap OY$ имеет координаты $0, y_1$. Треугольники $A_1B_1C_1$ и $A_2B_2C_2$ перспективны относительно идеальной прямой и $D = A_1A_2 \cap B_1B_2$. Поскольку для плоскости $S_{2,q}$ справедлива теорема Дезарга, мы получаем, что $D \in C_1C_2$. Поэтому

условие $\beta = \gamma$ (т. е. $y_2 = y_3$) означало бы принадлежность точек D, C_1, C_2 одной прямой, параллельной оси OX , что невозможно *). Полученное противоречие доказывает ортогональность пары (L_s, L_t) .

Теперь мы установим, что *по всякой полной ортогональной системе латинских квадратов порядка q можно построить проективную плоскость того же порядка.*

Мы не будем пытаться обратить λ -процедуру, поскольку такое обращение не всегда возможно.

Пусть имеется полная ортогональная система L_1, L_2, \dots, L_{q-1} латинских квадратов порядка q с элементами из множества $Q = \{0, 1, \dots, q-1\}$. Пример такой системы представлен на рис. 33.

(1)					(2)					(3)					(4)				
0	1	2	3	4	0	2	4	1	3	0	3	1	4	2	0	4	3	2	1
1	2	3	4	0	1	3	0	2	4	1	4	2	0	3	1	0	4	3	2
2	3	4	0	1	2	4	1	3	0	2	0	3	1	4	2	1	0	4	3
3	4	0	1	2	3	0	2	4	1	3	1	4	2	0	3	2	1	0	4
4	0	1	2	3	4	1	3	0	2	4	2	0	3	1	4	3	2	1	0

Рис. 33.

Систему L_1, L_2, \dots, L_{q-1} будем сокращенно обозначать символом LQ , а каждый индивидуальный квадрат системы — символом (ξ) , где ξ — элемент множества $Q^* = \{1, 2, \dots, q-1\}$. Клетку системы LQ , расположенную в квадрате (ξ) на пересечении строки с номером ξ и столбца с номером η ($\xi, \eta \in Q$), будем обозначать через (ξ, η, ζ) .

Обыкновенными точками будем называть пары (x, y) элементов из Q , а идеальными точками — одноэлементные множества (z) , $z \in Q$, и (∞) . Таким образом, в общей сложности получается $q^2 + q + 1$ точек.

*) Действительно, в силу $x_1 \neq x_2$ одно из этих чисел, скажем x_2 , отлично от нуля. Но так как ординаты точек D, C_1, C_2 равны, то $y_1 = y_2$. Это значит, что гомологичные клетки квадратов $C^{m_1 x_1}, C^{m_2 x_2}$ содержали знак инцидентности — в противоречии с D_3 из параграфа 1.4. — *Прим. перев.*

Множество точек (0) , (1) , ..., $(q-1)$ и (∞) будем считать идеальной прямой. Определим также два семейства прямых:

Прямой первого семейства будем считать множество, состоящее из идеальной точки (0) и обыкновенных точек (x, b) , где x пробегает множество Q , а b — фиксированный элемент этого множества. Число таких прямых равно, следовательно, q .

Прямая второго семейства — это множество, состоящее из идеальной точки (∞) и обыкновенных точек (a, y) , где y пробегает множество Q , а a — фиксированный элемент из Q . Число таких прямых также равно q .

Мы знаем, что клетки, содержащие элемент $j \in Q$, распределены в любом латинском квадрате диагональным образом. На рис. 33 выделено диагональное распределение клеток с элементом 2 в латинском квадрате (3). В связи с подобными диагональными распределениями в системе LQ мы будем говорить о *диагональных прямых* $[j, \zeta]$, а именно, прямая $[j, \zeta]$ определяется как множество, состоящее из идеальной точки (ζ) и обыкновенных точек (x, y) таких, что клетка (x, y, ζ) содержит элемент j . Легко видеть, что число диагональных прямых $[j, \zeta]$ ($j \in Q, \zeta \in Q^*$) равно $q(q-1)$.

Таким образом, в общей сложности мы определили $1 + 2q + q(q-1) = q^2 + q + 1$ прямых. Каждая прямая состоит из $q+1$ точек. Систему из точек и прямых, полученную указанным способом из LQ , будем называть фигурой S , а переход от LQ к S , $LQ \rightarrow S$, — ω -процедурой.

Т е о р е м а. *Фигура S , получающаяся в результате применения ω -процедуры к полной ортогональной системе латинских квадратов, является проективной плоскостью порядка q .*

Д о к а з а т е л ь с т в о. На рис. 34 приведена графическая модель, на которой изображены точки фигуры S (соответствующей примеру рис. 33). Идеальная прямая, а также прямые первого и второго семейств представлены на рисунке прямыми линиями. Каждая диагональная прямая будет изображаться ломаной из q звеньев, заканчивающейся идеальной точкой данной прямой (на рисунке изображены только прямая $[2, 3]$ и прямая $[0, 4]$).
 Сначала мы докажем, что любые две прямые пересекаются в единственной точке. Ограничимся случаем

двух диагональных прямых — остальные случаи очевидны непосредственно из определения. Пусть даны две диагональные прямые $[i, r]$ и $[j, s]$, где $r \neq s$. Ввиду ортогональности квадратов L_r и L_s пара (i, j) встречается в таблице $U_{rs} = L_r \cap L_s$ ровно один раз; пусть эта пара

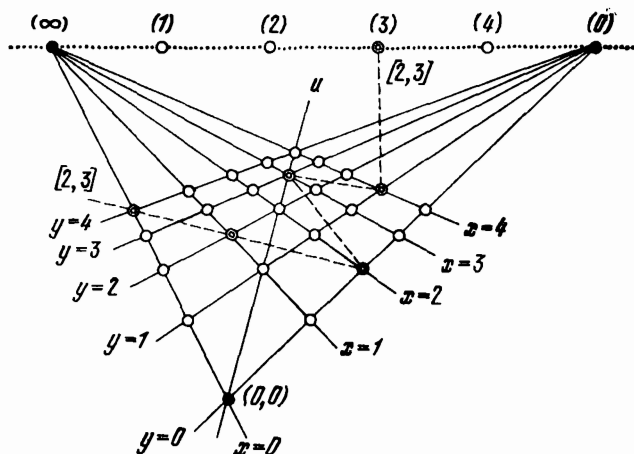


Рис. 34.

попадает в клетку (ξ, η) таблицы U_{rs} . Это означает, что число i попадает в клетку (ξ, η, r) и число j попадает в клетку (ξ, η, s) . Поэтому точка (ξ, η) будет единственной общей точкой прямых $[i, r]$ и $[j, s]$.

Аналогично, существование и единственность прямой, соединяющей две точки, непосредственно очевидны во всех случаях, кроме двух: когда одна точка идеальная, а другая обыкновенная и когда обе точки (a, b) и (c, d) обыкновенные, причем $a \neq c$ и $b \neq d$.

В первом случае рассмотрим обыкновенную точку (a, b) и идеальную точку (j) . Если $j = 0$, то прямая первого семейства, содержащая точку (a, b) , будет искомой; если $j = \infty$, то искомой будет прямая второго семейства, содержащая эту точку; наконец, если $j \in Q^*$ и клетка (a, b, j) содержит элемент i , то единственной прямой, соединяющей точки (a, b) и (j) , будет диагональная прямая $[i, j]$.

Во втором случае рассмотрим $q + 1$ прямых, соединяющих точку (a, b) со всеми идеальными точками. Любые две из этих прямых пересекаются в единственной точке, и каждая такая прямая содержит $q + 1$ точек, поэтому всего на этих прямых лежит $(q + 1)q + 1 = q^2 + q + 1$ точек фигуры S , т. е. все ее точки. Следовательно, одна и только одна из этих прямых содержит точку (c, d) .

Наконец, ясно, что точки (0) , (∞) , $(0, 0)$, $(1, 1)$ являются вершинами собственного четырехугольника. Теорема доказана.

Эта простая комбинаторная теорема позволяет считать геометрию конечных плоскостей одним из разделов комбинаторики. В этом разделе имеется много трудных задач, некоторые из них не решены до сих пор.

Интересно было бы проанализировать связь между λ - и ω -процедурами; мы, однако, не будем этим заниматься.

1.15. Композиция линейных функций и плоскость $D(X, Y)$

В этом параграфе будет установлена связь между конечными проективными геометриями и некоторыми конечными алгебраическими структурами.

Мы начнем с рассмотрения линейных функций $y = ax + b$, заданных на поле действительных чисел \mathbf{R} ; при этом будем пользоваться геометрическим представлением этих функций на евклидовой плоскости. Графически поле \mathbf{R} изображается

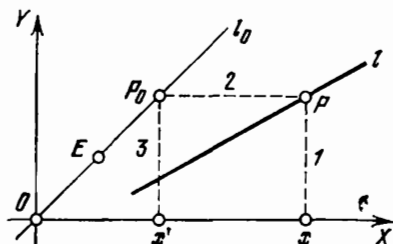


Рис. 35.

осью x . Линейная функция есть отображение

$$x \rightarrow ax + b \quad (a \neq 0)$$

поля \mathbf{R} на себя, которому отвечает следующая геометрическая операция на евклидовой плоскости (рис. 35). Пусть на плоскости дана система координат. Рассмотрим наряду с осями координат прямую l_0 , соединяющую единичную точку $E = (1, 1)$ с началом координат O . Пусть прямая l

задана уравнением $y = ax + b$ ($a \neq 0$). Указанное выше отображение может быть следующим образом описано с помощью прямой l . Возьмем точку x на оси абсцисс и проведем через нее прямую l , параллельную оси y . Прямая l пересечет прямую l в точке P . Проведем через точку P прямую l_0 , параллельную оси x . Прямая l_0 пересечет прямую l в точке P_0 . Проведем через точку P_0 прямую l_1 , параллельную оси y . Прямая l_1 пересечет ось x в точке x' , которая называется образом точки x . Если дана точка x' , то ее прообраз — точка x — получается из x' теми же действиями в обратном порядке. Ясно, что если прямая l пересекает прямую l_0 , то отображение имеет единственную неподвижную точку, а именно точку оси x с той же абсциссой, что и точка пересечения прямых l и l_0 .

Пусть даны две линейные функции

$$l_1: x \rightarrow ax + b \quad \text{и} \quad l_2: x \rightarrow cx + d \quad (a \neq 0, \quad c \neq 0).$$

Под композицией $l_1 l_2 = l$ этих функций будем понимать функцию

$$l: x \rightarrow c(ax + b) + d.$$

Операция композиции линейных функций, вообще говоря, не коммутативна даже для функций, определенных на \mathbf{R} , поскольку равенство $cb + d = ac + b$ выполняется тогда и только тогда, когда имеет место один из следующих случаев:

1° По крайней мере одна из прямых l_1, l_2 совпадает с l_0 .

2° Прямые l_1 и l_2 совпадают.

3° Обе прямые l_1 и l_2 параллельны прямой l_0 .

4° $l_1 \cap l_2 \in l_0$.

Эти четыре возможности можно свести в одно условие, а именно: *прямые l_0, l_1, l_2 (необязательно различные) являются элементами одного плоского пучка прямых; при этом условии композиция $l = l_1 l_2 = l_2 l_1$ будет,¹ конечно, элементом того же пучка.*

Легко видеть, что операция композиции ассоциативна.

Дадим теперь геометрическую интерпретацию композиции линейных функций (рис. 36). Пусть две линейные функции порождаются соответственно прямыми l_1 и l_2 . Исходя из произвольной точки x на оси абсцисс, мы выполняем следующее построение. Пусть: (1) прямая,

проведенная через точку x параллельно оси y , пересекает прямую l_1 в точке P_1 ; (2) прямая, проведенная через точку P_1 параллельно оси x , пересекает прямую l_0 в точке P_0 ; (3) прямая, проведенная через точку P_0 параллельно оси y , пересекает прямую l_2 в точке P_2 ; (4) прямая, проведенная через точку P_2 параллельно оси x , пересекает прямую xP_1 в точке P . Тогда прямая P_2P пересечет

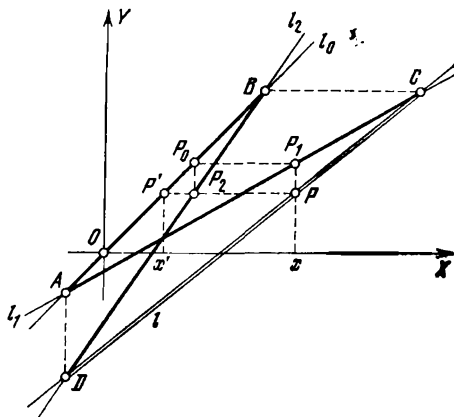


Рис. 36.

прямую l_0 в точке P' , а прямая, проведенная через точку P' параллельно оси y , пересечет ось x в точке x' . Варьируя положение точки x на оси абсцисс, мы получаем отображение $x \rightarrow x'$, являющееся искомым композицией функций. При этом точка P описывает прямую $l = l_1 l_2$, порождающую это отображение. Четырехугольник $P_1 P_0 P_2 P$, опирающийся на прямые l_0, l_1, l_2 , называется *координатным четырехугольником*.

Пусть точки $A = l_0 \cap l_1$ и $B = l_0 \cap l_2$ — различные и не идеальные. Если точка x выбрана так, что точка P_0 совпадает с точкой A , то точка P совпадает с точкой D , получающейся в пересечении прямой l_2 с прямой, проведенной через точку A параллельно оси y . Аналогично, если точка P_0 совпадает с точкой B , то точка P совпадает с точкой C , получающейся в пересечении прямой l_1 с прямой, проведенной через точку B параллельно оси x . Система координат и заданные прямые l_0, l_1, l_2 одно-

значно определяют четверку точек $ABCD$; получившаяся фигура является как бы ортогональной проекцией тетраэдра. При этом всякий координатный четырехугольник можно считать проекцией плоского сечения тетраэдра, параллельного сторонам AD и BC (и разбивающего тетраэдр на две треугольные призмы: $AP_1P_0 \cdot DPP_2$ и $BP_0P_2 \cdot CP_1P$).

В случае конечной плоскости можно указать аналог понятию линейной функции, а именно тернарную функцию, определенную в параграфе 1.5. Решающим, однако, является следующий вопрос: какая функция получается в результате композиции тернарных функций? Если выбраны две тернарные функции $F(-, m_1, b_1)$ и $F(-, m_2, b_2)$ ($m_1, m_2 \neq 0$), то существует ли тернарная функция $F(-, m, b)$ ($m \neq 0$) такая, что для всех x

$$x' = F(x, m_1, b_1) \text{ \& } x'' = F(x', m_2, b_2) \Rightarrow \\ \Rightarrow x'' = F(x, m, b)?$$

Исследуя этот вопрос, мы будем по-прежнему пользоваться рис. 36, только теперь будем считать, что построение четырехугольника $ABCD$ выполнено на конечной плоскости. Наш вопрос равносильен следующему: всегда ли (т. е. при всяком ли x) вершина P координатного четырехугольника, опирающегося на прямые l_0, l_1, l_2 , лежит на прямой CD ?

Рассмотрим треугольники CP_1P и BP_0P_2 и следующее соответствие между их вершинами:

$$\begin{pmatrix} C & P_1 & P \\ B & P_0 & P_2 \end{pmatrix}$$

— вершине C сопоставляется вершина B и т. д.; эти треугольники перспективны относительно центра X , являющегося идеальной точкой. Стороны CP_1 и BP_0 пересекаются в точке A , а стороны P_1P и P_0P_2 — в идеальной точке Y . Теперь нам потребуется теорема Дезарга в следующем ослабленном виде: если два треугольника перспективны относительно фиксированной точки X и одной из трех точек пересечения соответственных сторон треугольников является фиксированная точка Y , то указанные три точки коллинеарны. Применяя эту теорему к рассматриваемым треугольникам, мы получаем, что точка D , являющаяся точкой пересечения прямых AY

и l_2 , лежит на прямой CP . Таким образом, ослабленная теорема Дезарга играет роль необходимого и достаточного условия принадлежности точки P прямой $l = CD$. Легко видеть, что ту же роль играет и теорема, которая получается из ослабленной теоремы Дезарга, если в ней поменять местами X и Y . Действительно, из того, что треугольники

$$\begin{pmatrix} D & P_2 & P \\ A & P_0 & P_1 \end{pmatrix}$$

перспективны относительно центра Y , мы можем заключить о принадлежности точки C прямой BX . Ослабленную теорему Дезарга в указанной выше формулировке будем обозначать символически $D(X, Y)$.

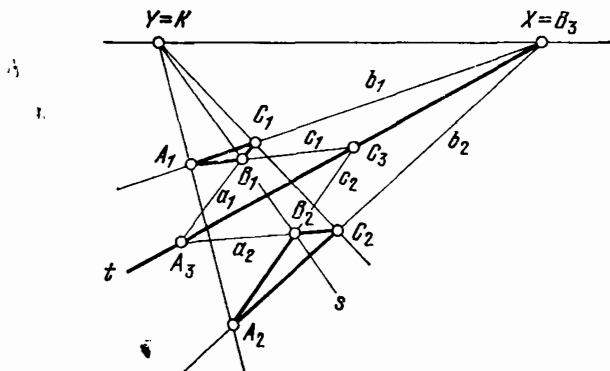


Рис. 37.

Будем пока предполагать, что теорема $D(X, Y)$ выполняется, и рассмотрим рис. 37. Связь между рис. 36 и 37 выражается следующим соответствием:

$$\begin{pmatrix} A & B & C & D & P_1 & P_0 & P_2 & P & l_0 & l_1 & l_2 & l \\ B_1 & C_3 & A_3 & B_2 & C_1 & A_1 & A_2 & C_2 & c_1 & a_1 & c_2 & a_2 \end{pmatrix}.$$

Фигуру на рис. 37 тоже можно считать изображением пространственной фигуры. В сечении тетраэдра $B_1C_3A_3B_2$ плоскостью, содержащей прямую YX , получается четырехугольник $C_1A_1A_2C_2$; точнее, стороны пространственного четырехугольника $A_3B_1C_3B_2$ пересекаются плоскостью в вершинах плоского четырехугольника $C_1A_1A_2C_2$. Из

этой фигуры] легко] усмотреть, что X и Y можно менять ролями.

Предположим, что дана плоскость, удовлетворяющая аксиомам I_1 , I_2 и I_3 , и две различные точки X и Y на этой плоскости. Мы сейчас докажем, что из теоремы $D(X, Y)$ для плоскости вытекает теорема $D(Y, X)$, и обратно. Для удобства будем считать, что порядок данной плоскости больше 2; нетрудно проверить, что для плоскости порядка 2 обе теоремы $D(X, Y)$ и $D(Y, X)$ справедливы.

Пусть теорема $D(X, Y)$ верна. Рассмотрим два треугольника $A_1B_1C_1$ и $A_2B_2C_2$ такие, что прямые A_1A_2 , B_1B_2 и C_1C_2 пересекаются в точке Y (рис. 37); таким образом, эти треугольники перспективны относительно точки Y . Положим $A_1B_1 \cap A_2B_2 = C_3$, $B_1C_1 \cap B_2C_2 = A_3$, $C_1A_1 \cap C_2A_2 = B_3$, и пусть, в соответствии с условием теоремы $D(Y, X)$, $B_3 = X$.

Рассуждая от противного, допустим, что прямая A_3C_3 не проходит через точку X . Пусть прямые XA_3 и A_1B_1 пересекаются в точке C ($\neq C_3$). Тогда мы получим пару треугольников

$$\begin{pmatrix} A_3 & C_1 & C_2 \\ C & A_1 & A_2 \end{pmatrix},$$

которые перспективны относительно точки $X = B_3$. Тогда в силу нашего предположения о том, что теорема $D(X, Y)$ верна, точки B_1 , Y и $B = A_3C_2 \cap A_2C$ будут лежать на одной прямой. Но в этом случае прямая A_3C_2 пересечет прямую YB_1 как в точке B_2 , так и в отличной от нее точке B , что невозможно. Следовательно, прямая A_3C_3 проходит через точку X , т. е. теорема $D(Y, X)$ также верна.

Вернемся теперь к рис. 36. Мы предполагали, что A и B — две различные неидеальные точки. Остается еще определить, какие линии описывает вершина P координатного четырехугольника, опирающегося на прямые l_0 , l_1 , l_2 , в следующих случаях: когда $A \neq B$ и B — идеальная точка; когда $A \neq B$ и A — идеальная точка; когда точка A обыкновенная и $A = B$; когда обе точки A и B идеальные. Предполагается, что теорема $D(X, Y)$ имеет место.

Чтобы исследовать первые два случая, обратимся к рис. 38, *i* и 38, *ii*. Если прямая l_2 параллельна прямой l_0 ,

то, установив соответствие

$$\begin{pmatrix} A & P_0 & P_1 \\ D & P_2 & P \end{pmatrix},$$

мы получим пару треугольников, перспективных относительно точки Y . Поскольку $AP_0 \parallel DP_2$ и $P_0P_1 \parallel P_2P$,

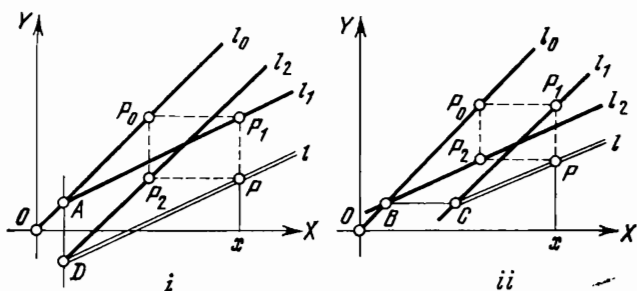


Рис. 38.

то по теореме D (Y, X) прямые AP_1 и DP параллельны. Таким образом, точка P всегда лежит на прямой, проведенной через точку D параллельно l_1 . Аналогично, во втором случае точка P всегда лежит на прямой, проведенной через точку C параллельно l_2 .

Два других случая представлены на рис. 39, *i* и 39, *ii*. Если обе точки A и B совпадают с обыкновенной точкой

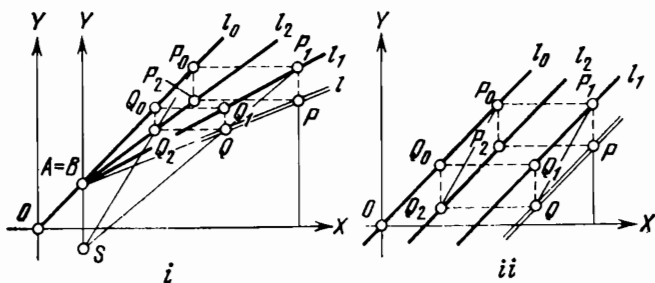


Рис. 39.

на прямой l_0 , то рассмотрим два координатных четырехугольника, опирающихся на наши прямые, один из которых дает точку P , а другой — точку Q . Рассмотрим пару

треугольников

$$\begin{pmatrix} P_0 & Q_0 & Q_2 \\ P_1 & Q_1 & Q \end{pmatrix},$$

перспективных относительно точки X ; из теоремы $D(X, Y)$ следует, что P_0Q_2 и P_1Q пересекаются в некоторой обыкновенной точке S , лежащей на прямой AY . Применяя теорему $D(X, Y)$ к паре треугольников

$$\begin{pmatrix} P_0 & P_2 & Q_2 \\ P_1 & P & Q \end{pmatrix},$$

перспективных относительно точки X , мы получаем, что точки S, Y и $QP \cap Q_2P_2$ лежат на одной прямой, скажем прямой t ; следовательно, прямая $l = QP$ проходит через точку $A = t \cap l_2$. Фиксируя точку Q и варьируя точку x на оси абсцисс, мы заставим переменную точку P пробегать прямую AQ . Аналогичные рассуждения применяются в четвертом случае; разумеется, в этом случае прямая l параллельна прямой l_0 .

Заметим, что, ввиду соответствия между тернарными функциями и наклонными прямыми (т. е. прямыми, не параллельными ни одной из осей) в данной системе координат, можно вместо композиции двух тернарных функций говорить о *произведении двух наклонных прямых*.

В итоге доказана следующая

Т е о р е м а. *Произведение двух произвольных наклонных прямых проективной плоскости тогда и только тогда является наклонной прямой, когда для плоскости выполняется теорема $D(X, Y)$.*

Подобную плоскость будем для краткости называть плоскостью $D(X, Y)$. Отображение $x \rightarrow x'$, порождаемое наклонной прямой, будем называть λ -отображением (рис. 35). Отображение, соответствующее прямой l_0 , является тождественным. Если отображения λ_1, λ_2 и λ соответствуют прямым l_1, l_2 и $l = l_1l_2$, то произведением отображений λ_1 и λ_2 является отображение λ (рис. 40). Поскольку умножение отображений ассоциативно, то умножение наклонных прямых также ассоциативно.

Пусть L означает множество наклонных прямых с операцией умножения, определенной выше. Множество L содержит нейтральный элемент l_0 , т. е. для каждой прямой $l \in L$ имеет место $l_0l = ll_0 = l$. Рисунок 41 показы-

вает, что для всякой прямой $l_1 \in L$ существует прямая $l_2 \in L$ такая, что $l_1 l_2 = l_0$, т. е. для всякой наклонной

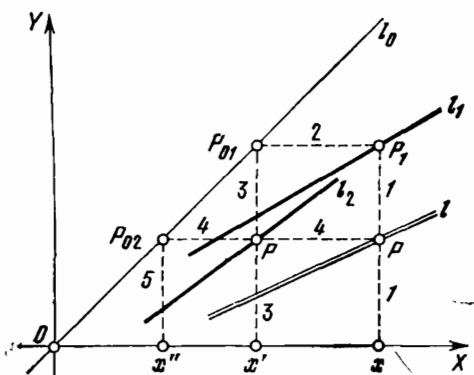


Рис. 40.

прямой имеется прямая, играющая роль обратного элемента относительно операции умножения прямых. (В случае евклидовой плоскости прямая, обратная l_1 , получается зеркальным отражением l_1 относительно прямой l_0 .) Обозначим множество λ -отображений через Λ . Мы можем подытожить наши результаты следующим образом.

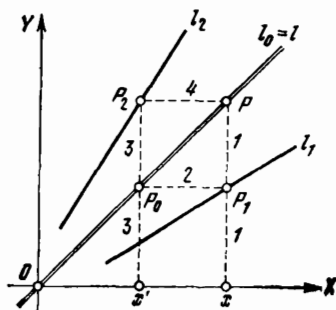


Рис. 41.

Т е о р е м а. Множество L есть группа относительно операции умножения наклонных прямых, а множество Λ есть группа относительно умножения отображений.

Как известно, произведение двух прямых пучка, содержащего прямую l_0 , также содержится в этом пучке; кроме того, прямая, обратная прямой этого пучка, снова принадлежит данному пучку. Следовательно, пучок, содержащий прямую l_0 , относительно определенной выше операции умножения прямых образует подгруппу группы L .

При этом предполагается, конечно, что из пучка исключены прямые, проходящие через его центр параллельно осям. Если S — точка прямой l_0 , обыкновенная или идеальная, то множество наклонных прямых, проходящих через S , равно как и подгруппу, образуемую этими прямыми, будем обозначать через S .

В заключение этого параграфа мы вкратце наметим схему, позволяющую применить описанную выше теоретико-групповую конструкцию для сведения задач геометрии к задачам теории групп. В настоящее время это наиболее плодотворный метод в конечной геометрии.

Пусть дана группа G порядка q ($q - 1$). Пусть G имеет $q + 1$ подгрупп, одна из них порядка q , а остальные — порядка $q - 1$, причем каждый элемент группы G , кроме нейтрального, принадлежит ровно одной из этих подгрупп. Пусть Π обозначает множество всех указанных подгрупп. Множество Π называется *покрытием* группы G , а подгруппы из Π — *компонентами* этого покрытия. Мы снабдим группу G следующей структурой:

1. *Наклонными прямыми* будем считать элементы группы G .

2. *Обыкновенными точками* будем считать смежные классы gP , где P — подгруппа из Π порядка $q - 1$, а $g \in G$.

3. *Идеальными точками* будем считать смежные классы gP_0 , где P_0 — подгруппа из Π порядка q , а $g \in G$.

Мы покажем сейчас на примере, что из этой структуры получается конечная плоскость. Пусть G — полная группа симметрий правильного тетраэдра (в этом случае $q = 4$). Выпишем таблицу Кэли для этой группы, обозначая элементы группы натуральными числами с условием, что нейтральный элемент обозначается числом 1 (рис. 42). Компонентами покрытия тогда будут

$$A = \{1, 2, 3\}, \quad B = \{1, 5, 12\}, \quad C = \{1, 6, 8\},$$

$$D = \{1, 9, 11\}, \quad U = \{1, 4, 7, 10\}.$$

В самом деле, элемент 1 является единственным общим элементом любых двух компонент и, кроме того, $A \cup B \cup C \cup D \cup U = G$.

Составим с помощью таблицы Кэли смежные классы, считающиеся обыкновенными точками:

$$\begin{aligned}
 P_1 &= \{1, 2, 3\}, & P_2 &= \{1, 5, 12\}, & P_3 &= \{1, 6, 8\}, \\
 P_4 &= \{1, 9, 11\}, & P_5 &= \{4, 8, 12\}, & P_6 &= \{4, 11, 3\}, \\
 P_7 &= \{4, 9, 2\}, & P_8 &= \{4, 6, 5\}, & P_9 &= \{7, 11, 6\}, \\
 P_{10} &= \{7, 8, 9\}, & P_{11} &= \{7, 3, 5\}, & P_{12} &= \{7, 12, 2\}, \\
 P_{13} &= \{10, 5, 9\}, & P_{14} &= \{10, 2, 6\}, & P_{15} &= \{10, 12, 11\}, \\
 & & P_{16} &= \{10, 3, 8\}.
 \end{aligned}$$

Теперь, по определению, элементы 1, 2, ..., 12 являются наклонными прямыми (чтобы подчеркнуть, что

34.

1	2	3	4	5	6	7	8	9	10	11	12
2	3	1	5	6	4	8	9	7	11	12	10
3	1	2	6	4	5	9	7	8	12	10	11
4	8	12	1	11	9	10	2	6	7	5	3
5	9	10	2	12	7	11	3	4	8	6	1
6	7	11	3	10	8	12	1	5	9	4	2
7	11	6	10	8	3	1	5	12	4	2	9
8	12	4	11	9	1	2	6	10	5	3	7
9	10	5	12	7	2	3	4	11	6	1	8
10	5	9	7	2	12	4	11	3	1	8	6
11	6	7	8	3	10	5	12	1	2	9	4
12	4	8	9	1	11	6	10	2	3	7	5

Рис. 42.

это прямые, их можно обозначить l_1, l_2, \dots, l_{12} , а P_1, P_2, \dots, P_{16} — это обыкновенные точки; мы поэтому можем интерпретировать некоторые инцидентности. Например, можно считать, что запись $P_{11} = \{7, 3, 5\}$ означает инцидентность точки P_{11} наклонным прямым l_7, l_3, l_5 . Или же, пользуясь данным выше перечнем классов, можно сразу сказать, что прямая $l_3 (=3)$ проходит через точки P_1, P_6, P_{11}, P_{16} , откуда следует, что

эта прямая содержит четыре обыкновенные точки. Действуя таким образом, мы приходим к таблице инцидентности из 12 строк и 16 столбцов, которая содержит по три знака инцидентности в каждом столбце и по четыре — в каждой строке. На первый взгляд в этой таблице не угадывается никакого знакомого распределения. Если, однако, переставить строки в соответствии с подстановкой

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1 & 4 & 7 & 10 & 3 & 12 & 6 & 9 & 2 & 5 & 8 & 11 \end{pmatrix},$$

сохраняя порядок столбцов, то мы получим таблицу инцидентности, изображенную на рис. 43.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	•	•	•	•												
4					•	•	•	•								
7									•	•	•	•				
10												•	•	•	•	
3	•					•					•					•
12		•			•							•			•	
6			•					•	•						•	
9				•			•			•			•			
2	•						•				•		•			
5		•						•		•		•				•
8			•		•					•						•
11				•	•				•						•	

Рис. 43.

Сразу же легко заметить, что эту таблицу можно дополнить строками и столбцами с таким распределением знаков инцидентности, что получится таблица рис. 7. Новые строки будут соответствовать ненаклонным прямым и идеальной прямой, а новые столбцы — идеальным точкам.

1.16. Задачи и упражнения к главе 1

Задачи и упражнения различной степени трудности будут приводиться в конце каждой главы. Они имеют целью, во-первых, дополнить материал каждой главы, во-вторых, привить читателю практические навыки в обращении с новыми идеями, а быть может, и побудить его к самостоятельным исследованиям.

1. В Г-таблице проективной плоскости порядка 4 (см. рис. 7) сохраняется известный произвол для распределения знаков инци-

дентности в Θ -части. Как с помощью строчных и столбцевых преобразований привести это распределение к некоторому заранее определенному виду, доказав тем самым, что существует только одна проективная плоскость порядка 4?

2. Исходя из правильного 31-угольника, вписанного в окружность, найти путем перебора его максимальный вполне неправильный подмногоугольник. Как можно упростить перебор?

3. Пусть для правильного многоугольника с $q^2 + q + 1$ вершинами, вписанного в окружность k , существует вполне неправильный выпуклый подмногоугольник Λ с $q + 1$ вершинами. Показать, что при $q = 4$ центр окружности k будет лежать внутри подмногоугольника Λ .

4. Пусть дан правильный 43-угольник, вписанный в окружность k . Пусть каждые две из каких-нибудь его семи вершин соединены хордами (общее число этих хорд равно 21). Показать путем перебора, что среди этих хорд найдутся две хорды равной длины.

5. Можно ли раскрасить точки плоскости порядка $q > 2$ в два цвета, белый и черный, так, чтобы каждая прямая содержала точки каждого цвета? Можно ли это сделать при $q = 2$?

6. Доказать, что диагональные точки всякого собственного четырехугольника на плоскости Галуа $S_{2,4}$ лежат на одной прямой (таблицы операций поля $GF(4)$ приведены в параграфе 1.6).

7. С помощью рис. 7 и таблиц операций поля $GF(4)$ проверить справедливость следующих утверждений. Координаты пяти точек плоскости $S_{2,4}$ удовлетворяют уравнению $x_1^2 + x_2^2 + x_3^2 = 0$ и пяти точек — уравнению $x_1^2 + x_2x_3 = 0$. Первые пять точек лежат на одной прямой, и из вторых пяти точек в точности две лежат на этой прямой.

8. Рассмотреть последовательность расширяющихся таблиц из параграфа 1.11 (рис. 16 и 17). Определить число строк и столбцов в таблице T^k .

9. Для $\langle 3, 3 \rangle$ -плоскости, заданной таблицей рис. 14, справедливы следующие теоремы. 1. Отношение параллельности не транзитивно. 2. Существует четырехугольник, не имеющий диагональных точек. 3. Существует пара треугольников, перспективных относительно точки, никакие две соответственные стороны которых не пересекаются. Доказать эти теоремы с помощью рис. 14.

10. Хотя ряд свойств удается проиллюстрировать с помощью плоскости порядка 4, имеются, естественно, другие свойства, например недезарговость, для иллюстрации которых эта плоскость непригодна. Мы поэтому рассмотрим еще две плоскости порядка 9 (таков наименьший порядок плоскости, отвечающей нашим целям). Поскольку таблицы инцидентности этих плоскостей слишком громоздки, мы не будем приводить их полностью.

Прежде всего составим таблицы операций поля $GF(9)$; они указаны на рис. 44.

11. Построение таблицы инцидентности $\Gamma(9)$. Следуя примеру, представленному на рис. 7, мы можем расставить знаки инцидентности в первых 10 строках и первых 10 столбцах. Остаточная $\Gamma\Theta$ -часть разделена на 9×9 квадратов. Диагональное распределение, соответствующее элементу k в таблице сложения поля $GF(9)$, будем называть k -распределением. Всего получается, таким образом,

9 диагональных распределений. Занумеруем квадраты $\Gamma\Theta$ -части так, как показано на таблице G рис. 45 (таблица G совпадает с таблицей умножения поля $GF(9)$, приведенной на рис. 44).

+	0	1	2	3	4	5	6	7	8	x	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8	0	0	0	0	0	0	0	0	0	0
1	1	2	0	4	5	3	7	8	6	1	0	1	2	3	4	5	6	7	8
2	2	0	1	5	3	4	8	6	7	2	0	2	1	6	8	7	3	5	4
3	3	4	5	6	7	8	0	1	2	3	0	3	6	7	1	4	5	8	2
4	4	5	3	7	8	6	1	2	0	4	0	4	8	1	5	6	2	3	7
5	5	3	4	8	6	7	2	0	1	5	0	5	7	4	6	2	8	1	3
6	6	7	8	0	1	2	3	4	5	6	0	6	3	5	2	8	7	4	1
7	7	8	6	1	2	0	4	5	3	7	0	7	5	8	3	1	4	2	6
8	8	6	7	2	0	1	5	3	4	8	0	8	4	2	7	3	1	6	5

Рис. 44.

Расставим знаки инцидентности в $\Gamma\Theta$ -части так, чтобы любой квадрат с номером k имел k -распределение. Это предписание согласуется с общим правилом построения $\Gamma(q)$ -таблицы по произвольному полю $GF(q)$ (параграф 1.6).

G	0	1	2	3	4	5	6	7	8	V	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8	0	0	1	2	3	4	5	6	7	8
1	1	2	0	4	5	3	7	8	6	0	0	2	1	6	8	7	3	5	4
2	2	0	1	5	3	4	8	6	7	0	0	3	6	7	1	4	5	8	2
3	3	4	5	6	7	8	0	1	2	0	0	4	8	1	5	6	2	3	7
4	4	5	3	7	8	6	1	2	0	0	0	5	7	4	6	2	8	1	3
5	5	3	4	8	6	7	2	0	1	0	0	6	3	5	2	8	7	4	1
6	6	7	8	0	1	2	3	4	5	0	0	7	5	8	3	1	4	2	6
7	7	8	6	1	2	0	4	5	3	0	0	8	4	2	7	3	1	6	5
8	8	6	7	2	0	1	5	3	4	0	0	0	0	0	0	0	0	0	0

Рис. 45.

12. На рис. 46 даны 27 диагональных распределений, из которых только 9 (под номерами 0, 1, ..., 8) были использованы при построении таблицы $\Gamma(9)$. Мы не останавливаемся здесь на устройстве остальных 18 распределений. Эти распределения потребуются нам для построения таблицы инцидентности Γ^* плоскости порядка 9, не являющейся плоскостью Галуа.

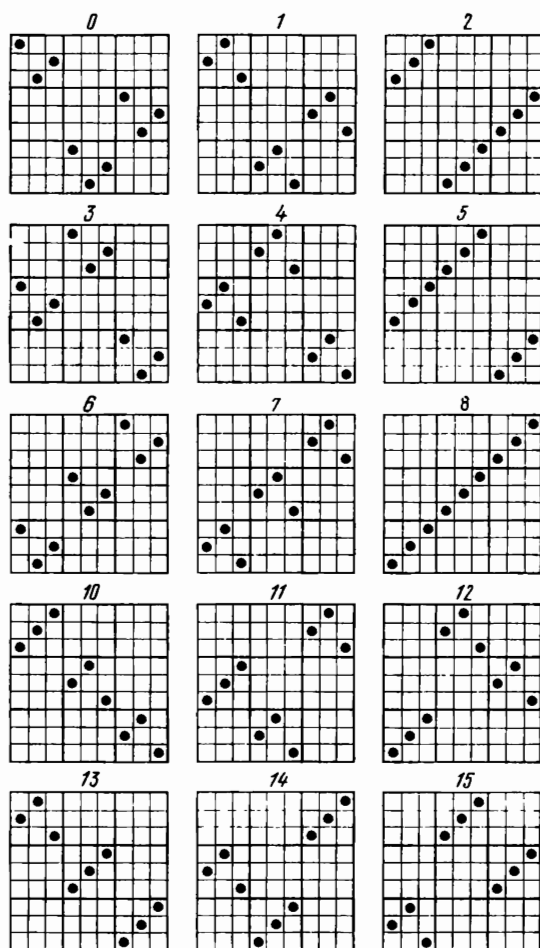


Рис. 46 а.

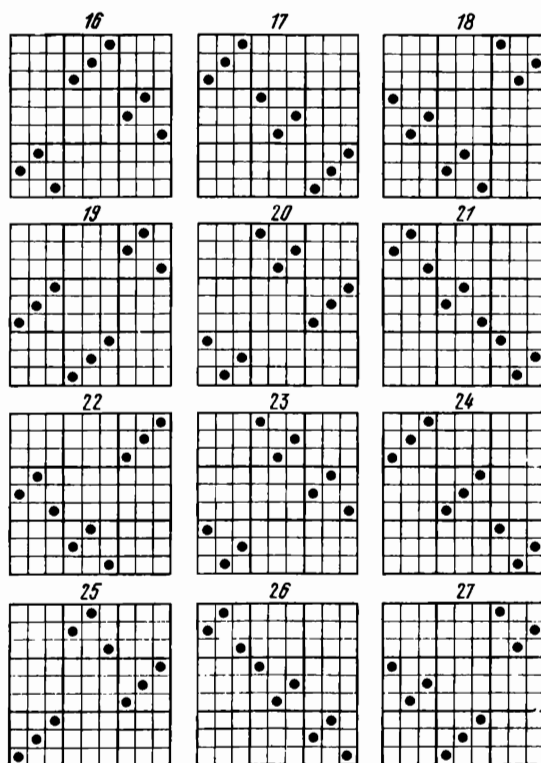


Рис. 46 б.

Возьмем Γ -структуру размером 91×91 . Распределим знаки в первых $1 + 4 \times 9 = 37$ строках и первых 37 столбцах так же, как и в таблице $\Gamma(9)$, рассмотренной выше. Распределение знаков в оставшихся 6×6 квадратах задается таблицей V на рис. 45: например, индекс 24, встречающийся в двух клетках этой таблицы, означает, что оба соответствующих квадрата имеют распределение, указанное под номером 24.

(Таблица Γ^* не может быть изоморфна таблице $\Gamma(9)$, поскольку для первой число различных распределений $\delta = 27$, а для второй $\delta = 9$.)

13. Доказать, что плоскость Галуа порядка 9 не содержит четырехугольников Фано, в то время как плоскость порядка 9, определяемая таблицей Γ^* , содержит как обычные четырехугольники, так и четырехугольники Фано; найти по таблице Γ^* примеры тех и других.

14. Показать, что для плоскости, определяемой таблицей Γ^* , теорема Дезарга не выполняется, т. е. что эта плоскость недезаргова. Заметим, что это не означает антидезарговости, поскольку, как можно убедиться на примере, на этой плоскости имеются как конфигурации, удовлетворяющие теореме Дезарга, так и конфигурации, не удовлетворяющие ей.

15. Показать, что плоскость, определяемая таблицей Γ^* , имеет подплоскость порядка три.

(Это позволяет нам говорить, что $\Gamma(3)$ имеет своими расширениями как $\Gamma(9)$, так и Γ^* . При этом Γ^* содержит четырехугольник Фано и, таким образом, обладает подплоскостью порядка 2. Отсюда следует, что плоскость порядка 2 можно расширить как до дезарговой, так и до недезарговой плоскости (например, расширениями $\Gamma(2)$ служат $\Gamma(4)$ и Γ^*).)

16. Выбрать какую-нибудь Γ -таблицу и найти композицию двух прямых (с помощью координатных четырехугольников).

*

В заключение сделаем несколько указаний к решениям упражнений 13, 14 и 15.

Рассмотрим в таблице Γ^* строки с номерами 1, 4, 6, 22, 28, 68, 65 и столбцы с номерами 1, 3, 8, 29, 32, 52, 55. В пересечении этих строк и столбцов получается таблица $\Gamma(2)$. Аналогично, пересечение строк и столбцов с номерами 1, 2, 3, 4, 11, 12, 13, 20, 21, 22, 29, 30 и 31 дает таблицу $\Gamma(3)$.

Из той же таблицы Γ^* находим, что треугольники

$$\begin{pmatrix} P_{40} & P_{59} & P_{80} \\ P_{54} & P_{85} & P_{86} \end{pmatrix}$$

перспективны относительно точки P_5 , а их соответственные стороны пересекаются в точках P_{48} , P_{21} и P_{34} ; эти точки не коллинеарны, так как

$$P_{48}P_{21} = l_{13}, \quad P_{21}P_{34} = l_{50} \quad \text{и} \quad P_{34}P_{48} = l_{42}.$$

После изложения основных понятий в главе 1 мы займемся теперь наиболее изученным разделом конечных геометрий, а именно геометриями пространств Галуа. Чисто арифметический способ, с помощью которого определяются пространства Галуа, и аналитический подход к изучению их геометрии с особой силой подчеркивают сходство между классической проективной геометрией и геометрией Галуа. В дальнейшем мы будем рассматривать главным образом *плоскую* геометрию, хотя и определим n -мерное пространство Галуа порядка q , обозначаемое $S_{n,q}$. Изучение случая $n > 2$ привело бы к значительному увеличению объема книги, однако не обогатило бы нас новыми методами.

В связи с аналитическим подходом мы будем часто использовать понятия и теоремы, относящиеся к теории конечных алгебраических структур. Поскольку эти сведения могут быть незнакомы читателю, мы приводим в Приложении в сжатом виде необходимые факты из алгебры.

2.1. Понятие пространства Галуа

Арифметическая характеристика пространств $S_{n,q}$ представляет собой обобщение процедуры, изложенной в параграфе 1.10. С точки зрения такого подхода можно считать, что мы имеем здесь дело с геометрической алгеброй. Действительно, мы будем изучать алгебраические понятия, пользуясь языком геометрии, поэтому более уместно говорить именно о геометрической алгебре, чем об алгебраической геометрии.

Пусть r — натуральное число, p — простое, и $q = p^r$. Поле $GF(q)$ будем, как и ранее, обозначать \mathbf{K} . Предположим, что $x_j \in \mathbf{K}$, $j = 1, 2, \dots, n$, и рассмотрим совокупность всех последовательностей (x_1, x_2, \dots, x_n) .

Число таких последовательностей есть q^n . Разобьем всю совокупность последовательностей на классы следующим образом. Будем считать, что две последовательности (x_1, x_2, \dots, x_n) и $(x'_1, x'_2, \dots, x'_n)$ принадлежат одному классу в том и только в том случае, когда существует $\lambda \in K, \lambda \neq 0$, такое, что $x'_j = \lambda x_j$ для всех $j = 1, \dots, n$. Вводя обозначение $(x) = (x_1, \dots, x_n)$, имеем:

$$\begin{aligned}(x') &= (x'_1, \dots, x'_n) = \\ &= (\lambda x_1, \dots, \lambda x_n) = \lambda (x_1, \dots, x_n) = \lambda (x).\end{aligned}$$

Для последовательности $(0, 0, \dots, 0)$ ее класс состоит только из нее самой. Условимся эту последовательность, называемую иногда *не-точкой* или *пустым пространством*, из дальнейшего рассмотрения исключить. Оставшиеся $q^n - 1$ последовательностей разбиваются на классы, причем каждый класс содержит $q - 1$ последовательностей. Следовательно, число классов есть

$$(q^n - 1)/(q - 1) = \theta_{n-1}.$$

Определенные таким образом классы будем называть *точками*, а сами элементы x_1, x_2, \dots, x_n последовательности (x_1, x_2, \dots, x_n) данного класса — *однородными координатами* точки. Множество всех точек будем обозначать $S_{n-1, q}$ и называть $(n - 1)$ -*мерным пространством Галуа порядка q* .

В данный момент мы знаем относительно этого множества лишь то, что число точек в нем есть

$$\theta_{n-1} = q^{n-1} + q^{n-2} + \dots + 1.$$

Однако самый способ построения этого множества с помощью поля K позволяет ввести в нем определенную структуру, напоминающую классическую проективную геометрию. набросок такой структуры был дан в параграфе 1.10 для случая $n = 3$. Этот набросок мы хотим теперь обобщить. Введем ряд понятий, играющих существенную роль в определении геометрической структуры $S_{n-1, q}$.

1° Пусть даны последовательности $(a_{j1}, a_{j2}, \dots, a_{jn})$ и коэффициенты λ_j , где $j = 1, 2, \dots, k, \lambda_j \in K, a_{jl} \in K$ для $l = 1, 2, \dots, n$. Будем называть *линейной комбинацией* данных последовательностей, образованной с помощью данных коэффициентов, последовательность

(b_1, b_2, \dots, b_n) , где

$$b_l = \lambda_1 a_{1l} + \lambda_2 a_{2l} + \dots + \lambda_k a_{kl}.$$

Введем в связи с этим такие обозначения:

$$\begin{aligned} (b) = (b_1, b_2, \dots, b_n) &= \lambda_1 (a_{11}, a_{12}, \dots, a_{1n}) + \\ &+ \lambda_2 (a_{21}, a_{22}, \dots, a_{2n}) + \dots + \lambda_k (a_{k1}, a_{k2}, \dots, a_{kn}) = \\ &= \lambda_1 (a_1) + \lambda_2 (a_2) + \dots + \lambda_k (a_k). \end{aligned}$$

2° Будем называть *фиксацией* координатной последовательности для данной точки выбор одной определенной координатной последовательности из $q - 1$ последовательностей, задающих данную точку. Если произведена фиксация, то во всех рассуждениях, касающихся данной точки, мы пользуемся выбранной координатной последовательностью.

3° Будем называть *нормированием* координатной последовательности данной точки такую фиксацию, при которой последний отличный от нуля элемент последовательности есть единичный элемент поля K . Таким образом, существует взаимно однозначное соответствие между точками и их нормированными координатными последовательностями.

4° Будем называть *линейной комбинацией* $\lambda_1 A_1 + \lambda_2 A_2 + \dots + \lambda_k A_k$ данных точек A_j , образованной при помощи данных коэффициентов λ_j ($j = 1, 2, \dots, k$), последовательность

$$(b) = \lambda_1 (a_1) + \lambda_2 (a_2) + \dots + \lambda_k (a_k),$$

где (a_j) обозначает нормированную последовательность для точки A_j ($j = 1, \dots, k$). Последовательность (b) (уже не обязательно нормированная) либо определяет некоторую точку *) S , либо же $(b) = (0, 0, \dots, 0)$, т. е. (b) есть пустое пространство, обозначаемое 0.

Мы будем говорить, что точки A_1, A_2, \dots, A_k образуют (*линейно*) *независимую систему точек*, если равенство

$$\lambda_1 A_1 + \lambda_2 A_2 + \dots + \lambda_k A_k = 0$$

возможно лишь в случае

$$\lambda_1 = \lambda_2 = \dots = \lambda_k = 0.$$

*) И в этом случае точка S также называется *линейной комбинацией точек* A_1, \dots, A_k . — *Прим. перев.*

Рассмотрим две линейные комбинации

$$\lambda_1 A_1 + \lambda_2 A_2 + \dots + \lambda_k A_k \text{ и } \lambda'_1 A_1 + \lambda'_2 A_2 + \dots + \lambda'_k A_k,$$

где точки A_1, A_2, \dots, A_k образуют линейно независимую систему. Пусть эти комбинации суть последовательности

$$(b_1, b_2, \dots, b_n) \text{ и } (b'_1, b'_2, \dots, b'_n).$$

Могут ли эти две последовательности принадлежать одному классу? Иначе говоря, существует ли такое $v \in K$, $v \neq 0$, что

$$b'_1 = vb_1, \quad b'_2 = vb_2, \quad b'_n = vb_n?$$

Очевидно, это возможно лишь в том случае, когда

$$\begin{aligned} v(\lambda_1 A_1 + \lambda_2 A_2 + \dots + \lambda_k A_k) - \\ - (\lambda'_1 A_1 + \lambda'_2 A_2 + \dots + \lambda'_k A_k) = (v\lambda_1 - \lambda'_1) A_1 + \\ + (v\lambda_2 - \lambda'_2) A_2 + \dots + (v\lambda_k - \lambda'_k) A_k = 0. \end{aligned}$$

Согласно определению линейно независимой системы точек, это означает, что

$$\lambda'_1 = v\lambda_1, \quad \lambda'_2 = v\lambda_2, \quad \lambda'_k = v\lambda_k.$$

Таким образом, для точек, представимых в виде линейных комбинаций линейно независимых точек A_1, A_2, \dots, A_k , последовательность коэффициентов $\lambda_1, \lambda_2, \dots, \lambda_k$ играет сходную роль с последовательностью однородных координат для точек из $S_{k-1, q}$. Это позволяет нам сказать, что $(\lambda_1, \lambda_2, \dots, \lambda_k)$, где

$$(\lambda_1, \lambda_2, \dots, \lambda_k) \neq (0, 0, \dots, 0),$$

есть последовательность однородных координат для точки

$$\lambda_1 A_1 + \lambda_2 A_2 + \dots + \lambda_k A_k$$

относительно заданной линейно независимой системы $\{A_1, A_2, \dots, A_k\}$.

Рассмотрим теперь множество всех точек $\lambda_1 A_1 + \lambda_2 A_2 + \dots + \lambda_k A_k$, порожденных линейно независимой системой $\{A_1, A_2, \dots, A_k\}$. Очевидно, каждая из базисных точек A_j является элементом этого множества: для этой точки следует взять $\lambda_j = 1$ и $\lambda_i = 0$ при $i \neq j$.

Совершенно ясно, что существует взаимно однозначное соответствие между указанным множеством точек и пространством Галуа $S_{k-1, q}$, так что указанное множество содержит

$$\theta_{k-1} = q^{k-1} + q^{k-2} + \dots + 1$$

точек. Это множество точек называется *подпространством* пространства Галуа $S_{n-1, q}$, порожденным системой точек $\{A_1, A_2, \dots, A_k\}$. В случаях $k = 2$, $k = 3$ или $k = n - 1$ определенные таким образом подпространства называются соответственно *прямыми*, *плоскостями* или *гиперплоскостями*.

Рассмотрим теперь точки из $S_{n-1, q}$, определенные с помощью координатных последовательностей

$$A_1(1, 0, \dots, 0), A_2(0, 1, \dots, 0), \dots, A_n(0, 0, \dots, 1).$$

Очевидно, указанные точки образуют независимую систему. Подпространство, порожденное этой системой, совпадает со всем пространством $S_{n-1, q}$; действительно, точку, отвечающую координатам (x_1, x_2, \dots, x_n) , можно записать в виде линейной комбинации $x_1 A_1 + x_2 A_2 + \dots + x_n A_n$. Таким образом, $S_{n-1, q}$ есть подпространство в себе самом; мы будем называть его *несобственным* подпространством.

Простое число p называется характеристикой поля $GF(p^r)$. Мы будем также называть p *характеристикой пространства* S_{n-1, p^r} . Позднее мы дадим интересную геометрическую интерпретацию характеристики пространства; эта интерпретация может быть распространена на недезарговы плоскости.

2.2. Пространство Галуа как конфигурация его подпространств

В этом параграфе будет идти речь о теоремах, относящихся к свойствам инцидентности, а также к операциям объединения и пересечения подпространств пространства Галуа.

1° Если система точек $\{A_1, A_2, \dots, A_k\}$ независима, то каждая ее подсистема также независима.

Докажем сначала независимость подсистемы $\{A_2, A_3, \dots, A_k\}$. Допустив противное, мы получили бы,

что существует последовательность $(\lambda_2, \lambda_3, \dots, \lambda_k) \neq (0, 0, \dots, 0)$, для которой $\lambda_2 A_2 + \lambda_3 A_3 + \dots + \lambda_k A_k = 0$, т. е. $\lambda_1 A_1 + \lambda_2 A_2 + \dots + \lambda_k A_k = 0$, где $\lambda_1 = 0$, но $(\lambda_1, \lambda_2, \dots, \lambda_k) \neq (0, 0, \dots, 0)$. Однако это по условию невозможно. Если теперь принять во внимание, что порядок точек в системе безразличен, то повторным применением нашего рассуждения можно доказать независимость любой подсистемы исходной системы $\{A_1, A_2, \dots, A_k\}$.

2° Если система $\{A_1, A_2, \dots, A_k\}$ не является независимой, то она содержит точку, являющуюся линейной комбинацией остальных точек системы; обратно, если одна из точек системы является линейной комбинацией остальных точек, то система не является независимой.

В самом деле, если система не является независимой, то существует последовательность коэффициентов $\lambda_1, \dots, \lambda_k$, не равных одновременно нулю, для которой справедливо соотношение $\lambda_1 A_1 + \lambda_2 A_2 + \dots + \lambda_k A_k = 0$. Не ограничивая общности, можно считать $\lambda_1 \neq 0$. Тогда

$$A_1 = \lambda_2' A_2 + \lambda_3' A_3 + \dots + \lambda_k' A_k,$$

где $\lambda_j' = \lambda_j \lambda_1^{-1}$ ($j = 2, 3, \dots, k$).

Обратно, если имеет место соотношение $A_1 = \lambda_2' A_2 + \lambda_3' A_3 + \dots + \lambda_k' A_k$, то, полагая $\lambda_1 = 1$, $\lambda_j = -\lambda_j'$ ($j = 2, 3, \dots, k$), получим $\lambda_1 A_1 + \lambda_2 A_2 + \dots + \lambda_k A_k = 0$, причем среди элементов $\lambda_1, \lambda_2, \dots, \lambda_k$ имеются не равные нулю. Это означает, что система $\{A_1, A_2, \dots, A_k\}$ не является независимой.

3° Множество S , состоящее из точек вида $P = \xi_1 A_1 + \xi_2 A_2 + \dots + \xi_k A_k$, где A_1, A_2, \dots, A_k — фиксированный набор точек, есть подпространство.

Если система $\{A_1, A_2, \dots, A_k\}$ независима, то S есть подпространство по определению. Пусть теперь система не является независимой. Выбрав подходящим образом порядок точек, будем иметь $A_1 = \lambda_2 A_2 + \lambda_3 A_3 + \dots + \lambda_k A_k$. Обозначим через S' множество точек вида $P = \xi_2' A_2 + \xi_3' A_3 + \dots + \xi_k' A_k$. Если $P \in S$, то $P \in S'$, так как из $P = \xi_1 A_1 + \xi_2 A_2 + \dots + \xi_k A_k$ следует $P = (\xi_1 \lambda_2 + \xi_2) A_2 + (\xi_1 \lambda_3 + \xi_3) A_3 + \dots + (\xi_1 \lambda_k + \xi_k) A_k$. Очевидно также, что если $P \in S'$, то $P \in S$. Следовательно, $S = S'$.

Повторяя это рассуждение, мы придем в конце концов к независимой системе точек $\{A_{h+1}, A_{h+2}, \dots, A_k\}$, $h \leq k-1$, причем $S = S' = \dots = S^{(h)}$, где $S^{(h)}$ обозначает множество точек вида $\xi_{h+1}A_{h+1} + \dots + \xi_k A_k$, являющееся уже подпространством. Таким образом, S есть подпространство, содержащее

$$\theta_{h-1} = q^{h-1} + q^{h-2} + \dots + 1$$

точек.

4° Множество точек, порожденных подпространством *) S , совпадает с S .

Пусть S — подпространство, порожденное независимой системой точек $\{A_1, A_2, \dots, A_k\}$. Рассмотрим какие-либо точки

$$B_j = \lambda_{j1}A_1 + \lambda_{j2}A_2 + \dots + \lambda_{jk}A_k \quad (j = 1, 2, \dots, l)$$

из S , причем будем предполагать, что коэффициенты λ_{jl} выбраны таким образом, что координатная последовательность для каждой из точек B_j является нормированной.

Рассмотрим теперь точку

$$P = \xi_1 B_1 + \xi_2 B_2 + \dots + \xi_l B_l.$$

Очевидно,

$$P = \eta_1 A_1 + \eta_2 A_2 + \dots + \eta_k A_k,$$

где $\eta_h = \lambda_{1h}\xi_1 + \lambda_{2h}\xi_2 + \dots + \lambda_{lh}\xi_l$ ($h = 1, 2, \dots, k$). Отсюда видно, что $P \in S$.

5° В подпространстве S , порожденном независимой системой $\{A_1, A_2, \dots, A_k\}$, существует не более k независимых точек.

Число всех точек рассматриваемого подпространства есть θ_{k-1} . Согласно 4° каждая точка подпространства, порожденного независимой системой $\{B_1, B_2, \dots, B_l\}$ точек из S , принадлежит S , следовательно, $\theta_{l-1} \leq \theta_{k-1}$. Отсюда вытекает $l \leq k$.

Мы уже знаем, что в пространстве $S_{n-1,q}$ система из n точек, определяемых координатными последовательностями $(1, 0, 0, \dots, 0)$, $(0, 1, 0, \dots, 0)$, \dots , $(0, 0, 0, \dots, 1)$, является независимой системой точек. Следовательно, в этом пространстве существует не более

*) То есть являющихся линейными комбинациями точек из S . — Прим. перев.

n независимых точек. Любая максимальная система независимых точек пространства называется *базисом*, а число точек базиса минус 1 называется *размерностью* пространства. Очевидно, это соответствует употреблению указанных слов в обычной геометрии. (Прямая есть одномерное пространство, плоскость — двумерное; прямая порождается двумя из ее точек, плоскость — тремя.) Таким образом, в символе $S_{n-1,q}$ первый индекс обозначает размерность. Разумеется, пространство, содержащее более одной точки, имеет различные базисы. Например, любая из двух систем:

$$(1, 0, 0, \quad 0), (0, 1, 0, \quad 0), \quad (0, 0, 0, \quad 1)$$

и

$$(1, 0, 0, \quad 0), (1, 1, 0, \quad 0), \quad (1, 1, 1, \quad 1),$$

содержащих каждая n точек, является базисом пространства $S_{n-1,q}$.

В дальнейшем пространство Галуа размерности n будет обозначаться S_n ; при этом предполагается, что q фиксировано.

Пусть S_k , S_l и S_n заданы таким образом, что $S_k \subset S_n$ и $S_l \subset S_n$, $k \leq l$. Рассмотрим ряд предложений о пересечении и объединении подпространств S_k и S_l .

6° Если множество $S^* = S_k \cap S_l$ не пусто, то оно является m -мерным подпространством в S_n , где $m \leq k$.

Пусть $\{Q_1, Q_2, \dots, Q_{m+1}\}$ будет максимальная независимая система точек в множестве S^* . Очевидно, $m \leq k$. Каждая точка подпространства S_m , порожденного этой системой точек, принадлежит множеству S^* , ибо, в силу 4°, эта точка должна принадлежать как S_k , так и S_l . Если бы существовала точка Q такая, что $Q \in S^*$, но $Q \notin S_m$, то, в силу 2°, система $\{Q_1, Q_2, \dots, Q_m, Q\}$ была бы независимой системой точек, что противоречит нашим допущениям. Таким образом, $S^* = S_m$.

Подпространство $S^* = S_m$ называется *пересечением* подпространств S_k и S_l ; оно является *максимальным подпространством*, содержащимся в обоих данных подпространствах.

7° Если множество $S_k \cap S_l$ пусто, то $k + l < n$.

Допустим, рассуждая от противного, что $k + l \geq n$. Тогда $k + 1 + l + 1 \geq n + 1$. Пусть $\{A_1, A_2, \dots, A_{k+1}\}$ и $\{B_1, B_2, \dots, B_{l+1}\}$ — линейно независимые системы

точек, порождающие S_k и S_l соответственно. Базис пространства S_n состоит из $n + 1$ точек; следовательно, система

$$\{A_1, \quad A_{k+1}, B_1, \quad B_{l+1}\},$$

содержащая $k + l + 2$ точек, не является независимой. В силу 2° можно считать, что точка B_{l+1} есть линейная комбинация остальных точек системы. Положим, что

$$B_{l+1} = \lambda_1 A_1 + \quad + \lambda_{k+1} A_{k+1} + \mu_1 B_1 + \quad + \mu_l B_l.$$

Тогда

$$\lambda_1 A_1 + \quad + \lambda_{k+1} A_{k+1} = -\mu_1 B_1 - \quad - \mu_l B_l + B_{l+1}.$$

Последний из коэффициентов в правой части отличен от нуля, следовательно, правая часть есть точка из S_l ; эта точка, как показывает левая часть, принадлежит S_k , что противоречит условию. Предложение 7° доказано.

Если множество $S_k \cap S_l$ пусто, то подпространства S_k и S_l называются *расходящимися* или *независимыми*. Необходимым условием этого является $k + l < n$.

Пусть теперь S_k и S_l — два произвольных подпространства в S_n . Пересечение всех подпространств, содержащих S_k и S_l , называется *объединением* *) двух данных подпространств. Очевидно, объединение подпространств S_k и S_l можно определить эквивалентным образом как *подпространство наименьшей размерности*, содержащее оба данных подпространства.

8° Если $S_k, S_l \subset S_n$ и $S_k \cap S_l$ пусто, то для объединения S_r имеем $r = k + l + 1$.

Если мы допустим, что $r < k + l + 1$, то число точек в любой независимой системе, принадлежащей S_r , будет $< k + l + 2$. Но тогда система точек, составленная из двух систем $\{A_1, A_2, \dots, A_{k+1}\}$ и $\{B_1, B_2, \dots, B_{l+1}\}$, порождающих соответственно S_k и S_l , не будет независимой. Используя рассуждение, примененное в доказательстве предложения 7°, выводим отсюда, что подпространства S_k и S_l имеют общую точку.

*) Не следует смешивать с объединением в теоретико-множественном смысле, т. е. с множеством $S_k \cup S_l$. — *Прим. перев.*

Наше допущение, таким образом, приводит к противоречию. Теорема доказана *).

9° Если $S_k, S_l \subset S_n$ и $S_k \cap S_l = S_m$ ($m \geq 0$), то для размерности объединения S_r подпространств S_k и S_l справедливо соотношение $r + m = k + l$.

Подпространства S_k и S_l порождаются независимыми системами точек, содержащими $k + 1$ и $l + 1$ точек соответственно. Эти системы можно выбрать таким образом, что каждая из них будет содержать независимую систему $\{C_1, C_2, \dots, C_{m+1}\}$, порождающую S_m . Пусть указанные две системы суть

$$\{A_1, \dots, A_{k-m}, C_1, \dots, C_{m+1}\}$$

и

$$\{B_1, \dots, B_{l-m}, C_1, \dots, C_{m+1}\}.$$

Мы утверждаем, что система точек $\{A_1, \dots, A_{k-m}, B_1, \dots, B_{l-m}, C_1, \dots, C_{m+1}\}$ является независимой, т. е. что соотношение

$$\lambda_1 A_1 + \dots + \lambda_{k-m} A_{k-m} + \nu_1 C_1 + \dots + \nu_{m+1} C_{m+1} = \mu_1 B_1 + \dots + \mu_{l-m} B_{l-m}$$

возможно только в случае, когда все коэффициенты равны нулю.

В самом деле, если отличные от нуля коэффициенты встречаются в этом соотношении, то по крайней мере один из коэффициентов μ , не равен нулю — в противном случае, ввиду независимости системы $\{A_1, \dots, A_{k-m}, C_1, \dots, C_{m+1}\}$, были бы равны нулю также и все коэффициенты λ и ν . Так как точки B независимы, то отсюда следует, что выражение, стоящее в правой части нашего соотношения, определяет настоящую точку; обозначим последнюю P . Поскольку каждая из точек B принадлежит подпространству S_l , мы имеем $P \in S_l$. С другой стороны, выражение, стоящее в левой части, показывает,

*) Следует учесть, что в любом случае $r \leq k + l + 1$. Действительно, если $\{A_1, \dots, A_{k+1}\}$ и $\{B_1, \dots, B_{l+1}\}$ — базисы S_k и S_l соответственно, то множество точек, порожденное системой $\{A_1, \dots, A_{k+1}, B_1, \dots, B_{l+1}\}$, есть подпространство размерности $\leq k + l + 1$. Это подпространство очевидным образом содержит S_r . Отсюда $r \leq k + l + 1$. — *Прим. перев.*

что $P \in S_k$. Следовательно, $P \in S_m$. Таким образом, точка P представима как в виде линейной комбинации точек B , так и в виде линейной комбинации точек C :

$$\begin{aligned} P &= \xi_1 C_1 + \xi_2 C_2 + \dots + \xi_{m+1} C_{m+1} = \\ &= \mu_1 B_1 + \mu_2 B_2 + \dots + \mu_{l-m} B_{l-m}. \end{aligned}$$

Это, однако, противоречит предположению, что система $\{C_1, \dots, C_{m+1}, B_1, \dots, B_{l-m}\}$ независима.

Итак, мы видим, что можно выбрать $k + l - m + 1$ независимых точек из S_k и S_l . Эти точки не могут содержаться в подпространстве размерности меньшей, чем $k + l - m$, откуда следует $r \geq k + l - m$. С другой стороны, подпространство, порожденное этими точками, содержит S_r , следовательно, $k + l - m \geq r$. Доказательство закончено.

10° Точки $(x_1, x_2, \dots, x_{n+1})$ пространства $S_{n,q}$, удовлетворяющие уравнению

$$a_1 x_1 + a_2 x_2 + \dots + a_{n+1} x_{n+1} = 0,$$

где коэффициенты $a_1, \dots, a_{n+1} \in GF(q)$ не равны одновременно нулю, образуют гиперплоскость. Обратно, все точки произвольной гиперплоскости удовлетворяют некоторому уравнению указанного вида.

Докажем первое утверждение теоремы. Если последовательность $(x_1, x_2, \dots, x_{n+1})$ удовлетворяет данному уравнению, то, очевидно, и любая последовательность $(x'_1, x'_2, \dots, x'_{n+1}) = (\lambda x_1, \lambda x_2, \dots, \lambda x_{n+1})$ также ему удовлетворяет; мы можем, следовательно, говорить просто о точке, удовлетворяющей уравнению.

Ясно, что не все точки пространства $S_{n,q}$ удовлетворяют данному уравнению: если предположить (что не ограничивает общности) $a_1 \neq 0$, то получим, что точка $(1, 0, 0, \dots, 0)$ не принадлежит множеству S , определяемому данным уравнением.

Очевидно также, что если каждая из независимых точек $\{A_1, \dots, A_k\}$ принадлежит S , то любая точка подпространства S_{k-1} , порожденного $\{A_1, \dots, A_k\}$, принадлежит S .

Из двух последних утверждений следует, что S не может содержать $n + 1$ независимых точек. Покажем, однако, что S содержит n независимых точек. Будем

считать, что $a_1 \neq 0$, — этого можно добиться перенумерацией индексов (если необходимо); пусть $-a_j a_1^{-1} = c_j$ ($j = 2, 3, \dots, n+1$). Очевидно, каждая из n точек $(c_2, 1, 0, \dots, 0), (c_3, 0, 1, \dots, 0), \dots, (c_{n+1}, 0, 0, \dots, 1)$ удовлетворяет данному уравнению. Легко также видеть, что эти точки независимы. Обозначим их соответственно C_2, C_3, \dots, C_{n+1} . Всевозможные точки вида

$$\lambda_2 C_2 + \lambda_3 C_3 + \dots + \lambda_{n+1} C_{n+1}$$

исчерпывают S , так как в противном случае S содержало бы более n независимых точек, что невозможно. Тем самым мы доказали первую часть предложения 10°.

Рассмотрим теперь какое-либо подпространство S_{n-1} , т. е. подпространство, порожденное n независимыми точками. Точки

$$(1, 0, 0, \dots, 0), (0, 1, 0, \dots, 0), \dots, (0, 0, 0, \dots, 1),$$

образующие базис пространства $S_{n,q}$, не могут все вместе лежать в подпространстве S_{n-1} ; допустим, что первая из них не принадлежит S_{n-1} . Пусть $l_{12}, l_{13}, \dots, l_{1,n+1}$ — прямые, соединяющие первую точку с каждой из остальных соответственно. Каждая из указанных прямых должна иметь общую точку с S_{n-1} . Пусть эти точки — скажем, B_2, B_3, \dots, B_{n+1} — задаются координатными последовательностями

$$(b_2, 1, 0, \dots, 0), (b_3, 0, 1, \dots, 0), \dots, (b_{n+1}, 0, 0, \dots, 1)$$

соответственно. Очевидно, указанные точки образуют независимую систему и каждая из них удовлетворяет уравнению

$$x_1 - b_2 x_2 - b_3 x_3 - \dots - b_{n+1} x_{n+1} = 0.$$

Множество точек, определяемое этим уравнением, состоит только из точек вида

$$\mu_2 B_2 + \mu_3 B_3 + \dots + \mu_{n+1} B_{n+1},$$

так как более чем n независимых точек удовлетворять уравнению не могут. Мы доказали, таким образом, вторую часть теоремы.

Сделаем теперь некоторые замечания к доказанным теоремам.

Прежде всего, сравним формулы $r = k + l + 1$ и $r = k + l - m$, фигурирующие в 8° и 9° соответственно, т. е. формулы, дающие размерность объединения S_r двух подпространств S_k и S_l пространства $S_{n,q}$. Первая из этих формул относится к случаю, когда $S_k \cap S_l$ есть пустое множество, вторая — к случаю, когда указанное пересечение S_m содержит по крайней мере одну точку, т. е. когда $m \geq 0$. Если мы условимся считать, что пустое множество имеет размерность -1 , то первая формула может рассматриваться как частный случай второй.

Наше второе замечание значительно важнее. Очевидно, уравнение

$$a_1x_1 + a_2x_2 + \dots + a_{n+1}x_{n+1} = 0,$$

в котором не все коэффициенты равны нулю, и уравнение

$$\lambda a_1x_1 + \lambda a_2x_2 + \dots + \lambda a_{n+1}x_{n+1} = 0,$$

где $\lambda \neq 0$, определяют одно и то же множество точек. Допустим, что уравнение

$$b_1x_1 + b_2x_2 + \dots + b_{n+1}x_{n+1} = 0$$

определяет это же самое множество. Как связаны в этом случае коэффициенты a и b ?

Рассмотрим сначала базис

$$A_1(1, 0, 0, \dots, 0), A_2(0, 1, 0, \dots, 0), \dots, A_{n+1}(0, 0, 0, \dots, 1)$$

пространства $S_{n,q}$. Изменив, если нужно, нумерацию координат, можно считать, что точка A_1 не удовлетворяет уравнению, определенному с помощью коэффициентов a , и, следовательно, не удовлетворяет уравнению с коэффициентами b . Подпространство S_{n-1} , определенное уравнениями, пересекается с каждой из прямых A_1A_j ($j = 2, 3, \dots, n+1$) в единственной точке, и n полученных таким образом точек образуют независимую систему. Если мы выразим координатные последовательности этих точек в терминах коэффициентов каждого из уравнений, то получим

$$(-a_1^{-1}a_2, 1, 0, \dots, 0), (-a_1^{-1}a_3, 0, 1, \dots, 0), \dots, (-a_1^{-1}a_{n+1}, 0, 0, \dots, 1).$$

и

$$(-b_1^{-1}b_2, 1, 0, \dots, 0), \quad (-b_1^{-1}b_3, 0, 1, \dots, 0), \\ \dots, (-b_1^{-1}b_{n+1}, 0, 0, \dots, 1).$$

Но, согласно нашему допущению, эти два множества состоят из одних и тех же n точек, следовательно,

$$b_1 = \lambda a_1, \quad b_2 = \lambda a_2, \quad \dots, \quad b_{n+1} = \lambda a_{n+1},$$

где $\lambda = b_1 a_1^{-1} \neq 0$.

Таким образом, мы можем отождествить гиперплоскости с классами последовательностей из $n + 1$ элементов, не равных одновременно нулю, как мы это делаем с точками. Чтобы отличать задаваемые таким образом гиперплоскости от точек, мы используем обозначение $[u_1, u_2, \dots, u_{n+1}]$, где элементы u_1, u_2, \dots, u_{n+1} называются *однородными координатами* гиперплоскости. Таким образом, точка (x_1, \dots, x_{n+1}) и гиперплоскость $[u_1, \dots, u_{n+1}]$ инцидентны в том и только в том случае, когда $u_1 x_1 + \dots + u_{n+1} x_{n+1} = 0$. Ввиду симметрии между элементами u и x в условии инцидентности, в пространстве $S_{n,q}$ справедлив *принцип двойственности*. Согласно этому принципу, если какая-то теорема верна в пространстве $S_{n,q}$, то, поменяв в утверждении теоремы ролями точки и гиперплоскости, мы получим другую теорему, которая также верна в $S_{n,q}$.

В пространстве Галуа можно ввести понятие, совершенно аналогичное двойному отношению в классическом проективном пространстве. Пусть нормированные последовательности $(a_1, a_2, \dots, a_{n+1})$ и $(b_1, b_2, \dots, b_{n+1})$ определяют две независимые точки A и B . Рассмотрим точки $\lambda A + \mu B = C$ и $\rho A + \sigma B = D$, где C отлична от A и B , а D отлична от A . Мы будем понимать под *двойным отношением* $(ABCD)$ точек A, B, C, D , заданных в указанном порядке, элемент

$$(ABCD) = \lambda^{-1} \mu \rho \sigma^{-1} = \theta$$

координатного поля.

Мы увидим, что это понятие дает возможность **развивать** геометрию Галуа, используя штейнеровский подход к проективной геометрии.

В заключение заметим, что множество нетривиальных решений системы однородных линейных уравнений, опре-

деленных над полем Галуа, есть в точности пересечение множества гиперплоскостей в пространстве Галуа, отвечающих данным уравнениям; первое из этих понятий принадлежит алгебре, второе — геометрии.

2.3. Обобщение теоремы Паппа на плоскости Галуа

В последующем изложении мы ограничимся случаем плоскости Галуа и будем использовать результаты параграфов 1.10 и 2.2. Прежде всего рассмотрим следующую теорему Паппа для классической проективной плоскости.

Если прямые u_1, u_2, u_3, u_4 , принадлежащие одному пучку, пересекаются прямой a , не принадлежащей пучку, соответственно в точках X_1, X_2, X_3, X_4 , то двойное отношение $(u_1 u_2 u_3 u_4)$ четверки прямых равно двойному отношению $(X_1 X_2 X_3 X_4)$ четверки точек.

Двойное отношение четверки прямых, принадлежащих одному пучку, определяется двойственным образом к двойному отношению четверки коллинеарных точек. Пусть $[a_1, a_2, a_3]$ и $[b_1, b_2, b_3]$ — две нормированные линейно независимые координатные последовательности и a, b — соответствующие им различные прямые. Прямая c , проходящая через общую точку прямых a и b , характеризуется последовательностью координат (не обязательно нормированной)

$$[c_1, c_2, c_3] = [\lambda a_1 + \mu b_1, \lambda a_2 + \mu b_2, \lambda a_3 + \mu b_3],$$

что записывается кратко $c = \lambda a + \mu b$. Другая подобным же образом выбранная прямая будет $d = \rho a + \sigma b$. Под двойным отношением $(abcd)$ рассматриваемой четверки прямых, в данном их порядке, понимается элемент

$$(abcd) = \lambda^{-1} \mu \rho \sigma^{-1}$$

координатного поля.

Мы будем использовать следующую сокращенную запись:

$$[u_1, u_2, u_3] = [u], \quad (x_1, x_2, x_3) = (x),$$

$$u_1 x_1 + u_2 x_2 + u_3 x_3 = [u](x),$$

$$[\lambda u_{k1}, \lambda u_{k2}, \lambda u_{k3}] = \lambda [u_{k1}, u_{k2}, u_{k3}] = \lambda [u]_k,$$

$$(\lambda x_{k1}, \lambda x_{k2}, \lambda x_{k3}) = \lambda (x_{k1}, x_{k2}, x_{k3}) = \lambda (x)_k.$$

Ниже, говоря о двух различных прямых, мы будем подразумевать две нормированные линейно независимые последовательности координат. Пусть $[u]_1$ и $[u]_2$ — такие прямые. Пусть две другие прямые, проходящие через точку пересечения $[u]_1$ и $[u]_2$, будут $[u]_3 = \lambda [u]_1 + \mu [u]_2$ и $[u]_4 = \rho [u]_1 + \sigma [u]_2$. Аналогичным образом рассмотрим четверку точек, принадлежащих одной прямой: пусть эти точки будут

$$(x)_1, (x)_2, (x)_3 = \alpha (x)_1 + \beta (x)_2, (x)_4 = \gamma (x)_1 + \delta (x)_2.$$

Условия теоремы Паппа запишутся следующим образом:

$$\begin{aligned} [u]_1 (x)_1 &= 0, & [u]_2 (x)_2 &= 0, & [u]_1 (x)_2 &= \xi \neq 0, \\ [u]_2 (x)_1 &= \eta \neq 0, & [u]_3 (x)_3 &= 0, & [u]_4 (x)_4 &= 0. \end{aligned}$$

Для линейных комбинаций, которыми являются $[u]_3$, $[u]_4$, $(x)_3$ и $(x)_4$, последние два из написанных уравнений означают, что пара элементов (ξ, η) удовлетворяет соотношениям

$$\begin{aligned} \lambda\beta \cdot \xi + \mu\alpha \cdot \eta &= 0, \\ \rho\delta \cdot \xi + \sigma\gamma \cdot \eta &= 0. \end{aligned}$$

Рассматривая эти два соотношения как систему уравнений с неизвестными ξ , η и учитывая $(\xi, \eta) \neq (0, 0)$, находим, что определитель системы есть нулевой элемент координатного поля:

$$\lambda\beta\sigma\gamma - \mu\alpha\rho\delta = 0.$$

Если λ , σ , α и δ отличны от нуля, то **это соотношение** может быть представлено в виде

$$\lambda^{-1}\mu\rho\sigma^{-1} = \alpha^{-1}\beta\gamma\delta^{-1}.$$

Но выражение, стоящее в правой части, есть двойное отношение четверки точек $(x)_1, (x)_2, (x)_3, (x)_4$, а выражение в левой части есть двойное отношение четверки прямых $[u]_1, [u]_2, [u]_3, [u]_4$. Таким образом, мы проверили справедливость теоремы Паппа для плоскости Галуа.

Рассмотрим три различные точки X_1, X_2, X_3 прямой. Любой точке X_4 , отличной от X_1 , можно сопоставить двойное отношение $(X_1X_2X_3X_4)$. Легко видеть, что таким путем мы получаем взаимно однозначное соответствие

между элементами координатного поля K и точками данной прямой, отличными от X_1 . При этом, как нетрудно видеть, нулевой и единичный элементы из K отвечают соответственно X_1 и X_3 . Эти заключения могут быть двойственным образом перенесены на четверку прямых, принадлежащих одному пучку.

Из определения двойного отношения очевидным образом вытекают следующие свойства:

$$(\alpha) \quad (X_1 X_2 X_3 X_4) + (X_1 X_3 X_2 X_4) = 1;$$

$$(\alpha\alpha) \quad (X_1 X_2 X_3 X_4) - (X_3 X_4 X_1 X_2) = 0;$$

$$(\alpha\alpha\alpha) \quad \text{если } (X_1 X_2 X_3 X_4) \neq 0, \text{ то}$$

$$(X_1 X_2 X_3 X_4) \cdot (X_1 X_2 X_4 X_3) = 1.$$

Доказательства предоставляем читателю.

Результаты, полученные в этой главе, могут с первого взгляда вызвать мысль о полной тождественности между геометрией Галуа и классической проективной геометрией. Однако это не так; мы обсудим теперь некоторые свойства, которые указывают на существование различий между этими двумя геометриями.

Начиная с этого момента наш подход уже не будет чисто алгебраическим; там, где это окажется удобнее, мы будем обращаться к рисунку.

Докажем, что *двойное отношение есть инвариант проектирования*. Обратимся к рис. 47. Согласно теореме Паппа имеем $(ABCD) = (abcd)$ и $(A'B'C'D') = (abcd)$, откуда следует $(ABCD) = (A'B'C'D')$. При этом не обязательно предполагать, что $B = B'$, как показано на рисунке; мы использовали лишь тот факт, что $b \cap u = B$ и $b' \cap u' = B'$. Более того, мы не предполагаем, что прямые a, b, c, d различны, так как теорема Паппа остается верной и в том случае, когда $d = b$ или $d = c$. В частности, теорема Паппа остается справедливой для $S_{2,2}$, когда имеются только три прямые, проходящие через общую точку.

Более сложно обстоит дело с доказательством соотношения $(ABXY) = -1$, относящегося к рис. 48. Мы применяем полученный выше результат сначала к проектированию из точки C , затем к проектированию из точки D .

Находим

$$^*(ABXY) = (UVZY) \text{ и } (UVZY) = (BAXY).$$

Отсюда вытекает $(ABXY) = (BAXY)$. Обозначая этот элемент через θ , получим на основании указанных выше

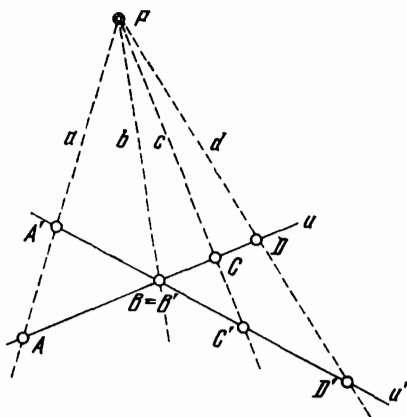


Рис. 47.

свойств двойного отношения, что $\theta^2 = 1$. Заметим, что мы использовали тот факт, что точки A, B, C, D опре-

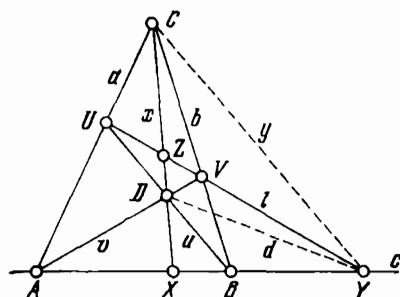


Рис. 48.

деляют собственный четырехугольник, и получили, отправляясь от них, три дальнейшие точки, именно:

$$U = AC \cap BD, \quad V = AD \cap BC, \quad X = AB \cap CD.$$

Итак, мы должны решить уравнение $\theta^2 = 1$; вместе с тем следует дать геометрическую интерпретацию решения. В случае $K = GF(2^r)$ решение существенно другое, чем в случае $GF(p^r)$, $p \neq 2$.

Если поле координат есть $GF(2^r)$, то уравнение $\theta^2 = 1$ имеет одно и только одно решение, а именно $\theta = 1$. (Любой элемент поля характеристики 2 совпадает с противоположным ему элементом по сложению.) Следовательно, в этом случае мы имеем $(ABXY) = 1$, откуда следует $X = Y$; это означает, что прямая $l = UV$ пересекает прямую AB в точке $X = Y$. Такой случай невозможно реализовать на рис. 48; рис. 22, b больше подходит для изображения этого факта.

Мы можем, таким образом, сделать следующее заключение: *любой (собственный) четырехугольник на плоскости Галуа четного порядка есть четырехугольник Фано.*

В случае поля $GF(p^r)$ при $p \neq 2$ существует ровно два решения уравнения $\theta^2 = 1$. Это — единичный элемент 1 и противоположный ему элемент по сложению; эти элементы отличны один от другого. Докажем, что $(ABXY) \neq 1$. С этой целью рассмотрим нормированные тройки координат для точек A , B , C и D . Точку D можно представить следующим образом:

$$D = \lambda A + \mu B + \nu C, \quad \lambda \cdot \mu \cdot \nu \neq 0.$$

Так как $X = AB \cap CD$, то координатная тройка (не обязательно нормированная) для X есть $\lambda A + \mu B = D - \nu C$. Подобным же образом $\lambda A + \nu C = D - \mu B = U$ и $\mu B + \nu C = D - \lambda A = V$. Значит, $U - V = \lambda A - \mu B = Y$. Выражения

$$\lambda A + \mu B = X \quad \text{и} \quad \lambda A - \mu B = Y$$

имеют место безотносительно к характеристике координатного поля. Теперь непосредственно находим, что $(ABXY) = \lambda^{-1}\mu\lambda(-\mu)^{-1} = -1$.

Приведенное выше рассуждение, не использующее теорему Паппа, очевидно, ближе к сути дела, чем то, которое мы дали для случая $X = Y$. Точки X и Y совпадают тогда и только тогда, когда существуют ρ и σ такие, что $(\rho, \sigma) \neq (0, 0)$, но $\rho X + \sigma Y = 0$, т. е. $\lambda(\rho + \sigma)A + \mu(\rho - \sigma)B = 0$. Отсюда, ввиду независимости A и B , следует $\rho + \sigma = \rho - \sigma = 0$, и, значит, $\sigma = -\rho \neq 0$.

Следовательно, $X = Y$ тогда и только тогда, когда $\sigma = -\sigma$, т. е. в том и только в том случае, когда поле имеет характеристику 2.

Как заключение мы получаем следующий результат.
Диагональные точки любого (собственного) четырехугольника на плоскости Галуа нечетного порядка определяют собственный треугольник.

Из доказанного ясно, что аналогия между плоскостями четного порядка и классической проективной плоскостью не столь тесная, как между плоскостями нечетного порядка и классической проективной плоскостью. Поэтому в ряде случаев необходим совершенно разный подход к плоскостям четного и нечетного порядков.

2.4. Координаты на плоскости Галуа

Пусть $\{A_1, A_2, A_3\}$ — независимая система точек в $S_{2,q}$, где A_1, A_2 и A_3 заданы нормированными тройками координат

$$(2.4.1) \quad (a_{11}, a_{12}, a_{13}), (a_{21}, a_{22}, a_{23}), (a_{31}, a_{32}, a_{33})$$

соответственно.

Рассмотрим точку E такую, что

$$(2.4.2) \quad \rho E = A_1 + A_2 + A_3;$$

эта запись означает, что последовательность (e_1, e_2, e_3) , определяющая точку E , получается нормированием последовательности

$$(a_{11} + a_{21} + a_{31}, a_{12} + a_{22} + a_{32}, a_{13} + a_{23} + a_{33}).$$

Очевидно, система точек $\{A_1, A_2, A_3, E\}$ не является независимой, но любые три из этих четырех точек образуют независимую систему, т. е. мы имеем дело с вершинами собственного четырехугольника. Фигура, состоящая из таких четырех точек, называется *системой координат* или *системой отнесения*; первые три точки называются *фундаментальными точками*, четвертая — *единичной точкой*. (Система аксиом, определяющая конечные плоскости, гарантирует, что такой четырехугольник существует.)

Пусть система координат выбрана следующим образом:

$$(2.4.3) \quad A_1^\circ(1, 0, 0), A_2^\circ(0, 1, 0), A_3^\circ(0, 0, 1); E^\circ(1, 1, 1).$$

Тогда координаты точки $P(x_1, x_2, x_3)$ можно рассматривать как коэффициенты линейной комбинации

$$x_1 A_1^\circ + x_2 A_2^\circ + x_3 A_3^\circ,$$

порождающей точку P . Если мы возьмем теперь другую, произвольно выбранную систему координат, то эта же самая точка P будет порождаться другой линейной комбинацией фундаментальных точек: K

$$(2.4.4) \quad \sigma P = x'_1 A_1 + x'_2 A_2 + x'_3 A_3.$$

Это позволяет сопоставить точке P другую последовательность координат, а именно (x'_1, x'_2, x'_3) .

Условимся называть (x_1, x_2, x_3) координатами точки P относительно системы координат $\{A_1^\circ, A_2^\circ, A_3^\circ, E^\circ\}$ или *старыми координатами* P , а (x'_1, x'_2, x'_3) — координатами P относительно системы координат $\{A_1, A_2, A_3, E\}$ или *новыми координатами* P . Легко получить, используя (2.4.1) и (2.4.4), следующие соотношения между старыми и новыми координатами:

$$(2.4.5) \quad \begin{cases} \sigma x_1 = a_{11}x'_1 + a_{21}x'_2 + a_{31}x'_3, \\ \sigma x_2 = a_{12}x'_1 + a_{22}x'_2 + a_{32}x'_3, \\ \sigma x_3 = a_{13}x'_1 + a_{23}x'_2 + a_{33}x'_3. \end{cases}$$

При этом линейная независимость фундаментальных точек эквивалентна отличию от нуля определителя

$$\begin{vmatrix} a_{11} & a_{21} & a_{31} \\ a_{12} & a_{22} & a_{32} \\ a_{13} & a_{23} & a_{33} \end{vmatrix} = A.$$

Обратно, координаты x'_1, x'_2, x'_3 можно **выразить из** (2.4.5) — с точностью до множителя $\rho \neq 0$ — **как линейные функции** от координат x_1, x_2, x_3 :

$$(2.4.6) \quad \begin{cases} \rho x'_1 = c_{11}x_1 + c_{12}x_2 + c_{13}x_3, \\ \rho x'_2 = c_{21}x_1 + c_{22}x_2 + c_{23}x_3, \\ \rho x'_3 = c_{31}x_1 + c_{32}x_2 + c_{33}x_3, \end{cases}$$

причем матрица этой системы обратна матрице системы (2.4.5).

Линейное преобразование $(x) \rightarrow (x')$, определенное с помощью (2.4.6), мы будем называть *невыврожденным линей-*

ным преобразованием. (Употребление термина «преобразование» не грозит в данном случае недоразумением.)

Из (2.4.2) получаем $A_1 + A_2 = \rho E - A_3$, что дает точку $E_3 = A_1 A_2 \cap A_3 E$. Подобным же образом, линейные комбинации $x'_1 A_1 + x'_2 A_2 = \sigma P - x'_3 A_3$, получаемые из (2.4.4), дают точку $P_3 = A_1 A_2 \cap A_3 P$ (рис. 49). Будем

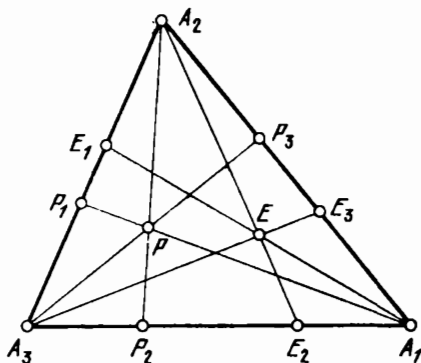


Рис. 49.

предполагать, что $x'_1 \cdot x'_2 \cdot x'_3 \neq 0$. Рассмотрим четверку точек $A_1, A_2, E_3 = A_1 + A_2, P_3 = x'_1 A_1 + x'_2 A_2$. Очевидно,

$$(A_1 A_2 E_3 P_3) = x'_1 x'_2{}^{-1}.$$

Аналогичным образом получим точки $E_1 = A_2 A_3 \cap A_1 E$ и $P_1 = A_2 A_3 \cap A_1 P$, для которых

$$(A_2 A_3 E_1 P_1) = x'_2 x'_3{}^{-1},$$

и точки $E_2 = A_3 A_1 \cap A_2 E$ и $P_2 = A_3 A_1 \cap A_2 P$ такие, что

$$(A_3 A_1 E_2 P_2) = x'_3 x'_1{}^{-1}.$$

Из этих соотношений следует

$$(A_1 A_2 E_3 P_3) \cdot (A_2 A_3 E_1 P_1) \cdot (A_3 A_1 E_2 P_2) = 1.$$

Обратно, пусть дана последовательность ненулевых элементов (ξ_1, ξ_2, ξ_3) . Точки A_2, A_3 и $E_1 = A_2 + A_3$ определяют единственным образом точку P_1 на прямой

A_2A_3 такую, что

$$(A_2A_3E_1P_1) = \frac{\xi_2}{\xi_3}.$$

Подобным же образом, точки A_3 , A_1 и $E_2 = A_3 + A_1$ определяют единственную точку P_2 , для которой

$$(A_3A_1E_2P_2) = \frac{\xi_3}{\xi_1}.$$

Пусть точка $P = A_1P_1 \cap A_2P_2$ задается линейной комбинацией $\eta_1A_1 + \eta_2A_2 + \eta_3A_3$; тогда, согласно предыдущему,

$$(A_2A_3E_1P_1) = \frac{\eta_2}{\eta_3}, \quad (A_3A_1E_2P_2) = \frac{\eta_3}{\eta_1}.$$

Мы имеем, следовательно,

$$\frac{\xi_2}{\xi_3} = \frac{\eta_2}{\eta_3}, \quad \frac{\xi_3}{\xi_1} = \frac{\eta_3}{\eta_1},$$

откуда вытекает

$$\frac{\xi_2}{\xi_1} = \frac{\eta_2}{\eta_1},$$

т. е.

$$(\xi_1, \xi_2, \xi_3) = (\rho\eta_1, \rho\eta_2, \rho\eta_3),$$

где $\rho \neq 0$. Из полученного равенства мы заключаем, что если P_3 есть точка, определенная двойным отношением $(A_1A_2E_3P_3) = \xi_1\xi_2^{-1}$, то прямая, соединяющая P_3 и A_3 , проходит через точку $P = A_1P_1 \cap A_2P_2$.

Заметим, что если $\xi_1\xi_2\xi_3 = 0$, то точка P будет лежать на одной из прямых A_1A_2 , A_2A_3 и A_3A_1 . Точнее, если $\xi_1 = 0$, но $\xi_2\xi_3 \neq 0$, то P есть точка прямой A_2A_3 , определенная двойным отношением $(A_2A_3E_1P_1) = \xi_2\xi_3^{-1}$, и аналогично для точек на двух других прямых; если $\xi_1 = 0$ и $\xi_2 = 0$, то $P = A_3$; если $\xi_2 = 0$ и $\xi_3 = 0$, то $P = A_1$; если $\xi_3 = 0$ и $\xi_1 = 0$, то $P = A_2$.

Подводя некоторый итог, можно дать геометрическое истолкование координатам точки в произвольной системе координат. Пусть A_1 , A_2 , A_3 и E суть фундаментальные точки и единичная точка некоторой системы координат. Из $q^2 + q + 1$ точек плоскости ровно $3(q + 1) - 3$ лежат на сторонах треугольника $A_1A_2A_3$, поскольку

каждая прямая содержит $q + 1$ точек. Мы можем установить взаимно однозначное соответствие между остальными $q^2 - 2q + 1$ точками плоскости и классами троек (x_1, x_2, x_3) , удовлетворяющих условию $x_1 \cdot x_2 \cdot x_3 \neq 0$. Это соответствие получается следующим образом. Пусть E_1 (соответственно E_2, E_3) будет проекция E из A_1 (соответственно из A_2, A_3) на A_2A_3 (соответственно на A_3A_1, A_1A_2). Зададим тройку (x_1, x_2, x_3) , где $x_1 \cdot x_2 \cdot x_3 \neq 0$. Рассмотрим три точки P_1, P_2, P_3 , определенные с помощью двойных отношений

$$(2.4.7) \quad (A_1A_2E_3P_3) = \frac{x_1}{x_2}, \quad (A_2A_3E_1P_1) = \frac{x_2}{x_3}, \\ (A_3A_1E_2P_2) = \frac{x_3}{x_1}.$$

Тогда прямые A_1P_1, A_2P_2 и A_3P_3 пересекаются в некоторой точке P . Сопоставив последовательности (x_1, x_2, x_3) эту точку P , мы получим требуемое соответствие. Что касается точек, лежащих на сторонах треугольника $A_1A_2A_3$, то их характеристика была дана выше.

Все, о чем говорилось в предшествующей части этого параграфа, можно без особого труда перенести по двойственности на координаты прямой. Кратко изложим соответствующие результаты — детали предоставляются читателю.

Системой координат теперь будет система прямых $\{a_1, a_2, a_3, e\}$, из которых никакие три не имеют общей точки. Роль точек E_l, P_l выполняют прямые e_l и p_l , соединяющие точку пересечения $a_j \cap a_k$ с точками $e \cap a_l$ и $p \cap a_l$ соответственно; здесь $(j \ k \ l)$ означает поочередно $(1 \ 2 \ 3), (2 \ 3 \ 1)$ и $(3 \ 1 \ 2)$. Вместо (2.4.7) мы имеем теперь соотношения

$$(2.4.8) \quad (a_j a_k e_l p_l) = u_j u_k^{-1},$$

определяющие координаты $[u_1, u_2, u_3]$ прямой; в исключительных случаях, когда прямая проходит через точку $a_j \cap a_k$ или в точности совпадает с a_j , для ее координат $[u_1, u_2, u_3]$ имеем соответственно $u_l = 0$ или $u_l = u_k = 0$.

В терминах первоначальной системы координат (2.4.3) коэффициенты в уравнении прямой мы рассматривали как координаты прямой, а инцидентность между точкой (x_1, x_2, x_3) и прямой $[u_1, u_2, u_3]$ выражали равенством

$$u_1 x_1 + u_2 x_2 + u_3 x_3 = 0.$$

Пусть мы изменяем систему координат для точек. Всегда ли можно найти такую систему координат для прямых, чтобы инцидентность между точкой и прямой выражалась точно таким же образом? Это означает: если новые координаты точки и прямой суть соответственно (x'_1, x'_2, x'_3) и $[u'_1, u'_2, u'_3]$, то точка лежит на прямой в том и только в том случае, когда

$$u'_1 x'_1 + u'_2 x'_2 + u'_3 x'_3 = 0.$$

Чтобы дать ответ на поставленный вопрос, необходимо исследовать зависимость между первоначальными координатами точек и прямых. Пусть координаты (x_1, x_2, x_3) точки относятся к системе координат (2.4.3), а координаты $[u_1, u_2, u_3]$ прямой — к системе координат

$$(2.4.9) \quad a_1^* [1, 0, 0], \quad a_2^* [0, 1, 0], \quad a_3^* [0, 0, 1]; \quad e^* [1, 1, 1].$$

Из соотношения инцидентности $[u](x) = 0$ следует, что прямые a_1^*, a_2^*, a_3^* суть $A_2^* A_3^*, A_3^* A_1^*$ и $A_1^* A_2^*$ соответственно. Таким образом, фундаментальный треугольник — один и тот же для обеих систем координат, только в случае координат точек он рассматривается как фигура, состоящая из трех точек, а в случае координат прямых — как фигура из трех прямых.

Найдем, далее, связь между единичной точкой и единичной прямой, а также выясним, как они соотносятся с фундаментальным треугольником. Оказывается, что здесь имеет существенное значение характеристика координатного поля. Если координатное поле есть $K = GF(p')$, то необходимо рассмотреть по отдельности три случая: $p = 2$, $p = 3$ и $p \neq 2, 3$.

Рассмотрим сначала случай $p \neq 2, 3$ (см. рис. 50, где мы заменили E_1^* на E_1 и т. д.). Без труда находим координаты точек E_1^*, E_2^*, E_3^* :

$$(2.4.10) \quad E_1^* (0, 1, 1), \quad E_2^* (1, 0, 1), \quad E_3^* (1, 1, 0).$$

Пусть

$$e^* \cap a_1^* = E_1^{**}, \quad e^* \cap a_2^* = E_2^{**}, \quad e^* \cap a_3^* = E_3^{**}$$

Уравнения четырех прямых суть

$$\begin{aligned} e^\circ: x_1 + x_2 + x_3 &= 0, \\ a_1^\circ: x_1 &= 0, \\ a_2^\circ: x_2 &= 0, \\ a_3^\circ: x_3 &= 0. \end{aligned}$$

Отсюда непосредственно находим координаты точек пересечения, указанных выше. В нормированном виде они будут

$$(2.4.11) \quad E_1^{\circ*}(0, -1, 1), \quad E_2^{\circ*}(-1, 0, 1), \quad E_3^{\circ*}(-1, 1, 0).$$

Из (2.4.10) и (2.4.11) легко выясняется структура полной фигуры отнесения, если $p \neq 2, 3$.

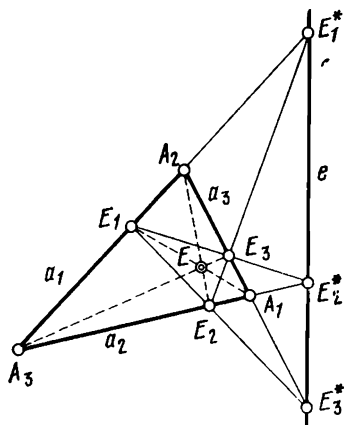


Рис. 50.

- 1° Точка E° не лежит на прямой e° .
- 2° Тройка точек $E_1^\circ, E_2^\circ, E_3^\circ$ есть собственный треугольник.
- 3° Каждая из систем точек $\{A_j^\circ, A_k^\circ, E_l^\circ, E_l^{\circ*}\}$, где $(j k l) = (1 2 3), (2 3 1)$ или $(3 1 2)$, представляет собой гармонический ряд, т. е. четверку коллинеарных точек, двойное отношение которых равно -1 . Действительно, $A_j^\circ + A_k^\circ = E_l^\circ$ и $A_j^\circ - A_k^\circ = E_l^{\circ*}$, откуда следует, что $(A_j^\circ A_k^\circ E_l^\circ E_l^{\circ*}) = -1$ и $E_l^\circ \neq E_l^{\circ*}$.

4° Фундаментальный треугольник $A_1^{\circ}A_2^{\circ}A_3^{\circ}$ и треугольник $E_1^{\circ}E_2^{\circ}E_3^{\circ}$ перспективны с центром E° и осью e° . Это вытекает непосредственно из $A_j^{\circ} - A_k^{\circ} = A_j^{\circ*}$ и $E_j^{\circ} - E_k^{\circ} = E_l^{\circ*}$.

Рис. 50 иллюстрирует эти четыре свойства.

Рассмотрим теперь случай $p = 3$. Здесь выполняются свойства 2°, 3° и 4°, однако ввиду того, что $3 \cdot 1 = 0$, имеем $E^{\circ} \in e^{\circ}$.

4 В случае $p = 2$ остается в силе только свойство 1°; вместо же свойств 2°, 3° и 4° имеем следующее: точки $E_1^{\circ} = E_1^{\circ*}$, $E_2^{\circ} = E_2^{\circ*}$, $E_3^{\circ} = E_3^{\circ*}$ суть три различные точки прямой e° .

То обстоятельство, что фундаментальный треугольник и единичная точка определяют однозначно единичную прямую, остается верным во всех трех случаях.

Теперь мы можем вернуться к вопросу о выборе фигур отнесения $\{A_1, A_2, A_3, E\}$ и $\{a_1, a_2, a_3, e\}$ для новой координатной системы.

Рассмотрим прямую, определяемую уравнением $u_1x_1 + u_2x_2 + u_3x_3 = 0$ относительно первоначальной системы координат. Для новых координат точек прямой мы получаем, согласно (2.4.5), уравнение

$$\frac{1}{\sigma}(a_{11}u_1 + a_{12}u_2 + a_{13}u_3)x'_1 + \frac{1}{\sigma}(a_{21}u_1 + a_{22}u_2 + a_{23}u_3)x'_2 + \frac{1}{\sigma}(a_{31}u_1 + a_{32}u_2 + a_{33}u_3)x'_3 = 0.$$

Обозначим коэффициенты при x'_1, x'_2, x'_3 в этом уравнении соответственно u'_1, u'_2, u'_3 .

Таким образом, уравнение прямой в новых координатах будет

$$u'_1x'_1 + u'_2x'_2 + u'_3x'_3 = 0,$$

и мы назовем прямые, выражающиеся в новых координатах уравнениями $x'_1 = 0$, $x'_2 = 0$, $x'_3 = 0$, прямыми отнесения (новыми), а прямую

$$x'_1 + x'_2 + x'_3 = 0$$

единичной прямой (новой). Итак, новые коэффициенты определяются с помощью такого преобразования:

$$(2.4.12) \quad \begin{cases} \sigma u'_1 = a_{11}u_1 + a_{12}u_2 + a_{13}u_3, \\ \sigma u'_2 = a_{21}u_1 + a_{22}u_2 + a_{23}u_3, \\ \sigma u'_3 = a_{31}u_1 + a_{32}u_2 + a_{33}u_3. \end{cases}$$

Матрица этого линейного преобразования получается транспонированием из матрицы преобразования (2.4.5). Следовательно, она имеет тот же самый определитель $A \neq 0$. Это означает, что преобразование обратимо; обратное преобразование имеет вид

$$(2.4.13) \quad \begin{cases} \rho u_1 = c_{11}u'_1 + c_{21}u'_2 + c_{31}u'_3, \\ \rho u_2 = c_{12}u'_1 + c_{22}u'_2 + c_{32}u'_3, \\ \rho u_3 = c_{13}u'_1 + c_{23}u'_2 + c_{33}u'_3. \end{cases}$$

Из (2.4.11) — (2.4.13) становится ясно, что отношения инцидентности между фигурами $\{A_1, A_2, A_3, E\}$ и $\{a_1, a_2, a_3, e\}$ те же самые, что и между фигурами $\{A_1^\circ, A_2^\circ, A_3^\circ, E^\circ\}$ и $\{a_1^\circ, a_2^\circ, a_3^\circ, e^\circ\}$.

Следовательно, мы можем рассматривать коэффициенты $[u'_1, u'_2, u'_3]$ уравнения прямой в новых координатах как координаты прямой.

В заключение проверим, [как ведет себя двойное отношение при линейном преобразовании.

Пусть (x_1, x_2, x_3) и (y_1, y_2, y_3) — нормированные координатные тройки, определяющие точки X и Y соответственно. Рассмотрим точку Z , определенную с помощью тройки (не обязательно нормированной)

$$(z_1, z_2, z_3) = (\lambda x_1 + \mu y_1, \lambda x_2 + \mu y_2, \lambda x_3 + \mu y_3).$$

После преобразования (2.4.6) новые координаты точек X и Y , в нормированной форме, будут $(\rho x'_1, \rho x'_2, \rho x'_3)$ и $(\rho^* y'_1, \rho^* y'_2, \rho^* y'_3)$ соответственно, где $\rho, \rho^* \neq 0$. Точка Z будет иметь тогда координатную тройку

$$(2.4.14) \quad (\lambda \rho x'_1 + \mu \rho^* y'_1, \lambda \rho x'_2 + \mu \rho^* y'_2, \lambda \rho x'_3 + \mu \rho^* y'_3).$$

Подобным же образом, новые координаты точки T , полученной как линейная комбинация X и Y с коэффициентами ν, ω , будут

$$(2.4.15) \quad (\nu \rho x'_1 + \omega \rho^* y'_1, \nu \rho x'_2 + \omega \rho^* y'_2, \nu \rho x'_3 + \omega \rho^* y'_3).$$

Итак, в первоначальных координатах двойное отношение $(XYZT) = \lambda^{-1} \mu \nu \omega^{-1}$, а в новых координатах

$$(XYZT) = (\lambda \rho)^{-1} \cdot (\mu \rho^*) \cdot (\nu \rho) \cdot (\omega \rho^*)^{-1}.$$

Но

$$(\lambda\rho)^{-1} \cdot (\mu\rho^*) \cdot (\nu\rho) \cdot (\omega\rho^*)^{-1} = \lambda^{-1}\mu\nu\omega^{-1},$$

откуда следует такое заключение: *двойное отношение не зависит от выбора системы координат.*

2.5. Отображения, определенные с помощью линейных преобразований

Пусть линейное преобразование

$$(2.5.1) \quad \begin{cases} \rho x'_1 = c_{11}x_1 + c_{12}x_2 + c_{13}x_3, \\ \rho x'_2 = c_{21}x_1 + c_{22}x_2 + c_{23}x_3, \\ \rho x'_3 = c_{31}x_1 + c_{32}x_2 + c_{33}x_3 \end{cases}$$

является невырожденным (т. е. определитель C матрицы, составленной из коэффициентов, не равен нулю). Будем интерпретировать его как *отображение* плоскости $S_{2,q}$ в себя. А именно, пусть (x_1, x_2, x_3) и (x'_1, x'_2, x'_3) означают нормированные тройки, отнесенные к одной и той же системе координат, скажем к первоначальной системе $\{A_1^\circ, A_2^\circ, A_3^\circ, E^\circ\}$. Очевидно, первая тройка будет нулевой в том и только в том случае, когда вторая тройка — нулевая: это вытекает из условия $C \neq 0$. Следовательно, *невырожденное линейное преобразование (2.5.1) выражает взаимно однозначное отображение плоскости $S_{2,q}$ на себя.* Будем записывать это отображение $C(X) = X'$, где C обозначает матрицу, составленную из коэффициентов в (2.5.1), а X и X' обозначают точки, определяемые тройками (x_1, x_2, x_3) и (x'_1, x'_2, x'_3) соответственно. Обозначая $C^{-1}(X)$ отображение, определенное с помощью матрицы C^{-1} , обратной к C , можем записать $C^{-1}(X') = X$, т. е. отображение $C^{-1}(X)$ является *обратным к отображению $C(X)$.*

Установим теперь некоторые свойства отображения $C(X)$. Мы уже знаем, что уравнение

$$(2.5.2) \quad u_1x_1 + u_2x_2 + u_3x_3 = 0$$

*) В этом месте одним и тем же символом C обозначается и матрица, и ее определитель. — Прим. перев.

эквивалентно

$$(2.5.3) \quad u'_1 x'_1 + u'_2 x'_2 + u'_3 x'_3 = 0,$$

где

$$(2.5.4) \quad \begin{cases} \sigma u'_1 = C_{11}u_1 + C_{12}u_2 + C_{13}u_3, \\ \sigma u'_2 = C_{21}u_1 + C_{22}u_2 + C_{23}u_3, \\ \sigma u'_3 = C_{31}u_1 + C_{32}u_2 + C_{33}u_3. \end{cases}$$

Здесь C_{jk} обозначает алгебраическое дополнение для элемента c_{jk} матрицы C *). Итак, образ множества точек, удовлетворяющих уравнению (2.5.2), есть множество точек, удовлетворяющих (2.5.3). Мы получили следующий результат:

1° *Отображение $C(X)$, определенное формулами (2.5.1), переводит прямые в прямые.*

Соотношения (2.5.4) выражают тот факт, что прямая, определенная тройкой $[\sigma u'_1, \sigma u'_2, \sigma u'_3]$, является образом прямой, определенной посредством нормированной тройки $[u_1, u_2, u_3]$. Мы можем, следовательно, сказать, что отображение $C(X)$ индуцирует взаимно однозначное отображение множества прямых на себя. Из предложения, доказанного в конце параграфа 2.4, вытекает следующее:

2° *Отображение $C(X)$ сохраняет двойные отношения.*

Иначе говоря, если отображение переводит точки A, B, C, D прямой в точки A', B', C', D' , то последние коллинеарны и справедливо равенство $(ABCD) = (A'B'C'D')$.

Рассматривая отображение (2.5.4), можно двойственным к 1° и 2° образом получить:

Образ множества прямых, принадлежащих одному пучку, есть снова множество прямых, принадлежащих одному пучку; при этом, если прямые a', b', c', d' являются образами прямых a, b, c, d , то справедливо равенство $(abcd) = (a'b'c'd')$.

Начиная с этого места, отображение множества точек, определенное с помощью линейного преобразования, и индуцированное им отображение множества прямых будем называть совокупно *линейным отображением*. В параграфе 1.12 мы встретились с понятием коллинеации, т. е. взаимно однозначного отображения плоскости на себя,

*) Напомним, что, согласно предыдущему параграфу, матрицы, выражающие x' через x и u' через u , обратны и транспонированы по отношению друг к другу. — *Прим. перев.*

сохраняющего прямолинейное расположение точек. Очевидно, *любое линейное отображение есть коллинеация*. Однако значительно труднее определить, является ли всякая коллинеация линейным отображением.

2.6. Линейное отображение данного четырехугольника в другой данный четырехугольник

Рассмотрим собственный четырехугольник, образованный точками $A_1^{\circ}(1, 0, 0)$, $A_2^{\circ}(0, 1, 0)$, $A_3^{\circ}(0, 0, 1)$ и $E^{\circ}(1, 1, 1)$ в плоскости $S_{2,q}$. Наряду с ним рассмотрим другой четырехугольник, образованный точками

$$A_j(a_{j1}, a_{j2}, a_{j3}) \quad (j = 1, 2, 3, 4),$$

никакие три из которых не принадлежат одной прямой; координатные последовательности точек A_j предполагаются нормированными.

Линейное отображение

$$(2.6.1) \quad \begin{cases} \rho x'_1 = \lambda_1 a_{11} x_1 + \lambda_2 a_{21} x_2 + \lambda_3 a_{31} x_3, \\ \rho x'_2 = \lambda_1 a_{12} x_1 + \lambda_2 a_{22} x_2 + \lambda_3 a_{32} x_3, \\ \rho x'_3 = \lambda_1 a_{13} x_1 + \lambda_2 a_{23} x_2 + \lambda_3 a_{33} x_3, \end{cases}$$

отнесенное к системе координат $\{A_1^{\circ}, A_2^{\circ}, A_3^{\circ}, E^{\circ}\}$, где ρ , λ_1 , λ_2 , λ_3 означают четыре отличных от нуля элемента, сопоставляет точкам A_1° , A_2° , A_3° точки A_1 , A_2 , A_3 соответственно. Это отображение является невырожденным, поскольку его определитель есть

$$A^* = \lambda_1 \lambda_2 \lambda_3 A,$$

где

$$(2.6.2) \quad A = \begin{vmatrix} a_{11} & a_{21} & a_{31} \\ a_{12} & a_{22} & a_{32} \\ a_{13} & a_{23} & a_{33} \end{vmatrix},$$

в силу же независимости точек A_1 , A_2 , A_3 элемент A не равен нулю.

Подходящим выбором коэффициентов λ_1 , λ_2 , λ_3 можно добиться того, чтобы было

$$(2.6.3) \quad \begin{cases} a_{41} = \lambda_1 a_{11} + \lambda_2 a_{21} + \lambda_3 a_{31}, \\ a_{42} = \lambda_1 a_{12} + \lambda_2 a_{22} + \lambda_3 a_{32}, \\ a_{43} = \lambda_1 a_{13} + \lambda_2 a_{23} + \lambda_3 a_{33}, \end{cases}$$

т. е. чтобы точка A_4 являлась образом точки E° . Действительно, ввиду независимости точек A_j каждый из миноров третьего порядка матрицы

$$\begin{pmatrix} a_{11} & a_{21} & a_{31} & a_{41} \\ a_{12} & a_{22} & a_{32} & a_{42} \\ a_{13} & a_{23} & a_{33} & a_{43} \end{pmatrix}$$

не равен нулю. Следовательно, система уравнений (2.6.3) имеет единственное решение $\lambda_1, \lambda_2, \lambda_3$, причем все три этих элемента отличны от нуля.

Подводя итог, можно сказать, что *существует линейное отображение, которое переводит вершины собственного четырехугольника $A_1^\circ A_2^\circ A_3^\circ E^\circ$ в вершины другого произвольного выбранного собственного четырехугольника $A_1 A_2 A_3 E$.*

Обозначим это отображение φ , а обратное отображение φ^{-1} . Отвлекаясь от прежних обозначений, запишем отображение φ^{-1} в виде *)

$$(2.6.4) \quad \varphi^{-1}: \begin{cases} \rho x'_1 = a_{11}x_1 + a_{12}x_2 + a_{13}x_3, \\ \rho x'_2 = a_{21}x_1 + a_{22}x_2 + a_{23}x_3, \\ \rho x'_3 = a_{31}x_1 + a_{32}x_2 + a_{33}x_3 \end{cases} \quad (\det(a_{jh}) \neq 0).$$

Пусть B_1, B_2, B_3, B_4 — произвольно выбранный собственный четырехугольник. Рассмотрим линейное отображение, переводящее точки $A_1^\circ, A_2^\circ, A_3^\circ$ и E° соответственно в точки B_1, B_2, B_3 и B_4 ; пусть это отображение

$$(2.6.5) \quad \psi: \begin{cases} \sigma x'_1 = b_{11}x_1 + b_{12}x_2 + b_{13}x_3, \\ \sigma x'_2 = b_{21}x_1 + b_{22}x_2 + b_{23}x_3, \\ \sigma x'_3 = b_{31}x_1 + b_{32}x_2 + b_{33}x_3 \end{cases} \quad (\det(b_{jh}) \neq 0).$$

Пусть отображение φ^{-1} переводит точку X , определенную с помощью нормированной тройки (x_1, x_2, x_3) , в точку X' , определенную нормированной тройкой (x'_1, x'_2, x'_3) , а отображение ψ переводит X' в точку X'' , задаваемую нормированной тройкой (x''_1, x''_2, x''_3) ; тогда отображение $X \rightarrow X''$ называется *композицией* (или *произведением*) отображения φ^{-1} (рассматриваемого как первое) и отображения ψ (второго) и обозначается $\varphi^{-1}\psi$.

*) В формулах (2.6.4) элементы a_{ij} другие, нежели в (2.6.1), а именно: a_{1j}, a_{2j}, a_{3j} — это координаты точки A'_j , являющейся образом точки A_j° при отображении φ^{-1} . — *Прим. перев.*

Мы утверждаем, что *отображение* $\varphi^{-1}\psi$ *снова является линейным*.

В самом деле, рассмотрим линейное отображение

$$(2.6.6) \quad \begin{cases} \rho x_1'' = c_{11}x_1 + c_{12}x_2 + c_{13}x_3, \\ \rho x_2'' = c_{21}x_1 + c_{22}x_2 + c_{23}x_3, \\ \rho x_3'' = c_{31}x_1 + c_{32}x_2 + c_{33}x_3, \end{cases}$$

где коэффициенты суть

$$(2.6.7) \quad c_{jk} = b_{j1}a_{1k} + b_{j2}a_{2k} + b_{j3}a_{3k} \quad (j, k = 1, 2, 3).$$

Тогда непосредственным подсчетом, основываясь на (2.6.4) и (2.6.5), легко показать, что отображение $\varphi^{-1}\psi = \tau$ задается формулами (2.6.6).

Обозначим матрицы, отвечающие отображениям φ^{-1} , ψ и τ , соответственно A , B и C . Равенство $\varphi^{-1}\psi = \tau$ обусловлено тем, что $B \cdot A = C$. Так как для определителей имеет место равенство $B \cdot A = C$, то из $A \neq 0$, $B \neq 0$ следует $C \neq 0$.

Резюмируя, можно сказать, что *для любых двух собственных четырехугольников $A_1A_2A_3A_4$ и $B_1B_2B_3B_4$ на плоскости существует линейное отображение, которое переводит точки A_1, A_2, A_3, A_4 соответственно в точки B_1, B_2, B_3, B_4* .

Единственность линейного отображения, удовлетворяющего условиям $\tau(A_j) = B_j$ ($j = 1, 2, 3, 4$), можно доказать, например, следующим образом. Предположим, что указанным условиям удовлетворяют два различных линейных отображения τ_1 и τ_2 . Так как $\tau_1 \neq \tau_2$, то существует по крайней мере одна точка P такая, что $\tau_1(P) = P'$, $\tau_2(P) = P''$ и $P' \neq P''$. Разумеется, точка P отлична от каждой из точек A_j . Точно так же точка P должна быть отлична от точек $A_1A_2 \cap A_3A_4$, $A_2A_3 \cap A_1A_4$, $A_3A_1 \cap A_2A_4$, поскольку линейное отображение переводит точку пересечения снова в точку пересечения. Далее, точка P не может лежать ни на одной из прямых A_jA_k . Действительно, в противном случае, скажем, если P лежала бы на прямой A_3A_4 и $P \neq U = A_1A_2 \cap A_3A_4$, точки P' и P'' лежали бы на прямой B_3B_4 , причем каждая из них была бы отлична от $U^* = B_1B_2 \cap B_3B_4$. Поскольку линейное отображение сохраняет двойные отношения, мы должны были бы тогда иметь $(A_3A_4UP) = (B_3B_4U^*P')$

и $(A_3A_4UP) = (B_3B_4U^*P'')$. Вытекающее отсюда равенство $(B_3B_4U^*P'') = (B_3B_4U^*P')$ влечет за собой $P' = P''$, что противоречит сделанному допущению. Итак, P не может лежать ни на одной из прямых A_jA_k . Тем самым, P' и P'' не могут лежать ни на одной из прямых B_jB_k , или, что то же самое, прямая $P'P''$ может содержать не более одной из точек B_j . Значит, мы можем считать, что она не проходит, скажем, через B_1 . Итак, прямые l' и l'' , соединяющие B_1 с P' и P'' соответственно (т. е. образы прямой $A_1P = l$ при отображениях τ_1 и τ_2 соответственно), не совпадают. Кроме того, ни одна из них не совпадает ни с одной из прямых B_jB_k . Если мы введем обозначения $A_1A_k = l_{1k}$ и $B_1B_k = l'_{1k}$, то условие сохранения двойных отношений для τ_1 и τ_2 даст равенства

$$(l_{12}l_{13}l_{14}l) = (l'_{12}l'_{13}l'_{14}l')$$

и

$$(l_{12}l_{13}l_{14}l) = (l'_{12}l'_{13}l'_{14}l''),$$

из которых будет следовать $(l'_{12}l'_{13}l'_{14}l') = (l'_{12}l'_{13}l'_{14}l'')$, а значит, и $l' = l''$. Полученное противоречие завершает доказательство единственности τ .

2.7. Понятие овала на конечной плоскости

Мы снова будем изучать аналогии с классической геометрией, но теперь плоскости нечетного и четного порядков должны рассматриваться раздельно.

Эллипс на евклидовой плоскости есть частный случай замкнутой кривой, называемой *овалом*. Число точек пересечения овала с прямой есть 2, 1 или 0. Соответственно этому прямая называется *секущей*, *касательной* или *внешней прямой* относительно овала. Мы будем искать фигуры, обладающие этим свойством, на конечной плоскости (не обязательно плоскости Галуа). Прямая на конечной плоскости есть некоторое подмножество, состоящее из $q + 1$ точек; поэтому кажется естественным потребовать, чтобы и овал состоял из такого же числа точек.

Итак, будем понимать под *овалом* множество Ω из $q + 1$ точек на конечной плоскости порядка q , никакие три из которых не лежат на одной прямой. Прямую будем называть *секущей*, *касательной* или *внешней прямой* отно-

сительно овала, если число общих точек овала и прямой равно соответственно 2, 1 или 0.

Легко привести пример овала на плоскости Галуа.

Рассмотрим на $S_{2,q}$ множество Ω_0 точек, определяемое уравнением

$$(2.7.1) \quad x_1 x_2 - x_3^2 = 0.$$

Очевидно, точками Ω_0 являются $(1, 0, 0)$, а также q других точек, определяемых последовательностями $(\omega^2, 1, \omega)$, где ω пробегает все элементы координатного поля. Таким образом, Ω_0 содержит ровно $q + 1$ точек.

Мы должны еще проверить, что любые три (различные) точки множества Ω_0 линейно независимы, но это следует непосредственно из тождеств

$$\begin{vmatrix} 1 & 0 & 0 \\ \omega_1^2 & 1 & \omega_1 \\ \omega_2^2 & 1 & \omega_2 \end{vmatrix} = \omega_2 - \omega_1$$

и

$$\begin{vmatrix} \omega_1^2 & 1 & \omega_1 \\ \omega_2^2 & 1 & \omega_2 \\ \omega_3^2 & 1 & \omega_3 \end{vmatrix} = (\omega_1 - \omega_2)(\omega_2 - \omega_3)(\omega_3 - \omega_1).$$

Попытаемся выяснить, сколько секущих овала Ω_0 проходит через фундаментальную точку $(0, 0, 1)$. Если точки $(0, 0, 1)$, $(\omega_1^2, 1, \omega_1)$ и $(\omega_2^2, 1, \omega_2)$ коллинеарны, то, рассмотрев определитель, составленный из их координат, получим соотношение $\omega_1^2 - \omega_2^2 = 0$. Отсюда, ввиду $\omega_1 \neq \omega_2$, следует $\omega_2 = -\omega_1$. Если q четно, то $\omega_2 = -\omega_1 = \omega_1$, что исключается; в этом случае не существует секущих, проходящих через $(0, 0, 1)$. Но число всех прямых, проходящих через эту точку, есть $q + 1$; следовательно, каждая из них содержит одну и только одну точку из Ω_0 . Другими словами, любая прямая, проходящая через $(0, 0, 1)$, является касательной к овалу. Такое положение, конечно, невозможно для овалов классической геометрии. В случае, когда q нечетно, только фундаментальные прямые $[1, 0, 0]$ и $[0, 1, 0]$ являются касательными, проходящими через $(0, 0, 1)$; эти прямые проходят через $(0, 1, 0)$ и $(1, 0, 0)$ соответственно. Через фунда-

ментальную точку $(0, 0, 1)$ здесь проходит столько секущих, сколько существует неупорядоченных пар, состоящих из элемента и противоположного ему (по сложению), исключая $(0, 0)$; это значит, что существует $(q - 1)/2$ секущих, проходящих через $(0, 0, 1)$. Остальные $(q - 1)/2$ прямых, проходящих через $(0, 0, 1)$, являются, очевидно, внешними прямыми. Таким образом, в случае нечетного q фундаментальная точка $(0, 0, 1)$ ведет себя подобно внешним точкам овала в классической геометрии: через нее проходят две касательные к овалу, а также прямые, пересекающие овал, и прямые, не имеющие с овалом общих точек.

$q + 1$ точек овала Ω_0 на плоскости Галуа четного порядка определяют попарно $(q + 1)q/2$ секущих; при этом через каждую из точек овала проходит q секущих. Прямая, соединяющая точку овала с фундаментальной точкой $(0, 0, 1)$, является касательной, и эта касательная вместе с q секущими, проходящими через данную точку овала, исчерпывает все прямые плоскости, инцидентные с данной точкой. Укажем еще раз, что все касательные овала Ω_0 проходят через фундаментальную точку O $(0, 0, 1)$. Эта особая точка по отношению к овалу — не лежащая, однако, на нем — называется *ядром* овала. Точки овала вместе с его ядром образуют множество из $q + 2$ точек такое, что на каждой прямой лежит не более двух из них. Любое такое множество называется *гиперовалом*. Далее мы увидим, что гиперовалы существуют только на плоскостях четного порядка.

В последующей части параграфа плоскость порядка q не обязательно означает плоскость Галуа порядка q . Вопросы, которые мы будем здесь обсуждать, требуют для своего решения лишь совершенно элементарных комбинаторных соображений.

1° Рассмотрим сначала овалы в плоскостях нечетного порядка. Овал Ω плоскости состоит из $q + 1$, т. е. из четного числа точек. Обозначим их A_0, A_1, \dots, A_q . Из определения овала следует, что если мы соединим точку A_k поочередно с каждой из остальных точек, то получим q различных прямых, а $(q + 1)$ -я прямая, проходящая через A_k , является касательной. Таким образом, через каждую точку овала проходит касательная, имеющая эту точку своей *точкой касания*.

Возьмем произвольную точку овала Ω , скажем точку A_0 , и рассмотрим касательную a_0 к овалу в этой точке. Пусть остальные точки касательной будут P_1, P_2, \dots, P_q . Каждая из остальных q касательных к Ω должна проходить через одну из точек P_1, \dots, P_q , так как в противном случае нашлась бы точка P_i , через которую проходила бы только одна касательная a_0 , а все остальные прямые, проходящие через P_i , были бы секущими или внешними прямыми. Однако это невозможно, так как точки A_1, \dots, A_q лежали бы тогда на секущих, проходящих через P_i , и число q было бы четным. Таким образом, через каждую точку касательной, отличную от точки касания, проходят две *) касательные; такие точки называются *внешними точками* относительно овала. Из наших рассуждений следует, что *число внешних точек равно $(q + 1)q/2$* . Если из всей плоскости, насчитывающей $q^2 + q + 1$ точек, удалить $q + 1$ точек самого овала и $(q + 1)q/2$ внешних точек, то останутся $(q - 1)q/2$ точек, ни одна из которых не лежит на касательной. Такие точки называются *внутренними точками* относительно овала.

Итак, подобно прямым, точки плоскости также разделяются на три класса по отношению к овалу: внешние точки, точки овала и внутренние точки. Можно было бы считать, что такое разделение на классы аналогично ситуации, имеющей место в классической плоскости. Однако в случае конечной плоскости порядка q *любая внешняя прямая состоит из $(q + 1)/2$ внешних точек и такого же числа внутренних точек*.

Это утверждение вытекает из того факта, что каждая касательная пересекает внешнюю прямую во внешней точке, причем через эту точку проходят ровно две касательные.

Из подобного же рассуждения следует, что каждая секущая содержит $(q - 1)/2$ внешних точек и столько же внутренних.

2° Рассмотрим теперь овалы в плоскостях *четного* порядка. Число точек овала, равное $q + 1$, теперь нечетно. Через каждую точку овала, как уже говорилось, прохо-

*) К такому же противоречию, как выше, приводит и допущение, что через точку, лежащую на касательной, проходит более двух касательных. — *Прим. перев.*

дит одна касательная; все остальные прямые, проходящие через точку овала, являются секущими.

Рассмотрим секущую l , соединяющую точки A_j и A_k овала. Через каждую из остальных $q - 1$ точек прямой l проходит касательная к овалу. В самом деле, если бы прямая l содержала точку P , через которую не проходит касательная, то, соединяя P с каждой из указанных $q - 1$ точек овала, мы получили бы секущие, что невозможно, так как $q - 1$ — нечетное число. Так как число касательных в точности равно числу точек прямой l , то *через каждую точку из l проходит теперь ровно одна касательная*.

Пусть M будет точка пересечения двух касательных к овалу, скажем a_0 и a_1 . Соединим M с каждой из точек овала. Ни одна из прямых, полученных таким образом, не является секущей, так как в противном случае через одну и ту же точку секущей, а именно через M , проходили бы две касательные (a_0 и a_1), что, по доказанному, невозможно. Следовательно, каждая прямая, проходящая через M , должна быть касательной к овалу. Точка M называется *ядром* овала. Множество из $q + 2$ точек, составленное из овала и его ядра, называется *гиперовалом*.

3° Множество, состоящее из k точек конечной плоскости, не более чем две из которых коллинеарны, будем называть *k-дугой*. Если k -дуга не содержится ни в какой $(k + 1)$ -дуге, то она называется *полной*. Овал в плоскости четного порядка является неполной $(q + 1)$ -дугой, так как он содержится в гиперовале, являющемся $(q + 2)$ -дугой.

Теорема Бозе *). *Если в конечной плоскости порядка q существует k -дуга, то $k \leq q + 2$ в случае четного q и $k \leq q + 1$ в случае нечетного q **).*

Эта теорема легко следует из 1° и 2°. Допустим, что q четно. Пусть A_0 будет произвольная точка k -дуги. Соединяя A_0 с остальными точками k -дуги, получим $k - 1$ различных прямых, но полное число прямых, проходя-

*) Начиная примерно с 1940 года появилось много работ, посвященных k -дугам, особенно в плоскостях Галуа. Одна из причин этого заключалась в том, что полученные результаты часто представляли ценность для других областей, например, для математической статистики.

**) Таким образом, в случае нечетного q овал, а в случае четного q гиперовал являются полными дугами. — *Прим. перев.*

щих через A_0 , есть $q + 1$; отсюда $k - 1 \leq q + 1$, т. е. $k \leq q + 2$.

Допустим теперь, что q нечетно и существует k -дуга, для которой $k > q + 1$. Взяв какие-либо $q + 1$ точек k -дуги, получим овал Ω . Пусть A_0 будет точка k -дуги, не принадлежащая овалу Ω . Соединим A_0 с точками из Ω , тогда получим $q + 1$ различных прямых, являющихся секущими k -дуги, но касательными к овалу Ω . Отсюда следует $q + 1 \leq 2$, но для конечной плоскости $q + 1 \geq 3$. Полученное противоречие доказывает второе утверждение теоремы.

2.8. Коник в плоскости Галуа

Начиная с данного момента мы вводим понятие коники как точечного множества Ω_0 , определенного уравнением (2.7.1), и приступаем к изучению свойств этого множества, которые аналогичны свойствам коник в классической проективной плоскости.

Полином второй степени, фигурирующий в (2.7.1), неприводим над любым конечным полем. Однако нам придется встречаться и с полиномами, которые приводимы над некоторыми конечными полями.

Указанные ниже примеры можно рассматривать при любом координатном поле $GF(q)$.

1° Уравнение $x_1 x_2 = 0$ определяет множество, состоящее из $2q + 1$ точек; это множество есть объединение всех точек прямых $x_1 = 0$ и $x_2 = 0$. Очевидно, оно не является овалом.

2° Уравнение $x_1^2 - x_2^2 = 0$ определяет множество, являющееся объединением точек прямых $x_1 - x_2 = 0$ и $x_1 + x_2 = 0$; это множество тоже не является овалом.

Следующий пример относится к случаю, когда координатное поле имеет характеристику 2.

3° Уравнения $x_1^2 + x_2^2 + x_3^2 = 0$ и $x_1 + x_2 + x_3 = 0$ определяют одно и то же множество точек. Это множество состоит из $q + 1$ точек прямой и, следовательно, не является овалом.

Следующие два примера также относятся к координатному полю $GF(2^r)$, но первый из них мы рассмотрим для случая $r = 2$, а второй — для случая $r = 3$. Приве-

дем таблицы операций для $GF(8)$ в том виде, как они будут использоваться дальше (рис. 51).

В случае координатного поля $GF(2^r)$ множество точек, определяемое уравнением $x_1^2 + x_1x_2 + x_2^2 = 0$, содержит фундаментальную точку $(0, 0, 1)$; для любой другой точки из этого множества обе координаты x_1 и x_2 не равны нулю.

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3	3	2	1	0	7	6	5	4
4	4	5	6	7	0	1	2	3
5	5	4	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1
7	7	6	5	4	3	2	1	0

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	3	1	7	5
3	0	3	6	5	7	4	1	2
4	0	4	3	7	6	2	5	1
5	0	5	1	4	2	7	3	6
6	0	6	7	1	5	3	2	4
7	0	7	5	2	1	6	4	3

Рис. 51.

Предположим, что $x_2 \neq 0$, тогда замена $x_1x_2^{-1} = z$ приводит к уравнению $z^2 + z + 1 = 0$. Из условия $q = 2^r$ следует $-1 = 1$, так что наше уравнение может быть записано в виде $z(z + 1) = 1$.

4° Рассмотрим решения уравнения над $GF(8)$. Из таблиц операций непосредственно видно, что при $z = 0, 2, 3, 4, 5, 6, 7$ произведение $z(z + 1)$ поочередно равно 0, 6, 6, 2, 2, 4, 4. Таким образом, уравнение $z(z + 1) = 1$ не имеет решений над $GF(8)$, и множество точек, определенное уравнением $x_1^2 + x_1x_2 + x_2^2 = 0$, состоит из единственной точки, а именно $(0, 0, 1)$.

5° Рассмотрим теперь решения уравнения $z(z + 1) = 1$ над $GF(4)$. Таблицы операций были даны в 1.6. Теперь при $z = 0, 1, 2, 3$ произведение $z(z + 1)$ есть соответственно 0, 0, 1, 1. Таким образом, $z = 2$ и $z = 3$ являются решениями, и мы видим, что уравнение $x_1^2 + x_1x_2 + x_2^2 = 0$ эквивалентно $(x_1 + 2x_2)(x_1 + 3x_2) = 0$. Следовательно, искомое множество есть объединение точек двух прямых, т. е. снова не овал.

После проведенного нами разбора примеров естественно возникает вопрос: какому условию должны удов-

летворять коэффициенты уравнения второй степени, чтобы определенное этим уравнением множество точек было овалом? Можно поставить и следующий вопрос: всегда ли для данного овала, определенного уравнением второй степени, существует такая система координат, в которой уравнение овала принимает вид $x_1x_2 - x_3^2 = 0$? Ответы на эти вопросы будут даны позже. Сейчас мы ограничимся только изучением геометрических свойств специального овала Ω_0 , определенного уравнением (2.7.1). Вообще говоря, мы будем рассматривать произвольное координатное поле $GF(q) = K$, но в частных случаях будем специализировать значения q . При необходимости будем обращаться к рис. 52.

Рассмотрим множество, состоящее из $q^2 - 1$ пар $(\lambda, \mu) \neq (0, 0)$, где $\lambda, \mu \in K$. Разобьем это множество на классы, приняв (λ, μ) и (λ', μ') принадлежащими одному классу в том и только в том случае, когда существует отличное от нуля $\rho \in K$ такое, что $\rho\lambda = \lambda'$, $\rho\mu = \mu'$. Очевидно, мы получим таким путем $(q^2 - 1)/(q - 1) = q + 1$ классов, т. е. столько, сколько точек содержит овал Ω_0 . Легко видеть, что соответствие между классами и точками множества Ω_0 , заданное формулами

$$(2.8.1) \quad x_1 = \lambda^2, \quad x_2 = \mu^2, \quad x_3 = \lambda\mu,$$

будет взаимно однозначным. Таким образом, задавая точку $(\lambda^2, \mu^2, \lambda\mu)$ парой (λ, μ) , мы параметризуем Ω_0 . Эта параметризация сильно упростит наши рассуждения.

Теперь мы можем вывести важные геометрические свойства овала Ω_0 .

Точки

$$(2.8.2) \quad A_1(1, 0, 0), \quad A_2(0, 1, 0) \quad \text{и} \quad E(1, 1, 1)$$

из Ω_0 параметризуются парами $(1, 0)$, $(0, 1)$ и $(1, 1)$ соответственно. Пусть P будет точка из Ω_0 , отличная от A_1 , A_2 и E , параметризованная парой (λ, μ) . Будем говорить, что прямая, соединяющая произвольную точку из Ω_0 с A_1 , *проектирует* эту точку из A_1 ; касательную к Ω_0 в точке A_1 будем считать проектирующей A_1 из этой же точки. Далее, будем обозначать $A_1(A_1A_2EP)$ двойное отношение прямых, проектирующих A_1, A_2, E, P из точки A_1 . Аналогично, $A_2(A_1A_2EP)$ будет обозначать двойное отноше-

ние прямых, проектирующих те же четыре точки из A_2 . Согласно теореме Паппа (рис. 52) имеем

$$A_1 (A_1 A_2 EP) = (a_2 a_3 e_1 p_1) = (A_3 A_2 E_1 P_1) = x_3 x_2^{-1}$$

и

$$A_2 (A_1 A_2 EP) = (a_3 a_1 e_2 p_2) = (A_1 A_3 E_2 P_2) = x_1 x_3^{-1},$$

где

$$(x_1, x_2, x_3) = (\lambda^2, \mu^2, \lambda\mu);$$

следовательно,

$$x_3 x_2^{-1} = x_1 x_3^{-1} = \lambda\mu^{-1} = \theta$$

и, тем самым,

$$(2.8.3) \quad A_1 (A_1 A_2 EP) = A_2 (A_1 A_2 EP) = \theta.$$

Если P пробегает множество $\Omega_0 \setminus A_1$, то P_1 пробегает $a_1 \setminus A_3$, следовательно, $(A_3 A_2 E_1 P_1) = \lambda\mu^{-1} = \theta$ пробегает элементы поля K . Значения $\theta = 0$ и $\theta = 1$ отвечают положениям $P = A_2$ и $P = E$ соответственно.

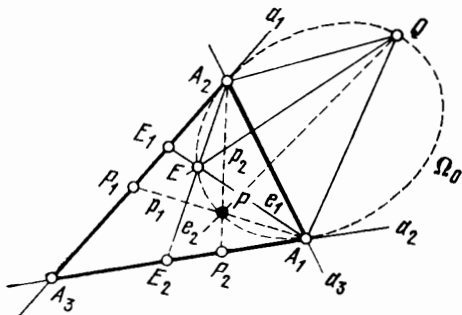


Рис. 52.

Обратно, каждому значению θ соответствуют точка P_2 из $a_2 \setminus A_3$ и точка P_1 из $a_1 \setminus A_3$. Таким образом, каждое значение θ определяет одну точку $A_2 P_2 \cap A_1 P_1 = P$ на Ω_0 .

Итак, мы доказали следующую лемму.

Если установить соответствие между прямыми, проектирующими точки A_1, A_2, E, P овала Ω_0 из точки A_1 ,

и прямыми, проектирующими те же точки из A_2 , то будет выполняться равенство (2.8.3). С помощью неединственного параметра θ устанавливается взаимно однозначное соответствие между точками множества $\Omega_0 \setminus A_1$ и элементами координатного поля K .

Пусть $Q(\xi^2, \eta^2, \xi\eta)$ — точка овала, отличная от $P(\lambda^2, \mu^2, \lambda\mu)$. Координаты точки $A_1A_3 \cap QP = P_3^*$, как легко видеть, будут

$$(2.8.4) \quad (\lambda\eta + \mu\xi, 0, \mu\eta).$$

Ясно, что точку P_3^* можно рассматривать как проекцию P на прямую $A_1A_3 = a_2$ из точки Q . Заменяя P по очереди на A_1, A_2, E , получим точки

$$A_1^* = A_1(1, 0, 0), \quad A_2^*(\xi, 0, \eta), \quad E^*(\xi + \eta, 0, \eta);$$

следовательно,

$$E_3^* = \eta A_1^* + A_2^*, \quad P_3^* = \lambda\eta A_1^* + \mu A_2^*$$

и

$$(2.8.5) \quad (A_1^* A_2^* E_3^* P_3^*) = \eta^{-1} \cdot 1 \cdot \lambda\eta \cdot \mu^{-1} = \lambda\mu^{-1} = (A_1 A_2 E_3 P_3).$$

Применяя теорему Паппа к проектирующим четверкам прямых, получаем теперь следующую лемму.

Все четверки прямых, проектирующие четыре фиксированные точки A_1, A_2, E, P овала Ω_0 из любой другой точки овала, имеют одно и то же двойное отношение.

Можно, таким образом, говорить о двойном отношении этой четверки точек.

С помощью доказанной леммы и теоремы Паппа можно распространить понятие двойного отношения на любую четверку точек овала. Для этой цели следует воспользоваться еще одной леммой, которая устанавливает проективный характер соответствия между двумя пучками при некоторых условиях.

Тривиальный случай $q = 2$ и малоинтересный случай $q = 3$ исключим из дальнейшего рассмотрения. Пусть U и V будут две различные точки плоскости, a, b и c — три различные прямые, проходящие через V , a', b' и c' — три различные прямые, проходящие через U (рис. 53). Обозначим A, B и C точки пересечения прямых a, b и c с прямой a' ; аналогично, пусть A', B' и C' будут точки

пересечения прямых a' , b' и c' с a . Очевидно, $A = A'$. Положим $A^* = A$, $B^* = CB' \cap C'B$ и $C^* = A^*B^* \cap CC'$; прямую A^*B^* обозначим l . Пусть x и x' будут какие-то две прямые, проходящие через U и V соответственно и удовлетворяющие условию

$$(2.8.6) \quad (abcx) = (a'b'c'x');$$

пусть также

$$X = x \cap a', \quad X' = x' \cap a'.$$

Прямая $C'X$ пересекает l в некоторой точке X_1 , а CX'

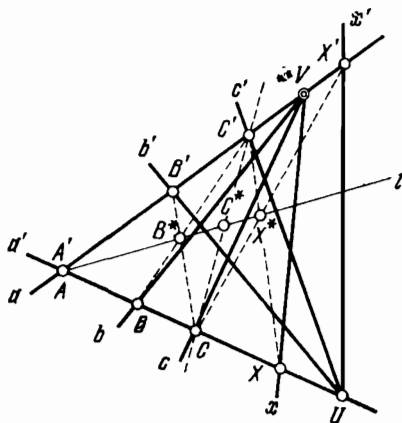


Рис. 53.

пересекает l в точке X_2 . Из теоремы Паша следует, что

$$\begin{aligned} (abcx) &= (ABCX) = \\ &= C' (ABCX) = \\ &= (A^*B^*C^*X_1). \end{aligned}$$

Аналогично,

$$(a'b'c'x') = (A^*B^*C^*X_2),$$

поэтому из (2.8.6) находим

$$(A^*B^*C^*X_1) = (A^*B^*C^*X_2).$$

Отсюда имеем $X_1 = X_2$, т. е. прямые $C'X$ и CX' пересекаются в точке, лежащей на l .

При любом выборе прямой x среди множества $q - 2$ прямых, отличных от a, b, c и проходящих через V , мы получаем, в силу (2.8.6), соответствующую прямую x' , проходящую через U и отличную от a', b', c' . Легко видеть, что таким путем мы приходим к взаимно однозначному соответствию

$$(2.8.7) \quad \varphi: \begin{pmatrix} a & b & c & x & \dots \\ \downarrow & \downarrow & \downarrow & \downarrow & \\ a' & b' & c' & x' & \dots \end{pmatrix}.$$

Более того, мы показали, что при любом выборе x определенные выше прямые $C'X$ и CX' пересекаются на прямой l . Отсюда ясно, что для каждой четырех прямых x_1, x_2, x_3, x_4 , проходящих через V , и соответствующих им (посредством φ) прямых x'_1, x'_2, x'_3, x'_4 мы должны иметь равенство

$$(x_1 x_2 x_3 x_4) = (x'_1 x'_2 x'_3 x'_4).$$

Наши рассуждения подытоживает следующая (третья) лемма.

Соответствие φ взаимно однозначно и сохраняет двойное отношение; другими словами, φ является проективным соответствием.

Нижеследующая теорема непосредственно вытекает из наших трех лемм. Она аналогична теореме Штейнера, относящейся к хорошо известному свойству коник на классической проективной плоскости.

Соответствие между двумя пучками, составленными из прямых, проектирующих точки овала Ω_0 из двух фиксированных точек того же овала, является проективным, если соответствующие прямые пучков проектируют одну и ту же точку овала.

Близость между свойствами множества Ω_0 на плоскости Галуа и свойствами коники на классической проективной плоскости служит оправданием тому, что мы называем это множество коникой. С этого момента множество Ω_0 и только оно будет называться коникой на плоскости Галуа.

2.9. Точечные конфигурации порядка 2 на плоскости Галуа четного порядка

На протяжении этого параграфа координатное поле K будет предполагаться полем характеристики 2.

Рассмотрим наиболее общий вид уравнения второй степени с коэффициентами из K :

$$(2.9.1) \quad f(x) = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + b_1x_2x_3 + b_2x_3x_1 + b_3x_1x_2 = 0.$$

Мы будем искать критерий неприводимости уравнения второй степени над K .

Если $b_1 = b_2 = b_3 = 0$, то уравнение (2.9.1) может быть записано в виде

$$f(x) = 0: c_1^2x_1^2 + c_2^2x_2^2 + c_3^2x_3^2 = (c_1x_1 + c_2x_2 + c_3x_3)^2 = 0^*),$$

где $c_i^2 = a_i$ ($i = 1, 2, 3$).

Пусть $(b) = (b_1, b_2, b_3) \neq (0, 0, 0)$. Предположим, что $f(x)$ можно разложить на два неэквивалентных линейных множителя, т. е. $f(x) = \alpha(x)\beta(x)$, где

$$\alpha(x) \equiv \alpha_1x_1 + \alpha_2x_2 + \alpha_3x_3$$

и /

$$\beta(x) \equiv \beta_1x_1 + \beta_2x_2 + \beta_3x_3.$$

Тогда данное уравнение запишется в виде

$$\alpha_1\beta_1x_1^2 + \alpha_2\beta_2x_2^2 + \alpha_3\beta_3x_3^2 + (\alpha_2\beta_3 + \alpha_3\beta_2)x_2x_3 + (\alpha_3\beta_1 + \alpha_1\beta_3)x_3x_1 + (\alpha_1\beta_2 + \alpha_2\beta_1)x_1x_2 = 0.$$

Рассмотрим систему уравнений

$$\begin{cases} \alpha_1x_1 + \alpha_2x_2 + \alpha_3x_3 = 0, \\ \beta_1x_1 + \beta_2x_2 + \beta_3x_3 = 0. \end{cases}$$

Одно из решений этой системы будет

$$\rho x_1 = \alpha_2\beta_3 - \alpha_3\beta_2, \quad \rho x_2 = \alpha_3\beta_1 - \alpha_1\beta_3, \quad \rho x_3 = \alpha_1\beta_2 - \alpha_2\beta_1.$$

*) В поле $K = GF(2^r)$ имеем $ab + ba = 0$, следовательно, $(a + b)^2 = a^2 + ab + ba + b^2 = a^2 + b^2$; повторное применение этого равенства дает $(a + b + c)^2 = a^2 + b^2 + c^2$.

Так как координатное поле имеет характеристику 2, то можем записать это решение по-другому:

$$\rho x_1 = \alpha_2 \beta_3 + \alpha_3 \beta_2, \rho x_2 = \alpha_3 \beta_1 + \alpha_1 \beta_3, \rho x_3 = \alpha_1 \beta_2 + \alpha_2 \beta_1,$$

т. е.

$$\rho x_1 = b_1, \quad \rho x_2 = b_2, \quad \rho x_3 = b_3.$$

Мы установили следующий факт.

Если квадратичная форма $f(x)$ разлагается в произведение двух линейных множителей, то $f(b) = 0$. (1)

Покажем теперь, что если каждая точка плоскости удовлетворяет уравнению $f(x) = 0$, то все коэффициенты уравнения равны нулю. (2)

Действительно, подставляя в уравнение координаты фундаментальных точек $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$, получим $a_1 = 0$, $a_2 = 0$, $a_3 = 0$. Следовательно,

$$f(x) = 0: b_1 x_2 x_3 + b_2 x_3 x_1 + b_3 x_1 x_2 = 0,$$

и так как этому уравнению удовлетворяют также точки $(0, 1, 1)$, $(1, 0, 1)$, $(1, 1, 0)$, то $b_1 = 0$, $b_2 = 0$, $b_3 = 0$. Утверждение (2) доказано.

* * *

Пусть $X(x_1, x_2, x_3)$ и $Y(y_1, y_2, y_3)$ — две точки плоскости. Допустим, что точка $Z(\lambda x_1 + \mu y_1, \lambda x_2 + \mu y_2, \lambda x_3 + \mu y_3) = (z_1, z_2, z_3)$ прямой XY удовлетворяет рассматриваемому уравнению, т. е. $f(z) = 0$. Это можно записать более подробно следующим образом:

$$(2.9.2) \quad f(x) \cdot \lambda^2 + \varphi(x, y) \cdot \lambda \mu + f(y) \cdot \mu^2 = 0,$$

где (в случае характеристики 2)

$$(2.9.3) \quad \varphi(x, y) = (b_3 x_2 + b_2 x_3) y_1 + \\ + (b_3 x_1 + b_1 x_3) y_2 + (b_2 x_1 + b_1 x_2) y_3.$$

Непосредственно ясно, что $\varphi(x, y) = \varphi(y, x)$.

Мы можем теперь определить некое симметричное отношение между X и Y . А именно, мы скажем, что две точки сопряжены (относительно множества точек, заданного уравнением $f = 0$), если $\varphi(x, y) = 0$.

Предположим, что две сопряженные относительно множества $f = 0$ точки X и Y существуют и что ни одна из них не принадлежит этому множеству, т. е. что $f(x) = \alpha \neq 0$, $f(y) = \gamma \neq 0$ и $\varphi(x, y) = 0$.

Очевидно, точка $Z = \lambda X + \mu Y$, $\lambda, \mu \neq 0$, будет принадлежать указанному множеству в том и только в том случае, когда

$$\alpha\lambda^2 + \gamma\mu^2 = 0.$$

Пусть это равенство имеет место; тогда уравнение $\sigma^2 = -\frac{\alpha}{\gamma}$ будет эквивалентно $\sigma^2 = \left(\frac{\lambda}{\mu}\right)^2$ и, значит, будет иметь единственное решение σ в поле характеристики 2. Таким образом, мы можем сказать, что *прямая, содержащая сопряженные точки X и Y , не принадлежащие фигуре $f = 0$, имеет с этой фигурой единственную общую точку Z ; иначе говоря, прямая XY есть касательная к фигуре, а Z есть точка касания.* (3)

Рассмотрим теперь точку $B(b_1, b_2, b_3)$. Очевидно, при $(x_1, x_2, x_3) = (b_1, b_2, b_3)$ все коэффициенты в (2.9.3) обращаются в нуль, поэтому

$$(2.9.4) \quad \varphi(b, y) = 0.$$

Итак, *любая точка плоскости сопряжена точке B .* (4)

Далее, полагая в (2.9.3) $(x_1, x_2, x_3) = (y_1, y_2, y_3)$, получим $\varphi(x, y) = 0$. Следовательно, *любая точка плоскости сопряжена себе самой.* (5)

Предположим, что $f(b) = \alpha \neq 0$, так что полином $f(x)$ неприводим. Используя тот факт, что B сопряжена любой точке плоскости, можно легко найти число точек фигуры, определенной уравнением $f(x) = 0$. Если Y — какая-либо точка плоскости, то, согласно (3), прямая BY содержит только одну точку Z указанной фигуры, т. е. она касается фигуры в точке Z . Число прямых, проходящих через B , есть $q + 1$, следовательно, фигура содержит ровно $q + 1$ точек. Точка B называется *ядром* фигуры. Таким образом, можно сказать, что *фигура, имеющая ядро, состоит из $q + 1$ точек.* (6)

Допустим теперь, что B принадлежит фигуре. В этом случае, если точка Y , $(y) \neq (b)$, принадлежит фигуре, то и *каждая точка прямой BY принадлежит фигуре.* (7) Ибо, если $f(b) = f(y) = \varphi(b, y) = 0$, то (2.9.2) выполняется при любом выборе пары (λ, μ) .

Пусть $X, Y, Z = \lambda X + \mu Y$ — три различные точки фигуры, принадлежащие одной прямой. Тогда $f(x) = f(y) = 0$ и $f(z) = \varphi(x, y) \cdot \lambda\mu = 0$, откуда следует, ввиду условия $\lambda\mu \neq 0$, что $\varphi(x, y) = 0$. Это, однако, означает, что любая точка прямой XY принадлежит фигуре. Можно, следовательно, сказать, что *если три точки прямой принадлежат фигуре, то любая точка этой прямой также принадлежит фигуре*. (8)

Если точки B и $Y (\neq B)$ принадлежат фигуре, то, согласно (7), каждая точка прямой BY принадлежит фигуре. Если при этом фигура содержит точку Y^* , не лежащую на прямой BY , то она содержит и все точки прямой BY^* . В этом случае из (8) следует, что никаких других точек фигура не имеет. Действительно, если бы точка Y_0 фигуры не принадлежала ни одной из прямых BY и BY^* , то, рассмотрев какую-нибудь прямую l , проходящую через Y_0 , и обозначив через Y_l и Y_l^* ее точки пересечения с BY и BY^* соответственно, мы получили бы, что три точки Y_0, Y_l, Y_l^* , лежащие на прямой l , принадлежат фигуре. Но тогда, согласно (8), все точки прямой l принадлежали бы фигуре. Так как при этом l есть любая прямая, проходящая через Y_0 , то получается, что все точки плоскости принадлежат фигуре. Согласно (2) это означало бы, что все коэффициенты в $f(x)$ равны нулю, что по предположению исключается. Таким образом, можно заключить, что *если $f(b) = 0$, то фигура не является овалом*. (9)

Суммируя сказанное выше, приходим к следующей теореме.

Т е о р е м а. *Множество точек, отвечающее уравнению второй степени $f(x) = 0$, является овалом тогда и только тогда, когда $f(b) \neq 0$.*

Любой овал, получаемый таким путем, т. е. определяемый уравнением второй степени, называется *кривой второго порядка* и обозначается дальше \mathcal{C}^*).

Известно, что на плоскости Галуа порядка 2^r , $r > 2$, существует овал, не являющийся кривой второго порядка. Мы не будем на этом останавливаться.

*) Здесь мы отклоняемся от общепринятой терминологии. Обычно каждая точечная фигура, отвечающая уравнению второго порядка, называется кривой второго порядка,

По аналогии с классической проективной плоскостью можно ввести *поляритет*, определяемый кривой второго порядка. Множество точек Y , сопряженных данной точке X относительно кривой \mathcal{C} второго порядка, называется *полярной точки X* . Из уравнения (2.9.3) видно, что точка $Y(u_1, u_2, u_3)$ лежит на поляре точки X тогда и только тогда, когда она удовлетворяет уравнению

$$(2.9.5) \quad u_1 y_1 + u_2 y_2 + u_3 y_3 = 0,$$

где

$$(2.9.6) \quad \begin{cases} \rho u_1 = 0 + b_3 x_2 + b_2 x_3, \\ \rho u_2 = b_3 x_1 + 0 + b_1 x_3, \\ \rho u_3 = b_2 x_1 + b_1 x_2 + 0. \end{cases}$$

Так как точка X сопряжена самой себе, а также точке B , то поляра X есть, очевидно, прямая BX . Следовательно, для точек любой прямой, проходящей через B , полярной служит эта же самая прямая. Поляра ядра B есть вся плоскость, ибо, полагая $(x_1, x_2, x_3) = (b_1, b_2, b_3)$ в (2.9.6), получаем $[u_1, u_2, u_3] = [0, 0, 0]$.

Итак, справедлива следующая

Т е о р е м а. Если B есть ядро кривой второго порядка \mathcal{C} , то множество поляр идентично множеству прямых, проходящих через B , т. е. множеству касательных к кривой.

Эта теорема показывает, что отношение полярности на плоскости четного порядка совершенно не похоже на соответствующее отношение для классической проективной плоскости.

В заключение поставим вопрос: какие взаимоотношения существуют между произвольной кривой \mathcal{C} второго порядка и специальным овалом Ω_0 ? Этот вопрос будет обсуждаться в следующем параграфе.

2.10. Каноническое уравнение кривой второго порядка на плоскости Галуа четного порядка

Мы будем по-прежнему считать, что характеристика поля K равна 2.

Рассмотрим невырожденное линейное отображение

$$\varphi: \begin{cases} \sigma x_1 = c_{11}y_1 + c_{12}y_2 + c_{13}y_3, \\ \sigma x_2 = c_{21}y_1 + c_{22}y_2 + c_{23}y_3, \\ \sigma x_3 = c_{31}y_1 + c_{32}y_2 + c_{33}y_3, \end{cases}$$

матрицу которого будем обозначать C . Если мы выберем треугольник отнесения для системы координат (y_1, y_2, y_3) , как в (2.4.3), а именно $A_1^\circ = (1, 0, 0)$, $A_2^\circ = (0, 1, 0)$ и $A_3^\circ = (0, 0, 1)$, то образ A_i^* точки A_i° будет иметь координаты $(c_{1i}, c_{2i}, c_{3i}) = (c_i)$ ($i = 1, 2, 3$). Образом стороны a_i треугольника отнесения будет являться прямая

$$C_{1i}x_1 + C_{2i}x_2 + C_{3i}x_3 = 0 \quad (i = 1, 2, 3),$$

где C_{jk} обозначает алгебраическое дополнение элемента c_{jk} в матрице C ($j = 1, 2, 3; k = 1, 2, 3$).

Пусть снова $f(x)$ есть квадратичная форма, фигурирующая в (2.9.1), и пусть $C_{1i}b_1 + C_{2i}b_2 + C_{3i}b_3 = c_i$ ($i = 1, 2, 3$). После несложных вычислений находим, что φ преобразует $f(x)$ в квадратичную форму $g(y)$, где

$$(2.10.1) \quad g(y) \equiv f(c_1) \cdot y_1^2 + f(c_2) \cdot y_2^2 + f(c_3) \cdot y_3^2 + \\ + C_1 \cdot y_2 y_3 + C_2 \cdot y_3 y_1 + C_3 \cdot y_1 y_2.$$

Выберем теперь коэффициенты в φ так, чтобы A_2^* и A_3^* принадлежали кривой \mathcal{C} , определяемой уравнением $f(x) = 0$, и чтобы $A_1^* = B$ было ядром кривой. Тогда $f(c_1) = f(b) \neq 0$ и $f(c_2) = f(c_3) = 0$, а также $C_1 \neq 0$, $C_2 = C_3 = 0$, поскольку $B (= A_1^*)$ лежит на прямых $A_1^* A_2^*$ и $A_1^* A_3^*$ ($A_1^* A_2^*$ и $A_1^* A_3^*$ касаются кривой в точках A_2^* , A_3^* соответственно и проходят через ядро).

Итак, уравнение $g(y) = 0$ приводится к виду

$$(2.10.2) \quad g(y) \equiv f(c_1) \cdot y_1^2 + C_1 \cdot y_2 y_3 = 0.$$

Пусть α обозначает такой элемент поля K , что $\alpha^2 = \frac{1}{f(c_1)}$, и пусть β и γ — такие два элемента K , что $\beta\gamma = \frac{1}{C_1}$.

Рассмотрим невырожденное линейное отображение

$$\psi: \begin{cases} \rho y_1 = \alpha z_3, \\ \rho y_2 = \beta z_2, \\ \rho y_3 = \gamma z_1. \end{cases}$$

Это отображение переводит (2.10.2) в уравнение $z_1 z_2 + z_3^2 = 0$, которое в случае поля K характеристики 2 совпадает с уравнением

$$(2.10.3) \quad z_1 z_2 - z_3^2 = 0.$$

Эффект отображения $\varphi\psi = \omega$ эквивалентен такому выбору системы координат, при котором точки отнесения A_2° , A_3° и единичная точка E° лежат на \mathcal{C} , а точка отнесения A_1° есть ядро \mathcal{C} . Иначе говоря, взаимоотношения новой системы координат с \mathcal{C} такие же, как взаимоотношения старой системы координат с Ω_0 . Мы скажем, что уравнение кривой \mathcal{C} приведено к канонической форме (2.10.3). Таким образом, справедлива следующая

Т е о р е м а. Любые две кривые второго порядка на плоскости Галуа четного порядка эквивалентны (относительно линейного отображения *).

Ссылаясь на эту теорему, мы можем при выяснении свойств кривых второго порядка ограничиться кривой $\mathcal{C}_0: x_1x_2 - x_3^2 = 0$. Докажем, например, аналог следующей теоремы классической проективной геометрии: *поляра одной из диагональных точек четырехугольника, вписанного в конику, есть прямая, соединяющая две другие диагональные точки.* Рассмотрим кривую

$$\mathcal{C}_0: x_1x_2 - x_3^2 = 0$$

и на ней — четыре точки:

$$\begin{aligned} Q_1 (\lambda_1^2, \mu_1^2, \lambda_1\mu_1), \quad Q_2 (\lambda_2^2, \mu_2^2, \lambda_2\mu_2), \\ Q_3 (\lambda_3^2, \mu_3^2, \lambda_3\mu_3), \quad Q_4 (\lambda_4^2, \mu_4^2, \lambda_4\mu_4). \end{aligned}$$

Прямые вычисления находим, что

$$\begin{aligned} Q_1Q_2 \cap Q_3Q_4 &= D_1 (\lambda_1\lambda_2, \mu_1\mu_2, 0), \\ Q_1Q_3 \cap Q_2Q_4 &= D_2 (\lambda_1\lambda_2, \mu_1\mu_2, \lambda_1\mu_2), \\ Q_1Q_4 \cap Q_2Q_3 &= D_3 (\lambda_1\lambda_2, \mu_1\mu_2, \lambda_2\mu_1). \end{aligned}$$

Рассмотрим теперь прямую

$$d: [\mu_1\mu_2, \lambda_1\lambda_2, 0],$$

которая проходит через ядро $(0, 0, 1)$, т. е. является касательной; эта прямая проходит и через диагональные точки D_1 , D_2 , D_3 . Координаты точки касания D прямой d с линией \mathcal{C}_0 суть

$$\rho x_1 = \lambda_1\lambda_2, \quad \rho x_2 = \mu_1\mu_2, \quad \rho x_3 = \sqrt{\lambda_1\lambda_2\mu_1\mu_2} = v$$

*) Как известно, в классической проективной геометрии справедлива аналогичная теорема.

($v \in K$, поскольку каждый элемент из K является квадратом).

Мы уже знаем, что касательная к кривой \mathcal{C}_0 в некоторой точке есть поляра этой точки относительно \mathcal{C}_0 и что через каждую точку, исключая ядро, проходит одна и только одна касательная. Таким образом, прямая d является полярной каждой из точек D_1, D_2, D_3 . Мы доказали следующую теорему.

Т е о р е м а. *Диагональные точки четырехугольника, вписанного в кривую второго порядка на плоскости Галуа четного порядка, лежат на одной касательной к кривой; эта касательная служит полярной каждой из диагональных точек.*

Точка касания прямой, содержащей диагональные точки четырехугольника, с кривой называется точкой, ассоциированной с четырехугольником.

2.11. Точечные конфигурации порядка 2 на плоскости Галуа нечетного порядка

В этом параграфе координатное поле K считается полем нечетной характеристики.

Некоторые детали доказательств мы будем теперь опускать, так как они повторяют рассуждения, используемые в классической проективной геометрии.

Общее уравнение «фигуры второго порядка» можно записать в следующей форме:

$$(2.11.1) \quad f(x) = 0: a_{11}x_1^2 + a_{22}x_2^2 + a_{33}x_3^2 + \\ + 2a_{12}x_1x_2 + 2a_{23}x_2x_3 + 2a_{31}x_3x_1 = 0.$$

Условимся считать $a_{jk} = a_{kj}$, тогда симметрический определитель

$$(2.11.2) \quad A = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$$

будет называться *определителем фигуры второго порядка*.

Квадратичная форма $f(x)$ разлагается в произведение двух линейных форм в том и только в том случае, когда $A = 0$; следовательно, условием неприводимости $f(x)$ является $A \neq 0$. Если это условие выполнено, то множество точек, определяемое уравнением $f(x) = 0$, назы-

вается *кривой второго порядка* или *квадратичной кривой*. Здесь слово «кривая» подчеркивает тот факт, что фигура не содержит прямых. Квадратичную кривую (где это потребуется) будем обозначать \mathcal{C} .

Пусть X и Y будут две точки, заданные неэквивалентными координатными последовательностями (x_1, x_2, x_3) и (y_1, y_2, y_3) соответственно. Точка Z , являющаяся линейной комбинацией X и Y , принадлежит кривой \mathcal{C} , если

$$(2.11.3) \quad f(z) = f(\lambda x + \mu y) = \\ = f(x) \cdot \lambda^2 + 2\varphi(x, y) \cdot \lambda\mu + f(y) \cdot \mu^2 = 0,$$

где

$$(2.11.4) \quad \varphi(x, y) = (a_{11}x_1 + a_{12}x_2 + a_{13}x_3)y_1 + \\ + (a_{21}x_1 + a_{22}x_2 + a_{23}x_3)y_2 + \\ + (a_{31}x_1 + a_{32}x_2 + a_{33}x_3)y_3.$$

Ввиду того, что $a_{jk} = a_{kj}$, имеем, очевидно,

$$(2.11.5) \quad \varphi(x, y) = \varphi(y, x) \quad \text{и} \quad \varphi(x, x) = f(x).$$

Мы скажем, что точка Y *сопряжена* точке X относительно кривой \mathcal{C} , если

$$(2.11.6) \quad \varphi(x, y) = 0.$$

Из (2.11.5) следует, что сопряженность есть симметричное отношение между двумя точками; при этом точки кривой \mathcal{C} сопряжены *сами себе*.

В необходимых случаях мы будем использовать некоторые хорошо известные теоремы теории полей Галуа. Некоторый элемент поля называется *квадратом*, если он равен квадрату хотя бы одного элемента поля. Среди $q - 1$ отличных от нуля элементов поля нечетной характеристики имеется $(q - 1)/2$ квадратов и ровно столько же не-квадратов. Каждый квадрат является квадратом в точности двух элементов, и эти два элемента противоположны друг другу по сложению. Существует элемент $S \neq 1$ поля, называемый *примитивным элементом*, такой, что

$$S^{q-1} = 1 \quad \text{и} \quad S^n \neq 1$$

для всякого n , меньшего $q - 1$. Таким образом, каждый ненулевой элемент поля может быть представлен как

степень элемента S ; в частности, все отличные от нуля квадраты являются четными степенями S .

В качестве примера рассмотрим элемент 3 в таблице, приведенной на рис. 44: $3^1 = 3$, $3^2 = 7$, $3^3 = 8$, $3^4 = 2$, $3^5 = 6$, $3^6 = 5$, $3^7 = 4$, $3^8 = 1$. Мы видим, что квадраты в поле $GF(9)$ суть 0, $3^2 = 7$, $3^4 = 2$, $3^6 = 5$, $3^8 = 1$; эти элементы стоят как раз на главной диагонали таблицы умножения.

Наконец, рассмотрим корни квадратного уравнения $ax^2 + bx + c = 0$ в конечном поле, а именно элементы

$$(-b + \sqrt{b^2 - 4ac})/2a \quad \text{и} \quad (-b - \sqrt{b^2 - 4ac})/2a.$$

Если $d = b^2 - 4ac$ есть отличный от нуля квадрат, то существуют в точности два (различных) корня; если $d = 0$, то имеется только один корень; если же d не является квадратом, то уравнение не имеет решений. Если $b = 0$ и $-c/a$ есть квадрат (но $c \neq 0$), то существуют два корня и их сумма равна нулю.

Приняв во внимание эти алгебраические факты, продолжим изучение кривой \mathcal{C} .

Точки пересечения кривой \mathcal{C} с прямой можно найти, используя (2.11.3) и (2.11.4). Число таких точек будет всегда 2, 1 или 0; соответственно этому прямая называется *секущей*, *касательной* или *внешней прямой*.

Пусть X и Y — две точки, не лежащие на кривой \mathcal{C} , но сопряженные относительно кривой. Если прямая XY пересекает кривую в точках P и Q , то $(XYPQ) = (-1)$ — это следует из (2.11.3).

Множество всех точек, сопряженных данной точке X относительно кривой \mathcal{C} , является прямой; эта прямая называется *полярной точки* X . Ее уравнение будет (2.11.4), где x_1, x_2, x_3 фиксированы (координаты точки X). Если точка X лежит на кривой \mathcal{C} , то ее полярна есть касательная к кривой в точке X .

Если четырехугольник $Q_1Q_2Q_3Q_4$ вписан в кривую \mathcal{C} , то его диагональные точки

$$D_1 = Q_1Q_2 \cap Q_3Q_4, \quad D_2 = Q_1Q_3 \cap Q_2Q_4, \quad D_3 = Q_1Q_4 \cap Q_2Q_3$$

образуют треугольник, в котором каждая сторона является полярной противоположающей вершины. Такой треугольник называют *автополярной фигурой* относительно кривой \mathcal{C} или *автополярным треугольником*.

Сопоставив каждой точке ее поляр, мы получаем взаимно однозначное отображение, задаваемое, согласно (2.11.4), формулами

$$(2.11.7) \quad \pi(x) = [u]: \begin{cases} \rho u_1 = a_{11}x_1 + a_{12}x_2 + a_{13}x_3, \\ \rho u_2 = a_{21}x_1 + a_{22}x_2 + a_{23}x_3, \\ \rho u_3 = a_{31}x_1 + a_{32}x_2 + a_{33}x_3, \end{cases}$$

где u_1, u_2, u_3 суть координаты прямой линии — поляры точки (x_1, x_2, x_3) . Это отображение линейно, и его определитель A есть как раз определитель уравнения кривой \mathcal{C} . Ввиду $A \neq 0$ отображение π имеет обратное, следовательно, каждая прямая является полярной одной и только одной точки. Эта точка называется *полюсом* данной прямой. Отображение $\pi(x) = [u]$ называют поляритетом, установленным с помощью кривой \mathcal{C} .

Если поляр некоторой точки X пересекает кривую в двух точках, то прямые, соединяющие эти точки с X , являются касательными к кривой.

Рассмотрим теперь невырожденное линейное преобразование

$$(2.11.8) \quad \gamma: \begin{cases} \rho x_1 = c_{11}y_1 + c_{12}y_2 + c_{13}y_3, \\ \rho x_2 = c_{21}y_1 + c_{22}y_2 + c_{23}y_3, \\ \rho x_3 = c_{31}y_1 + c_{32}y_2 + c_{33}y_3. \end{cases}$$

Как и прежде, точка отнесения A_i для новой системы координат (y_1, y_2, y_3) имеет первоначальные координаты $(c_i) = (c_{1i}, c_{2i}, c_{3i})$ ($i = 1, 2, 3$)*.

С помощью γ квадратичная форма $f(x)$ преобразуется в $g(y)$, где

$$g(y) \equiv f(c_1)y_1^2 + f(c_2)y_2^2 + f(c_3)y_3^2 + \\ + 2\varphi(c_1, c_2)y_1y_2 + 2\varphi(c_2, c_3)y_2y_3 + 2\varphi(c_3, c_1)y_3y_1.$$

*) Формулы (2.11.8) следует рассматривать как формулы преобразования координат при переходе от первоначальной системы координат x_1, x_2, x_3 к новой системе координат y_1, y_2, y_3 . Таким образом, в этих формулах x_1, x_2, x_3 означают первоначальные координаты точки, а y_1, y_2, y_3 — ее новые координаты. — Прим. перев.

Конкретный вид формы $g(y)$ зависит, естественно, от взаимного расположения треугольника $A_1A_2A_3$ и кривой \mathcal{C} .

Наибольший интерес представляют следующие три случая:

1° Треугольник $A_1A_2A_3$ вписан в кривую \mathcal{C} .

2° Треугольник $A_1A_2A_3$ является автополярным треугольником относительно \mathcal{C} .

3° Стороны A_1A_2 и A_2A_3 треугольника $A_1A_2A_3$ касаются кривой \mathcal{C} в точках A_1 и A_2 соответственно.

Соответственно этим случаям уравнение $g(y) = 0$ запишется:

$$\begin{aligned} b_{12}y_1y_2 + b_{23}y_2y_3 + b_{31}y_3y_1 &= 0, \\ b_{11}y_1^2 + b_{22}y_2^2 + b_{33}y_3^2 &= 0, \\ b_{12}y_1y_2 + b_{33}y_3^2 &= 0, \end{aligned}$$

где $b_{jj} = f(c_j)$ и $b_{jk} = 2\varphi(c_j, c_k)$, если $j \neq k$.

Третье уравнение можно упростить дальше с помощью линейного преобразования

$$\beta: \rho z_1 = \beta_1 y_1, \quad \rho z_2 = \beta_2 y_2, \quad \rho z_3 = y_3,$$

где $\beta_1 = b_{12}$ и $\beta_2 = b_{33}^{-1}$; это преобразование приводит к уравнению канонического вида

$$(2.11.9) \quad z_1 z_2 - z_3^2 = 0.$$

Мы перешли от исходного уравнения $f(x) = 0$ к каноническому уравнению с помощью линейного преобразования $\omega = \gamma\beta$. В зависимости от того, как понимается ω , этот факт можно истолковывать двумя различными способами:

1° ω понимается как преобразование системы координат. Это будет означать, что уравнение кривой \mathcal{C} принимает канонический вид (2.11.9) в подходящим образом выбранной системе координат.

2° ω понимается как линейное отображение на плоскости. Это означает, что исходная кривая \mathcal{C} переводится линейным отображением в кривую \mathcal{C}_0 , определяемую (в той же самой исходной системе координат) уравнением $x_1 x_2 - x_3^2 = 0$.

Так или иначе, мы можем теперь сказать, что *любая кривая \mathcal{C} второго порядка есть овал*. Позже будет показано,

что обратное утверждение тоже справедливо, а именно: на плоскости Галуа нечетного порядка каждый овал есть кривая второго порядка.

Комбинируя результаты этого параграфа с результатами 2. 10, мы видим, что любая кривая второго порядка \mathcal{C} на плоскости Галуа *произвольной* характеристики имеет каноническое уравнение $x_1x_2 - x_3^2 = 0$. Поэтому в следующем параграфе мы не будем делать различия между случаями нечетной и четной характеристик.

2.12. Соответствие между двумя пучками прямых

Пусть A и B будут две различные точки плоскости Галуа. Предположим, что установлено некоторое соответствие между прямыми пучка прямых, проходящих через B , и прямыми пучка прямых, проходящих через A . Для каждой пары соответствующих прямых можно найти точку их пересечения. Фигура, образованная точками пересечения, называется *проективно порожденной траекторией*, полученной с помощью данного соответствия. Разумеется, если отображение обладает тем свойством, что прямая AB соответствует самой себе, т. е. она является общей прямой данного соответствия, то эта прямая будет одной из компонент траектории. В общем же случае из всех точек прямой AB только точки A и B принадлежат траектории, так как прямая, проходящая через A и соответствующая прямой AB , пересекает AB в точке A , а прямая, проходящая через B и соответствующая AB , пересекает AB в точке B .

Если рассматриваемое соответствие является проективным и прямая AB соответствует самой себе, то траектория состоит из прямой AB и еще одной прямой, как можно легко вывести из теоремы Паппа. В этом частном случае проективное соответствие между двумя пучками называется *перспективным* (или *перспективой*).

Ниже мы будем рассматривать траектории, образованные точками пересечения прямых двух проективно соответствующих пучков, причем соответствие между ними не будет перспективным.

Пусть дан собственный четырехугольник $P_1P_2P_3Q$ (рис. 54). Пучок прямых с центром P_1 переводится в пучок с центром P_2 с помощью проективного соответствия, уста-

навливаемого с помощью данного четырехугольника следующим образом (предполагается, что плоскость Галуа имеет порядок > 2). Пусть

$$P_1Q = l_1 \rightarrow P_2P_1 = l'_1, \quad P_1P_2 = l_2 \rightarrow P_2Q = l'_2,$$

$$P_1P_3 = l_3 \rightarrow P_2P_3 = l'_3.$$

Каждой прямой l из оставшихся $q - 2$ прямых пучка P_1 мы сопоставляем прямую l' пучка P_2 таким образом, чтобы было

$$(l_1 l_2 l_3 l) = (l'_1 l'_2 l'_3 l').$$

Пересекая l и l' , мы получаем точку P проективно порожденной траектории. Таким образом, траектория

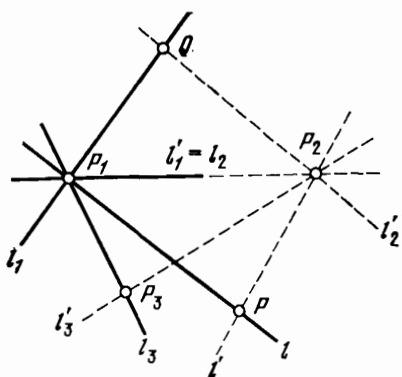


Рис. 54.

состоит из $q + 1$ точек P_1, \dots, P_{q+1} . Мы можем получить уравнение траектории $\{P_1, \dots, P_{q+1}\}$, воспользовавшись линейным отображением ω , при котором

$$P_1 \rightarrow A_1^\circ, \quad P_2 \rightarrow A_2^\circ, \quad P_3 \rightarrow A_3^\circ, \quad P_4 \rightarrow E^\circ.$$

Так как соответствие между пучками P_1 и P_2 задано условием сохранения двойного отношения и так как линейное отображение тоже сохраняет двойные отношения, то для любой из точек $P^\circ = \omega(P)$ должно выполняться равенство

$$A_1^\circ (A_1^\circ A_2^\circ E^\circ P^\circ) = A_2^\circ (A_1^\circ A_2^\circ E^\circ P^\circ) = \theta,$$

откуда для множества точек P° получается **уравнение** $x_1 x_2 - x_3^2 = 0$. Если это уравнение преобразовать посред-

ством $\omega^{-1}(x) = y$, то мы получим неприводимое уравнение $f(y) = 0$ второй степени, которое и будет уравнением исходной траектории. Итак, *уравнение множества точек пересечения соответствующих прямых двух проективно (но не перспективно) связанных пучков есть неприводимое уравнение второй степени.*

Далее, мы теперь знаем, что кривая \mathcal{C} , определяемая неприводимым уравнением второй степени, всегда может быть переведена с помощью линейного отображения в овал Ω_0 . Следовательно, *кривая, определяемая неприводимым уравнением второй степени, всегда может быть получена как множество точек пересечения соответствующих прямых двух проективно (но не перспективно) связанных пучков.*

Теперь можно легко доказать следующую теорему.

Т е о р е м а. *На плоскости Галуа порядка > 3 существует одна и только одна кривая второго порядка, проходящая через пять данных точек, никакие три из которых не коллинеарны.*

Предположим, что пять точек P_1, P_2, P_3, P_4, P_5 принадлежат одновременно двум различным кривым второго порядка \mathcal{C}_1 и \mathcal{C}_2 . Так как каждая из этих кривых состоит из $q + 1$ точек, то кривые могут быть различными только в том случае, если \mathcal{C}_1 содержит по крайней мере одну точку X , не принадлежащую \mathcal{C}_2 .

Поскольку кривая второго порядка обладает всеми свойствами овала Ω_0 , сохраняющимися при линейном отображении, она должна иметь следующее свойство: *двойное отношение четырех прямых, соединяющих какие-либо четыре точки кривой с какой-то другой точкой P кривой, не зависит от выбора точки P* (предполагается, что четыре точки берутся всякий раз в одном и том же порядке). Таким образом, для кривой \mathcal{C}_1 мы имеем

$$P_1(P_2P_3P_4X) = P_5(P_2P_3P_4X).$$

Рассмотрим теперь кривую \mathcal{C}_2 , которая не проходит через X . Она пересекает прямую P_1X в точке P_1 и в точке X^* , отличной от X , так что P_5X и P_5X^* различны и

$$P_1(P_2P_3P_4X^*) = P_5(P_2P_3P_4X^*).$$

Поскольку $X^* \in P_1X$, $X^* \neq X$, то

$$\begin{aligned} P_1(P_2P_3P_4X^*) &= P_1(P_2P_3P_4X) = \\ &= P_5(P_2P_3P_4X) = P_5(P_2P_3P_4X^*). \end{aligned}$$

Отсюда следует $P_5X = P_5X^*$, вопреки нашему допущению. Полученное противоречие завершает доказательство теоремы.

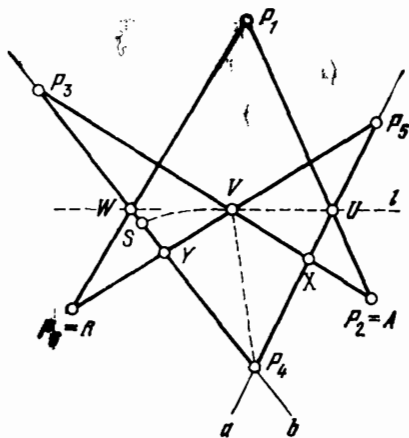


Рис. 55.

Подобными же рассуждениями можно доказать следующие теоремы.

Прямая, проходящая через вершину собственного четырехугольника, определяет (как касательная) совместно с другими вершинами четырехугольника одну и только одну кривую второго порядка.

Вершины собственного треугольника и две прямые, проходящие через различные вершины и не являющиеся сторонами треугольника, определяют одну и только одну кривую второго порядка.

В качестве иллюстрации предыдущих фактов обсудим вопрос о порождении неприводимой кривой второго порядка с помощью пяти точек, никакие три из которых не коллинеарны.

Обратимся к рис. 55. Пусть точки P_1 , $P_2 (=A)$, P_3 , P_4 , P_5 , $P_6 (=B)$ таковы, что никакие три из них не лежат

на одной прямой. Предположим, что эти шесть точек лежат на кривой второго порядка \mathcal{C} . Из наших допущений следует, что $q > 4$ и, далее, что пять точек

$$P_1P_2 \cap P_4P_5 = U, \quad P_2P_3 \cap P_5P_6 = V, \quad P_3P_4 \cap P_6P_1 = W, \\ P_2P_3 \cap P_4P_5 = X, \quad P_3P_4 \cap P_5P_6 = Y$$

различны. Рассмотрим прямые, проектирующие точки P_1, P_3, P_4, P_5 кривой \mathcal{C} из точек A и B соответственно. Из свойств кривой \mathcal{C} и из теоремы Паппа следует, что

$$A(P_1P_3P_4P_5) = B(P_1P_3P_4P_5), \quad A(P_1P_3P_4P_5) = (UXP_4P_5), \\ B(P_1P_3P_4P_5) = (WP_3P_4Y).$$

Сопоставляя эти равенства, находим, что

$$(UXP_4P_5) = (WP_3P_4Y).$$

Проекции точек P_5, X, P_4 прямой $P_4P_5 = a$ из точки V на прямую $P_3P_4 = b$ суть точки Y, P_3, P_4 ; если, далее, мы примем, что проекция точки U есть точка S , то по теореме Паппа будем иметь

$$(UXP_4P_5) = (SP_3P_4Y).$$

Отсюда и из предыдущего равенства следует

$$(WP_3P_4Y) = (SP_3P_4Y),$$

что и доказывает совпадение точек S и W . Таким образом, точки U, V и W лежат на одной прямой l . Итак:

Если шестиугольник $P_1P_2P_3P_4P_5P_6$ вписан в кривую второго порядка, то три пары его противоположных сторон (при данном порядке следования вершин) пересекаются в коллинеарных точках.

Если кривая \mathcal{C} определена пятью точками P_1, P_2, P_3, P_4, P_5 , то любая из оставшихся $q - 4$ точек кривой может быть принята за точку P_6 из предыдущей теоремы. Тем самым мы получаем способ построения оставшихся $q - 4$ точек кривой \mathcal{C} .

А именно, данные пять точек определяют точки прямой b , в которых эта прямая встречается стороны треугольника $P_1P_2P_5$; вместе с P_3 и P_4 получается уже пять точек прямой b . Любая из оставшихся $q - 4$ точек прямой b может играть роль указанной ранее точки W . Выбор же

точки W приводит к точке P_6 путем следующих построений:

$$UW = l, \quad P_2P_3 \cap l = V, \quad P_5V \cap P_1W = P_6.$$

Полученная таким способом точка P_6 лежит на кривой \mathcal{C} , так как в противном случае мы получили бы противоречие доказанной выше теореме. Варьируя точку W , находим $q - 4$ экземпляра точки P_6 .

2.13. Теорема Сегре

В этом параграфе наши рассуждения будут относиться к плоскости нечетного порядка. Легко показать, что любая кривая второго порядка обладает следующим свойством: *треугольник, вписанный в кривую второго порядка, и треугольник, составленный из касательных в вершинах первого треугольника, перспективны*. Это свойство называют π -свойством. Сегре принадлежит идея о том, что овал, обладающий π -свойством, есть кривая второго порядка. Благодаря этому исследованию овалов на плоскости Галуа нечетного порядка может быть преобразовано в чисто алгебраическую задачу.

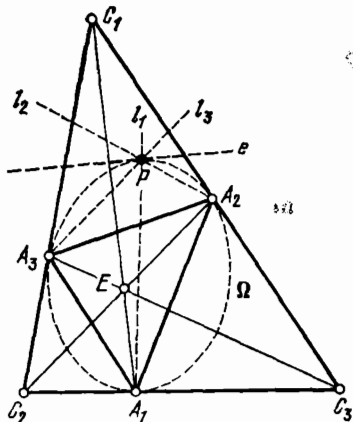


Рис. 56.

Прямые, касательные к произвольному овалу Ω в вершинах вписанного треугольника $A_1A_2A_3$, являются сторонами треугольника $C_1C_2C_3$ на рис. 56. Если овал обладает π -свойством, то прямые A_kC_k ($k = 1, 2, 3$) встречаются в общей точке E . Примем $A_1A_2A_3$ за фундаментальный треугольник и точку E за единичную точку, тогда координаты точек C_k будут

$$(2.13.1) \quad C_1(-1, 1, 1), \quad C_2(1, -1, 1), \quad C_3(1, 1, -1).$$

В самом деле, при подходящем выборе элемента ξ_k имеем $C_k = \xi_k A_k + E$, т. е. k -я координата точки C_k

есть $\lambda_k = \xi_k + 1$, остальные две координаты равны 1. Так как точки C_1, C_2, A_3 коллинеарны, имеем

$$\begin{vmatrix} \lambda_1 & 1 & 1 \\ 1 & \lambda_2 & 1 \\ 0 & 0 & 1 \end{vmatrix} = 0,$$

т. е. $\lambda_1 \lambda_2 = 1$. По симметрии имеем $\lambda_2 \lambda_3 = 1$ и $\lambda_3 \lambda_1 = 1$. Из полученных трех равенств следует $\lambda_1^2 = \lambda_2^2 = \lambda_3^2$, и так как $C_k \neq E$, то $\lambda_k = -1$. Этим доказано (2.13.1).

Выберем на овале Ω произвольную точку P , отличную от точек A_k , и рассмотрим касательную e в этой точке:

$$P(a_1, a_2, a_3) \quad \text{и} \quad e: e_1 x_1 + e_2 x_2 + e_3 x_3 = 0.$$

Так как точки A_k и C_k ($k = 1, 2, 3$) не лежат на прямой e , то e_1, e_2, e_3 отличны от нуля и

$$(2.13.2) \quad -e_1 + e_2 + e_3 = c_1 \neq 0, \quad e_1 - e_2 + e_3 = c_2 \neq 0, \\ e_1 + e_2 - e_3 = c_3 \neq 0.$$

Пусть jkl будет произвольная перестановка чисел 1, 2, 3. Найдем координаты точки $E_j = e \cap C_k C_l$. Легко видеть, что прямыми

$$C_2 C_3: [0, 1, 1], \quad C_3 C_1: [1, 0, 1], \quad C_1 C_2: [1, 1, 0],$$

отвечают точки

$$(2.13.3) \quad \begin{aligned} E_1(e_2 - e_3, -e_1, e_1), \\ E_2(e_2, e_3 - e_1, -e_2), \\ E_3(-e_3, e_3, e_1 - e_2). \end{aligned}$$

Касательная к овалу Ω в точке P есть прямая e , откуда имеем

$$(2.13.4) \quad e_1 a_1 + e_2 a_2 + e_3 a_3 = 0.$$

Теперь непосредственно находим прямые

$$(2.13.5) \quad \begin{aligned} C_1 P: [a_3 - a_2, a_3 + a_1, -a_1 - a_2], \\ E_2 A_3: [e_3 - e_1, -e_2, 0], \\ E_3 A_2: [e_2 - e_1, 0, -e_3]. \end{aligned}$$

Так как по предположению овал Ω обладает π -свойством, вписанный треугольник $PA_3 A_2$ и треугольник

$C_1E_2E_3$, образованный касательными к овалу в вершинах первого треугольника, перспективны. Следовательно, прямые C_1P , E_2A_3 и E_3A_2 принадлежат одному пучку. Отсюда вытекает, что определитель, составленный из координат этих прямых, равен нулю:

$$\begin{vmatrix} a_3 - a_2 & a_3 + a_1 & -a_1 - a_2 \\ e_3 - e_1 & -e_2 & 0 \\ e_2 - e_1 & 0 & -e_3 \end{vmatrix} = \begin{vmatrix} 0 & a_3 + a_1 & -a_1 - a_2 \\ c_1 & -e_2 & 0 \\ c_1 & 0 & -e_3 \end{vmatrix} = 0.$$

(Второй определитель получен из первого вычитанием из первого столбца суммы двух других столбцов.) Отсюда находим, учитывая $c_1 \neq 0$, что $(a_1 + a_2)e_2 = (a_3 + a_1)e_3$. Заменяя касательный треугольник $E_2E_3C_1$ поочередно на $E_3E_1C_2$ и $E_1E_2C_3$, получаем с помощью таких же рассуждений еще два равенства. Итак,

$$(2.13.6) \quad \begin{cases} (a_1 + a_2)e_1 = (a_2 + a_3)e_3, \\ (a_2 + a_3)e_2 = (a_3 + a_1)e_1, \\ (a_3 + a_1)e_3 = (a_1 + a_2)e_2. \end{cases}$$

Отсюда заключаем, что все суммы $a_j + a_k$ отличны от нуля: в случае, если бы одна из них равнялась нулю, две другие, в силу $e_1 \neq 0$, $e_2 \neq 0$, $e_3 \neq 0$, тоже были бы нулями, что давало бы $a_1 = a_2 = a_3 = 0$, т. е. противоречило бы смыслу чисел a_1 , a_2 , a_3 .

Из (2.13.6) и сказанного выше вытекает существование такого элемента $\rho \in K$, отличного от нуля, что

$$(2.13.6') \quad \begin{cases} \rho e_1 = 0 + a_2 + a_3, \\ \rho e_2 = a_1 + 0 + a_3, \\ \rho e_3 = a_1 + a_2 + 0. \end{cases}$$

Если теперь мы рассмотрим кривую второго порядка \mathfrak{C} , определяемую уравнением

$$x_1x_2 + x_2x_3 + x_3x_1 = 0,$$

то устанавливаемый с ее помощью поляритет

$$\begin{cases} \rho u_1 = 0 + x_2 + x_3, \\ \rho u_2 = x_1 + 0 + x_3, \\ \rho u_3 = x_1 + x_2 + 0 \end{cases}$$

будет, в силу (2.13.6'), переводить точку (a_1, a_2, a_3) в прямую $[e_1, e_2, e_3]$. Таким образом, каждая из $q + 1$ точек овала Ω обладает тем свойством, что ее поляра относительно \mathcal{C} проходит через эту точку. Другими словами, каждая точка овала Ω принадлежит кривой \mathcal{C} . Так как число точек в Ω и \mathcal{C} одинаково, мы заключаем отсюда, что $\mathcal{C} = \Omega$. Полученный результат может быть сформулирован в виде следующей теоремы.

Т е о р е м а 1. *На плоскости Галуа нечетного порядка любой овал, обладающий π -свойством, есть кривая второго порядка.*

Пусть K — произвольное поле Галуа. Произведение всех элементов множества $K^* = K \setminus 0$ обозначим Π а). Хорошо известно, что

$$(2.13.7) \quad \Pi(a) = -1,$$

где -1 обозначает элемент, противоположный по сложению к единичному элементу поля. (Если число элементов поля K простое, то соотношение (2.13.7) выражает теорему Вильсона.) Доказательство следующей теоремы основано на соотношении (2.13.7).

Т е о р е м а 2. *На плоскости Галуа нечетного порядка каждый овал обладает π -свойством.*

Д о к а з а т е л ь с т в о. Пусть фундаментальный треугольник $A_1A_2A_3$ вписан в овал Ω . Уравнение прямой, проходящей через вершину A_j , но отличной от сторон A_jA_k и A_jA_l , может быть представлено в виде

$$x_k = cx_l \quad c \in K^*)$$

(где jkl есть циклическая перестановка элементов 1, 2, 3).

Пусть уравнения касательных в точках A_1, A_2, A_3 будут соответственно

$$x_2 = \alpha_1 x_3, \quad x_3 = \alpha_2 x_1, \quad x_1 = \alpha_3 x_2$$

(очевидно, $\alpha_1 \alpha_2 \alpha_3 \neq 0$). Если точка $P(a_1, a_2, a_3)$ овала отлична от фундаментальных точек, то уравнения прямых $l_1 = A_1P$, $l_2 = A_2P$, $l_3 = A_3P$ будут соответственно

$$x_2 = \lambda_1 x_3, \quad x_3 = \lambda_2 x_1, \quad x_1 = \lambda_3 x_2,$$

где $\lambda_i \neq 0$, $\lambda_i \neq \alpha_i$ $i = 1, 2, 3$). Так как P лежит на каждой из прямых l_1, l_2, l_3 , имеем

$$a_2 = \lambda_1 a_3, \quad a_3 = \lambda_2 a_1, \quad a_1 = \lambda_3 a_2;$$

отсюда

$$\lambda_1 = a_2 a_3^{-1}, \quad \lambda_2 = a_3 a_1^{-1}, \quad \lambda_3 = a_1 a_2^{-1}$$

и, следовательно,

$$(2.13.8) \quad \lambda_1 \lambda_2 \lambda_3 = 1.$$

Для каждой из $q - 2$ точек овала Ω , отличных от A_1, A_2, A_3 , мы получаем, таким образом, три элемента $\lambda_1, \lambda_2, \lambda_3$ таких, что $\lambda_1 \lambda_2 \lambda_3 = 1$. Пусть S обозначает произведение всех $q - 2$ произведений $\lambda_1 \lambda_2 \lambda_3$. Очевидно, λ_i будет принимать каждое значение, исключая α_i , один и только один раз ($i = 1, 2, 3$). Следовательно, в произведении $\alpha_1 \alpha_2 \alpha_3 S$ каждый элемент из K^* будет встречаться ровно три раза, т.е.

$$\alpha_1 \alpha_2 \alpha_3 S = (\Pi(a))^3.$$

Но в силу (2.13.8) имеем $S = 1$ и в силу (2.13.7) $\Pi(a) = -1$, следовательно,

$$(2.13.9) \quad \alpha_1 \alpha_2 \alpha_3 = -1.$$

Теперь мы можем определить вершины треугольника, образованного касательными к Ω в фундаментальных точках. Обозначим касательную в точке A_j через t_j . Координаты касательных будут

$$t_1: [0, -1, \alpha_1], \quad t_2: [\alpha_2, 0, -1], \quad t_3: [-1, \alpha_3, 0].$$

Отсюда находим координаты точек $C_1 = t_2 \cap t_3$, $C_2 = t_3 \cap t_1$, $C_3 = t_1 \cap t_2$:

$$C_1(\alpha_3, 1, \alpha_2 \alpha_3), \quad C_2(\alpha_3 \alpha_1, \alpha_1, 1), \quad C_3(1, \alpha_1 \alpha_2, \alpha_2).$$

Таким образом, уравнения прямых $A_1 C_1$, $A_2 C_2$, $A_3 C_3$ суть

$$x_3 = \alpha_2 \alpha_3 x_2, \quad x_1 = \alpha_3 \alpha_1 x_3, \quad x_2 = \alpha_1 \alpha_2 x_1$$

соответственно, и мы легко замечаем, учитывая (2.13.9), что эти три прямые проходят через точку

$$(2.13.10) \quad Q(\alpha_3 \alpha_1, -\alpha_1, 1).$$

Отсюда вытекает, что $\triangle A_1 A_2 A_3$ и $\triangle C_1 C_2 C_3$ перспективны относительно точки Q . Теорема 2 доказана.

Из теорем 1 и 2 вытекает следующая

Теорема 3. *Любой овал на плоскости Галуа нечетного порядка есть кривая второго порядка.*

В заключение, чтобы подчеркнуть различие между плоскостями Галуа нечетного и четного порядков, приведем тривиальный пример, показывающий, что теорема 3 неверна для плоскости Галуа четного порядка. Мы знаем, что в каждой такой плоскости $q + 1$ точек кривой второго порядка совместно с ядром образуют гиперова́л. Исключим из гиперовала одну из точек, принадлежащих кривой. Оставшиеся $q + 1$ точек образуют другой овал, но этот овал не является кривой второго порядка, если $q > 4$; в противном случае мы имели бы две кривые второго порядка с q общими точками, что противоречит теореме о единственности кривой второго порядка, проходящей через данные 5 точек.

2.14. Дополнительные замечания относительно конструкции плоскостей Галуа

В этом и следующих пяти параграфах мы сообщаем некоторую дополнительную информацию, главным образом алгебраического характера. Ее можно было бы изложить и в начале главы, но мы отложили это с тем, чтобы возможно быстрее рассмотреть интересные и неожиданные *геометрические* свойства прямолинейных фигур, овалов и квадратичных фигур.

Напомним, что в параграфе 1.6 была описана явная конструкция плоскости $S_{2,q}$ с помощью {пары таблиц $[A, M]$ операций в поле $GF(q)$ }. Однако будет ли пара $[A, M]$ однозначно определяться числом q , а если нет, то какого рода связь существует между плоскостями, определенными с помощью различных пар таблиц? Займемся сейчас этим вопросом.

Как обычно, будем обозначать элементы конечного поля $GF(q)$, где $q = p^r$, целыми числами $0, 1, 2, \dots, q - 1$, считая при этом, что нулевой элемент обозначен 0 , а единичный элемент 1 ; далее, элементы простого подполя $GF(p)$ обозначим

$$(2.14.1) \quad 0, 1, \dots, p - 1,$$

где $1 + 1 = 2, 1 + 1 + 1 = 3$ и т. д.

Тем самым таблицы операций для подполя $GF(p)$ определены однозначно, и таблица сложения (соответственно умножения) поля $GF(q)$ будет содержать в своем левом верхнем углу таблицу сложения (соответственно умножения) поля классов вычетов по модулю p .

Перечислим теперь некоторые понятия и теоремы теории конечных полей.

Число элементов в $K = GF(q)$ есть $|K| = p^r$, число элементов в $P = GF(p)$ есть $|P| = p$. Степень поля K над P , обозначаемая $|K| : |P|$, равна r .

Очевидно, K можно рассматривать как векторное пространство над подполем P ; тогда $|K| : |P|$ есть в точности размерность этого пространства. Каждый элемент поля K удовлетворяет уравнению $x^q - x = 0$, т. е. множество элементов поля есть множество корней полинома $x^q - x$. Поле K содержит элемент S такой, что $S^q = S$, но $S^n \neq S$ при любом $n < q$. Этот элемент называется примитивным корнем уравнения. Очевидно, последовательность

R^0

$$0, 1, S, S^2, \quad S^{q-2}$$

должна содержать все элементы поля K .

В качестве примера укажем элемент $S = 3$ поля $GF(9)$ (см. рис. 44). Легко проверить, используя таблицу M , что упомянутая выше последовательность состоит в этом случае из элементов $0, 1, 3, 3^2 = 7, 3^3 = 8, 3^4 = 2, 3^5 = 6, 3^6 = 5, 3^7 = 4$, т. е. из всех элементов поля.

Пусть K и L — два конечных поля, оба порядка q , и пусть $x \rightarrow x'$ есть взаимно однозначное отображение K на L . Если это отображение обладает свойствами $(x+y)' = x' + y'$ и $(xy)' = x'y'$ (где $x, y \in K, x', y' \in L$), т. е. если оно сохраняет операции, то оно называется *изоморфизмом*, а в случае $K = L$ — *автоморфизмом*. Очевидно, тождественное отображение $x \rightarrow x$ поля на себя, которое мы обозначим ε , является автоморфизмом. Могут ли существовать другие автоморфизмы? Если $q = p$ есть простое число, то других автоморфизмов быть не может; однако, если $q = p^r$, причем $r > 1$, то существует r автоморфизмов (включая ε).

А именно, отображение $x \rightarrow x^p$ является автоморфизмом; если обозначить его α , то все автоморфизмы поля

будут

$$\varepsilon, \alpha, \alpha^2, \quad \alpha^{r-1}.$$

Автоморфизм α называют *фробениусовским*.

В качестве примера перечислим все автоморфизмы поля $GF(8)$ (см. рис. 51). В этом случае

$$\varepsilon = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}, \quad \alpha = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 1 & 4 & 5 & 6 & 7 & 2 & 3 \end{pmatrix},$$

$$\alpha^2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 1 & 6 & 7 & 2 & 3 & 4 & 5 \end{pmatrix}.$$

Каждый автоморфизм поля K индуцирует тождественный автоморфизм его простого подполя P . Например, в случае поля $GF(9)$ (см. снова рис. 44), где $r = 2$, существуют в точности два автоморфизма, а именно ε и

$$\alpha = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 0 & 1 & 2 & 8 & 6 & 7 & 4 & 5 & 3 \end{pmatrix},$$

и каждый из них оставляет на месте элементы 0, 1 и 2 поля P .

Наконец, укажем способ построения таблиц операций для поля K из $q = P^r$ элементов, где $r > 1$.

Как уже говорилось, элементам простого подполя P мы сопоставляем целые числа 0, 1, ..., $p - 1$. Среди элементов множества $K \setminus P$ существует такой, который является корнем неприводимого полинома степени r над P . Выберем такой элемент и обозначим его p ; соответствующий неприводимый полином пусть будет $f(x)$.

Мы можем теперь установить взаимно однозначное соответствие между элементами поля K и полиномами степени не выше $r - 1$ над P . А именно, полиному

$$a_{r-1}x^{r-1} + \dots + a_1x + a_0 \quad (a_0, \dots, a_{r-1} \in P)$$

следует сопоставить элемент

$$a_{r-1}p^{r-1} + \dots + a_1p + a_0$$

поля K .

Пусть элементам s и t отвечают полиномы $g(x)$ и $h(x)$ соответственно. Тогда элементу $s + t$ будет отвечать полином $g(x) + h(x)$, а элементу $s \cdot t$ — полином $g(x)h(x)$, редуцированный по модулю $f(x)$. Таким путем мы можем получить таблицы $[A, M]$ операций в поле K . Указанный

способ имеет ту особенность, что при любом выборе элемента p таблица сложения A будет одна и та же, в то время как таблица умножения M будет, очевидно, зависеть от полинома $f(x)$, имеющего p своим корнем.

x^2+1									
\times	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	1	6	8	7	3	5	4
3	0	3	6	2	5	8	1	4	7
4	0	4	8	5	6	1	7	2	3
5	0	5	7	8	1	3	4	6	2
6	0	6	3	1	7	4	2	8	5
7	0	7	5	4	2	6	8	3	1
8	0	8	4	7	3	2	5	1	6

$M^{(1)}$

x^2+x+2									
\times	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	1	6	8	7	3	5	4
3	0	3	6	7	1	4	5	8	2
4	0	4	8	1	5	6	2	3	7
5	0	5	7	4	6	2	8	1	3
6	0	6	3	5	2	8	7	4	1
7	0	7	5	8	3	1	4	2	6
8	0	8	4	2	7	3	1	6	5

$M^{(2)}$

x^2+2x+2									
\times	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	1	6	8	7	3	5	4
3	0	3	6	4	7	1	8	2	5
4	0	4	8	7	2	3	5	6	1
5	0	5	7	1	3	8	2	4	6
6	0	6	3	8	5	2	4	1	7
7	0	7	5	2	6	4	1	8	3
8	0	8	4	5	1	6	7	3	2

$M^{(3)}$

Рис. 57.

Рассмотрим, например, поле $K = GF(3^2)$. Здесь имеются три неприводимых полинома степени 2 над $P = GF(3)$, а именно:

$$f_1: x^2 + 1, \quad f_2: x^2 + x + 2, \quad f_3: x^2 + 2x + 2.$$

Шесть элементов из $K \setminus P$ являются корнями этих полиномов. Таким образом, мы имеем здесь три возможности для выбора полинома $f(x)$. Это приводит к трем парам таблиц: $[A, M^{(1)}], [A, M^{(2)}], [A, M^{(3)}]$ ($M^{(1)}, M^{(2)}, M^{(3)}$ представлены на рис. 57). Соответствующие поля обозначим $K^{(1)}, K^{(2)}, K^{(3)}$. Легко проверить, что каждое из

отображении

$$\rho: K^{(1)} \rightarrow K^{(2)}: \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 0 & 1 & 2 & 7 & 8 & 6 & 5 & 3 & 4 \end{pmatrix},$$

$$\sigma: K^{(1)} \rightarrow K^{(3)}: \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 0 & 1 & 2 & 4 & 5 & 3 & 8 & 6 & 7 \end{pmatrix}$$

является изоморфизмом.

В действительности такое положение является общим. Любые два поля, состоящие из одинакового числа q элементов, изоморфны *). Доказывать это мы здесь не будем.

Обозначим плоскости, построенные исходя из $[A, M^{(1)}]$, $[A, M^{(2)}]$ и $[A, M^{(3)}]$, через $S_{2,q}^{(1)}$, $S_{2,q}^{(2)}$ и $S_{2,q}^{(3)}$ соответственно **).

Как соотносятся друг с другом плоскости $S_{2,q}^{(1)}$ и $S_{2,q}^{(2)}$? Мы не получили бы взаимно однозначного соответствия между ними, приняв, что точке с координатами (x_1, x_2, x_3) отвечает точка с теми же самыми координатами. В самом деле, например, последовательности $(2, 6, 5)$ и $(5, 1, 8)$ представляют одну и ту же точку (ее нормированные координаты $(8, 7, 1)$) на плоскости $S_{2,q}^{(1)}$, но *разные* точки (а именно $(3, 4, 1)$ и $(6, 7, 1)$) на плоскости $S_{2,q}^{(2)}$.

Однако ненулевой тройке элементов (x_1, x_2, x_3) поля $K^{(1)}$ отвечает точка P на плоскости $S_{2,q}^{(1)}$. Отображение ρ переводит x_1, x_2 и x_3 в какие-то элементы x'_1, x'_2 и x'_3 поля $K^{(2)}$, и тройка (x'_1, x'_2, x'_3) определяет точку P' на плоскости $S_{2,q}^{(2)}$. Таким путем мы получаем взаимно однозначное отображение

$$\rho^*: S_{2,q}^{(1)} \rightarrow S_{2,q}^{(2)},$$

индуцированное отображением $\rho: K^{(1)} \rightarrow K^{(2)}$. Отображение ρ^* сохраняет линейную зависимость или независимость между точками, и, следовательно, любым трем коллинеарным точкам плоскости $S_{2,q}^{(1)}$ отвечают три коллинеарные точки плоскости $S_{2,q}^{(2)}$ (и обратно); короче, ρ^* сохраняет коллинеарность.

Легко видеть, что построение отображения ρ^* исходя из изоморфизма ρ может быть перенесено на плоскости любого порядка.

*) Однако до сих пор мы пользовались той парой таблиц $[A, M]$ для поля порядка q , которая строится по методу параграфа 1.6.

**) На самом деле здесь $q = 9$. — *Прим. перев.*

Взаимно однозначное отображение одной конечной плоскости на другую конечную плоскость, сохраняющее коллинеарность, называется *изоморфизмом* или *коллинеацией*; в случае, когда плоскость отображается на себя, мы называем изоморфизм *автоморфизмом*.

Таким образом, можно сказать, что *различные пары таблиц, задающих поле из q элементов, определяют с точностью до изоморфизма одну плоскость Галуа порядка q .*

2.15. Коллинеации и гомографии на плоскости Галуа

Как мы указывали в предыдущем параграфе, все плоскости Галуа данного порядка q изоморфны друг другу. Кроме того, нам известно, что линейное отображение, преобразующее плоскость Галуа в себя, сохраняет как коллинеарность точек, так и двойное отношение.

Мы знаем также, что в случае классической проективной плоскости из сохранения коллинеарности следует сохранение двойного отношения. Для классической проективной плоскости линейное отображение (определяемое аналитическим путем) и коллинеация (определяемая геометрически) — эквивалентные понятия. Для плоскости Галуа это не так.

На плоскости Галуа коллинеация необязательно сохраняет двойное отношение; в случае, если она сохраняет его, она называется *гомографией*. Рассмотрим снова плоскость Галуа порядка 9, представленную таблицей сложения рис. 44 и таблицей умножения $M^{(2)}$ рис. 57; обозначим эту плоскость S . В параграфе 2.14 уже определялся автоморфизм α поля $GF(9)$, отличный от тождественного. Приведем его снова:

$$\alpha: x \rightarrow x^3,$$

или, в форме подстановки,

$$\alpha: \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 0 & 1 & 2 & 8 & 6 & 7 & 4 & 5 & 3 \end{pmatrix}.$$

Мы знаем, что автоморфизм α индуцирует автоморфизм α^* плоскости, т. е. коллинеацию. Ее запись:

$$\alpha^*: \begin{cases} \rho x'_1 = x_1^3 + 0 + 0, \\ \rho x'_2 = 0 + x_2^3 + 0, \\ \rho x'_3 = 0 + 0 + x_3^3 \end{cases} \quad (0 \neq \rho \in K).$$

Оказывается, α^* не сохраняет двойное отношение. Рассмотрим, например, точки

$$A(1, 1, 0), \quad B(4, 8, 1), \quad C(1, 5, 1), \quad D(2, 3, 1).$$

Под действием α^* они перейдут в

$$A'(1, 1, 0), \quad B'(6, 3, 1), \quad C'(1, 7, 1), \quad D'(2, 8, 1).$$

С помощью таблиц операций легко проверить, что

$$6 \cdot A + B = C, \quad 7 \cdot A + B = D, \quad 4 \cdot A' + B' = C', \\ 5 \cdot A' + B' = D'.$$

Добавим к этому, что автоморфизм α переводит элементы 1, 6, 7 в 1, 4, 5. Рассмотрев теперь двойные отношения, получим

$$\theta = (ABCD) = \frac{1}{6} : \frac{1}{7} = 6, \quad \theta' = (A'B'C'D') = \frac{1}{4} : \frac{1}{5} = 4.$$

Беря композицию линейного отображения φ с α^* , получим коллинеацию плоскости S ; однако эта коллинеация

$$\alpha^* \varphi: \begin{cases} \tau x'_1 = a_{11}x_1^3 + a_{12}x_2^3 + a_{13}x_3^3, \\ \tau x'_2 = a_{21}x_1^3 + a_{22}x_2^3 + a_{23}x_3^3, \\ \tau x'_3 = a_{31}x_1^3 + a_{32}x_2^3 + a_{33}x_3^3 \end{cases}$$

не будет гомографией.

Вообще, можно получить целое семейство коллинеаций плоскости, составляя композиции линейных отображений с отображениями, индуцированными автоморфизмами поля. Однако мы не можем быть уверенными в том, что каждая коллинеация плоскости получается таким путем. К этой проблеме мы еще вернемся в параграфе 2.17.

Пусть теперь число элементов поля K есть снова $q = p^r$. Если φ — невырожденное линейное отображение с коэффициентами $a_{jk} \in K$, то отображение

$$(2.15.1) \quad \psi_t: \begin{cases} \tau x'_1 = a_{11}x_1^{p^t} + a_{12}x_2^{p^t} + a_{13}x_3^{p^t}, \\ \tau x'_2 = a_{21}x_1^{p^t} + a_{22}x_2^{p^t} + a_{23}x_3^{p^t}, \\ \tau x'_3 = a_{31}x_1^{p^t} + a_{32}x_2^{p^t} + a_{33}x_3^{p^t}, \end{cases}$$

где $0 \leq t \leq r-1$, является коллинеацией. Покажем, что из всех ψ_t только $\psi_0 = \varphi$ является гомографией.

Обозначая образ точки P при отображении ψ_t через P' , можем записать для любой четверки коллинеарных точек A, B, C, D равенство

$$(2.15.2) \quad (A'B'C'D') = (ABCD)^{p^t}.$$

Отсюда видно, что $(A'B'C'D') = (ABCD)$ лишь в случае $t = 0$ *).

2.16. Характеристика конечной проективной плоскости

Мы будем теперь интерпретировать характеристику поля $GF(q)$ свойством замкнутости некоторой фигуры в плоскости $S = S_{2,q}$. Эта фигура играет также важную роль в описании строения конечных плоскостей.

Рассмотрим точки

$$O = Q_0 (0, 0, 1), \quad X (1, 0, 0),$$

$$Y (0, 1, 0), \quad P_0 (1, 1, 1)$$

плоскости S (рис. 58); иначе говоря, $OXYP_0$ есть фигура отнесения плоскости S . Пусть $Z = OP_0 \cap XY$, т.е. $Z = (1, 1, 0)$. Прямые x, z и e , изображенные на рис. 58, задаются уравнениями $x_2 = 0$, $x_3 = 0$ и

$x_2 = x_3$ соответственно; прямая y имеет уравнение $x_1 = 0$.

Построим теперь многоугольник с $2p$ сторонами, где p есть характеристика координатного поля K , следующим образом.

Исходную точку Q_0 проектируем из Z на e , полученную точку P_0 — из Y на x , полученную точку Q_1 — из Z на e , полученную точку P_1 — из Y на x и так далее, т.е.

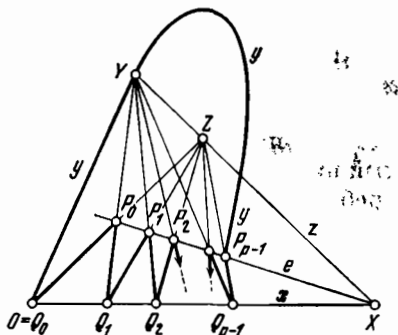


Рис. 58.

*) Чтобы получить (2.15.2), следует учесть, что в случае поля характеристики p выполняются равенства $(x + y)^{p^t} = x^{p^t} + y^{p^t}$ и $(xy)^{p^t} = x^{p^t}y^{p^t}$ (отображение $x \rightarrow x^{p^t}$ есть автоморфизм поля); следовательно, если точки A, B, C, D плоскости S связаны соотношениями $C = \lambda A + \mu B$, $D = \rho A + \sigma B$, то их образы A', B', C', D' связаны соотношениями $C' = \lambda^{p^t}A' + \mu^{p^t}B'$, $D' = \rho^{p^t}A' + \sigma^{p^t}B'$. — Прим. перев.

проектируем попеременно из Z и Y на e и x . Координаты каждой точки получаемой последовательности легко определяются по координатам предыдущей точки. Таким путем после $p - 1$ шагов получаем точки

$$P_{p-2} (p - 1, 1, 1) \text{ и } Q_{p-1} (p - 1, 0, 1).$$

Рассмотрим теперь точку $P_{p-1} = XP_0 \cap ZQ_{p-1}$. Очевидно, $P_{p-1} (p, 1, 1) = (0, 1, 1)$, поскольку поле K имеет характеристику p . Тогда $Q_p = XQ_0 \cap YP_{p-1} = Q_0$. Таким образом, рассматриваемый процесс замыкается после $2p$ проектирований. Особого рода многоугольник с $2p$ сторонами, получаемый указанным способом, будем обозначать P_0 . На рисунке он изображен с помощью жирных линий.

Мы могли бы провести такое же построение, исходя из любого собственного четырехугольника $O^*X^*Y^*P_0^*$, и получить многоугольник подобного же вида. Это очевидно, поскольку существует коллинеация ψ (ср. 2.6), которая преобразует четырехугольник $O^*X^*Y^*P_0^*$ во взятый нами первоначально четырехугольник $OXY P_0$, и тогда требуемый многоугольник есть образ P_0 при отображении ψ^{-1} .

Для краткости обозначим исходный четырехугольник через N , а рассматриваемую конструкцию, начинающуюся с него, через $\pi(N)$ или (там, где это не может вызвать недоразумений) просто π ; замкнутый многоугольник, порожденный описанным процессом, обозначим P (т. е. $\pi(N) = P$). Из способа построения P ясно, что четырехугольник N можно однозначно восстановить по данному многоугольнику P .

Многоугольник P можно описать следующим образом. Его вершины образуют последовательность из $2p$ точек $P_0, Q_0, P_1, Q_1, \dots, P_{p-1}, Q_{p-1}$ такую, что

- (а) последовательности P_0, P_1, \dots, P_{p-1} и Q_0, Q_1, \dots, Q_{p-1} лежат соответственно на прямых e и x ;
- (б) прямые $P_0Q_0, P_1Q_1, \dots, P_{p-1}Q_{p-1}$ пересекаются в точке Z , а прямые $P_0Q_1, P_1Q_2, \dots, P_{p-1}Q_0$ — в точке Y ;
- (с) точка $e \cap x = X$ совместно с точками Y и Z образует коллинеарную тройку точек.

Определенный таким образом многоугольник P , очевидно, порождается как раз четырехугольником $Q_0XY P_0$. Если дана проективная плоскость H (необязательно плос-

кость Галуа), то можно пытаться найти многоугольник P с такими свойствами. Допустим, что для данного четырехугольника N существует число p и многоугольник с $2p$ сторонами, удовлетворяющий условиям (а), (b) и (с). Если p — наименьшее число такого рода, то мы говорим, что на плоскости H выполняется условие « $p = 0$ » относительно данного четырехугольника N . Если же условие « $p = 0$ » выполняется для каждого собственного четырехугольника на плоскости с одним и тем же числом p , то мы говорим, что в плоскости H справедлива теорема « $p = 0$ » или что плоскость имеет характеристику p .

Если для четырехугольника N выполняется условие « $2 = 0$ », то N есть четырехугольник Фано. Если это же условие выполняется для каждого четырехугольника на плоскости H , то H называется плоскостью Фано. Структура плоскости Фано полностью описана Глисоном. Некоторые математики (особенно Ломбардо Радиче и Цалпа) рассматривали плоскости характеристики 3. Ломбардо Радиче высказал предположение, что все плоскости характеристики p являются плоскостями Галуа.

Вернемся, однако, к случаю плоскости Галуа (снова будем пользоваться рис. 58).

Если исключить из прямых e и x четырехугольника $Q_0XYP_0 = N_0$ все точки P_i и Q_j ($i, j = 0, 1, \dots, p-1$), то на каждой из этих прямых останется $q - p + 1$ точек. Выберем какую-нибудь одну из оставшихся точек прямой x ; обозначим ее Q_0^s , где $s > p - 1$. Пусть P_0^s будет проекция Q_0^s из точки Z на прямую e . Проводя описанное выше построение, получим последовательность точек $(P_0^s, Q_0^s, P_1^s, Q_1^s, \dots, P_{p-1}^s, Q_{p-1}^s)$, где $P_i^s \in x$ и $Q_i^s \in e$ ($i = 1, \dots, p-1$); соответствующий многоугольник обозначим $P_{s,p}$. Таким путем можно разбить множество точек прямых e и x , отличных от точки X , на множества вершин p^{r-1} многоугольников, каждый из которых имеет p вершин на прямой e и p вершин на x . Обозначим эти многоугольники

$$P_0, P_p, P_{2p}, \dots, P_{(p^{r-1}-1)p}.$$

Очевидно, каждая вершина многоугольника P_0 является неподвижной точкой коллинеации α^* (индуцированной фробениусовским автоморфизмом α), которая переводит

каждую из точек Q_0, X, Y, P_0 системы отнесения в себя. Однако, вообще говоря, мы не можем сказать ничего определенного об образе многоугольника $P_{s,p}$ ($s \neq 0$) при коллинеации α^* . В частном случае, когда α^* есть коллинеация плоскости $S_{2,q}$, индуцированная автоморфизмом $x \rightarrow x^3$ поля $GF(9)$ ($q = 3^2$), многоугольник P_3 переходит в P_6 (а P_6 — в P_3).

Другой пример коллинеации α^* мы приведем для плоскости $S_{2,4}$. Используя таблицы операций, данные в параграфе 1.6, найдем, что α^* осуществляет следующую подстановку:

$$\alpha^*: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 13 & 12 & 18 & 19 & 21 & 20 & 14 & 15 & 17 & 16 \end{pmatrix},$$

где числа служат индексами точек (и прямых) на рис. 7 и 10. Например,

$$l_{15} = \{P_4, P_7, P_{13}, P_{16}, F_{18}\} \rightarrow l_{19} = \{P_5, P_7, P_{12}, P_{21}, P_{14}\}.$$

2.17. Множество коллинеаций плоскости Галуа в себя

Мы будем искать коллинеации плоскости Галуа характеристики p , для которых точки $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$, $(1, 1, 1)$ являются неподвижными точками. Очевидно, тождественное отображение ε есть одна из таких коллинеаций. Более того, в случае классической проективной плоскости никакая коллинеация, кроме тождественной, не оставляет на месте указанные четыре точки. В противоположность этому для плоскостей Галуа можно указать примеры нетождественных коллинеаций, удовлетворяющих поставленному условию. Таковы, скажем, коллинеации

$$(2.17.1) \quad \omega^0: \rho x_1^t = x_1^{p^t}, \quad \rho x_2^t = x_2^{p^t}, \quad \rho x_3^t = x_3^{p^t} \\ (t = 1, \dots, r-1)$$

плоскости S_{2,p^r} , индуцированные степенями автоморфизма $\omega: x \rightarrow x^p$ поля $K = GF(p^r)$.

Мы утверждаем, что не существует других коллинеаций, удовлетворяющих поставленному условию, кроме

$$(2.17.2) \quad \omega^0 = \varepsilon, \quad \omega^1, \quad \omega^2, \quad \dots, \quad \omega^{r-1}.$$

Прежде чем доказывать это положение, подчеркнем особо тот факт, что плоскость S_{2,p^r} над простым подполем

Р поля **K** есть (замкнутая) подплоскость плоскости $S_{2,q}$ над **K** и каждый автоморфизм $x \rightarrow x^{p^i}$ поля **K** индуцирует коллинеацию ω^i плоскости $S_{2,q}$, оставляющую на месте каждую точку подплоскости $S_{2,p}$. Это вытекает из того, что любой автоморфизм поля **K** переводит каждый элемент из **P** в себя.

В последующих рассуждениях мы будем ссылаться на рис. 59 и 60 и пользоваться обозначениями, введенными в начале предыдущего параграфа.

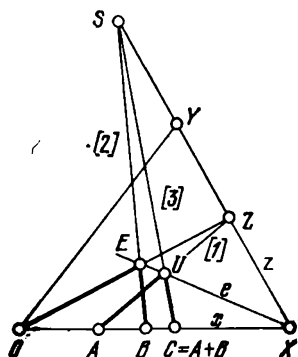


Рис. 59.

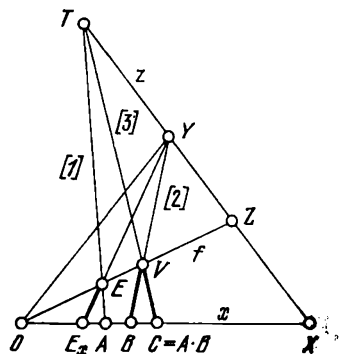


Рис. 60.

Рассмотрим точки $A(a, 0, 1)$ и $B(b, 0, 1)$ прямой x , а также определенную ими, в арифметическом смысле, точечную сумму

$$(2.17.3) \quad A + B = C = (a + b, 0, 1).$$

Точку C можно построить, исходя из A и B , следующим образом: пусть $ZA = [1]$ и $[1] \cap e = U$; пусть $BE = [2]$ и $[2] \cap z = S$; пусть $US = [3]$; тогда $[3] \cap x = C$. Назовем это линейное построение построением α .

Координаты точек, участвующих в построении, легко подсчитываются. Прямая e содержит все точки вида $(\xi, 1, 1)$, и так как $Z + A = (1, 1, 0) + (a, 0, 1) = (a + 1, 1, 1)$, то

$$U = (a + 1, 1, 1).$$

Прямая z содержит все точки вида $(\xi, 1, 0)$, и так как $E - B = (1, 1, 1) - (b, 0, 1) = (1 - b, 1, 0)$, то

$$S = (1 - b, 1, 0).$$

Все точки прямой x , кроме X , представимы в виде $(\xi, 0, 1)$, и так как $U - S = (a + 1, 1, 1) - (1 - b, 1, 0) = (a + b, 0, 1)$, то

$$C = (a + b, 0, 1),$$

что подтверждает правильность построения точки C .

Аналогично, рис. 60 показывает способ построения, исходя из A и B , точки

$$(2.17.4) \quad A \cdot B = C = (ab, 0, 1).$$

Построение можно осуществить так: пусть $AE = [1]$ и $[1] \cap z = T$; пусть $BY = [2]$, $OE = f$ и $[2] \cap f = V$; пусть $VT = [3]$; тогда $[3] \cap x = C$. Это построение обозначим μ .

Правильность такого способа построения точки C проверяется следующим образом. Имеем $T = (1 - a, 1, 0)$, так как $E - A = (1, 1, 1) - (a, 0, 1) = (1 - a, 1, 0)$. Прямая f содержит все точки вида $(\xi, \xi, 1)$, и так как $B + b \cdot Y = (b, 0, 1) + (0, b, 0) = (b, b, 1)$, то

$$V = (b, b, 1).$$

Наконец, так как $V - b \cdot T = (b, b, 1) - (b - b \cdot a, b, 0) = (b \cdot a, 0, 1)$, то

$$C = (a \cdot b, 0, 1).$$

Пусть теперь ω^* — любая коллинеация, оставляющая на месте точки O , X , Y и E . Обозначая, как обычно, образ точки P через P' , будем иметь для точек прямой x $(A + B)' = A' + B'$ и $(A \cdot B)' = A' \cdot B'$. Это означает, что действие коллинеации ω^* на точки A $(a, 0, 1)$ прямой x совпадает с действием (на элементы a) некоторого автоморфизма координатного поля K . Итак, действие коллинеации ω^* , оставляющей неподвижными точки O , X , Y и E , на прямую x совпадает с действием на эту прямую коллинеации, индуцированной автоморфизмом ω^i координатного поля K .

Легко видеть, что точка $W(-1, 1, 0)$ может быть получена из фундаментальной фигуры линейным построе-

нием: а именно, она является точкой пересечения прямой XU с прямой, соединяющей точки $XE \cap OY$ и $YE \cap OX$ (рис. 61). Отсюда следует, конечно, $\omega^*(W) = W$. Значит, образ прямой $l = AW$ есть прямая $A'W = l'$, а образ точки $\check{A} = OY \cap l$ — точка $OY \cap l' = \check{A}'$. Если координаты точек A и A' суть $(a, 0, 1)$ и $(a', 0, 1)$ соответственно, то координаты точек \check{A} и \check{A}' можно найти следующим путем:

$$\begin{aligned} a \cdot W + A &= (-a, a, 0) + \\ &+ (a, 0, 1) = (0, a, 1) = \check{A}, \\ a' \cdot W + A' &= (-a', a', 0) + \\ &+ (a', 0, 1) = (0, a', 1) = \check{A}'. \end{aligned}$$

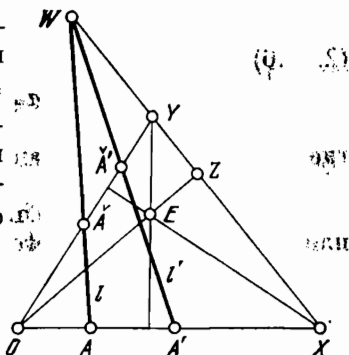


Рис. 61.

Это показывает, что действие коллинеации ω^* на прямую $OY = y$ совпадает с действием на эту прямую коллинеации, индуцированной указанным выше автоморфизмом ω^t .

Пусть теперь $P = (a, b, 1)$ есть общая точка прямой, проектирующей точку $A(a, 0, 1)$ из Y , и прямой, проектирующей точку $B(0, b, 1)$ из X . Пусть $A'(a', 0, 1)$ и $B'(0, b', 1)$ — образы точек A и B ; тогда из двух последних утверждений следует, что $P'(a', b', 1)$ есть образ точки P как при коллинеации ω^* , так и при коллинеации, индуцированной указанным выше автоморфизмом. Следовательно, коллинеация ω^* сама индуцируется автоморфизмом поля K . Этим доказано утверждение (2.17.2).

Рассмотрим теперь линейное отображение λ , переводящее вершины собственного четырехугольника $N = OXYE$ в вершины данного собственного четырехугольника $N' = O'X'Y'E'$, и коллинеацию ϕ , удовлетворяющую тому же условию, но не обязательно совпадающую с λ . Очевидно, отображение

$$(2.17.5) \quad \psi = \phi\lambda^{-1}$$

есть коллинеация, оставляющая каждую из точек O, X, Y, E на месте, т. е. коллинеация, индуцированная

некоторым автоморфизмом поля K . Отсюда следует, что каждая коллинеация плоскости $S_{2,q}$ на себя может быть представлена следующим образом:

$$(2.17.6) \quad \begin{cases} \rho x'_1 = a_{11}x_1^{p^t} + a_{12}x_2^{p^t} + a_{13}x_3^{p^t}, \\ \rho x'_2 = a_{21}x_1^{p^t} + a_{22}x_2^{p^t} + a_{23}x_3^{p^t}, \\ \rho x'_3 = a_{31}x_1^{p^t} + a_{32}x_2^{p^t} + a_{33}x_3^{p^t}, \end{cases} \quad (t=0, 1, \dots, r-1),$$

где определитель, составленный из коэффициентов a_{jh} , не равен нулю.

В заключение подсчитаем число всех коллинеаций плоскости $S_{2,q}$. Для этого нам нет нужды обращаться к (2.17.6), воспользуемся простыми комбинаторными соображениями. Существует ровно одно линейное отображение, переводящее данный (упорядоченный) собственный четырехугольник $OXUE$ в любой другой данный (упорядоченный) собственный четырехугольник $O'X'Y'E'$. Следовательно, чтобы найти число линейных отображений, достаточно подсчитать, сколько собственных упорядоченных четырехугольников можно выбрать среди $q^2 + q + 1$ точек плоскости.

Точку O' можно выбрать $q^2 + q + 1$ различными способами. Если O' выбрана, то X' можно выбрать $q^2 + q$ различными способами. Если O' и X' выбраны, то за Y' можно принять любую точку, не лежащую на прямой $O'X'$, что дает q^2 способов. Наконец, если фиксированы O' , X' и Y' , то за Z' можно принять любую точку, не принадлежащую прямым $O'X'$, $O'Y'$, $X'Y'$, что дает $q^2 + q + 1 - [3(q + 1) - 3] = (q - 1)^2$ способов. Таким образом, число упорядоченных собственных четырехугольников, а значит, и число всех линейных отображений равно

$$(q^2 + q + 1)(q + 1)q^3(q - 1)^2.$$

Если еще учесть, что существует ровно r автоморфизмов поля K , то получим, что число всех коллинеаций плоскости $S_{2,q}$ есть

$$(2.17.7) \quad r(q^2 + q + 1)(q + 1)q^3(q - 1)^2.$$

Легко видеть, что множество всех коллинеаций плоскости является группой. Число элементов этой группы

быстро возрастает с ростом порядка плоскости. Например, для плоскости Галуа порядка 9 порядок группы коллинеаций равен (см. (2.17.7)) $84\,913\,920^*)$.

2.18. Декарговы конечные плоскости

В этом параграфе мы будем рассматривать плоскости, для которых справедлива система аксиом **ID**, объединяющая систему аксиом **I** и теорему Декарга. Начиная с этого момента плоскость порядка q , удовлетворяющую

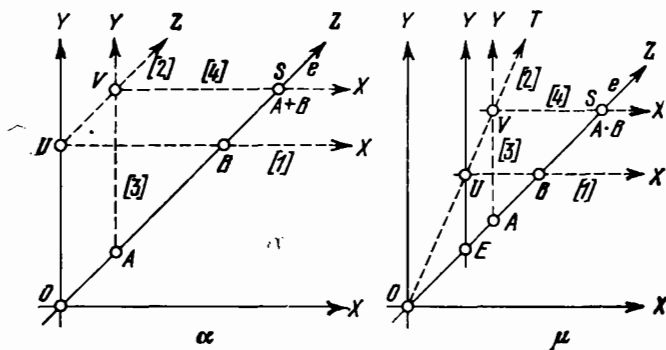


Рис. 62.

ID, будем обозначать $D_{2,q}$. Наша цель — показать эквивалентность понятия плоскости $S_{2,q}$ (определенного арифметическим путем) и понятия плоскости $D_{2,q}$ (введенного геометрически).

1° Согласно аксиомам I_1, I_2, I_3 существуют четыре точки, скажем,

$$A_1 (=O), \quad A_2 (=X), \quad A_3 (=Y) \text{ и } E,$$

никакие три из которых не лежат на одной прямой. На рис. 62 изображен случай евклидовой плоскости (дополненной идеальными элементами), когда X и Y суть идеальные точки.

Пусть $OE = e$ и $Z = e \cap XY$. С помощью четырехугольника $OXYE$ можно определить на множестве

*) В оригинале ошибочно указано другое число. — Прим. перев.

$e^* = e \setminus Z$ две операции, называемые соответственно сложением и умножением.

Под сложением α точек A и B (в указанном порядке) понимается следующая конструкция, приводящая к точке, называемой $A + B$:

(2.18.1) Пусть $BX \cap OY = U$ и $UZ \cap AY = V$,
тогда $VX \cap OZ = A + B$.

Под умножением μ точек A и B (в указанном порядке) понимается следующая конструкция, приводящая к точке, называемой $A \cdot B$:

(2.18.2) Пусть $BX \cap EY = U$ и $UO \cap AY = V$,
тогда $VX \cap EO = A \cdot B$.

Сравним операции α и μ . В обоих случаях, исходя из данных точек, строятся (в обозначениях, данных на рис. 62) элементы $[1]$, U , $[2]$, $[3]$, V , $[4]$, S . Конструкция μ использует обе точки O и E , в то время как конструкция α использует только O . Роли точек Z и O в конструкции α берут на себя в конструкции μ точки O и E соответственно.

Наша программа будет состоять в следующем: из аксиом системы **ID** мы постараемся вывести, что операции α и μ задают на множестве e^* структуру *тела*. Сначала мы рассмотрим те аксиомы тела, справедливость которых на e^* вытекает из I_1 , I_2 и I_3 , а затем уже те, которые требуют присоединения теоремы Дезарга.

Следующие факты очевидны. Если в конструкции α положим $A = O$, то $V = U$, $[4] = [1]$ и, следовательно, $O + B = B$. Аналогично, если $B = O$, то $[1] = OX$, $U = O$; тем самым, $[2] = e$ и $V = A$, так что $A + O = A$. Если $A = O = B$, то $U = O = V$ и $[1] = OX = [4]$, $[3] = OY$; следовательно, $O + O = O$. В итоге имеем:

(A₁) Если $P \in e^*$, то $O + P = P + O = P$.

Таким же образом можно проверить два основных свойства операции μ :

(M₀) Если $P \in e^*$, то $O \cdot P = P \cdot O = O$.

(M₁) Если $P \in e^*$, то $E \cdot P = P \cdot E = P$.

Если даны точки S и A , то, обращая последовательность построений α , можно найти точку Q такую, что $A + Q =$

$= S$. Аналогично, если даны S и B , то можно найти такую точку P , что $P + B = S$. Такие же заключения справедливы в отношении конструкции μ , если только $A \neq O$, соответственно $B \neq O$. Таким образом, имеют место свойства:

(A₂) Если $C, S \in e^*$, то существуют единственная точка P и единственная точка Q такие, что $P + C = S$ и $C + Q = S$.

(M₂) Если $C, S \in e^*$ и $C \neq O$, то существуют единственная точка P и единственная точка Q такие, что $P \cdot C = S$ и $C \cdot Q = S$.

Чтобы проверить дальнейшие свойства, нам придется использовать теорему Декарта.

(A₃) Если $A, B, C \in e^*$, то справедливо соотношение $(A + B) + C = A + (B + C)$.

При доказательстве будем ссылаться на рис. 63.

Конструкция α участвует в рисунке четырежды: при построении точек $A + B$, $B + C$, $(A + B) + C$ и

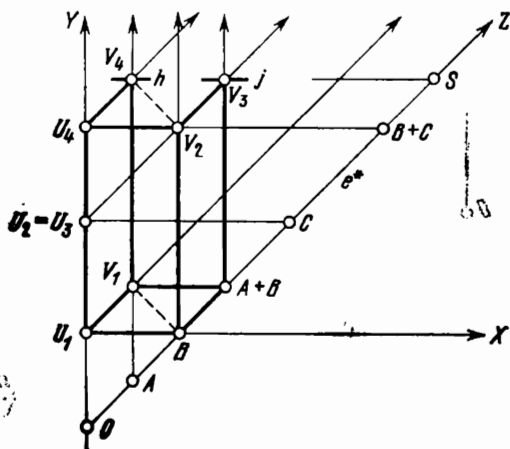


Рис. 63.

$A + (B + C)$. Последние две конструкции на рисунке не завершены *).

) Прямые h и j на рис. 63 проводятся на последнем этапе построения точек $A + (B + C)$ и $(A + B) + C$ (соответственно). Требуется доказать, что эти прямые совпадают и, следовательно, пересекают прямую e^ в одной и той же точке S — Приж. перев.

Чтобы доказать (A_3) , рассмотрим треугольники BU_1V_1 и $V_2U_4V_4$, которые перспективны относительно точки Y . Согласно теореме Дезарга пары соответствующих сторон пересекаются в трех коллинейрных точках X , Z и W , где $W = BV_1 \cap V_2V_4$. Таким образом, точки X , Z и W коллинейрны (на рисунке W есть идеальная точка). Рассмотрим теперь треугольники V_1B ($A + B$) и $V_4V_2V_3$, которые также перспективны относительно Y . Одна пара

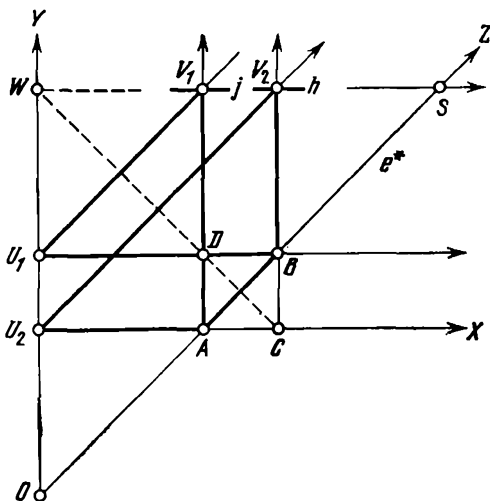


Рис. 64.

соответствующих сторон пересекается в точке W , другая — в точке Z ; следовательно, третья пара пересекается в точке, принадлежащей прямой WZ . Так как последняя прямая пересекает прямую V_1 ($A + B$) в точке X , то через эту точку пройдет и прямая V_3V_4 . Этим доказано (A_3) .

Доказательство следующего свойства снова опирается на теорему Дезарга. Соответствующие построения показаны на рис. 64.

(A_4) Для любых двух точек A и B из e^* имеем $A + B = B + A$.

Чтобы это доказать, рассмотрим точки $U_2X \cap BY = C$, $U_1X \cap AY = D$ и $V_1X \cap OY = W$. Треугольники ABC и V_1U_1W перспективны относительно оси XY ; соглас-

но теореме Декарта прямые U_1B , V_1A , DC , соединяющие соответственные точки, пересекаются в одной точке, а именно в точке D . Итак, прямая WC проходит через точку D . Рассмотрим теперь треугольники U_1V_1D и U_2V_2C , перспективные относительно оси XY ; по теореме Декарта прямые U_1U_2 , V_1V_2 , DC должны пересекаться в одной

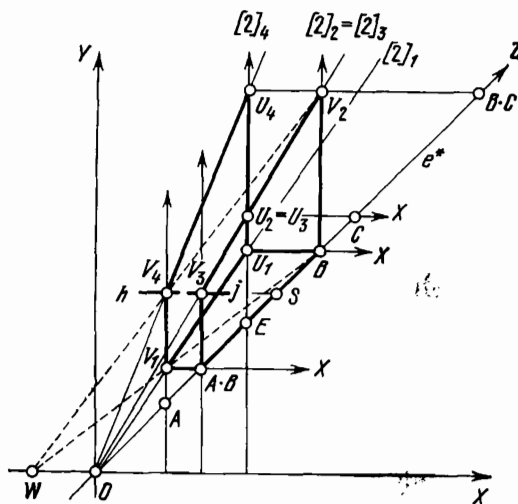


Рис. 65.

точке, а именно в точке W . Следовательно, точки V_1 , V_2 , W коллинеарны, т. е. прямые V_1X и V_2X совпадают. Это означает, что $A + B = V_1X \cap e^* = V_2X \cap e^* = B + A$.

Таким образом, операция сложения α на множестве e^* удовлетворяет (A_1) , (A_2) , (A_3) и (A_4) , т. е. относительно этой операции e^* является коммутативной группой.

(M_3) Если A , B , C — три точки из e^* , то

$$(A \cdot B) \cdot C = A \cdot (B \cdot C).$$

Доказательство этого утверждения иллюстрируется рис. 65. Оно подобно доказательству (A_3) .

На рис. 65 конструкция μ применяется четырежды, а именно для построения точек

$$A \cdot B, B \cdot C, (A \cdot B) \cdot C, A \cdot (B \cdot C).$$

Рассмотрим треугольники BU_1V_1 и $V_2U_4V_4$, которые перспективны относительно точки Y . Согласно теореме Дезарга соответственные стороны пересекаются в точках, лежащих на одной прямой; следовательно, точка $W = BV_1 \cap V_2V_4$ лежит на прямой OX . Рассмотрим теперь треугольники $(A \cdot B)BV_1$ и $V_3V_2V_4$, которые перспективны относительно Y ; из теоремы Дезарга следует, что прямая WO должна содержать точку пересечения прямых V_3V_4 и $(A \cdot B)V_1$. Но последняя прямая пересекает WO в точке X , значит, прямая V_3V_4 проходит через X , откуда и следует наше утверждение.

Итак, операция μ на множестве $e^* \setminus O$ удовлетворяет (M_1) , (M_2) и (M_3) , т. е. относительно этой операции $e^* \setminus O$ является группой.

Если мы сравним систему аксиом, определяющую тело, с установленными выше свойствами

$$(A_1), (A_2), (A_3), (A_4), (M_1), (M_2), (M_3),$$

то обнаружим следующее: для установления того, что $(e^*; \alpha, \mu)$ есть структура тела, достаточно проверить выполнение аксиом правой и левой дистрибутивности.

Сейчас мы только сформулируем недостающие свойства; их доказательства будут даны после рассмотрения некоторых следствий из свойств (A) и (M) .

Мы должны доказать, что для любых трех точек A, B, C из e^* справедливы равенства

$$(D_1) \quad A \cdot (B + C) = A \cdot B + A \cdot C$$

и

$$(D_2) \quad (B + C) \cdot A = B \cdot A + C \cdot A.$$

Заметим, что при доказательстве свойств (A) и (M) мы не рассматривали специально случаи совпадения точек; однако наши утверждения верны и в этих случаях, что легко докажет сам читатель.

2° Свойств (A) и (M) уже достаточно для введения координатной системы на плоскости и, в какой-то степени, для развития аналитического подхода к геометрии плоскости.

Будем обозначать (как это сделано на рис. 66) фундаментальные точки X и Y координатной системы через *

и η ; соответственно и другие точки фундаментальных прямых OX и OY будут обозначаться греческими буквами.

Сравнивая рис. 62, иллюстрирующий определение операции α , и рис. 66, мы видим, что если зафиксировать точку B и заставить точку X пробегать множество e^* , то прямая $[2] = l$, участвующая в построении точки $X + B = Y$, остается неизменной. Более того, точка P , играющая роль вспомогательной точки V , будет пробегать

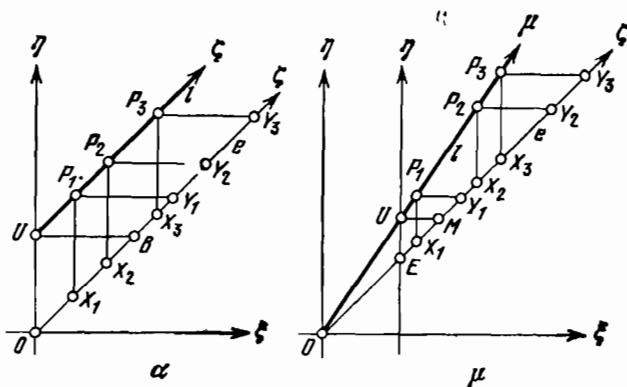


Рис. 66.

все точки прямой l , за исключением точки ζ . Таким образом, можно установить взаимно однозначное соответствие между точками прямой $U\zeta = l$ (исключая ζ) и упорядоченными парами (X, Y) точек прямой $O\zeta = e$ (также без ζ), удовлетворяющими соотношению $Y = X + B$; при этом соответствии, очевидно, $U = P_0 \rightarrow (O, B)$.

О п р е д е л е н и е. Точечными координатами точки $P \notin \xi\eta$ относительно системы координат $O\xi\eta E$ будем называть упорядоченную пару (X, Y) точек множества e^* таких, что

$$(2.18.3) \quad P = X\eta \cap Y\xi, \text{ где } X = P\eta \cap e, Y = P\xi \cap e.$$

Поскольку точки прямой $\xi\eta$ мы исключаем, то данное определение позволяет снабдить координатами лишь q^2 точек проективной плоскости порядка q .

Соответствие между точками P плоскости и упорядоченными парами (X, Y) аналогично введению координат (x, y) на обычной плоскости.

Возвращаясь к прямой l рис. 66, мы можем теперь сказать, что уравнение множества $l^* = l \setminus \xi$ есть

$$(2.18.4) \quad l^*: Y = X + B.$$

Очевидно, когда точка B пробегает все точки множества e^* , индуцированное ею множество l^* заполняет всю плоскость, за исключением точек прямой $\xi\eta$.

Аналогичные рассуждения можно провести для части рис. 66, иллюстрирующей операцию μ . Если зафиксировать точку M и заставить точку X пробегать множество e^* , то прямая $[2] = l$, участвующая в построении точки $X \cdot M = Y$, остается неизменной. Точка P , играющая роль вспомогательной точки V на рис. 62, будет пробегать все точки множества $l^* = l \setminus \mu$. Таким образом, можно установить взаимно однозначное соответствие между точками множества l^* и упорядоченными парами (X, Y) точек множества e^* , удовлетворяющими соотношению $Y = X \cdot M$; при этом соответствии, очевидно, $P_0 = U \rightarrow (E, M)$. Можно, следовательно, сказать, что уравнение множества l^* есть

$$(2.18.5) \quad Y = X \cdot M.$$

Если точка M пробегает все элементы множества e^* , индуцированное ею множество l^* заполняет всю плоскость, за исключением точек линий $O\eta$ и $\xi\eta$.

С помощью уравнений вида $Y = X + B$ и $Y = X \cdot M$ могут быть описаны лишь $2q - 1$ прямых плоскости. Рассматривая прямые, проходящие через точку η , но отличные от $\xi\eta$, мы видим, что их точки характеризуются условием постоянства первой координаты $x = A$, в то время как вторая координата пробегает все точки e^* . В этом смысле можно сказать, что уравнение любой из таких прямых есть

$$(2.18.6) \quad P\eta: X = A \quad (A \in e^*).$$

Таким образом, еще q прямых снабжаются уравнениями.

Введем теперь координаты прямой как упорядоченные пары точек.

О п р е д е л е н и е. Координатами прямой f , не проходящей через точку η , относительно системы координат $O\xi\eta E$ назовем упорядоченную пару $[M, B]$ точек множества

e^* , определяемых следующим построением (рис. 67):

$$(2.18.7) \quad \begin{cases} \mu = f \cap \xi\eta, \\ M = F\xi \cap e, \text{ где } F = E\eta \cap m, \quad m = O\mu, \\ B = U\xi \cap e, \text{ где } U = f \cap O\eta. \end{cases}$$

Очевидно, это построение может быть обращено, т. е. прямую f можно однозначно восстановить по данной паре $[M, B]$. Построение позволяет приписать координаты

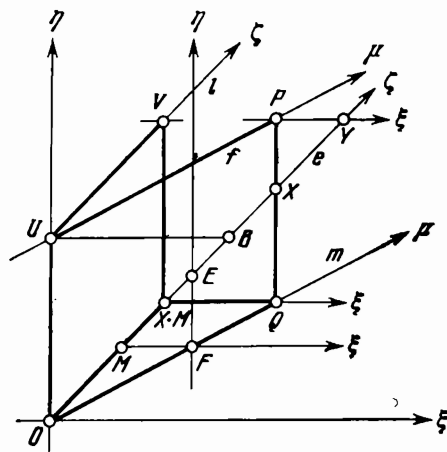


Рис. 67.

лишь таким прямым — их число есть q^2 , — которые не проходят через точку η . Отношение между координатами $[M, B]$ прямой f и точечными координатами (X, Y) любой точки этой прямой (исключая μ) выражается уравнением прямой f :

$$(2.18.8) \quad (L): Y = X \cdot M + B.$$

Справедливость (L) можно легко установить следующим путем (рис. 67). Прямая f и точка P определены соответственно парами точек $[M, B]$ и (X, Y) . При построении точки $X \cdot M$, исходя из X и M , роли точки U , прямой [2] и точки V играют соответственно точка F , прямая m и точка Q . При построении суммы $X \cdot M + B$ роль прямой [2] берет на себя прямая l . Таким образом, единственное, что нужно проверить, — это что точка $V\xi \cap e$ совпадает

с координатой Y точки P , т. е. что прямая VP проходит через точку ξ .

Для этого рассмотрим два перспективных треугольника $(X \cdot M) OQ$ и VUP . Одна пара соответствующих

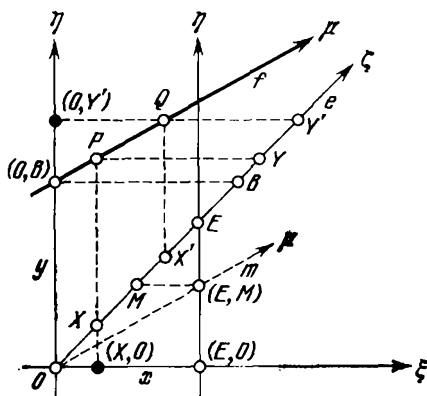


Рис. 68.

сторон пересекается в точке ξ , другая — в точке μ , т. е. в обоих случаях — на прямой $\xi\eta$. По теореме Дезарга прямая $\xi\eta$ является осью перспективности. Так как эта ось пересекает прямую $(X \cdot M) Q$ в точке ξ , то прямая VP должна проходить через ξ , что и требовалось доказать.

Очевидно, (2.18.4) и (2.18.5) суть частные случаи (2.18.8). Первый из них отвечает случаю $M = E$, второй — случаю $B = O$.

3° Используя свойства операций α и μ , можно ввести понятие *линейной функции точки* (рис. 68).

Пусть M и B — две точки из e^* . Прямая f , определяемая парой $[M, B]$, порождает линейную функцию $Y = f(X; M, B)$, где X и Y принадлежат e^* . Явное выражение для $f(X; M, B)$ есть $X \cdot M + B$. И обратно, функция такого вида порождает прямую, если M и B фиксированы.

Следуя обычной аналитической геометрии, мы называем прямые $O\xi$, $O\eta$ и точку E соответственно *осью x* , *осью y* и *единичной точкой* системы координат. Если дана прямая f и указана проекция одной из ее точек T на ось x

из точки η или же на ось y из точки ξ , то по этим данным точку T можно восстановить однозначно. Так, например, на рис. 68 точка P восстанавливается по (X, O) , а точка Q — по (O, Y) .

Теперь мы можем вернуться к доказательству свойств (D_1) и (D_2) .

Чтобы доказать свойство (D_1) , рассмотрим четыре прямые, заданные указанными ниже уравнениями:

$$u: Y = X \cdot C,$$

$$v: Y = X \cdot (B + C),$$

$$g: Y = X \cdot B + C,$$

$$f: Y = X \cdot B + A \cdot C$$

(рис. 69). Координаты точек $u \cap y_1 = Q$ и $u \cap y_2 = Q'$ (определяемые из уравнения прямой u) суть $(E, E \cdot C) =$

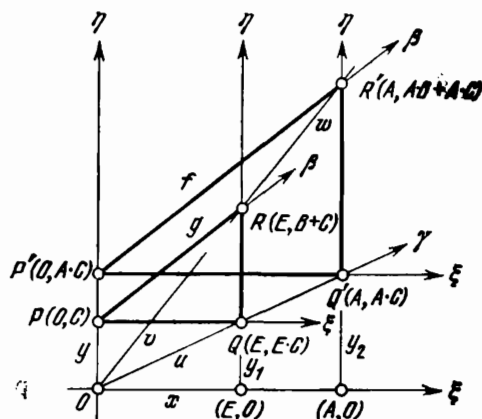


Рис. 69.

$= (E, C)$ и $(A, A \cdot C)$ соответственно. Аналогично, из уравнений прямых g и f можно найти координаты точек

$$P = g \cap y, \quad P' = f \cap y, \quad R = g \cap y_1, \quad R' = f \cap y_2;$$

эти координаты указаны на рисунке. Поскольку первые координаты прямых g и f обе равны B , точка $g \cap f$ лежит на прямой $\xi\eta$ (на рисунке эта точка обозначена β). Таким

а именно:

$$\begin{aligned} C' &= (C, C \cdot A), & D' &= (B + C, (B + C) \cdot A), \\ U' &= (O, C \cdot A), & V' &= (B, B \cdot A + C \cdot A). \end{aligned}$$

Сравнивая первые члены уравнений для e и l с первыми членами уравнений для s и f , замечаем, что обе точки $e \cap s = \xi$ и $l \cap f = \lambda$ лежат на прямой $\xi\eta$. Таким образом, треугольники VUU' и DCC' (где $D = B + C$, как показано на рисунке) перспективны относительно точки ξ , откуда по теореме Декарта следует, что точки η , ξ и $d_1 \cap d_2 = \delta$ (где $d_1 = U'V$ и $d_2 = DC'$) коллинеарны. Но тогда треугольники $VU'V'$ и $DC'D'$ перспективны относительно оси $\xi\eta$, поскольку соответствующие прямые пересекаются в точках δ , λ , η , лежащих на этой оси. По теореме Декарта отсюда находим — учитывая $VD \cap U'C' = \xi$, — что прямая $V'D'$ проходит через точку ξ . Но тогда вторые координаты точек D' и V' совпадают, т. е. $(B + C) \cdot A = B \cdot A + C \cdot A$, что и требовалось доказать.

Итогом наших рассуждений является следующая

Т е о р е м а. *Операции α , μ относительно заданного собственного четырехугольника $O\xi\eta E$ определяют на множестве e^* структуру тела.*

В действительности эта структура является даже структурой поля. Это следует из хорошо известной теоремы Веддербарна, которая утверждает, что операция умножения в конечном теле всегда коммутативна. Следовательно, (2.18.8) можно записать по-другому в виде

$$Y = M \cdot X + B.^1$$

Это уравнение аналогично уравнению $y = mx + b$ прямой в обычной аналитической геометрии.

4° Рассмотрим плоскость Галуа $S_{2,q}$ над координатным полем K порядка q . Сопоставим точкам

$$A_3(0, 0, 1), \quad E(1, 1, 1), \quad A_1(1, 0, 0), \quad A_2(0, 1, 0)$$

этой плоскости точки

$$O, E, \xi, \eta$$

плоскости $D_{2,q}$. Пусть f — прямая в плоскости $S_{2,q}$, определяемая уравнением $u_1x_1 + u_2x_2 + u_3x_3 = 0$. Предположим, что f не проходит через точку A_2 , т. е. что

$u_2 \neq 0$. Рассмотрим точку $P(x_1, x_2, x_3)$, не лежащую на прямой A_1A_2 , т. е. удовлетворяющую условию $x_3 \neq 0$. Если мы положим

$$-\frac{u_1}{u_2} = m \in K, \quad -\frac{u_3}{u_2} = b \in K; \quad \frac{x_1}{x_3} = x \in K, \quad \frac{x_2}{x_3} = y \in K,$$

то каждая точка прямой f , кроме точки, для которой $x_3 = 0$, будет удовлетворять уравнению

$$y = mx + b.$$

В частности, это означает, что существует взаимно однозначное соответствие Q между элементами поля K и точками прямой $y = x$ плоскости $S_{2,q}$, исключая точку $(1, 1, 0)$, а именно:

$$Q(x) = (x, x) \text{ для } x \in K.$$

Легко видеть, что точечные операции α и μ , порожденные четырехугольником $A_3EA_1A_2$, превращают множество точек (x, x) в поле K^* , изоморфное K .

В самом деле, обратимся к построениям, показанным на рис. 62.

В случае операции α , если $A(a, a)$ и $B(b, b)$, уравнение прямой [1] есть $y = b$ и $U(0, b)$; уравнение прямой [2] есть $y = x + b$, и уравнение [3] есть $x = a$, откуда следует $V(a, a + b)$; уравнение [4] есть $y = a + b$, и, следовательно, прямая $y = x$ пересекает ее в точке $S(a + b, a + b)$.

В случае операции μ имеем $E(1, 1)$, $A(a, a)$, $B(b, b)$, уравнение прямой [1] есть $y = b$ и $U(1, b)$, так что уравнение [2] есть $y = xb$, уравнение [3] есть $x = a$ и $V(a, ab)$; уравнение [4] есть $y = ab$, следовательно, прямая $y = x$ пересекает [4] в точке $S(ab, ab)$.

Мы видим, что операциям α и μ над точками соответствуют операции сложения и умножения над координатами этих точек, так что отображение Q поля K на K^* действительно является изоморфизмом.

Поскольку точечные операции, устанавливаемые при помощи четырехугольника $OE\xi\eta$, сообщают множеству e^* в плоскости $D_{2,q}$ структуру поля из q элементов и поскольку поля, имеющие одно и то же число элементов, изоморфны, приходим к заключению, что поле на множестве e^* изоморфно полю K^* , определенному выше.

Теперь становится очевидно, что $D_{2,q}$ и $S_{2,q}$ — две изоморфные структуры *), и, таким образом, *понятия дезарговой плоскости порядка q и плоскости Галуа порядка q эквивалентны*.

В заключение отметим, что для справедливости системы аксиом ID не обязательно требовать выполнения теоремы Дезарга (точнее, аксиомы Дезарга) в полной общности; достаточно потребовать, чтобы она выполнялась для некоторых специальных случаев. Действительно, в приведенных выше доказательствах была использована справедливость теоремы лишь в нескольких частных случаях. Но справедливость в этих частных случаях влечет за собой, как мы видим, справедливость теоремы Дезарга в общем виде; более того, с помощью теоремы Веддербарна получаем, что будет верна и более сильная аксиома Р (аксиома Паскаля — Паппа)**). Важность этих замечаний проявляется при изучении плоскостей, в которых существуют пары треугольников, перспективных относительно точки, но не перспективных относительно оси. Такие плоскости называются недезарговыми. Разумеется, на недезарговой плоскости могут встречаться и такие пары треугольников, для которых теорема Дезарга выполняется (пример такой плоскости фигурирует в упражнении 14).

2.19. Задачи и упражнения к главе 2

17. Пусть шесть различных точек $P_1, P_2, P_3, P_4, P_5, P_6$ плоскости Галуа выбраны так, что P_1, P_3, P_5 лежат на прямой u и P_2, P_4, P_6 — на прямой v , но при этом точка $u \cap v = Q$ не совпадает ни с одной из данных шести точек. Докажите, что точки $P_1P_2 \cap P_4P_5 = Q_1$, $P_2P_3 \cap P_5P_6 = Q_2$ и $P_3P_4 \cap P_6P_1 = Q_3$ отличны

*) Действительно, точки плоскостей $D_{2,q}$ и $S_{2,q}$ координатизируются парами (x, y) элементов одного и того же поля K , прямые также задаются парами $[m, b]$ элементов из K , и условие инцидентности точки и прямой в обоих случаях одинаково: $y = mx + b$. — *Прим. перев.*

**) Чтобы лучше ориентировать читателя, укажем, каковы, в конечном счете, взаимоотношения между понятиями. Понятие плоскости, удовлетворяющей аксиомам ID (т. е. аксиомам I и аксиоме Дезарга), эквивалентно понятию проективной плоскости над *телом*. Более узкое понятие плоскости, удовлетворяющей аксиомам IP (т. е. аксиомам I и аксиоме Паскаля — Паппа), эквивалентно понятию проективной плоскости над *полем*. В случае конечных плоскостей эти понятия идентичны, поскольку (по теореме Веддербарна) любое конечное тело есть поле. — *Прим. перев.*

от P_i ($i = 1, \dots, 6$), от Q , отличны друг от друга, а также что эти три точки лежат на одной прямой ω .

18. Пусть условия упражнения 17 усилены требованием коллинеарности точек Q, Q_1, Q_2 . Докажите тогда, что коллинеарность точек Q_1, Q_2, Q_3 можно вывести из аксиом системы ID.

19. Рассмотрим на плоскости Фано (т. е. на плоскости, удовлетворяющей системе аксиом I и теореме Фано) шесть точек P_1, \dots, P_6 , удовлетворяющих условиям упражнения 17. Докажите, что коллинеарность точек Q, Q_1, Q_2, Q_3 следует из аксиом системы IF.

В литературе встречается термин «конечная паскалева плоскость». Будем понимать под этим конечную плоскость, в которой выполняются аксиомы I и аксиома P, т. е. выполняются все аксиомы системы IP. Доволение аксиомы P влечет за собой следующее: тройка точек Q_1, Q_2, Q_3 , построенных по точкам P_1, \dots, P_6 из упражнения 17, коллинеарна.

20. Докажите, что на паскалевой плоскости справедлива следующая теорема T: если из шести точек $P_1, P_2, P_3, P_4, P_5, P_6$ не более чем две коллинеарны и прямые P_1P_2, P_3P_6 и P_4P_5 имеют общую точку W_1 , а прямые P_1P_4, P_2P_3 и P_5P_6 — общую точку W_2 , то прямые P_1P_6, P_2P_5, P_3P_4 также имеют общую точку.

Из упражнения 20 вытекает, что теорема T есть просто переформулированная теорема P. В некоторых случаях удобнее пользоваться теоремой T.

21. На проективной плоскости порядка 5 для любого овала существует 10 «внутренних» точек и 10 «внешних» прямых. Докажите, что 10 внутренних точек лежат по три на каждой «внешней» прямой и что эти 10 точек являются точками дезарговой конфигурации, т. е. 6 из 10 точек являются вершинами двух перспективных треугольников, одна точка есть центр перспективности, а три остальных точки лежат на оси перспективности.

22. Рассмотрим точки

$$B_1(0, b_1, 1), \quad B_2(1, 0, b_2), \quad B_3(b_3, 1, 0),$$

$$C_1(0, c_1, 1), \quad C_2(1, 0, c_2), \quad C_3(c_3, 1, 0)$$

плоскости Галуа порядка $q > 4$; пусть

$$b_j \neq c_j \quad \text{и} \quad b_j c_j \neq 0 \quad (j = 1, 2, 3).$$

Докажите, что данные шесть точек удовлетворяют уравнению второй степени тогда и только тогда, когда $a_1 a_2 a_3 b_1 b_2 b_3 = 1$.

23. Докажите, что в плоскости $S_{2,q}$ справедлива теорема Паскаля — Паппа.

24. Выведите из последнего утверждения, что теорема T верна в плоскости $S_{2,q}$.

25. Докажите, что точечная операция μ на плоскости $D_{2,q}$ коммутативна *).

*) Это — очень трудная задача, если не ссылаться на теорему Веддербарна. Дело в том, что любое геометрическое доказательство должно использовать конечность плоскости. Весьма неясно, как это осуществить. — *Прим. перев.*

ГЕОМЕТРИЧЕСКИЕ КОНФИГУРАЦИИ И СЕТИ

В этой небольшой главе мы будем иметь дело с понятиями, которые возникли из наглядных построений, но впоследствии получили абстрактное истолкование и приобрели важную роль в построении теории конечных плоскостей.

3.1. Понятие геометрической конфигурации

Пусть дана таблица $m \times n$ из m строк и n столбцов. Если в некоторых ее клетках содержится знак инцидентности \bullet , а остальные клетки пусты, то эта таблица называется *таблицей инцидентности*. Конфигурации Σ_1 , Σ_2 , Σ_3 на рис. 71 являются таблицами инцидентности.

Исходя из множества столбцов таблицы инцидентности, можно каждой строке таблицы сопоставить подмножество этого множества, а именно подмножество тех столбцов, которые содержат знак инцидентности в рассматриваемой строке. Если не сделано каких-либо оговорок, то строки будем нумеровать числами от 1 до m , а столбцы — числами от 1 до n . Тогда получается, например, что таблица Σ_1 на рис. 71 задает в множестве $\{1, 2, 3, 4, 5, 6\}$ следующую систему подмножеств: $\{1, 2, 3\}$, $\{1, 2, 5\}$, $\{1, 3, 4\}$, $\{2, 3, 6\}$, $\{2, 5, 6\}$, $\{3, 4, 6\}$, $\{1, 4, 5\}$, $\{4, 5, 6\}$.

Сравним теперь три таблицы инцидентности на рис. 71. Произведем в таблице Σ_1 следующую перестановку столбцов:

$$\omega = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 5 & 4 & 6 \end{pmatrix},$$

а затем — следующую перестановку строк:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 7 & 5 & 6 & 2 & 3 & 4 & 8 \end{pmatrix}.$$

Композиция этих двух перестановок является примером *элементарного преобразования*, и это преобразование τ переводит Σ_1 в Σ_2 : $\tau(\Sigma_1) = \Sigma_2$. Легко видеть, что таблицу Σ_3 нельзя получить подобным преобразованием из Σ_1 или из Σ_2 . Действительно, в системе восьми подмножеств, соответствующих строкам Σ_3 , имеется подмножество

1	2	3	4	5	6
1	•	•	•		
2	•				•
3	•		•		
4		•	•		•
5	•			•	•
6		•	•		•
7	•			•	•
8			•	•	•

Σ_1

1	2	3	5	4	6
1	•	•	•		
7			•	•	
5	•		•	•	•
6			•	•	•
2	•	•	•		
3	•		•		•
4	•	•		•	•
8			•	•	•

Σ_2

1	2	3	4	5	6
1	•	•	•		
2	•		•		
3		•		•	
4		•	•		•
5				•	•
6	•		•		•
7	•			•	•
8			•	•	•

Σ_3

Рис. 71.

$\{1, 2, 4\}$, пересечение которого с каждым из остальных семи подмножеств не пусто. Это свойство сохраняется при элементарных преобразованиях. Однако в системе подмножеств для Σ_2 каждое подмножество не пересекается по меньшей мере с одним из остающихся семи подмножеств.

Две таблицы инцидентности, которые получаются одна из другой элементарными преобразованиями, называются *изоморфными*; в противном случае их называют *гетероморфными*. Говорят, что изоморфные таблицы определяют одну и ту же *структуру инцидентности*, тогда как гетероморфные таблицы инцидентности задают различные структуры.

Если в таблице инцидентности из m строк и n столбцов каждая строка содержит v знаков, а каждый столбец μ знаков инцидентности, то такая таблица называется *таблицей конфигурации* или, короче, *конфигурацией*. При этом *тип конфигурации* считается матрица

$$\begin{pmatrix} n & m \\ \mu & v \end{pmatrix}.$$

Число $J = mv = n\mu$ является, очевидно, общим числом знаков инцидентности, содержащихся в таблице. Все три

конфигурации на рис. 71 имеют тип

$$\begin{pmatrix} 6 & 8 \\ 4 & 3 \end{pmatrix}.$$

Из этого примера видно, что тип мало что говорит о структуре конфигурации.

Конфигурация является *симметричной*, если $m = n$ (и, значит, $v = \mu$). Симметричная конфигурация показана на рис. 72. С другой стороны, все три конфигурации на рис. 71 не симметричны.

Фигуру на евклидовой плоскости, изображенную на рис. 72, можно отождествить с приведенной на том же

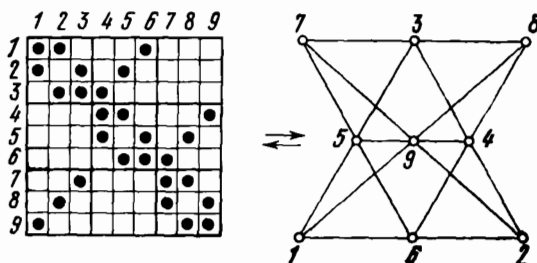


Рис. 72.

рисунке таблицей конфигурации, если сопоставить точкам фигуры столбцы таблицы с теми же номерами, а прямым — соответствующие строки этой таблицы. Любая таблица, полученная подобным образом, во всякой своей подтаблице размером 2×2 имеет по крайней мере одну пустую клетку. Конфигурация, удовлетворяющая этому условию, называется *геометрической*. Разумеется, не всякая геометрическая конфигурация допускает реализацию на евклидовой или хотя бы на классической проективной плоскости. Действительно, рассмотрим какую-нибудь конечную проективную плоскость. Всякая такая плоскость представляет собой геометрическую конфигурацию, удовлетворяющую даже некоторым дополнительным условиям (эквивалентным аксиомам I_1 и I_2). Однако мы знаем, что даже плоскость порядка 2 не реализуема на классической проективной плоскости.

Пусть таблица конфигурации Σ есть таблица инцидентности из m строк и n столбцов. Выберем в этой таблице какие-нибудь m^* ($< m$) строк и n^* ($< n$) столбцов. В пересечении этих строк и столбцов получается m^*n^* клеток, которые вместе с содержащимися в них знаками инцидентности составляют таблицу Σ^* ; эта таблица, вообще говоря, не является таблицей конфигурации. Например, в случае таблицы на рис. 72 подтаблица, получаемая в пересечении строк и столбцов с номерами 4, 5, 6, есть таблица конфигурации, а подтаблица, образованная пересечением строк 1, 3, 9 и столбцов 1, 2, 6, таковой не является. Если подтаблица таблицы конфигурации Σ сама является таблицей конфигурации, то ее называют *подконфигурацией* Σ .

Одна из основных задач при исследовании конечной проективной плоскости заключается в том, чтобы установить, существуют ли у этой плоскости определенные подконфигурации и если существуют, то каково их число.

3.2. Пятиугольники, вписанные друг в друга

Мы рассмотрим теперь некоторые любопытные конфигурации на классической проективной плоскости. Кажущиеся, возможно, тривиальными, эти конфигурации, однако, часто приводят к простым и интересным интерпретациям абстрактных геометрических понятий.

Будем считать сторонами многоугольников $A = A_1A_2 \dots A_n$ и $B = B_1B_2 \dots B_n$ прямые $A_1A_2, A_2A_3, \dots, A_nA_1$ и $B_1B_2, B_2B_3, \dots, B_nB_1$ соответственно. Многоугольник будем называть *обыкновенным*, если никакие три его вершины не коллинеарны, и *особым* — в противном случае. Прямая, соединяющая две вершины многоугольника и не являющаяся его стороной, называется *диагональной прямой* или, более коротко, *диагональю*.

Если можно установить такое взаимно однозначное соответствие между сторонами многоугольника A и вершинами многоугольника B , что каждая сторона проходит через соответствующую вершину, то многоугольник A считается *описанным* относительно B , а многоугольник B — *вписанным* относительно A . Для этого отношения примем обозначение $A \succ B$.

На рис. 72 и 73 представлены таблицы инцидентности геометрических конфигураций одного и того же типа

$$\begin{pmatrix} 9 & 9 \\ 3 & 3 \end{pmatrix},$$

а также их геометрические реализации; легко видеть, однако, что эти таблицы гетероморфны. Рассмотрим на обоих рисунках треугольники

$$A = \{1, 2, 3\}, \quad B = \{4, 5, 6\}, \quad C = \{7, 8, 9\}.$$

В обоих случаях имеем

$$A \succ B \succ C \succ A.$$

Таблицы инцидентности не могут быть переведены одна в другую с помощью элементарных преобразований — в этом состоит их различие с комбинаторной точки зрения.

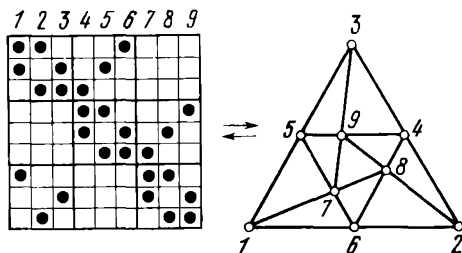


Рис. 73.

В то же время геометрические представления этих конфигураций на классической проективной плоскости позволяет понять, чем они отличаются также и геометрически. В самом деле, пусть треугольники A и B таковы, что $A \succ B$, и требуется построить треугольник C , удовлетворяющий условию $B \succ C \succ A$; тогда, в случае фигуры на рис. 72, одну из вершин треугольника C , скажем вершину 7, можно выбрать на прямой $\{5, 6\}$ произвольно, после чего две другие вершины 8 и 9 однозначно определяются, как это следует из теоремы Паскаля, примененной к шестиугольнику $1\ 9\ 2\ 4\ 6\ 5^*$). С другой стороны,

*) Это нужно понимать следующим образом: выбрав вершину 7, мы находим вершину $9=54 \cap 27$, а затем вершину $8=46 \cap 91$. Теорема Паскаля показывает, что вершина 8 принадлежит прямой 73, что обеспечивает выполнение условия $B \succ C \succ A$. — *Прим. перев.*

в случае фигуры на рис. 73, положение точки 7 на прямой $\{5, 6\}$ фиксировано. Действительно, при перемещении точки 7 по направлению к точке 5 точка $9 = 45 \cap 37$ также сместится в сторону точки 5, тогда как точка $8 = 46 \cap 17$ сдвинется к точке 4. Следовательно, при смещении точки 7 прямая $\{8, 9\}$ изменит свое положение и не пройдет через точку 2.

Пусть A и B — два треугольника на классической проективной плоскости, все шесть вершин которых — различные точки. Легко доказать, что отношения $A \prec B$ и $A \succ B$ не могут выполняться одновременно. Удивительно, однако, что для пятиугольников это возможно, т. е. *существуют два пятиугольника A и B , вписанные друг в друга.*

Мы докажем это утверждение, используя одну пространственную фигуру. Пусть в пространстве выбраны точки 1, ..., 5, никакие четыре из которых не лежат в одной плоскости (рис. 74). Рассмотрим пространственные пятиугольники $A = 1\ 2\ 3\ 4\ 5$ и $B = 1'\ 2'\ 3'\ 4'\ 5' = 1\ 3\ 5\ 2\ 4$. Обозначим их стороны через a_1, \dots, a_5 и b_1, \dots, b_5 соответственно. Стороны каждого из этих пятиугольников являются диагоналями другого. Десять сторон данных пятиугольников определяют десять треугольников. Пять из них имеют по две общих стороны с A и по одной с B , а остальные пять — по две общих стороны с B и по одной с A . Плоскости таких треугольников попарно различны. Так определенная пространственная конфигурация из 5 точек, 10 прямых и 10 плоскостей называется θ -конфигурацией. Исследуем теперь сечение θ -конфигурации плоскостью Σ , не проходящей ни через одну из ее вершин.

Пусть прямые a_j и b_j пересекают эту плоскость в точках A_j и B_j соответственно. Рассматривая прямые пересечения секущей плоскости с плоскостями конфигурации, мы сразу же замечаем, что имеется коллинеарная тройка из двух A -точек и одной B -точки, а также коллинеарная тройка из двух B -точек и одной A -точки. На рис. 75 показано, какого вида получается при этом фигура.

Этот рисунок свидетельствует о том, что для пятиугольников отношение $A \succ B \succ A$ действительно может выполняться. Кроме того, нетрудно доказать, что конфигурация, подобная данной, дезаргова. Так, например, осью

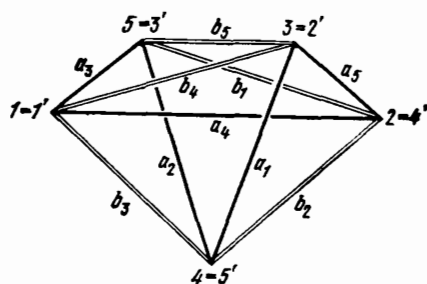


Рис. 74.

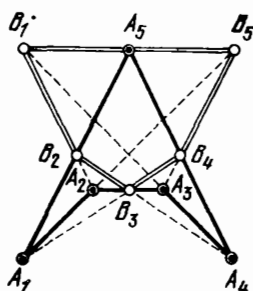


Рис. 75.

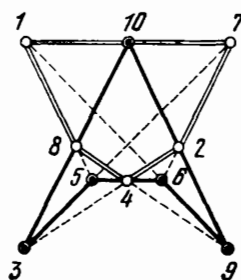


Рис. 76.

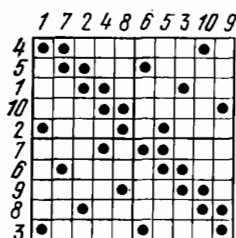


Рис. 77.

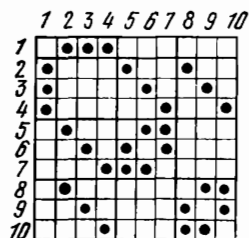


Рис. 78.

пары треугольников $A_2A_3B_5$, $B_2A_4A_5$, перспективных относительно точки B_1 , является прямая $B_4A_1B_3$.

Вершины конфигурации двойного пятиугольника на рис. 76 занумерованы числами от 1 до 10, и в соответствии с этой нумерацией на рис. 77 составлена таблица инцидентности данной конфигурации. Эта таблица наглядным образом выражает отношение между двумя пятиугольниками.

На рис. 78 представлена таблица инцидентности, полученная из предыдущей таблицы элементарными преобразованиями. Она позволяет судить о структуре конфигурации с несколько иной точки зрения, а именно считать, что конфигурация состоит из пары треугольников $\{5, 6, 7\}$ и $\{8, 9, 10\}$, перспективных относительно точки 1 и относительно оси $\{2, 3, 4\}$.

3.3. Теорема пятиугольника и дезаргова конфигурация

1° В связи с конфигурацией двойного пятиугольника можно получить некоторую теорему замыкания, эквивалентную теореме Дезарга. Обозначим сторону пятиугольника A , противоположную вершине A_k , через a_k ; аналогичные обозначения примем для пятиугольника B . Далее, проекцией (A, a) , $A \notin a$, будем считать преобразование, которое каждой точке $X \neq A$ ставит в соответствие точку $X' = AX \cap a$. Цепью проекций будем называть композицию некоторого числа проекций, в которой всякая очередная проекция применяется к точке, полученной от предыдущей проекции. Цепь проекций называется замкнутой, если каждую точку она переводит в себя; число проекций в замкнутой цепи называется длиной цепи. Теперь будет доказана следующая

Т е о р е м а п я т и у г о л ь н и к а. *Если теорема Дезарга верна, то цепь проекций*

$$(A_5, a_4), (A_3, a_2), (A_1, a_5), (A_4, a_3), (A_2, a_1)$$

переводит произвольную точку B_1 стороны a_1 пятиугольника A в ту же точку B_1 (рис. 75).

Д о к а з а т е л ь с т в о. В указанной цепи проекций первая проекция переводит точку B_1 в точку B_5 , вторая — точку B_5 в точку B_4 , третья — точку B_4 в точку B_3 , четвертая — точку B_3 в точку B_2 . Отсюда вытекает, что тре-

угольники $B_2A_2B_3$ и $A_5B_5B_4$ перспективны относительно центра A_1 . Но тогда ось перспективы является прямой $A_3A_4 = a_1$, причем сторона B_5A_5 треугольника $A_5B_5B_4$ пересекает эту ось в точке B_1 . Если теорема Дезарга верна, то сторона A_2B_2 треугольника $B_2A_2B_3$ должна пересекать ось в той же точке. А это как раз и означает, что проекция (A_2, a_1) переводит точку B_2 в исходную точку B_1 .

Можно сказать, что теорема пятиугольника представляет собой теорему Дезарга, переформулированную в виде некоторой теоремы замыкания. Возможна еще и такая формулировка: для любого пятиугольника A и любой точки на прямой a_1 найдется пятиугольник B , удовлетворяющий условию $A \succ B \succ A$ и притом такой, что одна из его вершин совпадает с данной точкой прямой a_1 .

2° Имея в виду расстановку знаков в таблицах инцидентности дезарговой конфигурации на рис. 77 и 78, мы будем говорить о распределениях Θ и Γ или, короче, о таблицах Θ и Γ соответственно. В каждой из этих таблиц содержится по 30 знаков инцидентности. Заметим, что конфигурация, не являющаяся геометрической, т. е. содержащая подтаблицу 2×2 , все клетки которой заполнены знаками инцидентности, не допускает реализации ни на какой проективной плоскости, поскольку две различные прямые проективной плоскости не могут пересекаться в двух различных точках.

В дальнейшем мы будем называть дезаргову конфигурацию (с таблицей, содержащей 30 знаков инцидентности) *обыкновенной дезарговой конфигурацией*.

Если теперь обратиться к таблице Γ на рис. 78, то можно заметить, что, поместив в ее левой верхней клетке тридцать первый знак инцидентности, мы получим *расширенную таблицу инцидентности*, которая снова является геометрической конфигурацией *). Однако, поместив тридцать первый знак инцидентности, скажем, в правую нижнюю клетку, мы придем к расширенной конфигурации, уже не являющейся геометрической. В этом смысле

*) Здесь и в дальнейшем термин «конфигурация» понимается несколько шире, чем в определении на стр. 204, а именно не предполагается, что в любых двух строках (столбцах) содержится одно и то же число знаков инцидентности. — *Прим. перев.*

можно говорить о *свободных* и *фиксированных* клетках исходной таблицы.

На рис. 79 указаны свободные клетки таблиц инцидентности рис. 78 и 77. Мы пока интересуемся возможностью расширения таблицы за счет одного знака инцидентности. Заметим, что каждая строка и каждый столбец таблицы имеют в точности одну свободную клетку.

При расширении исходной Г-таблицы путем введения в ее клетку, помеченную на рис. 79 цифрой 1, дополнительного знака инцидентности, мы приходим к *специальной дезарговой конфигурации*. Для краткости будем

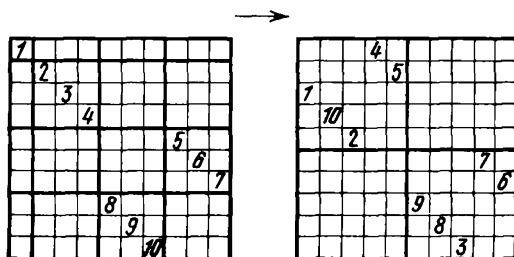


Рис. 79.

называть ее D_1 -конфигурацией. Сравнение моделей обыкновенной D -конфигурации и специальной D_1 -конфигурации показывает, что в первом случае каждая прямая состоит из трех точек и через каждую точку проходят три прямых, тогда как во втором случае имеется точка, через которую проходят четыре прямых, и имеется прямая, состоящая из четырех точек (на рис. 80 указанные точка и прямая выделены двойными линиями).

Для получения расширенной таблицы мы выбрали из 10 свободных клеток на рис. 79 клетку под номером 1. На самом деле выбор любой другой свободной клетки приводит к той же самой конфигурации. Действительно, любую из клеток с номерами 2, 3, ..., 10 можно перевести в левую верхнюю клетку с помощью такого элементарного преобразования, которое не меняет распределения первоначальных 30 знаков инцидентности, показанного на рис. 78. Например, поместив 31-й знак инцидентности

в клетку 9 и переставив строки согласно подстановке

$$\sigma = (7, 9, 4, 8, 3, 10, 2, 5, 1, 6),$$

а затем столбцы — согласно подстановке

$$\omega = (10, 6, 4, 5, 8, 1, 9, 3, 7, 2)^*,$$

мы получим распределение, совпадающее с распределением на рис. 80. Таким образом, добавление одного знака инцидентности дает единственную D_1 -конфигурацию.

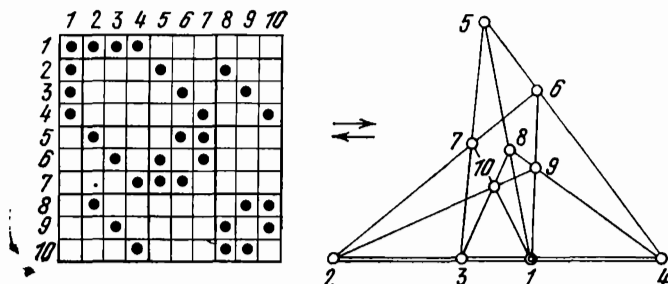


Рис. 80.

В таблице инцидентности D_1 -конфигурации на рис. 80 содержится на четыре свободных клетки меньше, поскольку после введения дополнительного знака инцидентности в клетку 1 клетки 2, 3, 4 (рис. 79) перестают быть свободными. Следовательно, дальнейшее расширение можно осуществлять, помещая новый знак инцидентности только в одну из клеток 5, 6, 7, 8, 9, 10. Здесь опять-таки несущественно, какая из этих шести клеток выбирается, так как в любом из шести случаев таблицу инцидентности можно подходящим элементарным преобразованием привести к виду, показанному на рис. 81. При этом происходит дальнейшая потеря свободных клеток; для последующего расширения свободными остаются лишь клетки 4, 7 и 10. Полученную в результате двойного расширения конфигурацию будем называть D_2 -конфигурацией.

На рис. 82 изображена реализация этой конфигурации. В ней имеются две точки, через которые проходят

*) Это сокращенная запись подстановки:

$(1, 2, 3, 4, 5, 6, 7, 8, 9, 10) \rightarrow (10, 6, 4, 5, 8, 1, 9, 3, 7, 2)$.

Аналогичное сокращение употребляется и далее. — *Прим. перек.*

четыре прямых, и две прямые, состоящие из четырех точек.

Если, однако, пытаться произвести дальнейшее расширение, то результат его будет зависеть от того, какая

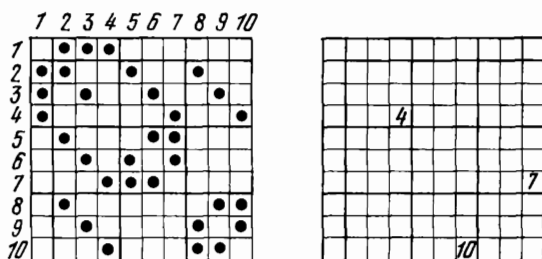


Рис. 81.

из клеток 4, 7, 10 выбирается. Точнее говоря, выбор любой из клеток 7, 10 дает одну и ту же конфигурацию, но эта

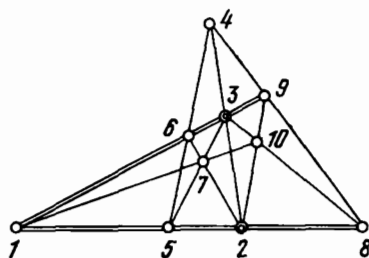


Рис. 82.

конфигурация не эквивалентна той, которая получается при расширении с помощью клетки 4.

Рассмотрим сначала расширение, получаемое с помощью клетки 7. Если знак инцидентности поместить в клетку 7, то клетка 4 перестает быть свободной и дальнейшее расширение возможно только за счет клетки 10 (рис. 83).

Получающаяся несимметрическая таблица инцидентности допускает реализацию на классической проективной плоскости.

Чтобы сделать отношение инцидентности более обозримым, можно преобразовать таблицу инцидентности в симметрическую таблицу. Это достигается с помощью следующих перестановок строк и столбцов:

$$\sigma = (10, 4, 5, 6, 1, 9, 8, 7, 2, 3),$$

$$\omega = (7, 4, 8, 9, 1, 6, 5, 10, 2, 3).$$

В результате этих преобразований мы приходим к фигуре, которую будем называть D_3 -конфигурацией; она содержит три особых точки, через которые проходит

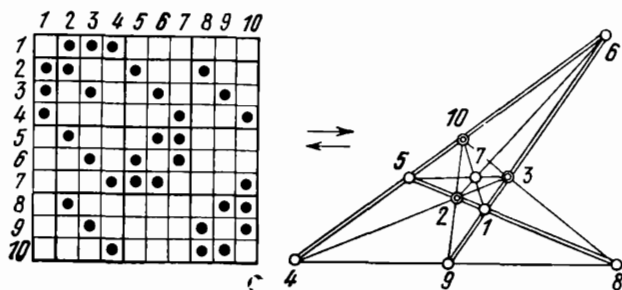


Рис. 83.

по четыре прямых, и три особых прямых, содержащих по четыре точки. Эта симметрическая таблица инцидентности представлена на рис. 84.

При расширении D_2 -конфигурации путем введения знака инцидентности в клетку 4 обе клетки 7 и 10 перестают быть свободными: в этом случае мы получаем *полную* конфигурацию (т. е. конфигурацию, любое дальнейшее расширение которой не будет уже геометрической конфигурацией, рис. 85). Подтаблица данной конфигурации, получающаяся в пересечении первых семи строк и столбцов, есть не что иное, как конфигурация Фано (конечная плоскость порядка два), откуда вытекает, что для этой конфигурации не существует модели из точек и прямых на классической проективной плоскости.

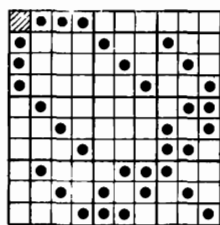


Рис. 84.

Построенную полную конфигурацию будем называть D_3^* -конфигурацией. В ней тоже содержится три прямых, состоящих из четырех точек, и три точки, через которые проходит по четыре прямых. Однако фигура, составленная из этих особых точек и прямых, отлична от соответствующей фигуры в случае D_3 -конфигурации. Можно также

сказать, что D_3^2 -конфигурация является расширением конфигурации Фано (F-конфигурации).

Вернемся теперь к таблице инцидентности D_3 -конфигурации, приведенной на рис. 84. Ее верхняя левая клетка

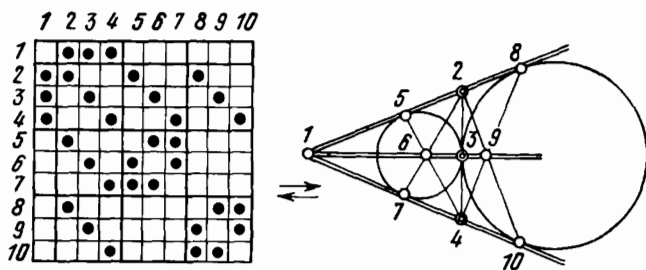


Рис. 85.

еще остается свободной. Поместив в нее знак инцидентности, мы получаем полную конфигурацию (рис. 86). Построенная D_4 -конфигурация содержит четыре прямых,

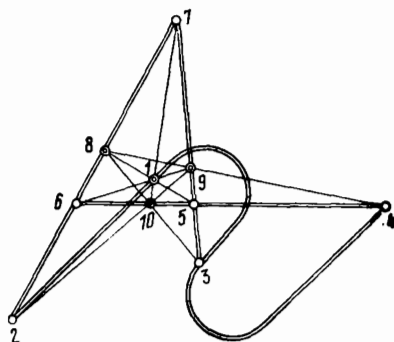


Рис. 86.

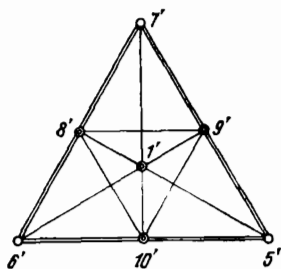


Рис. 87.

имеющих по четыре точки, и четыре точки, через каждую из которых проходят четыре прямых.

D_4 -конфигурация не имеет модели на классической проективной плоскости.

В самом деле, допустим, что плоскость π , рассматриваемая как плоскость трехмерного пространства, содержит такую модель. Пусть S — произвольная точка, не при-

надлежащая π . Спроектируем нашу модель из точки S на какую-нибудь плоскость, которая параллельна плоскости, проходящей через эту точку и прямую $l = \{1, 2, 3, 4\}$. Обозначим образ точки k через k' . Поскольку $1 \in l$, каждый из образов $1', 2', 3', 4'$ будет идеальной точкой. Следовательно, стороны треугольника-образа $8' 9' 10'$ и стороны описанного около него треугольника-образа $5' 6' 7'$ попарно параллельны (рис. 87). Это означает, что точка пересеченная $1'$ прямых $5' 8', 6' 9', 7' 10'$ является центром подобия указанных треугольников, т. е. не является идеальной точкой. Из полученного противоречия и следует наше утверждение.

Если обозначить исходную дезаргову конфигурацию через D_0 , то для конфигураций на рис. 78, 80, 82, 83, 85 и 86 принимаются соответственно обозначения $D_0, D_1, D_2, D_3, D_3^*$ и D_4^* . Нижний индекс показывает, сколько знаков инцидентности добавлено к исходным тридцати, а верхним индексом отмечены полные конфигурации. Говоря о «D-конфигурации», мы будем иметь в виду одну из конфигураций $D_0, D_1, D_2, D_3, D_3^*, D_4^*$.

3° Прямая D-конфигурации, содержащая четыре точки, называется *особой прямой*, и точка, через которую проходят четыре прямых, — *особой точкой* конфигурации. Особые точки и прямые сами составляют подконфигурации, а именно такие:

D_1 . Точка и содержащая ее прямая.

D_2 . Две точки, через каждую из которых проходит по одной прямой.

D_3 . Три точки, через каждую из которых проходит по одной прямой; эти точки и прямые задают перспективную пару треугольников с неособой точкой в качестве центра и неособой прямой в качестве оси.

D_3^* . Три прямые с общей (неособой) точкой, содержащие каждая по одной из трех точек одной (неособой) прямой.

D_4^* . Особые элементы D_3 -конфигурации, а также их ось и центр, лежащий на этой оси.

Мы уже видели, что D_3^* и D_4^* не имеют реализаций на классической проективной плоскости, но допускает ли каждая из этих конфигураций вообще реализацию на какой-либо плоскости? Мы покажем, что плоскость Галуа порядка четыре содержит D_3^* -конфигурацию, а плоскость Галуа порядка три — D_4^* -конфигурацию.

Рассмотрим таблицу на рис. 7 (стр. 22). Выберем строки с номерами

1, 2, 3, 6, 7, 8, 10, 11, 14, 16

и столбцы с номерами

1, 2, 3, 4, 6, 7, 8, 10, 11, 12.

Переставим их следующим образом:

6, 1, 2, 3, 7, 10, 11, 8, 14, 16

и

1, 2, 6, 10, 3, 7, 11, 4, 8, 12

соответственно. После такой перестановки в пересечении этих строк и столбцов получится таблица 10×10 , совпадающая с таблицей рис. 85.

Если же в таблице на рис. 8, *iii* (стр. 24) взять строки

1, 2, 3, 4, 6, 7, 8, 9, 11, 12

и столбцы

1, 2, 3, 4, 5, 7, 9, 10, 12, 13

и соответственно переставить их в порядке

1, 2, 3, 4, 7, 9, 12, 6, 8, 11

и

1, 2, 3, 4, 5, 10, 13, 7, 9, 12,

то в пересечении этих строк и столбцов получится таблица 10×10 , отношение инцидентности в которой полностью соответствует фигуре на рис. 86.

3.4. Понятие геометрической сети

В параграфе 1.5 мы видели, каким образом точки конечной плоскости могут быть параметризованы на ее евклидовой модели с помощью двух семейств прямых — семейства прямых, параллельных оси x , и семейства прямых, параллельных оси y . Мы ввели также «диагональное» семейство прямых конечной плоскости, изображаемых на евклидовой модели кривыми линиями. Это приводит нас к следующему определению.

Будем называть *сетью* множество n^2 элементов, называемых точками, если для этого множества выполнены следующие условия:

(i) Существуют три семейства подмножеств ξ , η , ζ , содержащих по n подмножеств, называемых прямыми, причем каждая прямая состоит из n точек.

(ii) Любые две прямые различных семейств имеют одну и только одну общую точку; любые две различные прямые одного семейства не имеют общих точек. (Таким образом, каждое семейство содержит все n^2 точек.)

(iii) Для любой точки в каждом семействе найдется единственная прямая, которой эта точка принадлежит.

Структуру сети можно изобразить в виде таблицы $n \times n$ следующим образом. Клетки таблицы будут представлять точки сети, ее строки — подмножества семейства ξ , ее столбцы — подмножества семейства

η , а ее n не имеющих общих клеток диагоналей — подмножества семейства ζ (под диагональю по-прежнему понимается набор из n клеток таблицы, по одной в каждой строке и каждом столбце). На рис. 88, например, наборы темных и светлых кружков изображают две непересекающиеся диагонали.

Выписывая по порядку для последовательных строк таблицы номера столбцов тех клеток, через которые проходит фиксированная диагональ, мы получим перестановку, однозначно определяющую эту диагональ. Так, диагонали из темных и светлых кружков на рис. 88 задаются соответственно перестановками

2, 1, 3, 4, 5, 7, 6, 9, 10, 8

и

6, 5, 4, 3, 2, 1, 10, 7, 8, 9.

Занумеровав прямые каждого семейства сети числами от 1 до n и записав в каждой клетке таблицы номер содержащей ее диагонали, мы получим, как легко видеть, латинский квадрат.

Числовая таблица, представляющая собой латинский квадрат, может быть истолкована как таблица некоторой

	1	2	3	4	5	6	7	8	9	10
1		●				○				
2	●				○					
3			●	○						
4			○	●						
5		○			●					
6	○						●			
7						●			○	
8							○			●
9								○		●
10								●	○	

Рис. 88.

операции, причем имеется несколько вариантов такого истолкования, каждому из которых отвечает своя операция. Поместив в заглавной строке и заглавном столбце таблицы какие-нибудь две перестановки чисел 1, 2, ..., n

\circ	1	2	3	4
1	1	2	4	3
2	4	3	1	2
3	2	4	3	1
4	3	1	2	4

U

\circ	1	2	3	4	5
1	1	2	3	4	5
2	2	3	1	5	4
3	5	4	2	1	3
4	3	5	4	2	1
5	4	1	5	3	2

V

Рис. 89.

(не обязательно одинаковые), мы зададим тем самым следующую операцию \circ на множестве этих чисел: если на пересечении строки с номером j и столбца с номером k

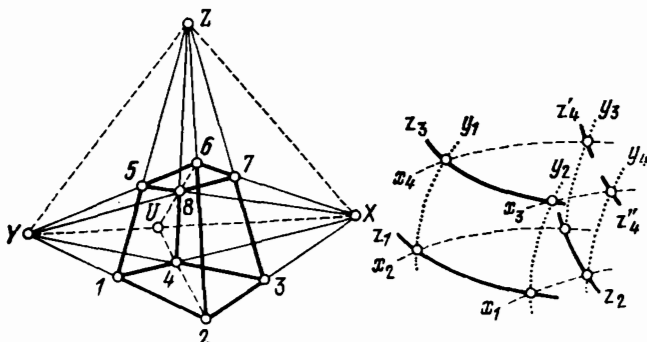


Рис. 90.

находится элемент s , то полагаем $j \circ k = s$. Рассмотрим, например, таблицы U и V на рис. 89. Операция, задаваемая таблицей U , не обладает ни левым, ни правым нейтральным элементом. В случае операции с таблицей V существует только левый нейтральный элемент, а именно элемент 1. Если бы в заглавном столбце таблицы V стояла перестановка 1 2 5 3 4, то элемент 1 был бы также и правым нейтральным элементом.

Рассмотрим конфигурацию, изображенную на рис. 90 и напоминающую центральную проекцию параллелепи-

педа. Возможен особый случай, когда точки X , Y и Z коллинеарны, но мы не приводим здесь соответствующей фигуры. Если исключить точку U вместе с тремя пересекающимися в ней прямыми, а также прямые XZ и YZ , то получится конфигурация из 11 точек и 12 прямых. Ее называют *конфигурацией Рейдемейстера* и обозначают символом R . В случае, когда точки X , Y и Z коллинеарны, говорят о микро-конфигурации Рейдемейстера и пользуются обозначением R_0^*).

Если в каждом из семейств ξ , η , ζ сети можно выбрать по четыре прямых с теми же отношениями инцидентности, что и в R_0 -конфигурации, то мы будем говорить о R_0 -конфигурации данной сети.

Теперь можно поставить вопрос о том, *при каких условиях на проективной плоскости существует R -конфигурация или R_0 -конфигурация*. Этот вопрос тесно связан с выполнимостью соответственно теоремы Дезарга и того ее частного случая, когда центр перспективы пары треугольников лежит на оси; указанный частный случай будем называть микро-теоремой Дезарга и обозначать MD .

Возьмем на плоскости три различные точки X , Y и Z . Выберем какую-нибудь точку 1, не коллинеарную ни с какими двумя из них. Выберем еще по одной точке на каждой из прямых $1X$, $1Y$ и $1Z$. Пусть это будут соответственно точки 4, 2 и 5. Рассмотрим следующие прямые и точки:

$$2X, 4Y, 2X \cap 4Y = 3; \quad 5Y, 2Z, 5Y \cap 2Z = 6;$$

$$5X, 4Z, 5X \cap 4Z = 8; \quad 6X, 8Y, 6X \cap 8Y = 7.$$

Если добавить сюда еще прямую 37 и если прямая 37 пройдет через точку Z , то получится либо R -, либо R_0 -конфигурация.

Если на плоскости выполняется D -теорема (соответственно MD -теорема), то, в силу перспективности треугольников 1 2 4 и 5 6 8 относительно точки Z , точки U , X и Y коллинеарны. Но так как треугольники 2 4 3 и 6 8 7 перспективны относительно оси XU , то точка Z лежит на прямой 37. Итак, R -конфигурация и R_0 -конфигурация

*) Конфигурацию R_0 можно получить ортогональным проектированием параллелепипеда при условии, что проекции всех 12 сторон параллелепипеда — различные прямые.

могут существовать и на плоскостях, отличных от классической проективной плоскости.

По аналогии с R-конфигурацией на плоскости для сети также можно ввести понятие R-конфигурации. В связи с этим для сети формулируется следующее условие (см. рис. 90): пусть $\{x_1, x_2, x_3, x_4\}$, $\{y_1, y_2, y_3, y_4\}$ и $\{z_1, z_2, z_3\}$ — любые подмножества семейств ξ , η и ζ сети; если $x_1 \cap y_2 \in z_1$, $x_2 \cap y_1 \in z_1$, $x_1 \cap y_4 \in z_2$, $x_2 \cap y_3 \in z_2$, $x_3 \cap y_2 \in z_3$, $x_4 \cap y_1 \in z_3$, а $x_4 \cap y_3 \in z'_4$ и $x_3 \cap y_4 \in z'_4$, то $z'_4 = z''_4 (= z_4)$ (условие Рейдемейстера). Сеть, удовлетворяющую этому условию, называют R-сетью.

Вернемся теперь к таблицам U и V на рис. 89. Выше уже отмечалось, что они существенно различны. Подчеркнем это различие также с еще одной точки зрения. Рассматривая латинские квадраты, соотнесенные сетям, как таблицы операций, мы можем исследовать, как истолковываются R-конфигурации в терминах этих таблиц.

Таблица задает на множестве $N = \{1, 2, \dots, n\}$ операцию \circ по такому правилу: если для $x_j, y_k, z_l \in N$ элемент z_l находится в пересечении строки с номером x_j и столбца с номером y_k , то $x_j \circ y_k = z_l$. Определение R-сети на языке таблицы операции выражается в следующем виде. Если

$$x_1 \circ y_2 = x_2 \circ y_1, \quad x_1 \circ y_4 = x_2 \circ y_3 \quad \text{и} \quad x_3 \circ y_2 = x_4 \circ y_1,$$

то

$$x_3 \circ y_4 = x_4 \circ y_3.$$

Это легко следует из того факта, что прямые семейств сети, отвечающие данному значению параметра $c (\in N)$, представляют собой множества клеток, удовлетворяющих соответственно условиям $x = c$, $y = c$, $x \circ y = c$.

Рассматривая латинские квадраты как матрицы, мы можем выразить свойство R также в следующей простой форме: если эта матрица имеет подматрицу

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

то в каждой ее подматрице вида

$$\begin{pmatrix} a & b \\ c & * \end{pmatrix}, \quad \begin{pmatrix} c & * \\ a & b \end{pmatrix}, \quad \begin{pmatrix} b & a \\ * & c \end{pmatrix} \quad \text{или} \quad \begin{pmatrix} * & c \\ b & a \end{pmatrix}$$

на месте, отмеченном звездочкой, должен находиться элемент d . Мы будем выражать этот факт, говоря, что *матрица удовлетворяет условию прямоугольника*.

Проверяя теперь таблицы операций U и V на рис. 89, мы обнаруживаем, что в первом случае соответствующая матрица удовлетворяет условию прямоугольника, а во втором — нет. Например, из первой и второй строк таблицы V и второй и третьей строк можно составить соответственно матрицы

$$\begin{pmatrix} 1 & 4 \\ 2 & 5 \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} 1 & 4 \\ 2 & 3 \end{pmatrix}, *$$

где $3 \neq 5$.

3.5. Группы и R-сети

Конечная группа может быть задана с помощью так называемой таблицы Кэли. Вообще говоря, отнюдь не просто установить, задает ли некоторая наперед взятая таблица операции группу. Особенно кропотлива и громоздка проверка ассоциативности операции, определяемой таблицей; трудно также выяснить, когда структуры, определяемые двумя таблицами, изоморфны. Существование и единственность обратных элементов и нейтрального элемента проверить проще. Если число элементов основного множества равно q , то для проверки условия $(ab)c = a(bc)$ потребуется $4q^3$ обращений к таблице, поскольку для каждой из q^3 троек элементов a, b, c нужно последовательно найти по таблице $ab, (ab)c, bc, a(bc)$.

Мы сейчас покажем, что подход к таблице операции как к сети можно применить к исследованию ассоциативности операции. Условимся называть операцию умножением, а нейтральный элемент — единичным элементом. Пусть заглавная строка и заглавный столбец представлены последовательностью натуральных чисел $1, 2, \dots, q$, где 1 — единичный элемент. Таким образом, наша таблица будет таблицей операции *луны*, т. е. квазигруппы с единичным элементом. Посмотрим, как отражается свойство R , т. е. условие прямоугольника для таблицы операции, на самой операции.

1° Таблица операции, удовлетворяющая условию R, обладает следующим свойством: если

$$(3.5.1) \quad x_2 = y_2, \quad x_3 y_2 = x_4, \quad x_2 y_3 = y_4,$$

то

$$x_3 y_4 = x_4 y_3.$$

Это следует из равенств предыдущего параграфа, определяющих условие R, в которых положено $x_1 = y_1 = 1$.

Из (3.5.1) получаем

$$x_3 (x_2 y_3) = x_3 y_4 = x_4 y_3 = (x_3 y_2) y_3 = (x_3 x_2) y_3.$$

Поскольку полученное равенство $x_3 (x_2 y_3) = (x_3 x_2) y_3$ выполняется для любой тройки (x_2, x_3, y_3) элементов основного множества $Q = \{1, 2, \dots, q\}$, то операция ассоциативна. Итак, если таблица операции квазигруппы Q с единичным элементом удовлетворяет условию R, то квазигруппа является группой.

2° Допустим теперь, что таблица операции задает группу с основным множеством Q. В этом случае мы имеем

$$(xy)^{-1} = y^{-1}x^{-1}.$$

Пусть $x_3 y_2 = x_4 y_1$, $x_1 y_2 = x_2 y_1$ и $x_1 y_4 = x_2 y_3$. Из равенства $x_1 y_2 = x_2 y_1$, в силу единственности обратного элемента, получаем

$$y_2^{-1} x_1^{-1} = y_1^{-1} x_2^{-1}.$$

Последнее равенство вместе с предыдущими дает

$$(x_3 y_2) (y_2^{-1} x_1^{-1}) (x_1 y_4) = (x_4 y_1) (y_1^{-1} x_2^{-1}) (x_2 y_3),$$

или

$$x_3 y_4 = x_4 y_3.$$

Мы установили, что таблица операции группы, рассматриваемая как сеть, обладает свойством R.

Результаты пунктов 1° и 2° подытоживает следующая

Т е о р е м а. Таблица операции квазигруппы с единичным элементом, рассматриваемая как сеть, удовлетворяет условию прямоугольника тогда и только тогда, когда квазигруппа является группой.

Условие существования единичного элемента у квазигруппы существенно. Рассмотрим, например, таблицу U

на рис. 89. Легко убедиться, что она удовлетворяет условию прямоугольника, но не содержит нейтрального элемента; операция не является также и ассоциативной, так как

$$(2 \cdot 3) 4 = 1 \cdot 4 = 3, \quad 2 (3 \cdot 4) = 2 \cdot 1 = 4.$$

3.6. Задачи и упражнения к главе 3

26. Сформулировать специальные условия, определяющие структуру конфигурации двойного пятиугольника в случаях конфигураций $D_0, D_1, D_2, D_3, D_3^*, D_4^*$.

27. Выяснить с помощью таблицы $\Gamma(4)$ на рис. 7, сколько дезарговых конфигураций имеется на конечной проективной плоскости порядка четыре.

28. Из определения $\Gamma(q)$ -таблицы, приведенного в параграфе 1.4, и вытекающих из него свойств D_1, D_2, D_3, D_4 легко следует, что латинский квадрат можно получить следующим путем.

В каждом квадрате C^{1k} ($k = 0, 1, \dots, q-1$) каждый знак инцидентности заменяется числом k , а затем все эти квадраты совмещаются в одном. Получающийся при этом латинский квадрат порядка q обозначим через L .

29. Снабдив латинский квадрат L , полученный в предыдущем примере, заглавной строкой и заглавным столбцом из чисел $1, 2, \dots, q$, мы получим таблицу операции квазигруппы, но не обязательно квазигруппы с нейтральным элементом (т. е. лупы); обозначим эту таблицу Q .

Доказать, что путем подходящих перестановок строк и столбцов таблицу инцидентности можно преобразовать в таблицу, по-прежнему удовлетворяющую определению Γ -таблицы и притом такую, что соответствующая таблица Q задает лупу.

30. Пусть Q — таблица из предыдущего примера. Доказать следующий факт: для того чтобы эта таблица задавала группу, необходимо и достаточно, чтобы теорема Дезарга выполнялась на конечной плоскости, определяемой таблицей $\Gamma(q)$, во всех случаях, когда осью является прямая l_1 , а центром — одна из точек P_1, P_2, \dots, P_{q+1} .

З а м е ч а н и е. Возвращаясь к недезарговой плоскости, которая соответствует таблице $\Gamma^*(9)$, заданной на рис. 45 (стр. 101), мы можем проверить по таблице V на рис. 45 с помощью ряда квадратов $C^{10}, C^{11}, \dots, C^{18}$, что эта плоскость обладает свойством, указанным в упражнении 30. Кроме того, как было отмечено в комментариях к упражнениям главы 1, на этой плоскости существует пара перспективных треугольников, для которых теорема Дезарга не выполняется. Если считать прямую l_1 идеальной, то эта плоскость будет так называемой *плоскостью транслаций*.

Глава 4

НЕКОТОРЫЕ ПРИЛОЖЕНИЯ КОНЕЧНЫХ ГЕОМЕТРИЙ К КОМБИНАТОРИКЕ

В этой главе мы применим некоторые свойства конечных проективных плоскостей к решению ряда комбинаторных задач. Мы будем заниматься экстремальными задачами комбинаторного анализа, а также реализациями экстремальных геометрических фигур (графов), дающими решения этих задач. Первый параграф, в котором излагается некоторый вспомогательный материал, может быть опущен читателем без ущерба для понимания дальнейшей части книги. В параграфе, посвященном понятию графа, приводятся лишь самые необходимые сведения, касающиеся графа как геометрической структуры.

4.1. Теорема замыкания для гиперболического пространства

Пусть a и b — две прямые в пространстве Бойаи — Лобачевского. Факт взаимной перпендикулярности прямых a и b будем выражать записью $a \times b$. Если $a \times b$, то будем говорить, что две прямые образуют *крест*. Пусть прямые g_1, g_2, g_3, g_4 попарно скрещивающиеся, а n_{jk} означает прямую, перпендикулярную прямым g_j и g_k . Всего имеется шесть таких прямых, и для них выполняется следующая

Т е о р е м а. Если $n_{12} \times n_{34}$ и $n_{13} \times n_{42}$, то $n_{14} \times n_{23}$.
То же самое верно и для евклидова пространства.

В условии теоремы говорится о крестах, образованных $10 = 4 + 6$ прямыми, поскольку прямая n_{jk} перпендикулярна прямым g_j и g_k , и теорема утверждает, что существование 14 крестов влечет существование пятнадцатого креста.

Диаграмма, показанная на рис. 91, дает ясное представление о комбинаторной структуре указанных 15 крестов. Точка G_j представляет прямую g_j , а точка N_{jk} —

прямую n_{jk} нашей фигуры; две точки соединены ребром, т. е. отрезком линии, в том случае, когда соответствующие прямые образуют крест; сами точки диаграммы изображены в виде маленьких кружков. Эта фигура является так называемым *графом Петерсена*. Граф легче изобразить, чем описать. Структура данного графа будет изучена позднее, а пока обратимся к доказательству нашей теоремы. В доказательстве будут использованы хорошо известные теоремы классической проективной геометрии и факты, касающиеся сферической модели Пуанкаре для гиперболической геометрии.

Начнем с модели Пуанкаре. Поверхность сферы проектируется из одной ее точки на плоскость. Точки этой плоскости представляют комплексные числа. Моделью гиперболического

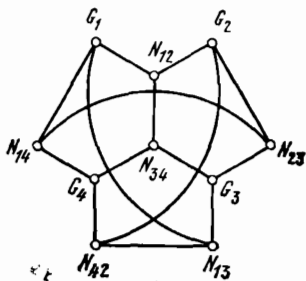


Рис. 91.

пространства служит внутренняя часть сферы, моделью прямых являются дуги окружностей, лежащие внутри сферы и пересекающие ее под прямым углом; две концевые точки дуги не считаются точками прямой. Если проекциям концевых точек дуги, представляющей прямую a , отвечают комплексные числа a_1 и a_2 , то эти числа определяют прямую a однозначно. Прямые $a: (a_1, a_2)$ и $b: (b_1, b_2)$ считаются лежащими в одной плоскости гиперболического пространства тогда и только тогда, когда точки сферы, соответствующие комплексным числам $a_1, a_2; b_1, b_2$, лежат на одном и том же круге сферы; они считаются перпендикулярными, если удовлетворяется следующее условие для двойного отношения:

$$(a_1 a_2 b_1 b_2) = -1.$$

Это условие можно также представить в виде

$$(a_1 + a_2)(b_1 + b_2) = 2(a_1 a_2 + b_1 b_2).$$

Можно было бы также рассмотреть модель на комплексной декартовой координатной плоскости, т. е. на множестве пар комплексных чисел. Пусть

$$A(a_1 a_2, a_1 + a_2) \text{ и } B(b_1 b_2, b_1 + b_2)$$

— две точки плоскости, для которых a_1, a_2, b_1 и b_2 удовлетворяют указанному выше условию. Рассмотрим теперь на плоскости параболу, заданную уравнением

$$y^2 = 4x.$$

Пару точек $P' (x', y')$, $P'' (x'', y'')$ будем называть *сопряженной* относительно этой параболы, если выполняется равенство

$$y'y'' = 2(x' + x'').$$

Очевидно, указанные выше точки A и B являются сопряженными точками относительно параболы. Таким образом, в этой модели пара A, B сопряженных относительно параболы точек соответствует кресту, образованному парой прямых a и b в первой модели, и обратно.

Точка G_1 , соответствующая данной прямой g_1 , сопряжена с каждой из точек N_{12}, N_{13} и N_{14} , отвечающих соответственно прямым n_{12}, n_{13} и n_{14} . Поэтому последние три точки лежат на одной прямой — поляре точки G_1 . Аналогично, тройки точек (N_{12}, N_{23}, N_{24}) , (N_{13}, N_{23}, N_{34}) , (N_{14}, N_{24}, N_{34}) коллинеарны — они лежат соответственно на полярах точек G_2, G_3 и G_4 . Следовательно, шесть точек N_{jk} являются шестью вершинами полного четырехсторонника, образованного полярами точек G_j .

Условия $n_{12} \times n_{34}$ и $n_{13} \times n_{42}$ теоремы означают, что диагональные пары вершин N_{12}, N_{34} и N_{13}, N_{42} полного четырехсторонника являются сопряженными парами точек. Отсюда, однако, в силу хорошо известной теоремы Гессе, вытекает, что третья пара вершин является сопряженной парой. А это означает, что отношение $n_{14} \times n_{23}$ выполняется, что и доказывает теорему.

Справедливость этой теоремы в евклидовом пространстве может быть установлена исходя из случая гиперболического пространства с помощью предельного перехода. Таким образом, эта теорема может считаться абсолютной в смысле Бойаи.

4.2. Некоторые основные факты, касающиеся графов

В настоящем параграфе мы рассмотрим понятие графа в узком смысле, а именно понятие так называемого *геометрического графа*.

Под *графом* будет пониматься фигура, составленная из *точек* и *ребер*, соединяющих точки, если выполнены следующие условия:

1° Множество точек не пусто.

2° Каждое ребро соединяет ровно две различные точки.

3° Две точки соединены самое большее одним ребром.

Пример графа, удовлетворяющего этому определению, показан на рис. 91.

Граф, не имеющий ребер, называется *пустым*. Если любые две (различные) точки графа соединены ребром, то граф называется *полным*. Полный граф, если он конечен, т. е. содержит конечное число точек, можно реализовать в виде множества вершин правильного n -угольника, каждые две вершины которого соединены отрезком прямой. Число точек графа называется его *порядком*, а число ребер — его *классом*. Таким образом, на рис. 91 представлен граф порядка десять и класса пятнадцать. Любой граф порядка n можно получить из полного графа того же порядка удалением некоторого числа ребер.

Пусть A и B — две точки графа. Говорят, что существует *маршрут*, соединяющий точки A и B , если существует такая последовательность точек $\{P_1, P_2, \dots, P_s\}$, что точки A и P_1 , P_1 и P_2 , \dots , P_{s-1} и P_s , P_s и B соединены ребрами. Граф называется *связным*, если для любых его двух точек существует соединяющий их маршрут. Число ребер, составляющих маршрут, называется *длиной* маршрута. Маршрут, соединяющий точку с самой этой точкой, называется *циклом*. Кратчайший цикл графа на рис. 91 состоит из пяти ребер, а самый длинный — из девяти ребер. Если в точке сходится k ребер, то говорят, что эта точка имеет *степень* k . Если все точки графа имеют одну и ту же степень k , то граф называют *регулярным графом степени* k . Наш пример на рис. 91 представляет собой регулярный граф степени три. Длина кратчайшего цикла графа называется *обхватом* графа. Обхват графа на рис. 91 равен 5. Обхват графа либо равен нулю, либо не меньше трех (в силу пунктов 2° и 3° определения). *Деревом* называется непустой связный граф, не содержащий циклов; отсюда следует, что обхват дерева равен 0. Цикл, проходящий через каждую точку графа, называется *гамильтоновой цепью*, а граф с такой цепью — *графом Гамильтона*.

Если удаление точки связного графа делает граф несвязным, то эта точка называется *точкой сочленения графа*. В нашем примере на рис. 91 точки сочленения отсутствуют. Если дерево содержит хотя бы два ребра, то оно имеет точку сочленения. Точки дерева, не являющиеся точками сочленения, называются *концевыми точками*. Каждая две точки дерева соединены единственным маршрутом.

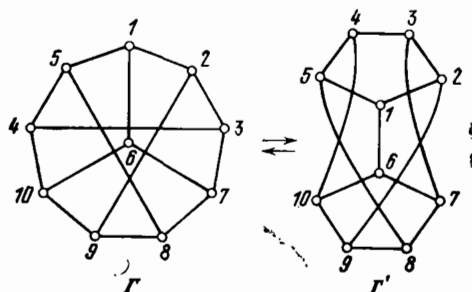


Рис. 92.

Действительно, если бы две точки дерева были соединены двумя маршрутами, то эти два маршрута либо составляли, либо содержали бы цикл. Длина маршрута, соединяющего две точки дерева, называется *расстоянием* между этими двумя точками.

Если множество точек графа можно разбить на два непересекающихся подмножества таким образом, что любое ребро соединяет точки разных подмножеств, то граф называется *бихроматическим* или *двудольным*. Граф на рис. 94 (стр. 233) — бихроматический, точки разных подмножеств изображены светлыми и темными кружками.

Конечно, граф имеет много различных моделей с присущим каждой модели способом выделения основных элементов графа и тех пар точек, которые соединены ребрами. Поэтому в ряде случаев бывает чрезвычайно трудно установить, представляют ли некоторые две модели один и тот же граф. Например, оба графа на рис. 92, по существу, совпадают с графом на рис. 91, т. е. оба являются графами Петерсена.

Понятие изоморфизма существенно необходимо в теории графов. Взаимно однозначное отображение ϕ множе-

ства точек графа Γ на множество точек графа Γ' , сохраняющее отношение связности, называется *изоморфизмом*, а в случае отображения графа на себя — *автоморфизмом*. Сохранение отношения связности означает, что две точки тогда и только тогда соединены ребром, когда то же самое верно для их образов. Если указанное отображение существует, то графы Γ и Γ' называются *изоморфными*, в противном случае они называются *гетероморфными*. Очевидно, изоморфизм является отношением эквивалентности на множестве графов. Легко проверить, что графы на рис. 92 изоморфны. Изоморфные графы в теории графов не различаются.

Непосредственно видно, что определенные выше свойства и числовые характеристики графа (связность, регулярность, порядок, класс, обхват, степень точки, длина маршрута и т. д.) инвариантны относительно изоморфизма. Кроме того, нетрудно доказать, что автоморфизмы графа образуют группу. Если занумеровать точки графа порядками n числами от 1 до n , то автоморфизмы графа будут выражаться перестановками множества $\{1, 2, \dots, n\}$. Интересная задача заключается в определении группы автоморфизмов графа, например графа Петерсена. Мы, однако, не будем здесь этим заниматься.

Вообще, описание того или иного графа может привести к интересным теоремам. Мы, например, отмечали, что описать граф Петерсена сложнее, чем изобразить его. Попробуем, однако, охарактеризовать его в терминах введенных выше инвариантов.

Граф Петерсена (рис. 91) есть регулярный граф степени $k = 3$, обхвата $l = 5$. Такими же свойствами обладают и многие другие графы; пусть, например, вершинами и ребрами графа являются вершины и ребра додекаэдра. Этот граф, как и граф на рис. 91, регулярен, имеет степень 3 и обхват 5. Вместе с тем рассматриваемые графы, очевидно, гетероморфны, поскольку порядок одного из них 10, а другого — 20. Постараемся определить минимальный порядок регулярного графа степени 3 и обхвата 5. Обозначим этот минимальный порядок через $f(3, 5) = n$.

Всякий граф степени $k = 3$ имеет точку, из которой исходят три ребра; на рис. 93 эти точка и ребра обозначены буквами O и e_1, e_2, e_3 , а другие концы трех указан-

ных ребер — цифрами 1, 2, 3. Из точек 1, 2, 3 должно исходить еще по два ребра, концы которых дают еще шесть точек графа, а именно точки 1·1, 1·2, 2·1, 2·2, 3·1, 3·2. Следовательно, граф должен включать в себя 9 ребер, а составленная из них фигура должна быть деревом, поскольку обхват данного графа $l = 5$. Итак, всякий граф, удовлетворяющий условиям $k = 3, l = 5$, содержит по крайней

мере $1 + 3 + 6 = 10$ точек, следовательно, $f(3, 5) \geq 10$.

Но граф на рис. 91 имеет порядок 10, откуда получается, что $f(3, 5) = 10$.

Всякий граф с параметрами $k = 3, l = 5$ и $n = f(3, 5) = 10$ будем обозначать символом $(10; 3, 5)$, а общее число классов изоморфизма таких графов — символом $g(3, 5) = r$. С помощью рис. 93 легко установить, что $g(3, 5) = 1$.

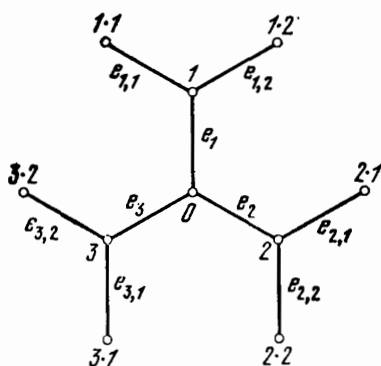


Рис. 93.

В самом деле, выберем на дереве рис. 93 какую-нибудь точку степени 1, скажем точку 1·1. В этой точке начинаются еще два ребра, конец одного из них совпадает либо с точкой 3·1, либо с точкой 3·2, а конец другого — либо с точкой 2·1, либо с точкой 2·2. Указанные четыре возможности, по существу, представляют собой одно и то же. Например, поворот ломаной $e_{3,2} - e_{3,1}$ на 180° вокруг оси e_3 индуцирует изоморфизм, переводящий ребро 1·1 — 3·1 в ребро 1·1 — 3·2. Поэтому без потери общности можно считать, что граф содержит ребра 1·1 — 2·2 и 1·1 — 3·2. Продолжая процесс определения ребер графа в соответствии с условием $l = 5$, мы получаем ребра 2·2 — 3·1, 3·2 — 2·1, 2·1 — 1·2 и 3·1 — 1·2. В результате получается граф, изображенный на рис. 91.

Таким образом, с точностью до изоморфизма граф Петерсена представляет собой единственный регулярный граф степени 3 наименьшего порядка, кратчайший цикл которого имеет длину 5.

4.3. Обобщения графа Петерсена

Мы будем обозначать через $\Gamma(n; k, l)$ регулярный граф степени k и обхвата l , имеющий наименьшее число $n = f(k, l)$ точек. Разумеется, не для всяких k и l регулярный граф степени k и обхвата l вообще существует, но если он существует, то число $n = f(k, l)$ однозначно определено. Тогда возникает новая задача: найти число

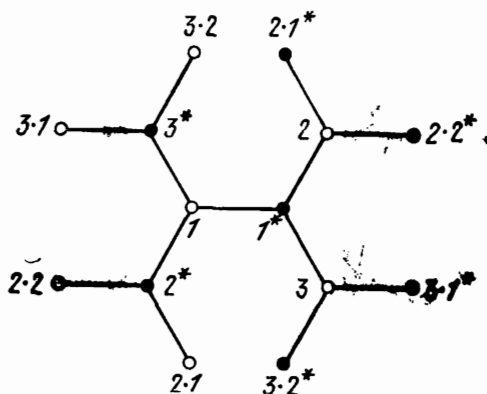


Рис. 94.

$g(k, l) = r$ (т. е. число классов изоморфизма). Общие результаты о возможных значениях n и r и реализациях экстремальных графов весьма немногочисленны. Мы отметим сейчас некоторые специальные случаи.

1° Экстремальные графы существуют при $k = 3$ и $l = 7$ или $l = 8$.

2° В этих случаях $f(3, 7) = 24$ и $f(3, 8) = 30$.

3° В тех же случаях $g(3, 7) = 1$ и $g(3, 8) = 1$.

Граф $\Gamma(n; k, l)$ по аналогии с графом, рассмотренным в предыдущем параграфе, будем называть (обобщенным) графом Петерсена. Прежде чем доказывать общие теоремы об этих графах, рассмотрим один частный пример, который будет полезен для понимания структуры таких графов.

Постараемся выяснить, существует ли граф Петерсена при $k = 3$ и $l = 6$.

Допустим, что он существует. Рассмотрим какое-нибудь его ребро (на рис. 94 ребро $1-1^*$). Отметим один конец

этого ребра светлым кружком, а другой — темным. Двигаясь от данного ребра симметрично вправо и влево, будем в соответствии с предположениями $k = 3$, $l = 6$ строить дерево, являющееся частью нашего графа. Процесс построения дерева продолжаем до тех пор, пока расстояние между «свободными концами» ребер не станет равным

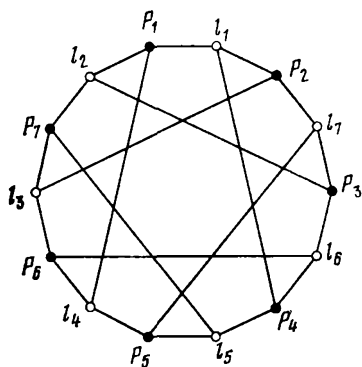


Рис. 95.

$6 - 1 = 5$. При этом каждое новое ребро должно иметь на одном конце светлый, а на другом — темный кружок. Ввиду $l = 6$ получится, как нетрудно видеть, дерево, показанное на рис. 94.

Это дерево содержит 7 темных и 7 светлых точек, и, следовательно, $f(3, 6) = n \geq 14$. Мы можем теперь продолжить построение графа, не добавляя новых точек; если, например, соединить ребром точки $2 \cdot 1$ и $3 \cdot 2^*$, то условие $l=6$ не нарушится, так как это ребро замыкает цикл,

длина которого равна 6. Действуя таким образом, мы получаем граф, изображенный на рис. 95, который удовлетворяет определению графа $\Gamma(14; 3, 6)$; чтобы убедиться в этом, достаточно подсчитать число ребер в каждом цикле. Следовательно, $f(3, 6) = 14$.

На рис. 95 светлые точки обозначены буквами l_j , а темные — буквами P_k ($j, k = 1, 2, \dots, 7$). При этом устанавливается следующее соответствие между графом на рис. 95 и таблицей инцидентности на рис. 2 (стр. 11): точкам P_k соответствуют точки плоскости, а точкам l_j — прямые плоскости. Если понимать отношение принадлежности точек одному ребру как отношение инцидентности, то нетрудно будет убедиться, что наш граф является моделью плоскости Галуа порядка два.

Исходя из данного примера, можно предположить, что для $k = q + 1$ и $l = 6$, где $q = p^r$ есть степень простого числа, существует экстремальный граф $\Gamma(n; q + 1, 6)$, порядок которого $n = f(q + 1, 6) = 2(q^2 + q + 1)$, и что моделью этого графа является плоскость Галуа порядка q .

Тот факт, что $f(q+1, 6) \geq 2(q^2 + q + 1)$, можно доказать так же, как и в случае $k = 2 + 1 = 3$. А именно, рассмотрим следующее симметричное дерево. Возьмем одно ребро и из двух его концов проведем по q ребер, а из $2q$ свободных концов этих ребер — еще по q ребер. В построенном таким образом дереве получится в общей сложности $2 + 2q + 2q^2$ точек, а наибольшее расстояние между его свободными концами будет равно 5.

Ясно, что если граф с параметрами $k = q + 1$ и $l = 6$ существует, то он должен содержать такое дерево. Следовательно, $f(q+1, 6) \geq 2(q^2 + q + 1)$.

Построим теперь граф по таблице инцидентности конечной плоскости порядка q следующим образом. Возьмем $q^2 + q + 1$ «темных» и столько же «светлых» точек; первые точки занумеруем теми же числами, что и столбцы таблицы, а вторые — теми же числами, что и строки. Соединим ребрами те и только те пары из одной светлой и одной темной точки, для которых в пересечении соответствующей строки и соответствующего столбца содержится знак инцидентности. Мы, очевидно, получим регулярный граф степени $q + 1$, состоящий из $2(q^2 + q + 1)$ точек. Каждое ребро этого графа соединяет одну светлую и одну темную точку, поэтому граф является бихроматическим. Ясно, что никакой его цикл не может состоять из нечетного числа ребер. Не может также существовать и цикла из четырех ребер, ибо в этом случае для таблицы инцидентности не выполнялись бы аксиомы I_1 и I_2 . Следовательно, длина кратчайшего цикла должна быть не меньше шести. Но по аксиоме I_3 плоскость обладает собственным треугольником, которому на графе соответствует цикл из шести ребер. Отсюда и из оценки, полученной выше, следует, что $f(q+1, 6) = 2(q^2 + q + 1)$. Таким образом, мы доказали существование экстремального графа $\Gamma(2(q^2 + q + 1); q + 1, 6)$.

Граф $\Gamma(2(q^2 + q + 1); q + 1, 6)$, построенный по таблице $\Gamma(q)$, является моделью плоскости, определяемой этой таблицей. Обратно, можно построить $\Sigma(q)$ -таблицу, определяющую плоскость порядка q , по всякому графу $\Gamma(2(q^2 + q + 1); q + 1, 6)$. Граф и соответствующая ему таблица представляют собой две эквивалентные модели. Особой правильностью отличается граф инцидентности в случае плоскости Галуа. (Мы пользуемся термином «граф

инцидентности» с целью подчеркнуть эквивалентность графа и таблицы инцидентности.)

В силу хорошо известной теоретико-числовой теоремы Зингера таблицу инцидентности всякой плоскости Галуа, как уже отмечалось ранее в связи с рисунками 5 и 6

параграфа 1.3, можно привести к циклическому виду.

В этом случае можно строить граф инцидентности по Ω -таблице плоскости. Эта таблица предварительно перестраивается таким образом, чтобы в пересечении строки l_1 со столбцами P_1 и P_2 содержались знаки инцидентности. Такая перестройка всегда возможна: в противном случае в многоугольнике Λ отсутствовала бы сторона, стягивающая угол φ (см. рис. 5, стр. 17). Построение графа по этой Ω -таблице можно произвести следующим образом (рис. 96).

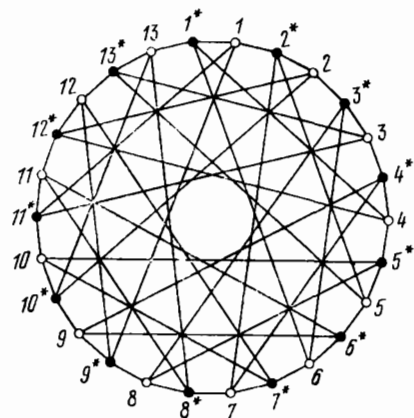


Рис. 96.

1° Вершины правильного $2(q^2 + q + 1)$ -угольника попеременно обозначаются светлыми и темными кружками; они будут служить точками графа.

2° Выбирается какое-нибудь направление обхода, и светлые точки нумеруются одна за другой в этом направлении последовательными числами $1, 2, \dots, q^2 + q + 1$. Аналогичным образом нумеруем темные точки, приписывая им индексы $1^*, 2^*, \dots, (q^2 + q + 1)^*$, где точка с индексом 1^* берется между точками 1 и $q^2 + q + 1$. Строке l_j Ω -таблицы мы сопоставляем светлую точку с индексом j , столбцу P_k — темную точку с индексом k^* , а инцидентность прямой l_j и точки P_k понимаем как наличие ребра, соединяющего точки j и k^* .

Этот симметричного вида экстремальный граф, соответствующий плоскости Галуа, будет не только бихроматическим, но также и графом Гамильтона.

В итоге наших рассмотрений получается следующая

Т е о р е м а. *Граф инцидентности плоскости Галуа является регулярным бихроматическим гамильтоновым графом степени $q + 1$ и обхвата 6, имеющим наименьший возможный порядок.*

4.4. Одна экстремальная задача комбинаторики

Экстремальная задача, рассмотренная в предыдущем параграфе, заключалась в определении минимального числа n вершин графа степени k и обхвата l . Мы ставим сейчас аналогичную задачу об определении максимального числа ребер графа с теми же параметрами. Эта задача представляет собой геометрическую интерпретацию одной проблемы Заренкевича, формулируемой следующим образом.

Пусть для некоторого n имеется бихроматический граф из n светлых и n темных точек, не содержащий цикла длины 4. Требуется определить максимальное число ребер такого графа и построить соответствующий экстремальный граф. (Искомые число и граф будем обозначать соответственно $F(n) = e$ и $\Gamma(n, e)$.)

Удобнее иметь дело не с самими такими графами, а с их матрицами инцидентности, т. е. следующими матрицами $n \times n$:

1° Строки матрицы соответствуют светлым точкам, обозначенным буквами P_i , а столбцы — темным точкам, обозначенным буквами P_k^* , $j, k = 1, 2, \dots, n$.

2° Если точки P_j и P_k^* соединены ребром, то элемент матрицы равен 1, в противном случае он равен нулю.

На языке матриц наша задача состоит в том, чтобы определить наибольшее число единиц в матрице порядка n , состоящей из единиц и нулей и не содержащей подматриц вида

$$Z = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix};$$

требуется также построить соответствующую экстремальную матрицу.

Строки и столбцы матрицы, рассматриваемые как векторы, будем обозначать соответственно через a_j и a_k^* . В силу условия, исключающего подматрицы Z , имеем:

при $j \neq k$

$$(4.4.1) \quad (a_j, a_k) = 0 \text{ или } 1 \text{ и } (a_j^*, a_k^*) = 0 \text{ или } 1,$$

где выражения в скобках означают скалярные произведения соответствующих векторов. Скалярное произведение строки (столбца) на себя есть натуральное число, равное числу единиц в этой строке (в этом столбце).

Примем обозначения

$$(4.4.2) \quad a_k^2 = \rho_k, \quad a_k^{*2} = \sigma_k \quad (k = 1, 2, \dots, n).$$

Обозначив число единиц в матрице через η , получаем

$$(4.4.3) \quad \rho_1 + \rho_2 + \dots + \rho_n = \sigma_1 + \sigma_2 + \dots + \sigma_n = \eta.$$

Мы пришли к следующей арифметической задаче: при данном n найти наибольшее число η , удовлетворяющее условиям (4.4.1) — (4.4.3), и построить матрицу, отвечающую найденному числу η .

Ключ к решению этой арифметической задачи дает хорошо известное неравенство

$$(4.4.4) \quad \frac{1}{n} (c_1 + c_2 + \dots + c_n)^2 \leq c_1^2 + c_2^2 + \dots + c_n^2,$$

которое применяется здесь к целым неотрицательным числам c_1, c_2, \dots, c_n ; равенство в (4.4.4) имеет место тогда и только тогда, когда $c_1 = c_2 = \dots = c_n = 0$.

Рассмотрим равенство

$$\begin{aligned} (a_1 + a_2 + \dots + a_n)^2 &= \\ &= (a_1^2 + a_2^2 + \dots + a_n^2) + 2(a_1, a_2) + \dots + 2(a_{n-1}, a_n). \end{aligned}$$

Левая его часть равна числу $\sigma_1^2 + \sigma_2^2 + \dots + \sigma_n^2$, которое, в силу (4.4.3) и (4.4.4), больше или равно $\frac{\eta^2}{n}$; в то же время второй член правой части, ввиду (4.4.3), не может превосходить числа $n(n-1)$ и равен этому числу только тогда, когда каждые две строки дают в скалярном произведении единицу.

Отсюда

$$\frac{\eta^2}{n} \leq \eta + (n-1)n,$$

т. е.

$$\eta^2 - n\eta - n^2(n-1) \leq 0.$$

Следовательно, для положительного числа η выполняется неравенство

$$(4.4.5) \quad \eta \leq \frac{1}{2} (1 + \sqrt{4n-3}) n.$$

Вывод этого неравенства показывает, что случай равенства имеет место тогда и только тогда, когда

$$(4.4.6) \quad \sigma_1 = \sigma_2 = \dots = \sigma_n \text{ и } (a_j, a_k) = 1 \\ (j, k = 1, 2, \dots, n; j \neq k).$$

Аналогично, исходя из скалярного квадрата суммы столбцов, мы получаем следующее необходимое и достаточное условие для равенства в (4.4.5):

$$(4.4.7) \quad \rho_1 = \rho_2 = \dots = \rho_n \text{ и } (a_j^*, a_k^*) = 1 \\ (j, k = 1, 2, \dots, n; j \neq k).$$

Таким образом, условия (4.4.6) и (4.4.7) эквивалентны. Если существует матрица, удовлетворяющая одному из них, то она удовлетворяет и другому, и в этом случае $\eta = n(1 + \sqrt{4n-3})/2 = e$.

Пусть теперь для некоторого натурального q имеем

$$(4.4.8) \quad n = q^2 + q + 1.$$

Тогда из (4.4.5) получаем $\eta \leq (q^2 + q + 1)(q + 1)$. Сравнивая теперь (4.4.3), (4.4.6) и (4.4.7), мы видим, что условие $\eta = (q^2 + q + 1)(q + 1) = e$ может выполняться только тогда, когда в каждой строке и в каждом столбце матрицы содержится по $q + 1$ единиц. С другой стороны, если существует проективная плоскость порядка q , то матрица, полученная из ее таблицы инцидентности заменой клеток, содержащих знаки инцидентности, единицами и пустых клеток нулями, в точности удовлетворяет условиям (4.4.6) и (4.4.7). ■

Таким образом, если существует плоскость порядка q , то задача полностью решается: мы не только находим максимальное число ребер $e = (q + 1)(q^2 + q + 1)$, но и строим граф, имеющий указанное число ребер.

4.5. Граф дезарговой конфигурации

Между рис. 75 и 92 существует определенная связь. На первом из них представлена общая дезаргова конфигурация (реализованная в виде двух вписанных друг в друга пятиугольников).

Рассмотрим следующее соответствие между множеством точек графа на рис. 92 и множествами точек и прямых дезарговой конфигурации на рис. 75:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ A_1 & A_3 & A_5 & A_2 & A_4 & B_1 & B_3 & B_5 & B_2 & B_4 \\ a_1 & a_3 & a_5 & a_2 & a_4 & b_1 & b_3 & b_5 & b_2 & b_4 \end{pmatrix}.$$

В этом соответствии каждое ребро истолковывается двойным образом. Например, ребро, соединяющее точки 4 и 10 на рис. 92, означает, во-первых, что вершина A_2 на рис. 75 принадлежит прямой $b_4 = B_1B_2$ и, во-вторых, что прямая $a_2 = A_4A_5$ проходит через вершину B_4 .

В этом смысле граф Петерсена является графом инцидентности дезарговой конфигурации. Действительно, концевые точки ребер, исходящих из некоторой точки графа, означают в точности те прямые (соответственно точки) конфигурации, которые инцидентны точке (соответственно прямой), отвечающей выбранной точке графа.

Следует подчеркнуть, что граф на рис. 92 представляет собой двойную диаграмму конфигурации: при истолковании отношения инцидентности с помощью ребер, считая один из концов ребра образом точки конфигурации, следует считать другой конец образом прямой.

Коллинеации конфигурации D на себя образуют группу. Очевидно, исследование этой группы может производиться в терминах группы автоморфизмов графа Петерсена. Заметим, что циклы длины s переходят при автоморфизме снова в циклы длины s , и ограничимся здесь рассмотрением циклов длины 5, т. е. циклов наименьшей длины, составленных из ребер графа. Мы утверждаем, что имеется 12 таких циклов, составляющих 6 пар по два не пересекающихся между собой цикла. Вершины этих непересекающихся циклов попарно соединены (непересекающимися) ребрами. Эти пять ребер образуют стягивающую систему графа, состоящую из наименьшего числа

ребер (каждая точка графа принадлежит, по крайней мере одному ребру).

Одно из таких разложений графа на непересекающиеся два цикла показано на рис. 92. Предположим, что ребра пятиугольника (1, ., 5) выкрашены в красный цвет, а ребра пятиугольника (6, ., 10) — в зеленый цвет. Допустим, далее, что всякое ребро, соединяющее красную и зеленую точку, например ребро 1 — 6 выкрашено белым.

Ясно, что всякий другой пятиугольник графа содержит ровно два белых ребра. Красные концы белых ребер либо соединены красным ребром, либо маршрутом из двух красных ребер, и соответственно этому зеленые концы соединены либо маршрутом из двух зеленых ребер, либо зеленым ребром. Имеется по пять пятиугольников того и другого вида, и они образуют пять пар непересекающихся пятиугольников. Учитывая пару из красного и зеленого пятиугольников, получаем, что общее число пар пятиугольников в графе равно шести.

Аналогичные рассуждения позволяют исследовать циклы большей длины. Интересно отметить, что граф Петерсена и граф додекаэдра, для каждого из которых $k = 3$ и $l = 5$, имеют одинаковое число пятиугольников, а именно 12.

4.6. Задачи и упражнения к главе 4

31. Доказать, что теорема, рассмотренная в параграфе 4.1, эквивалентна следующей теореме замыкания. Пусть даны три попарно скрещивающиеся прямые, не параллельные одной плоскости и такие, что ни одна из них не перпендикулярна двум другим; пусть для каждой прямой построена прямая, перпендикулярная как к данной прямой, так и к прямой, перпендикулярной двум другим прямым. Тогда существует прямая, перпендикулярная всем трем построенным прямым.

32. Теорема, сформулированная в задаче 31, эквивалентна также следующей теореме. Пусть все углы двух пространственных пятиугольников прямые и никакие две из десяти сторон не параллельны. Допустим, что сторонам одного пятиугольника можно таким образом сопоставить стороны другого, что несоседним сторонам отвечают соседние стороны. Тогда, если четыре пары соответствующих сторон взаимно перпендикулярны, то это же верно и для пятой пары.

33. Доказать существование графа $\Gamma(n; 3, 7)$; доказать также, что $n = 24$ и $r = 1$. Построить этот граф в виде возможно более простой фигуры.

34. Доказать существование графа $\Gamma(n; 3, 8)$; доказать также, что $n = 30$ и $r = 1$. Построить этот граф в виде возможно более простой фигуры.

35. Доказать, что граф $\Gamma(86; 7, 6)$ не существует.

36. Определить число циклов каждой длины в графе $\Gamma(10; 3, 5)$.

37. Доказать, что коллинеации, отображающие общую дезаргову конфигурацию на себя, образуют группу, изоморфную группе подстановок из пяти элементов.

Мы дадим несколько указаний к решениям этих задач, так как некоторые из них весьма трудны, а другие довольно громоздки.

33*. (Указание к задаче 33.) Вершины правильного 24-угольника, вписанного в окружность, занумеровать в каком-нибудь направлении числами от 1 до 24. Провести следующие 12 хорд: 1,18; 2,14; 3,10; 4,21; 5,17; 6,13; 7,24; 8,20; 9,16; 11,20; 12,19; 15,22. Эти 12 хорд вместе с 24 сторонами многоугольника исчерпывают множество ребер искомого экстремального графа.

34*. Рассмотреть такие 15 пар вершин правильного 30-угольника, вписанного в окружность: 1,18; 2,23; 3,10; 4,27; 5,14; 6,19; 7,24; 8,29; 9,16; 11,20; 12,25; 13,30; 15,22; 17,26; 21,28. Хорды, соединяющие эти пары точек, вместе с 30 сторонами многоугольника исчерпывают множество ребер искомого экстремального графа.

35*. Поскольку не существует проективной плоскости порядка шесть, искомым граф не существует.

36*. Рекомендуются рассуждать в соответствии с фигурой Γ^* на рис. 92.

КОМБИНАТОРИКА И КОНЕЧНЫЕ
ГЕОМЕТРИИ

Начальное развитие теории конечных геометрий шло по пути аналогий с классической геометрией. Однако вскоре теория стала испытывать сильное воздействие со стороны комбинаторики и алгебры. В этой главе мы рассмотрим более детально упоминавшиеся ранее связи между конечными геометриями и комбинаторным анализом.

5.1. Основные понятия комбинаторики

Пусть $H = \{1, 2, \dots, v\}$ — конечное множество, состоящее из v элементов (обозначенных целыми числами). Любое взаимно однозначное отображение множества H на себя называется подстановкой на H . Совокупность всех подстановок множества H образует группу. Эта группа называется *полной группой подстановок* на H , а любая ее подгруппа Γ называется просто *группой подстановок*.

Пусть $c \in H$. Группа подстановок Γ называется транзитивной на множестве H , если для любого элемента $x \in H$ существует подстановка из Γ , переводящая c в x .

Понятие транзитивности можно сформулировать так, чтобы оно не зависело от выбранного элемента c из H . Пусть x и y — два произвольных элемента из H . По предположению, существуют такие $\sigma, \tau \in \Gamma$, что $c^\sigma = x$ и $c^\tau = y$. Обозначим через σ^{-1} подстановку, обратную σ , и через ω композицию σ^{-1} и τ : $\sigma^{-1} \cdot \tau = \omega$. Тогда $\omega \in \Gamma$ и $x^\omega = (x^{\sigma^{-1}})^\tau = y$, так что в группе Γ имеется подстановка, переводящая x в y .

Если группа подстановок Γ не транзитивна на множестве H , или, как говорят, *интранзитивна*, то H можно разбить на подмножества, на каждом из которых Γ транзитивна. Эти подмножества называют *областями транзитивности* множества H . Два элемента $a, b \in H$ тогда

и только тогда принадлежат одной области транзитивности, когда в группе Γ существует подстановка σ , для которой $a^\sigma = b$. В этом случае можно сказать, что a и b связаны посредством Γ . Легко видеть, что отношение «связанности» рефлексивно, симметрично и транзитивно, т. е. является отношением эквивалентности; области транзитивности суть классы эквивалентности.

	1	2	3	4	5	6	7	8	9	10	11	12	13
σ_1	1	2	3	4	5	6	7	8	9	10	11	12	13
σ_2	7	2	5	10	3	12	1	8	11	4	9	6	13
σ_3	4	9	7	1	10	13	3	8	2	5	11	12	6
σ_4	3	9	10	5	7	12	4	8	11	1	2	13	6
σ_5	10	11	1	7	4	13	5	8	2	3	9	6	12
σ_6	5	11	4	3	1	6	10	8	9	7	2	13	12

Рис. 97а.

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_7	σ_4	σ_3	σ_6	σ_5
σ_3	σ_3	σ_5	σ_7	σ_6	σ_2	σ_4
σ_4	σ_4	σ_6	σ_2	σ_5	σ_7	σ_3
σ_5	σ_5	σ_3	σ_6	σ_7	σ_4	σ_2
σ_6	σ_6	σ_4	σ_5	σ_2	σ_3	σ_7

Рис. 97б.

Пример, приведенный на рис. 97а и 97б, изображает группу Γ подстановок множества $N = \{1, 2, \dots, 13\}$; элементы этой группы обозначены $\sigma_1, \sigma_2, \dots, \sigma_6$. Если мы рассмотрим элемент $8 \in N$, то непосредственно увидим, что группа Γ интранзитивна на множестве N . Легко указать ее области транзитивности:

$$N_1 = \{8\}, \quad N_2 = \{2, 9, 11\}, \quad N_3 = \{6, 12, 13\},$$

$$N_4 = \{1, 3, 4, 5, 7, 10\}; \quad N = N_1 \cup N_2 \cup N_3 \cup N_4.$$

Если исключить из рис. 97а столбцы 2, 6, 8, 9, 11, 12, 13, то оставшиеся столбцы будут изображать группу, состоящую из 6 подстановок множества N_4 . Рассмотрим разбиение этого множества

$$N_4 = N_{41} \cup N_{42} \cup N_{43},$$

где

$$N_{41} = \{1, 4\}, \quad N_{42} = \{3, 5\}, \quad N_{43} = \{7, 10\}.$$

Это разбиение на непересекающиеся подмножества обладает тем свойством, что любая из подстановок $\sigma_1, \dots, \sigma_6$ преобразует каждое из указанных подмножеств снова в одно из этих подмножеств (возможно, в то же самое).

Пусть группа Γ транзитивна на множестве N . Если можно разбить N на несколько (по крайней мере два) непересекающихся подмножеств, из которых хотя бы одно содержит не менее двух элементов, и любой элемент группы Γ отображает каждое из подмножеств снова в одно из подмножеств, то группа Γ называется *импримитивной*. Если же N не допускает такого разбиения, группа Γ называется *примитивной*. Любая транзитивная группа на N , содержащая простое число элементов, является примитивной.

Степенью группы подстановок множества N будем называть число $|N| = v$. Если группа подстановок Γ транзитивна на множестве N , то порядок группы, т. е. число $|\Gamma| = g$, делится на степень группы — доказательство этого факта предоставляется читателю в качестве упражнения. Если $g = v$, группа Γ называется *регулярной*.

Транзитивная абелева группа всегда регулярна. Доказательство снова предоставляем читателю.

Рассмотрим теперь возникшее сравнительно недавно в комбинаторном анализе понятие, которое исключительно важно с точки зрения конечных геометрий.

Пусть задан набор непустых подмножеств (называемых *блоками*) множества N , причем:

1° Число элементов множества N есть заданное натуральное число v .

2° Число блоков есть заданное натуральное число b .

3° Каждый блок состоит из одного и того же числа элементов. Обозначим это число k .

4° Каждый элемент множества N принадлежит одному и тому же числу блоков. Пусть это число есть r .

5° Каждая пара различных элементов множества N принадлежит одному и тому же числу блоков. Пусть это число есть λ .

Набор блоков $\{B_1, \dots, B_b\}$, удовлетворяющий перечисленным условиям, называется *блок-схемой*. Разумеется, существование или единственность блок-схемы с данными значениями параметров v , b , k , r и λ нуждаются в специальном исследовании. Пусть, например, $v = 21$, $b = 21$, $k = 5$, $r = 5$ и $\lambda = 1$. В этом случае можно утверждать не только существование, но и единственность блок-схемы. А именно, рассмотрим проективную плоскость порядка 4. Примем множество всех точек этой плоскости за N , а пря-


мые будем рассматривать как блоки. Получим, очевидно, блок-схему с указанными выше значениями параметров. Напомним, что плоскость такого вида единственна — это плоскость Галуа порядка 4 (см. рис. 7, стр. 22) *).

Пять параметров блок-схемы не являются независимыми. Действительно, блок-схему можно представить с помощью таблицы инцидентности, подобной таблице рис. 71. Число знаков инцидентности, содержащихся в таблице, можно подсчитать двумя способами: по столбцам, что дает $v \cdot r$ знаков, или по строкам, что дает $b \cdot k$ знаков. Таким образом,

$$(5.1.1) \quad v \cdot r = b \cdot k.$$

Далее, число пар знаков в каждой строке есть C_k^2 , следовательно, число всех пар такого типа, содержащихся в таблице, есть $b \cdot C_k^2$. Но существует ровно λ строк, каждая из которых пересекает данную пару столбцов по квадратам, содержащим знаки; поэтому число тех же пар равно $\lambda \cdot C_v^2$. Отсюда находим $bk(k-1) = \lambda v(v-1)$. Сравнивая с (5.1.1), получаем отсюда

$$(5.1.2) \quad \lambda(v-1) = r(k-1).$$

Условия (5.1.1) и (5.1.2) необходимы, но недостаточны для существования блок-схемы данного типа. Например, эти условия выполнены при $v = 43$, $b = 43$, $r = 7$, $k = 7$, $\lambda = 1$, однако мы знаем, что проективной плоскости порядка 6 не существует. 

Мы уже видели — а именно на примере проективной плоскости порядка 4, — что существуют блок-схемы, для которых $v = b$. Для таких схем, в силу (5.1.1), должно быть $k = r$. В этом случае мы говорим о *симметричной* (v, k, λ) -схеме. Можно также называть ее *симметричной*

*) Единственность блок-схемы указанного типа вытекает из простых соображений. Рассмотрим какой-либо блок B_α . Для любого элемента $i \in B_\alpha$ число блоков, отличных от B_α и содержащих i , равно 4. Следовательно, число блоков, отличных от B_α и имеющих непустое пересечение с B_α , равно $5 \cdot 4 = 20 = 21 - 1$. Это показывает, что пересечение любых двух различных блоков не пусто, т. е. состоит в точности из одного элемента. Отсюда вытекает, что любая блок-схема с указанными значениями параметров реализует некоторую проективную плоскость порядка 4 (ибо все аксиомы выполнены). Поскольку такая плоскость единственна, то единственна и блок-схема. — *Прим. перев.*

(v, k, λ) -конфигурацией. Необходимое условие существования блок-схемы такого типа есть (5.1.2) или, ввиду симметричности,

$$(5.1.3) \quad \lambda(v-1) = k(k-1).$$

Разумеется, это условие выполняется в случае проективной плоскости порядка q , когда $v = q^2 + q + 1$, $k = q + 1$, $\lambda = 1$.

Не входя в подробности, укажем, что необходимое условие существования симметричной (v, k, λ) -конфигурации было известно еще двадцать лет назад. Высказывалось предположение, что это условие является также и достаточным; однако до сих пор доказать это не удалось. Условие формулируется для нечетного v и состоит в следующем: уравнение

$$(5.1.4) \quad z^2 = (k-\lambda)x^2 + (-1)^{\frac{v-1}{2}} \cdot \lambda y^2$$

должно иметь решение в целых x, y, z (не равных одновременно нулю). Подтверждение достаточности этого условия представляется весьма трудной задачей.

Рассматривая определение симметричной (v, k, λ) -конфигурации, можно прийти к обобщению этого понятия — так называемым t -(v, k, λ)-схемам. Последние определяются следующими условиями:

1° Множество H состоит из v элементов.

2° Каждый блок есть подмножество, состоящее из k элементов.

3° Любое подмножество из t элементов содержится ровно в λ блоках.

Это обобщение — не просто искусная выдумка; напротив, оно совершенно естественно возникает в теории конечных плоскостей, как мы увидим в ближайших параграфах.

5.2. Две основные теоремы инверсной геометрии

Так называемая мёбиусова (или инверсная) плоскость получается из евклидовой плоскости присоединением единственной идеальной точки, которая считается принадлежащей всем прямым плоскости. После такого присоединения мы уже не делаем различия между прямыми линиями и окружностями, и те и другие теперь называем *циклами*.

ми. Это позволяет достичь единой формулировки теорем евклидовой геометрии, относящихся к пересечению прямых и окружностей.

Структура мёбиусовой плоскости «идентична» структуре сферы в том смысле, что существует *стереографическое отображение* (стереографическая проекция) сферы на плоскость Мёбиуса. Пусть t — прямая, проходящая через центр сферы, и U — одна из точек пересечения этой прямой со сферой. Рассмотрим плоскость, ортогональную прямой t , как мёбиусову. Точка P сферы, отличная от U , считается соответствующей точке P' плоскости, если прямая PP' проходит через U , а точка U отвечает идеальной точке плоскости. Такое отображение сохраняет циклы, пересекающиеся окружности на сфере переходят в пересекающиеся циклы на плоскости с сохранением угла между ними; при этом сферическим циклом, проходящим через U , отвечают прямые на плоскости. Именно это свойство стереографической проекции наводит на мысль рассматривать прямые на плоскости как циклы, когда плоскость дополнена идеальной точкой.

В математической литературе прошлого столетия много говорилось о так называемом *ассоциированном точечном октете*, который может быть определен следующим образом. Три квадрики, не содержащие общих кривых, могут иметь ровно восемь общих точек; фигура, состоящая из этих восьми точек, называется ассоциированным точечным октетом и обозначается $R(8)$. Среди множества всех квадрик, проходящих через точки октета $R(8)$, может оказаться сфера Γ и квадратичная поверхность, состоящая из двух плоскостей. Изучение этих специальных случаев приводит к двум основным теоремам инверсной (или действительной инверсной) геометрии. Опишем теперь точно конструкцию специального $R(8)$.

Рассмотрим *замкнутую цепочку*, образованную циклами c_1, c_2, c_3, c_4 сферы Γ , где предполагается, что

циклы c_1 и c_2 пересекают друг друга в точках A_1 и B_1 ,
циклы c_2 и c_3 пересекают друг друга в точках A_2 и B_2 ,
циклы c_3 и c_4 пересекают друг друга в точках A_3 и B_3 ,
циклы c_4 и c_1 пересекают друг друга в точках A_4 и B_4 .

Плоскость цикла c_k обозначим γ_k . Четыре плоскости в общем случае образуют грани тетраэдра; пусть C_k есть вершина этого тетраэдра, противоположная грани γ_k .

Очевидно, точки A_k, B_k ($k = 1, 2, 3, 4$) составляют ассоциированный октет, поскольку они могут быть получены как общие точки трех квадрик, а именно: сферы Γ , пары плоскостей γ_1, γ_3 и пары плоскостей γ_2, γ_4 .

Описание этого специального $R(8)$ можно дать, не используя замкнутой цепочки циклов, следующим образом. Пусть некомпланарная четверка точек (C_1, C_2, C_3, C_4) обладает тем свойством, что каждая из прямых C_1C_2, C_2C_3, C_3C_4 и C_4C_1 пересекает сферу Γ в двух точках. Полученные при этом восемь точек сферы образуют фигуру $R(8)$.

Два указанных способа приводят к одной и той же восьмерке точек сферы. Но способ, связанный с замкнутой цепочкой циклов, может быть интерпретирован на плоскости Мёбиуса.

Опишем некоторое вырождение фигуры $R(8)$. Оно получается, если плоскости γ_k различны, но четверка точек A_1, B_1, A_3, B_3 принадлежит одной плоскости γ . Это возможно лишь в том случае, когда прямые A_1B_1, A_3B_3 и A_2B_2 имеют общую точку C (через эту точку проходят три плоскости γ_2, γ_3 и γ). Так как прямая A_4B_4 является линией пересечения плоскости γ_1 , инцидентной с прямой A_1B_1 , и плоскости γ_4 , инцидентной с прямой A_3B_3 , она также должна проходить через точку $C = A_1B_1 \cap A_3B_3$. Итак, вырождение состоит в том, что прямые A_kB_k ($k = 1, 2, 3, 4$) имеют общую точку C (тетраэдр вырождается в этом случае в четверку плоскостей, пересекающихся в точке C). Следовательно, четверка точек (A_2, B_2, A_4, B_4) также компланарна. Разумеется, четыре компланарные точки на сфере принадлежат одному циклу. Таким образом, нами доказана следующая

Т е о р е м а. Если (A_k, B_k) , $k = 1, 2, 3, 4$, — четыре пары точек, определенные с помощью замкнутой цепочки циклов на сфере, причем A_1, B_1, A_3, B_3 принадлежат одному циклу, то A_2, B_2, A_4, B_4 также принадлежат одному циклу.

Эта теорема верна и в случае плоскости Мёбиуса (т. е. она является теоремой инверсной геометрии) и может быть легко доказана с помощью стереографической проекции. Будем называть ее *N-теоремой*.

Вернемся теперь к специальной $R(8)$ -конфигурации, определенной с помощью тетраэдра S общего вида. Имеется

классическая теорема, устанавливающая, что если точки A_k ($k = 1, 2, 3, 4$) компланарны, то и точки B_k тоже компланарны.

В терминах замкнутой цепочки циклов этот факт дает теорему инверсной геометрии, называемую *теоремой Мизуэля* или *М-теоремой* (рис. 98).

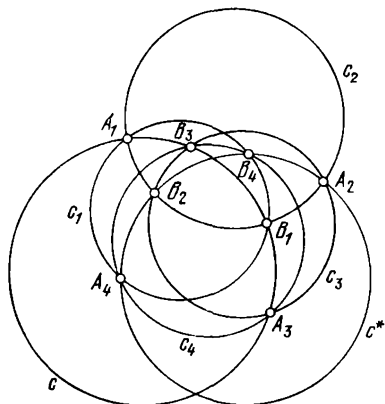


Рис. 98.

М-теорема. Пусть четыре пары (A_k, B_k) точек определены с помощью замкнутой цепочки циклов. Тогда четверка точек B_k будет концикулярной *) в том и только в том случае, когда концикулярна четверка точек A_k .

Эту теорему можно получить как следствие более сильного результата, относящегося к ассоциированным точечным октетам. Здесь, однако, мы приведем

совсем элементарное доказательство (рис. 99).

Возьмем произвольную сферу, в ней — некоторую точку и будем проектировать плоскую фигуру из этой точки на сферу. (Мы должны доказать существование цикла c^* , содержащего четверку B_1, B_2, B_3, B_4 .) Затем сферическую фигуру снова отобразим с помощью стереографической проекции из точки A_1 сферы на плоскость. В итоге получим на плоскости фигуру той же структуры, что исходная фигура, но теперь циклы c_1, c_2 будут прямыми линиями, поскольку на сфере эти циклы проходят через центр A_1 проектирования (рис. 100). Так как оба последовательно примененных нами отображения сохраняют циклы, достаточно показать, что точки B_1, B_2, B_3, B_4 на рис. 100 концикулярны.

Утверждение, подлежащее доказательству, можно истолковать следующим образом: если ни одна из точек A_3, B_4 и B_2 , лежащих на сторонах треугольника $A_2A_4B_1$, не совпадает с вершиной этого треугольника, то описан-

*) То есть принадлежащей одному циклу. — Прим. перев.

ные окружности треугольников $B_2A_2A_3$, $B_4A_3A_4$, $B_1B_2B_4$ проходят через общую точку B_3 . Это есть так называемая малая теорема Мигуэля; ее легко доказать, используя теорему о вписанных углах.

Подобными же рассуждениями можно доказать и N-теорему. В этом случае мы должны доказать существование цикла c^* , содержащего точки A_2 , B_2 , A_4 , B_4 рис. 98. Первый шаг снова заключается в проектировании плоской фигуры на сферу Γ , второй шаг — в последующем проектировании из A_4 сферы снова на плоскость. После двух проектирований получается фигуру, изображенную на

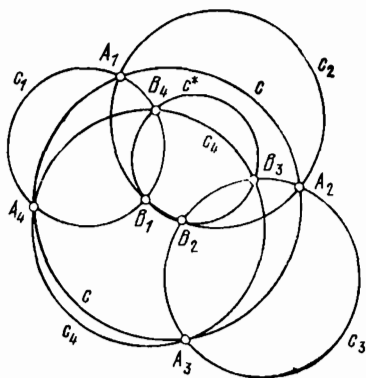


Рис. 99.

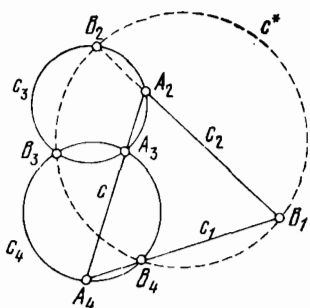


Рис. 100.

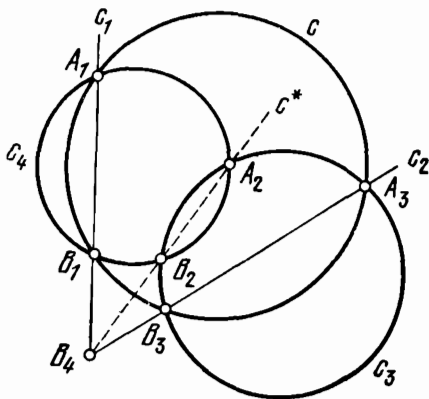


Рис. 101.

рис. 101, где c_1 и c_2 — прямые (в евклидовом смысле) линии. Рассматривая нашу плоскость как плоскость Мёбиуса, мы должны теперь доказать, что точки A_2 , B_2 , B_4 коллинеарны (в евклидовом смысле), поскольку A_4 есть иде-

альная точка плоскости. Но это легко следует из теоремы, относящейся к прямой степеней трех окружностей: B_4 есть степень окружностей c_3, c_4, c .

В двух последних доказательствах прослеживается общая идея: из справедливости специальной М-теоремы (см. рис. 100) и специальной N-теоремы (см. рис. 101) выводится справедливость теорем в общем виде двукратным применением стереографической проекции.

Мы будем теперь изучать вопрос: существуют ли конечные плоскости, аналогичные инверсной плоскости, и верны ли в них теоремы, аналогичные М-теореме и N-теореме?

5.3. Конечные инверсные геометрии и t -(v, k, λ)-схемы

Мы уже знакомы с интересным примером блок-схемы t -(v, k, λ), а именно с конечной проективной плоскостью, для которой $t = 2$, $v = q^2 + q + 1$, $k = q + 1$ и $\lambda = 1$. Теперь мы можем указать пример, отвечающий случаю $t = 3$, $v = q^2 + 1$, $k = q + 1$, $\lambda = 1$, пользуясь геометрическим языком. Для определенности будем считать $q = 3$. Рассмотрим таблицу инцидентности, показанную на рис. 102, где столбцы отвечают точкам P_0, P_1, \dots, P_9 , а строки — циклам c_1, c_2, \dots, c_{30} (соответственно).

Легко проверить, что эта структура, содержащая 10 точек и 30 циклов, обладает следующими свойствами:

K_1 . Любой цикл содержит точки.

K_2 . С любой тройкой точек инцидентен единственный цикл.

K_3 . Если $P_j \in c_r$ и $P_h \in c_r$, то существует по крайней мере один цикл $c_s \neq c_r$, для которого $P_j \in c_s$ и $P_h \in c_s$.

K_4 . Существуют 4 точки, не принадлежащие одному циклу (4 неконцикулярные точки).

Аксиомы K_1, K_2, K_3, K_4 образуют вместе систему аксиом, которую мы будем обозначать K .

Плоскость, удовлетворяющая система аксиом K , называется *инверсной плоскостью* или *плоскостью Мёбиуса*. Если число точек такой плоскости конечно — как в рассмотренном выше случае, — мы говорим о конечной плоскости Мёбиуса.

Возникает ряд вопросов:

1° Сколько таблиц инцидентности, подобных таблице предыдущего примера, можно построить?

2° Какими общими свойствами обладают все инверсные плоскости?

Мы не станем давать подробные ответы на эти вопросы, а рассмотрим только общий план изучения таких плоскостей.

1° Пусть p — нечетное простое число. Рассмотрим трехмерное пространство Галуа над координатным полем $K = GF(p')$ и параллельно с ним — классическое проективное пространство. В последнем случае уравнению

$$(5.3.1) \quad x_1^2 + x_2^2 + x_3^2 = x_4^2$$

отвечает единичная сфера. Если проектировать точки сферы, за исключением $U(0, 0, 1, 1)$, из точки U на (фундаментальную) плоскость $x_4 = 0$, получим стереографическое отображение сферы на плоскость. Рассматривая то же самое уравнение (5.3.1) над координатным полем K , получим в пространстве Галуа квадрику, называемую *овалоидом*. (Мы понимаем под *квадрикой* множество точек, определенное уравнением второй степени; если квадрика содержит более одной точки и не содержит прямых, она называется овалоидом.) Любую точку овалоида, не лежащую в плоскости $x_4 = 0$, можно принять за центр U проектирования. Мы будем называть проекции плоских сечений овалоида на фундаментальную плоскость $x_4 = 0$ «циклами».

Изображенный на рис. 102 пример может быть получен именно таким путем. Мы берем овалоид (5.3.1) над

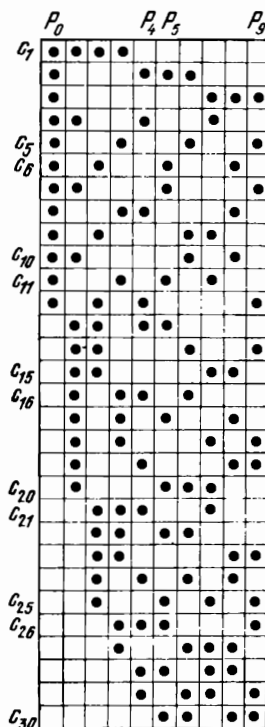


Рис. 102.

координатным полем $GF(3)$ и проектируем его точки из $U(0, 0, 2, 1)$ на плоскость, образуемую точками $(x_1, x_2, x_3, 0)$. Читатель легко проверит, что все точки овалоида (кроме U) суть

$$Q_1(0, 0, 1, 1), Q_2(0, 1, 0, 1), Q_3(0, 2, 0, 1), Q_4(1, 0, 0, 1), \\ Q_5(1, 1, 1, 0), Q_6(1, 2, 1, 0), Q_7(2, 0, 0, 1), Q_8(2, 1, 1, 0), \\ Q_9(2, 2, 1, 0).$$

Обозначим проекцию точки Q_j через P_j . Очевидно, $Q_5 = P_5$, $Q_6 = P_6$, $Q_8 = P_8$, $Q_9 = P_9$; остальные проекции суть

$$P_1(0, 0, 1, 0), P_2(0, 1, 1, 0), P_3(0, 2, 1, 0), \\ P_4(1, 0, 1, 0), P_7(2, 0, 1, 0).$$

Если вместо $(x_1, x_2, 1, 0)$ воспользоваться **неоднородными координатами** (x_1, x_2) , то будем иметь

$$P_1(0, 0), P_2(0, 1), P_3(0, 2), \\ P_4(1, 0), P_5(1, 1), P_6(1, 2), \\ P_7(2, 0), P_8(2, 1), P_9(2, 2).$$

Таким образом, мы получили точки аффинной плоскости третьего порядка. Ее пополнение идеальной точкой P_{10} (отвечающей U) есть плоскость Мёбиуса порядка 3 (ср. рис. 8, iii и первые 12 строк рис. 102).

Теперь можно найти плоские сечения овалоида $\{U, Q_1, Q_2, \dots, Q_9\} = \Omega$. Так как прямая имеет с овалоидом не более двух общих точек, каждая тройка точек овалоида определяет единственную плоскость. Каждая такая плоскость имеет с овалоидом четыре общие точки, и если спроектировать их из точки U на фундаментальную плоскость, будем получать множества из четырех точек, образующие циклы на плоскости Мёбиуса. Таблица инцидентности точек и циклов в этой плоскости и представлена как раз на рис. 102.

2° Понятие овалоида в пространстве $S_{3,q}$ можно определить по-другому — более геометрично. Оставив в стороне случай $q = 2^r$, будем понимать под овалоидом подмножество из $q^2 + 1$ точек проективного пространства порядка q , обладающее тем свойством, что никакие три точки в нем не коллинеарны (ср. с параграфами 2.7 и 2.13).

Число общих точек плоскости и овалоида не может превышать числа точек овала на плоскости порядка q , т. е. не может превышать $q + 1$ *). Однако это число (если только оно > 1) не может быть и меньше, чем $q + 1$. В самом деле, рассмотрим плоскости, проходящие через точки Q_j и Q_k ($j \neq k$) овалоида. Прямая $l_{jk} = Q_j Q_k$ и любая точка расходящейся с ней прямой определяют плоскость; отсюда число плоскостей, инцидентных с прямой l_{jk} , есть $q + 1$. Пусть в этих плоскостях лежат соответственно $\pi_1, \pi_2, \dots, \pi_{q+1}$ точек овалоида. Учитывая, что точки Q_j и Q_k принадлежат каждой из этих плоскостей, находим

$$\pi_1 + \pi_2 + \dots + \pi_{q+1} = (q^2 + 1) + 2q = (q + 1)^2.$$

Но $\pi_j \leq q + 1$, и, значит,

$$\pi_1 = \pi_2 = \dots = \pi_{q+1} = q + 1.$$

Таким образом, *плоскость, содержащая по крайней мере две точки овалоида, имеет с овалом ровно $q + 1$ общих точек.*

Число плоскостей, проходящих через данную точку овалоида и имеющих с ним более одной общей точки, есть $q^2(q + 1)/q = q^2 + q$. А так как число плоскостей, инцидентных с данной точкой пространства, есть $q^2 + q + 1$, то среди них существует ровно одна плоскость, касающаяся овалоида (т. е. имеющая с ним ровно одну общую точку).

Число таких касательных плоскостей к овалом равно, очевидно, $q^2 + 1$. Но число плоскостей, содержащих более одной точки овалоида, равно отношению числа троек точек овалоида к числу троек точек овала, т. е. числу

$$C_{q^2+1}^3 / C_{q+1}^3 = q^3 + q.$$

Отсюда находим, что число всех плоскостей, содержащих хотя бы одну точку овалоида, равно $(q^2 + 1) + (q^3 + q) = q^3 + q^2 + q + 1$, что совпадает с числом всех плоскостей пространства.

Итак, *любая плоскость пространства или касается овалоида, или пересекает его в $q + 1$ точках.*

Этот результат является неожиданным, так как в классическом проективном пространстве только линейчатые

*) Это следует, например, из теоремы пункта 3° параграфа 2.7.— *Прим. перев.*

квадрики обладают свойством пересекаться со всякой плоскостью.

Следующие несколько свойств читатель легко установит самостоятельно.

Любая внешняя по отношению к овалويدу прямая инцидентна двум касательным плоскостям и $q - 1$ плоскостям, пересекающим овалويد по овалам.

Прямая, касающаяся овалоида, инцидентна одной касательной к овалويدу плоскости и еще q плоскостям, пересекающим овалويد по овалам.

Как уже упоминалось, прямая, пересекающая овалويد в двух точках, инцидентна $q + 1$ плоскостям, пересекающим овалويد по овалам.

Получающиеся таким путем три вида пучков овалов аналогичны эллиптическим, параболическим и гиперболическим пучкам окружностей на обычной сфере.

Каждая точка овалоида содержится в $q(q + 1)$ овалах данного овалоида, всего же на овалоиде имеется $q(q^2 + 1)$ овалов. Число овалов, не пересекающихся с данным овалом, равно $q(q - 1)(q - 2)/2$ *), а число овалов, касающихся данного овала, есть $q^2 - 1$.

Таким образом, мы дали комбинаторную интерпретацию понятию овалоида и полностью выяснили структуру инцидентностей точек и овалов, исходя из элементарных (комбинаторных) соображений. Так как каждые три точки овалоида определяют в точности один овал и так как овалы овалоида как точечные множества можно рассматривать в качестве блоков, овалويد служит реализацией блок-схемы $3-(v, k, \lambda)$, где $v = q^2 + 1$, $k = q + 1$, $\lambda = 1$.

Связь между инверсной геометрией, т. е. плоскостью Мёбиуса порядка q , и блок-схемами $3-(q^2 + 1, q + 1, 1)$ легко усматривается из того факта, что плоскость Мёбиуса с ее циклами изоморфна (посредством стереографической проекции) «сфере», заданной в пространстве Галуа порядка q уравнением (5.3.1), с ее «сферическими циклами». И эта сфера с ее циклами есть не что иное, как определенный выше овалويد с его овалами.

*) В случае плоскости порядка q число внешних прямых к овалу равно $q^2 + q + 1 - 4q + 1 = q/2 - (q + 1)$ (число всех точек минус число секущих и минус число касательных), т. е. равно $q(q - 1)/2$. Это число нужно умножить на $(q + 1) - 1 - 2 = q - 2$ (исключаются данная плоскость и две касательные плоскости к овалоиду). — *Прим. перев.*

Можно, таким образом, утверждать существование неограниченного числа конечных плоскостей, удовлетворяющих системе аксиом К, которая, тем самым, заслуживает изучения.

5.4. Некоторые теоремы, относящиеся к плоскости Мёбиуса

Сравнивая примеры, изображенные на рис. 102 и 101, мы видим, что если сопоставить циклам c_1, c_2, c_3, c_4 , с рис. 101 строки $c_1, c_3, c_{30}, c_{22}, c_{23}$ рис. 102, то столбцы $P_4, P_6, P_{10}; P_3, P_7, P_9, P_1$ будут отвечать точкам пересечения $A_1, A_2, A_3; B_1, B_2, B_3, B_4$. Далее, строка c_2 рис. 102 соответствует прямой c^* , проходящей через три точки A_2, B_2, B_4 , т. е. теорема, аналогичная N-теореме классической инверсной геометрии, имеет место для фигуры рис. 102.

Можно поставить вопрос, верны ли M-теорема или N-теорема для инверсной плоскости, определенной аксиоматически. Мы лишь кратко опишем результаты, которые известны по этому поводу.

Если для некоторой плоскости Мёбиуса верна теорема Мигуэля, плоскость называется *мигуэлевой* или просто *M-плоскостью*.

Конечная инверсная плоскость тогда и только тогда является мигуэлевой плоскостью, когда она изоморфна нелинейчатой квадрике в пространстве Галуа. При этом точкам плоскости сопоставляются точки квадрики, прямым — плоские сечения квадрики, содержащие более чем одну точку этой квадрики.

В пространстве нечетного порядка любая нелинейчатая квадрика является оваломидом, и обратно. В пространствах четного порядка это неверно (ср. теорему Сегре).

Таким образом, в случае нечетного порядка можно говорить об *овалоидоподобных плоскостях* вместо M-плоскостей.

До сих пор известны лишь овалоидоподобные мёбиусовы плоскости; свойства этих плоскостей зависят от свойств соответствующих оваломидов.

Соберем теперь факты, касающиеся числа точек и циклов на M-плоскости порядка q :

M₁. Число всех точек плоскости есть $q^2 + 1$.

M₂. Число всех циклов есть $q(q^2 + 1)$.

M_3 . Каждый цикл инцидентен $q + 1$ точкам.

M_4 . Каждая точка инцидентна $q(q + 1)$ циклам.

M_5 . Каждый гиперболический пучок состоит из $q + 1$ циклов.

M_6 . Каждый параболический пучок состоит из q циклов.

M_7 . Каждый эллиптический пучок состоит из $q - 1$ циклов.

Заметим, что число циклов гиперболического пучка в точности равно числу точек одного цикла.

Отношения инцидентности в конечной плоскости можно весьма прозрачным образом изобразить в виде матрицы инцидентности. Эта матрица получается из таблицы инцидентности вписыванием 0 в каждый пустой квадрат и заменой каждого знака инцидентности на 1. Полезность матрицы инцидентности мы уже показали при рассмотрении экстремальной комбинаторной задачи. Теперь нас будет интересовать, сколько раз символ 1 содержится в матрице инцидентности, когда имеются n элементов и m блоков, т. е. в матрице из n столбцов и m строк, если столбцы рассматриваются как точки, а строки как циклы, причем 1 и 0 обозначают соответственно инцидентность и неинцидентность. Предполагается, что система точек и циклов удовлетворяет требованиям системы аксиом K^*). Число всех символов 1 в матрице обозначим η .

Из аксиомы K_4 следует, что матрица содержит не менее 4 столбцов. Из K_2 следует, что в матрице не менее 4 строк. Таким образом, $\eta \geq 12$.

Количества единиц, содержащихся в строках матрицы, обозначим соответственно $\lambda_1, \lambda_2, \dots, \lambda_m$, в столбцах — $\pi_1, \pi_2, \dots, \pi_n$. Очевидно,

$$(5.4.1) \quad \lambda_1 + \lambda_2 + \dots + \lambda_m = \pi_1 + \pi_2 + \dots + \pi_n = \eta.$$

Сами векторы строк, соответственно столбцов, обозначим x_1, \dots, x_m и y_1, \dots, y_n . Установим ряд соотношений между числами λ, π и векторами x, y .

Очевидно, $x_j^2 = \lambda_j$ и $y_j^2 = \pi_j$, так что

$$(5.4.2) \quad \begin{cases} x_1^2 + x_2^2 + \dots + x_m^2 = \lambda_1 + \lambda_2 + \dots + \lambda_m = \eta, \\ y_1^2 + y_2^2 + \dots + y_n^2 = \pi_1 + \pi_2 + \dots + \pi_n = \eta. \end{cases}$$

*) В последующих рассуждениях это предположение, по существу, не используется. — Прим. перев.

Для сумм векторов-строк, соответственно векторов-столбцов, мы имеем, с одной стороны, соотношения

$$(5.4.3) \quad \begin{cases} (x_1 + x_2 + \dots + x_m)^2 = \pi_1^2 + \pi_2^2 + \dots + \pi_n^2, \\ (y_1 + y_2 + \dots + y_n)^2 = \lambda_1^2 + \lambda_2^2 + \dots + \lambda_m^2, \end{cases}$$

а с другой — соотношения

$$(5.4.4) \quad \begin{cases} \left(\sum_1^m x_j\right)^2 = \sum_1^m x_j^2 + \sum_1^m x_j x_k, \\ \left(\sum_1^n y_j\right)^2 = \sum_1^n y_j^2 + \sum_1^n y_j y_k \end{cases} \quad (j \neq k).$$

Сопоставляя (5.4.2) — (5.4.4), находим

$$(5.4.5) \quad (\lambda_1^2 + \lambda_2^2 + \dots + \lambda_m^2) - \\ - (\lambda_1 + \lambda_2 + \dots + \lambda_m) = \sum_1^n y_j y_k.$$

Обозначим скалярное произведение $y_j y_k$ через ω_{jk} ($j \neq k$). Пусть наибольшее из этих чисел есть ω . Так как число таких произведений есть $n(n-1)$, находим из (5.4.5)

$$(5.4.6) \quad (\lambda_1^2 + \lambda_2^2 + \dots + \lambda_m^2) - (\lambda_1 + \lambda_2 + \dots + \lambda_m) \leq \\ \leq \omega n(n-1),$$

где равенство достигается в том и только в том случае, когда любое из чисел ω_{jk} равно ω (условие (α)).

Хорошо известно, что для любого набора чисел c_1, c_2, c_s справедливо неравенство

$$c_1^2 + c_2^2 + \dots + c_s^2 \geq \frac{(c_1 + c_2 + \dots + c_s)^2}{s},$$

причем знак равенства имеет место только в случае $c_1 = c_2 = \dots = c_s$ (условие (β)). Отсюда и из (5.4.6) имеем следующее неравенство:

$$\frac{\eta^2}{m} - \eta \leq \omega n(n-1).$$

В свою очередь из этого неравенства, а также из $\eta > 0$ следует

$$(5.4.7) \quad 2\eta \leq m + \sqrt{m^2 + 4\omega mn(n-1)},$$

причем равенство имеет место в том и только в том случае, когда выполнены оба условия (α) и (β) .

Сформулируем каждое из этих условий в терминах инверсной геометрии. Условие (α) означает, что через каждые две точки должно проходить одно и то же число циклов. Условие (β) означает, что каждый цикл должен содержать одно и то же число точек; пусть это число есть v . Формулируя для таблицы инцидентностей полученные результаты, можно сказать следующее.

Для данных ω , m , n рассмотрим все таблицы инцидентностей типа $m \times n$ такие, что число строк, пересекающих некоторые два столбца по квадратам, содержащим знак \bullet , не больше ω , и существует пара столбцов, для которой это число равно ω . Назовем таблицы такого рода $\theta(\omega; m, n)$ -таблицами. Пусть η обозначает число всех знаков \bullet в таблице. Для $\theta(\omega; m, n)$ -таблиц число η не может превышать границы, определенной неравенством (5.4.7); обозначая эту границу через $E(\omega; m, n)$, можем записать

$$\eta \leq E(\omega; m, n).$$

Число η достигает своей верхней границы E тогда и только тогда, когда каждые два столбца пересекают в точности ω строк по квадратам, содержащим знак инцидентности, и при этом каждая строка содержит одно и то же число v знаков инцидентности.

Легко видеть, что если $\theta(\omega; m, n)$ -таблица удовлетворяет этим условиям, т. е. имеет указанное выше экстремальное свойство, то она характеризуется некоторой степенью регулярности также и относительно своих столбцов: в каждом из столбцов имеется одно и то же число знаков инцидентности.

Мы докажем это утверждение с помощью одного вспомогательного понятия. Назовем *звеном* таблицы любую пару знаков инцидентности, расположенных в одной и той же строке; под *членами звена* будем понимать два столбца, содержащие знаки инцидентности данного звена.

Определим теперь, скольким звеньям может принадлежать (как член звена) произвольно выбранный столбец P_j . Подсчет можно осуществить двумя различными способами:

1° π_j строк таблицы пересекают столбец P_j по квадратам, содержащим знак инцидентности, и в каждой из этих строк имеется еще $v - 1$ знаков. Отсюда число звеньев, членом которых является P_j , равно $\pi_j (v - 1)$.

2° Столбец P_j входит в $n - 1$ пар столбцов таблицы. Каждая пара столбцов содержит ω звеньев. Отсюда число звеньев, членом которых является P_j , равно $\omega (n - 1)$.

Сопоставляя результаты двух подсчетов, находим

$$(5.4.8) \quad \pi_j = \frac{\omega (n - 1)}{v - 1}.$$

Отсюда и следует наше утверждение: $\pi_1 = \pi_2 = \dots = \pi_n (= \mu)$.

Таким образом, инверсные геометрии могут служить источником экстремальных таблиц. При этом согласно M_1, M_2, M_5 имеем

$$n = q^2 + 1, \quad m = q (q^2 + 1), \quad \omega = q + 1,$$

а согласно M_3, M_4 $v = q + 1, \mu = q (q + 1)$. Подставляя значения m, n, ω в (5.4.7), получим справа следующее число:

$$2q (q + 1) (q^2 + 1).$$

5.5. Структура инцидентности и t -блок-схема

1° Блок-схему $t(v, k, \lambda)$ можно рассматривать как некоторую специальную структуру инцидентности. Соответствующая таблица инцидентности характеризуется следующими свойствами:

(1) В каждой строке таблицы имеется ровно k знаков инцидентности:

$$\lambda_1 = \lambda_2 = \dots = \lambda_m = k.$$

(2) Для любых t столбцов существуют ровно λ строк, пересекающих каждый из этих столбцов по квадратам, содержащим знак инцидентности.

Из этих свойств t -блок-схемы вытекает еще одно свойство:

(3) Все столбцы содержат одно и то же число знаков инцидентности.

Доказательство (3) будет дано позже; сначала сделаем ряд замечаний.

Рисунок 102 представляет блок-схему $3\text{--}(10, 4, 1)$. В предыдущем параграфе мы упоминали о том, что эту схему можно также рассматривать как блок-схему $2\text{--}(10, 4, 4)$. (А именно, каждая пара точек на M -плоскости порядка 3 инцидентна в точности четырем циклам.)

В действительности справедлива следующая

Т е о р е м а. *Каждая t -блок-схема есть одновременно t' -блок-схема для любого целого $t', 2 \leq t' \leq t$.*

Пусть θ есть таблица инцидентности блок-схемы $t\text{--}(v, k, \lambda)$. Тогда число строк, пересекающих любые t столбцов по заполненным квадратам (т. е. квадратам, содержащим знак инцидентности), есть одно и то же число λ . Выберем какие-либо $t - 1$ столбцов таблицы θ . Рассмотрим строки, пересекающие каждый из этих столбцов по заполненным квадратам; пусть число таких строк равно m . Если мы исключим остальные строки, а также выбранные $t - 1$ столбцов, то останется таблица θ' , которая будет содержать $v' = v + 1 - t$ столбцов и m строк. Каждый столбец таблицы θ' пересекает ровно λ строк по заполненным квадратам. Отсюда число звеньев в θ' будет $v'\lambda = \lambda(v + 1 - t)$. Это число можно подсчитать и при помощи строк. Первоначально каждая строка содержала k знаков, после же удаления в каждой строке таблицы θ' остается только $k + 1 - t$ знаков. Отсюда общее число знаков в таблице θ' есть $m(k + 1 - t)$. Сравнивая оба подсчета, имеем

$$m = \lambda \frac{v + 1 - t}{k + 1 - t}.$$

Это число не зависит от выбора $t - 1$ удаленных строк; оно полностью определяется параметрами t, v, k, λ первоначальной блок-схемы. Теперь ясно, что первоначальную блок-схему $t\text{--}(v, k, \lambda)$ можно рассматривать как блок-схему $t'\text{--}(v, k, \lambda')$, где $t' = t - 1$, а $\lambda' = m$. Повторяя это рассуждение пужное число раз, докажем нашу теорему.

Вернемся теперь к доказательству свойства (3) t -блок-схемы.

Данная нам θ -таблица блок-схемы $t\text{--}(v, k, \lambda)$, по доказанному, является в то же время таблицей блок-схемы $2\text{--}(v, k, \lambda^*)$. Как было показано в конце предыдущего параграфа, каждый столбец блок-схемы $2\text{--}(v, k, \lambda^*)$ содер-

жит одно и то же число знаков инцидентности, что и доказывает (3).

2° Назовем *автоморфизмом* t -блок-схемы точечное взаимно однозначное отображение, которое блоки отображает в блоки. В этом смысле мы говорим об отображении, *сохраняющем блоки*, а также об *образе* блока.

Автоморфизмы t -блок-схемы образуют группу.

Если элементы t -блок-схемы обозначить $1, 2, \dots, v$, то каждый автоморфизм может быть выражен подстановкой множества $\{1, 2, \dots, v\}$. Таким образом, группа всех автоморфизмов t -блок-схемы превращается в подгруппу полной группы S_v подстановок степени v .

В последние годы изучение групп подстановок сильно способствовало изучению t -блок-схем.

Группа, образованная всеми автоморфизмами t -блок-схемы, называется *полной группой автоморфизмов*, а ее подгруппы называются просто *группами автоморфизмов*.

Группа P_n подстановок множества $H = \{1, 2, \dots, n\}$ называется *k -транзитивной*, если для любых двух подмножеств множества H , состоящих из k элементов:

$$X = \{x_1, x_2, \dots, x_k\}, \quad Y = \{y_1, y_2, \dots, y_k\},$$

существует подстановка $\pi \in P_n$ такая, что

$$y_j = x_j^\pi \quad (j = 1, 2, \dots, k).$$

Очевидно, если группа k -транзитивна на множестве H , то она и h -транзитивна для любого $h \leq k$.

Приведем (без доказательства) теорему из теории групп подстановок.

Т е о р е м а (Кофман). Пусть M есть плоскость Мёбиуса порядка q , группа автоморфизмов которой A отображает подмножество H плоскости M , состоящее из k ($> q + 1$) точек, в себя, причем индуцированная ею на H группа подстановок 3-транзитивна. Тогда H совпадает с M и в плоскости M справедлива теорема Мизуэля.

5.6. Задачи и упражнения к главе 5

38. Найдите полную группу автоморфизмов графа Петерсена. (Связь с полной группой автоморфизмов D -конфигурации упрощает решение этой задачи.)

39. Докажите, что порядок любой группы подстановок, транзитивной на множестве H , делится на число элементов в H .

40. Докажите, что транзитивная абелева группа всегда регулярна.

41. Пусть $q = 2^r$. С помощью квадратки

$$x_1x_2 + x_3x_4 + \rho x_3^2 + \rho x_4^2 = 0,$$

определенной над координатным полем $K = GF(2^r)$, строится плоскость Мёбиуса, где элемент $\rho \in K$ обладает тем свойством, что $\rho x^2 + x + \rho$ есть неприводимый полином над K . Воспользовавшись этим, составьте таблицу инцидентности для плоскости Мёбиуса порядка 4.

42. Постройте таблицу инцидентности плоскости Мёбиуса порядка 2 и найдите полную группу автоморфизмов этой плоскости.

НЕКОТОРЫЕ ДОПОЛНИТЕЛЬНЫЕ ВОПРОСЫ ТЕОРИИ КОНЕЧНЫХ ГЕОМЕТРИЙ

В этой последней главе мы расскажем выборочно о полученных сравнительно недавно интересных результатах в теории конечных геометрий.

6.1. Плоскость Фано и теорема Глисона

Фано впервые обратил внимание на важную роль, которую играют в теории конечных геометрий плоскости — названные затем плоскостями Фано, — в которых диагональные точки любого полного четырехугольника коллинеарны. Спустя более половины столетия (в 1956 г.) появилась фундаментальная теорема Глисона, раскрывающая структурные свойства этого класса конечных проективных плоскостей. Оказалось, что любая плоскость Фано изоморфна плоскости Галуа четного порядка. Таким образом, изучение проективных пространств, в которых каждый плоский четырехугольник есть четырехугольник Фано, уже не связано с какими-либо новыми принципиальными проблемами, изучение этих пространств можно считать, с указанной выше точки зрения, завершенным.

1° Докажем сначала лемму, относящуюся к плоскостям Фано; из этой леммы следует, что порядок каждой плоскости Фано есть четное число.

Л е м м а. Плоскость Фано допускает координатную структуру, в которой порядок каждого элемента абелевой группы, порожденной сложением точек, в точности равен 2.

Д о к а з а т е л ь с т в о. Рассмотрим операцию сложения точек, для иллюстрации которой нам служил рис. 62 на стр. 187. Все, что можно получить в этой связи без использования теоремы Дезарга, т. е. опираясь только на аксиомы системы I, справедливо для каждой плоскости Фано. Таким образом, мы должны доказать, не используя D-теорему, что для любых трех точек A, B, C пря-

мой e , отличных от точки Z , т. е. для любых трех точек A, B, C множества e^* , имеют место равенства

$$A + A = O, \quad A + B = B + A,$$

$$(A + B) + C = A + (B + C).$$

Рассмотрим сначала сумму $A + A$. Согласно нашему допущению, диагональные точки четырехугольника $OAUV$, т. е. точки $OU \cap AV = Y$, $OA \cap UV = Z$ и $UA \cap OV = R$, лежат на одной прямой (на рис. 62 это идеальная прямая плоскости). Поскольку теперь $B = A$, прямые AU и UX совпадают, откуда следует $R = X$. Таким образом, O, V, X коллинеарны, и точка $OZ \cap VX$, играющая роль суммы $A + A$, совпадает с O . Этим доказано, что порядок каждого элемента равен 2.

Докажем теперь, что $A + B = B + A$ (для иллюстрации см. рис. 103). Рассмотрим

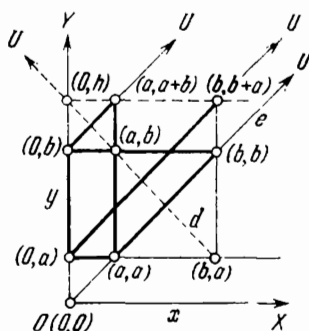


Рис. 103.

следующие три четырехугольника, вершины которых заданы своими неоднородными координатами:

$$\alpha: \{(b, b), (a, a), X, Y\},$$

$$\beta: \{(a, a+b), (0, b), X, Y\},$$

$$\gamma: \{(b, b+a), (0, a), X, Y\}.$$

Диагональные точки этих четырехугольников образуют следующие коллинеарные тройки:

$$\{U, (a, b), (b, a)\}, \quad \{U, (a, b), (0, a+b)\},$$

$$\{U, (b, a), (0, b+a)\}.$$

Отсюда, в свою очередь, вытекает коллинеарность пяти точек:

$$U, (a, b), (b, a), (0, a+b), (0, b+a).$$

Последние две точки должны совпадать, так как в противном случае соединяющая их прямая u должна проходить через точку U . Итак, $(0, a+b)$ и $(0, b+a)$ совпадают, и $A + B = B + A$.

Таким образом, следующие пять точек оказываются **коллинеарными**:

$$U, (c, a + b), (a, b + c), (0, a + (b + c)), \\ (0, (a + b) + c).$$

Если бы последние две из этих точек не совпадали, то соединяющая их прямая u должна была бы пройти через точку U , что невозможно. Следовательно, эти точки совпадают, откуда имеем

$$a + (b + c) = (a + b) + c,$$

— ассоциативность сложения доказана. Тем самым доказана и вся лемма.

Итак, операция сложения точек превращает множество e^* в абелеву группу, в которой порядок каждого элемента равен 2. В силу хорошо известной теоремы теории групп, если каждый элемент абелевой группы имеет порядок 2, то порядок всей группы есть 2^n .

Еще раз отметим тот факт, что в доказательстве леммы мы ни разу не использовали теорему Дезарга.

2° Плоскость Фано обладает R-свойством (см. параграф 3.4) при любом выборе трех коллинеарных точек X, Y, Z . Рассмотрим множество, элементами которого являются прямые, проходящие через точку X , причем каждая из этих прямых берется без точки X ; обозначим это множество через $\{x\}$. Подобным же образом пучок прямых, проходящих через точку Y , образует множество $\{y\}$ и пучок с центром Z — множество $\{z\}$. Семейства прямых $\{x\}, \{y\}, \{z\}$ образуют R-сеть; этот факт эквивалентен ассоциативности операции, порожденной сетью *), а как мы видели, ассоциативность имеет место в случае плоскости Фано. Глисон был первым, кто сделал далеко идущие следствия из этого факта; он дал новое истолко-

) Обратимся к рис. 62. Параметризуем каждое из семейств $\{x\}, \{y\}, \{z\}$ точками множества e^ , а именно: любой прямой пучка $\{x\}$ или $\{y\}$ сопоставим точку пересечения этой прямой с прямой e , а любой прямой UV пучка $\{z\}$ — точку B . При такой параметризации отображение $A, B \mapsto A + B$ превращается в отображение $y, z \mapsto x$, ставящее в соответствие прямым y и z прямую x , проходящую через точку $y \cap z$, т. е. в операцию, связанную с сетью $\{y\}, \{z\}, \{x\}$. — *Прим. перев.*

вание R-конфигурации, которое будет ниже названо *G-условием*. Введем сначала ряд новых понятий.

Пусть l -произвольная прямая на плоскости Фано и A, B, U — три различные точки этой прямой (рис. 105). Пусть, далее, i и r — прямые, проходящие через U и отличные от l . Если наша плоскость имеет порядок q , то точки

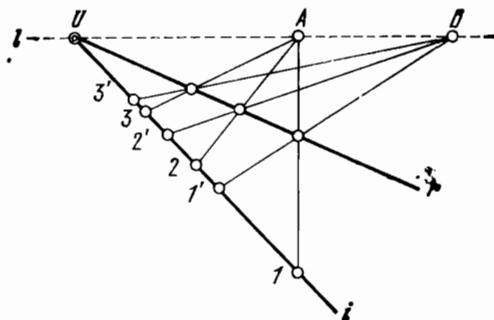


Рис. 105.

прямой i , отличные от U , можно снабдить номерами $1, 2, \dots, q$. Проектируя точки $1, 2, \dots, q$ из A на прямую r , получим отображение множества $i \setminus U$ на $r \setminus U$; обозначим это отображение $[i_r^\alpha]$ *). Взяв его композицию с проектированием $[r_i^\beta]$, получим отображение

$$(6.1.1) \quad \begin{bmatrix} \alpha \\ i r \end{bmatrix} \begin{bmatrix} \beta \\ r i \end{bmatrix}$$

множества $i \setminus U$ на себя, т. е. подстановку множества $\{1, 2, \dots, q\}$ (образы точек $1, 2, \dots, q$ при этой подстановке обозначены на рис. 105 через $1', 2', \dots, q'$). Различным положениям прямой r отвечают q таких подстановок; обозначим совокупность этих подстановок через

$$(6.1.2) \quad \left(\begin{matrix} \alpha \beta \\ i \end{matrix} \right).$$

*) Более логичным было бы обозначение $\begin{bmatrix} A \\ i r \end{bmatrix}$. — Прим. перев.

Очевидно, множество (α_i^β) подстановок просто транзитивно на множестве точек $i \setminus U$. Это означает, что если $P \in i \setminus U$ и $P' \in i \setminus U$, то существует в точности одна прямая r такая, что подстановка (6.1.1) переводит P в P' . Действительно, эта прямая должна соединять U с $AP \cap BP'$.

Аналогичным образом, произведение проектирований

$$(6.1.3) \quad \begin{bmatrix} \alpha \\ ir \end{bmatrix} \begin{bmatrix} \beta \\ rs \end{bmatrix} \begin{bmatrix} \alpha \\ sj \end{bmatrix} \begin{bmatrix} \beta \\ jt \end{bmatrix} = \pi$$

является подстановкой множества $i \setminus U$ (рис. 106). Разумеется, эта подстановка может обладать свойством — как

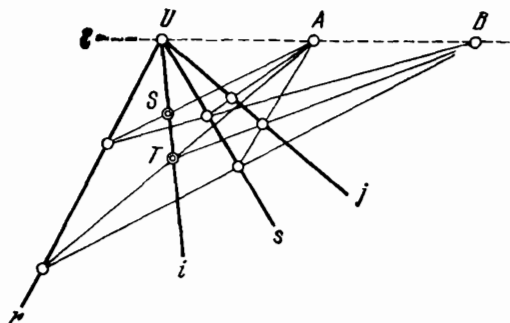


Рис. 106.

это показано на рисунке — оставлять некоторую точку $T \in i \setminus U$ неподвижной. В связи с этим мы формулируем следующее

Условие Г. Если при некотором выборе трех различных точек U, A, B на прямой l , а также четырех прямых i, j, r, s , проходящих через U , подстановка π имеет неподвижную точку в множестве $i \setminus U$, то и любая другая точка этого множества неподвижна относительно π .

Если мы сравним точки U, A, B рис. 106 с точками Z, X, Y рис. 90, то легко обнаружим, что условие Г эквивалентно условию R.

3° Вернемся к рассмотрению множества (α_i^β) подстановок. В этом множестве всегда существует подстановка, оставляющая на месте каждый элемент из $i \setminus U$; чтобы получить эту подстановку, мы полагаем в (6.1.1) $r = i$.

Для каждой подстановки, принадлежащей $\left(\begin{smallmatrix} \alpha\beta \\ i \end{smallmatrix}\right)$, обратная подстановка снова принадлежит $\left(\begin{smallmatrix} \alpha\beta \\ i \end{smallmatrix}\right)$ (рис. 107). Чтобы это доказать, рассмотрим какую-либо точку $S \in i \setminus U$ и ее образ S' при подстановке $\begin{bmatrix} \alpha \\ ir \end{bmatrix} \begin{bmatrix} \beta \\ ri \end{bmatrix}$. Прямая j , соединяющая точку U с $S'A \cap SB$, совместно с прямыми $s = i$ и r образует четверку прямых (i, r, s, j) такую, что подстановка π , индуцированная этой четверкой, оставляет

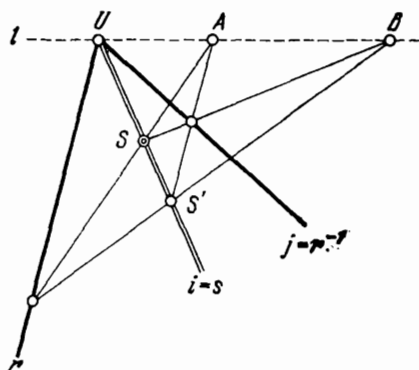


Рис. 107.

точку S неподвижной. Но тогда, в силу условия G, каждая точка из $i \setminus U$ неподвижна относительно π , а значит, подстановка $\begin{bmatrix} \alpha \\ ij \end{bmatrix} \begin{bmatrix} \beta \\ ji \end{bmatrix}$, индуцированная прямой j , обратна подстановке $\begin{bmatrix} \alpha \\ ir \end{bmatrix} \begin{bmatrix} \beta \\ ri \end{bmatrix}$, индуцированной прямой r . На рисунке этот факт выражен записью $j = r^{-1}$.

Произведение любых двух подстановок из множества $\left(\begin{smallmatrix} \alpha\beta \\ i \end{smallmatrix}\right)$ есть снова подстановка из $\left(\begin{smallmatrix} \alpha\beta \\ i \end{smallmatrix}\right)$. Чтобы это доказать, рассмотрим подстановки, индуцированные r и s (соответственно), где r и s — любые две прямые, проходящие через U и отличные от l . На рис. 108 показано последовательное действие этих подстановок на элемент $1 \in i \setminus U$. Подстановка

$$- \begin{bmatrix} \alpha \\ ir \end{bmatrix} \begin{bmatrix} \beta \\ ri \end{bmatrix} = [r],$$

индуцированная r , переводит точку 1 в точку $S = 3$.
Подстановка

$$\begin{bmatrix} \alpha \\ is \end{bmatrix} \begin{bmatrix} \beta \\ si \end{bmatrix} = [s],$$

индуцированная s , переводит точку $S = 3$ в точку 5. Следовательно, произведение подстановок $[r]$ и $[s]$ переводит 1 в 5. Однако существует прямая j такая, что подстановка

$$\begin{bmatrix} \alpha \\ ij \end{bmatrix} \begin{bmatrix} \beta \\ ji \end{bmatrix} = [j]$$

также переводит 1 в 5. Таким образом, подстановки $[r][s]$ и $[j]$ оказывают одно и то же действие на точку 1. Ввиду

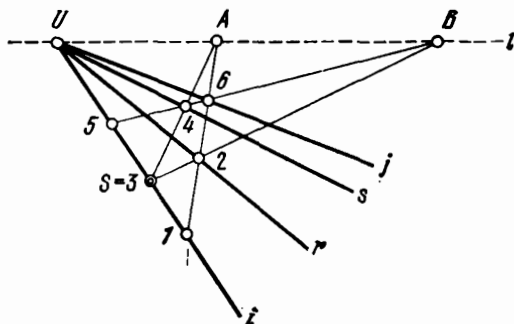


Рис. 108.

справедливости условия G отсюда следует, что $[r][s]$ и $[j]$ одинаково действуют на любую точку из $i \setminus U$. Значит, $[r][s] = [j]$ и $[j] \in \begin{pmatrix} \alpha\beta \\ i \end{pmatrix}$.

Итак, рассматриваемое множество $\begin{pmatrix} \alpha\beta \\ i \end{pmatrix}$ подстановок содержит тождественную подстановку, вместе с каждой подстановкой содержит обратную и вместе с любыми двумя подстановками содержит их произведение. Следовательно, это множество есть группа.

Обратно, если исходить из предположения, что множество $\begin{pmatrix} \alpha\beta \\ i \end{pmatrix}$ является группой, то условие G будет выполняться. В самом деле, пусть подстановка $[r][s]$ оставляет

неподвижной некоторую точку множества $i \setminus U$, скажем, точку 1. Поскольку $[r]$ $[s]$ совпадает с некоторой подстановкой $[j]$, то отсюда находим, что $[j]$ оставляет неподвижной точку 1. Но в таком случае прямая j совпадает с i , т. е. $[j]$ — тождественная подстановка. Тем самым, справедливо условие G .

Тот факт, что множество $\left(\begin{smallmatrix} \alpha \\ i \end{smallmatrix} \right)$ подстановок образует группу, будем называть *условием* G^* . Тогда полученный нами результат может быть сформулирован как

Л е м м а Г л и с о н а. Условие G (а значит, и R) эквивалентно G^* .

Подчеркнем, что наши утверждения относятся к любому выбору прямой l на плоскости.

4° Мы будем теперь изучать строение плоскости порядка q , удовлетворяющей условию G , связывая этот вопрос со *сдвигами* (элациями) на плоскости. Очевидно, сдвиги всегда существуют — примером их может служить тождественное отображение. Если пара (U, l) определяет более чем один сдвиг, то во всяком случае число таких сдвигов не больше q . Сдвиги, определяемые (U, l) , образуют группу; эта группа будет обозначаться $\Gamma(U, l)$.

Каждый элемент этой группы индуцирует на прямой i , проходящей через U , подстановку, сохраняющую U ; эта подстановка, если только она отлична от тождества, не имеет других неподвижных точек, кроме U . Так как элемент группы $\Gamma(U, l)$ однозначно определяется парой точек (P, P') (отличных от U) прямой i (где P' есть образ P), то подстановки, индуцированные на прямой i сдвигами из $\Gamma(U, l)$, взаимно однозначным образом представляют элементы группы $\Gamma(U, l)$.

Условимся выражать записью $P' = P \cdot \omega$ тот факт, что точка P' есть образ точки P при отображении ω прямой i на себя. Для любого сдвига $\omega \in \Gamma(U, l)$ имеет место соотношение коммутативности

$$(6.1.4) \quad \left[\begin{smallmatrix} \alpha \\ ij \end{smallmatrix} \right] \omega = \omega \left[\begin{smallmatrix} \alpha \\ ij \end{smallmatrix} \right].$$

Рисунок 109 поясняет это равенство: точки $P, Q = P \cdot \left[\begin{smallmatrix} \alpha \\ ij \end{smallmatrix} \right]$, A коллинеарны, точки P', Q', A' — тоже, при этом $A' = A$. Вместо P', Q', A' , разумеется, можно записать

$P \cdot \omega$, $P \cdot \begin{bmatrix} \alpha \\ ij \end{bmatrix} \cdot \omega$, A . Мы видим, что точка $P \cdot \begin{bmatrix} \alpha \\ ij \end{bmatrix} \cdot \omega$ есть не что иное, как проекция точки $P \cdot \omega$ из A на прямую j , —

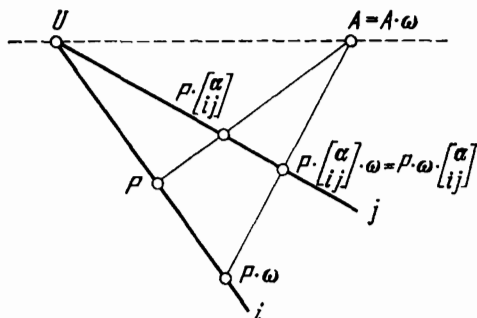


Рис. 109.

в этом и состоит как раз условие (6.1.4). Как следствие имеем еще одно правило коммутативности:

$$(6.1.5) \quad \omega \begin{bmatrix} \alpha \\ ir \end{bmatrix} \begin{bmatrix} \beta \\ ri \end{bmatrix} = \begin{bmatrix} \alpha \\ ir \end{bmatrix} \begin{bmatrix} \beta \\ ri \end{bmatrix} \omega,$$

где прямая r проходит через U .

Очевидно, справедливы соотношения

$$(6.1.6) \quad \begin{bmatrix} \alpha \\ ij \end{bmatrix} \begin{bmatrix} \alpha \\ jk \end{bmatrix} = \begin{bmatrix} \alpha \\ ik \end{bmatrix} \text{ и } \begin{bmatrix} \alpha \\ ij \end{bmatrix} \begin{bmatrix} 1 \\ jl \end{bmatrix} = 1,$$

где i, j, k суть прямые, проходящие через U , и 1 обозначает тождественное отображение.

Рассмотрим теперь на прямой i какую-нибудь подстановку σ , которая коммутирует с каждой подстановкой $\begin{bmatrix} \alpha \\ ij \end{bmatrix} \begin{bmatrix} \beta \\ ji \end{bmatrix}$, где j — любая прямая (отличная от l), проходящая через U , и $A \in l, B \in l, A \neq U \neq B \neq A$. Докажем, что σ можно расширить до отображения σ^* всей плоскости такого, что $\sigma^* \in \Gamma(U, l)$.

Пусть P — точка плоскости, не инцидентная прямым i и l ; прямую PU обозначим j (рис. 110). Действие искомого отображения σ^* на P можно получить, взяв произвольную точку A , отличную от U , на прямой l . А именно, положим

$$P \cdot \sigma^* = P \cdot \begin{bmatrix} \alpha \\ ji \end{bmatrix} \cdot \sigma \cdot \begin{bmatrix} \alpha \\ ij \end{bmatrix}.$$

В случае, когда $P \in l$, положим

$$P \cdot \sigma^* = P.$$

Определенное таким образом отображение σ^* есть коллинеация. Чтобы доказать это, достаточно рассмотреть действие σ^* на любую тройку коллинеарных точек, из которых одна лежит на фиксированной прямой l . (Ибо, если каждая из троек X, Y, V и Y, Z, V коллинеарна, где

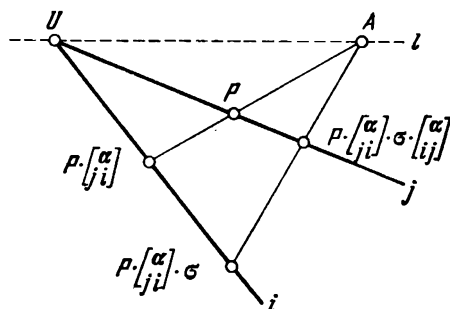


Рис. 110.

$V \in l$, то X, Y, Z есть также коллинеарная тройка.) Пусть точки P и Q лежат соответственно на прямых j и k , проходящих через U и отличных друг от друга, а также от прямых l и i ; пусть, далее, $PQ \cap l = B \neq A$. Пусть $P' = P \cdot \sigma^*$ и $Q' = Q \cdot \sigma^*$, $B' = B \cdot \sigma^*$; очевидно, $B' = B$. Мы должны проверить коллинеарность точек B, P', Q'

Из коллинеарности B, P, Q следует

$$P \cdot \left[\begin{smallmatrix} \beta \\ jk \end{smallmatrix} \right] = Q.$$

Далее, проекция точки P' (лежащей вместе с P на прямой j) из точки B на прямую k может быть записана в виде

$$P' \cdot \left[\begin{smallmatrix} \beta \\ jk \end{smallmatrix} \right] = P \cdot \sigma^* \cdot \left[\begin{smallmatrix} \beta \\ jk \end{smallmatrix} \right],$$

откуда следует, если учесть определение σ^* , а также соотношения (6.1.5) и (6.1.6), что

$$\begin{aligned} P' \cdot \begin{bmatrix} \beta \\ jk \end{bmatrix} &= P \cdot \begin{bmatrix} \alpha \\ ji \end{bmatrix} \cdot \sigma \cdot \begin{bmatrix} \alpha \\ ij \end{bmatrix} \cdot \begin{bmatrix} \beta \\ jk \end{bmatrix} = \\ &= P \cdot \begin{bmatrix} \alpha \\ ji \end{bmatrix} \cdot \sigma \cdot \begin{bmatrix} \alpha \\ ij \end{bmatrix} \begin{bmatrix} \beta \\ ji \end{bmatrix} \cdot \begin{bmatrix} \beta \\ ik \end{bmatrix} \begin{bmatrix} \alpha \\ ki \end{bmatrix} \cdot \begin{bmatrix} \alpha \\ ik \end{bmatrix} = \\ &= P \cdot \begin{bmatrix} \alpha \\ ji \end{bmatrix} \cdot \begin{bmatrix} \alpha \\ ij \end{bmatrix} \begin{bmatrix} \beta \\ ji \end{bmatrix} \cdot \begin{bmatrix} \beta \\ ik \end{bmatrix} \begin{bmatrix} \alpha \\ ki \end{bmatrix} \cdot \sigma \cdot \begin{bmatrix} \alpha \\ ik \end{bmatrix} = \\ &= P \cdot \begin{bmatrix} \beta \\ jk \end{bmatrix} \cdot \begin{bmatrix} \alpha \\ ki \end{bmatrix} \cdot \sigma \cdot \begin{bmatrix} \alpha \\ ik \end{bmatrix}. \end{aligned}$$

Таким образом, имеем

$$P' \cdot \begin{bmatrix} \beta \\ jk \end{bmatrix} = Q \cdot \sigma^* = Q'.$$

Это означает, что, проектируя точку P' прямой j из B на прямую k , мы получаем в точности точку Q' . Тем самым коллинеарность точек B, P', Q' доказана. Теперь остается лишь учесть, что $P \cdot \sigma^* = P$, когда $P \in l$, и мы убеждаемся, что σ^* есть сдвиг, т. е. $\sigma^* \in \Gamma(U, l)$.

Полученный нами в этом пункте результат можно сформулировать так.

Вторая лемма Глисона. *Существует взаимно однозначное соответствие между элементами группы $\Gamma(U, l)$ сдвигов и подстановками прямой i , коммутирующими с каждой подстановкой из $\begin{pmatrix} \alpha\beta \\ i \end{pmatrix}$ при любом выборе точек A и B . Подстановки множества $i \setminus U$, принадлежащие $\begin{pmatrix} \alpha\beta \\ i \end{pmatrix}$, представляют сдвиги из $\Gamma(U, l)$.*

5° В этом пункте мы изложим в общих чертах доказательство основной теоремы Глисона, которая устанавливает достаточное условие дезарговости конечной плоскости. Глисон доказал свою теорему, используя некоторые факты, относящиеся к конечным группам. Мы укажем сначала — под названием «теорема Глисона» — следствие из этой теоремы для плоскости Фано. А именно, на плоскости Фано, как мы показали, сложение точек обладает свойством ассоциативности. Этому факту соответствует такое следствие основной теоремы.

Теорема Глисона. *Каждая плоскость Фано дезаргова.*

Сформулируем теперь основной результат.

Основная теорема Глисона. *Если конечная проективная плоскость, порядок которой есть степень простого числа, удовлетворяет условию G^* , то эта плоскость дезаргова.*

Доказательство существенно опирается на теоремы, которые носят сугубо алгебраический характер.

Итак, будем предполагать, что выполняется условие G^* , т. е. что подстановки $\begin{bmatrix} \alpha \\ ij \end{bmatrix} \begin{bmatrix} \beta \\ ji \end{bmatrix}$ образуют группу; последняя обозначается символом $\begin{pmatrix} \alpha\beta \\ i \end{pmatrix}$. Очевидно, подстановка $\begin{bmatrix} \beta \\ ij \end{bmatrix} \begin{bmatrix} \alpha \\ ji \end{bmatrix}$ обратна к $\begin{bmatrix} \alpha \\ ij \end{bmatrix} \begin{bmatrix} \beta \\ ji \end{bmatrix}$. Так как совокупность обратных элементов к элементам данной группы образует ту же самую группу, то имеем равенство

$$(6.1.7) \quad \begin{pmatrix} \alpha\beta \\ i \end{pmatrix} = \begin{pmatrix} \beta\alpha \\ i \end{pmatrix}.$$

Возвращаясь к рис. 106, замечаем, что порядок группы $\begin{pmatrix} \alpha\beta \\ i \end{pmatrix}$ в точности равен порядку плоскости, т. е. p^r , где p — простое. Действительно, если известен образ K' точки K на прямой i , то этим однозначно определяется прямая g , индуцирующая данную подстановку (эта прямая соединяет точку U с $KA \cap K'B$); но образ K' фиксированной точки K может быть выбран $q = p^r$ способами.

Рассмотрим теперь группу всех подстановок множества $i \setminus U$, состоящего из p^r точек; обозначим эту группу Q_i . Пусть $D \in l \setminus U$, $D \neq A$, и пусть прямая j пробегает множество из p^r прямых, проходящих через U и отличных от l . Элементы (подстановки) групп

$$\begin{pmatrix} \alpha\beta \\ i \end{pmatrix} = \begin{pmatrix} \beta\alpha \\ i \end{pmatrix} \text{ и } \begin{pmatrix} \alpha\delta \\ i \end{pmatrix} = \begin{pmatrix} \delta\alpha \\ i \end{pmatrix}$$

можно связать в пары

$$\begin{bmatrix} \beta \\ ij \end{bmatrix} \begin{bmatrix} \alpha \\ ji \end{bmatrix}, \quad \begin{bmatrix} \alpha \\ ij \end{bmatrix} \begin{bmatrix} \delta \\ ji \end{bmatrix}.$$

Произведение подстановок пары есть

$$\begin{bmatrix} \beta \\ ij \end{bmatrix} \begin{bmatrix} \delta \\ ji \end{bmatrix} \in \begin{pmatrix} \beta\delta \\ i \end{pmatrix}.$$

Когда прямая j пробегает множество всех прямых, проходящих через U (кроме l), указанное произведение пробегает все элементы группы $\begin{pmatrix} \alpha\delta \\ i \end{pmatrix}$

Будем обозначать подстановки

$$\begin{bmatrix} \alpha \\ ij \end{bmatrix} \begin{bmatrix} \beta \\ ji \end{bmatrix} \text{ и } \begin{bmatrix} \alpha \\ ij \end{bmatrix} \begin{bmatrix} \delta \\ ji \end{bmatrix}$$

кратко через B_j и D_j . Далее, обозначим подгруппы

$$\begin{pmatrix} \alpha\beta \\ i \end{pmatrix}, \begin{pmatrix} \alpha\delta \\ i \end{pmatrix}, \begin{pmatrix} \beta\delta \\ i \end{pmatrix}$$

группы Q_i символами B, D, G . Таким образом, мы можем сказать, что каждый элемент группы G может быть представлен в виде произведения $B_j D_j$, где $B_j \in B, D_j \in D$; обратно, каждое произведение $B_j D_j$ принадлежит G . Но тогда при любом выборе прямых r и s (проходящих через U) из $B_r D_r \in G, B_s D_s \in G$ следует $(B_r D_r)(B_s D_s) \in G$. Но последняя подстановка, будучи элементом группы G , представима в виде $B_k D_k$:

$$(B_r D_r)(B_s D_s) = B_k D_k.$$

Отсюда следует

$$D_r B_s = (B_r^{-1} B_k)(D_k D_s^{-1}),$$

и, тем самым,

$$D \cdot B \subseteq B \cdot D.$$

Вместе с тем, если воспользоваться равенством

$$B_s^{-1} D_r^{-1} = (D_k D_s^{-1})^{-1} (B_r^{-1} B_k)^{-1},$$

то получим

$$B \cdot D \subseteq D \cdot B.$$

Сопоставляя два включения, находим $B \cdot D = D \cdot B$, т. е.

$$(6.1.8) \quad \begin{pmatrix} \alpha\beta \\ i \end{pmatrix} \begin{pmatrix} \alpha\delta \\ i \end{pmatrix} = \begin{pmatrix} \alpha\delta \\ i \end{pmatrix} \begin{pmatrix} \alpha\beta \\ i \end{pmatrix}.$$

Итак, для пар A, X точек множества $l \setminus U = \{A, B, \dots, L, \dots, Z\}$, где точка A фиксирована, а X пробегает все элементы множества $l \setminus U$, все группы

$\left(\alpha_i^{\xi}\right)$ имеют порядок $q = p^r$ и любые две из этих групп коммутируют.

По хорошо известной теореме *) теории групп *произведение*

$$(6.1.9) \quad K = \left(\alpha_i^{\beta}\right) \cdot \left(\alpha_i^{\lambda}\right) \cdot \left(\alpha_i^{\xi}\right)$$

будет являться p -группой; отсюда, в свою очередь, следует, что центр этой группы содержит подстановки, отличные от тождественной (см. Приложение, стр. 301).

Пусть B есть подстановка, принадлежащая центру группы K и отличная от тождественной. Мы уже видели, что $\left(\alpha_i^{\beta}\right) \left(\alpha_i^{\delta}\right)$ содержит $\left(\beta_i^{\delta}\right)$; следовательно, B коммутирует с каждой из подгрупп $\left(\beta_i^{\delta}\right)$. Но B есть подстановка множества $i \setminus U$; поэтому из доказанной ранее леммы следует, что группа $\Gamma(U, l)$ содержит преобразования, отличные от тождественного. Отсюда, в свою очередь,

со ссылкой на формулируемую ниже теорему Т (также принадлежащую Глисону), следует, что на рассматриваемой нами плоскости верна теорема Дезарга. Этим завершается доказательство теоремы Глисона.

Приведем теперь формулировку теоремы Т.

Т е о р е м а Т. Если группа $\Gamma(U, l)$ сдвигов конечной плоскости, где $U \in l$, содержит преобразования, отличные от тождественного, то в этой плоскости для прямой l и точки U справедливо утверждение теоремы Дезарга.

Доказательства этой теоремы мы не приводим.

Завершающую часть доказательства основной теоремы Глисона можно разделить на следующие две части.

Сначала из условий теоремы Т выводится справедливость микро-теоремы Дезарга для рассматриваемой плоскости (т. е. теоремы Дезарга в специальном случае, когда центр перспективы лежит на оси перспективы). Затем применяется известная

Т е о р е м а Ц о р н а — Л е в и. Любая конечная микро-дезаргова плоскость является дезарговой.

Эта классическая теорема в действительности является алгебраической, ее доказательство редуцируется к дока-

*) Можно считать, что речь идет о следующей теореме: произведение нескольких попарно коммутирующих p -подгрупп конечной группы снова есть p -подгруппа. — Прим. перев.

зательству теоремы Веддербарна, утверждающей, что *каждое конечное тело является полем*.

6° Предпринимались отдельные попытки упростить доказательство теоремы Веддербарна и теоремы Цорна — Леви, так же как и теоремы Глисона.

6.2. Построение новых плоскостей из плоскостей Галуа

Когда в конце прошлого столетия Гильберт показал, что теорема Дезарга не следует из аксиом инцидентности, он использовал метод, который был затем упрощен почти до уровня тривиальности Моултоном (1902 г.) в его остроумной модели. Для начала мы рассмотрим моултоновскую

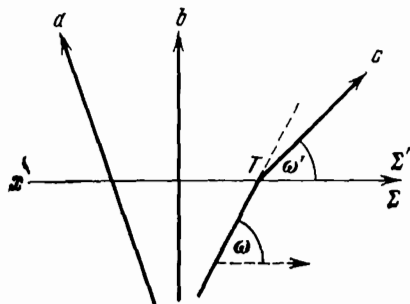


Рис. 111.

модель, затем покажем, как идеи Гильберта и Моултона могут быть использованы в теории конечных проективных плоскостей.

1° Будем исходить из классической проективной плоскости. Изменим определение «прямой», но так, чтобы аксиомы системы I оставались верными в новой «плоскости» (рис.

111). Для этой цели разобьем плоскость осью x на две полуплоскости Σ и Σ' . Каждую прямую, имеющую положительный наклон (к оси x), изменим следующим образом: ее луч, лежащий в полуплоскости Σ' , заменим лучом, имеющим вдвое меньший угловой коэффициент: $\operatorname{tg} \omega = 2 \operatorname{tg} \omega'$. Таким образом, первоначальная прямая изламывается в точке T , и полученная ломаная рассматривается как новая «прямая». Все остальные прямые (т. е. прямые, образующие с осью x тупые или прямые углы, а также параллельные оси x) остаются прежними. Легко показать, что на определенной таким образом плоскости Моултона выполняются аксиомы I_1, I_2, I_3, I_4 — читатель сделает это самостоятельно.

Рассмотрим, далее, на классической проективной плоскости дезаргову конфигурацию, порожденную парой тре-

угольников ABC и $A'B'C'$, перспективных относительно центра D и оси d (рис. 112). Если мы деформируем исходную плоскость в плоскость Моултона, беря в качестве оси x прямую, перпендикулярную d , то структура нашей конфигурации остается неизменной, исключая сторону AB треугольника ABC . На новой плоскости «прямая», соединяющая точки A и B , будет ломаной $BATZ$. Мы можем, следовательно, сказать, что треугольники ABC и $A'B'C'$ на плоскости Моултона перспективны относительно точки D , но не перспективны относительно оси, поскольку точки X , Y и Z , в которых встречаются соответственные стороны, не лежат на одной прямой: $Z \notin d = XY$. Разумеется, на новой плоскости можно указать и такие конфигурации, для которых теорема Дезарга выполняется. Например, если сдвинуть конфигурацию из 10 точек, указанную на рисунке, вниз так, чтобы все точки оказались лежащими в полуплоскости Σ , то получится как раз такой случай.

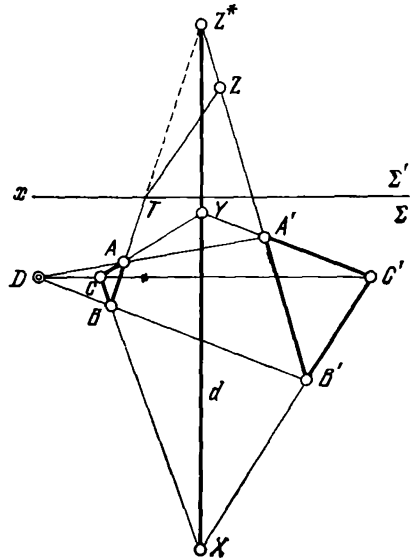


Рис. 112.

Итак, теорема Дезарга независима от аксиом системы I. Аксиомы инцидентности позволяют ввести понятие параллелограмма. Можно ввести также понятия переноса, вектора, сложения векторов, если противоположные стороны параллелограмма интерпретировать как равные векторы. Однако для того, чтобы отношение равенства между векторами было транзитивным, систему аксиом I необходимо расширить.

Пусть на классической аффинной плоскости прямые, несущие векторы $\overline{A_1A_2} = a$, $\overline{B_1B_2} = b$, $\overline{C_1C_2} = c$, раз-

личны и параллельны (рис. 113). В силу MD (микро-дезарговой) теоремы выполнение равенств $a = b$, $a = c$ влечет за собой $b = c$: поскольку $A_1A_2B_2B_1$ и $A_1A_2C_2C_1$ суть параллелограммы, то, в силу MD-теоремы, четырехугольник $B_1B_2C_2C_1$ тоже является параллелограммом. Однако

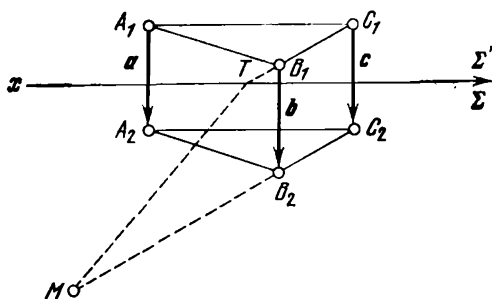


Рис. 113.

если MD-теорема для данной плоскости неверна, то может нарушаться и транзитивность равенства векторов.

Рассмотрим, например, плоскость, полученную из обычной плоскости моултоновской деформацией относительно оси x . На этой плоскости имеем $A_1B_1 \parallel A_2B_2$ и $A_1C_1 \parallel A_2C_2$, однако прямые B_1C_1 и B_2C_2 не параллельны — они пересекаются в некоторой точке M . Следовательно, $b \neq c$, хотя $a = b$ и $a = c$. А

Разумеется, для векторов на плоскости Галуа отношение равенства является транзитивным, поскольку теорема Деарга здесь справедлива без всяких ограничений. Если бы удалось найти для таких плоскостей способ, аналогичный моултоновской конструкции, то оказалось бы возможным получать из плоскостей Галуа недезарговы плоскости. Это — весьма интересная задача, поскольку плоскости Галуа нам хорошо знакомы, тогда как примеров недезарговых конечных плоскостей мы знаем лишь один, а именно плоскость порядка 9. Разумеется, поиск процедуры, аналогичной моултоновской, на плоскости Галуа затруднен тем, что здесь отсутствуют метрические понятия (ясно, что должно соответствовать «излому прямой положительного наклона» в конструкции Моултона).

Дадим теперь подробное описание некоторого способа построения новой плоскости исходя из данной конечной проективной плоскости Σ . Эта новая плоскость Σ' также является проективной плоскостью, ее порядок совпадает с порядком исходной плоскости Σ . Описываемая нами конструкция изменяет некоторое число прямых плоскости Σ , заменяя их таким же числом *искусственных прямых*. Искусственная прямая состоит из того же числа точек, что и прямая плоскости Σ .

Покажем сначала на примере, как осуществить такое построение.

2° Рисунок 114 показывает в сопоставлении таблицы инцидентности для плоскости Галуа Σ порядка 4 и для ее производной плоскости Σ' . Обе плоскости состоят из одних и тех же точек; k -й точке ($k = 1, 2, \dots, 21$) отвечают k -е столбцы обеих таблиц. Строки обеих таблиц, имеющие номера 1, 14, 15, ..., 21, совпадают; строки 2, 3, ..., 13 различны. А именно, прямые $l'_2, l'_3, \dots, l'_{13}$ плоскости Σ' получаются заменой прямых l_2, l_3, \dots, l_{13} плоскости Σ подмножествами из пяти точек (не являющимися прямыми на плоскости Σ), четыре из которых образуют собственный четырехугольник, а пятая есть одна из его диагональных точек. Например, из сравнения таблиц мы видим, что подмножество $l'_2 = \{P_1, P_6, P_7, P_{10}, P_{11}\}$ содержит точки P_1, P_6, P_7 прямой l_2 и точки P_1, P_{10}, P_{11} прямой l_3 ; P_1 есть диагональная точка четырехугольника $P_6P_7P_{10}P_{11}$.

Легко проверить по рис. 114, что подмножества $l'_2, l'_3, \dots, l'_{13}$ представляют собой пятерки точек, принадлежащих следующим прямым плоскости Σ :

$$\begin{array}{cccc} l_2, l_3; & l_3, l_2; & l_4, l_5; & l_5, l_4; \\ l_6, l_8; & l_7, l_9; & l_8, l_6; & l_9, l_7; \\ l_{10}, l_{13}; & l_{11}, l_{12}; & l_{12}, l_{11}; & l_{13}, l_{10}. \end{array}$$

Общая диагональная точка первой четверки четырехугольников есть P_1 , второй — P_2 , третьей — P_3 .

Непосредственным путем можно было бы проверить, что для таблицы Σ' выполняются три аксиомы инцидентности. Однако проще осуществить такую проверку, преобразовав таблицу Σ с помощью перестановки

$$\omega = \begin{pmatrix} 8 & 9 & 10 & 11 & 16 & 17 & 18 & 19 \\ 10 & 11 & 8 & 9 & 18 & 19 & 16 & 17 \end{pmatrix}$$

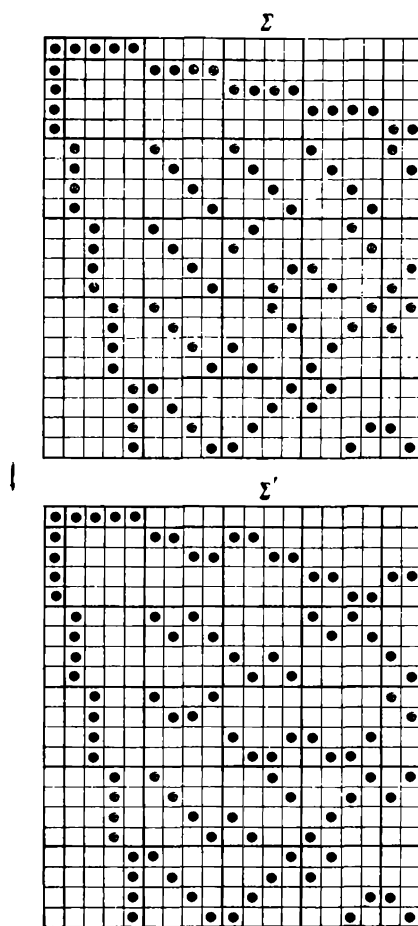


Рис. 114.

ее столбцов (другие столбцы при этом остаются неизменными), а также транспозиции

$$\sigma = \begin{pmatrix} 20 & 21 \\ 21 & 20 \end{pmatrix}$$

строк; получится как раз таблица Σ' . Преобразование $\omega\sigma = \pi$, как и другие подобные ему элементарные преобразования, не нарушает справедливости аксиом I_1, I_2, I_3 . Следовательно, Σ' есть снова таблица инцидентности конечной проективной плоскости порядка 4, что и доказывает наше утверждение.

Мы знаем, однако, что существует лишь одна, с точностью до изоморфизма, плоскость порядка 4, а именно плоскость Галуа порядка 4; поэтому в данном случае наша конструкция не может привести к педзарговой плоскости (в общем случае, однако, это не так, чему примером служит $q = 9$).

Как уже говорилось, искусственная прямая состоит из четырехугольника и одной из его диагональных точек; для четырех таких прямых диагональной точкой является P_1 , для других четырех — P_2 , еще для четырех — P_3 ; остальные две диагональные точки суть (для тех же четверок) идеальные точки P_2 и P_3 , P_3 и P_4 , P_4 и P_2 соответственно *).

Если мы исключим идеальные точки искусственных прямых, то получим 12 множеств вершин четырехугольников исходной плоскости; эти четырехугольники, естественно, являются четырехугольниками Фано **), с общими тройками (коллинеарных) диагональных точек. Из таблицы Σ' можно видеть непосредственно, что любые два из указанных 12 четырехугольников имеют самое большее одну общую вершину. Два четырехугольника, не имеющих общей вершины, определяют искусственные прямые с общей (идеальной) диагональной точкой; такие четырехугольники следовало бы называть параллельными. Каждая собственная (не идеальная) точка плоскости Σ является общей вершиной ровно трех из 12 четырехугольников.

*) Мы принимаем (в данном случае) прямую l_1 за идеальную прямую, а ее точки (в данном случае P_1, P_2, P_3, P_4, P_5) — за идеальные точки.

**) Напомним читателю, что плоскость Галуа четного порядка является плоскостью Фано. — *Прим. перев.*

Далее, из рисунка видно, что каждая из прямых $l_{44} = l'_{44}$, $l_{15} = l'_{15}$, ..., $l_{21} = l'_{21}$ плоскости Σ' , являющихся одновременно прямыми исходной плоскости, содержит одну вершину каждого из 12 четырехугольников (но, разумеется, не содержит ни одной из его диагональных точек).

Как существенный итог проведенного нами анализа отметим следующее: *искусственные прямые плоскости порядка 4 суть подплоскости порядка 2 (тем самым — плоскости Фано), имеющие в качестве идеальных точек три фиксированные идеальные точки исходной плоскости.*

Теперь мы подготовлены к тому, чтобы рассмотреть обобщение разобранного выше примера.

3° Мы будем иметь дело с плоскостями (не обязательно плоскостями Галуа), порядки которых n суть квадраты: $n = q^2$ (при этом q не обязательно является степенью простого числа). Пусть Σ — какая-либо плоскость такого рода, l_1 — прямая плоскости Σ . Будем рассматривать l_1 как идеальную прямую, а ее точки $P_1, P_2, \dots, P_{q^2+1}$ — как идеальные точки. Если исключить из Σ идеальные элементы, получим аффинную плоскость, состоящую из $n^2 = q^4$ точек. Потребуем, чтобы для плоскости Σ выполнялось следующее

У с л о в и е. Пусть выбраны некоторые $q + 1$ точек прямой l_1 : P_1, P_2, \dots, P_{q+1} . Рассмотрим любые две точки A и B , $A \neq B$, не принадлежащие l_1 и такие, что $AB \cap l_1 = P_r$, $1 \leq r \leq q + 1$. Тогда существует собственная подплоскость Σ^ , содержащая каждую из точек $A, B, P_1, P_2, \dots, P_{q+1}$, но не содержащая других точек прямой l_1 .*

Будем обозначать подплоскость Σ^* , упомянутую в условии, символом $(H; A, B)$, где $H = \{P_1, P_2, \dots, P_{q+1}\}$. Постараемся описать конструкцию этой подплоскости и выяснить ее свойства (рис. 115).

S_1 . Подплоскость $(H; A, B) = \Sigma^*$ имеет порядок q .

Это непосредственно вытекает из того факта, что ровно $q + 1$ точек прямой l_1 принадлежат Σ^* .

Пусть $AB \cap l_1 = P_r$, $AP_j = a_j$, $BP_h = b_h$, где P_j, P_h, P_r — различные элементы из H . Из определения подплоскости следует, что $a_j \cap b_h = C_{jh} \in \Sigma^*$. Таким путем мы получаем, однако, лишь $q(q - 1)$ точек. Добавив к ним $q + 1$ точек P_1, P_2, \dots, P_{q+1} , а также точки A и B , получим уже $q^2 + 3$ точек, принадлежащих Σ^* . Еще $q - 2$ точек из Σ^* получаются проектированием мно-

жества $H \setminus \{P_j, P_h, P_r\}$ из точки C_{jh} на прямую AB . В итоге имеем уже $q^2 + q + 1$ точек из Σ^* . Но подплоскость порядка q должна содержать именно столько точек.

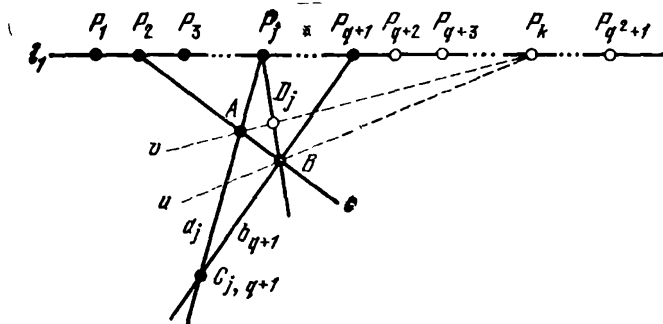


Рис. 115.

Тем самым мы указали способ построения всех точек из Σ^* .

S_2 . *Существование подплоскости $(H; A, B) = \Sigma^*$ влечет за собой единственность этой подплоскости.*

Это следует из указанного выше построения, дающего все $q^2 + q + 1$ точек подплоскости Σ^* .

На рис. 115 точки исходной плоскости Σ , образующие плоскость Σ^* , изображены темными (остальные точки изображены светлыми кружками).

S_3 . *Подплоскость Σ^{**} на исходной плоскости Σ пересекает в единственной точке каждую прямую, проходящую через точку множества $l_1 \setminus H$ и отличную от l_1 .*

В самом деле, пусть $P_k \in l_1$, но $P_k \notin H$. Пусть, далее, B есть собственная (не идеальная) точка подплоскости Σ^* . Если $BP_k = u$ пересекает Σ^* в некоторой точке A , то мы должны иметь $AB = BP_k = u$. Так как $A, B \in \Sigma^*$, точка пересечения прямой u с l_1 должна принадлежать H , что противоречит нашим допущениям. Если Σ^* и P_k фиксированы, то число прямых u в точности совпадает с числом собственных точек из Σ^* , т. е. с q^2 . Следовательно, каждая собственная прямая, проходящая через точку P_k , пересекает подплоскость Σ^* в единственной точке.

) Имеется в виду любая подплоскость Σ^ плоскости Σ , удовлетворяющая условию $\Sigma^* \cap l_1 = H$. — Прим. перев.

S_4 . Если множество H и собственная точка B фиксированы, то число подплоскостей $(H; A, B) = \Sigma^*$ есть $q + 1$.

Для доказательства рассмотрим прямые $u = BP_k$ и $v = AP_k$, $P_k \notin H$ (см. рис. 115). Ни прямая u , ни v не имеют общих точек с подплоскостью Σ^* , отличных соответственно от B и A . Через каждую собственную точку X прямой v проходит подплоскость, которая инцидентна H ; действительно, если мы рассмотрим собственную точку Y такую, что $Y \in XP_j$, $P_j \in H$, то $(H; X, Y)$ и будет требуемая подплоскость. Следовательно, проектируя точки множества H из B на прямую v , мы получим все точки D_j ($j = 1, 2, \dots, q + 1$), в которых подплоскость, принадлежащая B и H , пересекает прямую v ; при этом различным точкам D_j будут принадлежать различные подплоскости $(H; B, D_j) = \Sigma_j^*$. Отсюда число рассматриваемых подплоскостей есть $q + 1$.

S_5 . Если множество H фиксировано, то число подплоскостей $(H; A, B) = \Sigma^*$ равно $q^3 + q$.

Каждая из q^2 собственных точек упомянутой выше прямой u содержится в $q + 1$ подплоскостях, и каждая подплоскость пересекает u в собственной точке; отсюда число подплоскостей есть $q^3 + q$.

S_6 . Если собственная точка P не содержится в некоторой подплоскости Σ_0^* , инцидентной H , то существует единственная подплоскость Σ^* , содержащая P и такая, что $\Sigma_0^* \cap \Sigma^* = H$.

В этом случае мы говорим, что подплоскости Σ_0^* и Σ^* параллельны друг другу, и выражаем это записью $\Sigma_0^* \parallel \Sigma^*$.

Весь смысл конструкции производной плоскости именно в этом предложении. Если заменить в нем слово «подплоскость» словом «прямая», то получится следующее утверждение: если дана прямая и точка вне ее, то существует одна и только одна прямая, содержащая данную точку и параллельная данной прямой. Заметим, что это утверждение будет верно и в том случае, когда вместо данной подплоскости Σ_0^* мы возьмем прямую u такую, что $u \cap l_1 \notin H$. В самом деле, согласно S_3 прямая u пересекает в идеальной точке только «обычную» прямую, соединяющую P с $u \cap l_1$.

После этого замечания обратимся к доказательству S_6 . Условие $u \cap l_1 \notin H$ выполняется для $q^2 - q$ прямых u ,

проходящих через точку P ; каждая из этих прямых пересекает Σ_0^* в одной собственной точке X . Это дает $q^2 - q$ собственных точек из Σ_0^* ; остальные $q^2 - (q^2 - q) = q$ собственных точек будем называть Y -точками. Очевидно, каждая прямая PY плоскости Σ может пересекать идеальную прямую l_1 только в точке, принадлежащей H ; такая прямая не может содержать две различные Y -точки, скажем Y_1 и Y_2 , ибо в противном случае подплоскость Σ_0^* должна была бы (в силу S_2) совпадать с $(H; Y_1, Y_2)$ и, значит (по доказанному ранее), содержать все точки прямой Y_1Y_2 (на плоскости Σ), в том числе P , что противоречит условию. Однако q подплоскостей $(H; P, Y) = \Sigma^*$ не исчерпывают все множество подплоскостей, проходящих через точку P , ибо число последних, согласно S_4 , равно $q + 1$. Значит, найдется ровно одна подплоскость Σ^* , проходящая через P и не имеющая с Σ_0^* общих собственных точек.

4° Опираясь на предложения $S_1 - S_6$, можно построить производную плоскость для Σ , которую будем обозначать Σ' .

Мы сохраняем все точки исходной плоскости, за исключением точек прямой l_1 , т. е. переходим сначала к аффинной плоскости $\bar{\Sigma}$, которая получается из проективной плоскости Σ исключением l_1 . Мы сохраняем все прямые исходной плоскости, идеальные точки которых лежат в H , но, разумеется, эти идеальные точки мы исключаем из прямых. Будем называть эти прямые r -прямыми.

Мы исключаем все остальные прямые и вместо них вводим в качестве «прямых» подплоскости Σ^* , определенные с помощью H , но при этом, разумеется, точки из H мы снова исключаем. Будем эти прямые называть s -прямыми.

Теперь, если не делать различия между r -прямыми и s -прямыми, называя те и другие просто «прямыми», то получим производную аффинную плоскость $\bar{\Sigma}'$. Следующие структурные свойства этой плоскости легко вытекают из ее построения:

а) $\bar{\Sigma}'$ состоит из $q^4 = n^2$ точек и $q^4 + q^2 = n^2 + n$ прямых.

б) Любая прямая в $\bar{\Sigma}'$ состоит из $q^2 = n$ точек; через любую точку проходят $q^2 + 1 = n + 1$ прямых.

Таким образом, число элементов в $\bar{\Sigma}'$ как раз такое, какое необходимо для построения аффинной плоскости порядка q^2 . Что эти элементы действительно образуют аффинную плоскость, вытекает из следующих свойств $\bar{\Sigma}'$:

A'_1 . Существует одна и только одна прямая, проходящая через две данные (различные) точки (см. I_1 и S_2).

A'_2 . Если даны прямая и точка вне ее, то существует одна и только одна прямая, содержащая данную точку и параллельная данной прямой (см. S_6).

A'_3 . Существует собственный треугольник (это очевидно, поскольку существуют по крайней мере две различные r -прямые).

Мы перечислили аксиомы, определяющие аффинную плоскость.

Если мы расширим аффинную плоскость $\bar{\Sigma}'$ — классическим способом, т. е. присоединением идеальных точек, определенных классами эквивалентности параллельных прямых, — то получим проективную плоскость того же порядка. Последняя и есть производная плоскость Σ'

«Минимальный» пример, дающий нетривиальный результат, получается применением указанной процедуры к плоскости Галуа порядка 9. Производная плоскость в этом случае будет недезарговой. Заметим, что в общем случае исходная плоскость Σ необязательно должна быть дезарговой.

Кроме рассмотренного выше способа построения новых плоскостей, существуют и другие способы; обсуждать их здесь мы не будем.

6.3. Обобщение понятия аффинной плоскости

Мы уже видели, что аксиомы инцидентности проективной плоскости не обеспечивают выполнения теоремы Дезарга. Вместе с тем хорошо известно, что аксиомы инцидентности проективного пространства размерности выше 2 столь «сильны», что из них следует справедливость теоремы Дезарга — даже в том случае, когда оба рассматриваемых треугольника лежат в одной и той же плоскости пространства.

Естественно возникает вопрос: можно ли так «ослабить» аксиомы проективного пространства, чтобы среди

пространств, удовлетворяющих новой системе аксиом, содержались недезарговы пространства?

Одна из возможностей заключается в использовании метода «центрального изображения» в дискриптивной геометрии. Другие подходы были исследованы Ломбардо Радиче, (1951 г.), Е. Спернером (1960 г.), А. Барлотти (1962 г.); мы расскажем здесь только об идеях Барлотти.

1° Из метода центрального изображения мы выберем лишь некоторые специфические детали, которые позволяют ввести понятие трехмерного аффинного пространства по Барлотти.

Рассмотрим классическое проективное пространство размерности 3. Выделим в нем плоскость, которую будем считать идеальной. Возьмем, далее, еще одну плоскость π , которую примем за плоскость проекций; пусть центр проектирования есть некоторая точка K (собственная), не принадлежащая π . Образом произвольной точки P , $P \neq K$, пространства будем считать точку $\pi \cap KP = P'$. Такое отображение определено на всем пространстве, но не является взаимно однозначным. Однако это обстоятельство можно исправить введением других элементов, позволяющих однозначно восстановить исходную точку. Для этой цели мы рассмотрим сначала некоторый способ взаимно однозначного изображения прямых, а также плоскостей; это позволит нам определить взаимно однозначным образом изображение точек.

Прямую или плоскость пространства будем изображать *парой элементов*, из которых один является *следом* данной прямой или плоскости, а другой задает ее *направление*. А именно, *следовой точкой* прямой l будем считать точку $\pi \cap l = N_l$, а *следовой прямой* плоскости σ — прямую $\pi \cap \sigma = n_\sigma$. *Направляющей точкой* прямой l будем считать точку M_l , в которой прямая, параллельная l и проходящая через K , пересекает плоскость π , а *направляющей прямой* плоскости σ — прямую m_σ , по которой плоскость, параллельная σ и проходящая через K , пересекает плоскость π . (Мы не будем сейчас обсуждать случаи специального расположения прямой l и плоскости σ по отношению к «системе отсечения» K , π ; эти случаи легко разберет сам читатель.) Можно сказать, что пара (N_l, M_l) есть *модель прямой* l пространства, а пара (n_σ, m_σ) — *модель плоскости* σ .

С помощью этих моделей очень удобно выражать отношения инцидентности и параллельности. Действительно, отношение $l \in \sigma$ равнозначно $N_l \in n_\sigma$, $M_l \in m_\sigma$, а отношения $l \parallel g$, $l \parallel \sigma$, $\sigma \parallel \tau$ равнозначны соответственно $M_l = M_g$, $M_l \in m_\sigma$, $m_\sigma = m_\tau$. Укажем также следующий очевидный факт: следовая прямая и направляющая прямая плоскости параллельны друг другу. Другими словами, $n_\sigma \cap m_\sigma \in u$, где u — идеальная прямая плоскости π .

Любое утверждение относительно прямых и плоскостей пространства (или, в силу двойственности, относительно прямых и точек пространства), выраженное в терминах инцидентности и параллелизма прямых, можно превратить в некоторое утверждение о свойствах плоскости π . Идея Барлотти как раз и состояла в построении модели, подобной указанной выше, исходя из плоскости, которая *необязательно является дезарговой*. Рассмотрим теперь этот вопрос более подробно.

2° Пусть π будет проективная плоскость порядка q , и пусть u — произвольная прямая в π , а U — произвольная точка на u . Будем говорить, что u есть *фундаментальная прямая*, а U — *фундаментальная точка*. Наряду с парой u, U мы фиксируем еще пару прямых m и n , отличных друг от друга, а также от прямой u и удовлетворяющих условию $m \cap n = U$.

Определим *аффинное пространство* S , реализованное посредством модели в плоскости π , следующим образом. Под точкой P будем понимать пару n_p, m_p прямых плоскости π , удовлетворяющих условиям

$$n_p \neq u \neq m_p \text{ и } U \neq n_p \cap m_p \in u.$$

Мы пишем в этом случае $P = (n_p, m_p)$.

Под *прямой первого рода* (r -прямой) пространства S будем понимать пару N_r, M_r точек плоскости π , удовлетворяющих условиям

$$N_r \notin u, \quad M_r \notin u;$$

под *прямой второго рода* (s -прямой) — пару точек N_s, M_s плоскости π такую, что

$$U \neq N_s \in u \text{ и } M_s \neq U.$$

Задание прямой выражаем записью $r = (N_r, M_r)$ или $s = (N_s, M_s)$.

Определим теперь отношение инцидентности между точками и прямыми, а также отношение параллельности между прямыми одного рода (параллелизм между прямыми разных родов исключается).

Инцидентность между точкой $A = (n_A, m_A)$ и r -прямой $r = [N_r, M_r]$ понимается следующим образом: $N_r \in n_A$, $M_r \in m_A$, а инцидентность между точкой A и s -прямой $s = [N_s, M_s]$ означает, что точки

$$M_s, n_A \cap n, m_A \cap m$$

коллинеарны и $N_s = n_A \cap u$.

По определению, параллельность двух прямых первого рода $r_1 = [N_{r_1}, M_{r_1}]$ и $r_2 = [N_{r_2}, M_{r_2}]$ означает, что тройки точек

$$N_{r_1}, N_{r_2}, U \text{ и } M_{r_1}, M_{r_2}, U$$

коллинеарны. Параллельность двух прямых второго рода $s_1 = [N_{s_1}, M_{s_1}]$ и $s_2 = [N_{s_2}, M_{s_2}]$ означает, что тройка точек M_{s_1}, M_{s_2}, U коллинеарна.

Легко показать—читатель сделает это, самостоятельно,—что если π есть дезаргова плоскость, то построенное указанным способом аффинное пространство (модель) есть обычное аффинное пространство; идеальные точки последнего вводятся условием: «множество всех прямых, параллельных данной, определяет одну идеальную точку, являющуюся общей точкой этих прямых».

Однако, если π есть недезаргова плоскость, полученная методом, изложенным в параграфе 6.2, мы уже не получаем обычного аффинного пространства. Фиксируя свойства этого пространства, мы приходим к системе аксиом, которая является более слабой, чем система аксиом, описывающая аффинное пространство Галуа. Однако мы не будем здесь развивать эту программу; мы лишь укажем без доказательства, что наша модель удовлетворяет следующей системе аксиом, описанной Спернером:

SA₁. Двум различным точкам инцидентна одна и только одна прямая.

SA₂. Каждой прямой инцидентно одно и то же число точек; это число называется порядком пространства.

SA₃. Параллельность прямых является отношением эквивалентности.

SA₄. Если даны точка P и прямая t , то существует одна и только одна прямая, проходящая через P и параллельная t .

6.4. Задачи и упражнения к главе 6

43. Рассмотрим следующую специальную форму теоремы Паскаля:

«Пусть четверки точек U, A_1, A_3, A_5 и U, A_2, A_4, A_6 принадлежат соответственно прямым a и b , $a \neq b$. Тогда тройка точек $U, X = A_1A_2 \cap A_4A_5, Y =$

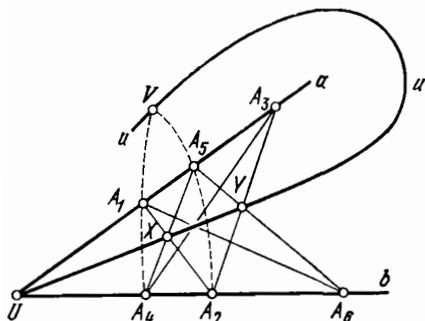


Рис. 116.

$= A_2A_3 \cap A_5A_6$ лежит на одной прямой u ». Этот частный случай теоремы Паскаля называется *малой теоремой Паскаля* (MP-теоремой); см. рис. 116. Докажите, что MP-теорема справедлива для плоскости Фано.

44. Пользуясь обозначениями рис. 116 к упражнению 43, убедитесь, что в случае плоскости Фано порядка $q \geq 3$ прямые A_1A_4, A_2A_5, A_3A_6 пересекаются с прямой u в одной точке (точке V на рисунке).

45. Пусть a и $b, a \neq b$, — две фиксированные прямые,

A_1 и $A_2, A_1 \neq A_2$, — две точки прямой a, B_1 и $B_2, B_1 \neq B_2$, — две точки прямой b , причем все указанные четыре точки отличны от $a \cap b = U$. Точки

$$A_1B_1 \cap A_2B_2 = P, \quad A_1B_2 \cap A_2B_1 = P'$$

называются *сопряженными* (друг другу) относительно пары $\{a, b\}$ прямых. Докажите, что если на плоскости справедлива MP-теорема, то совокупность точек, сопряженных относительно $\{a, b\}$ данной точке P ($P \notin a, b$), есть некоторая прямая l_P , проходящая через U . (Прямая l_P , сопоставленная указанным образом точке P , называется *полярной* точки P относительно $\{a, b\}$.)

46. Докажите следующий факт: если точка Q принадлежит прямой l_P из упражнения 45, причем $Q \neq U$, то $l_Q = \overline{UP}$. Прямые $l = l_P, l' = l_Q$ называются *сопряженными* относительно $\{a, b\}$.

47. Если прямые l и l' из упражнения 46 сопряжены друг другу относительно $\{a, b\}$, то прямые a и b сопряжены друг другу относительно $\{l, l'\}$. Докажите это предложение.

В дальнейшем, говоря о сопряженности прямых l и l' относительно $\{a, b\}$, мы будем понимать под этим, что прямые l и l' сопоставлены друг другу в указанном выше смысле, причем $a \neq b \neq l \neq a$ и $a \cap b \in l$.

48. На плоскости Фано каждая прямая l сопряжена самой себе относительно $\{a, b\}$. Докажите этот факт.

49. Плоскость, в которой выполняется МР-теорема, называется МР-плоскостью. Докажите, что на МР-плоскости четного порядка существует прямая, сопряженная самой себе относительно $\{a, b\}$.

50. Пусть прямая l на МР-плоскости сопряжена самой себе относительно $\{a, b\}$. Докажите, что тогда l сопряжена самой себе относительно любой пары $\{u, v\}$, где $u \neq l \neq v \neq u$ и $u \cap v \in l$.

51. Если на МР-плоскости прямая l сопряжена самой себе относительно $\{a, b\}$, то a сопряжена себе относительно $\{b, l\}$.

52. Докажите, что на МР-плоскости четного порядка справедливо следующее: если три различные прямые a, b, c проходят через общую точку, то прямая c сопряжена себе относительно $\{a, b\}$.

53. Докажите, что любая МР-плоскость четного порядка является плоскостью Фано.

Располагая решением последней задачи, можно вывести из теоремы Глисона, что справедлива следующая

Т е о р е м а Л ю н е б у р г а. *Любая МР-плоскость четного порядка является дезарговой.*

Нижеследующие задачи могут потребовать значительных усилий, но являются весьма поучительными.

54. Мы уже знакомы с таблицей инцидентности плоскости Галуа порядка 9 (см. в этой связи рис. 44, 45, 46); в частности, мы знаем, что подтаблица $\Gamma(3)$ таблицы $\Gamma(9)$, расположенная в пересечении строк и столбцов с номерами

1, 2, 3, 4, 11, 12, 13, 20, 21, 22, 29, 30, 31,

представляет собой таблицу инцидентности подплоскости порядка 3. Обозначим плоскость Галуа, описываемую таблицей $\Gamma(9)$, через Σ и рассмотрим множество $H = \{P_1, P_2, P_3, P_4\}$. Легко проверить, что, например, подплоскость $\{H; P_{13}, P_{20}\}$ имеет указанную выше таблицу инцидентности $\Gamma(3)$. Постройте таблицу инцидентности производной плоскости (для Σ), определенной с помощью H по методу параграфа 6.2. Полученная таблица из 91×91 клеток дает ясную картину этой сравнительно сложной структуры.

55. Постарайтесь установить некоторые свойства производной плоскости Σ' порядка 9 с помощью ее таблицы инцидентности. Например, докажите, что эта плоскость недезаргова.

56. Проверьте справедливость аксиом Спернера для модели Барлотти.

Следующая интересная задача возникает при попытке ввести понятие плоскости в пространстве, фигурирующем в упражнении 56. Плоскость есть множество, содержащее по крайней мере две прямые, причем:

V_1 . Любая прямая, соединяющая две различные точки плоскости, принадлежит этой плоскости.

V_2 . Если две различные прямые принадлежат одной и той же плоскости, то они либо параллельны, либо имеют общую точку.

Если базисная плоскость Π модели не является дезарговой, то мы пока не знаем, определяют ли две пересекающиеся прямые плоскость, удовлетворяющую V_1, V_2 .

57. Докажите, что совокупность точек $P = (n_p, m_p)$, удовлетворяющих условию $n_p = m_p$, образует плоскость.

58. В случае модели пространства, реализованной в плоскости Π , выясните, когда две прямые лежат в одной плоскости (которая, однако, не того типа, что в упражнении 57).

Упражнения 43—58 продолжают темы, затронутые в главе 6. Упражнения в конце предыдущих глав носили такой же характер. Приведем теперь некоторое количество упражнений, относящихся ко всему материалу данной книги. Они позволят читателю с различных точек зрения подойти к вопросам, изложенным в книге.

59. Следующая система аксиом определяет трехмерное пространство.

PT_0 . Пространство S есть множество абстрактных элементов A, B, \dots , называемых точками, и элементов a, b, \dots , называемых прямыми, удовлетворяющих аксиомам:

PT_1 . Если $A, B \in S$ и $A \neq B$, то существует в точности одна прямая l такая, что $A \in l, B \in l$. (В этом случае мы пишем $AB = l$.)

PT_2 . Пусть $A, B, C \in S$ и не существует прямой l такой, что $A, B, C \in l$. Если $P \in BC$ и $Q \in CA$, причем $P \neq Q$, то существует такая точка R , что $R \in PQ$ и $R \in AB$.

Мы можем ввести понятие плоскости в терминах этой системы аксиом следующим образом. Пусть три различные точки U, V, W не лежат на одной прямой. Рассмотрим множество, состоящее из точек всех прямых UQ , где $Q \in VW$; это множество назовем плоскостью и будем обозначать (U, VW) . Продолжим перечень аксиом пространства.

PT_3 . Каждой прямой принадлежат по крайней мере три различные точки.

PT_4 . Существует не менее одной прямой.

PT_5 . Все точки пространства не могут принадлежать одной прямой.

PT_6 . Все точки пространства не могут принадлежать одной плоскости.

Если из пространства S , удовлетворяющего системе аксиом PT , удалить одну плоскость, вместе с ее точками и прямыми, то приходим к понятию аффинного пространства. Обратно, покажите, каким образом это аффинное пространство можно расширить до проективного пространства, удовлетворяющего системе аксиом PT , путем присоединения идеальных элементов.

60. Сравните систему аксиом аффинного пространства, определенного в упражнении 59, с системой аксиом Спернера.

Следующие задачи относятся к геометрии плоскости, в которой выполняются аксиомы I_1, I_2, I_3 .

Аutomорфизм плоскости называется перспективной коллинеацией, если: 1) существует фиксированная точка K , называемая центром, такая, что точки любой прямой, проходящей через K , отображаются в точки этой же прямой; 2) существует такая прямая, называемая осью, что каждая точка этой прямой является неподвижной точкой.

61. Докажите, что перспективная коллинеация, имеющая более чем один центр, является тождеством; то же самое для перспективной коллинеации с более чем одной осью.

62. Пусть даны прямая t , точка K , а также точки P и P' , удовлетворяющие условиям

$$K \in PP', \quad K \neq P \neq P' \neq K, \quad P \notin t, \quad P' \notin t.$$

Докажите, что существует не более одной перспективной коллинеации с центром K и осью t , такой, что образ точки P есть P' .

63. Определите максимальное число перспективных коллинеаций с центром K и осью t , причем $K \in t$.

64. Докажите, что если автоморфизм проективной плоскости имеет ось, то он обладает и центром; обратно, если автоморфизм имеет центр, то он обладает и осью.

65. Рассмотрим следующие два условия: 1) для каждой пары точек (P, P') существует перспективная коллинеация с осью t и центром K , переводящая P в P' ; 2) пусть даны два треугольника, перспективные относительно центра K и такие, что две пары соответственных сторон пересекаются на прямой t ; тогда третья пара соответственных сторон тоже пересекается на t . Докажите, что эти условия выполняются или не выполняются одновременно.

66. Докажите, что справедливость условия 1) из упражнения 65 для любого выбора центра K и оси t эквивалентна выполнению теоремы Дезарга.

67. Пусть $K_1 \neq K_2$, $K_1 \in t$, $K_2 \in t$. Пусть, далее, π_1 и π_2 — перспективные коллинеации с осью t и центрами K_1 и K_2 соответственно. Докажите, что отображение $\pi_1\pi_2$ также является перспективной коллинеацией с осью t и некоторым центром $K \in t$, где $K_1 \neq K \neq K_2$.

68. Пусть оба центра K_1 и K_2 , $K_1 \neq K_2$, лежат на оси t , и пусть $\Gamma(K_j, t) = \Gamma_j$ ($j = 1, 2$) обозначает группу всех перспективных коллинеаций с центром K_j и осью t , а $\Gamma(t) = \Gamma$ обозначает группу всех перспективных коллинеаций с осью t , центры которых принадлежат t . Допустим, что каждая из групп Γ_1 и Γ_2 содержит более одного элемента. Докажите, что тогда Γ есть коммутативная группа (теорема Бэра).

З а м е ч а н и е. Известно, что если $\Gamma_1 = \{1\}$ и $\Gamma_2 \neq \{1\}$, то группа Γ не обязательно коммутативна.

69. Дополним условия предыдущего упражнения условием, что плоскость конечна. Докажите тогда, что каждый элемент группы Γ , кроме единицы группы, имеет один и тот же простой порядок p (теорема Бэра).

70. Рассмотрим расширение системы аксиом инцидентности, в котором четвертая аксиома D есть некоторый вариант ограниченной выполнимости теоремы Дезарга. Определите координатную структуру, предполагая, что плоскость конечна.

Упражнения 59—70 мы сочли нужным включить, чтобы дополнить основной текст книги, в котором анализу аксиом не уделялось большого внимания. После этих упражнений даже начинающий читатель лучше прочувствует необходимость строгого аксиоматического подхода.

7. ПРИЛОЖЕНИЕ

В настоящем приложении содержится, прежде всего, краткое алгебраическое резюме. Не весь излагаемый здесь материал необходим для понимания читателем содержания книги, но зато при желании он сможет пополнить свои алгебраические познания, не обращаясь к другим источникам. Кроме того, здесь приводятся дополнения к основному материалу книги, представляющие одновременно и интересными, и полезными.

7.1. Общие сведения об алгебраических структурах

1° *Произведением* $A \times B = C$ множеств A и B называется множество упорядоченных пар $\langle a, b \rangle$, где $a \in A$ и $b \in B$.

Пусть даны множество $H = \{1, 2, \dots, n\}$ и группа подстановок Γ этого множества. *Стабилизатором* элемента $x \in H$ называется следующая подгруппа группы Γ :

$$\Gamma_x = \{\pi \in \Gamma \mid x^\pi = x\}.$$

Орбитой элемента x относительно группы Γ называется множество $x^\Gamma = \{x^\pi \mid \pi \in \Gamma\}$. В обоих случаях через x^π обозначается элемент, в который подстановка π переводит x .

Чтобы лучше представить себе эти два важных понятия, рассмотрим примеры, приведенные на рис. 97а и 97б (стр. 244). На этих рисунках элементы H обозначены цифрами 1, 2, ..., 13, а элементы Γ — буквами $\sigma_1, \sigma_2,$

..., σ_6 (σ_1 — единичный элемент). Легко проверить, что, например, $\Gamma_{11} = \{\sigma_1, \sigma_3\}$ и что это множество составляет подгруппу группы Γ ; $\Gamma_3 = \{\sigma_1\}$, т. е. Γ_3 является единичной тривиальной подгруппой; Γ_8 совпадает со всей группой Γ и является другой тривиальной подгруппой. Легко также проверить, что $3^\Gamma = \{1, 3, 4, 5, 7, 10\}$; $2^\Gamma = \{2, 9, 11\}$; $8^\Gamma = \{8\}$.

Группа подстановок Γ множества N называется *регулярной*, если для каждого $x \in N$ имеет место $\Gamma_x = 1$.

2° Пусть A — произвольное непустое множество и $A \times A$ — согласно сказанному выше, множество всех упорядоченных пар

$$(x, y) \quad (x, y \in A).$$

Отображение множества $A \times A$ в множество A называется *бинарной операцией*, при этом образ пары (x, y) обозначается символом $x \circ y$. Непустое множество A называется *основным множеством* операции.

Можно составить следующую иерархию множеств с бинарной операцией.

Группоид, обозначаемый символом (A, \circ) , есть множество A с бинарной операцией, обозначаемой знаком \circ . Если множество A группоида конечно, $|A| = n$, то таблица операции группоида есть таблица $n \times n$, в которой элемент $x \circ y \in A$ находится в клетке пересечения строки x и столбца y . Группоид можно считать заданным, если выписана его таблица операции.

Квазигруппа есть группоид (A, \circ) , в котором для любых двух элементов $a, b \in A$ каждое из уравнений $a \circ x = b$, $y \circ a = b$ имеет в точности одно решение. Таблица операции конечной квазигруппы является латинским квадратом. Квазигруппа с единичным элементом называется также *луной*.

Полугруппа есть группоид (A, \circ) , в котором для каждой тройки элементов a, b, c выполняется условие $a \circ (b \circ c) = (a \circ b) \circ c$.

Группа есть луна, являющаяся в то же время полугруппой. Таблица операции конечной группы уже рассматривалась в связи с понятием R -сети.

Абелева группа есть группа (A, \circ) , в которой для любых двух элементов $a, b \in A$ имеет место $a \circ b = b \circ a$. При одинаковом порядке элементов в заглавной строке и заглавном столбце таблица операции абелевой группы симметрична относительно главной диагонали.

Очередность образования этих понятий наглядно представлена в виде направленного графа на рис. 117. Буквы, приписанные точкам графа, означают: G — группоид, K — квазигруппа, F — полугруппа, C — группа, A — абелева группа.

3° Укажем теперь некоторые теоретико-групповые понятия и теоремы, играющие особо важную роль в конечных геометриях.

Циклическая группа. Группа называется циклической, если она содержит элемент, множество степеней которого исчерпывает всю группу.

Если группа G содержит две такие подгруппы A и B , что каждый элемент $g \in G$ можно единственным образом представить в виде $g = ab$, где $a \in A$ и $b \in B$, и для любых элементов $a \in A$ и $b \in B$ имеет место $ab = ba$, то группу G называют прямым произведением подгрупп A и B и пишут: $G = A \times B$. Аналогично определяется прямое произведение нескольких подгрупп группы G .

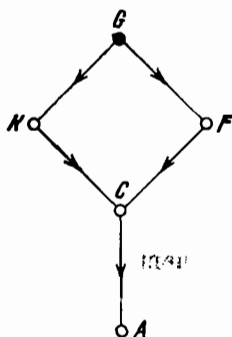


Рис. 117.

Теорема Лагранжа. Если A — подгруппа конечной группы G , то $|G|$ делится нацело на $|A|$.

Следствием этой теоремы является тот факт, что порядок любого элемента конечной группы служит делителем порядка группы. Другое следствие состоит в том, что группа простого порядка является циклической.

Примарной группой (p -группой) называется группа, порядки всех элементов которой являются степенями некоторого заданного простого числа p .

Элементарной группой называется группа, в которой порядок каждого элемента, отличного от единичного, есть некоторое заданное простое число. Очевидно, всякая элементарная группа является p -группой.

Нормальный делитель. Подгруппа N группы G называется нормальным делителем группы G , если для каждого элемента $x \in G$ множество $Nx = \{nx \mid n \in N\}$ совпадает с множеством $xN = \{xn \mid n \in N\}$. Это записывается в виде $N \triangleleft G$.

Инвариантный элемент. Элемент s группы G называется инвариантным, если он перестановочен с каждым элементом группы G , т. е. если $sx = xs$ для всякого $x \in G$.

Центр группы. Инвариантные элементы группы G образуют ее нормальный делитель $Z(G)$, называемый центром этой группы.

Теорема. Если порядок группы является степенью простого числа, то ее центр содержит элементы, отличные от единичного элемента.

¶ **Сопряженные элементы группы.** Два элемента a и b группы G называются сопряженными, если существует

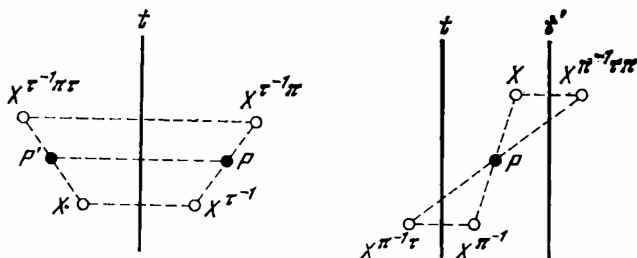


Рис. 118.

такой элемент g , что $ag = gb$, т. е. если $g^{-1}ag = b$. Говорят также, что a получается *трансформацией* элемента b элементом g . Если $g^{-1}ag = a$, то элемент a называется *инвариантным* относительно трансформации элементом g .

Сопряженная подгруппа. Если для подгрупп A и B группы G найдется такой элемент $g \in G$, что $Ag = gB$, т. е. $g^{-1}Ag = B$, то подгруппа B называется сопряженной подгруппе A в G . Говорят также, что подгруппа B получается *трансформацией* подгруппы A элементом g . Если $g^{-1}Ag = A$, то подгруппа A называется *инвариантной* относительно трансформации элементом g . Поскольку нормальный делитель группы инвариантен относительно трансформации любым ее элементом, то его называют также *инвариантной подгруппой* группы.

Мы покажем сейчас на примере, как понятия теории групп позволяют сжато выражать некоторые геометрические факты. Чертеж слева на рис. 118 (где P — фиксированная точка, t — фиксированная прямая, X — переменная точка, пробегающая множество всех точек плоскости) приводит нас к следующей теореме. Результат последовательного отражения точки X относительно пря-

мой t , полученного образа относительно точки P и этого нового образа опять относительно прямой t совпадает с результатом отражения точки X относительно точки P' , симметричной точке P относительно прямой t . Сформулируем этот факт в терминах группы движений плоскости. Отражение относительно точки P обозначим через π . Очевидно, $\pi^2 = 1$, т. е. $\pi = \pi^{-1}$. Аналогично, обозначив отражение относительно прямой t через τ , получаем, что $\tau^2 = 1$, откуда $\tau^{-1} = \tau$. Теперь наше геометрическое утверждение о трех последовательных отражениях может быть выражено следующей формулой: $\pi' = \tau^{-1}\pi\tau$. Чертеж справа на нашем рисунке показывает, что три последовательных отражения — относительно точки P , затем прямой t и, наконец, снова точки P — равносильны отражению относительно прямой t' , симметричной прямой t относительно точки P . Это можно выразить формулой: $\tau' = \pi^{-1}\pi\tau$.

Кроме того, легко проверить, что условие принадлежности точки P прямой t равносильно условию $\pi\tau = \tau\pi$. Чтобы убедиться в этом, достаточно заметить, что в первом случае условие $\tau^{-1}\pi\tau = \pi$ означает совпадение точек P и P' , тогда как во втором случае условие $\pi^{-1}\tau\pi = \tau$ означает совпадение прямых t и t' .

Преимущества языка теории групп становятся особенно убедительными, если выраженные на этом языке геометрические понятия и отношения попытаться выразить также средствами аналитической геометрии. Достаточно, быть может, ограничиться следующим примером:

$$\begin{array}{l} P: (x, y) \\ t: [m, b] \end{array} \left\} P \in t: y = mx + b, \quad \begin{array}{l} P: \pi \\ t: \tau \end{array} \left\} P \in t: \pi\tau = \tau\pi.$$

После этого небольшого отступления продолжим наш обзор по теории групп.

Теорема Силова. Если порядок конечной группы делится на степень p^r простого числа p , то эта группа имеет подгруппу порядка p^r .

Силовская подгруппа. Если $|G| = p^k s$ и s не делится на p , то подгруппы порядка p^k группы G называются силовскими p -подгруппами.

Следствие 1. Если порядок конечной группы делится на простое число p , то в группе имеется элемент порядка p .

Следствие 2. Порядок любой конечной p -группы является степенью числа p .

Основная теорема об абелевых группах. Любая конечная абелева группа разлагается в прямое произведение циклических групп, порядки которых являются степенями простых чисел; множество степеней простых чисел, являющихся порядками указанных групп, однозначно определяется порядком самой группы.

Это надо понимать следующим образом: если $|G| = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$, то можно указать такие циклические группы A_1, A_2, \dots, A_k порядков $p_1^{r_1}, p_2^{r_2}, \dots, p_k^{r_k}$ соответственно, что $G = A_1 \times A_2 \times \dots \times A_k$. Отсюда следует, что конечная абелева группа однозначно определяется с точностью до изоморфизма конечным набором степеней простых чисел.

4° Переходя к множествам с двумя бинарными операциями, мы ограничимся только самыми важными фактами. Основное множество будем обозначать буквой A , а две операции — символами \perp и \lrcorner (или, если это не сможет вызвать недоразумения, — знаками $+$ и \cdot). Системы с двумя операциями будут записываться в виде (A, \perp, \lrcorner) или в виде $(A, +, \cdot)$.

Кольцо есть такая система (A, \perp, \lrcorner) , что система (A, \perp) является абелевой группой, система (A, \lrcorner) — полугруппой и операция \lrcorner дистрибутивна относительно операции \perp , т. е.

$$(a \perp b) \lrcorner c = (a \lrcorner c) \perp (b \lrcorner c),$$

$$c \lrcorner (a \perp b) = (c \lrcorner a) \perp (c \lrcorner b).$$

Кольцо является обобщением системы $(Z, +, \cdot)$ целых чисел, однако в кольце (1) условие $ab = ba$ может нарушаться и (2) равенство $ab = 0$ может иметь место и тогда, когда $a \neq 0$ и $b \neq 0$.

Тело есть такая система (A, \perp, \lrcorner) , что система (A, \perp) является абелевой группой, система (A', \lrcorner) , где A' получается из A удалением нулевого элемента (т. е. нейтрального элемента абелевой группы), является группой и операция \lrcorner дистрибутивна относительно операции \perp . Если система (A', \lrcorner) также является абелевой группой, то тело называют коммутативным (или полем).

Теорема. Кольцо является телом тогда и только тогда, когда оно содержит не менее двух элементов и оба уравне-

ния $a \lrcorner x = b$ и $x \lrcorner a = b$ разрешимы для любых элементов $a, b \in A$, где $a \neq 0$.

Тело служит обобщением системы $(Q, +, \cdot)$ рациональных чисел, однако требование коммутативности умножения опускается.

Теорема Веддербарна. *Всякое конечное тело коммутативно.*

Эта глубокая теорема сыграла важную роль в развитии конечной геометрии.

Квазитело есть такая система (A, \perp, \lrcorner) , что система (A, \perp) является абелевой группой, а система (A, \lrcorner) — квазигруппой с единичным элементом (т. е. лупой), причем имеет место левая дистрибутивность, т. е. для любых трех элементов $a, b, c \in A$ выполняется равенство

$$a \lrcorner (b \perp c) = (a \lrcorner b) \perp (a \lrcorner c).$$

Если имеет место также и правая дистрибутивность, то квазитело называется *дистрибутивным*.

Если операция \lrcorner ассоциативна, то квазитело называется *ассоциативным*.

Альтернативное квазитело есть дистрибутивное квазитело, для которого выполняются следующие условия:

$$\begin{aligned} a(a'x) &= x, \text{ если } a \neq 0 \text{ и } aa' = 1; \\ (xa')a'' &= x, \text{ если } a'' \neq 0 \text{ и } a'a'' = 1. \end{aligned}$$

Теорема. *Дистрибутивное и ассоциативное квазитело является телом.*

Укажем, как можно построить неассоциативное квазитело. Пусть $K = GF(q)$, $q = p^r$, $p \neq 2$, $r > 2$. По системе $K = (A, +, \cdot)$ строится новая система $K^* = (A, \perp, \lrcorner)$ следующим образом. Полагаем $(A, +) = (A, \perp)$, а операцию \lrcorner определяем условием $a \lrcorner b = a \cdot b$, если существует такой элемент $c \in A$, что $a = c^2$, и $a \lrcorner b = a \cdot b^p$ в противном случае (т. е. если a не является квадратом). Нетрудно доказать, что K^* есть квазитело, и притом неассоциативное. Для нас этот пример представляет особый интерес, поскольку с помощью координатной системы на K^* можно получить недезаргову конечную проективную плоскость.

Иерархия систем с двумя бинарными операциями изображена на рис. 119. Буквы на схеме означают: G — кольцо,

Q — квазиполе, D — дистрибутивное квазиполе, A — ассоциативное квазиполе, T — тело, K — коммутативное тело.

5° **Векторное (линейное) пространство** над полем K есть абелева группа M (элементы которой называются векторами) такая, что для всякого элемента $\alpha \in K$ и всякого вектора $a \in M$ определен вектор $\alpha \cdot a \in M$ (называемый скалярным произведением α на a) и выполняются следующие условия:

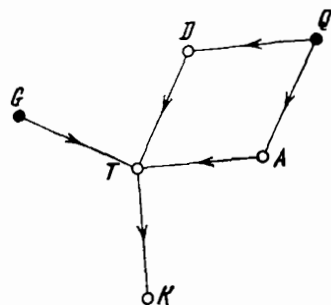
Для любых $a, b \in M$ и $\alpha, \beta \in K$

$$\alpha \cdot (a + b) = \alpha \cdot a + \alpha \cdot b,$$

$$(\alpha + \beta) \cdot a = \alpha \cdot a + \beta \cdot a,$$

$$(\alpha \cdot \beta) \cdot a = \alpha \cdot (\beta \cdot a),$$

$$1 \cdot a = a,$$



где 1 — единичный элемент поля K .

Рис. 119.

Линейная независимость. Система $\{a_1, a_2, \dots, a_k\}$ векторов векторного пространства M называется линейно независимой, если из равенства

$$\lambda_1 a_1 + \lambda_2 a_2 + \dots + \lambda_k a_k = 0$$

следует, что

$$\lambda_1 = \lambda_2 = \dots = \lambda_k = 0.$$

Базис, размерность, координаты. Если в пространстве M не содержится линейно независимой системы из $n + 1$ векторов, а система $\{e_1, e_2, \dots, e_n\}$ из n векторов этого пространства линейно независима, то эта система называется *базисом* пространства M , а число n — его *размерностью*. Если система $\{e_1, e_2, \dots, e_n\}$ является базисом и для элементов $\xi_1, \xi_2, \dots, \xi_n \in K$ и вектора $x \in M$ выполняется равенство

$$x = \xi_1 e_1 + \xi_2 e_2 + \dots + \xi_n e_n,$$

то последовательность $(\xi_1, \xi_2, \dots, \xi_n)$ называется *координатной n -кой* вектора x в базисе (e_1, e_2, \dots, e_n) .

Теорема. *Всякий вектор x векторного пространства можно единственным образом выразить через векторы базиса в виде*

$$x = \xi_1 e_1 + \xi_2 e_2 + \dots + \xi_n e_n;$$

при этом нулевой вектор выражается координатной n -кой $(0, 0, \dots, 0)$.

6° В заключительной части этого параграфа мы постараемся проиллюстрировать тесную связь между развитием проективной геометрии и алгебры. В 1942 году Бэр исследовал проективные плоскости, обладающие следующим свойством: если l — идеальная прямая, Y — фиксированная идеальная точка, а точки P и P' таковы, что $P \neq Y$, $P' \neq Y$, $Y \in PP'$, $P, P' \notin l$, то существует перспективная коллинеация с осью l и центром Y , переводящая точку P в точку P' . Это — так называемые (Y, l) -транзитивные плоскости. Позднее изучались плоскости трансляций, которые представляют собой (Y, l) -транзитивные плоскости для всякой точки Y прямой l . Оказалось, что понятие плоскости трансляций эквивалентно понятию алгебраической плоскости над квазителом.

Чем сильнее условия, налагаемые на множество трансляций плоскости, тем более строгим ограничениям удовлетворяет координатная система.

(1) Если потребовать, чтобы существовали всевозможные перспективные коллинеации, имеющие в качестве центра любую из двух фиксированных идеальных точек, а в качестве оси — прямую, проходящую через другую из них, то множество соответствующих координат образует ассоциативное квазитело.

(2) Если потребовать, далее, чтобы существовали всевозможные элации, имеющие в качестве центра фиксированную идеальную точку, а в качестве оси — любую прямую, проходящую через эту точку, то множество соответствующих координат образует дистрибутивное квазитело. (Напомним, что в определении квазитела содержится лишь требование дистрибутивности слева.)

Плоскость, на которой существуют всевозможные элации, имеющие в качестве центра фиксированную идеальную точку, а в качестве оси — прямую, проходящую через эту точку, можно назвать *двойственной плоскостью трансляций*. Общепринятого термина для обозначения подобных

плоскостей нет, в немецкой литературе пользуются термином «Scherungsebene».

Правое квазиполе есть система (Q, \perp, \lrcorner) такая, что система (Q, \perp) является абелевой группой (ее нейтральный элемент обозначается через 0); (Q', \lrcorner) , где $Q' = Q - \{0\}$, является квазигруппой с единичным элементом обозначаемым символом 1); для каждого элемента $a \in Q$ (имеет место $a \cdot 0 = 0 \cdot a = 0$; для любых элементов $a, b, c \in Q$ выполняется равенство $(a \perp b) \lrcorner c = (a \lrcorner c) \perp (b \lrcorner c)$; если $a \neq b$, то уравнение $(-x \lrcorner b) \perp (x \lrcorner a) = c$ имеет одно и только одно решение в Q , где $-x$ обозначает элемент, противоположный элементу x в абелевой группе (Q, \perp)).

Известно, что в случае конечного правого квазитела последнее требование является следствием предыдущих четырех. В 1965 году ⁵ Бартолоцци построил примеры *собственных* конечных левых квазител, содержащих p^{2^n} элементов, где $p \neq 2$. Термин *собственный* означает здесь, что эти квазитела не являются ни коммутативными, ни ассоциативными и что правая дистрибутивность не имеет места. Укажем еще, что уже в 1931 году, исследуя плоскости, удовлетворяющие аксиомам I_1, I_2, I_3 и MD-теореме, Муфанг пришла к понятию альтернативного квазитела. Мы, однако, изучали в этой книге конечные плоскости, а как следует из теоремы Цорна — Леви, конечных альтернативных квазител не существует.

7.2. Сведения из теории конечных полей и теории чисел

Простейшим примером конечного поля является поле классов вычетов по модулю p (p — простое число); оно будет обозначаться здесь символом Π_p (или короче — просто буквой Π).

Изоморфные поля. Если существует взаимно однозначное отображение поля K на поле K' такое, что для любых $a, b \in K$ и $a', b' \in K'$ из

$$a \rightarrow a', \quad b \rightarrow b'$$

следует

$$a + b \rightarrow a' + b', \quad ab \rightarrow a'b'$$

(или, как говорят, отображение сохраняет операции), то поля K и K' называют изоморфными; символически это записывается в виде $K \cong K'$.

Теорема. *Отношение изоморфизма рефлексивно, симметрично и транзитивно; при изоморфном отображении поля K на поле K' нулевой и единичный элементы поля K переходят соответственно в нулевой и единичный элементы поля K' .*

Подполе, простое поле. Если подмножество K поля L само является полем (относительно операций, заданных в L), то K называется *подполем* L , а L — *расширением* K . Символически это записывается в виде $K \subseteq L$. Если поле не имеет собственных подполей, то оно называется *простым*.

Теорема. *Всякое конечное поле имеет единственное простое подполе, и это подполе изоморфно полю Π по некоторому модулю p .*

Характеристика. Пусть в конечном поле имеет место равенство $e + e + \dots + e = 0$, где e — единичный элемент поля, а число слагаемых в сумме слева равно n . Наименьшее число n с таким свойством называется характеристикой данного поля.

Теорема. *Характеристика p поля K есть простое число, и простое подполе поля K изоморфно полю Π_p .*

Линейная независимость в поле Λ относительно поля Π . Пусть для любых двух элементов $\alpha \in \Lambda$ и $c \in \Pi$ определено произведение $c\alpha \in \Lambda$. Если из равенства $c_1\alpha_1 + c_2\alpha_2 + \dots + c_n\alpha_n = 0$, где $\alpha_k \in \Lambda$, $c_k \in \Pi$ ($k = 1, 2, \dots, n$), следуют равенства $c_1 = c_2 = \dots = c_n = 0$, то система элементов $\alpha_1, \alpha_2, \dots, \alpha_n$ поля Λ называется линейно независимой относительно поля Π .

Ранг поля. Если элементы $\alpha_1, \alpha_2, \dots, \alpha_n$ поля Λ образуют максимальную линейно независимую систему относительно поля Π , то число n элементов этой системы называется рангом поля Λ относительно поля Π (обозначается: $n = \Lambda : \Pi$).

Степень расширения. Если $\Pi \subseteq \Lambda$, то ранг Λ относительно Π называется степенью расширения Λ поля Π .

Теорема. *Если $\Pi \subset \Gamma \subset \Lambda$, то $(\Lambda : \Pi) = (\Lambda : \Gamma) \cdot (\Gamma : \Pi)$.*

Символом $\Lambda[x]$ обозначают множество многочленов одной переменной x с коэффициентами из Λ , в котором сумма и произведение многочленов определяются обычным образом, с тем только условием, что подсчет коэффициен-

тов ведется по правилам для операций, заданных в поле Λ . В качестве примера рассмотрим конечное поле Λ , таблицы операций которого приведены на рис. 44 (стр. 101); пусть, например, даны два многочлена:

$$a(x) = 2x^3 + x + 1 \quad \text{и} \quad b(x) = 5x^4 + 3x^3 + 7x + 6.$$

Пользуясь таблицами операций, легко проверить, что

$$a(x) + b(x) = c(x) = 5x^4 + 5x^3 + 8x + 7,$$

$$a(x) \cdot b(x) = 7x^7 + 6x^6 + 5x^5 + x^4 + 6x^3 + 7x^2 + 4x + 6.$$

Ясно, что степень произведения двух многочленов равна сумме степеней сомножителей, тогда как степень суммы двух многочленов может быть меньше степени каждого из слагаемых.

С помощью указанных выше понятий и фактов можно сформулировать ряд теорем, играющих важную роль в геометриях Галуа.

Основная теорема. Число элементов конечного поля есть степень простого числа; для всякого числа q , являющегося степенью простого числа, $q = p^r$, существует поле из q элементов; любые два поля из q элементов изоморфны.

Ясно, что характеристика поля из $q = p^r$ элементов равна p .

1° Любой элемент поля в степени p^r , где p^r — число элементов поля, равен самому себе. В случае простого поля это утверждение совпадает с теоремой Ферма.

2° Каждый элемент поля является корнем p -й степени; более точно: когда x пробегает все элементы поля, x^p дает некоторую перестановку элементов поля.

3° Для любых двух элементов поля a, b

$$(a + b)^p = a^p + b^p, \quad (ab)^p = a^p b^p.$$

4° Отображение $x \rightarrow x^p$ есть автоморфизм поля (автоморфизм Фробениуса). Все автоморфизмы поля являются степенями этого автоморфизма.

5° Мультипликативная группа конечного поля является циклической.

6° Пусть a_1, a_2, \dots, a_{q-1} — все ненулевые элементы конечного поля, тогда

$$a_1 a_2 \dots a_{q-1} = -1,$$

где -1 означает элемент, противоположный единичному, в аддитивной группе поля. Формулируя это утверждение для поля классов вычетов, мы получаем теорему Вильсона: $(p-1)! \equiv -1 \pmod{p}$.

Сделаем следующее замечание по поводу теоремы Вильсона. В ней указывается некоторое характеристическое свойство простых чисел, а именно: для всех составных чисел n , за исключением числа 4,

$$(n-1)! \equiv 0 \pmod{n},$$

тогда как для каждого простого числа p

$$(p-1)! \equiv -1 \pmod{p}.$$

7° Пусть дано поле Λ из p^r элементов и его простое подполе Π_p (т. е. поле классов вычетов по модулю p). Выберем в множестве $\Pi_p[x]$ какой-нибудь неприводимый многочлен

$$a(x) = x^r + a_1 x^{r-1} + \dots + a_r,$$

и рассмотрим множество всех многочленов

$$c(x) = c_{r-1} x^{r-1} + c_{r-2} x^{r-2} + \dots + c_0$$

степени $r-1$ с коэффициентами из Π_p ; число таких многочленов совпадает с числом упорядоченных r -ок $(c_{r-1}, c_{r-2}, \dots, c_0)$, составленных из элементов поля Π_p , т. е. равно p^r . Указанное множество многочленов является полем относительно операций сложения и умножения при условии, что произведение и сумма многочленов приводятся по модулю p и по модулю $a(x)$. Это поле изоморфно полю Λ .

Напомним, что эта теорема уже использовалась при построении конечных полей. Там же объяснялось, в чем заключается приведение суммы и произведения, но мы повторим это еще раз. Коэффициенты результата заменяются их наименьшими неотрицательными вычетами по модулю p . Степень произведения может оказаться больше, чем $r-1$, но она меньше, чем $2r-1$. В этом

случае результат заменяется остатком, полученным при делении на многочлен $a(x)$.

8° Число квадратных корней из элемента конечного поля может быть 0, 1 или 2. Если поле имеет характеристику $p = 2$, то каждый его элемент имеет ровно один квадратный корень; если $p \neq 2$, то множество ненулевых элементов поля разбивается на два таких подмножества с равным числом элементов, что элементы одного подмножества не имеют квадратных корней, а элементы другого имеют два квадратных корня. Последнее подмножество образует подгруппу мультипликативной группы поля.

9° Сопоставим каждому элементу d поля Λ из 2^r элементов элемент

$$D = d^{2^{r-1}} + d^{2^{r-2}} + \dots + d.$$

Тогда поле разбивается на два таких подмножества по 2^{r-1} элементов в каждом, что для элементов одного подмножества $D = 0$, а для элементов другого $D = 1$.

10° В любом поле четной характеристики уравнение $z^2 + z + d = 0$ неразрешимо при $D = 1$ и имеет два различных решения при $D = 0$, где D определяется по коэффициенту d в соответствии с 9°.

11° В любом поле четной характеристики уравнение $x^2 + bx + c = 0$ имеет единственное решение при $b = 0$, а при $b \neq 0$ подстановкой

$$z = xb^{-1}, \quad d = cb^{-2}$$

приводится к уравнению $z^2 + z + d = 0$.

12° В поле нечетной характеристики число решений уравнения $x^2 + bx + c = 0$ равно 0, 1 или 2 соответственно числу квадратных корней из элемента $b^2 - 4c$.

Заметим, что теоремами 8° — 12° приходится пользоваться при исследовании кривых второго порядка на плоскости Галуа.

В заключение нашего обзора, посвященного конечным полям, отметим, что раздел теории чисел, известный под названием *циклические разностные базы*, также можно считать одним из приложений теории конечных групп. Первый значительный результат в этой области был получен Зингером, который в своей работе, появившейся в 1938 году, построил примеры простых циклических раз-

ностных баз. Результат Зингера позволяет непосредственно получать таблицы инцидентности плоскостей Галуа. (См. текст, относящийся к рис. 5 и 6, стр. 17, 20.)

7.3. Сведения из теории плоскостных тернарных систем

Понятие проективной плоскости, возникшее из понятия классической проективной плоскости, постепенно обобщалось, и одновременно с этим обобщалось понятие координат, служивших для алгебраического описания плоскости. Когда возникла потребность в алгебраическом описании недезарговых плоскостей, для задания координат стали применяться новые виды алгебраических систем, так называемые тернарные системы — с операцией, определяемой на множестве троек элементов основного множества. При фиксировании того или иного элемента тройки получаются некоторые бинарные операции, в терминах которых можно описать существенные свойства тернарных систем.

Пусть задано некоторое основное множество S , имеющее не менее двух элементов. Пусть каждой упорядоченной тройке (m, x, b) элементов из S сопоставлен определенный элемент из S , обозначенный символом $\langle xmb \rangle$. Тогда отображение $(m, x, b) \rightarrow \langle xmb \rangle$ будем называть *тернарной операцией*, а систему $(S, \langle \rangle)$ — *тернарной системой*.

Различные виды тернарных систем определяются с помощью аксиом для тернарных операций. Названия этих систем скорее связаны с «исторической традицией», чем выражают существо дела.

Плоскостное тернарное кольцо (обозначается PTR). Эта система определяется следующими аксиомами:

Θ_1 . Для любых $a, b, c \in S$ существует единственный элемент $u \in S$ такой, что $\langle abu \rangle = c$.

Θ_2 . Для любых $a, b, c, d \in S$ при условии $a \neq c$ существует единственный элемент $u \in S$ такой, что $\langle uab \rangle = \langle ucd \rangle$.

Θ_3 . Для любых $a, b, c, d \in S$ при условии $a \neq c$ существуют два элемента $u, v \in S$, такие, что $\langle auv \rangle = b$ и $\langle civ \rangle = d$.

Промежуточное тернарное кольцо (обозначается ITR). Эта система удовлетворяет аксиомам PTR, а также следующим аксиомам:

Θ_4 . Для любых $a, b, c, d, t, x \in S$ при условии $a \neq c$ из равенств $\langle atb \rangle = \langle ctb \rangle = d$ следует равенство $\langle xtb \rangle = d$.

Θ_5 . Для любых $a, b, c, d, t, x \in S$ при условии $a \neq c$ из равенств $\langle tab \rangle = \langle tcb \rangle = d$ следует равенство $\langle txb \rangle = d$.

Тернарное кольцо Холла (обозначается НТР). Эта система удовлетворяет аксиомам PTR, а также следующим аксиомам:

Θ_0 . Множество S содержит элементы $0, 1, (0 \neq 1)$, и для любых $a, b \in S$ $\langle a0b \rangle = \langle 0ab \rangle = b, \langle a10 \rangle = \langle 1a0 \rangle = a$.

Θ_2^* . Для любых $a, b, c \in S$ и $a \neq 0$ уравнение $\langle xab \rangle = c$ имеет в S ровно одно решение.

Для тернарных колец справедливы следующие теоремы:

1° В PTR пара (u, v) , существование которой утверждается в аксиоме Θ_3 , единственна.

2° В ИТР аксиомы Θ_4 и Θ_5 независимы от предыдущих аксиом.

3° Пусть основное множество PTR конечно. Тогда аксиома Θ_3 является необходимым и достаточным условием равносильности систем аксиом Θ_0, Θ_1 и $\Theta_1, \Theta_2, \Theta_3, \Theta_0, \Theta_2^*$.

4° Каждому четырехугольнику $OXYE$ на плоскости, определяемой системой аксиом I, можно сопоставить координатную систему $(K, \langle \rangle)$, а именно НТР, такую, что существует взаимно однозначное соответствие между множеством точек плоскости, за исключением точек прямой XY , и множеством упорядоченных пар (x, y) элементов из K ; прямой на плоскости отвечает при этом либо множество пар, удовлетворяющих условию $x = a$, либо множество пар, удовлетворяющих условию $y = \langle xmb \rangle$, где a, b, m — фиксированные элементы множества K .

Важно отметить, что координатная система НТР, вообще говоря, зависит от выбора четырехугольника.

5° Пусть система $(K, \langle \rangle)$ есть НТР. Будем считать «точками» упорядоченные пары (x, y) элементов из K , а прямыми — множества пар, удовлетворяющих условию $x = a$, и множества пар, удовлетворяющих условию $y = \langle xmb \rangle$. Тем самым мы получим аффинную плоскость с основным четырехугольником, имеющим следующие вершины: точка O — пара $(0, 0)$, точка E — пара $(1, 1)$, точки Y и X — идеальные точки прямых, заданных соответственно уравнениями $x = 0$ и $y = 0$.

ЛИТЕРАТУРА

Мы не в состоянии привести здесь исчерпывающий список литературы по конечным геометриям вплоть до настоящего времени. В превосходной монографии Дембовского, упоминаемой в следующей ниже краткой библиографии, на 48 страницах дается полная библиография за период с 1782 по 1968 год.

Мы указываем здесь статьи и монографии, позволяющие глубже изучить те разделы, которые лишь едва намечены в этой книге.

Книги

- Б л у м е н т а л ь (Blumenthal L. M.) A Modern View of Geometry.— San Francisco: Freeman, 1961.
- Б у с а к е р, С а а т и (Busacker R. G., Saaty T. L.) Finite Graphs and Networks.— N. Y.: McGraw-Hill, 1966.
- Д е м б о в с к и й (Dembowsky P.) Finite Geometries.— Berlin: Springer, 1968.
- К е р е к ь я р т о (Kerékjártó B.) Les Fondementas de la Geometry. Tome 2: Geometry projective.— Budapest: Académiai Kiadó, 1966.
- Р е д е и (Redei L.) Algebra. Vol. 1.— Budapest: Académiai Kiadó, 1967.
- Р и о р д а н (Riordan J.) An Introduction to Combinatorial Analysis.— N.Y.: Wiley, 1958.
- С е г р е (Segre B.) Lectures on Modern Geometry.— Roma: Cremonese, 1961. В книге имеется приложение: Л о м б а р д о Р а д и ч е (Lombardo Radice L.). Non-Desarguesian Finite Graphic Planes.
- Х о л л (Hall M.) The Theory of Groups.— N.Y.: The Macmillan, 1959. Русский перевод: Х о л л М. Теория групп.— М.: ИЛ, 1962.

Статьи

- А ц е л (Aczél J.) Quasigroups, net and nomograms.— Advances Math., 1965, 1, p. 383—450.
- А ц е л, К а р т е с и (Aczél J., Kárteszi F.) Funktionskomposition, vertauschbare Funktionen und Iterationsgruppen vom geometrischen Standpunkt aus.— Math.-Phys. Semesterberichte, 1967, 14, № 1, S. 79—88.
- Б а р л о т т и (Barlotti A.) Una costruzione di una classe di spazi affini generalizzati.— Boll. Un. Mat. Ital., 1962, 17, p. 394—398.
- Б а р т о л о ц ц и (Bartolozzi F.) Su una classe di quasicorpi (sinistri) finiti.— Rend. Mat., 1965, 24, p. 165—173.

- Б о з е (Bose R. C.). On the application of the properties of Galois fields to the problem of the construction of hyper Greco-Latin squares. — *Sankhya, Ind. J. Statistics*, 1938, 3, p. 323—338.
- Б р у к, Р а й з е р (Bruck R. H., Ryser J. H.) The non-existence of certain finite projective planes. — *Canad. J. Math.*, 1949, 1, p. 88—93.
- Г л и с о н (Gleason A. M.) Finite Fano planes. — *Amer. J. Math.*, 1956, 78, p. 797—807.
- З и н г е р (Singer J.) A theorem in finite projective geometry and some applications to number theory. — *Trans. Amer. Math. Soc.*, 1938, 43, p. 377—386.
- К а р т е с и (Kármányi F.) 1. Piano finite ciclici come risoluzioni di un certo problema di minimo. — *Boll. Un. Mat. Ital.*, 1960, 15, p. 522—528.
2. Alcuni problemi della geometria d'incidenza. — *Confer. Sem. Mat. Univ. Bari*, 1963, 88, p. 1—14.
- К в и с т (Quist B.) Some remarks concerning curves of the second degree in a finite plane. — *Ann. Acad. Fenn.*, 1952, 134, p. 1—27.
- К о ф м а н (Cofman J.) Triple transitivity in finite Möbius planes. — *Atti Accad. Naz. Lincei Rend.*, 1967, 42, p. 616—620.
- К р о у (Crowe D. W.) The construction for finite regular hyperbolic planes from inversive planes of even order. — *Coll. Math.*, 1965, 13, p. 247—250.
- Л ю н е б у р г (Lüneburg H.) 1. Gruppentheoretische Methoden in der Geometrie. — *Jahresber. Deutsch. math. Ver.*, 1967, 70, S. 16—51.
2. Transitive Erweiterungen endlicher Permutationsgruppen. — *Berlin: Springer (Lecture Notes in Math., 84)*, 1969, S. 1—119.
- Р е й м а н (Reiman I.) Su una proprietà dei 2-disegni. — *Rend. Mat.*, 1968, p. 1—7.
- Р о з а т и (Rosati L. A.) Piani proiettivi desarguesiani non ciclici. — *Boll. Un. Mat. Ital.*, 1957, 12, p. 230—240.
- С е г р е (Segre B.) 1. Ovals in a finite projective plane. — *Canad. J. Math.*, 1955, 7, p. 414—416.
2. Introduction to Galois geometries. — *Atti Accad. Naz. Lincei, Memorie*, 1967, 8, p. 135—236.
- С е л е (Szele T.) Elemi bizonyítás a véges testek elméletének alaptelelre. — *Mat. Lapok.*, 1956, 7, p. 249—254.
- Т а л л и н и (Tallini G.) Le geometrie di Galois a le loro applicazioni alla statistica e alla teorie dell'informazione. — *Rend. Mat.*, 1960, 19, p. 379—400.
- Т у р а н, Ш о ш, К ё в а р и (Turán P., Sós V., Köváry T.) On a problem of K. Zaremkiewicz. — *Coll. Math.*, 1954, 3, p. 50—57.
- Ф а н о (Fano G.) Sui postulati fondamentali della geometria proiettiva. — *Giorn. Mat.*, 1892, 30, p. 106—112.
- Х о л л (Hall M.) Projective planes. — *Trans. Amer. Math. Soc.*, 1943, 54, p. 229—277.
- Ц а п п а (Zappa G.) Piano grafici a caratteristica 3. — *Ann. Math. Pura Appl.*, 1960, 49, p. 157—166.
- Ш п е р н е р (Sperner E.) Affine Räume mit schwacher Inzidenz und zugehörige algebraische Strukturen. — *J. reine und angew. Math.*, 1960, 204, S. 205—215.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ *)

Автоморфизм 173, 177
 Ассоциированная плоскость 43
 Ассоциированный точечный октет 248
 Аффинная плоскость 42—44
 Аффинное преобразование 73

 Базис 112
 Бихроматический граф 230
 Блок 245
 Блок-схема 245

Внешняя прямая 138, 159
 — точка 141
 Внутренняя точка 141

Гамильтонова цепь 229
 Гамма (Γ -) крюк 21
 — (Γ -) таблица 23
 Гетероморфные графы 231
 — таблицы инцидентности 204
 Гиперболическая плоскость 45
 Гипервал 140
 Гомография 177
 Гомологичные элементы 26
 Гомология 68
 Гомотетия 75
 Граф 229
 — Гамильтона 229
 — Петерсена 227
 Группа коллинеаций 68
 — подстановок 243

Двойное отношение 118—124
 Двойственность 9, 118
 Дезаргова конфигурация 210—218

Дерево 229
 Диагональная точка 70
 Диагональное распределение 23

Единичная точка 124

Замкнутая цепочка 248

Идеальная точка 44
 Изоморфизм 13, 173, 177
 Изоморфные графы 231
 — плоскости 13
 — таблицы инцидентности 204
 Импримитивная группа 245
 Инвариантная прямая 66
 — точка 66
 Инверсная плоскость 247
 Инволюция 68
 Интранзитивная группа подстановок 243
 Инцидентность 8

Каноническая форма 156
 Касательная 138, 157, 159
 Квадрика 253
 Квазигруппа 77
 Класс графа 229
 Классическая проективная геометрия 9
 — проективная плоскость 7
 Классы эквивалентности 244
 Коллинеация 65
 Комбинаторная структура 11
 Конфигурация 204
 — Рейдемейстера 221
 Кривая 156, 158
 k -транзитивная группа перестановок 263

Латинские квадраты 78
 Линейная комбинация 51
 Линейное преобразование 133

Максимальное подпространство 112
 Маршрут 229
 Модель Холла 58

Недезаргова плоскость 58
 Независимая система точек 107
 Независимые подпространства 113
 неподвижные прямые 66
 — точки 66
 Не-точка 106
 Нормирование координатной последовательности 107
 N -теорема 249

*) Термины приложения не входят в указатель.

Обхват графа 229
Объединение (двух подпространств) 113
Обыкновенная дезаргова конфигурация 211
Овал 138
Овалоид 253
Однородные координаты 106, 118
Омега (Ω -)таблица 21

Параллельность 44
Пересечение подпространств 112
Плоскость Галуа 49—54
— Мебиуса 247
— порядка q 11
— трансляции 225
— Фано 8, 265
Подплоскость 41
Полная группа подстановок 68, 243
— ортогональная система латинских квадратов 77, 78
Полный Γ -крюк 21
— граф 229
Полус прямой 160
Поляра точки 159
Порядок графа 229
Преобразования (ω -, σ -, τ -) 12
Примитивная группа 245
Проективная геометрия 9, 49
— плоскость 11
Прямая 8, 51
Прямоугольник знаков 23
— квадратов 26
Пустой граф 229

Размерность пространства 112
Ребро графа 229
Регулярная гиперболическая плоскость 45
Регулярный граф 229

Самосопряженная точка 152, 158
Секунция 138, 159
Сеть 218
Система аксиом для аффинной плоскости 44
Система аксиом для плоскости Мёбиуса 247
— аксиом для проективной плоскости 8, 10, 11
— аксиом для пространства Галуа 105, 106

Система аксиом для регулярной гиперболической плоскости 48
— аксиом для трехмерного пространства 296
— координат 124
Специальная дезаргова конфигурация 212
Стереографическое отображение 248
Ступени плоскости 58
Сферическая модель Пуанкаре 227

Таблица инцидентности 13, 20, 26, 28
— конфигурации 204
— Кэли 223
Теорема Глисона 276
— Дезарга 56
— Зингера 44
— Кроува 48
— пятиугольника 210
— Сегре 167
Тернарная операция 28
Точка 8, 51
— графа 229
— сочленения графа 230
Тракт 42
Транзитивная группа подстановок 243

Фигура Фано 7
Фундаментальная точка 124
Фундаментальный треугольник 129, 131

Центрально-осевая коллинеация 67
Центр коллинеации 66
Цикл графа 229
Циклическая группа 68
— таблица инцидентности (Ω -таблица) 20
Циклический вид 44

Четырехугольник Фано 71

Эляция 68
Элементарное преобразование 204

Ядро овала 140

ОГЛАВЛЕНИЕ

Предисловие	3
Символы и обозначения	5

Глава 1

ОСНОВНЫЕ ПОНЯТИЯ, ОТНОСЯЩИЕСЯ К КОНЕЧНЫМ ГЕОМЕТРИЯМ

1.1. Конечная плоскость	7
1.2. Изоморфные плоскости, таблицы инцидентности	11
1.3. Конструирование конечных плоскостей. Циклические плоскости	15
1.4. Г-таблица конечной проективной плоскости	21
1.5. Системы координат на конечной плоскости	28
1.6. Понятие о плоскостях Галуа и полях Галуа	32
1.7. Замкнутые подплоскости конечной проективной плос- кости	39
1.8. Понятие конечной аффинной плоскости	42
1.9. Различные виды конечных гиперболических плоскостей . .	45
1.10. Плоскости Галуа и теорема Дезарга	49
1.11. Недезаргова плоскость	58
1.12. Коллинеации и группы коллинеаций конечной плоско- сти	62
1.13. Сохраняющие коллинеарность отображения аффинной и регулярной гиперболической конечной плоскости	72
1.14. Конечные проективные плоскости и полные ортогональ- ные системы латинских квадратов	77
1.15. Композиция линейных функций и плоскость $D(X, Y)$. .	88
1.16. Задачи и упражнения к главе 1	99

Глава 2

ГЕОМЕТРИИ ГАЛУА

2.1. Понятие пространства Галуа	105
2.2. Пространство Галуа как конфигурация его подпро- странств	109
2.3. Обобщение теоремы Паппа на плоскости Галуа	119
2.4. Координаты на плоскости Галуа	124
2.5. Отображения, определенные с помощью линейных пре- образований	133
2.6. Линейное отображение данного четырехугольника в другой данный четырехугольник	135
2.7. Понятие овала на конечной плоскости	138

2.8. Коники в плоскости Галуа	143
2.9. Точечные конфигурации порядка 2 на плоскости Галуа четного порядка	150
2.10. Каноническое уравнение кривой второго порядка на плоскости Галуа четного порядка	154
2.11. Точечные конфигурации порядка 2 на плоскости Галуа нечетного порядка	157
2.12. Соответствие между двумя пучками прямых	162
2.13. Теорема Сегре	167
2.14. Дополнительные замечания относительно конструкции плоскостей Галуа	172
2.15. Коллинеации и гомографии на плоскости Галуа	177
2.16. Характеристика конечной проективной плоскости	179
2.17. Множество коллинеаций плоскости Галуа в себя	182
2.18. Дезарговы конечные плоскости	187
2.19. Задачи и упражнения к главе 2	201

Глава 3

ГЕОМЕТРИЧЕСКИЕ КОНФИГУРАЦИИ И СЕТИ

3.1. Понятие геометрической конфигурации	203
3.2. Пятиугольники, вписанные друг в друга	206
3.3. Теорема пятиугольника и дезаргова конфигурация	240
3.4. Понятие геометрической сети	248
3.5. Группы и R-сети	223
3.6. Задачи и упражнения к главе 3	225

Глава 4

НЕКОТОРЫЕ ПРИЛОЖЕНИЯ КОНЕЧНЫХ ГЕОМЕТРИЙ К КОМБИНАТОРИКЕ

4.1. Теорема замыкания для гиперболического пространства	226
4.2. Некоторые основные факты, касающиеся графов	228
4.3. Обобщения графа Петерсена	233
4.4. Одна экстремальная задача комбинаторики	237
4.5. Граф дезарговой конфигурации	240
4.6. Задачи и упражнения к главе 4	241

Глава 5

КОМБИНАТОРИКА И КОНЕЧНЫЕ ГЕОМЕТРИИ

5.1. Основные понятия комбинаторики	243
5.2. Две основные теоремы инверсной геометрии	247
5.3. Конечные инверсные геометрии и t -(v , k , λ)-схемы	252
5.4. Некоторые теоремы, относящиеся к плоскости Мёбиуса	257
5.5. Структура инцидентности и t -блок-схема	261
5.6. Задачи и упражнения к главе 5	263

Глава 6**НЕКОТОРЫЕ ДОПОЛНИТЕЛЬНЫЕ ВОПРОСЫ ТЕОРИИ
КОНЕЧНЫХ ГЕОМЕТРИЙ**

6.1. Плоскость Фано и теорема Глисона	265
6.2. Построение новых плоскостей из плоскостей Галуа	280
6.3. Обобщение понятия аффинной плоскости	290
6.4. Задачи и упражнения к главе 6	294

7. ПРИЛОЖЕНИЕ

7.1. Общие сведения об алгебраических структурах .	298
7.2. Сведения из теории конечных полей и теории чисел	307
7.3. Сведения из теории плоскостных тернарных систем	312

Литература	314
------------	-----

Предметный указатель	316
----------------------	-----

Ференц Картеси

«Введение в конечные геометрии»

М., 1980 г., 320 стр. с илл.

Редактор *Н. Р. Камышанский*
Техн. редактор *Е. В. Морозова*
Корректор *А. Л. Ипатова*

ИБ № 11541

Сдано в набор 04.09.79. Подписано к печати 23.01.80. Бумага 84×108¹/₃₂. тип. № 1. Обыкновенная гарнитура. Высокая печать. Условн. печ. л. 16,80. Уч.-изд. л. 15,41. Тираж 7 500 экз. Заказ № 0446. Цена книги 1 р. 40 к.

Издательство «Наука». Главная редакция физико-математической литературы 117071, Москва. В-71, Ленинский проспект, 15

Набрано в Ордена Трудового Красного Знамени Московской типографии № 7 «Искра революции» Союзполиграфпрома Государственного Комитета СССР по делам издательства, полиграфии и книжной торговли, Москва 103001, Трехпрудный пер., 9

Отпечатано во 2-й типографии издательства «Наука», 121099, Москва, Шубинский пер., 10. Зак. 2795