Наш семинар: математические сюжеты

Конечные проективные плоскости

Ю. И. Ионин

§1. Определение проективной плоскости

Истоки проективной геометрии можно найти в попытках художников Возрождения создать правдоподобные двумерные образы трехмерных объектов. Зритель видит точку на картине посредством луча, направленного из этой точки в глаз зрителя. Если глаз зрителя находится в начале координат, то каждая точка в плоскости картины определяется прямой, проходящей через эту точку и начало координат, а каждая прямая в плоскости картины определяется плоскостью, проходящей через эту прямую и начало координат.

Прямые и плоскости, проходящие через начало координат, естественным образом отождествляются с одномерными и двумерными подпространствами трехмерного векторного пространства.

Определение 1.1. Пусть V — трехмерное векторное пространство над полем F. Точками *проективной плоскости над полем* F являются все одномерные подпространства пространства V, а прямыми — все двумерные подпространства. Проективная плоскость над F обозначается $PG(2, F)$. Если F — конечное поле порядка q, то проективная плоскость над F обозначается $PG(2, q)$.

Для того чтобы сделать это определение более наглядным, рассмотрим плоскость $z = 1$ в трехмерном координатном пространстве над полем F. Каждая прямая, проходящая через начало координат и не лежащая в плоскости xy, однозначно определяется точкой пересечения $(a, b, 1)$ с плоскостью $z = 1$, и мы обозначим (a, b) соответствующую этой прямой точку

проективной плоскости $PG(2, F)$. Каждая прямая, проходящая через начало координат и лежащая в плоскости xy, однозначно определяется ее угловым коэффициентом a, и мы обозначим (a) соответствующую точку в $PG(2, F)$. Для углового коэффициента прямой $x = 0$ в плоскости xy мы используем символ ∞. Таким образом, множество P всех точек проективной плоскости $PG(2, F)$ может быть представлено как

$$P = \{(a, b)\colon a, b \in F\} \cup \{(a)\colon a \in F\} \cup \{(\infty)\}. \tag{1}$$

Каждая плоскость, проходящая через начало координат, кроме плоскости xy, однозначно определяется прямой, по которой она пересекает плоскость $z = 1$. Если эта прямая задается в плоскости $z = 1$ уравнением $y = xa + b$, мы обозначаем $[a, b]$ соответствующую прямую в $PG(2, F)$. Если же эта прямая задается уравнением $x = a$, то соответствующая прямая в $PG(2, F)$ обозначается $[a]$. Наконец, прямая в $PG(2, F)$, соответствующая плоскости xy, обозначается $[\infty]$.

Таким образом, множество $\mathcal{L}$ всех прямых проективной плоскости $PG(2, F)$ может быть представлено как

$$\mathcal{L} = \{[a, b]\colon a, b \in F\} \cup \{[a]\colon a \in F\} \cup \{[\infty]\}. \tag{2}$$

Прямые в $PG(2, F)$ можно представить как множества точек следующим образом:

$$[a, b] = \{(x, xa + b)\colon x \in F\} \cup \{a\}, \tag{3}$$

$$[a] = \{(a, y)\colon y \in F\} \cup \{(\infty)\}, \tag{4}$$

$$[\infty] = \{(a)\colon a \in F\} \cup \{(\infty)\}. \tag{5}$$

Подобное представление проективной плоскости называется ее *координатизацией*.

Точки (a), $a \in F$, и (∞) называют *идеальными точками* проективной плоскости, так что на каждой прямой, кроме $[\infty]$, лежит одна идеальная точка. Прямую $[\infty]$ называют *идеальной прямой*. «Неидеальные» точки и прямые образуют $AG(2, F)$ — *аффинную плоскость над полем* F.

Через любые две точки прективной плоскости проходит одна и только одна прямая, и любые две прямые пересекаются в единственной точке. Мы примем эти свойства за основу аксиоматического определения проективной плоскости.

Определение 1.2. *Проективная плоскость* $\Pi = (P, \mathcal{L})$ состоит из множества P, элементы которого называются точками, из множества $\mathcal{L}$, элементы которого называются прямыми, и из бинарного отношения $\in$ между точками и прямыми. Если $x \in L$, где x — точка, L — прямая, мы говорим «x лежит на L», «L проходит через x», «x и L инцидентны» и т. п.

Точки и прямые проективной плоскости должны удовлетворять следующим аксиомам.

P1. Через любые две точки проходит одна и только одна прямая.

P2. Любые две прямые имеют одну и только одну общую точку.

P3. Существуют четыре точки, никакие три из которых не лежат на одной прямой.

Если $x, y \in P$, $x \neq y$, то xy — это прямая, проходящая через x и y; если $L, M \in \mathcal{L}$, $L \neq M$, то LM — это точка пересечения L и M.

Плоскость Фано. На рис. 1 изображена проективная плоскость, в которой точки — это вершины, середины сторон и центр правильного тругольника, а прямые — стороны, медианы и вписанная окружность. Эта проективная плоскость называется *плоскостью Фано*. Если плоскость Фано координатизировать, как показано на рисунке, она превращается в $PG(2, 2)$.

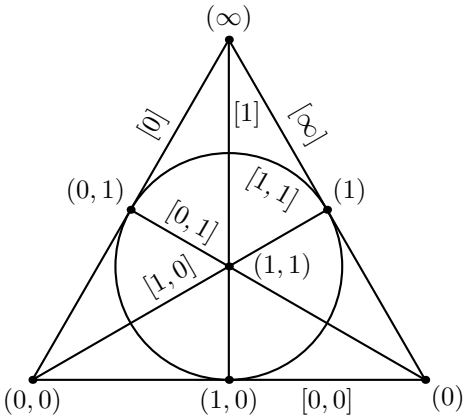

Рис. 1.

Как показывает следующее упражнение, аксиома P3 нужна для того чтобы избежать нескольких вырожденных примеров.

Упражнение. Предположим, что система $\Pi = (P, \mathcal{L})$ точек и прямых удовлетворяет аксиомам P1 и P2, но не удовлетворяет аксиоме P3. Докажите, что имеет место один (или более) из следующих случаев: (а) $P = \varnothing$; (б) есть только одна прямая (и все точки лежат на этой прямой); (в) существуют $x \in P$ и $L \in \mathcal{L}$ такие, что все точки, кроме x, лежат на L и все прямые, кроме L, проходят через x.

Аксиома P2 может быть получена из P1 заменой точек прямыми, а прямых — точками. Если a, b, c, d — четыре точки, никакие три из которых не лежат на одной прямой (аксиома P3), то ab, bc, cd, da — четыре

прямые, никакие три из которых не пересекаются в одной точке. Поэтому для проективной плоскости справедлив следующий *принцип двойственности*: если в верном утверждении о проективных плоскостях заменить точки прямыми, а прямые — точками, то снова получится верное утверждение о проективных плоскостях.

Проективная плоскость называется *конечной*, если множество ее точек (и, следовательно, прямых) конечно. В проективной плоскости над конечным полем порядка q каждая прямая проходит через $q+1$ точек и каждая точка лежит на $q+1$ прямых. Аналогичное утверждение справедливо для любой конечной проективной плоскости.

Теорема 1.3. Для любой конечной проективной плоскости $\Pi = (P, \mathcal{L})$ сучествует натуральное число $n \geqslant 2$ — *порядок* Π, такое что

(а) каждая прямая проходит через $n+1$ точек,

(б) каждая точка лежит на $n+1$ прямых,

(в) $|P| = |\mathcal{L}| = n^2 + n + 1$.

Доказательство. Пусть $L, M \in \mathcal{L}$, $L \neq M$, и пусть a — точка, не лежащая ни на L, ни на M (такая точка существует в силу аксиомы P3). Зададим отображение f множества точек на прямой L в множество точек на прямой M следующим образом:

если $x \in L$, то $f(x)$ — точка пересечения прямых xa и M.

Проверьте, что f — биекция, откуда следует, что число точек на любой прямой одно и то же. Представим это число как $n+1$. В силу принципа двойственности через любую точку проективной плоскости проходят $n+1$ прямых. Зафиксируем точку a. Каждая прямая, проходящая через a, проходит через n других точек, и все точки плоскости лежат на этих прямых, так что $|P| = (n+1)n + 1 = n^2 + n + 1$. В силу принципа двойственности $|\mathcal{L}| = n^2 + n + 1$. Если $n = 0$ или 1, то $|P| < 4$, что противоречит аксиоме P3, так что $n \geqslant 2$.

С понятием проективной плоскости тесно связано понятие аффинной плоскости.

Определение 1.4. *Аффинная плоскость* состоит из множества точек и из множества прямых, удовлетворяющих следующим аксиомам.

A1. Через любые две точки проходит одна и только одна прямая.

A2. Если точка x не лежит на прямой L, то существует единственная прямая M, проходящая через x и не имеющая с L общих точек.

A3. Существуют три точки, не лежащие на одной прямой.

В аффинной плоскости две прямые *параллельны*, если они не имеют общих точек или совпадают. Присоединив к каждой прямой в аффинной

плоскости идеальную точку таким образом, что две прямые получают одну и ту же идеальную точку в том и только в том случае, если они параллельны, и присоединив к плоскости идеальную прямую, образованную всеми идеальными точками, мы получим проективную плоскость. Обратно, удалив из проективной плоскости одну прямую и все лежащие на ней точки, мы получим аффинную плоскость.

§2. Другие примеры проективных плоскостей

Соотношения (1)–(5) предыдущего параграфа описывают проективную плоскость над полем F. Оказывется, те же соотношения описывают проективную плоскость, если поле F заменено почтиполем.

Определение 2.1. *Почтиполе* — это множество F с двумя бинарными операциями — сложением и умножением, удовлетворяющими следующим условиям:

(а) F — абелева группа относительно сложения, нейтральный элемент которой обозначается 0;

(б) $F^* = F \setminus \{0\}$ — группа относительно умножения;

(в) $(a+b)c = ac + bc$ для любых $a, b, c \in F$.

Таким образом, почтиполе, в отличие от поля, не требует коммутативности умножения и одного из дистрибутивных законов.

Пример. Пусть q — нечетное простое число или степень нечетного простого числа и пусть F — поле порядка q^2. Чтобы получить почтиполе, мы сохраним все элементы поля F, оставим неизменной операцию сложения и введем новую операцию умножения, обозначаемую $\circ$:

$$a \circ b = \begin{cases} ab, \text{ если } b \text{ является квадратом элемента поля } F, \\ a^q b, \text{ если } b \text{ не является квадратом элемента поля } F. \end{cases}$$

Упражнение. Проверьте, что $(F, +, \circ)$ — почтиполе. При проверке ассоциативности умножения воспользуйтесь тем, что в конечном поле произведение двух неквадратов — квадрат. Дистрибутивный закон следует из тождества $(a+b)^q = a^q + b^q$.

Наименьшее почтиполе (не являющееся полем) состоит из девяти элементов. Его мультипликативную группу можно представить как $\{\pm 1, \pm i, \pm j, \pm k\}$ с кватернионным умножением: $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$.

Пусть F — произвольное конечное почтиполе. Определим множество точек P и множество прямых $\mathcal{L}$ соотношениями (1)–(5). Мы утверждаем, что $\Pi = (P, \mathcal{L})$ — проективная плоскость.

Аксиома P3 очевидна, а проверка аксиомы P1 проводится точно так же, как и в случае поля. Однако, если мы попытаемся проверить аксиому P2 «в лоб», мы обнаружим, что требуется отсутствующий дистрибутивный закон. Мы «пойдем в обход» и сначала заметим, что из соотношений (3)–(5) следует, что каждая прямая состоит из $n+1$ точек, где n — число элементов почтиполя F, что через каждую точку проходят $n+1$ прямых и что общее число прямых равно n^2+n+1. Теперь мы зафиксируем прямую L и подсчитаем число пар (x, M), где M — прямая, отличная от L, а x — общая точка L и M. Если мы сначала выберем точку $x \in L$, а затем прямую $M \neq L$, проходящую через x, мы получим, что число таких пар равно $(n+1)n$. Поскольку имеется n^2+n прямых $M \neq L$ и ни одна из них (в силу аксиомы P1) не пересекает L более чем в одной точке, мы получаем, что каждая такая прямая пересекает L ровно в одной точке.

Приведенное рассуждение существенно использует конечность почтиполя F. В бесконечном случае для получения проективной плоскости на почтиполе налагается дополнительное требование *планарности*: для любых $a, b, c \in F$, уравнение $xa + xb = c$ имеет единственное решение. Всякое конечное почтиполе планарно.

Если F — почтиполе, то множество $K = \{x \in F\colon x(a+b) = xa + xb$ для всех $a, b \in F\}$ называется *ядром* F и обозначается $\ker(F)$.

Упражнение. Проверьте, что $K = \ker(F)$ — поле, F — векторное пространство над K.

Если F — конечное поле, то F является конечномерным векторным пространством над конечным полем K. Отсюда следует, что число элементов любого конечного почтиполя — степень простого числа.

Мы приведем еще один пример построения проективной плоскости.

Пусть F — поле, V — векторное пространство четной размерности $2d$ над F. Будем считать элементы множества V точками проективной плоскости. Прямой назовем любое множество точек вида $U + x$, где $x \in V$, а U — d-мерное подпространство пространства V. Прямые вида $U + x$ и $U + y$ с одним и тем же подпространством U назовем параллельными. Множество всех прямых таким образом разбивается на классы параллельных прямых. Присоединим к каждой прямой идеальную точку так, что две прямых получают одну и ту же идеальную точку в том и только в том случае, если они параллельны. Кроме того, образуем идеальную прямую, состоящую из всех идеальных точек.

Упражнение. Проверьте, что множество точек и множество прямых, описанных в предыдущем абзаце, образуют проективную плоскость.

§3. Координатизация

Начав с поля или почтиполя F, мы построили проективную плоскость, точки и прямые которой удовлетворяют соотношениям (1)–(5). Можно ли получить проективную плоскость, исходя из менее жесткой алгебраической структуры? В этом параграфе мы начнем с проективной плоскости, введем на ней координаты, базирующиеся на бесструктурном множестве F и затем используем свойства проективной плоскости для определения операций сложения и умножения на F. Хотя нижеследующие построения могут быть проведены для любой проективной плоскости, мы ограничимся конечным случаем.

Пусть $\Pi = (P, \mathcal{L})$ — проективная плоскость порядка $n \geqslant 2$ и пусть F — множество из n элементов. Выберем два элемента в множестве F и обозначим их 0 и 1. Пусть ∞ — символ, не являющийся элементом F. Выберем в плоскости Π *начальный четырехугольник*, т. е. упорядоченную четверку точек, никакие три из которых не лежат на одной прямой. Обозначим эти точки последовательно $(0,0)$, (0), (∞) и $(1,1)$. Обозначим шесть прямых, проходящих через пары обозначенных точек следующим образом: $(0,0)(0) = [0,0]$, $(0,0)(\infty) = [0]$, $(0)(\infty) = [\infty]$, $(1,1)(\infty) = [1]$, $(1,1)(0) = [0,1]$, $(0,0)(1,1) = [1,0]$. (Напомним, что если x и y — различные точки, то xy — проходящая через них прямая, а если L и M — различные прямые, то LM — их общая точка.) Если бы F было полем или почтиполем, то указанные прямые представляли бы соответственно ось абсцисс, ось ординат, идеальную прямую и прямые $x = 1$, $y = 1$ и $y = x$. Мы теперь можем координатизировать еще три точки: $(1,0) = [1][0,0]$, $(0,1) = [0][0,1]$, $(1) = [\infty][1,0]$ (рис. 2).

На идеальной прямой $[\infty]$ остается $n-2$ точек, кроме (0), (∞) и (1), а в множестве F есть $n-2$ элементов, кроме 0 и 1. Обозначим оставшиеся точки идеальной прямой символами (a), где $a \in F$, $a \neq 0$, $a \neq 1$, так чтобы разные точки обозначались разными символами.

Мы готовы завершить координатизацию плоскости Π. Для каждого $a \in F$ положим $(0,0)(a) = [a,0]$, $[1][a,0] = (1,a)$, $(0)(1,a) = [0,a]$, $[0,a][1,0] = (a,a)$, $(a,a)(\infty) = [a]$, $[a][0,0] = (a,0)$, $[0,a][0] = (0,a)$ (рис. 2). Наконец, для любых $a, b \in F$ положим

$$(a,b) = [a][0,b], \quad [a,b] = (a)(0,b).$$

Если F — поле, то $(a, a+b)$ — это точка пересечения прямых $[a]$ и $[1,b]$, а (a,ab) — это точка пересечения прямых $[a]$ и $[b,0]$. Поэтому мы определяем сложение и умножение на произвольном координатизирующем множестве F так, чтобы следующие соотношения выполнялись для любых $a, b \in F$:

$$(a, a+b) = [a][1,b], \quad (a,ab) = [a][b,0]. \tag{6}$$

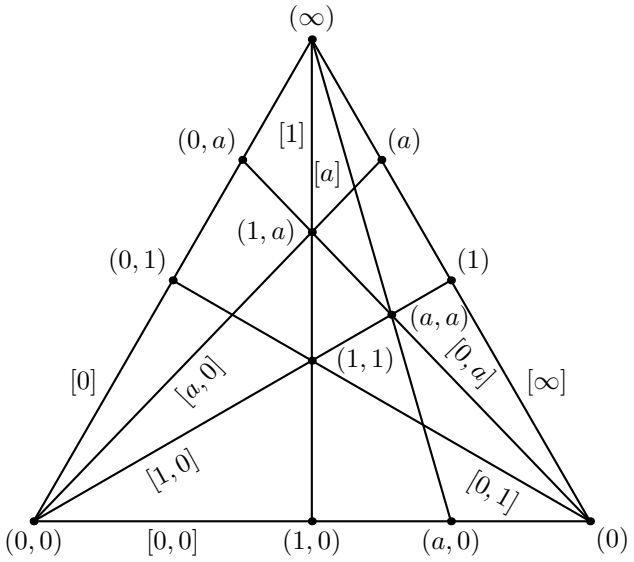

Рис. 2.

Итак, у нас есть множество F с операциями сложения и умножения и при этом точки и прямые плоскости Π удовлетворяют условиям (1), (2), (4) и (5). Мы будем называть множество F *координатным кольцом* проективной плоскости Π. Предостережение: координатное кольцо не обязано быть кольцом в обычном алгебраическом смысле этого термина. При этом примеры «плохих» координатных колец совсем не очевидны (мы их получим в последующих параграфах). Отметим также, что алгебраические свойства координатного кольца могут зависеть от выбора начального четырехугольника.

Теорема 3.1. Введенные операции сложения и умножения в координатном кольце F обладают следующими свойствами:

(a) $a+0=0+a=a$, $a\cdot 1=1\cdot a=a$, $a\cdot 0=0\cdot a=0$ для любого $a\in F$;

(b) для любых $a,b\in F$ каждое из уравнений $a+x=b$, $x+a=b$ имеет единственное решение;

(c) для любого $a\in F^*=F\setminus\{0\}$ и для любого $b\in F$ каждое из уравнений $ax=b$, $xa=b$ имеет единственное решение.

Мы докажем по одному свойству из каждой группы и предоставим читателю доказательство остальных свойств.

(a) $(1,1\cdot a)=[1][a,0]=(1,a)$ (рис. 2). Поэтому $1\cdot a=a$.

(b) $a+x=b\ \Leftrightarrow\ (a,a+x)=(a,b)\ \Leftrightarrow\ [a][1,x]=(a,b)\ \Leftrightarrow\ (a,b)\in[1,x]$.

Последнее условие означает, что $[1, x]$ — единственная прямая, проходящая через точки (1) и (a, b), что однозначно определяет x.

(c) $xa = b \Leftrightarrow (x, xa) = (x, b) \Leftrightarrow [x][a, 0] = (x, b) \Leftrightarrow (x, b) \in [a, 0]$. Последнее условие означает, что (x, b) — точка пересечения различных $(a \neq 0)$ прямых $[a, 0]$ и $[0, b]$, так что x определен однозначно.

Нам предстоит долгий и не всегда успешный путь от этих простых свойств до аксиом поля или почтиполя, и центральную роль на этом пути будет играть знаменитая теорема проективной геометрии.

§4. Теорема Дезарга

Жерар Дезарг (1591–1661) — французский инженер, архитектор и математик — считается одним из создателей проективной геометрии. Для формулировки теоремы Дезарга нам понадобится следующее определение.

Определение 4.1. Треугольник в проективной плоскости — это упорядоченная тройка точек, не лежащих на одной прямой.

Треугольники $x_1x_2x_3$, $y_1y_2y_3$, такие что $x_1 \neq y_1$, $x_2 \neq y_2$, $x_3 \neq y_3$, называются *центрально перспективными*, если прямые x_1y_1, x_2y_2, x_3y_3 попарно различны и проходят через общую точку.

Треугольники $x_1x_2x_3$, $y_1y_2y_3$, такие что $x_1x_2 \neq y_1y_2$, $x_2x_3 \neq y_2y_3$, $x_3x_1 \neq y_3y_1$, называются *аксиально перспективными*, если точки пересечения прямых x_1x_2 и y_1y_2, x_2x_3 и y_2y_3, x_3x_1 и y_3y_1 попарно различны и лежат на одной прямой.

Треугольники $x_1x_2x_3$, $y_1y_2y_3$ на рис. 3 центрально и аксиально перспективны.

Теорема Дезарга. Два треугольника в проективной плоскости (над полем вещественных чисел) центрально перспективны в том и только в том случае, если они аксиально перспективны.

Заметим, что определения центрально перспективных и аксиально перспективных треугольников взаимно двойственны. (Строго говоря, в случае аксиальной перспективы следует заменить треугольники трехсторонниками, образованными прямыми, проходящими через пары вершин треугольника.) Поэтому для получения теоремы Дезарга во всей полноте достаточно доказать, что центрально перспективные треугольники аксиально перспективны.

Предположим, что треугольники $x_1x_2x_3$, $y_1y_2y_3$ на рис. 3 центрально перспективны и обозначим через z_1, z_2, z_3 точки пересечения прямых x_2x_3 и y_2y_3, x_3x_1 и y_3y_1, x_1x_2 и y_1y_2 соответственно. Представим себе, что рис. 3 является двумерной проекцией трехмерного объекта, т. е. что прямые x_1y_1, x_2y_2, x_3y_3 на самом деле не лежат в одной плоскости. Тогда

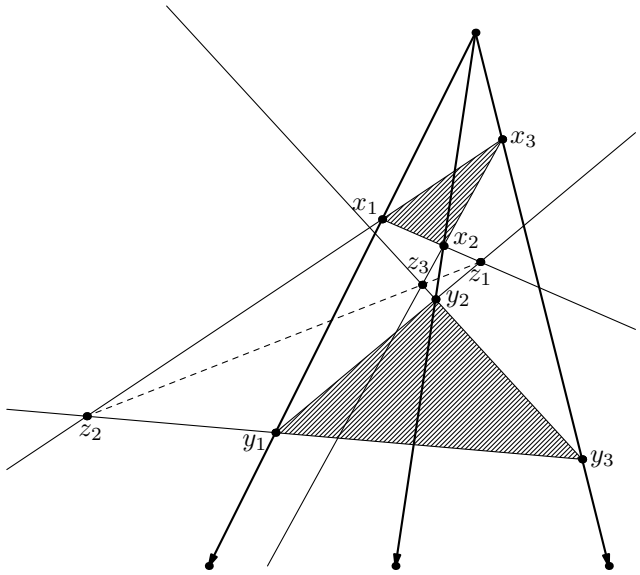

Рис. 3.

точки z_1, z_2, z_3 лежат как в плоскости $x_1x_2x_3$, так и в плоскости $y_1y_2y_3$, и потому лежат на прямой, являющейся пересечением этих плоскостей. Поскольку проектирование на плоскость под разумно выбранным углом не нарушает ни инцидентности, ни прямолинейности, из трехмерной теоремы Дезарга следует двумерная.

Приведенное рассуждение является наброском доказательства, которое может быть формализовано для проективной плоскости над произвольным полем. Мы, однако, приведем другое доказательство, которое послужит нам и в дальнейшем.

Теорема 4.2. Теорема Дезарга справедлива для проективной плоскости $PG(2, F)$, где F — поле.

Доказательство. Мы будем опираться на определение 1.1, так что отмеченные точки на рис. 3 представляют одномерные подпространства трехмерного векторного пространства V над полем F, а прямые — двумерные подпространства. Пусть прямые x_1y_1, x_2y_2, x_3y_3 пересекаются в точке c (т. е. пересечение соответствующих двумерных подпространств одномерно). Мы должны показать, что точки z_1, z_2, z_3 лежат на одной прямой. Если точка c лежит на каждой из прямых z_1z_2, z_2z_3, z_3z_1, то доказывать нечего, так что мы предположим, что $c \notin z_2z_3$.

В каждом одномерном подпространстве, отмеченном на рис. 3, выберем по ненулевому вектору и обозначим этот вектор той же буквой,

но жирным шрифтом. Так как векторы $\mathbf{x_1}$, $\mathbf{y_1}$ и $\mathbf{c}$ принадлежат одному двумерному подпространству, они линейно зависимы, и мы можем выбрать эти векторы в их одномерных подпространствах так, что $\mathbf{y_1} = \mathbf{x_1} + \mathbf{c}$. Векторы $\mathbf{x_1}, \mathbf{z_2}, \mathbf{z_3}$ линейно независимы (в противном случае точки x_1, z_2, z_3 лежали бы на одной прямой, что легко приводится к противоречию). Поэтому мы можем положить $\mathbf{y_1} = \alpha_1\mathbf{x_1} + \alpha_2\mathbf{z_2} + \alpha_3\mathbf{z_3}$, где $\alpha_1, \alpha_2, \alpha_3 \in F$. Рассмотрим невырожденный линейный оператор φ на V, задаваемый условиями $\varphi(\mathbf{x_1}) = \mathbf{y_1}$, $\varphi(\mathbf{z_2}) = \mathbf{z_2}$, $\varphi(\mathbf{z_3}) = \mathbf{z_3}$. Тогда $\varphi(\mathbf{c}) = \varphi(\mathbf{y_1}-\mathbf{x_1}) = (\alpha_1-\mathbf{1})\mathbf{y_1}+\alpha_2\mathbf{z_2}+\alpha_3\mathbf{z_3} = (\alpha_1-\mathbf{1})\mathbf{y_1}+\mathbf{y_1}-\alpha_1\mathbf{x_1} = \alpha_1\mathbf{c}$.

Так как оператор φ линеен и невырожден, он отображает одномерные подпространства в одномерные и двумерные в двумерные. В частности, $\varphi(x_1) = y_1$, $\varphi(z_2) = z_2$, $\varphi(z_3) = z_3$ и $\varphi(c) = c$. Векторы $\mathbf{z_2}, \mathbf{z_3}$ образуют базис прямой z_2z_3 (как двумерного подпространства), так что оператор φ тождественнен на этой прямой. Если L — любая прямая, проходящая через c, то, так как φ оставляет на месте c и точку пересечения L с прямой z_2z_3, мы получаем, что $\varphi(L) = L$ (что вовсе не означает, что φ тождественнен на L).

Так как точка x_2 лежит на прямых cx_2 и x_1z_3, $\varphi(x_2)$ — это точка пересечения прямых cx_2 и y_1z_3, т. е. $\varphi(x_2) = y_2$. Аналогично, $\varphi(x_3) = y_3$. Следовательно, $\varphi(x_2x_3) = y_2y_3$. Пусть z — точка пересечения прямых x_2x_3 и z_2z_3. Тогда $\varphi(z)$ лежит на прямой y_2y_3 и в то же время $\varphi(z) = z$. Следовательно, $z = z_1$ и точка z_1 лежит на прямой z_2z_3, что и требовалось доказать.

§5. Дезарговы плоскости

Приведенное доказательство теоремы Дезарга для проективной плоскости $PG(2, F)$ существенным образом использует тот факт, что координатное кольцо F этой плоскости является полем. Как мы увидим далее, для других проективных плоскостей теорема Дезарга не выполняется.

Определение 5.1. Проективная плоскость, в которой выполняется Теорема Дезарга, называется *дезарговой*.

Мы употребляем термин «теорема» по отношению к теореме Дезарга в этом определении, только отдавая дань традиции. По существу, дезаргова проективная плоскость — это проективная плоскость, удовлетворяющая дополнительной аксиоме

D. Два треугольника центрально перспективны в том и только в том случае, если они аксиально перспективны.

Перефразируя Льва Николаевича Толстого, *все дезарговы плоскости похожи друг на друга, каждая недезаргова плоскость недезаргова по-своему.* Следующая теорема подтверждает первую часть этого тезиса.

Теорема 5.2. Любое координатное кольцо конечной дезарговой проективной плоскости является полем.

Пусть F — координатное кольцо конечной дезарговой проективной плоскости $\Pi = (P, \mathcal{L})$. Мы должны проверить, что операции сложения и умножения, заданные формулами (6), удовлетворяют аксиомам поля. Справедливость нескольких аксиом установлена теоремой 3.1, так что остаются следующие аксиомы: (F1) $a+b = b+a$, (F2) $(a+b)+c = a+(b+c)$, (F3) $(ab)c = a(bc)$, (F4) $(a+b)c = ac+bc$, (F5) $a(b+c) = ab+ac$, (F6) $ab = ba$. При доказательстве свойств (F1)–(F5) мы многократно используем теорему Дезарга. Каждый раз мы выбираем три прямые L_1, L_2, L_3, проходящие через одну и ту же точку, называемую *полюсом*. Кроме того, мы выбираем точки $x_1, y_1 \in L_1$, $x_1 \neq y_1$, точки $x_2, y_2 \in L_2$, $x_2 \neq y_2$, и точки $x_3, y_3 \in L_3$, $x_3 \neq y_3$. Прямые x_1x_2 и y_1y_2 пересекаются в точке z_3, прямые x_2x_3 и y_2y_3 пересекаются в точке z_1, прямые x_3x_1 и y_3y_1 пересекаются в точке z_2. Применяя теорему Дезарга, мы получаем, что точки z_1, z_2, z_3 лежат на одной прямой, называемой *осью*.

В ходе доказательства мы будем называть прямые L_1 и L_2 *параллельными*, $L_1 \parallel L_2$, если эти прямые пересекают идеальную прямую $[\infty]$ в одной и той же точке. Отметим также, что основные идеи доказательства позаимствованы из книги [3] (в которой, между прочим, речь идет не о конечных плоскостях).

Коммутативность сложения.

Лемма 5.3. Для любых $a, b \in F^*$, прямые $(a,0)(0,a)$ и $(b,0)(0,b)$ параллельны.

Доказательство. Пусть $L_1 = [0,0]$, $L_2 = [1,0]$, $L_3 = [0]$ с полюсом $(0,0)$. Пусть $x_1 = (a,0)$, $y_1 = (b,0)$, $x_2 = (a,a)$, $y_2 = (b,b)$, $x_3 = (0,a)$, $y_3 = (0,b)$ (рис. 4). Тогда $x_1x_2 = [a]$, $y_1y_2 = [b]$, так что $z_3 = (\infty)$; $x_2x_3 = = [0,a]$, $y_2y_3 = [0,b]$, так что $z_1 = (0)$. Следовательно, ось — это прямая $(0)(\infty) = [\infty]$ и точка пересечения прямых x_3x_1 и y_3y_1 лежит на этой прямой, что и требовалось доказать.

Мы обозначим (-1) общую идеальную точку всех прямых $(a,0)(0,a)$, $a \in F^*$.

Лемма 5.4. Точка (x,y) лежит на прямой $[-1,c]$ в том и только в том случае, если $x + y = c$.

Доказательство. Прямая $[-1,c]$ проходит через точки (-1) и $(0,c)$. В силу леммы 5.3 она проходит также через точку $(c,0)$.

Пусть $(x,y) \in [-1,c]$, $x \neq 0$, $y \neq 0$, $x \neq c$, $y \neq c$. Пусть $L_1 = [0]$, $L_2 = [-1,c]$, $L_3 = [0,c]$ с полюсом $(0,c)$. Пусть $x_1 = (0,0)$, $y_1 = (0,y)$, $x_2 = (c,0)$, $y_2 = (x,y)$, $x_3 = (c,c)$, $y_3 = (x,c)$ (рис. 5). Тогда $x_1x_2 = [0,0]$,

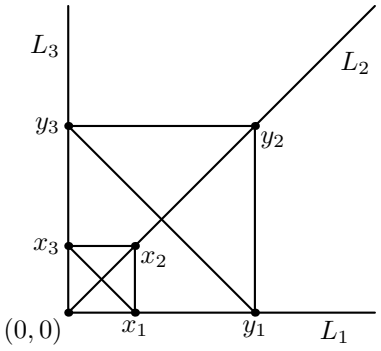

Рис. 4.

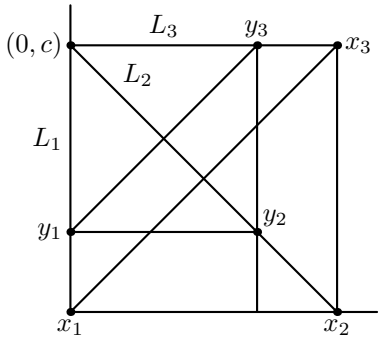

Рис. 5.

$y_1y_2 = [0, y]$, так что $z_3 = (0)$; $x_2x_3 = [c]$, $y_2y_3 = [x]$, так что $z_1 = (\infty)$. Следовательно, ось — это прямая $[\infty]$, и точка пересечения прямых $x_3x_1 = [1, 0]$ и y_3y_1 лежит на оси. Так как (1) — идеальная точка на прямой x_3x_1, то (1) лежит и на прямой y_3y_1, а так как $y_1 = (0, y)$, мы получаем, что $y_3y_1 = [1, y]$.

Следовательно, $y_3 \in [1, y]$, т. е. $y_3 = (x, c)$ — это точка пересечения прямых $[x]$ и $[1, y]$. По определению сложения $x + y = c$.

Так как для каждого $x \in F$ уравнение $x + y = c$ имеет решение (теорема 3.1), то точки (x, z), где $x + z \neq c$, не лежат на прямой $[1, c]$.

Мы готовы доказать коммутативность сложения, применив еще раз теорему Дезарга. Пусть $a \neq 0$, $b \neq 0$. Пусть $L_1 = [a]$, $L_2 = [1, 0]$, $L_3 = [0, a]$ с полюсом (a, a). Пусть $x_1 = (a, 0)$, $y_1 = (a, b)$; $x_2 = (0, 0)$, $y_2 = (b, b)$; $x_3 = (0, a)$, $y_3 = (b, a)$ (рис. 6). Тогда $x_1x_2 = [0, 0]$, $y_1y_2 = [0, b]$, так что $z_3 = (0)$; $x_2x_3 = [0]$, $y_2y_3 = [b]$, так что $z_1 = (\infty)$. Опять идеальная прямая $[\infty]$ оказывается осью. В силу леммы 5.3 прямая x_1x_3 пересекает ось в

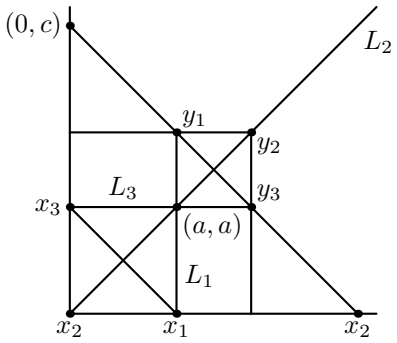

Рис. 6.

точке (-1), так что прямая y_1y_3 проходит через (-1). Пусть эта прямая пересекает ось оординат в точке $(0, c)$. Из леммы 5.4 следует, что $a+b=c$ и $b+a=c$, т. е. $a+b=b+a$.

Лемма 5.5. Пусть $a, b \in F^*$.

(а) Все прямые $(a+t, 0)(t, b)$, где $t \in F$, параллельны друг другу.

(б) Все прямые $(0, a+t)(b, t)$, где $t \in F$, параллельны друг другу.

Доказательство. (а) Мы докажем, что все такие прямые параллельны прямой $(a, 0)(0, b)$. Предположим сначала, что $a = b$. В силу леммы 5.4 прямая $(a+t, 0)(t, a)$ совпадает с прямой $[-1, a+t]$ и потому (лемма 5.3) параллельна прямой $(a, 0)(0, a)$.

Пусть $a \neq b$ и $t \neq 0$. Положим $L_1 = [0, 0]$, $L_2 = [0, a]$, $L_3 = [0, b]$ (с полюсом (0)), $x_1 = (a, 0)$, $y_1 = (a+t, 0)$, $x_2 = (0, a)$, $y_2 = (t, a)$, $x_3 = (0, b)$, $y_3 = (t, b)$ (рис. 7). Прямые x_1x_2 и y_1y_2 пересекаются в точке (-1) (леммы 5.3 и 5.4), прямые x_2x_3 и y_2y_3 пересекаются в точке (∞), так что прямые x_1x_3 и y_1y_3 должны пересечься в точке, лежащей на идеальной прямой $[\infty]$, что и требовалось доказать.

Утверждение (б) доказывается аналогично.

Ассоциативность сложения. Пусть $a, b, c \in F^*$. Пусть $d \in F^*$. Рассмотрим точки $x_1 = (b, 0)$, $y_1 = (b+c, 0)$, $x_2 = (0, d)$, $y_2 = (c, d)$, $x_4 = (a+b, 0)$, $y_4 = ((a+b)+c, 0)$, $x_5 = (b, d)$, $y_5 = (b+c, d)$. Пусть x_3 — точка пересечения прямых x_1x_5 и x_2x_4, а y_3 — точка пересечения прямых y_1y_5 и y_2y_4 (рис. 8). Из леммы 5.5 следует, что $x_1x_2 \parallel y_1y_2$ и $x_2x_4 \parallel y_2y_4$. Кроме того, $x_1x_5 \parallel y_1y_5$. Следовательно, треугольники $x_1x_2x_3$, $y_1y_2y_3$ аксиально перспективны.

Так как прямые x_1y_1, x_2y_2 проходят через (0), через эту же точку (теорема Дезарга) проходит прямая x_3y_3. Следовательно, тругольники $x_3x_4x_5$,

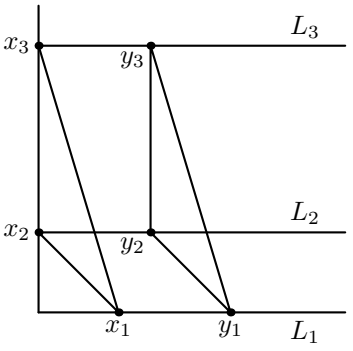

Рис. 7.

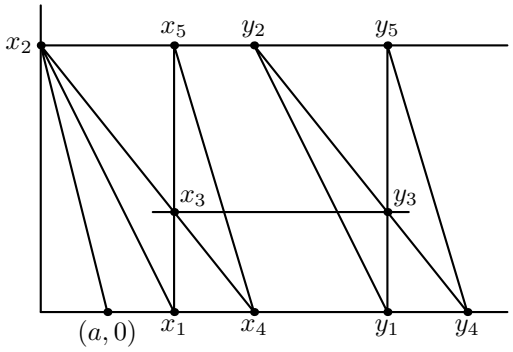

Рис. 8.

$y_3y_4y_5$ центрально перспективны. Так $x_3x_4 \parallel y_3y_4$ и $x_3x_5 \parallel y_3y_5$, то по теореме Дезарга $x_4x_5 \parallel y_4y_5$.

Из леммы 5.5 следует, что $x_4x_5 \parallel (a,0)(0,d)$. Следовательно, $y_4y_5 \parallel (a,0)(0,d)$. С другой стороны, $((b+c)+a,0)y_5 \parallel (a,0)(0,d)$ (лемма 5.5). Следовательно, $y_4 = ((b+c)+a,0)$, т. е. $((a+b)+c,0) = ((b+c)+a,0) = (a+(b+c),0)$, так что $(a+b)+c = a+(b+c)$.

Прежде чем перейти к свойствам умножения, мы получим более наглядное представление произведения.

Лемма 5.6. Для любых $a, b \in F^*$ прямые $(1,0)(0,b)$ и $(a,0)(0,ab)$ параллельны.

Доказательство. Если $a = 1$, утверждение леммы очевидно; если $b = 1$, см. лемму 5.3. Пусть $a \neq 1$, $b \neq 1$. Рассмотрим прямые $L_1 = [0]$, $L_2 = [b,0]$, $L_3 = [0,0]$ с полюсом $(0,0)$. Пусть $x_1 = (0,b)$, $y_1 = (0,ab)$, $x_2 = (1,b)$, $y_2 = (a,ab)$, $x_3 = (1,0)$, $y_3 = (a,0)$ (рис. 9). Так как $x_1x_2 \parallel y_1y_2$ и $x_2x_3 \parallel y_2y_3$, то по теореме Дезарга $x_1x_3 \parallel y_1y_3$.

Ассоциативность умножения.

При доказательстве формулы $(ab)c = a(bc)$ мы можем предположить, что a, b, c не равны ни 0, ни 1. Пусть $x_1 = (b,0)$, $y_1 = (ab,0)$, $x_2 = (0,b)$, $y_2 = (0,ab)$, $x_4 = (1,0)$, $y_4 = (a,0)$, $x_5 = (0,bc)$, $y_5 = (0,(ab)c)$. Пусть x_3 — точка пересечения прямых x_1x_5 и x_2x_4, y_3 — точка пересечения прямых y_1y_5 и y_2y_4 (рис. 10).

Из леммы 5.3 следует, что $x_1x_2 \parallel y_1y_2$, а из леммы 5.6 следует, что $x_4x_2 \parallel y_4y_2$, $x_1x_5 \parallel y_1y_5$. Следовательно, треугольники $x_1x_2x_3$ и $y_1y_2y_3$ аксиально перспективны. По теореме Дезарга прямые x_1y_1, x_2y_2 и x_3y_3 пересекаются в одной точке. Поэтому треугольники $x_3x_4x_5$ и $y_3y_4y_5$ центрально перспективны. Применяя еще раз теорему Дезарга, мы получим,

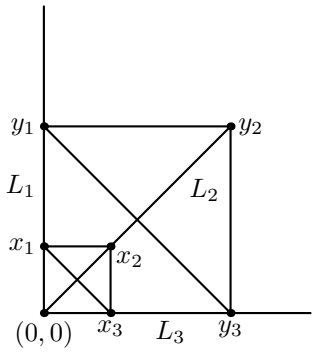

Рис. 9.

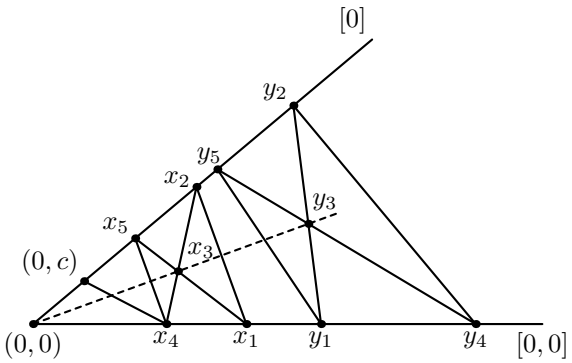

Рис. 10.

что $x_4x_5 \parallel y_4y_5$. Теперь из леммы 5.6 следует, что $y_5 = (0, a(bc))$, так что $(ab)c = a(bc)$.

Правая дистрибутивность: $(a+b)c = ac + bc$.

Мы можем предположить, что $a, b, c \in F^*$. Рассмотрим прямые $(1,0)(0,c)$, $(a,0)(0,ac)$, $(b,0)(0,bc)$ (рис. 11). В силу леммы 5.6 эти прямые параллельны. Проведем параллельную им прямую через точку (b, ac). Пусть эта прямая пересекает оси координат в точках $(x,0)$ и $(0,y)$. Применим лемму 5.5 дважды:

$$(a+b,0)(b,ac) \parallel (a,0)(0,ac), \quad (0,bc+ac)(b,ac) \parallel (0,bc)(b,0).$$

Первая из этих параллельностей означает, что $x = a+b$, вторая означает, что $y = bc+ac = ac+bc$. Следовательно, $(a+b,0)(0,ac+bc) \parallel (1,0)(0,c)$ и поэтому $ac + bc = (a+b)c$ (лемма 5.6).

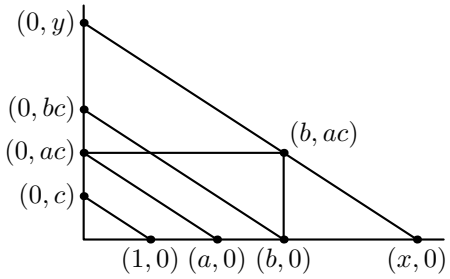

Рис. 11.

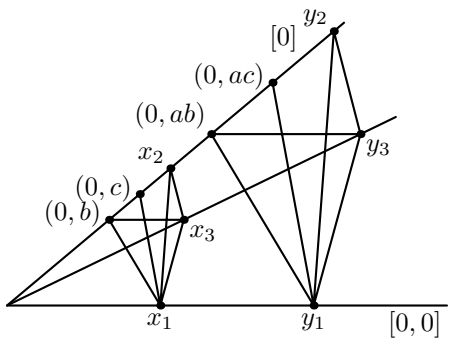

Рис. 12.

Левая дистрибутивность: $a(b+c) = ab + ac$.

Мы предположим, что $a, b, c \in F^*$ и $a \neq 1$. Рассмотрим точки x_1Q $Q = (1,0)$, $y_1 = (a,0)$, $x_2 = (0, b+c)$, $y_2 = (0, a(b+c))$, $x_3 = (1,b)$, $y_3 = (a, ab)$ (рис. 12). Прямые $x_1y_1 = [0,0]$ и $x_2y_2 = [0]$ проходят через точку $(0,0)$. По определению умножения $(1,b) = (1, 1 \cdot b) \in [b,0]$ и $(a,ab) \in [b,0]$, так что прямая x_3y_3 тоже проходит через $(0,0)$. Так как $x_1x_2 \parallel y_1y_2$ (лемма 5.6) и $x_3x_1 \parallel y_3y_1$, то из теоремы Дезарга следует, что $x_3x_2 \parallel y_3y_2$, т. е. $(1,b)(0,b+c) \parallel (a,ab)(0,a(b+c))$. Применим лемму 5.5:

$$(1,b)(0,b+c) \parallel (1,0)(0,c), \quad (a,ab)(0,ab+ac) \parallel (a,0)(0,ac).$$

В силу леммы 5.6 прямые $(a,0)(0,ac)$ и $(1,0)(0,c)$ параллельны, так что мы получаем, что

$$(a,ab)(0,ab+ac) \parallel (1,0)(0,c) \parallel (1,b)(0,b+c) \parallel (a,ab)(0,a(b+c)).$$

Следовательно, $a(b+c) = ab + ac$.

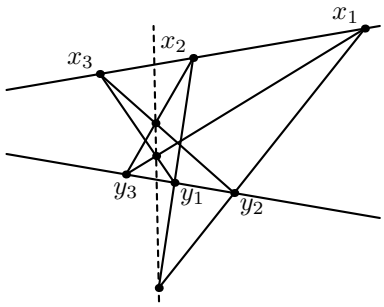

Рис. 13.

Коммутативность умножения.

Заметим, что при выводе аксиом поля мы до сих пор не пользовались конечностью данной проективной плоскости. Коммутативность умножения мы теперь получаем «даром» благодаря знаменитой теореме Веддерберна, которая утверждает, что в конечном случае коммутативность умножения является следствием остальных аксиом поля.

В бесконечном случае теорема Дезарга недостаточна для вывода коммутативности умножения — вместо нее требуется более сильная

Теорема Паппа. Если точки x_1, x_2, x_3 проективной плоскости лежат на одной прямой, точки y_1, y_2, y_3 лежат на другой прямой и все шесть точек отличны от точки пересечения этих прямых, то точки пересечения прямых x_1y_2 и y_1x_2, прямых x_2y_3 и y_2x_3, прямых x_3y_1 и y_3x_1 лежат на одной прямой (рис. 13).

Однако, рассмотрение бесконечных проективных плоскостей не входит в нашу задачу, и мы перейдем к конечным недезарговым плоскостям.

§6. Недезарговы плоскости

Чтобы определить, насколько недезарговой может быть недезаргова проективная плоскость, мы вернемся к доказательству теоремы Дезарга для плоскостей $PG(2, F)$. Большая часть приведенного рассуждения (за исключением последнего абзаца) состояла в доказательстве следующего утверждения:

> если даны точка c и прямая A, то для любых точек x, y, лежащих на одной прямой с точкой c, отличных от c и не лежащих на A, существует биективное отображение множества всех точек плоскости в себя, которое (1) переводит каждую прямую в прямую, (2) переводит в себя все точки прямой A и все прямые, проходящие через c, и (3) переводит точку x в точку y.

Определение 6.1. Пусть $\Pi = (P, \mathcal{L})$ — проективная плоскость. Биективное отображение $f\colon P \to P$ называется *коллинеацией* плоскости Π, если для любой прямой L множество $f(L) = \{f(x)\colon x \in L\}$ является прямой (точнее, множеством всех точек, лежащих на некоторой прямой).

Пусть c — точка, A — прямая в плоскости Π. Коллинеация f называется (c, A)-*коллинеацией*, если $f(L) = L$ для любой прямой L, проходящей через c, и $f(x) = x$ для любой точки x, лежащей на A. Точка c называется *центром* (или *полюсом*), а прямая A — *осью* коллинеации f. Если $c \notin A$, то (c, A)-коллинеация называется (c, A)-*гомологией*. Если $c \in A$, то (c, A)-коллинеация называется (c, A)-*элацией*.

Пусть f — (c, A)-коллинеация проективной плоскости Π. Предположим, нам известен образ $y = f(x)$ некоторой точки x, отличной от c и не лежащей на A. Пусть u — любая точка, не лежащая на A и не лежащая на прямой cx (рис. 14). Чтобы найти $v = f(u)$, мы построим точку пересечения прямых ux и A. Прямая, проходящая через эту точку и точку y, должна пересечь прямую cu в точке v. Поскольку теперь мы знаем образ точки u, мы можем применить аналогичное построение для нахождения образа любой точки прямой cx.

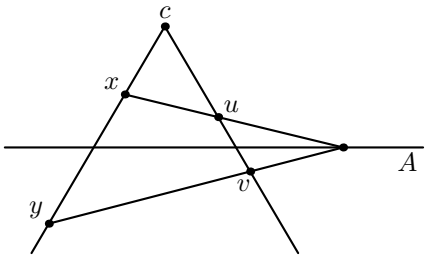

Рис. 14.

Таким образом, (c, A)-коллинеация однозначно определяется образом одной точки (отличной от c и не лежащей на A).

Определение 6.2. Пусть $\Pi = (P, \mathcal{L})$ — проективная плоскость, $c \in P$, $A \in \mathcal{L}$. Плоскость Π называется (c, A)-*транзитивной*, если для любых точек x, y, лежащих на одной прямой с точкой c, отличных от c и не лежащих на A, существует (c, A)-коллинеация f такая, что $f(x) = y$.

Пусть $\Pi = (P, \mathcal{L})$ — конечная проективная плоскость порядка n, $c \in P$, $A \in \mathcal{L}$. Нетрудно видеть, что все (c, A)-коллинеации плоскости Π образуют группу (относительно композиции отображений). Поскольку (c, A)-коллинеация однозначно определяется образом одной точки, отличной от c и не лежащей на A, и число таких точек равно n или $n - 1$, в зависимости от того, лежит ли c на A, мы получаем следующее утверждение.

Теорема 6.3. Пусть $\Pi = (P, \mathcal{L})$ — конечная проективная плоскость порядка n, $c \in P$, $A \in \mathcal{L}$. Плоскость Π является (c, A)-транзитивной в том и только в том случае, если порядок группы всех (c, A)-коллинеаций равен $n-1$ (если $c \notin A$) или n (если $c \in A$).

Таким образом, доказательство теоремы Дезарга, приведенное в §4, показывает, что проективная плоскость над полем (c, A)-транзитивна для любой точки c и любой прямой A. Это и другие соображения привели Ленца и Барлотти в 50-х годах прошлого века к идее классифицировать проективные плоскости согласно структуре множества $T(\Pi)$ всех пар (c, A), для которых плоскость Π является (c, A)-транзитивной. Множество $T(\Pi)$ подчиняетсся ряду ограничений. Для примера приведем без доказательства следующий результат.

Теорема 6.4. Если $(c, A), (d, A) \in T(\Pi)$, где $c \neq d$, то $(a, A) \in T(\Pi)$ для любой точки a на прямой cd.

В настоящее время *классификация Ленца – Барлотти* для конечных проективных плоскостей насчитывает 15 классов. Два крайних класса — дезарговы плоскости, для которых $T(\Pi)$ состоит из всех пар (c, A), и *антидезарговы плоскости*, для которых $T(\Pi) = \varnothing$.

§7. Антидезаргова плоскость

Можно доказать, что все проективные плоскости порядка 2, 3, 4, 5, 7, и 8 — дезарговы. Не существует проективной плоскости порядка 6 (см. §8). Поскольку существует почтиполе F порядка 9, не являющееся полем (см. §2), равенства (1)–(5) определяют недезаргову плоскость порядка 9 над F. (Если бы эта плоскость была дезарговой, то F было бы полем.) Можно показать, однако, что эта плоскость не антидезаргова. В этом параграфе мы используем то же самое почтиполе F для построения антидезарговой проективной плоскости порядка 9.

Почтиполе F состоит из 9 элементов: $0, \pm 1, \pm i, \pm j, \pm k$, которые перемножаются как кватернионы. По сложению F — абелева группа. Всю таблицу сложения для F можно вывести из следующих правил: (1) $a + a = -a$ для всех $a \in F$; (2) $i - j = j - k = k - i = 1$. Например, $i + j = i - j + j + j = 1 - j = -k$. Ядро K почтиполя F состоит из элементов $0, 1, -1$.

Пусть V — множество всех ненулевых 3×1 матриц $A = \begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix}$, где $a_1, a_2, a_3 \in F$, так что $|V| = 9^3 - 1 = 728$. Матрицы A и At, где $t \in F$, $t \neq 0$, назовем эквивалентными. Тогда множество V разбивается на $728/8 = 91$ класс эквивалентности. Каждый класс мы назовем точкой будущей проективной плоскости $\Pi = (P, \mathcal{L})$, так что $|P| = 91 = 9^2 + 9 + 1$. Мы будем обозначать через $\langle A \rangle$ точку, содержащую $A \in V$. Если M —

невырожденная 3×3 матрица над F, то $MA \in V$ для любой матрицы $A \in V$ и, более того, из $\langle A\rangle = \langle B\rangle$ следует $\langle MA\rangle = \langle MB\rangle$. (При проверке последнего факта потребуется как раз тот дистрибутивный закон, который выполняется в F.) Поэтому мы можем считать, что матрица M действует на множестве P.

Выберем невырожденную 3×3 матрицу M над полем K, обладающую следующим свойством: M^{13} — диагональная матрица и ни одна из матриц M^s, где $1 \leqslant s \leqslant 12$, не является диагональной. Примером такой матрицы может служить $M = \left[\begin{smallmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 1 & 0 & 1 \end{smallmatrix}\right]$.

Для каждого $x \in F$, обозначим через $L(x)$ множество всех точек $\langle A\rangle \in P$ таких, что произведение 1×3 матрицы $[1\ x\ 1]$ и 3×1 матрицы A равно 0. Нетрудно подсчитать, что для $x \neq 0$ имеется 80 ненулевых матриц A, удовлетворяющих этому условию, и они образуют 10 классов эквивалентности. Следовательно, $|L(x)| = 10$. Теперь для $x = 1$ и для каждого $x \in F\setminus K$ определим 13 прямых $L_s(x)$, где $0 \leqslant s \leqslant 12$, следующим образом: $L_s(x) = \{M^s a\colon a \in L(x)\}$. Обозначим через $\mathcal{L}$ множество всех таких прямых. Тогда $|\mathcal{L}| = 7 \cdot 13 = 91$. Мы опустим проверку того, что $\Pi = (P, \mathcal{L})$ — проективная плоскость.

Назовем точку $a \in P$ *ближней*, если $a = \langle A\rangle$, где все элементы матрицы A принадлежат полю K. Все точки, не являющиеся ближними, мы назовем *дальними*. Можно проверить, что каждая прямая содержит либо четыре, либо одну ближнюю точку. Соответственно мы назовем прямую либо *ближней*, либо *дальней*. Дальнейший анализ плоскости Π показывает, что каждая ближняя точка лежит на четырех ближних прямых, а каждая дальняя точка лежит на одной ближней прямой. Отсюда следует, что ближние точки и ближние прямые образуют проективную плоскость порядка 3. Наконец, преодолев определенные технические трудности, можно показать, что никакая коллинеация плоскости Π не переводит ближнюю точку в дальнюю.

Теорема 7.1. Проективная плоскость Π антидезаргова.

Доказательство. Пусть $c \in P$ и $A \in \mathcal{L}$. В силу сделанного выше замечания о коллинеациях плоскости Π достаточно показать, что существует прямая L, проходящая через c, и две точки на L, отличные от c и не лежащие на A, одна из которых — ближняя, а другая — дальняя. Если c — дальняя точка, то в качестве L возьмем любую дальнюю прямую, проходящую через c и отличную от A. Если c — ближняя точка, то L — любая ближняя прямая, проходящая через c и отличная от A.

Аналогичное построение можно провести, если F — любое почтиполе порядка q^2, описанное в §2. Показатель степени 13 в описании матрицы M нужно заменить на $q^2 + q + 1$. Построенные таким образом антидезарговы

проективные плоскости называются *плоскостями Хьюза*. Построение и свойства плоскостей Хьюза можно най ти в книгах [2] и [4]. Антидезаргова и три других проективных плоскости порядка 9 детально проанализированы в элементарно написанной книге [7].

§8. Три гипотезы

Порядок любой известной конечной проективной плоскости является простым числом или степенью простого числа. Однако, единственное известное универсальное ограничение на порядок представлено следующей теоремой, доказанной в 1949 году.

Теорема Брака – Райзера. Пусть $n \equiv 1$ или $2 \pmod 4$. Если существует проективная плоскость порядка n, то n может быть представлено в виде суммы квадратов двух целых чисел.

Таким образом, не существует проективных плоскостей порядка 6, 14, 21, 22, 30 и многих других порядков. Первый случай, не покрытый этой теоремой, — $n = 10$. Огромный компьютерный поиск, завершенный в 1991 году, убедил специалистов, что проективной плоскости порядка 10 не существует (см. [6]).

Следующий порядок, не покрытый теоремой Брака – Райзера, — $n = 12$. К настоящему времени известно, что если проективная плоскость порядка 12 существует, то она должна быть антидезарговой.

Вопрос о возможном порядке проективной плоскости тесно связан с с *взаимно ортогональными латинскими квадратами*. Латинский квадрат порядка n — это квадратная матрица порядка n, в каждом столбце и каждой строке которой встречаются все натуральные числа от 1 до n. Два латинских квадрата $A = [a_{ij}]$ и $B = [b_{ij}]$ одного и того же порядка n называются ортогональными, если для любой упорядоченной пары (k, l) натуральных чисел, не превосходящих n, можно найти индексы i и j такие, что $a_{ij} = k$, $b_{ij} = l$. Например, следующие три латинских квадрата порядка 4 взаимно ортогональны:

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{bmatrix}$$

Теоема 8.1. Проективная плоскость порядка n существует в том и только в том случае, если существуют $n - 1$ взаимно ортогональных латинских квадратов порядка n.

Интересно, что хотя невозможность проективной плоскости порядка 10 эквивалентна отсутствию девяти попарно ортогональных латинских

квадратов порядка 10, никто пока не сумел найти даже трех таких квадратов (два ортогональных латинских квадрата порядка 10 существуют).

Несмотря на значительные усилия, следующие две гипотезы остаются открытыми.

Гипотеза 1. Порядок любой конечной проективной плоскости — простое число или степень простого числа.

Гипотеза 2. Все проективные плоскости простого порядка дезарговы.

Один из возможных подходов к доказательству (или опровержению) этих гипотез — проанализировать их в применении к каждому из 15 классов Ленца – Барлотти (см. §7). Чем больше множество $T(\Pi)$ (множество всех пар (c, A), для которых плоскость Π (c, A)-транзитивна), тем богаче алгебраическая структура координатного кольца плоскости Π и тем больше шансов, что анализ этой структуры даст необходимую информацию о порядке плоскости. Пять из 15 классов Ленца – Барлотти, возможно, являются пустыми (хотя в каждом из них есть бесконечные плоскости).

Класс I.2. $T(\Pi)$ состоит из единственной пары (c, A), где $c \notin A$.

Класс I.3. $T(\Pi)$ состоит из двух пар, (a, A) и (b, B), где $a \in B$, $a \notin A$, $b \in A$, $b \notin B$.

Класс I.4. $T(\Pi)$ состоит из трех пар, образованных вершинами и противоположными сторонами треугольника.

Класс II.2. $T(\Pi)$ состоит из двух пар, (c, A) и (b, B), где $b \in A$, $b \notin B$, c — точка пересечения прямых A и B.

Класс III.1. $T(\Pi)$ состоит из всех пар (x, cx), где x — произвольная точка фиксированной прямой L, а c — фиксированная точка, не лежащая на L.

Гипотеза 3. Перечисленные выше классы Ленца – Барлотти не содержат конечных проективных плоскостей.

§9. H-матрицы

В четырех из пяти перечисленных выше классов Ленца – Барлотти плоскость Π (c, A)-транзитивна, где $c \notin A$, т. е. Π допускает группу (c, A)-гомологий порядка $n - 1$, где n — порядок Π. В этом случае свойства плоскости Π тесно связаны со свойствами определенной матрицы, к описанию которой мы переходим.

Итак, пусть $\Pi = (P, \mathcal{L})$ — проективная плоскость порядка n, содержащая такие прямую и не лежащую на ней точку, что соответствующая группа гомологий H имеет порядок $n-1$. Вспомним, что при координатизации проективной плоскости (см. §3) мы можем выбрать в качестве осей

координат и идеальной прямой любые три прямые, не пересекающиеся в одной точке. Мы предположим, что ось и центр гомологий из группы H — прямая $[0]$ и точка (0). В качестве координатного кольца мы выберем множество $F = H \cup \{0\}$ (мы предполагаем, что H — мультипликативная группа с нейтральным элементом 1). Точку $(1,1)$ мы выберем произвольно и затем найдем точку (1) на идеальной прямой. Так как все коллинеации из группы H являются $((0),[0])$-гомологиями, они преобразуют идеальную прямую в себя (оставляя на месте точки (0) и (∞)). Для каждого $a \in H$ обозначим через (a) точку $a(1)$. После этого координатизация плоскости Π завершается как в §3. Достоинство предложенной координатизации в том, что мы можем описать действие коллинеаций из группы H на всей плоскости Π.

Предложение 9.1. Пусть $a \in H$ и $x, y \in F$. Тогда: (1) $a(\infty) = (\infty)$ и $a[\infty] = [\infty]$; (2) $a(x) = (ax)$ и $a[x,0] = [ax,0]$; (3) $a(x,0) = (xa^{-1},0)$ и $a[x] = [xa^{-1}]$; (4) $a(x,y) = (xa^{-1},y)$ и $a[x,y] = [ax,y]$.

Мы докажем (2) и оставим (1), (3) и (4) читателю. Так как (0) — центр гомологии a, $a(0) = (0) = (a \cdot 0)$; если $x \in H$, то $a(x) = a(x(1)) = (ax)(1) = = (ax)$; так как прямая $[x,0]$ проходит через точку (x) и точку $(0,0)$, лежащую на оси гомологии a, $a[x,0] = [ax,0]$.

Операция умножения в координатном кольце F совпадает с операцией умножения в группе H, т. е. для любых $a, b \in H$, точка (a,ab) является точкой пересечения прямых $[a]$ и $[b,0]$. Для доказательства применим гомологию b^{-1} к точке (a,b) и к обеим прямым: $b^{-1}(a,ab) = (ab,ab)$, $b^{-1}[a] = [ab]$, $b^{-1}[b,0] = [1,0]$. Остается заметить, что (ab,ab) — точка пересечения прямых $[ab]$ и $[1,0]$.

Для индексирования строк и столбцов матрицы порядка n обычно используются числа $1, 2, \ldots, n$. Однако, любое множество из n элементов может быть использовано для этой цели и мы рассмотрим матрицу C порядка n над координатным кольцом F, строки и столбцы которой индексированы (в одном и том же порядке) элементами множества F. При этом удобно считать, что первая строка и первый столбец индексируются нулем. Для любых $x, y, z \in F$ положим

$$C(x,y) = z \text{ в том и только том случае, если } (1,x) \in [z,y].$$

Мы обозначаем через $C(x,y)$ элемент матрицы C, расположенный в строке с индексом x и столбце с индексом y. Поскольку существует единственная прямая через точки $(1,x)$ и $(0,y)$ и эта прямая содержит единственную идеальную точку $(z) \neq (\infty)$, матрица C определена корректно.

Предложение 9.2. Пусть $a, b \in F$, $a \neq b$. Тогда
(1) $C(a,a) = 0$, $C(a,0) = a$ и $C(a,b) \in H$;

(2) каждая строка и каждый столбец матрицы C содержат все элементы множества F по одному разу;

(3) множество $Q(a,b) = \{C(a,x)C(b,x)^{-1}\colon x \in F, x \neq a, x \neq b\}$ совпадает с множеством всех неединичных элементов группы H.

Доказательство. (1) $(1,a) \in [0,a]$, $(1,a) = (1 \cdot a, a) \in [a,0]$ и $(1,a) \notin [0,b]$.

(2) Если $C(x,b) = C(y,b) = z$, то $(1,x), (1,y) \in [z,b]$. Так как, кроме того, $(1,x), (1,y) \in [1]$, мы заключаем, что $x = y$. Если $C(a,x) = C(a,y) = z$, то точка $(1,a)$ лежит на прямых $[z,x]$ и $[z,y]$. Так как эти прямые проходят также через точку (z), то $x = y$. Следовательно, ни один элемент множества F не повторяется ни в строке, ни в столбце матрицы C.

(3) Пусть $x, y \in F$, $x \neq a$, $x \neq b$, $y \neq a$, $y \neq b$, и пусть $x \neq y$. Из предыдущего свойства следует, что $1 \notin Q(a,b)$. Пусть $C(a,x) = s$, $C(b,x) = t$, $C(a,y) = u$, $C(b,y) = v$. Тогда $(1,a)$ — точка пересечения прямых $[s,x]$ и $[u,y]$, $(1,b)$ — точка пересечения прямых $[t,x]$ и $[v,y]$. Предположим, что $st^{-1} = uv^{-1} = z$. Применив гомологию z к точке $(1,b)$, мы получаем, что $z(1,b) = (z^{-1},b)$ — точка пересечения прямых $z[t,x] = [zt,x] = [s,x]$ и $z[v,y] = [zv,y] = [u,y]$, т. е. $(z^{-1},b) = (1,a)$, $b = a$. Полученное противоречие доказывает, что ни один элемент множества F не повторяется в множестве $Q(a,b)$ и потому $Q(a,b) = H \setminus \{1\}$.

Определение 9.3. Пусть H — мультипликативная группа порядка $n-1$ и пусть $F = H \cup \{0\}$. Матрица C порядка n, строки и столбцы которой индексированы множеством F называется H-матрицей, если она обладает свойствами (1)–(3) предложения 9.2.

Пример. Пусть $G = \{1, a, a^2, a^3\}$ — циклическая группа порядка 4, а $H = \{1, b, b^2\}$ — циклическая группа порядка 3. Тогда M — G-матрица, N — H-матрица.

$$M = \begin{bmatrix} 0 & a^2 & a^3 & a & 1 \\ 1 & 0 & a^2 & a^3 & a \\ a & 1 & 0 & a^2 & a^3 \\ a^3 & a & 1 & 0 & a^2 \\ a^2 & a^3 & a & 1 & 0 \end{bmatrix} \quad N = \begin{bmatrix} 0 & 1 & b & b^2 \\ 1 & 0 & b^2 & b \\ b & b^2 & 0 & 1 \\ b^2 & b & 1 & 0 \end{bmatrix}$$

Таким образом, начав с проективной плоскости порядка n и группы гомологий H порядка $n-1$, мы получили H-матрицу C. Справедливо и обратное утверждение, доказательство которого мы оставляем читателю.

Предложение 9.4. Пусть H — мультипликативная группа порядка $n-1$. Для любой H-матрицы C существует проективная плоскость порядка

n с координатным кольцом $F = H \cup \{0\}$, для которой H является группой $((0), [0])$-гомологий. При этом выполняются следующие свойства:

(а) умножение ненулевых элементов в F совпадает с умножением в H;

(б) для любых $a, b \in F$,$[a, b] = \{(x, y) \colon C(y, b) = xa\} \cup \{(a)\}$;

(в) сложение в F определятся равенством $C(a + b, b) = a$.

Следующая теорема дает бесконечное множество H-матриц.

Теорема 9.5. Пусть F — поле или почтиполе порядка n. Определим матрицу C порядка n над F со строками и столбцами, индексированными множеством F: $C(x, y) = x - y$.

Тогда C — H-матрица, где $H = F^*$.

Доказательство. Первые два свойства H-матриц очевидны. Проверим свойство (3) из предложения 9.2. Пусть $a, b \in F$, $a \neq b$. Пусть $x \in F$, $x \neq a$, $x \neq b$. Тогда

$$C(x, a)C(x, b)^{-1} = (x - a)(x - b)^{-1} = ((x - b) - (a - b))(x - b)^{-1} = \\ = 1 - (a - b)(x - b)^{-1}.$$

Когда x пробегает все элементы F, кроме a и b, $(x - b)^{-1}$ пробегает все элементы F, кроме $(a-b)^{-1}$ и 0, так что $(a-b)(x-b)^{-1}$ пробегает все элементы F, кроме 1 и 0 и потому $C(x, a)(C(y, b))^{-1}$ пробегает все элементы F, кроме 0 и 1, что и требовалось доказать.

Заметим, что матрица C, описанная в этой теореме, является кососимметрической, если характеристика F не равна 2. В случае характеристики 2 матрица C симметрична. Оказывается, любая H-матрица над абелевой группой H симметрична или кососимметрична. Прежде чем доказать это утверждение, нужно понять, что означает кососимметричность H-матрицы для произвольной группы H. Мы называем матрицу M над полем F кососимметричной, если $M^\top = -M$. Заметим, что -1 — единственный элемент второго порядка в мультипликативной группе поля. Поэтому мы даем следующее определение.

Определение 9.6. Пусть H — конечная группа с единственным элементом π второго порядка. H-матрица C называется *кососимметричной*, если $C^\top = \pi C$.

Теорема 9.7. Пусть H — конечная абелева группа. Если группа H не имеет элементов второго порядка, то любая H-матрица симметрична. Если группа H имеет ровно один элемент второго порядка, то любая H-матрица косоимметрична. Если группа H имеет два или более элементов второго порядка, то H-матриц не существует.

Для доказательства теоремы нам понадобится следующая лемма.

Лемма 9.8. Пусть π — произведение всех элементов конечной абелевой группы H. Если H имеет ровно один элемент второго порядка, то этот элемент равен π. В противном случае $\pi = 1$.

Доказательство. Все элементы группы H, порядок которых равен 1 или 2, образуют подгруппу K. Все элементы множества $H \setminus K$ распадаются на пары $\{x, x^{-1}\}$. Поэтому произведение всех элементов группы H равно произведению всех элементов подгруппы K. Отсюда следует, что $\pi \in K$. Если H не имеет элементов порядка 2, то $K = \{1\}$, и потому $\pi = 1$. Если τ — единственный элемент порядка 2 в H, то $K = \{1, \tau\}$, и потому $\pi = \tau$. Предположим, что H имеет два или более элементов второго порядка и что $\pi \neq 1$. Тогда $|K| \geqslant 3$. Пусть $\tau \in K$, $\tau \neq 1$, $\tau \neq \pi$. Тогда $\{1, \pi, \tau, \pi\tau\}$ — подгруппа группы K. Следовательно, $|K| \equiv 0 \pmod 4$. Все элементы группы K распадаются на пары $\{x, \pi x\}$, причем $x \cdot \pi x = \pi$. Следовательно, произведение всех элементов группы K, т. е. π, равно $\pi^{|K|/2} = 1$, так как $|K|/2$ четно.

Доказательство теоремы 9.7. Пусть $F = H \cup \{0\}$, пусть π — произведение всех элементов группы H и пусть C — H-матрица. Пусть $a, b \in F$, $a \neq b$. Из первых двух свойств H-матриц следует, что

$$\prod_{x \in F, x \neq a, x \neq b} C(a, x) = \pi(C(a, b))^{-1}, \qquad \prod_{x \in F, x \neq a, x \neq b} C(b, x) = \pi(C(b, a))^{-1}.$$

Из третьего свойства H-матриц теперь следует, что

$$\pi(C(a, b))^{-1}(\pi(C(b, a))^{-1})^{-1} = \pi$$

и потому $C(b, a) = \pi C(a, b)$.

Если группа H не имеет элементов второго порядка, то $\pi = 1$, так что матрица C симметрична. Если H имеет ровно один элемент второго порядка, то матрица C кососимметрична.

Предположим, что H имеет два или более элементов второго порядка. Тогда $\pi = 1$, так что матрица C должна быть симметричной. Следовательно, матрица C имеет выше диагонали и ниже диагонали одно и то же число элементов, равных 1. Так как на диагонали единиц нет, матрица C содержит четное число единиц. С другой стороны, так как группа H содержит элементы второго порядка, порядок группы H четен, и потому порядок матрицы C нечетен. По определению матрица C содержит по одной единице в каждой строке и, следовательно, общее число единиц в C должно быть нечетным. Полученное противоречие доказывает, что если H содержит два или более элементов второго порядка, то H-матриц не существует.

Теорема 9.7 устанавливает ограничение на возможные абелевы группы (c, A)-гомологий в (c, A)-транзитивной плоскости.

Свойства H-матриц могут быть использованы для изучения классов Ленца – Барлотти I.3, I.4. и II.2. Доказательство следующей теоремы мы опускаем.

Теорема 9.9. Пусть H — группа всех $((0),[0])$-гомологий $((0),[0])$-транзитивной конечной проективной плоскости Π, $F = H \cup \{0\}$, C — соответствующая H-матрица.

(а) Плоскость Π $((0,0),[\infty])$-транзитивна в том и только в том случае, если $C(ax, ay) = aC(x, y)$ для любых $a, x, y \in F$.

(б) Плоскость Π $((\infty),[0,0])$-транзитивна в том и только в том случае, если $C(xa, ya) = C(x, y)a$ для любых $a, x, y \in F$.

(в) Плоскость Π $((0,0),[\infty])$- и $((\infty),[0,0])$-транзитивна в том и только в том случае, если группа H абелева и $(x + y)z = xz + yz$ для любых $x, y, z \in F$.

(г) Плоскость Π $((\infty),[\infty])$-транзитивна в том и только в том случае, если F — группа относительно сложения. Если это условие выполняется, то $C(x + z, y + z) = C(x, y)$ для любых $x, y, z \in F$.

Заметим, что в случае (в) для дезарговости плоскости Π недостает «всего лишь» ассоциативности сложения (при наличии которой коммутативность сложения может быть выведена).

§10. Порядок проективной плоскости

В этом параграфе мы приведем примеры того, как информация о гомологиях проективной плоскости может привести к доказательству гипотезы 1 (см. §8). Существенную роль при этом будут играть H-матрицы.

Теорема 10.1. Пусть Π — проективная плоскость порядка n, которая при надлежащей координатизации $((0),[0])$- и $((\infty),[\infty])$-транзитивна. Пусть H — группа всех $((0),[0])$-гомологий. Если группа H абелева и сложение в координатном кольце $F = H \cup \{0\}$ коммутативно, то n — простое число или степень простого числа.

Доказательство. Пусть C — H-матрица, соответствующая данной координатизации плоскости Π. Пусть K — мультипликативная группа, изоморфная аддитивной группе координатного кольца F. Удобно считать, что строки и столбцы матрицы C индексированы элементами группы K, а не множества F. В частности, первый столбец и первая строка имеют индекс 1. Тогда $C(\alpha, 1) = \alpha$ и, в силу теоремы 9.9(д), $C(\alpha\gamma, \beta\gamma) = C(\alpha, \beta)$ для любых $\alpha, \beta, \gamma \in K$.

Случай 1: n — четное число.

В этом случае группа H порядка $n-1$ не имеет элементов порядка 2, так что матрица C симметрична. Следовательно, для любого $\alpha \in K$

$$C(\alpha, 1) = C(1, \alpha) = C(\alpha^{-1}, \alpha\alpha^{-1}) = C(\alpha^{-1}, 1).$$

Так как никакой столбец матрицы C не содержит двух равных элементов, то $\alpha = \alpha^{-1}$, т. е. $\alpha^2 = 1$. Так как это верно для любого элемента группы K, мы получаем, что $n = |K|$ является степенью числа 2.

Заметим, что коммутативность сложения в F не играла в этом случае никакой роли.

Случай 2: n — нечетное число.

Этот случай значительно сложнее, и нам понадобится понятие *группового кольца.*

Пусть S — коммутативное ассоциативное кольцо с единицей и пусть G — конечная мультипликативная группа. Групповое кольцо SG группы G над кольцом S состоит из формальных линейных комбинаций $\sum_{x\in G} \alpha_x x$, где все коэффициенты α_x принадлежат кольцу S. Сложение и умножение в SG определяются следующим образом:

$$\sum_{x\in G} \alpha_x x + \sum_{x\in G} \beta_x x = \sum_{x\in G} (\alpha_x + \beta_x)x, \quad \sum_{x\in G} \alpha_x x \cdot \sum_{y\in G} \beta_y y = \sum_{z\in G} \left(\sum_{xy=z} \alpha_x \beta_y \right) z.$$

Относительно этих операций SG является ассоциативным кольцом. Мы отождествляем элемент β кольца S с элементом $\sum_{x\in G} \alpha_x x$ кольца SG, где $\alpha_x = \beta$, если $x = 1$, и $\alpha_x = 0$, если $x \neq 1$. Кроме того, мы отождествляем элемент y группы G с элементом $\sum_{x\in G} \alpha_x x$ кольца SG, где $\alpha_x = 1$, если $x = y$, и $\alpha_x = 0$, если $x \neq y$. При таком отождествлении единица кольца S, единица группы G и единица кольца SG — один и тот же элемент, обозначаемый 1.

Вернемся к нашему доказательству. Пусть p — простой делитель числа n. Нам нужно доказать, что n — степень p.

Пусть S — групповое кольцо группы H над полем (и, следовательно, кольцом) классов вычетов по модулю p. Матрица C может рассматриваться как матрица над кольцом S. Так как группа H абелева, кольцо S коммутативно, так что мы можем рассмотреть групповое кольцо SK группы K над кольцом S. Напомним, что строки и столбцы матрицы C индексированы элементами группы K и при этом $C(\alpha\gamma, \beta\gamma) = C(\alpha, \beta)$ для всех $\alpha, \beta, \gamma \in K$. Мы будем называть все матрицы порядка n над кольцом S, обладающие таким свойством K*-инвариантными.* K-инвариантная матрица A полностью определяется своим первым столбцом и потому такая матрица однозначно определяется элементом $\mathrm{supp}(A) = \sum_{\alpha\in K} A(\alpha, 1)\alpha$ кольца SK. Очевидно, $\mathrm{supp}(A+B) = \mathrm{supp}(A) + \mathrm{supp}(B)$. Несколько менее

очевидна формула $\operatorname{supp}(AB) = \operatorname{supp}(A)\operatorname{supp}(B)$:

$$\operatorname{supp}(A)\operatorname{supp}(B) = \sum_{\alpha\in K} A(\alpha,1)\alpha \cdot \sum_{\beta\in K} B(\beta,1)\beta =$$
$$= \sum_{\gamma\in K}\sum_{\alpha\beta=\gamma} A(\alpha,1)B(\beta,1)\gamma = \sum_{\gamma\in K}\sum_{\beta\in K} A(\gamma\beta^{-1},1)B(\beta,1)\gamma =$$
$$= \sum_{\gamma\in K}\sum_{\beta\in K} A(\gamma,\beta)B(\beta,1)\gamma = \sum_{\gamma\in K}(AB)(\gamma,1)\gamma = \operatorname{supp}(AB).$$

Обозначим чрез C^* K-инвариантную матрицу, определяемую равенствами $C^*(\alpha,\beta) = 0$, если $\alpha = \beta$; $C^*(\alpha,\beta) = (C(\beta,\alpha))^{-1}$, если $\alpha \neq \beta$. Кроме того, обозначим через h сумму всех элементов группы H в кольце S, через I — единичную матрицу порядка n и через J — матрицу порядка n, все элементы которой равны 1. Каждый диагональный элемент матрицы CC^* равен сумме $n-1$ единиц, а так как S — кольцо характеристики p, то все диагональные элементы матрицы CC^* равны -1. Каждый внедиагональный элемент матрицы CC^* равен $h-1$. Поэтому

$$CC^* = -I + (h-1)(J-I) = -hI + (h-1)J.$$

Кроме того, $J^2 = nJ = O$, $CJ = JC = C^*J = JC^* = hJ$ и $hC = Ch = hC^* = C^*h = h(J-I)$. Используя эти равенства, нетрудно показать индукцией по m, что для любого натурального числа m

$$C^m(CC^*) = (-1)^{m-1}h(I-(m+2)J).$$

Положив $m = p-1$, мы получаем

$$C^pC^* = h(J-I). \tag{7}$$

В коммутативном кольце SK характеристики p выполняется равенство $(x+y)^p = x^p + y^p$. Поэтому

$$\operatorname{supp}(C^p) = (\operatorname{supp}(C))^p = \sum_{\alpha\in K}(C(\alpha,1))^p\,\alpha^p = \sum_{\alpha\in K,\alpha\neq 1}(C(\alpha,1))^p\alpha^p.$$

Пусть $D = C^pC^*$. Тогда

$$\operatorname{supp}(D) = \sum_{\alpha\in K,\alpha\neq 1}(C(\alpha,1))^p\alpha^p \cdot \sum_{\beta\in K,\beta\neq 1} C^*(\beta,1)\beta = \sum_{\gamma\in K} x_\gamma\gamma,$$

где $x_\gamma = D(\gamma,1)$. Уравнение (7) показывет, что $D(1,1) = 0$. Следовательно,

$$0 = \gamma_1 = \sum_{\beta\neq 1,\alpha^p=\beta^{-1}}(C(\alpha,1))^pC^*(\beta,1).$$

Равенство этой суммы нулю означает, что никакой элемент группы K, кроме 1, не является p-й степенью. Иными словами, $\alpha^p = 1$ для любого

$\alpha \in K$. Но тогда $n = |K|$ — степень простого числа p, что и требовалось доказать.

Список литературы

Наиболее полную информацию о конечных проективных плоскостях и других конечных геометриях можно найти в книгах [2] и [4]. О теоремах Дезарга и Паппа и связанных с ними алгебраических структурах см. [1] и [3]. Книги [1] и [7] особенно хороши для первого знакомства с предметом. H-матрицы детально изучаются в книге [5] (там H-матрица фигурирует как *the core of a normalized generalized conference matrix*).

[1] Артин Э. *Геометрическая алгебра*. М.: Наука, 1969.

[2] Dembowski P. *Finite Geometries*. Springer, 1968.

[3] Гильберт Д. *Основания геометрии*. М.: Гостехиздат, 1948.

[4] Hughes D. R., Piper F. C. *Projective Planes*. Springer, 1982.

[5] Ionin Y. J., Shrikhande M. S. *Combinatorics of Symmetric Designs*. Cambridge University Press, 2006.

[6] Lam C. W. H. *The search for a finite prolective plane of order* 10 // The American Mahematical Monthly, 1991, pp. 305–318.

[7] Room T. G., Kirkpatrick P. B. *Miniquaternion Geometry*. Cambridge University Press, 1971.

Ю. И. Ионин