вию, называются *линейными преобразованиями* (или *линейными отображениями*). При этом множество $f^{-1}[0]$ называется нуль-пространством *) преобразования f; оно всегда является линейным подпространством области определения преобразования (относительно индуцированных в $f^{-1}[0]$ операций сложения и умножения на число).

Предположим, что f — линейное преобразование X в Y и g — линейное преобразование X на Z такие, что нуль-пространство f содержит нуль-пространство g. Тогда существует единственное линейное преобразование h Z в Y, для которого $f=h\circ g$ (а именно, $h(z)$ является единственным элементом множества $f\circ g^{-1}[z]$). (Говорят при этом, что преобразование h *индуцировано* преобразованиями f и g.) Из отмеченного обстоятельства, в частности, следует, что каждое линейное преобразование можно представить как композицию проектирования в фактор-пространство и последующего взаимно однозначного линейного преобразования.

ВЕЩЕСТВЕННЫЕ ЧИСЛА

Этот раздел посвящен доказательству нескольких важнейших результатов, касающихся вещественных чисел.

Упорядоченное поле — это поле F, в котором выделено некоторое подмножество P, называемое множеством *положительных элементов*, такое, что

(а) *если x и y — элементы P, то $x+y$ и xy тоже принадлежат P* и (б) *для любого элемента x из F выполняется в точности одно из следующих трех соотношений*: $x\in P$, $-x\in P$ *или* $x=0$.

Легко проверяется, что отношение $<$, определенное правилом: $x<y$ в том и только в том случае, когда $y-x\in P$, является линейным упорядочением множества F. Справедливы обычные предложения о сложении и умножении неравенств. Элементы x из F, для которых $-x\in P$, называются *отрицательными*.

Будем предполагать, что вещественные числа образуют упорядоченное поле, полное относительно заданного на нем порядка, в том смысле, что каждое его непустое

*) Чаще $f^{-1}(0)$ называют ядром преобразования f.

ограниченное сверху подмножество имеет наименьшую верхнюю грань, или supremum. В силу 0.9 последнее требование эквивалентно условию, что у каждого непустого ограниченного снизу подмножества есть наибольшая нижняя грань, или infimum.

Докажем, прежде всего, несколько предложений о натуральных числах. Множество A вещественных чисел называется *индуктивным*, если $0 \in A$ и, коль скоро $x \in A$, то и $x+1 \in A$. Вещественное число x называется *неотрицательным целым числом* тогда и только тогда, когда оно принадлежит каждому индуктивному множеству. Иными словами, множество ω неотрицательных целых чисел определяется как пересечение всех индуктивных множеств. Каждый элемент из ω действительно неотрицателен, ибо множество всех неотрицательных чисел индуктивно. Очевидно, ω само индуктивно и является подмножеством любого другого индуктивного множества. Отсюда следует (*принцип математической индукции*), что каждое индуктивное подмножество множества ω совпадает с ω. Доказательства, опирающиеся на этот принцип, называются *доказательствами по индукции*. Докажем в качестве примера следующую маленькую теорему: если p и q — неотрицательные целые числа и $p<q$, то $q-p \in \omega$. Заметим сначала, что множество, содержащее 0 и все числа вида $p+1$, где $p \in \omega$, индуктивно; следовательно, каждый ненулевой элемент из ω можно представить в виде $p+1$. Далее, пусть A — множество всех неотрицательных целых чисел p таких, что $q-p \in \omega$ для любого большего элемента q из ω. Ясно, что $0 \in A$. Пусть p — какой-нибудь элемент из A и q — произвольный элемент множества ω, больший $p+1$. Тогда $p<q-1$, и из $p \in A$ и $q-1 \in \omega$ следует, что $q-1-p \in \omega$. Следовательно, $p+1 \in A$, т. е. A — индуктивное множество. Значит, $A=\omega$. Так же легко показать, что сумма любых двух элементов множества ω принадлежит ω. А из этих двух утверждений следует, что множество $\{x : x \in \omega$ *или* $-x \in \omega\}$ является группой. Это — *группа целых чисел.*

Часто бывает удобна другая форма принципа математической индукции: *в каждом непустом подмножестве A множества ω есть наименьший элемент.* Для

доказательства этого утверждения рассмотрим множество B всех элементов множества ω, являющихся нижними гранями множества A; таким образом, $B=\{p : p \in \omega$ *и* $p \leqslant q$ *для всех* q *из* $A\}$. Множество B не индуктивно, ибо если $q \in A$, то $q+1 \notin B$. Из $0 \in B$ следует, что в B существует элемент p, для которого $p+1 \notin B$. Если $p \in A$, то ясно, что p является наименьшим элементом множества A. Если же $p \notin A$, то в A найдется элемент q такой, что $p<q<p+1$. Но тогда $q-p$ — ненулевой элемент множества ω и, значит, $q-p-1$ — отрицательный элемент, принадлежащий ω, что невозможно.

Можно *определять функцию по индукции* в следующем смысле. Для каждого неотрицательного целого числа p положим $\omega_p=\{q : q \in \omega$ *и* $q \leqslant p\}$. Предположим, что мы хотим определить на всем множестве ω некоторую функцию, значение a которой в нуле уже задано, и пусть для каждой функции g, определенной на ω_p, задано $F(g)$, которое должно служить значением искомой функции для $p+1$, если ее сужение на ω_p совпадает с g. Таким образом, значение определяемой функции для $p+1$ может зависеть от ее значений на всех меньших целых числах. В описанной ситуации существует единственная функция f на ω такая, что $f(0)=a$ и $f(p+1)=F(f|\omega_p)$ для каждого p из ω. (Через $f|\omega_p$ здесь согласно принятому нами условию обозначено сужение функции f на множество ω_p.) Обычно это утверждение считается очевидным, но доказательство его не вполне тривиально.

13. Теорема. *Предположим, что заданы* a *и* $F(g)$ *для любой функции* g, *областью определения которой служит множество* ω_p, *где* p — *любой элемент множества* ω. *Тогда существует единственная функция* f, *для которой* $f(0)=a$ *и* $f(p+1)=F(f|\omega_p)$ *при любом* $p \in \omega$.

Доказательство. Пусть $\mathfrak{F}$ — семейство всех функций g, каждая из которых определена на некотором множестве вида ω_p, где $p \in \omega$, и удовлетворяет условиям: (а) $g(0)=a$ и (б) для каждого q из ω такого, что $q \leqslant p-1$, непременно $g(q+1)=F(g|\omega_q)$. (Интуитивно ясно, что элементы семейства $\mathfrak{F}$ — это начальные куски искомой функции.) Семейство $\mathfrak{F}$ обладает важным свойством: если $g, h \in \mathfrak{F}$, то либо $g \subset h$, либо $h \subset g$. Для дока-

зательства достаточно обнаружить, что $g(q)=h(q)$ для всех q, принадлежащих области определения как той, так и другой функции. Предположим, что написанное равенство выполняется не всегда, и пусть q — наименьшее целое число, для которого $g(q)\neq h(q)$. Тогда $q\neq 0$, ибо $g(0)=h(0)=a$; следовательно, $g(q)=F(g|\omega_{q-1})$. Но $F(g|\omega_{q-1})=F(h|\omega_{q-1})$, так как g и h согласуются на элементах, меньших q. Значит, $g(q)=F(g|\omega_{q-1})=F(h|\omega_{q-1})=h(q)$, что ведет к противоречию. Пусть $f=\bigcup\{g: g\in\mathfrak{F}\}$. Элементами множества f являются, очевидно, упорядоченные пары. Далее, если $(x, y)\in g\in\mathfrak{F}$ и $(x, z)\in h\in\mathfrak{F}$, то пары (x, y) и (x, z) принадлежат обе либо g, либо h и, следовательно, $y=z$. Значит, f является функцией. Надо показать, что эта функция искомая. Прежде всего, так как $\{(0, a)\}\in\mathfrak{F}$, то $f(0)=a$. Далее, если $q+1$ принадлежит области определения функции f, то $q+1$ является элементом области определения некоторой функции $g\in\mathfrak{F}$. Поэтому $f(q+1)=g(q+1)=F(g|\omega_q)=F(f|\omega_q)$. Наконец, покажем, что областью определения функции f является все множество ω. Предположим, что q — первый элемент из ω, не принадлежащий ей. Тогда $q-1$ — последний элемент области определения функции f. В то же время функция $f\cup\bigcup\{(q, F(f))\}$ является элементом семейства $\mathfrak{F}$. Значит, q принадлежит области определения функции f, что ведет к противоречию *).

Предшествующей теоремой можно систематически пользоваться при доказательстве элементарных свойств вещественных чисел. Например, если b — положительное число и p — целое число, то b^p определяется следующим образом. Положим в условии предшествующей теоремы $a=1$, и пусть для каждой функции g с областью определения ω_p будет $F(g)=bg(p)$. Тогда $f(0)=1$ и $f(p+1)=bf(p)$ для всех p из ω, если в качестве f взять функцию, существование которой гарантируется доказанной теоремой. Положим $b^p=f(p)$. Тогда $b^0=1$ и $b^{p+1}=bb^p$, откуда по индукции можно вывести, что $b^{p+q}=b^pb^q$ для всех p и q из ω. Если b^{-p} определить как $1/b^p$ для всех неотрицательных целых p, то обычным элементарным

*) Единственность искомой функции очевидна. (*Прим. перев.*)

рассуждением устанавливается, что $b^{p+q}=b^p \cdot b^q$ для всех целых p и q.

Пока в наших рассуждениях о вещественных числах мы не пользовались тем, что заданное упорядочение полно. Докажем теперь простое, но достойное внимания следствие полноты порядка. Прежде всего, множество неотрицательных целых чисел не ограничено сверху. Ибо если бы элемент x был наименьшей верхней гранью множества ω, то элемент $x-1$ не был бы верхней гранью этого множества. Тогда было бы $x-1<p$ для некоторого p из ω. Отсюда $x<p+1$, что противоречит тому, что x является верхней гранью ω. Значит, для любых положительных вещественных чисел x и y найдется целое положительное p такое, что $px>y$, так как существует $p\in\omega$, большее y/x. Упорядоченное поле, удовлетворяющее этому условию, называется *архимедовым упорядочением*.

Нам полезно будет знать, что каждое неотрицательное вещественное число обладает b-адическим разложением для любого целого b, большего единицы. Говоря нестрого, мы хотим записать число x в виде суммы степеней числа b, используя неотрицательные целые числа, меньшие b, в качестве коэффициентов (разрядов). Конечно, b-адическое разложение числа не всегда определено однозначно — при десятичном разложении 0,999... (всюду девятки) и 1,000... (всюду нули) являются разложениями одного и того же вещественного числа. Разложение фиксированного числа — это функция, которая ставит в соответствие каждому целому числу некоторое целое число, заключенное между 0 и $b-1$, такая, что (поскольку мы хотим, чтобы до запятой стояло лишь конечное число ненулевых членов) имеется первый ненулевой разряд. Формально a является *b-адическим разложением* *) тогда и только тогда, когда a — функция, определенная на множестве всех целых чисел, областью значений которой служит множество $\omega_{b-1}(=\{q: q\in\omega \text{ и } q\leqslant b-1\})$, такая, что имеется наименьшее целое p, для которого $a_p(=a(p))$ отлично от нуля. b-адическое

*) В русской литературе принято также название «разложение по основанию b». (*Прим. перев.*)

разложение a называется *рациональным* в том и только в том случае, когда существует наибольший ненулевой разряд (т. е. если для некоторого целого p $a_q=0$ при $q>p$). С каждым рациональным b-адическим разложением a можно весьма просто связать некоторое вещественное число $r(a)$. Для всех — за исключением конечного множества — целых чисел p число $a_p b^{-p}$ равно нулю; тогда сумма чисел $a_p b^{-p}$, где p пробегает упомянутое конечное множество, и есть вещественное число $r(a)$, соответствующее a. Мы пишем при этом: $r(a)=\Sigma\{a_p b^{-p} : p$ — *целое число*$\}$. Каждое вещественное число, представимое в таком виде, называется *b-адическим* рациональным (рациональным по основанию b). Таковы числа вида qb^{-p}, где p и q — целые числа. Обозначим через E множество всех b-адических разложений. Его можно лексикографически упорядочить, а именно, b-адическое разложение a предшествует b-адическому разложению c *при словарном порядке* (*лексикографическом порядке*) тогда и только тогда, когда для наименьшего целого p такого, что $a_p\neq c_p$, имеет место $a_p<c_p$. Легко видеть, что, как и в случае обыкновенного словаря, отношение $<$ упорядочивает множество E линейно. Описанное нами соответствие r сохраняет порядок; в этом — ключ к следующему предложению.

14. Теорема. *Пусть E — множество всех b-адических разложений и R — множество всех рациональных разложений; положим для каждого a из R $r(a)=\Sigma\{a_p b^{-p} : p$ — целое число$\}$. Тогда существует единственное монотонное продолжение $\bar{r}$ отображения r, определенное на всем E, при котором множество $E\setminus R$ взаимно однозначно отображается на множество всех вещественных положительных чисел.*

Доказательство. Согласно теореме 0.10 монотонное продолжение $\bar{r}$ отображения r будет существовать, если r переводит каждое подмножество множества R, ограниченное в E, в ограниченное подмножество множества вещественных чисел. Но, очевидно, для каждого $a\in E$ существует элемент $b\in R$ такой, что $b>a$. Если a — верхняя грань подмножества A множества R, то $r(b)$ является верхней гранью множества $f[A]$. Аналогичное рассуждение проходит для нижних граней;

следовательно, r переводит ограниченные множества в ограниченные множества. Поэтому у r есть монотонное продолжение $\bar{r}$, определенное на всем E.

Для доказательства единственности достаточно в силу теоремы 0.10 убедиться, что, каковы бы ни были неотрицательные вещественные числа x и y, из $x<y$ следует, что для некоторого $a\in R$ $x<r(a)<y$. Так как $b^p>p$, каково бы ни было неотрицательное целое число p (это легко доказать по индукции), и так как множество неотрицательных целых чисел не ограничено, то существует целое p, для которого $b^p>1/(y-x)$. Тогда $b^{-p}<(y-x)$. Существует целое число q такое, что $qb^{-p}\geqslant y$, ибо упорядочение архимедово. Так как среди таких q есть наименьшее, то можно предположить, что $(q-1)b^{-p}<y$. Тогда $(q-1)b^{-p}>x$, ибо b^{-p} меньше $(y-x)$. Этим доказано, что существует b-адическое рациональное число, а именно $(q-1)b^{-p}$, являющееся образом некоторого элемента из R и лежащее между x и y. Следовательно, монотонное продолжение $\bar{r}$ единственно.

Покажем теперь, что отображение $\bar{r}$ взаимно однозначно на подмножестве $E\setminus R$. Непосредственно видно, что $\bar{r}$ взаимно однозначно на R; этот факт будет дальше использован. Пусть $a\in E$, $c\in E\setminus R$ и $a<c$. Тогда для первого из тех p, для которых a_p и c_p различны, непременно $a_p<c_p$. Разложение d, определенное следующим образом: $d_q=a_q$ при $q<p$, $d_q=0$ при $q>p$ и $d_p=a_p+1$, — является элементом множества R, бóльшим a. Так как у c нет последнего ненулевого разряда, то $a<d<c$. Повторяя рассуждение, найдем в R элемент e, для которого $a<d<e<c$. Тогда из взаимной однозначности отображения $\bar{r}$ на R вытекает, что $\bar{r}(a)\leqslant\bar{r}(d)<\bar{r}(e)\leqslant\bar{r}(c)$. Значит, $\bar{r}$ взаимно однозначно на $E\setminus R$.

Наконец, надо показать, что образ множества $E\setminus R$ при отображении $\bar{r}$ представляет собой все множество положительных чисел. Заметим сначала, что для каждой пары элементов c и d из R, для которой $c<d$, найдется такое $a\in E\setminus R$, что $c<a<d$. Следовательно, для любых положительных вещественных чисел x и y, где $x<y$, можно найти в $E\setminus R$ такой элемент a, что $x<\bar{r}(a)<y$. Пусть теперь x — некоторое вещественное

положительное число, не являющееся образом никакого элемента из $E \setminus R$ при отображении $\bar{r}$. Положим $F = \{a : a \in E \setminus R \text{ и } \bar{r}(a) < x\}$. Если у множества F есть верхняя грань — элемент c, то при $\bar{r}(c) < x$ ни одна точка из $E \setminus R$ не может отобразиться в интервал $(\bar{r}(c), x)$, а при $\bar{r}(c) > x$ (так как $\bar{r}$ сохраняет порядок) ни одна точка из $E \setminus R$ не может отобразиться в интервал $(x, \bar{r}(c))$. В любом случае имеем противоречие. Таким образом, теорема будет доказана, если мы обнаружим, что каждое ограниченное сверху непустое подмножество множества $E \setminus R$ имеет верхнюю грань, т. е. что $E \setminus R$ полно в рассматриваемом упорядочении.

Пусть F — произвольное непустое ограниченное сверху подмножество множества $E \setminus R$. Тогда среди чисел p таких, что $a_p \neq 0$ для некоторого a из F, существует наименьшее. Положим по определению, что c_q равно нулю при $q < p$; пусть F_p — множество всех элементов a из F, p-й разряд a_p у которых отличен от нуля, и $c_p = \max\{a_p : a \in F_p\}$. Определим F_{p+1} как множество всех элементов $a \in F_p$, для которых $a_q = c_q$ при $q = p$, и положим $c_{p+1} = \max\{a_{p+1} : a \in F_{p+1}\}$; продолжим построение по индукции. Ни одно из множеств F_p не может быть пустым. Легко видеть, что разложение c, к которому приводит описанная конструкция, является верхней гранью множества F — в действительности его наименьшей верхней гранью — и что $c \in E \setminus R$.

Предшествующая теорема будет применена в случаях $b = 2$, $b = 3$ и $b = 10$. Соответствующие b-адические разложения называются *двоичным*, *троичным* и *десятичным*.

СЧЕТНЫЕ МНОЖЕСТВА

Множество называется конечным тогда и только тогда, когда можно установить взаимно однозначное соответствие между его элементами и элементами некоторого множества вида $\{p : p \in \omega \text{ и } p < q\}$, где $q \in \omega$. Множество A называется *счетно бесконечным* в том и только в том случае, когда можно установить взаимно однозначное соответствие между его элементами и элементами множества ω всех неотрицательных целых чисел.