ПРИДНЕСТРОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
им. Т.Г. ШЕВЧЕНКО

**Физико-математический факультет**

Кафедра алгебры, геометрии и МПМ

# ОСНОВНЫЕ АЛГЕБРАИЧЕСКИЕ СИСТЕМЫ И ИХ ЭЛЕМЕНТАРНЫЕ СВОЙСТВА

## Кольцо целых чисел и алгебраические системы

***Учебно-методическое пособие***

***Часть I***

Тирасполь - 2019

УДК511.125(075.8)
ББК В131я73
Т33
Составители:

**Ю.М. Рябухин,** академик АН РМ,д.ф-м.н., профессор кафедры алгебры, геометрии и МПМ, ПГУ им. Т.Г. Шевченко.

**Г.Н. Ермакова,** к.п.н., доцент, зав. кафедрой алгебры, геометрии и МПМ, ПГУ им. Т.Г. Шевченко.

**Н.Л. Григорьева,** учитель математики высшей квалификационной категории кадетской школы г. Бендеры.

**Общая алгебра. Кольцо целых чисел и алгебраические системы**: *Учебно-методическое пособие. Часть* I. Сост.: Ю.М. Рябухин, Г.Н. Ермакова, Н.Л. Григорьева – Тирасполь, 2019 - 108с.

*Учебно-методическое пособие содержит теоретический материал по курсу* «*Основные алгебраические системы и их элементарные свойства*», *посвящено одному из разделов универсальной алгебры, молодой развивающейся науке, нашедшей свои приложения как внутри математики, так и информатике и ряде других наук. Адресовано студентам и магистрантам, аспирантам математикам, информатикам, а так же научным работникам в этих областях.*

Рекомендовано Научно-методическим советом ПГУ им. Т.Г. Шевченко

© Составители, 2019

Оглавление

Введение ..... 4
§1 Наиболее известные алгебраические системы ..... 6
§2. Общие конструкции и утверждения о подмножествах и образах отображений непустых множеств ..... 11
§3. Общие конструкции и теоремы о подсистемах и гомоморфизмах алгебраических систем ..... 30
§4. Натуральный ряд ℕ и арифметические операции ..... 67
§5. Многообразие группоидов ..... 73
§6. Специфика полугрупп и групп (теорема о гомоморфизмах для групп) ..... 87
§ 7 Аддитивные подгруппы кольца целых чисел и основная теорема арифметики ..... 93
§8 Гомоморфные образы кольца $\mathbb{Z}\boldsymbol{m}$ (кольца вычетов), циклические группы и описание конечных абелевых групп ... 101

## Введение

Универсальная алгебра сравнительно молодая наука, изучающая поведение функций на произвольных множествах. Возникшая на стыке математической логики и классической алгебры, универсальная алгебра, в свою очередь, оказала влияние, как на эти разделы математики, так и на более далекие области этой науки. В частности, непосредственное применение универсальная алгебра нашла в программировании, в теории баз данных и ряде других областей, получивших развитие в нынешнюю эпоху широкого применения вычислительных машин. Тем не менее, круг людей, знакомых с универсальной алгеброй и владеющих её методами, довольно узок. Сам курс универсальной алгебры читается в виде спецкурсов в довольно ограниченном числе университетов.

Одна из проблем, с которой столкнулся один из авторов при подготовке и чтении курса «Основные алгебраические системы и их элементарные свойства» – отсутствие подходящей учебной литературы на русском языке. Классический учебник А.И.Мальцева "Алгебраические системы" является в настоящее время библиографической редкостью, да и материал этой книги, написанный в 60-е годы, далеко не полностью отражает современные достижения универсальной алгебры. То же можно сказать и о имеющейся на русском языке книге П.Кона "Универсальная алгебра". Учебники А.Г.Куроша "Лекции по общей алгебре" и Л.А.Скорнякова "Общая алгебра" вопросов универсальной алгебры касаются лишь косвенно. Книга Д.М.Смирнова "Многообразия алгебр" носит скорее монографический, а не учебный характер, да и изданная малым тиражом, малодоступна студентам. На английском языке можно указать на книгу Г.Гретцера "Универсальная алгебра" и С.Барриса, Х.П.Санкапанавара "Курс универсальной алгебры", но они велики по объёму материала и недоступны для наших студентов.

Эти обстоятельства и подтолкнули одного из авторов на написание первой части учебно-методического пособия под ту часть курса универсальной алгебры, которую в течение нескольких лет он читал студентам бакалавриата и магистратуры ФМФ ПГУ им. Т.Г. Шевченко, специализирующимся по прикладной математике и математике.

## §1 Наиболее известные алгебраические системы

Алгебраические системы, как непустые множества с некоторым набором алгебраических операций, весьма разнообразны. При этом, *n-арная* операция любому упорядоченному набору из $n$ элементов данного множества $a_1, a_2, \dots, a_n \in G$ ставит в соответствие однозначно определённый элемент $a_1 a_2 \dots a_n \omega \in G$. Как правило, используются *бинарная операция* (каждой упорядоченной паре элементов данного множества ставится в соответствие один и только один элемент этого же множества), *унарная операция* (каждому элементу данного множества ставится в соответствие один и только один элемент этого же множества) и, иногда, *нульарная операция* (фиксирует определённый элемент).

Некоторые из операций и их свойства известны из школьного курса математики. Так, например, операции сложения и умножения являются бинарными алгебраическими операциями на любом из известных школьникам числовых множеств: натуральных чисел $\mathbb{N}$, натуральных чисел с нулём $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, целых чисел $\mathbb{Z}$, рациональных чисел $\mathbb{Q}$, действительных чисел $\mathbb{R}$. При этом, справедливо каноническое вложение

$$\mathbb{N} \subset \mathbb{N}_0 = \mathbb{N} \cup \{0\} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

Специфика алгебраической системы $A = A(\Omega)$ определяется с помощью законов и тождеств, связывающих заданные на $A$ операции. Рассмотрим некоторые их них.

Множество $G$ с одной бинарной операцией$*$называют *группоидом* и обозначают через $G(*)$.

Определение показывает, что для задания группоида, на множестве $G$ нужно ввести правило, по которому можно найти значение операции $*$ для любых двух элементов из $G$. В некоторых группоидах могут существовать элементы со специальными свойствами. Примерами группоидов служат $\mathbb{N}(+), \mathbb{N}_0(+), \mathbb{Z}(+), \mathbb{Q}(+), \mathbb{R}(+)$, а так же $\mathbb{N}(\cdot), \mathbb{N}_0(\cdot), \mathbb{Z}(\cdot),. \mathbb{Q}(\cdot), \mathbb{R}(\cdot)$.

Заметим, что вычитание будет бинарной операцией на $\mathbb{Z}, \mathbb{Q}$ и $\mathbb{R}$, но не на множествах $\mathbb{N}$ и $\mathbb{N}_0$.

Элемент $\eta$ группоида $G(*)$ называют нейтральным элементом относительно операции $*$, если для любого элемента $a$ из множества $G$ выполняется равенство:

$$a * \eta = \eta * a = a.$$

Например, в группоидах $\mathbb{N}_0(\cdot)$, $\mathbb{Q}(\cdot)$ нейтральным элементом является единица 1 $(a \cdot 1 = 1 \cdot a = a)$. В группоидах $\mathbb{N}_0(+), \mathbb{Z}(+), \mathbb{Q}(+)$ нейтральным элементом будет нуль $(a + 0 = 0 + a = a)$.

Элемент $a'$ группоида $G(*)$ с нейтральным элементом $\eta$ называют *симметричным* для элемента $a \in G$, если для элементов $a$ и $a'$ выполняется равенство: $a * a' = a' * a = \eta$.

*Полугруппой* называется группоид, для элементов которого операция $*$ ассоциативна, т.е. для любых элементов $a, b$ и $c$ имеет место равенство:

$$(a * b) * c = a * (b * c)$$

Последнее равенство определяет тернарную операцию $*$ и придает ей однозначный смысл, т.е.

$$a * b * c = (a * b) * c = a * (b * c).$$

Таким образом, в выражении из трёх элементов связанных операцией $*$ скобки можно расставлять произвольно.

По индукции полученный результат можно обобщить на случай любого конечного числа элементов полугруппы: для любого конечного числа элементов $n$ полугруппы можно считать -арную операцию, определённой через $(n-1)$-арную, т.е.

$$a_1 * a_2 * \ldots * a_n = (a_1 * a_2 * \ldots * a_{n-1}) * a_n,$$

при этом в полученном выражении скобки можно расставлять произвольно.

Все перечисленные множества относительно операции сложения, или операции умножения являются полугруппами.

Полугруппу с нейтральным элементом назовём*моноидом*.

Моноид $G(*)$ назовём *группой*, если для каждого его элемента существует симметричный элемент.

Таким образом, группа это непустое множество с тремя основными операциями: бинарной операцией $*$, унарной операцией, сопоставляющей каждому элементу симметричный и нульарной, выделяющей нейтральный элемент.

При этом для бинарной операции выполняются свойства: для любых элементов $a, b$ и $c$ группы $G(*)$

$(a * b) * c = a * (b * c), a * \eta = \eta * a = a, a * a' = a' * a = \eta.$

Если выполняется условие коммутативности операции $*$, т.е. выполняется равенство $a * b = b * a$, то группа $G(*)$ называется коммутативной, или абелевой.

Если под операцией $*$ понимаем сложение, то группа называется *аддитивной*, если под операцией $*$ понимаем умножение, то группа называется *мультипликативной*.

Для операции сложения нейтральный элемент – нуль, для операции умножения – единица. Симметричные элементы относительно операции сложения являются противоположными, а относительно операции умножения – обратными.

Рассмотрим примеры: группоиды$\mathbb{Z}(+), \mathbb{Q}(+), \mathbb{R}(+)$ – аддитивные группы, $\mathbb{N}(+)$ не является группой, так как не содержит нулевого элемента , $\mathbb{N}_0(+)$ не является группой, так как противоположный элемент есть только у нуля. Группоиды $\mathbb{N}(\cdot), \mathbb{N}_0(\cdot), \mathbb{Z}(\cdot), \mathbb{Q}(\cdot), \mathbb{R}(\cdot)$ группами не являются. Для $\mathbb{Q}(\cdot), \mathbb{R}(\cdot)$ не существует обратных элементов для нуля. На множестве целых чисел обратимы только два элемента 1 и –1.

Естественно возникают и другие системы, например, кольца.

Непустое множество $K$ с введёнными на нём операциями сложения и умноженя $(K(+,\cdot))$ назовём *кольцом*, если $K(+)$ – абелева

группа, $K(\cdot)$ – полугруппа и для элементов множества $K$ операции сложения и умножения связаны двумя дистрибутивными законами, т.е.

$$(a+b)+c=a+(b+c),(a\cdot b)\cdot c=a\cdot(b\cdot c) \quad (1)$$

$$a+0=0+a,a+(-a)=(-a)+a=0 \quad (2)$$

$$(a+b)\cdot c=a\cdot c+b\cdot c,c\cdot(a+b)=c\cdot a+c\cdot b \quad (3)$$

Таким образом, в кольце фиксируется (всегда существует) нуль и задана унарная операция взятия противоположного элемента, связанные законами (2). Корме того, сложение коммутативно, т.е. $a+b=b+a$, а из указанных свойств вытекает равенство$a\cdot 0=0\cdot a=0$, дополняющие специфику нуля.

Простейшим примером кольца является нулевое кольцо $\mathbb{O}=\{0\}$. Кольцом является множество целых чисел $\mathbb{Z}(+,\cdot)$. Однако можно построить и другие кольца – специальные.

В школьном курсе математики рассматривается примеры и других алгебраических систем.

Так, например, рассматриваются вектора и линейные операции над ними на плоскости (в двумерном пространстве) и в пространстве (в трёхмерном пространстве). Однако определение арифметического векторного пространства, так же как определения группы, кольца и, следующего определения поля, школьникам не знакомы. Они знают перечисленные выше числовыеи векторные множества и операции над их элементами.

Введём ещё одно определение.

*Полем* называют коммутативное кольцо с единицей, в котором каждый ненулевой элемент обратим.

Наиболее распространённые примеры полей – поле действительных $\mathbb{Q}$и рациональных чисел $\mathbb{R}$. Так как поля являются кольцами, то они обладают всеми общими свойствами колец. Вместе с тем, поля обладают и некоторыми специфичными свойствами.

Таким образом, студенты первого курса подготовлены к встрече с абстрактными алгебраическими системами.

## §2. Общие конструкции и утверждения о подмножествах и образах отображений непустых множеств

Для уточнения специфики даже «хорошо известных» алгебраических систем, применяют разнообразные общие конструкции и «рабочие» утверждения или договорённости о произвольных множествах. Обычно строят только непустые множества, после уточнения специфики их элементов. Иногда элементами построенных множеств оказываются некоторые множества и тогда соответствующие построения или определения нужно уточнять (часто строится одно и то же, но называется по разному!). Чтобы избежать возможных недоразумений, мы будем постепенно увеличивать «набор» конструкций, определений или утверждений, иногда делая пояснения (даже известного !).

Вместе с «всегда непустым» множеством $A$ естественно возникает или строится *полная решётка* $\mathcal{B}(A)$ *подмножеств в* $A$. Элементами в $\mathcal{B}(A)$ являются подмножества $B \subseteq A$ и они сравниваются по включению. При этом в $\mathcal{B}(A)$ выделяется наибольший элемент и это конечно $A \in \mathcal{B}(A)$ , а после этого оказывается, что для любого непустого семейства элементов $A_i \in \mathcal{B}(A)$ всегда существуют (строятся) *пересечения* $\bigcap A_i = C \in \mathcal{B}(A)$ *и объединения* $\bigcup A_i = S \in \mathcal{B}(A)$, но это уже нужно пояснять, когда множество $A$имеет разные элементы или не одноэлементно.

Учтём, что пересечение $C = \bigcap A_i$ состоит из элементов попадающих сразу во все указанные $A_i$ и поэтому $C \in \mathcal{B}(A)$ оказывается наибольшим среди подмножеств $R \in \mathcal{B}(A)$ содержащихся во всех $A_i \in \mathcal{B}(A)$.

$$R \subseteq C = \bigcap A_i \Leftrightarrow (\forall i | R \subseteq A_i)$$

При этом, если в $A$ имеются различные элементы $x, y \in A$, то конечно получается равенство $\{x\} \bigcap \{y\} = \emptyset$ (так как $x \neq y$). Именно поэтому нужно учитывать и пустое множество $\emptyset$, как наименьший элемент $\emptyset \in \mathcal{B}(A)$, а наибольший в $\mathcal{B}(A)$ элемент$A \neq \emptyset$ (по

договорённости!). Объединение $S = \bigcup A_i$ состоит из элементов, попадающих хотя бы в одно $A_i$ и потому $S \in \mathcal{B}(A)$ является наименьшим среди подмножеств $T \in \mathcal{B}(A)$ содержащих все заданные $A_i \in \mathcal{B}(A)$.

$$T \supseteq S = \bigcup A_i \Leftrightarrow (\forall i | T \supseteq A_i)$$

Одновременно получается, что $S \neq \emptyset$ тогда и только тогда, когда хотя бы одно $A_i \neq \emptyset$.

Кроме того, можно учесть, что для $B \in \mathcal{B}(A)$ всегда строится *дополнение* $\mathcal{B}(A)$, состоящее из элементов $a \in A$, которые не попадают в $B$. При этом, конечно, $\bar{A} = \emptyset$, $\bar{\emptyset} = A$ и очевидны равенства $B \cap \bar{B} = \emptyset$, $A = B \cup \bar{B}$, а потому $B \neq \bar{B}$. Чуть сложнее заметить, что всегда $(B \subseteq R \Leftrightarrow \bar{B} \supseteq \bar{R})$, то есть «переход к дополнениям меняет включения на противоположные» и этот переход взаимно однозначен, но не тождественен. Одновременно получается, что для $S = \bigcup A_i$ всегда $\bar{S} = \bigcap \bar{A}_i$, а для $C = \bigcap A_i$ всегда $\bar{C} = \bigcup \bar{A}_i$, согласно уже отмеченным свойствам пересечений, объединений и дополнений.

После этого можно описать *минимальные* в $\mathcal{B}(A)$ элементы (строго меньше которых только наименьший элемент) и это, конечно одноэлементные $\{a\} \in \mathcal{B}(A)$ для всех $a \in A$. Но тогда, благодаря переходу к дополнениям, описываются *максимальные* в $\mathcal{B}(A)$ элементы (строго больше которых только наибольший элемент) – это дополнения $A \setminus \{a\}$ минимальных. А учитывая и это получаем, что непустые $C \in \mathcal{B}(A)$ однозначно представляются в виде $C = \bigcup\{c\}$, где $c \in C$, т.е. являются объединением минимальных и это очевидно (просто указываются элементы $c \in C$). Менее очевидно, что отличные от $A$ элементы $S \in \mathcal{B}(A)$ представляются в виде $S = \bigcap A \setminus \{t\}\, (t \notin S)$ пересечения максимальных и тоже однозначно.

Все сказанное выше и характеризует $\mathcal{B}(A)$, как полную (булеву) решётку, а с её помощью строятся и другие «решётки подмножеств», продолжая учитывать специфику включений на множестве $A$. Можно

просто «зафиксировать» элемент $0 \in A$ и тогда получается *полная решётка* $\mathcal{B}(A)$ *подмножеств с отмеченной точкой* $0$. При этом в $\mathcal{B}_0(A)$ конечно строятся пересечения и объединения (как в $\mathcal{B}(A)$, но наименьшим элементом оказывается $\{0\} \in \mathcal{B}_0(A)$. Можно учесть «более общие» *системы замыкания на* $A$ (или в $\mathcal{B}(A)$) – это такие $\mathfrak{R} \subseteq \mathcal{B}(A)$, что $A \in \mathfrak{R}$ и $\bigcap A_i = C \in \mathfrak{R}$ ля любых $A_i \in \mathfrak{R}$, но это уже нужно пояснять (а затем применять!).

**Теорема 1.** Благодаря специфике системы $\mathfrak{R} \subseteq \mathcal{B}(A)$ замыкания, строится соответствующий *оператор*$X \rightsquigarrow \xi(X)$*замыкания*, согласно правилу $(*)$ и это означает (по определению!), что оказываются справедливы соотношения $(**)$.

$$A \supseteq X \rightsquigarrow \xi(X) = \bigcap\{C \in \mathfrak{R} | C \supseteq X\} \in \mathfrak{R} \qquad (*)$$

$$\big(X \subseteq \xi(X) = \xi\big(\xi(X)\big), X \subseteq Y\big) \Rightarrow \xi(X) \subseteq \xi(Y) \quad (**)$$

При этом, конечно, $A = \xi(A)$ и возникающие элементы $R = \xi(R)$– это в точности элементы $R \in \mathfrak{R}$. С другой стороны, если задан оператор $X \rightsquigarrow \xi(X)$ замыкания на $A$ (т.е. справедливы соотношения$(**)$), то отмечаются -*замкнутые* $R = \xi(R)$, которые и образуют соответствующую систему $\mathfrak{R} \subseteq \mathcal{B}(A)$ замыкания.

**Доказательство.**

В самом деле, согласно указанному (перед теоремой) определению системы $\mathfrak{R} \subseteq \mathcal{B}(A)$ замыкания на $A$,выписанное правило $(*)$ корректно – для $X \subseteq A$ действительно построен элемент $\xi(X) \in \mathfrak{R}$ и он оказывается наименьшим среди $C \in \mathfrak{R}$ таких, что $C \supseteq X$. Именно поэтому $A = \xi(A)$ и становится очевидным, что справедливы соотношения $(**)$, т.е. действительно построен оператор $X \rightsquigarrow \xi(X)$ замыкания. Но не менее очевидно, согласно ужесказанному, что $R = \xi(R)$ тогда и только тогда, когда $R \in \mathfrak{R}$, а потому отмечаются в точности все элементы системы $\mathfrak{R} \subseteq \mathcal{B}(A)$замыкания.

С другой стороны, если задан оператор $X \rightsquigarrow \xi(X)$ замыкания (элементов $X \in \mathcal{B}(A)$, то справедливы указанные соотношения $(**)$ (просто по определению!). Но тогда, конечно, $A = \xi(A)$ и возникают *-замкнутые* $R = \xi(R)$ . Для любого семейства таких элементов $A_i = \xi(A_i)$ всегда строится «обычное» пересечение $\bigcap A_i = C \in \mathcal{B}(A)$, а именно $(**)$ и специфике пересечений (отмеченной при построении $\mathcal{B}(A)$ всегда, $C \supseteq A_i = \xi(A_i) \supseteq \xi(C) \supseteq C$ и потому $C = \xi(C)$. Именно поэтому $\xi$ *–замкнутые* элементы образуют систему $\mathfrak{R} \subseteq \mathcal{B}(A)$ замыкания и это заканчивает доказательство теоремы.

**Следствие.** В системе $\mathfrak{R} \subseteq \mathcal{B}(A)$ замыкания выделяется наибольший элемент $A \in \mathfrak{R}$ и для любого семейства элементов $A_i \in \mathfrak{R}$ строится «обычное» (как в $\mathcal{B}(A)$) пересечение $\bigcap A_i = C \in \mathfrak{R}$, а потому имеется и наименьший элемент $O \in \mathfrak{R}$ (как пересечение всех элементов из $\mathfrak{R}$). Всегда строятся, по правилу $(***)$,

$$\vee A_i = \xi(\bigcup A_i) \in \mathfrak{R} \qquad (***)$$

и соответствующие *-замкнутые* объединения $\vee A_i \in \mathfrak{R}$ – это наименьшие среди $R \in \mathfrak{R}$, содержащих все заданные $A_i \in \mathfrak{R}$, но может оказаться, что $\vee A_i = S \neq \bigcup A_i$, так как возникающие «системы замыкания» весьма разнообразны.

Всё отмеченное «почти очевидно», благодаря теореме и её доказательству – мы просто пояснили специфику ситем $\mathfrak{R} \subseteq \mathcal{B}(A)$ замыкания и учли соответствующий оператор замыкания (построенный по правилу $(*)$ ). При этом, конечно, $\mathcal{B}(A)$ является «системой замыкания» (с тождественным оператором замыкания $X \rightsquigarrow \xi(X)$ ), все полные решётки $\mathcal{B}_0(A)$ тоже являются «системами замыкания» (с оператором $X \rightsquigarrow X \bigcup\{0\}$ замыкания), но если множество $A$имеет хотя бы *три* различных элемента, то легко строятся и другие системы $\mathfrak{R} \subseteq \mathcal{B}(A)$ замыкания – в которых иногда $\vee A_i \neq \bigcup A_i$ , но всегда $\bigcap A_i \in \mathfrak{R}$ для любых$A_i \in \mathfrak{R}$.

Продолжая «набор общих конструкций» учтём, что для произвольно заданных непустых множеств $A, B$ всегда строится их *декартово произведение* $A \times B = \{(a.b)|a \in A, b \in B\}$ – его элементами являются указанные пары, причём применяется «правило равенства»:$(a_1, b_1) = (a_2, b_2) \Leftrightarrow (a_1 = a_2$ и $b_1 = b_2)$.

Можно строить и декартовы произведения$A_1 \times A_2 \times \ldots \times A_n$ – они состоят из соответствующих *упорядоченных наборов из* $n$ элементов $(a_1, a_2, \ldots, a_n)$ с соответствующим «покомпонентным правилом равенства». А если учтём копии $A_i = A$ заданного множества $A$, то получаются его *декартовы степени*
$A^{(n)} = A \times A \times \ldots \times A$, начиная с $A^{(1)} = A$ и $A^{(2)} = A \times A$. После этого строятся *алгебраические операции* на $A$– это -арные
$\mu: A^{(n)} \to A$, которые с каждой $n$-кой $(a_1, a_2, \ldots, a_n) \in A^{(n)}$ всегда *однозначно* связывают элемент $(a_1, a_2, \ldots, a_n)\mu = a \in A$, как результат применения этой операции. Возникающие на $A$ алгебраические операции весьма разнообразны, когда множество $A$ не одноэлементно, иногда возникают разные алгебраические операции с одинаковой «арностью». Поэтому весьма разнообразны и алгебраические системы $A = A(\Omega)$, как всегда непустые множества $A$ с некоторым набором $\Omega$ алгебраических операций и обычно уточняется их специфика.

С другой стороны, вместе с квадратом $A \times A$ (не одноэлементным, когда множество $A$ не одноэлементтно) возникают разнообразные *бинарные отношения* на $A$– это просто подмножества $\sigma \subseteq A \times A$. Как правило$\sigma \neq \emptyset$, а тогда вместо записи $(x, y) \in \sigma$ применяют запись $x\sigma y$ и говорят, что элемент $x \in A$ находится в отношении $\sigma$ с элементом $y \in A$. Если же выполнены выписанные условия рефлексивности, антисимметричности и транзитивности
$\forall a \in A|a\sigma a, (x\sigma y, y\sigma x) \Rightarrow x = y, (x\sigma y, y\sigma a) \Rightarrow x\sigma a$,
то говорят, что $\sigma$ *задаёт частичный* порядок на $A$ или «превращает» $A$ в *частично упорядоченное множество* $A = A(\sigma)$. В этой ситуации вместо $x\sigma y$ иногда говорят, что $x$ меньше $y$ или $y$ больше $x$, а затем

учитывается, что *каждое непустое* $S \subseteq A$ *частично упорядочено* в*месте* с $A = A(\sigma)$, благодаря индуцированному на $S$частичному порядку $\sigma \bigcap (S \times S)$.

Поясняя эти «названия и договорённости» можно учесть, что в произвольном частично упорядоченном множестве$A$иногда имеются «не сравнимые» элементы – такие $x, y \in A$, что и $x\sigma y$ и $y\sigma x$ не получается. Если же таких элементов нет, то $A$ *линейно упорядочено* и в этой ситуации всегда $x\sigma y$ или $y\sigma x$ или $x = y$.Ещё более специальны, но часто возникают *вполне упорядоченные* множества$A$, в которых каждое непустое $S \subseteq A$ всегда имеет элемент $s \in S$ такой, что $s\sigma t$ для всех $t \in S$ (или наименьший в $S$ элемент).

Более того, согласно уже сказанному легко заметить, что в произвольном частично упорядоченном множестве всегда имеются линейно упорядоченные подмножества (или «цепочки» элементов), и среди них выделяются и вполне упорядоченные. Для этого можно учесть «уже построенные» полные решётки $\mathcal{B}(M)$, как весьма специальные частично упорядоченные множества, а затем учесть, что все непустые$A \subseteq \mathcal{B}(M)$, тоже частично упорядочены вместе с $\mathcal{B}(M)$.

**Предложение 1.** Частично упорядоченное множество $A$ и его частичный порядок $\sigma$ можно «представить» с помощью полной решётки $\mathcal{B}(A)$ с включениями в качестве частичного порядка. А именно, согласно выписанному правилу, с каждым элементом $a \in A$ всегда *однозначно* связан элемент $\vec{a} \in \mathcal{B}(A)$ и эти элементы образуют в $\mathcal{B}(A)$подмножество

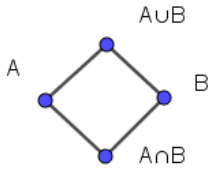
$\vec{A} = \{\vec{a} | a \in A\}$, т.е. $A \ni a \rightsquigarrow \vec{a} = \{x \in A | x\sigma a\} \in \mathcal{B}(A)$

Но при этом оказывается, что $x\sigma y$ *тогда и только тогда, когда* $\vec{x} \subseteq \vec{y}$, то есть построено естественное представление $A(\sigma) \approx \vec{A}(\subseteq)$ частично упорядоченного множества $A$ (и его частичного порядка $\sigma$) в виде частично упорядоченного множества $\vec{A}$ (с включениями указанных подмножеств в качестве частичного порядка).

В самом деле, построенные подмножества $\vec{a} \subseteq A$ это подмножества с наибольшим элементом $a \in \vec{a}$,согласно выписанному правилу построения, причём все $x \in A$ меньшие $a$ попадают в $\vec{a}$. Поэтому, если $x\sigma y$, то$x \in \vec{y}$, но тогда$\vec{x} \subseteq \vec{y}$, так как$z\sigma x$и$x\sigma y$влекут$z\sigma y$. Обратно, если $\vec{x} \subseteq \vec{y}$, то $x\sigma y$, так как $x \in \vec{x}$, а потому и получилось, что $x\sigma y \Leftrightarrow \vec{x} \subseteq \vec{y}$ (частичный порядок $\sigma$ представлен как отношение включения).

Это заканчивает «доказательство», а благодаря построенному представлению $A(\sigma) \approx \vec{A}(\subseteq)$ получается «наглядное представление» всего сказанного о специфике частично упорядоченного множества $A$ или частичного порядка $\sigma$, когда множество $A$ не одноэлементно. Так, например, всегда существующие в $\mathcal{B}(A)$ не сравнимые (по включению) элементы $B, C \in \mathcal{B}(A)$ из которых строятся решётки из четырёх элементов, что весьма «наглядно представляется» в виде выписанной диаграммы включений их элементов.

При этом может оказаться, что $B, C \in \vec{A}$ и тогда $B = \vec{b}$, $C = \vec{c}$ для соответствующих элементов $b, c \in A$, но $b\sigma c$ и $c\sigma b$ не получается, согласно предложению, а потому элементы $b, c \in A = A(\sigma)$ не сравнимы относительно $\sigma$. Но в $\mathcal{B}(A)$ возникают и цепочки $A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots$, которые и оказываются линейно упорядоченными подмножествами в $\mathcal{B}(A)$ не одноэлементными, когда указанные $A_i$ различны. После этого получается, что и в $A = A(\sigma)$ возникают не одноэлементные линейно упорядоченные подмножества, когда имеются различные, но сравнимые элементы – получаются цепочки $a_1\sigma a_2\sigma a_3$ ..., когда $A_i = \overrightarrow{a_i}$ образуют указанную цепочку в $\mathcal{B}(A)$. Но тогда возникают и вполне упорядоченные подмножества, например, конечные цепочки всегда вполне упорядочены.




Заканчивая «пояснения» специфики частичного порядка отметим, что с помощью выписанной диаграммы легко описываются все частично упорядоченные множества из двух элементов и «почти все» частично упорядоченные множества из трёх элементов – это лёгкое упражнение.

Продолжая считать множество $A$ не одноэлементным можно заметить, что вместе с $A \times A$ возникают разнообразные отношеания эквивалентности на $A$. А именно, бинарное отношение $\theta \subseteq A \times A$ *эквиваленция* на $A$, если выполнены выписанные условия рефлексивности, симметричности и транзитивности. В этой ситуации говорят, что элемент $x \in A$ эквивалентен элементу $a \in A$, когда $x\theta a$ (и конечно получится, что $a\theta x$), т.е.

$$\forall a \in A | a\theta a, \qquad x\theta a \Rightarrow a\theta x, (x\theta y, y\theta a) \Rightarrow x\theta a$$

При этом получается, конечно, что $A \times A$ – тривиальная эквиваленция, когда любые два элемента эквивалентны, но учитывается и эквиваленция $\Delta_A = \{(a,a) | a \in A\}$, когда эквивалентны только равные элементы, причём $\Delta_A \neq A \times A$ , из-за не одноэлементности множества $A$.

**Предложение 2.** Эквиваленции $\theta$ на множестве $A$ конечно можно сравнивать «по включению» и тогда получается, что $\Delta_A \subseteq \theta \subseteq A \times A$. Более того, если учесть полную решётку $\mathcal{B}(A \times A)$, то получится, что обычное пересечение $\bigcap \theta_i$ эквиваленций всегда является эквиваленцией. Поэтому *все*эквиваленции на

$A$ образуют «полную решётку» или систему $\mathcal{E}(A) \subseteq \mathcal{B}(A \times A)$ замыкания на $A \times A$, с наибольшим элементом $A \times A$, наименьшим элементом $\Delta_A$ и обычными пересечениями $\bigcap \theta_i = \theta \in \mathcal{E}(A)$, с помощью которых строятся и «объединения $\vee \theta_i$эквиваленций, как эквиваленций» (см. следствие из теоремы 1). Однако может оказаться, что $\vee \theta_i \neq \bigcup \theta_i$ (и это надо уточнять!).

Почти всё сказанное с очевидностью вытекает из уже указанных «общих определеней» с помощью соответствующих конструкций. В частности, если заданы или построены эквиваленции $\theta_i \subseteq A \times A$, то для всех $\theta_i$ выполнены указанные условия рефлексивносст, симметричности и транзитивности. Но тогда эти условия выполнены и для пересечения $\theta_i = \bigcap \theta_i$ (всегда $(a.a) \in \theta$, так как $(a.a) \in \theta_i$, а потому $\theta$ рефлексивно и т.д.). Поэтому $\theta$ оказывается эквиваленцией, а множество $\mathcal{E}(A)$ всех эквиваленций системы замыкания на $A \times A$( или в $\mathcal{B}(A \times A)$, согласно определению. Но тогда можно учесть соответствующий оператор замыкания (согласно теоремы 1 и её следствия), а потому вместе с обычными пересечениями $\bigcap \theta_i \in \mathcal{E}(A)$, стоятсяэквиваленции $\vee \theta_i \in \mathcal{E}(A)$.

Осталось показать, что иногда $\vee \theta_i \neq \bigcup \theta_i \in \mathcal{B}(A \times A)$ и это можно сделать с помощью конкретных примеров. В частности, если $A = \{a, b\}$(где $a \neq b$), то конечно получается, что

$$A \times A = \{(a, a), (a, b), (b, a), (b, b)\},$$

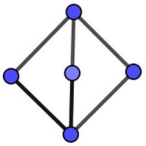
а после этого легко строится и множество $\mathcal{E}(A)$всех эквиваленций на указанном множестве $A$. Однако в этой ситуации оказывается, что $\mathcal{E}(A) = \{\Delta_A, A \times A\}$и «примера нет».

Но примеры есть, когда в множестве $A$имеется хотя бы *три различных элемента* $a, b, c \in A$, так как тогда различны и элементы $(a, b), (b, c), (c, a) \in A \times A$. А именно, применяя оператор замыкания на $\mathcal{B}(A \times A)$ соответствующий $\mathcal{E}(A)$, легко построить *все минимальные*

*эквиваленции* (меньше которых только$\Delta_A$) – получаются эквиваленции $\{(x,y),(y,x)\} \cup \Delta_A$ порождённые (при $x \neq y$) элементами $(x,y) \in A \times A$, согласно условиям симметричности и рефлексивности. В частности, элемент $(a,b) \in A \times A$ порождает эквиваленцию $\theta_1 = \{(a,b),(b,a)\} \cup \Delta_A$ и аналогично строится эквиваленция $\theta_2 = \{(b,c),(c,b)\} \cup \Delta_A$. При этом очевидно, согласно построению, что простое объединение $\theta_1 \cup \theta_2 \in \mathcal{B}(A \times A)$ симметрично и рефлексивно, но *не является эквиваленцией*, так как $\{(a,b),(b,c)\} \subseteq \theta_1 \cup \theta_2$, но элемент $(a,c) \in A \times A$ не попадает в $\theta_1 \cup \theta_2$ и потому нарушается условие транзитивности.

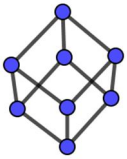
Это заканчивает доказательство предложения, так как строится и эквиваленция $\theta_1 \vee \theta_2 \in \mathcal{E}(A)$ (наименьшая среди $\theta \in \mathcal{E}(A)$ таких, что $\theta_1 \subseteq \theta$ и $\theta_2 \subseteq \theta$), но $(a,c) \in \theta_1 \vee \theta_2$ и потому$\theta_1 \cup \theta_2 \neq \theta_1 \vee \theta_2$.

**Следствие.** Если $A = \{a,b,c\}$, то возникает *точно 3 минимальныхэквиваленции* – это построенные $\theta_1, \theta_2$ и эквиваленцция $\theta_3 = \{(c,a),(c,c)\} \cup \Delta_A$. Приэтом получаются выписанные равенства и диаграмма, дающие «наглядное представление» соответствующей решётки$\mathcal{E}(\{a,b,c\})$эквивиленций из 5 элемнетов – вместе с $\Delta_A$ и $A \times A$.



$$\theta_1 \cap \theta_2 = \theta_2 \cap \theta_3 = \theta_3 \cap \theta_1 = \Delta_A$$
$$\theta_1 \vee \theta_2 = \theta_2 \vee \theta_3 = \theta_3 \vee \theta_1 = A \times A$$

В полной решётке $\mathcal{B}(A)$ тоже имеется точно 3 минимальных элемента – это $\{a\},\{b\},\{c\}$, но получается 8 элементов, вместе с максимальными элементами – дополнениями минимальных, наибольшим элементом $A$и наименьшим элементом $\emptyset$,что «наглядно представляет» выписанная диаграмма этой полной решётки$\mathcal{B}(\{a,b,c\})$.А выписанные равенства «отражают специфику» решётки $\mathcal{E}(A)$по сравнению с полными решётками$\mathcal{B}(A \times A)$ и $\mathcal{B}(A)$.



Всё отмеченное фактически «уже доказано», так как минимальные эквиваленции уже построены в доказательстве предложения. Конечно, нужно учесть и то, что для $A = \{a, b, c\}$его квадрат $A \times A$имеет точно 9 элементов – кроме элементов $(a, a), (b, b), (c, c) \in \Delta_A$возникают ещё $(a, b), (b, a), (b, c), (c, b), (a, c), (c, a)$ и потому получается только 3 минимальных элемента эквиваленции – это $\theta_1, \theta_2, \theta_3$. Одновременно получаются выписанные равенства и оказывается, что
$\theta_3 \cap (\theta_1 \vee \theta_2) = \theta_3 \neq \Delta_A = (\theta_3 \cap \theta_1) \vee (\theta_3 \cap \theta_2)$,хотя
$\theta_3 \cap (\theta_1 \cup \theta_2) = (\theta_3 \cap \theta_1) \cup (\theta_3 \cap \theta_2)$ в $\mathcal{B}(A)$, так как в полной решётке $\mathcal{B}(A \times A)$ всегда справедливы соответствующие «законы дистрибутивности пересечений относительно объединений». А это уже отражает специфику решётки $\mathcal{E}(A)$ эквиваленций.

Продолжая уточнять специфику эквиваленций мы естественно приходим к ещё одной «общей конструкции», учитывая специфику полных решёток $\mathcal{B}(A)$ . А именно, для не одноэлементного множества $A$ всегда возникают «не тривиальные» разбиения – представления $A = \bigcup A_i$ в виде объединения *попарно не пересекающихся и различных подмножеств*. С другой стороны, если построенаэквиваленция $\theta \in \mathcal{E}(A)$, то с каждым элементом $a \in A$ всегда *однозначно* связывается, согласно выписанному правилу, множество $\hat{a} \subseteq A$ из всех элементов эквивалентных $a$относительно $\theta$.

$$A \ni a \rightsquigarrow \hat{a} = \{x \in A | x\theta a\} \in \mathcal{B}(A)$$

При этом можно считать «для нетривиальности», что $\theta \neq A \times A$.

**Предложение 3.** Вместе с эквиваленцией $\theta \neq A \times A$ всегда строится *фактор-множество* $\hat{A} = A/\theta$ *множества* $A$ *по эквиваленции* $\theta$– его элементами являются классы $\hat{a}$

эквивалентности с правилом равенства: $\hat{x} = \hat{a}$ тогда и только тогда, когда $x\theta a$. При этом всегда $a \in \hat{a}$, возникают различные классы эквивалентности и $\hat{x} \cap \hat{y} = \emptyset$, когда $\hat{x} \neq \hat{y}$. Поэтому получается *разбиение* множества $A$ на эти классы эквивалентности, а по разбиению *однозначно* восстанавливается соответствующаяэквиваленция$\theta$.

Действительно, для эквиваленции $A \times A$любые два элемента из $A$эквивалентны и потому можно считать, что заданная эквиваленция $\theta \neq A \times A$. В этой ситуации конечно получается, что множество $A$не одноэлементно и возникают элементы $(x, y) \in A \times A$не попадающие в $\theta$, то есть не эквивалентные относительно $\theta$. Но тогда, согласно указанному построению классов $\hat{a}$ эквивалентности, элемент $x \in \hat{x}$ и этот элемент не попадает в $\hat{y}$, и потому $\hat{x} \neq \hat{y}$ – построенное *фактор-множество* $\hat{A} = A/\theta$ оказалось не одноэлементным, так как оно состоит из всех классов эквивалентности.

Благодаря рефлексивностиэквиваленции$\theta$получается, что всегда $a \in \hat{a}$ и поэтому все классы эквивалентности непусты, причём их объединением конечно будет всё множество $A$. С другой стороны, если $\hat{x} \cap \hat{a} \neq \emptyset$,то найдётся элемент $z \in \hat{x} \cap \hat{a}$ и получится, что $z\theta x$ и $z\theta a$. Но тогда из-за симметричности и транзитивности эквиваленции $\theta\,\theta$ получается, что $x\theta a$ и $a\theta x$, а потому получается, что $\hat{x} = \hat{z} = \hat{a}$. В итоге оказалось, что $\hat{x} = \hat{a}$тогда и только тогда, когда $x\theta a$ (и это является правилом равенства на фактор-множестве $\hat{A} = A/\theta$ ), но одновременно получилось, что$\hat{x} \cap \hat{y} = \emptyset$,когда $\hat{x} \neq \hat{y}$.

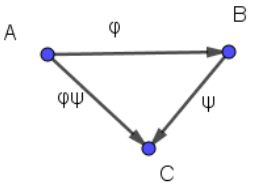
В результате получилось и «не тривиальное» разбиение $A = \bigcup A_i$, где $A_i$ пробегает все классы эквивалентности – все эти подмножества $A_i$ непусты и попарно не пересекаются. Учитывая специфику разбиения строится соответствующее отношение эквивалентности – элементы $x, a \in A$ эквивалентны тогда и только тогда, когда они попадают в некоторое $A_i$ (единственное $A_i \supseteq \{x, a\}$). Рефлексивность,

симметричность и танзитивность построенного бинарного отношения легко проверяется (элемент $a \in A = \bigcup A_i$ попадает в некоторое $A_i$ и поэтому $a$эквивалентно$a$, затем учитывается, что$\{x, a\} = \{a, x\}$ и так далее). Остаётся заметить, что по разбиению $A$ на классы $\hat{a}$ эквивалентности «однозначно восстанавливается» именно заданная эквиваленция $\theta$на $A$(или отношение равенства на соответствующем фактор-множестве).

Согласно этому предложению, эквиваленции на одноэлементном множестве $A$*в точности соотвеиствуют разбиениям* этого множества. В частности тривиальному разбиению $A = A$ соответствует «тривиальная» эквиваленция $A \times A$, а разбиению $A = \bigcup\{\{a\}|a \in A\}$– эквиваленция $\Delta_A$ . Менее счевидно, что *точно описываются максимальные эквиаленции* (больше которых только $A \times A$,) – *они соответствуют разбиениям* $A = A_1 \cup A_2$, где конечно $A_1 \neq \emptyset \neq A_2$, но $A_1 \cap A_2 = \emptyset$. *Однако* это уточняется после уточнения специфики отображений рассматриваемого множества $A$на другие множества.

Вместе с непустыми множествами $A, B$ , всегда непусто и *множество* $Mor(A, B)$ *всех отображений* $\varphi: A \to B$ . При этом учитывается, что отображение $\varphi: A \to B$ задано, если для каждого элемента $a \in A$*однозначно* указан элемент $a\varphi = b \in B$ (образ элемента $a$ при отображении $\varphi$ ). Поэтому как правило, возникают разнообразные отображения $\varphi_1, \varphi_2 \in Mor(A, B)$ равны тогда и только тогда, когда $a\varphi_1 = a\varphi_2$ для всех $a \in A$. В частности, можно учесть отображении $O_b^A \in Mor(A, B)$ действующее по правилу: $aO_b^A = b$ для всех $a \in A$и соответствующего $b \in B$. При этом конечно получается, что $O_b^A = O_c^A$ $0_b^A = 0_c^A$ тогда и только тогда, когда $b = c$ , но если множества $A$и $B$не одноэлементны, то конечно возникают и другие отображения множества $A$в множество $B$.

Благодаря указанной специфике, можно умножать согласованные $\varphi \in Mor(A,B), \psi \in Mor(A,C)$– получается произведение $\varphi\psi \in Mor(A,C)$, согласно выписанной диаграмме




или после последовательного применения, то есть согласноправилу $a(\varphi\psi) = (a\varphi)\psi \in C$ для всех $a \in A$. Нужно только иметь в виду, что перемножаются именно «согласованные» отображения (как в диаграмме). После этого легко увидеть, что для соответствующихсогласованных отображений всегда справедливы равенства $(\varphi\psi)\rho = \varphi(\psi\rho)$ (или законы ассоциативности умножения), а если учесть тождественные отображения, то получаются равенства $\varepsilon_A\varphi = \varphi = \varphi\varepsilon_B$.

Уточняя специфику отображения $\varphi: A \to B$ можно учесть его *ядро* $\sigma_\varphi = \{(x,y) \in A \times A | x\varphi = y\varphi\}$ и *образ* $A\varphi = \{a\varphi | a \in A\} \subseteq B$, конечно являющийся *непустым* подмножеством множества $B$. Если для отображения $\nu: A \to R$ получилось равенство $A\nu = R$, то говорят, что $\nu$*сюрьекция*, как отображение множества $A$ на множество $R$. Если же $\sigma_\varphi = \Delta_A$, то получается, что $x\varphi = y\varphi$ тогда и только тогда, когда $x = y$ и тогда говорят, что – $\varphi$ *инъекция* (вложение) множества $A$ в множество $B$, как взаимно однозначное отображение множества $A$на его образ $A\varphi \subseteq B$.

Если же для отображения $\mu: R \to C$ одновременно справедливы равенства $R\mu = C$ и $\sigma_\mu = \Delta_R$, то есть $\mu$ является сюрьекцией и инъекцией, то $\mu$– биекция, как взаимно однозначное отображение множества $R$на множество $C$. В этом случае получается, что вместе с

$\mu: R \to C$ однозначно строится *обратное* $\mu^{-1}: C \to R$ (тоже являющееся биекцией), согласно переходам $r \rightsquigarrow r\mu = c \rightsquigarrow c\varphi^{-1} = r$. А если учесть «согласованность» этих отображений, то конечно получаются равенства $\mu\mu^{-1} = \varepsilon_R$, $\mu^{-1}\mu = \varepsilon_C$ для соответствующих тождественных отображений ($r\varepsilon_R \equiv r$ и аналогично для $\varepsilon_C$). При этом тождественные отображения конечно являются биекциями, но «весьма специальными», так как получается равенство $\varepsilon = \varepsilon^{-1}$.

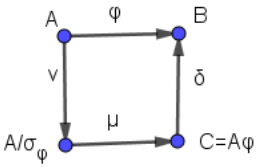
**Предложение 4**. Образы отображений в множество $B$ – это в точности все его *непустые* подмножества $C \subseteq B$. Ядра отображений множества $A$ – это в точности все эквиваленции $\theta \subseteq A \times A$ на множестве $A$. В частности, ядром «нулевых» отображений $O_b^A: A \to \{b\}$ является $A \times A$.

Действительно, если $\emptyset \neq C \subseteq B$, то можно учесть *тождественное вложение* $\varepsilon_B^C: C \to B$ (такое, что $c\varepsilon_B^C = c \in B$) и уже отмечено, что образ $A\varphi$ отображения $\varphi: A \to B$ конечно является непустым подмножеством $A\varphi \subseteq B$. Чуть сложнее увидеть, что ядро $\sigma_\varphi$ отображения $\varphi: A \to B$ является эквиваленцией на $A$ (так как всегда $x\varphi = x\varphi$, если $x\varphi = y\varphi$,, то $y\varphi = x\varphi$ и так далее). Поэтому остаётся доказать, что каждая экавиваленция $\theta \neq A \times A$ является ядром некоторого отображения множества $A$ на не одноэлементное множество.

Но для произвольной эквиваленции $\theta \neq A \times A$ уже построено (в предложении 3) соответствующее не одноэлементное *фактор-множество* $A/\theta = \hat{A}$, состоящее из классов $\hat{a}$ эквивалентности относительно $\theta$. Но на самом деле уже построено и *естественное отображение* $\nu_\theta: A \to \hat{A} = A/\theta$ – с каждым элементом $a \in A$ однозначно строится $a\nu_\theta = \hat{a} \in \hat{A}$. При этом для $\nu = \nu_\theta$ оказалось, что $x\nu = \hat{x} = \hat{y} = y\nu$ тогда и только тогда, когда $x\theta y$. Поэтому ядро $\sigma_\nu = \theta$, согласно построению и определениям, что заканчивает доказательство.

В итоге оказалось, что в этом предложении «дана характеристика» ядер $Ker\varphi = \sigma_\varphi$ и образов $Im\varphi = A\varphi$ произвольных отображений $\varphi: A \to B$ как эквиваленций на $A$ и непустых подмножеств в $B$, соответственно. При этом построены и некоторые «специальные» отображения – естественные отображения $\nu_\theta: A \to A/\theta$ (являющиеся сюръекциями) и тождественные вложения $\varepsilon_B^C: C \to B$. Кроме того, можно учесть и умножение «согласованных» отображений.

**Теорема 2.** Вместе с отображением $\varphi: A \to B$ учтём его образ $C = A\varphi$, ядро $\sigma = \sigma_\varphi$, вложение $\delta = \varepsilon_B^C: C \to B$ и естественное отображение $\nu = \nu_\sigma: A \to \hat{A} = A/\sigma$, а затем учтём и умножение «согласованных» отображений. Тогда получается выписанная диаграмма связывающая указанные отображения – *существует и единственное такое отображение* $\mu: \hat{A} \to C$, что $\varphi = \nu\mu\delta$.




Более того, возникающее отображение $\mu$ оказывается взаимно однозначным (или биекцией), а потому, конечно, строится и обратное отображение
$\varphi^{-1}: A\varphi \to A/\sigma_\varphi$, то есть «образы множества $A$являются его фактор-множествами по соответствующим эквиваленциям» с точностью до биекций.

**Доказательство.** По построению ядер отображений и естественных отображений на фактор-множества, получаются равенства
$\sigma_\nu = \sigma = \sigma_\varphi$ и это можно переписать в виде импликаций

$$a\nu = \hat{a} = \hat{x} = x\nu \Leftrightarrow a\sigma x \Leftrightarrow a\varphi = x\varphi.$$

После этого получается, что если нужное $\mu$ (такое, что $\varphi = \nu\mu\delta$) существует, то оно *должно действовать* согласно построению умножения согласованных отображений, именно по правилу $(*)$, где учтено построение естественного отображения $\nu: A \to \hat{A} = A/\sigma$ и вложения $\delta: C \to B$.

$$\forall a \in A | \hat{a}\mu = a\varphi = c \equiv c\delta \qquad (*)$$

Но оказывается, что правило $(*)$ корректно, благодаря отмеченным импликациям, и поэтому действительно строится *единственное* $\mu: \hat{A} \to C = A\varphi$, указанное в диаграмме, так как переходы $a \to a\nu = \hat{a} \to \hat{a}\mu = a\varphi = c \equiv c\delta$ и приводят к равенству $\varphi = \nu\mu\delta$. После этого получается, снова согласно указанным импликациям и правилу $(*)$, что построенное отображение $\mu: \hat{A} \to C$ взаимно однозначно, и поэтому строится и обратное отображение $\mu^{-1}: C \to \hat{A}$, как «каноническая» биекция $A\varphi \approx A/\sigma_\varphi$ между образами отображения множества $A$ и его фактор-множествами по соответствующим эквиваленциям.

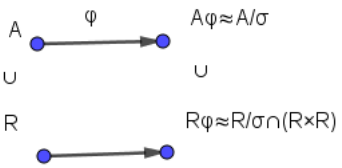
**Теорема 3.** Для непустого подмножества $R$ множества $A$ его *образ* $R\varphi = \{r\varphi | r \in R\}$ при отображении $\varphi: A \to A\varphi$ конечно является непустым подмножеством множества $A\varphi$, а из эквиваленции $\sigma \subseteq A \times A$ на $A$ всегда получается эквиваленция $\sigma \cap R \times R$ на $R$. После этого вместе с биекцией $A\varphi \approx \frac{A}{\varphi}$ строятся и «канонические» биекции $R\varphi \approx \frac{R}{\sigma} \cap (R \times R)$,, а для указанного «перехода к образам» очевидны импликации $R_1 \subseteq R_2 \Rightarrow R_1\varphi \subseteq R_2\varphi$. С другой стороны, для непустого подмножества $\bar{R} \subseteq A\varphi$ строится его *полный прообраз* $\varphi^{-1}(\bar{R}) = \{a \in A | a\varphi \in \bar{R}\} \subseteq A$ и получается равенство $\left(\varphi^{-1}(\bar{R})\right)\varphi = \bar{R}$, то есть *все непустые подмножества множества* $A\varphi$ *являются образами некоторых непустых подмножеств множества*

$A$. А если учесть, что для классов $\hat{a}$ эквивалентности относительно эквиваленции $\sigma = \sigma_\varphi$ всегда справедливо равенство $\hat{a} = \varphi^{-1}(\{a\varphi\})$, то получаются и соотношения

$$R \subseteq \varphi^{-1}(R\varphi) = \hat{R} = \bigcup \{\hat{r} | r \in R\}$$

для всех непустых подмножеств $R \subseteq A$, вместе с равенством $\hat{R}\varphi = R\varphi$. Одновременно получается *взаимно однозначное* соответствие между непустыми подмножествами множества $A\varphi$ и *возникающими* «насыщенными» подмножествами $\hat{R}$.

Действительно, согласно указанному построению, образы $R\varphi$ непустых подмножеств $R \subseteq A$ при отображении $\varphi: A \to A\varphi$ конечно являются непустыми подмножествами множества $A\varphi$. После этого можно учесть «индуцированные» отображения $\bar{\varphi}: R \to R\varphi = \bar{R}$, действующие, конечно, по правилу $r\bar{\varphi} = r\varphi$ для всех$r \in R$. При этом получится, конечно, равенство $\sigma_{\bar{\varphi}} = \sigma_\varphi \cap (R \times R)$, а для «наглядности»можно учесть выписанную диаграмму.




можно учесть выписанную диаграмму. Поэтому оказывается справедливо первое утверждение теоремы, а вместе с биекцией, согласно $A\varphi \approx A/\sigma$ строится соответствующая биекция $R\varphi \approx R/\sigma \cap (R \times R)$, согласно теореме 2. Кроме того, снова «по построению образов подмножеств», очевидны и импликации

$$R_1 \subseteq R_2 \subseteq A \Rightarrow R_1\varphi \subseteq R_2\varphi \subseteq A\varphi.$$

Не менее очевидно, согласно указанному построению, что полные прообразы $\varphi^{-1}(R) = \{a \in A | a\varphi \in \bar{R}\}$ непустых подмножеств $\bar{R} \subseteq A\varphi$ являются непустыми подмножествами в $A$, причём конечно получаются и равенства $\left(\varphi^{-1}(\bar{R})\right)\varphi = \bar{R}$ и имликации

$$\overline{R_1} \subseteq \overline{R_2} \subseteq A\varphi \Rightarrow \varphi^{-1}(\overline{R_1}) \subseteq \varphi^{-1}(\overline{R_2}) \subseteq \varphi^{-1}(A\varphi) = A.$$

Но тогда, согласно «очевидным» импликациям при переходе к образам, получаются и обратные импликации

$$\varphi^{-1}(\overline{R_1}) \subseteq \varphi^{-1}(\overline{R_2}) \Rightarrow \overline{R_1} \subseteq \overline{R_2},$$

то есть получилось взаимно однозначное соответствие между непустыми подмножествами $\bar{R} \subseteq A\varphi$ и их полными прообразами $\varphi^{-1}(\bar{R}) \subseteq A$.

Но по построению эквиваленции $\sigma = \sigma_\varphi$ и соответствующих классов $\hat{a}$ эквивалентности, всегда $a \in \hat{a}$ и легко понять, что $x \in \varphi^{-1}(\{a\varphi\}) \Leftrightarrow x\varphi = a\varphi \Leftrightarrow x \in \hat{a}$, то есть справедливо равенство $\varphi^{-1}(\{a\varphi\}) = \hat{a}$. Именно поэтому оказываются справедливыми соотношения $R \subseteq \varphi^{-1}(R\varphi) = \hat{R} = \cup\{\hat{r} | r \in R\}$, то есть получаются «насыщенные» относительно $\sigma = \sigma_\varphi$ непустые подмножества множества $A$, которые и являются полными прообразами непустых подмножеств множества $A\varphi$.

Это заканчивает доказательство теоремы и одновременно получилось, что $R/\sigma \cap (R \times R) \approx R\varphi = \hat{R}\varphi \approx \hat{R}/\sigma \cap \left(\hat{R} \times \hat{R}\right)$, согласно сказанному в начале доказательства.

## §3. Общие конструкции и теоремы о подсистемах и гомоморфизмах алгебраических систем

Согласно договорённостям, специфика алгебраических операций уже указана – это *-арные* операции на рассматриваемых непустых множествах, а *алгебраическая система* – это непустое множество $A$ с некоторым набором $\Omega$ алгебраических операций или $\Omega$-*алгебра*. Набор $\Omega$ обычно предполагается непустым, чаще применяют бинарные $\mu: A \times A \to A$ операции и унарные $\xi: A \to A$, но иногда учитывают и *нуль-арные* операции, которые просто «фиксируют» в алгебраической системе $A = A(\Omega)$ некоторые элементы.

Вместе с заданной алгебраической системой $A = A(\Omega)$ можно строить *её подсистемы* или $\Omega$-*подалгебры*, как непустые подмножества $B \subseteq A$, замкнутые относительно операций из $\Omega$. Таким образом, например, если операция $\omega \in \Omega$ бинарная, то $(b_1, b_2)\omega = b \in B$ для любых $b_1, b_2 \in B$ и аналогично для остальных операций из $\Omega$, а если в $\Omega$ имеется *нульарная* операция, то зафиксированный ею элемент должен попадать в эту подсистему. Одновременно получится, конечно, что все подсистемы являются $\Omega$-*алгебрами* вместе с $A = A(\Omega)$.

Можно строить *гомоморфизмы* $\varphi: A \to R$ или $\Omega$-*гомоморфизмы*, как отображения, согласованные с операциями из $\Omega$ или «сохраняющие» операции. Таким образом, например, если имеется унарная операция $\xi \in \Omega$, то $(a\xi)\varphi = (a\varphi)\xi \in R$, если же операция $\omega \in \Omega$, то $\big((a_1, a_2)\omega\big)\varphi = (a_1\varphi, a_2\varphi)\omega \in R$ и аналогично для остальных операций. Одновременно получится, что *гомоморфный образ* $A\varphi = \{a\varphi | a \in A\}$ *является подсистемой в* $R = \Re(\Omega)$, согласно указанным «общим» определениям. Не менее очевидно, что если гомоморфизм $\varphi: A \to R$ является биекцией или взаимно однозначен, то обратное отображение $\varphi^{-1}: R \to A$ тоже является гомоморфизмом и биекцией, а в этом случае говорят, что $\varphi$ и $\varphi^{-1}$ задают *изоморфизмы*

$A \approx R$ и $R \approx A$, которые «сохраняют» все операции и свойства этих алгебраических систем.

Продолжая «специализацию» общих конструкций непустых множеств на однотипные алгебраические системы (с одинаковым набором $\Omega$ алгебраических операций), можно учесть, что для любого непустого семейства $\Omega$ -*алгебр* $A_i$ соответствующее декартово *произведение* $\mathcal{D} = \prod_i A_i$ *превращается в* $\Omega$-*алгебру*, *если переносить операции «покомпонентно»*. А именно: если мы построили, например, декартово произведение $A \times B = \{(a, b) | a \in A, b \in B\}$ и «переносим» тернарную или 3-арную операцию $\omega \in \Omega$, то получаются (по построению) равенства

$$\big((a_1, b_1), (a_2, b_2), (a_3, b_3)\big)\omega = \big((a_1, a_2, a_3)\omega, (b_1, b_2, b_3)\omega\big) \in A \times B$$

и аналогично для остальных операций из $\Omega$. После этого можно учесть, что и квадрат $A \times A$ заданной $\Omega$-*алгебры* $A$ тоже «превращается» в $\Omega$-*алгебру*, согласно сказанному.

Одним из простейших примеров алгебраических систем можно считать *множества* $A$ *с выделенным непустым подмножеством* $O$, элементы которого можно рассматривать как результаты *нульарных* операций. Для таких алгебраических систем $A = A(O)$ подсистемы конечно образуют решётку $\mathcal{B}_0(A)$ из подмножеств $B \supseteq O$, строятся обычные (как в полной решётке $\mathcal{B}(A)$ всех подмножеств) пересечения $\bigcap B_i \supseteq O$ и объединения $\bigcup B_i \in \mathcal{B}_0(A)$, хотя наименьшей подсистемой оказывается $O \in \mathcal{B}_0(A)$. Если $A \neq O$, то конечно получается, что некоторые непустые $X \subseteq A$ не являются подсистемами, но они «порождают» соответствующие подсистемы $X \cup O \in \mathcal{B}_0(A)$. А если $O = \{0\}$, то получаются «уже построенные» полные решётки $\mathcal{B}_0(A)$, можно учесть, что строятся гомоморфизмы и это просто такие отображения $\varphi: A \to R$, что $0\varphi = 0$ для отмеченной точки.

В общем случае алгебраических систем $A = A(\Omega)$ ситуация оказывается более сложной, а учитывая сказанное выше, можно предполагать «для нетривиальности», что набор $\Omega$ не только непуст, но

*имеются -арные операции* $\omega \in \Omega$ *для некоторых* $n \geq 1$, хотя возможны и *нульарные* операции (что оговаривается особо – может и не быть *нульарных*операций в Ω).

**Теорема 4.** Для произвольно заданной алгебраической системы $A = A(\Omega)$ её *подсистемы образуют решётку* $\mathcal{B}_\Omega(A)$ с наибольшим элементом $A \in \mathcal{B}_\Omega(A)$ и обычными пересечениями (как в полной решётке $\mathcal{B}(A)$. *Точнее*, для произвольного непустого семейства подсистем $B_i \in \mathcal{B}_\Omega(A)$ пересечение $\bigcap B_i = C$ *будет подсистемой, когда оно непусто* (так как подсистемы всегда непусты, как Ω-*алгебры*!). После этого получается, что для любого непустого $X \subseteq A$ всегда строится *подсистема* $\langle X \rangle_\Omega$ , *порождённая заданным* $X \in \mathcal{B}(A)$ , как наименьшая среди подсистем, содержащих $X$ , согласно выписанному правилу.

$$\emptyset \neq X \subseteq A \Rightarrow \bigcap \{B \in \mathcal{B}_\Omega(A) | B \supseteq X\} = \langle X \rangle_\Omega \in \mathcal{B}_\Omega(A)$$

Поэтому и для любого непустого семейства подсистем $B_i$ всегда существует $\vee B_i = \langle \cup B_i \rangle_\Omega$ и это «объединение подсистем $B_i \in \mathcal{B}_\Omega(A)$ как подсистем», то есть *наименьшая среди подсистем содержащих все заданные* $B_i$ .Отмеченное и позволяет говорить, что построена решётка $\mathcal{B}_\Omega(A)$ , благодаря пересечениям $\bigcap B_i$ , хотя иногда $\bigvee B_i \neq \bigcup B_i$ . Может не быть и наименьшей подсистемы, но если среди операций из Ω имеются *нульарные*, то зафиксированные ими элементы «порождают» наименьшую подсистему.

**Доказательство.** Согласно уже сказанному «общему» определению, подсистемы в $A = A(\Omega)$ – это её *непустые* подмножества, замкнутые относительно всех операций из Ω . Поэтому и оказывается, что пересечение $\bigcap B_i = C$ подсистем $B_i$ является подсистемой, когда

$C \neq \emptyset$. Но если «пересечение иногда пусто», то можно и пустое подмножество объявить подсистемой, чтобы эти пересечения всегда существовали. Поэтому оказалось, что *подсистемы образуют систему* $\mathcal{B}_\Omega(A) \subseteq \mathcal{B}(A)$ *замыкания* из-за наибольшего элемента $A \in \mathcal{B}_\Omega(A)$ и обычных пересечений. После этого можно учесть и соответствующий оператор $X \rightsquigarrow \langle X \rangle_\Omega \in \mathcal{B}_\Omega(A)$ замыкания непустых $X \subseteq A$, который и указан в теореме (сравните со сказанным в следствии из теоремы 1). Благодаря этому оператору и построены соответствующие «объединения $\vee B_i = \langle \cup B_i \rangle_\Omega \in \mathcal{B}_\Omega(A)$подсистем как подсистем» для любых $B_i \in \mathcal{B}_\Omega(A)$.

Отмеченное уже позволяет считать, что подсистемы образуют решётку $\mathcal{B}_\Omega(A)$ , с наибольшим элементом $A$ и обычными пересечениями, но «объединениями $\vee B_i$ подсистем как подсистем» (как это сделано в следствии из теоремы 1 для соответствующих систем замыкания в $\mathcal{B}(A)$. При этом иногда $\vee B_i \neq \cup B_i$, то есть простое объединение подсистем может не быть подсистемой – это зависит, конечно, от специфики алгебраической системы $A = A(\Omega)$ и «показывается на конкретных примерах» (что будет сделано немного позже, хотя имеются и «школьные» примеры). Кроме того, наименьшей подсистемы может не быть, но если среди операций из$\Omega$имеются *нульарные*, то наименьшая подсистема возникает, что и отмечено в теореме.

После этой теоремы можно уточнять построение подсистемы $\langle X \rangle_\Omega$ как «порождённой» заданным непустым подмножеством $X$ в алгебраической системе $A = A(\Omega)$. Но на самом деле оказывается, что $\langle X \rangle_\Omega$ строится как замыкание соответствующего непустого подмножества *с помощью всех операций из*$\Omega$, и поэтому зависит от специфики этих операций. Чтобы это «показать на примерах», можно учесть построение некоторых *весьма специальных* алгебраических систем, которые и уточняют «процесс порождения», благодаря

договорённости о наборе $\Omega$ применяемых алгебраических операций (указанной перед теоремой).

Учтём, что мы строим только непустые множества и возьмём произвольный *алфавит* $X$ – непустое множество, в котором «различаются» его элементы или *буквы*. Обычно это делается для не одноэлементного алфавита, с помощью «нумерации» его элементов и тогда $X = \{x_i | i \in I\}$, где при точной нумерации получается, что $x_i = x_j \Leftrightarrow i = j$. Затем строим *слова над алфавитом* $X$– это конечные последовательности или строка $y_1 \dots y_k = w$ конечной длины $d(w) = k \geq 1$ $d(w) = k \geq 1$, составленные из букв (причём возможны и «повторения», как в словах $x_i x_i$ или $x_i x_i x_i$, например).

Слова различаем «по записи и буквам», то есть, считаем, что $y_1 \dots y_k = z_1 \dots z_m$, но при этом $k = m$, а если $k \geq 2$, то должны выполняться и равенства $y_1 = z_1, \dots y_k = z_k$ для указанных букв. В результате строится *множество* $S(X)$ *слов над* $X$, конечно непустое вместе с алфавитом $X$ (и даже бесконечное, так как уже слова$x, xx, xxx, \dots$различны по длине).

Теперь учтём договорённость о наборе $\Omega$ применяемых алгебраических операций – эти операции мы тоже «должны различать» по их действию, причём предполагается, что *имеются* $\omega \in \Omega$ *-арные операции для некоторых* $n \geq 1$ (хотя возможны и *нульарные* операции, что оговаривается особо). Поэтому и множество $\Omega$операций или их символов можно считать алфавитом, вместе с алфавитом $X$, но конечно считаем, что «операции не являются буквами из $X$и наоборот», то есть считаем, что $X \cap \Omega = \emptyset$. После этого строится возникающий алфавит $X \cup \Omega$ и множество $S(X \cup \Omega)$ слов над этим алфавитом.

Для построения «нужной специальной $\Omega$ *-алгебры*», учтём однозначную запись всех слов над $X \cup \Omega$, но будем выбирать или строить более *специальные* $\Omega$*-слова над* $X$, последовательно или по индукции. Начиная «индуктивный процесс» их порождения, просто *объявляем* $\Omega$ *-словами* буквы алфавита $X$ и символы *нульарных*

операций, если такие есть в Ω. В результате в $S(X \cup \Omega)$ выделяется непустое подмножество $W_0$ из указанных «простейших» Ω -*слов*, причём $X \subseteq W_0$, а если в Ω нет *нульарных* операций, то $W_0 = X$.

Затем учитываем, что *имеются n-арные* $\omega \in \Omega$ для некоторых $n \geq 1$ (по договорённости!), но такие Ω не участвуют в записи слов из $W_0$, и поэтому *не попадают* в $W_0$ соответствующие слова $y_1 \dots y_n\omega$, где $y_i \in W_0$, но «последней буквой» является $\omega$. Эти слова *объявляем* Ω-*словами* и получаем множество

$$W_1 = W_0 \cup \{y_1 \dots y_n\omega | y_i \in W_0, \omega \in \Omega\} \neq W_0,$$

так как к $W_0$ добавлены указанные «новые» Ω-*слова* над $X$, в записи которых участвуют и не *нульарные* $\omega \in \Omega$, и поэтому и не попадающие в $W_0$.

Поясняя отмеченное и считая, например, что операция $\omega \in \Omega$ бинарна, а затем, учитывая буквы из $X$, мы получаем Ω -*слово* $xy\omega \in W_1$, которое не попадает в $W_0$, затем можно построить и слово $xy\omega x\omega$, которое уже не попадает в $W_1$, а слова $x\omega$, $y\omega$ просто не являются Ω-*словами*, так как операция $\omega$бинарная. После этого можно уточнить «индуктивный переход» от уже построенного множества $W_m$ Ω -*слов* к следующему множеству $W_{m+1}$, снова учитывая однозначность записи слов и только не *нульарные* $\omega \in \Omega$, как это уже сделано при переходе от $W_0$ к $W_1$.

А именно, если операция $\omega \in \Omega$ имеет арность $n \geq 1$ и уже построены Ω -*слова* $a_1, a_2, \dots, a_n \in W_m$, но хотя бы одно из них не попадает в $W_{m-1}$, то слово $a_1, \dots a_n\omega$ *не попадает* в $W_m$, но мы объявляем его Ω-*словом*над $X$. Затем строится множество

$$W_{m+1} = W_m \cup \{a_1 \dots a_n\omega | a_i \in W_m, \omega \in \Omega\} \neq W_m,$$

так как мы добавили указанные «новые» Ω-*слова* над $X$. В результате указанного «индуктивного процесса» строится цепочка

$$X \subseteq W_0 \subseteq W_1 \subseteq \cdots \subseteq W_m \subseteq W_{m+1} \subseteq \cdots,$$

а затем и множество $\bigcup_m W_m = \mathcal{W}(X, \Omega)$ *всех* Ω-*слов над* $X$, то есть считаем, что Ω-*слова* – это именно слова из $S(X \cup \Omega)$, построенные в

ходе указанного «процесса порождения» подмножеств слов $W_m$ вместе с точной записью Ω-*слов*.

Благодаря указанному «процессу порождения» легко заметить, что на множестве $\mathcal{W}(X,\Omega)$ строятся все операции из $\Omega$. А именно: для *-арной* операции $\omega \in \Omega$ и любых $a_1, \dots, a_n \in \mathcal{W}(X,\Omega)$ всегда найдётся соответствующее подмножество $W_m$, как «первое» содержащее все указанные $\Omega$-*слова* $a_i$, а после этого строится и соответствующее $\Omega$-*слово* $a_1 \dots a_n\omega$, как однозначный «результат» применения этой $n$-арной операции $\omega \in \Omega$ (при $n \geq 1$), то есть по правилу

$$(a_1 \dots a_n)\omega = a_1 \dots a_n\omega \in \mathcal{W}(X,\Omega).$$

А если в Ω есть *нульарные* операции, то они «просто фиксируют» свой символ, который в этой ситуации имеется в $W_0$.

Отмеченное показывает, что уже построена «весьма специальная» Ω-*алгебра* $W = \mathcal{W}(X,\Omega)$ из Ω-*слов над* $X$, вместе с указанным «почти очевидным» построением соответствующих операций из Ω. Не менее очевидно, что справедливо равенство $\mathcal{W}(X,\Omega) = \langle X\rangle_\Omega$, то есть эта $\Omega$ *-алгебра порождается своим непустым подмножеством* $X$, благодаря однозначной записи или «порождению» Ω-*слов* над $X$. Более того, можно заметить, что благодаря указанному «процессу порождения» $\Omega$ *-слов*каждое непустое $Y \subseteq X$ порождает в $\mathcal{W}(X,\Omega)$подсистему из Ω-*слов* над $Y$и поэтому оказывается, что $\mathcal{W}(X,\Omega) = \langle X\rangle_\Omega$ является подсистемой в $\mathcal{W}(X,\Omega) = \langle X\rangle_\Omega$.

Благодаря отмеченному строятся «примеры», о которых говорилось в теореме и конце её доказательства, причём именно из-за специфики $\Omega$ *-алгебры* $\mathcal{W}(X,\Omega)$ и существования в $\Omega$ не *нульарных* операций (сравните с уже построенными алгебраическими системами $A(O)$, где применялись только нульарные операции). При этом будем считать, что алфавит $X$имеет хотя бы два элемента, и поэтому его можно разбить – представить в виде $X = X_1 \cup X_2$, где $X_1 \cap X_2 = \emptyset$, хотя $X_1 \neq \emptyset \neq X_2$.

Применяя это разбиение получаем, конечно, что подсистемы $\langle X_1\rangle_\Omega \equiv \mathcal{W}(X_1,\Omega)$ и $\langle X_2\rangle_\Omega \equiv \mathcal{W}(X_2,\Omega)$ различны, так как $X_1 \neq X_2$. Более того, *если в* Ω*нет нульарных операций*, то получается равенство $\langle X_1\rangle_\Omega \cap \langle X_2\rangle_\Omega = \emptyset = X_1 \cap X_2$, так как все Ω-*слова* над $X_1$ не являются Ω-*словами* над $X_2$, из-за однозначности записи Ω-*слов* над $X$. При этом $W_0 = X$и в указанной ситуации наименьшей подсистемы нет, так как *«пересечение подсистем иногда пусто»*, а все подсистемы всегда непусты (как Ω-*алгебры*!), по определению.

С другой стороны, учитывая и равенство $X_1 \cup X_2 = X$ получаем, что $\langle X_1\rangle_\Omega \cup \langle X_2\rangle_\Omega \neq \langle X_1\rangle_\Omega \vee \langle X_2\rangle_\Omega = \langle X\rangle_\Omega$, так как уже в записи Ω-*слов* над $X$, построенных в $W_3$ могут *одновременно* возникать и буквы из $X_1$ и $X_2$, причём именно из-за имеющихся не *нульарных* операций в Ω, которые применяются в указанном «индуктивном процессе» порождения всех Ω-*слов*. Поэтому *«простое объединение подсистем иногда не является подсистемой»* и одновременно оказалось, что доказательство теоремы закончено, так как с помощью Ω-*алгебры* $W = \mathcal{W}(X,\Omega)$ уже построены и «примеры».

Более того, уточняя специфику $\mathcal{W}(X,\Omega)$ и применяя указанный «индуктивный процесс» порождения Ω-*слов* над $X$, можно строить и другие подсистемы или Ω-*алгебры*. В частности, *если в* Ω *есть нульарные операции*, то $W_0 = X \cup O$ для уже непустого множества $O$ из символов этих *нульарных* операций. При этом в указанной выше ситуации получается равенство $\langle X_1\rangle_\Omega \cap \langle X_2\rangle_\Omega = \langle O\rangle_\Omega$ и это наименьшая подсистема в $W = \mathcal{W}(X,\Omega)$, причём оказывается, что $X \cap \langle O\rangle_\Omega = \emptyset$ из-за специфики этой Ω-*алгебры*, хотя $O \neq \emptyset$.

Поясняя это можно учесть «индуктивный процесс» порождения Ω-*слов* и для этой наименьшей подсистемы, так как из равенства $\mathcal{W}(X,\Omega) = \cup W_m$ с очевидностью вытекает и равенство $\langle O\rangle_\Omega = \cup_m(\langle O\rangle_\Omega \cap W_m)$. Поэтому нужно просто последовательно строить указанные подмножества $\langle O\rangle_\Omega \cap W_m$, начиная с $O = \langle O\rangle_\Omega \cap W_0$ и учесть соответствующий «индуктивный переход» от $\langle O\rangle_\Omega \cap W_m$ к

$\langle O\rangle_\Omega \cap W_{m-1}$ , который выполняется уже с помощью не *нульарных*операций. А именно, сначала учтём, что $X \cap O = \emptyset$, а затем получаем, что если в записи $\Omega$-*слов* $a_1, \dots, a_n \in \langle O\rangle_\Omega \cap W_m$ нет букв из $X$, то такие буквы не появятся и в $a_1 \dots a_n\omega \in \langle O\rangle_\Omega \cap W_{m+1}$. Поэтому и получается, что $X \cap \langle O\rangle_\Omega = \emptyset$, причём можно считать, что справедливо равенство $\langle O\rangle_\Omega = \mathcal{W}(O, \Omega)$, так как фактически применяется «тот же индуктивный процесс» порождения $\Omega$-*слов*, но над алфавитом $O$, так как буквы алфавита $X$не применялись (и не возникают в $\langle O\rangle_\Omega$!).

Согласно доказанному, если $\Omega$-*слово* $w$ не попадает в наименьшую подсистему $\Omega$ -*алгебры* $W = \mathcal{W}(X, \Omega)$ , то в записи этого $w \in W$ обязательно *возникают* буквы алфавита $X$ . В этом случае будем считать, что $w = \omega(x_1, \dots, x_k)$ , если указанных букв $x_i \in X$ (с возможными повторениями) уже *достаточно* для построения указанного $\Omega$-*слова* над $X$. А учитывая это можно учесть *подстановки* $x_i \to u_i \in W$ и заметить, что из заданного $\Omega$ -*слова* $\omega(x_1, \dots, x_k)$ получается $\Omega$ -*слово* $\omega(u, \dots, u_k) \in W$ , как результат указанной подстановки (вместо букв $x_i$ подставляются $\Omega$-*словами*).

Применяя отмеченное, мы получаем одно из основных, отражающих специфику $W = \mathcal{W}(X, \Omega)$, свойств: *каждое отображение* $\theta: X \to U \subseteq W$ *всегда продолжается и притом единственным образом до гомоморфизма* $\varphi_\theta: W \to W$. А именно, если $x_i\theta = u_i$, то $\omega(x_1, \dots, x_k)\varphi_\theta = \omega(x_1, \dots, x_k)$, то есть гомоморфизм $\varphi_\theta$ просто действует как указанная подстановка, благодаря однозначной записи $\Omega$-*слов* над $X$. Но при этом нужно учитывать и «возможные» *нульарные*операции, и поэтому мы поясним построение указанного гомоморфизма или соответствующий процесс подстановки.

Учитываем, что $\mathcal{W}(X, \Omega) = W = \bigcup_m W_m$ и уже указанное «общее» определение гомоморфизма, как отображения сохраняющего или согласованного с операциями из $\Omega$. Построение производим, конечно, в согласии с указанным «индуктивным процессом» порождения $\Omega$-*слов* над $X$ или последовательным построением множеств $W_m$.

Согласно определению «продолжения» и заданному отображению $\theta: X \to U$, на первом шаге построение «однозначно и очевидно». А именно, $x_i\varphi = x_i\theta = u_i$ для всех $x_i \in X$, а если имеются символы $0_j \in O$ *нульарных* операций, то $0_j\varphi = 0_j$, так как гомоморфизм $\varphi$ должен «сохранять» соответствующую операцию из $\Omega$. Поэтому уже указано действие $a \to a\varphi$ гомоморфизма $\varphi = \varphi_\theta$ на всех $a \in W_0$, то есть подстановка $w(x_1, \dots, x_k) \to w(u, \dots, u_k)$ для $\Omega$ -*слов* из $W_0$ осуществлена: буквы $x_i \in X$ заменяются на $u_i = x_i\theta$, а символы *нульарных* операций (если такие есть) просто не меняются.

Следующие $\Omega$-*слова*, уже из $W_1$ не попадающие в $W_0$, однозначно записываются в виде $a_1 \dots a_n\omega$, где $a_j \in W_0$ и $n$-арная операция $\omega \in \Omega$ уже не *нульарна*, но гомоморфизм $\varphi$должен сохранять и эти $\omega \in \Omega$, и поэтому соответствующая подстановка в $\Omega$ -*слова* из $W_1$ осуществляется (и должна осуществляться!) по правилу $(a_1 \dots a_n\omega)\varphi = (a_1\varphi, \dots, a_n\varphi)\omega$. После этого становится ясным, что если уже осуществлена подстановка в $\Omega$-*слова*из $W_m$, то есть построено продолжение $a \to a\varphi$ отображения $\theta$ для $\Omega$ -*слов* из $W_m$, то оно однозначно продолжается на следующее подмножество $W_{m+1}$, причём именно по правилу $(a_1 \dots a_n\omega)\varphi = (a_1\varphi, \dots, a_n\varphi)\omega$ (где $a_j \in W_m$, $\omega \in \Omega$).

По индукции, все подстановки $w(x_1, \dots, x_k) \to w(u, \dots, u_k)$ осуществлены, благодаря однозначности записи $\Omega$ -*слов* – при построении $\Omega$ -*слова* $w\varphi = w(u, \dots, u_k)$ нужно произвести над подставляемыми $\Omega$-*словами* $u_i = x_i\theta$, те операции и в том же порядке, как это сделано над буквами $x_i \in X$ при порождении $\Omega$ -*слова* $w(x_1, \dots, x_k)$. Поэтому и получается, что отображение $\theta: X \to U \subseteq W$ всегда однозначно продолжается до гомоморфизма $\varphi_\theta: W \to W$, который и действует как указанная подстановка, *что и утверждалось*, но одновременно оказалось, что образом построенного гомоморфизма $\varphi_\theta$ является подсистема $\langle U\rangle_\Omega = W\varphi_\theta$ порождённая в $W = \mathcal{W}(X, \Omega)$

непустым подмножеством $U = X_\theta \subseteq W$, так как эта подсистема и состоит из указанных Ω-*слов* $w(u, \dots, u_k)$.

**Теорема 5.** Построенная (из Ω-*слов* над $X$) Ω-*алгебры* $\mathcal{W}(X, \Omega)$ *порождается алфавитом* $X$ *свободно в классе всех* Ω-*алгебр*. *Это означает* (по определению), что для любой Ω-*алгебры* $A$ каждое отображение $\theta: X \to U$ всегда *продолжается и при том единственным образом* до гомоморфизма $\varphi_\theta: W \to W$. Указанное свойство «характеризует $\mathcal{W}(X, \Omega)$ с точностью до изоморфизма» и одновременно получается, что образом гомоморфизма $\varphi_\theta: W \to A$ является порождённая подмножеством $X\theta \subseteq A$ подсистема $\langle X\theta \rangle_\Omega$ (а если алфавит $X$ достаточно «велик», то может получиться вся Ω-*алгебра* $A$!).

**Доказательство.** Согласно уже отмеченному, однозначная запись Ω-*слова* $w = w(x_1, \dots, x_k)$ указывает какие операции из Ω и в каком порядке нужно произвести над буквами $x_i \in X$ для «порождения» этого элемента $w \in W = \mathcal{W}(X, \Omega)$. Но гомоморфизмы должны «сохранять» все операции из Ω, и поэтому получается, что отображение $\theta: X \to A = A(\Omega)$ всегда продолжается до гомоморфизма $\varphi_\theta: W \to A$, причём именно по правилу $\big(w(x_1, \dots, x_k)\big)\varphi = w(a_1 \dots a_k) \in A$ подстановки, то есть над элементами $a_i = x_i\theta = x_i\varphi \in A$ нужно произвести те операции из Ω и в том же порядке, как это сделано над буквами $x_i \in X$ для «порождения» Ω-*слова* $w(x_1, \dots, x_k) \in \mathcal{W}(X, \Omega)$.

Поэтому и получается указанное в теореме свойство построенной Ω-*алгебры* $\mathcal{W}(X, \Omega)$, а образом построенного гомоморфизма $\varphi_\theta: W \to A$ конечно оказывается соответствующая подсистема $\langle X\theta \rangle_\Omega$ в $A = A(\Omega)$, порождённая указанным непустым подмножеством $X\theta \subseteq A$. При этом получается, согласно построению гомоморфизма $\varphi = \varphi_\theta$, что эта подсистема состоит из элементов $w(a_1 \dots a_k) = \big(w(x_1, \dots, x_k)\big)\varphi$, как «порождённых» соответствующими элементами $a_i = x_i\theta = x_i\varphi \in A$.

Применяя «уже доказанное свойство» получаем, что именно указанным способом строятся все гомоморфизмы $\varphi: W \to W$ или *эндоморфизмы* $\Omega$-*алгебры* $\mathcal{W}(X, \Omega)$, причём оказывается, что только тождественный изоморфизм $\mathcal{E}_W$ продолжает тождественное отображение $\mathcal{E}_X$ (или вложение $X$ в $W$), согласно единственности продолжений $\varphi_\theta$ отображений $\theta: X \to W$.

Учитывая уже отмеченное допустим, что $\Omega$-*алгебра* $A$ тоже «свободно» порождается некоторым непустым подмножеством $Y = \{y_i | i \in I\} \subseteq A$ также «занумерованным» как алфавит $X = \{x_i | i \in I\} \subseteq W$. Благодаря этому получаются обратные друг другу отображения $\theta: X \to Y$ и $\bar{\theta}: Y \to X$, согласно правилам $x_i\theta = y_i$ и $y_i\bar{\theta} = x_i$, соответственно. После этого, получаем согласно указанному «свойству свободы», что однозначно строятся соответствующие гомоморфизмы $\varphi_\theta: W \to A$, $\varphi_{\bar{\theta}}: A \to W$ и оказывается, что $\varphi_\theta\varphi_{\bar{\theta}}: W \to W$ тождественен на $X$, вместе с $\theta\bar{\theta} = \mathcal{E}_X$, а $\varphi_{\bar{\theta}}\varphi_\theta: A \to A$ тождественен на $Y$. Поэтому, снова в силу «единственности продолжений», получаются равенства $\varphi_\theta\varphi_{\bar{\theta}} = \mathcal{E}_W$, $\varphi_{\bar{\theta}}\varphi_\theta = \mathcal{E}_X$, то есть $\varphi_\theta$ и $\varphi_{\bar{\theta}}$ обратные друг другу изоморфизмы, и поэтому $W \approx A$ и $A \approx W$.

Именно поэтому указанное свойство «свободы» характеризует $\Omega$-*алгебру* $W = \mathcal{W}(X, \Omega)$ с точностью до изоморфизма, причём легко заметить, что если мы имеем изоморфизм $\mu: W \approx \overline{W}$, то $\bar{X} = X\varphi$ свободно порождает $\Omega$-*алгебру* $\overline{W}$ в классе всех $\Omega$-*алгебр*, так как $X$ свободно порождает $W$. Кроме того, для $\Omega$-*алгебры* $A = A(\Omega)$ всегда можно построить такой алфавит $X$, что $X\theta = A$ (можно просто взять $A$ в качестве алфавита). Но тогда получится, конечно, что $A = W\varphi_\theta$ для соответствующего гомоморфизма $\varphi_\theta: W \to A$, то есть $\Omega$-*алгебра* $A(\Omega)$ окажется гомоморфным образом $\Omega$-*алгебры* $W = \mathcal{W}(X, \Omega)$, что заканчивает доказательство теоремы.

Благодаря этой теореме получается, что в любой $\Omega$-*алгебре* $A = A(\Omega)$ подсистема $\langle Y \rangle_\Omega$, порождённая непустым подмножеством

$Y \subseteq A$, строится как замыкание этого $Y$ с помощью всех операций из $\Omega$, так как это справедливо для $\Omega$-*алгебры* $W = \langle Y \rangle_\Omega$ (и было пояснено в доказательстве). Можно указать и другие применения построенной «весьма специальной» алгебраической системы $\mathcal{W}(X, \Omega)$, но мы сделаем это немного позже – после «специализации» некоторых общих конструкций и утверждений о непустых множествах.

На самом деле это уже начато и простым примером «специализации» является теорема 4 – мы просто рассматривали подсистемы алгебраической системы $A = A(\Omega)$ и учли соответствующие «общие конструкции и утверждения» о подмножествах рассматриваемых непустых множеств. Кроме того, неявно учтено, что произведение согласованных гомоморфизмов $\varphi: R \to A$, $\psi: A \to B$ как отображений, всегда является гомоморфизмом $\varphi\psi: R \to B$, так как гомоморфизмы сохраняют операции из $\Omega$. Аналогично получилось, что образ $A\psi$ гомоморфизма $\psi: A \to B$ является подсистемой в $\Omega$-*алгебре* $B$, а для подсистемы $C$ в $A$ её образ $C\psi$ – подсистема в $A\psi$.

Почти аналогичная ситуация получилась при построении декартовых произведений – декартово произведение $\Omega$ -*алгебр* оказывается $\Omega$ -*алгеброй*, но только после «покомпонентного перенесения» операций из $\Omega$. Именно поэтому оказалось, что квадрат $A \times A$ является $\Omega$-*алгеброй* вместе с $A = A(\Omega)$, а это уже можно учесть при уточнении специфики гомоморфизмов рассматриваемой алгебраической системы $A = A(\Omega)$.

Уточняя специфику гомоморфизма $\varphi: A \to B$, учитываем его образ $A\varphi = \{a\varphi | a \in A\}$ и ядро $\sigma_\varphi = \{(x, y) \in A \times A | x\varphi = y\varphi\}$, как это делалось при уточнении специфики отображения $\varphi: A \to B$. При этом, если $A\varphi = B$, то получается гомоморфизм $\Omega$-*алгебры* $A$ на $\Omega$-*алгебру* $B$ или *эпиморфизм* $A = A(\Omega)$ на $B = B(\Omega)$, если же $A\varphi = B$ и $\sigma_\varphi = \Delta_A = \{(a, a) | a \in A\}$, то конечно получается *изоморфизм* $A \approx B$, как гомоморфизм являющийся биекцией (и это уже отмечалось). В

частности тождественное отображение $\mathcal{E}_A$ конечно является изоморфизмом $A \approx A$, а вместе с изоморфизмом $\mu: C \approx D$ всегда строится «обратный» изоморфизм $\mu^{-1}: D \approx C$ (что тоже уже отмечалось).

С другой стороны, для гомоморфизма $\delta: C \to B$ может оказаться, что справедливо «только» равенство $\sigma_\delta = \Delta_C$ и в этом случае говорят, что -изоморфное вложение $C$ в $B$, так как получается изоморфизм $C \approx C\delta \subseteq B$. В частности, если $C$ является подсистемой Ω-*алгебры* $B$, то тождественное вложение $\mathcal{E}_B^C$ будет, конечно, изоморфным вложением $C$ в $B$. Одновременно получается «характеристика» образов гомоморфизмов $\varphi: A \to B$ в Ω -*алгебру* $B$ -образ $A\varphi$ является подсистемой в $B$, а каждая подсистема $C \subseteq B$ конечно является образом некоторого гомоморфизма в $B$. Немного сложнее получается «характеристика» ядер $\sigma_\delta$ гомоморфизмов $\varphi: A \to B$ произвольно заданной $A = A(\Omega)$.

**Теорема 6.** Для гомоморфизма $\varphi: A \to B$ его ядро $\sigma_\delta$ (по построению и определению) – это *конгруенция* на Ω -*алгебре* $A$, т.е. эквиваленция $\sigma \subseteq A \times A$, которая является и Ω -*подалгеброй* в $A \times A$. С другой стороны, каждая конгруенция $\sigma \subseteq A \times A$ является ядром некоторых гомоморфизмов заданной Ω-*алгебры* $A = A(\Omega)$. Более того, благодаря специфике конгруенции $\sigma \subseteq A \times A$, фактор-множество $A / \sigma = \hat{A} = \{\hat{a} | a \in A\}$ естественно «превращается» в Ω-*алгебру* и получается *фактор-алгебра* $A / \sigma$ этой Ω-*алгебры* $A$ по конгруенци $\sigma$, а естественное отображение $\nu_\sigma: A \to \hat{A} = A / \sigma$ превращается в *естественный гомоморфизм* $\nu_\sigma: A \to A / \sigma$, ядром которого и оказывается заданная конгруенция $\sigma$. При этом получается, что справедливо равенство $A\nu_\sigma = \hat{A} = A / \sigma$ (как для отображений).

**Доказательство.** Согласно уже указанному построению, ядро $\sigma_\varphi = \{(x, y) \in A \times A | x\varphi = y\varphi\}$ гомоморфизма $\varphi: A \to B$ является эквиваленцией на $A$ и подсистемой $\Omega$ -*алгебры* $A \times A$, так как гомоморфизм $\varphi: A \to B$ сохраняет все операции из $\Omega$, перенося их «покомпонентно» на $A \times A$ и на $\sigma_\varphi \subseteq A \times A$. Поэтому и оказывается, что $\sigma = \sigma_\varphi$ – *конгруенция* «по определению», как эквиваленция на $A$ являющаяся подсистемой в $\Omega$-*алгебре* $A \times A$.

После этого можно учесть, что одноэлементное множество $O = \{0\}$ превращается в $\Omega$-*алгебру*, согласно очевидному построению $(0, \dots, 0)\omega = 0$ соответствующих операций. При этом получается, что отображение $o: A \to \{0\} = O$ конечно является гомоморфизмом с ядром $\sigma_0 = A \times A$. С другой стороны, для тождественного изоморфизма $\mathcal{E} = \mathcal{E}_A$ конечно получается, что $\sigma_\mathcal{E} = \Delta_A$, и поэтому на $A = A(\Omega)$ всегда имеются конгруенции. Остаётся доказать, что каждая конгруэнция $\sigma \subseteq A \times A$ является ядром некоторого гомоморфизма $\varphi: A \to B$, но это «фактически доказано в формулировке теоремы». При этом можно предполагать, что $\sigma \neq A \times A$ (и в этом случае получится, конечно, что $\Omega$-*алгебра* $A = A(\Omega)$ не одноэлементна и $\Delta_A \neq A \times A$), но мы всё же поясним доказательство «не совсем тривиальное».

Учитывая, что конгруэнция $\sigma$ является эквиваленцией на множестве $A$, мы строим соответствующее не одноэлементное фактор-множество $A / \sigma = \hat{A} = \{\hat{a} | a \in A\}$. По построению, элементами в $\hat{A}$ являются классы $\hat{a} = \{x \in A | (a, x) \in \sigma\}$ эквивалентности и $\hat{A}$ не одноэлементно, так как $\sigma \neq A \times A$, по предположению. После этого учитываем естественное отображение $\nu_\sigma: A \to \hat{A} = A / \sigma$ – оно строится по правилу $a\nu_\sigma = \hat{a}$, что приводит к равенству $\sigma_\nu = \sigma$ для $\nu = \nu_\sigma$, так как получается, по построению, что

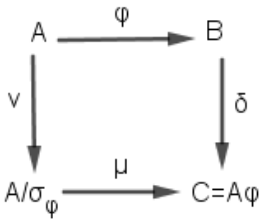
$$a\nu = x\nu \Leftrightarrow \hat{a} = \hat{x} \Leftrightarrow (a, x) \in \sigma.$$

Поэтому остаётся указать «естественное превращение» фактор-множества $\hat{A} = A / \sigma$ в $\Omega$-*алгебру*. Но конгруэнция $\sigma$ является $\Omega$-*подалгеброй* в $A \times A$, и поэтому получается, что операции $\omega \in \Omega$

переносятся на фактор-алгебру $\hat{A} = A \,/\, \sigma$ по правилу: если $a_1 \dots a_n \omega = a$, то $\widehat{a_1} \dots \widehat{a_n} \omega = \hat{a}$ . Это просто показывает, что естественное отображение $\nu_\sigma : A \to A \,/\, \sigma$ является гомоморфизмом $\Omega$-*алгебры* $A$ на $\Omega$-*алгебру* $\hat{A} = A \,/\, \sigma$ (так и должно быть!) с заданным ядром $\sigma_\nu = \sigma$, что и заканчивает доказательство теоремы, согласно уже отмеченному.

В результате оказалось, что и указанная конструкция фактор-алгебр $A \,/\, \sigma$ рассматриваемых $\Omega$-*алгебр* $A(\Omega)$ по конгруэнциям $\sigma$ тоже является «специализацией» соответствующей общей конструкции для непустых множеств. Кроме того, мы уже имеем примеры разнообразных гомоморфизмов – вместе с тождественными изоморфизмами $\mathcal{E}_A$ возникают тождественные вложения $\mathcal{E}_B^C$ подсистем $C$ в в соответствующие $\Omega$-*алгебры* $B$ , а вместе с конгруэнциями $\sigma \subseteq A \times A$ уже построены соответствующие естественные гомоморфизмы $\nu_\sigma : A \to A \,/\, \sigma$, согласно уже отмеченному. После этого «простой специализацией» соответствующей теоремы об отображениях непустых множеств (см. теоремы 2,3) получается «почти такая же теорема» о гомоморфизмах алгебраических систем.

**Теорема 7.** Вместе с гомоморфизмом $\varphi : A \to B$ учтём его образ $C = A\varphi$ , ядро $\sigma = \sigma_\varphi$ , вложение $\delta = \mathcal{E}_B^C : C \to B$ и естественный гомоморфизм $\nu = \nu_\sigma : A \to \hat{A} = A \,/\, \sigma$, а затем учтём и умножение соответствующих «согласованных» гомоморфизмов. Тогда получается выписанная диаграмма, связывающая указанные гомоморфизмы – точнее,



*существует и единственный такой гомоморфизм* $\mu: \hat{A} \to C$, *что* $\varphi = \nu\mu\delta$. Более того, этот гомоморфизм действует по правилу $\hat{a}\mu = a\varphi$ (для всех $a \in A$) и оказывается взаимно однозначным, а потому и изоморфизмом. Но тогда строится и «обратный» изоморфизм $\varphi^{-1}: C \to \hat{A}$, т.е. получается *канонический изоморфизм* $A\varphi \approx A/\sigma_\varphi$ (*гомоморфные образы* Ω-*алгебры* $A$ *являются её фактор-алгебрами* по соответствующим конгруэнциям, с точностью до изоморфизмов). При этом можно учесть, что гомоморфизм $\nu\mu: A \to C$ уже являющийся гомоморфизмом Ω-*алгебры* $A$ на Ω-*алгебру* $C$ в точности соответствует заданному гомоморфизму $\varphi: A \to B$, то есть имеет то же образ и то же самое ядро (что неявно отражено в диаграмме).

**Доказательство.** Действительно, указанная диаграмма уже построена для отображения $\varphi: A \to B$, так как $\sigma_\varphi = \sigma = \sigma_\nu$, построено и единственное $\mu: \hat{A} \to C$ такое, что $\varphi = \nu\mu\delta$, благодаря указанному правилу $\hat{a}\mu = a\varphi$, причём оказалось биекцией. Всё это уже сделано в теореме 2 и остаётся «произвести специализацию», то есть учесть, что рассматривается гомоморфизм $\varphi: A \to B$. Именно это отмечено в формулировке теоремы: $A\varphi = C$ является подсистемой в $B = B(\Omega)$ и вложение $\delta = \mathcal{E}_B^C$ оказывается гомоморфизмом, $\sigma = \sigma_\varphi$ является конгруэнцией и поэтому $\nu = \nu_\sigma$ оказывается гомоморфизмом $A = A(\Omega)$ наеё фактор-алгебру $\hat{A} = A / \sigma$.

Поэтому построенная биекция $\mu: \hat{A} \to C$ тоже является гомоморфизмом, то есть сохраняет операции из Ω, вместе с $\delta$ и $\nu$, что легко увидеть согласно указанному построению, которое и привело к равенству $\varphi = \nu\mu\delta$. В результате оказалось, что построен изоморфизм $\mu: \hat{A} \approx C$, но тогда строится и «обратный» изоморфизм $\varphi^{-1}: A\varphi \approx A/\sigma_\varphi$, то есть гомоморфные образы $A\varphi$ алгебраической

системы $A(\Omega)$ являются её фактор-алгебрами $A/\sigma_\varphi$, с точностью до изоморфизма. Осталось заметить, что $\nu\mu\colon \hat{A} \to C$ является гомоморфизмом на $C = A\varphi$, а ядром этого гомоморфизма оказывается конгруэнция $\sigma = \sigma_\varphi = \sigma_\nu$.

Это заканчивает «доказательство» теоремы и показывает, что вычисление ядер и образов фактически производится только для «гомоморфизмов на», то есть таких как $\nu\mu$.

**Теорема 8.** Для подсистемы $R$ в $A = A(\Omega)$ её образ $R\varphi$ при гомоморфизме $\varphi\colon A \to \bar{A} = A\varphi$ является подсистемой в $A\varphi = \bar{A}$, а из конгруэнции $\sigma_\varphi = \sigma \subseteq A \times A$ получается конгруэнция $\sigma \cap (R \times R)$ на $R$, как ядро индуцированного гомоморфизм $\varphi'\colon R \to R\varphi \subseteq A\varphi$. Поэтому получается и изоморфизм $R\varphi \approx R/\sigma \cap (R \times R)$, вместе с изоморфизмом $A\varphi \approx A/\sigma_\varphi$. С другой стороны, для подсистемы $\bar{R}$ в $\bar{A} = A\varphi$ её *полный прообраз* $\varphi^{-1}(\bar{R}) = \{a \in A | a\varphi \in \bar{R}\}$ оказывается подсистемой в $A$ и очевидно, что $\big(\varphi^{-1}(\bar{R})\big)\varphi = \bar{R}$, и поэтому *все подсистемы* в $A\varphi = \bar{A}$ являются образами $R\varphi$ некоторых подсистем в $A$. При этом для всех подсистем $R$ в $A$, всегда
$R \subseteq \varphi^{-1}(R\varphi) = \hat{R} = \bigcup\{\hat{r} | r \in R\}$, где $\hat{a} = \varphi^{-1}(\{a\varphi\})$ – это классы эквивалентности относительно конгруэнции $\sigma = \sigma_\varphi$, причём получается и равенство $\hat{R}\varphi = R\varphi$. Поэтому полные прообразы подсистем $\bar{R}$ в $\bar{A} = A\varphi$ – это в точности указанные *насыщенные относительно конгруэнции* $\sigma = \sigma_\varphi$, подсистемы $\hat{R}$ в $A$ и одновременно получается взаимно однозначное (и сохраняющее включения) соответствие между подсистемами в $A\varphi = \bar{A}$ и указанными насыщенными подсистемами в $A$.

Доказательство этой теоремы тоже получается «простой специализацией» соответствующей теоремы 3 об образах и полных

прообразах непустых подмножеств при отображении $\varphi: A \to A\varphi$, то есть снова остаётся учесть, что мы рассматриваем гомоморфизм $\varphi: A \to \bar{A} = A\varphi$. При этом конечно нужно учесть, что указанные переходы «сохраняют» свойство быть подсистемой, а соответствующие изоморфизмы получаются благодаря теореме 7. Кроме того, можно учесть, что при переходах к образам подсистем из $A$ всегда $R_1 \subseteq R_2 \Rightarrow R_1\varphi \subseteq R_2\varphi$, а при переходах к полным прообразам подсистем из $\bar{A} = A\varphi$ получаются «точные» импликации $\overline{R_1} \subseteq \overline{R_2} \Leftrightarrow \varphi^{-1}(\overline{R_1}) \subseteq \varphi^{-1}(\overline{R_2})$, так как $\left(\varphi^{-1}(\bar{R})\right)\varphi = \bar{R}$. Поэтому и получилось указанное взаимно однозначное соответствие между подсистемами из $\bar{A} = A\varphi$ и их полными прообразами, то есть «насыщенными» подсистемами в $A$. А благодаря теореме 7 и сказанному о «насыщениях» получается, что всегда $R \,/\, \sigma \cap (R \times R) \approx R\varphi = \hat{R}\varphi \approx \hat{R}/\sigma \cap \left(\hat{R} \times \hat{R}\right)$ для подсистем $R$ в $A$, хотя включение $R \subseteq \hat{R} = \varphi^{-1}(R\varphi)$ иногда строгое (то есть иногда $R \neq \hat{R}$, что можно показать на «конкретных примерах»).

Теперь учтём, что «превращение» квадрата $A \times A$ в $\Omega$-*алгебру*, вместе с $A = A(\Omega)$, получилось благодаря «покомпонентному» переносу операций из $\Omega$. Именно поэтому конгруэнции $\sigma \subseteq A \times A$ оказались не просто эквиваленциями, но и подсистемами в $A \times A$, согласно теореме 6, что учтено и в теореме 7. После этого можно заметить, что и гомоморфизмы «покомпонентно» переносятся с $\Omega$-*алгебры* $A$ на её квадрат $A \times A$. А именно, если задан гомоморфизм $\varphi: A \to \bar{A} = A\varphi$, то согласно «покомпонентному» правилу $(x, y)\varphi = (x\varphi, y\varphi) \in \bar{A} \times \bar{A}$, строится гомоморфизм $\varphi: A \times A \to \bar{A} \times \bar{A}$, что позволяет применить доказанное в теореме 8 к подсистемам в $A \times A$ и указанным гомоморфизмам $\Omega$-*алгебры* $A \times A$.

**Теорема 9.** Применяя гомоморфизм $\varphi: A \times A \to \bar{A} \times \bar{A}$, соответствующий гомоморфизму $\varphi: A \to \bar{A} = A\varphi$ с ядром $\sigma = \sigma_\varphi$, получаем, что для конгруэнции $\theta \subseteq A \times A$ её образ $\theta\varphi = \{(x\varphi, y\varphi) | (x, y) \in \theta\}$ оказывается

конгруэнцией на $A\varphi = \bar{A}$,. При этом *все конгруэнции* $\bar{\theta} \subseteq \bar{A} \times \bar{A} = (A \times A)\varphi$ *оказываются образами* некоторых конгруэнций $\theta \subseteq A \times A$, так как (в согласии с теоремой 8) строятся «полные прообразы» $\varphi^{-1}(\bar{\theta}) = \{(x, y) \in A \times A \mid (x\varphi, y\varphi) \in \bar{\theta}\}$ конгруэнций $\bar{\theta} \subseteq \bar{A} \times \bar{A}$, которые оказываются конгруэнциями на $A$, а затем учитывается, что $\left(\varphi^{-1}(\bar{\theta})\right)\varphi = \bar{\theta}$. При указанных переходах всегда «сохраняются включения» и потому получается, что $\varphi^{-1}(\bar{\theta}) \supseteq \varphi^{-1}(\Delta_{\bar{A}}) = \sigma_\varphi$, так как $\Delta_{\bar{A}}$ наименьшая конгруэнция на $\bar{A} = A\varphi$ и $\sigma_\varphi\varphi = \Delta_{\bar{A}}$. Поэтому *полные прообразы* $\varphi^{-1}(\bar{\theta})$ *конгруэнций на* $\bar{A} = A\varphi$ *– это в точности все конгруэнции* $\theta$ *на* $A$ *содержащие* $\sigma_\varphi$, так как именно для этих конгруэнций справедливо равенство $\varphi^{-1}(\theta\varphi) = \theta$. Одновременно *построено взаимно однозначное соответствие* между конгруэнциями $\bar{\theta} \subseteq \bar{A} \times \bar{A} = (A \times A)\varphi$ и указанными конгруэнциями $\theta \supseteq \sigma_\varphi$ на $A$, а после этого получаются и соответствующие *изоморфизмы* $A/\theta \approx \bar{A}/\bar{\theta}$ для фактор-алгебр $\Omega$ *-алгебр* $A$ и $\bar{A}$ по указанным конгруэнциям.

Легко увидеть, что эта теорема (согласно сказанному перед ней) является простым следствием теорем 8 и 7 – нужно только заметить, что полный прообраз $\varphi^{-1}(\bar{\theta}) \subseteq A \times A$ конгруэнции $\bar{\theta} \subseteq \bar{A} \times \bar{A}$ является конгруэнцией на $A$.

В связи с этой теоремой можно учесть, что (согласно предложению 2) эквиваленции на $A$ образуют решётку $\mathcal{E}(A)$ с наибольшим элементом $A \times A$, наименьшим $\Delta_A$ и обычными пересечениями $\bigcap \theta_i = \theta \in \mathcal{E}(A)$ (то есть систему замыкания в $\mathcal{B}(A \times A)$), а благодаря теореме 4 получается «почти такая же» ситуация для подсистем в $A \times A$. Поэтому согласно теоремам 4 и 6,

становится очевидным, что *конгруэнции на A образуют решётку* $\mathcal{K}(A)$ с наибольшим элементом $A \times A$, наименьшим элементом $\Delta_A$ и обычными пересечениями, как в $\mathcal{E}(A)$.

Это неявно учтено в теореме 9, так как мы учли, что конгруэнции «сравниваются по включению» (как эквиваленции и подсистемы), причём $\Delta_{\bar{A}}$ – наименьшая конгруэнция на $\bar{A} = A\varphi$, а $\bar{A} \times \bar{A} = (A \times A)\varphi$ является наибольшей конгруэнцией. После этого получилось, что решётка $\mathcal{K}(\bar{A})$ оказалась образом решётки $\mathcal{K}(A)$, благодаря гомоморфизму $\varphi: A \times A \to \bar{A} \times \bar{A}$ или указанным в теореме 9 переходам.

Применяя уже отмеченные «рабочие утверждения» о подсистемах и гомоморфных образах алгебраических систем, мы можем указать «характеристику» декартовых произведений с точностью до изоморфизма, но сначала сделаем некоторые пояснения или уточнения для «специализации» при переходе от непустых множеств к Ω-*алгебрам*.

При построении декартовых произведений $\mathcal{D} = \prod A_i$ произвольных непустых множеств $A_i$ мы учитываем, что элементы $a \in \mathcal{D}$ представляются в виде строк $a = (a_i | i \in I)$ с компонентами $a_i \in A_i$ (как это сделано для $A_1 \times A_2 \times \ldots \times A_n$). При этом можно учесть, что согласно выписанному правилу

$$\forall a \in \mathcal{D}\ \forall i \in I | a\pi_i = a_i \in A_i = \mathcal{D}\pi_i$$

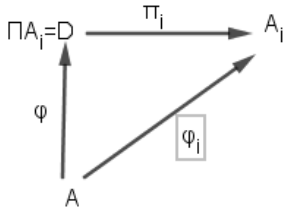
строятся соответствующие проектирования $\pi_i: \mathcal{D} \to A_i = \mathcal{D}\pi_i$ которые и отмечают соответствующие компоненты. После этого оказывается, что *справедливо равенство* $\bigcap Ker\pi_i = \Delta_{\mathcal{D}}$ для ядер $Ker\pi_i$ построенных проектирований, так как элементы из $\mathcal{D} = \prod A_i$ сравниваются «покомпонентно»: $a = b \Leftrightarrow \forall i \in I | a_i = b_i$.

Всё отмеченное конечно учитывается при уточнении специфики декартовых произведений Ω-*алгебр* $A_i$ и мы будем говорить, что $\mathcal{D} = \prod A_i$ – *прямое произведение* заданного непустого семейства Ω-*алгебр* $A_i$, чтобы отличить его от декартова произведения «просто»

непустых множеств. Иначе говоря, мы учитываем, что на $A_i = A_i(\Omega)$ заданы операции $\omega \in \Omega$, которые «покомпонентно» перенесены на прямое произведение $\mathcal{D} = \prod A_i$, которое оказывается $\Omega$-*алгеброй* $\mathcal{D} = \mathcal{D}(\Omega)$. Но это просто означает, что все построенные проектирования $\pi_i : \mathcal{D} \to A_i$ *являются гомоморфизмами* $\mathcal{D} = \mathcal{D}(\Omega)$ *на соответствующие компоненты* $A_i = A_i(\Omega)$, причём справедливы и равенства $\bigcap Ker\pi_i = \Delta_{\mathcal{D}}$, согласно уже отмеченному.

**Теорема 10.** Благодаря специфике прямого произведения $\mathcal{D} = \prod A_i$ и проектирований $\pi_i : \mathcal{D} \to A_i = \mathcal{D}\pi_i$ (уже гомоморфизмов) получается, что для любой алгебры $A = A(\Omega)$ и любого набора гомоморфизмов $\varphi_i : A \to A_i$ *всегда существует и единственен* гомоморфизм $\varphi : A \to \mathcal{D}$ такой, что справедливы равенства $\varphi_i = \varphi\pi_i$ одновременно для всех проектирований $\pi_i$. При этом окажется, что если $A\varphi_i = A_i$ для всех указанных $\varphi_i$, то и $\bar{A}\pi_i = A_i$ для всех проектирований $\pi_i$ и гомоморфного образа $A\varphi = \bar{A} \subseteq \mathcal{D}$, а если $\bigcap Ker\varphi_i = \Delta_A$, то гомоморфизм $\varphi$ оказывается изоморфным вложением, то есть получается *изоморфизм* $A \approx \bar{A} = A\varphi$ на подсистему $\bar{A}$ в $\mathcal{D} = \prod A_i$. Более того, указанное свойство «характеризует» прямое произведение $\mathcal{D} = \prod A_i$ с точностью до изоморфизма, благодаря проектированиям $\pi_i : \mathcal{D} \to A_i = \mathcal{D}\pi_i$ и равенству $\bigcap Ker\pi_i = \Delta_{\mathcal{D}}$.

**Доказательство**. Указанное свойство прямого произведения $\mathcal{D} = \prod A_i$ с набором проектирований $\pi_i : \mathcal{D} \to A_i = \mathcal{D}\pi_i$ (отмечающих компоненты и построение элементов $a \in \mathcal{D}$, согласно равенству $\bigcap Ker\pi_i = \Delta_{\mathcal{D}}$), весьма «наглядно» представляется выписанной диаграммой.




Более того, эта диаграмма «подсказывает» построение гомоморфизма $\varphi: A \to \mathcal{D}$ такого, что $\varphi_i = \varphi\pi_i$ сразу для всех проектирований $\pi_i: \mathcal{D} \to A_i$ и заданных для $A = A(\Omega)$ гомоморфизмов $\varphi_i: A \to A_i$. А именно, если такой гомоморфизм $\varphi: A \to \mathcal{D} = \prod A_i$ существует, то для каждого элемента $a \in \mathcal{D}$ однозначно строится его образ $a\varphi \in \mathcal{D}$ и оказывается, что для этого элемента $a\varphi \in \mathcal{D}$ указываются (согласно диаграмме) все его компоненты $(a\varphi)\pi_i = a\varphi_i$. Поэтому получается, что гомоморфизм $\varphi: A \to \mathcal{D}$ должен строиться согласно выписанному правилу.

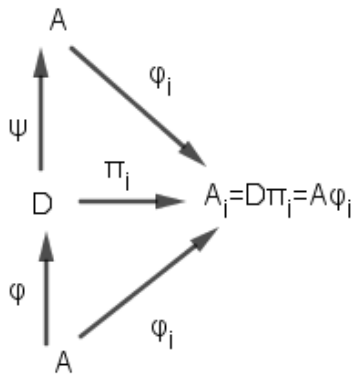
$$\forall a \in A \left| a\varphi = (a\varphi_i | i \in I) \in A\varphi \subseteq \mathcal{D} = \prod A_i \right.$$

Но это правило построения действительно задаёт гомоморфизм $\varphi: A \to \mathcal{D}$, так как все $\varphi_i: A \to A_i$ являются гомоморфизмами, причём (уже согласно правилу) получаются и равенства $\varphi\pi_i = \varphi_i$ для всех проектирований $\pi_i: \mathcal{D} \to A_i$ и то, что образ $A\varphi = \bar{A}$ является подсистемой в $\mathcal{D}$, так как все операции $\omega \in \Omega$ тоже «покомпонентно» строятся.

В результате уже доказано указанное свойство прямого произведения $\mathcal{D} = \prod A_i$ с его проектированиями $\pi_i: \mathcal{D} \to A_i = \mathcal{D}\pi_i$, для которых справедливо равенство $\bigcap Ker\pi_i = \Delta_{\mathcal{D}}$. Корме того, снова согласно правилу построения гомоморфизма $\varphi: A \to \mathcal{D}$, всегда справедливо равенство $Ker\varphi = \bigcap Ker\varphi_i$, а потому и оказывается, что $A \approx A\varphi$, когда $\bigcap Ker\varphi_i = \Delta_A$. С другой стороны, если все $A\varphi_i = A_i$, то для подсистемы $\bar{A} = A\varphi$ в $\mathcal{D} = \prod A_i$ получаются равенства $\bar{A}\pi_i = A_i = \mathcal{D}\pi_i$ сразу для всех проектирований $\pi_i: \mathcal{D} \to A_i$, так как все

$\varphi_i = \varphi\pi_i$. Это отражает специфику подсистемы $\bar{A} \subseteq \mathcal{D} = \prod A_i$, но это мы ещё уточним, так как может оказаться, что $\bar{A}$ отлична от Ω-*алгебры* $\mathcal{D}$ .

Теперь допустим, что Ω-*алгебра* $A$, с набором гомоморфизмов $\varphi_i: A \to A_i = A\varphi_i$ для которых $\bigcap Ker\varphi_i = \Delta_A$ , тоже обладает указанным свойством (уже доказанным для $\mathcal{D} = \prod A_i$). Таким образом, согласно отмеченному, предполагаем, что для любой Ω-*алгебры* $B$ , с набором гомоморфизмов $\psi_i: B \to A_i$ , всегда *существует и единственен* гомоморфизм $\psi: B \to A$ такой, что все $\psi_i = \psi\varphi_i$, согласно указанному свойству. В частности, вместо $B$ можно взять прямое произведение $\mathcal{D} = \prod A_i$ с его проектированиями $\pi_i: \mathcal{D} \to A_i$ и дополнить уже отмеченное (в том числе и диаграмму, выписанную в начале доказательства). В результате получается «дополненная» диаграмма, в которой указан соответствующий *единственный* гомоморфизм $\psi: \mathcal{D} \to A_i$ такой, что все $\pi_i = \psi\varphi_i$, согласно предполагаемому свойству Ω-*алгебры* $A$, но указан и единственный гомоморфизм $\varphi: A \to \mathcal{D}$, для которого все $\varphi_i = \varphi\pi_i$, согласно уже доказанному для прямого произведения $\mathcal{D} = \prod A_i$.



Но одновременно построен и гомоморфизм $\varphi\psi: A \to A$, для которого $(\varphi\psi)\varphi_i = \varphi_i$ для всех $\varphi_i: A \to A_i$ (так как $\psi\varphi_i = \pi_i$), а такой гомоморфизм *единственен*, согласно указанному свойству $\Omega$-*алгебры* $A$ и поэтому оказалось, что $\varphi\psi = \mathcal{E}_A$ (так как конечно справедливы равенства $\mathcal{E}_A\varphi_i = \varphi_i$). С другой стороны, построен и гомоморфизм $\psi\varphi: \mathcal{D} \to \mathcal{D}$, для которого справедливы равенства $(\varphi\psi)\pi_i = \pi_i$ (так как $\varphi\pi_i = \varphi_i$ и $\psi\varphi_i = \pi_i$), а поэтому $\psi\varphi = \mathcal{E}_{\mathcal{D}}$, согласно «единственности такого гомоморфизма», так как прямое произведение $\mathcal{D} = \prod A_i$обладает указанным свойством.

В результате получилось, что $\varphi\psi = \mathcal{E}_A$ и $\psi\varphi = \mathcal{E}_{\mathcal{D}}$, а поэтому гомоморфизмы $\varphi: A \to \mathcal{D}$ и $\psi: \mathcal{D} \to A$ оказались *обратными друг другу изоморфизмами*, для которых конечно известны и образы, то есть $A \approx A\varphi = \mathcal{D} = \prod A_i$ и $\mathcal{D} \approx \mathcal{D}\psi = A$. Поэтому оказалось, что $A = \prod A_i$ – прямое произведение с проектированиями $\varphi_i: A \to A_i = A\varphi_i$, с точностью до изоморфизма и уже доказано, что «указанное свойство характеризует прямое произведение $\mathcal{D} = \prod A_i$ с набором проектирований $\pi_i$, с точностью до изоморфизма» и это заканчивает доказательство.

Благодаря этой теореме получается ещё одна «рабочая конструкция» – вместе с прямым произведением $\mathcal{D} = \prod A_i$ возникают её подсистемы $\bar{A}$ такие, что $\bar{A}\pi_i = A_i = \mathcal{D}\pi_i$ сразу для всех проектирований $\pi_i: \mathcal{D} \to A_i$. При этом возможно, что $\bar{A} \neq \mathcal{D}$ и в этом случае говорят, что $\bar{A}$ – подпрямое произведение $\Omega$-*алгебр* $A_i$, в отличие от прямого произведения $\mathcal{D} = \prod A_i$. А благодаря отмеченному в доказательстве получается, что $\Omega$-*алгебра* $A$ *изоморфна подпрямому произведению* $\bar{A} \subseteq \prod A_i = \mathcal{D}$, когда имеются гомоморфизмы $\varphi_i: A \to A_i = A\varphi_i$ такие, что $\bigcap Ker\varphi_i = \Delta_A$.

Это можно считать «характеристикой» подпрямых произведений с точностью до изоморфизма, а если учесть теорему 9, то можно заметить, что если $\theta = \bigcap \theta_i$ для некоторого набора конгруэнций $\theta_i$ на $A = A(\Omega)$, то фактор-алгебра $A/\theta$ оказывается подпрямым

произведением фактор-алгебр $A/\theta_i$ с точностью до изоморфизма. С другой стороны, одним из примеров подпрямого, но не прямого произведения может служить $\Delta_B = B \times B$ для не одноэлементной $\Omega$-*алгебры* $B$ (но это можно и не пояснять, так как $B \approx \Delta_B \neq B \times B$).

Заканчивая набор «общих конструкций и утверждений» учтём, что специфика алгебраической системы $A = A(\Omega)$ обычно уточняется с помощью тождеств связывающих заданные на $A$ алгебраические операции $\omega \in \Omega$. При этом «понятие тождества» можно уточнять с помощью уже построенной $\Omega$-*алгебры* $W = \mathcal{W}(X, \Omega)$ предполагая, что алфавит $X = \{x_n | n \in \mathbb{N}\}$, то есть буквы занумерованы натуральными числами $n \in \mathbb{N}$ и что $\Omega$-*слова* $w(x_1, \dots, x_k)$, $v(x_1, \dots, x_k)$ равны только тогда, когда они «просто совпадают по записи и буквам». Именно поэтому $\Omega$ -*алгебру* $W = \mathcal{W}(X, \Omega)$ обычно называют *абсолютно свободной*, в том числе и потому, что в этой $\Omega$-*алгебре* имеются только тривиальные тождества.

Поясняя это получаем «естественное определение» тождества на $\Omega$ -*алгебре* $A$ – пара $(w, v) \in W \times W$ является тождеством $w(x_1, \dots, x_k) \equiv v(x_1, \dots, x_k)$ на $A = A(\Omega)$, если при любой подстановке $x_i \to a_i \in A$ всегда получается (уже на $A$) равенство $w(x_1, \dots, x_k) = v(x_1, \dots, x_k)$ . После этого можно учесть основное свойство $W = \mathcal{W}(X, \Omega)$ – эта $\Omega$ -*алгебра* $W$ *свободно порождена алфавитом* $X$ *в классе всех* $\Omega$-*алгебр*, и поэтому тождества на этой $\Omega$-*алгебре* тривиальны, хотя на других $\Omega$-*алгебрах* $A = A(\Omega)$ могут возникать и «не тривиальные тождества». Так, например, на одноэлементной $\Omega$-*алгебре* $0$ все пары $(w, v) \in W \times W$ оказываются тождествами, но это особый случай, что можно пояснить с помощью основного свойства уже построенной $\Omega$-*алгебры* $W = \mathcal{W}(X, \Omega)$, если учесть, что описаны все изоморфизмы, согласно теореме 5, а затем учесть и теорему 9 об «образах конгруэнций».

**Теорема 11.** Согласно основному свойству $W = \mathcal{W}(X, \Omega)$, каждое отображение $\xi: X \to A$ алфавита $X$ в $\Omega$-*алгебру* $A$ всегда

продолжается (и притом единственным образом!) до гомоморфизма $\varphi_\xi: W \to A$, и поэтому определяется и соответствующая конгруэнция $\sigma_\xi = Ker\varphi_\xi$. Применяя это получаем, что строится, согласно выписанному правилу, и конгруэнция $T(A,X) \subseteq W \times W$, причём оказывается, что $T(A,X)$ – это полный набор тождеств выполняющихся на алгебраической системе $A(\Omega)$.

$$T(A,X) = \bigcap \{\sigma_\xi | \xi: X \to A\}$$

При этом конгруэнция $G = T(A,X)$ оказывается вполне характеристической, то есть выдерживающий все эндоморфизмы $\Omega$-*алгебры* $W = \mathcal{W}(X,\Omega)$: если $(v,w) \in \sigma$, то $(v\psi, w\varphi) \in \sigma$ для любого эндоморфизма. Именно поэтому оказывается, что $T(A,X) = W \times W$ только для $A = \{0\} = O$.

***Действительно,*** согласно уже сказанному определению, если $(v,w) \in W \times W$ является тождеством на $A = A(\Omega)$, то для любого отображения $\xi: x_i \to a_i \in A$ получается (уже в $A$) равенство $v(a_1, \dots, a_k) = w(x_1, \dots, x_k)$, то есть $v\varphi_\xi = w\varphi_\xi$ или $(v,w) \in \sigma_\xi$, поэтому и получается, что конгруэнция $T(A,X)$ является полным набором тождеств выполняющихся на $A = A(\Omega)$. Иначе говоря, $(v,w)$ – тождество на $A = A(\Omega)$ тогда и только тогда, когда
$(v,w) \in \sigma = T(A,X)$, а потому оказывается, что $\sigma$ выдерживает все эндоморфизмы $\psi: W \to W$. Нужно только заметить, что если $v(x_1, \dots, x_k) \equiv w(x_1, \dots, x_k)$ – тождество на $A$, то
$v(u_1, \dots, u_k) \equiv w(u_1, \dots, u_k)$ – тоже тождество на $A = A(\Omega)$ для любой подстановки $x_i \to u_i \in W$, а это и означает, что мы применили соответствующий эндоморфизм $\psi: W \to W$, что и отмечено «формулировкой» теоремы. В частности, окажется, что

$T(A,X) = W \times W$, то $x_1 \equiv x_2$– тождество на $A$ и поэтому $a_1 = a_2$ для любых $a_1, a_2 \in A$, то есть эта $\Omega$-*алгебра* $A = \{0\} = O$ одноэлементна, что и отмечено в теореме.

Благодаря этой «уже доказанной» теореме определяются или сроятся многообразия $\mathfrak{M}_T$ заданные набором $T$ тождеств, как такие классы $\mathfrak{M}_T$, что $T \subseteq T(A,X)$ для $A \in \mathfrak{M}_T$, то есть из $\Omega$-*алгебр* $A$ на которые все $(v,w) \in T$ являются тождествами. При этом обычно предполагается, что многообразие $\mathfrak{M}_T$ *не вырождено*, то есть в этом $\mathfrak{M}_T$ имеются не одноэлементные $\Omega$-*алгебры* $A$. После этого можно учесть, что для любого семейства $\sigma_i$ вполне характеристических конгруэнций на $W = \mathcal{W}(X,\Omega)$ обычное пересечение $\bigcap \sigma_i = \sigma$ тоже является вполне характеристической конгруэнцией, причём $W \times W$ и $\Delta_W$ очевидно являются вполне характеристическими конгруэнциями, так как $T(O,X) = W \times W$ и $T(W,X) = \Delta_W$, что фактически уже отмечалось.

$$T(\mathfrak{M},X) = \bigcap \{T(A,X) | A \in \mathfrak{M}\}$$

С другой стороны, с любым классом $\mathfrak{M}$ связывается, согласно выписанному правилу, конгруэнция $T(\mathfrak{M},X)$ на $W = \mathcal{W}(X,\Omega)$ и это полный набор тождеств, выполняющихся на всех $A \in \mathfrak{M}$, тоже являющийся вполне характеристической конгруэнцией на $W$, согласно теореме 11 и по построению (как пересечение вполне характеристических конгруэнций). Кроме того, можно считать, что «многообразия образуют решётку», так как обычное пересечение многообразий очевидно является многообразием, вырожденное многообразие является наименьшим, а класс всех $\Omega$ -*алгебр* – наибольшим многообразием.

**Теорема 12.** Для конгруэнции $\sigma$ абсолютно на $W = \mathcal{W}(X,\Omega)$ равносильны указанные утверждения (и можно считать, что $\sigma \neq W \times W$):

***а***. Конгруэнция $\sigma$ является вполне характеристической.

***б***. Справедливо равенство $\sigma = T(A, X)$ для некоторой $\Omega$-*алгебры* $A$.

***в***. Для некоторого класса $\mathfrak{M}$ справедливо равенство $\sigma = T(\mathfrak{M}, X)$.

***г***. Равенство $\sigma = T(\mathfrak{M}, X)$ справедливо для некоторого многообразия $\mathfrak{M} = \mathfrak{M}_1$ $\boldsymbol{m_j = m_{j1}}$ (которое можно считать невырожденным).

***Действительно***, конгруэнция $W \times W$ является вполне характеристической, но соответствует только вырожденному многообразию, так как $T(O, X) = W \times W$, и поэтому можно предполагать «для нетривиальности», что конгруэнция $\sigma \neq W \times W$, то есть считать, что фактор-алгебра $\widehat{W} = W/\sigma$ не одноэлементна. Так и будем предполагать при доказательстве равносильности утверждений, указанных в формулировке теоремы.

Пусть $\sigma = T(\mathfrak{M}, X)$ для некоторого класса $\mathfrak{M}$. Строим многообразие $\mathfrak{M}_\sigma$ и замечаем, что *в*ключение $\mathfrak{M}_\sigma \supseteq \mathfrak{M}$ очевидно, в силу специфики $\sigma$ ($A \in \mathfrak{M} \Rightarrow T(A, X) \supseteq \sigma = T(\mathfrak{M}, X)$, по построению), но «почти очевидно» и равенство $T(\mathfrak{M}_\sigma, X) = \sigma$ именно потому, что $\sigma = T(\mathfrak{M}, X)$. Поэтому импликация ***в*** $\Rightarrow$***г*** доказана и утверждения ***в***, ***г*** равносильны, так как импликация ***г*** $\Rightarrow$ ***в*** очевидна (многообразие является классом!).

***б***$\Rightarrow$***в***. Если $\sigma = T(\mathfrak{M}, X)$, то для класса $\mathfrak{M}$ из всех $\Omega$-*алгебр* $B \approx A$ (или для класса всех $\Omega$-*алгебр* $B$ изоморфно вложимых в $A$, так как $T(B, X) \supseteq T(A, X)$ для таких $B$).

***в*** $\Rightarrow$ ***а***. Конгруэнция $\sigma = T(\mathfrak{M}, X)$ является вполне характеристической конгруэнцией на $W = \mathcal{W}(X, \Omega)$ и это уже отмечалось.

***а*** $\Rightarrow$ ***б***. Предполагая, что $\sigma$ – вполне характеристическая конгруэнция на $W$ и учитывая, что $\sigma \neq W \times W$ (согласно сказанному выше), строим не одноэлементную $\widehat{W} = W/\sigma$, применяя естественный гомоморфизм $\nu = \nu_\sigma : W \to \widehat{W} = W_\nu$. Затем учитываем, что $\widehat{W} = \langle \hat{X} \rangle_\Omega$ –

эта подсистема, порождённая подмножеством $\hat{X} = \{\hat{x} | x \in X\}$, совпадает с $\widehat{W}$, так как справедливо равенство $W = \langle X \rangle_\Omega$ для алфавита $X \subseteq W$.

Замечаем, что для различных букв $x, y \in X$ всегда различны и элементы $\hat{x}, \hat{y} \in \hat{X} = X\nu$, так как $\hat{v} = \hat{w}$ тогда и только тогда, когда $(v, w) \in \sigma = Ker\nu$, по построению гомоморфизма $\nu$, а затем учитывается вполне характеристичность конгруэнции $\sigma$.

В самом деле, если допустить, что $\hat{x} = \hat{y}$, хотя $x \neq y$, то получается, что $(x, y) \in \sigma$ и поэтому $(x\psi, y\psi) \in \sigma$ для любого эндоморфизма $\psi: W \to W$, так как конгруэнция $\sigma$ вполне характеристична. Но из-за различности букв $x, y \in X$ можно построить такое отображение $X \to W$, что $x\psi = v$ и $y\psi = w$ для произвольно выбранных $v, w \in W$, а затем продолжив это отображение до эндоморфизма (согласно основному свойству $W = \mathcal{W}(X, \Omega)$, указанному в теореме 5). В результате получится, что $(v, w) \in \sigma$, а из-за произвольности выбора получается, что $W \times W = \sigma$, хотя $\sigma \neq W \times W$.

Согласно специфике $\widehat{W} = \langle \hat{X} \rangle_\Omega = W(\sigma)$, для $\hat{u} \in \widehat{W}$ всегда существует $u(x_1, \dots, x_k) = u \in W$ такой, что $\hat{u} = u(\hat{x}_1, \dots, \hat{x}_k) = u\nu$, причём $u(\hat{x}_1, \dots, \hat{x}_k) = v(\hat{x}_1, \dots, \hat{x}_k) \Leftrightarrow (u, v) \in \sigma$, так как $\sigma = Ker\nu$ для гомоморфизма $\nu: W \to \widehat{W}$, что уже отмечалось. Учитывая, что строим отображение $\xi: X \to \widehat{W}$ и для каждого $x_i\xi = \hat{u}_i \in \widehat{W}$ фиксируем $u_i = u(x_1, \dots, x_k) \in W$, для которого $\hat{u}_i = u(\hat{x}_1, \dots, \hat{x}_k) = u_i\nu$. После этого возникла подстановка $x_i \to u_i \in W$, и из-за специфики $W$ эта подстановка *продолжается до эндоморфизма* $\psi: W \to W$, причём согласно правилу $\big(w(x_1, \dots, x_k)\big)\psi = w(u_1, \dots, u_k)$, но тогда получаются и равенства $\big(w(x_1, \dots, x_k)\big)\psi\nu = w(\hat{u}_1, \dots, \hat{u}_k)$.

Но тогда оказывается, что единственным гомоморфным продолжением отображения $\xi: X \to \widehat{W}$ является построенный гомоморфизм $\psi\nu: W \to \widehat{W}$. При этом получаются импликации

$(w, v) \in \sigma \Rightarrow (w\psi, v\psi) \in \sigma \Rightarrow (w\psi)\nu = (v\psi)\nu \Rightarrow (w, v) \in Ker\psi\nu,$

то есть получилось включение $\sigma \subseteq Ker\psi\nu$ из-за вполне характеристичности конгруэнции $\sigma$. Кроме того, $\sigma = Ker\nu$ и гомоморфизм $\nu$ является единственным гомоморфным продолжением отображения $x \to \hat{x}$ алфавита $X$ на $\hat{X}$, а в итоге оказалось, согласно теореме 11, что $T(\widehat{W}, X) = \sigma$ и поэтому импликация ***а⇒б*** доказана, что заканчивает доказательство теоремы 12.

**Теорема 13.** Каждой вполне характеристической конгруэнции $\sigma$ на $W = \mathcal{W}(X, \Omega)$ соответствует многообразие $\mathfrak{M}_\sigma$, и многообразию $\mathfrak{M}$ соответствует вполне характеристическая конгруэнция $T(\mathfrak{M}, X)$ на $W$.

$\mathfrak{M}_1 \subseteq \mathfrak{M}_2 \Leftrightarrow T(\mathfrak{M}_1, X) \supseteq T(\mathfrak{M}_2, X),$

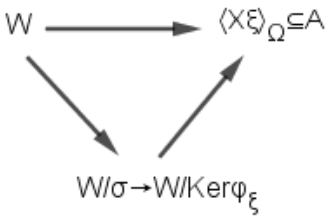
$\mathfrak{M}_{\sigma_1} \subseteq \mathfrak{M}_{\sigma_2} \Leftrightarrow \sigma_1 \supseteq \sigma_2.$

Эти переходы обратны друг другу, но получаются выписанные импликации: то есть включения заменяются на противоположные, а поэтому решётка многообразий $\Omega$ -*алгебр* «обратно изоморфна» решётке вполне характеристических конгруэнций $\Omega$-*алгебры* $W = \mathcal{W}(X, \Omega)$ свободно порождённой алфавитом $X$ в классе всех $\Omega$-*алгебр*. При этом, если $\sigma \neq W \times W$, то соответствующее многообразие $\mathfrak{M}$, для которого $\sigma = T(\mathfrak{M}, X)$ не вырождено, а соответствующая $\Omega$ -*алгебра* $\widehat{W} = W/\sigma$ *свободно порождается подмножеством* $\hat{X} \approx X$ *в многообразии* $\mathfrak{M}$, то есть для $\Omega$ -*алгебр* $A \in \mathfrak{M}$ каждое отображение $\hat{X} \to A$ всегда продолжается до гомоморфизма $\widehat{W}$ в $A$ (причём единственным образом!).

***Доказательство.*** Первое утверждение теоремы является почти очевидным следствием теоремы 12 и определений, а поэтому отметим только, что для вполне характеристической конгруэнции $\sigma$ на

$W = \mathcal{W}(X, \Omega)$ при $\sigma \neq W \times W$ получается, конечно, невырожденное многообразие $\mathfrak{M}_\sigma$, так как $\Omega$ -*алгебра* $\widehat{W} = W/\sigma$ порождается подмножеством $\hat{X} \approx X$ и попадает в $\mathfrak{M}_\sigma$, согласно равенству $T(\mathfrak{M}_\sigma, X) = \sigma = T(\widehat{W}, X)$. Это фактически отмечено в теореме 12 и её доказательстве, а поэтому остаётся пояснить специфику $\Omega$-*алгебры* $\widehat{W} = W/\sigma$.

Согласно уже отмеченному, $\widehat{W} \in \mathfrak{M} = \mathfrak{M}_\sigma$ и порождается своим подмножеством $\hat{X} \approx X$ (где учтена биекция $x \to \hat{x}$), причём справедливо равенство $\sigma = T(\mathfrak{M}, X) = T(\widehat{W}, X)$. Учитывая это, возьмём любое отображение $\xi: \hat{X} \to A$ в произвольную $\Omega$-*алгебру* $A \in \mathfrak{M}$ и будем рассматривать это отображение как отображение $\xi: X \to A$ (так как $\hat{X} \approx X$).




$$\langle \hat{X} \rangle_\Omega = \widehat{W} = W/\sigma \to W/Ker\varphi_\xi$$

Применяя специфику (указанную в теореме 5) получаем (согласно отмеченному в диаграмме) единственное гомоморфное продолжение $\varphi_\xi: W \to A$ отображения $\xi$, причём конечно получится равенство $W\varphi_\xi = \langle X\xi \rangle_\xi \subseteq A$ и изоморфизм $W\varphi_\xi \approx W/Ker\varphi_\xi$. Но из включения $A \in \mathfrak{M}$ вытекает
$Ker\varphi_\xi \supseteq T(A, X) \supseteq T(\mathfrak{M}, X) = \sigma = Ker\nu$, и потому строится

гомоморфизм $W/\sigma$ на $W/Ker\varphi_\xi$, который индуцирует гомоморфизм $\hat{\varphi}_\xi: \widehat{W} \to A$ (такой, что $\hat{v}\hat{\varphi}_\xi = \varphi_\xi$), а этот гомоморфизм и оказывается продолжением отображения $\xi: \hat{X} \to A$ (так как $\big(w(\hat{x}_1, \dots, \hat{x}_k)\big)\hat{\varphi}_\xi = w\big(x_{1\xi}, \dots, x_{k\xi}\big)$).

А из-за произвольности отображения $\xi: \hat{X} \to A$ и получается, что $\widehat{W} = \langle \hat{X} \rangle_\Omega \in \mathfrak{M}$ свободно порождается подмножеством $\hat{X}$ уже в многообразии $\mathfrak{M}$ (по определению!).

**Теорема 14.** Класс $\mathfrak{M}$ является многообразием тогда и только тогда, когда он замкнут относительно взятия подсистем, гомоморфных образов и прямых произведений (и это будет пояснено в доказательстве). При этом учитывается, что в невырожденном многообразии $\mathfrak{M}$ для любого алфавита $X$ всегда строится $\Omega$-*алгебра* $\widehat{W} = \langle \hat{X} \rangle_\Omega \in \mathfrak{M}$ свободно порождённая этим алфавитом, но в многообразии $\mathfrak{M}$.

***Доказательство***. Уточняя специфику многообразия $\mathfrak{M}$ можно считать, что это многообразие не вырождено и справедливо равенство $\mathfrak{M} = \mathfrak{M}_T$ для $T = T(\mathfrak{M}, X) \neq W \times W$, согласно теоремам 12 и 13. При этом, по определению $A \in \mathfrak{M}$ тогда и только тогда, когда $T(A, X) \supseteq T$, а затем можно учесть, что для подсистем$B$в$A$ всегда $T(B, X) \supseteq T(A, X)$ (тождества справедливы на $A$ справедливы и на подсистеме $B \subseteq A$) и всегда $T(\overline{A}, X) \supseteq T(A, X)$ для гомоморфных образов $\bar{A}$. Поэтому, если $A \in \mathfrak{M}$, то и её подсистема $B \in \mathfrak{M}$ и все гомоморфные образы $\bar{A} \in \mathfrak{M}$, а это и означает, что многообразие $\mathfrak{M}$ замкнуто относительно взятия подсистем и гомоморфных образов.

С другой стороны, по построению, операции $\omega \in \Omega$ переносятся с компонент $A_i$ на прямое произведение $\mathcal{D} = \prod A_i$ всегда «покомпонентно», так как проектирования $\pi: \mathcal{D} \to A_i = \mathcal{D}\pi_i$ являются гомоморфизмами. Поэтому и справедливость тождеств на $\mathcal{D}$ всегда «проверяется покомпонентно», а поэтому легко заметить, что

$\prod(\mathcal{D}, X) = \cap T(A, X)$. Но тогда оказывается, что если все $A_i \in \mathfrak{M} = \mathfrak{M}_T$ (то есть $T(A_i, X) \supseteq T$), то конечно и $\prod A_i = \mathcal{D} \in \mathfrak{M}$, а поэтому и оказывается, что многообразие $\mathfrak{M}$ замкнуто относительно прямых произведений. Одновременно оказывается, что многообразие $\mathfrak{M}$ замкнуто и относительно *подпрямых произведений*, так как они являются подсистемами прямых произведений.

Теперь допустим, что в классе $\mathcal{K}$ имеются не одноэлементные $\Omega$-*алгебры*, причём будем считать, что этот класс замкнут относительно подсистем и гомоморфных образов, а затем сравним класс $\mathcal{K}$ и многообразие $\mathfrak{M}_\sigma$, где вполне характеристическая конгруэнция $\sigma = T(\mathcal{K}, X) \neq W \times W$. Применяя теорему 13 легко заметить, что многообразие $\mathfrak{M}_\sigma$ порождено классом $\mathcal{K}$, то есть является наименьшим среди многообразий, содержащих $\mathcal{K}$, причём это равносильно равенству $T(\mathfrak{M}_\sigma, X) = \sigma = T(\mathcal{K}, X)$, что фактически уже было отмечено при доказательстве теоремы 12.

При этом неявно учитывается абсолютно свободная $\Omega$-*алгебра* $W = \mathcal{W}(X, \Omega)$ (свободно порождённая бесконечным алфавитом $X X$), так как мы применяем $T(\mathcal{K}, X) = \sigma$, а это полный набор тождеств справедливых на всех $A \in \mathcal{K}$ и на всех $\Omega$-*алгебрах* из многообразия $\mathfrak{M} = \mathfrak{M}_\sigma$, порождённые $\mathcal{K}$. Применяя сказанное и уже доказанное, учтём и равенства

$T(\mathcal{K}, X) = \{T(A, X) | A \in \mathcal{K}\}, T(A, X) = \{\sigma_\xi | \xi : X \to A\}$,

где применены ядра $\sigma_\xi = Ker\varphi_\xi$ гомоморфизмов $\varphi_\xi : W \to A$, как «единственных» гомоморфизмов продолжающих отображения $\xi : X \to A$, согласно специфике $W$. При этом, «мы просто учли определения», но ещё не учли, что класс $\mathcal{K}$ замкнут относительно взятия подсистем и гомоморфных образов. Учитывая и это, замечаем, что для заданных гомоморфизмов $\varphi_\xi : W \to A \in \mathcal{K}$ всегда

$W\varphi_\xi = \langle X\xi \rangle_\Omega \subseteq A$ и поэтому $W/\sigma_\xi \approx W\varphi_\xi \in \mathcal{K}$, так как $W\varphi_\xi$ – подсистема в $\Omega$-*алгебре* $A \in \mathcal{K}$.

В результате оказалось, что $T(\mathcal{K},X)=\sigma=T(\mathfrak{M}_\sigma,X)$, причём, $\sigma=\bigcap\{\sigma_j|W/\sigma_j\in\mathcal{K}\}$ для некоторого набора конгруэнций $\sigma_j$ на $W$, благодаря замкнутости класса $\mathcal{K}$ относительно взятия подсистем и гомоморфных образов. Но тогда получается, что *фактор-алгебра* $W/\sigma=\langle\hat{X}\rangle_\Omega$ *свободная в многообразии* $\mathfrak{M}_\sigma$ *оказывается подпрямым произведением некоторого семейства* $\Omega$*-алгебр* $W/\sigma_j\in\mathcal{K}$. Допуская теперь, что класс $\mathcal{K}$ замкнут и относительно прямых произведений, получаем и замкнутость относительно подпрямых произведений. Поэтому, согласно уже доказанному, в этой ситуации все $\Omega$*-алгебры свободные в многообразии* $\mathfrak{M}_\sigma$ *попадают в класс* $\mathcal{K}\subseteq\mathfrak{M}_\sigma$, и поэтому $\mathcal{K}=\mathfrak{M}_\sigma$, так как все $\Omega$*-алгебры* из $\mathfrak{M}_\sigma$ являются гомоморфными образами некоторых «достаточно больших» свободных в этом многообразии.

Именно поэтому и оказывается, что все классы $\mathcal{K}$, замкнутые относительно взятия подсистем, гомоморфных образов и прямых произведений всегда являются многообразиями, что заканчивает доказательство теоремы.

**Теорема 15.** Если многообразие $\mathfrak{M}$ порождено классом $\mathcal{K}$, замкнутым относительно взятия подсистем и гомоморфных образов (причём в $\mathcal{K}$ имеются не одноэлементные $\Omega$*-алгебры* – для невырожденности***m***), то все $\Omega$*-алгебры*, *свободные в многообразии* $\mathfrak{M}$ *являются подпрямыми произведениями некоторых* $\Omega$*-алгебр из* $\mathcal{K}$ (вместе с $W/T(\mathfrak{M},X)$, так как $T(\mathfrak{M},X)\equiv T(\mathcal{K},X)$). В частности, если $\mathcal{K}$ состоит из $\Omega$ *-алгебр*, изоморфно вложимых в не одноэлементную $\Omega$ *-алгебру* $A$, то свободные в многообразии $\mathfrak{M}=Var(\mathcal{K})$ $\Omega$ *-алгебры* изоморфно вкладываются в некоторую *прямую степень* $A^x$.

Всё отмеченное с очевидностью следует из теоремы 14 и фактически содержится в доказательстве этой теоремы, а последнее утверждение вытекает из того, что соответствующее многообразие

$\mathfrak{M} = Var(\mathcal{K})$ порождено Ω-*алгеброй* $A$, как наименьшее многообразие, содержащее $A$. При этом учесть, конечно, что прямая степень $A^I$ – это прямое произведение $\mathcal{D} = \prod_I A_i$ соответствующих $A_i \approx A$ (или копой $A$), а соответствующие свободные Ω-*алгебры* многообразия $\mathfrak{M}$ – это фактор-алгебры $\widehat{W} = W/\sigma$, где $\sigma = T(\mathcal{K}, X) = T(A, X)$.

На этом можно закончить «набор общих конструкций и утверждений» о произвольных Ω-*алгебрах* и многообразиях, но мы всё же дополним указанный «набор», применяя специфику вполне характеристических конгруэнций для построения более специальных многообразий. А именно: будем учитывать, с одной стороны, что любое многообразие $\mathfrak{M}$ (конечно невырожденное!) всегда задаётся соответствующей вполне характеристической конгруэнцией $\sigma = T(\mathfrak{M}, X) \neq W \times W$ абсолютно свободной Ω-*алгебры* $W = \mathcal{W}(X, \Omega)$, то есть всегда справедливо равенство $\mathfrak{M} = \mathfrak{M}_\sigma$, а с другой стороны, с каждой не одноэлементной Ω-*алгеброй* $A$ всегда можно связать многообразие $Var(A)$, как наименьшее (невырожденное!) многообразие, содержащее заданную Ω-*алгебру* $A$.

**Теорема 16.** Благодаря специфике абсолютно свободной $W = \mathcal{W}(X, \Omega)$, конечно, существуют вполне характеристические в $W$ конгруэнции $\sigma \neq W \times W$, причём для каждой такой конгруэнции $\sigma$ всегда существуют соответствующие максимальные вполне характеристические конгруэнции $T \supseteq \sigma$ (то есть такие, что строго больше $T$ только наибольшая конгруэнция $W \times W$). Поэтому в каждом невырожденном многообразии $\mathfrak{M}$ всегда содержатся минимальные многообразия $\mathfrak{M}_T$ (строго меньше которых только вырожденные многообразия), которые и задаются соответствующими максимальными вполне характеристическими конгруэнциями $T \supseteq T(\mathfrak{M}, X)$. При этом для минимального многообразия $\mathfrak{M}$ всегда найдутся

не одноэлементные $A \in \mathfrak{M}$, но при этом оказывается, что $\mathfrak{M} = Var(A)$ для любой не одноэлементной $A \in \mathfrak{M}$.

В самом деле, если $\sigma$ – вполне характеристическая конгруэнция на $W = \mathcal{W}(X, \Omega)$ и $\sigma \neq W \times W$, то это означает, что $(x_1, x_2) \notin \sigma$.Но тогда, если $\sigma$ не максимально, то найдётся вполне характеристическая конгруэнция $\sigma_1 \supset \sigma$, такая, что снова $(x_1, x_2) \notin \sigma_1$. Если и эта $\sigma_1$ не максимальна, то можно продолжить «процесс увеличения» и в результате возникает строго возрастающая цепочка вполне характеристических конгруэнций $\sigma \subset \sigma_1 \subset \cdots \subset \sigma_i \subset \cdots$ таких, что $(x_1, x_2) \notin \sigma_i$. Однако объединение такой цепочки снова оказывается вполне характеристической конгруэнцией, и поэтому оказывается, что существуют максимальные вполне характеристические конгруэнции $T \supseteq \sigma$. А это и означает, согласно уже доказанным теоремам, что каждое невырожденное многообразие $\mathfrak{M}_\sigma$, содержит некоторое минимальное многообразие $\mathfrak{M}_T$.

Это заканчивает доказательство теоремы, так как очевидно, что минимальное многообразие $\mathfrak{M}$ конечно содержит не одноэлементные $\Omega$-*алгебры* (из-за невырожденности!) и порождается любой своей не одноэлементной $\Omega$-*алгеброй* $A$ (уже из-за минимальности).

После этой теоремы иногда удаётся описать минимальные многообразия $\mathfrak{M}$ и его свободные $\Omega$-*алгебры*, после представления $\mathfrak{M} = Var(A)$ для некоторых специальных $\Omega$-*алгебр*. В частности, можно заметить, что если на $A$ имеются только две конгруэнции (это, конечно, $\Delta_A$ и $A \times A$), то многообразие $Var(A)$ окажется минимальным многообразием, а после этого получается и некоторое представление его свободных $\Omega$-*алгебр*, согласно теореме 16. Однако, в $\Omega$-*алгебрах* может и не быть максимальных конгруэнций (что можно показать на примерах), и поэтому существование указанных $\Omega$-*алгебр*, порождающих минимальные многообразия и содержащихся в многообразии $\mathfrak{M}$ уже требует доказательства, и поэтому зависит от специфики этого многообразия.

## §4. Натуральный ряд $\mathbb{N}$ и арифметические операции

Указанный набор «общих» конструкций и утверждений о произвольных $\Omega$-*алгебрах* можно применять для построения более конкретных алгебраических систем или уточнения их специфики. На самом деле это оказывается полезным (а иногда и необходимым!) даже при уточнении специфики «первых» или классических алгебраических систем, среди которых выделяется *натуральный ряд* $\mathbb{N}$ из *натуральных чисел*, так как он применяется, явно или неявно, для построения других алгебраических систем и при доказательстве «почти всех» утверждений (хотя это нужно уточнять).

Построение самого натурального ряда $\mathbb{N}$ (и натуральных чисел естественно возникающих при «счёте») и уточнение его специфики можно делать по разному, но обычно учитывают наиболее «очевидные» свойства натуральных чисел и соответствующие аксиомы (не требующие доказательства). Укажем только один набор аксиом (обычно называемых аксиомами Пеано), который оказывается «достаточным» для построения натурального ряда $\mathbb{N}$.

Можно считать очевидным, что *для каждого натурального числа* $n \in \mathbb{N}$ *всегда однозначно определяется непосредственно следующее натуральное число* $n' \in \mathbb{N}$, то есть на множестве $\mathbb{N}$ задана унарная операция $n \to n'$ взятия (или построения) непосредственно следующего натурального числа. После этого можно учесть набор аксиом, уточняющих свойства этой операции и натурального ряда $\mathbb{N}$ как множества натуральных чисел.

***а.*** Выделяется «первое» натуральное число $1 \in \mathbb{N}$, которое не следует ни за каким другим, то есть такое, что $1 \neq n'$ для всех $n \in \mathbb{N}$.

***б.*** Для натуральных чисел $m, n \in \mathbb{N}$ всегда $m = n \Rightarrow m' = n'$, но справедливо и «обратное», то есть всегда $m' = n' \Rightarrow m = n$.

***в.*** Если $1 \in A \subseteq \mathbb{N}$ и всегда $n \in A \Rightarrow n' \in A$, то $A = \mathbb{N}$.

Оказывается, что указанных аксиом «уже достаточно» для построения натурального ряда $\mathbb{N}$, а последняя аксиома ***в***, обычно

называемая «аксиомой математической индукции», позволяет производить построения и доказательства «по индукции». Именно это и приводит к построению наиболее известных операций на натуральном ряде $\mathbb{N}$ вместе с уточнением их свойств, причём строится и естественный «линейный» порядок для натуральных чисел.

А именно, благодаря указанной операции $n \to n'$, на $\mathbb{N}$ строится (уже бинарная!) операция сложения или построения суммы натуральных чисел, согласно следующим правилам:

1) Для любого натурального числа $m \in \mathbb{N}$ всегда $m + 1 = m'$.

2) Если для $n, m \in \mathbb{N}$ уже построена сумма $n + m \in \mathbb{N}$, то однозначно строится и следующая сумма $n + m' = (n + m)'$.

В результате оказывается, что для любых $n, m \in \mathbb{N}$ всегда однозначно определяется или строится сумма $n + m \in \mathbb{N}$, благодаря указанному «индуктивному построению» (для $n \in \mathbb{N}$ учитывается множество $A$ всех таких $m \in \mathbb{N}$, что определена сумма $n + m \in \mathbb{N}$, причём однозначно и получается, что $1 \in A$, согласно первому правилу и $m \in A \Rightarrow m' \in A$, согласно второму правилу, и поэтому оказывается, что $A = \mathbb{N}$). Уточняя специфику уже построенной операции сложения, обратим внимание на то, что во втором правиле фактически отмечено равенство $n + (m + 1) = (n + m) + 1$, справедливые для всех натуральных чисел $n, m \in \mathbb{N}$, а в частности получается и равенство $1 + (1 + 1) = (1 + 1) + 1$. А после этого легко получается обобщение этих равенств, отражающее специфику указанной операции сложения или алгебраической системы $\mathbb{N}(+)$.

**Утверждение 1.** Для операции сложения на натуральном ряде $\mathbb{N}$ справедливы выписанные равенства – законы ассоциативности и коммутативности сложения.

$\forall n, m, k \in \mathbb{N} | n + (m + k) = (n + m) + k, n + m = m + n$

$n + m = n + k \Leftrightarrow m = k \Leftrightarrow m + n = k + n$

Кроме того, получается и выписанный закон сокращения, а в результате получается и естественный линейный порядок на натуральном ряде $\mathbb{N}$.

В самом деле, рассматривая множество всех таких $k \in \mathbb{N}$, что $n + (m + k) = (n + m) + k$, для произвольно заданных $n, m \in \mathbb{N}$, получаем, что в этом множестве $A$ содержится единица 1 и легко проверяется, что $k \in A \Rightarrow k + 1 \in A$. Но тогда «доказываем по индукции», что и поэтому справедлив закон ассоциативности. После этого, учитывая «очевидные» равенства $1 + 1 = 1 + 1$ и $1 + (1 + 1) = (1 + 1) + 1$ и снова «применяя индукцию» получаем закон коммутативности. Аналогично доказывается и закон сокращения, так как в аксиоме ***a*** уже отмечено, что $m = n \Leftrightarrow m + 1 = n + 1$ (а затем применяется уже доказанное).

После этого для натуральных чисел $x, y \in \mathbb{N}$ полагаем, что $x < y$, когда $y = x + m$ для некоторого $m \in \mathbb{N}$ и $x \leq y$, когда $x < y$ или $x = y$. В результате оказывается (благодаря уже указанным законам), что для $m, n \in \mathbb{N}$ всегда $m < n$ либо $m = n$, либо $n < m$ (или $m > n$), а если $m \leq n$ и $n \leq k$, то $m \leq k$. В результате и получается естественный линейный порядок для натуральных чисел, а натуральный ряд $\mathbb{N}$ весьма «наглядно» представляется в виде выписанной цепочки

$$1 < 2 = 1 + 1 < 3 = 2 + 1 < \cdots < m < m + 1 < \cdots$$

где фактически указаны все натуральные числа и их построение. А именно, получается, что наибольшего натурального числа нет (и поэтому ряд $\mathbb{N}$ бесконечен!), но наименьшим является *единица* $1 \in \mathbb{N}$, а все остальные «последовательно» строятся прибавлением единицы.

**Утверждение 2.** Относительно указанного естественного линейного порядка, натуральный ряд $\mathbb{N}$ является вполне упорядоченным множеством, то есть в каждом непустом $A \subseteq \mathbb{N}$ всегда имеется наименьший элемент $a \in A$ –

такой, что $a \leq b$ для всех $b \in A$ (и конечно единственный!)

Действительно, в заданном непустом $A \subseteq \mathbb{N}$ конечно существует хотя бы одно натуральное число $n \in A$ и если этот элемент не является наименьшим в $A$, то найдётся $m \in A$ такой, что $m < n$, то есть можно начать «процесс уменьшения» оставаясь в $A$. Но этот «процесс» заканчивается за конечное число шагов, доходя до наименьшего $a \in A$, который оказывается и единственным, согласно уже выписанному представлению натуральных чисел ряда $\mathbb{N}$.

Применяя уже построенную операцию сложения, легко построить и операцию умножения на $\mathbb{N}$ или произведения натуральных чисел, согласно следующим правилам (дополняющих предыдущие):

3) Для любого натурального числа $m \in \mathbb{N}$ всегда $m \cdot 1 = m$.

4) Если для $m, n \in \mathbb{N}$ уже построено произведение $m \cdot n \in \mathbb{N}$, то однозначно строится и следующее произведение
$m \cdot (n + 1) = m \cdot n + m$.

В результате оказывается, что для любых $m, n \in \mathbb{N}$ всегда однозначно определяется или строится произведение $m \cdot n \in \mathbb{N}$, благодаря указанному «индуктивному построению», где конечно учтена и операция сложения. Более того, благодаря специфике, оказывается, что «операция умножения сводится к сложению».

**Утверждение 3.** Операция умножения на натуральном ряде $N$ дистрибутивна относительно операции сложения, то есть всегда справедливы выписанные законы дистрибутивности.

$\forall n, m, k \in \mathbb{N} | n \cdot (m + k) = n \cdot m + n \cdot k,$

Более того, если учесть равенства

$m \cdot 1 = m = 1 + \cdots + 1 = 1 \cdot m$ для натуральных чисел $m \geq 2$, то для умножения получаются законы ассоциативности, коммутативности и сокращения такие

же, как для сложения, так как операция умножения на $N$ просто сводится к сложению (!).

$n \cdot (m \cdot k) = (n \cdot m) \cdot k, n \cdot m = m \cdot n,$

$n \cdot m = n \cdot k \Leftrightarrow m = k \Leftrightarrow m \cdot n = k \cdot n.$

В самом деле, указанные законы дистрибутивности умножения относительно сложения легко «доказываются по индукции», так как после равенств $m \cdot (n+1) = m \cdot n + m$ получаются равенства $m \cdot (n+2) = m \cdot (n+1) + m = m \cdot n + m + m$ (и так далее), то есть $m \cdot k = m + \cdots + m$ ($k$ раз) при $k \geq 2$, вместе с $m \cdot 1 = m$. При этом мы конечно учли законы ассоциативности и коммутативности для сложения, а благодаря законам дистрибутивности умножения относительно сложения уже получилось, что операция умножения на натуральном ряде $\mathbb{N}$ просто сводится к операции сложения. А после этого конечно получается, что для умножения справедливы законы ассоциативности, коммутативности и сокращения «такие же» как для сложения.

После уже доказанных утверждений легко получается, что построенные «арифметические» операции сложения и умножения согласованы с естественным линейным порядком на $\mathbb{N}$,

$(m_1 \leq n_1, m_2 \leq n_2) \Rightarrow (m_1 + m_2 \leq n_1 + n_2, m_1 \cdot m_2 \leq n_1 \cdot n_2),$

то есть справедливы выписанные импликации (причём из строгих неравенств получаются такие же строгие неравенства). С другой стороны, благодаря умножению, естественно возникает *отношение делимости* на натуральном ряде $\mathbb{N}$, которое оказывается частичным порядком, но уже не линейным.

А именно, говорят, что натуральное число $m \in \mathbb{N}$ делится на натуральное число $k \in \mathbb{N}$, если $m = k \cdot n$ для некоторого $n \in \mathbb{N}$. Это можно записывать по разному и иногда применяется запись $m \vdots k$ и тогда оказывается, например, что $m \vdots m$ и $m \vdots 1$. При этом, конечно, если $m \vdots n$ и $n \vdots k$, то $m \vdots k$, а если $m \vdots n$ и $n \vdots m$, то конечно получается, что $m = n$ (хотя бы потому, что $m \geq n$ и $n \geq m$ в этом

случае). Именно поэтому *отношение делимости на* $\mathbb{N}$ *является частичным порядком*, но этот порядок не линеен хотя бы потому, что $m+2$ не делится на $m+3$ и $m+3$ не делится на $m+2$ для любого натурального числа $m \in \mathbb{N}$, так как единица $1 \in \mathbb{N}$ не делится на все остальные натуральные числа $n \in \mathbb{N}$ (то есть $n \geq 2$).

После этого легко заметить, что в натуральном ряде $\mathbb{N}$ естественно выделяются простые числа $p \in \mathbb{N}$ – такие $p \neq 1$, что $p$ делится только на $p$ и на $1$. Более того, первые простые числа легко указать и это $2 = 1 + 1$, $3 = 2 + 1$, $5 = 2 \cdot 2 + 1$, $7 = 2 \cdot 3 + 1$,…, а затем можно заметить, что простых чисел бесконечно много, причем каждое непростое число $m \geq 2$ всегда представляется в виде произведения $m = p_1 \dots p_k$ простых чисел, причём единственным образом, с точностью до перестановки сомножителей (но это доказать сложнее, и это было известно ещё Эвклиду!).

В результате оказывается, что построенные алгебраические системы $\mathbb{N}(+)$ и $\mathbb{N}(\cdot)$ весьма различны хотя бы потому, что $\mathbb{N}(+)$ порождается одним элементом $1 \in \mathbb{N}$ (что очевидно благодаря наглядному представлению $\mathbb{N}(+)$, а $\mathbb{N}(\cdot)$ *не порождается даже любым своим конечным подмножеством* (из-за бесконечного множества простых чисел). Всё это можно пояснять, но уже показано, что с помощью натурального ряда $\mathbb{N}$ получаются разнообразные алгебраические системы (в том числе $\mathbb{N}(+)$, $\mathbb{N}(\cdot)$, $\mathbb{N}(+,\cdot)$, но можно строить и многие другие!), но оказывается, что возникающие методы построения и доказательств фактически применяются и при уточнении специфики произвольных алгебраических систем.

## §5. Многообразие группоидов

Можно применить сказанное и набор «общих конструкций и утверждений» о произвольных Ω-*алгебрах*, рассматривая случай, когда $\Omega$ состоит только из одной бинарной операции. Иначе говоря, будем строить группоиды. Иначе говоря, будем строить *группоиды* $G = G(\cdot)$ – *это непустые множества, на которых задана одна бинарная операция* (обычно называемая умножением), то есть для любых двух элементов $x, y \in G$ однозначно определяется элемент $x \cdot y \in G$, как результат этой операции. При этом оказывается, что «если не предполагать заранее тождеств», то легко строятся разнообразные группоиды.

Для начала замечаем, что на группоиде $G = \{a, b\}$ из двух элементов имеются *только две конгруэнции* (это $G \times G$ и $\Delta_G$, конечно), так как для гомоморфизма $\varphi: G \to G\varphi$ либо $a\varphi = b\varphi$ и тогда группоид $G\varphi$ одноэлементен (ядро $Ker\varphi = G \times G$ ), либо $a\varphi \neq b\varphi$ и тогда оказывается, что $G \approx G\varphi$ (потому, что $Ker\varphi = \Delta_G$), так как «имеются только два элемента». Однако эти группоиды весьма разнообразны, что можно уточнять применяя «таблицы умножения» указанного вида.

| $\cdot$ | $a$ | $b$ |
|---|---|---|
| $a$ | $a \cdot a$ | $a \cdot b$ |
| $b$ | $b \cdot a$ | $b \cdot b$ |

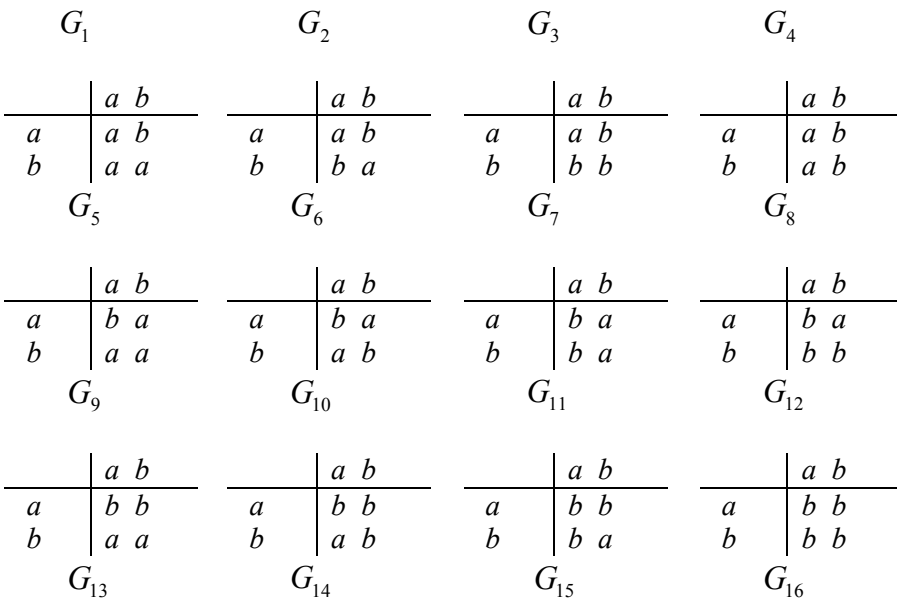
При этом строятся все возможные таблицы, в которых $x \cdot y = \{a, b\}$, что легко делается. Всего получается 16 таблиц, а разнообразие построенных группоидов уточняется с помощью подгруппоидов (очевидных благодаря таблицам) или с помощью тождеств, которые можно «увидеть» благодаря таблицам, что тоже уточняет специфику построенных группоидов «с точностью до изоморфизма».

| | $a$ $b$ |
|---|---|
| $a$ | $a$ $a$ |
| $b$ | $a$ $a$ |

| | $a$ $b$ |
|---|---|
| $a$ | $a$ $a$ |
| $b$ | $a$ $b$ |

| | $a$ $b$ |
|---|---|
| $a$ | $a$ $a$ |
| $b$ | $b$ $a$ |

| | $a$ $b$ |
|---|---|
| $a$ | $a$ $a$ |
| $b$ | $b$ $b$ |




Более того, единственно возможный изоморфизм действует, конечно, по правилу $a \to b$, $b \to a$ и поэтому *получается* 10 *попарно не изоморфных группоидов* – это $G_1 \approx G_{16}$, $G_2 \approx G_7$, $G_3 \approx G_{12}$, $G_4, G_5 \approx G_{14}$ , $G_6 \approx G_{10}$ , $G_8, G_9 \approx G_{15}, G_{11}, G_{13}$ . Одновременно оказывается, что в группоидах $G_9, G_{11}, G_{13}$ имеется *только* 1 *подгруппоид* и это «очевидно» благодаря их таблицам умножения, в $G_1, G_3, G_5, G_6$ возникает 2 *подгруппоида*, так как $\{a\}$ оказывается наименьшим подгруппоидом, а в $G_2, G_4, G_8$ , наименьшего подгруппоида нет и *возникает* 3 *подгруппоида*.

Кроме того, благодаря таблицам легко увидеть, что на группоидах $G_1$ и $G_{16}$ , справедливо *тождество* $x_1x_2 \equiv x_3x_4$ , которое и обеспечивает изоморфизм $G_1 \approx G_{16}$, но очевидно, что это тождество нарушается в остальных группоидах. С другой стороны, $G_4$ и $G_8$ не изоморфны, так как в $G_4$ очевидно справедливо *тождество* $x_1 \cdot x_2 \equiv$

$x_1$, а в $G_8$ очевидно тождество $x_1 x_2 \equiv x_2$. Чуть сложнее увидеть, что в группоиде $G_2$ справедливо тождество $(x_1 \cdot x_2) \cdot (x_1 \cdot x_2) \equiv x_1 \cdot x_2$, которое нарушается в группоиде $G_6$, а в $G_6$ почти очевидно тождество $x_1 \cdot (x_2 \cdot x_2) \equiv x_1$, которое нарушается в $G_2$. При этом в группоидах $G_1, G_2, G_6$ очевидно общее *тождество* $x_1 \cdot x_2 \equiv x_2 \cdot x_1$, которое нарушается в $G_4$ и $G_8$, а затем можно увидеть *тождество* $x_1 \cdot (x_2 \cdot x_3) \equiv (x_1 \cdot x_2) \cdot x_3$, которое оказывается общим для группоидов $G_1, G_2, G_4, G_6, G_8$.

Немного сложнее указать «специальные» тождества для группоидов $G_3, G_5, G_9, G_{11}$ и $G_{13}$, на которых *нарушается* тождество $x_1 \cdot (x_2 \cdot x_3) \equiv (x_1 \cdot x_2) \cdot x_3$, так как, например, $(b \cdot a) \cdot b = a \neq b = b \cdot (a \cdot b)$ на группоиде $G_5$. Однако можно «увидеть», что в группоиде $G_{11}$ справедливо *тождество* $x \cdot (x \cdot x) \equiv x$, которое нарушается в группоиде $G_{13}$, где справедливо *тождество* $(x \cdot x) \cdot x \equiv x$. Затем можно увидеть тождество $(x \cdot x) \cdot (x \cdot x) \equiv x$ общее для группоидов $G_9, G_{11}$ и $G_{13}$, но на $G_9$ очевидно тождество $x_1 \cdot x_2 \equiv x_2 \cdot x_1$, которое нарушается в группоидах $G_3, G_5, G_{11}$ и $G_{13}$. Кроме того, на $G_3$ можно «увидеть» *тождество* $(x_1 \cdot x_1) \cdot x_1 = (x_2 \cdot x_2) \cdot x_2$, а на $G_5$ - *тождество* $x_1 \cdot (x_1 \cdot x_1) = x_2 \cdot (x_2 \cdot x_2)$, но всё это получилось из-за того, что мы рассматривали группоиды $G = \{a, b\}$, имеющие только два элемента.

После этого строятся и другие «интересные» группоиды из уже построенных. Так, например, группоид из 4-х элементов $s, y, z, t$, с указанной таблицей умножения имеет только *один подгруппоид*, что почти очевидно.

| | *s* | *y* | *z* | *t* |
|---|---|---|---|---|
| *s* | *t* | *t* | *y* | *y* |
| *y* | *z* | *z* | *s* | *s* |
| *z* | *t* | *t* | *y* | *y* |
| *t* | *z* | *z* | *s* | *s* |

На самом деле этот группоид построен (!) как прямое произведение $G_{11} \times G_{13}$, и поэтому имеет 4 элемента $s = (a, a)$, $y = (a, b)$, $z = (b, a)$, $t = (b, b)$. Но тогда получается, что этот группоид гомоморфно отображается, благодаря проектированиям, на группоиды $G_{11}$ и $G_{13}$, которые не изоморфны (согласно уже отмеченному). Поэтому на этом группоиде из 4-х элементов возникает 4 *конгруэнции*, хотя на группоидах $G_{11}$ и $G_{13}$, тоже с одним подгруппоидом, возникают только две конгруэнции.

Оказывается «интересен» и группоид $G_{11} \times G_{11}$ (хотя бы потому, что с его помощью строятся конгруэнции на группоиде $G_{11}$) тоже имеющий 4 элемента, как уже построенный. Для этого группоида из «тех же» 4 элементов $s = (a, a)$, $y = (a, b)$, $z = (b, a)$, $t = (b, b)$, получается таблица умножения, имеющая указанный вид (существенно отличный от предыдущего!).

| | *s* | *y* | *z* | *t* |
|---|---|---|---|---|
| *s* | *t* | *z* | *y* | *s* |
| *y* | *t* | *z* | *y* | *s* |
| *z* | *t* | *z* | *y* | *s* |
| *t* | *t* | *z* | *y* | *s* |

Благодаря этой таблице легко увидеть, что в построенном группоиде *имеются* 3 *подгруппоида* – кроме наибольшего возникает подгруппоид $\{s, t\}$ (и это наименьшая конгруэнция на $G_{11}$) и изоморфный ему подгруппоид $\{y, z\}$ (а этот подгруппоид в $G_{11} \times G_{11}$ конгруэнцией не является!). указанные подгруппоиды различны, но изоморфны группоиду $G_{11}$, а после этого «можно увидеть», что на группоиде $G_{11} \times G_{11}$ *возникают* 3 *конгруэнции* именно потому, что «его компоненты» изоморфны (хотя и не совпадают).

С другой стороны, построение группоида $G_{11}$ подсказывает, что *для любого натурального числа* $k + 1 \geq 3$ всегда существует группоид $H_{k+1}$, имеющий точно $k + 1$ элемент, но *только* 1 *подгруппоид и*

*только* 2 *конгруэнции*. Можно выписать соответствующую таблицу умножения для элементов $x_1, \dots, x_k, x_{k+1}$ этого группоида, но «проще описать» эту таблицу. А именно, если $1 \le n \le k$, то на «диагонали» последовательно записываются равенство $x_{k+1} \cdot x_{k+1} = x_1$. Выше диагонали записываются равенства $x_i \cdot x_{i+s} = x_1$, а ниже диагонали $x_{i+s} \cdot x_i = x_{i+1}$.

Уже «диагональные» равенства с очевидностью показывают, что в $H_{k+1}$ имеется только 1 подгруппоид (точно так же, как в группоиде $G_{11}$), так как получается, что $H_{k+1} = \langle x_i \rangle$ порождается любым своим элементом. Немного сложнее увидеть, что в группоиде $H_{k+1}$ имеются только две конгруэнции, то есть доказать, что для гомоморфизма $\varphi: H_{k+1} \to H_{k+1}\varphi$ либо всегда $x_i\varphi \ne x_{i+s}\varphi$ (и тогда $H_{k+1} \to H_{k+1}\varphi$), либо $x_i\varphi = x_{i+s}\varphi$ для некоторых различных элементов $x_i, x_{i+s} \in H_{k+1}$. Но во втором случае сначала получается, что $x_{i+1}\varphi = x_i\varphi \cdot x_i\varphi = x_i\varphi \cdot x_{i+s}\varphi = x_1\varphi$, а затем через «некоторое число шагов» получится, что всегда $x_i\varphi = x_j\varphi$, то есть подгруппоид и гомоморфный образ $H_{k+1}\varphi$ одноэлементен (и $Ker\varphi = H_{k+1} \times H_{k+1}$).

Несколько неожиданно и проще оказалось, что существуют или строятся *бесконечные группоиды* $H = \{x_1, x_2, x_3, \dots, x_m, x_{m+p}, \dots\}$, но с таким же свойством, то есть *имеющие только один подгруппоид и только две конгруэнции*. При этом можно даже легко выписать соответствующую таблицу умножения, но всё же проще её описать. А именно, на «диагонали» последовательно записываются *равенства* $x_m \cdot x_m = x_{m+1}$ *для всех* $m \in \mathbb{N}$, а выше записываются *равенства* $x_i \cdot x_{i+s} = x_1$, что оказывается уже достаточным (все остальные равенства $x_{i+s} \cdot x_i = x_j \in H$ произвольны).

В самом деле, если $B$ – подгруппоид в $H$, то существует хотя бы один элемент $x_i \in B$, но тогда и $x_{i+1} = x_i \cdot x_i \in B$. После этого получается, что $x_1 = x_i \cdot x_{i+1} \in B$ и становится очевидным, что все элементы $x_m \in B$, и поэтому в группоиде $H$ *имеется только один подгруппоид*. С другой стороны, если $x_i\varphi = x_{i+s}\varphi$ для гомоморфизма

$\varphi: H \to H\varphi$ и некоторых различных $x_i, x_{i+s} \in H$, то оказывается, что $x_{i+1}\varphi = x_i\varphi \cdot x_i\varphi = x_i\varphi \cdot x_{i+s}\varphi = x_1\varphi$. После этого получается, что $x_2\varphi = x_1\varphi \cdot x_1\varphi = x_1\varphi \cdot x_{i+1}\varphi = x_1\varphi$ , и поэтому справедливы равенства $x_2\varphi \cdot x_2\varphi = x_1\varphi \cdot x_1\varphi$ , то есть $x_3\varphi = x_2\varphi = x_1\varphi$ и становится очевидным, что всегда $x_i\varphi = x_j\varphi$. А в итоге оказалось, что в этом случае группоид $H\varphi$ одноэлементен и поэтому ядро $Ker\varphi = H \times H$ . Поэтому в группоиде $H$ *имеются только две конгруэнции*, так как если для гомоморфизма $\varphi: H \to H\varphi$ всегда $x_i\varphi \neq x_{i+s}\varphi$, то $H\varphi \approx H$, так как в этом случае $Ker\varphi = \Delta_H$.

А учитывая, что равенство можно «задавать произвольно», мы построили на самом деле, даже бесконечно много группоидов $H$, имеющих только один подгруппоид и только две конгруэнции – таких «построенных» группоидов оказалось столько же, сколько непустых подмножеств в множестве $\{x_m | m \in \mathbb{N}\}$. В результате уже построены разнообразные группоиды (начиная с двухэлементных) и примеры тождеств, и поэтому возникают разнообразные многообразия группоидов.

При этом для построения всех многообразий нужно учесть, согласно теореме 13, *абсолютно свободный группоид* $W = \mathcal{W}(X)$, то есть свободно порождённый алфавитом в классе или многообразии всех группоидов, так как именно с его помощью строятся *полные наборы* $T = T(A, X)$ *тождеств* на любом группоиде $A$, согласно теореме 11. Точнее, указанные $T = T(A, X)$ – это все *вполне характеристические конгруэнции* на $W = \mathcal{W}(X)$ , которые и определяют все многообразия, согласно теореме 12. Но применяя указанные «общие теоремы и конструкции» нужно пояснить построение абсолютно свободного группоида $W$ и его специфику, по сравнению с «общим» построением $\mathcal{W}(X, \Omega)$.

На самом деле специфика только в том, что на группоидах применяется единственная (бинарная!) операция и для её записи вместо $xy\cdot$ учитывается «естественная» запись $x \cdot y$ или даже $xy$.

Однако для точной записи более длинных произведений уже нужно «расставлять скобки и делать это правильно», что и учитывается при построении абсолютно свободного группоида $\mathcal{W}(X)$. При этом учитывается, конечно, и *множество* $\mathcal{S}(X)$ *всех слов над алфавитом* $X$ с длинами $d(w) \geq 1$, но применяя это можно учесть, что на $\mathcal{S}(X)$ возникает *операция приписывания* – для любых слов $u, v \in \mathcal{S}(X)$ однозначно строится слово $uv \in \mathcal{S}(X)$ простым приписыванием. Одновременно получается, что $d(uv) = d(u) + d(v)$ (так как в записи слов скобки отсутствуют!), а затем учитывается, что элемент из $\mathcal{W}(X)$ и получаются с помощью «расстановок скобок» на соответствующих словах из $\mathcal{S}(X)$.

Уточняя отмеченное, при построении элементов $w \in \mathcal{W}(X)$ можно «расставлять скобки почти сначала» и тогда буквы $x_i \in X$ остаются элементами длины 1, а затем строятся элементы $(x_i x_j) \in X$ длины 2, соответствующие словам $x_i x_j \in \mathcal{S}(X)$, на которых «расставлены скобки» – одна открывающая скобка «(» и одна закрывающая скобка «)». После этого из слова $x_i x_j x_k \in \mathcal{S}(X)$, получается уже два элемента $\big(x_i(x_j x_k)\big), \big((x_i x_j)x_k\big) \in \mathcal{W}(X)$ длины 3 и уже можно указать «индуктивный процесс» порождения всех элементов из $\mathcal{W}(X)$ и правильных расстановок скобок.

А именно, если уже построены элементы с длинами $d \leq m$, то следующие элементы, с длиной $m+1$, всегда *однозначно записываются в виде* $w \equiv (uv) \in W$ для однозначно определяемых (элементом $w$) элементов $w, v \in \mathcal{W}(X)$ таких, что
$d(u) + d(v) = m + 1 = d(w)$. При этом вместе с «правильными расстановками скобок» на уже построенных $u, v \in \mathcal{W}(X)$ получается и «правильная расстановка скобок» на $w \equiv (uv)$. Но нужно учитывать, что $w = u \cdot v \in W$ оказывается произведением именно указанных элементов $u, v \in \mathcal{W}(X)$, то есть $(uv) = (u_1 v_1)$ тогда и только тогда, когда $u = u_1$, $v = v_1$, согласно однозначности записи элемента $w \in W$.

Указанный «процесс порождения» оказывается чуть проще в ходе построения абсолютно свободного группоида $W_1 = W(\{x\})$, так как в этом случае всё сводится к «правильным расстановкам скобок» на соответствующих словах $x, xx, xxx, xxxx, \ldots$ над алфавитом $\{x\}$. При этом получается один элемент $x \in W$, длины 1, один элемент длины 2 и это $(xx) \in W$, затем получаются уже две «правильные расстановки скобок» на слове $xx \in \mathcal{S}(\{x\})$ и строятся элементы $\big(x(xx), \big((xx)x\big)\big) \in W_1$ длины 3 (и так далее), согласно «индуктивному процессу». Таким образом, элементы из $W_1$, начиная с длины 3, представляются в виде $w = (uv)$ для уже построенных однозначно определяемых $u, v \in W_1$ и легко увидеть, например, что в записи $w = \langle uv \rangle \in W_1$ возникает точно $d(w) - 1$ открывающих и $d(w) - 1$ закрывающих скобок.

**Предложение 1.** Специфику абсолютно свободного группоида $\mathcal{W}(X)$ весьма точно отражают соответствующие гомоморфизмы $\mathbf{1}: \mathcal{W}(X) \to W_1 = W(\{x\})$ и $\boldsymbol{s}: \mathcal{W}(X) \to \mathcal{S}(X)$, продолжающие отображения $X \to \{x\} \subseteq W_1$ и тождественные вложения алфавита $X$ в $\mathcal{S}(X)$. А именно, для каждого $x \in W$ элемент $w\mathbf{1} \in W_1 = W\mathbf{1}$ фактически указывает «правильную расстановку скобок» (одинаковую на $w$ и $w\mathbf{1} \in w(x, \ldots, x)$, а элемент $w\boldsymbol{s} \in \mathcal{S}(X) = W\mathbf{s}$ – это слово соответствующее $W$ (получаемое «стиранием скобок», так как их нет в словах над $X$). Поэтому отображение $w \to (w\boldsymbol{s}, w\mathbf{1})$ оказывается *изоморфным вложением* абсолютно свободного группоида $\mathcal{W}(X)$ в прямое произведение $\mathcal{S}(X) \times W_1$ свободной полугруппы $\mathcal{S}(X)$ на абсолютно свободный группоид $W_1 = W(\{x\})$ и представляет $\mathcal{W}(X)$ как *подпрямое произведение* $\mathcal{S}(X)$ и $W_1$, с точностью до изоморфизма. Одновременно оказывается, что для каждого $w \in \mathcal{W}(X)$ подстановка $x \to w$ однозначно

продолжается до гомоморфизма $\varphi_w: W_1 \to \mathcal{W}(X)$, который оказывается изоморфным вложением – это изоморфизм $W_1 \approx \langle x \rangle \subseteq \mathcal{W}(X)$ группоида $W_1 = \mathcal{W}(X)$ на подгруппоид $\langle w \rangle$ в $\mathcal{W}(X)$ порождённый (свободно!) заданным $w \in W$.

В самом деле, согласно уже указанному построению абсолютно свободного группоида $\mathcal{W}(X)$ его элементы $w$ однозначно определяются (или записываются) после соответствующей «правильной расстановки скобок» на слове $w\boldsymbol{s} \in \mathcal{S}(X)$, а «правильная расстановка скобок» на $w$ и $w_1 \in W_1(\{x\})$ – одна и та же. Именно поэтому отображение $w \to (w\boldsymbol{s}, w\mathbf{1})$ является вложением, то есть для $u, v \in \mathcal{W}(X)$ всегда $(u\boldsymbol{s}, u\mathbf{1}) = (v\boldsymbol{s}, v\mathbf{1})$ тогда и только тогда, когда $u = v$. После этого учитываем, что умножение на прямом произведении $\mathcal{S}(X) \times W_1$ строится «покомпоненино», а с другой стороны, для $u, v \in W = \mathcal{W}(X)$ всегда справедливы равенства $(u \cdot v)\boldsymbol{s} = u\boldsymbol{s}v\boldsymbol{s}$ и $(u \cdot v)\mathbf{1} = (u\mathbf{1}v\mathbf{1})$, то есть $\boldsymbol{s}$ и $\mathbf{1}$ являются гомоморфизмами $\mathcal{W}(X)$ на $\mathcal{S}(X)$ и $W_1 = W(\{x\})$ соответственно. Поэтому оказывается, что указанное отображение $w \to (w\boldsymbol{s}, w\mathbf{1})$ является изоморфным вложением в прямое произведение $\mathcal{S}(X) \times W_1$ и представлением $\mathcal{W}(X)$ в виде подпрямого произведения $\mathcal{S}(X)$ на $W_1$, с точностью до изоморфизма, так как $Ker\boldsymbol{s} \cap Ker\mathbf{1} = \Delta_W$.

С другой стороны, учитывая специфику «тоже абсолютно свободного группоида» $W_1 = W(\{x\})$, конечно получаем, что отображение или подстановка $x \to w \in \mathcal{W}(X)$ *однозначно* продолжается до гомоморфизма $\varphi_W: W_1 \to w_1\varphi_W = \langle w \rangle \subseteq \mathcal{W}(X)$, *согласно правилу* $u(x, \dots, x)\varphi_W = u(w, \dots, w)$, а возникающие элементы $u(w, \dots, w)$ – это в точности все элементы подгруппоида $\langle w \rangle$ порождённого в $\mathcal{W}(X)$ заданным $w \in W$. Но указанному элементу $u(w, \dots, w) \in \mathcal{W}(X)$ однозначно соответствует слово $w\boldsymbol{s} \dots w\boldsymbol{s} \in \mathcal{S}(X)$ и если учесть «правильную расстановку скобок» на элементе $w$ и «перенести » её на соответствующее слово $w\boldsymbol{s}$ вместе с «правильной

расстановкой скобок» на $u \in W_1$, то получается «правильная расстановка скобок» и на $u(w,\dots,w)$, что восстанавливает запись этого элемента, согласно уже отмеченному. Поэтому оказывается, что гомоморфизм $\varphi_W \mathbf{1}: W_1 \to W_1$ совпадает с тождественным изоморфизмом, то есть и $u(w,\dots,w) = v(w,\dots,w) \Leftrightarrow u = v$. А это и означает, что $\varphi_W$ является *изоморфизмом* $W_1 \approx \langle w \rangle$, и поэтому подгруппоид и группоид $\langle w \rangle$ свободно порождается своим элементом $w$, так как $W_1$ свободно порождается $x \in W_1$.

**Предложение 2**. Каждый подгруппоид $G$ свободного группоида $\mathcal{W}(X)$ тоже бесконечен, так как *свободно порождается, как группоид, своим подмножеством* $\pi(G)$ из всех неразложимых в $G$ элементов – как алфавит $X$ в $\mathcal{W}(X)$, но иногда конечным, а иногда бесконечным. Поэтому группоид $\mathcal{W}(X)$ можно изоморфно вложить в любой его подгруппоид и в группоид $W_1 = W(\{x\}) \approx \langle w \rangle \subseteq \mathcal{W}(X)$.

**Доказательство.** В подгруппоиде $G$ абсолютно свободного группоида $W = \mathcal{W}(X)$ существуют, конечно, элементы $w \in G$, и поэтому возникает и бесконечно много элементов, как в подгруппоиде $\langle w \rangle \approx W_1 = W_1(\{x\})$, согласно предложению 1. Одновременно получается, что многие $w \in G$ разложимы в $G$, то есть представляются в виде $w = (uv)$ для некоторых $u, v \in G$, причём *однозначно определённых, согласно построению* $W$ и с длинами строго меньшими $d(w) \in \mathbb{N}$, так как $d(w) = d(u) + d(v)$. Затем можно учесть, что если $u \in G$ тоже разложимыv в $G$, то $w = (uv) = \big((u_1u_2)v\big)$ для соответствующих $u_1, u_2 \in G$ таких, что $u = u_1u_2$, а если элемент $v \in G$ разложим в $G$, то получается, что $w = (uv) = \big((u_1u_2)(v_1v_2)\big)$ для $u_1, u_2, v_1, v_2 \in G$ (и так далее).

Но возникающий «процесс разложения» элемента $w \in G$ однозначно закончится на конечном шаге *именно из-за длины* $d(w) \in \mathbb{N}$, так как длины возникающих «сомножителей» строго уменьшаются. Поэтому для произвольно заданного (разложимого в $G$)

всегда возникает такой единственный элемент $f \in W$, что соответствующее ему слово $f\boldsymbol{s} = x_1 \dots x_k$, а элемент $w \in G$ *однозначно представляется в виде* $w = f(w_1, \dots, w_k)$ после подстановки $x_i \to w_i \in G$ для некоторых $w_i \in G$ уже *неразложимых* в $G$ (уже из-за окончания «процесса разложения»). Возникающее *множество* $\pi(G)$ *всех неразложимых в* $G$ *элементов* «конечно можно занумеровать натуральными числами», то есть представить в виде $\pi(G) = \{h_m | m \in \Delta\}$, где $\emptyset = \Delta \subseteq \mathbb{N}$ и $h_m = h_k \Leftrightarrow m = k$, как для соответствующего алфавита $X_\Delta = \{x_m | m \in \Delta\} \subseteq X$.

После этого можно учесть, что вместе с $X$ указанный алфавит $X_\Delta$ тоже *свободно порождает абсолютно свободный группоид* – подгруппоид $\mathcal{W}(X_\Delta) = \langle X_\Delta \rangle$ в $W = \mathcal{W}(X)$, а согласно указанному «процессу разложения» и уже отмеченному, получается, что отображение $x_m \to h_m \in \pi(G)$ однозначно продолжается до гомоморфизма и это оказывается изоморфизм $\mathcal{W}(X_\Delta) \approx G = \langle \pi(G) \rangle$. При этом мы учли, что для каждого $w \in G$ получается единственное указанное представление $w = f(w_1, \dots, w_k)$ в виде произведения неразложимых в $G$ элементов с помощью $f \in \mathcal{W}(X_\Delta)$, и поэтому группоид $G$ *свободно порождается «своим»* $\pi(G)$*, так как правило* $f(x_1, \dots, x_k) = f(w_1, \dots, w_k)$ и задаёт указанный изоморфизм $\mathcal{W}(X_\Delta) \approx G = \langle \pi(G) \rangle$. Множество $\pi(G)$ оказывается, конечно, единственным свободно порождающим группоид $G$, так как $X_\Delta$ обладает этим свойством в $\mathcal{W}(X_\Delta)$.

Это заканчивает доказательство предложения, но можно заметить, в качестве пояснения, что $\pi(\langle w \rangle) = \langle w \rangle$, а элементы $(xx), \big((xx)x\big), \Big(\big((xx)x\big)x\Big), \dots$ свободно порождают в $W_1$ подгруппоид изоморфный $\mathcal{W}(X)$, так как указанные элементы не разложимы в порождённом ими подгруппоиде. После этого, конечно, можно легко строить и другие изоморфные вложения абсолютно свободных группоидов $\mathcal{W}(X)$ или $\mathcal{W}(X_\Delta)$ в $W_1 \approx \langle w \rangle$.

**Предложение 3**. Абсолютно свободный группоид $W_1$ порождает многообазие всех группоидов, так как абсолютно свободный группоид $\mathcal{W}(X)$ изоморфно вкладывается в группоид $W_1 = \mathcal{W}(\{x\})$. Из этого вытекает, что в группоиде $G$ справедливо некоторое нетривиальное тождество (не справедливое в $W$ или некотором другом группоиде), если в $G$ справедливо некоторое нетривиальное тождество $u(x, \dots, x) \equiv v(x, \dots, x)$. При этом, если в $G$ справедливо тождество $x \equiv (xx)$, то $T(G, \{x\}) = W_1 \times W_1$ и это равносильно тому, что все *однопоророждённые* подгруппоиды в $G$ одноэлементны, то есть всегда $\langle w \rangle = \{w\}$, хотя группоид $G$ может и не быть одноэлементным.

В самом деле, первое утверждение предложение с очевидностью вытекает из предложений 1, 2 и «общих утверждений», так как в многообразие $Var(W_1)$ попадает абсолютно свободный группоид $\mathcal{W}(X)$ и все другие. После этого можно учесть, что если $T(G, X) \neq W \times W$, то есть если в группоиде $G$ справедливо некоторое нетривиальное тождество, то $W$ не попадает в многообразие $Var(G)$. Но тогда, согласно сказанному выше и $W_1 = \mathcal{W}(\{x\})$. не попадает в многообразие $Var(G)$, и поэтому $T(G, \{x\}) \neq W_1 \times W_1$, то есть $T(G, \{x\}) \neq \Delta_{W_1}$, поэтому в $G$ возникает нетривиальное тождество $u(x, \dots, x) \equiv v(x, \dots, x)$, даже когда справедливо неравенство $T(G, \{x\}) \neq W_1 \times W_1$. После этого легко заметить, что тождество $x \equiv (xx)$ справедлмво в группоиде $G$ тогда и только тогда, когда $T(G, \{x\}) = W_1 \times W_1$ и это равносильно тому, что всегда $\langle w \rangle = \{w\}$ в группоиде $G$, даже когда группоид $G$ не одноэлементен (что можно увидеть, например, в группоидах $G_2, G_4, G_7$ и других).

Согласно уже отмеченному, если в не одноэлементном группоиде $G$ имеется только две конгруэнции, то соответствующее многообразие $Var(G)$ будет минимальным и свободные группоиды этого

многообразия в принципе можно описать. Соответствующие многообразия весьма специальны и это можно показать для уже построенных группоидов из двух элементов.

Как было отмечено, в группоиде $G_1$ справедливо тождество $x_1x_2 \equiv x_3x_4$, и поэтому этот группоид является группоидом с нулевым умножением - нулём будут все произведения двух и более элементов. Более того группоид $G_1$ оказывается однопорождённым свободным группоидом своего многообразия $Var(G_1)$, а из сказанного вытекает построение всех остальных свободных группоидов $\bar{S}_1(X)$ этого многообразия. А именно, $\bar{S}_1(X) = X \cup\{0\}$, где нуль не принадлежит $X$, а операция умножения строится по правилу $x_ix_j = 0 = x_i0 = 0x_j = 00$. После этого получается, что в многообразии $Var(G_1)$ все не одноэлементные группоиды свободны, так как все не одноэлементные подгруппоиды и гомоморфные образы $\bar{S}_1(X)$ имеют такой же вид.

Аналогичная ситуация (и даже более простая) получается и для группоидов $G_4$ и $G_8$, но в этих группоидах однопорождённые подгруппоиды одноэлементны, так как справедливо тождество $xx \equiv x$. В результате получается, согласно тождеству $x_1x_2 \equiv x_1$. что $G_4$ является свободным группоидом своего многообразия $Var(G_4)$, а все остальные свободные группоиды этого многообразия имеют вид $\bar{S}_4(X) = X = \{x_i | i \in I\}$. При этом умножение задаётся по правилу $x_ix_j \equiv x_i$, а все буквы – элементы оказываются свободными порождающими. Аналогичная ситуация получается для группоида $G_8$, и при этом свободные группоиды $\bar{S}_8(X) = X$, но умножение задаётся по правилу $x_ix_j \equiv x_j$, согласно соответствующему тождеству. Можно построить многообразие $Var(G_6)$ и описать его свободные группоиды, но это уже немного сложнее. Отметим только, что это многообразие минимально и состоит из групп, так как справедливы тождества $x_1x_1x_2 = x_2 = x_2x_1x_1$, $x_ix_i = x_jx_j$ и тождество $(x_ix_j)x_k = x_i(x_jx_k)$, вместе с тождеством коммутативности. Иначе говоря, все группоиды из многообразия $Var(G_6)$ являются группами, причём

коммутативными с единицей $xx = e$, и поэтому элементы этих групп обратны себе. После этого можно заметить, что группы $G$ из простого числа $p \geq 2$ элементов тоже образует минимальное многообразие $Var(G)$ группоидов, состоящее из соответствующих групп. Но это можно доказать после соответствующего описания групп. При этом вполне возможно, что все группоиды из соответствующего многообразия тоже всегда свободны в этом минимальном многообразии, но это требует дополнительных вычислений.

Для остальных группоидов $G$, имеющих точно две конгруэнции соответствующее многообразие $Var(G)$ минимально и свободные группоиды этого многообразия уже не обязаны быть полугруппами, и поэтому соответствующее тождество и свободные группоиды описать уже значительно сложнее. Отметим только, что таким разным группоидам соответствуют разные многообразия и таких многообразий уже «очень много», согласно уже построенным примерам указанных специальных группоидов. В частности, некоторые из этих группоидов нельзя задать конечным набором тождеств. Однако, не совсем ясно, что любое минимальное многообразие группоидов порождается указанными специальными группоидами (т.е. с двумя конгруэнциями), так как эти группоиды могут быть весьма сложными и не обязаны быть полугруппами.

## §6. Специфика полугрупп и групп (теорема о гомоморфизмах для групп)

Можно заметить, что натуральный ряд $\mathbb{N}(+)$ является свободной полугруппой с одной свободной порождающей (единицей). Если же мы рассмотрим натуральный ряд $\mathbb{N}(\cdot)$ (с операцией умножения), то получается свободная коммутативная полугруппа со счётным множеством свободных порождающих (из всех простых чисел). Кроме того, как уже было отмечено, множество $\mathcal{S}(X)$ всех слов над алфавитом $X$ (с операцией приписывания в качестве умножения) является абсолютно свободной полугруппой, весьма отличной от абсолютно свободного группоида $\mathcal{W}(X)$. А именно, как было уже отмечено, в $\mathcal{W}(X)$ все подгруппоиды абсолютно свободны и даже в однопорождённом подгруппоиде содержатся не однопорождённые. А в $\mathcal{S}(X)$ однопорождённые подполуруппы коммутативны и имеются не свободные подполугруппы (очень много!). Кроме того, можно заметить, что в $\mathcal{S}(\{x, y\})$ элементы $xy^n = x_n$ порождают свободную полугруппу с указанным множеством свободно порождающих, но это одно из исключений. Так, например, $x^6$ и $x^4$ порождают подполугруппу, но не свободную – если $y_1 = x^4$ и $y_2 = x^6$, то $y_1^6 = y_2^4$. Кроме того, это двупорождённая полугруппа не порождается одним элементом, хотя коммутативна, как подполугруппа в $\mathcal{S}(\{x\}) \approx \mathbb{N}(+)$.

После этого, можно строить разнообразные полугруппы и возможно описание минимальных многообразий полугрупп (которое уже начато - это многообразие полугрупп $Var(G_1)$, $Var(G_4)$, $Var(G_6)$ и так далее). Минимальное многообразие групп легко описывается,

после соответствующего описания конечных абелевых групп (но уже с помощью кольца $\mathbb{Z}$ целых чисел).

На самом деле, полугруппы естественно возникают как полугруппы отображений. А именно, мы уже отмечали, что множество $\mathcal{M}(M) = Mor(M, M)$ всех отображений $\xi: M \to M$ образуют полугруппу $\mathcal{E} = \mathcal{E}_M$.

**Теорема*(о представлении полугупп).*** Любая полугруппа представляется (с точностью до изоморфизма) как подполугруппа некоторой полугруппы $\mathcal{M}(M)$. Иначе говоря, любая полугруппа изоморфно представляется как полугруппа отображений (точнее – в доказательстве).

***Доказательство.*** Заметим сначала, что любая полугруппа $S$ является подполугруппой некоторого моноида, то есть полугруппой с единицей $e$. Например, можно взять элемент $e \notin S$ и превратить $S^6 = S \cup \{e\}$ в полугруппу с единицей $e$ при этом умножение на $S = S(\cdot)$ не меняется и дополняется правилами $se = s = es$, $ee = e$, то есть получается моноид $S^6$ с единицей $e$, в котором $S$ – подполугруппа. Учитывая это сначала будем представлять моноиды.

А именно: допустим, что $T$ – моноид с единицей $e$ строим моноид $\mathcal{M}(T)$ и с каждым $t \in T$ свяжем $\rho(t) \in \mathcal{M}(T)$ по правилу $x\rho(t) = xt$. Тогда легко увидеть, что $\rho(a, b) = \rho(a)\rho(b)$, так как это соответствует закону ассоциативности $x(a, b) = (xa)b$. Одновременно получается, что $\rho: T \to \mathcal{M}(T)$ – гомоморфизм полугрупп, а его образ $\rho(T)$ – подполугруппа в $\mathcal{M}(T)$. Но благодаря специфике моноида получается, с одной стороны, что $\rho(e) = \mathcal{E}$, то есть $\rho(T)$ – подмоноид в $\mathcal{M}(T)$, а с другой стороны, всегда $\rho(a) = \rho(b) \Leftrightarrow a = b$. В результате получилось, что $T \approx \rho(T)$ и мы представили моноид $T$ как моноид правых умножений.

Если $S$ не содержит единицу и $S \subseteq S^6$, то получается, что $\rho(S^6) \approx S^6 \subseteq \mathcal{M}(S^6)$ и осталось учесть $\rho(S) \approx S$, где $\rho(S) \subseteq \rho(S^6)$ и $\rho(S)$ является подполугруппой в $\rho(S^6)$, а $S$ – подполугруппа в $S^6$.

В результате получили «универсальный» способ построения полугрупп – это подполугруппы полугрупп $\mathcal{M}(T)$. Благодаря этому можно легко описать подполугруппы малых порядков, так как соответствующие полугруппы $\mathcal{M}(T)$ известны и легко описываются.
С другой стороны, ещё одним универсальным способом построения получается представление полугрупп как гомоморфных образов соответствующей свободной полугруппы $\mathcal{S}(X)$. Благодаря этому можно строить и многообразия полугрупп.

С помощью теоремы о представлении полугрупп получается и соответствующая теорема о представлениях групп. А именно, в полугруппе $\mathcal{M}(T)$ естественно выделяется как полугруппа и подмоноид, группа $\mathcal{U}(M)$ всех взаимно однозначных отображений $\mu: T \to T$. Такие отображения обратимы, то есть существует обратное $\mu^{-1}: T \to T$, для которого $\mu\mu^{-1} = \mu^{-1}\mu = \mathcal{E}$, а благодаря этому и получается соответствующая теорема о представлении групп.

**Теорема.** Любая группа представляется (с точностью до изоморфизма) как подгруппа некоторой полугруппы $\mathcal{U}(M)$. Иначе говоря, любая группа изоморфно представляется как группа отображений.

***Доказательство.*** Теорема справедлива в силу того, что группа $\mathcal{U}(M)$ является подмоноидом в $\mathcal{M}(M)$ (то есть $\mathcal{U}(M) \subseteq \mathcal{M}(M)$) и любая группа является моноидом. Поэтому соответствующий результат снова получается с помощью правых умножений как в теореме о представлении полугрупп.

После этого построения полугрупп и групп можем применять соответствующие теоремы о подсистемах и гомоморфных образах (смотри §3). При этом точно так же как же как в общем случае строятся решётки подсистем (подполугрупп или подгрупп). Одновременно строятся соответствующие конгруэнции как ядра гомоморфизмов и для полугрупп получаются соответствующие теоремы о гомоморфизмах –

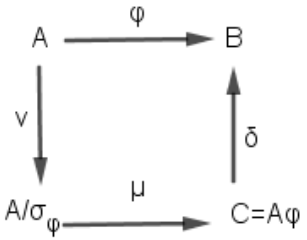
простой специализацией (то есть для гомоморфизмов соответствующих конгруэнций, фактор-полугрупп и т.д.).

Благодаря этому, можно, например, из свободных полугрупп строить все полугруппы как гомоморфные образы. Для групп учитывается специфика возникающих конгруэнций.

**Теорема.** Для гомоморфизма $\varphi: A \to B$ групп ядро $Ker\varphi = \{a \in A | a\varphi = e\} = H$ и оказывается, что конгруэнция $\sigma_{\varphi}$ определяется этим $H$. А именно: смежные классы $\hat{a} = aH$ (если $A = A(\cdot, e, ^{-1})$ ) и отображение $h \to ah$ взаимно однозначно (то есть все эти смежные классы имеют одно и то же количество элементов). При этом $H$ – инвариантная подгруппа или нормальный делитель в $A$ (то есть $aha^{-1} \in H$ для всех $h \in H$ и $a \in A$ для этой подгруппы). После этого вместо фактор-групп по конгруэнции можно рассматривать фактор-группы по нормальному делителю $A / H$ и строить соответствующий гомоморфизм, ядрами которого будет именно $H$.

После этого можно сформулировать и соответствующие теоремы о гомоморфизмах для групп.

**Теорема.** Вместе с гомоморфизмом $\varphi: A \to B$ учтём его образ $C = A\varphi$, ядро $Ker\varphi$, вложение $\sigma = \varepsilon_B^C: C \to B$ и естественный гомоморфизм на соответствующую подгруппу $A / Ker\varphi$, а затем учтём и умножение соответствующих «согласованных» гомоморфизмов. Тогда получается выписанная диаграмма, связывающая указанные гомоморфизмы – точнее, *существует и единственный такой гомоморфизм* $\mu: \hat{A} \to C$, *что* $\varphi = \nu\mu\delta$. Более того, этот гомоморфизм действует по правилу $\hat{a}\mu = a\varphi$ (для всех $a \in A$ ) и оказывается взаимно однозначным, и поэтому и изоморфизмом.




Но тогда строится и «обратный» изоморфизм $\mu^{-1}: C \to \hat{\hat{A}}$, то есть получается *канонический изоморфизм* $A\varphi \approx A/\sigma_\varphi$ (*гомоморфные образы* $\Omega$ *-алгебры* $A$ *являются её фактор-алгебрами* по соответствующим конгруэнциям, с точностью до изоморфизмов). При этом можно учесть, что гомоморфизм $\nu\mu: A \to C$ уже являющийся гомоморфизмом $\Omega$-*алгебры* $A$ на $\Omega$-*алгебру* $C$ в точности соответствует заданному гомоморфизму $\varphi: A \to B$, то есть имеет то же образ и то же самое ядро (что неявно отражено в диаграмме).

Эта теорема вытекает из сказанного выше и общей теоремы. А после этого можно доказать и другую теорему о гомоморфизмах групп.

**Теорема.** Рассмотрим гомоморфизм $\varphi: A \to B$ групп. Каждый такой гомоморфизм индуцирует соответствующие гомоморфизмы $\bar{\varphi}: R \to R\varphi \subseteq B$ соответствующих подгрупп группы $A$, при этом $Ker\bar{\varphi} = R \cap Ker\varphi$. Для подгрупп $R \to A$ индуцируются гомоморфизмы и оказывается, что $Ker\bar{\varphi} = R \cap Ker\varphi$, поэтому $R\varphi \approx R/R \cap H$. С другой стороны, благодаря специфике нормальных делителей, получается, что $RH = \{rh | r \in R, h \in H\}$ подгруппа в $A$. А для индуцированного гомоморфизма получается, что $RH/H \approx R/R \cap H$, так как $(RH)\varphi = R\varphi$. Поэтому все подгруппы в $A\varphi$ являются образами соответствующих

подгрупп, и у нас получились изоморфизмы
$RH/H \approx R\varphi \approx R/R \cap H$.

В связи с этой теоремой, нужно только заметить, что $RH$ действительно является подгруппой, построенные по указанному правилу, и это наименьшая подгруппа, содержащая и $R$ и $H$, но при этом используется специфика $H$ для подгрупп $R, S$ всегда строится их объединение как подгрупп $R \vee S$, но если $S$ не инвариантен (не является нормальным делителем), то его построить значительно сложнее.

Таким образом, специфика групп проверяется именно при построении гомоморфизмов, так как вместо конгруэнций нужно рассматривать соответствующие нормальные делители (или инвариантные подгруппы).

Подгруппы абелевой группы $A(+,0,-)$ всегда являются нормальными делителями, так как $a + h + (-h) \equiv h$, поэтому получаются фактор-группы по подгруппе, что мы ещё учтём.

После этого можно учесть, что кольцо $K$ является абелевой группой и мультипликативной полугруппой, связанными законами дистрибутивности. Поэтому при рассмотрении гомоморфизмов $\varphi: A \to B$ получим идеалы $Ker\varphi$ – это такие подкольца $H$, что $ah, ha \in H$ для всех $a \in A, h \in H$ они просто подкольца. Это и учитывается в соответствующих теоремах о гомоморфизмах для колец, в которых строятся соответствующие фактор-кольца $A/I$ по идеалам. Соответствующие теоремы получаются как в теоремах о группах (которые упоминались ранее) и в частности получаем, например, что если $I$ – идеал в $A$, $R$ – подкольцо, то $R/R \cap I \approx R + I/I$

## § 7 Аддитивные подгруппы кольца целых чисел и основная теорема арифметики

Целые числа возникают как разности натуральных чисел, то есть ячвяются решениями уравнений $a + x = b$ для $a, b \in \mathbb{N}$. При этом получается и правило равенства $b - a = c - d \Leftrightarrow b + d = a + c$. В результате получается, что выделяется нуль $0 = 1 - 1 = \cdots = m - m$ натуральные числа можно отождествить по правилу
$n = (n + 1) - 1 = \cdots = (n + m) - m$=… кроме них возникают ещё и отрицательные числа $-n = 1 - (n + 1) = \cdots = m - (n + m) = \cdots$

В результате получаем, что множество целых чисел $\mathbb{Z}$ представляется в виде цепочки
$\ldots < -n < \cdots < -2 < -1 < 0 < 1 < 2 < \cdots < n < n + 1 < \cdots$,
а операции сложения и умножения, уже заданные на натуральном ряде, продолжаются на множестве $\mathbb{Z}$, например по правилу

$$(a - b) + (c - d) = (a + c) - (b + d)$$
$$(a - b) \cdot (c - d) = (ac + bd) - (ad + bc)$$

На самом деле можно считать кольцо $\mathbb{Z}$ целых чисел построенным и получается, что построена абелева (или аддитивная) группа $\mathbb{Z}(+, 0, -)$ и мультипликативная полугруппа $\mathbb{Z}(\cdot)$ связанные законами дистрибутивности. Таким образом, получаются законы:

$$(a + b) + c = a + (b + c)$$
$$a + b = b + a$$
$$a + 0 = 0 + a = a$$
$$a + (-a) = 0 = -a + a$$
$$a - b = a + (-b)$$

Другими словами, среди целых чисел выделяется $0 \in \mathbb{Z}$, строятся противоположные числа $-z$, для которых справедливы указанные равенства. Кроме того, конечно, выделяется единица 1, для которой всегда $z \cdot 1 = z = 1 \cdot z$, а из указанных законов, в том числе закона дистрибутивности получается равенство $z \cdot 0 = 0 = 0 \cdot z$, из-за которого 0 и называется нулём.

Таким образом, кольцо $\mathbb{Z}$ целых чисел можно считать построенным и его отличие от натурального ряда в том, что получается группа $\mathbb{Z}(+,0,-)$ и специфику этой группы можно уточнять.

А именно, мы учтём, что для абелевой группы $A(+,0,-)$ можно учесть и умножение на целые числа: если $a \in A, z \in \mathbb{Z}$, то строится произведение $za \in A$, при этом $0a = 0$, $1a = a$, $-1a = -a$ и $za + ta = (z + t)a$ . Благодаря этому, можно учесть построение решётки $P(A)$. А именно: подгруппы сравниваются по включению и получается, что $A$ – наименьший элемент в $P(A)$ – наибольшая подгруппа, $0 = \{0\} \in P(A)$ – наименьшая подгруппа. Для элементов $B, C \in P(A)$ можно строить пересечение $B \cap C \in P(A)$ и сумму $B + C = \{b + c | b \in B, c \in C\} \in P(A)$ – это наименьшая подгруппа, содержащая $B$ и $C$. Одновременно получается, что если $A \neq \{0\}$, то есть $A$ не одноэлементна, то выделяется циклическая подгруппа $\mathbb{Z}a = \{za | z \in \mathbb{Z}\}$, порождённая соответствующими элементами.

Для $\mathbb{Z} = \mathbb{Z}(+,0,-)$ получается больше, в частности получается, что $\mathbb{Z} = \mathbb{Z}1$, а после этого можно описать все аддитивные подгруппы этой аддитивной группы. При этом будем иметь в виду, что операция умножения на целых числах сводится к операции сложения, и поэтому можно применять умножение на целые числа как в любой абелевой группе $A$. Уточняя эту специфику, будем иметь в виду, что справедлива теорема о делении с остатком.

**Теорема.** Для любого целого числа $z \in \mathbb{Z}$ и натурального числа $n \in \mathbb{N}$ $(n \geq 2)$ всегда получается единственное представление $z = qn + r$, где $q, r \in \mathbb{Z}$ и $0 \leq r \leq n - 1$ для остатков. Другими словами, можно производить деление с остатком на натуральные числа.

***Доказательство.*** В указанном представлении $z = qn + r$ одно из слагаемых $qn$, но $qn = \underbrace{q + \cdots + q}_{n \text{ раз}}$, поэтому мы применили на самом

деле операцию аддитивной группы. Эту теорему можно доказывать по-разному. И мы будем считать её хорошо известной.

Благодаря этой теореме и указанной специфике, получим точное описание аддитивных подгрупп кольца $\mathbb{Z}$ с помощью натуральных чисел.

**Теорема.** Если $A$ аддитивная подгруппа в $\mathbb{Z}$ и $A \neq 0 = \{0\}$, то получается представление $A = \mathbb{Z}n = n\mathbb{Z} = \{nz | n \in \mathbb{N}, z \in \mathbb{Z}\}$ для соответствующих натуральных чисел. Таким образом, все ненулевые подгруппы $\mathbb{Z} = \mathbb{Z}(+,0,-)$ оказываются циклическими и однозначно представляются в виде $n\mathbb{Z}$ для соответствующего натурального числа $n$

***Доказательство.*** Пусть $A = A(+,0,-)$ подгруппа в $\mathbb{Z} = \mathbb{Z}(+,0,-)$, причём $A \neq 0$, тогда $A$ замкнуто относительно разности (или операций группы), причём существует $a \in A, a \neq 0$. Но из чисел $a, -a$ точно одно является натуральным, и поэтому $A \bigcap \mathbb{N}$ не пусто, то есть существуют натуральные числа, попадающие в $A$, а в силу специфики натурального ряда, получается, что существует наименьшее число $n = min(A \bigcap \mathbb{N})$ и одновременно получается, что $A \supseteq \mathbb{Z}n$. Если $n = 1$, то окажется, что $A = \mathbb{Z}1 = \mathbb{Z}$. Поэтому будем считать, что $n \geq 2$.

В этом случае элемент $a \in A$ можно разделить с остатком на $n$ $a = qn + r$ и учесть, что $a \in A, n \in \mathbb{N} \Rightarrow r = a - qn \in A$, так как $A$ замкнуто относительно разности и умножения на натуральные числа. Но в силу специфики $n = min(A \bigcap \mathbb{N})$ получается, что и $r = 0$, и поэтому $a = qn \in \mathbb{Z}n$ и мы доказали, что $A = \mathbb{Z}n$. Это и заканчивает доказательство.

***Следствие.*** Для ненулевых аддитивных подгрупп в $\mathbb{Z}$ и соответствующих натуральных чисел всегда $n\mathbb{Z} \subset m\mathbb{Z} \Leftrightarrow n = md$. Другими словами, включение аддитивных подгрупп соответствует делимости натуральных чисел.

**Теорема.** Ненулевые аддитивные подгруппы в $\mathbb{Z}$ образуют мультипликативную решётку, то есть строится пересечение, сумма и произведение аддитивных подгрупп. При этом, для соответствующих натуральных чисел $m, n \in \mathbb{N}$ получаются равенства

$$m\mathbb{Z} \bigcap n\mathbb{Z} = c\mathbb{Z}, m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}, m\mathbb{Z} \cdot n\mathbb{Z} = d\mathbb{Z}$$

Одновременно оказывается, что $c$ – это наименьшее общее кратное чисел $m$ и $n \in \mathbb{N}$, а $d$ – наибольший общий делитель.

***Доказательство***. Учитывая уже сказанное о решётке $P(A)$ подгрупп аддитивной группы $A$ и уже полученное точное описание ненулевых аддитивных подгрупп в $\mathbb{Z}$, с помощью натуральных чисел.

Пусть $m\mathbb{Z}$ и $n\mathbb{Z}$ аддитивные подгруппы. Тогда сумма $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ и $m\mathbb{Z} \bigcap n\mathbb{Z} = c\mathbb{Z}$ . При этом нужно учесть, что пересечение указанных ненулевых подгрупп будет ненулевым, хотя бы потому, что $mn \in m\mathbb{Z} \bigcap n\mathbb{Z}$ . Из-за этого и получаются указанные равенства. Кроме того, строятся и произведения $m\mathbb{Z} \cdot n\mathbb{Z} = mn\mathbb{Z} \subseteq m\mathbb{Z} \bigcap n\mathbb{Z}$, так как $mz \cdot nt = mn(z \cdot t)$. Таким образом, суммы, пересечения и произведения аддитивных подгрупп уже построены.

Согласно специфике пересечения, $m\mathbb{Z} \bigcap n\mathbb{Z} = c\mathbb{Z}$ – это наибольшая аддитивная подгруппа, содержащая $m\mathbb{Z}$ и $n\mathbb{Z}$ . Но тогда, согласно следствию, с – это наименьшее общее кратное чисел $m, n \in \mathbb{N}$. Но при этом можно учитывать, что одним из кратных будет $mn \in \mathbb{N}$. С другой стороны, сумма $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ – это наименьшая аддитивная подгруппа, содержащая $m\mathbb{Z}$ и $n\mathbb{Z}$. Поэтому, согласно следствию, $d$ – наибольший общий делитель чисел $m, n \in \mathbb{N}$ . И одновременно получилось, что $d = mz + nt$ для некоторых $z, t \in \mathbb{Z}$.

В результате оказалось, что для натуральных чисел $m, n \in \mathbb{N}$ всегда строятся их наименьшее общее кратное $c \in \mathbb{N}$ и наибольший общий делитель $d \in \mathbb{N}$, при этом, мы учли отношение делимости,

соответствующее включению аддитивных подгрупп и поэтому, с – кратное чисел $m, n \in \mathbb{N}$ которое делит все остальные кратные, а $d$ – общий делитель $m, n \in \mathbb{N}$, который делится на остальные общие делители. Теорема доказана.

Применяя доказанные теоремы и утверждения, можно уточнить специфику отношения делимости на натуральном ряде $\mathbb{N}$ и доказать основную теорему арифметики.

Из специфики аддитивных подгрупп в $\mathbb{Z}$, получаем, что любая строго возрастающая цепочка $n_1\mathbb{Z} \subset n_2\mathbb{Z} \subset \cdots$ аддитивных подгрупп в $\mathbb{Z}$ всегда конечна, или обрывается на конечном шаге. При этом учитывается $n_2$ – делитель $n_1$, $n_1 \neq n_2$ и т.д., а в частности $n_2 > n_1 > \cdots$ таким образом, мы учли, что число $n_1 \geq 2$ имеет только конечное число делителей, а из этого и вытекает, что указанная цепочка конечна.

Одновременно получается, что для $n\mathbb{Z} \neq \mathbb{Z} = 1\mathbb{Z}$ всегда существует максимальная $p\mathbb{Z} \supseteq n\mathbb{Z}$, строго больше которой только $\mathbb{Z}$. При этом максимальным $p\mathbb{Z}$ соответствуют простые числа $p \geq 2$, у которых делителями являются только $p$ и $1$, согласно определению и уже сказанного. После этого получается, что каждое натуральное число, отличное от 1, представляется в виде произведения $n = s_1 s_2 \dots s_r \dots$ простых чисел или $n = p$ - простое число. При этом учитывается, что множество $\pi(n)$ всех простых делителей числа $n \geq 2$ всегда непусто и конечно.

После этого можно учесть и другие свойства простых чисел $p$, кроме максимальности аддитивной подгруппы $p\mathbb{Z} \neq \mathbb{Z} = 1\mathbb{Z}$. Так, например, если $a \notin p\mathbb{Z}$, то $p\mathbb{Z} + a\mathbb{Z} = 1\mathbb{Z} = \mathbb{Z}$ и поэтому $pz + at = 1$, для некоторых $z, t \in \mathbb{Z}$. Это свойство в точности соответствует максимальности $p\mathbb{Z}$ и одновременно получается, что, если простое число $p$ не делит числа $m, n \in \mathbb{N}$, то оно не делит и произведение $mn \in \mathbb{N}$. Другими словами, если произведение $ab$ натуральных чисел

делится на простое число $p$, то $a$ делится на $p$ или $b$ делится на $p$. Ну а применяя всё указанное мы получаем нужные теоремы.

**Теорема (*основная теорема арифметики*).** Для натурального числа $n \geq 2$ множество $\pi(n)$ его простых делителей всегда конечно и непусто. При этом, если $\pi(n) = \{p | p \in \mathbb{N}\}$ одоэлементно, то $n = p^t$ (степень простого числа) или $n = p$ простое. Если же $\pi(n) = \{p_1, \dots, p_k\}$ состоит из $k \geq 2$ простых чисел, то $n = p_1^{t_1} \dots p_k^{t_k}$ произведение степеней этих простых чисел, причём указанное представление единственное. В этом представлении отмечены все $p_i \in \pi(n)$.

***Доказательство.*** В самом деле, будем считать, что $\pi(n) = \{p_1, \dots, p_k\}$ состоит из $k \geq 2$ простых чисел. Затем строим представление $n = s_1 s_2 \dots s_r$ числа $n$ в виде произведения простых чисел. после этого замечаем, что если $p_i \in \pi(n)$, то $p_i$ делит указанное произведение, и поэтому $p_i = s_g$ для некоторых простых делителей. В результате оказывается, что в представлени $n = s_1 s_2 \dots s_r$ все $p_i \in \pi(n)$ участвуют (возможно с повторениями) и никаких других простых делителей $s_g$ нет, а собирая равные простые делители, получаем $n = p_1^{t_1} \dots p_k^{t_k}$, где $t_1 + \dots + t_k = r$ . Одновременно получается, что указанное представление единственное, то есть показатели однозначно определяются. А случай $\pi(n) = p$ рассматривается аналогично и получается, что $n = p^t$ степень простого числа или $n = p$.

Укажем только некоторые следствия основной теоремы арифметики (которая доказана после уточнения специфики мультипликативной решётки аддитивных подгрупп в $\mathbb{Z}$).

**Теорема Эвклида.** Простых чисел бесконечно много и их можно расположить в виде цепочки $p_1 = 2 < p_2 = 3 < \cdots$. После этого оказывается, что каждое натуральное число

однозначно записывается в виде $p_1^{t_1} \dots p_k^{t_k}$, если учесть нулевые степени $p^0 = 1$.

***Доказательство.*** Возьмём любое конечное множество $\{s_1, \dots, s_r\}$ различных простых чисел и строим натуральное число $n = 1s_1s_2 \dots s_r$.. Ясно, что $n \geq 3$, а поэтому $\pi(n)$ не пусто, но если $p \in \pi(n)$, то $p \neq s_i$ (иначе получится, что $p$ делит 1). В результате оказывается, что множество простых чисел можно увеличить, добавляя новые простые числа. Именно поэтому множество простых чисел бесконечно, а вместе с цепочкой натуральных чисел получается цепочка
$p_1 = 2 < p_2 = 3 < p_3 = 5 < \cdots$.

**Предложние.** Применяя указанные разложения натуральных чисел, получаем, что, если $a = p_1^{a_1} \dots p_k^{a_k}$, $b = p_1^{b_1} \dots p_k^{b_k}$, а $c$ – наименьшее общее кратное чисел $a, b \in \mathbb{N}$, $d$ – наибольший общий делитель тех же чисел, то справедливы равенства

$c = p_1^{c_1} \dots p_k^{c_k}$, где $c_i = max\{a_i, b_i\}$,

$d = p_1^{d_1} \dots p_k^{d_k}$, где $d_i = min\{a_i, b_i\}$.

Одновременно получается, что $ab = cd$.

В самом деле, мы учитываем единственность указанных представлений, в которых некоторые показатели могут быть нулевыми (когда соответствующего простого делителя нет). После этого, учитывая специфику наименьшего общего кратного $c$ и наибольшего общего делителя $d$, получаем указанное представление (разложение) для $c$ и $d$. А после этого мы получаем, что $ab = p_1^{a_1+b_1} \dots p_k^{a_k+b_k}$, то $a_i + b_i = max\{a_i, b_i\} + min\{a_i, b_i\}$ и поэтому $ab = cd$.

Указанное равенство можно доказывать и без основной теоремы арифметики, но доказательство получается значительно сложнее. С другой стороны, для соответствующих аддитивных подгрупп отмеченное равенство можно переписать в виде
$(a\mathbb{Z} \cap b\mathbb{Z}) \cdot (a\mathbb{Z} + b\mathbb{Z}) = a\mathbb{Z}b\mathbb{Z}$. Это отражает специфику

мультипликативной решётки аддитивных подгрупп. После этого можно указать и некоторые другие равенства в этой решётке. Так, например, $n\mathbb{Z}\,(a\mathbb{Z}+b\mathbb{Z})=na\mathbb{Z}+nb\mathbb{Z}$ умножение аддитивных подгрупп дистрибутивно относительно сложения. (На самом, деле это легко вытекает из дистрибутивности сложения на целых или натуральных числах). Немного сложнее моно показать, что $n\mathbb{Z}\bigcap(a\mathbb{Z}+b\mathbb{Z})=(n\mathbb{Z}\bigcap a\mathbb{Z})+(n\mathbb{Z}\bigcap b\mathbb{Z})$.

## §8 Гомоморфные образы кольца $\mathbb{Z}_m$ (кольца вычетов), циклические группы и описание конечных абелевых групп

Для кольца целых чисел $\mathbb{Z}$ выполняется теорема о делении с остатком, то есть если $z \in \mathbb{Z}$ и $m \in \mathbb{N}$ $(m \geq 2)$, то получим единственное представление $z = qm + r$, где $q, r \in \mathbb{Z}$ $(0 \leq r \leq m-1)$. Рассмотрим отображение $\mathbb{Z} \xrightarrow{\varphi_m} \mathbb{Z}_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$, которое задаётся по правилу $z\varphi_m = \bar{z}$, где $z$ – остаток от деления на любого целого числа на $m$.

На $\mathbb{Z}$ выполняются операции кольца, то есть $\mathbb{Z} = \mathbb{Z}(+, -, 0, \cdot)$, которые должны выполняться и на $\mathbb{Z}_m$. Для любых $\bar{x}, \bar{y} \in \mathbb{Z}_m$ положим $\bar{x} \oplus \bar{y} = \overline{x+y} = (x+y)\varphi_m$, $\bar{x} \odot \bar{y} = \overline{x \cdot y} = (x \cdot y)\varphi_m$. Так мы определили операции сложения и умножения, а $\varphi_m \colon \mathbb{Z} \to \mathbb{Z}_m$ – по построению, значит, $\mathbb{Z}_m = \mathbb{Z}_m(\oplus, \ominus, \bar{0}, \odot, )$ - кольцо коммутативное и с единицей, а $\varphi_m$ – гомоморфизм.

Действительно, $\bar{x} \oplus \bar{y} = \bar{y} \oplus \bar{x}$, так как на $\mathbb{Z}$ выполняется условие коммутативности. При этом справедливы равенства: $\bar{x} \oplus \bar{0} = \bar{x}$, $\bar{x} \oplus (\ominus \bar{x}) = \bar{0}$, где $\ominus \bar{x} = \overline{m - x}$. И поэтому $\mathbb{Z}_m$ – абелева группа по сложению. Аналогично проверяются законы ассоциативности для сложения и умножения, а так же закон дистрибутивности, и поэтому $\mathbb{Z}_m$ – кольцо, как полный образ кольца $\mathbb{Z}_m$.

Рассмотрим, как выполняются операции сложения и умножения на некоторых из колец. Это можно сделать с помощью соответствующих таблиц.

$\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$

| $\oplus$ | $\bar{0}$ | $\bar{1}$ |
|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{0}$ |

| $\odot$ | $\bar{0}$ | $\bar{1}$ |
|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{0}$ |

$\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

| $\oplus$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{0}$ | $\bar{1}$ |

| $\odot$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{2}$ | $\bar{0}$ | 2 | $\bar{1}$ |

$\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

| $\oplus$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |

| $\odot$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{2}$ | $\bar{0}$ | $\bar{2}$ |
| $\bar{3}$ | $\bar{0}$ | $\bar{3}$ | $\bar{2}$ | $\bar{1}$ |

$\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

| $\oplus$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
|---|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{4}$ | $\bar{1}$ | $\bar{2}$ | $\bar{4}$ |
| $\bar{4}$ | $\bar{4}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |

| $\odot$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
|---|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{2}$ | $\bar{4}$ | $\bar{1}$ | $\bar{3}$ |
| $\bar{3}$ | $\bar{0}$ | $\bar{3}$ | $\bar{1}$ | $\bar{4}$ | $\bar{2}$ |
| $\bar{4}$ | $\bar{0}$ | $\bar{4}$ | $\bar{3}$ | $\bar{2}$ | $\bar{1}$ |

$\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

| $\oplus$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ |
|---|---|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{4}$ | $\bar{4}$ | $\bar{5}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{5}$ | $\bar{5}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |

| $\odot$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ |
|---|---|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{2}$ | $\bar{4}$ | $\bar{0}$ | $\bar{2}$ | $\bar{4}$ |
| $\bar{3}$ | $\bar{0}$ | $\bar{3}$ | $\bar{0}$ | $\bar{3}$ | $\bar{0}$ | $\bar{3}$ |
| $\bar{4}$ | $\bar{0}$ | $\bar{4}$ | $\bar{2}$ | $\bar{0}$ | $\bar{4}$ | $\bar{2}$ |
| $\bar{5}$ | $\bar{0}$ | $\bar{5}$ | $\bar{4}$ | $\bar{3}$ | $\bar{2}$ | $\bar{1}$ |

Уже это показывает, что возникшие кольца (конечные!) весьма различны, и их аддитивные группы – циклические, а специфика на самом деле учитывает теорему о делении с остатком и основную теорему арифметики. Укажем только некоторые теоремы.

**Теорема 1.** Для натурального числа $m \geq 2$ следующие теоремы равносильны:

а) $m = p$ ($p$ – простое число);

б) $\mathbb{Z}_m$ не содержит делителей нуля;

в) $\mathbb{Z}_m$ – поле.

**Теорема 2.** Если натуральное число $m \geq 2$ не является простым, то:

а) $\mathbb{Z}_m$ без нильпотентных элементов тогда и только тогда, когда $m$ без квадратов простых чисел, то есть $m = p_1 \dots p_s$ ($p_i$ – различные простые числа);

б) $\mathbb{Z}_m$ содержит нильпотентные элементы, если его разложение есть $p^s$ $(s \geq 2)$.

Напомним, что элемент называется нильпотентным, если для $q \neq 0$, $q^m = 0$..

Из таблицы умножения можно увидеть, что кольцо $\mathbb{Z}_4$ содержит нильпотентные элементы, $\mathbb{Z}_6$ – нет.

Итак, мы построили гомоморфизмы $\mathbb{Z} \to \mathbb{Z}p = \mathbb{Z}_m = \{\overline{0}, \overline{1}, \dots, \overline{m-1}\}$ . Другими словами, построили гомоморфные образы кольца $\mathbb{Z}$ целых чисел с точностью до изоморфизма, кроме самого кольца $\mathbb{Z}$ и $\mathcal{O} = \mathbb{Z}/\mathbb{Z}$.

Мы уже отмечали, что группы $\mathbb{Z}_m$ – является циклической группой – группой, порожденной единицей 1, но все циклические группы являются гомоморфными образами свободной, что уже отмечалось, поэтому, на самом деле, мы описали и все циклические группы, которые можно записывать аддитивно.

В самом деле, при гомоморфизме $\mathbb{Z} \to \mathbb{Z}a$ на циклическую группу $\mathbb{Z}a$ его ядром будет соответствующая аддитивная подгруппа $m\mathbb{Z}$, поэтому все циклические группы уже описаны – бесконечная

циклическая группа изоморфна $\mathbb{Z}$, а все остальные изоморфны соответствующим $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$.

Из таблиц видно, что иногда возникают прямые суммы. В частности $\mathbb{Z}_6 \approx \mathbb{Z}_2 + \mathbb{Z}_3$, а $\mathbb{Z}_{30} \approx \mathbb{Z}_2 + \mathbb{Z}_3 + \mathbb{Z}_5$. С другой стороны, группы $\mathbb{Z}_2, \mathbb{Z}_4, \mathbb{Z}_5$ оказались неразложимы в прямую сумму. На самом деле, можно заметить, что подгруппы групп $\mathbb{Z}_m$ тоже описаны и оказывается, что $\mathbb{Z}_m$ не является прямой суммой, когда $m = p^s$ – степень простого числа.

Примарная циклическая подгруппа не разлагается в прямую сумму.

Это доказывается после уточнения конструкции прямых сумм групп.

А именно, если $B, C$ – абелевы группы (по сложению), то декартово произведение $B \times C = \{(b, c) | b \in B, c \in C\}$ превращается в абелеву группу после покомпонентного определения операций $(b_1, c_1) + (b_2, c_2) = (b_1 + b_2, c_1 + c_2)$. При этом группу $B$ можно отождествлять с $\{(b, 0) | b \in B\}$, которая является подгруппой $B \times C$ и аналогично $C$ отождествляется с подгруппой $\{(0, c) | c \in C\}$. В результате получается $B \times C = A = B + C$, но $B \cap C = \mathcal{O}$, поэтому $A = B \oplus C$ – прямая сумма $B$ и $C$.

Аналогично, прямая сумма строится для любого числа групп $B_1 \times B_2 \times \ldots \times B_n = H = B_1 \oplus B_2 \oplus \ldots \oplus B_n$, а специфика представляется тем, что элемент представляется в виде $h = b_1 + b_2 + \cdots + b_n$ для $b_i \in B_i$.

Именно поэтому оказалось, что $\mathbb{Z}_6 = \mathbb{Z}_2 \oplus \mathbb{Z}_3$ и $\mathbb{Z}_{30} = \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$ с точностью до изоморфизма.

**Предложение.** Если $m$ не степень простого числа и $m = p_1^{s_1} \ldots p_r^{s_r}$, тогда $\mathbb{Z}_m$ можно представить в виде прямой суммы примарных циклических подгрупп
$\mathbb{Z}_m = \mathbb{Z}_{p_1^{s_1}} \oplus \ldots \oplus \mathbb{Z}_{p_r^{s_r}}$.

На самом деле, с помощью указанной конструкции можно доказать более общие утверждения – описание всех конечных абелевых групп $A = A(+,-,0)$ с конечным числом $|A| = m \geq 2$ элементов. При этом снова учитывается основная теорема арифметики или соответствующее разложение $m = p_1^{s_1} \dots p_r^{s_r}$. Более того, можно учесть, что если $|H| = p^\gamma$ степень простого числа, то $H \approx \mathbb{Z}_p$ – циклическая группа такого же порядка. Учитывая это, будем описывать абелевы группы $A$, для которых $|A| = p_1^{s_1} \dots p_r^{s_r}$, $r \geq 2$.

**Лемма.** Для абелевой группы $A$ (указанной!) и любого простого числа $p = p_i$ всегда возникает соответствующая примарная подгруппа $A^{(p)} = \{a \in A | p^s a = 0\}$. Более того, благодаря указанным примарным подгруппам получаем разложение $A = A^{(p_1)} \oplus \dots \oplus A^{(p_r)}$.

**Доказательство.** Замечаем, что числа $m_i = \frac{m}{p^{s_i}}$ имеют общим делителем только 1, поэтому $1 = z_1 m_1 + \dots + z_r m_r$ для некоторых $z_i \in \mathbb{Z}$. Кроме того, легко заметить, что $ma = 0$ для всех $a \in A$. Поэтому получается равенство $a = 1a = \mathbb{Z}_1(m_1 a) + \dots + \mathbb{Z}_r(m_r a)$. Но $p_i^{s_i}(z_i m_i a) = z_i m_i a = 0$, то есть $a_i = z_i m_i a \in A^{(p_i)}$ и мы легко получаем прямое разложение $A = A^{(p_1)} \oplus \dots \oplus A^{(p_r)}$, то есть каждый элемент $a \in A$ однозначно представляется в виде в виде суммы своих примарных компонент.

Примарные подгруппы $A^{(p_i)}$ могут оказаться разложимыми в прямую сумму, а в результате получается теорема.

**Теорема.** Абелева группа $A = A(+,-,0)$, имеющая $|A| = p_1^{s_1} \dots p_r^{s_r}$ элементов является прямой суммой $A = H_{p_1}^{(1)} \oplus \dots \oplus H_{p_1}^{k_1} \oplus \dots \oplus H_{p_r}^{(1)} \oplus H_{p_r}^{k_r}$ далее не разложимых абелевых групп $H_{p_i}^{k_i}$. При этом $H_{p_i}^{k_i}$ – это прямые слагаемые групп $A^{(p_i)}$ и эти подгруппы являются примарными

циклическими подгруппами, изоморфные соответствующим $\mathbb{Z}_{p_i^{t_i}}$ $(\sum t_i = s_i)$.

В частности для циклической группы $\mathbb{Z}_m$ получается указанное в предложении разложение $\mathbb{Z}_m$, так как в этом случае все примарные компоненты циклические и не разложимые.

С другой стороны, конечная абелева группа $A$ не обязана быть циклической, и тогда некоторые соответствующие примарные подгруппы разложимы. Для подтверждения этого укажем некоторые примеры:

1) Абелева группа $A$ из 4-х элементов может быть либо группой $\mathbb{Z}_4$, либо прямой суммой $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, причём вторая группа не циклическая. Нужно только учесть, что $4 = 2 \times 2$.

2) Если группа $A$ имеет 12 элементов, то это оказывается либо циклической группой $\mathbb{Z}_{12}$, либо $\mathbb{Z}_2 \oplus \mathbb{Z}_6 = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$, либо $\mathbb{Z}_4 \oplus \mathbb{Z}_3$.

3) Если группа $A$ имеет 1024 элемента, то получается весьма много не изоморфных абелевых групп, имеющих $2^{10}$ элементов. (Это предоставляется читателем в качестве простого упражнения следствия теоремы.)

Применяя эту теорему, можно описать и некоторые конечные коммутативные кольца. При этом, учитывая, что любую абелеву группу можно превратить в кольцо $A^{(0)}$ по правилу $xy = 0$. Учитывая, что в кольцах умножение не всегда нулевое и то, что $A = A^{(p_1)} \oplus \ldots \oplus A^{(p_r)}$, получается, что если $x \in A^{(p_i)}$, $y \in A^{(p_j)}$ $(p_i \neq p_j)$, то $xy = 0$, поэтому остаётся превратить соответствующие примарные компоненты в кольцо. Иногда это легко сделать.

В частности, если мы описываем коммутативное кольцо из 6-ти элементов, то получаются следующие кольца: $\mathbb{Z}_6$, $\mathbb{Z}_2 \oplus \mathbb{Z}_3$, , $\mathbb{Z}_2 \oplus \mathbb{Z}_3^{(0)}$, $\mathbb{Z}_2^{(0)} \oplus \mathbb{Z}_3$, $\mathbb{Z}_2^{(0)} \oplus \mathbb{Z}_3^{(0)} \approx \mathbb{Z}_6^{(0)}$. И эти все кольца из 6-ти элементов коммутативные.

Аналогично можно описать все кольца из 111-ти элементов.

**Замечание.** Любую решётку $\mathcal{B}(A)$ можно превратить в кольцо, где в качестве операции умножения $(\cdot)$ будет пересечение $\cap$, а в качестве суммы $(+)$будет объединение $\cup$: $(B \setminus C) \cup (C \setminus B)$. Если $A$ имеет $m$ элементов, то $\mathcal{B}(A)$ и указанное кольцо имеет $2^n$ элементов. После этого оказывается, что возникшее кольцо будет прямой суммой полей из 2-х элементов.

Учебное издание
**Общая алгебра.**
**Теория делимости в кольце целых чисел**
Учебно-методическое пособие
Составители:
Юрий Михайлович Рябухин
Галина Николаевна Ермакова
Наталья ЛеонидовнаГригорьева

Формат 60×84/16 Уч.-изд. л. 10,00
Гарнитура «TimesNewRoman»
Заказ,т. 20

Отпечатано с готового оригинал-макета
В типографии ООО «РВТ»
г. Бендеры, ул. Московская, 30