Математические структуры
Курс 1998 г. Информационные системы

Непейвода Н. Н.

2

Оглавление

Введение

Математика является в своей основе единым организмом. Но это единство затушевывается разделением на специальности, представители которых зачастую с трудом понимают друг друга. Скажем, возникают большие трудности при общении аналиста и алгебраиста, логика и тополога и т. д. Поэтому практически нигде в российских вузах нет курса, который пытался бы охватить многообразие математических методов с единой точки зрения.

Определение Декарта

> Математика — наука о порядке и мере (1)

остается непревзойденным с точки зрения разъяснения предмета математики обычным людям, да и с общелогической точки зрения. Но оно не годится для разъяснения предмета математики самим математикам, поскольку, в частности, слова “порядок” и “мера” стали в математике терминами и, соответственно, изменили свой смысл. Описание

> Математика изучает объекты, свойства которых точно сформулированы (2)

не является определением с точки зрения общей логики, а внутреннее коварство его выявляется в курсе математической логики. Поскольку мы имеем действительно *точную* формулировку, скажем, в языке классической логики предикатов, мы оказываемся ограничены. В частности, мы не можем выразить даже понятия конечного множества или транзитивного замыкания. Выразив же их в другом точном языке, мы получаем другие ограничения.

Если же брать достаточно сильную систему, описывающую развитые математические понятия, то, согласно теореме Гёделя, она оказывается неполной и вступают в действие эффекты неформализуемости, нестандартные модели и прочее. Так что точность остается лишь идеалом, виднеющимся на недостижимом горизонте.

Поскольку никто не спорит, что доказательство и точность являются атрибутами математики, то отсюда следует, что понятие точности *неформализуемо* и в значительной своей части передается на прецедентах, непосредствен-

но от учителя к ученику. Тем не менее на основе данных прецедентов с неизбежностью появляются более строгие формулировки, выделяются и явно описываются важные системы понятий.

Новое определение математики неявно содержалось в работе легендарного французского математика Н. Бурбаки [2]. Они описали понятие *математической структуры*, стараясь действовать таким образом, чтобы все наиболее известные на конец 40-х гг. классические математические конструкции им охватывались. Конечно же, ввиду неформализуемости, такое понятие не могло быть полным, и оно быстро породило альтернативные подходы, в частности, теорию категорий. Таким образом, в данный момент есть несколько точных определений математической структуры, которые явно представляют собой ипостаси одного и того же неформализуемого понятия. Поэтому для математика можно сформулировать определение современной математики следующим образом.

Математика — наука, изучающая математические структуры. (3)

Хотя кажется, что в данном определении содержится порочный круг, оно на самом деле не хуже многих других, поскольку математические структуры имеют несколько точных определений. Уж лучше иметь несколько точных расходящихся определений, чем не иметь ни одного либо иметь только одно, но заведомо неполное.[1]

Единый и весьма общий подход потребовался в математике, в частности, потому, что при ее стихийном развитии плодится великое множество подобных друг другу теорем, свести которые воедино можно лишь через идеальные понятия более высокого уровня, чем используемые в каждой теореме. Так, бесчисленные теоремы Коши в анализе были сведены к нескольким базовым формам при создании современных топологии и функционального анализа. Теория групп, а из нее — современная алгебра появились в результате упорядочивания множества формулировок об инвариантных свойствах систем преобразований либо систем корней уравнений. Но и в современной алгебре появилось в начале XX века великое множество подобных друг другу теорем о гомоморфизмах, о факторизации, о представлениях. А чтобы их унифицировать, надо было подниматься на следующие этажи. И, наконец, из необходимости преобразовывать понятия из алгебры в топологию и обратно родилась теория категорий и современные алгебраическая топология и алгебраическая геометрия.

Внесли свою лепту в развитие высших математических структур информатика и когнитивная наука. Типы данных и алгоритмические языки высо-

[1] Тем более что в случае безальтернативности слишком велик соблазн объявить данное определение истинным.

кого уровня потребовали и математических моделей высокого уровня. А в когнитивной науке проблема понятий, зависящих от контекста, приводит к тому, что даже местоимение “я” требует для своего описания функционала очень высокого порядка, включающего и говорящего, и его окружение. А что уж говорить о более сложных конструкциях!

Необходимость единого взгляда на математику важна и потому, что наиболее важные и красивые методы возникают при наведении мостов между на первый взгляд разнородными математическими понятиями. Примерами здесь являются современная теория кодирования, теория автоматов, алгебраическая геометрия и многие другие.

Поэтому для тех, кто собирается квалифицированно обрабатывать сложную информацию, необходимо представлять математику как единое целое и лучше видеть взаимосвязи математики с той системой[2] знаний, которую накопила современная наука (и не только наука.)

Рассмотрим пару примеров, когда соотношения между разными областями математики позволяют быстро решать задачи.

Пример 0.0.1. Рассмотрим матричное уравнение $\mathbf{A}^2 = \mathbf{E}$ для обычных двумерных матриц. Чтобы почти начисто исключить вычисления при его решении, достаточно вспомнить смысл матриц. Они задают линейшые преобразования соответствующего пространства. Значит, нужно найти описание отображений, которые обратны самим себе, или же, другими словами, применяясь два раза, дают тождественное. Но такие отображения являются композициями поворота на 180° и отражения относительно некоторой оси, проходящей через начало координат. Формулы для отражения относительно оси легко либо вывести самим, либо посмотреть в общедоступном справочнике (например, [4]).

Предполагаемые знания

Изучение данного курса должно следовать за базовыми курсами анализа, геометрии с топологией, логики и алгебры. Поскольку опыт показывает, что на уровень изложения *важнейших понятий и основных идей* в данных курсах полагаться нельзя, то знания в данных областях предполагаются самые рудиментарные.[3] Очень желательно знакомство с учебным пособием [5], хотя бы с его первой частью. В некоторых случаях в данном пособии имеются и прямые ссылки на [5].

[2] Либо, по мнению скептиков, кучей.

[3] В качестве анекдотического примера можно привести то, что в курсах математического анализа нетривиальное и достаточно широко используемое понятие подпоследовательности упорно считается самоочевидным и не определяется строго.

Глава 1

Базовые структуры

В данной главе вводятся базовые структуры, применяемые в математике, без углубления в их особенности и соотношения.

1.1 Множества и классы

В современной математике понятие множества является одним из центральных и окутанных наибольшим числом предрассудков. Множества являются прежде всего удобным средством превращать высказывания в объекты и, соответственно, операции над высказываниями в функции. При этом логика теории переходит в алгебру. Лучше всего охарактеризовать множество как “единое имя для совокупности всех объектов, обладающих данным свойством." Но это предложение, конечно же, не может считаться определением.

Пытаясь выразить на точном языке данную характеризацию, Г. Фреге пришел к следующей *операции свертки*.

Определение 1.1.1. Класс всех объектов, обладающих свойством $A(x)$, обозначается $\{x \mid A(x)\}$. Если $Y = \{x \mid A(x)\}$, то $A(x)$ называется *характеристическим свойством* класса Y, а Y — *сверткой* предиката A. По определению Y, выполнена следующая эквивалентность:

$$\forall y(y \in Y \Leftrightarrow A(y)).$$

Два класса считаются равными, если их характеристические свойства эквивалентны (*свойство объемности*).[1] (Часто это выражают словами: “Классы равны, если они содержат одни и те же элементы.”) Класс

[1] Мы используем термин *класс*, а не множество, поскольку данный термин в современной математике более общий, он охватывает, в частности, и множества.

X вложен в класс Y ($X \subset Y$), если характеристическое свойство Y следует из характеристического свойства X. Поскольку

$$(A \Leftrightarrow B) \Leftrightarrow (A \Rightarrow B)\ \&\ (B \Rightarrow A),$$

$X \subset Y$ и $Y \subset X$ тогда и только тогда, когда $X = Y$.

Не всякое выразимое на языке логики свойство множеств определяет множество (на самом деле проще всего здесь пример из парадокса Рассела: несуществование $\{x \mid x \notin x\}$). В современной математике принято совокупности множеств и других математических объектов, удовлетворяющих данному свойству, называть *классами*. В традиционной логике понятие класса означало совокупность объектов, удовлетворяющих данному свойству. Г. Кантор, создатель теории множеств, ввел новое понятие потому, что стал рассматривать *сами множества как элементы множеств*. Поэтому часто принимается следующее формальное определение:

Определение 1.1.2. *Множество* — класс, который может быть элементом другого класса.

Классы, не являющиеся множествами (именно такой смысл обычно кладывается в термин ‘класс’ при употреблении в математических работах) не могут быть элементами других классов, и тем более множеств. Таким образом, классы рассматриваются скорее как сокращения, а не как объекты. Доказано, что добавление классов к обычным теориям множеств ничего существенно не меняет.

Тождественно истинное условие, например $x = x$, определяет “полный” класс. Но полный класс является множеством не во всех принятых теориях множеств. Если нет полного множества, то вступает в свои права контекст, и мы вспоминаем о том, что неотъемлемым элементом математической интерпретации является универс — множество всех рассматриваемых в данной теории предметов. Очевидно, что тождественно истинное условие определяет универс, и тождественно истинные формулы, относящиеся к разным теориям, определяют разные универсы.

Второй из простейших классов, и чаще всего встречающееся в формулах — пустое множество $\emptyset$, вообще не содержащее элементов. Очевидно, что пустое множество задается тождественно ложным характеристическим свойством, и соответственно, все пустые множества равны. Пустое множество во всех известных в данный момент теориях множеств является множеством. Далее, *оно является единственным классом, для которого может нарушаться формально понимаемое свойство объемности*, поскольку, если в теории присутствуют сущности, не являющиеся множествами, то они также не имеют элементов.[2]

[2]Строго говоря, в данном случае математически непротиворечивое описание концепту-

В настоящий момент имеется три типа теорий, которые описывают понятие множества. Первый из них возник, когда после осознания несовместимости с классической логикой (и вообще с традиционным понятием импликации, как показал Карри) полного принципа свертки, стали пытаться аксиоматически описать множества, применявшиеся в математике. Неявной предпосылкой данного подхода является то. что множества рассматриваются как некоторые имеющиеся сущности, которые надо охарактеризовать. Наиболее известной и широко применяемой из теорий множеств такого сорта стала теория Цермело-Френкеля ZF. Язык данной теории содержит два бинарных предиката $\in$ и $=$, не содержит ни констант, ни функций. Аксиомы ее следующие:

1. Аксиома объемности:

$$\forall X, Y (\forall z (z \in X \Leftrightarrow z \in Y) \Rightarrow X = Y)$$

Если множества имеют одни и те же элементы, они равны.

2. Пустое множество:

$$\exists X \, \forall x \, x \notin X$$

3. Двухэлементное множество:

$$\forall x, y \, \exists X \, \forall z (z \in X \Leftrightarrow z = x \vee z = y)$$

4. Объединение множества множеств:

$$\forall X \, \exists Y \, \forall y (y \in Y \Leftrightarrow \exists x (x \in X \, \& \, y \in x)$$

(это множество обозначается просто $\bigcup X$.)

5. Множество всех подмножеств:

$$\forall X \, \exists Y \, \forall Z (Z \in Y \Leftrightarrow \forall x (x \in Z \Rightarrow x \in X))$$

Множество всех подмножеств X обозначается $\mathfrak{P} X$.

6. Аксиома подстановки. Если X — множество, и $\forall x (x \in X \Rightarrow \exists 1 y \, A(x, y)$, то

$$\{y \mid \exists x (x \in X \, \& \, A(x, y))\}$$

также множество.

ально противоречиво, поскольку сущности, не являющиеся множествами, сваливаются в одну кучу с множествами и не дается никаких средств их различать.

7. Аксиома бесконечности:
   Существует множество, у которого есть инъекция самого в себя.

$$\exists X\, \exists f \left(\begin{array}{ll} f : X \to X & \& \\ \forall x, y (x \in X \ \& \ y \in X \ \& \ f(x) = f(y) \Rightarrow x = y) & \& \\ \exists y (y \in X \ \& \ \forall x (x \in X \Rightarrow f(x) \neq y)) & \end{array} \right)$$

8. Аксиома выбора:

$$\forall X \left(\begin{array}{ll} \forall Y (Y \in X \Rightarrow \exists y\, y \in Y) & \Rightarrow \\ \exists f (f : X \to \bigcup X \ \& \ \forall Y (Y \in X \Rightarrow f(Y) \in Y) & \end{array} \right)$$

9. Аксиома регулярности:

$$\forall X\, \exists x\, (x \in X \ \& \ \neg\, \exists y (y \in x \ \& \ y \in X))$$

   Суть ее в том, чтобы запретить ситуации вида $x \in x$. Эта аксиома служит примером технических улучшений, необходимых в каждой новой теории для ее логического замыкания.

Контрапозицией аксиомы подстановки получаем, что, если X — класс, φ — инъективное отображение X в Y, то Y — также класс.

Теории ZF достаточно, чтобы описать большинство структур, встречающихся в современной математике, но иногда ее пополняют новыми аксиомами, постулирующими существование “очень больших” множеств.

Другое направление идет от идеи строгой типизации и базируется на предположении, что множества являются идеальными конструкциями, которые нужно построить так, чтобы они составляли концептуально единую систему и обеспечивали бы мощные окольные пути в доказательствах. Впервые было показано, что на идее строгой типизации можно построить практически всю математику, в фундаментальной трехтомной монографии Дж. Уайтхеда и его ученика Б. Рассела [8], которые разделили множества на типы и разрешили им содержать лишь элементы предыдущего типа. Таким образом, отношение принадлежности разрешается использовать лишь в форме $X^i \in Y^{i+1}$, где верхними индексами объектов являются типы. Соответственно, в равенстве типы объектов должны совпадать. Кванторы навешиваются также по типизированным переменным. После такого ограничения вопрос о множестве всех множеств уже не встает, а свертка оказывается безвредной. Впоследствии конструкции теории типов были обобщены и упрощены Л. Хвистеком и Дж. Рамсеем. Хвистек отбросил вторую иерархию,[3] содержавшуюся в [8]. Внутри каждого типа, кроме нулевого, который состоял из ‘внешних’ объектов,

[3] На самом деле также ценную и полезную.

множества были разделены на *порядки*, или *слои*. В определении множества следующего порядка моли быть лишь кванторы по множествам предыдущих порядков. Но сами авторы [8] в значительной степени выхолостили данную конструкцию, постулировав, что для каждого множества существует равное ему множество 0-го порядка.[4]. Рамсей независимо от Хвистека (который опубликовал свою работу на польском языке и она, соответственно, осталась незамеченной) сделал то же упрощение и показал, что для избежания парадоксов достаточно ослабить требование строгой типизации и рассматривать *кумулятивную теорию типов*, в которой в принадлежности $X^i \in Y^j$ $i < j$. Таким образом, каждый следующий тип включает элементы всех ранее построенных типов. Данная конструкция давала возможность выразить практически все, что нужно математикам, но 'несколько сковывала свободу их выражения', заставляя все-таки следить за типами выражений, а математики не привыкли действовать аккуратно в тех случаях, когда это не диктуется математической традицией. Поскольку тогда еще не было программирования, которое заставило бы их сжиться с идеей типов, они предпочли ZF.

В теории типов, помимо аксиомы свертки, нужны лишь аксиома бесконечности (и лишь для нулевого типа, для 'внешних объектов') и аксиома выбора. Но типизация имеет один недостаток. Одни и те же определения мы вынуждены дословно переписывать для разных типов.

В качестве третьей альтернативы, описывающей неформализуемое понятие множества, рассмотрим теорию Куайна NF. Она возникла из идеи преодолеть технические трудности, связанные со строгой типизацией, путем стирания типов.

Определение 1.1.3. Формула называется *стратифицируемой*, если можно приписать типы всем входящим в нее объектам таким образом, чтобы в результате получилась формула теории типов.

Например, формула

$$x \in u \Leftrightarrow \exists z(x \in z \,\&\, z \in y),$$

выражающая наличие множества $\bigcup_{z \in y} z$, стратифицируема, такова же формула $x = x$, определяющая множество всех множеств, а вот формула $x \in x$ такой не является.

Теория множеств NF имеет всего две аксиомы: аксиому объемности и принцип свертки, ограниченный стратифицированными формулами.

Можете спросить, но как такая теория может быть непротиворечива, ведь в ней есть множество всех множеств V и выводимы нестратифицированные

[4] Иначе никак не удавалось построить верхней грани для ограниченного множества действительных чисел

утверждения тоже, например, $V \in V$? Да, в ней выводимы некоторые нестратифицированные утверждения, например, несуществование парадоксального расселовского множества:

$$\neg\, \exists X\, \forall x (x \in X \Leftrightarrow x \notin x).$$

А вот утверждение $V \in V$ не просто доказуемо, оно и стратифицируемо. Ведь констант в нашей теории нет, V вводится в результате описательного определения как $\iota X\ \forall x (x \in X \Leftrightarrow x = x)$. Расшифровывая $V \in V$, получаем утверждение, в котором разным V соответствуют разные связанные переменные. Так что любое конкретное, однозначно определенное множество может иметь разные типы в различных своих вхождениях.

В теории NF доказывается аксиома бесконечности, доказываются другие аксиомы ZF, постулирующие существование конкретных множеств (в аксиоме подстановки формула $A(x, y)$ должна быть стратифицирована), но опровергаются аксиома выбора и аксиома регулярности.

Длительная история развития исследований вокруг NF, которые никогда не прерывались, но текли весьма вяло, привела к установлению многих любопытных фактов. Аксиома математической индукции выполнена в NF лишь для стратифицированных формул, а ее добавление для произвольных приводит к резкому усилению теории и, соответственно, снижению степени правдоподобия предположения о ее непротиворечивости. Тем не менее ни в самой NF, ни в ее усилении аксиомой индукции противоречий не найдено. Никак не удается и сравнить силу двух теорий NF и ZF.

Для наших целей существенно следующее расширение теории NF. Возьмем произвольное множество D, явно определимое в ZF. Возьмем также множество всех его подмножеств, и т.д., на столько этажей, на сколько это необходимо. Введем в NF новый исходный предикат ‘быть объектом’ $\mathrm{Ob}(x)$, объекты не содержат элементов и аксиома объемности ограничивается на множества, т.е. на значения, для которых $\neg\, \mathrm{Ob}(x)$. В стратифицируемых формулах все объекты имеют один и тот же тип. Тогда, если NF непротиворечива, то имеется модель расширенной теории, в которой множество объектов в точности данное множество D, множество множеств объектов — множество $\mathfrak{P}\, D$.[5] Такое расширение NF некоторой структурой S назовем NF_S.

Упражнения к §1.1

1.1.1. Покажите, что в теории NF нельзя воспользоваться кумулятивными типами Рамсея (на самом деле противоречие можно получить, если стратификация нарушится всего на 1 тип).

[5] Заметим, что если просто ограничить аксиому объемности непустыми множествами, то NF весьма ослабляется, в ней уже нельзя доказать аксиому бесконечности и она моделируется внутри ZF.

1.1.2. Покажите, что в расширении NF натуральными числами и их множествами $\mathsf{NF}_{\mathbb{N}}$ для вновь введенных натуральных чисел будет иметь место полный принцип математической индукции.[6]

1.2 Порядок

Структура порядка задается бинарным отношением.

Определение 1.2.1. Если отношение транзитивно и антирефлексивно, оно называется *отношением (частичного) порядка* и обозначается символом $<$ либо похожими на него (например, $\succ$). Если отношение транзитивно и рефлексивно, то оно называется *отношением предпорядка* и обозначается символом, похожим на $\leqslant$ (например, $\succcurlyeq$). Частичный порядок называется *линейным*, если выполнено условие

$$\forall x\, \forall y (x \succ y \vee x = y \vee y \succ x).$$

Множество с отношением частичного порядка на нем называется *частично упорядоченным множеством (чум)*.[7] Множество с отношением предпорядка — *пум* . Множество с отношением линейного порядка — *линейно упорядоченное множество (лум)*.

Определение 1.2.2. Предпорядок называется *строгим предпорядком* (или *нестрогим порядком*), если выполнено

$$\forall x\, \forall y (x \succcurlyeq y \;\&\; y \succcurlyeq x \Rightarrow x = y).$$

Предложение 1.2.1. *R — отношение частичного порядка тогда и только тогда R^{-1} — отношение частичного порядка.*[8]

Для изображения частично-упорядоченных множеств имеется графический аппарат, известный под названием *диаграммы Гессе*. Пример диаграммы Гессе см. на рис. 1.1. На этой диаграмме, как видите, изображаются не все пары из отношения порядка. Элемент y больше элемента x, если есть путь, составленный из идущих вверх дуг диаграммы, ведущий из x в y. Поэтому, в частности, нет нужды проводить дугу, например, от 0 к 1.

Введем несколько понятий, касающихся упорядоченных множеств.

[6] В $\mathsf{NF}_{\mathbb{N}}$ не удается доказать эквивалентность внешнего натурального ряда с внутренним натуральным рядом NF, поскольку из нее следовала бы аксиома индукции для внутреннего натурального ряда.

[7] Симпатичное русское сокращение *чум* введено новосибирской школой. Московская математическая школа его не признает, видимо потому, что в Европе ни чумов, ни чумы нет.

[8] Этот порядок называется *обратным* к R.

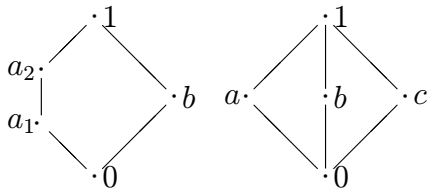


Рис. 1.1: Диаграммы Гессе двух важных пятиэлементных множеств

Определение 1.2.3. Элемент x_0 чума $\mathcal{X}$ называется *наибольшим*, если

$$\forall y(y \in \mathcal{X} \ \& \ y \neq x_0 \Rightarrow x_0 \succ y).$$

Таким образом, он больше всех остальных. *Максимальный* элемент не меньше никакого другого.

$$\forall y(y \in \mathcal{X} \Rightarrow \neg y \succ x_0).$$

Соответственно определяются *минимальный* и *наименьший* элементы. Элемент a называется *верхней гранью* множества $Y \subseteq \mathcal{X}$ (обозначается $\sup Y$ либо $\bigcup Y$), если

$$\forall x(x \in Y \Rightarrow x \prec a \vee x = a) \ \&$$
$$\forall x(x \in \mathcal{X} \ \& \ x \prec a \Rightarrow \exists y(y \in Y \ \& \ x \prec y \ \& \ (y \prec a \vee y = a))).$$

Соответственно определяется нижняя грань ($\inf Y$, $\bigcap Y$). Верхняя (нижняя) грань двух элементов обозначается $a \cup b$ ($a \cap b$). Чум, в котором у каждых двух элементов имеется верхняя и нижняя грань, существуют наибольший и наименьший элементы, называется *структура* или *решетка*. Решетка называется *полной*, если верхние и нижние грани существуют у любого подмножества элементов. Аналогично, чум, у которого есть наименьший элемент и верхняя грань у любых двух элементов, называется *верхней полурешеткой*, а чум, у которого есть наибольший элемент и нижняя грань у любых двух элементов, называется *нижней полурешеткой*. Полурешетки *полные*, если есть соответствующая грань у любого множества элементов.

Полурешетки играют важную роль при оценивании величин, для которых числовые оценки некорректны. Например, часто ресурсы, требуемые для вычисления программы, естественно представлять как верхнюю полурешетку, поскольку ясно, что значит объединить ресурсы для вычисления двух программ сразу, но выделить общие ресурсы этих программ зачастую затруднительно.

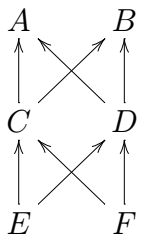


Рис. 1.2: Не решетка

На рис. 1.2 приведен простейший пример чума, не являющегося ни решеткой, ни полурешеткой.

Решетка *дистрибутивна*, если выполнены два закона дистрибутивности для $\cup$ и $\cap$:

$$\begin{array}{c} a \cup (b \cap c) = (a \cup b) \cap (a \cup c); \\ a \cap (b \cup c) = (a \cap b) \cup (a \cap c) \end{array} \tag{1.1}$$

Предложение 1.2.2. *Решетка дистрибутивна тогда и только тогда. когда она не содержит пятиэлементных подмножеств, изоморфных изображенным на рис. 1.1.*

Определение 1.2.4. Упорядоченное множество $\mathfrak{O}$ называется *фундированным*, если для него выполнен принцип возвратной индукции:

$$\forall x \in \mathfrak{O}(\forall y \in \mathfrak{O}\ A(y) \Rightarrow A(x)) \Rightarrow \forall x \in \mathfrak{O}\ A(x).$$

Линейное фундированное множество называется *вполне упорядоченным*.

Предложение 1.2.3. *В непустом фундированном чуме есть хотя бы один минимальный элемент.*

Доказательство. Запишем условие

Существует минимальный элемент, не бóльший x. (1.2)

Это условие удовлетворяет шагу возвратной индукции, значит, оно выполнено для любого элемента $\mathfrak{O}$. Таким образом, мы доказали более сильное утверждение: есть минимальный элемент, не превосходящий произвольный данный. □

Теорема 1.1. *Чум фундирован тогда и только тогда, когда любая убывающая последовательность элементов конечна.*

Доказательство. Пусть чум фундирован. Тогда фундировано и любое его подмножество $\mathfrak{Q}$. В самом деле, можно вести возвратную индукцию по формуле $x \in \mathfrak{Q} \Rightarrow A(x)$, которая эквивалентна возвратной индукции на $\mathfrak{Q}$. Возьмем теперь любую невозрастающую последовательность α элементов $\mathfrak{O}$. Обозначим множество значений данной последовательности через $\mathfrak{Q}$. $\mathfrak{Q}$ — линейно упорядоченное подмножество $\mathfrak{O}$. В нем, по предложению 1.2.3, есть минимальный элемент a, который в данном случае является и наименьшим. Он является некоторым значением последовательности:

$$\exists n\, \alpha(n) = a.$$

Возьмем такое n и обозначим его m. При всех $k > m$, если $\alpha(k)$ определено, то $\alpha(k) = a$. Таким образом, любая невозрастающая последовательность стабилизируется на некотором шаге, значит, любая убывающая последовательность конечна.

> Важное замечание!!
> В данной половине доказательства не используется закон исключенного третьего, поэтому оно применимо значительно шире, чем классическая математика. В частности, конечность последовательностей может использоваться при построении вычислительных алгоритмов. Вообще. доказательство, из которого можно естественно получить построение, называется *конструктивным*. Конструктивность в чистом виде не накладывает ограничений ни на ресурсы, потребляемые получаемым алгоритмом, ни на сложность используемых вычислительных структур. Одним из классических примеров такой конструктивности, которая при *прямом* применении дает:
>
> - невообразимо большую сложность алгоритма и по времени, и по памяти;
> - его реализация требует структур исключительно высокого уровня, недоступных либо безобразно плохо реализованных как в стандартных, так и в наиболее распространенных академических системах программирования,—
>
> является только что рассмотренная конструкция перехода от возвратной индукции к фундированности убывающих последовательностей.

Теперь пусть любая убывающая последовательность конечна. Докажем от противного, что выполнен принцип возвратной индукции. В самом деле, пусть

для некоторого свойства $A(x)$ выполнено отрицание возвратной индукции. Тогда имеется такое $a \in \mathfrak{O}$, что $\neg A(a)$, но вместе с тем шаг индукции выполнен для всех элементов $\mathfrak{O}$. Обозначим a через a_0. Применяя контрапозицию к шагу индукции, получаем

$$\neg A(a_0) \Rightarrow \exists x(x \prec a_0 \;\&\; \neg A(x)).$$

Обозначим данное x через a_1. Повторяя те же действия. получаем бесконечную убывающую последовательность a_i, что противоречит фундированности $\mathfrak{O}$. □

Имеется три важных результата о порядке, зависящих от аксиомы выбора.

Теорема 1.2. ***(Лемма Цорна)*** *Если каждое линейно упорядоченное подмножество чума имеет верхнюю грань, то в чуме существует максимальный элемент.*

Доказательство. Предположим противное. Пусть каждое линейно упорядоченное подмножество чума $\mathfrak{X}$ имеет верхнюю грань, но ни одного максимального элемента нет.

Возьмем произвольный элемент $a_0 \in \mathfrak{X}$. Построим возрастающую ординальную последовательность a_α,идущую по *всем* ординалам.

Для каждого α a_α не может бать максимальным элементом, и поэтому можно выбрать $a_{\alpha\oplus 1}$ как некоторый элемент, больший a_α (применяя аксиому выбора). Для предельных ординалов положим

$$a_\alpha = \sup_{\beta \prec \alpha} a_\beta.$$

По построению, множество a_β линейно упорядочено и не имеет наибольшего элемента, поскольку $a_\beta \prec a_{\beta\oplus 1}$. Значит,

$$a_\alpha \notin \{a_\beta \mid \beta \prec \alpha\}.$$

Таким образом, мы получили, что некоторое подмножество $\mathfrak{X}$ является взаимно-однозначным образом класса ординалов, но по аксиоме подстановки, тогда класс ординалов был бы множеством.

Полученное противоречие доказывает теорему. □

Теорема 1.3. *Каждое множество можно вполне упорядочить.*

Доказательство. Воспользуемся леммой Цорна. Рассмотрим множество $\mathcal{X}$ всех вполне упорядочений на подмножествах X. Таким образом, его элементами являются пары $\langle Y, \prec_Y \rangle$, где $\prec_Y$ — полный порядок на $Y \subseteq X$. Упорядочим элементы $\mathcal{X}$ следующим образом:

$$\langle Y_1, \prec_1 \rangle \prec \langle Y_2, \prec_2 \rangle \Leftrightarrow Y_1 \subset Y_2 \;\&\prec_1 \subset \prec_2 .$$

Вспоминая, что частичный порядок — отношение, т. е. множество пар, видим, что согласно данному определению, $\prec_2$ продолжает $\prec_1$ на Y_2. Возьмем теперь произвольное линейно упорядоченное подмножество $\mathcal{Y} \subseteq \mathcal{X}$. Объединение его элементов также будет элементом $\mathcal{X}$, и поэтому к $\mathcal{X}$ можно применить лемму Цорна. Таким образом, в $\mathcal{X}$ есть максимальный элемент. Возьмем какой-либо максимальный элемент $\mathfrak{X}$. Он и будет искомым полным порядком на X, поскольку, если бы он содержал не все элементы X, то можно было бы к нему добавить еще один элемент и сделать его больше всех старых, таким образом, мы расширили бы $\mathfrak{X}$, и $\mathfrak{X}$ не был бы максимальным. □

Теорема 1.4. *Каждый частичный порядок можно продолжить до линейного порядка.*

Доказательство. По лемме Цорна, аналогично предыдущей теореме, рассматривая множество всех расширений данного частичного порядка. □

Например, лексикографическое упорядочение кортежей букв используется при построении словарей.

Упражнения к §1.2

1.2.1. Что является верхней гранью пустого множества элементов?

1.2.2. А нижней гранью?

1.2.3. Что является верхней гранью всего чума?

1.2.4. А его нижней гранью?

1.2.5. Какой класс чумов определяется условием:

У любого конечного множества элементов есть верхняя и нижняя грань. (1.3)

1.2.6. С какими из определений данного параграфа взаимосвязаны предыдущие задачи?

1.2.7. Если R — линейный порядок, то чем является R^{-1}?

1.2.8. Если R — полный порядок, то чем является R^{-1}?

1.2.9. Если R — линейный порядок, то является ли он решеткой?

1.2.10. Сформулируйте критерий того, что конечный чум не является решеткой, как можно близкий к критерию 1.2.2.

1.2.11. Дано следующее определение (корректное):

Лум *полон*, если он является полной решеткой. (1.4)

Расшифруйте его. Полно ли множество действительных чисел $\mathbb{R}$ с обычным порядком?

1.2.12. Для произвольной решетки законы (1.1) превращаются в неравенства. В какие?

1.2.13. Какой из законов (1.1) влечет другой?

1.3 Алгебраические системы

Настало время подытоживающих и обобщающих определений. Мы начнем с класса *алгебраических систем*, выделенного выдающимся логиком и алгебраистом А. И. Мальцевым, основателем новосибирской школы алгебры и логики. Он объединяет целую совокупность алгебраических и логических структур, популярных в современной математике. Начнем с понятия *рода структуры* или *сигнатуры*.[9]

Определение 1.3.1. *Сигнатура (род алгебраической структуры)* σ — кортеж

$$\langle \mathbb{T}, \mathbb{C}, \mathbb{F}, \mathbb{P}, \chi \rangle ,$$

где $\mathbb{T}$ — непустое множество, называемое *множеством типов* σ, $\mathbb{C}$ — множество *констант* σ, $\mathbb{F}$ — множество *функциональных символов (функций)*, $\mathbb{P}$ — непустое множество *предикатных символов (предикатов)*.

χ — отображение (*характеристика*), удовлетворяющее следующим условиям:

1. $\chi(c) \in \mathbb{T}$, $c \in \mathbb{C}$;
2. $\chi(f)$, $f \in \mathbb{F}$ имеет вид $(\tau_1, \ldots, \tau_n \to \tau)$, $\tau_1, \ldots, \tau_n, \tau \in \mathbb{T}$.
3. $\chi(P)$, $P \in \mathbb{P}$ имеет вид $(\tau_1, \ldots, \tau_n)$, $\tau_1, \ldots, \tau_n \in \mathbb{T}$.
4. $\chi\,(=_\tau) = (\tau, \tau)$.

Заметим, что данное определение отличается от определения сигнатуры в [5] лишь в одном отношении. У нас может быть много исходных типов.

[9] Первый термин идет от Н. Бурбаки, а второй — из логики. В контексте алгебраических структур они — синонимы.

Определение 1.3.2. *Алгебраической системой* сигнатуры σ называется отображение ζ, удовлетворяющее следующим условиям.

1. $\zeta(\tau) \neq \emptyset$ для $\tau \in \mathbb{T}$.
2. $\zeta(\tau_1) \cap \zeta(\tau_2) \neq \emptyset \Rightarrow \tau_1 = \tau_2$ для всех $\tau_1, \tau_2 \in \mathbb{T}$.[10]
3. $\zeta(c) \in \zeta(\chi(c))$ для $c \in \mathbb{C}$.
4. Если $\chi(f) = (\tau_1, \ldots, \tau_n \to \tau)$, $f \in \mathbb{F}$, то $\zeta(f) \in \mathfrak{F}(\zeta(\tau_1) \times \cdots \times \zeta(\tau_n), \zeta(\tau)))$.
5. Если $\chi(P) = (\tau_1, \ldots, \tau_n)$, $P \in \mathbb{P}$, то $\zeta(P) \subseteq \zeta(\tau_1) \times \cdots \times \zeta(\tau_n)$.
6. $\zeta\,(=_\tau) = \{(x, x) \mid x \in \zeta(\tau)\}$.

Здесь и далее $\mathfrak{F}(X, Y)$ — множество функций из X в Y.

Если множество типов состоит из одного элемента, система называется *одноосновной*, если более чем из одного — *многоосновной*. Если множество предикатов состоит лишь из предикатов $=_\tau$, то система называется просто *алгеброй*,[11] если же множество функций пусто, то она называется *логической (реляционной)* системой.[12]

Мы видим, что часто индексы используются для различения подобных понятий в применении к разным типам, например, $=_\tau$. Но для применений равенства тип отношения равенства однозначно определяется типами аргументов. Поскольку накопление индексов препятствует пониманию текста, в сущности ничего не добавляя для строгости, мы принимаем следующее соглашение.

[10] Данное условие означает просто, что множества элементов разных типов не пересекаются. Оно избавляет от кучи технических неприятностей, на которые все время нарываются в математике и в информатике, в частности, из-за привычки изображать единицу и ноль целого, рационального и действительного типов одинаково. Но на самом деле любая такая "техническая частность" скрывает некоторые принципиальные трудности. Данное определение, проводимое в рамках теории множеств, не может быть адекватно многим содержательным условиям, лучше выражаемым в теории категорий. Из-за неформализуемости есть и другие содержательные условия, которые большей частью еще не выражаются на точном языке и поэтому *формально* остаются за рамками математического рассмотрения, но *содержательно* учитываются математиками.

[11] Традиционно в алгебре требуется равенство для всех исходных типов. Но в последнее время в связи с компьютерными приложениями стало ясно, что равенство не всегда является простейшей и/или корректной операцией. Например, равенство машинных действительных чисел означает чаще всего просто то, что они скопированы из одного и того же источника (ввиду неточности вычислений.) Поэтому в нашем определении равенства для *всех* исходных типов не требуется.

[12] Термин "реляционная система" употребляется в современной теории баз данных и частично в алгебре.

Соглашение 1.

Индексы опускаются, если они однозначно определяются из контекста.

Если значениями функциональных символов могут быть не всюду определенные функции, то алгебраическая система называется *частичной*. $a \in \zeta(\tau)$ называются *элементами типа* τ, а само $\zeta(\tau)$ — *носителем* типа τ. *Элементы* — элементы всех типов.[13]

Поскольку часто придется идентифицировать, какой системе, определенной как кортеж понятий, принадлежит то или иное понятие, мы принимаем следующее соглашение, позволяющее использовать достаточно удобную ПАСКАЛеподобную запись.

Соглашение 2.

Поле ϖ кортежа Σ обозначается $\Sigma.\varpi$. $\Sigma.$ может вообще опускаться, если Σ однозначно определена контекстом.

Видно, что алгебраическая система отличается от интерпретации ([5, §**??**]) лишь тем, что у нас может быть несколько исходных типов. таким образом, в ней возникает понятие истинности для логических формул, и мы далее будем ссылаться на истинность или ложность некоторых формул в сигнатуры σ на алгебраической системе S.

Пример 1.3.1. Группа представляет собой одноосновную алгебру с двумя функциональными символами $\circ, {}^{-1}$, двуместным предикатом $=$ и одной константой e. Сигнатуру групп обозначим σ_G.

В упорядоченных группах добавляется еще один двуместный предикат $\leqslant$. Полученную сигнатуру назовем $\sigma_{G\leqslant}$.

Пример 1.3.2. Векторное пространство над полем $\mathbf{P}$ представляется как частичная двуосновная алгебраическая система с исходными типами v и p (вектор и скаляр.) Операции имеют следующие характеристики:

1. Векторное сложение $\chi(\oplus) = (v, v \to v)$.
2. Скалярное сложение $\chi(+) = (p, p \to p)$.
3. Скалярное умножение $\chi(*) = (p, p \to p)$.

[13] Несколько более пуристично было бы сказать:

Множество элементов $\mathbb{U}$ — объединение множеств элементов всех типов.

Но цель данного курса состоит не только в том, чтобы охватить математические структуры достаточно строгим изложением, но и в том, чтобы показать особенности математического языка, принятого при работе с разными структурами.

4. Умножение на скаляр $\chi(\cdot) = (p, v \to v)$.

5. Векторное вычитание $\chi(\ominus) = (v, v \to v)$.

6. Скалярное вычитание $\chi(-) = (p, p \to p)$.

7. Скалярное деление $\chi(/) = (p, p \to p)$.

Последняя из перечисленных операций является частичной. Константами являются скаляры 0 и 1 и вектор $\mathbf{0}$.[14]

Пример 1.3.3. Алгебраические системы, соответствующие действительным числам, многообразны. В качестве одной из них можно привести систему, примерно соответствующую изучаемым в стандартном курсе анализа функциям. Она одноосновная, частичная, содержит константы 0, 1, e, π и функции $+$, $-$, $\cdot$, $/$, $\exp$, $\ln$, $\sin$, $\cos$, $\arcsin$, arctg, mod.

Пример 1.3.4. Элементами алгебраических систем могут быть и объекты более высоких порядков. Так, например, можно рассмотреть алгебраическую систему, состоящую из функций с операцией композиции, или из множеств с булевыми операциями.

Пример 1.3.5. Еще одна интересная алгебра — алгебра *аналитических функций* комплексных чисел. Функция комплексных чисел называется *аналитической*, если она имеет производную. Эта алгебра одноосновная и имеет двуместные операции $+$, $-$, $\times$ и одноместную операцию дифференцирования $\mathbf{D}$.

Пример 1.3.6. Примером реляционной системы может служить частично-упорядоченное множество. Данная система одноосновная. Сигнатуру частично-упорядоченных множеств составляют два двуместных предиката: $=$ и $<$.

Пример 1.3.7. (Ориентированные) графы естественно определить как алгебраические структуры одноосновной сигнатуры $\langle\{v\}, \emptyset, \{R\}\rangle$, где R — двуместный предикат.

Пример 1.3.8. Простейшей алгебраической системой сигнатуры σ является *единичная система* E_σ, определяемая следующим образом:

1. все $\zeta(\tau)$ — одноэлементные множества;

2. значения всех констант и функций — единственные элементы соответствующего типа;

[14] В отличие от математической практики мы использовали разные символы для одноименных операций над векторами и скалярами, чтобы избежать перегрузки операций и возможных двусмысленностей.

3. все предикаты истинны.

В данных примерах видно, что такое «голое» понятие алгебраической системы не отражает многих существенных качеств рассматриваемых в математике структур. В частности, чтобы алгебраическая система сигнатуры σ_G на самом деле была группой, нужно выполнение некоторых условий. Условиями мы займемся в соответствующей главе, а пока что сделаем то, что возможно и без них. Но один вид условий, касающийся частичных структур, нужно рассмотреть сейчас.

В частичных структурах не все выражения определены, и поэтому мы введем *квазипредикат* $!t$, истинный. если t имеет значение, и ложный, если t его не имеет. Мы говорим квазипредикат, а не предикат, потому, что он определен не над элементами наших множеств, а над выражениями. Мы считаем истинным $t = u$, где t и u — выражения, включающие частичные операции, если обе части этого равенства одновременно определены и в случае определенности их значения равны (*мягкое* равенство). Но если в формуле встречается выражение $!t$, то равенство понимается *жестко*: оба значения определены и равны. Для различия жесткого и мягкого равенства для жесткого используется отношение $\doteq$, а для мягкого — $\simeq$.

В математике было замечено, что во многих рассматривавшихся алгебраических системах появлялись одни и те же понятия — гомоморфизма, изоморфизма и т. п. и доказывались теоремы, столь же «нетривиальные» и «разнообразные», как бесчисленные теоремы Коши в традиционном изложении анализа. Появилось желание определить все эти понятия на чуть более высоком уровне, но зато одним махом.

Определение 1.3.3. Отображение φ называется *гомоморфизмом* (или *алгебраическим гомоморфизмом*) алгебраических систем M_1 и M_2 одной и той же сигнатуры σ, если оно для каждого типа τ отображает $M_1.\zeta(\tau)$ в $M_2.\zeta(\tau)$ и для каждой константы, предикатного и функционального символа сигнатуры σ выполнены следующие свойства:

1. $\varphi(M_1.\zeta(c)) = \zeta_{M_2}(c)$.

2. $\varphi(M_1.\zeta(f)(x_1, \ldots x_n)) = M_2.\zeta(f)(\varphi(x_1), \ldots \varphi(x_n))$.

3. $M_1.\zeta(P)(x_1, \ldots x_n) \Rightarrow M_2.\zeta(P)(\varphi(x_1), \ldots \varphi(x_n))$.

Гомоморфизм называется *мономорфизмом*, если он является инъекцией, он — *эпиморфизм*, если он является сюръекцией.

Гомоморфизм — *логический* или *сильный*, если для предикатов выполнено

$$M_1.\zeta(P)(x_1, \ldots x_n) \Leftrightarrow M_2.\zeta(P)(\varphi(x_1), \ldots \varphi(x_n)).$$

Гомоморфизм — *изоморфизм*, если он логический и является биекцией. Две алгебраические системы *изоморфны*, если между ними существует изоморфизм.

Применяя данное определение, скажем, к сигнатуре σ_G, получаем обычное определение гомоморфизма групп:

$$\varphi(e) = e;$$
$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b);$$
$$\varphi(a^{-1}) = \varphi(a)^{-1}.$$

Применяя это же определение к сигнатуре $\sigma_{G\leqslant}$, получаем определение гомоморфизма упорядоченных групп, в котором вдобавок выполнено свойство:

$$a \leqslant b \Rightarrow \varphi(a) \leqslant \varphi(b).$$

Здесь определение гомоморфизма заодно позволяет сделать выбор в пользу одного из исходных понятий: $<$ либо $\leqslant$. Если бы мы выбрали в качестве исходного предиката $<$, то все гомоморфизмы были бы мономорфизмами, что несколько нежелательно в данном случае.

Предложение 1.3.1. *Всякая биекция, являющаяся гомоморфизмом алгебр, является изоморфизмом.*

Доказательство. Биекция является инъекцией, а для инъекций

$$\forall x, y(\varphi(x) = \varphi(y) \Leftrightarrow x = y).$$

А других предикатов, кроме равенств, у нас нет. □

Предложение 1.3.2. *Композиция гомоморфизмов — гомоморфизм.*

Предложение 1.3.3. *Отношение изоморфности рефлексивно, транзитивно и симметрично, т. е. является отношением эквивалентности.*

Эти предложения очевидны. Таким образом, можно факторизовать класс алгебраических систем данной сигнатуры по отношению эквивалентности и рассматривать системы с точностью до изоморфизма.

Упражнения к §1.3

1.3.1. Рассмотрим алгебраическую систему, элементами которой являются функции и объекты, а операциями — применение функции к аргументу и композиция функций. Запишите ее сигнатуру.

1.3.2. А что такое алгебраическая система сигнатуры $\langle\{T\}, \emptyset, \emptyset, \emptyset, \emptyset\rangle$?

1.4 Топологические пространства

1.5 Категории

К началу 50-х гг. стало ясно, что сохраняющие структуру отображения сами образуют некоторую математическую структуру, и порою именно *соотношения между структурой отображений* позволяют навести мосты между разными математическими теориями. Поэтому возник вопрос о создании теории, которая изучала бы на самом нижнем уровне взаимосвязи между отображениями, а на более высоком — между их структурами. Когда она появилась, первоначально даже некоторые математики называли ее *абстрактной чепухой*. Но ныне она получила почтенное название *теории категорий*.

Определение 1.5.1. Категория — двуосновная частичная алгебраическая система с типами Ob (тип *объектов*) и Mor (тип *морфизмов*), частичной операцией $\circ : \mathrm{Mor}, \mathrm{Mor} \to \mathrm{Mor}$, тотальными операциями $\mathrm{Dom} : \mathrm{Mor} \to \mathrm{Ob}$, $\mathrm{CoDom} : \mathrm{Mor} \to \mathrm{Ob}$, $\mathrm{e} : \mathrm{Ob} \to \mathrm{Mor}$, и предикатами равенства для обоих типов, принадлежащая многообразию, определяемому следующими квазитождествами:

$$\begin{gathered}
\mathrm{Dom}\, g = \mathrm{CoDom}\, f \Rightarrow !g \circ f; \\
\mathrm{Dom}\, g = \mathrm{CoDom}\, f \;\&\; \mathrm{Dom}\, h = \mathrm{CoDom}\, g \Rightarrow f \circ (g \circ h) = (f \circ g) \circ h; \\
\mathrm{Dom}\, \mathrm{e}\, a = a, \quad \mathrm{CoDom}\, \mathrm{e}\, a = a; \\
\mathrm{Dom}\, f = a \Rightarrow \mathrm{e}\, a \circ f = f, \quad \mathrm{CoDom}\, f = a \Rightarrow f \circ \mathrm{e}\, a = f.
\end{gathered}$$

Операция $\circ$ называется *композицией морфизмов*, $\mathrm{Dom}\, f$ — *началом* или *областью* морфизма f, $\mathrm{Dom}\, f$ — его *концом* или *кообластью*, $\mathrm{e}\, a$ — *единичным морфизмом* или *единицей* объекта a.

То, что начало f есть a, а его конец — b, обозначается $a \xrightarrow{f} b$ либо $f : a \to b$.

Рассмотрим примеры категорий самой разной природы.

Пример 1.5.1. Пусть совокупность объектов — все множества.[15] Пусть морфизмы — функции. Начало морфизма — область определения функции, конец — ее область значений. Единицей X, очевидно, является функция $\lambda x \in X\, x$. Эту категорию обозначим Set.

[15] Проницательный читатель воскликнет:

— А как же так? Ведь множества всех множеств нет!

Нет его в чаще всего используемой аксиоматике теории множеств. Ее использование связано с тем, что она дает возможность неограниченно применять аксиому выбора. А в теории категорий аксиома выбора попросту не нужна, основные конструкции строго типизированы (вернее, стратифицированы), и мы можем воспользоваться теорией множеств NF.

Пример 1.5.2. А теперь возьмем множества и частично-определенные функции над ними. Они также образуют категорию. Эту категорию обозначим Set_1.

Пример 1.5.3. Поскольку понятие композиции определяется для произвольных бинарных отношений (напомним, что

$$R \circ S = \{(x,z) | x \in X \ \& \ z \in Z \ \& \ \exists y (y \in Y \ \& \ (x,y) \in R \ \& \ (y,z) \in S)\}),$$

множества и их бинарные отношения также образуют категорию. Эту категорию обозначим Set_R.

В данной последовательности примеров общая идея морфизмов как функций сохраняется, хотя сами морфизмы постепенно отходят все дальше и дальше от традиционных функций в сторону обобщения. Но гораздо чаще они отходят от произвольных функций в сторону сужения.

Пример 1.5.4. Алгебраические системы данной сигнатуры и их гомоморфизмы образуют категорию. Точно так же категорию образует любой класс алгебраических систем (все равно, аксиоматизируемый либо нет). Поскольку сами категории являются алгебраическими системами, они вместе с их гомоморфизмами образуют категорию всех категорий Cat.

Далее, поскольку сами категории являются алгебраическими системами, для них определено понятие подсистемы. Подсистема данной категории $\mathfrak{C}$ называется ее *подкатегорией*. $\mathfrak{D}$ — *полная* подкатегория $\mathfrak{C}$, если для любых объектов $a, b \in \mathfrak{D}.\mathsf{Ob}$ любой морфизм $f \in \mathfrak{C}.\mathsf{Mor}$, такой, что $f : a \to b$, принадлежит $\mathfrak{D}.\mathsf{Mor}$. Таким образом, в полной подкатегории сохраняются все морфизмы для оставшихся объектов. Категории алгебраических систем из данного класса данной сигнатуры являются частным случаем общей конструкции: ограничения множества объектов данной категории и взятия соответствующей полной подкатегории. Еще одним примером таких подкатегорий являются категории конечных множеств и их отображений, частичных отображений и отношений.

Пример 1.5.5. Топологические пространства с непрерывными отображениями в качестве морфизмов образуют категорию.

Данные категории стали рассматриваться раньше всего, но уже гомоморфизм не только ограничивает функции, но и обобщает их, поскольку является системой отображений для всех типов из данной сигнатуры. Обратим внимание на определенную буквально одним словом категорию Cat. Это — пример мощности понятий высших порядков. Прежде чем читать дальше, попробуйте расшифровать ее определение сами (что является объектами, а что — морфизмами).

Определение 1.5.2. Гомоморфизм φ категории $\mathfrak{C}$ в категорию $\mathfrak{D}$ называется *функтором* из $\mathfrak{C}$ в $\mathfrak{D}$.

Функтор обладает следующими свойствами:

$$f : a \to b \Rightarrow \varphi(f) : \varphi(a) \to \varphi(b);$$
$$!f \circ g \Rightarrow \varphi(f \circ g) = \varphi(f) \circ \varphi(g).$$

Отсюда следует, что $\varphi(\mathrm{e}\, a) = \mathrm{e}\, \varphi(a)$.

Пример 1.5.6. Рассмотрим несколько категорий, у которых один и тот же единственный объект — множество натуральных чисел $\mathbb{N}$. В категории $\mathfrak{Pr}$ морфизмами являются частично-рекурсивные функции, в $\mathfrak{Gr}$ — обще-рекурсивные функции, а в $\mathfrak{Pr}$ — примитивно-рекурсивные.

Пример 1.5.7. Рассмотрим в качестве объекта переменную x, а в качестве морфизмов — термы данной сигнатуры с единственной свободной переменной x. Композиция термов t и r — подстановка $t[x|r]$. Единица — терм x.

Пример 1.5.8. Рассмотрим в качестве категории комбинаторную логику, в качестве морфизмов — классы эквивалентности λ-термов с единственной свободной переменной x по отношению “Доказуемо $t = u$”. Композиция морфизмов — терм $t[x|u]$. Единица — опять-таки просто x.

Пример 1.5.9. Рассмотрим в качестве объекта множество состояний памяти вычислительного комплекса, в качестве морфизмов — программы, написанные на алгоритмическим языке, удовлетворяющем следующим требованиям:

1. Пустой текст является программой, не меняющей состояния памяти.

2. Если P и Q — программы, то $P; Q$ — программа, выполняющая сначала P, затем Q. В других контекстах символ ; не встречается.

Примером языка, удовлетворяющего подобным требованиям, может служить язык Shell системы UNIX. Такие программы образуют категорию.

В данной последовательности примеров мы двигались от функций к алгоритмам и программам, не теряя общую идею функциональности. Рассмотрим теперь категории несколько другой природы.

Пример 1.5.10. Пусть L — произвольный чум. Превратим его в категорию следующим образом. Объектами являются элементы L, а морфизмами — истинные отношения $a \leqslant b$. Таким образом, морфизм из a

в b есть тогда и только тогда, когда $a \leqslant b$, и он только один. Композиция морфизмов определяется однозначно, и определена по транзитивности отношения порядка. Такая категория обозначается $\mathfrak{C}_L$.

Пример 1.5.11. Ориентированный граф (и даже мультиграф) может рассматриваться как категория, объектами которой служат вершины, а морфизмами — пути. Единица — это пустой путь из 0 дуг, имеющий лишь начало. Композиция морфизмов — конкатенация путей. Эта категория для графа G обозначается $\mathfrak{C}_G$ либо просто G.

И, наконец, рассмотрим случай, когда морфизмы являются "более конкретными" сущностями, чем объекты.

Пример 1.5.12. Пусть единственным объектом категории является моноид H. Морфизмами являются элементы данного моноида, композицией морфизмов — произведение элементов. Для того, чтобы данная конструкция была категорией, достаточно, чтобы произведение было ассоциативным, что гарантируется определением моноида.

Теория категорий пользуется в первую очередь языком коммутативных диаграмм.

Определение 1.5.3. *Диаграмма* — оснащенный мультиграф, вершинам которого приписаны объекты категории, а ребрам — морфизмы из начала ребра в его конец. Диаграмма *коммутативна*, если для любых двух путей из вершины v_1 в вершину v_2 композиции морфизмов этих путей равны.

Например, коммутативность диаграммы (коммутативного квадрата)

$$\begin{array}{ccc} a & \xrightarrow{f} & b \\ {\scriptstyle h_1}\downarrow & & \downarrow{\scriptstyle h_2} \\ c & \xrightarrow[g]{} & d \end{array} \tag{1.5}$$

означает совпадение композиций $f \circ h_2 = h_1 \circ g$. Но *коммутативность диаграмм предполагается, лишь если противное явно не оговорено в тексте, окружающем диаграмму*. Так что читайте тексты внимательнее.

Упражнения к §1.5

1.5.1. В тройке категорий Set, Set_1, Set_R что является подкатегорией чего?

1.5.2. Почему мы не потребовали в расшифровке определения функтора, что $\varphi(\mathrm{e}\, a) = \mathrm{e}\, \varphi(a)$?

1.5.3. Пусть диаграмма (1.5) рассмотрена в категории $\mathfrak{C}_L$, получающейся из чума L (пример 1.5.10). Окружающий текст либо изложен достаточно запутанно, либо просто написан на языке, который Вы разбираете очень плохо (выбирайте согласно степени общей образованности: польский, голландский, японский…) Сумеете ли Вы сделать какие-то выводы относительно ее коммутативности?

1.5.4. Пример 1.5.6 студенты предложили модифицировать несколькими способами. Интеллектуалов предложил рассмотреть категории элементарных функций и функций, вычислимых за полиномиальное время, Талантов — за линейное время и конечно-автоматных. В каком предложении есть некорректности и какие?

1.5.5. Определим несколько более абстрактную категорию на базе графа. Объекты ее — по-прежнему вершины графа, морфизмы — пути, не содержащие циклов. При композиции двух путей мы выкидываем появляющиеся циклы. Корректно ли данное определение, и если нет, то почему?

Глава 2

Конкретные алгебраические структуры

Педагогическое замечание. В изложении курса материал данной главы целесообразно чередовать с материалом предыдущей.

2.1 Полугруппы

2.1.1 Элементарные факты

Понятие *полугруппы* несоизмеримо по своему значению с местом, уделяемым ему в традиционных курсах алгебры, которые по традиции XIX века рассматривают абстрактные алгебраические структуры на примере групп и чуть-чуть полей.

Определение 2.1.1. *Полугруппы* — многообразие одноосновных алгебр сигнатуры $\sigma_S = \langle\{\mathbf{t}\}, \emptyset, \{\circ\}, \{=\}\rangle$, определяемое тождеством:

$$\forall x, y, z\; x \circ (y \circ z) = (x \circ y) \circ z.$$

Моноид — многообразие алгебр сигнатуры $\sigma_{Se} = \langle\{\mathbf{t}\}, \{e\}, \{\circ\}, \{=\}\rangle$, определяемое тождеством полугрупп и следующими двумя:

$$\forall x\; e \circ x = x \quad \forall x\; x \circ e = x.$$

e называется *единицей* полугруппы (моноида). Полугруппа *коммутативна*, если выполнено тождество $a \circ b = b \circ a$, *идемпотентна*, если $a \circ a = a$. Идемпотентная полугруппа называется *связкой*.

Пример 2.1.1. Целые числа, натуральные числа, положительные натуральные числа и вообще натуральные числа больше некоторого n

составляют полугруппы как по сложению, так и по умножению. Эти полугруппы коммутативны.

Пример 2.1.2. Каждая решетка является полугруппой как относительно операции $\cup$, так и относительно $\cap$. Обе эти полугруппы коммутативны и идемпотентны.

Пример 2.1.3. Множество слов над данным алфавитом A является полугруппой и даже моноидом. Оно — свободный моноид над A. Множество непустых слов также полугруппа и является свободной полугруппой над A.

Пример 2.1.4. Любое множество с умножением, определенным как $x \circ y = y$, является полугруппой. Аналогично для алгебраической системы с константой 0 и тождеством $x \circ y = 0$. Такой элемент, что $\forall x, y\, x \circ y = a$, называется *нулем* полугруппы.

Пример 2.1.5. Поскольку операция композиции для функций и отношений ассоциативна, любое множество отношений, замкнутое относительно композиции, является полугруппой.

Этот последний пример показывает, почему полугруппы стали столь важным понятием. А именно, они выявляют алгебраическую структуру, существующую на функциях. Более того, любая полугруппа представима как полугруппа функций.

Теорема 2.1. ***(Теорема о представлениях для полугрупп)*** *Каждая полугруппа изоморфна полугруппе функций с операцией композиции.*

Доказательство. Построим для каждого элемента a полугруппы функцию $f_a = \lambda x.\, x \circ a$. Проверим сохранение операций.

$$f_{a \circ b}(x) = x \circ (a \circ b) = (x \circ a) \circ b = f_b(f_a(x)) = (f_a \circ f_b)(x).$$

□

Как мы заметили, любая решетка определяет коммутативную связку. Теперь докажем, что любая связка определяет строгий предпорядок.

Определим $a \leqslant b$ как $a \circ b = a \;\&\; b \circ a = a$. Транзитивность и рефлексивность введенного отношения установить легко. Теперь установим свойство

$$\forall x, y (x \leqslant y \;\&\; y \leqslant x \Rightarrow x = y).$$

В самом деле, возьмем произвольные a, b, такие, что $a \leqslant b \;\&\; b \leqslant a$. Тогда, по условиям, $a \circ b = a \;\&\; a \circ b = b$. Значит, $a = b$.

Пример 2.1.6. Рассмотрим произвольное непустое множество со следующей операцией умножения: $x \circ y = x$. Это — полугруппа, она идемпотентна, а порядок, ею определяемый, дискретен.

Если связка коммутативна, то ее операция выражается через данный порядок. См. ниже, упражнение 7. Связка является удобной формой выражения ресурсов, которые не зависят от их количества, но зависят от порядка поступления. Например, обед можно определить как произведение

$$\text{Закуска} \circ \text{Суп} \circ \text{Второе} \circ \text{Чай}.$$

Для китайца, скажем, чай стоял бы на первом месте.

Упражнения к §2.1.1

2.1.1.1. Логично ли рассуждение, которое автор однажды слышал в Новосибирском Институте Математики:

> Теория групп — это наука. Следовательно, теория полугрупп — полунаука, а что такое теории квазигрупп и псевдогрупп, даже выговорить стыдно.

2.1.1.2. Элемент a называется *левой единицей*, если для всех x $a \circ x = x$. Элемент a называется *левым нулем*, если для всех x $a \circ x = a$. Соответственно определяются понятия правой единицы и правого нуля. Ответьте на следующие вопросы:

1. Может ли быть в полугруппе несколько левых единиц?
2. А несколько левых нулей?
3. А как насчет правых единиц и нулей?
4. А одновременно левые и правые?

2.1.1.3. Верно ли, что любая идемпотентная полугруппа коммутативна?

2.1.1.4. Может ли в полугруппе быть и единица, и ноль?

2.1.1.5. Можно ли произвольную полугруппу дополнить до моноида?

2.1.1.6. А до полугруппы с нулем?

2.1.1.7. Чем является коммутативная связка с точки зрения порядка? Как в ней выражается умножение через порядок?

2.1.1.8. Элемент a моноида $\mathbb{G}$ называется *расширителем*, если есть такое подмножество $X \subset \mathbb{G}$, что $\{a \circ x \mid x \in X\} = \mathbb{G}$.

1. Пусть моноид состоит из функций с обычной композицией. Чем в данном случае является расширитель?

2. Приведите пример моноида с расширителем.
3. Может ли быть расширитель в группе?
4. А в коммутативном моноиде?

Если да, то приведите пример. Если нет, то обоснуйте.

2.1.1.9. Пусть f — инъекция X в X, а g — ассоциированное с ней накрытие. Что можно сказать о моноиде, порожденном $\{f, g\}$?

2.1.1.10. Пусть f — сюръекция X на X, а g — ассоциированная с ней ретракция. Что можно сказать о моноиде, порожденном $\{f, g\}$?

2.1.2 Строение полугрупп

Для того, чтобы изучать строение математических структур, нужно прежде всего определить операции, с помощью которых можно строить более сложные структуры из более простых того же рода.

Прежде всего, рассмотрим прямое произведение полугрупп как алгебраических структур. Расшифровывая общее понятие теоретико-множественного прямого произведения, получаем, что элементами произведения полугрупп $\mathbb{H}_1$ и $\mathbb{H}_2$ являются пары $\langle a, b\rangle$, где $a \in \mathbb{H}_1$, $b \in \mathbb{H}_2$. Произведение пар определяется покомпонентно.

Пример 2.1.7. Аддитивная полугруппа комплексных чисел может рассматриваться как прямое произведение двух аддитивных полугрупп действительных чисел, поскольку

$$(a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2)i; \tag{2.1}$$
$$a_1 + b_1 i = a_2 + b_2 i \Leftrightarrow a_1 = a_2 \;\&\; b_1 = b_2. \tag{2.2}$$

Предупреждение!

В алгебре прямые произведения полугрупп и групп принято называть прямыми суммами и обозначать $\mathbb{H}_1 \oplus \mathbb{H}_2$. В некоторых более современных изложениях они уже называются прямыми произведениями.

Имеется еще одно любопытное понятие произведения полугрупп — свободное произведение.

Элементами свободного произведения $\mathbb{H}_1$ и $\mathbb{H}_2$ являются такие кортежи, в которых элементы $\mathbb{H}_1$ и $\mathbb{H}_2$ чередуются. При вычислении произведения кортежей $[a_1, \ldots, a_n] * [b_1, dots, b_m]$, кортежи соединяются, и, если на стыке образовались два элемента из одной и той же полугруппы, они перемножаются.

Предупреждение! Заметим, что в классе коммутативных полугрупп свободное произведение является неестественной операцией, поскольку при сохраниении коммутативности оно совпадает с прямым произведением, а при прямом применении оно уничтожает коммутативность, поскольку для элементов двух разных полугрупп $[a] \circ [b] \neq [b] \circ [a]$.

Упражнения к §2.1.2

2.1.2.1. А как определить свободное произведение двух моноидов? Однозначно ли дается такое определение?

2.2 Группы и связанные с ними структуры

Упражнения к §2.2.0

2.2.0.1. Приведите пример группы ортогональных преобразований евклидова пространства, изоморфной группе перестановок n элементов.

2.2.0.2. Приведите пример группы ортогональных преобразований евклидова пространства, изоморфной *мультипликативной* группе вычетов по модулю n.

2.2.0.3. Приведите пример многогранника, группа симметрий которого изоморфна прямой сумме двух циклических групп порядка 4.

2.2.0.4. Приведите пример многогранника, группа симметрий которого изоморфна прямому произведению циклических групп порядка 5 и порядка 2.

2.3 Векторы, модули, тензоры

Одним из важнейших понятий математики является векторное пространство. Традиционно в физике и изложении математики для инженеров векторное пространство определяют через конкретное представление вектора —n-ку координат.[1] Но это определение мало того, что слишком конкретно, оно привязывается к достаточно случайному выбору координатных осей и масштабов на них.

[1] Напомним, что n-ка — кортеж с фиксированной длиной n.

2.4 Алгоритмы и автоматы

2.5 Конечные поля

Упражнения к §2.5

2.5.1. Постройте простейшее поле характеристики 3, не являющееся полем вычетов.

2.5.2. Разложить многочлены на множители в поле вычетов по модулю 2 $\mathbb{Z}_2$.

1. $x^2 + 1$;
2. $x^2 + x + 1$;
3. $x^3 + x^2 + x + 1$;
4. $x^3 + x + 1$.

2.5.3. Разложить многочлены на множители в поле вычетов по модулю 3 $\mathbb{Z}_3$.

1. $x^2 + 1$;
2. $x^2 + x + 1$;
3. $x^3 + 1$;
4. $x^3 + x + 1$.

Глава 3

Алгебраические системы

3.1 Операции над системами

Определение 3.1.1. *Подсистемой* системы S называется такая система S_1 той же сигнатуры, что для всех $\tau \in \mathbb{T}$ $S_1.\zeta(\tau) \subseteq S.\zeta(\tau)$ и для всех объектов, принадлежащих $\bigcup_{\tau\in\mathbb{T}} S_1.\zeta(\tau)$ выполнено

$$S.\zeta(f)(a_1, \ldots, a_n) = S_1.\zeta(f)(a_1, \ldots, a_n),$$
$$S.\zeta(P)(a_1, \ldots, a_n) \Leftrightarrow S_1.\zeta(P)(a_1, \ldots, a_n).$$

Соответственно, S называется *надсистемой* S_1.

Прочтение данного определения просто: подсистема — часть данной системы. Естественно, что любая система является собственной подсистемой и поэтому говорят, что у S нет подсистем. если у нее нет отличных от S подсистем.

Любые алгебраические системы могут быть представлены как логические. В самом деле, заменим все функции f на предикаты

$$P_f(x_1, \ldots, x_n, y) \Leftrightarrow f(x_1, \ldots, x_n) = y.$$

Такое представление систем в логическом виде будем называть *каноническим*.

Каноническое логическое представление не совсем эквивалентно исходной системе. В частности, подсистем у канонического представления может быть гораздо больше, чем у исходной системы (приведите пример!).

Как известно (см. [5, §**??**]) операции и предикаты переносятся на фактормножество по отношению эквивалентности $\cong$ тогда и только тогда, когда они согласованы с данным отношением. Обобщим этот результат на произвольные алгебраические системы.

Определение 3.1.2. *Логическая конгруэнция* на алгебраической системе S — семейство отношений эквивалентности $\cong_\tau$ на $\tau \in \mathbb{T}$, таких, что[1]

$$x_1 \cong y_1 \,\&\, \cdots \,\&\, x_n \cong y_n \Rightarrow f(x_1, \ldots, x_n) \cong f(y_1, \ldots, y_n) \tag{3.1}$$

$$x_1 \cong y_1 \,\&\, \cdots \,\&\, x_n \cong y_n \Rightarrow P(x_1, \ldots, x_n) \Leftrightarrow P(y_1, \ldots, y_n). \tag{3.2}$$

для всех предикатов, кроме $=$

Функция $f/\cong$ называется *фактор-функцией* f по $\cong$, если она удовлетворяет следующим условиям.

$$f/\cong (\hat{x}_1, \ldots, \hat{x}_n) = \hat{f}(x_1, \ldots, x_n)$$

и аналогично для предикатов. Здесь $\hat{x}$ —класс эквивалентности x.

Конгруэнция называется *алгебраической* или просто *конгруэнцией*, если опускается пункт (3.2).

Предложение 3.1.1. *Существуют и однозначно определяются фактор-функции и фактор-предикаты для любой логической конгруэнции $\cong$ на системе S.*

Таким образом, любая логическая конгруэнция определяет фактор-алгебру, значениями функций и предикатов в которой являются фактор-функции и фактор-предикаты соответствующих значений в исходной алгебре.

Для алгебраической конгруэнции предикаты можно определять разными способами, но предпочтительнее всего считать $P(X_1, \ldots, X_n)$ истинным на классах эквивалентности $X_1, \ldots, X_n$, если существуют такие $a_1 \in X_1, \ldots, a_n \in X_n$, что $P(a_1, \ldots, a_n)$ истинно. Итак, мы считаем предикат истинным на классах эквивалентности, если он истинен на некоторых их представителях. Любому гомоморфизму сопоставим конгруэнцию, определяемую им следующим образом.

$$x \cong_\varphi y \Leftrightarrow \varphi(x) = \varphi(y).$$

Теорема 3.1. ***(Теорема о гомоморфизмах)*** *Образ алгебры S при гомоморфизме φ изоморфен $S/\cong_\varphi$.*

Доказательство. Искомый изоморфизм ψ определяется как

$$\psi(\hat{x}) = \varphi(x).$$

Таким образом, он является фактор-гомоморфизмом φ по $\cong_\varphi$. □

[1] Индексы отношений эквивалентности восстанавливаются однозначно, поэтому их опускаем; это — применение Соглашения 1. В дальнейшем применения этого соглашения явно не отмечаются.

Константы задают *примитивные элементы* алгебраической системы, которые входят в любую ее подсистему. Но этим свойством обладают не только они.

Предложение 3.1.2. *Элемент принадлежит пересечению всех подсистем S тогда и только тогда, когда он является значением замкнутого терма.*

Это предложение очевидно, но оно обращает внимание на общее понятие *алгебраической выразимости* (или просто выразимости).

Определение 3.1.3. X называется *множеством типизированных констант*, если на X задана функция χ_X, сопоставляющая каждому $x \in X$ $\chi_X(x) \in \mathbb{T}$. Сигнатура, получающаяся расширением множества констант сигнатуры σ константами из X, обозначается σ_X.

Если X — множество элементов (т. е. $X \subset \mathbb{U}$, то σ_X — сигнатура σ, пополненная константами для всех элементов X, с характеристиками, соответствующим типам этих элементов (т. е. элементы Xслужат типизированными константами для самих себя). a *алгебраически выразим* через X, если a является значением некоторого терма сигнатуры σ_X. Множество элементов, выразимых через X, обозначим $\overline{X}$. Множество элементов X называется *независимым* или *множеством образующих*, если ни один из его членов $a \in X$ не выразим через $X \setminus \{a\}$. Множество X *порождает* алгебру S, если $S.\mathbb{U} = \overline{X}$, т. е. все элементы выразимы через X. Множество образующих *полно* (и тогда часто называется *полной системой образующих*), если оно порождает S.

a *логически выразим* через $b_1, \ldots, b_n$, если есть формула $A(x, \vec{b})$, такая, что истинно

$$\forall x(A(x, \vec{b}) \Leftrightarrow x = a) \tag{3.3}$$

Предложение 3.1.3. *a выразимо через X, если оно выразимо через некоторое конечное число элементов X.*

Предложение 3.1.4. *Выполнены следующие свойства $\overline{X}$, где X — некоторое множество элементов S.*

1. *$\overline{X}$ — наименьшая подсистема S, содержащая X.*
2. *$\overline{\emptyset}$ состоит из значений всех термов без свободных переменных.*
3. *$X \subseteq \overline{X}$.*
4. *$\overline{\overline{X}} = \overline{X}$.*
5. *$X \subseteq Y \Rightarrow \overline{X} \subseteq \overline{Y}$.*

Каждое из этих свойств тривиально, но вместе они характеризуют $\overline{X}$ как *операцию замыкания*. К этому мы вернемся в топологической главе и далее.

И, наконец, если система X независима, то это не означает отсутствия всяких зависимостей между ее элементами. Одно и то же значение может представляться разными термами.

Определение 3.1.4. Система X *свободна*, если любые два различных терма сигнатуры σ_X имеют разные значения. Алгебраическая система S *свободна*, если у нее есть свободная полная система образующих.

Теорема 3.2. *В алгебраической системе может быть не более одной свободной полной системы образующих.*

Доказательство. Пусть X и Y — две различные системы образующих. Тогда их симметрическая разность непуста, и может быть два случая: либо в X есть элемент, не принадлежащий Y, либо наоборот. Разберем их.

Пусть $x_0 \in X$, $x_0 \notin Y$. Поскольку Y — полная система, x_0 выражается как значение некоторого терма в сигнатуре σ_Y. Пусть $\zeta(t(y_1, \ldots, y_n)) = x_0$ и $y_1, \ldots, y_n$ — полный список входящих в него элементов Y. Но каждое из y_i представимо через X, и пусть

$$\begin{cases} y_1 = r_1, \\ \quad \ldots \\ y_n = r_n \end{cases}$$

соответствующие представления. Тогда $x_0 = \zeta(t(r_1, \ldots, r_n))$, но получившийся терм уже в сигнатуре σ_X. Итак, мы получили два выражения для x_0, и X вопреки предположению не является свободной системой.

Второй случай приводится к абсурду аналогично.

Итак, мы привели к абсурду предположение о различии свободных систем образующих, и, значит, любые две такие системы должны совпадать. □

Свободные алгебраические системы интенсивно используются в последнее время в теории типов данных. Там они являются базисом, на основе которого строится теория определений типов данных.

Теперь рассмотрим операцию прямого произведения алгебраических структур.

Определение 3.1.5. Пусть $(S_i)_{i \in I}$ — семейство алгебраических структур сигнатуры σ. *Прямым произведением* алгебраических структур назы-

вается структура $\prod_{i\in I} S_i$, определяемая следующим образом.

$$\prod_{i\in I} S_i.\zeta(\tau) = \{f \mid \mathrm{Dom}\, f = I \;\&\; \forall i(i \in I \Leftrightarrow f(i) \in S_i.\zeta(\tau)\}$$

$$\begin{array}{l}\forall f(f \in \mathbb{F} \;\&\; \chi(f) = (\tau_1, \ldots, \tau_n \to \tau) \Rightarrow \\ \quad \forall g_1 \in \prod_{i\in I} S_i.\zeta(\tau_1) \cdots \forall g_n \in \prod_{i\in I} S_i.\zeta(\tau_n) \\ \qquad \prod_{i\in I} S_i.\zeta(f)(g_1, \ldots, g_n) = \lambda i.\, S_i.\zeta(f)(g_1(i), \ldots, g_n(i)))\end{array} \tag{3.4}$$

$$\begin{array}{l}\forall P(P \in \mathbb{P} \;\&\; \chi(P) = (\tau_1, \ldots, \tau_n) \Rightarrow \\ \quad \forall g_1 \in \prod_{i\in I} S_i.\zeta(\tau_1) \cdots \forall g_n \in \prod_{i\in I} S_i.\zeta(\tau_n) \\ \qquad \prod_{i\in I} S_i.\zeta(P)(g_1, \ldots, g_n) \Leftrightarrow \forall i\, S_i.\zeta(P)(g_1(i), \ldots, g_n(i)))\end{array}$$

В случае конечного I можно в определении элементов функции заменить на n-ки.[2] В произведениях вместо $x(i)$, где x — элемент произведения и $i \in I$, пишем $\mathrm{pr}_i\, x$.

Выделим один важный крайний частный случай. Пусть в произведении 0 членов. Тогда естественно считать произведением структур единичную структуру E_σ. Именно так мы и принимаем в дальнейшем.

В смысле данного определения пространство $\mathbb{R}^n$ является прямым произведением n пространств $\mathbb{R}^1$. Но определение 3.1.5 имеет и ахиллесову пяту — условие истинности предикатов. Принятое в нам условие естественно для равенства. Действительно, два элемента прямого произведения стоит считать равными, лишь если все их компоненты равны. Но почему так же подходить и к другим условиям? Поэтому возникло понятие фильтрованного произведения.

Определение 3.1.6. Пусть $\mathcal{L}$ — решетка. Ее подмножество $\Phi \subset \mathcal{L}$ называется *фильтром*, если выполнены следующие условия:

1. Если $a \in \Phi$ и $a \preccurlyeq b$, то $b \in \Phi$;
2. Если $a \in \Phi$ и $b \in \Phi$, то $a \cap b \in \Phi$;
3. $0 \notin \Phi$.

Фильтр называется *максимальным*, или *ультрафильтром*, если он не вложен ни в какой другой фильтр.

Фильтры и ультрафильтры чаще всего рассматриваются на множестве всех подмножеств некоторого множества индексов I, обозначаемом $\mathcal{P}\, I$. Одно семейство ультрафильтров построить очень легко. В самом деле, очевидно, что множество всех подмножеств I, содержащих некоторый элемент a_0:

$$\{X \mid X \subset I \;\&\; a_0 \in X\}$$

[2] Эти два представления изоморфны для конечных I.

является ультрафильтром на $\mathcal{P}\,I$. Такие ультрафильтры называются *главными* либо *тривиальными*.[3]

Предложение 3.1.5. *Каждый фильтр можно расширить до ультрафильтра.*

Доказательство. Ординальная последовательность фильтров Φ_α называется *направленной*, если из $\alpha \prec \beta$ следует $\Phi_\alpha \subset \Phi_\beta$. Объединение направленной последовательности фильтров является фильтром.

В самом деле, $\mathbf{0}$ не принадлежит ни одному из ее членов, значит, он не принадлежит и объединению. Если $a, b \in \bigcup_\alpha \Phi_\alpha$, то существует β, такое, что $a, b \in \Phi_\beta$, но тогда и $a \cap b \in \Phi_\beta$. Последнее условие тривиально.

Теперь пусть Φ_0 — произвольный фильтр. Вполне упорядочим все фильтры над $\mathcal{L}$, так, чтобы Φ_0 был ее первым членом.[4] Фильтр с номером α обозначим Φ_α.

Построим последовательность фильтров следующим образом:

$$\begin{cases} \Psi_0 = \Phi_0, \\ \Psi_{\alpha+1} = \Phi_{\mu\beta.\,\Phi_\beta \supset \Psi_\alpha}, \\ \Psi_{\omega\cdot\alpha} = \bigcup_{\beta \prec \omega\cdot\alpha} \Psi_\beta. \end{cases}$$

Здесь μ — квантор нахождения наименьшего числа, удовлетворяющего данному условию.

Найдется такой минимальный ординал γ, что $\Psi_{\gamma+1}$ не определено. Тогда Ψ_γ — максимальный фильтр, т.е. ультрафильтр. По построению он расширяет Φ_0. □

Следствие 3.1.6. *Существует неглавный ультрафильтр на $\mathcal{P}(I)$, где I — бесконечное множество.*

Доказательство. Все *коконечные* подмножества I (т.е. подмножества, чье дополнение до I конечно) образуют фильтр. Расширим его до ультрафильтра. Ни один элемент на входит во все множества из построенного ультрафильтра, поскольку он не входит в свое собственное дополнение до I, являющееся коконечным. □

Не просите меня привести хотя бы один пример неглавного ультрафильтра хотя бы над $\mathbb{N}$. Еще в 1968 г. Соловей доказал, что *явно* построить его невозможно.

[3] В данном контексте эти два слова синонимичны (но трудно подобрать другой, где они тоже были бы равнозначными.)

[4] Вот то единственное, но критическое, место, где используется в максимальном объеме аксиома выбора!

Следствие 3.1.7. *В любой булевой алгебре для любого элемента a и ультрафильтра Φ либо a, либо $\bar{a}$ принадлежит Φ.*

Доказательство. Пусть для некоторого элемента ни a, ни $\bar{a}$ не принадлежат Φ. Пусть есть два элемента $b, c \in \Phi$, такие, что $b \cap a = \mathbf{0}$, $c \cap \bar{a} = \mathbf{0}$. Тогда $b \cap c = \mathbf{0}$, но $\mathbf{0}$ не может принадлежать фильтру. Итак, мы привели к противоречию предложение

$$\exists x, y (x \in \Phi \ \& \ y \in \Phi \ \& \ x \cap a = \mathbf{0} \ \& \ y \cap \bar{a} = \mathbf{0}).$$

Но оно эквивалентно предложению

$$\exists x (x \in \Phi \ \& \ x \cap a = \mathbf{0}) \ \& \ \exists y (y \in \Phi \ \& \ y \cap \bar{a} = \mathbf{0}).$$

Формулируя отрицание последнего предложения, получаем

$$\forall x (x \in \Phi \Rightarrow x \cap a \neq \mathbf{0}) \vee \forall y (y \in \Phi \Rightarrow y \cap \bar{a} \neq \mathbf{0}).$$

Таким образом, либо $\{a \cap x \mid x \in \Phi\}$, либо $\{a \cap x \mid x \in \Phi\}$ является фильтром, и Φ — не ультрафильтр. □

Определение 3.1.7. Пусть Φ — фильтр на I. *Фильтрованное произведение* семейства структур $(S_i)_{i \in I}$ по фильтру Φ — фактор-структура $\prod_{i \in I} S_i$ по следующей конгруэнтности:

$$x \cong_\Phi y \Leftrightarrow \left\{ i \mid i \in I \ \& \ \operatorname*{pr}_i x = \operatorname*{pr}_i y \right\} \in \Phi. \tag{3.5}$$

Фильтрованное произведение обозначается $\prod_{i \in I} / \Phi \, S_i$

Определение 3.1.8. Формула $A(\vec{x})$ со свободными переменными $\vec{x}$ *фильтруется по фильтру* $\Phi \subset \mathcal{P}(I)$, если для любого семейства структур $(S_i)_{i \in I}$ $\prod_{i \in I} / \Phi \, S_i \models A(\vec{a})$ тогда и только тогда, когда $\{i \mid S_i \models A(\vec{\mathrm{pr}_i} a)\} \in \Phi$.

Предложение 3.1.8. ***(Теорема Лося)*** *Любая формула фильтруется по любому ультрафильтру.*

Доказательство. Элементарные формулы фильтруются по любому фильтру согласно определению фильтрованного произведения. Далее действуем индукцией по построению формулы.

Пусть для компонент формулы фильтруемость уже установлена. Рассмотрим различные логические связки.

$A \ \& \ B$. Эта формула истинна тогда и только тогда, когда обе ее компоненты истинны. Но, по предположению индукции, тогда оба они истинны на

некоторых множествах индексов из Φ. Но пересечение множеств из фильтра также принадлежит фильтру, по определению.

$A \vee B$. В одну сторону. Поскольку $A \vee B$ истинна на фильтрованном произведении, на нем истинна либо A, либо B. Пусть истинна A. Тогда, по предположению индукции, множество $\{i \mid S_i \models A(\mathrm{pr}_i\, \vec{a})\} \in \Phi$. Но тогда, по определению фильтра, и множество

$$\left\{i \mid S_i \models A(\underset{i}{\mathrm{pr}}\, \vec{a}) \vee B(\underset{i}{\mathrm{pr}}\, \vec{a})\right\} \in \Phi.$$

Второй случай разбирается аналогично.

В другую сторону. Пусть

$$X = \left\{i \mid S_i \models A(\underset{i}{\mathrm{pr}}\, \vec{a}) \vee B(\underset{i}{\mathrm{pr}}\, \vec{a})\right\} \in \Phi.$$

Тогда на некотором подмножестве X истинна A, а на другом — B. Обозначим эти подмножества X_A и X_B. $X \cap \bar{X}_A \supseteq B$. Поскольку либо X_A, либо его дополнение принадлежат ультрафильтру Φ, либо X_A либо X_B принадлежит Φ.

$\forall x\, A(x)$. Пусть $\forall x\, A(x)$ истинно на множестве из ультрафильтра. Если $\forall x\, A(x)$ ложно на произведении, то имеется такое ξ, что

$$\prod_{i \in I} / \Phi\, S_i \nvDash A(\xi),$$

но тогда множество

$$X = \{i \mid i \in I \;\&\; S_i \nvDash A(\underset{i}{\mathrm{pr}}\, \xi)\}$$

принадлежит ультрафильтру, и на всех S_i, $i \in X$ ложно $\forall x\, A(x)$. Но это противоречит предположению.

Обратно, если $\forall x\, A(x)$ истинно на произведении, но множество

$$X = \{i \mid i \in I \;\&\; S_i \models \forall x\, A(x)$$

не принадлежит Φ, то $\bar{X} \in \Phi$ и для каждого $i \in \bar{X}$ найдется $\xi_i \in S_i.\mathbb{U}$, такое, что $U_i \nvDash A(\xi_i)$. Построим ξ следующим образом:

$$\begin{cases} \xi(i) = \xi_i, & i \in \bar{X} \\ \xi(i) \text{ произвольно}, & \text{иначе.} \end{cases}$$

$A(\xi)$ ложно на произведении, что противоречит предположению.

Остальные логические связки разбираются подобным же образом и остаются в качестве упражнения. □

Произведение, фильтрованное по ультрафильтру, называется *ультрапроизведением*. Один частный случай ультрапроизведения встречается достаточно часто — это *ультрастепень*, произведение одинаковых S_i.

Предложение 3.1.9. *Любая ультрастепень S содержит подструктуру, изоморфную S.*

Доказательство. Элементами данной структуры являются классы эквивалентности отображений $\lambda i \in I.\, a$ для всех $a \in \mathbb{U}$. □

Заметим, что такое изоморфное вложение выполнено для любого фильтрованного произведения, но для ультрастепеней оно обладает дополнительным свойством, которое стоит отметить. *Все* формулы, истинные на S, истинны на любой ультрастепени S.

Определение 3.1.9. Две структуры называются *элементарно эквивалентными*, если сохраняются все замкнутые формулы сигнатуры σ. $varphi$ называется *элементарным вложением* S в S_1, если φ — логический мономорфизм и для любой формулы $A(\vec{x})$

$$S \models A(\vec{a}) \Leftrightarrow S_1 \models A(\varphi(\vec{a}).$$

Таким образом, элементарное вложение сохраняет все формулы. Вложение любой структуры в ее ультрастепень — элементарное.

Пример 3.1.1. Частично-упорядоченное множество рациональных чисел элементарно вкладывается в частично-упорядоченное множество действительных чисел.

И, наконец, коснемся вопроса о соотношениях между структурами разной сигнатуры.

Определение 3.1.10. Будем говорить, что $\sigma_1 \subset \sigma_2$, если соответствующие множества вложены и характеристики совпадающих элементов одни и те же.[5] В этом случае называем сигнатуру σ_1 *ограничением* σ_2, а σ_2 — *расширением* σ_1. Расширение (ограничение) *типовое*, если все символы σ_2, в характеристике которых нет типов из $\sigma_2.\mathbb{T} \setminus \sigma_1.\mathbb{T}$, принадлежат соответствующим множествам σ_1.

Алгебраическая структура S_1 сигнатуры σ_1 — *сужение* структуры S_2 сигнатуры σ_2, а S_2 — *расширение* S_1, если все носители типов S_1 совпадают с соответствующими носителями в S_2, и значения всех присутствующих в σ_1 символов одни и те же.

[5] Мы пишем здесь $\subset$ просто потому, что нам данный знак больше нравится, а математическую традицию употреблять его в менее естественном случае не удалось сломать даже Н. Бурбаки.

Пример 3.1.2. Аддитивная группа действительных чисел является сужением поля действительных чисел, а вот мультипликативная группа таковой не является, поскольку из носителя выбрасывается 0.[6]

Векторное пространство над полем P можно рассматривать как типовое расширение соответствующего поля.

В связи с расширениями структур и с приложениями структур в современном программировании важно рассмотреть следующее понятие *относительной структуры*.

Определение 3.1.11. Пусть $\sigma_1 \subset \sigma$. Пусть R — некоторая структура сигнатуры σ. Класс относительных структур для R в сигнатуре σ — класс таких структур,[7] для которых R является типовым ограничением.

В частности, класс векторных пространств над полем действительных чисел — один из классов относительных структур над структурой поля действительных чисел $\mathbb{R}_{+-\cdot/}$.

Над относительными структурами операции обычно производятся несколько по-другому. Например, прямое произведение относительных над одним и тем же $\mathbb{R}$ структур берется лишь для типов, не входящих в $\mathbb{R}$. Само $\mathbb{R}$ остается неизменным.[8] Гомоморфизмы таких структур не изменяют $\mathbb{R}$.

Пример 3.1.3. Рассмотрим случай, как использование переходов и соотношений между различными алгебраическими структурами позволяет сократить рассуждения. Известно, что любая конечная группа изоморфна некоторой группе подстановок. Чему изоморфна мультипликативная группа невырожденных матриц второго порядка над булевым полем[9] $\mathbb{B} = \{\mathbf{0}, \mathbf{1}\}$?

Можно прямо выписать все невырожденные матрицы, их произведения и потратить час на решение данной здачи. А можно рассудить следующим образом и закончить решение за пару минут.

Матрицы второго порядка представляют собой линейные отображения двумерного векторного пространства над данным полем. В данном случае векторное пространство представляет собой совокупность

---

[6] Таким образом, наше понятие сужения и расширения структур не совсем отражает интуитивное.

[7] Как всегда, с точностью до изоморфизма.

[8] Это — первый из встретившихся нам примеров *приведенного произведения*, которое будет рассмотрено подробнее в главе о категориях.

[9] Или, что то же самое, полем вычетов по модулю 2.

четырех точек

$$(\mathbf{1},\mathbf{0})\circ \qquad \circ(\mathbf{1},\mathbf{1})$$

$$(\mathbf{0},\mathbf{0})\circ \qquad \circ(\mathbf{0},\mathbf{1})$$

$(\mathbf{0},\mathbf{0})$ не изменяется при линейных отображениях, и, поскольку невырожденная матрица задает взаимно-однозначное линейное отображение, то остальные три точки переставляются между собой. Так как все они попарно линейно независимы, любые две из них могут стать образом базиса, а третья тогда будет образом $(\mathbf{1},\mathbf{1})$, и мы получаем все перестановки.[10]

Упражнения к §3.1

3.1.1. А почему в примере 1.3.3 мы не добавили tg и ctg?

3.1.2. Сформулируйте сигнатуру для евклидовых векторных пространств.[11]

3.1.3. Сформулируйте сигнатуру для булевой алгебры.

3.1.4. Можно ли рассматривать как алгебраическую структуру формулы логики предикатов? Если да, то какие операции над логическими формулами при этом остаются вне структуры?

3.1.5. Можно ли рассматривать полную булеву алгебру как алгебраическую структуру? Что этому мешает?

3.1.6. Алгебраическая система из примера 1.3.5 является таковой, лишь если выполнена некоторая теорема. Сформулируйте ее.[12]

3.1.7. Приведите пример взаимно-однозначного гомоморфизма, не являющегося изоморфизмом.

[10] В данном случае последний аргумент можно было бы заменить на прямой подсчет числа невырожденных матриц. Но это — тупиковый для обобщений вариант. Смотри ниже упражнение 3.1.16.

[11] **Указание.** Воспользуйтесь тем, что для определения евклидовой метрики и евклидового базиса достаточно ввести операцию скалярного произведения векторов.

[12] Эта теорема и на самом деле выполнена, но, может быть, у Вас не было ее в курсе математики.

3.1.8. Приведите пример алгебраической системы, не имеющей подсистем, каноническое логическое представление которой имеет подсистемы.

3.1.9. А что является значениями констант в фактор-алгебре?

3.1.10. Приведите пример, когда для алгебраической системы $\cong_\varphi$ для некоторого гомоморфизма φ не является конгруэнцией.

3.1.11. Пусть алгебраическая система $\mathbb{Z}^+_-$ имеет носителем множество целых чисел $\mathbb{Z}$ и две обычные операции $+$ и $-$. Очевидно, что $\{1\}$ является полной системой образующих для $\mathbb{Z}^+_-$. Приведите примеры других систем образующих, в том числе из нескольких элементов. Свободна ли хоть одна из них?

3.1.12. Приведите пример системы, в которой нет полных систем образующих и любая система образующих состоит не более чем из одного элемента.

3.1.13. Верно ли, что в программировании производный объект можно рассматривать как расширение исходного? Ведь все операции и поля остаются, могут быть лишь добавлены новые?

3.1.14. Студент Интеллектуалов заявил:

— А зачем все эти тонкости с фильтрами? Просто разделим предикаты на два класса: сильные и слабые. Сильные будем считать истинными, если они истинны на всех компонентах, а слабые — если они истинны хотя бы на одном.

Что Вы можете сказать по поводу этого предложения?

3.1.15. Вдохновленные примером 3.1.1, студенты начали обобщать данное предложение. Классиков доказал, что элементарно эквивалентны аддитивные группы рациональных и действительных чисел, Талантов обобщил это до упорядоченных аддитивных групп, Гениалькис — до упорядоченных мультипликативных групп, а Лыцаренко свел два последних результата в эквивалентность полей рациональных и действительных чисел. Вас просят рассудить данную дискуссию.

1. Кто из студентов сильно увлекся и как легко опровергнуть их предложения?
2. А что же остается верным?

3.1.16. Какой группе подстановок изоморфна группа невырожденных булевых матриц n-го порядка?

3.1.17. А мультипликативная группа невырожденных матриц второго порядка над полем вычетов по модулю 3?

3.2 Многообразия и другие аксиоматизируемые классы

Как мы уже говорили, даже группы не описываются просто как алгебраические структуры. Поэтому перейдем к алгебраическим структурам с дополнительными ограничениями. Эти ограничения могут накладываться двояко: через формулы в данной сигнатуре (внутренние, или аксиоматические, ограничения) и через прямое ограничение класса рассматриваемых структур.

Определение 3.2.1. Пусть задан некоторый класс структур Ξ сигнатуры σ. Теория Th данной сигнатуры является *теорией для* Ξ, если каждая структура из Ξ является моделью Th.[13] Th *полна на* Ξ, если каждая формула сигнатуры σ, истинная на всех $S \in \Xi$, является теоремой Th. Класс Ξ *аксиоматизируем*, если имеется теория Th для Ξ, такая, что на любой структуре $S \notin \Xi$ сигнатуры σ ложна хотя бы одна из аксиом Th.

Пример 3.2.1. Группы и полугруппы являются примерами аксиоматизируемых классов структур, а векторные пространства над $\mathbb{R}$ — неаксиоматизируемого, поскольку $\mathbb{R}$ не может быть описано никакой теорией и всегда возможны нестандартные модели.

Особенно интересны и получили в последнее время широкое применение в теории и частично в практике программирования некоторые частные аксиоматизируемые классы теорий.

Определение 3.2.2. Π-*формула* — формула вида $\forall \vec{x}\, A(\vec{x})$, где $A(\vec{x})$ — бескванторная. *Тождество* — формула вида $\forall \vec{x}\, P(\vec{x})$, где $P(\vec{x})$ — элементарная. *Квазитождество (хорновский дизъюнкт, хорновская формула)*[14] — формула вида

$$\forall \vec{x}\, (Q_1(\vec{x}) \,\&\, \cdots \,\&\, Q_n(\vec{x}) \Rightarrow P(\vec{x}))\,, \tag{3.6}$$

где Q_i, P — элементарные формулы.

[13] Мы специально дали такое понятие теории для Ξ, поскольку нам часто нужна не любая теория, а конечно аксиоматизируемая либо с разрешимым множеством аксиом, и в таком случае лучше пожертвовать полнотой, что и делают и в математике. и в информатике.

[14] Термины квазитождество и хорновская формула употребляются в алгебре и логике, а хорновский дизъюнкт — в программировании и «искусственном интеллекте».

Класс Ξ называется *многообразием*, если он аксиоматизируем теорией из тождеств, *квазимногообразием*, если он аксиоматизируем теорией из квазитождеств, Π-*классом*, если он аксиоматизируем теорией из Π-формул.

Пример 3.2.2. Группы являются многообразием, описываемым, например, теорией

$$\begin{array}{cc} \forall x,y,z\, x\circ(y\circ z)=(x\circ y)\circ z & \forall x\, e\circ x=x \\ \forall x\, x\circ x^{-1}=e & \forall x\, x^{-1}\circ x=e \end{array} \tag{3.7}$$

Теорию групп будем обозначать G.

Заметим, что, если чисто формально заявить, что вводить операцию взятия обратного и единицу нет необходимости, достаточно постулировать разрешимость уравнений

$$\forall x,y\,\exists z\, x\circ z=y \quad \forall x,y\,\exists z\, z\circ x=y \tag{3.8}$$

то класс групп перестает быть даже Π-классом. таким образом, чисто логическая эквивалентность не всегда дает самую удобную формулировку.

Пример 3.2.3. Упорядоченные группы являются квазимногообразием, поскольку к аксиомам G добавляются следующие тождества и квазитождества:

$$\begin{array}{cc} \forall x\, x\leqslant x & \forall x,y,z(x\leqslant y\ \&\ y\leqslant x\Rightarrow x\leqslant z) \\ \forall x,y(x\leqslant y\ \&\ y\leqslant x\Rightarrow x=y) & \\ \forall x,y,z(x\leqslant y\Rightarrow x\circ z\leqslant y\circ z) & \forall x,y,z(x\leqslant y\Rightarrow z\circ x\leqslant z\circ y) \end{array} \tag{3.9}$$

заметим, что, если бы мы взяли в качестве исходного понятия $<$, то у нас появилась бы не хорновская аксиома

$$\forall x,y(x<y\Rightarrow\neg\, y<x).$$

Итак, и здесь мы видим, насколько важен правильный выбор исходных понятий.

Пример 3.2.4. Поля не являются даже квазимногообразием, поскольку в аксиомах для x^{-1} необходимо оговаривать условие $x\neq 0$:

$$\begin{array}{cc} \forall x,y,z\, x\cdot(y\cdot z)=(x\cdot y)\cdot z & \forall x\, 1\cdot x=x \\ \forall x(x\neq 0\Rightarrow x\cdot x^{-1}=1) & \forall x(x\neq 0\Rightarrow x^{-1}\cdot x=1) \\ \forall x,y,z\, x+(y+z)=(x+y)+z & \forall x\, 0+x=x \\ \forall x,y\, x+y=y+x & \forall x\, x+(-x)=0 \\ \multicolumn{2}{c}{\forall x,y,z\, x\cdot(y+z)=x\cdot y+x\cdot z} \end{array} \tag{3.10}$$

Поля являются Π-классом.

Заметим, что понятие свободной алгебраической системы, введенное в предыдущем параграфе, не совпадает с понятиями свободных групп, свободных полугрупп и т.д., принятыми в алгебре. В частности, в любой группе $e \circ e = e$, и значения некоторых термов совпадают. Но в любом квазимногообразии можно выделить алгебраическую систему, в которой принимаются *лишь* такие соотношения между элементами, которые мы *вынуждены* принять, исходя из аксиом. Эта система и служит формализацией различных понятий свободных алгебр из алгебры.

Определение 3.2.3. Пусть Ξ — квазимногообразие алгебраических систем, X — множество типизированных констант, $\Xi * X$ — квазимногообразие, получаемое переходом к сигнатуре σ_X с сохранением тех же аксиом. Ξ_X — совокупность алгебраических систем из $\Xi * X$, порождаемых X. M — инициальная модель относительно Ξ_X, если сама M принадлежит Ξ_X и существует эпиморфизм из M на любую другую алгебраическую систему из Ξ_X.

Теорема 3.3. ***(Теорема об инициальной модели)*** *В любом квазимногообразии Ξ инициальная модель относительно X существует тогда и только тогда, когда есть алгебраическая структура, в которой значения всех констант для X различны.*

Доказательство. Рассмотрим множество термов над сигнатурой σ_X. Пусть Th — теория, аксиоматизирующая Ξ и состоящая из квазитождеств. Пусть Th_X — ее расширение константами из X без добавления новых аксиом. Рассмотрим множество элементарных формул, являющихся теоремами Th_X. Теперь построим алгебраическую систему S в два этапа. Этап 1. Строим алгебраическую систему S_0. Множеством $\zeta(\tau)$ для каждого типа будет множество термов соответствующего типа, f переводит термы $t_1, \ldots, t_n$ в терм $f(t_1, \ldots, t_n)$, $P(t_1, \ldots, t_n)$ считается истинным тогда и только тогда, когда оно доказуемо в Th_X.[15]

Теперь заметим, что отношение $\mathsf{Th}_X \vdash t = u$ является конгруэнцией на алгебраической системе S_0. Обозначим его $\cong_{Th}$.

Этап 2. Возьмем в качестве S фактор-систему S_0 по отношению $\cong_{Th}$. То, что существует эпиморфизм из S на любую систему S_1 из Ξ_X, очевидно.

[15] Таким образом, все недоказуемые элементарные формулы считаются ложными. Это предположение получило в современном логическом программировании и искусственном интеллекте громкое название

Принцип замкнутости мира

и приобрело чрезвычайную популярность в данных кругах. Здесь мы лишь показываем давно известные предпосылки для возможности его принятия, при нарушении которых этот принцип совершенно неприемлем. Смотри ниже упражнения.

Любой элемент S_1 является значением некоторого терма t. Соответственно, отношение $S_1 \models t = u$ является отношением конгруэнтности на множестве термов, оно сильнее $\cong_{Th}$, поскольку S_1 является моделью Th_X. Так что любой класс эквивалентности отображается в класс эквивалентности некоторого своего представителя.

Осталось доказать, что S — модель Th_X. Для этого нужно показать истинность всех аксиом Th_X.

Возьмем произвольную аксиому Th_X. Она имеет вид (3.6). Чтобы она была истинна, достаточно, чтобы для любых значений $x_1, \ldots, x_m$, при которых истинны все Q_i, было истинно P. Подставим вместо $x_1, \ldots, x_m$ произвольные классы эквивалентности термов $t_1, \ldots, t_m$. Если все $Q_i(\hat{t}_1, \ldots, \hat{t}_m)$ истинны, то по построению S, доказуемы $Q_i(t_1, \ldots, t_m)$. Значит, по (3.6), доказуемо и $P(t_1, \ldots, t_m)$, и по построению истинно $P(\hat{t}_1, \ldots, \hat{t}_m)$. □

Итак, построение инициальной модели по виду очень просто: отождествляем лишь те термы, для которых равенство доказуемо и применяем принцип замкнутости мира. По поводу невозможности обобщения теоремы об инициальной модели см. упражнения.

Пример 3.2.5. Свободная группа с образующими $A = \{a_1, \ldots, a_n\}$ является инициальной моделью G_A.

Пример 3.2.6. В современном “логическом программировании,"дабы преодолеть тупик, в который они сами себя загнали, приняв частный случай ПРОЛОГа за общий, понятие поля порою формулируется следующим образом. Вводится новый предикат $\mathsf{NEQ}(x, y)$, для всех различных констант данного типа постулируется $\mathsf{NEQ}(c, d)$ и, поскольку нигде нет ни одной аксиомы, которая вела бы от $\mathsf{NEQ}(x, y)$ к $x = y$, в инициальной модели он выражает неравенство. Но при расширении таких теорий либо моделей очень легко просмотреть неявную цепочку зависимостей, разрушающую данное умолчание.

Рассмотрим теперь несколько тонких логико-алгебраических результатов, показывающих приятные свойства многообразий, квазимногообразий и П-классов.

Определение 3.2.4. Класс *замкнут относительно подсистем,* если он содержит вместе с любой алгебраической системой все ее подсистемы. Класс *замкнут относительно конечных прямых произведений,* если он содержит вместе с любыми системами $S_1, \ldots, S_n$ их прямое произведение $S_1 \times \cdots \times S_n$.

Теорема 3.4. ***(Теорема Лося-Тарского)*** *Класс Ξ является* П*-классом тогда и только тогда, когда он аксиоматизируем и замкнут относительно перехода к подсистемам.*

Доказательство. Докажем более общее предложение. Пусть Th — какая-либо теория, аксиоматизирующая Ξ_1 и полная на Ξ_1. Через Th_Π обозначим множество всех П-формул, являющихся теоремами Th. Класс всех подсистем систем из Ξ_1 обозначим Ξ_2. Докажем, что Ξ_2 — в точности класс всех моделей Th_Π.

Возьмем некоторую модель M теории Th_Π. Введем константы для всех ее элементов и рассмотрим *диаграмму* M — теорию, состоящую из всех истинных и всех отрицаний ложных элементарных формул вида $P(\vec{c})$. Обозначим эту теорию D_M. Докажем, что теория $D_M \cup \mathsf{Th}$ совместима.

В самом деле, если она противоречива, то противоречиво некоторое конечное расширение Th формулами из диаграммы. Выпишем конъюнкцию этих формул $D_0(\vec{c})$, где $\vec{c}$ — совокупность всех констант, входящих в данные формулы. По предположению, в теории Th доказуемо $\neg D_0(\vec{c})$, но ни одна из констант $\vec{c}$ не входит в сигнатуру теории Th, и, значит, на самом деле доказуемо $\forall\vec{x} \neg D_0(\vec{x})$. Но это уже П-формула, и, значит, она истинна на M. Но тогда, подставляя в нее $\vec{c}$, получаем $\neg D_0(\vec{c})$, что противоречит определению $D_0(\vec{c})$.

Теперь, по теореме полноты, построим модель $D_M \cup \mathsf{Th}$. Обозначим ее M_1. Поскольку на ней истинны все формулы из диаграммы M, имеется естественный логический мономорфизм M в M_1. Итак, мы вложили произвольную модель теории Th_Π в модель теории Th.

Обратное утверждение тривиально, поскольку любая истинная П-формула остается таковой после выбрасывания некоторых элементов из модели. □

Отметим сложную логическую структуру данного короткого доказательства. Сначала мы обобщили доказываемое предложение, затем воспользовались компактностью в одну сторону, потом в другую. И, наконец, мы воспользовались свойством моделей.

Теорема 3.5. ***(Характеризация квазимногообразий)*** *Аксиоматизируемый класс является квазимногообразием тогда и только тогда, когда он замкнут относительно подструктур и конечных прямых произведений.*

Доказательство. Первое условие определяет П-классы. Второе рассмотрим аналогично предыдущей теореме. Начнем с **достаточности**, и докажем большее: замкнутость квазимногообразия относительно *произвольных фильтрованных произведений*. В самом деле, пусть квазитождество

$$\forall\vec{x}(Q_1(\vec{x}\ \&\ \cdots\ \&\Rightarrow P(\vec{x}))$$

истинно на S_i, где $i \in \Phi$, и тем не менее ложно на фильтрованном произведении. Тогда есть $\vec{\xi}$, на котором ложно

$$Q_1(\vec{\xi})\ \&\ \cdots\ \&\ Q_n(\vec{\xi}) \Rightarrow P(\vec{\xi}).$$

Значит, выполнены следующие условия:

$$\begin{array}{l} \prod_{i\in I}/\Phi S_i \models Q_1(\vec{\xi}) \Leftrightarrow \quad \{i \mid i \in I \ \&\ S_i \models Q_1(\mathrm{pr}_i\,\vec{\xi})\} \\ \qquad\qquad\qquad\qquad \cdots \\ \prod_{i\in I}/\Phi S_i \models Q_n(\vec{\xi}) \Leftrightarrow \{i \mid i \in I \ \&\ S_i \models Q_n(\mathrm{pr}_i\,\vec{\xi})\} \in \Phi \\ \prod_{i\in I}/\Phi S_i \dashv P(\vec{\xi}) \ \Leftrightarrow \ \{i \mid i \in I \ \&\ S_i \dashv P(\mathrm{pr}_i\,\vec{\xi})\} \in \Phi \end{array} \tag{3.11}$$

Пересекая все приведенные в (3.11) множества, получаем, что

$$Q_1(\vec{\xi}) \ \&\ \cdots \ \&\ Q_n(\vec{\xi}) \Rightarrow P(\vec{\xi})$$

ложно на множестве из фильтра, а, значит, наше предположение ложно.

В обратную сторону, если квазитождество истинно на фильтрованном произведении, а формулы вида

$$Q_1(\vec{a_i}) \ \&\ \cdots \ \&\ Q_n(\vec{a_i}) \Rightarrow P(\vec{a_i})$$

опровергаются на $i \in I$, образующих множество $X \in \Phi$, то определяем

$$\xi(i) = \begin{cases} a_i, & i \in I; \\ \text{произвольно}, & i \notin I. \end{cases}$$

На этом ξ опровергается наше квазитождество.

Переходим к доказательству второй части теоремы. Пусть Th_H — совокупность всех хорновских формул, выводимых в Th. Рассмотрим произвольную модель S теории Th_H. Покажем, что ее диаграмма не противоречит Th. Для этого по теореме компактности достаточно построить модель для всех теорий

$$\mathsf{Th} \cup \{P_1(\vec{a}), \ldots, P_k(\vec{a})\} \cup \{\neg\, Q_1(\vec{a}), \ldots, \neg\, Q_m(\vec{a})\},$$

где $P_i(\vec{a})$ — истинные на S элементарные формулы, а $Q_j(\vec{a})$ — ложные на S.

Поскольку на S ложны все

$$\forall x(P_1(\vec{x}) \ \&\ \cdots \ \&\ P_k(\vec{x}) \Rightarrow Q_j(\vec{x})),$$

эти формулы невыводимы в Th, значит, для каждого j есть модель S_j теории

$$\mathsf{Th} \cup \{\exists x\, \neg(P_1(\vec{x}) \ \&\ \cdots \ \&\ P_k(\vec{x}) \Rightarrow Q_j(\vec{x}))\}.$$

Взяв в качестве значений $\vec{a}$ соответствующие $\vec{x}$, получаем искомую S_j. А теперь строим модель, на которой удовлетворяются все искомые элементарные утверждения, как прямое произведение S_j.

По теореме компактности теперь можно построить модель $\mathsf{Th} \cup D_S$. Эта модель содержит подсистему, изоморфную S, и, следовательно, по замкнутости Ξ относительно подсистем, S является моделью Th. $\square$

Теорема 3.6. *Аксиоматизируемый класс — многообразие тогда и только тогда, когда он — квазимногообразие и замкнут относительно гомоморфизмов.*

Доказательство. **Только тогда** устанавливается легко.

Тогда. Аналогично теореме Лося-Тарского, доказываем, что замыкание квазимногообразия относительно гомоморфизмов является классом моделей теории Th_T, состоящей из всех тождеств, являющихся теоремами Th.

Возьмем произвольную модель S теории Th_T и докажем, что она изоморфна гомоморфному образу некоторой модели Th. Для этого возьмем диаграмму S и рассмотрим лишь ложные элементарные формулы из нее. Для каждой формулы вида $A_{\_} = \neg P(\vec{a})$ из диаграммы D_S тождество $\forall x\, P(\vec{x})$ ложно на S. Следовательно, оно не выводимо из Th и имеется модель теории Th $M_{A_{\_}}$, в которой оно ложно. Она может быть расширена до модели $\mathsf{Th} \cup \neg P(\vec{a})$. Возьмем прямое произведение всех таких моделей. Оно по-прежнему является моделью Th, и в нем ложны все опровержимые на S тождества. Возьмем его подструктуру, порождаемую всеми элементами S. Обозначим ее M. Определим на M отношение конгруэнтности следующим образом:

$$t(\vec{a}) \cong r(\vec{a}) \Leftrightarrow S.\zeta(t)(\vec{a}) = S.\zeta(r)(\vec{a}).$$

Оно не может перевести истинное равенство в ложное, поскольку все ложные равенства из S. Таким образом, данное отношение конгруэнтности определяет гомоморфизм, образ которого изоморфен S. □

Для приложений в информатике важны следующие *относительные* формы данных теорем.

Определение 3.2.5. Ξ — *относительный* Π-класс над R, если он состоит из всех моделей M некоторой теории Th_R, аксиомы которой, содержащие объекты типов, не входящих в сигнатуру R, являются Π-формулами, таких, что R — ограничение M.

Аналогично определяются квазимногообразия и многообразия над R.

Три теоремы характеризации сохраняются и для структур над R, конечно, в замыканиях теперь участвуют только R-структуры и прямое произведение не видоизменяет R, как и определялось в предыдущем параграфе.

Пример 3.2.7. Рассмотрим следующее определение т. н. "*абстрактного типа данных* (АТД)."Он состоит из объектов, типы которых обозначаются $\mathbf{v}$, $\mathbf{a}$ и операций $\mathsf{vertex}(\mathbf{string})\mathbf{v}$, $\mathsf{arc}(\mathbf{string})\mathbf{a}$, $\mathsf{v}_{\mathsf{name}}(\mathbf{v})\mathbf{string}$, $\mathsf{a}_{\mathsf{name}}(\mathbf{a})\mathbf{string}$,

$\mathsf{source}(\mathbf{a})\mathbf{v}$, $\mathsf{dest}(\mathbf{a})\mathbf{v}$ со следующими свойствами новых операций:

$$\mathsf{vertex}(\mathsf{v}_{\mathsf{name}}(v)) = v; \tag{3.12}$$

$$\mathsf{arc}(\mathsf{a}_{\mathsf{name}}(a)) = a; \tag{3.13}$$

$$\mathsf{source}(a) = \mathsf{source}(a1)\ \&\ \mathsf{dest}(a) = \mathsf{dest}(a1) \Rightarrow a = b. \tag{3.14}$$

Это можно рассматривать как описание графов с именованными ребрами и вершинами. Заметим, что условие (3.12) означает лишь инъективность операции присвоения имен. Далее заметим, что в настоящей инициальной модели оно могло бы означать и взаимную однозначность, но у нас множество возможных имен фиксировано: это строки.

Пример 3.2.8. Классическим примером абстрактного типа данных является стек элементов типа $\mathbf{t}$. Он описывается следующими тождествами над фиксированной моделью типа $\mathbf{t}$.

$$\mathsf{push}(\mathsf{empty}) = \mathsf{empty}; \tag{3.15}$$

$$\mathsf{top}(\mathsf{pop}(s, x)) = x; \tag{3.16}$$

$$\mathsf{push}(\mathsf{pop}(s, x)) = s. \tag{3.17}$$

Константа интерпретируется как пустой стек, а операции — как добавление элемента, чтение элемента с вершины стека и удаление вершины. Поскольку все операции у нас функциональные и никакого контекста, который может изменяться в их ходе[16], нет, операции чтения вершины и ее удаления разделены.

Но настоящие сложности начинаются, когда пытаются использовать уже определенные абстрактные типы данных в качестве основы для других АТД, когда, скажем, пытаются дать определение стека элементов из произвольного абстрактного типа данных. Ввиду того, что в АТД по умолчанию предполагается инициальная модель, нет никакой гарантии, что добавление новых квазитождеств не разрушит умолчания.

Упражнения к §3.2

3.2.1. Пусть в сигнатуре одноосновной реляционной системы есть лишь $=$ и две константы a, b. Пусть аксиома имеет вид $\forall x(x = a \vee x = b$. Рассмотрим естественную модель S данной формулы, где $\mathbb{U} = \{a, b\}$. Будет ли аксиома истинна на $S \times S$?

3.2.2. Ответьте, имеет ли инициальную модель относительно $\emptyset$ следующий П-класс одноосновных алгебр. Пусть функциональных и предикатных

[16] Как происходит в стандартном программистском окружении.

символов, кроме $=$, нет, и класс описывается единственной аксиомой: $a = b \vee a = c$. В каком месте не удается здесь применить доказательство теоремы об инициальной модели?

3.2.3. А почему в предыдущем пункте мы назвали класс П-классом? Ведь в аксиоме кванторов вообще нет?

3.2.4. Покажите, с длиной доказательства не более полстраницы, что класс упорядочиваемых групп (т. е. групп, на которых можно ввести отношение порядка, превращающее их в упорядоченную группу) является квазимногообразием. Сумеете ли Вы выписать квазитождества, характеризующие такие группы?

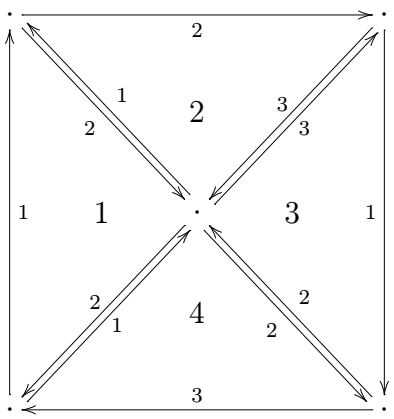
3.2.5. Пусть сигнатура σ состоит из одного типа данных to и равенства на нем. Рассмотрим алгебраическую структуру S_0 с двумя элементами. Пополним σ новым типом данных from с одной константой и одной одноместной функцией f из from в to. Есть ли в классе многообразий над S_0 инициальная модель? Почему здесь нельзя прямо применить теорему об инициальной модели?

Глава 4

Топология

4.1 Симплициальные комплексы

Поскольку топологическая классификация пространств достаточно грубая, можно надеяться найти дискретное представление, которое бы однозначно определяло топологические свойства пространства. Здесь мы рассмотрим такие представлени для важного класса пространств — emphмногообразий.



(4.1)

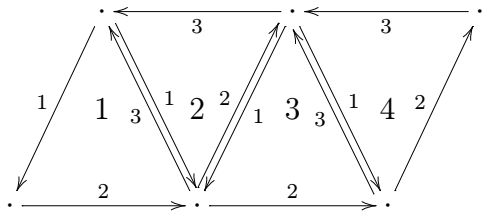
Это многообразие задается как

$$\begin{array}{cccc} 1 & 2 & 2 & 1 & - \\ 1 & 3 & 4 & 1 & - \\ 2 & 3 & 3 & 3 & - \\ 3 & 2 & 4 & 2 & - \end{array} \tag{4.2}$$

Склейкой свободных сторон симплексов 1 и 3 в одном и том же направлении образуется кольцо Мебиуса, а в противоположных — обычное кольцо. Если

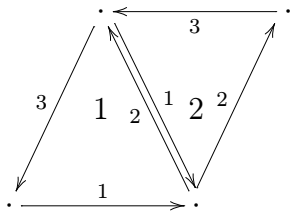
в кольце Мебиуса склеить свободные стороны 2 и 4 в одном и том же направлении, образуется проективная плоскость, в противоположных — бутылка Клейна.

Следующие примеры не будем рассматривать столь детально. Первый из них также лента, которую склеиваем аналогичным образом.



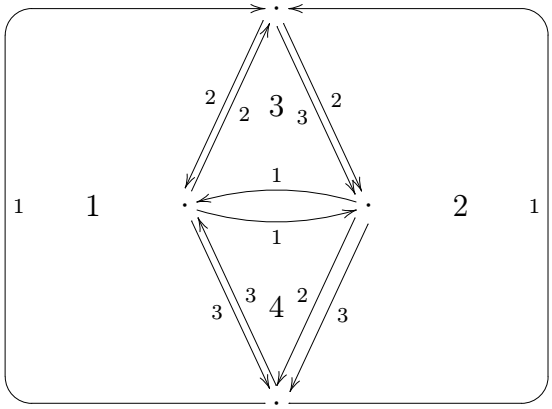
$$\begin{array}{cccc} 1 & 3 & 2 & 1 \\ 2 & 2 & 3 & 1 \\ 3 & 3 & 4 & 1 \end{array} \; -$$

Второй — исключительно простая склейка



$$1 \quad 2 \quad 2 \quad 1 \quad -$$

И последний — изначально с дырой (т. е. кольцо).



$$\begin{array}{cccc} 1 & 2 & 3 & 2 \\ 1 & 3 & 4 & 3 \\ 2 & 2 & 3 & 3 \\ 2 & 3 & 4 & 2 \end{array} \; \begin{array}{c} - \\ - \\ + \\ + \end{array}$$

Глава 5

Категории

5.1 Простейшие понятия

Уже простейшие понятия теории категорий являются понятиями высокого порядка и требуют некоторых усилий и техники мышления для понимания. Например, рассмотрим понятие функтора.

То, что функтор φ является гомоморфизмом категории $\mathfrak{C}$ в категорию $\mathfrak{D}$, означает сохранение всех операций. Так что диаграмма $a \xrightarrow{f} b$ переходит в $\varphi(a) \xrightarrow{\varphi(f)} \varphi(b)$, а для композиций выполнено обычное алгебраическое равенство

$$\mathrm{CoDom}\, f = \mathrm{Dom}\, g \Rightarrow \varphi(f \circ g) = \varphi(f) \circ \varphi(g).$$

Для единиц ничего требовать не нужно, так как сохранение композиций гарантирует их сохранение.

Как видите, перевод краткого и точного определения высшего уровня на более низкоуровневый язык требует некоторых творческих усилий, разные части получающегося разъяснения иногда стоит формулировать на несколько разных языках, а некоторые элементы конкретизации опускать.

Теперь рассмотрим другой пример — подъема более конкретного понятия на высокоуровневый язык. Вспомним определение диаграммы как оснащенного графа 1.5.3 и сформулируем его на чисто алгебраическом языке.

Определение 5.1.1. *Диаграмма* над графом G в категории $\mathfrak{D}$ — функтор из категории $\mathfrak{C}_G$ в $\mathfrak{D}$.

В самом деле, поскольку морфизмами в $\mathfrak{C}_G$ являются пути, и при функторном отображении композиции сохраняются, морфизм, сопоставленный пути α есть композиция морфизмов, сопоставленных составляющим его ребрам, взятым в соответствующем порядке. Коммутативность диаграммы данным

определением не обеспечивается, поскольку разным путям могут соответствовать разные морфизмы.

Упражнения к §5.1

5.1.1. Какое условие надо наложить в алгебраическом определении диаграммы, чтобы она стала коммутативной?

Глава 6

Математические модели концепций программирования

6.1 Рекурсия как неподвижная точка

Рассмотрим очень простое рекурсивное определение

$$f(x) \Leftarrow f(x). \tag{6.1}$$

Каждый, конечно же, скажет, что это — нигде не определенная функция. Но почему же так? Ведь уравнению (6.1) удовлетворяет *любая* функция. Почему же мы выбираем из этого множества решений именно нигде не определенную функцию, а не другую простую, скажем, тождественную?

Мы могли бы задать просто способ вычисления рекурсивных схем, сказав, что каждый раз определение подставляется вместо определяемого в одном из мест получившегося выражения. Но тогда могут вычисляться разные результаты в зависимости от того, какую стратегию вычислений мы примем.

Упражнения к §6.1

6.1.1. Что вычисляет следующая функция

$$f(x) \Leftarrow \mathsf{if}\ x > 100\ \mathsf{then}\ x - 10\ \mathsf{else}\ f(f(x + 11))\ \mathsf{fi};$$

6.1.2. Что вычисляет следующая функция действительных чисел ($\mathbf{D}$ — оператор дифференцирования):

$$F(f, x, n) \Leftarrow \mathsf{if}\ n = 0\ \mathsf{then}\ f(0)\ \mathsf{else}\ F(f, x, n - 1) + \mathbf{D}^n(f)(x)/n!\ \mathsf{fi};$$

6.1.3. А следующая функция:

$$F(f, x, n) \Leftarrow \mathsf{if}\ n \geq 0\ \mathsf{then}\ F(f, x, n + 1) + \mathbf{D}^n(f)(x)/n!\ \mathsf{else\ error\ fi};$$

Литература

[1] *Алгебраическая теория автоматов, языков и полугрупп*. М. А. Арбиб (ред.) М.: Статистика, 1975 (пер. с изд. *Algebraic theory of machines, languages and semigroups.* Edited by Michael A. Arbib. New York & London, Academic Press, 1968.)

[2] N. Bourbaki. *Theorie des ensembles*. Русский перевод:

[3] Ю. Л. Ершов, Е. А. Палютин. *Математическая логика*. М.: Наука, 1979.

[4] Г. Корн, Т. Корн. *Справочник по математике*. М.: Наука, 1973.

[5] Н. Н. Непейвода. *Прикладная логика*. Ижевск, 1998.

[6] А. И. Мальцев. *Алгебраические системы*. М.: Наука, 1970.

[7] *Топология*. А. С. Феденко (ред.), Минск: Вышэйшая школа, 1990.

[8] Whitehead A. N., Russell B. *Principia Mathematica*. v. 1–3. Cambridge University Press, 1910–1913.

Предметный указатель

Персоналии