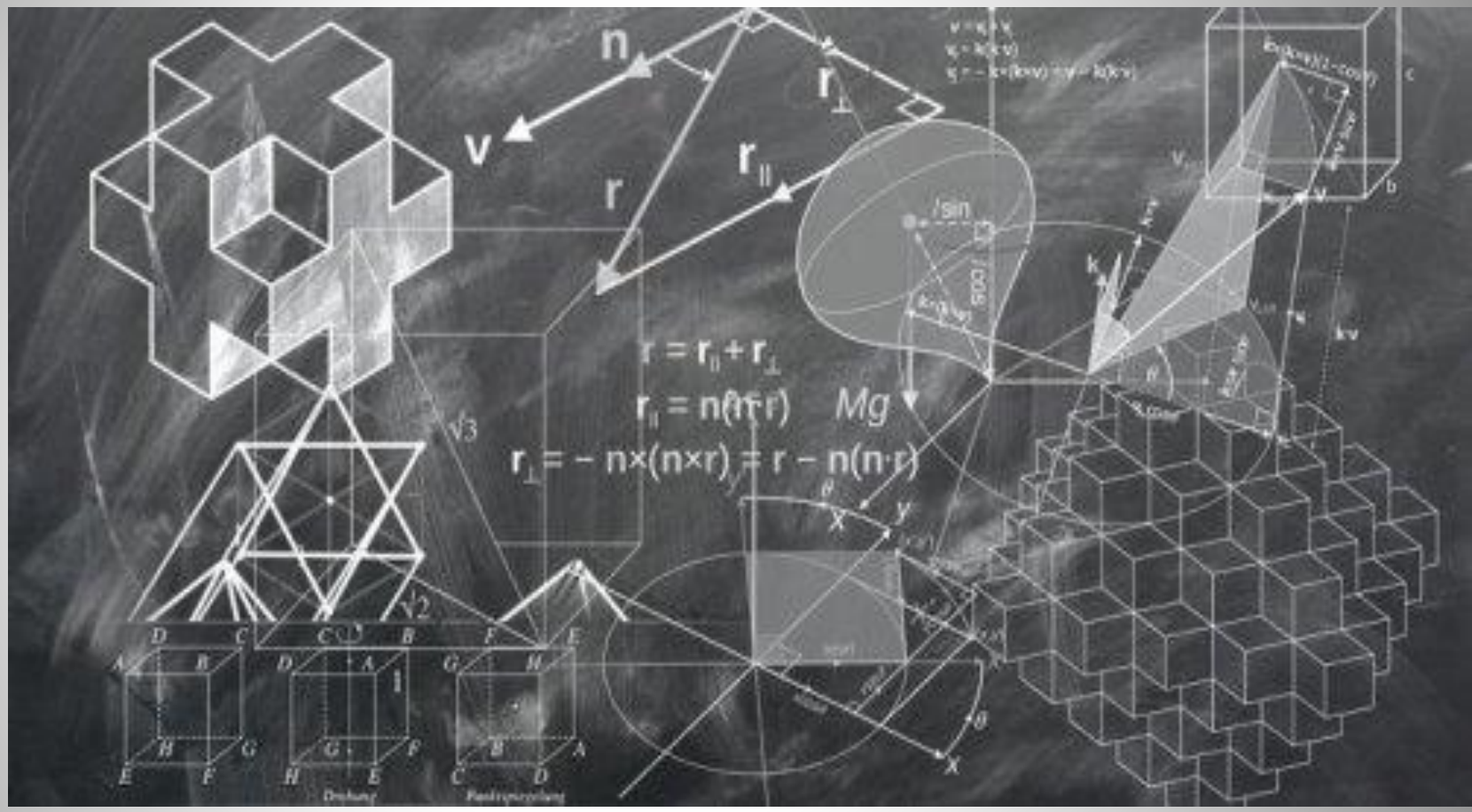
Курс лекций «Дискретная математика»
Ф.И. Каган, к.ф.-м.н., доцент,
Заслуженный работник культуры РФ



06

МАТЕМАТИЧЕСКИЕ СТРУКТУРЫ

6.1. Группа математиков Николя Бурбаки

Н. Бурбаки́ - коллективный псевдоним группы французских математиков (позднее в неё вошли несколько иностранцев), созданной в 1935 году. Целью группы являлось написание серии книг, отражающих состояние математики того времени. Книги Бурбаки написаны в строгой аксиоматической манере и дают замкнутое изложение математики на основе теории множеств.

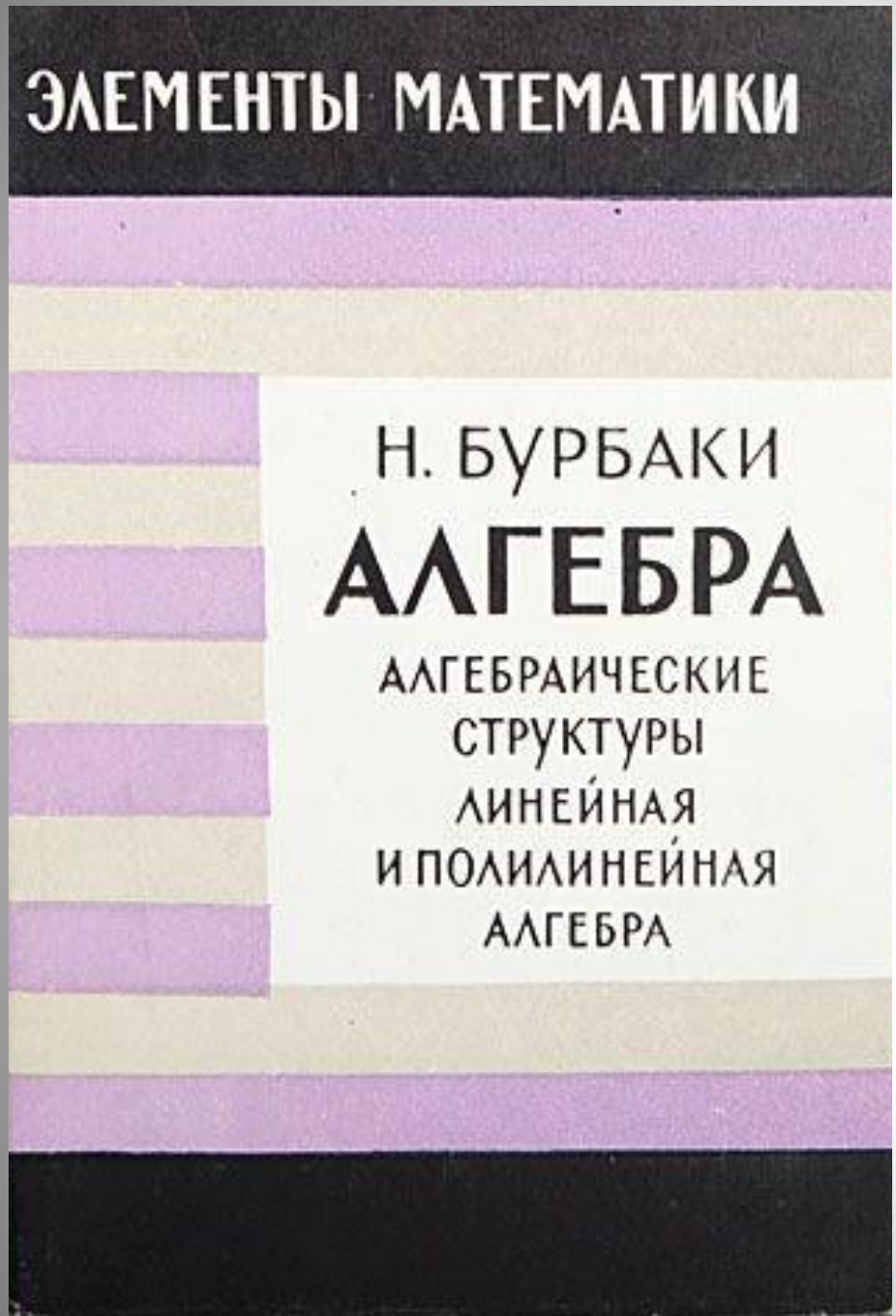
На группу огромное влияние оказала немецкая математическая школа — Д. Гильберт, Г. Вейль, Дж. фон Нейман и особенно алгебраисты Э. Нётер, Э. Артин и Б. Л. ван дер Варден.

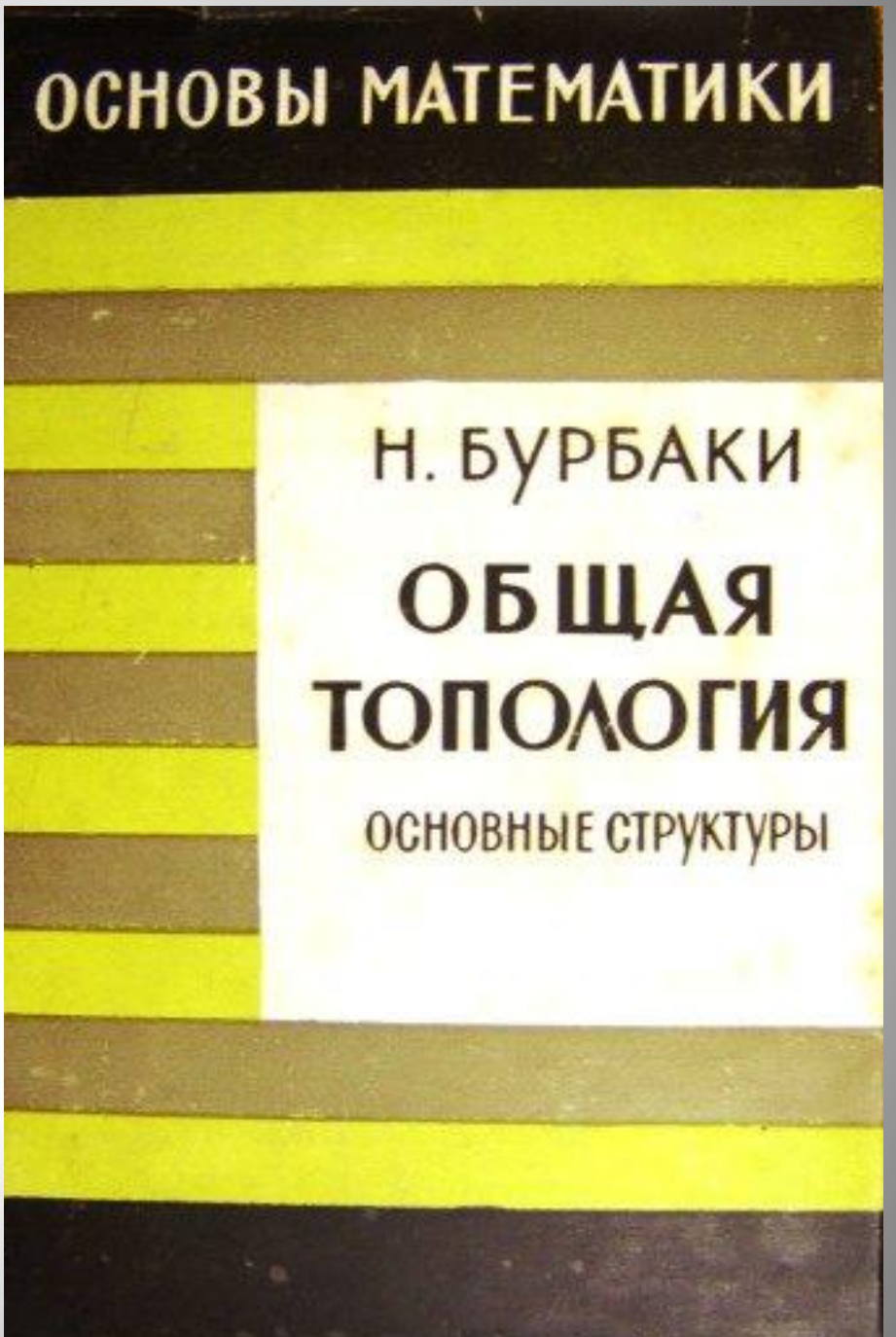
Среди основателей группы крупнейшие французские математики А. Картан, К. Шевалле, Ж. Дьедонне, А. Вейль. и др.

Шарль Дени Бурбаки, французский генерал, фамилия которого была взята в качестве псевдонима группы


НАЧАЛА МАТЕМАТИКИ
Н. БУРБАКИ
ТЕОРИЯ МНОЖЕСТВ


ЭЛЕМЕНТЫ МАТЕМАТИКИ
Н. БУРБАКИ
ОЧЕРКИ ПО ИСТОРИИ МАТЕМАТИКИ


ЭЛЕМЕНТЫ МАТЕМАТИКИ
Н. БУРБАКИ
АЛГЕБРА
АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ
ЛИНЕЙНАЯ И ПОЛИЛИНЕЙНАЯ АЛГЕБРА


ОСНОВЫ МАТЕМАТИКИ
Н. БУРБАКИ
ОБЩАЯ ТОПОЛОГИЯ
ОСНОВНЫЕ СТРУКТУРЫ

6.2. Математические структуры

Под математическая структурой понимается абстрактное множество, элементы которого находятся в некоторых отношениях, причем эти отношения удовлетворяют определенным условиям, которые рассматриваются как аксиомы данной математической структуры.

Понятие математической структуры первоначально было неформальным. Стремясь подвести под громадное здание современной математики надежный логический фундамент, группа Н. Бурбаки поставила своей целью изложить теорию математических структур, последовательно используя аксиоматический метод.

С этим связано неоднозначное отношение части математиков к сочинениям Н. Бурбаки. Тем не менее, понимание математической структуры на основе теории множеств стало практически общепринятым.

Следует также иметь в виду, что использование математических структур при разработках информационных систем и технологий требует точных определений, ибо в конечном счете все сведется к применению процедур программирования, предполагающих высокую степень упорядоченности.

Теория математических структур является иерархической системой.

На первом уровне рассматриваются основные математические структуры, среди них в качестве главнейших, порождающих выделены:

- **алгебраические структуры;**
- **структуры порядка;**
- **топологические структуры.**

В каждом из этих типов структур присутствует достаточное разнообразие. При этом следует различать наиболее общую структуру рассматриваемого типа с наименьшим числом аксиом и структуры, которые получаются из неё в результате её обогащения дополнительными аксиомами, каждая из которых влечёт за собой и новые следствия.

На второй уровень поставлены сложные математические структуры структуры, в которые входят одновременно одна или несколько порождающих структур, но не просто совмещённые друг с другом, а органически скомбинированные при помощи связывающих их аксиом.

Например, топологическая алгебра изучает структуры, которые связаны тем условием, что алгебраические операции являются непрерывными (в рассматриваемой топологии) функциями элементов.

На третьем уровне – частные математические структуры, в которых элементы рассматриваемых множеств, бывшие в общих структурах совершенно неопределёнными, получают более определённую индивидуальность. Именно таким образом получают такие теории классической математики, как математический анализ функций вещественной и комплексной переменной, дифференциальная геометрия, алгебраическая геометрия.

Еще один тип математических структур, который мы будем рассматривать, это так называемы метрические структуры, в которых тем или иным способом присутствует понятие расстояния между элементами основного множества. Такие структуры актуальны для ряда важных приложений.

6.3. Алгебраические структуры

Говорят, что на множестве M имеется алгебраическая структура, если для элементов этого множества определены операции, свойства которых задаются некоторыми аксиомами. Причем с точки зрения алгебры совершенно безразлично, из каких элементов состоит множество, важно лишь, какими свойствами обладают имеющиеся на этом множестве операции. Чаще всего под операцией подразумевается правило (закон), по которому двум элементам из множества, взятым в определенном порядке, сопоставляется третий элемент из этого множества. Такие операции называются бинарными.

Если, например, взять множество действительных чисел, то операциями являются сложение и умножение чисел. Как правило, в алгебре бинарная операция называется или сложением, или умножением и для нее используются обычные обозначения "+" или " ", но это не означает, что операция непременно обладает теми же свойствами сложения или умножения, к которым мы привыкли в элементарной алгебре из школьной программы. Например, в алгебре логики мы имеем дело с бинарными операциями конъюнкции и дизъюнкции, которые обладают свойствами, отличными от свойств алгебры на множестве действительных чисел.

Если на произвольном множестве задать произвольно некоторую операцию, то как правило, ничего интересного из этого образования извлечь не удастся.

Далее мы рассмотрим несколько важных алгебраических структур, а именно, группы, кольца и поля.

6.3.1. Алгебраические структуры: группы

Группой называется непустое множество M , на котором задана некоторая бинарная операция $a \theta b = c$, где $a, b, c \in M$, обладающая следующими свойствами:

- $\forall\ a, b, c \in M\ \ (a \theta b) \theta c = a \theta (b \theta c)$ - свойство ассоциативности;
- $\exists\ e \in M\ \forall\ a \in M\ \ a \theta e = e \theta a = a$ - существование нейтрального элемента;
- $\forall\ a \in M\ \exists\ a^* \in M\ a \theta a^* = a^* \theta a = e$ - существование обратного элемента.

Если операция обладает свойством коммутативности, то группа называется коммутативной или **абелевой** по имени норвежского математика Н.Х. Абеля.

Примеры.

1. Множество Z целых чисел является абелевой группой относительно операции сложения. В роли нейтрального элемента здесь выступает число нуль, а в роли обратного элемента для числа a – противоположное ему число $-a$.
2. Множество Q рациональных чисел и множество R действительных чисел также являются абелевыми группами относительно операции сложения, так что множество Z является подгруппой группы Q, а группа Q – подгруппой группы R.
3. Множества Q и R, соответственно, рациональных и действительных чисел являются абелевыми группами относительно операции умножения чисел. В роли нейтрального элемента здесь выступает число 1, в роли обратного элемента для каждого отличного от нуля числа a – число $1/a$.

4. **Множество Z целых числе не является группой относительно операции умножения. Почему?**

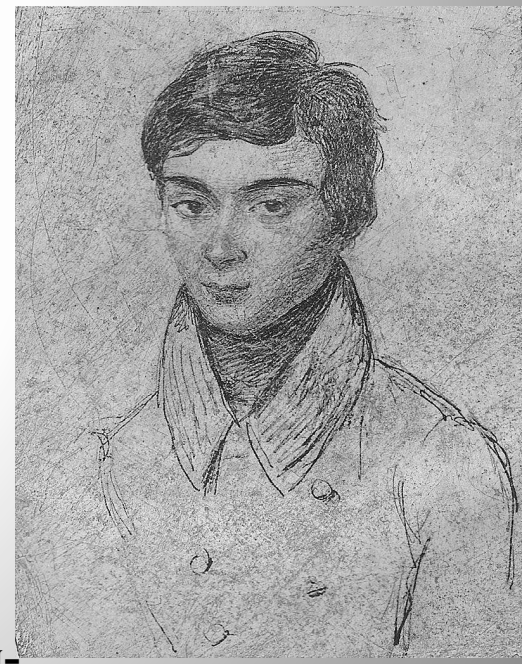
Вопрос.

Является ли группой множество всех высказываний относительно операции конъюнкции? То же относительно операции дизъюнкции?

Теории групп посвящены обширные математические исследования. Они эффективно используются в различных областях математики. С помощью теории групп было, например, доказано, что корни многочлена степени выше четвертой нельзя выразить через конечную комбинацию арифметических операций над коэффициентами многочлена и операций извлечения корней.

Эварист Галуа (Франция, 1811 – 1832)

Родился в семье убежденного республиканца и с юных лет исповедовал взгляды отца. Лишь с 16 лет Галуа начал читать серьёзные математические сочинения. В числе прочих ему попался мемуар Нильса Абеля о решении уравнений произвольной степени. Тема захватила Галуа, он начал собственные исследования и уже в 17 лет опубликовал свою первую работу. Однако талант Галуа не способствовал его признанию так как его решения часто превосходили уровень понимания преподавателей, а свои умозаключения он зачастую не трудился ясно излагать на бумаге. Из-за этого он дважды, с разрывом в год, проваливал экзамен в Политехническую школу.



Карандашный портрет с натуры в 15 лет

Галуа продолжил участвовать в выступлениях республиканцев, вёл себя вызывающе. Дважды он был заключён в тюрьму. Двадцатилетним он был смертельно ранен на дуэли. Конфликт был формально связан с любовной интригой, но имелись также подозрения, что он был спровоцирован роялистами. Обстоятельства дуэли выяснить не удалось. В ночь перед дуэлью Галуа написал длинное письмо своему другу, в котором кратко изложил итоги своих исследований.

За 20 лет жизни и 4 года увлечения математикой Галуа успел сделать открытия, ставящие его на уровень крупнейших математиков XIX века. Галуа исследовал проблему нахождения общего решения уравнения произвольной степени, то есть задачу, как выразить его корни через коэффициенты, используя только арифметические действия и радикалы.

Открытия Галуа произвели огромное впечатление и положили начало новому направлению – теории абстрактных алгебраических структур. Следующие 20 лет Кэли и Жордан развивали и обобщали идеи Галуа, которые совершенно преобразили облик всей математики.

Подробно и интересно – в книге: Инфельд Л. Эварист Галуа. Избранник богов / Жизнь замечательных людей. М., 1965.

6.3.2. Преобразования множеств. Группы преобразований

Пусть M – некоторое множество. Его преобразованием называется любое взаимно-однозначное отображение (биекция) множества M на себя.

Символическая запись отображения t: M → M. Если y = t(x), то y называется образом x, а x – прообразом y.

Композицией (произведением) двух преобразований t_1 и t_2 множества M называется преобразование $t_2 * t_1$, которое каждому x из M ставит в соответствие элемент $t_2(t_1(x))$.

Преобразование e называется тождественным, если для каждого x из M имеет место $e(x) = x$.

Преобразование t^{-1} называется обратным для преобразования t, если

$$t^{-1} * t = t * t^{-1} = e .$$

Обозначим через S(M) множество всех возможных преобразований во множестве M. Можно убедиться, что S(M) удовлетворяет всем аксиомам группы, т.е. является группой преобразований.

Множество $T_G = \{ t \}$ преобразований элементов множества M, являющееся подмножеством множества S(M) всех преобразований во множестве M, может быть подгруппой группы всех преобразований в M, если оно замкнуто относительно операций умножения преобразований и перехода к обратному преобразованию.

Примеры

1. **Группа параллельных сдвигов во множестве точек плоскости.**
2. **Группа преобразований подобия относительно выбранной точки евклидовой плоскости.**
3. **Группа вращений вокруг выбранной точки в евклидовой плоскости.**

Понятие группы, фактически введенное юношей Эваристом Галуа, оказалось исключительно плодотворным как в самой математике, так и в самых разных ее приложениях – в теоретической и экспериментальной физике (физике элементарных частиц, физической теории пространства-времени), в теоретической и экспериментальной химии, в кристаллографии и т.д.

6.3.3. Алгебраические структуры: кольца

Кольцо – это множество R, на котором заданы две бинарные операции: + и × (называемые сложение и умножение), со следующими свойствами, выполняющимися для любых a , b , c ∈ R:

- **a + b = b + a – коммутативность сложения;**
- **a + (b + c) = (a + b) + c – ассоциативность сложения;**
- **∃ 0 ∈ R (a + 0 = 0 + a = a) – существование нейтрального элемента относительно сложения;**
- **∀ a ∈ R ∃ b ∈ R (a + b = b + a = 0) – существование противоположного элемента относительно сложения;**
- **(a × b) × c = a × (b × c) – ассоциативность умножения;**
- **a × (b + c) = (a × b) + (a × c); (b + c) × a = (b × a) + (c × a) – дистрибутивность.**

Иными словами, кольцо – универсальная алгебра (R , + , ×), являющаяся абелевой группой относительно сложения +, полугруппой относительно умножения ×, и обладающая двусторонней дистрибутивностью × относительно + .

6.3.4. Алгебраические структуры: поля

Поле в общей алгебре – множество, для элементов которого определены операции сложения, взятия противоположного значения, умножения и деления (кроме деления на нуль), причём свойства этих операций близки к свойствам обычных числовых операций.

Простейшим полем является поле рациональных чисел. Хотя названия операций поля взяты из арифметики, следует иметь в виду, что элементы поля не обязательно являются числами, и определения операций могут быть далеки от арифметических.

Поле – основной предмет изучения теории полей. Рациональные, вещественные, комплексные числа – примеры полей.

Более строгое определение поля.

Поле – это множество F с введёнными на нём алгебраическими операциями сложения $+$ и умножения $*$, если выполнены следующие аксиомы:

1. Коммутативность сложения: $\forall a, b \in F \; a + b = b + a$.
2. Ассоциативность сложения: $\forall a, b, c \in F \; (a + b) + c = a + (b + c)$.
3. Существование нулевого элемента: $\exists 0 \in F : \forall a \in F \; a + 0 = 0 + a = a$.
4. Существование противоположного элемента: $\forall a \in F \; \exists (-a) \in F : a + (-a) = 0$.
5. Коммутативность умножения: $\forall a, b \in F \; a * b = b * a$.
6. Ассоциативность умножения: $\forall a, b, c \in F \; (a * b) * c = a * (b * c)$.
7. Существование единичного элемента: $\exists e \in F \setminus \{0\} : \forall a \in F \; a * e = a$.
8. Существование обратного элемента для ненулевых элементов: $(\forall a \in F : a \neq 0) \; \exists a^{-1} \in F : a * a^{-1} = e$.

9. Дистрибутивность умножения относительно сложения: $\forall\ a, b, c \in F\ (a + b) * c = (a * c) + (b * c)$.

Здесь аксиомы 1—4 соответствуют определению коммутативной группы по сложению + над F, аксиомы 5—8 соответствуют определению коммутативной группы по умножению * над $F \setminus \{0\}$, а аксиома 9 связывает операции сложения и умножения дистрибутивным законом.

Аксиомы 1-7 и 9 — это определение коммутативного кольца с единицей. Исключив аксиому коммутативности умножения, получим определение тела. В связи с другими структурами (исторически возникшими позднее) поле может быть определено как коммутативное кольцо, являющееся телом.

6.4. Линейные пространства

Линейным (векторным) пространством называется множество V произвольных элементов, называемых векторами, в котором определены операции сложения векторов и умножения вектора на число, т.е. любым двум векторам u и v поставлен в соответствие вектор u+v, называемый суммой векторов u и v, любому вектору v и любому числу λ из поля действительных чисел R поставлен в соответствие вектор λv, называемый произведением вектора v на число λ; так что выполняются следующие условия:

1. **$\forall\ u, v \in V\ u + v = v + u$ (коммутативность сложения);**
2. **$\forall\ u, v, w \in V\ u + (v + w) = (u + v) + w$ (ассоциативность сложения);**
3. **$\exists\ o \in V\ \forall\ v \in V\ v + o = v$ (существование нулевого вектора);**

4. $\forall\ \mathbf{v} \in V\ \exists\ (-\mathbf{v}) \in V\ \mathbf{v} + (-\mathbf{v}) = \mathbf{o}$ **(существование противоположного вектора);**
5. $\forall\ \mathbf{u}, \mathbf{v} \in V, \forall\ \lambda \in \mathbf{R}\ \lambda(\mathbf{u} + \mathbf{v}) = \lambda\,\mathbf{u} + \lambda\,\mathbf{v}$ **(дистрибутивность умножения на число относительно сложения векторов);**
6. $\forall\ \mathbf{v} \in V, \forall\ \lambda, \mu \in \mathbf{R}\ (\lambda + \mu)\,\mathbf{v} = \lambda\,\mathbf{v} + \mu\,\mathbf{v}$ **(дистрибутивность умножения вектора на число относительно сложения чисел) ;**
7. $\forall\ \mathbf{v} \in V, \forall\ \lambda, \mu \in \mathbf{R}\ \ \lambda(\mu\,\mathbf{v}) = (\lambda\,\mu)\,\mathbf{v}$ **(ассоциативность умножения вектора на число).**
8. $\forall\ \mathbf{v} \in V\ 1 \cdot \mathbf{v} = \mathbf{v}$ **(единица как нейтральный элемент при умножении векторов на число).**

Условия 1-8 называются аксиомами линейного пространства. Знак равенства, поставленный между векторами, означает, что в левой и правой частях равенства представлен один и тот же элемент множества V, такие векторы называются равными.

В определении линейного пространства операция умножения вектора на число введена для действительных чисел. Такое пространство называют линейным пространством над полем действительных (вещественных) чисел, или, короче, вещественным линейным пространством. В качестве числового поля можно выбрать и поле Q рациональных чисел, при этом получим линейное пространство над полем рациональных чисел. Далее будут рассматриваться вещественные линейные пространства. В некоторых случаях для краткости будем говорить о пространстве, опуская слово линейное, так как все пространства, рассматриваемые ниже — линейные.

6.5. Метрические пространства

Метрическое пространство есть пара (X , d), где X – множество, а d – числовая функция двух переменных, которая определена на декартовом произведении X × X, принимает значения в множестве вещественных чисел, и такова, что

1. $\forall$ x, y $\in X$ d (x , y) = 0 $\Leftrightarrow$ x = y (*аксиома тождества*).

2. $\forall$ x, y $\in X$ d (x , y) = d (y , x) (*аксиома симметрии*).

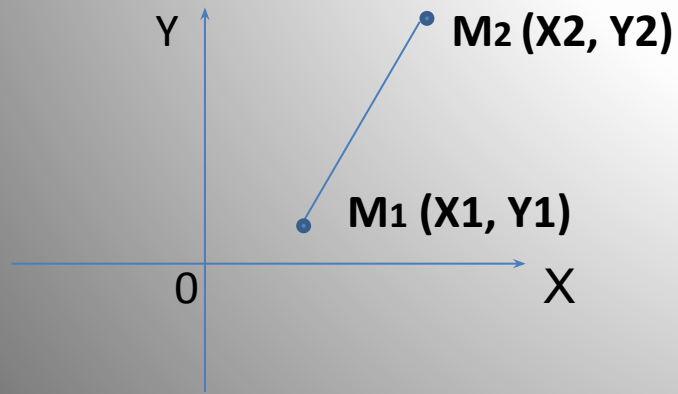
3. $\forall$ x, y, z $\in X$ d (x , z) $\leqslant$ d (x , y) + d (y , z) (*аксиома треугольника* или неравенство треугольника).

При этом множество X называется подлежащим множеством метрического пространства, элементы множества X называются точками метрического пространства, функция d называется метрикой.

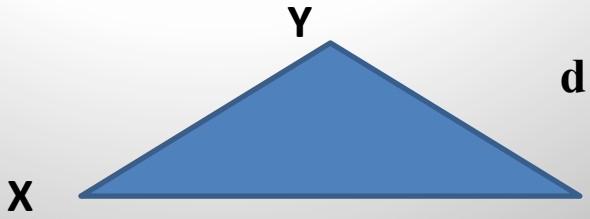
Взаимно-однозначное соответствие (биекция) между различными метрическими пространствами (X , d_X) и (Y , d_Y), сохраняющая расстояния, называется изометрией. В этом случае пространства называются изометричными.

Приведем два примера метрических пространств.

6.5.1. Двумерное евклидово пространство



$$d(M1, M2) = \sqrt{(X2 - X1)^2 + (Y2 - Y1)^2}$$



$$d(x, z) \leqslant d(x, y) + d(y, z)$$

6.5.2. Метрическое пространство непрерывных на отрезке функций

Пусть F – множество, элементами которого являются всевозможные функции, непрерывные на отрезке [a, b] числовой оси. Метрика, определяемая формулой

$$d(f, g) = \max_{t \in [a, b]} |f(t) - g(t)|,$$

превращает множество F функций в метрическое пространство. Это простейший пример метрических пространств, которыми занимается специальный раздел математики, получивший название «функциональный анализ».

6.6. Упорядоченные множества

До сих пор мы рассматривали математические структуры, в основе определения которых лежали либо операции над элементами, обладающие заданными аксиомами свойствами, либо парам элементов приписывалось некоторое число, которое в случае метрических пространств определяло метрику в пространстве, т.е. аналог расстояния между элементами множества.

Вместе с тем многие важные математические структуры определяются с помощью так называемых бинарных отношений, в частности, отношения порядка.

6.6.1. Декартово произведение множеств. Бинарные отношения

Пусть даны два множества X и Y. Прямое (декартово) произведение множества X и множества Y есть такое множество $X \times Y$, элементами которого являются упорядоченные пары (x , y) для всевозможных $x \in X$ и $y \in Y$.

Упорядоченную пару, образованную из элементов a и b, принято записывать, используя круглые скобки: (a; b). Элемент a называют первой координатой (компонентой) пары, а элемент b – второй координатой (компонентой) пары.

В частности, сомножители в декартовом произведении могут быть одинаковы. Тогда мы говорим о декартовой степени (квадрате, кубе,…, n-ой степени) множества X: X^2, X^3, …, X^n.

Бинарное (двухместное) отношение – это отношение между двумя множествами X и Y, то есть всякое подмножество декартова произведения этих множеств: $R \subseteq X \times Y$. Смысл определения в том, что подмножество R декартова произведения $X \times Y$ состоит из набора тех пар (x, y), которые и находятся в задаваемом соотношении.

Бинарное отношение на X – это любое подмножество $R \subseteq X^2 = X \times X$.

Бинарные отношения наиболее часто используются в математике, в частности, таковы отношения равенства, неравенства, эквивалентности, отношения порядка. В этом случае подмножество R декартова квадрата содержит в себе те и только те пары элементов множества X, которые находятся в рассматриваемом отношении равенства, неравенства, эквивалентности, порядка и т.д.

6.6.2. Отношение порядка

Бинарное отношение R на множестве X называется отношением нестрогого частичного порядка если имеют место:

***Рефлексивность*: $\forall x : x \, R \, x$;**

***Антисимметричность*: $\forall x, y : x \, R \, y \wedge y \, R \, x \Rightarrow x = y$;**

***Транзитивность*: $\forall x, y, z : x \, R \, y \wedge y \, R \, z \Rightarrow x \, R \, z$.**

Множество X, на котором введено отношение частичного порядка, называется частично упорядоченным. Отношение нестрогого частичного порядка часто обозначают знаком $\leqslant$.

Отношение частичного порядка R называется линейным порядком, если выполнено условие:

$$\forall\ x, y \in X\ \ x\ R\ y \vee y\ R\ x.$$

Множество X, на котором введено отношение линейного порядка, называется линейно упорядоченным, или цепью.

Отношение R, удовлетворяющее только условиям рефлексивности и транзитивности, называется предпорядком, или квазипорядком.

Если условие рефлексивности заменить на условие антирефлексивности: $\forall\ x \in X\ \neg\ (\ x\ R\ x\ )$, то получим определение строгого, или антирефлексивного частичного порядка (обозначается обычно символом $\prec$).

Примеры.

1. На множестве вещественных чисел отношения «больше» и «меньше» являются отношениями строгого порядка, а «больше или равно» и «меньше или равно» — нестрогого.

2. На множестве S(M) всех подмножеств данного множества M отношение включения подмножеств ($A \subset B$) превращает S(M) в частично упорядоченное множество.

6.6.3. Минимальный/максимальный и наименьший/наибольший элементы

Из-за того, что в частично упорядоченном множестве могут быть пары несравнимых элементов, вводятся два различных определения: минимального элемента и наименьшего элемента.

Элемент $a \in M$ называется минимальным, если не существует элемента $b < a$. Другими словами, a – минимальный элемент, если для любого элемента $b \in M$ либо $b > a$, либо $b = a$, либо b и a несравнимы.

Элемент a называется наименьшим, если для любого элемента $b \in M$ имеет место неравенство $b \geqslant a$.

Очевидно, всякий наименьший элемент является также минимальным, но обратное в общем случае неверно: минимальный элемент a может и не быть наименьшим, если существуют элементы b, не сравнимые с a.

Очевидно, что если в множестве существует наименьший элемент, то он единственен. А вот минимальных элементов может быть несколько.

Аналогично вводятся понятия максимального и наибольшего элементов.

6.6.4. Верхние и нижние грани

Пусть A – подмножество частично упорядоченного множества $\langle M , \leqslant \rangle$. Элемент $u \in M$ называется верхней гранью A, если любой элемент $a \in A$ не превосходит u. Аналогично вводится понятие нижней грани множества A.

Любой элемент, больший, чем некоторая верхняя грань A, также будет верхней гранью A. А любой элемент, меньший, чем некоторая нижняя грань A, также будет нижней гранью A.

6.7. Отношение эквивалентности. Фактор-множество. Разбиение

Отношение эквивалентности на множестве X – это бинарное отношение, для которого выполнены следующие условия:

1. a ~ a для любого a (рефлексивность);
2. если a ~ b, то b ~ a (симметричность);
3. если a ~ b и b ~ c, то a ~ c (транзитивность).

Запись вида «a ~ b» читается как «a эквивалентно b».

Классом эквивалентности $[a] \subset X$ элемента $a \in X$ называется подмножество элементов, эквивалентных a; то есть,

$$[a] = \{ x \in X \mid x \sim a \}.$$

Из вышеприведённого определения немедленно следует, что если $b \in [a]$, то $[a] = [b]$.

Фактор-множество – это множество всех классов эквивалентности заданного множества X по заданному отношению ~, обозначается $X / \sim$.

Множество классов эквивалентности по отношению ~ является **разбиением множества X на непересекающиеся подмножества**.

Примеры

1. В евклидовой геометрии: отношение конгруэнтности фигур, отношение подобия фигур, отношение параллельности прямых.
2. В теории множеств Кантора: отношение равномощности множеств.