Алгебра
Лекции

Дима Трушин

2022

Содержание

1 Бинарные операции

В математике часто изучаются разные структуры. Обычно это множества снабженные дополнительной структурой. В алгебре обычно множества снабжаются разного рода операциями. Простейший тип операций – бинарные операции, то есть операции с двумя аргументами. Давайте обсудим какие бывают бинарные операции и после перейдем к определению самой простой алгебраической структуры – группы.

1.1 Определения

Определение 1. Пусть X – некоторое множество. Бинарная операция на X – это отображение $\circ\colon X \times X \to X$ по правилу $(x, y) \mapsto x \circ y$ для всех $x, y \in X$.

В этом случае $\circ$ – это имя операции. Проще говоря, операция – это правило, которое съедает два элемента из X и выплевывает один новый элемент, называемый $x \circ y$, из того же множества X. Новый элемент $x \circ y$ обычно называется произведением элементов x и y.[1]

Обратите внимание, что у бинарных операций есть функциональный стиль обозначения, когда имя операции пишется не между аргументами, а в виде имени функции перед аргументами. Давайте я повторю определение операции в функциональном стиле.

Определение 2. Пусть X – некоторое множество. Бинарная операция на X – это отображение $\mu\colon X \times X \to X$ по правилу $(x, y) \mapsto \mu(x, y)$ для всех $x, y \in X$.

Это не новое определение, это всего лишь переобозначение предыдущего. Я буду предпочитать операторное обозначение.

Примеры 3. Бинарные операции:

1. Сложение целых чисел. В операторной форме

$$+\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m + n$$

   В функциональной форме

$$\mathrm{add}\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto \mathrm{add}(m, n) = m + n$$

   Так как мы привыкли к сложению в форме $m + n$, мы хотим, чтобы общее определение было похоже на привычную нам запись. С другой стороны, многие языки программирования допускают оба вида нотаций. Но по сути $\mathrm{add}(m, n)$ и $m + n$ это одно и то же.

2. Умножение целых чисел. В операторной форме

$$\cdot\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m \cdot n$$

   В функциональном стиле

$$\mathrm{mult}\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto \mathrm{mult}(m, n) = m \cdot n$$

3. Максимум целых чисел. В операторной форме

$$\vee\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m \vee n$$

   В функциональной форме

$$\max\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto \max(m, n) = m \vee n$$

   На всякий случай поясню, что $\max(m, n) = m \vee n$, то лишь разные обозначения максимума.

[1] Операция может быть какой угодно, например, на множестве целых чисел можно рассматривать сложение, взятие максимума, или что-либо другое, но с абстрактной точки зрения результат операции все равно называется произведением элементов. Не забывайте, что математика – это искусство обозначать одинаковые вещи по разному и разные вещи одинаково.

4. Минимум целых чисел. В операторной форме

$$\wedge\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z},\quad (m,n)\mapsto m\wedge n$$

В функциональной форме

$$\min\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z},\quad (m,n)\mapsto \min(m,n)=m\wedge n$$

Как и выше $\min(m,n)=m\wedge n$ это разные обозначения минимума.

5. Просто случайная дурацкая бинарная операция на целых числах

$$\phi\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z},\quad (m,n)\mapsto m^2-n^2$$

Давайте резюмируем, что бинарная операция на X – это любое отображение вида $f\colon X\times X\to X$. И вы вольны задать его как вам вздумается по любому правилу. Но разные операции будут иметь разные свойства, какие-то операции будут лучше, чем другие. Давайте теперь обсудим какие же есть свойства у операций.

1.2 Свойства

Можно рассматривать множество различных свойств операций. Я хочу обсудить лишь те, которые нам понадобятся в дальнейшем для определения группы.

1.2.1 Ассоциативность

Определение 4. Операция $\circ\colon X\times X\to X$ называется ассоциативной, если для любых элементов $x,y,z\in X$ выполнено $(x\circ y)\circ z=x\circ(y\circ z)$.

Если у вас есть бинарная операция $\circ$ на множестве X, то вы можете посчитать произведение трех элементов x, y, z двумя разными способами:

- сначала посчитаем произведение $w=x\circ y$ и потом вычислим $w\circ z=(x\circ y)\circ z$.
- сначала посчитаем произведение $u=y\circ z$ и потом вычислим $x\circ u=x\circ(y\circ z)$.

Если операция взята произвольно, то может случится, что эти два способа дают разные результаты для каких-то значений x, y и z. Ассоциативность означает, что не важен порядок, в котором вы вычисляете операции. Кроме того, если $(x\circ y)\circ z=x\circ(y\circ z)$ для всех $x,y,z\in X$, то на самом деле не имеет значения, как вы расставляете скобки в произвольных произведениях. Например, все следующие выражения равны $(x\circ y)\circ(z\circ w)$, $x\circ(y\circ(z\circ w))$ and $((x\circ y)\circ z)\circ w$, а значит мы можем убрать все скобки и просто записать $x\circ y\circ z\circ w$. Поэтому для ассоциативных операций обычно не используют скобки, так как они не существенны.

Примеры 5. Ниже примеры ассоциативных и не ассоциативных операций.

1. Целочисленное сложение ассоциативно.

$$+\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z},\quad (m,n)\mapsto m+n$$

Если $m,n,k\in\mathbb{Z}$, то мы знаем, что $(m+n)+k=m+(n+k)$.

2. Вычитание целых чисел не ассоциативно.

$$-\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z},\quad (m,n)\mapsto m-n$$

Тогда равенство $(m-n)-k=m-(n-k)$ не выполняется для всех целых чисел. Действительно, если взять $m=n=0$ и $k=1$, то левая часть равенство будет -1, а правая – 1. Так что, $(0-0)-1\neq 0-(0-1)$.

1.2.2 Нейтральный элемент

Определение 6. Пусть $\circ\colon X \times X \to X$ – некоторая операция на X. Элемент $e \in X$ называется нейтральным если для каждого элемента $x \in X$ выполнены равенства $x \circ e = x$ и $e \circ x = x$.

По простому, нейтральный элемент $e \in X$ – это такой элемент, который ничего не меняет по умножению в смысле операции.

Примеры 7. Нейтральный элемент может существовать, а может и не существовать.

1. Целочисленное сложение имеет нейтральный элемент.

$$+\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m + n$$

   Ясно, что элемент $e = 0$ удовлетворяет всем требованиям на нейтральный элемент. Действительно, для всех $m \in \mathbb{Z}$ имеем $m + 0 = m$ и $0 + m = m$.

2. Целочисленное вычитание не имеет нейтрального элемента.

$$-\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m - n$$

   Давайте покажем, что нет элемента $e \in \mathbb{Z}$ такого, что $e - m = m$ для всех $m \in \mathbb{Z}$. Действительно, если такой e существует, то $e = 2m$ для каждого $m \in \mathbb{Z}$. Но это не возможно, поскольку для $m = 0$, $e = 0$ а для $m = 1$, $e = 2$, противоречие. С другой стороны, отметим, что $m - 0 = m$ для всех $m \in \mathbb{Z}$. То есть 0 является нейтральным только с одной стороны для вычитания.

Последний пример показывает, что вообще говоря не достаточно проверять только одно из условий $x \circ e = x$ или $e \circ x = x$. Это очень частая ошибка. Постарайтесь не забыть оба условия.

Правильный вопрос, которым теперь надо задаться: а сколько нейтральных элементов может быть? Правильный ответ – не более одного. Давайте покажем это.

Утверждение 8. *Пусть X – некоторое множество и $\circ\colon X \times X \to X$ – бинарная операция. Тогда существует не более одного нейтрального элемента.*

Доказательство. Если нейтральных элементов нет, то и доказывать нечего. Пусть теперь e и e' – два произвольных нейтральных элемента. Мы должны показать, что они равны. Рассмотрим произведение $e \circ e'$. Так как e является нейтральным элементом, $e \circ x = x$ для любого $x \in X$. В частности при $x = e'$ мы получим, что $e \circ e' = e'$. С другой стороны, так как e' является нейтральным элементом, то $x \circ e' = x$ для любого $x \in X$. И значит в частности при $x = e$ имеем $e \circ e' = e$. То есть $e = e \circ e' = e'$. □

1.2.3 Обратный элемент

Я хочу начать с замечания, что это свойство зависит от предыдущего. А именно, для того чтобы говорить об обратных элементах необходимо, чтобы для операции существовал нейтральный элемент. Если же нейтрального элемента нет, то нет и способа говорить об обратимых элементах.

Определение 9. Пусть $\circ\colon X \times X \to X$ – некоторая операция с нейтральным элементом $e \in X$. Элемент $y \in X$ называется обратным к элементу $x \in X$, если выполнено $x \circ y = e$ и $y \circ x = e$.

Я напомню, что нейтральный элемент единственный если существует. Потому элемент e корректно определен в равенствах выше.

Правильный вопрос, которым надо задаться: а сколько может быть обратных элементов для заданного элемента $x \in X$? Оказывается, что не больше одного, если операция ассоциативна.

Утверждение 10. *Пусть $\circ\colon X \times X \to X$ – некоторая ассоциативная бинарная операция с нейтральным элементом $e \in X$. Тогда, для любого $x \in X$ существует не более одного обратного элемента.*

Доказательство. Давайте зафиксируем элемент $x \in X$. Если для него нет обратного, то и доказывать нечего. Теперь предположим, что y_1 и y_2 – это два обратных элемента к x. Последнее означает, что выполнены равенства

$$\begin{cases} x \circ y_1 = e \\ y_1 \circ x = e \end{cases} \quad \text{и} \quad \begin{cases} x \circ y_2 = e \\ y_2 \circ x = e \end{cases}$$

Теперь рассмотрим произведение $y_1 \circ x \circ y_2$. Так как $\circ$ ассоциативна, то расстановка скобок не имеет значение, то есть $(y_1 \circ x) \circ y_2 = y_1 \circ (x \circ y_2)$. Если посчитать левую часть, то получим:

$$(y_1 \circ x) \circ y_2 = e \circ y_2 = y_2$$

А для правой части имеем:

$$y_1 \circ (x \circ y_2) = y_1 \circ e = y_1$$

Значит $y_2 = (y_1 \circ x) \circ y_2 = y_1 \circ (x \circ y_2) = y_1$ и все доказано. □

Так как в общем случае существует не более одного обратного для элемента x, то его принято обозначать через x^{-1}.

Примеры 11. 1. Предположим, что операция – сложение целых чисел.

$$+ \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m + n$$

Нейтральный элемент у нас 0. Если $n \in \mathbb{Z}$, то обратный к нему будет $-n$. Действительно, $n + (-n) = 0$ и $(-n) + n = 0$. Значит любой элемент имеет обратный для этой операции.

2. Предположим, что операция – это умножение целых чисел

$$\cdot \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m \cdot n$$

Нейтральный элемент – 1. Если $n = 1$, то его обратный будет тоже 1. Если $n = -1$, то его обратный будет -1. Если же $n \neq \pm 1$, то обратного не существует в $\mathbb{Z}$. Потому только два элемента обратимы для этой операции.

1.2.4 Коммутативность

Определение 12. Бинарная операция $\circ \colon X \times X \to X$ называется коммутативной если для любых $x, y \in X$ выполнено $x \circ y = y \circ x$.

То есть коммутативность означает, что нам не важен порядок операндов в операции.

Примеры 13. 1. Целочисленное сложение коммутативно.

$$+ \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m + n$$

Действительно, для любых $m, n \in \mathbb{Z}$, мы имеем $m + n = n + m$.

2. Целочисленное вычитание не коммутативно.

$$- \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m - n$$

Коммутативность означает равенство $m - n = n - m$ для всех целых m, n. Ясно, что это не выполнено уже в случае $m = 0$ и $n = 1$.

2 Группы

2.1 Определение

Теперь мы готовы к тому, чтобы дать определение одного из самых важных в алгебре объектов – группы. Прежде чем сделать это, я хочу пояснить, что мы встретим много абстрактных определений в будущем и все они будут сотканы по единому шаблону. Давайте я проясню этот шаблон в начале. В любом абстрактном определении есть две части. В первой части говорится какие данные нам даны. А во второй части говорится каким аксиомам эти данные должны удовлетворять.[2]

Определение 14. Определение группы

- **Данные:**

[2] Если проводить аналогию с программированием, то первая часть описывает интерфейс, а вторая часть – это контракт на интерфейс.

1. G – множество.
2. Операция $\circ\colon G \times G \to G$.

- **Аксиомы:**

1. Операция $\circ$ ассоциативна.
2. Операция $\circ$ обладает нейтральным элементом.
3. Каждый элемент $x \in G$ имеет обратный.

В этом случае мы будем говорить, что пара $(G, \circ)$ является группой. Чтобы упростить обозначения, мы будем обычно говорить, что просто G является группой, подразумевая, что на G задана некоторая фиксированная операция. Если в дополнение к аксиомам выше выполнена следующая аксиома

4. Операция $\circ$ коммутативна.

То группа G называется абелевой или просто коммутативной.

Если коротко, то группа – это множество с «хорошей» операцией. Здесь слово «хорошая» означает, что нам не важно как расставлять скобки, у нас есть нейтральный элемент и на любой элемент можно поделить. Если же в дополнение ко всему не важно в каком порядке стоят аргументы операции, то группа называется абелевой.

Примеры 15.
1. Целые числа по сложению $(\mathbb{Z}, +)$ образуют абелеву группу. Действительно, операция $+$ ассоциативна, нейтральный элемент – 0, для каждого числа n есть его обратный $-n$ и порядок аргументов в сложении не важен $n + m = m + n$. Мы обычно называем эту группу просто $\mathbb{Z}$ подразумевая, что операция обязательно сложение.

2. Целые числа по умножению $(\mathbb{Z}, \cdot)$ группу не образуют. Мы знаем, что операция ассоциативна и есть нейтральный элемент 1. И мы уже проверяли, что только ± 1 являются обратимыми элементами.

3. Не нулевые вещественные числа по умножению $(\mathbb{R}^*, \cdot)$ образуют абелеву группу. Действительно, умножение ассоциативно. Нейтральным элементом будет будет 1, для всякого элемента x обратным будет $1/x$, и порядок аргументов в умножении не важен $xy = yx$.

4. Пусть n – положительное целое, тогда множество $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ с операцией $a + b \pmod n$ является абелевой группой. Для простоты операция сложения по модулю n так же обозначается просто $+$.

5. Пусть n – положительное целое. Положим $\mathbb{Z}_n^* = \{m \in \mathbb{Z}_n \mid (m, n) = 1\}$ (множество всех чисел из $\mathbb{Z}_n$ взаимно простых с n), а операцию зададим как $a \cdot b \pmod n$. В этом случае мы так же получим абелеву группу. Для простоты операция в $\mathbb{Z}_n^*$ обозначается как операция умножения $\cdot$.

2.2 Мультипликативная и аддитивная нотации

В определении группы G мы обозначали операцию $\circ$. Если надо использовать произведение нескольких элементов, то нам приходится писать $x \circ y \circ z \circ w$. Это не очень удобно. Вместо этого есть два более привычных стиля. А именно, давайте будем обозначать операцию как умножение $\cdot$ или как сложение $+$. Тогда получаются две разные нотации: мультипликативная и аддитивная.

	Мультипликативная	Аддитивная
Операция	$\cdot\colon G \times G \to G$	$+\colon G \times G \to G$
На элементах	$(x, y) \mapsto xy$	$(x, y) \mapsto x + y$
Нейтральный элемент	1	0
Обратный элемент	x^{-1}	$-x$
Степень элемента	$x^n = \underbrace{x \cdot \ldots \cdot x}_{n}$	$nx = \underbrace{x + \ldots + x}_{n}$

Обычно мультипликативная нотация используется в случае неабелевых групп или когда свойство коммутативности вообще говоря не известно. А аддитивная нотация зарезервирована сугубо для абелевых групп. Я буду в основном использовать мультипликативную нотацию.

Я подчеркну, что указанные нотации – это всего лишь два разных способа обозначать операцию $\circ$, а не какие-то новые специальные операции. То есть мы выбираем обозначение для $\circ$ в виде $\cdot$ или $+$ в зависимости от наших предпочтений. Не надо путать эти обозначения с операциями сложения и умножения целых чисел. В случае произвольной группы G путаницы быть не должно, потому что там нет никаких заранее заданных операций сложения и умножения. Однако, если мы работаем с целыми числами (вещественными, рациональными, комплексными и т.д.), то операции $+$ и $\cdot$ обозначают обычные сложение и умножение.

2.3 Подгруппы

Определение 16. Пусть G – некоторая группа.[3] Определим подгруппу H в группе G следующим образом.

- **Данные:**
  1. Подмножество $H \subseteq G$.
- **Аксиомы:**
  1. Нейтральный элемент 1 группы G принадлежит H.
  2. Если $x, y \in H$, то $xy \in H$.
  3. Если $x \in H$, то $x^{-1} \in H$.

В этом случае, мы говорим, что H – подгруппа в группе G.

Стоит отметить, что если H – подгруппа в группе $(G, \cdot)$, то $\cdot$ можно ограничить на H и получится операция на H. В этом случае $(H, \cdot)$ удовлетворяет всем аксиомам группы. Таким образом подгруппа H сама является группой относительно той же самой операции (или точнее относительно ограничения операции), что была на группе G.

Примеры 17. Пусть $G = \mathbb{Z}$ по сложению.

1. Если $H \subseteq \mathbb{Z}$ – подмножество четных чисел $H = 2\mathbb{Z}$, то H является подгруппой.
2. Если $H \subseteq \mathbb{Z}$ – подмножество нечетных чисел $H = 1 + 2\mathbb{Z}$, то H не является подгруппой. В этом случае H не содержит нейтрального элемента 0 и не замкнуто относительно операции сложения.

2.4 Циклические группы

Пусть G – некоторая группа и $g \in G$ – ее элемент. Тогда мы можем определить целочисленные степени элемента g по следующим правилам.

Мультипликативная нотация	Аддитивная нотация
$g^n = \begin{cases} \underbrace{g \cdot \ldots \cdot g}_{n}, & n > 0 \\ 1, & n = 0 \\ \underbrace{g^{-1} \cdot \ldots \cdot g^{-1}}_{-n}, & n < 0 \end{cases}$	$ng = \begin{cases} \underbrace{g + \ldots + g}_{n}, & n > 0 \\ 0, & n = 0 \\ \underbrace{(-g) + \ldots + (-g)}_{-n}, & n < 0 \end{cases}$

Утверждение 18. *Пусть G – некоторая группа. Тогда*

1. *Для любых $x, y \in G$ выполнено $(xy)^{-1} = y^{-1}x^{-1}$.*
2. *Для любого $g \in G$ верно $(g^{-1})^n = (g^n)^{-1} = g^{-n}$.*
3. *Для любого $g \in G$ и любых $n, m \in \mathbb{Z}$ верно $g^n g^m = g^{n+m}$.*

Доказательство. 1) Нам надо показать, что $(xy)^{-1} = y^{-1}x^{-1}$. С психологической точки зрения удобно обозначить $y^{-1}x^{-1}$ через z. Если мы покажем, что $(xy)z = z(xy) = 1$, то это будет означать, что $z = (xy)^{-1}$ по определению. Теперь посчитаем

$$(xy)z = xyz = xyy^{-1}x^{-1} = xx^{-1} = 1$$

[3] Строго говоря $(G, \cdot)$, но я буду использовать более короткие обозначения.

Аналогично делается и второе равенство.

2) Сначала покажем первое равенство. Давайте применим предыдущее свойство несколько раз, получим

$$(g_1 \cdot \ldots \cdot g_n)^{-1} = g_n^{-1} \cdot \ldots \cdot g_1^{-1}, \quad \text{whenever } g_1, \ldots, g_n \in G$$

При подстановке $g_1 = \ldots = g_n = g$, получим нужное равенство для $n > 0$.

Если $n = 0$, то по определению $(g^{-1})^0 = 1$. С другой стороны, $(g^0)^{-1} = 1^{-1} = 1$ потому что обратный к 1 есть 1.

Если $n < 0$, то по определению

$$(g^{-1})^n = \underbrace{(g^{-1})^{-1} \cdot \ldots \cdot (g^{-1})^{-1}}_{-n}$$

С другой стороны

$$(g^n)^{-1} = \underbrace{(g^{-1} \cdot \ldots \cdot g^{-1})^{-1}}_{-n} = \underbrace{(g^{-1})^{-1} \cdot \ldots \cdot (g^{-1})^{-1}}_{-n}$$

где последнее равенство берется из предыдущего пунка утверждения.

Теперь надо проверить второе равенство. В случае $n > 0$ имеем по определению

$$(g^{-1})^n = \underbrace{(g^{-1} \cdot \ldots \cdot g^{-1})}_{n} \quad \text{и} \quad g^{-n} = \underbrace{(g^{-1} \cdot \ldots \cdot g^{-1})}_{n}$$

Значит левая часть равна правой. Если $n = 0$, то обе части равны 1. Теперь рассмотрим $n < 0$. Для удобства изменим степень с n на $-n$ и можно считать, что $n > 0$. Получаем

$$(g^{-1})^{-n} = \underbrace{((g^{-1})^{-1} \cdot \ldots \cdot (g^{-1})^{-1})}_{n} \quad \text{и} \quad g^{-(-n)} = \underbrace{(g \cdot \ldots \cdot g)}_{n}$$

То есть теперь достаточно показать, что $(g^{-1})^{-1} = g$. А это делается по определению. Элемент g удовлетворяет равенствам $gg^{-1} = 1$ и $g^{-1}g = 1$, то есть g является обратным к g^{-1}, что и требовалось.

3) Мы должны рассмотреть следующие 4 случая:

1. $n \geqslant 0$ and $m \geqslant 0$.
2. $n < 0$ and $m \geqslant 0$.
3. $n \geqslant 0$ and $m < 0$.
4. $n < 0$ and $m < 0$.

Пусть у нас первый случай:

$$g^n g^m = \underbrace{g \cdot \ldots \cdot g}_{n} \cdot \underbrace{g \cdot \ldots \cdot g}_{m} = \underbrace{g \cdot \ldots \cdot g}_{n+m} = g^{n+m}$$

Для удобства рассмотрим $g^{-n}g^m$ где $n > 0$ and $m \geqslant 0$ во втором случае. Тогда

$$g^{-n}g^m = \underbrace{g^{-1} \cdot \ldots \cdot g^{-1}}_{n} \cdot \underbrace{g \cdot \ldots \cdot g}_{m}$$

Мы сокращаем множители в середине выражения. Если $n > m$, получим

$$\underbrace{g^{-1} \cdot \ldots \cdot g^{-1}}_{n-m} = g^{-n+m}$$

Если $n < m$, имеем

$$\underbrace{g \cdot \ldots \cdot g}_{m-n} = g^{m-n}$$

Если $n = m$ получается $1 = g^{m-n}$.

Третий случай по сути является вторым с переставленными множителями. Значит остается разобрать четвертый случай. Опять же для удобства будем считать, что нам даны g^{-n} и g^{-m}, где $n > 0$ и $m > 0$. Тогда

$$g^{n-}g^{-m} = \underbrace{g^{-1} \cdot \ldots \cdot g^{-1}}_{n}\underbrace{g^{-1} \cdot \ldots \cdot g^{-1}}_{m} = \underbrace{g^{-1} \cdot \ldots \cdot g^{-1}}_{n+m} = g^{-n-m}$$

Что и требовалось показать. □

Определение 19. Пусть G – группа и $g \in G$ – некоторый элемент. Тогда обозначим множество всех целых степеней g следующим образом

$$\langle g \rangle = \{\ldots, g^{-2}, g^{-1}, 1, g, g^2, \ldots\} = \{g^k \mid k \in \mathbb{Z}\}$$

Данное подмножество удовлетворяет определению подгруппы в группе G.[4] Эта группа называется циклической подгруппой порожденной g. Элемент g называется порождающим подгруппы $\langle g \rangle$.

В аддитивной нотации циклическая подгруппа имеет вид

$$\langle g \rangle = \{\ldots, -2g, -g, 0, g, 2g, \ldots\} = \{kg \mid k \in \mathbb{Z}\}$$

По построению $\langle g \rangle$ – это самая маленькая подгруппа в G содержащая элемент g.

Определение 20. Пусть G – некоторая группа. Если найдется элемент $g \in G$ такой, что $\langle g \rangle = G$, то группа G называется циклической.

Примеры 21. 1. Группа $(\mathbb{Z}, +)$ является циклической. Ее образующие 1 и -1.

2. Группа $(\mathbb{Z}_n, +)$ является циклической.

3. Группа перестановок на n элементах S_n не является циклической при $n > 2$.

4. Группа $(\mathbb{R}, +)$ не является циклической.

Определение 22. Пусть G – некоторая группа и $g \in G$ – ее элемент. Порядок элемента g – это минимальное положительное целое число такое, что $g^n = 1$ и ∞ если такого числа нет. Порядок g обозначается $\operatorname{ord} g$.

Замечания

- Обратите внимание, что $g = 1$ тогда и только тогда, когда $\operatorname{ord} g = 1$.
- Если мы используем аддитивную нотацию, то есть будем обозначать операцию через $+$, то порядок $g \in G$ – это такое минимальное положительное целое n, что $ng = 0$.

Утверждение 23. *Пусть G – некоторая группа и $g \in G$ ее элемент. Тогда есть два возможных случая*

1. *Все элементы g^n и g^m различны при различных $n, m \in \mathbb{Z}$.*
2. *Существует положительное целое n такое, что степени $1, g, g^2, \ldots, g^{n-1}$ различны. Более того, степени повторяются по циклу, а именно в ряду*

$$\underbrace{\ldots, g^{-2}, g^{-1}}, \underbrace{1, g, g^2, \ldots, g^{n-1}}, \underbrace{g^n, g^{n+1}, \ldots, g^{2n-1}}, \underbrace{g^{2n}, \ldots}$$

элементы $g^{kn}, g^{1+kn}, \ldots, g^{n-1+nk}$ совпадают с элементами $1, g, \ldots, g^{n-1}$ для любого $k \in \mathbb{Z}$. В частности, в этом случае

$$\langle g \rangle = \{1, g, \ldots g^{n-1}\}$$

При этом $n = \operatorname{ord} g$.

Доказательство. Если $g^n \neq g^m$ для всех различных $m, n \in \mathbb{Z}$, то доказывать нечего, у нас первый случай.

Давайте предположим, что для каких-то $m \neq n \in \mathbb{Z}$ у нас выполнено равенство $g^n = g^m$. Можно считать, что $n > m$. Тогда умножим обе части равенства на g^{-m} и по правилам перемножения степеней получим $g^{n-m} = 1$. Значит для некоторого $n > 0$ имеем $g^n = 1$.

Рассмотрим минимальное положительное n такое, что $g^n = 1$. Я утверждаю, что все степени $1, g, \ldots, g^{n-1}$ различны. Действительно, если $g^k = g^s$ для некоторых $k, s \in [0, n-1]$ и $k > s$, тогда $g^{k-s} = 1$. А это значит, что $k - s$ не ноль и строго меньше, чем n. Последнее противоречит выбору n.

Теперь проверим, что любая степень g^N совпадает со степенью из списка $1, g, \ldots, g^{n-1}$. Для этого поделим N с остатком на n, получим $N = qn + r$, где $0 \leqslant r < n$. Тогда

$$g^N = g^{qn+r} = (g^n)^q g^r = g^r$$

Осталось лишь заметить, что выбранное нами n по определению является $\operatorname{ord} g$. □

[4] Действительно, нейтральный элемент содержится в ней. Это множество замкнуто по умножению в силу свойства (3) предыдущего утверждения и в силу свойства (2) предыдущего утверждения с каждым элементом лежит его обратный.

Замечания

- Отметим, что n может быть равным 1 в случае, когда g совпадает с нейтральным элементом.
- Из предыдущего утверждения следует, что $\operatorname{ord} g$ совпадает с количеством элементом в подгруппе $\langle g \rangle$.

Теперь я хочу описать все подгруппы в группе целых чисел по сложению.

Утверждение 24. *Всякая подгруппа H группы $\mathbb{Z}$, точнее $(\mathbb{Z}, +)$, имеет вид $k\mathbb{Z}$ для некоторого неотрицательного целого k.*

Доказательство. В начале давайте проверим, что $k\mathbb{Z}$ действительно является подгруппой для любого k. Мы должно проверить три свойства подгруппы. Во-первых, $k\mathbb{Z}$ должно быть замкнуто по сложению Но это ясно из определения. Во-вторых, нейтральный элемент, то есть ноль, должен быть в $k\mathbb{Z}$. Это так же ясно, так как $0 = k \cdot 0$. В-третьих, для любого $m = kh \in k\mathbb{Z}$, его обратный $-m = k(-h)$ так же в $\mathbb{Z}$, и мы проверили все три свойства.

Теперь покажем, что всякая подгруппа H имеет вид $k\mathbb{Z}$ с неотрицательным k. Если H содержит только нейтральный элемент 0, то $H = 0\mathbb{Z}$ и все доказано. Предположим H содержит ненулевой элемент. Возьмем произвольное ненулевое $n \in H$. Если $n < 0$, то $-n$ должно быть в H по определению подгруппы. А значит, мы можем считать, что H содержит некоторое положительное число. Пусть k – наименьшее положительное число в H. Давайте покажем, что $H = k\mathbb{Z}$.

В начале покажем, $H \supseteq k\mathbb{Z}$. Действительно, если $k \in H$, то по определению и вся подгруппа степеней k лежит в H. В аддитивной записи это значит, что

$$mk = \underbrace{k + \ldots + k}_{m} \in H \;\text{ и }\; (-n)k = \underbrace{(-k) + \ldots + (-k)}_{n} \in H \;\text{ для любых }\; m, n \in \mathbb{N}$$

Значит, $k\mathbb{Z} \subseteq H$.

Теперь покажем, что $H \subseteq k\mathbb{Z}$. Если $n \in H$ – произвольный элемент, давайте разделим его на k с остатком: $n = qk + r$, где $q \in \mathbb{Z}$ и $0 \leqslant r < k$. Мы уже знаем, что $qk \in k\mathbb{Z} \subseteq H$. Значит, $r = n - qk \in H$. Но r является неотрицательным целым числом из H меньшим k. Так как k является минимальным положительным целым в H, то остается только случай $r = 0$. А значит, $n = qk \in k\mathbb{Z}$ и все доказано. □

Утверждение 25. *Всякая подгруппа H группы $\mathbb{Z}_n$, точнее $(\mathbb{Z}_n, +)$, имеет вид $k\mathbb{Z}_n = \{kh \in \mathbb{Z}_n \mid h \in \mathbb{Z}_n\}$ для некоторого положительного целого $k \mid n$.*

Доказательство. В начале проверим, что все числа кратные k для $k \mid n$ образуют подгруппу в $\mathbb{Z}_n$. Во-первых, покажем, что $k\mathbb{Z}_n$ замкнуто относительно сложения по модулю n. Допустим $m_1 = kh_1$ и $m_2 = kh_2$ – элементы $k\mathbb{Z}_n$. Тогда их сумма по модулю n – это остаток r такой, что $m_1 + m_2 = r \pmod{n}$. В этом случае

$$r = m_1 + m_2 + qn = kh_1 + kh_2 + qn$$

Так как k делит n все выражение целиком делится на k. Значит и r делится на k. Последнее означает, что $k\mathbb{Z}_n$ замкнуто относительно сложения по модулю n. Во-вторых, надо проверить, что нейтральный элемент содержится в $k\mathbb{Z}_n$. Это ясно из равенства $0 = k \cdot 0 \in k\mathbb{Z}_n$. В-третьих, если $m \in k\mathbb{Z}_n$ – не нулевой элемент, то его обратный имеет вид $n - m$. А так как n делится на k, то и $n - m$ делится на k, а значит лежит в $k\mathbb{Z}_n$. В случае $m = 0$ его обратный есть 0, а он лежит в $k\mathbb{Z}_n$. Потому для любого $k \mod n$, $k\mathbb{Z}_n$ является подгруппой в $\mathbb{Z}_n$.

Теперь давайте покажем, что любая подгруппа H в $\mathbb{Z}_n$ совпадает с подгруппой вида $k\mathbb{Z}_n$ где $k \mid n$. Подгруппа H должна содержать нейтральный элемент 0. Если больше нет других элементов в H, то $H = \{0\} = n\mathbb{Z}_n$ и все доказано. Значит, мы можем предположить, что в H есть ненулевые элементы. Пусть k – наименьший положительный элемент в H. По определению циклическая подгруппа $k\mathbb{Z}_n$ лежит в H. Потому нам надо показать только обратное включение $H \subseteq k\mathbb{Z}_n$ и показать, что k делит n.

В начале покажем, что k делит n. Давайте разделим n с остатком на k, мы получим $n = qk + r$, где $0 \leqslant r < k$. Теперь, $r = n - qk$, а значит $r = -qk \pmod{n}$. Так как $k \in H$, последнее означает, что r тоже в H. Но это противоречит выбору k, оно было наименьшим положительным целым в H. Значит, r должен быть нулем, а это и означает, что k делит n. Теперь, давайте покажем, что каждый элемент H лежит в $k\mathbb{Z}_n$. Возьмем произвольный элемент $h \in H$. Разделим его на k с остатком и получим $h = qk + r$. Значит, $r = h - qk$. Так как $h \in H$ и $k \in H$, все выражение $h - qk$ лежит в H, то есть $r \in H$. Так как k был наименьшим положительным целым в H, получается, что $r = 0$. Последнее означает, что h делится на k, то есть лежит в $k\mathbb{Z}_n$. □

2.5 Смежные классы

Алгебра тяготеет к тому, чтобы изучать группы с помощью подгрупп, а не только элементов. Важным инструментом в таком подходе являются смежные классы.

Определение 26. Пусть G – некоторая группа, $H \subseteq G$ – ее подгруппа и $g \in G$ – произвольный элемент. Тогда множество

$$gH = \{gh \mid h \in H\}$$

называется левым смежным классом элемента g по подгруппе H. Аналогично определяются правые смежные классы. Множество

$$Hg = \{hg \mid h \in H\}$$

называется правым смежным классом элемента g по подгруппе H.

Замечания

1. Стоит заметить, что если G коммутативна, то нет разницы между левыми и правыми смежными классами для любой подгруппы $H \subseteq G$.
2. Сама подгруппа H является левым и правым смежным классом. Действительно, $H = 1 \cdot H = H \cdot 1$.
3. В произвольной группе, вообще говоря левый смежный класс gH не обязан равняться правому смежному классу Hg как показывает пример ниже.

Примеры 27. Некоторые примеры смежных классов.

1. Пусть $G = (\mathbb{Z}, +)$ и $H = 2\mathbb{Z}$ – подгруппа четных целых чисел. Тогда $2\mathbb{Z}$ и $1 + 2\mathbb{Z}$ – все возможные смежные классы H.
2. Пусть $G = S_3$ – группа перестановок на трех элементах и $H = \langle (1,2) \rangle$ – циклическая подгруппа порожденная элементом $(1,2)$. Мы можем перечислить все элементы G и H

   $$G = \{1, (1,2), (1,3), (2,3), (1,2,3), (3,2,1)\},\ H = \{1, (1,2)\}$$

   Теперь мы видим, что есть три разных левых смежных класса H

   $$H = \{1, (1,2)\},\ (1,3)H = \{(1,3), (1,2,3)\},\ (2,3)H = \{(2,3), (3,2,1)\}$$

   А так же, три разных правых смежных класса H

   $$H = \{1, (1,2)\},\ H(1,3) = \{(1,3), (3,2,1)\},\ H(2,3) = \{(2,3), (1,2,3)\}$$

   Этот пример показывает, что $(1,3)H \neq H(1,3)$. Так же этот пример показывает, что

   $$(1,2)H = H,\ (1,3)H = (1,2,3)H,\ (2,3)H = (3,2,1)H$$

   То есть одинаковые смежные классы могут порождаться разными элементами.
3. Пусть $G = S_n$ – группа перестановок на n элементах и $H = A_n$ – подгруппа четных перестановок. Тогда для всякой четной перестановки$\sigma \in A_n$, множество σA_n состоит из всех четных перестановок. Аналогично, для всякой нечетной перестановки $\sigma \in S_n \subseteq A_n$, множество σA_n состоит из всех нечетных перестановок. Потому, есть всего два левых смежных класса поA_n, это

   $$A_n \text{ и } (1,2)A_n$$

   Аналогично мы можем заметить, что есть всего два правых смежных класса по A_n, это

   $$A_n \text{ и } A_n(1,2)$$

   Более того, мы видим, что $\sigma A_n = A_n \sigma$ для всех $\sigma \in S_n$.

Определение 28. Пусть G группа и H ее подгруппа. Подгруппа H называется нормальной если $gH = Hg$ для любого элемента $g \in G$.

Утверждение 29. *Пусть G – некоторая группа и H – ее подгруппа. Следующие условия эквивалентны:*

1. *$gH = Hg$ для любого $g \in G$.*
2. *$gHg^{-1} = H$ для любого $g \in G$.*
3. *$gHg^{-1} \subseteq H$ для любого $g \in G$.*

Доказательство. (1)⇔(2). Предположим $gH = Hg$. Умножая это равенство справа на g^{-1}, мы получаем $gHg^{-1} = H$. А если нам задано равенство $gHg^{-1} = H$, умножая его справа на g, мы получим $gH = Hg$.

(2)⇔(3). Надо проверить, что если выполнено $gHg^{-1} \subseteq H$ для любого $g \in G$, то и $gHg^{-1} = H$ выполнено для любого $g \in G$. Если $gHg^{-1} \subseteq H$ для любого $g \in G$, то оно выполнено и для g^{-1} вместо g. Значит, $g^{-1}Hg \subseteq H$ для любого $g \in G$. Умножим это равенство слева на g, получим $Hg \subseteq gH$. Теперь умножим это равенство справа на g^{-1} и получим $H \subseteq gHg^{-1}$. А это завершает доказательство. □

2.6 Теорема Лагранжа

Свойства смежных классов Прежде всего я хочу доказать некоторые свойства смежных классов. Так окажется, что левые смежные классы образуют разбиение группы G на не пересекающиеся множества одного размера. Аналогичное верно и для правых смежных классов. Подобное утверждение позволяет применить к изучению группы комбинаторные соображения.

Утверждение 30. *Пусть G – некоторая группа, $H \subseteq G$ – ее подгруппа и $g_1, g_2 \in G$ – произвольные элементы. Тогда возможны только два случая:*

1. *Смежные классы не пересекаются: $g_1H \cap g_2H = \varnothing$.*
2. *Смежные классы совпадают: $g_1H = g_2H$.*

Последнее означает, что каждый элемент группы G лежит в единственном смежном классе.

Доказательство. Если g_1H не пересекает g_2H, то доказывать нечего.

Предположим, что пересечение смежных классов $g_1H \cap g_2H$ не пусто. Мы должны доказать, что $g_1H = g_2H$. Предположим, что $g \in g_1H \cap g_2H$. Тогда $g \in g_1H$, $g = g_1h_1$ для некоторого $h_1 \in H$. Аналогично, $g \in g_2H$ влечет $g = g_2h_2$ для некоторого $h_2 \in H$. Значит $g_1h_1 = g_2h_2$. Разделив на h_1 справа, мы получим $g_1 = g_2h_2h_1^{-1}$. Так как H является подгруппой, то $h = h_2h_1^{-1} \in H$. То есть $g_1 = g_2h$ для некоторого $h \in H$.

Давайте покажем, что $g_1H \subseteq g_2H$. Предположим, что произвольный элемент $g \in g_1H$ имеет вид $g = g_1h'$, где $h' \in H$. Тогда $g = g_2hh' \in g_2H$ потому что $hh' \in H$. Аналогично показывается обратное вложение $g_2H \subseteq g_1H$. А именно, возьмем $g \in g_2H$ в виде $g = g_2h'$ где $h' \in H$. Значит, $g = g_1h^{-1}h' \in g_1H$ потому что $h^{-1}h' \in H$. □

Замечание 31. Обратим внимание, что $g_1H = g_2H$ тогда и только тогда, когда $g_1H \cap g_2H \neq \varnothing$. Более того, это происходит тогда и только тогда, когда найдется элемент $h \in H$ такой, что $g_1 = g_2h$. Последнее эквивалентно условию $g_2^{-1}g_1 \in H$. Это дает нам удобный способ проверять являются ли смежные классы одинаковыми.

Утверждение 32. *Пусть G – некоторая группа, $H \subseteq G$ – конечная подгруппа и $g \in G$ – некоторый элемент. Тогда $|gH| = |H| = |Hg|$.*

Доказательство. Я докажу утверждение для левых смежных классов. Для правых делается аналогично. Рассмотрим отображение

$$\phi\colon H \to gH \quad x \mapsto gx$$

Оно переводит элементы H в элементы gH. С другой стороны, существует обратное отображение

$$\psi\colon gH \to H \quad x \mapsto g^{-1}x$$

Поэтому ϕ и ψ являются взаимно обратными биекциями. □

Утверждение 33. *Пусть G – конечная группа и $H \subseteq G$ – ее подгруппа. Тогда*

1. *Количество левых смежных классов группы H равно $|G|/|H|$.*
2. *Количество правых смежных классов группы H равно $|G|/|H|$.*

В частности, количество левых и правых смежных классов одно и то же.

Доказательство. Я докажу первое равенство для левых смежных классов. Утверждение 30 показывает, что G является дизъюнктным объединением своих смежных классов, то есть $G = g_1H \sqcup \ldots \sqcup g_kH$. С другой стороны, утверждение 32 говорит, что все смежные классы $g_1H, \ldots, g_kH$ имеют один и тот же размер $|H|$. Значит

$$|G| = |g_1H| + \ldots + |g_kH| = |H| + \ldots + |H| = k|H|$$

Здесь k – это число различных левых смежных классов. □

Определение 34. Пусть G – конечная группа и $H \subseteq G$ – некоторая ее подгруппа. Тогда количество левых смежных классов H называется индексом H и обозначается $(G : H)$. Это число так же совпадает с количеством правых смежных классов.

Используя это определение, мы можем переписать утверждение 33 следующим образом.

Утверждение 35 (Теорема Лагранжа)**.** *Пусть G – конечная группа и $H \subseteq G$ – некоторая ее подгруппа. Тогда, $|G| = (G : H)|H|$*

Следствия теоремы Лагранжа

1. Пусть G – конечная группа и $H \subseteq G$ – ее некоторая подгруппа. Тогда $|H|$ делит $|G|$.
2. Пусть G – конечная группа и $g \in G$ – произвольный элемент. Тогда $\mathrm{ord}(g)$ делит $|G|$. Действительно, $\mathrm{ord}(g) = |\langle g \rangle|$ по утверждению 23. Но $|\langle g \rangle|$ делит $|G|$ по предыдущему пункту.
3. Пусть G – конечная группа и $g \in G$ – некоторый элемент. Тогда $g^{|G|} = 1$. Действительно, мы уже знаем, что $|G| = \mathrm{ord}(g)k$. Значит,
$$g^{|G|} = g^{\mathrm{ord}(g)k} = \left(g^{\mathrm{ord}(g)}\right)^k = 1^k = 1$$
4. Пусть G – группа простого порядка. Тогда G циклическая. Действительно, так как порядок G прост, то он больше 1. Значит, существует элемент $g \in G$ такой, что $g \neq 1$. Тогда подгруппа $\langle g \rangle$ имеет порядок больше 1. Но $|\langle g \rangle|$ делит $|G| = p$. Так как p простое, единственно возможный случай – это $|\langle g \rangle| = p = |G|$. Последнее означает, что $\langle g \rangle = G$ и все доказано.
5. Малая теорема Ферма. Пусть $p \in \mathbb{Z}$ – простое число и $a \in \mathbb{Z}$. Если p не делит a, то p делит $a^{p-1} - 1$. Действительно, давайте рассмотрим группу $(\mathbb{Z}_p^*, \cdot)$. Для любого элемента $b \in \mathbb{Z}_p^*$, имеем $b^{|\mathbb{Z}_p^*|} = 1 \pmod p$ по пункту (3). Но $\mathbb{Z}_p^*$ состоит из $p - 1$ элемента. Теперь возьмем произвольное $a \in \mathbb{Z}$ взаимно простое с p. Пусть b – остаток от деления a на p. Тогда $a^{p-1} = b^{p-1} = 1 \pmod p$ и все доказано.

2.7 Гомоморфизмы и изоморфизмы

Существует много различных групп. Кроме того, мы с вами изучим методы по построению новых групп из уже имеющихся. В такой ситуации очень полезно иметь механизм для сравнения групп. Как понять, что мы построили уже знакомую нам группу? Чтобы ответить на этот вопрос, мы должны объяснить, что значит, что две группы одинаковые. То есть нам нужен способ сравнивать группы между собой. Тут на помощь нам приходят гомоморфизмы (способ сравнивать группы) и изоморфизмы (способ говорить, что две группы одинаковые). Давайте начнем с определений.

Определение 36. Пусть G и H – группы. Определим гомоморфизм $\varphi\colon G \to H$.

- **Данные** отображение $\varphi\colon G \to H$.
- **Аксиома** $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$ для всех $g_1, g_2 \in G$.

В таком случае φ называется гомоморфизмом из G в H.

Замечание 37. Давайте я явно проговорю определение. Нам даны две группы $(G, \circ)$ и $(H, \cdot)$. Гомоморфизм $\varphi\colon G \to H$ – это отображение такое, что $\varphi(g_1 \circ g_2) = \varphi(g_1) \cdot \varphi(g_2)$. В левой части равенства мы берем элементы g_1 и g_2 из группы G и перемножаем их с помощью операции из G и потом отправляем результат в H. В правой части, мы сначала отправляем элементы g_1 и g_2 в группу H и только потом перемножаем образы с помощью операции из H.

Примеры 38. 1. Пусть $G = (\mathbb{Z}, +)$ и $H = (\mathbb{Z}_n, +)$, тогда отображение $\pi\colon \mathbb{Z} \to \mathbb{Z}_n$ по правилу $k \mapsto k \pmod n$ является гомоморфизмом.

2. Пусть $G = S_n$ – группа перестановок и $H = \mu_2 = \{\pm 1\}$ снабжено умножением. Тогда отображение $\operatorname{sgn}\colon S_n \to \mu_2$ сопоставляющее каждой перестановке ее знак (четные идут в 1, а нечетные в -1) является гомоморфизмом.

3. Пусть $G = (\mathrm{GL}_n(\mathbb{R}), \cdot)$ и $H = (\mathbb{R}^*, \cdot)$ – множество ненулевых вещественных чисел с операцией умножения. Тогда отображение $\det\colon \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$ по правилу $A \mapsto \det(A)$ является гомоморфизмом.

4. Пусть $G = (\mathbb{R}, +)$ и $H = (\mathbb{R}^*, \cdot)$. Тогда отображение $\exp\colon \mathbb{R} \to \mathbb{R}^*$ по правилу $x \mapsto e^x$ является гомоморфизмом.

5. Пусть $G = (\mathbb{Z}, +)$, H – произвольная группа и $h \in H$ – произвольный элемент. Тогда отображение $\phi\colon \mathbb{Z} \to H$ по правилу $k \mapsto h^k$ является гомоморфизмом.

6. Пусть $G = (\mathbb{Z}_n, +)$, H – произвольная группа и $h \in H$ – произвольный элемент такой, что $h^n = 1$. Тогда отображение $\phi\colon \mathbb{Z}_n \to H$ по правилу $k \mapsto h^k$ является гомоморфизмом групп.

Давайте докажем некоторые свойства гомоморфизмов.

Утверждение 39. *Пусть $\varphi\colon G \to H$ – некоторый гомоморфизм групп. Тогда*

1. *$\varphi(1) = 1$, то есть нейтральный элемент G идет в нейтральный элемент H.*
2. *$\varphi(g^{-1}) = \varphi(g)^{-1}$ для любого $g \in G$.*

Доказательство. 1) Мы знаем, что $1 = 1 \cdot 1$. Давайте применим φ к этому равенству. Тогда мы получим

$$\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1) \in H$$

Теперь умножим это равенство на $\varphi(1)^{-1}$, будет $1 = \varphi(1)$.

2) Пусть $g \in G$ – некоторый элемент. Тогда $gg^{-1} = 1$. Теперь применим φ к этому равенству и получим

$$\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(1) = 1$$

Умножая полученное равенство слева на $\varphi(g)^{-1}$, мы получаем $\varphi(g^{-1}) = \varphi(g)^{-1}$. □

Определение 40. Пусть G и H – группы. Определим изоморфизм $\varphi\colon G \to H$.

- **Данные** гомоморфизм $\varphi\colon G \to H$.
- **Аксиома** φ является биекцией.

В этом случае φ называется изоморфизмом между G и H. Если найдется изоморфизм между G и H, то группы G и H называются изоморфными.

Давайте я поясню немного определение. В начале давайте разберемся, что значит, что у нас есть биекция множеств $\varphi\colon X \to Y$. Предположим $X = \{1, 2, 3\}$, $Y = \{a, b, c\}$ и φ устроено так: $1 \mapsto a$, $2 \mapsto b$ и $3 \mapsto c$. Тогда можно думать про эту биекцию следующим образом. Множество X – это множество имен элементов, а множество Y – это множество других имен тех же самых элементов. Тогда на биекцию можно смотреть, как на процедуру переименования. То есть можно считать, что Y это то же самое множество элементов, что и X, только с другими названиями элементов.

Теперь пусть у нас задан изоморфизм групп $\varphi\colon G \to H$. Такой гомоморфизм как минимум биекция, а значит мы можем считать, что подлежание множества G и H на самом деле одинаковые. Кроме того, условие $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$ означает, что при нашем отождествлении G и H операция на G превращается в операцию на H. То есть мы можем думать, что H – это то же самое множество, что и G с той же самой операцией, что на G. Или другими словами, мы считаем, что группа H – это та же самая группа, что и G, но только с другим множеством имен и другим обозначением операции. Однако, по существу это одна и та же группа. Как следствие, изоморфные группы имеют одинаковые свойства.

Примеры 41. 1. Пусть $G = (\mathbb{Z}_n, +)$ и $H = \mu_n \subseteq \mathbb{C}$ – множество комплексных корней из единицы степени n с операцией умножения. Давайте фиксируем примитивный корень $\xi \in \mu_n$. Тогда отображение $\mathbb{Z}_n \to \mu_n$ по правилу $k \mapsto \xi^k$ является изоморфизмом.

2. Пусть $G = (\mathbb{Z}, +)$ и
$$H = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \;\middle|\; n \in \mathbb{Z} \right\}$$
с операцией умножения. Тогда отображение $\varphi\colon \mathbb{Z} \to H$ по правилу $k \mapsto \left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right)$ является изоморфизмом.

3. Пусть $G = (\mathbb{C}, +)$ и $H = (\mathbb{R}^2, +)$. Тогда отображение $\varphi\colon \mathbb{C} \to \mathbb{R}^2$ по правилу $z \mapsto (\operatorname{Re} z, \operatorname{Im} z)$ является изоморфизмом.

4. Пусть $G = (\mathbb{C}^*, \cdot)$ и
$$H = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{R} \text{ такие что } a^2 + b^2 \neq 0 \right\}$$
с операцией умножения. Тогда отображение $\varphi\colon \mathbb{C}^* \to H$ по правилу $a + bi \mapsto \left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$ является изоморфизмом.

5. Claim 23 говорит, что циклическая группа $G = \langle g \rangle$ изоморфна $\mathbb{Z}$ или $\mathbb{Z}_n$ в зависимости от порядка образующего. Если $\operatorname{ord} g = \infty$, тогда $G \simeq \mathbb{Z}$. Если $\operatorname{ord} g = n$, тогда $G \simeq \mathbb{Z}_n$.

С каждым гомоморфизмом мы можем ассоциировать специальные подгруппы: ядро и образ.

Определение 42. Пусть $\varphi\colon G \to H$ – некоторый гомоморфизм групп. Тогда

1. ядро φ – это $\ker \varphi = \{g \in G \mid \varphi(g) = 1\} \subseteq G$.

2. образφ – это $\operatorname{Im} \varphi = \{\varphi(g) \mid g \in G\} = \varphi(G) \subseteq H$.

Стоит отметить, что ядро является подмножеством в G, а образ – в H.

Утверждение 43. *Пусть $\varphi\colon G \to H$ – гомоморфизм групп. Тогда*

1. *$\operatorname{Im} \varphi \subseteq H$ является подгруппой.*

2. *$\ker \varphi \subseteq G$ является нормальной подгруппой.*

3. *Отображение φ сюръективно тогда и только тогда, когда $\operatorname{Im} \varphi = H$.*

4. *Отображение φ инъективно тогда и только тогда, когда $\ker \varphi = \{1\}$.*

Доказательство. 1) Давайте проверим, что все свойства подгруппы выполняются. Во-первых, $1 = \varphi(1) \in \operatorname{Im} \varphi$, значит нейтральный элемент лежит в образе. Во-вторых, $\varphi(g_1)\varphi(g_2) = \varphi(g_1 g_2) \in \operatorname{Im} \varphi$, то есть образ замкнут относительно операции. В-третьих, $\varphi(g)^{-1} = \varphi(g^{-1}) \in \operatorname{Im} \varphi$, то есть с каждым элементом образ содержит его обратный.

2) В начале проверим, что ядро – подгруппа. Во-первых, $\varphi(1) = 1$, значит $1 \in \ker \varphi$ по определению. Во-вторых, если $x, y \in \ker \varphi$, тогда $\varphi(xy) = \varphi(x)\varphi(y) = 1 \cdot 1 = 1$, то есть $xy \in \ker \varphi$. В-третьих, если $x \in \ker \varphi$, то $\varphi(x^{-1}) = \varphi(x)^{-1} = 1^{-1} = 1$. Значит $x^{-1} \in \ker \varphi$. Мы только что проверили, что $\ker \varphi$ является подгруппой. Теперь надо показать, что $g \ker \varphi = \ker \varphi g$ для всех $g \in G$. По утверждению 29, достаточно проверить, что $g \ker \varphi g^{-1} \subseteq \ker \varphi$ для каждого $g \in G$. То есть мы должны показать, что $\varphi(g \ker \varphi g^{-1}) = 1$ для каждого $g \in G$. Действительно, пусть $h \in \ker \varphi$, тогда
$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(g) \cdot 1 \cdot \varphi(g^{-1}) = \varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(1) = 1$$

3) Это условие тривиально по определению.

4) Предположим, что φ инъективно и $x \in \ker \varphi$. Это значит, что $\varphi(x) = 1$. С другой стороны, мы всегда имеем $\varphi(1) = 1$. Значит, x и 1 идут в один и тот же элемент 1. По инъективности получаем $x = 1$.

Теперь предположим, что $\ker \varphi = \{1\}$. Рассмотрим два элемента $x, y \in G$ таких, что $\varphi(x) = \varphi(y)$. Умножим это равенство на $\varphi(x)^{-1}$ и получим
$$1 = \varphi(y)\varphi(x)^{-1} = \varphi(y)\varphi(x^{-1}) = \varphi(yx^{-1})$$
Значит $yx^{-1} \in \ker \varphi = \{1\}$. Поэтому $yx^{-1} = 1$. Тогда $y = x$, что завершает доказательство. □

2.8 Произведение групп

Вообще говоря нам не очень хочется каждый раз строить группы с нуля. Хочется иметь механизм по построению новых групп из уже заданных. Существует много подобных процедур в алгебре. Мы собираемся изучить одну из таких.

Определение 44. Пусть G и H – некоторые группы. Определим новую группу $G \times H$ следующим образом

1. Как множество это декартово произведение подлежащих множеств групп G и H: $G \times H = \{(g, h) \mid g \in G,\ h \in H\}$.
2. Операция
$$\cdot\colon (G \times H) \times (G \times H) \to G \times H$$
задана по правилу
$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2), \quad g_1, g_2, \in G,\ h_1, h_2 \in H$$

Группа $G \times H$ называется произведением групп G и H.

По-хорошему нам надо бы показать, что $G \times H$ действительно является группой. Мы только что определили все необходимые данные для группы, но осталось проверить аксиомы. Давайте я напомню их

- Операция ассоциативна
$$(g_1, h_1)\Big((g_2, h_2)(g_3, h_3)\Big) = \Big((g_1, h_1)(g_2, h_2)\Big)(g_3, h_3)$$
- Существует нейтральный элемент, $1 = (1, 1)$.
- У каждого элемента есть обратный, $(g, h)^{-1} = (g^{-1}, h^{-1})$.

Все свойства проверяются прямым вычислением. Если у нас есть несколько групп $G_1, \ldots, G_k$, мы можем определить произведение $G_1 \times \ldots \times G_k$ аналогично тому, как мы определили произведение двух групп.

2.9 Конечные абелевы группы

Теперь я хочу сосредоточиться на очень важном классе групп, класс конечных абелевых групп.

Определение 45. Конечная абелева группа – это коммутативная (абелева) группа G с конечным числом элементов.

Само по себе определение – не большой сюрприз, название говорит само за себя. Однако обратите внимание на следующий результат.

Утверждение 46. *Пусть G – конечная абелева группа, тогда G изоморфна группе вида $\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$.*

Я не буду доказывать этот результат. Доказательство не сложно, но требует некоторой технической работы, на которую у нас нет времени. Кроме того, само доказательство не проливает свет на какие-либо свойства конечных абелевых групп и потому не так интересно. На мой взгляд куда важнее научиться понимать как использовать этот результат. Давайте начнем с некоторых примеров.

Примеры 47. 1. Пусть $G = \mathbb{Z}_8^*$ с операцией умножения. Очевидно, что это конечная абелева группа, а значит она должна представляться в виде произведения циклических групп. Действительно, давайте проверим, что
$$\mathbb{Z}_8^* \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$$
Отображение задающее биекцию и уважающее операции можно задать так:
$$1 \leftrightarrow (0, 0),\ 3 \leftrightarrow (1, 0),\ 5 \leftrightarrow (0, 1),\ 7 \leftrightarrow (1, 1)$$
Это не единственный способ отождествить эти две группы. Например, вот другой изоморфизм:
$$1 \leftrightarrow (0, 0),\ 3 \leftrightarrow (1, 0),\ 7 \leftrightarrow (0, 1),\ 5 \leftrightarrow (1, 1)$$
Я не собираюсь описывать все изоморфизмы, самое главное, что мы видим, что таких изоморфизмов много. Так же обратите внимание, что группа не является циклической, так как в ней нет элемента порядка 4.

2. Пусть $G = \mathbb{Z}_9^*$ с операцией умножения. Это так же конечная абелева группа. В этом случае мы имеем:

$$\mathbb{Z}_9^* \simeq \mathbb{Z}_6$$

вот пример двух разных изоморфизомв

$$\begin{array}{ccc} \mathbb{Z}_6 \to \mathbb{Z}_9^* & & \mathbb{Z}_6 \to \mathbb{Z}_9^* \\ k \mapsto 2^k & \text{и} & k \mapsto 5^k \end{array}$$

Так же заметим, что в этом случае группа является циклической. Элементы 2 и 5 являются различными образующими группы. Изоморфизмы выше соответствуют одному из выбору образующего.

Утверждение 48 (Китайская теорема об остатках)**.** *Пусть $m, n \in \mathbb{N}$ – два взаимно простых натуральных числа, то есть $(m, n) = 1$. Тогда отображение*

$$\Phi\colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n, \quad k \mapsto (k \mod m,\ k \mod n)$$

является изоморфизмом групп.

Доказательство. В начале мы должны показать, что отображение является гомоморфизмом. Надо показать, что $\Phi(k+d) = \Phi(k) + \Phi(d)$, то есть

$$\Phi(k+d) = ((k+d) \mod m,\ (k+d) \mod n) = ((k \mod m) + (d \mod m),\ (k \mod n) + (d \mod n)) =$$
$$= (k \mod m,\ k \mod n) + (d \mod m,\ d \mod n) = \Phi(k) + \Phi(d)$$

Теперь я утверждаю, что гомоморфизм инъективен. Утверждение 43 пункт (4) гласит, что достаточно проверить, что ядро гомоморфизма содержит только нейтральный элемент. По определению, имеем

$$\ker \Phi = \{k \in \mathbb{Z}_{mn} \mid k = 0 \pmod m,\ k = 0 \mod n\}$$

Значит $k \in \ker \Phi$ тогда и только тогда, когда m делит k и n делит k. Так как m и n взаимно просты, последнее означает, что mn делит k. А значит, $k = 0$ в $\mathbb{Z}_{mn}$.

Чтобы показать, что Φ является изоморфизмом, нам надо показать сюръективность. Давайте посчитаем количество элементов в обеих группах. По определению $|\mathbb{Z}_{mn}| = mn$. С другой стороны, $|\mathbb{Z}_m \times \mathbb{Z}_n| = |\mathbb{Z}_m| \cdot |\mathbb{Z}_n| = mn$. Значит Φ – это инъективное отображение между множествами одинакового размера. А отсюда получаем, что оно обязательно сюръективно. □

В предыдущем утверждении явно сказано, как отображать элементы из $\mathbb{Z}_{mn}$ в элементы из $\mathbb{Z}_m \times \mathbb{Z}_n$. Однако, стоит сказать, как строится обратное отображение. Так как m и n взаимно просты, мы имеем $1 = um + vn$ для некоторых $u, v \in \mathbb{Z}$ по расширенному алгоритмы Евклида. Теперь рассмотрим элемент $a_1 = um = 1 - vn$. Ясно, что $a_1 \mapsto (0, 1)$ под действием отображения Φ. Аналогично, элемент $a_2 = vn = 1 - um$ идет в $(1, 0)$. Значит, элемент (a, b) соответствует элементу $aa_1 + ba_2 \pmod{mn}$ в группе $\mathbb{Z}_{mn}$.

Примеры 49.

1. В случае $m = 3$ и $n = 2$, мы имеем $\mathbb{Z}_6 \simeq \mathbb{Z}_3 \times \mathbb{Z}_2$. Здесь элемент 1 идет в $(1, 1)$. Значит $(1, 1)$ является образующим циклической группы $\mathbb{Z}_3 \times \mathbb{Z}_2$. Так как $1 = 3 - 2$, мы видим, что 3 идет в $(0, 1)$ и -2 идет в $(1, 0)$ (обратим внимание, что $-2 = 4$ в $\mathbb{Z}_6$). Потому, обратное отображение задано по правилу $(a, b) \mapsto -2a + 3b = 4a + 3b \pmod 6$.

2. Группа $\mathbb{Z}_2 \times \mathbb{Z}_2$ не является циклической. Значит, не существует изоморфизма между ней и группой $\mathbb{Z}_4$.

3. Еще один пример различного представления абелевой группы в виде произведения циклических

$$\mathbb{Z}_{30} \simeq \mathbb{Z}_6 \times \mathbb{Z}_5 \simeq \mathbb{Z}_3 \times \mathbb{Z}_{10} \simeq \mathbb{Z}_2 \times \mathbb{Z}_{15} \simeq \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

Так что, все пять конструкций дают одну и ту же циклическую группу.

4. В общем случае, если $m = p_1^{k_1} \dots p_r^{k_r}$, где p_i – простые, имеем

$$\mathbb{Z}_m = \mathbb{Z}_{p_1^{k_1}} \times \dots \times \mathbb{Z}_{p_r^{k_r}}$$

Как мы видели выше, одна и та же абелева группа может быть записана совершенно разными способами. Как же быстро понять, что два представления задают одну и ту же группу? Ответ содержится в следующем утверждении.

Утверждение 50. *Пусть G – конечная абелева группа. Тогда*

1. *G единственным образом представляется в следующем виде*

$$G = \mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_k}, \quad \text{где } 1 < d_1 | d_2 | \ldots | d_k \text{ натуральные}$$

2. *С точностью до перестановки множителей G единственным образом представляется в следующем виде*

$$G = \mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_r^{k_r}}, \quad \text{где } p_i \text{ – не обязательно различные простые числа, } k_i \text{ – натуральные}$$

Важно упомянуть, что простые p_i могут повторяться во втором представлении, например $\mathbb{Z}_2 \times \mathbb{Z}_4$ – один из возможных случаев.

Примеры 51. 1. Пусть $G = \mathbb{Z}_2 \times \mathbb{Z}_6$ и $H = \mathbb{Z}_{12}$. Обе эти группы представлены в первой форме. Так как такое представление единственно, то G и H не изоморфны.

2. Пусть $G = \mathbb{Z}_2 \times \mathbb{Z}_6$ и $H = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$. Мы видим, что G представлено в первой форме, а H представлено во второй. Давайте пересчитаем G во второй форме, используя Китайскую теорему об остатках:

$$G = \mathbb{Z}_2 \times \mathbb{Z}_6 = \mathbb{Z}_2 \times (\mathbb{Z}_2 \times \mathbb{Z}_3) = H$$

Значит группы изоморфны.

Теперь я хочу сформулировать вторую версию китайской теоремы об остатках.

Утверждение 52. *Пусть $m, n \in \mathbb{N}$ – два взаимно простых целых числа, то есть $(m, n) = 1$. Тогда отображение*

$$\Phi \colon \mathbb{Z}^*_{mn} \to \mathbb{Z}^*_m \times \mathbb{Z}^*_n, \quad k \mapsto (k \mod m, k \mod n)$$

является корректно определенным изоморфизмом групп.

Доказательство. Так как m и n взаимно простые, мы уже знаем, что отображение $\Phi \colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ является биекцией, по утверждению 48. Ясно, что число k взаимно просто с mn тогда и только тогда, когда оно взаимно просто с m и взаимно просто с n одновременно. Последнее означает, что Φ индуцирует биекцию $\Phi \colon \mathbb{Z}^*_{mn} \to \mathbb{Z}^*_m \times \mathbb{Z}^*_n$.

Теперь надо показать, что Φ уважает умножение. С одной стороны имеем

$$\Phi(k_1 k_2) = (k_1 k_2 \mod m, k_1 k_2 \mod n)$$

С другой стороны

$$\Phi(k_1)\Phi(k_2) = (k_1 \mod m, k_1 \mod n)(k_2 \mod m, k_2 \mod n) = (k_1 k_2 \mod m, k_1 k_2 \mod n)$$

А это доказывает, что $\Phi(k_1 k_2) = \Phi(k_1)\Phi(k_2)$, что и требовалось. □

Последний результат означает, что вычисление группы $\mathbb{Z}^*_n$ можно свести к вычислению групп $\mathbb{Z}^*_{p^k}$ где p простое. Действтительно, если $n = p_1^{k_1} \ldots p_r^{k_r}$, то

$$\mathbb{Z}^*_n \simeq \mathbb{Z}^*_{p_1^{k_1}} \times \ldots \times \mathbb{Z}^*_{p_r^{k_r}}$$

Чтобы закончить вычисление, нам надо знать ответ для степеней простых. Давайте сформулируем необходимые результаты без доказательства.

Утверждение 53. *Если p – нечетное простое и n – произвольное положительное целое, тогда*

$$\mathbb{Z}^*_{p^n} \simeq \mathbb{Z}_{p^{n-1}(p-1)}$$

является циклической группой. Кроме того, целое $a \in \mathbb{Z}_{p^n}$ является образующим $\mathbb{Z}^*_{p^n}$ тогда и только тогда, когда a является образующим в $\mathbb{Z}^*_p$ и $a^{p-1} \neq 1 \pmod{p^2}$. Значит, любой элемент $\mathbb{Z}^*_{p^n}$ однозначно представляется в виде a^k, где $0 \leqslant k < p^{n-1}(p-1)$.

В случае степени 2 ответ будет следующим

$$\mathbb{Z}_{2^n}^* \simeq \begin{cases} 0, & n \leqslant 1 \\ \mathbb{Z}_2, & n = 2 \\ \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}, & n \geqslant 3 \end{cases}$$

В случае $n = 2$ группа порождена элементом $3 = -1$. В случае $n \geqslant 3$, первый множитель $\mathbb{Z}_2$ порожден элементом $2^n - 1 = -1$, а второй множитель $\mathbb{Z}_{2^{n-2}}$ порожден элементом 5. Таким образом, любой элемент $\mathbb{Z}_{2^n}^*$ однозначно представляется в виде $\pm 5^k$, где $0 \leqslant k < 2^{n-2}$.

В частности группа $\mathbb{Z}_p^*$ циклическая порядка $p-1$ для любого простого числа p. Мы позже докажем более общий результат используя абстрактный алгебраический аппарат.

Утверждение 54. *Элемент $m \in \mathbb{Z}_n$ является образующим тогда и только тогда, когда m и n взаимно просты.*

Доказательство. ($\Rightarrow$). Предположим, что $(m, n) = d > 1$. Тогда все элементы $\langle m \rangle$ делятся на d. В частности, мы никогда не полчим 1. Значит m – не образующий, противоречие. То есть m и n обязаны быть взаимно простыми.

($\Leftarrow$). Мы хотим показать, что $\langle m \rangle = \mathbb{Z}_n$. Так как 1 – образующий $\mathbb{Z}_n$, достаточно показать, что $1 \in \langle m \rangle$. В силу взаимной простоты m и n существуют элементы $a, b \in \mathbb{Z}$ такие, что $1 = am + bn$. Значит $1 = am \pmod{n}$. Последнее означает, что 1 является a-ой степенью m, а значит, $1 \in \langle m \rangle$. □

3 Криптография

3.1 Общие слова

Давайте предположим, что у вас есть жена и любовница[5] и вы очень хотите послать сообщение любовнице. Однако, вы опасаетесь это делать в открытую, так как кто-то в вашей семье недавно купил дробовик и вы точно уверены, что это не вы. В такой неловкой ситуации приходится прибегать к помощи криптографии.

Основная идея стоящая за криптографическими методами состоит в следующем. Оказывается, что есть процедуры, которые в одну сторону вычисляются быстро, а в обратную очень медленно, то есть посчитать прямое отображение легко, а обратное сложно. На основе таких отображений можно строить более хитрые процедуры. Например, процедуры, которые легко выполняются, когда вы знаете некоторую дополнительную секретную информацию и сложно, если вы такой информацией не владеете.

Прежде чем переходить к деталям, давайте я дам пример самых популярных процедур, которые в одну сторону считаются легко, а в другую сложно.

- Очень легко считать произведение целых чисел, даже очень больших.[6] Однако, процедура разложения целого числа на множители очень сложная, в том смысле, что принципиально лучше чем прямой перебор множителей, мы ничего не знаем.
- Предположим, нам задана некоторая абелева группа G и ее элемент $g \in G$. Тогда очень легко считается g^n для любого n. А именно у нас есть алгоритм быстрого возведения в степень, который работает приблизительно за $O(\log n)$ операций. С другой стороны, если группа G подобрана правильно, то обратная операция будет медленной. То есть для $h \in \langle g \rangle$ найти такое $n \in \mathbb{Z}$, что $h = g^n$ будет сложной операцией.

Первая процедура активно используется в алгоритме шифрования RSA, а вторая в процедуре шифрования Диффи-Хеллмана.

3.2 Быстрое возведение в степень

В начале я хочу напомнить алгоритм быстрого возведения в степень. Пусть G – группа и $g \in G$ – некоторый элемент и $n \in \mathbb{N}$. Тогда в мультипликативной и аддитивной нотации имеем

$$g^n = \begin{cases} g(g^2)^k, & n = 2k+1 \\ (g^2)^k, & n = 2k \end{cases} \quad \text{or} \quad ng = \begin{cases} g + k(2g), & n = 2k+1 \\ k(2g), & n = 2k \end{cases}$$

[5] Или муж и любовник, если угодно.

[6] На сегодняшний день существует множество хитрых алгоритмов для перемножения очень больших чисел.

Обратите внимание, что левая часть от правой отличается лишь нотацией, то есть в обоих случаях мы умеем лишь применять операцию в группе к двум элементам, а надо быстро найти n кратное применение операции к одному элементу. Давайте для определенности сосредоточимся на мультипликативной нотации.

Дано: $g \in G$, $n \in \mathbb{N}$.

Вывод: $g^n \in G$.

Мы используем три временные переменные $r, d \in G$ и $k \in \mathbb{N}$. Будем поддерживать инвариант $rd^k = g^n$. Алгоритм останавливается, когда $k = 0$, при этом результат будет записан в r.

Алгоритм:

1. Инициализация $r = 1 \in G$, $d = g \in G$, $k = n \in \mathbb{N}$.
2. В цикле проверяем является ли k четным или нечетным. Останавливаем цикл, если $k = 0$.
   (a) Если k четное, то делаем присваивания $r = r$, $d = d^2$, $k = k/2$.
   (b) Если k нечетно, то делаем присваивания $r = r \cdot d$, $d = d^2$, $k = (k-1)/2$.

Замечания Давайте разберемся, как работает алгоритм. В процессе вычисления, мы имеем $rd^k = g^n$. В самом начале $r = 1$, $d = g$, $k = n$. Теперь посмотрим, что происходит на каждом шаге в обоих случаях:

- $k = 2m$. Тогда, $rd^{2m} = r(d^2)^m$. И мы обновляем данные $r = r$, $d = d^2$, и $k = m = k/2$.
- $k = 2m + 1$. Тогда, $rd^{2m+1} = (rd)(d^2)^m$. И мы обновляем данные $r = rd$, $d = d^2$, и $k = m = (k-1)/2$.

Таким образом наш инвариант поддерживается на протяжении всего алгоритма и при $k = 0$ в r будет содержаться ответ.

Я хочу обратить внимание на еще одну похожую процедуру. Пусть для определенности $n = 11$. Тогда в двоичной записи $11 = 1 + 2 + 2^3 = 1 + 2(1 + 2(0 + 2))$. Теперь можно вот как расписать возведение в степень

$$g^{11} = g^{1+2(1+2(0+2))} = g(g^{1+2(0+2)})^2 = g(g(g^{0+2})^2)^2 = g(g(g^2)^2)^2$$

Если $n = 2^k$, то вам потребуется в точности k операций. Например, если $n = 8 = 2^3$, то $g^8 = ((g^2)^2)^2$. Таким образом у нас $\log_2 n$ операций. В общем случае количество операций будет пропорционально $\log_2 n$. Но я не хочу считать его аккуратно.

3.3 Сложность проблемы дискретного логарифмирования

Пусть G – группа, $g \in G$ и $h \in \langle g \rangle$. Напомню, что поиск такого $n \in \mathbb{N}$, что $g^n = h$ называется проблемой дискретного логарифмирования. Важно понимать, что эта процедура может выполняться как быстро, так и медленно. Давайте приведем соответствующие примеры.

Примеры 55.
1. Пусть $G = \mathbb{Z}$ со сложением, $g = 1$ и $h = k$. Тогда ясно, что требуемое n равно k. Действительно, $ng = h$. В этом случае проблема дискретного логарифмирования тривиальна и не требует никаких вычислений.[7]
2. Пусть $G = \mathbb{Z}_m$ со сложением, $g = a \in \mathbb{Z}_m$, и $h = b \in \mathbb{Z}_n$. Тогда нам надо найти такое $n \in \mathbb{N}$, что $na = b \pmod m$. Эта проблема эффективно решается с помощью расширенного алгоритма Евклида.
3. Пусть p – простое число, $G = \mathbb{Z}_p^*$ с умножением и $g = a \in \mathbb{Z}_p^*$ – некоторый порождающий группы и $h = b \in \mathbb{Z}_p^*$. Тогда проблема заключается в поиске $n \in \mathbb{N}$ такого, что $a^n = b \pmod p$. Весь опыт человечества подсказывает нам, что эта проблема по видимому действительно сложная и быстро не решается.

[7] Даже изменение g на другой элемент группы, не делает проблему сложнее.

3.4 Диффи-Хеллман

В начале нам надо фиксировать некоторую группу G, ее элемент $g \in G$ и посчитать его порядок $n = \operatorname{ord} g$. Возможный выбор группы будет такой: $G = \mathbb{Z}_p^*$, где p простое, а g – провзвольный образующий. Порядок в этом случае будет равен $p-1$. Поиск образующего – неприятная задача, но ее достаточно проделать единожды.

Давайте я напомню контекст У нас есть три участника: вы, жена и любовница. Процесс обмены сообщениями состоит из следующих общих шагов.

1. Перевести текстовое сообщение (или его часть) в элемент группы $t \in G$.
2. Зашифровать элемент t и получить зашифрованный элемент $t' \in G$.
3. Элемент t' передается по сети и становится известен всем.
4. Расшифровать элемент t' и получить исходное сообщение в виде элемента t.
5. Перевести элемент t обратно в текстовое сообщение (или его часть).

Шаги (1) и (5) обычно делаются с помощью некой обще известной таблицы, которая известна всем участникам. То есть нет никакого секрета в том, как именно вы преобразуете сообщения из текста в элементы группы и обратно. Не волнуйтесь, ваша жена с этим справится. Все шифрование ведется только на уровне элементов групп.

Обмен ключами Прежде чем передавать зашифрованные сообщения, вы с любовницей должны подготовить специальный приватный ключ, с помощью которого и будет вестись шифровка и расшифровка. До создания такого ключа, коммуникация не возможна.

Давайте изобразим весь процесс на следующей диаграмме. Она показывает, что кому известно.

Участники	Вы	Жена	Любовница
Знания	G, g, n	G, g, n	G, g, n

Вы генерируете случайное число $a \in \mathbb{Z}_n^*$ и считаете открытый ключ $r = g^a \in G$. Ваша любовница генерирует случайное число $b \in \mathbb{Z}_n^*$ и считает свой открытый ключ $s = g^b \in G$.

Участники	Вы	Жена	Любовница
Знания	G, g, n $r{=}g^a$	G, g, n	G, g, n $s{=}g^b$

Вы и любовница передаете всем свои открытые ключи r и s. Поэтому эти элементы становятся известны всем в том числе и жене. Но никто не знает элементов a и b, так как для их поиска надо решить задачу дискретного логарифмирования в группе G, а мы выбрали ее и элемент $g \in G$ так, чтобы эта проблема была сложной.

Участники	Вы	Жена	Любовница
Знания	G, g, n $r{=}g^a$, s	G, g, n r, s	G, g, n $s{=}g^b$, r

Теперь можно построить приватный ключ. Делается это так. Вы возводите элемент s в степень a и получаете $s^a = (g^b)^a = g^{ab}$. Любовница возводит элемент r в степень b и получает $r^b = (g^a)^b = g^{ab}$. Теперь у вас у обоих есть секретный ключ $k = g^{ab}$.

Участники	Вы	Жена	Любовница
Знания	G, g, n $r{=}g^a$, s $k{=}s^a$	G, g, n r, s	G, g, n $s{=}g^b$, r $k{=}r^b$

В результате описанной выше процедуры у вас и любовницы есть общий приватный ключ $k \in G$ и никто, даже ваша жена, не способны его найти. Однако, чтобы эта процедура была надежная, надо аккуратно выбирать группу G и элемент $g \in G$.

Передача сообщений Теперь самое время слать сладкие сообщения друг другу. Как я уже описал, мы должны перевести текстовые сообщения в элементы группы G. Предположим, что мы используем русский алфавит с 33 буквами. Еще можно использовать точку, запятую, восклицательный знак и знак пробела. Итого в общей сложности 37 символов. Всего существует 37^m текстовых строк длины m. Если $37^m \leqslant n$, мы можем отобразить все такие последовательности в элементы группы G инъективно. Таким образом у нас есть механизм перевода сообщения в элементы группы G.

Теперь я собираюсь игнорировать стадию перевода. Наша цель – послать элемент группы G. Предположим, у нас есть элемент $h \in G$, который является сообщением, которое нужно послать любовнице.

Участники	Вы	Жена	Любовница
Знания	G, g, n $r{=}g^a$, s $k{=}s^a$ h	G, g, n r, s	G, g, n $s{=}g^b$, r $k{=}r^b$

В начале надо зашифровать сообщение h. Зашифровка представляет из себя умножение h на приватный ключ k. Полученное сообщение $m = hk$ мы пересылаем любовнице.

Участники	Вы	Жена	Любовница
Знания	G, g, n $r{=}g^a$, s $k{=}s^a$ h, $m = hk$	G, g, n r, s m	G, g, n $s{=}g^b$, r $k{=}r^b$ m

Любовнице, чтобы раскодировать сообщение надо поделить его на секретный ключ, то есть вычислить $h = mk^{-1}$. Если в группе операция взятия обратного отдельно не известна, то по следствию 3 из теоремы Лагранжа это выражение можно посчитать так: $h = mk^{-1} = mk^{n-1}$.

Участники	Вы	Жена	Любовница
Знания	G, g, n $r{=}g^a$, s $k{=}s^a$ h, $m = hk$	G, g, n r, s m	G, g, n $s{=}g^b$, r $k{=}r^b$ m, $h = mk^{n-1}$

И вуаля, никто не пострадал, сообщение благополучно доставлено.

Модификация передачи В описанной выше схеме передачи информации приватный ключ остается одним и тем же на протяжение всего сеанса связи. Это делает систему более уязвимой. Существует следующая модификация с односторонней передачей информации. Глобально она устроена так: вы создаете и публикуете свой открытый ключ. Этот этап рассматривается как приглашение передавать вам информацию. Далее любовница начинает транслировать вам сообщение с переменным ключом. Давайте опишем этот процесс более аккуратно.

Для приглашения транслировать вам сообщения, вы должны придумать секретное $a \in \mathbb{Z}_n^*$ и передать всем открытый ключ $r = g^a$.

Участники	Вы	Жена	Любовница
Знания	G, g, n $r{=}g^a$	G, g, n r	G, g, n r

Теперь предположим, что у любовницы есть последовательность сообщений $h_1, \ldots, h_k$. Тогда она выбирает для каждого сообщения h_i свое секретное $b_i \in \mathbb{Z}_n^*$. После создает открытый и приватный ключи по правилу $s_i = g^{b_i}$ и $k_i = r^{b_i}$. Каждое сообщение кодируется своим приватным ключом $m_i = h_i k_i$. После этого любовница транслирует в сеть пары $(m_1, s_1), \ldots, (m_k, s_k)$.

Участники	Вы	Жена	Любовница
Знания	G, g, n $r{=}g^a$ (m_i, s_i)	G, g, n r (m_i, s_i)	G, g, n r $h_1, \ldots, h_k \in G$ $b_1, \ldots, b_k \in \mathbb{Z}_n^*$ $s_i = g^{b_i}$, $k_i = r^{b_i}$ $m_i = h_i k_i$

Чтобы расшифровать сообщение надо построить приватный ключ $k_i = s_i^a$. Это можете сделать только вы, так как только вы знаете a. Далее надо найти $h_i = m_i k_i^{-1}$.

Участники	Вы	Жена	Любовница
Знания	G, g, n $r{=}g^a$ (m_i, s_i) $k_i = {s_i}^a$, $h_i = m_i {k_i}^{-1}$	G, g, n r (m_i, s_i)	G, g, n r $h_1, \ldots, h_k \in G$ $b_1, \ldots, b_k \in \mathbb{Z}_n^*$ $s_i = g^{b_i}$, $k_i = r^{b_i}$ $m_i = h_i k_i$

Если мы хотим передавать сообщения в обратную сторону, то надо повторить всю схему с начала но симметрично. То есть любовница публикует свой открытый ключ, а вы уже генерируете серию зашифрованных сообщений.

3.5 RSA

Давайте я кратко расскажу, как работает схема шифрования RSA. Это схема односторонней передачи. Давайте я опишу ее по шагам.

Установка связи Если вы хотите, чтобы любовница передала вам сообщение вы должны проделать подготовительную работу. В начале вы придумываете два простых числа p и q и вычисляете $n = pq$. Число n публикуется для всех. И в качестве сообщений рассматриваются элементы $\mathbb{Z}_n^*$.

Участники	Вы	Жена	Любовница
Знания	p, q, $n = pq$	n, $\mathbb{Z}_n^*$	n, $\mathbb{Z}_n^*$

Теперь мы хотим построить открытый ключ, который позволит слать нам сообщения. Делается это так. В начале вычисляем $\varphi(n) = (p-1)(q-1)$.[8] Теперь мы берем произвольное число $e \in \mathbb{Z}_{\varphi(n)}^*$. Открытым ключом считается пара (e, n).

Участники	Вы	Жена	Любовница
Знания	p, q, $n = pq$ e	n, $\mathbb{Z}_n^*$ (e, n)	$\mathbb{Z}_n^*$ (e, n)

Теперь мы должны построить приватный ключ, для расшифровки сообщений. Для этого мы находим число $d \in \mathbb{Z}_{\varphi(n)}^*$ такое, что $de = 1$ в $\mathbb{Z}_{\varphi(n)}^*$. Это делается по расширенному алгоритму Евклида применяя его для поиска наибольшего общего делителя e и $\varphi(n)$. Приватным ключом считается пара (d, n). Обратите внимание, что никто не может получить d, так как для его вычисления надо знать $\varphi(n)$. А для ее вычисления надо знать разложение n на множители, что сложно.

Участники	Вы	Жена	Любовница
Знания	p, q, $n = pq$ e $de = 1 \pmod{\varphi(n)}$	n, $\mathbb{Z}_n^*$ (e, n)	$\mathbb{Z}_n^*$ (e, n)

Передача сообщения Теперь предположим у любовницы есть для вас сообщение $h \in \mathbb{Z}_n^*$. Она должна вычислить зашифрованное сообщение по правилу $m = h^e \pmod{n}$. И сообщение m рассылается всем.

Участники	Вы	Жена	Любовница
Знания	p, q, $n = pq$ e $de = 1 \pmod{\varphi(n)}$ m	n, $\mathbb{Z}_n^*$ (e, n) m	$\mathbb{Z}_n^*$ (e, n) $h \in \mathbb{Z}_n^*$ $m = h^e \pmod{n}$

[8] Здесь $\varphi(n)$ – функция Эйлера, по определению $\varphi(n) = |\mathbb{Z}_n^*|$. С помощью результатов про структуру $\mathbb{Z}_n^*$ мы можем ее явно вычислить.

Чтобы расшифровать сообщение вы используете следующую функцию $h = m^d \pmod n$. Этот метод действительно работает, вот почему. Мы знаем, что $de = 1 \pmod{\varphi(n)}$. Это значит, что $de = 1 + \varphi(n)k = 1 + |\mathbb{Z}_n^*|k$. Теперь

$$m^d = m^{1+|\mathbb{Z}_n^*|k} = m\left(m^{|\mathbb{Z}_n^*|}\right)^k = m \text{ в группе } \mathbb{Z}_n^*$$

Последнее равенство выполнено по следствию 3 из теоремы Лагранжа.

Участники	Вы	Жена	Любовница
Знания	p, q, $n = pq$ e $de = 1 \pmod{\varphi(n)}$ m $h = m^d \pmod n$	n, $\mathbb{Z}_n^*$ (e, n) m	$\mathbb{Z}_n^*$ (e, n) $h \in \mathbb{Z}_n^*$ $m = h^e \pmod n$

4 Кольца и поля

4.1 Определения

До этого мы с вами изучали множество с одной операцией. Оказывается, что для многих приложений этого не достаточно и надо рассмотреть множество с двумя операциями. Это ведет нас к понятию кольца.

Определение 56. Я собираюсь определить кольцо $(R, +, \cdot)$ или более кратко R.

- **Данные:**
  1. Множество элементов R.
  2. Операция $+\colon R \times R \to R$ называемая сложением.
  3. Операция $\cdot\colon R \times R \to R$ называемая умножением.
- **Аксиомы:**
  1. $(R, +)$ является абелевой группой.
  2. Умножение дистрибутивно относительно сложения с обеих сторон:
  $$a(b + c) = ab + ac \quad \text{and} \quad (a + b)c = ac + bc \quad \text{для всех } a, b, c \in R$$
  3. Умножение ассоциативно: $(ab)c = a(bc)$ для всех $a, b, c \in R$.
  4. Умножение имеет нейтральный элемент обозначаемый 1.

В случае выполнения аксиом выше говорят, что $(R, +, \cdot)$ – ассоциативное кольцо с единицей. Мы же будем называть такие объекты просто кольцами, так как не будем рассматривать неассоциативные кольца или кольца в которых нет единицы. Как и раньше, мы будем опускать обозначения операций и говорить, что R является кольцом, подразумевая, что на R имеются нужные операции. Нейтральный элемент по сложению будет обозначаться 0 и называется нулем в кольце. Если $a \in R$ – произвольный элемент, то обратный по сложению обозначается $-a$. Для любых элементов $a, b \in R$, выражение $a + (-b)$ будет для краткости записываться так $a - b$.

Если в дополнение а аксиомам выше выполняется

5. Умножение коммутативно: $ab = ba$ для всех $a, b \in R$.

То кольцо называется коммутативным. А если мы добавим еще две аксиомы

6. Всякий ненулевой элемент обратим по умножению: для любого $a \in R \setminus \{0\}$, существует элемент $b \in R$ такой, что $ab = ba = 1$.[9]
7. $1 \neq 0$.

То кольцо называется полем. В этом случае обратный элемент к a обозначается a^{-1}.

[9] Стоит обратить внимание, что не достаточно проверять только одно из условий $ab = 1$ или $ba = 1$ в случае если кольцо не коммутативно.

Примеры 57. 1. Пусть $R = \{*\}$ – множество состоящее из одного элемента. Тогда существует только одна бинарная операция на таком множестве. Мы будем использовать эту операцию как сложение и как умножение на множестве R: $+\colon R \times R \to R$ задано по правилу $* + * = *$ и $\cdot\colon R \times R \to R$ задано по правилу $*\cdot* = *$. Тогда R – коммутативное кольцо. Его единственный элемент $*$ является одновременно и нулем (нейтральным по сложению) и единицей (нейтральным по умножению). Любой ненулевой элемент является обратимым, потому что в кольце нет ненулевых элементов, а значит аксиома (6) выполнена. Но при этом $1 = 0$ в кольце. Такое кольцо называется нулевым.

Давайте покажем, что если в кольце $1 = 0$, то все элементы равны нулю. То есть кольцо является нулевым. Действительно, пусть S – кольцо в котором $1 = 0$. Возьмем произвольный $x \in S$, тогда $x = x \cdot 1 = x \cdot 0$. Теперь надо показать, что $x \cdot 0 = 0$ в любом кольце. Это делается следующим образом. По определению нуля имеем $0 + 0 = 0$. Теперь умножим это равенство на x и получим $x \cdot (0 + 0) = x \cdot 0$. Раскроем левую часть по дистрибутивности $x \cdot 0 + x \cdot 0 = x \cdot 0$. А теперь прибавим обратный к $x \cdot 0$ к обеим частям и получим, что $x \cdot 0 = 0$.

Еще обратите внимание, что для нулевого кольца выполняются все аксиомы поля, кроме последней седьмой. По сути эта аксиома нужна для того, чтобы исключить из списка полей нулевое кольцо.

2. Целые числа с обычными сложением и умножением $(\mathbb{Z}, +, \cdot)$ являются коммутативным кольцом.

3. Кольцо матриц с матричными сложением и умножением $(\mathrm{M}_n(\mathbb{R}), +, \cdot)$ является кольцом.

4. Вещественные числа с обычными сложением и умножением $(\mathbb{R}, +, \cdot)$ являются полем.

5. Множество остатков по модулю натурального числа n с операциями сложения и умножения по модулю n $(\mathbb{Z}_n, +, \cdot)$ является коммутативным кольцом.

6. Если в предыдущем примере модуль p является простым, то кольцо $(\mathbb{Z}_p, +, \cdot)$ является полем. Давайте поясним это. Ясно, что $\mathbb{Z}_p$ коммутативное кольцо, в котором $1 \neq 0$. Потому надо лишь проверить аксиому (6). Для этого возьмем $a \in \mathbb{Z}_p \setminus \{0\}$, то есть $1 \leqslant a < p$. Так как число p простое, последнее означает, что a и p взаимно просты. А значит по расширенному алгоритму Евклида найдутся такие $u, v \in \mathbb{Z}$, что $ua + vp = 1$. Теперь рассмотрим последнее равенство по модулю p и получим $ua = 1 \pmod p$. Что и означает обратимость элемента a.

7. Пусть A – некоторое коммутативное кольцо и x – переменная. Тогда, $A[x] = \{a_0 + a_1 x + \ldots + a_n x^n \mid n \in \mathbb{N} \cup \{0\},\ a_i \in A\}$ – множество всех многочленов с коэффициентами из A. Множество $A[x]$ с обычными операциями сложения и умножения многочленов является коммутативным кольцом.

Замечание 58. Если нам дано кольцо R, то в нем выполняются некоторые естественные свойства, которые не включены в список аксиом, но которые полезно знать. Я хочу здесь привести небольшой список тех свойств, которые полезно иметь в виду:

1. Для любого элемента $x \in R$ выполнено $0x = x0 = 0$.
2. Для любых элементов $x, y \in R$ выполнено $x - (-y) = x + y$.
3. Для любого элемента $x \in R$ выполнено $(-1)x = -x$.
4. Для любых обратимых элементов $x, y \in R$ выполнено $(xy)^{-1} = y^{-1}x^{-1}$.

Определение 59. Пусть R – кольцо. Я собираюсь определить понятие подкольца $T \subseteq R$.

- **Данные:**
  1. Подмножество $T \subseteq R$.
- **Аксиомы:**
  1. $(T, +) \subseteq (R, +)$ является подгруппой.
  2. T замкнуто относительно умножения.
  3. T содержит 1.

Примеры 60. 1. Множество целых чисел $\mathbb{Z} \subseteq \mathbb{R}$ является подкольцом в поле вещественных чисел.

2. Верхнетреугольные матрицы являются подкольцом в кольце квадратных матриц.

3. Скалярные матрицы являются подкольцом кольца квадратных матриц.

4.2 Элементы кольца

Существуют разные подходы к изучению колец. Самый простой – поэлементный, то есть мы смотрим на то какого сорта элементы присутствуют в кольце. Давайте разберем, какие интересные классы элементов имеются.

Определение 61. Пусть R – некоторое кольцо и $x \in R$.

- Элемент x называется обратимым, если он обратим относительно операции умножения, то есть $y \in R$ такой, что $xy = yx = 1$. В этом случае y обозначается x^{-1}. Множество всех обратимых элементов в кольце R обозначается R^*.
- Элемент x называется левым делителем нуля, если найдется ненулевой элемент $y \in R$ такой, что $xy = 0$. Аналогично, x называется правым делителем нуля, если найдется ненулевой $y \in R$ такой, что $yx = 0$. Множество левых и правых делителей нуля обозначается $D_l(R)$ и $D_r(R)$ соответственно. Множество всех делителей нуля это $D(R) = D_l(R) \cup D_r(R)$.
- Элемент x называется нильпотентом, если $x^n = 0$ для некоторого $n \in \mathbb{N}$. Множество всех нильпотентов кольца R будем обозначать $\mathrm{nil}(R)$.
- Элемент x называется идемпотентом если $x^2 = x$. Множество всех идемпотентов кольца R обозначается $E(R)$.

Примеры 62. 1. Пусть $R = \mathbb{Z}$ – кольцо целых чисел. Тогда, $\mathbb{Z}^* = \{\pm 1\}$, $D(\mathbb{Z}) = 0$, $\mathrm{nil}(\mathbb{Z}) = 0$, $E(\mathbb{Z}) = \{1, 0\}$.

2. Пусть $R = \mathbb{R}$ – поле вещественных чисел. Тогда, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $D(\mathbb{R}) = 0$, $\mathrm{nil}(\mathbb{R}) = 0$, $E(\mathbb{R}) = \{1, 0\}$.

3. Пусть $R = \mathrm{M}_n(\mathbb{R})$ – кольцо квадратных матриц. Тогда, $\mathrm{M}_n(\mathbb{R})^* = \mathrm{GL}_n(\mathbb{R})$, $D(\mathrm{M}_n(\mathbb{R}))$ – множество вырожденных матриц, $\mathrm{nil}(\mathrm{M}_n(\mathbb{R})$ является множеством матриц с нулевыми комплексными собственными значениями, $E(\mathrm{M}_n(\mathbb{R}))$ – множество проекторов, оно описывается как множество матриц вида $C^{-1}DC$, где D диагональная с элементами 1 и 0 на диагонали.

4. Пусть $R = \mathbb{Z}_n$ и $n = p_1^{k_1} \dots p_r^{k_r}$, где p_i – различные простые числа и $k_i > 0$. Тогда, $\mathbb{Z}_n^* = \{k \in \mathbb{Z}_n \mid (k, n) = 1\}$, $D(\mathbb{Z}_n) = \{k \in \mathbb{Z}_n \mid (k, n) \neq 1\}$, $\mathrm{nil}(\mathbb{Z}_n) = \{k \in \mathbb{Z}_n \mid p_1 | k, \dots, p_r | k\}$. По Китайской теореме об остатках, существуют числа $e_i \in \mathbb{Z}_n$ такие, что $e_i = 1 \pmod{p_i^{k_i}}$ и $e_i = 0 \pmod{p_j^{k_j}}$ если $j \neq i$. Тогда, $E(\mathbb{Z}_n)$ состоит из всех сумм вид $\sum_t e_{i_t}$. Пустая сумма соответствует нулю, а сумма всех – единице.

4.3 Идеалы

Другой подход к изучению колец заключается в изучении специальных подмножеств кольца. К таким подмножествам относятся подкольца, которые мы уже определили, и идеалы. Давайте разберемся с понятием идеала.

Определение 63. Пусть $(R, +, \cdot)$ – кольцо. Я собираюсь определить идеал I в кольце R.

- **Данные:**
  1. Подмножество $I \subseteq R$.
- **Аксиомы:**
  1. $(I, +) \subseteq (R, +)$ – подгруппа.
  2. для любого $r \in R$ выполнено

$$rI = \{rx \mid x \in I\} \subseteq I \quad \text{и} \quad Ir = \{xr \mid x \in I\} \subseteq I$$

В этом случае говорят, что I – идеал в R. Подмножества 0 и R всегда являются идеалами и называются тривиальными идеалами кольца R.

Если выполняется первая аксиома и условие $rI = \{rx \mid x \in I\}$ для любого $r \in R$, то говорят, что I левый идеал. Аналогично, если выполняется первая аксиома и условие $Ir = \{xr \mid x \in I\}$, то говорят, что I – правый идеал. В коммутативных кольцах нет разницы между левыми и правыми идеалами.

Стоит отметить, что в некоммутативном кольце не достаточно проверять только одно включение из двух $rI \subseteq I$ и $Ir \subseteq I$.

Утверждение 64. *Пусть $R = \mathbb{Z}$, тогда все идеалы имеют вид $n\mathbb{Z}$ для некоторого неотрицательного $n \in \mathbb{Z}$.*

Доказательство. Пусть $I \subseteq \mathbb{Z}$ – некоторый идеал. Тогда $(I, +)$ как минимум является подгруппой в $(\mathbb{Z}, +)$. По утверждению 24, мы уже знаем, что $I = n\mathbb{Z}$ для некоторого неотрицательного $n \in \mathbb{Z}$. С другой стороны, возьмем произвольную подгруппу $I = n\mathbb{Z}$ и число $k \in \mathbb{Z}$. Тогда,

$$kI = \{kx \mid x \in n\mathbb{Z}\} = \{knm \mid m \in \mathbb{Z}\} = kn\mathbb{Z} \subseteq n\mathbb{Z}$$

То есть любая подгруппа по сложению является идеалом. □

Утверждение 65. *Пусть $R = \mathbb{Z}_n$, тогда любой идеал единственным образом представляется в виде $k\mathbb{Z}_n$ для некоторого $k|n$.*

Доказательство. Прежде всего давайте покажем, что множество $k\mathbb{Z}_n$ является идеалом. По утверждению 25, $k\mathbb{Z}_n$ – подгруппа по сложению в $\mathbb{Z}_n$. Потому мы только должны показать, что для любого $a \in \mathbb{Z}_n$ и любого $x \in k\mathbb{Z}_n$ их произведение $ax \pmod n$ тоже в $k\mathbb{Z}_n$. Положим $ax = r \pmod n$. Тогда $ax = qn + r$. Так как $k|x$ и $k|n$, то r делит k. Последнее означает, что r принадлежит $k\mathbb{Z}_n$ и все доказано.

В обратную сторону, пусть $I \subseteq \mathbb{Z}_n$ – некоторый идеал. Тогда как минимум он является подгруппой в $\mathbb{Z}_n$ по сложению. По утверждению 25, любая подгруппа по сложению в $\mathbb{Z}_n$ имеет вид $k\mathbb{Z}_n$ для некоторого $k|n$, и все доказано. □

4.4 Гомоморфизмы и кольца

Мы использовали понятие гомоморфизма групп чтобы «сравнивать» разные группы, а понятие изоморфизма позволяло нам сказать, что две группы одинаковые. Давайте распространим эти определения на случай колец.

Определение 66. Пусть $(R, +, \cdot)$ и $(S, +, \cdot)$ – кольца. Я собираюсь определить гомоморфизм колец $\phi\colon R \to S$.

- **Данные:**
  1. Отображение $\phi\colon R \to S$.
- **Аксиомы:**
  1. $\phi(a + b) = \phi(a) + \phi(b)$ для всех $a, b \in R$.
  2. $\phi(ab) = \phi(a)\phi(b)$ для всех $a, b \in R$.
  3. $\phi(1) = 1$.

В этом случае будем говорить, что ϕ – гомоморфизм из кольца R в кольцо S. Если дополнительно мы имеем

4. ϕ биективно

тогда ϕ называется изоморфизмом. В этом случае кольца R и S называются изоморфными.

Хочу сделать замечание, что это не самое общее определение гомоморфизма колец, но именно оно подходит для наших нужд больше всего.

Замечания 67.
1. Отметим, что если $\phi\colon R \to S$ – гомоморфизм колец, то как минимум $\phi\colon (R, +) \to (S, +)$ является гомоморфизмом абелевых групп. В частности, $\phi(0) = 0$ и $\phi(-a) = -\phi(a)$ по утверждению 39.
2. Если R и S – изоморфные кольца, то это по по сути означает, что кольца R и S одинаковые. Мы уже обсуждали как понимать изоморфизм в случае групп (см. обсуждение после определения 40). Кратко изоморфизм можно рассматривать как правило переименования элементов R в имена элементов S и при этом переименовании сложение и умножение на R превращается в сложение и умножение на S. Изоморфные кольца имеют одинаковые свойства.

Примеры 68.
1. Отображение $\mathbb{Z} \to \mathbb{Z}_n$ по правилу $k \mapsto k \pmod n$ является гомоморфизмом колец.
2. Отображение $\mathbb{R} \to \mathrm{M}_n(\mathbb{R})$ по правилу $\lambda \mapsto \lambda E$, где E – единичная матрица, является гомоморфизмом колец.

3. Отображение $\mathbb{R}[x] \to \mathbb{C}$ по правилу $f(x) \mapsto f(i)$, где $i^2 = -1$, является гомоморфизмом колец.

4. Отображение $\mathbb{C} \to \mathrm{M}_n(\mathbb{R})$ по правилу $a + bi \mapsto \left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$ является гомоморфизмом колец.

Утверждение 69 (Китайская теорема об остатках)**.** *Пусть n и m – взаимно простые натуральные числа, то есть $(n, m) = 1$. Тогда отображение*

$$\Phi\colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n, \quad k \mapsto (k \mod m, k \mod n)$$

является изоморфизмом колец.

Доказательство. По сути мы это уже с вами доказали, только не осознали этого. Мы уже знаем, что $\Phi\colon (\mathbb{Z}_{mn}, +) \to (\mathbb{Z}_m \times \mathbb{Z}_n, +)$ является изоморфизмом абелевых групп по утверждению 48. Кроме того, мы уже проверили, что Φ сохраняет умножение и единицу при доказательстве утверждения 52. А это ровно то, что надо было сделать для доказательства этого утверждения. □

Определение 70. Пусть $\phi\colon R \to S$ – гомоморфизм колец. Тогда

- Ядро ϕ – это $\ker\phi = \{r \in R \mid \phi(r) = 0\} \subseteq R$.
- Образ ϕ – это $\operatorname{Im}\phi = \{\phi(r) \mid r \in R\} = \phi(R) \subseteq S$.

Утверждение 71. *Пусть $\phi\colon R \to S$ – гомоморфизм колец. Тогда*

1. *$\operatorname{Im}\phi \subseteq S$ – подкольцо.*
2. *$\ker\phi \subseteq R$ – идеал.*
3. *Отображение ϕ сюръективно тогда и только тогда, когда $\operatorname{Im}\phi = S$.*
4. *Отображение ϕ инъективно тогда и только тогда, когда $\ker\phi = \{0\}$.*

Доказательство. 1) Мы уже знаем, что $\operatorname{Im}\phi$ является аддитивной подгруппой в $(S, +)$ по утверждению 43. По определению гомоморфизма $1 = \phi(1) \in \operatorname{Im}\phi$. Значит осталось лишь показать, что образ замкнут относительно умножения. Действительно, если $x, y \in \operatorname{Im}\phi$, тогда $x = \phi(a)$ и $y = \phi(b)$ для некоторых $a, b \in R$. Тогда,

$$xy = \phi(a)\phi(b) = \phi(ab) \in \operatorname{Im}\phi$$

2) Мы уже знаем, что $\ker\phi$ является подгруппой в $(R, +)$ по утверждению 43. Значит нам лишь надо показать, что она устойчива по умножению на любой элемент кольца R. Пусть $x \in \ker\phi$ и $r \in R$, мы должны показать, что $rx, xr \in \ker\phi$, то есть $\phi(rx) = 0$ и $\phi(xr) = 0$. Действительно, $\phi(rx) = \phi(r)\phi(x) = \phi(r)0 = 0$ и аналогично $\phi(xr) = 0$.

3) Этот пункт выполнен по определению.

4) Так как $\phi\colon (R, +) \to (S, +)$ – гомоморфизм групп, то результат следует из утверждения 43. □

5 Многочлены от одной переменной

5.1 Определение

Пусть F – поле. Многочлен f от переменной x – это картинка следующего вида

$$f = a_0 + a_1 x + \ldots + a_n x^n, \quad \text{где } a_i \in F$$

Здесь операции $+$ и $\cdot$ – это просто символы. Таким образом мы берем какие-то элементы a_i из поля F и составляем строку символов на листе бумаги как выше. Формально многочлен – это просто последовательность его коэффициентов $(a_0, \ldots, a_n)$. Мы так же можем считать, что у такого многочлена есть коэффициенты $a_{n+1}, a_{n+2}, \ldots$ и они все равны нулю. То есть можно считать, что у многочлена счетное число коэффициентов, но только конечное число из этих коэффициентов не равна нулю. Эта точка зрения очень удобна, особенно когда надо писать какие-то формулы в общем виде.

Пусть у нас заданы два многочлена

$$f = a_0 + a_1 x + \ldots + a_n x^n \text{ и } g = b_0 + b_1 x + \ldots + b_m x^m$$

мы скажем, что многочлены f и g равны, если $a_k = b_k$ для всех $k \in \mathbb{N}$.[10] Мы можем складывать и умножать многочлены используя следующие правила

$$f = \sum_{k=0}^{n} a_k x^k \quad \text{и} \quad g = \sum_{k=0}^{m} b_k x^k$$

$$f + g = \sum_{k \geqslant 0} (a_k + b_k) x^k \qquad fg = \sum_{k \geqslant 0} \Big(\sum_{u+v=k} a_u b_v \Big) x^k$$

Множество всех многочленов с коэффициентами в F от переменной x обозначается через $F[x]$. Прямая проверка показывает, что $F[x]$ с операциями сложения и умножения образуют коммутативное кольцо.

Замечание 72. Давайте сделаем одно важное замечание. Каждый многочлен $f \in F[x]$ определяет функцию $\hat{f} \colon F \to F$ по правилу $a \mapsto f(a)$. А именно, если $f = a_0 + a_1 x + \ldots + a_n x^n$, то $f(a) = a_0 + a_1 a + \ldots + a_n a^n$. Однако, в общем случае f не определяется однозначно полученной функцией $\hat{f}$. Действительно, предположим $F = \mathbb{Z}_2$. Тогда многочлены $f_n = x^n$ определяют одну и ту же функцию $\hat{f}_n \colon \mathbb{Z}_2 \to \mathbb{Z}_2$ отправляющую $0 \mapsto 0$ и $1 \mapsto 1$. Так что все полиномы f_n различны, но определяют одну и ту же функцию. Этот пример объясняет почему мы дали такое странное определение многочленам. Мы хотим, чтобы многочлен однозначно определялся именно своими коэффициентами, а для этого на них надо смотреть как на формальные картинки, а не как на функции. Такой формальный подход не мешает при этом по каждому многочлену построить функцию.

Если $f \in F[x]$ представлен в виде $f = a_0 + a_1 x + \ldots + a_n x^n$, где $a_n \neq 0$, то есть n – старший индекс с ненулевым коэффициентом в f. Тогда n называется степенью многочлена f и обозначается $\deg f$. Коэффициент a_n называется старшим коэффициентом многочлена. Степень нулевого многочлена надо определить отдельно, так как в нем нет ненулевых коэффициентов. Мы будем предполагать, что $\deg(0) = -\infty$. Многочлен $f \in F[x]$ принадлежит полю F тогда и только тогда, когда $\deg(f) \leqslant 0$, при этом f ненулевая константа тогда и только тогда, когда $\deg f = 0$.[11]

Утверждение 73. *Пусть F – поле. Тогда для любых $f, g \in F[x]$, имеем $\deg(fg) = \deg(f) + \deg(g)$.*[12]

Доказательство. Если хотя бы один из многочленов нулевой, обе части равенства содержат $-\infty$ и доказывать нечего. Поэтому можно считать, что f и g ненулевые. Пусть

$$f = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \quad \text{и} \quad g = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0$$

такие, что $a_n \neq 0$ и $b_m \neq 0$. Тогда

$$fg = a_n b_m x^{m+n} + h(x)$$

где $\deg h < m + n$. Так как F – поле, $a_n b_m \neq 0$. Значит $\deg fg = n + m = \deg f + \deg g$. □

Утверждение 74. *Пусть F – поле. Единственный делитель нуля в $F[x]$ – нулевой многочлен.*

Доказательство. Если $f, g \in F[x]$, $f \neq 0$, и $g \neq 0$, тогда $\deg(f) \geqslant 0$ и $\deg(g) \geqslant 0$. Значит $\deg(fg) = \deg(f) + \deg(g) \geqslant 0$. В частности $fg \neq 0$. □

Утверждение 75. *Пусть F – поле. Многочлен $f \in F[x]$ обратим тогда и только тогда, когда $f \in F^*$.*

Доказательство. Если f обратим, то $fg = 1$ для некоторого $g \in F[x]$. Тогда, $0 = \deg(1) = \deg(fg) = \deg(f) + \deg(g)$. Так как степени ненулевых многочленов неотрицательны, отсюда следует, что $\deg(f) = \deg(g) = 0$. Последнее означает, что f и g ненулевые константы. □

5.2 Алгоритм Евклида

Если F – некоторое поле, то в кольце $F[x]$ определено деление с остатком. Если $f, g \in F[x]$ и $g \neq 0$, то мы можем разделить f на g с остатком. Последнее означает, что существуют единственные $q, r \in F[x]$ такие, что $f = qg + r$ и $\deg(r) < \deg(g)$. Многочлен q называется частным, а r остатком.

Предположим $f, g \in F[x]$, будем говорить, что f делит g, если $g = fh$ для некоторого $h \in F[x]$. Стоит отметить, что любой многочлен делит 0. Так же, если $a \in F^*$, то f делит af и наоборот, так как F – поле.

[10] Здесь я использую замечание про степени многочленов, то есть предполагаю что $a_k = 0$ для $k > n$ и аналогично $b_k = 0$ для $k > m$.

[11] Здесь под константой понимаетя элемент поля F.

[12] Тут мы придерживаемся правила, что $-\infty + a = a + (-\infty) = -\infty$.

Определение 76. Пусть F – поле. Многочлен $f \in F[x]$ называется унитальным, если его старший коэффициент равен единице 1.

Определение 77. Пусть F – поле и $f, g \in F[x]$ – некоторые многочлены. Многочлен $d \in F[x]$ называется наибольшем общим делителем f и g, если

1. d делит и f и g.
2. если h делит одновременно f и g, то h делит d.
3. d унитальный если не равен нулю.

Утверждение 78. *Пусть F – поле и $I \subseteq F[x]$ – некоторый идеал. Тогда $I = fF[x] = \{fh \mid h \in F[x]\}$ для некоторого $f \in F[x]$.*

Доказательство. Если I состоит только из нулевого многочлена, то $I = 0F[x]$. Пусть теперь $f \in I$ – ненулевой многочлен минимальной степени в I. Возьмем произвольный $h \in I$ и разделим h с остатком на f, получим $h = qf + r$, где $\deg r < \deg f$. Тогда, $r = h - qf \in I$ и имеет меньшую степень, чем f. Так как f ненулевой многочлен минимальной степени в I, то r обязан быть нулевым. А это означает, что все многочлены из I делятся на f, что и требовалось. □

Небольшое замечание по поводу обозначений. Идеал $fF[x]$ обычно обозначается (f) для краткости.

Утверждение 79. *Пусть F – некоторое поле и $f, g \in F[x]$. Тогда*

1. *Существует наибольший общий делитель d многочленов f и g. Кроме того, существуют такие многочлены $u, v \in F[x]$, что $d = uf + vg$.*
2. *Наибольший общий делитель f и g единственный.*

Доказательство. (1) Рассмотрим следующее множество многочленов

$$I = \{af + bg \mid a, b \in F[x]\} \subseteq F[x]$$

Это подмножество является идеалом в $F[x]$. По утверждению 78, найдется унитальный многочлен $r \in I$ такой, что $I = rF[x]$. Так как $r \in I$, то $r = uf + vg$ для некоторых $u, v \in F[x]$. Из того, что $f, g \in I = rF[x]$ следует, что $f = sr$ и $g = tr$ для некоторых $s, t \in F[x]$.

Теперь давайте докажем, что r является наибольшим общим делителем. Равенства $f = sr$ и $g = tr$ означают, что r делит f и g, то есть r – общий делитель. Пусть теперь h делит f и g, тогда h делит оба слагаемых в правой части следующего равенства $r = uf + vg$. Значит h делит r. Мы проверили, что все свойства наибольшего общего делителя выполнены для r.

(2) Предположим, что у нас есть два наибольших общи делителя d_1 и d_2. Тогда d_1 делит d_2 потому что d_2 – наибольший общий делитель. И наоборот, d_2 делит d_1, потому что d_1 – наибольший общий делитель. Значит

$$d_1 = ad_2 \quad d_2 = bd_1$$

В частности, $d_1 = abd_1$. Значит, $d_1(1 - ab) = 0$ в кольце $F[x]$. Но в кольце $F[x]$ нет ненулевых делителей нуля по утверждению 74. Значит $1 - ab = 0$ и потому $1 = ab$. Следовательно a и b – обратимые элементы поля F. □

Замечания 80.

- я хочу явно проговорить некоторые крайние случаи в определении наибольшего общего делителя. Например, если $f = g = 0$, то наибольший общий делитель будет 0. Действительно, в этом случае любой многочлен делит f и g. А 0 – это делитель f и g делимый всеми многочленами.
- Если $f \neq 0$ и $g = 0$, тогда наибольший общий делитель – это f с нормализованным старшим коэффициентом, потому что в этом случае f делит g.

Утверждение 81. *Пусть F – поле и $f, g, h \in F[x]$ – некоторые многочлены. Тогда $(f, g) = (f, g - hf)$.*

Доказательство. Действительно, множество делителей у пары $\{f, g\}$ такое же, как и у пары $\{f, g - hf\}$. В частности максимальные элементы (относительно порядка делимости) тоже совпадают, то есть совпадают наибольшие общие делители. □

Последнее утверждение позволяет нам считать наибольший общий делитель эффективно с помощью алгоритма Евклида.

Дано: Два многочлена $f, g \in F[x]$. Здесь F – поле.

Результат: Наибольший общий делитель $d \in F[x]$ многочленов f и g.

Алгоритм Используются две временные переменные $u, v \in F[x]$.

1. Инициализируем $u = f$, $v = g$ в случае $\deg f \geqslant \deg g$ и $u = g$, $v = f$ в противном случае.
2. Пока $v \neq 0$ выполняем следующее:
   (a) Делим u на v с остатком $u = qv + r$.
   (b) делаем замену $u = v$, $v = r$.
3. Когда $v = 0$, u становится наибольшим общим делителем f и g.

5.3 Однозначное разложение на множители

Определение 82.
- Многочлен $f \in F[x] \setminus F$ называется приводимым если существуют многочлены $g, h \in F[x]$ такие, что $f = gh$, $0 < \deg(g) < \deg(f)$ и $0 < \deg(h) < \deg(f)$.
- Многочлен $f \in F[x] \setminus F$ называется неприводимым, если для любых $g, h \in F[x]$ таких, что $f = gh$, либо g либо h является ненулевой константой.

Надо отметить, что все ненулевые многочлены бьются на три класса: 1) обратимые многочлены, то есть F^*, 2) приводимые многочлены, 3) неприводимые многочлены.

Утверждение 83 (UFD)**.** *Пусть F – поле. Тогда каждый элемент $f \in F[x] \setminus F$ представляется в форме $f = ap_1^{k_1} \dots p_n^{k_n}$, где $a \in F$ – ненулевая константа, k_i – положительные целые числа, и p_i – различные унитальные неприводимые многочлены. При этом такое представление единственное с точностью до перестановки множителей.*

Я не очень хочу доказывать это утверждение, доказательство для многочленов полностью повторяет доказательство для целых чисел. Ключевым техническим утверждением является утверждение 79, а именно нам важно, что наибольший общий делитель можно представить в виде линейной комбинации исходных многочленов. Тем не менее, я хочу доказать следующий частный случай общего результата.

Утверждение 84. *Пусть F – поле, $f, g \in F[x]$ – два взаимно простых многочлена и $h \in F[x]$ делится на f и на g. Тогда, h делится на fg.*

Доказательство. Так как f и g взаимно просты, то $1 = uf + vg$ для некоторых $u, v \in F[x]$ по утверждению 79 пункт (1). Умножая это равенство на h получим $h = uhf + vhg$. Так как g делит h, gf делит uhf. Так как f делит h, fg делит vhg. Значит, fg делит h. □

5.4 Кольцо остатков

Теперь мы готовы познакомиться с очень важной конструкцией в алгебре – кольцо полиномиальных остатков.

Пусть F – поле и $f \in F[x]$ – некоторый многочлен. Я собираюсь определить кольцо $F[x]/(f)$. Чтобы определить кольцо, я должен определить множество и две операции на нем – сложение и умножение. А после этого надо проверить все необходимые аксиомы кольца. Начнем с тривиального случая. Пусть $f = 0$, тогда по определению $F[x]/(f)$ – это кольцо многочленов $F[x]$ с обычными операциями. Теперь интересный случай, когда $f \neq 0$:

- $F[x]/(f) = \{g \in F[x] \mid \det g < \deg f\}$ – множество остатков от деления на многочлен f.
- $+\colon F[x]/(f) \times F[x]/(f) \to F[x]/(f)$ – обычное сложение многочленов.
- $\cdot\colon F[x]/(f) \times F[x]/(f) \to F[x]/(f)$ – умножение по модулю многочлена f, а именно: для любых $g, h \in F[x]/(f)$, мы определяем умножение, как $gh \pmod f$. Последнее означает, что мы должны в начале посчитать обычное произведение многочленов gh, а потом найти остаток от деления на f, то есть $gh = qf + r$. В этом случае произведением g и h является r.

Утверждение 85. *Если F – поле и $f \in F[x]$ – некоторый многочлен, тогда множество $F[x]/(f)$ с введенными на нем операциями является коммутативным кольцом.*

Доказательство. Если $f = 0$, это ясно, так как $F[x]/(f) = F[x]$ по определению. Предположим, что $f \neq 0$. Множество $F[x]/(f) = \{g \in F[x] \mid \deg g < \deg f\}$ с операцией сложения является абелевой группой, так как это подгруппа в $(F[x], +)$.

Теперь мы мы должны показать: 1) дистрибутивный закон, 2) ассоциативность умножения, 3) существование нейтрального элемента по умножению, 4) коммутативность умножения.

1) Если $g, h, p \in F[x]/(f)$, нам надо показать, что

$$(g+h)p \mod f = gp \mod f + hp \mod f \quad \text{and} \quad g(h+p) \mod f = gh \mod f + gp \mod f$$

Мы покажем первое равенство. Второе будет следовать из коммутативности. Давайте разделим gp и hp на f с остатком и получим

$$gp = q_1 f + r_1,\ \deg r_1 < \deg f, \text{ и } hp = q_2 f + r_2,\ \deg r_2 < \deg f$$

Теперь, правая часть по определению совпадает с $r_1 + r_2$. С другой стороны, выражение

$$(g+h)p = (q_1 + q_2)f + r_1 + r_2$$

является делением $(g+h)p$ на f с остатком равным $r_1 + r_2$. Следовательно, левая часть равна тому же самому.

2) Если $g, h, p \in F[x]/(f)$, тогда

$$(g \cdot (h \cdot p \mod f)) \mod f = (g \cdot h \cdot p) \mod f = ((g \cdot h \mod f) \cdot p) \mod f$$

Я позволю себе оставить эту проверку читателю, как упражнение в абстрактной чепухе.

3) Многочлен 1 является нейтральным элементом по умножению.

4) Коммутативность произведения по модулю f следует из его определения. □

Замечания 86.

- Обратите внимание, хотя мы можем рассматривать $F[x]/(f)$ как подмножество в $F[x]$ (даже как абелеву подгруппу по сложению), однако, так делать не следует. Основная причина в том, что это вложение не согласовано с умножением (когда $f \neq 0$). Последнее означает, что $F[x]/(f)$ НЕ является подкольцом в $F[x]$.
- Отображение $F[x] \to F[x]/(f)$ по правилу $g \mapsto g \bmod f$ является сюръективным гомоморфизмом.

Утверждение 87. *Пусть F – поле, $f \in F[x]$ – многочлен и $I \subseteq F[x]/(f)$ – некоторый идеал. Тогда существует многочлен $g \in F[x]$ делящий f такой, что $I = (g) = \{gh \bmod f \mid h \in F[x]\}$.*

Доказательство. Случай $f = 0$ разобран в утверждении 78. Теперь мы предположим, что $f \neq 0$. Если I состоит только из нулей, то $I = (f)$ и все доказано.

Пусть $h \in I$ – ненулевой многочлен минимально возможной степени в I. Тогда для любого $g \in I$, разделим g на h с остатком и получим $g = qh + r$ где $\deg r < \deg h$. Также $r = g - qh \in I$. Так как h был ненулевым многочленом минимально возможной степени в I, такое может быть только если $r = 0$. Значит h делит любой $g \in I$. последнее означает, что $I = (h)$.

Теперь мы должны показать, что h делит f. Давайте разделим f на h с остатком, получим $f = qh + r$, где $\deg r < \deg h$. Это означает, что $r = -qh$ в кольце $F[x]/(f)$. В частности $r \in I$ и имеет степень меньше, чем h. Такое возможно только если $r = 0$, что завершает доказательство. □

А вот еще одна версия Китайской теоремы об остатках, только теперь для кольца полиномиальных остатков.

Утверждение 88 (Китайская теорема об остатках)**.** *Пусть $f, g \in F[x]$ – два взаимно простых многочлена, то есть $(f, g) = 1$. Тогда отображение*

$$\Phi\colon F[x]/(fg) \to F[x]/(f) \times F[x]/(g) \quad h \mapsto (h \mod f, h \mod g)$$

является изоморфизмом колец.

Доказательство. В начале проверим, что отображение является гомоморфизмом колец. Мы должны показать, что оно сохраняет сложение, умножение и единицу кольца. Это делается прямым вычислением и я позволю себе пропустить это вычисление.

Теперь покажем, что отображение инъективно. По утверждению 71 достаточно проверить, что ядро Φ состоит только из нуля. Предположим $h \in \ker \Phi$. Это значит, что $h = 0 \pmod f$ и $h = 0 \pmod g$, то есть h делится на f и g. Так как f и g взаимно просто, последнее означает, что h делится на fg. Но $\deg h < \deg fg$. Значит такое может быть только если $h = 0$.

Теперь мы хотим показать сюръективность. Так как F – поле, мы можем рассматривать $F[x]/(fg)$и $F[x]/(f) \times F[x]/(g)$ как векторные пространства над F. Кроме того, Φ является линейным отображением потому что по определению $\Phi(\lambda) = \lambda$ и значит $\Phi(\lambda f) = \Phi(\lambda)\Phi(f) = \lambda\Phi(f)$. Так как Φ инъективно, то для доказательства сюръективности достаточно показать, что оба пространства имеют одинаковую размерность. Ясно, что размерность $\dim_F F[x]/(fg) = \deg(fg)$. С другой стороны, с точки зрения векторных пространств $F[x]/(f) \times F[x]/(g)$ является прямой суммой $F[x]/(f)$ и $F[x]/(g)$. А значит размерность $F[x]/(f) \times F[x]/(g)$ совпадает с $\deg f + \deg g$. Теперь результат следует из утверждения 73. □

6 Поля

6.1 Характеристика

Определение 89. Пусть F – поле. Характеристика поля F – это такое минимальное натуральное число p, что

$$\underbrace{1 + \ldots + 1}_{p} = 0$$

Если такого числа p нет, то говорят, что характеристика равна нулю. Характеристика поля F обозначается через $\operatorname{char} F$.

Давайте я введу удобное обозначение, если мы хотим сложить элемент $x \in F$ n раз сам с собой, где $n \in \mathbb{N}$, то мы можем обозначить эту сумму следующим образом

$$nx = \underbrace{x + \ldots + x}_{n}$$

То есть мы можем говорить об умножении на натуральное число в поле. В частности, характеристика поля F – это такое наименьшее положительное число p , что $p \cdot 1 = 0$ если оно существует, и равна нулю если такого числа нет.

Примеры 90.

1. Если $F = \mathbb{Q}$, тогда сумма $1 + \ldots + 1$ никогда не равна нулю. Значит, $\operatorname{char} \mathbb{Q} = 0$.
2. Если $F = \mathbb{Z}_p$, где p – простое число, то p является наименьшим положительным числом таким, что $1 + \ldots + 1 = p \cdot 1 = 0$ в $\mathbb{Z}_p$. Значит, $\operatorname{char} \mathbb{Z}_p = p$.

Утверждение 91. *Если F – поле, то $\operatorname{char} F$ либо равна нулю, либо простое число.*

Доказательство. Предположим характеристика не ноль. Пусть $\operatorname{char} F = p = nm$ не простое. Тогда

$$0 = \underbrace{1 + \ldots + 1}_{nm} = (\underbrace{1 + \ldots + 1}_{n})(\underbrace{1 + \ldots + 1}_{m}) = (n \cdot 1)(m \cdot 1)$$

Кроме того, числа $n \cdot 1$ и $m \cdot 1$ не равны нулю, так как $p = nm$ было минимальным зануляющим единицу по определению. С другой стороны, мы получили, что произведение $n \cdot 1$ и $m \cdot 1$ – ноль. Это противоречит отсутствию ненулевых делителей нуля в поле F. □

Замечание 92. Пусть F – поле. У нас есть единственный гомоморфизм колец $\phi\colon \mathbb{Z} \to F$, который действует по правилу $n \mapsto n \cdot 1$. Ядро этого гомоморфизма является идеалом в $\mathbb{Z}$. Каждый идеал в кольце целых чисел имеет вид (p) для некоторого неотрицательного числа p (см. утверждение 64). В этом случае p есть ни что иное как характеристика поля F. Это объясняет связь характеристики с идеалами в кольце целых чисел.

Утверждение 93. *Пусть R – коммутативное кольцо. Тогда R является полем тогда и только тогда, когда в нем только два идеала 0 и R.*

Доказательство. Предположим, что R является полем и $I \subseteq R$ – некоторый идеал. Если $I = 0$, то доказывать нечего. Мы можем предположить, что I содержит ненулевой элемент и должны доказать, что в этом случае $I = R$. Пусть $x \in I$ – ненулевой элемент. Так как R – поле, то существует $x^{-1} \in R$. Так как I идеал, то $1 = x^{-1}x \in I$. А значит, для любого $y \in R$, элемент $y = y1 \in I$.

Теперь предположим, что R содержит только два идеала 0 и R. Пусть $x \in R$ – ненулевой элемент. Тогда множество $I = \{rx \mid r \in R\}$ является идеалом в R.[13] Так как у нас только два идеала 0 и R, то I должен быть одним из них. Так как I содержит ненулевой элемент, то он обязан совпасть с R. В частности $1 \in I$, то есть $1 = rx$ для некоторого $r \in R$. А так как R коммутативно, то x обратим и все доказано. □

Предыдущее утверждение показывает, что мы должны изучать поля в терминах элементов, так как идеалы не дают о полях никакой информации. С другой стороны, идеалы как бы измеряют разницу между произвольным кольцом и полем. Чем меньше идеалов в кольце, тем ближе оно к полю.

Утверждение 94. *Кольцо $\mathbb{Z}_n$ является полем тогда и только тогда, когда n является простым.*

Доказательство. Мы уже обсуждали это утверждение и показывали напрямую, что любой ненулевой элемент такого кольца обратим. Давайте теперь обсудим, как это можно показать через идеалы. В силу утверждения 65 мы знаем, что в $\mathbb{Z}_n$ только два идеала лишь в случае, когда n простое. А значит по предыдущему утверждению 93 это равносильно тому, что $\mathbb{Z}_n$ – поле. □

Утверждение 95. *Предположим F – поле простой характеристики p. Тогда F содержит $\mathbb{Z}_p$ как подполе.*

Доказательство. Поле F содержитт единицу $1 \in F$. Давайте рассмотрим множество элементов $\{0, 1, 2 \cdot 1, \ldots, (p-1) \cdot 1\} \subseteq F$. Тогда есть очевидная биекция между этим множеством и полем $\mathbb{Z}_p$. Мы должны показать, что эта биекция является изоморфизмом. Для этого нам достаточно показать

$$n \cdot 1 + m \cdot 1 = (n + m \mod p) \cdot 1 \quad \text{и} \quad (n \cdot 1)(m \cdot 1) = (mn \mod p) \cdot 1$$

Действительно, если $m + n = qp + r$, тогда

$$n \cdot 1 + m \cdot 1 = (m + n) \cdot 1 = (qp) \cdot 1 + r \cdot 1 = q(p \cdot 1) + r \cdot 1 = r \cdot 1$$

Второе утверждение показывается аналогично. □

6.2 Расширения полей

Предположим F – некоторое поле и K – другое поле содержащее F в качестве подполя. В этом случае мы будем говорить, что K – расширение поля F. В этом случае K можно рассматривать как векторное пространство над полем F. А значит, можно говорить о размерности K над F Размерность поля K над полем F называется степенью поля K над F и обозначается $[K : F] = \dim_F K$.

Я хочу обсудить методы по построению новых полей. Следующее утверждение объясняет один из наиболее удобных способов.

Утверждение 96. *Пусть F – поле, $f \in F[x] \setminus F$ – некоторый многочлен. Тогда кольцо $F[x]/(f)$ является полем тогда и только тогда, когда f неприводимый многочлен.*

Доказательство. Давайте дадим прямой доказательство через элементы. В начале предположим, что f приводим. Тогда $f = gh$, где $\deg g < \deg f$ и $\deg h < \deg f$. Тогда $h \neq 0$ в $F[x]/(f)$ так же как $g \neq 0$ в $F[x]/(f)$. Но $gh = f = 0$ в $F[x]/(f)$. Значит, g и h являются ненулевыми делителями нуля. Так как делители нуля необратимы, то это противоречит определению поля.

Если f неприводим, мы должны показать, что любой ненулевой многочлен $g \in F[x]/(f)$ обратим. Так как $\deg g < \deg f$ и $g \neq 0$, f и g взаимно просты. Значит, $1 = (g, f)$. По утверждению 79 пункт (1) следует, что $1 = ug + vf$ для некоторых $u, v \in F[x]$. Но последнее означает, что $1 = ug \pmod f$ а значит, $u = g^{-1}$ в $F[x]/(f)$.[14] □

Замечания 97.
- Давайте подчеркнем, что элемент $x \in F[x]/(p)$ является корнем многочлена p в поле $F[x]/(p)$. Действительно, $p(x) = 0$ в $F[x]/(p)$ по определению.

[13] Здесь важно, что R коммутативно.

[14] Мы могли бы дать другое доказательство с помощью идеалов. По утверждению 87 мы знаем, что в кольце остатков только два идеала лишь в случае неприводимого многочлена. Что по утверждению 93 равносильно тому, что кольцо остатков является полем.

- Давайте рассмотрим поле вещественных чисел $\mathbb{R}$. Тогда многочлен $x^2+1 \in \mathbb{R}[x]$ неприводим. Значит $\mathbb{R}[x]/(x^2+1)$ является полем и элемент x становится корнем многочлена x^2+1. Явно элементы поля $\mathbb{R}[x]/(x^2+1)$ имеют вид $a+bx$, где $a, b \in \mathbb{R}$ и мы знаем, что $x^2 = -1$. Значит это привычная нам модель комплексных чисел, где мы i обозначили за x.

- Если $\deg f = n$, тогда элементы $1, x, \ldots, x^{n-1}$ образуют базис поля $F[x]/(f)$ над полем F. Другими словами, $\dim_F F[x]/(f) = \deg f$.

Расширение с помощью корня Давайте обсудим, что нам дает доказанное утверждение в плане построения полей. Предположим F – поле и $f \in F[x]$ – некоторый многочлен. Теперь я хочу построить поле L содержащее F и некоторый элемент $\alpha \in L$ такой, что $f(\alpha) = 0$. То есть по простому, я хочу добавить к полю F корень многочлена f. Если нам повезло и F уже содержит корень, то нам нечего делать. Теперь обсудим, что делать, если желаемого корня в поле F нет. Мы знаем (см. утверждение 83), что f раскладывается в произведение неприводимых многочленов, то есть $f = p_1 \ldots p_n$ (p_i – необязательно различные неприводимые многочлены). Нам достаточно научиться присоединять корень хотя бы одного p_i к полю F, так как корень p_i автоматически корень f.

А теперь мы просто берем поле остатков по модулю неприводимого многочлена p_i, то есть $L = F[x]/(p_i)$. Утверждение 96, гарантирует, что L является полем. Как мы уже отмечали элемент $x \in F[x]/(p_i)$ будет корнем p_i, а значит и корнем f. Таким образом мы можем выбрать его за α. Обратим еще внимание на то, что степень L над F совпадает в точности со степенью многочлена f.

6.3 Конечные поля

Давайте обсудим как устроены поля состоящие только из конечного числа элементов. Такие поля будут самыми полезными в приложениях.

Утверждение 98. *Если F – конечное поле, то его характеристика не ноль. В частности, F содержит $\mathbb{Z}_p$, где $p = \operatorname{char} F$.*

Доказательство. Так как поле F конечно, то в частности это значит, что $(F, +)$ – конечная абелева группа. А значит любой элемент в ней имеет конечный порядок. В частности 1 имеет конечный порядок по сложению, а это и есть характеристика поля. Второе утверждение следует из утверждения 95. □

Утверждение 99. *Предположим F – конечное поле и $\operatorname{char} F = p$. Тогда, $|F| = p^n$ для некоторого n. Более того, можно уточнить, что $n = [F : \mathbb{Z}_p]$.*

Доказательство. По утверждению 95, F содержит $\mathbb{Z}_p$ как подполе. Теперь мы рассмотрим F как векторное пространство над $\mathbb{Z}_p$. Так как F конечно, то оно имеет и конечную размерность. Поэтому F изоморфно $\mathbb{Z}_p^n$ как векторное пространство. Но, $\mathbb{Z}_p^n$ имеет в точности p^n элементов. Более того, мы видим, что n равно размерности F над $\mathbb{Z}_p$. □

Утверждение 100. *Пусть F – конечное поле. Тогда группа F^* является циклической порядка $|F| - 1$.*

Доказательство. Группа F^* является конечной абелевой группой. А значит, она изоморфна группе вида $\mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_k}$, где $d_1 | \ldots | d_k$ (см. утверждение 50). В частности для любого элемента группы F^* выполнено $x^{d_k} = 1$. Потому все элементы группы F^* являются корнями многочлена $x^{d_k} - 1$. В силу единственного разложения на множители, каждый многочлен f имеет не более $\deg f$ корней. Значит, $|F^*| \leqslant d_k$. С другой стороны $|F^*| = d_1 \ldots d_k$. Единственное, когда такое возможно – у нас был один циклический множитель $\mathbb{Z}_{d_k}$. Но это и значит, что F^* изоморфно $\mathbb{Z}_{d_k}$ и все доказано. □

А вот очень важный классификационный результат для конечных полей (я не собираюсь его доказывать).

Утверждение 101. *Для любого простого числа p и любого натурального n существует единственное с точностью до изоморфизма поле F содержащее p^n элементов.*

Так как поле из p^n элементов единственно, то оно имеет специальное название $\mathbb{F}_{p^n}$. Обратите внимание, что $\mathbb{F}_p = \mathbb{Z}_p$. Однако, надо отметить, что для $n > 1$ такая конструкция не работает, то есть $\mathbb{F}_{p^n} \not\simeq \mathbb{Z}_{p^n}$, хотя бы потому что кольцо $\mathbb{Z}_{p^n}$ содержит делители нуля.

Хороший вопрос – как построить все конечные поля размера p^n. Прежде всего у нас есть хорошее начало $\mathbb{F}_p = \mathbb{Z}_p$. Теперь мы должны найти неприводимый многочлен $f \in \mathbb{Z}_p[x]$ степени n. И искомое поле строится

так $\mathbb{F}_{p^n} = \mathbb{Z}_p[x]/(f)$. Надо отметить, что количество неприводимых многочленов степени n над $\mathbb{Z}_p$ может быть большим. Однако, все такие многочлены дают изоморфные поля. В частности это означает, что вы можете выбрать любой многочлен f или тот, который вам удобен.

Пример 102. Давайте построим поле $\mathbb{F}_4$. Базовое поле будет $\mathbb{Z}_2$. Существует только один неприводимый многочлен степени 2 над полем $\mathbb{Z}_2$ – это $x^2 + x + 1 \in \mathbb{Z}_2[x]$. Тогда требуемое поле будет

$$\mathbb{F}_4 = \mathbb{Z}_2[x]/(x^2 + x + 1) = \{a + bx \mid a, b \in \mathbb{Z}_2\}$$

Сложение задается обычным покомпонентным сложением. Чтобы посчитать произведение элементов в $\mathbb{F}_4$ нам достаточно уметь перемножать все степени x между собой. Произведения $1 \cdot 1 = 1$ и $1 \cdot x = 1$ считаются легко. И нам лишь надо научиться считать $x \cdot x$. По определению $x^2 = 1 + x \pmod{x^2 + x + 1}$. Тогда в общем виде произведение выглядит так

$$(a + bx)(c + dx) = ac + adx + bcx + bdx^2 = ac + adx + bcx + bd(1 + x) = ac + bd + (ad + bc + bd)x$$

Замечания 103.

- Так как поле $\mathbb{Z}_p$ содержится в $\mathbb{F}_{p^n}$, то и группа $\mathbb{Z}_p^*$ содержится в группе $\mathbb{F}_{p^n}^*$. Мы уже отмечали в разделе 3.3, что проблема дискретного логарифмирования является сложной в группе $\mathbb{Z}_p^*$. Это означает, что и проблема дискретного логарифмирования является сложной в $\mathbb{F}_{p^n}^*$. Действительно, если бы мы могли быстро решать уравнения $g^x = h$ по x для всех $g, h \in \mathbb{F}_{p^n}^*$, мы могли бы решать такое и для $g, h \in \mathbb{Z}_p^* \subseteq \mathbb{F}_{p^n}^*$. Это делает привлекательной идею использовать группу $\mathbb{F}_{p^n}^*$ в криптографии. Однако, порядок этой группы достаточно далек от простого числа и это делает ее криптографически менее стойкой. Тем не менее, с помощью конечных полей можно построить другой класс интересных групп, которые будут криптографически более стойкими, чем $\mathbb{Z}_p^*$.

- Для различных вопросов бывает полезно знать образующий группы $\mathbb{F}_{p^n}^*$. Если мы строим поле как кольцо остатков вида $\mathbb{Z}_p[x]/(f)$, где $f \in \mathbb{Z}_p[x]$ – неприводимый многочлен степениn, то хорошим кандидатом в качестве образующего $\mathbb{F}_{p^n}^*$ кажется элемент x. Однако, x не обязан быть образующим $\mathbb{F}_{p^n}^*$. Является ли он образующим группы $\mathbb{F}_{p^n}^*$ зависит от выбора неприводимого многочлена f. Для одних многочленов он образующий, для других – нет.

  Давайте рассмотрим следующий пример. Над полем $\mathbb{Z}_3$ существует три неприводимых унитальных многочлена степени 2: $f_1 = x^2 + 1$, $f_2 = x^2 + x - 1$, $f_3 = x^2 - x - 1$. Если мы используем первый многочлен, мы получим $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2 + 1)$. Группа $\mathbb{F}_9^* \simeq \mathbb{Z}_8$, значит образующий должен быть порядка 8. Однако, $x^4 = (x^2)^2 = (-1)^2 = 1$ в этом случае. А значит, порядок x равен 4 и он не образующий. С другой стороны, если мы возьмем f_2, то получим $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2 + x - 1)$ или f_3, то получим $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2 - x - 1)$. В обоих случаях прямой подсчет показывает, что x оказывается образующим группы $\mathbb{F}_9^*$.

6.4 Случайный генератор Галуа

Существует понятие регистра сдвига с линейной обратной связью. Это специальный вид регистра производящий последовательность бит. На его основе можно строить генераторы псевдослучайных чисел. Существует две основные конструкции называемые в честь Фибоначчи и Галуа. Оказывается эти понятия можно обсуждать в терминах теории конечных полей. Я сделаю это на примере генератора Галуа.

Предположим у нас есть конечный алфавит $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ и мы хотим создать случайную последовательность элементов из этого алфавита. Существует много разных способов сделать это, но вот как выглядит подход на основе конечных полей. Давайте зафиксируем конечное поле $\mathbb{F}_{p^n}$. Тогда нам надо научиться производить случайную последовательность элементов $a_1, a_2, \ldots \in \mathbb{F}_{p^n}$, а потом по каждому такому элементу надо научиться строить элемент $\phi(a_1), \phi(a_2), \ldots \in \mathbb{Z}_p$. Оказывается, что хорошую последовательность из a_i можно построить с помощью возведения в степень в конечном поле. А чтобы научиться вычислять элементы $\mathbb{Z}_p$ по последовательности a_i, надо вспомнить, что $\mathbb{F}_{p^n}$ является векторным пространством над $\mathbb{Z}_p$. В этом случае в качестве ϕ годится любая процедура по вычислению какой-нибудь координаты. Давайте я теперь расскажу, как устроен весь процесс более детально.

Предположим p – простое число и мы фиксируем некоторое натуральное n. Возьмем неприводимый многочлен $f \in \mathbb{Z}_p[x]$ степени n и построим с помощью него поле $\mathbb{F}_{p^n} = \mathbb{Z}_p[x]/(f)$. По определению

$$\mathbb{F}_{p^n} = \{a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} \mid a_i \in \mathbb{Z}_p\}$$

То есть каждый элемент поля определяется последовательностью $(a_0, a_1, \ldots, a_{n-1})$. Теперь мы выберем образующий $g \in \mathbb{F}_{p^n}^*$. Это неприятная процедура, но это надо сделать единожды. Обычно, мы выбираем f так,

чтобы x оказался образующим. Теперь мы производим последовательность $g, g^2, g^3, g^4, \ldots$. Каждая степень элемента g соответствует последовательности коэффициентов a_i как выше. Тогда в качестве случайного элемента из $\mathbb{Z}_p$ можно выбрать a_0. Кроме того, мы можем начать нашу последовательность не обязательно с нулевой степени. Мы можем начать с произвольной степени k: $g^k, g^{k+1}, g^{k+2}, \ldots$. С практической точки зрения, это значит, что мы выбрали элемент $h \in \mathbb{F}_{p^n}^*$ и строим последовательность $hg, hg^2, hg^3, hg^4, \ldots$. Так как $h = g^k$ для некоторого k, это эквивалентный подход.

Матричная форма Теперь давайте перепишем конструкцию выше в координатах. Как и раньше, мы предполагаем, что

$$\mathbb{F}_{p^n} = \mathbb{Z}_p[x]/(f) = \{a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} \mid a_i \in \mathbb{Z}_p\}$$

В этом случае $1, x, x^2, \ldots, x^{n-1}$ является базисом $\mathbb{F}_{p^n}$ над $\mathbb{Z}_p$. Предположим, что многочлен $f = x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0$ выбран так, что x является образующим $\mathbb{F}_{p^n}^*$. Отображение $\phi\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ по правилу $h \mapsto xh$ является линейным. Давайте напишем матрицу этого отображения в базисе из степеней x:

$$\phi(1, x, \ldots, x^{n-2}, x^{n-1}) = (1, x, \ldots, x^{n-2}, x^{n-1}) \begin{pmatrix} 0 & 0 & \ldots & 0 & -c_0 \\ 1 & 0 & \ldots & 0 & -c_1 \\ 0 & 1 & \ddots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -c_{n-1} \end{pmatrix}$$

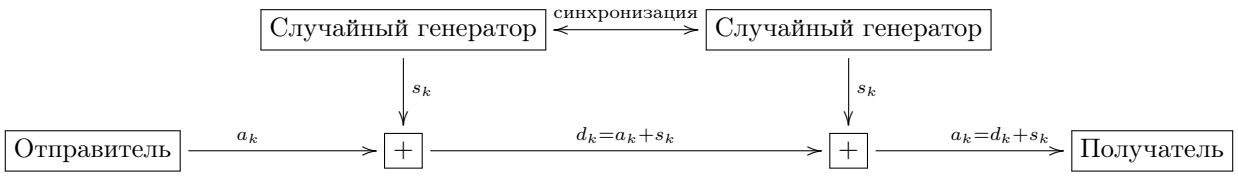
Обозначим матрицу отображения ϕ за A. Элемент $h = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$ в координатах описывается столбцом $v = (a_0, a_1, \ldots, a_{n-1})^t$. Тогда элемент xh описывается произведениемAv. Потому случайный генератор работает следующим образом. Мы фиксируем некоторый начальный вектор $v = (a_0, a_1, \ldots, a_{n-1})^t$ и строим последовательность векторов $v, Av, A^2v, A^3v, \ldots$. Далее у каждого вектора мы вычисляем первую координату и получаем требуемую случайную последовательность. Существует аналогичный подход под названием Фибоначчи. В этом случае используется матрица A^t вместо матрицы A. Существует так же концептуальный подход к генератору Фибоначчи, описывающий его в терминах поля $\mathbb{F}_{p^n}$, но я не буду на этом заострять внимание.

6.5 Потоковое шифрование

Существует применение случайных генераторов в шифровании. Давайте обсудим потоковое шифрование. Обратите внимание, что когда вы передаете данные, то шифрование накладывает дополнительные расходы. Потому передавать данные по шифрованному каналу может оказаться дорого, в том смысле, что мы не можем себе этого позволить делать часто. Тем не менее, мы все же не хотим передавать по незащищенному каналу открытые данные. Вот что можно сделать в этом случае.

Предположим, что у нас алфавит состоит из двух символов $\mathbb{Z}_2 = \{0, 1\}$. Наше сообщение – это последовательность бит $a_0, a_1, a_2, a_3, \ldots$. Предположим, что у нас есть некоторый случайный генератор $S\colon \mathbb{N} \to \mathbb{Z}_2$, Тогда мы можем построить последовательность случайных бит с помощью него $s_0 = S(0), s_1 = S(1), s_2 = S(2), \ldots$. Теперь каждый бит исходного сообщения можно зашифровать с помощью случайного бита следующим образом $d_k = a_k + s_k \pmod 2$ и передвать d_k вместо a_k. Чтобы восстановить сообщение, нам надо посчитать $a_k = d_k + s_k \pmod 2$. А для этого нам надо знать в точности последовательность случайных бит s_k. Вместо того, чтобы передавать последовательность s_k по зашифрованному каналу, мы передадим по нему «копию» нашего случайного генератора, а точнее мы передадим информацию для инициализации точно такого же случайного генератора. Тогда при наличии двух синхронизированных случайных генераторов, мы можем свободно шифровать и расшифровывать сообщения по озвученной схеме.

Давайте продемонстрирую описанную схему на диаграмме



Примером использования потокового шифрования является стандарт GSM. Современный стандарт GSM использует более сложную схему шифрования, однако в основе ее лежит идея описанная выше.

7 Коды исправляющие ошибки

Предположим, что у нас есть конечный алфавит F из q символов и мы представляем информацию в виде последовательностей символов из F. Теперь представим себе, что мы хотим передавать последовательность $a_1, a_2, \ldots, a_n, \ldots \in F$ по каналу связи, но при этом канал связи имеет некоторые помехи. В результате воздействия этих помех получателю приходит не оригинальная последовательность, а испорченная. Мы будем предполагать, что канал связи может лишь испортить какие-то отдельные символы нашей последовательности. В результате возникает задача – как восстановить исходную последовательность символов, зная испорченную.

Давайте я опишу общую концепцию, в рамках которой решается подобная задача. Прежде всего, пусть у нас передаваемая информация хранится порциями по k символов. То есть хранимая информация – это элементы F^k. Теперь нам нужно придумать некоторое инъективное отображение $\phi\colon F^k \to F^n$, которое и называется кодированием. Смысл этого отображения в том, что мы как-бы добавляем к исходной последовательности дополнительную контрольную информацию. После этого полученное слово длины n мы уже будем передавать по сети и именно это более длинное слово может как-то испортиться. После получения испорченного слова, нам нужна некоторая процедура $\psi\colon F^n \to F^k$, которая называется декодированием и которая должна восстановить исходное сообщение если это возможно. На картинке процесс можно изобразить так

$$\begin{array}{ccccccccc} \text{Сообщение} & \longmapsto & \text{Закодированное} & \longmapsto & \text{Канал} & \longmapsto & \text{Переданное} & \longmapsto & \text{Раскодированное} \\ & & & & \Uparrow\Uparrow\Uparrow & & & & \\ a \in F^k & & \phi(a) \in F^n & & \text{ШУМ} & & \tilde{c} \in F^n & & \psi(\tilde{c}) \in F^k \end{array}$$

Самая важная задача – сделать так, чтобы $\psi(\tilde{c})$ совпало с исходным сообщением $a \in F^k$. Конечно же, если канал может как угодно портить сообщение, то мы ничего не можем гарантировать. Однако, можно добиться некоторых гарантий, если мы знаем, что шум в канале не абы какой. Частым предположением является предположение о том, что шум может испортить не более e символов в передаваемой последовательности. То есть процент ошибок в канале равен e/n.

Пример Давайте начнем с очень простого, но понятного примера. Пусть мы хотим передавать последовательности F^k по каналу, который может максимум испортить один элемент. Тогда давайте рассмотрим следующую процедуру кодирования $\phi\colon F^k \to F^{3k}$ по правилу $w \mapsto w, w, w$, то есть мы просто повторяем слово три раза. Тогда понятно как восстановить одну ошибку. Если нам пришла последовательность w_1, w_2, w_3, то два слова из трех должны быть одинаковыми, вот это слово мы и берем. Главным недостатком такого подхода является увеличение количества передаваемой информации. Во-первых, это не эффективно в плане скорости. Во-вторых, это не эффективно, так как количество ошибок в канале может расти в зависимости от размера передаваемого сообщения и одна ошибка на слове длины k может легко превратиться в три ошибки на слове длины $3k$, а значит и кодирование может оказаться бесполезным. Тем не менее, это хороший концепт, показывающий как именно может происходить процедура кодирования и раскодирования. В дальнейшем мы постараемся построить более экономные процедуры кодирования и декодирования.

7.1 Общие замечания

Определение 104. Пусть F – конечный алфавит и $a, b \in F^n$ – два слова длины n в этом алфавите. Тогда расстояние Хэмминга между словами a и b это:

$$\rho(a, b) = |\{i \mid a_i \neq b_i\}| \quad \text{количество отличающихся символов}$$

Обратите внимание, если мы передавали по сети строчку $a \in F^n$, а нам пришла на вход строчка $b \in F^n$, то $\rho(a, b)$ – это в точности количество произошедших ошибок.

Определение 105. Пусть F – конечный алфавит. Тогда при $k < n$ инъективное отображение $\phi\colon F^k \to F^n$ называется кодированием, а образ $C = \operatorname{Im}\phi$ называется кодом.

Как мы увидим ниже, многие свойства кодирования зависят именно от свойств кода C. Вопросы нахождения функции кодирования и раскодирования больше сопряжены с эффективностью их вычисления, просто потому что при наличии множества C кодирование может осуществляться любым вложением $\phi\colon F^k \to C$, а декодирование в худшем случае можно делать полным перебором, если оно возможно.

Определение 106. Пусть F – конечный алфавит и $C \subseteq F^n$ – некоторое подмножество. Тогда код C исправляет t ошибок, если для любого $x \in F^n$ существует не более одного $c \in C$ такого, что $\rho(x, c) \leqslant t$.

Давайте обсудим последнее определение.

- Оно говорит, что если у вас есть произвольное слово $x \in F^n$, то меняя в нем не более t символов, мы максимум найдем одно слово из C. Потому, если у нас слово x возникло в результате не более t изменений в слове $c \in C$, то слово c будет единственным словом из C таким, что $\rho(x, c) \leqslant t$. А значит, мы точно можем восстановить слово c.
- Кроме того, может случиться такая ситуация, что $\rho(x, c) \leqslant t$ не выполняется ни для какого слова c. Это означает, что при передаче по каналу произошло больше t ошибок. Таким образом, по-хорошему процедура декодирования ψ должна не просто выплевывать раскодированную последовательность, а еще иногда сообщать, что мы получили недопустимое слово.
- Если нам дана процедура кодирования $\phi\colon F^k \to F^n$, то мы можем говорить, что ϕ допускает исправление t ошибок, если код $\operatorname{Im}\phi$ допускает исправление t ошибок.

Теперь я хочу получить численные характеристики кода, которые бы описывали его возможности по восстановлению ошибок.

Определение 107. Пусть F – конечный алфавит и $C \subseteq F^n$ – некоторое подмножество. Тогда минимальное расстояние кода C это

$$d_C = \min_{c \neq c' \in C} \rho(c, c')$$

Определение 108. Пусть F – конечный алфавит. Тогда шаром радиуса $r \in \mathbb{Z}$ с центром в $x \in F^n$ называется множество

$$B_r(x) = \{y \in F^n \mid \rho(x, y) \leqslant r\}$$

Утверждение 109. *Пусть F – конечный алфавит и $C \subseteq F^n$ – некоторое подмножество. Тогда эквивалентно*

1. *Код C исправляет t ошибок.*
2. *Для любых $x \neq y \in C$ верно $B_t(x) \cap B_t(y) = \varnothing$.*
3. *$d_C \geqslant 2t + 1$.*

Доказательство. (1)⇒(2). Предположим противное, что существует $z \in B_t(x) \cap B_t(y)$ для некоторых $x, y \in C$. Но тогда для слова z найдутся два слова $x, y \in C$ на расстоянии не более t, что противоречит тому, что код исправляет t ошибок.

(2)⇒(3). Предположим противное, то есть $d_C \leqslant 2t$. Тогда найдутся два слова $x, y \in C$ такие, что $\rho(x, y) \leqslant 2t$. Это значит, что слово y отличается от слова x в $s \leqslant 2t$ позициях. Давайте изменим в y $s/2$ позиций на значения из x. Тогда получим слово z, которое отличается от x и от y не более чем на $s/2 \leqslant t$ позиций. А это значит, что мы нашли слово в пересечении $B_t(x) \cap B_t(y)$, противоречие.

(3)⇒(1). Предположим противное, тогда для какого-то слова z найдутся два слова $x, y \in C$ такие, что $\rho(x, z) \leqslant t$ и $\rho(y, z) \leqslant t$. Но тогда по неравенству треугольника для ρ имеем $\rho(x, y) \leqslant \rho(x, z) + \rho(z, y) \leqslant 2t$, противоречие. □

Пример Давайте рассмотрим следующий код $C = \{(a, a, \ldots, a) \mid a \in F\} \subseteq F^n$. Очевидно, что минимальное расстояние кода $d_C = n$. А значит, код исправляет $t = [(n-1)/2]$ ошибок.

7.2 Линейная алгебра

Хороший вопрос – как эффективно задавать множество $C \subseteq F^n$, чтобы не работать с ним перебором. Оказывается один из подходов – воспользоваться достижениями линейной алгебры над конечными полями. Такой подход приводит к так называемым линейным кодам. Давайте поговорим о них.

Определение 110. Пусть $F = \mathbb{F}_q$ – конечное поле из $q = p^n$ элементов. Тогда подмножество $C \subseteq \mathbb{F}_q^n$ называется линейным кодом, если C является подпространством над полем $\mathbb{F}_q$. Если при этом размерность подпространства равна k, то говорят, что C – это (n, k)-код.

Если у нас есть линейный код $C \subseteq \mathbb{F}_q^n$, то легко построить кодирующую функцию. Пусть размер кода C равен k, тогда мы можем найти в C базис $c_1, \ldots, c_k$. Тогда кодирующее отображение $\phi\colon \mathbb{F}_q^k \to \mathbb{F}_q^n$ задано по правилу $x \mapsto Ax$, где у матрицы A по столбцам поставлены векторы $c_1, \ldots, c_k$.

Определение 111. Пусть $x \in \mathbb{F}_q^n$, тогда нормой вектора x будет называться его расстояние до нулевого вектора в норме Хэмминга, то есть

$$\|x\| = \rho(x, 0) = |\{i \mid x_i \neq 0\}|$$

Утверждение 112. *Пусть $C \subseteq \mathbb{F}_q^n$ – линейный код. Тогда $d_C = \min_{0 \neq c \in C} \|c\|$.*

Доказательство. Пусть $x, y \in \mathbb{F}_q^n$ два произвольных слова, обратим внимание, что $\rho(x, y) = \rho(x - y, 0) = \|x - y\|$, потому что количество разных координат у x и y – это в точности количество ненулевых координат у разности $x - y$. А тогда

$$d_C = \min_{c \neq c' \in C} \rho(c, c') = \min_{c \neq c' \in C} \|c - c'\| = \min_{0 \neq c \in C} \|c\|$$

Последнее равенство выполнено в силу того, что C является подпространством, потому если c, c' пробегают все C, то и их разность $c - c'$ пробегают все C. □

Определение 113. Пусть $C \subseteq F_q^n$ – некоторый линейный код размерности k и пусть $H \in \mathrm{M}_{n-k\,n}(\mathbb{F}_q)$ такая, что $\operatorname{rk} H = n - k$ и $C = \{y \in \mathbb{F}_q^n \mid Hy = 0\}$. Тогда матрица H называется проверочной матрицей для кода C.

Пример Если взять код $C = \{(a, \ldots, a) \mid a \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^n$, то это $(n, 1)$-код с проверочной матрицей (все незаполненные места – нулевые)

$$\begin{pmatrix} 1 & & & -1 \\ & \ddots & & \vdots \\ & & 1 & -1 \end{pmatrix}$$

Утверждение 114. *Пусть $C = \{y \in \mathbb{F}_q^n \mid Hy = 0\}$. Тогда эквивалентно*

1. *$d_C \geqslant s + 1$*
2. *Любые s столбцов матрицы H линейно независимы.*

Доказательство. Давайте рассмотрим $y \in \mathbb{F}_q^n$ у которого не более s ненулевых координат. Тогда Hy равно линейной комбинации не более s столбцов матрицы H. Таким образом условие, что любые s столбцов H линейно независимы означает, что системе $Hy = 0$ не удовлетворяет ни один вектор у которого не более s ненулевых координат. Или другими словами, условие (2) эквивалентно тому, что в C лежат векторы у которых хотя бы $s+1$ ненулевая координата. А это условие в точности равносильно тому, что $d_C \leqslant s+1$. □

7.3 Коды Хэмминга

Давайте рассмотрим случай бинарного алфавита $F = \mathbb{F}_2 = \{0, 1\}$. Фиксируем число k и составим матрицу H следующим образом. По столбцам матрицы H_k поставим все ненулевые векторы из $\mathbb{F}_2^k$. Тогда получится матрица размера k на $2^k - 1$. Пусть $n = 2^k - 1$. Тогда можно определить код с такой проверочной матрицей

$$C_k = \{y \in \mathbb{F}_2^n \mid H_k y = 0\} \subseteq \mathbb{F}_2^n$$

Полученный код называется бинарным кодом Хэмминга. Это $(2^k - 1, 2^k - k - 1)$-код. Обратите внимание, что закодированное слово имеет длину $n = 2^k - 1$, при этом количество проверочной информации равно $k \approx \log_2 n$. Чтобы построить кодирующее отображение $\phi\colon \mathbb{F}_2^{2^k-k-1} \to \mathbb{F}_2^{2^k-1}$ нам надо найти ФСР для системы $H_k y = 0$ и составить их по столбцам в матрицу A_k. Тогда $\phi(x) = A_k x$.

Если мы хотим раскодировать кодовые слова, то для начала давайте посчитаем минимальное расстояние кода. Мы видим, что в матрице H_k любые 2 вектора линейно независимы и существует 3 линейно зависимых вектора. Значит $d_{C_k} = 3$. То есть количество исправляемых ошибок будет $e = [(d_{C_k} - 1)/2] = 1$. Если ошибка произошла в i-ом символе, это значит, что кодовое слово y изменилось на $y + e_i$. А тогда $H_k(y + e_i) = H_k e_i$ – i-ый столбец матрицы H_k. Так как все столбцы уникальны это дает возможность однозначно узнать номер i. Более того, давайте смотреть на столбцы в H_k как на представление целых чисел в двоичной системе, то есть вектору $(a_1, \ldots, a_k)$ ставим в соответствие число $a_1 + a_2 2 + \ldots + a_k 2^{k-1}$. Расставим столбцы в порядке увеличения чисел. Тогда $H_k e_i$ будет двоичным разложением числа i.

Двоичные коды Хэмминга интересны тем, что они дают плотную упаковку шаров радиуса 1 в пространстве $\mathbb{F}_2^{2^k-1}$, то есть шары радиуса 1 с центрами в кодовых словах кода Хэмминга покрывают все пространство без пустот и пересечений. У этого кода очень простая функция кодирования и декодирования. Единственным его недостатком является малое число исправляемых ошибок.

7.4 Коды Рида-Соломона

Оказывается, что для линейных кодов можно оценить сверху минимальное кодовое расстояние, через размерность пространства. Это утверждение носит название «Неравенство Синглтона».

Утверждение 115 (Неравенство Синглтона)**.** *Пусть $C \subseteq \mathbb{F}_q^n$ – некоторый линейный (n,k)-код. Тогда $d_C \leqslant n-k+1$.*

Доказательство. Пусть $q_1, \ldots, q_{k-1} \in \mathbb{F}_q$ – фиксированные числа. Рассмотрим подмножество

$$D_{q_1,\ldots,q_{k-1}} = \{y \in \mathbb{F}_q^n \mid y = (q_1, \ldots, q_{k-1}, *, \ldots, *)\} \subseteq \mathbb{F}_q^n$$

То есть мы зафиксировали первые $k-1$ координату в последовательности, а остальные координаты могут быть какие угодно. Всего таких подмножеств q^{k-1} по количеству последовательностей $q_1, \ldots, q_{k-1}$. Более того, подмножества $D_{q_1,\ldots,q_{k-1}}$ образуют разбиение $\mathbb{F}_q^n$ на непересекающиеся множества. Теперь посмотрим на подпространство C в нем q^k элементов, так как размерность равна k. А значит по принципу Дирихле найдется хотя бы одна «клетка» $D_{q_1,\ldots,q_{k-1}}$ содержащая хотя бы два «кролика» – точки из C. То есть хотя бы два элемента из C совпадают в первых $k-1$ позиции. А это значит, что расстояние между этими точками не больше $n-k+1$. А значит и минимальное расстояние между точками C не больше $n-k+1$. □

Следующий пример кодов – коды Рида-Соломона. На этих кодах достигается равенство в неравенстве Синглтона. Пусть у нас $F = \mathbb{F}_q$ и число n выбрано так, что $n \leqslant q$. Теперь для любого $k < n$ построим кодирующую функцию $\phi\colon \mathbb{F}_q^k \to \mathbb{F}_q^n$. Обратите внимание, что для построения такого кода нам требуется достаточно большой алфавит (условие $n \leqslant q$).

Мы можем отождествить $\mathbb{F}_q^k$ с многочленами степени меньше k, а именно

$$a = (a_0, \ldots, a_{k-1}) \in \mathbb{F}_q^k \mapsto f_a = a_0 + a_1 x + \ldots + a_{k-1}x^{k-1}$$

Выберем n различных точек $x_1, \ldots, x_n$ поля $\mathbb{F}_q$.[15] Теперь построим отображение $\phi\colon \mathbb{F}_q^k \to \mathbb{F}_q^n$ по правилу $a \mapsto f_a \mapsto (f_a(x_1), \ldots, f_a(x_n))$. Давайте оценим минимальное кодовое расстояние. Если у нас есть два разных многочлена степени меньше k, то они могут иметь не более $k-1$ общего значения. Значит разные последовательности $\phi(a)$ и $\phi(b)$ для разных $a, b \in \mathbb{F}_q^k$ могут иметь не более $k-1$ одинаковых координат. То есть расстояние между ними будет не меньше $n-k+1$. С другой стороны, по неравенству Синглтона минимальное расстояние кода не больше $n-k+1$. Значит $d_C = n-k+1$. А значит, количество исправляемых кодом ошибок равно $e = [(n-k)/2]$.

Важно, что коды Рида-Соломона допускают эффективную процедуру декодирования. Предположим, что нам на вход пришла последовательность $b_1, \ldots, b_n \in \mathbb{F}_q$ и мы хотим восстановить многочлен f_a степени меньше k. Давайте я в начале опишу процедуру, как восстановить соответствующий многочлен, а уже потом обсудим, почему эта процедура корректная. Рассмотрим два многочлена $D, Q \in \mathbb{F}_q[x]$ следующего вида

$$D = x^e + d_{e-1}x + \ldots + d_0 \quad \text{и} \quad Q = q_{e+k-1}x^{e+k-1} + \ldots + q_0$$

то есть многочлен D имеет степень e и старший коэффициент 1, а многочлен Q имеет степень меньше $e+k$. Оба многочлена берутся с неопределенными коэффициентами. Теперь надо составить систему уравнений

$$Q(x_1) = b_1 D(x_1), \ldots, Q(x_n) = b_n D(x_n)$$

Это неоднородная система линейных уравнений на коэффициенты Q и D. Если последовательность $b_1, \ldots, b_n$ получена из последовательности кода Рида-Соломона в результате не более e ошибок, то оказывается, что такая система всегда имеет хотя бы одно решение. Пусть Q и D – какое-то решение. Оказывается, что в этом случае D делит Q и при этом Q/D – это искомый многочлен f_a. Таким образом мы получаем алгоритм декодирования последовательности b в последовательность a. Надо лишь объяснить, почему эта процедура действительно работает и дает, что надо.

Пусть $a \in \mathbb{F}_q^k$ – некоторое слово, $c = \phi(a) = (f_a(x_1), \ldots, f_a(x_n))$ – соответствующее кодовое слово и $b = (b_1, \ldots, b_n)$ – испорченное кодовое слово, где произошло не более e ошибок. Пусть ошибки произошли в позициях $i_1, \ldots, i_e$. Тогда мы можем рассмотреть многочлен $D = (x - x_{i_1}) \ldots (x - x_{i_e})$. Тогда последовательность $d = (D(x_1), \ldots, D(x_n))$ имеет нули ровно в тех позициях, где произошли ошибки. Тогда последовательность

[15] В этом месте мы пользуемся неравенством $n \leqslant q$.

bd совпадает с последовательностью cd, потому что b и c отличаются в позициях $i_1, \ldots, i_e$, где d равна нулю. Но что означает равенство $bd = cd$. Давайте его распишем.

$$f_a(x_1)D(x_1) = b_1D(x_1), \ldots, f_a(x_1)D(x_n) = b_nD(x_n)$$

Но тогда обозначим f_aD через Q. Мы получим многочлен степени строго меньше $k + e$. Последнее означает, что если последовательность $b_1, \ldots, b_n$ получена из кодового слова c не более чем e ошибками, то система на многочлены Q и D имеет решение.

Теперь пусть

$$Q(x_1) = b_1D(x_1), \ldots, Q(x_n) = b_nD(x_n)$$

и Q и D – произвольное решение. При этом отметим, что степень Q меньше $k + e$, а степень D равна e и его старший коэффициент – 1. Пусть a – кодовое слово, из которого получилась последовательность b. Рассмотрим последовательность

$$f_a(x_1)D(x_1), \ldots, f_a(x_n)D(x_n)$$

Эта последовательность имеет не менее $n - e \geqslant k + e$ общих элементов с последовательностью

$$b_1D(x_1), \ldots, b_nD(x_n)$$

А значит не менее $k + e$ общих элементов с последовательностью

$$Q(x_1), \ldots, Q(x_n)$$

То есть многочлены f_aD и Q имеющие степень меньше $k + e$ имеют хотя бы $k + e$ общих точек. А это значит, что они обязаны совпадать. Отсюда $f_aD = Q$ и мы доказали, что требовалось.

8 Базисы Грёбнера

Сейчас я хочу поговорить о многочленах от нескольких переменных. Одна из причин почему мы так любим многочлены от одной переменной – Евклидов алгоритм деления с остатком. Оказывается, что многие задачи эффективно решаются с помощью деления с остатком. Однако, когда мы переходим к многочленам от нескольких переменных у нас уже не существует Евклидова алгоритма деления (если дать строгие определения, то можно даже доказать, что в многочленах от нескольких переменных не может быть деления с остатком). Что же делать в такой тяжелой и грустной ситуации? Предлагается вместо честного деления с остатком ввести очень похожую процедуру называемую редукцией. Более того с помощью такой процедуры можно будет редуцировать многочлен относительно целого семейства многочленов и получать в результате аналоги остатков. Основная проблема будет заключаться в том, что если редуцировать по «плохому» множеству, то остатки будут получаться не единственными. В результате среди всех семейств выделяют только «хорошие», которые дают корректно определенные остатки. Такие хорошие множества и называются базисами Грёбнера.

8.1 Многочлены от нескольких переменных

Пусть F – некоторое поле. Многочлен f от переменных $x_1, \ldots, x_n$ с коэффициентами в F – это картинка следующего вида

$$f = \sum_{k_1,\ldots,k_n \geqslant 0} a_{k_1\ldots k_n} x_1^{k_1} \ldots x_n^{k_n}, \quad a_{k_1\ldots k_n} \in F$$

здесь только конечное число коэффициентов отлично от нуля. Сложение и умножение многочленов заданы обычными формулами. Множество всех многочленов от переменных $x_1, \ldots, x_n$ с коэффициентами в поле F будет обозначаться $F[x_1, \ldots, x_n]$. Множество $F[x_1, \ldots, x_n]$ с операциями сложения и умножения является коммутативным кольцом.

Выражение $m = x_1^{k_1} \ldots x_n^{k_n}$ называеся мономом. Степень монома – $\deg m = k_1 + \ldots + k_n$. Степень многочлена f – это максимум степеней всех мономов в него входящих с ненулевыми коэффициентами. Степень нулевого многочлена считается равной $-\infty$ так же как и в случае одной переменной. Прямое вычисление показывает, что если $f, g \in F[x_1, \ldots, x_n]$, то $\deg(fg) = \deg f + \deg g$. Моном умноженный на коэффициент из поля F называется термом. Таким образом любой многочлен всегда является какой-то конечной суммой термов.

8.2 Мономиальные порядки

Прежде всего нам нужен способ упорядочить мономы. В случае многочленов от одной переменной, мы могли эффективно сравнивать мономы по степени единственной переменной. В случае нескольких переменных требуется какая-то новая процедура, позволяющая сказать, какой моном в многочлене старший, а какой младший. Существует огромное количество «хороших» порядков на мономах. Однако, чтобы упростить изложение, я собираюсь обсудить лишь самый полезный для наших целей – лексикографический порядок.

Определение 116. Мы хотим определить лексикографический порядок на мономах.

1. Прежде всего надо зафиксировать порядок переменных $x_1, \ldots, x_n$. Пусть для определенности порядок будет $x_1 > x_2 > \ldots > x_n$. Тем не менее, мы можем взять любой порядок на переменных.

2. Теперь мы предполагаем порядок $x_1 > \ldots > x_n$ зафиксированным. Определим лексикографический порядок $\mathrm{Lex}(x_1, \ldots, x_n)$ следующим образом.

Пусть $m = x_1^{k_1} \ldots x_n^{k_n}$ и $m' = x_1^{k_1'} \ldots x_n^{k_n'}$ – два монома. В начале сравниваем k_1 и k_1'. Если $k_1 > k_1$, то $m > m'$. Если $k_1 < k_1'$, то $m < m'$. Если $k_1 = k_1'$, то мы переходим к сравнению k_2 и k_2' и повторяем алгоритм как и выше. В частности, $m > m'$ тогда и только тогда, когда существует $1 \leqslant j \leqslant n$ такой, что $k_1 = k_1', \ldots, k_{j-1} = k_{j-1}'$ и $k_j > k_j'$.

Примеры 117. Рассмотрим кольцо $F[x, y, z]$ и мономы $m_1 = x^2yz^4$, $m_2 = xy^3z$ и $m_3 = xyz^5$. Всего существует 6 способов упорядочить переменные x, y, z. Для каждого упорядочивания будет свой лексикографический порядок. Ниже написано как мономы будут сравниваться относительно всех шести порядков.

1. If $x > y > z$, then $m_1 > m_2 > m_3$.
2. If $x > z > y$, then $m_1 > m_3 > m_2$.
3. If $y > x > z$, then $m_2 > m_1 > m_3$.
4. If $y > z > x$, then $m_2 > m_3 > m_1$.
5. If $z > x > y$, then $m_3 > m_1 > m_2$.
6. If $z > y > x$, then $m_3 > m_1 > m_2$.

Замечания 118. Здесь я хочу перечислить некоторые свойства лексикографического порядка. Все мономы ниже от n переменных и мы используем какой-то лексикографический порядок.

1. Для любого монома $m \neq 1$, имеем $1 < m$.
2. Если m и m' – мономы такие, что m' делит m, то есть $m = m't$ для некоторого монома t, то $m' \leqslant m$. Если при этом $t \neq 1$, последнее неравенство является строгим.
3. Если m, t, s – некоторые мономы такие, что $m \leqslant t$, тогда $ms \leqslant ts$. Если при этом $m < t$, то $ms < ts$.

Утверждение 119. *Предположим у нас зафиксирован какой-то лексикографический порядок на мономах от n переменных и $m_1 > m_2 > \ldots > m_k > \ldots$ – строго убывающая цепочка мономов. Тогда эта цепочка конечная.*

Доказательство. Прежде всего мы можем переименовать переменные в $x_1, \ldots, x_n$ так, что они идут в порядке убывания $x_1 > x_2 > \ldots > x_n$. Теперь предположим, что существует бесконечная цепочка убывающих мономов. Давайте напишем явно степени всех мономов на картинке ниже

$$
\begin{array}{lcccc}
\text{Этап I} & x_1^{k_1(1)} & x_2^{k_2(1)} & \ldots & x_n^{k_n(1)} \\
& \vee\!\!/ & & & \\
& x_1^{k_1(2)} & x_2^{k_2(2)} & \ldots & x_n^{k_n(2)} \\
& \vee\!\!/ & & & \\
& \vdots & \vdots & & \vdots \\
& \vee\!\!/ & & & \\
& x_1^{k_1(r_1)} & x_2^{k_2(r_1)} & \ldots & x_n^{k_n(r_1)} \\
& \| & & & \\
& x_1^{k_1(r_1+1)} & x_2^{k_2(r_1+1)} & \ldots & x_n^{k_n(r_1+1)}
\end{array}
\qquad
\begin{array}{lcccc}
\text{Этап II} & x_1^{k_1} & x_2^{k_2(r_1)} & \ldots & x_n^{k_n(r_1)} \\
& \| & \vee\!\!/ & & \\
& x_1^{k_1} & x_2^{k_2(r_1+1)} & \ldots & x_n^{k_n(r_1+1)} \\
& \| & \vee\!\!/ & & \\
& \vdots & \vdots & & \vdots \\
& \| & \vee\!\!/ & & \\
& x_1^{k_1} & x_2^{k_2(r_2)} & \ldots & x_n^{k_n(r_2)} \\
& \| & \| & & \\
& x_1^{k_1} & x_2^{k_2(r_2+1)} & \ldots & x_n^{k_n(r_2+1)}
\end{array}
$$

В начале мы смотрим на степени по переменной x_1. По определению лексикографического порядка эти степени должны идти в невозрастающем порядке (возможно в нестрогом), то есть $k_1(1) \geqslant k_1(2) \geqslant \ldots$. Однако, это последовательность натуральных чисел, она не может быть строго убывающей бесконечно и рано или поздно стабилизируется на некотором числе r_1, а именно $k_1(r_1) = k_1(r_1+1) = \ldots$. Начиная с этого момента все степени у переменной x_1 будут одинаковыми и равными, скажем, k_1.

Теперь посмотрим на степени по переменной x_2 начиная с r_1 монома: $m_{r_1} > m_{r_1+1} > \ldots$. Так как степени при x_1 уже не меняются и равны, то мы должны иметь $k_2(r_1) \geqslant k_2(r_1+1) \geqslant \ldots$. Опять, это невозрастающая цепочка натуральных чисел, а потому она когда-нибудь стабилизируется. То есть найдется номер $r_2 > r_1$ такой, что $k_2(r_2) = k_2(r_2+1) = \ldots$. Обозначим эту общую степень по переменной x_2 через k_2. Значит для всех мономов m_i с условием $i \geqslant r_2$, степени при x_1 и x_2 будут равны k_1 и k_2 соответственно.

Повторяя этот процесс, мы найдем номер $r_3 > r_2$, начиная с которого перестают меняться степени x_3. Потом находим $r_4 > r_3$ начиная с которого перестают меняться степени x_4 и так далее. В итоге мы найдем номер r_n такой, что начиная с него все степени всех переменных должны быть одинаковыми. Но тогда начиная с этого номера цепочка мономов m_i не может быть строго убывающей. Полученное противоречие завершает доказательство. □

Замечание 120. Существует популярная ошибка, о которой я хочу поговорить. Мы только что доказали, что не существует бесконечной строго убывающей цепочки мономов. Однако, это не значит, что меньше данного монома у нас лишь конечное число мономов. Действительно, давайте рассмотрим $\mathbb{Q}[x,y]$ с порядком $x > y$ и соответствующим лексикографическим упорядочиванием. Тогда существует бесконечно много мономов меньше, чем x^2. Действительно, любой моном xy^n строго меньше, чем x^2. Однако, когда мы пытаемся построить убывающую цепочку, нам надо выбрать конкретный xy^n, тогда мы получаем цепочку

$$x^2 > xy^n > xy^{n-1} > \ldots > xy > x > y^m > y^{m-1} > \ldots > y > 1$$

Обратите внимание, что в ней мы пропустили бесконечное число членов между x^2 и xy^n, а так же бесконечное число членов между x и y^m. Таким образом убывающие цепочки начинающиеся с x^2 могут быть сколь угодно большой длины, но обязательно конечны.

8.3 Редукция

Теперь после разговора о порядках, давайте определим процедуру редукции. Мы это сделаем в два шага: в начале определим элементарную редукцию, а потом уже и общий случай. Давайте напомню контекст. У нас зафиксировано некоторое поле F, кольцо многочленов $F[x_1,\ldots,x_n]$, и произвольный лексикографический порядок на мономах от n переменных.

Определение 121. Предположим F – поле, мы фиксировали лексикографический порядок на мономах в $F[x_1,\ldots,x_n]$ и $f \in F[x_1,\ldots,x_n]$ – произвольный ненулевой многочлен. Тогда многочлен f может быть записан в виде

$$f = c_1m_1 + c_2m_2 + \ldots + c_km_k, \quad c_i \in F,\ m_i \text{ – мономы такие, что } m_1 > m_2 > \ldots > m_k$$

Терм c_1m_1 называется старшим термом многочлена f и будет обозначаться $T(f)$. Моном m_1 называется старшим мономом f и обозначается $M(f)$. Коэффициент c_1 называется старшим коэффициентом многочлена f и будет обозначаться $C(f)$. По определению $T(f) = C(f)M(f)$. Часть $c_2m_2 + \ldots + c_km_k$ называется хвостом f и будет обозначаться f_0. Таким образом, любой многочлен f может быть записан как $f = T(f) + f_0$.

Определение 122. Предположим $g \in F[x_1,\ldots,x_n]$ – ненулевой многочлен и $f \in F[x_1,\ldots,x_n]$ – произвольный многочлен. Предположим

$$f = c_1m_1 + \ldots + c_im_i + \ldots + c_km_k, \quad c_i \in F,\ m_i \text{ – мономы такие, что выполнено } m_1 > m_2 > \ldots > m_k$$

и

$$g = C(g)M(g) + g_0 = T(g) + g_0$$

Фиксируем моном $m = m_i$ в многочлене f и предположим, что m делится на старший моном g, то есть $m = tM(g)$. Мы определим элементарную редукцию f относительно g следующим образом

$$f \xrightarrow{g} f' = f - \frac{c_i}{C(g)}tg$$

Многочлен f' – это результат элементарной редукции.

Если описать редукцию по простому, то она действует следующим образом: мы находим в f моном m_i, который делится на $M(g)$ и заменяем его на хвост g умноженный на $-c_i m_i/T(g)$.

Пример 123. Рассмотрим кольцо $\mathbb{Q}[x,y,z]$, $f = xyz$, $g_1 = xy - z$, и $g_2 = yz - 1$. Порядок будет произвольным лексикографическим. Тогда

$$f \xrightarrow{g_1} xyz - z(xy - z) = z^2, \quad \text{или} \quad f \xrightarrow{g_2} xyz - x(yz - 1) = x$$

Определение 124. Предположим $G \subseteq F[x_1, \ldots, x_n] \setminus \{0\}$ – некоторое множество многочленов и $f, f' \in F[x_1, \ldots, x_n]$ – многочлены. Мы скажем, что f редуцируется к f' с помощью G, если существует конечная последовательность элементарных редукций как ниже[16]

$$f \xrightarrow{g_1} f_1 \xrightarrow{g_2} f_2 \xrightarrow{g_3} \ldots \xrightarrow{g_k} f_k = f' \quad \text{где } g_i \in G$$

Будем писать в этом случае $f \overset{G}{\rightsquigarrow} f'$.

Если многочлен f' уже не редуцируем никаким $g \in G$, будем говорить, что f' является остатком f относительно G.

Замечания 125.

1. Многочлен f' не редуцируем никаким $g \in G$ тогда и только тогда, когда каждый моном f' не делится ни на какой $M(g)$ для $g \in G$.

2. Важно отметить, что вообще говоря остаток не определен однозначно. Элементарные редукции f относительно членов G в разном порядке могут привести к разным остаткам. Вот пример подобного. Пусть $\mathbb{Q}[x,y,z]$ и фиксирован лексикографический порядок для $x > y > z$. Положим $f = xyz$, $g_1 = xy - 1$, $g_2 = yz - 1$, и $G = \{g_1, g_2\}$. Тогда,

$$f \xrightarrow{g_1} xyz - z(xy - 1) = z \quad \text{и} \quad f \xrightarrow{g_2} xyz - x(yz - 1) = x$$

   Тогда по определению $f \overset{G}{\rightsquigarrow} z$ и $f \overset{G}{\rightsquigarrow} x$. Более того, многочлены z и x не редуцируемы с помощью G. Значит, это два разных остатка f относительно G.

Как мы увидели в общем случае остаток многочлена f относительно G не единственный. Грубо говоря, такое происходит потому что множество G было выбрано не удачно. Таким образом можно выделить «хорошие» множества, для которых остаток будет получаться однозначным. Такая процедура ведет к понятию базиса Грёбнера.

Определение 126 (Базис Грёбнера)**.** Предположим F – некоторое поле, $G \subseteq F[x_1, \ldots, x_n] \setminus \{0\}$, и у нас зафиксирован какой-то лексикографический порядок.[17] Будем говорить, что G является базисом Грёбнера если для любого $f \in F[x_1, \ldots, x_n]$ все его остатки совпадают.

Давайте поговорим о еще одном важном вопросе связанном с редукцией. Предположим нам дали многочлен f и множество G. Если f редуцируем относительно G, то мы можем сделать элементарную редукцию и получить f_1. Теперь если f_1 тоже редуцируем, то мы можем провести элементарную редукцию и получить многочлен f_2 и так далее. Вопрос в том остановится ли этот процесс когда-либо. Оказывается, что ответ на этот вопрос положительный, как показывает утверждение 130.

Примеры 127. Мы с вами познакомимся со способами проверки является ли множество G базисом Грёбнера. Сейчас же я хочу привести пару примеров без доказательства, просто потому что мы пока не готовы это объяснить.

1. Для любого кольца многочленов $F[x_1, \ldots, x_n]$ с произвольным лексикографическим порядком множество $G = \{g\}$ состоящее из одного ненулевого многочлена всегда является базисом Грёбнера.

2. Пусть $F[x,y,z,w]$ и мы используем какой-нибудь лексикографический порядок. Тогда множество $G = \{xy - 1, zw + 1\}$ является базисом Грёбнера. Это происходит в силу того, что старшие мономы элементов G взаимно просты.

[16] Многочлены $g_1, \ldots, g_k$ не обязаны быть различными.

[17] Я хочу отметить, что понятие базиса Грёбнера сильно зависит от выбранного порядка. Если мы изменим порядок на переменных, то множество G может стать базисом Грёбнера или наоборот перестанет им быть.

Определение 128. Пусть F – некоторое поле и фиксирован некоторый лексикографический порядок на мономах от n переменных. Как и раньше, каждый многочлен $f \in F[x_1, \ldots, x_n]$ может быть представлен в виде

$$f = c_1 m_1 + c_2 m_2 + \ldots + c_k m_k, \quad c_i \in F,\ m_i \text{ – мономы такие, что } m_1 > m_2 > \ldots > m_k$$

Мы обозначим i-ый по старшинству моном m_i через $M_i(f)$. В частности $M_1(f)$ – это старший моном f, $M_2(f)$ – это второй по старшинству моном в f и так далее. Обратите внимание, что i-ый по старшинству моном не обязан существовать в f, это происходит если f содержит меньше i мономов.

Утверждение 129. *Пусть F – некоторое поле, мы работаем с многочленами $F[x_1, \ldots, x_n]$, и некоторый лексикографический порядок задан. Пусть $f, f', g \in F[x_1, \ldots, x_n]$ такие, что $f \xrightarrow{g} f'$ и $M_1(f) = M_1(f'), \ldots, M_{k-1}(f) = M_{k-1}(f')$, и пусть мономы $M_k(f)$ и $M_k(f')$ существуют. Тогда, $M_k(f) \geqslant M_k(f')$.*

Доказательство. Предположим, что $f = c_1 m_1 + \ldots + c_{k-1} m_{k-1} + c_k m_k + \ldots + c_s m_s$, где $c_i \in F$ и m_i – мономы расположенные в убывающем порядке. Многочлен f' получен из f с помощью одной элементарной редукции. Это означает, что есть какой-то моном m_i делящийся на $M(g)$, который мы заменили на линейную комбинацию более младших мономов в f'. По предположению первые $k-1$ моном в f и f' совпадают. А это значит, что ни один из них не был редуцирован. То есть $i \geqslant k$. Если $i > k$ то, k-ый моном в f' такой же как и k-ый моном в f. Это значит, что в этом случае $M_k(f) = M_k(f')$. Если $i = k$, то мы заменили m_k на линейную комбинацию более младших мономов. Например результат может выглядеть так

$$f \longleftrightarrow m_1 \quad \ldots \quad m_{k-1} \quad m_k \qquad m_{k+1} \qquad \ldots \quad m_s$$

$$f' \longleftrightarrow m_1 \quad \ldots \quad m_{k-1} \qquad m'_k \quad m'_{k+1} \quad m'_{k_2} \quad \ldots \qquad m'_{s'}$$

Но тогда моном $m'_k = M_k(f')$ строго младше монома $m_k = M_k(f)$, а это означает что надо. □

Утверждение 130. *Пусть F – некоторое поле, мы работаем с кольцом $F[x_1, \ldots, x_n]$, на котором зафиксирован какой-то лексикографический порядок. Тогда для любого многочлена $f \in F[x_1, \ldots, x_n]$ и любого подмножества $G \subseteq F[x_1, \ldots, x_n] \setminus \{0\}$, любая последовательность элементарных редукций f с помощью G конечна.*

Доказательство. Предположим, что верно противное и найдется бесконечная последовательность элементарных редукций.

$$f \xrightarrow{g_1} f_1 \xrightarrow{g_2} f_2 \xrightarrow{g_3} \ldots \xrightarrow{g_k} f_k \xrightarrow{g_{k+1}} \ldots$$

Давайте построим бесконечную убывающую цепочку мономов, что и даст нужное противоречие. Посмотрим на цепочку старших мономов $M_1(f), M_1(f_1), M_1(f_2), \ldots$. Применяя утверждение 129 в случае $k = 1$, мы видим, что $M_1(f) \geqslant M_1(f_1) \geqslant M_1(f_2) \geqslant \ldots$. По утверждению 119, эта цепочка обязана стабилизироваться, то есть найдется r_1 такое, что $M_1(f_{r_1}) = M_1(f_{r_1+1}) = \ldots$. Значит начиная с номера r_1 все редукции имеют одинаковый старший моном, обозначим его через m_1. Так как последовательность редукций бесконечно, у нас должен существовать второй по старшинству моном во всех редукциях с момента r_1. Опять воспользуемся утверждением 129 но теперь для случая $k = 2$. Мы получим $m_1 > M_2(f_{r_1}) \geqslant M_2(f_{r_1+1}) \geqslant \ldots$. Эта убывающая цепочка мономов должна стабилизироваться по утверждению 119. Значит найдется номер $r_2 > r_1$ такой, что $m_1 > M_2(f_{r_2}) = M_2(f_{r_2+1}) = \ldots$. То есть начиная с номера r_2 все редукции имеют одинаковый старший моном m_1 и одинаковый второй по старшинству моном, который обозначим через m_2. В итоге у нас получилась цепочка мономов $m_1 > m_2$. Так как цепочка бесконечная, то у нас обязательно существует третий моном во всех редукциях с номера r_2.

Значит мы как и выше можем повторить это рассуждение для третьего по величине монома. Потом для четвертого и так далее. В результате мы построим цепочку мономов $m_1 > m_2 > m_3 > \ldots > m_s > \ldots$. Построенная цепочка противоречит утверждению 119, что заканчивает доказательство. □