Дискретная математика

Алгебраические структуры

Константин Чухарев

Осень 2026

Зачем структуры

> *Если я не могу объяснить это проще, значит, я сам ещё не понял.*
>
> ***— Ричард Фейнман***

Одна операция и много лиц

На часах три часа дня, а мы прибавляем десять. Три плюс десять — тринадцать, но на циферблате это час дня.

Повернём квадрат на четверть оборота — он совпадёт с собой. Отражение относительно диагонали тоже оставляет квадрат на месте.

> Общего между циферблатом и квадратом на первый взгляд нет. Но и там, и там есть операция — действие, которое можно выполнять и отменять.

Главный вопрос

Какие правила делают набор действий структурой?

Почему одна и та же структура появляется и в остатках, и в симметриях, и в защите данных?

> Ответ строится лестницей. Полугруппа позволяет накапливать, моноид — начинать накопление, группа — отменять. Кольцо соединяет две операции, поле — позволяет делить.

Одна маленькая идея — и на ней держатся вычислимость, криптография и коды.

Бинарная операция

Два значения внутрь, одно наружу

Повсюду одно и то же: два элемента на входе, один на выходе.

- Семь плюс пять — двенадцать.
- ка и ша — каша.
- $1 \oplus 1 - 0$.
- $\{1, 2\}$ и $\{2, 3\} - \{1, 2, 3\}$.

Определение 1 (Бинарная операция)

Бинарная операция на множестве A — функция

$$f : A \times A \to A.$$

Паре (a, b) она сопоставляет результат $a \star b$. Требование $f(a, b) \in A$ называют **замкнутостью**.

Четыре свойства

Операция обладает свойствами, и они определяют структуру.

Определение 2

- **Ассоциативность**: $(a \star b) \star c = a \star (b \star c)$ — скобки не важны.
- **Коммутативность**: $a \star b = b \star a$ — порядок не важен.
- **Нейтральный элемент**: существует e с $a \star e = e \star a = a$.
- **Обратный элемент**: для каждого a найдётся a^{-1} с $a \star a^{-1} = e$.

Пример

- Сложение ассоциативно и коммутативно.
- Вычитание не ассоциативно: $(10 - 3) - 2 = 5$, а $10 - (3 - 2) = 9$.
- На $\mathbb{N}$ у сложения нет обратного для 3: $3 + x = 0$ неразрешимо.

Замкнутость встроена

Результат никогда не покидает множество, и операцию можно повторять сколько угодно. Без замкнутости свернуть список в одно значение было бы негде.

> Вычитание на $\mathbb{N}$ ломается: $2 - 3 = -1$, а -1 не натуральное. Деление ещё хуже: $\frac{1}{0}$ не определено. Такие правила — частичные функции, а не операции.

Таблица Кэли

На конечном множестве операцию можно записать одной таблицей.

Определение 3 (Таблица Кэли)

Квадрат, где строки и столбцы подписаны элементами, а в клетке — результат. Строка a, столбец b, в пересечении — $a \star b$.

Пример

XOR на $\{0, 1\}$:

$\star$	0	1
0	0	1
1	1	0

0 — нейтральный элемент, каждый бит обратен себе. Это уже группа.

Полугруппа и моноид

Fold: накопление без отмены

Свернуть список из тысячи чисел в одно — **fold**. Аккумулятор растёт, отмены в нём нет.

Определение 4 (Полугруппа)

Множество S с бинарной операцией $\star$ — **полугруппа**, если операция ассоциативна:

$$(a \star b) \star c = a \star (b \star c).$$

Полугруппа — место, где можно накапливать, но нельзя отменять. Обратных элементов здесь нет по определению.

Моноид: есть с чего начать

Добавим элемент, который ничего не меняет.

Определение 5 (Моноид)

Полугруппа — **моноид**, если в ней есть **нейтральный элемент** e:

$$e \star a = a \star e = a.$$

Чтобы свернуть список операцией fold, нужен стартовый аккумулятор. В моноиде аккумулятор — нейтральный элемент: свёртка пустого списка даёт e. В полугруппе без нейтрального стартовать не с чего.

Нейтральный элемент единственный

Теорема 1

Нейтральный элемент, когда он существует, единственный.

Доказательство

Если их два — e и e' — то $e = e \star e' = e'$.

Тот же приём встретится, когда появятся сложение и умножение вместе.

Примеры

Пример

- Натуральные числа со сложением — полугруппа, но не моноид (нет нуля).
- Строки Σ^* с конкатенацией — моноид: нейтральна пустая строка.
- $\mathbb{N}_0$ со сложением — моноид, нейтрален 0.
- Преобразования состояний автомата с композицией — моноид.

Группа: обратимость

> *Симметрия — это идея о том, что фигуру можно преобразовать, и она останется собой.*
>
> ***— Герман Вейль***

Обратимое преобразование

Любое отображение множества в себя формально «переводит фигуру в себя». Но постоянное отображение стягивает квадрат в точку и уничтожает форму.

> Дело в обратимой стороне преобразования. Повернули — найдётся поворот, возвращающий на место. Именно пара «преобразование и его отмена» превращает набор в группу.

Определение группы

Определение 6 (Группа)

Множество G с операцией $\cdot$ — **группа**, если:

- **Замкнутость**: $a \cdot b \in G$ для всех $a, b \in G$.
- **Ассоциативность**: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- **Нейтральный элемент**: существует e с $e \cdot a = a \cdot e = a$.
- **Обратный элемент**: для каждого a существует a^{-1} с $a \cdot a^{-1} = e$.

Второе условие — из полугрупп, третье — из моноидов. Новое — четвёртое, обратимость.

Симметрии квадрата: D_4

Перечислим преобразования, переводящие квадрат в себя. Четыре поворота: на 0, 90, 180, 270 градусов. Четыре отражения: две средние линии и две диагонали. Итого восемь преобразований.

r — поворот на 90 градусов, s — отражение относительно вертикальной оси. $a \cdot b$ понимаем как «сначала b, затем a».

e	r	r^2	s
e	r	r^2	s
r	r^2	r^3	rs
r^2	r^3	e	$r^2 s$
s	$r^3 s$	$r^2 s$	e

Латинский квадрат

Каждая строка и столбец таблицы Кэли содержат каждый элемент ровно один раз.

Теорема 2

Это свойство латинского квадрата — прямое следствие обратимости.

Доказательство

Наличие обратного позволяет сокращать. Уравнение $a \cdot x = b$ имеет единственное решение $x = a^{-1} \cdot b$. Если бы обратного у a не было, произведение $a \cdot x$ могло бы повторяться.

Не коммутативна

Таблица D_4 не симметрична относительно диагонали.

Пример

$s \cdot r = r^3 s$, а $r \cdot s = rs$. Повернуть и отразить — одно, отразить и повернуть — другое.

Группа, где порядок сомножителей важен, — **неабелева**. Абелева группа — коммутативная: $a \cdot b = b \cdot a$.

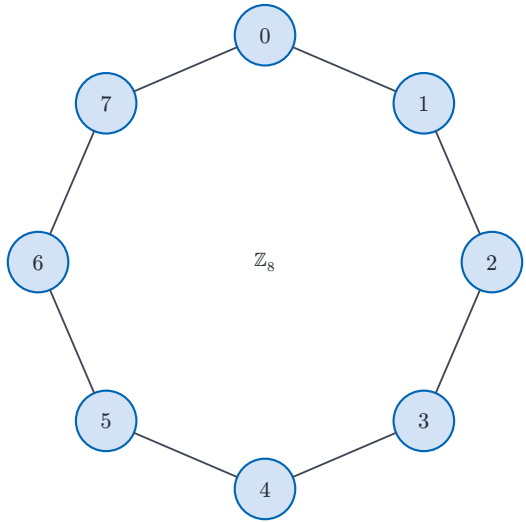
Сложение остатков

$\mathbb{Z}_n = \{0, 1, ..., n-1\}$ со сложением по модулю n — группа. Ноль — нейтральный элемент, обратный к a — это $n - a$.

Определение 7 (Образующий и циклическая группа)

Образующий — элемент, чьи повторные применения дают всё множество. Группа с образующим — **циклическая**. В $\mathbb{Z}_n$ образующим служит единица.

Образующая в $\mathbb{Z}_8$



Степени элемента

В конечной группе список $g, g^2, g^3, \ldots$ обязан повториться.

Определение 8 (Порядок элемента)

Порядок элемента g — наименьший показатель, дающий нейтральный элемент. Порядок группы — число её элементов. Это разные величины, и порядок элемента делит порядок группы.

Пример

В $\mathbb{Z}_5^*$ порядок 4 равен 2: $4^2 = 16 \equiv 1$. В D_4 поворот r имеет порядок 4, каждое отражение — порядок 2. Нейтральный элемент имеет порядок 1.

Подгруппы и теорема Лагранжа

Подгруппа

В $\mathbb{Z}_{12}$ возьмём чётные числа $\{0, 2, 4, 6, 8, 10\}$. Сумма двух чётных вычетов снова чётна, противоположный тоже чётен. Внутри $\mathbb{Z}_{12}$ сидит своя маленькая группа на шесть элементов.

Определение 9 (Подгруппа)

Непустое подмножество $H \subseteq G$ — **подгруппа** группы G, если:

- замкнуто относительно операции: $a \cdot b \in H$;
- замкнуто относительно обратного: $a^{-1} \in H$.

Нейтральный элемент бесплатно

В определении подгруппы нет ни слова про нейтральный элемент. Он появляется сам: если H непусто, возьмём $a \in H$, и $a \cdot a^{-1} = e \in H$.

Замкнутость относительно операции сама по себе не делает подгруппу. В $\mathbb{Z}$ неотрицательные числа замкнуты относительно сложения, но обратный ко 2 равен -2 — его в отобранном множестве нет. В конечной группе одной замкнутости достаточно.

Смежные классы

Раз подгруппа живёт внутри группы, попробуем её сдвинуть.

Определение 10 (Смежный класс)

Левый смежный класс подгруппы H по элементу a: $aH = \{a \cdot h \mid h \in H\}$. В аддитивной записи $a + H = \{a + h \mid h \in H\}$.

Смежные классы разбивают группу на части одинакового размера. Два разных класса не имеют общих элементов, а вместе покрывают всю группу.

Разбиение $\mathbb{Z}_{12}$ по $H = \{0, 4, 8\}$

Смежный класс	Элементы	Число элементов
$0 + H$	$\{0, 4, 8\}$	3
$1 + H$	$\{1, 5, 9\}$	3
$2 + H$	$\{2, 6, 10\}$	3
$3 + H$	$\{3, 7, 11\}$	3

Каждый класс из трёх элементов, классов ровно четыре: $12 = 4 \cdot 3$. Дальнейшие сдвиги повторяют уже найденные классы.

Теорема Лагранжа

Теорема 3 (Теорема Лагранжа)

Пусть G — конечная группа, H — её подгруппа. Тогда порядок $|H|$ делит порядок $|G|$.

Доказательство

Разобьём G на попарно непересекающиеся смежные классы одинакового размера.

Отображение $h \mapsto a \cdot h$ переводит H в aH взаимно однозначно. Значит $|aH| = |H|$ для любого a.

Разные классы не пересекаются: если aH и bH имеют общий элемент, они совпадают целиком.

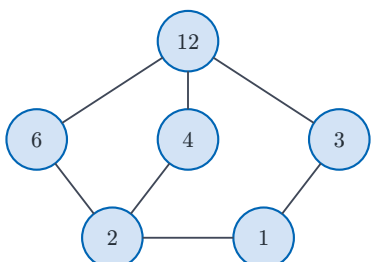
Каждый элемент лежит в своём классе, поэтому G — объединение непересекающихся классов. Если классов k, то $|G| = k \cdot |H|$, и $|H|$ делит $|G|$.

Следствия Лагранжа

Следствие 1 (Порядок элемента делит порядок группы)

Для любого элемента g конечной группы G порядок $\mathrm{ord}(g)$ делит $|G|$.

Степени g образуют подгруппу, а её порядок по Лагранжу делит $|G|$. Значит в группе порядка 6 нет элемента порядка 4 — ведь 4 не делит 6.



Действие группы на множестве

Группа действует

Пронумеруем вершины квадрата $1, 2, 3, 4$ и раскрасим в два цвета. Повернём квадрат — раскраска повернулась вместе с ним. Если одну раскраску можно получить из другой поворотом, они считаются одной.

Определение 11 (Действие группы)

Отображение $G \times X \to X$ — **действие** группы G на множестве X, если:

- $e \cdot x = x$ для всех $x \in X$;
- $(gh) \cdot x = g \cdot (h \cdot x)$ для всех $g, h \in G$, $x \in X$.

Вторая аксиома — главная

Вторая аксиома согласует последовательность преобразований с умножением в группе. Сначала подействовать h, потом g — то же, что подействовать произведением gh.

Для фиксированного g отображение $x \to g \cdot x$ — биекция X на себя. Элемент g^{-1} отменяет действие g. Каждый элемент группы действует как перестановка множества X.

Орбита и стабилизатор

Определение 12

Орбита элемента x: $G \cdot x = \{g \cdot x \mid g \in G\}$ — все точки, куда можно перевести x.

Стабилизатор точки x: $\mathrm{Stab}(x) = \{g \in G \mid g \cdot x = x\}$ — подгруппа, оставляющая x на месте.

Пример

Повороты квадрата на вершинах $\{1, 2, 3, 4\}$. Орбита вершины 1: $\{1, 2, 3, 4\}$ — вся четвёрка. Стабилизатор вершины 1 тривиален: на месте её держит только нейтральный элемент.

Счёт с точностью до симметрии

Раскрасок вершин квадрата в два цвета — $2^4 = 16$. Каждый поворот переводит раскраску в другую, так что группа действует на раскрасках. Орбиты — типы раскрасок с точностью до поворота.

Орбиты — классификация: одинаковое собрано в один класс. Число орбит — ответ на вопрос «сколько с точностью до симметрии».

В примере с квадратом орбит шесть: $1 + 1 + 4 + 4 + 2 + 4 = 16$. Лемма Бёрнсайда — среднее число неподвижных точек — даёт 6. Её полный разбор — в лекции о комбинаторике.

Кольцо: две операции

Умножение по модулю 6

На циферблате с шестью делениями считать можно по-разному. $2 \cdot 3 = 6$, а 6 на таком циферблате — ноль. Два элемента, отличных от нуля, дали в произведении ноль.

> У целых чисел такое невозможно: если произведение равно нулю, то хотя бы один сомножитель нулевой. По модулю 6 это правило ломается.

Определение кольца

Сложение — как в группе, умножение — как в полугруппе, связывает их дистрибутивность.

Определение 13 (Кольцо)

Множество R с $+$ и $\cdot$ — **кольцо**, если:

- По сложению R — абелева группа (нейтральный 0, обратный $-a$).
- По умножению R — полугруппа.
- Умножение дистрибутивно: $a \cdot (b + c) = a \cdot b + a \cdot c$.

Умножение свободно

Умножение в кольце не обязано быть коммутативным. Не обязано иметь нейтральный элемент. Не обязано иметь обратный для каждого элемента.

> Именно последняя свобода превращает кольцо из «поля» в «почти поле». Вся арифметика на месте, кроме главного — умения делить на любое ненулевое число.

Делители нуля

Определение 14 (Делитель нуля)

Делитель нуля — ненулевой элемент a кольца, для которого найдётся ненулевой b с $a \cdot b = 0$.

Пример

В $\mathbb{Z}_6$: $2 \cdot 3 = 6 \equiv 0 (\mathrm{mod}\, 6)$, и 2, и 3 отличны от нуля. $3 \cdot 4 = 12 \equiv 0$, значит и 4 — делитель нуля. Обратного к 2 нет: $2 \cdot a$ равно 0, 2 или 4, но не 1.

Делитель нуля необратим

Теорема 4

Делитель нуля не может иметь обратного по умножению.

Доказательство

Если $a \cdot b = 0$ при $a, b \neq 0$ и у a есть обратный a^{-1}, то, умножив на a^{-1}, получаем $b = 0$ — противоречие.

Кольцо тем дальше от поля, чем больше в нём делителей нуля. В $\mathbb{Z}$ их нет вовсе, в $\mathbb{Z}_6$ они почти у каждого ненулевого элемента.

Булево кольцо

$B = \{0, 1\}$ с $\oplus$ (сложение) и $\wedge$ (умножение) — кольцо.

Пример

$\oplus$ — абелева группа: нейтрален 0, каждый элемент обратен себе ($a \oplus a = 0$). $\wedge$ ассоциативно и коммутативно, нейтрален 1. Дистрибутивность: $1 \wedge (b \oplus c) = b \oplus c = (1 \wedge b) \oplus (1 \wedge c)$.

Кольцо, хотя ни сложение, ни умножение здесь не похожи на числовые двойники. Каждый элемент идемпотентен: $a \wedge a = a$.

Поле: можно делить

Деление становится законным

В кольце вычетов по модулю 6 у элемента 2 нет обратного. Стоит потребовать обратный у каждого ненулевого элемента — и деление законно.

Определение 15 (Поле)

Множество F с $+$ и $\times$ — **поле**, если:

- $(F, +)$ — абелева группа с нейтральным 0;
- $(F \setminus \{0\}, \times)$ — абелева группа с нейтральным 1;
- $a \times (b + c) = a \times b + a \times c$.

Поле $\mathbb{Z}_7$

a	1	2	3	4	5	6
a^{-1}	1	4	5	2	3	6

Пример

$2 \cdot 4 = 8 = 1 (\mathrm{mod}\, 7)$. $3 \cdot 5 = 15 = 1 (\mathrm{mod}\, 7)$. $6 \cdot 6 = 36 = 1 (\mathrm{mod}\, 7)$. У каждого ненулевого элемента есть обратный, значит $\mathbb{Z}_7$ — поле.

Порядок поля и простое поле

Число элементов поля — его **порядок**. $\mathbb{Z}_p$ для простого p — **простое поле** порядка p.

Для простого p каждое a от 1 до $p-1$ взаимно просто с p. Значит у a есть обратный по модулю p, и кольцо $\mathbb{Z}_p$ — поле. По модулю составного — нет.

В поле нет делителей нуля

Теорема 5

В поле нет делителей нуля.

Доказательство

Если $a \cdot b = 0$ и $a \neq 0$, умножаем на a^{-1}: получаем $b = 0$. Произведение двух ненулевых элементов в поле никогда не даёт нуль.

В $\mathbb{Z}_6$ это рушится: $2 \cdot 3 = 0$, а $2 \neq 0$ и $3 \neq 0$.

Деление — умножение на обратный

Деление в поле — это умножение на обратный элемент. Вместо деления a на b умножаем a на b^{-1}. Вся арифметика поля задаётся двумя операциями: $+$ и $\times$.

Байт из восьми битов принимает 256 значений. Но 256 — не простое, и $\mathbb{Z}_{256}$ полем не становится. Поле с 256 элементами существует — и это идея Галуа.

Конечные поля

> *Алгебра щедра: часто она даёт больше, чем у неё просят.*
>
> **— *Жан д'Аламбер***

Хочется делить байты

Над байтами хочется выполнять арифметику: складывать, умножать, делить. Деление возможно только там, где каждый ненулевой элемент обратим, то есть в поле. Но поля вычетов $\mathbb{Z}_p$ имеют ровно p элементов, и p обязано быть простым.

> $256 = 2^8$ полем по модулю 256 не становится: в нём есть делители нуля. Поле с 256 элементами существует — и это поле Галуа $\mathrm{GF}(2^8)$.

Идея Галуа

Взять простое поле $\mathbb{Z}_p$ и присоединить корень многочлена, который над ним не раскладывается.

Определение 16 (Неприводимый многочлен)

Многочлен $f(x)$ степени m с коэффициентами из $\mathbb{Z}_p$ — **неприводимый** над $\mathbb{Z}_p$, если его нельзя представить произведением двух многочленов меньших степеней.

Объявим $f(x) = 0$ и рассмотрим остатки от деления многочленов на f. Остатков ровно p^m — все многочлены степени меньше m. Сложение — покоэффициентно, умножение — с приведением по модулю f.

Поле $\mathrm{GF}(p^m)$

Определение 17 (Конечное поле)

Поле K — **конечное**, если множество его элементов конечно. Число элементов — **порядок** поля, обозначается $|K|$. Порядок конечного поля обязан быть степенью простого числа.

Запись $\mathrm{GF}(p^m) = \frac{\mathbb{Z}_{p[x]}}{f(x)}$ — та же конструкция, что $\mathbb{Z}_p = \frac{\mathbb{Z}}{p}$. Только роль числа p играет многочлен. Арифметика: сложить — сложить коэффициенты, умножить — перемножить и взять остаток.

Почему нужна неприводимость

Если f раскладывается в произведение $f = gh$, то по модулю f произведение gh равно нулю. Появляются делители нуля, и делить нельзя.

Доказательство

Раз f неприводим, то ненулевой многочлен $a(x)$ степени меньше m взаимно прост с f. Расширенный алгоритм Евклида даёт $u(x)a(x) + v(x)f(x) = 1$. По модулю f получаем $u(x)a(x) = 1$, и $u(x)$ — обратный к $a(x)$.

Поле $\mathrm{GF}(4)$

$f(x) = x^2 + x + 1$ неприводим над $\mathbb{Z}_2$: $f(0) = 1$, $f(1) = 1$. Остатки — $0, 1, x, x+1$. Обозначим $\alpha = x$. Правило поля: $\alpha^2 + \alpha + 1 = 0$, то есть $\alpha^2 = \alpha + 1$.

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

Степени α

$\times$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

Степени α: $\alpha^1 = \alpha$, $\alpha^2 = \alpha + 1$, $\alpha^3 = 1$. Порядок α равен трём, и степени пробегают все три ненулевых элемента поля.

Примитивный элемент

Ненулевые элементы $\mathrm{GF}(q)$ образуют по умножению группу $\mathrm{GF}(q)^*$ порядка $q-1$.

Определение 18 (Примитивный элемент)

Примитивный элемент — образующий циклической группы $\mathrm{GF}(q)^*$. Его степени $g^1, \ldots, g^{q-1}$ пробегают все ненулевые элементы поля.

В $\mathrm{GF}(4)$ примитивен α: порядок $3 = q-1$. Не любой элемент примитивен: в $\mathrm{GF}(2^8)$ элемент x имеет порядок 51, а $x+1$ — порядок $255 = 2^8 - 1$. Поиск примитивного элемента — перебор степеней.

Байты и AES

Над $\mathbb{Z}_2$ берут $f(x) = x^8 + x^4 + x^3 + x + 1$. Остатки от деления на него — ровно байты.

Каждый байт — коэффициенты многочлена степени меньше восьми. Сложение байтов — просто XOR. В этом поле живут шифр AES и коды Рида—Соломона.

Гомоморфизм и изоморфизм

Когда структуры одинаковы

$\mathbb{Z}_7$ и вращения семиугольника — разные множества. Но каждая несёт бинарную операцию, и обе подчиняются одним правилам.

Сравнивать по числу элементов нельзя: $\mathbb{Z}_4$ и $\mathbb{Z}_2 \times \mathbb{Z}_2$ имеют по четыре элемента. Но их таблицы различаются — в первой есть элемент порядка четыре, во второй нет. Решение — сопоставить элементы так, чтобы операции согласовались.

Дни недели

Пусть сегодня среда, каким будет день через сто дней? Сто — четырнадцать недель и два дня, ответ — пятница. Сто можно сократить: остаток от деления на семь равен двум.

Пример

Произведение двенадцати и девяти: $108 \equiv 3 \pmod 7$. Сведём множители: $12 \equiv 5$, $9 \equiv 2$, и $5 \cdot 2 = 10 \equiv 3$. Результат совпал.

Гомоморфизм

Отображение $\varphi : \mathbb{Z} \to \mathbb{Z}_7$ переводит число в остаток от деления на семь.

Определение 19 (Гомоморфизм)

Отображение $\varphi : A \to B$ — **гомоморфизм**, если для всех x, y:

$$\varphi(x \star y) = \varphi(x) \cdot \varphi(y).$$

Если есть нейтральные элементы, гомоморфизм сохраняет и их: $\varphi(e_A) = e_B$.

Операции могут быть несколькими, как в кольце. Тогда отображение обязано сохранять каждую.

«Сохранять» здесь получает точный смысл: вычислить в исходной структуре и перейти в новую — либо перейти в новую и вычислить — одно и то же.

Ядро

Элементы с нулевым остатком, то есть кратные семи, образуют **ядро**.

Определение 20 (Ядро)

Ядро гомоморфизма $\varphi : G \to H$ — множество тех $x \in G$, для которых $\varphi(x)$ равен нейтральному элементу H.

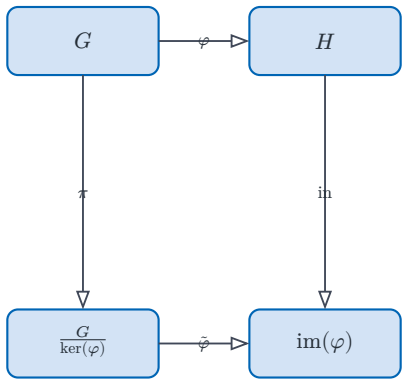
Ядро — подгруппа группы G, притом особая: оно нормально. Смежные классы по ядру устроены так же, как элементы образа. Для $\varphi : \mathbb{Z} \to \mathbb{Z}_7$ ядро — это $7\mathbb{Z}$, и факторгруппа $\frac{\mathbb{Z}}{7\mathbb{Z}}$ изоморфна $\mathbb{Z}_7$.

Подгруппа H нормальна, если $gHg^{-1} = H$ для всех g: левые и правые смежные классы совпадают. Умножение смежных классов через представителей корректно ровно для нормальных подгрупп, и тогда классы образуют факторгруппу.

Первая теорема об изоморфизме

Теорема 6

Факторгруппа $\frac{G}{\ker(\varphi)}$ изоморфна образу φ.



Пройти из G в образ напрямую или через факторгруппу — одно и то же.

Изоморфизм

Гомоморфизм переносит операцию, но не обязан быть обратимым. Обратимым его делает биективность.

Определение 21 (Изоморфизм)

Биективный гомоморфизм — **изоморфизм**. Если между структурами есть изоморфизм, они **изоморфны**. Изоморфизм, переводящий структуру в себя, — **автоморфизм**.

Две изоморфные группы неотличимы как алгебраические объекты. Утверждение, верное в одной структуре, верно и в любой изоморфной ей.

Изоморфизм для полей

Для конечных полей изоморфизм сильнее любых двух полей с p^m элементами изоморфны. Существует ровно одно поле $\mathrm{GF}(p^m)$.

Пример

То же явление у натурального ряда: любые две алгебры Дедекинда изоморфны. Отсюда категоричность аксиом Пеано: натуральный ряд — единственная структура с точностью до переименования.

Векторные пространства

Строки как векторное пространство

Есть несколько сообщений одинаковой длины, каждое — строка из нулей и единиц. Складывать умеем: поэлементно по модулю два.

Определение 22 (Векторное пространство)

Множество V над полем F — **векторное пространство**, если на нём заданы:

- сложение векторов $v + w$;
- умножение вектора на скаляр av, где $a \in F$.

Относительно сложения V — коммутативная группа, и выполнены аксиомы дистрибутивности и совместимости.

Зачем аксиомы

Дистрибутивность: можно сначала умножить каждую координату, потом сложить — порядок не важен. Совместимость: можно перемножить скаляры и умножить вектор. Требование $1v = v$ отсекает вырожденные случаи.

Группа требовала одной операции и обратимости. Векторное пространство требует поля скаляров и согласованной с ним второй операции.

$\mathrm{GF}(2)^n$

Все строки длины n из нулей и единиц — $\mathrm{GF}(2)^n$. Скаляры из $\mathrm{GF}(2) = \{0, 1\}$.

> Умножение на скаляр тривиально: $1v = v$, $0v$ — строка из нулей. Вся структура пространства спрятана в сложении. Сложение — ровно то самое XOR.

Для $\mathrm{GF}(2)^n$ и $\mathbb{R}^n$ законы одни: доказав свойство в терминах аксиом, получаем его для всех полей.

Базис и размерность

Определение 23 (Базис и размерность)

Набор векторов — **базис**, если он линейно независим и каждый вектор выражается через него. Все базисы содержат одно и то же число векторов — **размерность** $\dim V$.

Пример

$\mathbb{R}^2$ двумерна: точка задаётся двумя числами. $\mathrm{GF}(2)^n$ имеет размерность n: строка задаётся n битами. Базис $e_1, \ldots, e_n$ — «естественный»: каждая строка просто перечисляет, какие e_i складываются.

Подпространства дают коды

Возьмём подмножество W пространства V, замкнутое относительно сложения и умножения на скаляр. Оно само — векторное пространство.

Определение 24 (Подпространство)

Подпространство — подмножество, само являющееся векторным пространством над тем же полем. Проверка сводится к двум условиям: замкнутость относительно сложения и умножения на скаляр.

Пример

В $\mathrm{GF}(2)^3$ подпространств шестнадцать: одно нулевое, семь прямых, семь плоскостей и всё пространство.

Связь с кодами

Линейные коды — подпространства

Код — это подпространство $\mathrm{GF}(2)^n$, а его базис задаёт, какие сообщения кодируются. Размерность кода — число информационных бит.

> Подпространство само по себе не исправляет ошибки. Защиту добавляет расстояние: чем дальше разнесены кодовые слова, тем больше искажений код замечает и чинит.

Поле и коды Рида—Соломона

Поле $\mathrm{GF}(2^m)$ понадобилось кодам, потому что они работают с байтами.

Коду нужно делить: восстановление по потерянным значениям — это интерполяция. А она опирается на деление на ненулевые элементы. В кольце $\mathbb{Z}_{256}$ делить можно не всегда, и код на нём не построить.

Код Рида—Соломона кодирует сообщение значениями многочлена над $\mathrm{GF}(q)$. Получателю достаточно любых k значений: через них проходит ровно один многочлен степени меньше k.

Замкнутый круг

Мост к кодам замкнут: операция — структура — поле — векторное пространство — код.

Та же лестница ведёт и к криптографии. Поле $\mathrm{GF}(2^8)$ живёт в AES, а мультипликативная группа $\mathbb{Z}_p^*$ — в обмене ключами Диффи—Хеллмана.

Алгебра, выстроенная в этой лекции, — общий язык для защиты информации.