ТЕОРИЯ ГРУПП

Краткое содержание курса
Версия от 1.4.2024

Основано на лекциях Екатерины Михайлец
и их конспектах от Александра Васюкова (tgc @overmindv).
Автор - Артём Марченко. Обратная связь: tg @m3tr_0.

Порядок тем немного изменён мной
для более простой структуризации материала.

Спасибо Кайтуеву Абдулле за обратную связь и нахождение ошибок.
Пишите и вы при обнаружении ошибок и опечаток.

Содержание:

5. **Кольца.**
   - Кольцо, кольцо с единицей, коммутативное кольцо. Подкольцо. Критерий подкольца.
   - Делители нуля. Целостное кольцо.
   - Идеал. Главный идеал. Кольцо главных идеалов. Факторкольцо.
   - Гомоморфизм колец. Теорема о гомоморфизме колец. Леммы.
6. **Поля.**
   - Поле. Обратимый элемент.
   - Алгоритм Евклида. Следствие. Взаимно простые элементы кольца.
   - Характеристика поля.
   - Подполе и расширение поля. Простое подполе. Алгебраический элемент и трансцендентное число. Теорема.
   - Факторкольцо кольца многочленов. Теоремы.
7. **Применение в криптографии.**
   - Протокол шифрования Диффи-Хеллмана.
   - Криптосистема Эль-Гамаля.

1. Базовые элементы общей алгебры

1.1. Множества

Множество - совокупность каких-либо объектов, ***элементов*** этого множества. Определим следующие операции над множествами:

- ***Пересечение множеств*** A и B состояит из элементов, которые есть и в A, и в B:

$$A \cap B = \{x \mid x \in A \land x \in B\}$$

- ***Объединение множеств*** A и B состоит из элементов, которые есть либо в A, либо в B (в том числе в обоих множествах):

$$A \cup B = \{x \mid x \in A \lor x \in B\}$$

- ***Разность множеств*** A и B состоит из элементов, которые есть в A, но не в B:

$$A \setminus B = \{x \mid x \in A \land x \notin B\}$$

- ***Декартово (прямое) произведение множеств*** A и B состоит из всех *упорядоченных пар*, первые элементы которых принадлежат множеству A, а вторые - множеству B.

$$A \times B = \{(a, b) \mid a \in A \land b \in B\}$$

1.2. Отображения

Отображение из множества A в множество B - правило, в соответствии с которым каждому элементу $a \in A$ сопостовляется какой-либо элемент $b \in B$. Обозначение:

$$f : A \to B$$

Преобразование множества A, или ***оператор*** на A - отображение из множества A в само себя: $f : A \to A$.

Пусть дано отображение $f : A \to B$. Тогда:
Образ множества A под действием отображения f - множество всех элементов B, которые могут быть получены с помощью f:

$$\operatorname{Im} A = f(A) = \{f(a) \in B \mid a \in A\}$$
$$\operatorname{Im} A \subseteq B$$

Прообраз элемента $b \in \operatorname{Im} A$ - такой элемент $a \in A$, что $f(a) = b$).

Полный прообраз элемента $b \in \operatorname{Im} A$ - множество всех прообразов элемента b:

$$f^{-1}(b) = \{a \in A \mid f(a) = b\}$$

Отображение называется ***сюръективным***, если для каждого элемента $b \in B$ существует какой-либо элемент $a \in A$ такой, что $f(a) = b$. Иными словами, образ множества A равен множеству B.

$$f : A \to B$$
$$f \text{ сюръективно} \iff \forall b \in B\ \exists a \in A : f(a) = b \iff \operatorname{Im} A = B$$

Отображение называется ***инъективным***, если разные элементы множества A отображаются в разные элементы множества B. Иными словами, для каждого элемента $b \in B$ существует только один прообраз.

$$f : A \to B$$
$$f \text{ инъективно} \iff \forall a_1, a_2 \in A : a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$$
$$\iff \forall a_1, a_2 \in A : f(a_1) = f(a_2) \Rightarrow a_1 = a_2$$

Отображение называется ***биективным*** (или ***взаимно-однозначным***), если оно инъективно и сюръективно.

Композиция, или ***произведение*** отображений f и g - применение f к результату g. Пусть $g : A \to B$ и $f : B \to C$. Тогда их композиция:

$$f \circ g : A \to C$$
$$\forall a \in A : (f \circ g)(a) = f(g(a))$$

Композиция в общем случае ассоциативна и не коммутативна:

$$\forall f, f_0, g, h \text{ таких, что } h : A \to B, g : B \to C, f : C \to D, f_0 : D \to C$$
$$(f \circ g) \circ h = f \circ (g \circ h)$$
$$f \circ g \neq g \circ f$$

1.3. Бинарные отношения

Пусть даны множества A и B. Тогда любое подмножество их декартова произведения $A \times B$ называется ***бинарным отношением***. Если $X = Y$, то это бинарное отношение на множестве X.

Пусть $W \subseteq A \times B$ - бинарное отношение. Тогда обозначают $(a, b) \in W$ как aWb.

Бинарное отношение ~ на множестве A называется ***отношением эквивалентности***, если $\forall a_0, a_1, a_2 \in A$ выполняется:

- *Рефлексивность*: $a_0 \sim a_0$;
- *Симметричность*: $a_0 \sim a_1 \Rightarrow a_1 \sim a_0$;
- *Транзитивность*: $a_0 \sim a_1 \wedge a_1 \sim a_2 \Rightarrow a_0 \sim a_2$.

Класс эквивалентности элемента $a \in A$ - подмножество множества A, содержащее все значения, эквивалентные a:

$$\overline{a} = \{a_0 \in A \mid a_0 \sim a\} \subseteq A$$

Множество классов эквивалентности элементов A является *разбиением* множества A. Другими словами, классы эквивалентности либо не пересекаются, либо совпадают:

$$A = \bigcup_{a \in A} \overline{a}$$
$$\forall a_1, a_2 \in A : (\overline{a_1} = \overline{a_2}) \vee (\overline{a_1} \cap \overline{a_2} = \varnothing)$$

Утверждение: Если существует разбиение множества на непересекающиеся подмножества, то эти подмножества будут классами эквивалентности по некоторому отношению эквивалентности.

□
Зададим ~ следующим образом: $a_1 \sim a_2 \Leftrightarrow a_1$ и a_2 лежат в одном и том же из таких непересекающихся подмножеств. Это отношение рефлективно, симметрично и транзитивно. Значит, ~ является отношением эквивалентности.
■

Следовательно, задать разбиение множества ⇔ задать отношение эквивалентности.

Фактормножество относительно некоторого отношения эквивалентности - разбиение (множество классов эквивалентности), отвечающее этому отношению эквивалентности.

Пусть A - множество, и B - его разбиение, отвечающее отношению эквивалентности ~. Тогда обозначают: $B = A/\sim$.

1.4. Бинарные операции

Бинарной операцией на множестве A называется отображение $\tau : A \times A \to A$ (Отображает пары элементов множества в элементы множества).

Пусть задана бинарная операция $\star : X \times X \to X$. Тогда:

Бинарная операция $\star$ ***ассоциативна***, если $\forall a, b, c \in X : (a \star b) \star c = a \star (b \star c)$.

Бинарная операция $\star$ ***коммутативна***, если $\forall a, b \in X : a \star b = b \star a$.

2. Алгебраические структуры

2.1. Группоиды

Группоид (или магма) - множество с корректно заданой на нём *бинарной операцией*.
(Пусть A - множество. Операция должна отображать $A \times A$ в A, то есть множество замкнуто относительно операции.)

Группоид обозначают $(M, \star)$, где M - множество, а $\star$ - операция.

Полугруппа - группоид, операция которого *ассоциативна*. Иными словами полугруппа - множество с корректно заданной на нём ассоциативной бинарной операцией.

Нейтральный элемент e в полугруппе $(H, \star)$ - такой элемент, что выполняется:

$$\forall h \in H : e \star h = h \star e = h$$

Утверждение: Нейтральный элемент единственен.

□ Пусть e_1 и e_2 - нейтральные элементы в $(H, \star)$. Тогда $e_1 = e_1 \star e_2 = e_2 \Rightarrow e_1 = e_2$. ■

Моноид - полугруппа, в которой *существует нейральный элемент*.

Пусть $(M, \star)$ - моноид с нейтральным элементом e.
Обратный элемент $a^{-1} \in M$ к элементу $a \in M$ - такой, что выполняется:

$$a^{-1} \star a = a \star a^{-1} = e$$

(Следовательно, a - обратный элемент к a^{-1}.)

Группа - моноид, все элементы которого *обратимы* (к ним есть обратный элемент). Другими словами, группа $(G, \star)$ - множество G с корректно заданной на нём бинарной операцией $\star$, в котором выполняется:
- *Ассоциативность*: $\forall x, y, z \in G : (x \star y) \star z = x \star (y \star z)$;
- *Существование нейтрального элемента*: $\exists e \in G\ \forall x \in G : e \star x = x \star e = x$;
- *Обратимость* каждого элемента: $\forall x \in G\ \exists x^{-1} \in G : x^{-1} \star x = x \star x^{-1} = e$.

Порядок группы - количество элементов в ней (мощность). Обозначается $|G|$.

Абелева группа - группа, операция которой *коммутативна*:

$$\forall x, y \in (M, \star) : x \star y = y \star x$$

Прямое произведение групп $(G_1, \circ)$ и $(G_2, *)$ - их прямое (декартово) произведение $G_1 \times G_2$ (как множество), снабжённое операцией $\star$:

$$\forall (x_1, y_1), (x_2, y_2) \in G_1 \times G_2 : (x_1, y_1) \star (x_2, y_2) = (x_1 \circ x_2, y_1 * y_2)$$

2.2. Подгруппа

Пусть $(G, \star)$ - группа и $H \subseteq G$ - его непустое подмножество. H является ***подгруппой***, если выполняется:
- *замкнутость по бинарной операции*: $\forall x, y \in H : x \star y \in H$;
- *нейтральный элемент включён*: $\exists e \in H\ \forall x \in H : e \star x = x \star e = x$;
- *замкнутость по взятию обратного элемента*: $\forall x \in H\ \exists x^{-1} \in H : x \star x^{-1} = x^{-1} \star x = e$.

Подгруппа H группы G называется ***собственной***, если $H \neq \{e\} \land H \neq G$.

Простая группа - группа, не имеющая собственных подгрупп.

Критерий подгруппы: Пусть H - подмножество группы $(G, \star)$. Тогда:

$$H \text{ является подгруппой} \quad \Longleftrightarrow \quad \forall h_1, h_2 \in H : h_1 \star h_2^{-1} \in H$$

□

$\Longrightarrow$

Дано: H является подгруппой. Тогда:

$$\forall h_2 \in H : h_2^{-1} \in H \quad \Rightarrow \quad \forall h_1, h_2^{-1} \in H : h_1 \star h_2^{-1} \in H$$

$\Longleftarrow$

Дано: $\forall h_1, h_2 \in H : h_1 \star h_2^{-1} \in H$.

1. Возьмём $h_1 = h_2$. Тогда:

$$h_1 \star h_2^{-1} \in H \quad \Rightarrow \quad h_1 \star h_1^{-1} \in H \quad \Rightarrow \quad e \in H$$

Значит, обратный элемент включён.
2. Возьмём $h_1 = e \in H$. Тогда $\forall h_2 \in H$:

$$h_1 \star h_2^{-1} \in H \quad \Rightarrow \quad e \star h_2^{-1} \in H \quad \Rightarrow \quad h_2^{-1} \in H$$

Значит, выполняется замкнутость по взятию обратного элемента.
3. $\forall h_2 \in H : h_2^{-1} \in H \quad \Rightarrow \quad \forall h_1, h_2^{-1} \in H$:

$$h_1 \star \left(h_2^{-1}\right)^{-1} \in H \quad \Rightarrow \quad h_1 \star h_2 \in H$$

Значит, выполняется замкнутость по бинарной операции.
■

2.3. Циклические группы

Пусть e - нейтральный элемент группы $(G, \cdot)$ и $g \in G$ - некоторый элемент этой группы.
Пусть существует $q \in \mathbb{N}$ - наименьшее натуральное число такое, что $g^q = e$.
Тогда g называется элементом ***конечного порядка***, а q - ***порядком*** элемента g. Обозначают $q = \mathrm{ord}(g)$.
Если такого q не существует, то g называется элементом ***бесконечного порядка***.

Циклическая группа - группа $(G, \cdot)$, в которой существует такой элемент $a \in G$, что любой элемент $g \in G$ представим в виде $g = a^n$, где $n \in \mathbb{Z}$:

$$G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$$

(Существует *мультипликативная запись*: $g = a \cdot a \cdot \ldots \cdot a = a^n$; и *аддитивная запись*: $g = a + a + \ldots + a = n \cdot a$.)

В любой группе каждый элемент $g \in G$ порождает циклическую подгруппу $\langle g \rangle$ (состоящую из всех его степеней).

Утверждение: все циклические группы *абелевы*.

□ $\forall g_1 = a^k, g_2 = a^l \in \langle a \rangle : g_1 \cdot g_2 = a^k \cdot a^l = a^{k+l} = a^l \cdot a^k = g_2 \cdot g_1$ ■

Утверждение: порядок любого элемента группы равен порядку циклической подгруппы, порождённой им:

$$\forall g \in G : \mathrm{ord}(g) = |\langle g \rangle|$$

□
Пусть G - группа, и $g \in G$ некторый её элемент.
1. Пусть $g^k = g^s$ для некоторых $k \geq s$. Тогда $g^{k-s} = e$. Значит, элемент g имеет конечный порядок. Значит, если $\mathrm{ord}(g) = \infty$, то все степени g^n различны. Следовательно $|\langle g \rangle| = \infty$ (так как $\langle g \rangle$ состоит из всех степеней g^n).
2. Если порядок g конечен, то существует минимальное $m \in \mathbb{N}$, такое что $g^m = e$. Покажем, что $\langle g \rangle = \{g^0, g^1, \ldots, g^{m-1}\}$. $\forall g^n \in \langle g \rangle$:

$$g^n = g^{m \cdot q + r} = (g^m)^q \cdot q^r = e^q \cdot g^r = e \cdot g^r = g^r \quad, 0 \leq r < m$$

То есть любой элемент в $\langle g \rangle$ имеет вид g^r, где $0 \le r < m$. Значит, $|\langle g \rangle| = \mathrm{ord}(g) = m$.
■

2.4. Таблица Кэли

Таблицей Кэли для какой-либо алгебраической структуры (в частности, группы) называется следующая матрица ($g_1, g_2, ..., g_i, ... \in (G, \star)$ - элементы этой структуры):

	g_1	g_2	...	g_i	...
g_1	$g_1 \star g_1$	$g_1 \star g_2$	...	$g_1 \star g_i$	...
g_2	$g_2 \star g_1$	$g_2 \star g_2$	...	$g_2 \star g_i$	...
...	...	...	...	...	...
g_i	$g_i \star g_1$	$g_i \star g_2$	...	$g_i \star g_i$	...
...	...	...	...	...	...

Если таблица Кэли симметрична, то группа *абелева*.

Утверждение: Если $(G, \star)$ - группа, то в её таблице Кэли каждый элемент встречается только один раз в каждой строке и каждом столбце.

□
Для столбца. $\forall g_i, g_k, g_j$:

$$g_i \star g_j = g_k \star g_j \;\Rightarrow\; g_i \star g_j \star g_j^{-1} = g_k \star g_j \star g_j^{-1} \;\Rightarrow\; g_i = g_k$$

Для строки аналогично.
■

3. Гомоморфизмы

3.1. Виды гомоморфизмов

Пусть $(G_1, \star)$ и $(G_2, \circ)$ - группы. Тогда отображение $f : G_1 \to G_2$ называется ***гомоморфизмом***, если $\forall a, b \in G_1 : f(a \star b) = f(a) \circ f(b)$.

Инъективный гомоморфизм называется ***мономорфизмом***, *сюръективный* - ***эпиморфизмом***, *биективный* - ***изоморфизмом***.

Изоморфные группы G_1 и G_2 (между ними существует изоморфизм) обозначают $G_1 \cong G_2$.

Если две группы изоморфны, то с точки зрения алгебры они не различимы.

Утверждение: Все циклические группы одинакового порядка изоморфны.

□
Покажем, что для любой циклической группы бесконечного порядка выполняется $\langle a \rangle \cong (\mathbb{Z}, +)$.

Пусть отображение $\varphi : \langle a \rangle \to \mathbb{Z}$ задано как $\varphi(a^n) = n$.
Оно инъективно и сюръективно, а значит биективно. На нём выполняется $\varphi(a^m \star a^n) = \varphi(a^{m+n}) = m + n = \varphi(a^m) + \varphi(a^n)$, значит оно гомоморфизм и изоморфизм.

Покажем, что для любой циклической группы конечного порядка n выполняется $<a> \cong (\mathbb{Z}_n, +)$, где $(\mathbb{Z}_n, +)$ - группа вычетов по модулю n с операцией сложения.

Пусть отображение $\varphi : <a> \to \mathbb{Z}_n$ задано как $\varphi(a^k) = \overline{k}$.
Оно инъективно и сюръективно, а значит биективно. На нём выполняется $\varphi(a^m \star a^n) = \varphi(a^{m+n}) = \overline{m+n} = \overline{m} + \overline{n} = \varphi(a^m) + \varphi(a^n)$, значит оно гомоморфизм и изоморфизм.
■

3.2. Свойства гомоморфизма

Пусть задан гомоморфизм $f : (G_1, \star, e_1) \to (G_2, \circ, e_2)$. Тогда:
1. Нейтральный элемент всегда переходит в нейтральный: $f(e_1) = e_2$

□ $\forall g \in G_1 : f(g) \circ f(e_1) = f(g \star e_1) = f(g) = f(e_1 \star g) = f(e_1) \circ f(g) \Rightarrow f(e_1)$ - нейтральный элемент в G_2. ■

2. Обратный элемент всегда переходит в обратный: $\forall g \in G_1 : f(g^{-1}) = (f(g))^{-1}$

□ $\forall g \in G_1 : f(g^{-1}) \circ f(g) = f(g^{-1} \star g) = f(e_1) = e_2 = f(g \star g^{-1}) = f(g) \circ f(g^{-1})$
$\Rightarrow \quad f(g^{-1})$ - обратный элемент к $f(g)$ в G_2. ■

Утверждение: Если f - изоморфизм, то f^{-1} тоже изоморфизм.

□
Пусть задан изоморфизм $f : (G_1, \star) \to (G_2, \circ)$. f - биекция, следовательно f^{-1} тоже биекция.

$$f^{-1}(f(a) \circ f(b)) = f^{-1}(f(a \star b)) = a \star b = f^{-1}(f(a)) \star f^{-1}(f(b))$$

Значит, f^{-1} - гомоморфизм, а значит и изоморфизм.
■

3.3. Ядро и образ гомоморфизма

Ядро гомоморфизма $f : G_1 \to G_2$ - подмножество всех элементов G_1, которые переходят в нейтральный элемент из G_2:

$$\operatorname{Ker} f = \{a \in G_1 \mid f(a) = e_2\}$$

$\operatorname{Ker} f \neq \varnothing$, так как $f(e_1) = e_2$.

Утверждение: Ядро любого гомоморфизма $f : G_1 \to G_2$ является подгруппой в G_1.

□

$$\forall a, b \in \operatorname{Ker} f : f(a \star b^{-1}) = f(a) \circ f(b^{-1}) = f(a) \circ (f(b))^{-1} = e_2 \circ e_2^{-1} = e_2$$

Следовательно, $a \star b^{-1} \in \operatorname{Ker} f$ и по критерию подгруппы $\operatorname{Ker} f$ - подгруппа в G_1.
■

Пусть $f : G_1 \to G_2$ - гомоморфизм.
Критерий о тривиальности ядра гомоморфизма: f - мономорфизм $\iff$ $\operatorname{Ker} f = \{e_1\}$.

□
$\Longrightarrow$

$$\forall g_1, g_2 \in G_1 : g_1 \neq g_2 \Rightarrow f(g_1) \neq f(g_2)$$
$$\Downarrow$$
$$\forall g \in G_1 : g \neq e_1 \Rightarrow f(g) \neq f(e_1) = e_2$$
$$\Downarrow$$
$$\operatorname{Ker} f = \{e_1\}$$

$\Longleftarrow$
$\forall g_1, g_2$:

$$f(g_1) = f(g_2) \quad \Rightarrow \quad f(g_1) \circ (f(g_2))^{-1} = e_2 \quad \Rightarrow \quad f(g_1) \circ f(g_2^{-1}) = f(g_1 \star g_2^{-1}) = e_2$$

Значит, $g_1 \star g_2^{-1} \in \operatorname{Ker} f = \{e_1\}$, следовательно $g_1 \star g_2^{-1} = e_1$ и следовательно $g_1 = g_2$. Итого получаем $\forall g_1, g_2 \in G_1 : f(g_1) = f(g_2) \Rightarrow g_1 = g_2$, то есть f - мономорфизм.
■

Образ гомоморфизма $f : G_1 \to G_2$ - это образ множества G_1 под действием отображения f с операцией группы G_2:

$$\operatorname{Im} f = f(G_1) = \{g_2 \in G_2 \mid \exists g_1 \in G_1 : f(g_1) = g_2\} \subseteq G_2$$

Утверждение: Образ гомоморфизма $f : G_1 \to G_2$ является подгруппой в G_2.

□
1. Замкнутость по операции из определения гомоморфизма;
2. Содержит нейтральный элемент e_2, так как $e_2 = f(e_1)$;
3. Содержит обратный элемент к каждому, так как $(f(g))^{-1} = f(g^{-1})$

■

3.4. Автоморфизмы

Автоморфизм - изоморфизм группы в себя.
Множество всех автоморфизмов группы G обозначается $\operatorname{Aut}(G)$ и образует группу относительно операции композиции.

Внутренний автоморфизм - отображение $I_a : G \to G$, такое что $\forall g \in G : I_a(g) = aga^{-1}$ (переводит каждый элемент в сопряжённый к нему по a).
Множество всех внутренних автоморфизмов группы G обозначается $\operatorname{Inn}(G)$ и образует подгруппу в $\operatorname{Aut}(G)$.

Внутренний автоморфизм действительно является изоморфизмом:

$$I_a(g_1 g_2) = a g_1 g_2 a^{-1} = a g_1 a^{-1} a g_2 a^{-1} = I_a(g_1)\, I_a(g_2)$$

В абелевой группе G всегда выполняется $\mathrm{Inn}(G) = \{e\} = \{I_e\}$.

3.5. Теорема Кэли

Теорема Кэли: любая конечная подгруппа порядка $n \in \mathbb{N}$ изоморфна некоторой подгруппе в S_n (симметрической группе - группе всех подстановок n элементов).

□

Пусть G - группа порядка n. Для каждого элемента $a \in G$ рассмотрим отображение $L_a : G \to G$, заданное формулой $L_a(g) = ag$ (то есть L_a - это умножение слева на a, или левый сдвиг).

Пусть $e, g_2, ..., g_n$ - элементы группы G. Тогда $a, ag_2, ..., ag_n$ - это те же элементы, но в другом порядке ("склеиваний" нет: $ag_i = ag_j \;\Rightarrow\; a^{-1}ag_i = a^{-1}ag_j \;\Rightarrow\; g_i = g_j$). Значит, L_a - это биективное отображение, то есть перестановка элементов группы G.

Множество $\{L_a \mid a \in G\}$ является подгруппой в $S(G)$ (все биективные отображения G в себя с операцией композиции), так как:
- замкнуто относительно операции: $\forall g \in G : (L_a \circ L_b)(g) = L_a(L_b(g)) = a(bg) = (ab)g = L_{ab}(g)$;
- включает нейтральный элемент: $\forall g \in G : L_e(g) = eg = g \quad \Rightarrow \quad L_e = \mathrm{Id}$;
- замкнуто по взятию обратоного элемента: $\forall a \in G : (L_a)^{-1} = L_{a^{-1}}$, а значит для любого L_a: $L_{a^{-1}}(L_a(g)) = a^{-1}ag = g$;

Биективные отображения $g_1, ..., g_n$ в себя ничем не отличаются от отображений $1, ..., n$ в себя. Значит, $S(G) \cong S_n$.

Зададим отображение $\varphi : G \to \{L_a \mid a \in G\}$, где $\varphi(a) = L_a$. Это гомоморфизм: $\forall a, b \in G :$ $\varphi(ab) = L_{ab} = L_a \circ L_b = \varphi(a) \circ \varphi(b)$. Он инъективен и сюръективен, а значит φ - изоморфизм.
■

4. Классы смежности

4.1. Левые и правые смежные классы

Пусть $(G, \star)$ - группа и $H \subseteq G$ - подгруппа. Тогда:
Левый смежный класс элемента $g \in G$ по подгруппе H - это множество элементов из H, "умноженных" слева на g:

$$gH = \{g \star h \mid h \in H\}$$

Правый смежный класс элемента $g \in G$ по подгруппе H - это множество элементов из H, "умноженных" справа на g:

$$Hg = \{h \star g \mid h \in H\}$$

4.2. Теорема Лагранжа

Лемма 1: Левые (аналогично для правых) смежные классы по некоторой подгруппе либо совпадают, либо не пересекаются:

$$\forall g_1, g_2 \in G : (g_1H = g_2H) \lor (g_1H \cap g_2H = \varnothing)$$

□
Если $g_1H \cap g_2H \neq \varnothing$, то:

$$\exists h_1, h_2 \in H : g_1h_1 = g_2h_2$$
$$\Downarrow$$
$$\exists h_1, h_2 \in H : g_2 = g_1h_1h_2^{-1} \land g_1 = g_2h_2h_1^{-1}$$
$$\Downarrow$$
$$\exists h_1, h_2 \in H : g_2H = g_1h_1h_2^{-1}H \land g_1H = g_2h_2h_1^{-1}H$$
$$\Downarrow$$
$$g_2H \subseteq g_1H \land g_1H \subseteq g_2H$$

Значит, $g_1H = g_2H$.
■

Лемма 2: Для любого элемента $g \in G$ и для любой подгруппы $H \subseteq G$ порядок подгруппы H равен порядку левого (аналогично правого) класса элемента g по подгруппе H:

$$\forall g \in G : |gH| = |H|$$

□

$$gH = \{g \star h \mid h \in H\} \quad \Rightarrow \quad |gH| \leq |H|$$

$\forall h_1, h_2 \in H$:

$$gh_1 = gh_2 \quad \Rightarrow \quad g^{-1}gh_1 = g^{-1}gh_2 \quad \Rightarrow \quad h_1 = h_2$$

Значит, $|gH| \geq |H|$ и, следовательно, $|gH| = |H|$.
■

Индекс подгруппы H в группе G - число левых (аналогично правых, следует из т. Лагранжа ниже) смежных классов элементов G по H. Обозначается $[G : H]$.

Пусть G - конечная группа и H - подгруппа в ней.
Теорема Лагранжа: Порядок группы G равен произведению порядка подгруппы H и индекса подгруппы H в группе G:

$$|G| = |H| \cdot [G : H]$$

□
Любой элемент группы G лежит в своём смежном классе, и смежные классы не пересекаются (*лемма 1*). В то же время, любой смежный класс содержит по $|H|$ элементов (*лемма 2*). Значит, $|G| = |H| \cdot [G : H]$.
■

Следствие 1: Порядок любого элемента конечной группы делит порядок этой группы:

$$\forall g \in G : \mathrm{ord}(g) \mid |G|$$

□
Ранее доказано, что $\forall g \in G : \mathrm{ord}(g) = |<g>|$. $<g>$ - подгруппа, следовательно по теореме Лагранжа $|G| = |<g>| \cdot [G : <g>] = \mathrm{ord}(g) \cdot [G : <g>]$. Значит, $\mathrm{ord}(g) \mid |G|$.
■

Следствие 2: Пусть G - конечная группа с нейтральным элементом e. Тогда:

$$\forall g \in G : g^{|G|} = e$$

□
По следствию 1: $|G| = \mathrm{ord}(g) \cdot n$, где n - некоторое целое число. Значит:

$$g^{|G|} = g^{\mathrm{ord}(g) \cdot n} = \left(g^{\mathrm{ord}(g)}\right)^n = e^n = e$$

■
$\mathbb{Z}_p^* = \left(\mathbb{Z}_p \setminus \{\overline{0}\}, \cdot\right)$ - группа вычетов по простому модулю p с операцией умножения.
Следствие 3 - Малая теорма Ферма: пусть $\overline{a} \in \mathbb{Z}_p^*$ - некоторый ненулевой вычет по модулю p. Тогда:

$$\overline{a}^{p-1} = \overline{1}$$

Другими словами, a^{p-1} сравнимо с единицей по модулю p, где $a \in \mathbb{Z} \setminus \{0\}$, а p - простое число:

$$a^{p-1} \equiv 1 \bmod p$$

□ $|\mathbb{Z}_p^*| = p - 1$. Значит, по следствию 2: $\overline{a}^{p-1} = \overline{a}^{|\mathbb{Z}_p^*|} = e = \overline{1}$. ■

4.3. Нормальные подгруппы

Пусть $H \subseteq G$ - подгруппа группы G. Тогда H - ***нормальная подгруппа***, если все левые смежные классы по ней совпадают с правыми:

$$\forall g \in G : gH = Hg$$

В *абелевой группе* все подгруппы нормальные.

Естественный гомоморфизм - отображение, сопостовляющее каждому элементу $g \in G$ его смежный класс по некторой *нормальной* подгруппе $H \subseteq G$:

$$\varepsilon : G \to G/H$$
$$\forall g \in G : \varepsilon(g) = gH$$

Естественный гомоморфизм действительно является гомоморфизмом:

$$\varepsilon\left(g_1 \star g_2\right) = g_1 \star g_2 H = g_1 H \cdot g_2 H = \varepsilon\left(g_1\right) \cdot \varepsilon\left(g_2\right)$$

Элементы $x_1, x_2 \in G$ называются ***сопряжёнными***, если существует такой элемент $y \in G$, что $y \star x_1 \star y^{-1} = x_2$.

Пусть $H \subseteq G$ - подгруппа в группе G.

Критерий нормальности подгруппы с использованием сопряжения: Следущие три условия эквивалентны:

1. H - нормальная подгруппа ($H \triangleleft G$);
2. Вместе с каждым своим элементом H содержит все сопряжённые к нему. $\forall g \in G : gHg^{-1} \subseteq H$;
3. $\forall g \in G : gHg^{-1} = H$. (более строгий вариант пункта 2)

□

$1 \Longrightarrow 2$

H - нормальная подгруппа в G, а значит по определению $\forall g \in G : gH = Hg$, то есть $\forall g \in G$:

$$\forall h \in H \;\; \exists h` \in H : g \cdot h = h` \cdot g$$
$$\Downarrow$$
$$\forall g \in H \;\; \exists h` \in H : g \cdot h \cdot g^{-1} = h`$$
$$\Downarrow$$
$$\forall g \in H : g \cdot h \cdot g^{-1} \in H$$

Значит, $gHg^{-1} \subseteq H$.

$2 \Longrightarrow 3$

$gHg^{-1} \subseteq H$. Осталось доказать, что $H \subseteq gHg^{-1}$. Любой элемент $h \in H$ можно представить как:

$$h = \left(g \cdot g^{-1}\right) \cdot h \cdot \left(g \cdot g^{-1}\right) = g \cdot \left(g^{-1} \cdot h \cdot g\right) \cdot g^{-1}$$

$g^{-1} \cdot h \cdot g$ является элементом H по условию (мы можем взять $g` = g^{-1} \in G$). Значит, любой элемент $h \in H$ представим как $h = g \cdot h` \cdot g^{-1}$, где $h` \in H$. Следовательно, $H \subseteq gHg^{-1}$.

$3 \Longrightarrow 1$

$$\forall g \in G : H = gHg^{-1}$$
$$\Downarrow$$
$$\forall g \in G : Hg = gH$$
$$\Downarrow$$
$$\text{подгруппа нормальна по определению}$$

■

Критерий нормальности подгруппы с использованием понятия ядра: H - нормальная подгруппа в $G \iff H$ является ядром некоторого гомоморфизма из G.

□

$\Longrightarrow$

Рассмотрим естественный гомоморфизм $\varepsilon : G \to G/H, \;\; \varepsilon(g) = gH$.

$$\operatorname{Ker} \varepsilon = \{g \in G \mid \varepsilon(g) = gH = H\}$$

Заметим, что при $gH = H$ выполняется $g \in H$, так как из нормальности $\exists h_1, h_2 \in H : gh_1 = h_2 g$, а значит $\exists h_1, h_2 \in H : g = h_2 g h_1^{-1} \in H$.
Значит, $\operatorname{Ker} \varepsilon = H$ и ε - искомый гомоморфизм.

$\Longleftarrow$

Пусть f - некоторый гомоморфизм, и $H = \operatorname{Ker} f$. Тогда $\forall h \in H$:

$$f\left(g \cdot h \cdot g^{-1}\right) = f(g) \cdot f(h) \cdot f\left(g^{-1}\right) = f(g) \cdot f\left(g^{-1}\right) = f\left(g \cdot g^{-1}\right) = f\left(e_1\right) = e_2$$

Значит, по определению ядра $\forall h \in H : g \cdot h \cdot g^{-1} \in H$, то есть $gHg^{-1} \subseteq H$.
По критерию нормальности подгруппы с использованием сопряжения H является нормальной подгруппой.

$\blacksquare$

Следствие: *Ядро* гомоморфизма $f : G_1 \to G_2$ - всегда нормальная подгруппа в G_1.

4.4. Факторгруппа

Пусть H - *нормальная* подгруппа в группе G.
Факторгруппа группы G по подгруппе H - множество левых (= правых) смежных классов по подгруппе H с операцией умножения смежных классов:

$$\left(g_1 H\right) \cdot \left(g_2 H\right) = \left(g_1 \cdot g_2 H\right)$$

Факторгруппу обозначают: G/H.

Утверждение: Операция задана корректно. Результат умножения не зависит от выбора представителя смежных классов.

$\square$
Пусть G/H - факторгруппа.
Пусть $g_1, a_1 \in g_1 H$ и $g_2, a_2 \in g_2 H$, то есть $\exists h_1, h_2 \in H : a_1 = g_1 h_1$ и $a_2 = g_2 h_2$.

$\left(g_1 H\right) \cdot \left(g_2 H\right) = \left(a_1 H\right) \cdot \left(a_2 H\right)$. Хотим доказать, что $g_1 g_2 H = a_1 a_2 H$ - тогда результат умножения действительно не зависит от выбора представителя смежных классов.

$a_1 a_2 = g_1 h_1 g_2 h_2 = g_1 g_2 \left(g_2^{-1} h_1 g_2\right) h_2$. Хотим найти $h_3 = g_2^{-1} h_1 g_2$.
H - нормальная подгруппа, а значит $Hg_2 = g_2 H$. Следовательно, $\exists h_3 : h_1 g_2 = g_2 h_3$. Значит, $\exists h_3 = g_2^{-1} h_1 g_2$.

Получаем:

$$a_1 a_2 H = g_1 h_1 g_2 h_2 H = g_1 g_2 g_2^{-1} h_1 g_2 h_2 H = g_1 g_2 h_3 h_2 H = g_1 g_2 H$$

$\blacksquare$

Факторгруппа является группой, так как:
- операция задана корректно;
- операция ассоциативна;
- есть нейтральный элемент $eH = H$;
- для каждого элемента существует обратный: $(gH)^{-1} = g^{-1}H$.

Пусть $f : G_1 \to G_2$ - гомоморфизм.

Теорема о гомоморфизме групп: образ гомоморфизма f изоморфен факторгруппе группы G_1 по ядру гомоморфизма f:

$$G_1 / \operatorname{Ker} f \cong \operatorname{Im} f$$

□

Зададим отображение $\tau : G_1 / \operatorname{Ker} f \to \operatorname{Im} f$ в виде формулы $\tau(g \operatorname{Ker} f) = f(g)$.

1. τ заданно корректно - результат не зависит от выбора представителя смежного класса. $\forall h_1, h_2 \in \operatorname{Ker} f$:

$$f(gh_1) = f(g) \cdot f(h_1) = f(g) \cdot e_2 = f(g) = f(g) \cdot f(h_2) = f(gh_2)$$
$$\Downarrow$$
$$\tau(gh_1 H) = f(g) = \tau(gh_2 H)$$

2. τ - гомоморфизм. $\forall a, g \in G_1$:

$$\tau((g \operatorname{Ker} f)(a \cdot \operatorname{Ker} f)) = \tau((ga) \operatorname{Ker} f) = f(ga) = f(g) \cdot f(a) = \tau(g \operatorname{Ker} f) \circ \tau(a \operatorname{Ker} f)$$

3. τ задано формулой $\tau(g \operatorname{Ker} \mathrm{f}) = f(g)$, оно принимает всевозможные значения из $\operatorname{Im} f$. Значит оно сюъективно и является эпиморфизмом.
4. $\operatorname{Ker} \tau = \{g \operatorname{Ker} f \mid \tau(g \operatorname{Ker} f) = e_2\} = \{g \operatorname{Ker} f \mid f(g) = e_2\} = \{g \operatorname{Ker} f \mid g \in \operatorname{Ker} f\} = \{\operatorname{Ker} f\}$. Значит, оно инъективно и является мономорфизмом по критерию о тривиальности ядра гомоморфизма.

Получаем: τ - изоморфизм.

■

Пусть $f : G_1 \to G_2$ - некоторый гомоморфизм, $\varepsilon : G_1 \to G_1 / \operatorname{Ker} f$ - естественный гомоморфизм по ядру f, и $\tau : G_1 / \operatorname{Ker} f \to G_2$ - гомоморфизм по теореме о гомоморфизме групп. Тогда выполняется $f = \tau \circ \varepsilon$:

$$\begin{tikzcd}
G_1 \arrow[rr, "f"] \arrow[dr, "\varepsilon"'] & & G_2 \\
& G_1 / \operatorname{Ker} f \arrow[ur, "\tau"'] &
\end{tikzcd}$$

4.5. Центр группы

Центр группы - множество всех элемнтов $g \in G$ группы G, для которых выполняется коммутативность с прочими её элементами:

$$Z(G) = \{a \in G \mid \forall b \in G : ab = ba\}$$

Утверждение: Центр группы является её нормальной подгруппой.

□
1. Докажем, что $Z(G)$ - подгруппа в G.

Для любых $a, b \in Z(G)$ и для любого $g \in G$ выполняется:

$$\left(a \cdot b^{-1}\right) \cdot g = a \cdot b^{-1} \cdot \left(g^{-1}\right)^{-1} = a \cdot \left(g^{-1} \cdot b\right)^{-1} = a \cdot \left(b \cdot g^{-1}\right)^{-1} =$$
$$= a \cdot \left(g^{-1}\right)^{-1} \cdot b^{-1} = (a \cdot g) \cdot b^{-1} = (g \cdot a) \cdot b^{-1} = g \cdot \left(a \cdot b^{-1}\right)$$

Следовательно, по определению центра $a \cdot b^{-1} \in Z(G)$. Значит, по критерию подгруппы, $Z(G)$ является подгруппой.
2. Докажем нормальность $Z(G)$.

По определению центра:

$$\forall g \in G \;\; \forall h \in Z(G) : g \cdot h = h \cdot g$$

Значит, по определению смежного класса:

$$\forall g \in G : g \cdot Z(G) = Z(G) \cdot g$$

Следовательно, $Z(G)$ - нормальная подгруппа по определению.
■

Утверждение: Факторгруппа группы по её центру изоморфна группе её внутренних автоморфизмов:

$$G/Z(G) \cong \mathrm{Inn}G$$

□
Рассмотрим отображение $f : G \to \mathrm{Inn}(G), \;\; f(g) = I_g$. Оно является гомоморфизмом:

$$f\left(g_1 \cdot g_2\right) = I_{g_1 \cdot g_2} = I_{g_1} \cdot I_{g_2} = f\left(g_1\right) \cdot f\left(g_2\right)$$

Покажем, что $\mathrm{Ker}f = Z(G)$. По определению ядра $\forall g \in \mathrm{Ker}\, f : f(g) = I_g = I_e$. ($I_e$ - нейтральный элемент в $\mathrm{Inn}(G), \;\; \forall h \in G : I_e(h) = e \cdot h \cdot e^{-1} = h$.)

Значит:

$$\forall g \in \mathrm{Ker}\, f \;\; \forall h \in G : g \cdot h \cdot g^{-1} = h$$
$$\Downarrow$$
$$\forall g \in \mathrm{Ker}\, f \;\; \forall h \in G : g \cdot h = h \cdot g$$

Следовательно, $\mathrm{Ker}\, f = Z(G)$ по определению. Значит, по теореме о гомоморфизме групп, $G/Z(G) \cong \mathrm{Inn}\, G$.
■

5. Кольца

5.1. Определение

Кольцо - множество $K \neq \varnothing$ с двумя заданными операциями $+$ и $\cdot$, удовлетворяющее условиям:

1. $(K, +)$ - абелева группа (*аддиктивная группа кольца*) (нейтральный элемент - *ноль*).
2. $(K, \cdot)$ - полугруппа (*мультипликативная полугруппа кольца*).
3. Дистрибутивность: $\forall a, b, c \in K : (a + b) \cdot c = a \cdot c + b \cdot c \quad \wedge \quad c \cdot (a + b) = c \cdot a + c \cdot b$.

Подкольцо - подмножество $L \subseteq K$ кольца K, которое само является кольцом относительно сложения и умножения, заданных в K.

Критерий подкольца: $L \subseteq K$ - подкольцо в кольце $K \quad \Longleftrightarrow \quad$ Выполнены два условия:

1. $\forall x, y \in L : x - y \in L$ (критеорий подгруппы в $(K, +)$);
2. $\forall x, y \in L : x \cdot y \in L$ (замкнутость по умножению).

Кольцо с единицей - кольцо с нейтральным элементом по умножению (*единицей*).

Утверждение: Если в кольце K с единицей выполняется $0 = 1$, то $K = \{0\}$.

□ $\forall a \in K : a = a \cdot 1 = a \cdot 0 = 0$ ■

Кольцо $(K, +, \cdot)$ ***коммутативно***, если $\forall a, b \in K : a \cdot b = b \cdot a$.

5.2. Делители нуля

Если в кольце K для некоторых $a, b \in K$ выполняется $a \cdot b = 0 \wedge a \neq 0 \wedge b \neq 0$, то a - ***левый делитель нуля*** и b - ***правый делитель нуля***.

Утверждение: в кольце K всегда выполняется $\forall a \in K : a \cdot 0 = 0 \cdot a = 0$.

□

$$\begin{gathered} a + 0 = a \\ \Downarrow \\ a \cdot (a + 0) = a \cdot a \\ \Downarrow \\ a^2 + a \cdot 0 = a^2 \\ \Downarrow \\ a \cdot 0 = 0 \end{gathered}$$

Для умножение на 0 слева - аналогично.

■

Целостное кольцо (*область целостности*) - *коммутативное* кольцо с единицей, не равной нулю, и *без делителей нуля*.

Утверждение: Коммутативное кольцо с единицей, не равной нулю, целостное $\Longleftrightarrow$ в нём выполняется закон сокращения $a \cdot b = a \cdot c \wedge a \neq 0 \quad \Rightarrow \quad b = c$.

□

$\Longrightarrow$

$a \cdot b = a \cdot c \quad \Rightarrow \quad a(b - c) = 0$

Так как нет делителей нуля, то $b = c$.

$\Longleftarrow$

Пусть $a \cdot b = 0 \land a \neq 0$. Тогда по закону сокращения $a \cdot b = a \cdot 0 \;\Rightarrow\; b = 0$.

■

5.3. Идеалы

Идеал (*двухсторонний* идеал) - подмножество $I \subseteq K$ кольца K, которое:

1. Является подгруппой по сложению в K;
2. “Поглощает” элементы по умножению: $\forall a \in I \;\; \forall r \in K : r \cdot a \in I \land a \cdot r \in I$.

Любой идеал $I \subseteq K$ является *подкольцом* в K.

В коммутативном колце K:
$\forall a \in K : \; <a> = \{r \cdot a \mid r \in K\}$ является идеалом.

Главный идеал $I \subseteq K$ - такой, что $\exists a \in K : I = \; <a>$ (порождён одним элементом).

Кольцо главных идеалов - такое, в котором все идеалы главные. (например, кольцо $\mathbb{Z}$ целых чисел - в нём все подгруппы имеют вид $k\mathbb{Z} = \; <k>$)

Любой идеал является *нормальной* подгруппой в $(K, +)$, так как $(K, +)$ - *абелева* группа. Значит, можно по некоторому идеалу $I \subseteq K$ рассмотреть *факторгруппу* с операцией сложения $(K/I, +)$:

$$\forall a, b \in K : (a + I) + (b + I) = (a + b) + I$$

Введём на ней ужножение $(a + I) \cdot (b + I) = a \cdot b + I$. Оно корректно:

$$(a + I) \cdot (b + I) = a \cdot b + a \cdot I + b \cdot I + I = a \cdot b + I$$

(Так как $a \cdot I \in I \land I \cdot b \in I$ по определению идеала.)

Факторкольцо $(K/I, +, \cdot)$ кольца K по идеалу $I \subseteq K$ - это факторгруппа $(K/I, +)$ (задана выше) с операцией умножения (задана выше).

5.4. Гомоморфизм колец

Гомоморфизм колец - отображение $\varphi : (K_1, +, \cdot) \to (K_2, \oplus, \star)$, в котором $\forall x, y \in K_1$ выполняется:

1. $\varphi(x + y) = \varphi(x) \oplus \varphi(y)$;
2. $\varphi(x \cdot y) = \varphi(x) \star \varphi(y)$.

Ядро гомоморфизма колец $\varphi : K_1 \to K_2$:

$$\operatorname{Ker} \varphi = \{r \in K_1 \mid \varphi(r) = 0\} \subseteq K_1$$

Образ гомоморфизма колец $\varphi : K_1 \to K_2$:

$$\operatorname{Im} \varphi = \{\varphi(r) \mid r \in K_1\} \subseteq K_2$$

Пусть $\varphi : K_1 \to K_2$ - гомоморфизм колец.
Лемма 1: $\mathrm{Ker}\ \varphi$ - идеал в K_1.

□
1. Является подгруппой по сложению: φ - гомоморфизм колец, а значит и гомоморфизм групп $(K_1, +)$ и $(K_2, \oplus)$. Следовательно, $\mathrm{Ker}\ \varphi$ - подгруппа в $(K_1, +)$ (доказано ранее).
2. “Поглощает” элементы по умножению. $\forall a \in \mathrm{Ker}\ f \quad \forall r \in K_1$:

$$\varphi(a \cdot r) = \varphi(a) \cdot \varphi(r) = 0 \cdot \varphi(r) = 0 \quad \Longrightarrow \quad a \cdot r \in \mathrm{Ker}\ \varphi$$
$$\varphi(r \cdot a) = \varphi(r) \cdot \varphi(a) = \varphi(r) \cdot 0 = 0 \quad \Longrightarrow \quad r \cdot a \in \mathrm{Ker}\ \varphi$$

Значит, $\mathrm{Ker}\ \varphi$ - идеал в K_1 по определению.
■

Пусть $\varphi : K_1 \to K_2$ - гомоморфизм колец.
Лемма 2: $\mathrm{Im}\ \varphi$ - подкольцо в K_2.

□
Если $a, b \in \mathrm{Im}\ \varphi$, то $\exists a', b' \in K_1 : \varphi(a') = a \wedge \varphi(b') = b$. Значит $\forall a, b \in \mathrm{Im}\ \varphi$:
1. $a - b = \varphi(a') - \varphi(b') = \varphi(a' - b') \in \mathrm{Im}\ \varphi$
2. $a \cdot b = \varphi(a') \cdot \varphi(b') = \varphi(a' \cdot b') \in \mathrm{Im}\ \varphi$

Значит, $\mathrm{Im}\ \varphi$ - подкольцо в K_2 по *критерию подкольца*.
■

Пусть $\varphi : K_1 \to K_2$ - гомоморфизм колец.
Теорема о гомоморфизме колец: Факторкольцо кольца K_1 по ядру гомоморфизма φ изоморфно образу гомоморфизма φ:

$$K_1 / \mathrm{Ker}\ \varphi \cong \mathrm{Im}\ \varphi$$

□
$\mathrm{Ker}\ f = I$ - идеал по *лемме 1*. Значит, факторкольцо $K_1 / \mathrm{Ker}\ \varphi$ задано корректно.
$\mathrm{Im}\ \varphi$ - подкольцо в K_2 по *лемме 2*.
Рассмотрим отображение колец $\tau : K_1 / I \to \mathrm{Im}\ \varphi$, где $\tau(a + I) = \varphi(a)$. Из доказательства теоремы о гомоморфизме групп, τ - изоморфизм групп по сложению $(K_1 / I, +)$ и $(\mathrm{Im}\ \varphi, +)$ (так как τ корректно задано, является гомоморфизмом и биективно). Проверим, что τ “уважает” и умножение:

$$\tau((a + I) \cdot (b + I)) = \tau(a \cdot b + I) = \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) = \tau(a + I) \cdot \tau(b + I)$$

Значит, τ - изоморфизм колец $K_1 / \mathrm{Ker}\ \varphi$ и $\mathrm{Im}\ \varphi$.
■

6. Поля

6.1. Определение

Обратимый элемент a кольца K с единицей - такой, что:

$$\exists a^{-1} \in K : a \cdot a^{-1} = a^{-1} \cdot a = 1$$

Утверждение: все *обратимые* элементы кольца K с единицей образуют группу по умножению - *мультипликативную подгруппу кольца $U(K)$*.

□
Единица включена в группу: $1 \in U(K)$
Обратный элемент к каждому включен в группу: $\left(a^{-1}\right)^{-1} = a \;\Rightarrow\; a^{-1} \in U(K)$
Замкнутость по умножению: $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1} \;\Rightarrow\; a \cdot b \in U(K)$
■

Поле - это коммутативное кольцо с единицей, в котором каждый элемент кроме нуля обратим.

6.2. Алгоритм Евклида

Рассмотрим $K[x]$ - кольцо многочленов с коэффициентами из *целостного* кольца K.
Пусть $g(x) \in K[x]$ - некоторый многочлен, старший коэффициент которого обратим в K. Тогда:

$$\forall f(x) \in K[x] \;\; \exists! q(x), r(x) \in K[x] : f(x) = g(x)q(x) + r(x) \;\;, \quad \deg r(x) < \deg g(x)$$

Другими словами, $f(x)$ разделим с остатком на $g(x)$.

Пусть $F[x]$ - кольцо многочленов над полем F.
Тогда для любых многочленов $a(x), b(x) \in F[x]$ можно найти $\gcd(a(x), b(x))$ с помощью ***алгоритма Евклида*** - будем последовательно делить с остатком, пока не получим остаток, равный нулю:

$$\begin{gathered}
a = b \cdot q_1 + r_1, \quad \deg r_1 < \deg b \\
b = r_1 \cdot q_2 + r_2, \quad \deg r_2 < \deg r_1 \\
\vdots \\
r_{k-2} = r_{k-1} \cdot q_k + r_k, \quad \deg r_k < \deg r_{k-1} \\
r_{k-1} = r_k \cdot q_{k+1} + r_{k+1}, \quad r_{k+1} = 0
\end{gathered}$$

Получаем $\gcd(a(x), b(x)) = r_k(x)$.

Пусть $F[x]$ - кольцо многочленов над полем F.
Следствие из алгоритма Евклида: для любых многочленов $a(x), b(x) \in F[x]$ существуют такие многочлены $u(x), v(x) \in F[x]$, что выполняется $\gcd(a, b) = a \cdot u + b \cdot v$:

$$\forall a(x), b(x) \in F[x] \;\; \exists u(x), v(x) \in F[x] : \gcd(a, b) = a \cdot u + b \cdot v$$

□

По алгоритму Евклида:

$$r_1 = a + b \cdot (-q_1)$$
$$r_2 = b - (a - b \cdot q_1) = a \cdot (-1) + b \cdot (1 + q_1)$$
$$\vdots$$
$$r_k = a \cdot (\ldots) + b \cdot (\ldots) = \gcd(a, b)$$

■

Пусть K - коммутативное кольцо с единицей.
Взаимно простые элементы $a, b \in K$ - такие, что выполняется:

$$\exists x, y \in K : a \cdot x + b \cdot y = 1$$

6.3. Характеристика поля

Характеристика поля (обозначают $\operatorname{char} P$) - такое наименьшее натуральное q, что $1 + \ldots + 1 = q \cdot 1 = 0$. Если такого $q \in \mathbb{N}$ не существует, то $\operatorname{char} P = 0$.

Утверждение: $\mathbb{Z}_p$ является полем $\iff$ p - простое число.

□

$\Longrightarrow$

Предположим противное: $p = l \cdot k$ - составное число, где $1 < l, k < p$.
Тогда $\overline{l} \cdot \overline{k} = \overline{p} = \overline{0}$, то есть $\overline{l}$ и $\overline{k}$ - делители нуля. Они не обратимы:

$$\exists l^{-1} \quad \Rightarrow \quad l^{-1} \cdot l \cdot k = 1 \cdot k = k = l^{-1} \cdot 0 = 0$$

Противоречие с определением поля.

$\Longleftarrow$

$\mathbb{Z}_p$ - коммутативное кольцо с единицей. Покажем, что

$$\forall a \in \mathbb{Z}_p, a \neq 0 \quad \exists a^{-1}$$

. Если p - простое, то числа $1, 2, \ldots, p - 1$ взаимно просты с p. Значит:

$$\forall a \in \mathbb{Z}_p, a \neq 0 : \gcd(a, p) = 1$$

По следствию из алгоритма Евклида $\exists u, v \in \mathbb{N}$:

$$a \cdot u + p \cdot v = 1$$
$$\Downarrow$$
$$a \cdot u \equiv 1 \pmod p$$
$$\Downarrow$$
$$\overline{a} \cdot \overline{u} = \overline{1}$$
$$\Downarrow$$
$$\overline{u} \text{ - обратный для } \overline{a}$$

■

Утверждение: Любое поле характеристики 0 бесконечно.

□

$1 \cdot 1, 2 \cdot 1, 3 \cdot 1$ и так далеее - это различные числа: если $k \cdot 1 = l \cdot 1 \wedge k < l$, то $(l - k) \cdot 1 = 0$, а значит $\operatorname{char} P > 0$. Значит, число элеметов как минимум счётное.

■

Утверждение: характеристика поля либо равна 0, либо является простым числом.

□

Предположим противное: Пусть $\operatorname{char} P = m \cdot k = p \neq 0$, где $1 < m, k < p \wedge m, k \in \mathbb{N}$. Тогда по дистрибутивности:

$$0 = p \cdot 1 = (m \cdot 1) \cdot (k \cdot 1)$$

Так как p - минимальное число q такое, что $q \cdot 1 = 0$, то $m \cdot 1 \neq 0 \wedge k \cdot 1 \neq 0$. Значит, есть делители нуля, которые не обратимы. Противоречие.

■

6.4. Подполя

Подполе - подмножество в поле P, которое само является полем относительно сложения и умножения, заданных в P.

Пересечение двух подполей одного и того же поля является подполем.

Простое подполе - наименьшее по вложению (т.е. не имеющее собственных подполей) подполе.

Пусть P - поле, P_0 - его простое подполе.
Утверждение:
1. Если $\operatorname{char} P = p > 0$, то $P_0 \cong \mathbb{Z}_p$;
2. Если $\operatorname{char} P = 0$, то $P_0 \cong \mathbb{Q}$.

□

Рассмотрим $<1> \subseteq (P, +)$ - циклическую группу по сложению, порождённую “единицей”. Заметим, что $<1>$ - подкольцо. Так как любое подполе содержит единицу, то $<1> \subseteq P_0$.
1. $\operatorname{char} P = p > 0 \implies <1> \cong \mathbb{Z}_p \implies \mathbb{Z}_p \subseteq P_0$ (изоморфизмы считаем неразличимыми). Но $\mathbb{Z}_p$ - поле, а P_0 - наименьшее подполе. Значит, $P_0 \cong \mathbb{Z}_p$.
2. $\operatorname{char} P = 0 \implies <1> \cong \mathbb{Z} \implies \mathbb{Z} \subseteq P_0$. Но в P_0 должны быть и все обратные элементы вида $a \cdot b^{-1} = \frac{a}{b}$, где $a, b \in \mathbb{Z}, b \neq 0$ (а также в P_0 должны быть всевозможные произведения элементов). Значит, $\mathbb{Q} \subseteq P_0$ (изоморфизмы считаем неразличимыми). Так как P_0 - минимальное подполе, то $P_0 \cong \mathbb{Q}$.

■

Если P_1 - подполе в P_2, то поле P_2 является ***расширением*** поля P_1.

Любое поле является расширением своего простого поля, и у них одинаковая характеристика.

Пусть поле P_2 - расширение поля P_1.
Алгебраический элемент над полем P_1 - такой элемент $\alpha \in P_2$, что:

$$\exists f(x) \in P_1[x], f(x) \not\equiv 0 : f(\alpha) = 0$$

Трансцендентное число - число, не является алгебраическим элементом.

Пусть $\mathbb{F}$ - поле.
Теорема (док-во не приводится): для любого многочлена $f(x) \in \mathbb{F}[x]$ из кольца многочленов над $\mathbb{F}$ существует расширение $\mathbb{F}_1$ этого поля ($\mathbb{F} \subseteq \mathbb{F}_1$), в котором многочлен $f(x)$ имеет корень.

6.5. Факторкольцо кольца многочленов

Пусть $\mathbb{F}[x]$ - кольцо многочленов с коэффициентами из поля $\mathbb{F}$.
Пусть $<f(x)>$ - идеал, порождённый элементом $f(x)$.
Теорема: Факторкольцо $\mathbb{F}[x] / <f(x)>$ является полем $\iff$ многочлен $f(x)$ неприводим над $\mathbb{F}$.

□
$\Longrightarrow$
Предположим противное: пусть $f(x)$ приводим, то есть

$$f(x) = f_1(x) \cdot f_2(x) \text{, где } \deg f_1 < \deg f \wedge \deg f_2 < \deg f$$

Тогда $\overline{f_1(x)}$ и $\overline{f_2(x)}$ - смежные классы и $\overline{f_1(x)} \cdot \overline{f_2(x)} = \overline{f(x)} = \overline{0}$. Получаем противоречие - в факторкольце есть делители нуля.
$\Longleftarrow$
Докажем, что для любого смежного класса $\overline{a(x)} \not\equiv 0$ существует обратный элемент.
Пусть $a(x)$ - представитель смежного класса $\overline{a(x)}$ и $\deg a < \deg f$.
Так как $f(x)$ неприводим, то $\gcd(a(x), f(x)) = 1$. Значит, по следствию из алгоритма Евклида:

$$\exists u(x), v(x) \in \mathbb{F}[x] : a(x) \cdot u(x) + f(x) \cdot v(x) = 1$$

Значит:

$$\overline{a(x) \cdot u(x)} + \overline{f(x) \cdot v(x)} = \overline{1} \pmod{<f(x)>}$$
$$\Downarrow$$
$$\overline{a(x)} \cdot \overline{u(x)} = \overline{1} \pmod{<f(x)>}$$
$$\Downarrow$$
$$u(x) \text{ обратный для } a(x)$$

■

Теорема (док-во не приводится):
1. Пусть $\mathbb{F}_q$ - *конечное* поле размера $|\mathbb{F}_q| = q$. Тогда $q = p^n$, где p - простое число и $n \in N$.
2. Для любого простого p и любого $n \in N$ существует единственное поле из p^n элементов. (изоморфные поля считаем неразличимыми)

Пусть $\mathbb{F}_q$ - *конечное* поле размера $|\mathbb{F}_q| = q = p^n$.
Теорема (док-во не приводится): поле $\mathbb{F}_q$ изоморфно факторкольцу $\mathbb{Z}_p[x]$ / $\langle h(x) \rangle$, где $h(x)$ - неприводимый многочлен n-й степени над $\mathbb{Z}_p$.

7. Применение в криптографии

В криптографии, как правило, используются две "односторонние" функции:

1. *Показательная*. Обратная - *дискретное логарифмирование*.
2. *Умножение*. Обратная - *разложение на множители*.

Пусть G - конечная группа и $g \in G$, причём $\operatorname{ord} g$ достаточно большой.
Задача ***дискретного логарифмирования*** заключается в том, чтобы для некоторого $a \in G$ найти такое число k, что $g^k = a$.

7.1. Протокол шифрования Диффи-Хеллмана

Всем известна конечная группа G и элемент $g \in G$. *Участник А* фиксирует секретное натуральное число a, и сообщает всем *открытый ключ* g^a. Аналогично *участник Б* фиксирует секретное натуральное число b, и сообщает всем *открытый ключ* g^b.

Тогда *участник А*, имея a и g^b, может вычислить $\left(g^b\right)^a = g^{a \cdot b}$. Аналогично *участник Б*, имея b и g^a, может вычислить $(g^a)^b = g^{a \cdot b}$.

Тогда $g^{a \cdot b}$ известно только этим двоим участникам, и это значение может использоваться как ключ для секретной переписки.

7.2. Криптосистема Эль-Гамаля

Всем известна конечная группа G и элемент $g \in G$. *Участник А* фиксирует *закрытый ключ* $a \in \mathbb{N}$, и сообщает всем *открытый ключ* g^a.

Если *участник Б* хочет передать *участнику А* секретное сообщение $M \in G$, то выбирает некоторое $k \in \mathbb{N}$ и отправляет *участнику А* пару чисел $\left(g^k, M \cdot g^{a \cdot k}\right)$.

Тогда *участник А* может расшифровать это секретное сообщение:

$$M \cdot g^{a \cdot k} \cdot \left(g^k\right)^{|G| - a} = M \cdot g^{a \cdot k} \cdot g^{|G| \cdot k} \cdot g^{-a \cdot k} = M \cdot g^{a \cdot k} \cdot e \cdot g^{-a \cdot k} = M$$

В качестве группы G обычно используют $\mathbb{Z}_p^* = \left(\mathbb{Z}_p \setminus \{0\}, \cdot\right)$, где p - простое число. Это циклическая группа.

=== the end ===