Дискретные структуры

осень 2013

Александр Дайняк

www.dainiak.com

Группы

Группа — это множество $\mathbb{G}$ с заданной на нём бинарной операцией $\circ$, которая удовлетворяет свойствам:

- Ассоциативность: $\forall a, b, c \in \mathbb{G}$
$$(a \circ b) \circ c = a \circ (b \circ c)$$
- Существование нейтрального элемента:
$$\exists e \in \mathbb{G}: \quad \forall a \in \mathbb{G} \qquad a \circ e = e \circ a = a$$
- Существование обратных элементов:
$$\forall a \in \mathbb{G} \quad \exists b \in \mathbb{G}: \qquad a \circ b = b \circ a = e$$

Примеры групп

Группами, например, являются:

- множество $\mathbb{Z}$ относительно операции сложения чисел,
- множество чётных чисел относительно сложения чисел,
- множество $\mathbb{Q}$ относительно операции сложения чисел,
- множество $\mathbb{Q} \setminus \{0\}$ относительно операции умножения чисел,
- множество $\mathbb{R}^n$ относительно операции покоординатного сложения векторов.
- множество невырожденных матриц из $\mathbb{R}^{n \times n}$ относительно операции умножения матриц.

Группами *не являются*, например:

- множество $\mathbb{Z} \setminus \{0\}$ относительно операции умножения чисел,
- множество нечётных чисел относительно сложения чисел,
- множество всех матриц $\mathbb{R}^{n \times n}$ относительно операции умножения матриц.

Геометрические примеры

Группой является множество всевозможных поворотов плоскости относительно начала координат.

Операция $a \circ b$ означает, что сначала выполняется поворот a, а затем b (*композиция*).

- $(a \circ b) \circ c = a \circ (b \circ c)$ — очевидно
- Нейтральный элемент — поворот на 0^{o}
- Обратный элемент к повороту на угол α — поворот на угол $(-\alpha)$.

Единственность нейтрального и обратных элементов

Утверждение.
В любой группе нейтральный элемент единственный.

Доказательство:
Пусть e' и e'' — нейтральные элементы.

Т.к. e'' нейтральный, то $e' \circ e'' = e'$.

Т.к. e' нейтральный, то $e' \circ e'' = e''$.

Отсюда $e' = e''$.

Единственность нейтрального и обратных элементов

Утверждение.
В любой группе для любого элемента a
обратный к a элемент единственный.

Доказательство:
Пусть b' и b'' — обратные к a элементы.
Тогда

$$b' = b' \circ e = b' \circ (a \circ b'') = (b' \circ a) \circ b'' = e \circ b'' = b''$$

Изоморфизм групп

Группы $(\mathbb{G}', \circ)$ и $(\mathbb{G}'', \blacksquare)$ *изоморфны*, если существует биекция $\phi\colon \mathbb{G}' \leftrightarrow \mathbb{G}''$, такая, что

$$\forall a, b \in \mathbb{G}' \quad \phi(a) \blacksquare \phi(b) = \phi(a \circ b)$$

Изоморфизм ϕ всегда отображает нейтральный элемент в нейтральный:

$$\phi(e_{\mathbb{G}'}) = e_{\mathbb{G}''}$$

Кроме того, если a и b — взаимно обратные элементы в $\mathbb{G}'$, то $\phi(a)$ и $\phi(b)$ будут взаимно обратными в $\mathbb{G}''$. **(← упражнения!)**

Изоморфизм групп

Примеры:

- Группа $(\mathbb{Z}, +)$ изоморфна группе чётных чисел с операцией сложения.
  Изоморфизм: $x \to 2x$
- Группа поворотов плоскости на угол, кратный $\frac{\pi}{2}$,
  с операцией композиции изоморфна группе чисел $\{0,1,2,3\}$
  с операцией сложения по модулю 4.

Подгруппы

Если $(\mathbb{G},\circ)$ — группа, $\mathbb{H} \subseteq \mathbb{G}$ и $\mathbb{H}$ является группой относительно операции $\circ$, то $\mathbb{H}$ называется *подгруппой* группы $\mathbb{G}$.

Обозначение: $\mathbb{H} \leq \mathbb{G}$.

Примеры:

- При каждом фиксированном k все числа, делящиеся на k, образуют подгруппу в $(\mathbb{Z}, +)$
- Целые числа образуют подгруппу в группе $(\mathbb{R}, +)$

Аддитивные и мультипликативные обозначения

Операция $\circ$ часто обозначается также знаком «$+$» или «$\cdot$». Тогда обозначения такие:

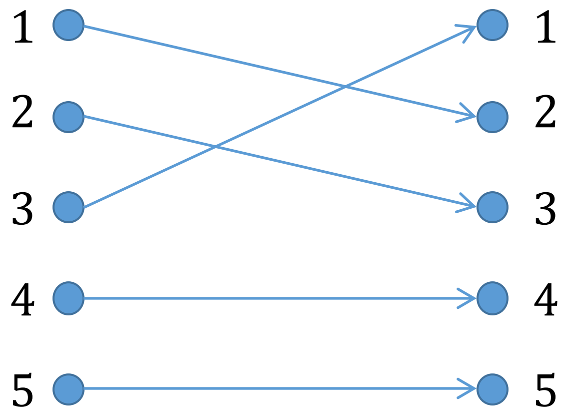
Общая запись	В обозначении «$+$»	В обозначении «$\cdot$»
$a \circ b$	$a + b$	$a \cdot b$ или просто ab
Нейтральный элемент e	0	1
Обратный элемент к элементу a	$-a$	a^{-1}
$\underbrace{a \circ a \circ \cdots \circ a}_{n \text{ раз}}$	na	a^n

Вместо $a + (-b)$ сокращённо пишут: $a - b$.

Вместо $a \cdot b^{-1}$ сокращённо пишут: a/b.

Группы подстановок

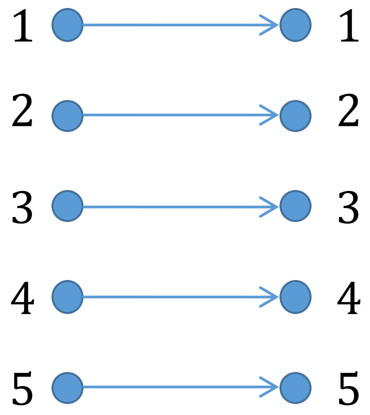
Подстановка (перестановка) — это биекция множества на себя:



Обозначение: 23145

Группы подстановок

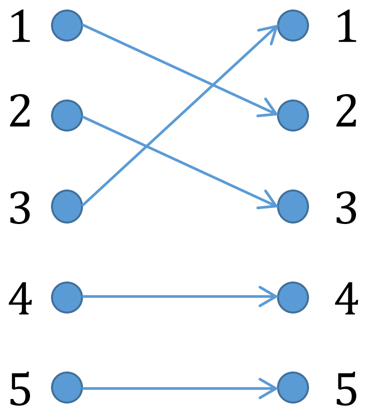
Тождественная подстановка:



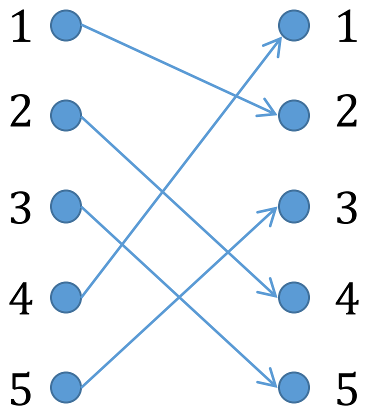
$$1$$

Группы подстановок

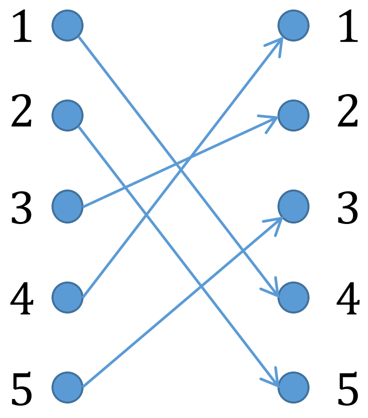
Композиция подстановок:



σ_1



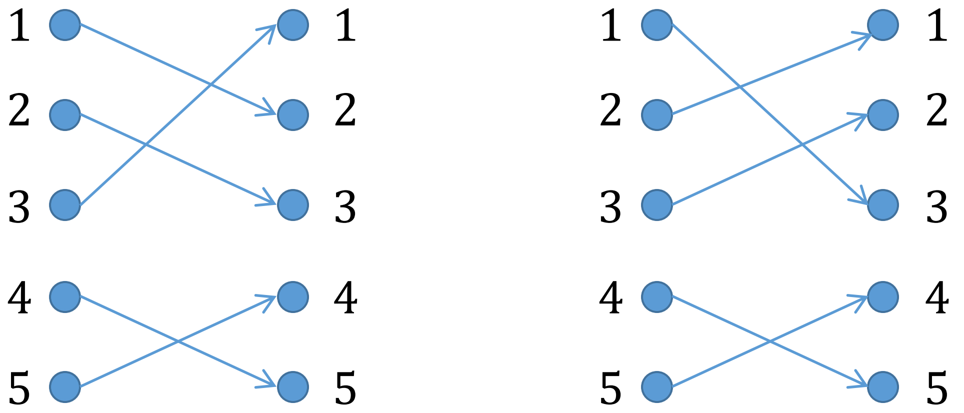
σ_2



$\sigma_1\sigma_2$

Группы подстановок

Обратная подстановка:



σ σ^{-1}

Группы подстановок

Совокупность всех подстановок на множестве $\{1,2,\ldots,n\}$ образует группу относительно композиции (последовательного применения).

Эта группа называется *симметрической группой* и обозначается $\mathbb{S}_n$.

Очевидно,

$$|\mathbb{S}_n| = n!$$

Упражнение.
Подстановки на множестве $\{1,2,\ldots,n\}$, оставляющие элемент k неподвижным, образуют подгруппу в группе $\mathbb{S}_n$. Эта подгруппа оказывается изоморфной группе $\mathbb{S}_{n-1}$.

Теорема Кэли

Теорема.
Любая конечная группа изоморфна некоторой группе подстановок.

Доказательство: предъявим изоморфизм.

Пусть $\mathbb{G} = \{g_1, g_2, \dots, g_n\}$.

Каждому элементу $a \in \mathbb{G}$ сопоставим перестановку σ_a на множестве $\mathbb{G}$:

$$\sigma_a(g_1) \coloneqq g_1 \circ a$$
$$\vdots$$
$$\sigma_a(g_n) \coloneqq g_n \circ a$$

Теорема Кэли

$$\sigma_a(g_1) \coloneqq g_1 \circ a$$
$$\vdots$$
$$\sigma_a(g_n) \coloneqq g_n \circ a$$

Каждое отображение σ_a — это действительно перестановка, т.к. при $i \neq j$ имеем

$$g_i \circ a \neq g_j \circ a$$

Очевидно также, что при $a \neq b$ имеем $\sigma_a \neq \sigma_b$, то есть рассматриваемое сопоставление элементам $\mathbb{G}$ перестановок является биекцией из $\mathbb{G}$ в $\{\sigma_{g_1}, \dots, \sigma_{g_n}\}$.

Теорема Кэли

$$\sigma_a(g_1) \coloneqq g_1 \circ a$$
$$\vdots$$
$$\sigma_a(g_n) \coloneqq g_n \circ a$$

Пусть σ_a и σ_b — перестановки, сопоставленные элементам $a, b \in \mathbb{G}$.
Посмотрим, как себя ведёт композиция этих перестановок $\sigma_a \sigma_b$.

Пусть $g \in \mathbb{G}$. Имеем

$$(\sigma_a \sigma_b)(g) = \sigma_b(g \circ a) = (g \circ a) \circ b = \sigma_{a \circ b}(g)$$

Осталось показать, что $\{\sigma_{g_1}, \dots, \sigma_{g_n}\}$ — группа.

Теорема Кэли

$$\sigma_a(g_1) \coloneqq g_1 \circ a$$
$$\vdots$$
$$\sigma_a(g_n) \coloneqq g_n \circ a$$

Множество перестановок $\{\sigma_{g_1}, \dots, \sigma_{g_n}\}$ является группой относительно операции композиции:

- Нейтральная перестановка у нас есть — это σ_e, где e — нейтральный элемент в $\mathbb{G}$.
- Обратная перестановка к σ_a — это σ_b, где элемент b обратен к a в $\mathbb{G}$:

$$\sigma_a \sigma_b(x) = x \circ a \circ b = x \circ e = x$$

Эквивалентное определение группы

Группу можно определить как множество $\mathbb{G}$ с ассоциативной операцией $\circ$, такой, что для любых $a, b \in \mathbb{G}$ существуют решения (относительно x) уравнений

$$a \circ x = b \quad \text{и} \quad x \circ a = b$$

Доказательство:
Будем работать в мультипликативных обозначениях.
Если $\mathbb{G}$ группа, и $ax = b$, то

$$x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}b$$

то есть x существует и определён однозначно.

Аналогично разбираемся с уравнением $xa = b$.

Эквивалентное определение группы

Обратно, пусть уравнения вида $ax = b$ и $xa = b$ разрешимы в $\mathbb{G}$.

Докажем существование нейтрального элемента.

Зафиксируем $a \in \mathbb{G}$.

Пусть e_{left} — решение уравнения $xa = a$.

Пусть $b \in \mathbb{G}$ — произвольный элемент в $\mathbb{G}$.

Пусть c — решение уравнения $ax = b$.

Имеем

$$e_{\text{left}}b = e_{\text{left}}(ac) = (e_{\text{left}}a)c = ac = b$$

Эквивалентное определение группы

Итак, $\forall b \in \mathbb{G}$ мы имеем $e_{\text{left}} b = b$.

Пусть e_{right} — решение уравнения $ax = a$.

Пусть d — решение уравнения $xa = b$.

Имеем

$$be_{\text{right}} = (da)e_{\text{right}} = d\left(ae_{\text{right}}\right) = da = b$$

Таким образом, $\forall b \in \mathbb{G}$ выполнено $be_{\text{right}} = b$.

Кроме того $e_{\text{left}} = e_{\text{left}} e_{\text{right}} = e_{\text{right}}$,
то есть $e := e_{\text{left}} = e_{\text{right}}$ — «полноценный» нейтральный элемент в $\mathbb{G}$.

Эквивалентное определение группы

Существование нейтрального элемента $e \in \mathbb{G}$ доказано. Осталось доказать существование обратных элементов.

Для любого a пусть a_{left}^{-1} и a_{right}^{-1} — решения уравнений $xa = e$ и $ax = e$ соответственно.

Достаточно показать, что $a_{\mathrm{left}}^{-1} = a_{\mathrm{right}}^{-1}$.
Имеем

$$a_{\mathrm{left}}^{-1} = a_{\mathrm{left}}^{-1}\, e = a_{\mathrm{left}}^{-1}\, a\, a_{\mathrm{right}}^{-1} = e a_{\mathrm{right}}^{-1} = a_{\mathrm{right}}^{-1}$$

что и требовалось.

«Сдвиги» множеств

Пусть $(\mathbb{G},\circ)$ — группа.

Для элемента $a \in \mathbb{G}$ и подмножества $S \subseteq \mathbb{G}$ обозначают

$$a \circ S \coloneqq \{a \circ s \mid s \in S\}$$

и

$$S \circ a \coloneqq \{s \circ a \mid s \in S\}$$

Мощности «сдвигов» множеств

Утверждение.
Для любого $a \in \mathbb{G}$ и любого $S \subseteq \mathbb{G}$ имеем

$$|a \circ S| = |S \circ a| = |S|$$

Доказательство (здесь и до конца лекции в мультипликативных обозначениях):

Пусть $S = \{a_1, \dots, a_m\}$, где $m \coloneqq |S|$.

Зафиксируем любой элемент $a \in \mathbb{G}$ и любые i, j. Если $aa_i = aa_j$, то $a^{-1}aa_i = a^{-1}aa_j$, откуда $a_i = a_j$.

Значит, все элементы $aa_1, aa_2 \dots, aa_m$ различны.

Смежные классы

Пусть $\mathbb{H} \leq \mathbb{G}$ и $a \in \mathbb{G}$.

Множество $a \circ \mathbb{H}$ называется *левым смежным классом элемента* a *по подгруппе* $\mathbb{H}$.

Аналогично, множество $\mathbb{H} \circ a$ называется *правым смежным классом*.

(Для групп, в которых операция коммутативна, соответствующие левые и правые смежные классы совпадают.)

Примеры смежных классов

Примеры:

- Множество чисел вида $7 + 3k$ образует смежный класс в абелевой группе $(\mathbb{Z}, +)$
- Совокупность перестановок на множестве $\{1,2, \dots, n\}$, меняющих друг с другом местами элементы i и j, образует смежный класс в группе $\mathbb{S}_n$

Смежные классы

Утверждение.
Различные левые смежные классы по одной и той же подгруппе не пересекаются.
Это же справедливо и для правых смежных классов.

Доказательство:

Пусть $\mathbb{H} \leq \mathbb{G}$ и $a', a'' \in \mathbb{G}$.

Допустим, что $a'\mathbb{H} \cap a''\mathbb{H} \neq \emptyset$ и покажем, что тогда $a'\mathbb{H} = a''\mathbb{H}$.

Если $a'\mathbb{H} \cap a''\mathbb{H} \ni b,$ то существуют $c, d \in \mathbb{H},$ такие, что

$$b = a'c = a''d$$

Смежные классы

$\exists c, d \in \mathbb{H}$ такие, что $a'c = a''d$.

Рассмотрим произвольный элемент $s \in a'\mathbb{H}$.

По определению, $\exists h \in \mathbb{H}$ такой, что $s = a'h$.

Имеем $s = a'h = a''(dc^{-1})h = a''(dc^{-1}h)$. То есть $s \in a''\mathbb{H}$.

Получили, что $a'\mathbb{H} \subseteq a''\mathbb{H}$.

Аналогично доказывается, что $a''\mathbb{H} \subseteq a'\mathbb{H}$.

Отсюда

$$a'\mathbb{H} = a''\mathbb{H}$$

Теорема Лагранжа

Теорема (Лагранжа о порядке подгруппы).
Если $\mathbb{H} \le \mathbb{G}$ и $|\mathbb{G}| < \infty$, то $|\mathbb{G}|$ делится на $|\mathbb{H}|$.

Доказательство:
Очевидно, любой элемент $a \in \mathbb{G}$ принадлежит некоторому смежному классу $\mathbb{H}$, например,

$$a \in a\mathbb{H}$$

Поэтому имеет место разбиение

$$\mathbb{G} = a_1\mathbb{H} \sqcup a_2\mathbb{H} \sqcup \cdots \sqcup a_m\mathbb{H}$$

где $a_i\mathbb{H}$ — различные смежные классы.

Так как $|a_i\mathbb{H}| = |\mathbb{H}|$ для каждого i, то $|\mathbb{G}| = m \cdot |\mathbb{H}|$.

Теорема Силова

Теорема. (Силова о существовании подгруппы)
Пусть $\mathbb{G}$ — конечная группа.
Для любого числа вида p^α, делящего $|\mathbb{G}|$, существует $\mathbb{H} \leq \mathbb{G}$, такая, что $|\mathbb{H}| = p^\alpha$.
(Здесь p простое, α произвольное натуральное.)

Доказательство:
Пусть $\beta \coloneqq \max\ \{x \mid |\mathbb{G}| \text{ делится на } p^x\}$.

Зафиксируем произвольное $\alpha \leq \beta$.

Доказательство теоремы Силова: мощность множества M

$|\mathbb{G}| = p^{\beta} l,$ где l не делится на p.

Положим $M \coloneqq \{S \subseteq \mathbb{G} \mid |S| = p^{\alpha}\}$. Имеем

$$|M| = \binom{p^{\beta} l}{p^{\alpha}} =$$

$$= \frac{p^{\beta} l \cdot (p^{\beta} l - 1) \cdot \ldots \cdot (p^{\beta} l - p^{\alpha} + 1)}{1 \cdot 2 \cdot \ldots \cdot p^{\alpha}} =$$

$$= p^{\beta-\alpha} l \cdot \prod_{k=1}^{p^{\alpha}-1} \frac{p^{\alpha}(p^{\beta-\alpha} l - 1) + k}{k}$$

Доказательство теоремы Силова: мощность множества M

$|\mathbb{G}| = p^{\beta} l,$ где l не делится на p.

Положим $M \coloneqq \{S \subseteq \mathbb{G} \mid |S| = p^{\alpha}\}$. Имеем

$$|M| = p^{\beta-\alpha} l \cdot \prod_{k=1}^{p^{\alpha}-1} \frac{p^{\alpha}\left(p^{\beta-\alpha} l - 1\right) + k}{k}$$

При $k < p^{\alpha}$ и $m \in \mathbb{N}$ степень, с которой p входит в разложение числа k, равна степени, с которой p входит в разложение числа $(p^{\alpha} m + k)$.

Поэтому наибольшая степень p, на которую делится $|M|$, равна $(\beta - \alpha)$.

Доказательство теоремы Силова: орбиты

$$M \coloneqq \{S \subseteq \mathbb{G} \mid |S| = p^{\alpha}\}$$

Для $S \subseteq \mathbb{G}$ и $g \in \mathbb{G}$ обозначим $Sg \coloneqq \{sg \mid s \in S\}$

Очевидно, если $S \in M$, то $Sg \in M$.

Орбитой множества S назовём

$$\operatorname{orb}(S) \coloneqq \{Sg \mid g \in \mathbb{G}\}$$

Для любого $S \in M$ имеем $S \in \operatorname{orb}(S) \subseteq M$.

Покажем, что если $\operatorname{orb}(S') \cap \operatorname{orb}(S'') \neq \emptyset$, то $\operatorname{orb}(S') = \operatorname{orb}(S'')$.

Допустим, что $\operatorname{orb}(S') \cap \operatorname{orb}(S'') \ni S$.

Доказательство теоремы Силова: различные орбиты не пересекаются

$$\mathrm{orb}(S) \coloneqq \{Sg \mid g \in \mathbb{G}\}$$

Допустим, что $\mathrm{orb}(S') \cap \mathrm{orb}(S'') \ni S$, тогда

$$\exists a, b \in \mathbb{G}: \qquad S'a = S''b$$

Отсюда $S' = S''ba^{-1}$.

Пусть $T \in \mathrm{orb}(S')$, т.е. $T = S'c$ для некоторого c.

Но тогда $T = S''(ba^{-1}c) \in \mathrm{orb}(S'')$.

Итак, $\mathrm{orb}(S') \subseteq \mathrm{orb}(S'')$.

Так же доказывается, что $\mathrm{orb}(S'') \subseteq \mathrm{orb}(S')$, и следовательно $\mathrm{orb}(S') = \mathrm{orb}(S'')$.

Доказательство теоремы Силова: подбираем специальную орбиту

$$M \coloneqq \{S \subseteq G \mid |S| = p^{\alpha}\}$$
$$\mathrm{orb}(S) \coloneqq \{Sg \mid g \in G\}$$
$$\forall S \in M \quad S \in \mathrm{orb}(S)$$
$$\mathrm{orb}(S') \cap \mathrm{orb}(S'') \neq \emptyset \quad \Rightarrow \quad \mathrm{orb}(S') = \mathrm{orb}(S'')$$

Следовательно, всё множество M разбивается на непересекающиеся орбиты: $\exists S_1, \dots, S_r$ такие, что

$$M = \mathrm{orb}(S_1) \sqcup \dots \sqcup \mathrm{orb}(S_r)$$

Наибольшая степень p, на которую делится $|M|$, равна $(\beta - \alpha)$, поэтому

$$\exists i: \quad |\mathrm{orb}(S_i)| \text{ не делится на } p^{\beta-\alpha+1}$$

Доказательство теоремы Силова: определяем искомую подгруппу

Зафиксируем $S \in M$, такое, что

$$\operatorname{orb}(S) = \{T_1, T_2, \dots, T_n\}$$

где n не делится на $p^{\beta-\alpha+1}$.

Положим $\mathbb{H} \coloneqq \{g \in \mathbb{G} \mid T_1 g = T_1\}$.

Если $g_1, g_2 \in \mathbb{H}$, то

$$T_1(g_1 g_2) = (T_1 g_1) g_2 = T_1 g_2 = T_1$$

то есть $g_1 g_2 \in \mathbb{H}$.

Доказательство теоремы Силова: определяем искомую подгруппу

Зафиксируем $S \in M$, такое, что

$$\operatorname{orb}(S) = \{T_1, T_2, \dots, T_n\}$$

где n не делится на $p^{\beta-\alpha+1}$.

Положим $\mathbb{H} \coloneqq \{g \in \mathbb{G} \mid T_1 g = T_1\}$.

Если $g_1, g_2 \in \mathbb{H}$, то $g_1 g_2 \in \mathbb{H}$. Если $g \in \mathbb{H}$, то

$$T_1 g^{-1} = (T_1 g) g^{-1} = T_1 (g g^{-1}) = T_1 e = T_1$$

то есть $g^{-1} \in \mathbb{H}$.

Отсюда $\mathbb{H}$ — подгруппа в $\mathbb{G}$.

Доказательство теоремы Силова: описываем смежные классы

$$\mathrm{orb}(S) = \{T_1, T_2, \dots, T_n\}$$
$$\mathbb{H} \coloneqq \{g \in \mathbb{G} \mid T_1 g = T_1\} \leq \mathbb{G}$$

Рассмотрим произвольный правый смежный класс $\mathbb{H}a$ по подгруппе $\mathbb{H}$.

Пусть $T_1 a = T_k$.

Рассмотрим произвольный элемент $g \in \mathbb{H}a$.

Т.к. $g = ha$ для некоторого $h \in \mathbb{H}$, то

$$T_1 g = T_1(ha) = (T_1 h)a = T_1 a = T_k$$

То есть оказалось, что $\mathbb{H}a = \{g \in \mathbb{G} \mid T_1 g = T_k\}$

Доказательство теоремы Силова: описываем смежные классы

$$\mathrm{orb}(S) = \{T_1, T_2, \dots, T_n\}$$
$$\mathbb{H} \coloneqq \{g \in \mathbb{G} \mid T_1 g = T_1\} \leq \mathbb{G}$$

Оказалось, что любой правый смежный класс по подгруппе $\mathbb{H}$ может быть представлен как

$$\{g \in \mathbb{G} \mid T_1 g = T_k\}$$

для некоторого k.

А значит, общее число различных смежных классов по $\mathbb{H}$ равно n.

Доказательство теоремы Силова: находим порядок подгруппы

$$\mathrm{orb}(S) = \{T_1, T_2, \dots, T_n\}$$
$$\mathbb{H} \coloneqq \{g \in \mathbb{G} \mid T_1 g = T_1\} \leq \mathbb{G}$$

Число различных смежных классов по $\mathbb{H}$ равно n.

Имеем

$$n \cdot |\mathbb{H}| = |G| = p^\beta l \quad \Rightarrow \quad |\mathbb{H}| = \frac{p^\beta l}{n}$$

и так как n не делится на $p^{\beta-\alpha+1}$, то

$$|\mathbb{H}| \text{ делится на } p^\alpha$$

Достаточно теперь показать, что $|\mathbb{H}| \leq p^\alpha$.

Доказательство теоремы Силова: находим порядок подгруппы

$$\operatorname{orb}(S) = \{T_1, T_2, \dots, T_n\}$$
$$\mathbb{H} \coloneqq \{g \in \mathbb{G} \mid T_1 g = T_1\} \leq \mathbb{G}$$

Возьмём произвольный $t \in T_1$.

Для любого $h \in \mathbb{H}$

$$th \in T_1 h = T_1$$

Отсюда

$$t\mathbb{H} \subseteq T_1$$

Следовательно $|\mathbb{H}| = |t\mathbb{H}| \leq |T_1| = p^\alpha$.

Теорема доказана.