Вступ до теорії груп. Короткий огляд

Аксіоми групи

Групою називається непорожня множина G, на якій задано бінарну алгебраїчну дію $*$, що задовольняє наступні аксіоми:
i. Замкненість: $\forall\, a, b \in G$: $a * b \in G$.
ii. Асоціативність: $(a * b) * c = a * (b * c)$, $\forall\, a, b, c \in G$.
iii. Існування нейтрального елемента: $\exists\, e \in G$, який називається нейтральним елементом G, такий, що $\forall\, a \in G$ виконується $a * e = e * a = a$.
iv. Існування оберненого: $\forall\, a \in G\ \exists\, a^{-1} \in G$, який називається оберненим до a, такий, що $a * a^{-1} = a^{-1} * a = e$.

Деякі властивості груп

i. Абелева група. Група G називається абелевою, якщо $a * b = b * a$ $\forall a, b \in G$.
ii. Скінченна група. Група G називається скінченною, якщо вона складається зі скінченної кількості елементів.
iii. Скорочення у групі. Якщо $a * b = a * c$, $\forall\, a, b, c \in G$, то $b = c$.
Якщо $b * a = c * a$, $\forall\, a, b, c \in G$, то $b = c$.
iv. Єдиність нейтрального та оберненого.
- У групі існує єдиний нейтральний елемент;
- $\forall\, a \in G$, a^{-1} визначений однозначно;
- $(a^{-1})^{-1} = a\ \forall\, a \in G$;
- $(a * b)^{-1} = (b^{-1})\ *\ (a^{-1})$;
- для $a_1, a_2, \ldots, a_n \in G$ значення виразу $a_1 * a_2 * \cdots * a_n$ не залежить від способу розстановки дужок.

Приклади груп

i. Діедральна група D_n — група рухів правильного n-кутника. Порядок групи $= 2n$.
ii. Симетрична група S_n — це група всіх бієктивних перетворень n-елементної множини. Порядок групи $= n!$
iii. Четверна група Кляйна K_4 — група рухів ромба, або ж група з 4 елементів, у якій кожний елемент є оберненим сам до себе.
iv. Група $\mathbb{Z}_n$ **лишків за модулем** $n \in \mathbb{N}$**.** Порядок групи $= n$.
v. Загальна лінійна група $GL_n(\mathbb{R})$ всіх невироджених матриць порядку n з дійсними коефіцієнтами. Нескінченна група.

Підгрупи

Нехай G — група. Непорожня підмножина H групи G називається **підгрупою**, якщо H є групою відносно заданої на G дії.
Критерій підгрупи. Непорожня підмножина H групи G є підгрупою $\Leftrightarrow$ $\forall\, x,\ y \in H:\ xy^{-1} \in H$.

Гомоморфізми та ізоморфізми

i. Гомоморфізм. Нехай $(G, *)$ та $(H, \circ)$ — групи.
Відображення $\varphi : G \to H$ називається **гомоморфізмом**, якщо $\varphi(x * y) = \varphi(x) \circ \varphi(y)\ \ \forall\, x, y \in G$.
ii. Ізоморфізм. Гомоморфізм $\varphi : G \to H$ називається **ізоморфізмом**, якщо φ є бієкцією.
iii. Автоморфізм. Ізоморфізм групи G на себе називається **автоморфізмом**. Множина всіх автоморфізмів групи G позначається $\mathrm{Aut}\, G$.

Теорема Келі

Теорема Келі: Кожна група ізоморфна деякій підгрупі симетричної групи. Якщо $|G| = n$, то G ізоморфна підгрупі групи S_n.

Порядок елемента

Порядком елемента називається найменше таке $n \in \mathbb{N}$, що $g^n = e$. Якщо такого n не існує, то порядок елемента вважають нескінченним. Позначається $\mathrm{ord}\, g$
i. $\mathrm{ord}(g^{-1}) = \mathrm{ord}(g)$.
ii. Якщо $\mathrm{ord}(g) = n$, то $g^m = e \Leftrightarrow n \mid m$.
iii. Якщо $\mathrm{ord}(g) = n$, то $\mathrm{ord}\, g^k = \frac{n}{(k,n)}$.

Циклічні групи

Підмножина X групи G називається **системою твірних** групи G, якщо кожний елемент $g \in G$ можна записати у вигляді добутку степенів елементів з X. Позначається $G = \langle X \rangle$.
Група G називається **циклічною**, якщо існує такий елемент $g \in G$, що всі елементи групи є його степенями. Позначається $G = \langle g \rangle$. Такий елемент g називається **твірним** групи G.

- Циклічна група може мати більше одного твірного.
- Всі циклічні групи абелеві.
- Усі нескінченні циклічні групи ізоморфні.
- Дві скінченні циклічні групи ізоморфні $\Leftrightarrow$ у них однакові порядки.

Класи суміжності та факторгрупи

Для довільних $N \leq G$ $g \in G$ множини
- $gN = \{gn \mid n \in N\} = \{g, gn_1, gn_2 \ldots\}$ та
- $Ng = \{ng \mid n \in N\} = \{g, n_1g, n_2g \ldots\}$ називаються лівим та правим класом суміжності G за N відповідно.

Підгрупа $N < G$ називається нормальною, якщо $gN = Ng\ \forall g \in G$. Позначається $N \lhd G$.
Критерій нормальної підгрупи. $N \lhd G \Leftrightarrow \forall g \in G\ \forall n \in N$: $g^{-1}ng \in N$.

Факторгрупа G за $N \lhd G$ — це група, елементами якої є класи суміжності gN з операцією $gN * hN = (g * h)N$.

Теорема Лагранжа

Теорема Лагранжа: У скінченній групі G порядок кожної її підгрупи H ділить порядок G.

Наслідки
- Якщо G — скінченна група, $H < G$, то кількість класів суміжності G за H дорівнює $\frac{|G|}{|H|}$.
- Якщо G — скінченна група та $g \in G$, то $\mathrm{ord}(g) \mid |G|$ та $g^{|G|} = e\ \forall\, g \in G$.
- Якщо G — група простого порядку, то G циклічна.

Лема Коші

Лема Коші: Якщо порядок скінченної групи ділиться на просте число p, то в групі є елемент порядку p.

Теореми про гомоморфізм

i. Перша теорема про гомоморфізм: Нехай $\varphi : G \to G'$ — гомоморфізм груп G та G'. Тоді $\mathrm{Ker}\, \varphi \lhd G$, $\mathrm{Im}\, \varphi < G'$ та $G/\mathrm{Ker}\, \varphi \simeq \mathrm{Im}\, \varphi$.
ii. Друга теорема про гомоморфізм: Нехай G — група, H — підгрупа групи G, N — нормальна підгрупа групи G. Тоді $HN < G$, $N \lhd HN$, $H \cap N \lhd H$ та $H/H \cap N \simeq HN/N$.
iii. Третя теорема про гомоморфізм: Нехай G — група, $N \lhd G$. Тоді існує взаємно однозначна відповідність між підгрупами G/N і підгрупами $H < G$, що містять N, та $H/N \lhd G/N \Leftrightarrow H \lhd G$ та $G/H \simeq (G/N)/(H/N)$.

Дія групи на множині

Дія групи G на множині M — це відображення з $M \times G$ в M, яке парі $(m, g) \in M \times G$ ставить у відповідність елемент $m^g \in M$ та яке має властивості:
i. $m^e = m$, $\forall m \in M$;
ii. $m^{g_1 g_2} = (m^{g_1})^{g_2}$, $\forall m \in M$, $\forall g_1, g_2 \in G$.
- **Стабілізатором** точки $m \in M$ називається множина $St_g(m) = \{g \in G \mid m^g = m\}$. Зауважимо, що $St_g(m) \leq G$.
- **Ядром дії** групи G на множині M називається множина $Ker(f) = \{g \in G \mid m^g = m\ \forall\, m \in M\}$.

Централізатори та нормалізатори

- **Централізатором** множини A у групі G називається множина $Z_G(A) = \{g \in G \mid g^{-1}ag = a\ \forall\, a \in A\}$. Зауважимо, що $Z_G(A) < G$.
- **Центром** групи G називається множина $Z(G) = \{g \in G \mid gx = xg\ \forall\, x \in G\}$. Зокрема, $Z(G) = Z_G(G)$, $Z(G) \lhd G$.
- **Нормалізатором** множин A у групі G називається множина $N_G(A) = \{g \in G \mid g^{-1}ag \in A\ \forall a \in A\}$. Зокрема, $Z_G(A) \leq N_G(A)$.

Орбіти дії

- Група G діє на множині M. Тоді $a \sim b \iff a = b^g$ для деякого $g \in G$, де $\sim$ — відношення еквівалентності, його класи — **орбіти** дії.
- **Орбіта** точки $a \in M$ — це множина $O(a) = \{a^g \mid g \in G\}$.
- Дія G на M називається транзитивною, якщо вона має лише одну орбіту.

Теорема: Нехай скінченна група G діє на множині M. Тоді для будь-якого $m \in M$: $|O(m)||St_G(m)| = |G|$.

Спряженість та формула класів

- **Клас спряженості** групи G — це орбіти дії групи G на собі спряженням, тобто $\{g^{-1}ag \mid g \in G\}$.
- **Формула класів** для скінченної групи G: $|G| = |Z(G)| + \sum |(\text{Неодноелементні класи спряженості } G)|$.

Основна теорема про скінченні абелеві групи

Теорема: Скінченна абелева група розкладається у прямий добуток своїх підгруп $H_1 \times \cdots \times H_k$, де кожна H_i — циклічна група порядку $p_i^{n_i}$, p_i — (не обов'язково різні) прості числа, $n_i \in \mathbb{N}$. Цей розклад однозначний з точністю до порядку множників.

p-групи та силовські p-підгрупи

- **p-група** — це група, порядки елементів якої є степенями простого числа p. Скінченна група є p-групою $\Leftrightarrow |G| = p^k$ для деякого $k \in \mathbb{N}$.
- **силовська p-підгрупа** Нехай G — скінченна група, p — просте число. Якщо $p^k \mid |G|$, а $p^{k+1} \nmid |G|$, то підгрупа порядку p^k називається **силовською** p**-підгрупою**.

Теореми Силова

i. Перша теорема Силова: Якщо p ділить $|G|$, то в G існує силовська p-підгрупа.
ii. Друга теорема Силова: Довільні дві силовські p-підгрупи скінченної групи спряжені.
iii. Третя теорема Силова: Нехай p — просте число, G — скінченна група порядку $p^k m$, де $(p, m) = 1$, n_p — кількість силовських p-підгруп. Тоді $n_p \equiv 1 \pmod p$; $n_p \mid m$.

Є. Кочубінська. Оригінал: https://imgur.com/a/cjA61w3