Лекция 20, 14.02.24

Опр: Группа наз. **простой**, если она не имеет собственных подгрупп. (т.е. отличных от самой группы и $\{e\}$).

Пример: $\mathbb{Z}_p$, где p - простое число. Цикл. гр. явл. простой, если p-простое.

Автоморфизм

Опр: **автоморфизм** - это изоморфизм группы G в себя.

Мн-во всех автоморфизмов гр. G в себя обознач. $Aut(G)$ и образует группу относительно операции композиции.

(Замкн., ассоц., $\exists$ нейтр. эл-т - тождеств. отобр., $\forall$ эл-т обратим)

Опр: **Внутренним автоморфизмом** наз. отображ. $I_a : g \mapsto aga^{-1}$ (сопряжение эл-тов группы по фикс. эл-ту a).

Проверим, что I_a изоморфизм:

$$I_a(g_1 \cdot g_2) = ag_1g_2a^{-1} = ag_1a^{-1}ag_2a^{-1} = I_a(g_1) \cdot I_a(g_2)$$

Замечание: Все внутренние автоморфизмы образуют подгруппу $Inn(G)$ группы $Aut(G)$.

Замечание: Если G - абелева, то $Inn(G) = \{e\} = \{I_e\}$

Пример: в $\mathbb{Z}_n$ $\forall$ гомоморфизм задаётся образом порожд. эл-та

$f(\bar{1}) = k \cdot \bar{1}$, где НОД$(k, n) = 1$ (т.е. $\bar{k}$ тоже порождающий эл-т)

$\Rightarrow$ f - автоморфизм.

Опр: Центр группы - мн-во всех элементов из группы G, которые коммутируют со всеми эл-тами группы G.

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

Пример: В группе кватернионов Q_8 $Z(Q_8) = \{1, -1\}$

Утв: $Z(G)$ явл. нормальной подгруппой в группе G.

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

Достаточно доказать, что $\forall a, b \in Z(G)$ $ab^{-1} \in Z(G)$ (крит. подгр.).

По определению центра $\forall g \in G$ это означает, что $g(ab^{-1}) = (ab^{-1})g$

Покажем это:

$$(a \cdot b^{-1})g = a \cdot b^{-1}(g^{-1})^{-1} = a \cdot (\overset{b \in Z(G)}{g^{-1} \cdot b})^{-1} = a(b g^{-1})^{-1} = a(g^{-1})^{-1} \cdot b^{-1} =$$

$$= (\overset{a \in Z(G)}{ag})b^{-1} = (ga)b^{-1} = g(ab^{-1}) \Rightarrow Z(G) \text{ - подгруппа}$$

2) Докажем нормальность:

$\forall g \in G$ $\forall h \in Z(G)$ $gh = hg$ по опр. центра $\overset{\text{по опр. см. класса}}{\Rightarrow}$ $g \cdot Z(G) = Z(G)g$

$\Rightarrow Z(G)$ - норм. подгруппа по опр. ■

Утв: $G / Z(G) \cong Im(G)$

Т.е. факторгруппа группы G по её центру изоморфна её группе внутр. автоморфизмов.

□ Рассмотрим отображение $f: G \to Aut(G)$, где $f(g) = I_g$,

(т.е. $I_g(h) = ghg^{-1}$ $\forall h \in G$) – гомоморфизм

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

Тогда $Im f = Inn(G)$ по построению.

Покажем, что $Ker f = Z(G)$.

По опр. ядра $\forall g \in Ker f$

$f(g) = I_g = I_e$, то есть (где $I_e(h) = ehe^{-1} = h$ $\forall h \in G$ – нейтр. эл-т в $Inn(G)$)

$$\Rightarrow \forall h \in G \quad \overbrace{ghg^{-1}}^{``I_g(h)"} = \overbrace{h}^{``I_e(h)"} \Leftrightarrow gh = hg$$

$\Rightarrow g \in Z(G)$ по опр. $\Rightarrow Ker f = Z(G)$

Применим к f теор. о гомоморфизме групп $G/_{Z(G)} \cong Im\, G$. ■

Применение теории групп в криптографии

Используются 2 „односторонние" функции

1) Показательная (обратная – дискретное логарифмирование)

2) Умножение (обратная – разложение на множители – исп. в RSA)

Задача дискретного логарифмирования

Пусть G – конечная группа и $g \in G$, причём $ord\, g$ достат. большой.

Задача состоит в том, чтобы для данного эл-та $a \in G = \langle g \rangle$ найти $k : g^k = a$.

1976. Схема (протокол) шифрования Диффи-Хелмана (Diffie-Hellman)

Всем известна конечная группа G и эл-т $g \in G$.

Участник А фиксирует натуральное число a:

- оно секретно и всем сообщает g^a

- открытый ключ.

У участника Б есть секретное значение $b \in \mathbb{N}$, и он всем сообщает g^b.

Тогда А вычисляет $(g^b)^a = g^{ba}$, а пользователь Б - $(g^a)^b = g^{ab}$.

Тогда g^{ab} известно только А и Б и может быть использовано, как ключ для секретной переписки.

Криптосистема Эль-Гама́ля (Elgamal, 1985)

Всем известна конечная группа G. и $g \in G$.

Участник А берёт $a \in \mathbb{N}$ (секр. ключ) и сообщает всем g^a.

Если Б хочет передать А конфиденциальное сообщение $M \in G$, то он берёт некоторое $k \in \mathbb{N}$ и отправляет А пару чисел $(g^k, M(g^a)^k)$.

Тогда пользователь А вычисляет:

$$\underbrace{Mg^{ak}}_{\text{2е число из пары}} \cdot \underbrace{(g^k)}_{\text{1е число}}^{\overbrace{|G|-a}^{\leftarrow \text{известно только А}}} = M \cdot g^{ak} \cdot (g^k)^{|G|} \cdot g^{-ak} = Mg^{ak} \cdot e \cdot g^{-ak} = M \leftarrow \text{сек. сообщ.}$$

В качестве группы G обычно берётся $\mathbb{Z}_p^* = (\mathbb{Z}_p \setminus \{0\}, \cdot)$ - это цикл. группа, если p - простое число.

$\Rightarrow g \in \mathbb{Z}_p^*$ – образующий эл-т в $\mathbb{Z}_p^*$ (первообразный корень по простому модулю p).

Кольцо

Опр: Мн-во $K \neq \emptyset$ наз-ся <u>кольцом</u>, если на нём заданы 2 бинарные операции „+" и „·" (сложение и умножение), удовлетворяющие следующим аксиомам:

1) $(K, +)$ – абелева группа по сложению (ассоц., коммут, $\exists$ нейтр. эл-та – нуля и $\forall a\ \exists -a \in K$) аддиктивная группа кольца

2) $(K, \cdot)$ – полугруппа (ассоц.) (Мультипликативная полугруппа кольца)

3) Дистрибутивность: $\forall a, b, c \in K \quad (a+b)c = ac + bc$
$$c(a+b) = ca + cb.$$

Опр: Если в кольце есть нейтр. эл-т по умножению, то оно наз-ся <u>кольцом с единицей</u>.

Опр: Кольцо наз. <u>коммутативным</u>, если $\forall x, y \in K \quad xy = yx$ (умн. комм.).

Пример: $(\mathbb{Z}, +, \cdot)$ – комм. кольцо с „1".