Семинар 20

1 Повторение

Простые группы. Пример.

Автоморфизмы и внутренние автоморфизмы. Примеры автоморфизмов: $\mathbb{Z}$, $\mathbb{Z}_n$.

Центр группы. Пример для Q_8. Утверждение о том, что центр группы является нормальной подгруппой. Утверждение о том, что факторгруппа группы по её центру изоморфна группе её внутренних автоморфизмов.

Применение теории групп в криптографии. Задача дискретного логарифмирования. Шифрование: схема Диффи-Хеллмана, схема Эль-Гамаля.

Определение кольца. Аддитивная группа кольца. Мультипликативная полугруппа кольца. Кольцо с единицей. Коммутативное кольцо. Примеры колец: числовые кольца (остальные примеры на следующей лекции).

2 Задачи

Задача 1. Описать все гомоморфизмы $\mathbb{Z}_n \to \mathbb{Z}_m$.

Пусть X – группоид. Для любого $x \in X$ определены отображения левого и правого умножения $l_x, r_x : X \to X$:

$$l_x : y \mapsto x \cdot y, \quad r_x : y \mapsto y \cdot x.$$

Задача 2. Доказать, что условие ассоциативности в X эквивалентно тому, что $l_x \circ r_z = r_z \circ l_x$ для всех $x, z \in X$.

Пусть G – группа. Тогда l_g, r_g – биекции (но не гомоморфизмы), $l_g r_h = r_h l_g$ для всех $g, h \in G$ и

$$l_g^{-1} = l_{g^{-1}},\ r_g^{-1} = r_{g^{-1}}, \quad l_{gh} = l_g l_h,\ r_{gh} = r_h r_g.$$

Для автоморфизма сопряжения c_g выполнено равенство $c_g = l_g r_{g^{-1}}$.

Подгруппа $H \subseteq G$ называется *нормальной*, если $gH = Hg$ (то есть $l_g(H) = r_g(H)$) для всех $g \in G$. Эквивалентные условия (здесь $c_g : G \to G$ – автоморфизм сопряжения элементом $g \in G$):

1. $c_g(H) = H \ \forall g \in G$;
2. $c_g(H) \subseteq H \ \forall g \in G$;
3. множество левых смежных классов G по H совпадает с множество правых смежных классов G по H;
4. структура группы $(g_1H) \cdot (g_2H) = (g_1g_2)H$ на множестве G/H левых смежных классов корректно определена (в этом случае группа G/H с заданным умножением называется *факторгруппой* G по H).

Задача 3. Доказать, что любая подгруппа индекса 2 является нормальной.

Пусть G – группа и $g \in G$. *Класс сопряжённости* элемента g – это множество

$$C_G(g) = \{xgx^{-1} \mid x \in G\} = \{c_x(g) \mid x \in G\}.$$

Группа G разбивается на дизъюнктные классы сопряжённости. Условие нормальности подгруппы $H \subseteq G$ можно переформулировать в виде

$$h \in H \implies C_G(h) \subseteq H.$$

Напомним, что для σ и $(k_1 \dots k_d)$ из S_n выполнено

$$c_\sigma((k_1 \dots k_d)) = (\sigma(k_1) \dots \sigma(k_d)).$$

Отсюда можно сделать вывод, что для $\tau \in S_n$ класс сопряжённости $C_{S_n}(\tau)$ состоит из всех перестановок, у которых *циклическая структура* совпадает с циклической структурой τ (под циклической структурой здесь имеется в виду неупорядоченное разбиение $n = k_1 + \dots + k_s$, где $k_1, \dots, k_s$ – длины независимых циклов в τ).

Задача 4. Найти все собственные нормальные подгруппы в группе S_3.

Напомним теорему о гомоморфизме: если $\phi : G \to H$ – гомоморфизм групп, то

$$G/\operatorname{Ker}\phi \cong \operatorname{Im}\phi, \ g\operatorname{Ker}\phi \mapsto \phi(g).$$

Для любой нормальной подгруппы $H \lhd G$ имеется *естественная проекция*

$$\pi : G \to G/H, \ g \mapsto gH.$$

Задача 5. Чему изоморфна факторгруппа $\mathbb{R}^\times/\mathbb{R}^\times_{>0}$?

Задача 6. Доказать, что в группе $\mathbb{Q}/\mathbb{Z}$ для каждого натурального n имеется в точности одна подгруппа порядка n.