Группы: абелевы и неабелевы

Напомним, что порядок элемента g группы G обозначается $\operatorname{ord} g$.

Задача 1. Пусть $x, y \in G$ — элементы взаимно простых порядков m и n соответственно.

a) Покажите, что $\langle x \rangle \cap \langle y \rangle = \{e\}$.

b) Пусть вдобавок $xy = yx$. Покажите, что $\operatorname{ord} xy = mn$.

c) Пусть $z \in G$ — элемент, и $\operatorname{ord} z = kn$. Проверьте, что $\operatorname{ord}(z^k) = n$.

Задача 2. Пусть G — конечная абелева группа порядка $n = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$. Пусть известно, что при любом $d \in \mathbb{N}$ уравнение $x^d = e$ имеет в G не более d решений.

a) Покажите, что $\operatorname{НОК}\{\operatorname{ord} g \mid g \in G\} = n$.

b) Покажите, что для любого $i = 1 \ldots k$ в G существует элемент порядка $p_i^{a_i}$.

c) Покажите, что в G существует элемент порядка n, и значит, G циклическая.

Задача 3. Выведите из предыдущей задачи, что любая конечная подгруппа в мультипликативной группе любого поля циклическая. В частности, группа $(\mathbb{Z}/p\mathbb{Z})^*$ при простом p циклическая.

Задача 4. Пусть $p \neq q$ — различные простые числа, $N = pq$, а d — число, взаимно простое с $\phi(N)$. Рассмотрим отображение $C\colon (\mathbb{Z}/N\mathbb{Z})^* \to (\mathbb{Z}/N\mathbb{Z})^*$, заданное формулой $C(x) = x^d$.

a) Предложите разумный алгоритм вычисления C, если известны N и d.

b) Предложите разумный алгоритм вычисления C^{-1}, если известны p, q и d.

c^{***}) Предложите разумный алгоритм вычисления C^{-1}, если известны только N и d.

На том, что никто не умеет решать пункт c), основан один из алгоритмов шифрования с открытым ключом.

Группа автоморфизмов группы G обозначается $\operatorname{Aut}(G)$.

Задача 5. Вспомните, как устроены автоморфизмы группы $\mathbb{Z}/n\mathbb{Z}$, и проверьте, что $\operatorname{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

Задача 6. Покажите, что действие S_n на себе сопряжениями задаёт гомоморфизм $S_n \to \operatorname{Aut}(S_n)$, который

a) инъективен при $n \geqslant 3$;

b) сюръективен при $n \neq 6$.

Задача 7*. Построим "экзотический" автоморфизм S_6. Проверьте, что:

a) Действие S_5 сопряжениями на множестве 5-элементных подгрупп в S_5 задаёт вложение $S_5 \to S_6$, отличное от стандартных. Обозначим его образ W.

b) В S_6 есть 6 подгрупп $W_1, \ldots, W_6$, сопряжённых к W.

c) Действие S_6 сопряжениями на множестве $\{W_1, \ldots, W_6\}$ задаёт гомоморфизм $S_6 \to S_6$, не сводящийся к сопряжению.

Задача 8. Пусть H_1, H_2 — подгруппы группы G. Покажите, что отображение $(h_1, h_2) \mapsto h_1 h_2$ является изоморфизмом групп $H_1 \times H_2 \to G \iff H_1$ и H_2 — нормальные подгруппы в G, $H_1 \cap H_2 = \{e\}$ и $H_1 H_2 = G$, т.е. любой элемент $g \in G$ имеет вид $g = h_1 h_2$, где $h_i \in G_i$. В таком случае говорят, что G *разлагается в прямое произведение* подгрупп H_1 и H_2.

Говорят, что группа G *разлагается в полупрямое произведение* своих подгрупп N и H, если отображение $(n, h) \mapsto nh$ является биекцией множеств $N \times H \to G$ и подгруппа N нормальна в G. Обозначение: $G = N \leftthreetimes H$.

Задача 9. a) Пусть $G = N \leftthreetimes H$. Покажите, что $G/N \cong H$.

b) Пусть подгруппа $N \subset G$ нормальна. Всегда ли найдётся такая подгруппа $H \subset G$, что $G = N \leftthreetimes H$?

Задача 10. Постройте следующие разложения в полупрямые произведения:

a) $S_n = A_n \leftthreetimes \langle (1,2) \rangle$;

b) $S_4 = V_4 \leftthreetimes S_3$, где $V_4 = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ — т.н. *четверная группа Клейна*;

c) {движения плоскости} = {параллельные переносы} $\leftthreetimes$ {движения, сохраняющие точку P};

d) {движения плоскости} = {движения, сохраняющие ориентацию} $\leftthreetimes \langle s \rangle$,

где P — фиксированная точка плоскости, а s — фиксированная осевая симметрия.

Задача 11. a) Пусть $G = N \leftthreetimes H$. Действуя элементами H на N сопряжениями, постройте гомоморфизм $f\colon H \to \mathrm{Aut}\,(N)$. Покажите, что $G = N \times H \iff f \equiv e$.

b) По паре групп N, H и гомоморфизму $f\colon H \to \mathrm{Aut}\,(N)$ постройте группу $N \leftthreetimes_f H$, раскладывающуюся в полупрямое произведение N и H.

c) Проверьте, что конструкции пунктов a) и b) обратны друг к другу.

Изучим полупрямые произведения циклических групп. Пусть $N = \langle x \rangle_n$, $H = \langle y \rangle_m$.

Задача 12. Покажите, что:

a) в любом полупрямом произведении $\langle x \rangle_n \leftthreetimes \langle y \rangle_m$ при некотором $k \in \mathbb{N}$ выполнено $yx = x^k y$. Каким может быть k? Что происходит с k при смене образующих в $\langle x \rangle_n$ и $\langle y \rangle_m$?

b) существуют нетривиальные полупрямые произведения $\langle x \rangle_n \leftthreetimes \langle y \rangle_m \iff (m, \phi(n)) \neq 1$.

Опишите все полупрямые произведения

c) $\langle x \rangle_p \leftthreetimes \langle y \rangle_2$, где p простое;

d) $\langle x \rangle_3 \leftthreetimes \langle y \rangle_m$;

e) $\langle x \rangle_{13} \leftthreetimes \langle y \rangle_m$, где $m = 3, 4, 5$.

f) Покажите, что группа движений правильного n-угольника изоморфна полупрямому произведению $\langle x \rangle_n \leftthreetimes_f \langle y \rangle_2$, где $f(y)$ — автоморфизм $\langle x \rangle_n$, переводящий z в z^{-1}.