ОВАиТК 1

Ковалев Алексей

Задача 1

$$\operatorname{ord} g = n,\ n \nmid m,\ d = \gcd(n, m)$$

1. $g^m = g^{qn+r} = g^r,\ r < n$
   $g^r \neq e$, так как $r < \operatorname{ord} g$. $\square$

2. Пусть $\operatorname{ord} g^m = k$. Тогда $(g^m)^k = g^{mk} = e \Rightarrow n \mid mk$, причем k – минимальное натуральное число, такое что это свойство выполнено. $n \mid mk \Rightarrow \exists q \colon qn = mk$. Значит $k = \frac{qn}{m} = \frac{q \cdot n/d}{m/d}$, причем $\gcd(n/d, m/d) = 1$. Отсюда $q = m/d$, так как $k \in \mathbb{N}$. То есть $\operatorname{ord} g^m = \frac{m/d \cdot n/d}{m/d} = \frac{n}{d}$.

Ответ: $\operatorname{ord} g^m = \frac{n}{d}$.

Задача 2

$$C_{nm} \cong C_n \times C_m \iff \gcd(n, m) = 1$$

Сначала предположим, что $C_{nm} \cong C_n \times C_m$. Тогда в C_{nm} есть элемент порядка nm. Обозначим его за $g = (f, h)$, где $f \in C_n, h \in C_m$. $\operatorname{ord} g = nm = \operatorname{lcm}(|f|, |h|) = \frac{|f| \cdot |h|}{\gcd(|f|, |h|)} \Rightarrow \gcd(|f|, |h|) = 1$. Значит $C_{nm} \cong C_n \times C_m \Rightarrow \gcd(n, m) = 1$.
Теперь будем считать, что $\gcd(n, m) = 1$. Тогда необходимо найти в $C_n \times C_m$ элемент порядка nm. Пусть $C_n = \langle g \rangle,\ C_m = \langle h \rangle$. Тогда $\operatorname{ord} g = n,\ \operatorname{ord} h = m$. Рассмотрим элемент $(g, h) \in C_{nm}$. Его порядок $|(g, h)| = \operatorname{lcm}(|g|, |h|) = \frac{|g| \cdot |h|}{\gcd(|g|, |h|)} = |g| \cdot |h| = nm$. Значит $C_{nm} \cong C_n \times C_m \iff \gcd(n, m) = 1$. $\square$

Задача 3

Рассмотрим $a, b \in G$:

$$(ab)(ab) = e = a^2 b^2$$

$$a^{-1} ababb^{-1} = a^{-1} a^2 b^2 b^{-1}$$

$$ba = ab$$

То есть $\forall a, b \in G\ \ ab = ba \Rightarrow G$ абелева. $\square$

Задача 4

В группе G ровно один элемент f имеет порядок 2. То есть $f^2 = e,\ f = f^{-1}$. Рассмотрим произведение всех элементов группы G. Для всех элементов $g \in G$ кроме f, в это произведение входят как сам элемент, так и обратный к нему.

$$\prod_{g \in G} g = f g_1 g_1^{-1} g_2 g_2^{-1} \ldots = f$$

Отсюда получаем, что произведение всех элементов группы равно f.
Ответ: f.

Задача 5

Для начала докажем, что если $g \in G,\ g^n = e$, то $\operatorname{ord} g \mid n$. Предпололжим обратное: $\operatorname{ord} g \nmid n \Rightarrow n = q \operatorname{ord} g + r,\ q, r \in \mathbb{Z},\ 0 < r < \operatorname{ord} g$. Тогда $g^n = g^{q \operatorname{ord} g + r} = g^{q \operatorname{ord} g} g^r = g^r \neq e$, так как $r < \operatorname{ord} g$ – противоречие. $\square$

1. Пусть $\operatorname{ord} g = n,\ \operatorname{ord} h = m,\ \operatorname{ord} gh = k$. Тогда $(gh)^k = e$. Рассмотрим $(gh)^{\operatorname{lcm}(n,m)}$. В силу того, что $\operatorname{lcm}(n,m) = xn = ym,\ x, y \in \mathbb{Z}$ имеем $(gh)^{\operatorname{lcm}(n,m)} = g^{\operatorname{lcm}(n,m)} h^{\operatorname{lcm}(n,m)} = g^{xn} h^{ym} = e \Rightarrow k \mid \operatorname{lcm}(n,m)$. $\square$

2. Рассмотрим группу $\mathbb{Z}_{16}$. В ней есть элементы $g = 2,\ h = 6$, причем $\operatorname{ord} g = 8,\ \operatorname{ord} h = 8$, в то время как $\operatorname{ord} gh = \operatorname{ord}(8) = 2 < \operatorname{lcm}(8,8) = 8$.

3. Пусть $\operatorname{ord} g = n,\ \operatorname{ord} h = m,\ \operatorname{ord} gh = k$, причем $\gcd(n,m) = 1$. Тогда $e = (gh)^{km} = g^{km} (h^m)^k = g^{km} \Rightarrow n \mid km \Rightarrow n \mid k$. Аналогично $e = (gh)^{kn} = (g^n)^k h^{kn} = h^{kn} \Rightarrow m \mid kn \Rightarrow m \mid k$. То есть $n \mid k,\ m \mid k,\ k$ – минимально $\Rightarrow k = mn$. $\square$

Задача 6

$$|\mathbb{Z}_5^*| = \varphi(5) = 4 = \varphi(12) = |\mathbb{Z}_{12}^*|$$

Рассмотрим группу $\mathbb{Z}_{12}^*$: она состоит из элементов $\{1, 5, 7, 11\}$, причем $\operatorname{ord}(1) = \operatorname{ord}(5) = \operatorname{ord}(7) = \operatorname{ord}(11) = 2$.
В группе $\mathbb{Z}_5^*$ есть элемент 3, причем $\operatorname{ord}(3) = 4 \Rightarrow \mathbb{Z}_{12}^* \ncong \mathbb{Z}_5^*$.
Ответ: $|\mathbb{Z}_5^*| = |\mathbb{Z}_{12}^*|,\ \mathbb{Z}_{12}^* \ncong \mathbb{Z}_5^*$.

Задача 7

Предпололжим обратное: пусть $G < \mathbb{Q},\ H < \mathbb{Q},\ \mathbb{Q} \cong G \times H$, причем G, H – нетривиальные подгруппы.
Для любых двух элементов $g = \frac{m}{n} \in \mathbb{Q},\ h = \frac{k}{l} \in \mathbb{Q}$ верно следующее свойтсво: $\exists q = \frac{1}{nl} : g = mlq,\ h = nkq$.
Рассмотрим некоторый изоморфизм $G \times H \to \mathbb{Q}$, такой что $(a, 0) \mapsto g,\ (0, b) \mapsto h,\ (c, d) \mapsto q$, где $a \neq 0,\ b \neq 0$.
В силу того что $g = mlq,\ h = nkq$ верно $(a, 0) = \alpha \cdot (c, d),\ (0, b) = \beta \cdot (c, d)$ для некоторых $\alpha,\ \beta$, причем $\alpha \neq 0,\ \beta \neq 0$, так как $a \neq 0,\ b \neq 0$. Также

$$(a, 0) = (\alpha c, \alpha d) \Rightarrow \alpha d = 0$$

$$(0, b) = (\beta c, \beta d) \Rightarrow \beta c = 0$$

Отсюда получаем, что $c = 0,\ d = 0$, а значит $a = b = 0$ – противоречие, значит такого изоморфизма не существует. $\square$