Определение. *Индекс* подгруппы H в группе G – это число левых смежных классов G по H.
Обозначение: $[G : H]$.

Теорема (Лагранж)**.** Пусть G – конечная группа, $H \subseteq G$ – подгруппа. Тогда $|G| = |H| \cdot [G : H]$.
Следствие. Пусть G – конечная группа и $H \subseteq G$ – подгруппа. Тогда $|H|$ делит $|G|$.
Следствие. Пусть G – конечная группа и $g \in G$. Тогда $\mathrm{ord}(g)$ делит $|G|$.
Следствие. Пусть G – конечная группа и $g \in G$. Тогда $g^{|G|} = e$.
Следствие. Пусть G – группа и $|G|$ – простое число. Тогда G – циклическая подгруппа, порождаемая любым своим неединичным элементом.
Следствие (Малая теорема Ферма)**.** Пусть $\bar{a}$ – ненулевой вычет по простому модулю p. Тогда выполняется $\bar{a}^{p-1} = \bar{1}$.

Определение. Подгруппа $H \subseteq G$ называется *нормальной*, если $gH = Hg$ для всех $g \in G$.
Обозначение: $H \lhd G$.

Предложение. Пусть H – подгруппа группы G. Следующие условия эквивалентны:
(а) $H \lhd G$
(б) $gHg^{-1} = H$ для всех $g \in G$
(в) $gHg^{-1} \subseteq H$ для всех $g \in G$

Пусть H – **нормальная** подгруппа в G. Обозначим через G/H множество всех смежных классов G по H и введём на нём бинарную операцию. Положим $(g_1H)(g_2H) = (g_1g_2)H$.
Данная операция задана корректно. Описанная $(G/H, \cdot)$ – группа.
Определение. $(G/H, \cdot)$ называется *факторгруппой* группы G по нормальной подгруппе H.

Пусть $(G, \circ)$ и $(F, \cdot)$ – группы.
Определение. Отображение $\varphi : G \to F$ называется *гомоморфизмом*, если $\varphi(a \circ b) = \varphi(a) \cdot \varphi(b)$ для любых $a, b \in G$.

Определение. Гомоморфизм $\varphi : G \to F$ называется *изоморфизмом*, если φ – биекция.
Определение. Группы G, F называются *изоморфными*, если существует изоморфизм $\varphi : G \to F$.
Обозначение: $G \simeq F$, $G \cong F$, $G \xrightarrow{\sim} F$.

Определение. *Ядро* гомоморфизма φ – это множество $\ker \varphi = \{g \in G \mid \varphi(g) = e_f\} \subseteq G$.
Определение. *Образ* гомоморфизма φ – это множество $\mathrm{Im}\, \varphi = \varphi(G) \subseteq F$.
Теорема (о гомоморфизме групп)**.** $G/\ker \varphi \simeq \mathrm{Im}\, \varphi$

Задание 1. Пусть G – группа невырожденных верхнетреугольных матриц (2×2)-матриц с коэффициентами из $\mathbb{Q}$. Докажите, что все содержащиеся в G матрицы вида

$$\begin{pmatrix} a^3 & b \\ 0 & a^2 \end{pmatrix}$$

образуют нормальную подгруппу в G.

1. Обозначим описанное множество матриц H. Покажем, что H – подгруппа. Для этого нужно проверить три следующих условия:
   (а) $e \in H$
   (б) $x, y \in H \Rightarrow x \circ y \in H$
   (в) $x \in H \Rightarrow x^{-1} \in H$

   Рассмотрим каждое из условий.
   - Найдём нейтральный элемент группы G, то есть такой элемент e, что $x \circ e = e \circ x = x$. Этот элемент – единичная матрица размера 2×2. Действительно, матрица E невырожденная, при умножении матрицы X на E слева или справа получается матрица X.

     Нейтральный элемент лежит в H. Матрица E имеет описанный вид. В данном случае значения $a = 1 \in \mathbb{Q}$, $b = 0 \in \mathbb{Q}$.
   - Проверим, что произведение двух матриц из H также матрица, лежащая в H:
     $$\begin{pmatrix} a^3 & b \\ 0 & a^2 \end{pmatrix} \cdot \begin{pmatrix} c^3 & d \\ 0 & c^2 \end{pmatrix} = \begin{pmatrix} a^3c^3 & a^3d + c^2b \\ 0 & a^2c^2 \end{pmatrix} = \begin{pmatrix} (ac)^3 & a^3d + c^2b \\ 0 & (ac)^2 \end{pmatrix} \in H$$
     Проверку на то, что матрица невырождена и имеет коэффициенты из $\mathbb{Q}$ можно не делать, так как рассматриваемые матрицы – элементы группы G, а значит, заданная бинарная операция не выводит из описанного множества матриц.
   - Для каждого элемента x из H найдём обратный ему, то есть такой, что $x \cdot x^{-1} = x^{-1} \cdot x = e$. Так как матрицы из G (и как следствие из H) невырожденные, для каждой матрицы из H существует обратная.

     Произведение матрицы из H на обратную коммутативно и равно E, а это нейтральный элемент в H, значит, обратная к рассматриваемой матрице может быть обратным элементом к этой матрице в H.

     Чтобы проверить, что для X матрица X^{-1} – обратный элемент в H, достаточно проверить, что матрица X^{-1} имеет описанный вид, то есть матрица X^{-1} лежит в H. Невырожденность матрицы X^{-1} очевидна.
     $$X^{-1} = \frac{1}{\det X} \begin{pmatrix} X_{11} & X_{21} \\ X_{12} & X_{22} \end{pmatrix} = \frac{1}{a^5} \begin{pmatrix} a^2 & -b \\ 0 & a^3 \end{pmatrix} = \begin{pmatrix} 1/a^3 & -b/a^5 \\ 0 & 1/a^2 \end{pmatrix} = \begin{pmatrix} (1/a)^3 & -b/a^5 \\ 0 & (1/a)^2 \end{pmatrix} \in H$$
     Полученные коэффициенты принадлежат $\mathbb{Q}$: значение $(\det X)^{-1}$ существует и принадлежит множеству рациональных чисел, а произведение рациональных чисел – рациональное.

   Таким образом, H – подгруппа в G по определению.

2. Докажем, что H – нормальная подгруппа в G. Для этого воспользуемся эквивалентным условием: $H \lhd G \Leftrightarrow gHg^{-1} \subseteq H$ для всех $g \in G$. Данное условие означает, что для любого элемента $g \in G$ и любого элемента $h \in H$ значение $ghg^{-1} \in H$.

   Рассмотрим произвольные матрицы $g \in G$ и $h \in H$:

$$g = \begin{pmatrix} p & q \\ 0 & r \end{pmatrix} \qquad\qquad h = \begin{pmatrix} a^3 & b \\ 0 & a^2 \end{pmatrix}$$

   Проверим, что $ghg^{-1} \in H$:

$$\begin{pmatrix} p & q \\ 0 & r \end{pmatrix} \cdot \begin{pmatrix} a^3 & b \\ 0 & a^2 \end{pmatrix} \cdot \begin{pmatrix} p & q \\ 0 & r \end{pmatrix}^{-1} = \begin{pmatrix} p & q \\ 0 & r \end{pmatrix} \cdot \begin{pmatrix} a^3 & b \\ 0 & a^2 \end{pmatrix} \cdot \begin{pmatrix} {}^{r}\!/_{pr} & -{}^{q}\!/_{pr} \\ 0 & {}^{p}\!/_{pr} \end{pmatrix} =$$

$$= \begin{pmatrix} p & q \\ 0 & r \end{pmatrix} \cdot \begin{pmatrix} a^3 & b \\ 0 & a^2 \end{pmatrix} \cdot \begin{pmatrix} {}^{1}\!/_{p} & -{}^{q}\!/_{pr} \\ 0 & {}^{1}\!/_{r} \end{pmatrix} = \begin{pmatrix} pa^3 & pb + qa^2 \\ 0 & ra^2 \end{pmatrix} \cdot \begin{pmatrix} {}^{1}\!/_{p} & -{}^{q}\!/_{pr} \\ 0 & {}^{1}\!/_{r} \end{pmatrix} =$$

$$= \begin{pmatrix} pa^3 & pb + qa^2 \\ 0 & ra^2 \end{pmatrix} \cdot \begin{pmatrix} {}^{1}\!/_{p} & -{}^{q}\!/_{pr} \\ 0 & {}^{1}\!/_{r} \end{pmatrix} = \begin{pmatrix} a^3 & {}^{-qa^3+qa^2+pb}\!/_{r} \\ 0 & a^2 \end{pmatrix} \in H$$

   Полученная матрица имеет описанный вид и лежит в подгруппе H. В силу произвольности g и h условие $gHg^{-1} \subseteq H$ выполнено.

3. Таким образом, множество в G, состоящее из матриц вида

$$\begin{pmatrix} a^3 & b \\ 0 & a^2 \end{pmatrix}$$

   образует нормальную подгруппу в G.

Задание 2. Найдите все гомоморфизмы из группы $\mathbb{Z}_{20}$ в группу $\mathbb{Z}_{12}$.

1. Пусть $\varphi : \mathbb{Z}_{20} \to \mathbb{Z}_{12}$ – гомоморфизм. Если $\varphi(1) = a$, то для каждого $x \in \mathbb{Z}_{20}$:

$$\varphi(x) = \varphi(\underbrace{1 + 1 + \ldots + 1}_{x \text{ раз}}) = \underbrace{\varphi(1) + \varphi(1) + \ldots + \varphi(1)}_{x \text{ раз}} = \underbrace{a + a + \ldots + a}_{x \text{ раз}} = xa$$

   Таким образом, гомоморфизм φ однозначно определяется образом единицы.

2. Известно, что для любого гомоморфизма $\varphi : G_1 \to G_2$ значение $\varphi(e_{G_1}) = e_{G_2}$. Для искомых гомоморфизмов для каждого $t \in \mathbb{Z}$ должно выполнятся

$$\begin{cases} \varphi(0) = 0 \\ \varphi(0) = \varphi(20t) = 20ta \end{cases} \Leftrightarrow 20ta = 0$$

   То есть $20ta = 0$ в $\mathbb{Z}_{12}$ для любого $t \in \mathbb{Z}$. Последнее равенство равносильно

$$20ta \equiv 0 \mod 12 \;\Leftrightarrow\; 5ta \equiv 0 \mod 3 \;\Leftrightarrow\; -ta \equiv 0 \mod 3 \;\Leftrightarrow\; ta \equiv 0 \mod 3$$

   Так как равенство должно выполнятся для всех $t \in \mathbb{Z}$, оно должно выполнятся для $t = 1$. Если равенство выполняется для $t = 1$, то оно выполняется и для любого другого значения t. При $t = 1$ получим уравнение $a \equiv 0 \mod 3$, решения которого удовлетворяют $at \equiv 0 \cdot t \equiv 0 \mod 3$ для любого другого значения t.

3. Для того , чтобы найти все возможные допустимые значения a нужно решить описанное сравнение $a \equiv 0 \mod 3$ в $\mathbb{Z}_{12}$. Решение этого уравнения: $a \in \{0, 3, 6, 9\}$.

4. Таким образом, искомые гомоморфизмы – это отображения $\varphi : \mathbb{Z}_{20} \to \mathbb{Z}_{12}$, имеющие следующий вид $\varphi(x) = xa$ для каждого x, $a \in \{0, 3, 6, 9\}$

Ответ: $\varphi(x) = 0 \quad \forall x \in \mathbb{Z}$

$\varphi(x) = 3x \quad \forall x \in \mathbb{Z}$

$\varphi(x) = 6x \quad \forall x \in \mathbb{Z}$

$\varphi(x) = 9x \quad \forall x \in \mathbb{Z}$

Задание 3. Пусть H – подгруппа всех элементов конечного порядка в группе $(\mathbb{C} \setminus \{0\}, \times)$. Докажите, что $H \simeq \mathbb{Q}/\mathbb{Z}$, где группы $\mathbb{Q}$ и $\mathbb{Z}$ рассматриваются с операцией сложения.

1. Если существует изоморфизм $H \simeq \mathbb{Q}/\mathbb{Z}$, то существует биективный гомоморфизм $\varphi : H \to \mathbb{Q}/\mathbb{Z}$. Значит, в силу того, что φ – биекция, существует φ^{-1}. Известно, что если φ – изоморфизм, то φ^{-1} также изоморфизм.

   Таким образом, чтобы доказать изоморфность H и $\mathbb{Q}/\mathbb{Z}$ можно доказать $\mathbb{Q}/\mathbb{Z} \simeq H$.

2. Каждый элемент подгруппы H имеет конечный порядок, следовательно, для $h \in H$ существует такое натуральное k, что $h^k = e$. Нейтральный элемент в группе $(\mathbb{C} \setminus \{0\}, \times)$ – это единица. Получаем, что H – это подгруппа, состоящая из элементов, являющихся корнем единицы натуральной степени, то есть верно следующее

$$h \in H \;\Leftrightarrow\; \exists n \in \mathbb{N}: \;\; h^n = 1, \;\Leftrightarrow\; h = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, \;\; n \in \mathbb{N}, \;\; k \in \{0, 1, \ldots, n-1\}$$

3. Рассмотрим отображение $\varphi : \mathbb{Q} \to H$ заданное формулой $x \mapsto e^{2\pi x i}$. Покажем, что данное отображение – гомоморфизм:

$$\varphi(x+y) = e^{2\pi(x+y)i} = e^{2\pi x i + 2\pi y i} = e^{2\pi x i} \cdot e^{2\pi y i} = \varphi(x) \cdot \varphi(y)$$

   Получаем, что для любых $x, y \in \mathbb{Q}$ выполнено $\varphi(x+y) = \varphi(x) \cdot \varphi(y)$, значит, построенное отображение – гомоморфизм.

4. Найдем ядро отображения, то есть такие элементы $x \in \mathbb{Q}$, что $\varphi(x) = e_H$. Нейтральный элемент подгруппы $H \subseteq \mathbb{C} \setminus \{0\}$ – это нейтральный элемент $\mathbb{C} \setminus \{0\}$, значит, $e_H = 1$. Получаем следующее уравнение:

$$\varphi(x) = e^{2\pi x i} = \cos 2\pi x + i \sin 2\pi x = 1 \;\Leftrightarrow\; \begin{cases} \cos 2\pi x = 1 \\ \sin 2\pi x = 0 \end{cases} \;\Leftrightarrow\; \begin{cases} 2\pi x = 2\pi m \\ 2\pi x = \pi n \end{cases} \quad m, n \in \mathbb{Z} \;\Leftrightarrow$$

$$\Leftrightarrow \begin{cases} x = m \\ 2x = n \end{cases} \quad m, n \in \mathbb{Z} \;\Leftrightarrow\; x = m, \;\; m \in \mathbb{Z}$$

   Таким образом, ядро отображения – это множество целых чисел $\mathbb{Z}$.

5. Покажем, что $\operatorname{Im}\varphi = H$.
   - Для каждого $x \in \mathbb{Q}$ верно, что $\varphi(x) \in H$. Представим элемент x в виде $x_0 + \frac{p}{q}$, где x_0 – целая часть числа x, а несократимая дробь $\frac{p}{q}$ – дробная часть числа x, причём будем представлять x так, чтобы $\frac{p}{q} \geqslant 0$ и $p \in \mathbb{N} \cup \{0\}$, $q \in \mathbb{N}$, $p < q$.

     Получаем следующее:

$$\varphi\left(x_0 + \frac{p}{q}\right) = \varphi\left(x_0\right) \cdot \varphi\left(\frac{p}{q}\right) = 1 \cdot \varphi\left(\frac{p}{q}\right) = \varphi\left(\frac{p}{q}\right) = e^{\frac{2\pi p}{q} i} = \cos\frac{2\pi p}{q} + i\sin\frac{2\pi p}{q} \neq 0$$

     Последнее выражение – это корень степени q из единицы.

Не трудно в этом убедиться, возведя полученное комплексное число в степень q:

$$\left(\cos\frac{2\pi p}{q} + i\sin\frac{2\pi p}{q}\right)^q = \cos\frac{2\pi pq}{q} + i\sin\frac{2\pi pq}{q} = \cos 2\pi p + i\sin 2\pi p = 1 + 0i = 1$$

Образ каждого элемента – это это корень натуральной степени из единицы, значит, $\operatorname{Im}\varphi \subseteq H$.

– Покажем, что для каждого элемента $h \in H$ существует элемент $x \in \mathbb{Q}$, такой что $\varphi(x) = h$.

Любой элемент из h при его представлении в тригонометрической форме имеет вид:

$$h = \cos\frac{2\pi p}{q} + i\sin\frac{2\pi p}{q},\ \ p \in \mathbb{N}\cup\{0\},\ q \in \mathbb{N},\ p < q$$

Возьмём элемент $x = \frac{p}{q} \in \mathbb{Q}$ и покажем, что $\varphi(x) = h$:

$$\varphi\left(\frac{p}{q}\right) = e^{\frac{2\pi p}{q}i} = \cos\frac{2\pi p}{q} + i\sin\frac{2\pi p}{q} = h$$

Таким образом, $H \subseteq \operatorname{Im}\varphi$.

– Получаем, требуемое: $H \subseteq \operatorname{Im}\varphi$, $\operatorname{Im}\varphi \subseteq H \ \Leftrightarrow\ H = \operatorname{Im}\varphi$.

6. По теореме о гомоморфизме групп получаем $\mathbb{Q}/\ker\varphi \simeq \operatorname{Im}\varphi$, то есть $\mathbb{Q}/\mathbb{Z} \simeq H$ (по построению отображения $\ker\varphi = \mathbb{Z}$, $\operatorname{Im}\varphi = H$). Последнее выражение равносильно $H \simeq \mathbb{Q}/\mathbb{Z}$.

Задание 4. Пусть $m, n \in \mathbb{N}$. Докажите, что следующие условия эквиваленты:

(1) m и n взаимнопросты

(2) для всякой группы G, всякой подгруппы $A \subseteq G$ порядка m и всякой подгруппы $B \subseteq G$ порядка n выполняется условие $A \cap B = \{e\}$.

1. Докажем, что пересечение $H_1 \cap H_2$ подгрупп $H_1 \subseteq G$ и $H_2 \subseteq G$ также подгруппа в G. Для этого проверим выполнение следующих условий:

   (а) $e \in H_1 \cap H_2$

   (б) $x, y \in H_1 \cap H_2 \Rightarrow x \circ y \in H_1 \cap H_2$

   (в) $x \in H_1 \cap H_2 \Rightarrow x^{-1} \in H_1 \cap H_2$

   Рассмотрим каждое из условий.

   – Каждая из подгрупп содержит нейтральный элемент e. Этот элемент один и тот же в обеих подгруппах, так как и H_1, и H_2 – подгруппы одной и той же группы.

   Таким образом, $e \in H_1 \cap H_2$.

   – Если элементы $x, y \in H_1 \cap H_2$, то оба элемента лежат и в H_1, и в H_2. Так как H_1 – подгруппа и $x, y \in H_1$ выполняется $x \circ y \in H_1$. Аналогично и для подгруппы H_2: $x, y \in H_2 \Rightarrow x \circ y \in H_2$. Элемент $x \circ y$ лежит и в H_1, и в H_2, значит, $x \circ y \in H_1 \cap H_2$.

   – Если элемент $x \in H_1 \cap H_2$, то $x \in H_1$ и $x \in H_2$. В силу того, что H_1 и H_2 – подгруппы $x^{-1} \in H_1$ и $x^{-1} \in H_2$. Обратный элемент лежит в обеих подгруппах, значит, он лежит в их пересечении.

   Все условия выполнены. Получаем, что $H_1 \cap H_2$ – подгруппа в G. Заметим, что данное утверждение верно и для пересечения большего количества подгрупп.

   Утверждение можно усилить: $H_1 \cap H_2$ – подгруппа в H_1 и H_2. Множество $H_1 \cap H_2$ является подмножеством групп H_1 и H_2 и удовлетворяет всем условиям подгруппы, значит, $H_1 \cap H_2$ – подгруппа в H_1 и H_2.

2. Из предыдущего пункта получаем, что $A \cap B$ – подгруппа в A и в B. По теореме Лагранжа для конечной группы G и подгруппы $H \subseteq G$ выполнено $|G| = |H| \cdot [G : H]$. Таким образом, для конечных A и B и их подгруппы $A \cap B$

$$\begin{cases} |A| = |A \cap B| \cdot [A : A \cap B] \\ |B| = |A \cap B| \cdot [B : A \cap B] \end{cases} \Rightarrow \begin{cases} |A| \vdots |A \cap B| \\ |B| \vdots |A \cap B| \end{cases} \Leftrightarrow \begin{cases} m \vdots |A \cap B| \\ n \vdots |A \cap B| \end{cases}$$

   Пусть порядок группы $A \cap B$ больше единицы, то есть $|A \cap B| = d > 1$. Тогда из делимости m на d и n на d следует, что НОД$(m, n) \geq d > 1$. Получаем противоречие с тем, что m и n взаимнопросты.

   Порядок пересечения $A \cap B$ не может быть больше единицы. В то же время, $A \cap B$ – подгруппа, значит она содержит нейтральный элемент, то есть порядок $A \cap B$ не меньше единицы. Из этого следует, что $|A \cap B| = 1 \Leftrightarrow A \cap B = \{e\}$.

3. Таким образом, если m и n – взаимнопросты, то $A \cap B = \{e\}$.

4. Докажем в обратную сторону: если $A \cap B = \{e\}$, то НОД$(m, n) = 1$. Предположим противное: пусть $A \cap B = \{e\}$, но m и n не взаимнопросты. Рассмотрим циклическую группу $G = \langle a \rangle$ с образующим a порядка $m \cdot n$ и подгруппы $A = \langle a^n \rangle$ и $B = \langle a^m \rangle$.

   Нетрудно убедиться, что порядки A и B равны m и n соответственно. Минимальная степень t элемента a, при которой $a^t = e$, равна $m \cdot n$ (по построению G). Порядок группы A – это порядок a^n, то есть минимальная степень s, такая что $a^{sn} = e$. Минимум достигается при $s \cdot n = m \cdot n \Leftrightarrow s = m$. Аналогично $|B| = \text{ord}(a^m) = n$.

   Опишем все общие элементы A и B. Заметим, что если a^t лежит и в A, и в B, то $a^t = a^{pn}$ и $a^t = a^{qm}$, то есть элементы, которые лежат в пересечении – это элементы удовлетворяющие равенству $a^{pn} = a^{qm}$ для каких-то целых p и q. Данные числа p и q равны:

$$p = \alpha \cdot \frac{m}{\text{НОД}(m,n)},\ q = \alpha \cdot \frac{n}{\text{НОД}(m,n)}, \quad \text{где } \alpha \in \mathbb{Z}$$

   В пересечении лежат элементы вида $a^{\alpha \frac{mn}{\text{НОД}(m,n)}} = a^{\alpha\, \text{НОК}(m,n)}$.

   Получаем, что $A \cap B = \langle a^{\text{НОК}(m,n)} \rangle$. Порядок этой группы равен порядку образующей, а порядок образующей равен

$$\frac{mn}{\text{НОК}(m,n)} = \text{НОД}(m,n) > 1$$

   Последнее означает, что $|A \cap B| > 1 = |\{e\}|$, значит, $A \cap B \neq \{e\}$. Получаем противоречие.

5. Таким образом, если $A \cap B = \{e\}$, то НОД$(m, n) = 1$.
6. Получаем, что описанные условия эквивалентны.

Несмотря на то, что условия эквиваленты, из тривиального пересечения **каких-то** двух подгрупп не следует взаимная простота m и n. В качестве примера приведём $\mathbb{Z}_2 \times \mathbb{Z}_2$ по сложению.
На множестве $\mathbb{Z}_2 \times \mathbb{Z}_2$ зададим бинарную операцию $(g_1,\ g_2)(g_1^{'},\ g_2^{'}) = (g_1 g_1^{'},\ g_2 g_2^{'})$. Проверим, что $\mathbb{Z}_2 \times \mathbb{Z}_2$ – группа, то есть проверим выполнение следующих условий:

– ассоциативность:

$$\big((a_1, a_2)(b_1, b_2)\big)(c_1, c_2) = (a_1 b_1, a_2 b_2)(c_1, c_2) = ((a_1 b_1)c_1, (a_2 b_2)c_2) = (a_1 b_1 c_1, a_2 b_2 c_2)$$
$$(a_1, a_2)\big((b_1, b_2)(c_1, c_2)\big) = (a_1, a_2)(b_1 c_1, b_2 c_2) = (a_1(b_1 c_1), a_2(b_2 c_2)) = (a_1 b_1 c_1, a_2 b_2 c_2)$$

– существование нейтрального элемента: $e = (e_{\mathbb{Z}_2}, e_{\mathbb{Z}_2})$, где $e_{\mathbb{Z}_2}$ – нейтральный элемент $\mathbb{Z}_2$

$$(e_{\mathbb{Z}_2}, e_{\mathbb{Z}_2})(g_1, g_2) = (e_{\mathbb{Z}_2} g_1, e_{\mathbb{Z}_2} g_2) = (g_1, g_2) = (g_1 e_{\mathbb{Z}_2}, g_2 e_{\mathbb{Z}_2}) = (g_1, g_2)(e_{\mathbb{Z}_2}, e_{\mathbb{Z}_2})$$

– существование обратного элемента: $\forall g = (g_1, g_2)$ из $\mathbb{Z}_2 \times \mathbb{Z}_2$ существует $g^{-1} = (g_1^{-1}, g_2^{-1})$

$$(g_1^{-1}, g_2^{-1})(g_1, g_2) = (g_1^{-1} g_1, g_2^{-1} g_2) = (e_{\mathbb{Z}_2}, e_{\mathbb{Z}_2}) = (g_1 g_1^{-1}, g_2 g_2^{-1}) = (g_1, g_2)(g_1^{-1}, g_2^{-1})$$

Рассмотрим две подгруппы этой группы: $\langle (0,1) \rangle,\ \langle (1,0) \rangle$. Порядок этих групп равен двум:

$$\langle (0,1) \rangle = \{(0,0),\ (0,1)\} \Rightarrow \big|\langle (0,1) \rangle\big| = 2 \quad \langle (1,0) \rangle = \{(0,0),\ (1,0)\} \Rightarrow \big|\langle (1,0) \rangle\big| = 2$$

Заметим, что пересечение этих подгрупп тривиально, но их порядки не взаимнопросты.