Упражнение 1. Существуют ли некоммутативные группы порядка 4? Порядка 5?

Решение.

1. Порядка 4.

   Пусть $G = \{e, a, b, c\}$ — некоммутативная группа порядка 4, где a и b не коммутируют.[1]

   Лемма 1. Пусть a и b не коммутируют. Тогда $a \neq b^{-1}$ *(и наоборот).*

   Доказательство. Пусть $a = b^{-1}$. Тогда

   $$\begin{aligned} a &= b^{-1} \\ ab &= e \\ bab &= be \\ (ba)b &= b \\ ba &= e = ab, !!! \end{aligned}$$

   □

   По лемме $ab \neq e$ и $ba \neq e$. Кроме того, $ab \neq a$ и $ba \neq a$, т.к. иначе $b = e$. Аналогично $ab \neq b$ и $ba \neq b$. Итого, $ab, ba \notin$[2] $\{e, a, b\}$ и при этом $ab \neq ba$. Тогда ab и ba различные элементы и $|G| \geq 5$, противоречие.

2. Порядка 5.

   Пусть $G = \{e, a, b, c, d\}$ — некоммутативная группа порядка 5, где a и b не коммутируют.

   Аналогично предыдущему случаю, $ab, ba \notin \{e, a, b\}$. Пусть $ab = c$ и $ba = d$ *(без потери общности).*

   $$ca = (ab)a = a(ba) = ad$$

   $$bc = b(ab) = (ba)b = db$$

   Т.к. $c \neq e, a \neq e$, $ca \notin \{c, a\}$. Аналогично, $ad \notin \{a, d\}$ и по их равенству $ca \notin \{a, c, d\}$. Кроме того, $ca \neq e$, т.к. иначе $c = a^{-1}$ и $d = a^{-1}$, но доказано, что $c \neq d$ — противоречие. Итого, $ca \notin \{a, c, d, e\}$, следовательно $ca = b$. Аналогично $bc = a$.

   $$b^2 = b(ca) = (bc)a = a^2$$

   Рассмотрим a^2.

   - $a^2 \neq a$, т.к. иначе $a = e$.

[1] e всегда коммутирует, а разницы между a, b, c нет, поэтому общность не теряется.

[2] Здесь (и далее) подразумевается, что и ab, и $ba \notin \ldots$

- Аналогично $a^2 = b^2 \neq b$.
- $a^2 \neq c = ab$, т.к. иначе $a = b$.
- $a^2 = b^2 \neq d = ba$, т.к. иначе $b = a$.

Единственный оставшийся вариант — $a^2 = e$, но тогда:

$$cb = ab^2 = a = db \Rightarrow c = d, !!!$$

$\square$

Упражнение 2. Рассмотрим группу $(\mathbb{Z}, +)$ по сложению. Выделим два подмножества:

$$A = \{1337n \mid n \in \mathbb{Z}\} \quad B = \{n \in \mathbb{Z} \mid n \,\vdots\, 1528\}$$

Показать, что A, B есть подгруппы, а также $H = A + B$ — тоже подгруппа. Найти индекс H относительно левых смежных классов.

Решение. A — подгруппа:

1. $0 \in A$
2. $\forall 1337n, 1337m \in A \;\; 1337n + 1337m = 1337(n+m) \in A$
3. $\forall 1337n \in A \;\; \exists 1337(-n) \in A : 1337n + 1337(-n) = 1337 \cdot 0 = 0$

Аналогичными выкладками B — подгруппа.

H — подгруппа:

1. $\underbrace{0}_{\in A} + \underbrace{0}_{\in B} \in H$
2. $\forall (1337n + 1528m), (1337k + 1528l) \in H \;\; 1337n + 1528m + 1337k + 1528l = 1337(n + k) + 1528(m + l) \in H$
3. $\forall 1337n + 1528m \in H \;\; \exists 1337(-n) + 1528(-m) \in H : 1337n + 1528m + 1337(-n) + 1528(-m) = 0$

Несложно посчитать, что НОД$(1337, 1528) = 191$ и тогда $H = 191\mathbb{Z}$, т.к.

$$1337n + 1528m = 191(7n + 8m)$$

и $7n+8m$ пробегает всё $\mathbb{Z}$. Кроме того, очевидно, что $[\mathbb{Z} : 191\mathbb{Z}] = 191$, т.к. левые смежные классы будут иметь вид $191\mathbb{Z} + n$, два класса для n_1 и n_2 совпадают $\Leftrightarrow n_1 \equiv n_2 \mod 191$.

$\square$

Упражнение 3. Рассмотрим группу G (не обязательно конечную) и некоторую её подгруппу H. Показать, что условия $[G : H] = 2$ достаточно для нормальности H. Найти G/H в таком случае.

Решение. Т.к. $[G : H] = 2$, все левые смежные классы равны либо H, либо aH для некоторого фиксированного $a \in G$. Кроме того, $aH \neq H \Rightarrow a \notin H$. Т.к. левые смежные классы делят группу на непересекающиеся множества, $ah = G \setminus H$.

Докажем, что $\forall g \in G \;\; gH = Hg$. Если $g \in H$, то искомое очевидно. Иначе $gH = G \setminus H$, т.к. $H \not\ni g = ge \in gH$. Аналогично $Hg = G \setminus H$. □

Упражнение 4. Определить все подгруппы групп: $\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_6$

Замечание: операция “$\hat{\oplus}$” в $\mathbb{Z}_2 \times \mathbb{Z}_2$ определяется покомпонентно:

$$z, w \in \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$z = (a, b), \quad w = (u, v)$$

$$z \hat{\oplus} w = (a, b) \hat{\oplus} (u, v) = (a \oplus u, b \oplus w)$$

где “$\oplus$” есть операция в $\mathbb{Z}_2$

Решение.

1. $\mathbb{Z}_4$

   $\mathbb{Z}_4, \{0\}$ — тривиальные подгруппы.

   Здесь и далее H — подгруппа рассматриваемой группы.

   Пусть $1 \in H$. По замкнутости $2 = 1 + 1 \in H, 3 = 2 + 1 \in H$, т.е. если $1 \in H$, то $H = \mathbb{Z}_4$.

   Пусть $2 \in H$. Тогда все искомые свойства выполнены без добавления каких-либо элементов[3], т.к. $2 + 2 = 0 \in H, 2^{-1} = 2$, $\{0, 2\}$ — подгруппа $\mathbb{Z}_4$.

   Пусть $3 \in H$. $3^{-1} = 1 \Rightarrow 1 \in H \Rightarrow H = \mathbb{Z}_4$

   Ответ: $\{0\}, \mathbb{Z}_4, \{0, 2\}$

2. $\mathbb{Z}_2 \times \mathbb{Z}_2$

   $\mathbb{Z}_2 \times \mathbb{Z}_2, \{(0, 0)\}$ — тривиальные подгруппы.

   Пусть $(1, 1) \in H$. Тогда все искомые свойства выполнены без добавления элементов, т.к. $(1, 1) + (1, 1) = (0, 0) \in H, (1, 1)^{-1} = (1, 1)$, $\{(0, 0), (1, 1)\}$ — подгруппа $\mathbb{Z}_2 \times \mathbb{Z}_2$.

   Пусть $(1, 0) \in H$. $(1, 0) + (1, 0) = (0, 0) \in H, (1, 0)^{-1} = (1, 0) \Rightarrow \{(0, 0), (1, 0)\}$ — подгруппа $\mathbb{Z}_2 \times \mathbb{Z}_2$. Аналогичное верно для $(0, 1)$.

   Пусть и $(1, 0)$, и $(0, 1) \in H$. Тогда $(1, 1) \in H$ по замкнутости и следовательно $H = \mathbb{Z}_2 \times \mathbb{Z}_2$.

[3] Кроме нейтрального.

Пусть и $(1, 1)$, и $(0, 1) \in H$. Тогда $(1, 1) + (0, 1) = (1, 0) \in H$ по замкнутости и $H = \mathbb{Z}_2 \times \mathbb{Z}_2$. Аналогично для $(1, 1)$ и $(0, 1)$.

Ответ: $\{(0, 0)\}, \mathbb{Z}_2 \times \mathbb{Z}_2, \{(0, 0), (1, 1)\}, \{(0, 0), (1, 0)\}, \{(0, 0), (0, 1)\}$

3. $\mathbb{Z}_6$

   $\mathbb{Z}_6, \{0\}$ — тривиальные подгруппы.

   Пусть $1 \in H$. Тогда $H = \mathbb{Z}_6$, аналогично первому случаю.

   Пусть $2 \in H$. Тогда $2 + 2 = 4 \in H$. $2^{-1} = 4, 4^{-1} = 2, 2 + 4 = 0, 4 + 4 = 2$, H — подгруппа.

   Пусть $3 \in H$. Тогда $3 + 3 = 0, 3^{-1} = 3, H$ — подгруппа.

   Пусть $4 \in H$. Тогда $4^{-1} = 2 \in H$, см. тот случай.

   Пусть $5 \in H$. Тогда $5 + 5 = 4 \in H \Rightarrow 2 \in H \Rightarrow 2 + 5 = 1 \in H \Rightarrow H = \mathbb{Z}_6$.

   Если $2, 3 \in H$, то $2 + 3 + 2 = 1 \in H \Rightarrow H = \mathbb{Z}_6$.

   Если $2, 5 \in H$, то $2 + 5 = 1 \in H \Rightarrow H = \mathbb{Z}_6$.

   Все случаи для $2 \in H$ разобраны, остался случай $3 \in H(2 \notin H)$. Если $5 \in H$, то $3 + 5 = 2 \in H$, !!!.

   Ответ: $\{0\}, \{0, 2, 4\}, \{0, 3\}, \mathbb{Z}_6$.

$\square$

Упражнение 5. Рассмотрим циклическую группу порядка 129. Найти все её подгруппы.

Решение. Рассмотрим H — подгруппу C_{129}. Пусть $C_{129} = \langle a \rangle$. Тогда $a^k \in H$. По замкнутости $\forall i \in \mathbb{Z} \;\; a^{ik} \in H$. Если $gcd(129, k) = 1$, то ik пробегает все элементы $\mathbb{Z}_{129}$ и тогда $H = C_{129}$. Если же $gcd(129, k) \neq 1$, то H не обязательно $= C_{129}$. Нетривиальных делителей 129 всего два: 3 и 43. Им соответствуют подгруппы $\{1, g^{43}, g^{126}\}$ и $\{1, g^3, g^6 \dots g^{126}\}$.

Ответ: $\{1, g^{43}, g^{126}\}, \{1, g^3, g^6 \dots g^{126}\}, \{e\}, C_{129}$. $\square$