Арунова Маргарита БПМИ2011

Предложение. Пусть G – циклическая, тогда

(а) $|G| = \infty \ \Leftrightarrow \ G \simeq (\mathbb{Z}, +)$

(б) $|G| = n \quad \Leftrightarrow \ G \simeq (\mathbb{Z}_n, +)$

Определение. *Прямое произведение* групп $G_1, G_2, \ldots, G_n$ – это множество $G_1 \times G_2 \times \ldots \times G_n$ с бинарной операцией $(g_1, g_2, \ldots, g_n)(g_1^{'}, g_2^{'}, \ldots, g_m^{'}) = (g_1 g_1^{'}, g_2 g_2^{'}, \ldots, g_m g_m^{'})$.

Замечание. Для $G_1 \times G_2 \times \ldots \times G_n$ верно следующее:

(а) группа $G_1 \times G_2 \times \ldots \times G_n$ абелева тогда и только тогда, когда все $G_1, G_2, \ldots, G_n$ абелевы

(б) если группы $G_1, G_2, \ldots, G_n$ кончены, то $|G_1 \times G_2 \times \ldots \times G_n| = |G_1| \cdot |G_2| \cdot \ldots \cdot |G_n|$

Определение. Говорят, что G *разлагается в произведение* своих подгрупп $H_1, \ldots, H_n$, если отображение $H_1 \times \ldots \times H_n \to G$, $(h_1, \ldots, h_n) \to h_1, \cdot \ldots \cdot h_n$ изоморфизмом.

Теорема. Пусть числа $n, m, l \in \mathbb{N}$ таковы, что $n = ml$ и НОД$(m, l) = 1$. Тогда $\mathbb{Z}_n \simeq \mathbb{Z}_m \times \mathbb{Z}_l$.
Следствие (разложение конечной циклической группы)**.** Пусть $n \geqslant 2$ – натуральное число и $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_s^{k_s}$ – его разложение на простые множители ($p_i \neq p_j$ при $i \neq j$). Тогда выполняется следующее: $\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_s^{k_s}}$.

Определение. Конечная абелева группа A называется *примарной*, если $|A| = p^k$, где p – простое и $k \in N$.

Теорема (классификация конечных абелевых групп)**.** Пусть A – конечная абелева группа.
Тогда $A \simeq \mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_t^{k_t}}$, где $p_1, \ldots, p_t$ – простые числа (не обязательно попарно различные) и $k_1, \ldots, k_t \in \mathbb{N}$. Более того, набор примарных циклических множителей $\mathbb{Z}_{p_1^{k_1}}, \ldots, \mathbb{Z}_{p_t^{k_t}}$ определён однозначно с точностью до перестановки (в частности, число этих множителей определено однозначно).

Пусть A – конечная абелева подгруппа.

Определение. *Экспонентой* группы A называется число

$$\exp A = \min\{m \in \mathbb{N} \mid ma = 0 \text{ для всех } a \in A\}$$

$(*)$ используется аддитивная запись групповой операции

Замечание. Для $\exp A$ выполняются следующие утверждения:

(а) $ma = 0 \ \Leftrightarrow \ m \,\vdots\, \mathrm{ord}(a)$ для всех $a \in A$, $m \in \mathbb{Z} \Rightarrow \exp A = \text{НОК}\{\mathrm{ord}(a) \mid a \in A\}$

(б) $|A| \,\vdots\, \mathrm{ord}(a)$ для всех $a \in A \Rightarrow |A|$ – общее кратное множества $\{\mathrm{ord}(a) \mid a \in A\} \Rightarrow |A| \,\vdots\, \exp A$ и $|A| \geqslant \exp A$

Предложение (критерий цикличности)**.** $\exp A = |A| \ \Leftrightarrow$ группа A является цикличной.

Задание 1. Сколько элементов порядков 2, 5, 10 и 25 в группе $\mathbb{Z}_2 \times \mathbb{Z}_{10} \times \mathbb{Z}_{25}$?

1. Пусть элемент $g = (a, b, c) \in \mathbb{Z}_2 \times \mathbb{Z}_{10} \times \mathbb{Z}_{25}$ имеет порядок m, тогда $(ma, mb, mc) = e$, где элемент e – нейтральный элемент (в данной группе, этот элемент равен $(0, 0, 0)$). Количество элементов, на порядок которых делится число m, – это число решений системы:
$$\begin{cases} ma \equiv 0 \mod 2 \\ mb \equiv 0 \mod 10 \\ mc \equiv 0 \mod 25 \end{cases}$$
Если какой-то элемент $(a, b, c) \in \mathbb{Z}_2 \times \mathbb{Z}_{10} \times \mathbb{Z}_{25}$ удовлетворяет данной системе, то порядок этого элемента делит число m. Для найденных элементов $\operatorname{ord}(a)$, $\operatorname{ord}(b)$, $\operatorname{ord}(c)$ делят m, значит, и $\operatorname{ord}((a, b, c)) = \text{НОК}(\operatorname{ord}(a),\ \operatorname{ord}(b),\ \operatorname{ord}(c))$ делит m (их НОК не больше m).

2. Найдём количество элементов, порядок которых равен 2. Для этого найдём число решений описанной системы при $m = 2$. Это число – количество элементов, порядок которых делит m. Для $m = 2$ будут посчитаны элементы с порядком 1 и 2. Из них нужны только элементы с порядком 2.
$$\begin{cases} 2a \equiv 0 \mod 2 \\ 2b \equiv 0 \mod 10 \\ 2c \equiv 0 \mod 25 \end{cases} \Leftrightarrow \begin{cases} 2a \equiv 0 \mod 2 \\ b \equiv 0 \mod 5 \\ c \equiv 0 \mod 25 \end{cases} \Leftrightarrow \begin{cases} a \in \{0, 1\} \\ b \in \{0, 5\} \\ c = 0 \end{cases}$$
Всего $2 \cdot 2 \cdot 1 = 4$ решения. Решение $e = (0, 0, 0)$ порядок 1, поэтому не подходит. Оставшиеся решения имеют порядок 2: их порядок больше 1, так как это не нейтральные элементы, и их порядок должен делить число 2.
Получаем, что элементов порядка 2 всего три.

3. Найдём количество элементов, порядок которых равен 5. Аналогичным образом посчитаем количество решений системы:
$$\begin{cases} 5a \equiv 0 \mod 2 \\ 5b \equiv 0 \mod 10 \\ 5c \equiv 0 \mod 25 \end{cases} \Leftrightarrow \begin{cases} a \equiv 0 \mod 2 \\ b \equiv 0 \mod 2 \\ c \equiv 0 \mod 5 \end{cases} \Leftrightarrow \begin{cases} a = 0 \\ b \in \{0, 2, 4, 6, 8\} \\ c \in \{0, 5, 10, 15, 20\} \end{cases}$$
Всего элементов, порядок которых делит 5, равно $1 \cdot 5 \cdot 5 = 25$. Из этого количества вычитаем единицу, так как нейтральный элемент имеет порядок 1. У остальных посчитанных элементов порядок 5, так как их порядок не равен 1 и делит число 5.
Таким образом, элементов, которые имеют порядок равный 5, всего 24.

4. Найдём количество элементов порядка 10. Для этого посчитаем количество решений системы:
$$\begin{cases} 10a \equiv 0 \mod 2 \\ 10b \equiv 0 \mod 10 \\ 10c \equiv 0 \mod 25 \end{cases} \Leftrightarrow \begin{cases} 10a \equiv 0 \mod 2 \\ 10b \equiv 0 \mod 2 \\ 2c \equiv 0 \mod 5 \end{cases} \Leftrightarrow \begin{cases} a \in \{0, 1\} \\ b \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} \\ c \in \{0, 5, 10, 15, 20\} \end{cases}$$

Всего элементов, порядок которых делит 10, равно $2 \cdot 10 \cdot 5 = 100$. Для нахождения количества элементов, порядок которых равен 10, нужно из полученного числа вычесть количество элементов порядка 1, 2, 5 (то есть порядков, являющихся делителями числа 10). Элементы порядков, не равных 1, 2, 5, 10, в найденное количестве не включены.

Искомое число элементов порядка 10 равно $100 - 1 - 3 - 24 = 72$.

5. Найдём количество элементов порядка 25.

$$\begin{cases} 25a \equiv 0 \mod 2 \\ 25b \equiv 0 \mod 10 \\ 25c \equiv 0 \mod 25 \end{cases} \Leftrightarrow \begin{cases} a \equiv 0 \mod 2 \\ 5b \equiv 0 \mod 2 \\ 5c \equiv 0 \mod 5 \end{cases} \Leftrightarrow \begin{cases} a = 0 \\ b \in \{0, 2, 4, 6, 8\} \\ c \in \{0, 1, \ldots, 24\} \end{cases}$$

Получаем, что количество элементов с порядком, делящим 25 равно $1 \cdot 5 \cdot 25 = 125$. Среди этих элементов посчитаны те, порядок которых равен 1, 5, 25 (делители 25).

Число элементов порядка 25 равно $125 - 1 - 24 = 100$.

Ответ: – элементов порядка 2 : 3

– элементов порядка 5 : 24

– элементов порядка 10 : 72

– элементов порядка 25 : 100

Задание 2. Сколько подгрупп порядков 3 и 15 в нециклической абелевой группе порядка 90?

1. Всякая конечная абелева группа A разлагается в прямое произведение примарных циклических групп $\mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_t^{k_t}}$. В случае, когда A – циклическая, $A \simeq \mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_s^{k_s}}$, где число n – порядок группы A и $n = |A| = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$ – каноническое разложение числа на простые множители.

2. Пусть абелева группа A имеет порядок 90. Это число представляется в виде следующего произведения простых множителей $90 = 2 \cdot 3^2 \cdot 5$.

   Если A циклическая, то она изоморфна $\mathbb{Z}_{90}$, а группа $\mathbb{Z}_{90}$ изоморфна следующим прямым произведениям с точностью до перестановки:

   $$\mathbb{Z}_{90} \simeq \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_9 \simeq \mathbb{Z}_5 \times \mathbb{Z}_{18} \simeq \mathbb{Z}_2 \times \mathbb{Z}_{45} \simeq \mathbb{Z}_9 \times \mathbb{Z}_{10}$$

   Используются теоремы о разложении конечной циклической группы и о том, что для $n = ml$ и НОД$(m, l) = 1$ выполняется $\mathbb{Z}_n \simeq \mathbb{Z}_m \times \mathbb{Z}_l$.

   Если взять какое-то разложение $t_1 \cdot \ldots \cdot t_s$ числа 90 на натуральные множители, где НОД$(t_i, t_j) = 1$ для каждого $i \neq j$, то прямое произведение $\mathbb{Z}_{t_1} \times \ldots \times \mathbb{Z}_{t_s}$ изоморфно $\mathbb{Z}_{90}$.

3. По условию рассматриваемая абелева группа A порядка 90 нециклическая $\Rightarrow$ A неизоморфна любой циклической группе. В частности, она неизоморфна $\mathbb{Z}_{90}$ и описанным прямым произведениям.

   Группа A – конечная абелева группа $\Rightarrow$ она разлагается в произведение примарных циклических групп, произведение порядков которых равно $|A| = 90$. Для числа 90 существует разложение на множители, такое что хотя бы два множителя не взаимнопросты. Например, $90 = 2 \cdot 3 \cdot 3 \cdot 5$. Таким образом, для группы A:

   $$A \simeq \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{15} \simeq \mathbb{Z}_6 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{10} \simeq \mathbb{Z}_6 \times \mathbb{Z}_{15}$$

   Других таких разложений, что A нециклическая нет.

4. Заметим, что подгруппы порядков 3 и 15 в A – циклические. Действительно, пусть H_3 и H_{15} какие-то подгруппы порядка 3 и 15 в A. Эти подгруппы конечные и абелевы, значит, они разлагаются в прямое произведение примарных групп.

   Произведение порядков примарных групп, на которые разлагается H, равно порядку H. Пользуясь тем, что $|H_3| = 3$ и $|H_{15}| = 15 = 3 \cdot 5$, получаем $H_3 \simeq \mathbb{Z}_3$ и $H_{15} \simeq \mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{15}$ (последнее верно в силу НОД$(3, 5) = 1$).

5. Известно, что порядок каждого элемента в группе делит порядок самой группы. Это означает, что в каждой подгруппе H_3 могут содержаться только элементы порядка 1 и 3.

   В каждой подгруппе содержится нейтральный элемент e, $\mathrm{ord}(e) = 1$. Это единственный элемент порядка 1 в группе и, следовательно, в подгруппе. Значит, оставшиеся два элемента в H_3 – это элементы порядка 3.

6. Найдём количество элементов порядка 3 в группе A. Существует изоморфизм $A \simeq \mathbb{Z}_6 \times \mathbb{Z}_{15} \Rightarrow$ количество элементов какого-то порядка в A равно количеству элементов этого же порядка в $\mathbb{Z}_6 \times \mathbb{Z}_{15}$. Таким образом, достаточно найти количество таких элементов в $\mathbb{Z}_6 \times \mathbb{Z}_{15}$.

   Каждый элемент группы $\mathbb{Z}_6 \times \mathbb{Z}_{15}$ имеет вид (a, b), где $a \in \mathbb{Z}_6$, $b \in \mathbb{Z}_{15}$. Если порядок элемента равен 3, то $(3a, 3b) = (0, 0) = e$. Решим систему:

$$\begin{cases} 3a \equiv 0 \bmod 6 \\ 3b \equiv 0 \bmod 15 \end{cases} \Leftrightarrow \begin{cases} a \equiv 0 \bmod 2 \\ b \equiv 0 \bmod 5 \end{cases} \Leftrightarrow \begin{cases} a \in \{0, 2, 4\} \\ b \in \{0, 5, 10\} \end{cases}$$

   Всего элементов, порядок которых делит число 3, в группе A равно $3 \cdot 3 = 9$. Среди этих элементов перечислены элементы с порядком 1 и 3. Таким образом, элементов с порядком 3 в рассматриваемой группе A равно $9 - 1 = 8$ (из найденного количества вычитаем элементы с порядком 1, а таких элементов в любой группе ровно одна штука – нейтральный).

7. Определим количество подгрупп порядка 3, зная число элементов порядка 3 в A.

   Заметим, что все подгруппы простого порядка p либо совпадают, либо пересекаются только в нейтральном элементе. Известно, что пересечение двух подгрупп $H_\cap = H \cap H'$ – подгруппа в каждой из них. По теореме Лагранжа порядок подгруппы делит порядок группы, значит $|H_\cap|$ делит $|H| = p$ и $|H'| = p \Rightarrow |H_\cap|$ равен либо p, то есть H и H' совпадают, либо 1, то есть подгруппы пересекаются в нейтральном элементе.

   Последнее означает, что каждый элемент порядка 3 может присутствовать только в одной подгруппе порядка 3 (иначе пересечение будет нетривиальным).

   Таким образом, подгрупп порядка 3 в A ровно $\frac{8}{2} = 4$ (в каждую подгруппу помещаем нейтральный элемент и какие-то два элемента из восьми имеющихся порядка 3).

8. Найдём число элементов порядка 5. Зная это число, будет несложно найти число элементов порядка 15. Тогда нужно будет найти число элементов, порядок которых делит 15, и вычесть из этого количества число элементов порядка 1, 3 и 5.

   Решим следующую систему:

$$\begin{cases} 5a \equiv 0 \bmod 6 \\ 5b \equiv 0 \bmod 15 \end{cases} \Leftrightarrow \begin{cases} a \equiv 0 \bmod 6 \\ b \equiv 0 \bmod 3 \end{cases} \Leftrightarrow \begin{cases} a = 0 \\ b \in \{0, 3, 6, 9, 12\} \end{cases}$$

   Получаем, что элементов, порядок которых делит 5, будет $1 \cdot 5 = 5$, а элементов порядка 5 всего $5 - 1 = 4$.

9. Найдём количество элементов порядка 15.

$$\begin{cases} 15a \equiv 0 \bmod 6 \\ 15b \equiv 0 \bmod 15 \end{cases} \Leftrightarrow \begin{cases} 5a \equiv 0 \bmod 2 \\ 15b \equiv 0 \bmod 15 \end{cases} \Leftrightarrow \begin{cases} a \in \{0, 2, 4\} \\ b \in \{0, \ldots, 14\} \end{cases}$$

   Количество элементов с порядком, делящим 15, равно $3 \cdot 15 = 45$. Чтобы получить элементы порядка 15, нужно из полученного количества вычесть число элементов порядка 1, 3 и 5.

   Искомое количество: $45 - 4 - 8 - 1 = 32$.

10. В силу того, что $H_{15} \simeq \mathbb{Z}_{15}$, описанная подгруппа порождается элементом порядка 15. Количество искомых подгрупп не обязательно равно количеству элементов порядка 15, так как одна и та же подгруппа порядка 15 может порождаться разными элементами порядка 15.

    Так как каждая подгруппа H_{15} изоморфна $\mathbb{Z}_{15}$, количество элементов, порядок которых равен 15, у них совпадает. Это количество – число элементов в $\mathbb{Z}_{15}$, которые удовлетворяют представленному ниже уравнению только при $m = 15k,\ k \in \mathbb{Z}$:

    $$mx \equiv 0 \bmod 15$$

    Эти элементы – взаимно простые с 15 числа, а их количество равно $\varphi(15) = \varphi(3) \cdot \varphi(5) = 8$ (где φ – функция Эйлера).

11. Один и тот же порождающий элемент в разные подгруппы входить не может, а значит, всего подгрупп порядка 15 – это количество элементов порядка 15 в A, делённое на количество элементов порядка 15 в каждой подгруппе, то есть $\frac{32}{8} = 4$.

Ответ: – подгрупп порядка 3 : 4

– подгрупп порядка 15 : 4

Задание 3. При каком наименьшем $n \in \mathbb{N}$ группа $\mathbb{Z}_{15} \times \mathbb{Z}_{18} \times \mathbb{Z}_{20}$ изоморфна прямому произведению n циклических групп?

1. Покажем, что группа $\mathbb{Z}_{15} \times \mathbb{Z}_{18} \times \mathbb{Z}_{20}$ не является циклической. Порядок этой группы равен $15 \cdot 18 \cdot 20 = 5400$. Если группа циклическая, то она порождается каким-то элементом g, и порядок этого элемента $\operatorname{ord}(g) = |\langle g \rangle| = 5400$, но в $\mathbb{Z}_{15} \times \mathbb{Z}_{18} \times \mathbb{Z}_{20}$ каждый элемент имеет порядок не больший $\text{НОК}(15, 18, 20) = 180$.

2. Используя теорему о том, что для чисел $n, m, l \in \mathbb{N}$, таких что $n = ml$ и $\text{НОД}(m, l) = 1$, верно $\mathbb{Z}_n \simeq \mathbb{Z}_m \times \mathbb{Z}_l$, выполним следующие преобразования:
$$\mathbb{Z}_{15} \times \mathbb{Z}_{18} \times \mathbb{Z}_{20} \simeq \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \simeq \underbrace{\mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_4}_{\mathbb{Z}_{15} \times \mathbb{Z}_4 \simeq \mathbb{Z}_{60}} \times \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5}_{\mathbb{Z}_{18} \times \mathbb{Z}_5 \simeq \mathbb{Z}_{90}} \simeq \mathbb{Z}_{60} \times \mathbb{Z}_{90}$$

3. Таким образом, рассматриваемая группа изоморфна произведению двух циклических групп $\mathbb{Z}_{60}$ и $\mathbb{Z}_{90}$. Группа $\mathbb{Z}_{15} \times \mathbb{Z}_{18} \times \mathbb{Z}_{20}$ не может быть изоморфна произведению меньшего числа циклических групп, так как иначе она будет изоморфна какой-то одной циклической группе, что противоречит доказанному в первом пункте (если она будет изоморфна циклической группе, то она будет также циклическая).

Ответ: 2

Задание 4. Пусть k – наибольший порядок элементов конечной абелевой группы A. Докажите, что порядок любого элемента A делит k.

1. Предположим противное: пусть в группе A существует элемент a, порядок которого равен n и не делит число k. Тогда существует такое простое число p в разложении числа n на простые множители, что степень вхождения p в n больше степени вхождения p в k.

2. Пусть число $n = p^\alpha s$, а число $k = p^\beta t$, причём $0 \leqslant \beta < \alpha$, s и t взаимнопросты с p. Покажем, что в A найдутся элементы порядков p^α и t.
   - Пусть группа G содержит элемент g порядка xy, тогда, рассмотрев элемент g^x, получим элемент порядка y (выполнено $(g^x)^y = g^{xy} = e$).
   - Порядок g^x не меньше y, так как иначе, если $\mathrm{ord}(g^x) = z < y$, получим $xz < xy$, то есть $g^{xz} \neq e$ (xy – порядок g, следовательно наименьшее натуральное, такое что $g^{xy} = e$).
   - Аналогично, получаем, что элемент порядка x также найдётся в A.

3. Пусть a_1 элемент порядка p^α, а a_2 элемент порядка t. Покажем, что порядок элемента $a_1 a_2 = a_2 a_1$ равен произведению порядков этих элементов.
   - Нетрудно заметить, что $(a_1 a_2)^{p^\alpha t} = a_1^{p^\alpha t} \cdot a_2^{p^\alpha t} = (a_1^{p^\alpha})^t \cdot (a_2^t)^{p^\alpha} = e \cdot e = e$ (группа абелева, следовательно, операции коммутативны). Таким образом, нужно показать, что число $p^\alpha t$ наименьшее с данным свойством.
   - Пусть $q = \mathrm{ord}(a_1 a_2)$, тогда $(a_1 a_2)^q = e \Rightarrow e = ((a_1 a_2)^q)^{p^\alpha} = (a_1 a_2)^{p^\alpha q} = a_1^{p^\alpha q} \cdot a_2^{p^\alpha q} = e \cdot a_2^{p^\alpha q} = a_2^{p^\alpha q}$, следовательно, $p^\alpha q \,\vdots\, \mathrm{ord}(a_2) = t$. Так как НОД$(p^\alpha, t) = 1$, получаем $q \,\vdots\, t$.
     Аналогично получаем, что $q \,\vdots\, p^\alpha$. Значит, $q \geqslant p^\alpha t$ и $p^\alpha t$ является порядком элемента $a_1 a_2$.

4. Получаем, что у элемента $a_1 a_2$ порядок равен $p^\alpha t = k p^{\alpha - \beta} > k$ – противоречие с тем, что k наибольший порядок элементов.

5. Таким образом в конечной абелевой группе порядок каждого элемента является делителем наибольшего порядка элементов.