Алгебра
Примеры решения вычислительных задач

Вадим Гринберг
157-1

Содержание

Надеюсь, это поможет вам при подготовке к контрольной

1 Домашнее задание №1

1.1 Элементы порядка 12

Задача №2. *Найдите все элементы порядка* 12 *в группе* $(\mathbb{C} \setminus \{0\}, \times)$.

Решение. Пусть $c \in (\mathbb{C} \setminus \{0\}, \times)$. Тогда порядком элемента c обозначается такое наименьшее число m, что $c^m = e$, где e – нейтральный элемент (единица группы).

Нейтральным элементом группы $(\mathbb{C} \setminus \{0\}, \times)$ является число 1:

$$\forall\ a + ib \in (\mathbb{C} \setminus \{0\}, \times) \Rightarrow 1 \cdot (a + ib) = (a + ib) \cdot 1 = a + ib$$

В данной задаче нужно найти все $c \mid c^{12} = 1$.

Заметим, что если $c^{12} = 1$, то $\Rightarrow \begin{cases} c^6 = 1 \text{ не подходит, так как тогда } m = 6 \\ c^6 = -1 \end{cases}$

Но тогда: $c^6 = -1 \Rightarrow \begin{cases} c^3 = i \\ c^3 = -i \end{cases}$

Пусть $c = a + ib$. Значит:

$$c^3 = (a + ib)^3 = (a^2 - b^2 + 2abi)(a + ib) =$$
$$a^3 - ab^2 + 2a^2bi + a^2ib - ib^3 - 2ab^2 =$$
$$(a^3 - 3ab^2) + i(3a^2b - b^3)$$

Итого 2 случая:

1. $c^3 = i$

   $(a^3 - 3ab^2) + i(3a^2b - b^3) = i$

   Тогда:

   - $a^3 - 3ab^2 = 0 \Rightarrow a(a^2 - 3b^2) = 0 \Rightarrow a = 0$, $a = b\sqrt{3}$ или $a = -b\sqrt{3}$
   - $3a^2b - b^3 = 1$
     (a) $a = 0 \Rightarrow -b^3 = 1 \Rightarrow b = -1 \Rightarrow c = -i$ – не подходит, так как $c^4 = 1$
     (b) $a = b\sqrt{3} \Rightarrow 9b^3 - b^3 = 1 \Rightarrow b^3 = \frac{1}{8} \Rightarrow b = \frac{1}{2} = a \Rightarrow c = \frac{\sqrt{3}}{2} + i\frac{1}{2}$
     (c) $a = -b\sqrt{3} \Rightarrow 9b^3 - b^3 = 1 \Rightarrow b^3 = \frac{1}{8} \Rightarrow b = \frac{1}{2} \Rightarrow a = -\frac{\sqrt{3}}{2} \Rightarrow c = -\frac{\sqrt{3}}{2} + i\frac{1}{2}$

2. $c^3 = -i$

   $(a^3 - 3ab^2) + i(3a^2b - b^3) = -i$

   Тогда:

   - $a^3 - 3ab^2 = 0 \Rightarrow a(a^2 - 3b^2) = 0 \Rightarrow a = 0$, $a = b\sqrt{3}$ или $a = -b\sqrt{3}$
   - $3a^2b - b^3 = -1$
     (a) $a = 0 \Rightarrow -b^3 = -1 \Rightarrow b = 1 \Rightarrow c = i$ – не подходит, так как $c^4 = 1$
     (b) $a = b\sqrt{3} \Rightarrow 9b^3 - b^3 = -1 \Rightarrow b^3 = -\frac{1}{8} \Rightarrow b = -\frac{1}{2} = a \Rightarrow c = -\frac{\sqrt{3}}{2} - i\frac{1}{2}$
     (c) $a = -b\sqrt{3} \Rightarrow 9b^3 - b^3 = -1 \Rightarrow b^3 = -\frac{1}{8} \Rightarrow b = -\frac{1}{2} \Rightarrow a = \frac{\sqrt{3}}{2} \Rightarrow c = \frac{\sqrt{3}}{2} - i\frac{1}{2}$

Таким образом, мы получили все 4 значения для c таких, что $c^{12} = 1$.

Q.E.D.

1.2 Смежные классы – первое решение (быстрое, но на подумать)

Задача №3. *Найдите все левые и правые смежные классы группы A_4 по подгруппе $\langle\sigma\rangle$, где* $\sigma = \begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}$

Решение (Анастасия Иовлева). Нам дана группа A_4 четных подстановок длины 4 и подгруппа, которую я обозначу за H, равная

$$\left\{\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}\right\}$$

Нам надо найти все правые и левые смежные классы к этой подгруппе. Для начала хотя бы посчитаем, сколько их. Всего количество элементов в A_n равно $4!/2 = 12$, а в нашей подгруппе 3 элемента. Значит, $[A_n : H] = [H : A_n] = 12/3 = 4$.

Рассмотрим сначала левые смежные классы. Заметим, что любая $\sigma \in H$ не сдвигает 4, а значит, если для $\omega \in A_n$ верно, что $\omega(i) = 4$, то и $\omega\sigma(i) = 4$. Также заметим, что для фиксированной ω и различных σ образы элементов 1, 2 и 3 в $\omega\sigma$ просто сдвигаются по циклу, то есть $\omega(1)\omega(2)\omega(3) \to \omega(2)\omega(3)\omega(1) \to \omega(3)\omega(1)\omega(2)$. Следовательно, подстановки, порождающие разные смежные классы, отличаются тем, под каким элементом стоит 4 и в каком порядке идут оставшиеся образы. А именно, это следующие подстановки:

$$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}$$
$$\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}$$

Осталось только выделить среди них четные:

$$G_l = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}$$

Итого, все левые смежные классы имеют вид gH, где $g \in G_l$.

Теперь рассмотрим правые смежные классы. Аналогично левым, получаем что подстановки, порождающие различные правые смежные классы, отличаются тем, какой образ у 4, и в каком порядке идут оставшиеся образы. То есть это следующие подстановки:

$$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix},$$
$$\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}$$

Теперь оставим из них только четные:

$$G_r = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}$$

Итого, все правые смежные классы имеют вид Hg, где $g \in G_r$. **Q.E.D.**

1.3 Смежные классы – второе решение (долгое, но очевидное)

Задача №3. *Найдите все левые и правые смежные классы группы A_4 по подгруппе $\langle\sigma\rangle$, где* $\sigma = \begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}$

Решение (я). Левым смежным классом элемента g группы G по подгруппе H называется подмножество $gH = \{gh \mid h \in H\}$.

Правым смежным классом элемента g группы G по подгруппе H называется подмножество $Hg = \{hg \mid h \in H\}$.

Лемма. *Пусть G – группа, $H \subset G$ – подгруппа, $g_1, g_2 \in G$. Тогда либо $g_1H = g_2H$, либо $g_1H \bigcap g_2H = \varnothing$. Аналогично, либо $Hg_1 = Hg_2$, либо $Hg_1 \bigcap Hg_2 = \varnothing$.*

Группа A_4 – чётные подстановки длины 4.

$\langle\sigma\rangle$ – циклическая подгруппа, то есть подмножество $\sigma^m \mid m \in \mathbb{Z}$ в A_4.

Для начала, найдём все элементы $\langle\sigma\rangle$, возводя подстановку в степени:

$\sigma^2 = \begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}$ $\sigma^3 = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix} = id = e$ $\sigma^4 = \begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix} = \sigma$

$\sigma^{-1} = \begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix} = \sigma^2 \Longrightarrow$

В подгруппе $\langle\sigma\rangle$ всего 3 элемента:

$\sigma^{-1} = \begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}$ $\sigma = \begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}$ $id = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$ – обозначим множество из этих элементов как H.

Найдём теперь смежные классы для всех элементов A_4. Было доказано на Линейной Алгебре в 1 семестре, что чётность произведения подстановок равна произведению их чётностей.

Выпишем все подстановки из A_4:

$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$ $\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}$ $\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}$
$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$ $\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}$ $\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}$
$\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}$ $\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix}$ $\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$
$\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}$ $\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}$ $\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$

- Левые смежные классы:

1. $\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$ – данная подстановка есть id, поэтому для неё левым смежным классом будет всё множество H.
2. $\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix} = \begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix}$
   $\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix} = \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$
   $\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix} = \begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}$
3. $\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix} = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$
   $\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix} = \begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}$
   $\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix} = \begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}$
4. $\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix} = \begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}$
   Элемент смежного класса совпал с элементом класса 2-го, значит, по лемме выше, левые смежные классы этих элементов совпадают.
5. $\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix} = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$
   Элемент смежного класса совпал с элементом класса 1-го, значит, по лемме выше, левые смежные классы этих элементов совпадают.
6. $\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix} = \begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}$
   Элемент смежного класса совпал с элементом класса 3-го, значит, по лемме выше, левые смежные классы этих элементов совпадают.

7. $\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}$

   Элемент смежного класса совпал с элементом класса 1-го, значит, по лемме выше, левые смежные классы этих элементов совпадают.

8. $\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$

   Элемент смежного класса совпал с элементом класса 2-го, значит, по лемме выше, левые смежные классы этих элементов совпадают.

9. $\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}$

   Элемент смежного класса совпал с элементом класса 3-го, значит, по лемме выше, левые смежные классы этих элементов совпадают.

10. $\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$

    $\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}$

    $\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}$

11. $\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}$

    Элемент смежного класса совпал с элементом класса 10-го, значит, по лемме выше, левые смежные классы этих элементов совпадают.

12. $\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$

    Элемент смежного класса совпал с элементом класса 10-го, значит, по лемме выше, левые смежные классы этих элементов совпадают.

- Правые смежные классы:

1. $\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$ – данная подстановка есть id, поэтому для неё правым смежным классом будет всё множество H.

2. $\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}=\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}$

   $\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$

   $\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}=\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}$

3. $\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$

   $\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}$

   $\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}$

4. $\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$

   Элемент смежного класса совпал с элементом класса 3-го, значит, по лемме выше, правые смежные классы этих элементов совпадают.

5. $\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}$

   Элемент смежного класса совпал с элементом класса 1-го, значит, по лемме выше, правые смежные классы этих элементов совпадают.

6. $\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}=\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix}$
$\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$
$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}=\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}$
7. $\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}$

Элемент смежного класса совпал с элементом класса 1-го, значит, по лемме выше, правые смежные классы этих элементов совпадают.

8. $\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix}=\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix}$

Элемент смежного класса совпал с элементом класса 6-го, значит, по лемме выше, правые смежные классы этих элементов совпадают.

9. $\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$

Элемент смежного класса совпал с элементом класса 2-го, значит, по лемме выше, правые смежные классы этих элементов совпадают.

10. $\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}=\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}$

Элемент смежного класса совпал с элементом класса 2-го, значит, по лемме выше, правые смежные классы этих элементов совпадают.

11. $\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}$

Элемент смежного класса совпал с элементом класса 3-го, значит, по лемме выше, правые смежные классы этих элементов совпадают.

12. $\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$

Элемент смежного класса совпал с элементом класса 6-го, значит, по лемме выше, правые смежные классы этих элементов совпадают.

Q.E.D.

2 Домашнее задание №2

2.1 Гомоморфизмы

Задача №2. *Найдите все гомоморфизмы из группы $\mathbb{Z}_{10}$ (остатки по модулю 10) в группу $\mathbb{Z}_{25}$ (остатки по модулю 25).*

Решение. Заметим, что в данном случае у нас группы с операцией $+$.

На лекции было доказано, что для любого гомоморфизма $f : G \to F$ выполнено, что: $\forall\, g \in G\ f(g^n) = (f(g))^n$. Кроме того, порядок элемента $f(g)$ делит порядок элемента g для любого $g \in G$.

Пусть $f : \mathbb{Z}_{10} \to \mathbb{Z}_{25}$ – гомоморфизм, $z_{10} \in \mathbb{Z}_{10}$ – порождающий элемент.

Пусть $f(z_{10}) = x \in \mathbb{Z}_{25}$. Тогда $f(k) = f(k \cdot z_{10}) = kf(z_{10}) = kx\ \forall\ k \in \mathbb{Z}_{10}$. Значит, для задания гомоморфизма достаточно указать образ порождающего элемента z_{10}.

Порядок элемента z_{10} в $\mathbb{Z}_{10}$ равен 10. Тогда $ord\big(f(g)\big) \mid 10$. Докажем следующий факт:

Теорема. *Пусть $g \in G$. Тогда $ord\big(g^k\big) = \frac{ord\big(g\big)}{GCD(k,\ ord\big(g\big))}$, где GCD – НОД.*

Доказательство. Пусть $d = GCD(k,\ ord\big(g\big))$, $k = k_0 d$, $ord\big(g\big) = s_0 d, GCD(k_0,\ s_0) = d$. Тогда $\forall\ m \in \mathbb{Z}\ (g^k)^m = e \Leftrightarrow g^{km} = e \Leftrightarrow ord\big(g\big) \mid km \Leftrightarrow s_0 \mid k_0 m \Leftrightarrow s_0 \mid m$. Значит, $(g^k)^m = e \Leftrightarrow \frac{ord\big(g\big)}{GCD(k,\ ord\big(g\big))} \mid m$.

Следовательно, $ord\big(g^k\big) = \frac{ord\big(g\big)}{GCD(k,\ ord\big(g\big))}$. **Q.E.D.**

Покажем, что условие $ord\big(x\big) \mid 10$ является достаточным, чтобы отображение $f(k) = kx$ было определено корректно и являлось гомоморфизмом.

Пусть $k = m$, где $m \in \mathbb{Z}$, тогда $n \mid (k - m) \Rightarrow ord\big(x\big) \mid (k - m) \Rightarrow (k - m)x = 0 \Rightarrow f(k) = f(m)$. Значит, отображение определено корректно.

$f(k + m) = f([k + m]) = (k + m)x = kx + mx = f(k) + f(m)$. Значит, отображение – гомоморфизм.

Из этого факта следует, что $ord\big(x\big) = \frac{25}{GCD(25,\ x)}$, где $x \in \big\{0,\ 1,\ \ldots,\ 24\big\}$. Тогда, по сказанному выше, $\frac{25}{GCD(25,\ x)} \mid 10$. Следовательно, $\frac{25}{GCD(25,\ x)} = \big\{1,\ 2,\ 5,\ 10\big\}$. Но это означает, что $GCD(25,\ x) = \big\{25,\ 5\big\}$ (чётные значения дроби невозможны, так как 25 – нечётное). Получается 2 случая:

1. $GCD(25,\ x) = 25$. Тогда $x = 25$ по модулю 25, то есть $x = 0$.
2. $GCD(25,\ x) = 5$. Тогда 4 варианта: $x = \big\{5,\ 10,\ 15,\ 20\big\}$.

Таким образом, существует всего 5 гомоморфизмов из $\mathbb{Z}_{10}$ в $\mathbb{Z}_{25}$:

1. $f(g) \equiv 0$
2. $f(g) = 5 \cdot g$
3. $f(g) = 10 \cdot g$
4. $f(g) = 15 \cdot g$
5. $f(g) = 20 \cdot g$

Q.E.D.

2.2 Изоморфизм групп

Задача №3. *Рассмотрим группу $G = \big\{2^m \cdot 3^n \mid m,\ n \in \mathbb{Z}\big\}$ с операцией умножения. Докажите, что $G \simeq \mathbb{Z} \times \mathbb{Z}$.*

Доказательство. Стоит отметить, что группа $\mathbb{Z}$, как и $\mathbb{Z} \times \mathbb{Z}$, берётся с операцией сложения (иначе не для всех элементов существует обратный).

Построим отображение $f : G \to \mathbb{Z} \times \mathbb{Z} \mid 2^m \cdot 3^n \to (m,\ n)$ – пара чисел $m,\ n \in \mathbb{Z}$. Покажем, что оно является изоморфизмом. Для этого необходимо выполнение следующих условий:

1. $f(ab) = f(a) + f(b)\ \forall\ a,\ b \in G$

   Пусть $a = 2^{m_1} \cdot 3^{n_1}$, $b = 2^{m_2} \cdot 3^{n_2}$. Тогда $ab = 2^{m_1+m_2} \cdot 3^{n_1+n_2}$. Значит, $f(ab) = f(2^{m_1+m_2} \cdot 3^{n_1+n_2}) = (m_1 + m_2,\ n_1 + n_2) = (m_1,\ n_1) + (m_2,\ n_2) = f(2^{m_1} \cdot 3^{n_1}) + f(2^{m_2} \cdot 3^{n_2}) = f(a) + f(b)$.

2. $Ker\{f\} = \{e_G\}$

   e_G – нейтральный элемент в поле G. Покажем, что $e_G = 2^0 \cdot 3^0 = 1$: $(2^0 \cdot 3^0)(2^n \cdot 3^m) = (2^n \cdot 3^m)(2^0 \cdot 3^0) = 2^{0+m} \cdot 3^{0+n} = 2^n \cdot 3^m = g\ \forall\ g = 2^n \cdot 3^m \in G$.

   Следовательно: $f(2^0 \cdot 3^0) = (0,\ 0)$, а пара целых чисел $(0,\ 0)$ является нулём в $\mathbb{Z} \times \mathbb{Z}$. Значит, $Ker\{f\} = \{e_G\}$.

3. $Im\{f\} = \mathbb{Z} \times \mathbb{Z}$

   Поскольку $G = \{2^m \cdot 3^n \mid m,\ n \in \mathbb{Z}\}$, то соответственно $(m,\ n) \in \mathbb{Z} \times \mathbb{Z}$. А поскольку $f : 2^m \cdot 3^n \to (m,\ n)$, то $Im\{f\} = \{(m,\ n) \mid m,\ n \in \mathbb{Z}\} = \mathbb{Z} \times \mathbb{Z}$.

Таким образом, отображение $f : G \to \mathbb{Z} \times \mathbb{Z} \mid 2^m \cdot 3^n \to (m,\ n)$ является изоморфизмом. А если между двумя группами есть изоморфизм, то они изоморфны. Значит, $G \simeq Z \times \mathbb{Z}$.

Q.E.D.

3 Домашнее задание №3

3.1 Дополнить до базиса

Задача №1. *Пусть A – свободная абелева группа с базисом e_1, e_2, e_3. Дополните элемент $e'_1 = 6e_1 + 10e_2 - 15e_3$ до базиса группы A.*

Решение: Положим e'_1, e'_2, e'_3 – искомый базис. По предложению из лекции, элементы e'_1, e'_2, e'_3 образуют базис тогда и только тогда, когда

$$(e'_1,\, e'_2,\, e'_3) = (e_1,\, e_2,\, e_3) \cdot C$$

где C – матрица с определителем ± 1. В данном случае матрица C будет содержать столбцы с коэффициентами базисных элементов e'_1, e'_2, e'_3. Пусть $e'_2 = a_2e_1 + b_2e_2 + c_2e_3$, $e'_3 = a_3e_1 + b_3e_2 + c_3e_3$. Тогда:

$$C = \begin{pmatrix} 6 & a_2 & a_3 \\ 10 & b_2 & b_3 \\ -15 & c_2 & c_3 \end{pmatrix} \Rightarrow \begin{vmatrix} 6 & a_2 & a_3 \\ 10 & b_2 & b_3 \\ -15 & c_2 & c_3 \end{vmatrix} = \pm 1$$

Будем искать коэффициенты так, чтобы определитель был 1 (это корректно с точностью до перемены знаков коэффициентов). Произведём линейные (целочисленные) преобразования строк, чтобы получить взаимно простые коэффициенты в первом столбце:

$$\begin{vmatrix} 6 & a_2 & a_3 \\ 10 & b_2 & b_3 \\ -15 & c_2 & c_3 \end{vmatrix} = \begin{vmatrix} 6 & a_2 & a_3 \\ 4 & b_2 - a_2 & b_3 - a_3 \\ -3 & c_2 + 2a_2 & c_3 + 2a_3 \end{vmatrix}$$

Ясно, что, взяв $a_3 = 1$, $b_3 - a_3 = 0$, $c_3 + 2a_3 = 0$, мы получим матрицу с углом нулей. Тогда:

$$\begin{vmatrix} 6 & a_2 & 1 \\ 4 & b_2 - a_2 & 0 \\ -3 & c_2 + 2a_2 & 0 \end{vmatrix} = 1 \Longleftrightarrow \begin{vmatrix} 4 & b_2 - a_2 \\ -3 & c_2 + 2a_2 \end{vmatrix} = 1$$

Пусть $a_2 = 0$:

$$\begin{vmatrix} 4 & b_2 \\ -3 & c_2 \end{vmatrix} = 1 \Longleftrightarrow 4c_2 + 3b_2 = 1 \Longleftrightarrow c_2 = 1,\, b_2 = -1$$

$a_3 = 1$, $b_3 - a_3 = 0 \Rightarrow a_3 = 1$, $c_3 + 2a_3 = 0 \Rightarrow c_3 = -2$. Таким образом, мы получили:

$$\begin{vmatrix} 6 & 0 & 1 \\ 4 & -1 & 0 \\ -3 & 1 & 0 \end{vmatrix} = 1 \Longleftrightarrow \text{обратными преобразованиями} \Longleftrightarrow \begin{vmatrix} 6 & 0 & 1 \\ 10 & -1 & 1 \\ -15 & 1 & -2 \end{vmatrix} = 1$$

Таким образом, искомый базис группы A e'_1, e'_2, e'_3 равен: $e'_1 = 6e_1 + 10e_2 - 15e_3$, $e'_2 = -e_2 + e_3$, $e'_3 = e_1 + e_2 - 2e_3$.

Q.E.D.

3.2 Факторгруппу в сумму циклических

Задача №2. *Пусть A – свободная абелева группа с базисом e_1, e_2, e_3 и B – её подгруппа, порождаемая элементами $f_1 = 7e_1 - e_2 + 5e_3$, $f_2 = e_1 - 7e_2 + 3e_3$, $f_3 = 3e_1 + 3e_2 + e_3$. Разложите факторгруппу A/B в прямую сумму циклических групп.*

Решение. По *Теореме о согласованных базисах*, запишем матрицу базисных векторов B и будем работать по следующему алгоритму:

1. Линейными (целочисленными) преобразованиями строк и столбцов поместим в левый верхний угол НОД матричных элементов.

2. Сократим элементы в соответствующих строках и столбцах.

3. Повторяем 1 и 2 для главной матрицы меньшего размера. (Главная – стоящая на главной диагонали), пока не получим диагональную матрицу.

$$\begin{pmatrix}7 & -1 & 5\\ 1 & -7 & 3\\ 3 & 3 & 1\end{pmatrix} \Rightarrow \begin{pmatrix}1 & -7 & 3\\ 7 & -1 & 5\\ 3 & 3 & 1\end{pmatrix} \Rightarrow \begin{pmatrix}1 & -7 & 3\\ 0 & 48 & -16\\ 0 & 24 & -8\end{pmatrix} \Rightarrow \begin{pmatrix}1 & 0 & 0\\ 0 & 48 & -16\\ 0 & 24 & -8\end{pmatrix} \Rightarrow$$

$$\Rightarrow \begin{pmatrix}1 & 0 & 0\\ 0 & 48 & -16\\ 0 & -24 & 8\end{pmatrix} \Rightarrow \begin{pmatrix}1 & 0 & 0\\ 0 & -24 & 8\\ 0 & 48 & -16\end{pmatrix} \Rightarrow \begin{pmatrix}1 & 0 & 0\\ 0 & 8 & -24\\ 0 & -16 & 48\end{pmatrix} \Rightarrow \begin{pmatrix}1 & 0 & 0\\ 0 & 8 & -24\\ 0 & 0 & 0\end{pmatrix} \Rightarrow \begin{pmatrix}1 & 0 & 0\\ 0 & 8 & 0\\ 0 & 0 & 0\end{pmatrix}$$

Таким образом, мы получили, что при $A = \langle e_1,\, e_2,\, e_3\rangle$ подгруппа $B = \langle e_1,\, 8e_2\rangle$. Обозначим $0 = e_{\mathbb{Z}}$ - нейтральный элемент $\mathbb{Z}$. Но тогда:

$$A/B = \langle e_1\rangle/\langle e_1\rangle \oplus \langle e_2\rangle/\langle 8e_2\rangle \oplus \langle e_3\rangle/\langle e_{\mathbb{Z}}\rangle = 0 \oplus \langle e_2\rangle/\langle 8e_2\rangle \oplus \langle e_3\rangle = \mathbb{Z}_8 \oplus \mathbb{Z}$$

Таким образом, мы получили, что факторгруппа A/B разлагается в прямую сумму циклических групп $\mathbb{Z}$ и $\mathbb{Z}_8$:

$$A/B = \mathbb{Z} \oplus \mathbb{Z}_8$$

Q.E.D.

3.3 Изоморфная подгруппа

Задача №3. *Найдите в группе $\mathbb{Z}^2$ подгруппу H, для которой $\mathbb{Z}^2/H \simeq \mathbb{Z}_6 \times \mathbb{Z}_{10} \times \mathbb{Z}_{15}$.*

Решение:

Теорема. *Пусть $n = mk$, где $GCD(m,\, k) = 1$. Тогда $\mathbb{Z}_n \simeq \mathbb{Z}_m \times \mathbb{Z}_k$.*

Из этого следует:

$$\mathbb{Z}_6 \times \mathbb{Z}_{10} \times \mathbb{Z}_{15} \simeq \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_3 \times \mathbb{Z}_5 = (\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5) \times (\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5) = \mathbb{Z}_{30} \times \mathbb{Z}_{30}$$

Пусть $H = H_1 \times H_2$. Значит, по *теореме о факторизации по сомножителям*:

$$\mathbb{Z}^2/H \simeq \mathbb{Z}_6 \times \mathbb{Z}_{10} \times \mathbb{Z}_{15} \Leftrightarrow \mathbb{Z}^2/H \simeq \mathbb{Z}_{30} \times \mathbb{Z}_{30} \Leftrightarrow \mathbb{Z}/H_1 \times \mathbb{Z}/H_2 \simeq \mathbb{Z}_{30} \times \mathbb{Z}_{30}$$

Пусть $\mathbb{Z} \simeq \langle z_1\rangle, z_1 \in \mathbb{Z}$ и $\mathbb{Z} \simeq \langle z_2\rangle, z_2 \in \mathbb{Z}$, где z_1 и z_2 – некие порождающие элементы. Тогда возьмём $H_1 = \langle z_1^{30}\rangle$, $H_2 = \langle z_2^{30}\rangle \Longrightarrow H = H_1 \times H_2 = \langle z_1^{30}\rangle \times \langle z_2^{30}\rangle$.

Q.E.D.

4 Домашнее задание №4

4.1 Порядок смежного класса

Задача №1. *В факторгруппе свободной абелевой группы A с базисом e_1, e_2, e_3 по подгруппе B, порождённой элементами $2e_1+3e_2+4e_3$ и $4e_1-3e_2+2e_3$, найдите порядок смежного класса $(5e_1-6e_2+e_3)+B$.*

Решение: Пусть $ord\big[(5e_1-6e_2+e_3)+B\big]=n$. Тогда $\big[(5e_1-6e_2+e_3)+B\big]^n = n\cdot\big[(5e_1-6e_2+e_3)+B\big] = B \Rightarrow n\cdot(5e_1-6e_2+e_3)+B=B \Rightarrow n\cdot(5e_1-6e_2+e_3)\in B$ – ввиду того, что мы факторизуем по подгруппе B.

$B=\langle 2e_1+3e_2+4e_3,\, 4e_1-3e_2+2e_3\rangle \Rightarrow$
$n\cdot(5e_1-6e_2+e_3)=s\cdot(2e_1+3e_2+4e_3)+t\cdot(4e_1-3e_2+2e_3),\ s,\,t\in\mathbb{Z}.$

$n\cdot(5e_1-6e_2+e_3)=s\cdot(2e_1+3e_2+4e_3)+t\cdot(4e_1-3e_2+2e_3) \Longleftrightarrow 5ne_1-6ne_2+ne_3=2se_1+3se_2+4se_3+4te_1-3te_2+2te_3=(2s+4t)e_1+(3s-3t)e_2+(4s+2t)e_3 \Longrightarrow$ Решим СЛУ:

$$\begin{cases}5n=2s+4t\\-6n=3s-3t\\n=4s+2t\end{cases} \Longrightarrow \begin{pmatrix}5&-2&-4\\-6&-3&3\\1&-4&-2\end{pmatrix}\Rightarrow\begin{pmatrix}1&-4&-2\\-6&-3&3\\5&-2&-4\end{pmatrix}\Rightarrow\begin{pmatrix}1&-4&-2\\0&-27&-9\\0&18&6\end{pmatrix}\Rightarrow$$
$$\Rightarrow\begin{pmatrix}1&-4&-2\\0&3&1\\0&3&1\end{pmatrix}\Rightarrow\begin{pmatrix}1&-4&-2\\0&3&1\end{pmatrix}\Rightarrow\begin{pmatrix}1&2&0\\0&3&1\end{pmatrix}\Longrightarrow\begin{cases}n=-2s\\t=-3s\end{cases}$$

Поскольку $s\in\mathbb{Z}$, то $n=-2s$ – любое число, кратное 2 (замечу, что $n>0$, поэтому $s<0$ всегда). Порядок – наименьшее такое число, значит, наиеньшее возможное натуральное чётное число. Но тогда, при $s=-1\Rightarrow n=2 \Longrightarrow 2\cdot(5e_1-6e_2+e_3)=10e_1-12e_2+2e_3=-2e_1+12e_1-3e_2-9e_2-4e_3+6e_3=-1\cdot(2e_1+3e_2+4e_3)+3\cdot(4e_1-3e_2+2e_3)\in B$.

А это означает, что $ord\big[(5e_1-6e_2+e_3)+B\big]=2$.

Q.E.D.

4.2 Элементы различного порядка

Задача №2. *Сколько элементов порядков 2, 3, 4, 6 в группе $\mathbb{Z}_2\oplus\mathbb{Z}_3\oplus\mathbb{Z}_4$?*

Решение. Пусть $a\in\mathbb{Z}_2$, $b\in\mathbb{Z}_3$, $c\in\mathbb{Z}_4 \Longrightarrow (a,\,b,\,c)\in\mathbb{Z}_2\oplus\mathbb{Z}_3\oplus\mathbb{Z}_4$. По следствию из *Теоремы о разложении на сумму примарных групп*, $ord\big[(a,\,b,\,c)\big]=\text{НОК}\big[ord(a),\,ord(b),\,ord(c)\big]$.

- $ord=2$

  Так как порядок – 2, то НОК порядков равен 2, и порядки a, b, c не превосходят 2. Посчитаем, сколько в каждой из групп $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$ элементов порядка не выше 2: $\{0,1\}\in\mathbb{Z}_2$, $\{0\}\in\mathbb{Z}_3$, $\{0,\,2\}\in\mathbb{Z}_4$. Значит, всего элементов порядка не выше 2 в $\mathbb{Z}_2\oplus\mathbb{Z}_3\oplus\mathbb{Z}_4=2\cdot1\cdot2=4$. Но здесь также посчитаны элементы порядка 1, который всего один: (0, 0, 0). Тогда количеством элементов порядка 2 ровно будет разность количеств элементов порядка не выше 2 и порядка 1: $|ord\big[(a,\,b,\,c)\big]=2|=4-1=3$.

- $ord=3$

  Так как порядок – 3, то НОК порядков равен 3.Значит, элементов порядка 2 быть не должно точно. Посчитаем, сколько в каждой из групп $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$ элементов порядка не выше 3, но не равных 2: $\{0\}\in\mathbb{Z}_2$, $\{0,\,1,\,2\}\in\mathbb{Z}_3$, $\{0\}\in\mathbb{Z}_4$. Значит, всего элементов порядка не выше 3 в $\mathbb{Z}_2\oplus\mathbb{Z}_3\oplus\mathbb{Z}_4=1\cdot3\cdot1=3$. Но здесь также посчитаны элементы порядка 1, который всего один: (0, 0, 0). Тогда количеством элементов порядка 3 ровно будет разность количеств элементов порядка не выше 3, но не равных 2, и порядка 1: $|ord\big[(a,\,b,\,c)\big]=3|=3-1=2$.

- $ord=4$

  Так как порядок – 4, то НОК порядков равен 4. Значит, элементов порядка 3 быть не должно точно. Посчитаем, сколько в каждой из групп $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$ элементов порядка не выше 4, но не равных 3: $\{0,\,1\}\in\mathbb{Z}_2$, $\{0\}\in\mathbb{Z}_3$, $\{0,\,1,\,2,\,3\}\in\mathbb{Z}_4$. Значит, всего элементов порядка не выше 4, но не равных 3, в $\mathbb{Z}_2\oplus\mathbb{Z}_3\oplus\mathbb{Z}_4=2\cdot1\cdot4=8$. Но здесь также посчитаны элементы порядка не

выше 2, которых, как было посчитано ранее, 4. Тогда количеством элементов порядка 4 ровно будет разность количеств элементов порядка не выше 4, но не равных 3, и порядков не выше 2: $|ord\big[(a,\, b,\, c)\big] = 4| = 8 - 4 = 4$.

- $ord = 6$

  Так как порядок – 6, то НОК порядков равен 6. Значит, точно должны присутствовать элементы порядка 3 и 2, но не должно быть элементов порядка 4 (иначе общий порядок будет 12). Посчитаем, сколько в каждой из групп $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$ элементов порядка не выше 6. но не равных 4: $\{0,\, 1\} \in \mathbb{Z}_2$, $\{0, 1, 2\} \in \mathbb{Z}_3$, $\{0, 2\} \in \mathbb{Z}_4$. Значит, всего элементов порядка не выше 6 в $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4 = 2 \cdot 3 \cdot 2 = 12$. Но здесь также посчитаны элементы порядка не выше 2, которых, как было посчитано ранее, 4, и элементов порядка 3 ровно, коих 2. Тогда количеством элементов порядка 6 ровно будет разность количеств элементов порядка не выше 6 и суммы количеств элементов порядка не выше 2 и элементов порядка 3 ровно: $|ord\big[(a,\, b,\, c)\big] = 6| = 12 - (4 + 2) = 6$.

Q.E.D.

4.3 Подгруппы различного порядка

Задача №3. *Сколько подгрупп порядков* 5 *и* 10 *в нециклической абелевой группе порядка* 50*?*

Решение. Всего существуют 2 группы порядка 50 (с точностью до изоморфизма): $\mathbb{Z}_{50} = \mathbb{Z}_{25} \times \mathbb{Z}_2$ и $\mathbb{Z}_{10} \times \mathbb{Z}_5 = \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$. Первая нам не подходит, так как она – циклическая.

По *Теореме о разложении в сумму примарных циклических групп*, наша группа A, $ord\big[A\big] = 50$ изоморфна группе $\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \simeq \mathbb{Z}_5 \times \mathbb{Z}_{10}$. Для удобства будем рассматривать группу $\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$. Положим $\mathbb{Z}_2 = \langle a \rangle$, $a \in \mathbb{Z}_2$, $\mathbb{Z}_5 = \langle b \rangle = \langle c \rangle$, $b,\, c \in \mathbb{Z}_5$. Тогда $\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \simeq \langle a \rangle_2 \times \langle b \rangle_5 \times \langle c \rangle_5$.

Так как число 5 – простое, то каждый (ненулевой) элемент порядка 5 порождает подгруппу порядка 5. Однако, подгруппы не должны пересекаться, значит, у них не должно быть общих порождающих. Сначала, чтобы найти число подгрупп порядка 5, найдём количество элементов порядка 5. Посчитаем, сколько в каждой из групп $\mathbb{Z}_2$, $\mathbb{Z}_5$, $\mathbb{Z}_5$ элементов порядка не выше 5: $\{0\} \in \mathbb{Z}_2$, $\{0,\, 1,\, 2,\, 3,\, 4\} \in \mathbb{Z}_5$, $\{0,\, 1,\, 2,\, 3,\, 4\} \in \mathbb{Z}_5$. Значит, всего элементов порядка не выше 5 в $\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5 = 1 \cdot 5 \cdot 5 = 25$. Но здесь также посчитаны элементы порядка не выше 2, который один: $(0,\, 0,\, 0)$. Значит, элементов порядка 5 всего $25 - 1 = 24$. Как упоминалось ранее, подгруппы не должны иметь общих порождающих (то есть, группы попарно должны иметь различные порождающие). Поскольку в каждой подгруппе порядка 5 есть ровно 4 элемента порядка 5, то эти 4 элемента порождаются каким-то одним из них. Тогда всего различных подгрупп порядка 5 будет $24/4 = 6$ подгрупп.

Любая группа порядка 10 изоморфна прямому произведению групп порядков 2 и 5. Заметим, что в группе $\mathbb{Z}_2$ всего один элемент порядка 2 – 1, поэтому он точно будет присутствовать в любом порождающем как слагаемое из $\mathbb{Z}_2$. Но тогда все подгруппы порядка 10 будут иметь вид $\{1\} \times \langle b \rangle_5 \times \langle c \rangle_5$, $b,\, c \in \mathbb{Z}_5$. Тогда найдём теперь число элементов порядка 5 в группе $\mathbb{Z}_5 \times \mathbb{Z}_5$. Элементов порядка не выше 5: $\{0,\, 1,\, 2,\, 3,\, 4\} \in \mathbb{Z}_5$. Значит, всего элементов порядка не выше 5 в $\mathbb{Z}_5 \times \mathbb{Z}_5 = 5 \cdot 5 = 25$. Но здесь также посчитаны элементы порядка 1, который один: $(0,\, 0)$. Значит, элементов порядка 5 всего $25 - 1 = 24$. Как упоминалось ранее, подгруппы не должны иметь общих порождающих (то есть, группы попарно должны иметь различные порождающие). Поскольку в каждой подгруппе порядка 5 есть ровно 4 элемента порядка 5, то эти 4 элемента порождаются каким-то одним из них. Тогда всего различных подгрупп порядка 5 будет $24/4 = 6$ подгрупп. Но тогда всего подгрупп порядка 10 в $\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$: $1 \cdot 6 = 6$.

Q.E.D.

5 Домашнее задание №5

5.1 Орбиты и стабилизаторы

Задача №1. *Пусть G – группа всех диагональных матриц в $GL_3(\mathbb{R})$ и $X = \mathbb{R}^3$. Опишите все орбиты и все стабилизаторы для действия группы G на множестве X, заданного формулой $(g,\, x) \to g \cdot x$.*

Решение: Пусть $x \in X$. Орбита x $orb\big[x\big] = \{g \cdot x \mid g \in G\} \subseteq X$ – те элементы X, которые мы можем получить действием G на $x \in X$. Стабилизатор x $St\big[x\big] = \{g \in G \mid g \cdot x = x\}$ – те элементы G, которые не изменяют элемент x при действии.

Возьмём $g = \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}$, $x = \begin{pmatrix} k \\ l \\ m \end{pmatrix}$, $a,\, b,\, c,\, k,\, l,\, n \in \mathbb{R} \setminus \{0\}$.

Тогда $gx = \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix} \cdot \begin{pmatrix} k \\ l \\ m \end{pmatrix} = \begin{pmatrix} ak \\ bl \\ cm \end{pmatrix} = a \cdot \begin{pmatrix} k \\ 0 \\ 0 \end{pmatrix} + b \cdot \begin{pmatrix} 0 \\ l \\ 0 \end{pmatrix} + c \cdot \begin{pmatrix} 0 \\ 0 \\ m \end{pmatrix}$.

Под действием матриц из G каждая координата вектора x умножается на какое-то целое ненулевое число. Однако, если на месте исходной координаты k, l, m будет 0, то 0 останется на месте. Но тогда все орбиты определены положением нулевых координат в исходном векторе. Тогда все орбиты будут иметь вид:

$$\left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right\}, \left\{ \begin{pmatrix} ak \\ 0 \\ 0 \end{pmatrix} \right\}, \left\{ \begin{pmatrix} 0 \\ bl \\ 0 \end{pmatrix} \right\}, \left\{ \begin{pmatrix} 0 \\ 0 \\ cm \end{pmatrix} \right\},$$

$$\left\{ \begin{pmatrix} ak \\ bl \\ 0 \end{pmatrix} \right\}, \left\{ \begin{pmatrix} ak \\ 0 \\ cm \end{pmatrix} \right\}, \left\{ \begin{pmatrix} 0 \\ bl \\ cm \end{pmatrix} \right\}, \left\{ \begin{pmatrix} ak \\ bl \\ cm \end{pmatrix} \right\}.$$

где ak, bl, cm – какие-то ненулевые целые числа.

Если $g = \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}$ – стабилизатор, то $gx = \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix} \cdot \begin{pmatrix} k \\ l \\ m \end{pmatrix} = \begin{pmatrix} ak \\ bl \\ cm \end{pmatrix} = \begin{pmatrix} k \\ l \\ m \end{pmatrix} \Longrightarrow$

$$\begin{cases} ak = k \Rightarrow a = \begin{cases} \text{любое целое, кроме нуля, } k = 0 \\ 1,\ k \neq 0 \end{cases} \\ bl = l \Rightarrow b = \begin{cases} \text{любое целое, кроме нуля, } l = 0 \\ 1,\ l \neq 0 \end{cases} \\ cm = m \Rightarrow c = \begin{cases} \text{любое целое, кроме нуля, } m = 0 \\ 1,\ m \neq 0 \end{cases} \end{cases}$$

– множество таких g и будет составлять $St\big[x\big]$.

Q.E.D.

5.2 Теорема Кэли и группа подстановок

Задача №2. *Используя доказательство теоремы Кэли, реализуйте группу $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ как подгруппу в S_8.*

Решение. Согласно теореме Кэли, для нахождения изоморфизма групп запишем все элементы $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ в таблицу и рассмотрим действия каждого элемента на все остальные и себя. Таким образом мы сможем понять, куда каждый из элементов $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ переходит при действии. В итоге набор переходов даст нам по подстановке на каждый элемент.

Элементы	(0, 0)	(0, 1)	(0, 2)	(0, 3)	(1, 0)	(1, 1)	(1, 2)	(1, 3)
(0, 0)	(0, 0)	(0, 1)	(0, 2)	(0, 3)	(1, 0)	(1, 1)	(1, 2)	(1, 3)
(0, 1)	(0, 1)	(0, 2)	(0, 3)	(0, 0)	(1, 1)	(1, 2)	(1, 3)	(1, 0)
(0, 2)	(0, 2)	(0, 3)	(0, 0)	(0, 1)	(1, 2)	(1, 3)	(1, 0)	(1, 1)
(0, 3)	(0, 3)	(0, 0)	(0, 1)	(0, 2)	(1, 3)	(1, 0)	(1, 1)	(1, 2)
(1, 0)	(1, 0)	(1, 1)	(1, 2)	(1, 3)	(0, 0)	(0, 1)	(0, 2)	(0, 3)
(1, 1)	(1, 1)	(1, 2)	(1, 3)	(1, 0)	(0, 1)	(0, 2)	(0, 3)	(0, 0)
(1, 2)	(1, 2)	(1, 3)	(1, 0)	(1, 1)	(0, 2)	(0, 3)	(0, 0)	(0, 1)
(1, 3)	(1, 3)	(1, 0)	(1, 1)	(1, 2)	(0, 3)	(0, 0)	(0, 1)	(0, 2)

На пересечении i-й строки и j-го столбца находится элемент, полученный в результате действия элемента i-й строки на j-й элемент по столбцам. Таким образом, мы можем записать все 8 подстановок, отражающих действия элементами из $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ на все остальные элементы:

- $(0,\,0) \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix} = s_1$
- $(0,\,1) \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 1 & 6 & 7 & 8 & 5 \end{pmatrix} = s_2$
- $(0,\,2) \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 \end{pmatrix} = s_3$
- $(0,\,3) \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 2 & 3 & 8 & 5 & 6 & 7 \end{pmatrix} = s_4$
- $(1,\,0) \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \end{pmatrix} = s_5$
- $(1,\,1) \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 7 & 8 & 5 & 2 & 3 & 4 & 1 \end{pmatrix} = s_6$
- $(1,\,2) \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 8 & 5 & 6 & 3 & 4 & 1 & 2 \end{pmatrix} = s_7$
- $(1,\,3) \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 5 & 6 & 7 & 4 & 1 & 2 & 3 \end{pmatrix} = s_8$

По следствию из доказательства теоремы Кэли, эти элементы-подстановки образуют подгруппу в S_8 (ввиду биективного отображения). Выполнение необходимых свойств проверяется напрямую из таблицы. Таким образом, мы реализовали группу $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ как подгруппу $S = \{s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8\} \subset S_8$.

Q.E.D.

5.3 Стабилизатор для сопряжений

Задача №3. *Для действия группы S_4 на себе сопряжениями найдите стабилизатор подстановки* $(1,\,2,\,3,\,4)$.

Решение (Ксения Закирова). Пусть $\sigma = (1,\,2,\,3,\,4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \in S_4$ – подстановка из S_4, циклически переставляющая компоненты.

Стабилизатор элемента σ есть множество $St\big[\sigma\big] = \{s \in S_4 \mid s \cdot \sigma \cdot s^{-1} = \sigma\}$ – те элементы S_4, которые не изменяют элемент σ при действии сопряжением. Стоит отметить, что

$$s \cdot \sigma \cdot s^{-1} = \sigma \iff s \cdot \sigma = \sigma \cdot s$$

. Пусть $s \in St\big[\sigma\big]$. Посмотрим, как действует сопряжением данная подстановка на компонетнах подстановки из S_4, то есть, на элементах $i \in \{1,\,2,\,3,\,4\}$:

- $i = 1 \Rightarrow s(\sigma(1)) = \sigma(s(1)) \Leftrightarrow s(2) = \sigma(s(1))$ – в силу вышеуказанного свойства
- $i = 2 \Rightarrow s(\sigma(2)) = \sigma(s(2)) \Rightarrow s(3) = \sigma(s(2))$
- $i = 3 \Rightarrow s(\sigma(3)) = \sigma(s(3)) \Rightarrow s(4) = \sigma(s(3))$
- $i = 4 \Rightarrow s(\sigma(4)) = \sigma(s(4)) \Rightarrow s(1) = \sigma(s(4))$

Из полученных результатов можно сделать вывод, что любой элемент стабилизатора будет определяться образом первой компоненты подстановки при действии. Тогда достаточно рассмотреть все возможные образы отображения $s(1)$

1. $s(1) = 1 \Rightarrow$
   $s(2) = \sigma(s(1)) = \sigma(1) = 2$
   $s(3) = \sigma(s(2)) = \sigma(2) = 3$
   $s(4) = \sigma(s(3)) = \sigma(3) = 4$
   Получается, что $s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = id$
2. $s(1) = 2 \Rightarrow$
   $s(2) = \sigma(s(1)) = \sigma(2) = 3$
   $s(3) = \sigma(s(2)) = \sigma(3) = 4$
   $s(4) = \sigma(s(3)) = \sigma(4) = 1$
   Получается, что $s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$
3. $s(1) = 3 \Rightarrow$
   $s(2) = \sigma(s(1)) = \sigma(3) = 4$
   $s(3) = \sigma(s(2)) = \sigma(4) = 1$
   $s(4) = \sigma(s(3)) = \sigma(1) = 2$
   Получается, что $s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$
4. $s(1) = 4 \Rightarrow$
   $s(2) = \sigma(s(1)) = \sigma(1) = 1$
   $s(3) = \sigma(s(2)) = \sigma(1) = 2$
   $s(4) = \sigma(s(3)) = \sigma(2) = 3$
   Получается, что $s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$

Итак, $St\big[\sigma\big] = \{id, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}\}$.

Q.E.D.

6 Домашнее задание №6

6.1 Размерность алгебры – первое решение (без использования ТГК)

Задача №3. *Найдите размерность* $\mathbb{R}$*-алгебры* $\mathbb{R}[x]/(x^3 - x + 1)$.

Решение (Анастасия Иовлева). Пусть $f = x^3 - x + 1$. Докажем, что $\mathbb{R}[x]/f \simeq \mathbb{R}[x]_{n\leqslant 2}$, где $\mathbb{R}[x]_{n\leqslant 2}$ кольцо с обычным сложением и умножением по модулю f (ассоциативность умножения будет выполняться в силу свойств модульной арифметики).

Рассмотрим идеал $I = (f)$ и два класса смежности $g_1 + I$ и $g_2 + I$, где $g_1, g_2 \in \mathbb{R}[x]$. Если существуют такие $r_1, r_2 \in \mathbb{R}[x]$, что $g_1 + r_1 f = g_2 + r_2 f$ (то есть данные классы совпадают), то будет выполнятся следующее:

$$\begin{gathered} g_1 + r_1 f = g_2 + r_2 f \\ g_2 - g_1 = f(r_1 - r_2) \\ (g_2 - g_1) \equiv 0 \mod f \end{gathered}$$

Аналогично, если $g_1 + I$ и $g_2 + I$ не пересекаются, то $g_2 - g_1 \equiv a \mod f$, где $a \neq 0$.

Теперь зафиксируем $g_1 = 0$. Тогда равенство выше преобразуется в $g_2 - g_1 = g_2 \equiv a \mod f$. Следовательно, все различные смежные классы можно представить в виде $a + I$, где a — какой-то остаток при делении на f, то есть $a \in \mathbb{R}[x]_{n\leqslant 2}$. Причем для любого такого a существует смежный класс $a + I$.

Очевидным образом можно ввести гомоморфизм колец $\varphi : (a+I) \mapsto a$ с обычной операцией сложения и операцией умножения по модулю f; то, что φ является биекцией, следует из предыдущего абзаца. Следовательно, φ это изоморфизм и $\mathbb{R}[x]/f \simeq \mathbb{R}[x]_{n\leqslant 2}$, что мы и хотели показать.

Итого, $\mathbb{R}[x]/f \simeq \mathbb{R}[x]_{n\leqslant 2}$. Причем в $\mathbb{R}[x]_{n\leqslant 2}$ мы знаем базис $(1, x, x^2)$. Следовательно, $\dim \mathbb{R}[x]/f = 3$.

Q.E.D.

6.2 Размерность алгебры – второе решение (с использованием ТГК)

Задача №3. *Найдите размерность* $\mathbb{R}$*-алгебры* $\mathbb{R}[x]/(x^3 - x + 1)$.

Решение (я). В условии нам дано факторкольцо кольца $\mathbb{R}[x]$ по идеалу $x^3 - x + 1$. Воспользуемся *Теоремой о гомоморфизме колец*: элементами факторкольца $\mathbb{R}[x]/(x^3 - x + 1)$ будут остатки от деления многочленов из $\mathbb{R}[x]$ на $x^3 - x + 1$ (так как $x^3 - x + 1$ есть ядро некоего гомоморфизма). Заметим, что $\forall\ g \in \mathbb{R}[x] \Rightarrow g = Q(x) \cdot (x^3 - x + 1) + P(x)$, где $Q(x)$ и $P(x)$ – некоторые многочлены. Но тогда $\mathbb{R}[x]/(x^3 - x + 1) \simeq \{P(x)\}$ (кольцо данных многочленов с операцией умножения по модулю данного порождающего идеал элемента $x^3 - x + 1$), так как все элементы, кратные $(x^3 - x + 1)$, в факторкольце переходят в 0.

Рассмотрим многочлен $g(x) = ax^3 + bx^2 + cx + d$, и выделим из него $f(x)$: $g(x) = a(x^3 - x + 1) + bx^2 + (c + a)x + (d - a)$. Но тогда $g(k) = bx^2 + (c + a)z + (d - a)$ – многочлен не выше второй степени.

Проведём рассуждение в общем виде. Пусть $g(x)$ – многочлен степени k. Тогда при делении g на f: $g/f = h$, r– остаток. Но $\deg g = k,\ \deg f = 3 \Rightarrow \deg r < 3$. Тогда $\deg P(x) < 3 \Leftrightarrow P(x) = ax^2 + bx + c$, a, b, $c \in \mathbb{R}$.

$\mathbb{R}[x]/(x^3 - x + 1) \simeq \{P(x)\} \Leftrightarrow \mathbb{R}[x]/(x^3 - x + 1) \simeq \{ax^2 + bx + c\}$. Поскольку $\mathbb{R}[x]/(x^3 - x + 1)$ – алгебра, то можно рассмотреть данное факторкольцо как векторное пространство и взять в нём базис. $\mathbb{R}[x]/(x^3 - x + 1) \simeq \{ax^2 + bx + c\}$, следовательно, возьмём стандартный базис в $\mathbb{R}[x]_{\leq 2}$: 1, x, x^2 – любой многочлен $P(x) = ax^2 + bx + c$ представим в виде линейной комбинации базисных элементов, которых 3 штуки.

По определению, размерность векторного пространства есть число элементов в базисе оного. Но тогда размерность $\mathbb{R}$-алгебры $\mathbb{R}[x]/(x^3 - x + 1)$ равна 3.

Q.E.D.

6.3 Изоморфизм колец

Задача №4. *При помощи теоремы о гомоморфизме для колец установите изоморфизм* $\mathbb{Q}[x]/(x^2 - x) \simeq \mathbb{Q} \oplus \mathbb{Q}$*, где* $\mathbb{Q} \oplus \mathbb{Q} = \{(q_1,\ q_2) \mid q_1,\ q_2 \in \mathbb{Q}\}$ *– кольцо с покомпонентными операциями сложения и умножения.*

Решение. $\mathbb{Q}[x]/(x^2-x)$ – факторкольцо кольца $\mathbb{Q}[x]$ по идеалу $f(x) = (x^2-x)$. Элементами данного факторкольца (как следствие из полученных в предыдущей задаче выводов) будут остатки от деления многочленов из $\mathbb{Q}[x]$ на $f(x)$, а это все многочлены степени не выше первой, то есть: $\forall\ g \in \mathbb{Q}[x] \Rightarrow g = S(x)\cdot(x^2-x)+P(x)$, где $S(x)$ и $P(x)$ – некоторые многочлены. Но тогда $\mathbb{Q}[x]/(x^2-x) \simeq \{P(x)\}$ (кольцо данных многочленов с операцией умножения по модулю данного порождающего идеал элемента x^2-x), так как все элементы, кратные (x^2-x), в факторкольце переходят в 0, причём $P(x) = ax+b$, $a,\ b \in \mathbb{Q}$. Значит, $\mathbb{Q}[x]/(x^2-x) \simeq \{ax+b\}$.

Зададим отображение $\varphi : \mathbb{Q}[x]/(x^2-x) \to \mathbb{Q}\oplus\mathbb{Q}$, где $\mathbb{Q}\oplus\mathbb{Q} = \{(q_1,\ q_2) \mid q_1,\ q_2 \in \mathbb{Q}\}$, следующим образом: $\forall\ ax+b \in \mathbb{Q}[x]/(x^2-x),\ a,\ b \in \mathbb{Q} \Longrightarrow ax+b \to \big(a+b,\ b\big)$ – так как каждый элемент факторкольца есть многочлен степени не выше первой, то в нём не более двух компонент. Положим, что многочлены нулевой степени есть многочлены первой степени с нулевым коэффициентом при x. Тогда будем сопоставлять такому многочлену из факторкольца $f(x) = ax+b \in \mathbb{Q}[x]/(x^2-x)$ пару в $\mathbb{Q}\oplus\mathbb{Q}$, являющуюся упорядоченной парой из суммы коэффициентов и свободного члена данного многочлена $f(x)$.

Покажем, что оно является изоморфизмом. Для этого необходимо выполнение следующих условий:

1. $\varphi\big(g+h\big) = \varphi\big(g\big) + \varphi\big(h\big)\ \forall\ g,\ h \in \mathbb{Q}[x]/(x^2-x)$

   Пусть $g = ax+b,\ h = cx+d,\ g,\ h \in \mathbb{Q}[x]/(x^2-x)$. Тогда $\varphi\big(g+h\big) = \varphi\big(ax+b+cx+d\big) = \varphi\big((a+c)x+(b+d)\big) = \big((a+c)+(b+d),\ b+d\big) = \big((a+b)+(c+d),\ b+d\big) = \big(a+b,\ b\big)+\big(c+d,\ d\big) = \varphi\big(ax+b\big)+\varphi\big(cx+d\big) = \varphi\big(g\big)+\varphi\big(h\big)$

2. $\varphi\big(g\cdot h\big) = \varphi\big(g\big)\cdot\varphi\big(h\big)\ \forall\ g,\ h \in \mathbb{Q}[x]/(x^2-x)$

   Пусть $g = ax+b,\ h = cx+d,\ g,\ h \in \mathbb{Q}[x]/(x^2-x)$ (отметим, что умножение происходит по модулю (x^2-x)). Тогда $\varphi\big(g\cdot h\big) = \varphi\big((ax+b)\cdot(cx+d)\big) = \varphi\big((acx^2+(ad+bc)x+bd)\ mod\ (x^2-x)\big) = \varphi\big((ac+ad+bc)x+bd\big) = \big(ac+bc+ad+bd,\ bd\big) = \big((a+b)(c+d),\ bd\big) = \big(a+b,\ b\big)\cdot\big(c+d,\ d\big) = \varphi\big(ax+b\big)\cdot\varphi\big(cx+d\big) = \varphi\big(g\big)\cdot\varphi\big(h\big)$

3. $Ker\big\{\varphi\big\} = \{e_{\mathbb{Q}[x]/f}\}$

   Пусть $h = ax+b \in Ker\big\{\varphi\big\}$ – какой-то элемент из ядра. Тогда, по определению ядра, $\varphi\big(ax+b\big) = e_{\mathbb{Q}\oplus\mathbb{Q}} = \big(0,\ 0\big)$. Но:

   $$\varphi\big(ax+b\big) = \big(a+b,\ b\big) = \big(0,\ 0\big) \Leftrightarrow \begin{cases} a+b=0 \\ b=0 \end{cases} \Leftrightarrow a=b=0 \Leftrightarrow h=0=e_{\mathbb{Q}[x]/f}.$$

   То есть, $Ker\big\{\varphi\big\} = \{e_{\mathbb{Q}[x]/f}\}$.

4. $Im\big\{\varphi\big\} = \mathbb{Q}\oplus\mathbb{Q}$

   Пусть $q = \big(c,\ d\big) \in \mathbb{Q}\oplus\mathbb{Q}$ – какой-то элемент из множества $\mathbb{Q}\oplus\mathbb{Q}$. Тогда возьмём элемент g из $\mathbb{Q}[x]/(x^2-x)$, такой, что $g = (c-d)x+d$ – существует такой элемент в факторкольце. Но тогда, по построению отображения, $\varphi\big((c-d)x+d\big) = \big(c,\ d\big) = q$. Следовательно, для любого элемента из $\mathbb{Q}\oplus\mathbb{Q}$ существует прообраз из $\mathbb{Q}[x]/(x^2-x)$ для отображения φ, то есть, оно сюръективно. А это в свою очередь означает, что $Im\big\{\varphi\big\} = \mathbb{Q}\oplus\mathbb{Q}$.

Таким образом, отображение $\varphi : \mathbb{Q}[x]/(x^2-x) \to \mathbb{Q}\oplus\mathbb{Q}$, где $\mathbb{Q}\oplus\mathbb{Q}\{(q_1,\ q_2) \mid q_1,\ q_2 \in \mathbb{Q}\}$, такое, что: $\forall\ ax+b \in \mathbb{Q}[x]/(x^2-x),\ a,\ b \in \mathbb{Q} \Longrightarrow ax+b \to \big(a+b,\ b\big)$ является изоморфизмом. То есть, мы установили изоморфизм $\mathbb{Q}[x]/(x^2-x) \simeq \mathbb{Q}\oplus\mathbb{Q}$, что и было необходимо.

Q.E.D.

7 Домашнее задание №7

7.1 НОД многочленов

Задача №1. *Найдите наибольший общий делитель многочленов*

$$f(x) = x^5 + x^4 - x^3 - 2x - 1 \text{ и } g(x) = 3x^4 + 2x^3 + x^2 + 2x - 2$$

а также его линейное выражение через $f(x)$ *и* $g(x)$.

Решение. Сначала выделим общие множители:

$$f(x) = x^5 + x^4 - x^3 - 2x - 1 = (x^2+1)(x^3 + x^2 - 2x - 1)$$
$$g(x) = 3x^4 + 2x^3 + x^2 + 2x - 2 = (x^2+1)(3x^2 + 2x - 2)$$

Множитель (x^2+1) точно входит в НОД. Искать НОД оставшихся множителей будем по алгоритму Евклида:

$$\begin{array}{r|l} x^3 + x^2 - 2x - 1 & 3x^2 + 2x - 2 \\ \cline{2-2} x^3 + \frac{2}{3}x^2 - \frac{2}{3}x & \frac{1}{3}x + \frac{1}{9} \\ \cline{1-1} \frac{1}{3}x^2 - \frac{4}{3}x - 1 & \\ \frac{1}{3}x^2 + \frac{2}{9}x - \frac{2}{9} & \\ \cline{1-1} -\frac{14}{9}x - \frac{7}{9} & \end{array}$$

$$\begin{array}{r|l} 3x^2 + 2x - 2 & -\frac{14}{9}x - \frac{7}{9} \\ \cline{2-2} 3x^2 + \frac{3}{2}x & -\frac{27}{14}x - \frac{9}{28} \\ \cline{1-1} \frac{1}{2}x - 2 & \\ \frac{1}{2}x + \frac{1}{4} & \\ \cline{1-1} \frac{-9}{4} & \end{array}$$

$$-\frac{14}{9}x - \frac{7}{9} = (\frac{56}{81}x + \frac{28}{81}) \cdot \frac{-9}{4} + 0$$

Значит, НОД$(x^3+x^2-2x-1, 3x^2+2x-2) = \frac{-9}{4}$. Но тогда НОД$\big(x^5+x^4-x^3-2x-1, 3x^4+2x^3+x^2+2x-2\big) = \frac{-9}{4} \cdot (x^2+1)$.

Теперь найдём его линейное выражение через $f(x)$ и $g(x)$ обратным ходом алгоритма Евклида:

$$\frac{-9}{4} = (3x^2 + 2x - 2) - \big(-\frac{27}{14}x - \frac{9}{28}\big) \cdot \big(-\frac{14}{9}x - \frac{7}{9}\big) =$$
$$= (3x^2 + 2x - 2) - \big(-\frac{27}{14}x - \frac{9}{28}\big) \cdot \big((x^3 + x^2 - 2x - 1) - (3x^2 + 2x - 2) \cdot (\frac{1}{3}x + \frac{1}{9})\big) =$$
$$= (3x^2 + 2x - 2) \cdot \big(1 + (\frac{1}{3}x + \frac{1}{9}) \cdot (-\frac{27}{14}x - \frac{9}{28})\big) - (-\frac{27}{14}x - \frac{9}{28}) \cdot (x^3 + x^2 - 2x - 1) \Longrightarrow$$
$$\Longrightarrow \Big\{\text{домножая обе части на } (x^2+1)\Big\} \Longrightarrow$$
$$\Longrightarrow \frac{-9}{4} \cdot (x^2+1) = g(x) \cdot \big(1 + (\frac{1}{3}x + \frac{1}{9}) \cdot (-\frac{27}{14}x - \frac{9}{28})\big) - f(x) \cdot (-\frac{27}{14}x - \frac{9}{28}) = \text{НОД}\big(f(x),\, g(x)\big)$$

Q.E.D.

7.2 Произведение неприводимых

Задача №3. *Разложите многочлен* $x^6 + 1$ *в произведение неприводимых над полем* ΓR.

Решение. • $\Gamma : 6, \ : .\text{R: z} = \text{a} + \text{ib} \in \acute{}a,\, b \in \mathbb{R}$. Тогда $(x-z)(x-\overline{z}) = x^2 - (ax+ibx) - (ax-ibx) + (a^2+b^2) = x^2 - 2ax + (a^2+b^2) = x^2 - 2Re(z) + |z|^2$ – получили многочлен над $\mathbb{R}$.

Тогда необходимо разложить многочлен в произведение квадратных двучленов $x^2 + bx + c = (x - z)(x - \overline{z})$. Сгруппируем корни над Γ : $\begin{cases} \begin{cases} e^{i\frac{\pi}{6}} \\ e^{-i\frac{\pi}{6}} \end{cases} \Rightarrow f_1(x) = x^2 + \sqrt{3}x + 1 \\ \begin{cases} e^{i\frac{\pi}{2}} \\ e^{-i\frac{\pi}{2}} \end{cases} \Rightarrow f_2(x) = x^2 + 1 \\ \begin{cases} e^{i(\frac{\pi}{6}+\frac{2\pi}{3})} \\ e^{i(\frac{\pi}{6}-\frac{2\pi}{3})} \end{cases} \Rightarrow f_3(x) = x^2 - \sqrt{3}x + 1 \end{cases} \Longrightarrow$

$$x^6 + 1 = (x^2 + \sqrt{3}x + 1)(x^2 + 1)(x^2 - \sqrt{3}x + 1)$$

Q.E.D.

7.3 Неприводимые многочлены

Задача №4. *Перечислите все неприводимые многочлены над полем $\mathbb{Z}_3$ со старшим коэффициентом 1, у которых степень не выше 2, и найдите количество таких многочленов степени 3.*

- *Решение.* Ненулевой необратимый многочлен называется неприводимым, если его нельзя представить в виде произведения необратимых многочленов над тем же полем. (На семинаре также доказывалось, что многочлен является неприводимым тогда и только тогда, когда он не имеет корней из данного поля.) Рассмотрим все степени многочленов над $\mathbb{Z}_3$ и отыщем неприводимые многочлены:

  - $deg = 0$

    Многочлены нулевой степени над $\mathbb{Z}_3$ – это константы. Заметим, что для любого элемента из $\mathbb{Z}_3$ многочлен-константа будет неприводимым по определению: $f_1(x) = 1$ является неприводимым и подходит ($f_0(x) = 0$ нельзя – многочлен должен быть ненулевым, $f_2(x) = 2$ нельзя – старший коэффициент 2).

  - $deg = 1$

    Рассмотрим многочлены $f_0(x) = x$, $f_1(x) = x + 1$ и $f_2(x) = x + 2$ – они являются неприводимыми над $\mathbb{Z}_3$ по определению. Заметим, что многочлены $f_1'(x) = x - 1$, $f_2'(x) = x - 2$ по модулю 3 совпадают соответственно с f_2 и f_1, значит, они уже перечислены.

  - $deg = 2$

    Рассмотрим все многочлены и покажем, какие являются неприводимыми, а какие нет:

    $f_0(x) = x^2 = x \cdot x$ – приводим. $f_1(x) = x^2 + 1 \simeq x^2 - 2$ – неприводим. $f_2(x) = x^2 - 1 \simeq x^2 + 2 = (x-1)\cdot(x-1) \simeq (x+2)\cdot(x-1) = x^2+x-2 \simeq (x+2)\cdot(x+2) = x^2+x+1 \simeq x^2-2x-2 \simeq x^2-2x+1$ – приводим. $f_3(x) = x^2 + x \simeq x^2 - 2x = (x+1)\cdot x$ – приводим. $f_4(x) = x^2 + 2x \simeq x^2 - x = (x+2)\cdot x$ – приводим.$f_5(x) = x^2 + 2x + 1 = (x+1)\cdot(x+1) \simeq (x-2)\cdot(x+1) = x^2 - x - 2 \simeq x^2 + 2x - 2 \simeq x^2 - x + 1 = (x-2)\cdot(x-2)$ – приводим. $f_6(x) = x^2 + x - 1 \simeq x^2 - 2x - 1 \simeq x^2 - 2x + 2 \simeq x^2 + x + 2$ – неприводим. $f_7(x) = x^2 + 2x + 2 \simeq x^2 - x + 2 \simeq x^2 - x - 1 \simeq x^2 + 2x - 1$ – неприводим.

    Значит, неприводимыми являются только многочлены $f_1(x) = x^2 + 1$, $f_6(x) = x^2 + x + 2$ и $f_7(x) = x^2 + 2x + 2$.

  - $deg = 3$

    Необходимо посчитать количество таковых. Для этого мы посчитаем количество вообще всех возможных многочленов степени 3 над $\mathbb{Z}_3$, а затем вычтем количество всех возможных многочленов третьей степени, являющихся произведением неприводимых многочленов меньших степеней (3 первой степени или 1 первой и 1 второй. Отрицательные коэффициенты будем опускать в силу аналогичного представления положительными.

    Всего многочленов: $1((x^3)) \cdot 3((x^2)) \cdot 3((x)) \cdot 3((1)) = 27$.

    Многочленов третьей степени, являющихся произведениями приводимых:

    Посчитаем формулой включений-исключений: приводимые многочлены раскладываются на неприводимые множители, являющиеся произведением чего-то на x, $x + 1$, $x + 2$, имеют своим корнем

соответственно 0, 2, 1. Заметим, что многочлен степени 2 и выше приводим тогда и только тогда, когда у него есть корень из данного поля (доказано на семинаре). Значит, чтобы найти общее число таких многочленов, нужно посчитать количество многочленов, имеющих своим корнем одно значение из $\mathbb{Z}_3$ (равносильно произведению вида $(x+k)\cdot(x^2+mx+l)$, $k, m, l \in \mathbb{Z}_3$), имеющих своим корнем какие-то два значения из $\mathbb{Z}_3$ (равносильно произведению вида $(x+k)^2\cdot(x+m)$, $k, m \in \mathbb{Z}_3$), и имеющих своим корнем сразу все значения (такой только один: $x(x+1)(x+2)$).

По формуле включений-исключений: количество приводимых многочленов степени $3 = 9 + 9 + 9\ \{(x+k)(3((x))\cdot 3((1))\} - 3 - 3 - 3\ \{(x+k)^2(3((1))\} + 1\ \{x(x+1)(x+2)\} = 19$ многочленов. Но тогда всего неприводимых многочленов третьей степени над $\mathbb{Z}_3$ будет $27 - 19 = 8$ штук.

Q.E.D.

8 Домашнее задание №8

8.1 Симметрический многочлен

Задача №1. *Докажите, что многочлен*

$$f(x_1,\, x_2,\, x_3,\, x_4) = (x_1 + x_2 - x_3 - x_4)(x_1 - x_2 + x_3 - x_4)(x_1 - x_2 - x_3 + x_4)$$

является симметрическим, и выразите его через элементарные симметрические многочлены.

Решение. Легко увидеть, что:

$$f = \big((x_1 + x_2) - (x_3 + x_4)\big)\big((x_1 + x_3) - (x_2 + x_4)\big)\big((x_1 + x_4) - (x_2 + x_3)\big)$$

Заметим, что любая перестановка двух элементов (элементарная транспозиция) просто меняет какие-то две большие скобки местами, но при этом само выражение остаётся неизменным. Но тогда, поскольку любая перестановка раскладывается в произведение элементарных транспозиций, то многочлен не изменяется при любой перестановке переменных. Тогда он симметрический по определению.

Первые 4 элементарных симметрических многочлена:

1. $\sigma_1 = x_1 + x_2 + x_3 + x_4$
2. $\sigma_2 = x_1x_2 + x_2x_3 + x_1x_3 + x_1x_4 + x_2x_4 + x_3x_4$
3. $\sigma_3 = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4$
4. $\sigma_4 = x_1x_2x_3x_4$

Теперь выразим его через элементарные симметрические. Для этого отыщем старший член многочлена. Из лекций известно, что старший член произведения является произведением старших членов сомножителей. Обозначим как L_0 – старший член всего многочлена, а L_i – старший член i-й скобки. Тогда:

$$L = L_1 \cdot L_2 \cdot L_3 = x_1 \cdot x_1 \cdot x_1 = x_1^3$$

Поскольку $L = x_1^3$, и представим как степень только одной из переменных, то $x_1^3 \simeq \sigma_1^3$ (значок $\simeq$ используется для обозначения соответствия данного слагаемого указанному симметрическому многочлену в следствие принадлежности разложению оного в сумму слагаемых).

Слагаемые в оставшейся части также имеют свои старшие члены. Однако, поскольку L_0 – старший для всего f, то они должны быть меньше его в лексикографическом порядке. Лемма из лекций гласит, что если $ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ – старший член какого-то многочлена, то степени переменных в нём должны невозрастать: $k_1 \geqslant k_2 \geqslant \dots \geqslant k_n$. Если мы будем повторять алгоритм выражения исходного многочлена через элементарные симметрические, то будут возникать многочлены со старшими членами меньше старшего члена исходного многочлена. Значит, следующие старшие члены должны быть строго меньше предыдущего полученного старшего члена. То есть, мы тем самым будем понижать степень той переменной в представлении последнего полученного старшего члена, которую возможно понизить и при этом останутся нетронутыми все предыдущие степени.

Получается, что следующий по старшинству старший член в оставшейся части многочлена будет $L_1 = x_1^2x_2$. $x_1^2x_2$ представим как произведение $x_1 \simeq \sigma_1$ на $x_1x_2 \simeq \sigma_2$, откуда $L_1 = \sigma_1\sigma_2$. Действуя по тому же алгоритму и применяя рассуждение выше, мы получаем ещё один старший член оставшейся части $L_2 = x_1x_2x_3$ – сразу же видно, что это первое слагаемое из σ_3, откуда $L_2 \simeq \sigma_3$.

Представим теперь наш симметрический многочлен через симметрические с какими-то пока что неопределёнными коэффициентами. Стоит отметить, что коэффициент при σ_1^3 равен 1, так как коэффициент при старшем члене многочлена f равен 1.

$$f(x_1,\, x_2,\, x_3,\, x_4) = \sigma_1^3 + \alpha\sigma_1\sigma_2 + \beta\sigma_3$$

Теперь будем подставлять различные значения переменных x_1, x_2, x_3, x_4 и наблюдать за изменением значений симметрических слагаемых и самого многочлена f.

x_1	x_2	x_3	x_4	σ_1^3	$\sigma_1\sigma_2$	σ_3	f
1	1	0	0	8	2	0	$0 = \sigma_1^3 + \alpha\sigma_1\sigma_2$
1	1	1	0	27	9	1	$-1 = \sigma_1^3 + \alpha\sigma_1\sigma_2 + \beta\sigma_3$

Подставив значения симметрических многочленов, получим систему с двумя неизвестными: $\begin{cases} 0 = 8 + 2\alpha \\ -1 = 27 + \end{cases}$

Таким образом, наш многочлен f выражается через элементарные симметрические следующим образом:

$$f(x_1, x_2, x_3, x_4) = \sigma_1^3 - 4\sigma_1\sigma_2 + 8\sigma_3$$

Q.E.D.

8.2 Франсуа Виет и корни многочлена

Задача №2. *Найдите сумму чисел, обратных к корням многочлена* $3x^3 + 2x^2 - 1$.

Решение. Пусть x_1, x_2, x_3 – корни многочлена $f = 3x^3 + 2x^2 - 1$. Воспользуемся *Теоремой Виета*, разобранной на лекции, и выпишем симметрические многочлены от корней, выразив их через коэффициенты при степенях переменных.

1. $\sigma_1 = x_1 + x_2 + x_3 = -\frac{2}{3}$
2. $\sigma_2 = x_1x_2 + x_2x_3 + x_1x_3 = 0$
3. $\sigma_3 = x_1x_2x_3 = \frac{1}{3}$

Теперь найдём сумму чисел, обратных к корням многочлена f, выраженную напрямую через сами корни x_1, x_2, x_3:

$$\Sigma = \frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} = \frac{x_1x_2 + x_2x_3 + x_1x_3}{x_1x_2x_3} = \frac{\sigma_2}{\sigma_3} = \frac{0}{\frac{1}{3}} = 3 \cdot 0 = 0$$

Таким образом, сумма чисел, обратных к корням многочлена f, равна 0.

Q.E.D.

8.3 Франсуа Виет и многочлен с кубами корней

Задача №3. *Найдите многочлен 4-й степени, корнями которого являются кубы всех комплексных корней многочлена* $x^4 + x - 1$.

Решение. Пусть x_1, x_2, x_3, x_4 – корни многочлена $f = x^4 + x - 1$. Воспользуемся *Теоремой Виета*, разобранной на лекции, и выпишем симметрические многочлены от корней данного многочлена, выразив их через коэффициенты при степенях переменных.

1. $\sigma_1(x) = x_1 + x_2 + x_3 + x_4 = 0$
2. $\sigma_2(x) = x_1x_2 + x_2x_3 + x_1x_3 + x_1x_4 + x_2x_4 + x_3x_4 = 0$
3. $\sigma_3(x) = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 = -1$
4. $\sigma_4(x) = x_1x_2x_3x_4 = -1$

Пусть $y_1 = x_1^3$, $y_2 = x_2^3$, $y_3 = x_3^3$, $y_4 = x_4^3$ – корни некоего многочлена четвёртой степени. Тогда, по *Теореме Виета*, разобранной на лекции, данный многочлен имеет вид $g(x) = x^4 + \big(-\sigma_1(y)\big)x^3 + \sigma_2(y)x^2 + \big(-\sigma_3(y)\big) + \sigma_4(y)$, где $\sigma_i(y)$ – элементарный симметрический многочлен от корней $g(x)$. Воспользуемся вышеуказанной теоремой и выпишем симметрические многочлены от корней данного многочлена в общем виде, выразив их через элементарные симметрические от x (по методе, подробно описанной в **Задаче №1**):

1. $\sigma_1(y) = y_1 + y_2 + y_3 + y_4 = x_1^3 + x_2^3 + x_3^3 + x_4^3$.

   Старший член всего $\sigma_1(y)$: $Ly_{10} = x_1^3 \simeq \sigma_1^3(x)$. Следующий по старшинству член оставшейся части: $Ly_{11} = x_1^2 x_2 \simeq \sigma_1(x)\sigma_2(x)$. Последний возможный старший член оставшейся части: $Ly_{12} = x_1 x_2 x_3 \simeq \sigma_3(x)$. Тогда $\sigma_1(y) = \sigma_1^3(x) + \alpha\sigma_1(x)\sigma_2(x) + \beta\sigma_3(x)$.

   Теперь будем подставлять различные значения переменных x_1, x_2, x_3, x_4 и наблюдать за изменением значений симметрических слагаемых и самого многочлена $\sigma_1(y)$.

x_1	x_2	x_3	x_4	$\sigma_1(x)^3$	$\sigma_1(x)\sigma_2(x)$	$\sigma_3(x)$	$\sigma_1(y)$
1	1	0	0	8	2	0	$2 = \sigma_1^3 + \alpha\sigma_1\sigma_2$
1	1	1	0	27	9	1	$3 = \sigma_1^3 + \alpha\sigma_1\sigma_2 + \beta\sigma_3$

   Подставив значения симметрических многочленов, получим систему с двумя неизвестными: $\begin{cases} 2 = 8 + 2 \\ 3 = 27 + \end{cases}$

   Таким образом, $\sigma_1(y) = \sigma_1^3(x) - 3\sigma_1(x)\sigma_2(x) + 3\sigma_3(x)$ – общий вид многочлена. Однако, на значениях корней (x): $\sigma_1^3(x) = 0 = \sigma_1(x)\sigma_2(x)$. Значит, остаётся только σ_3. Следовательно, $\sigma_1(y) = 3\sigma_3(x) = 3 \cdot (-1) = -3$.

2. $\sigma_2(y) = y_1y_2 + y_2y_3 + y_1y_3 + y_1y_4 + y_2y_4 + y_3y_4 = x_1^3x_2^3 + x_2^3x_3^3 + x_1^3x_3^3 + x_1^3x_4^3 + x_2^3x_4^3 + x_3^3x_4^3$

   Старший член всего $\sigma_2(y)$: $Ly_{20} = x_1^3x_2^3 \simeq \sigma_2^3(x)$. Следующий по старшинству член оставшейся части: $Ly_{21} = x_1^3x_2^2x_3 \simeq \sigma_1(x)\sigma_2(x)\sigma_3(x)$. Следующий по старшинству член оставшейся части: $Ly_{22} = x_1^3x_2x_3x_4 \simeq \sigma_1^2(x)\sigma_4(x)$. Следующий по старшинству член оставшейся части: $Ly_{23} = x_1^2x_2^2x_3^2 \simeq \sigma_3^2(x)$. Последний возможный старший член оставшейся части: $Ly_{24} = x_1^2x_2^2x_3x_4 \simeq \sigma_2(x)\sigma_4(x)$. Тогда $\sigma_2(y) = \sigma_2^3(x) + \alpha\sigma_1(x)\sigma_2(x)\sigma_3(x) + \beta\sigma_1^2(x)\sigma_4(x) + \gamma\sigma_3^2(x) + \delta\sigma_2(x)\sigma_4(x)$.

   Теперь будем подставлять различные значения переменных x_1, x_2, x_3, x_4 и наблюдать за изменением значений симметрических слагаемых и самого многочлена $\sigma_2(y)$.

x_1	x_2	x_3	x_4	$\sigma_2^3(x)$	$\sigma_1(x)\sigma_2(x)\sigma_3(x)$	$\sigma_1^2(x)\sigma_4(x)$	$\sigma_3^2(x)$	$\sigma_2(x)\sigma_4(x)$	$\sigma_2(y)$
1	-1	-1	0	-1	1	0	1	0	-1
1	1	1	0	27	9	0	1	0	3
1	1	1	-1	0	0	-4	4	0	0
1	1	1	1	216	96	16	16	6	6

   Подставив значения симметрических многочленов, получим систему с четырьмя неизвестными:

$$\begin{cases} -1 = -1 + \alpha + \gamma \Rightarrow \alpha = -\gamma \\ 3 = 27 + 9\alpha + \gamma \Rightarrow -24 = -8\gamma \Rightarrow \gamma = 3 \Rightarrow \alpha = -3 \\ 0 = -4\beta + 4\gamma \Rightarrow \beta = \gamma = 3 \\ 6 = 216 + 96\alpha + 16\beta + 16\gamma + 6\delta \Rightarrow -210 = 3 \cdot (-96 + 16 + 16) + 6\delta \Rightarrow 6\delta = -18 \Rightarrow \delta = -3 \end{cases}$$

   Таким образом, $\sigma_2(y) = \sigma_2^3(x) - 3\sigma_1(x)\sigma_2(x)\sigma_3(x) + 3\sigma_1^2(x)\sigma_4(x) + 3\sigma_3^2(x) - 3\sigma_2(x)\sigma_4(x)$ – общий вид многочлена. Однако, на значениях корней (x): $\sigma_2^3(x) = 0 = \sigma_1(x)\sigma_2(x)\sigma_3(x) = 0 = \sigma_1^2(x)\sigma_4(x) = 0 = \sigma_2(x)\sigma_4(x)$. Значит, остаётся только $\sigma_3^2(x)$. Следовательно, $\sigma_2(y) = 3\sigma_3^2(x) = 3 \cdot (-1)^2 = 3$.

3. $\sigma_3(y) = y_1y_2y_3 + y_1y_2y_4 + y_1y_3y_4 + y_2y_3y_4 = x_1^3x_2^3x_3^3 + x_1^3x_2^3x_4^3 + x_1^3x_3^3x_4^3 + x_2^3x_3^3x_4^3$

   Старший член всего $\sigma_3(y)$: $Ly_{30} = x_1^3x_2^3x_3^3 \simeq \sigma_3^3(x)$. Следующий по старшинству член оставшейся части: $Ly_{31} = x_1^3x_2^3x_3^2x_4 \simeq \sigma_2(x)\sigma_3(x)\sigma_4(x)$. Последний возможный старший член оставшейся части: $Ly_{32} = x_1^3x_2^2x_3^2x_4^2 \simeq \sigma_1(x)\sigma_4^2(x)$. Тогда $\sigma_3(y) = \sigma_3^3(x) + \alpha\sigma_2(x)\sigma_3(x)\sigma_4(x) + \beta\sigma_1(x)\sigma_4^2(x)$.

   Теперь будем подставлять различные значения переменных x_1, x_2, x_3, x_4 и наблюдать за изменением значений симметрических слагаемых и самого многочлена $\sigma_3(y)$.

x_1	x_2	x_3	x_4	$\sigma_3^3(x)$	$\sigma_2(x)\sigma_3(x)\sigma_4(x)$	$\sigma_1(x)\sigma_4^2(x)$	$\sigma_3(y)$
1	1	1	-1	-8	0	2	-2
1	1	1	1	64	24	4	4

   Подставив значения симметрических многочленов, получим систему с двумя неизвестными: $\begin{cases} -2 = -8 \\ 4 = 64 + \end{cases}$

Таким образом, $\sigma_3(y) = \sigma_3^3(x) - 3\sigma_2(x)\sigma_3(x)\sigma_4(x) + 3\sigma_1(x)\sigma_4^2(x)$ – общий вид многочлена. Однако, на значениях корней (x): $\sigma_2(x)\sigma_3(x)\sigma_4(x) = 0 = \sigma_1(x)\sigma_4^2(x)$. Значит, остаётся только $\sigma_3^3(x)$. Следовательно, $\sigma_3(y) = \sigma_3^3(x) = (-1)^3 = -1$.

4. $\sigma_4(y) = y_1y_2y_3y_4 = x_1^3x_2^3x_3^3x_4^3$

   Старший член всего $\sigma_4(y)$: $Ly_{40} = x_1^3x_2^3x_3^3x_4^3 \simeq \sigma_4^3(x)$. Заметим, что это и есть сам $\sigma_4(y)$, значит, мы уже получили необходимое представление.

   Таким образом, $\sigma_4(y) = \sigma_4^3(x) = (-1)^3 = -1$.

Итого, учитывая перемену знака в элементарных многочленах из *Теоремы Виета*, получаем следующий многочлен 4-й степени, корнями которого являются кубы всех комплексных корней многочлена $x^4 + x - 1$:

$$g(x) = x^4 + \big(-\sigma_1(y)\big)x^3 + \sigma_2(y)x^2 + \big(-\sigma_3(y)\big) + \sigma_4(y) = x^4 + 3x^3 + 3x^2 + x - 1$$

Многочлен $g(x) = x^4 + 3x^3 + 3x^2 + x - 1$ — искомый.

Q.E.D.

8.4 Франсуа Виет и дискриминант

Задача №4. *Найдите все комплексные значения λ, при которых многочлен $x^3 - \lambda x + 2$ имеет кратный комплексный корень.*

Решение.
Определение: Дискриминатом многочлена $h(x) = a_nx^n + \ldots + a_1x + a_0$ с корнями $\alpha_1, \alpha_2, \ldots, \alpha_n$ называется выражение:

$$D(h) = a_n^{2n-2} \prod_{1 \leqslant i < j \leqslant n} (a_i - a_j)^2$$

Найдём дискриминант многочлена $f(x) = x^3 + px + q$.

Пусть x_1, x_2, x_3 – корни $f(x)$. Тогда $D(f) = (x_1 - x_2)^2(x_2 - x_3)^2(x_1 - x_3)^2$. Воспользуемся *Теоремой Виета*, разобранной на лекции, и выразим дискриминат данного многочлена, записанного в общем виде, через элементарные симметрические (по методе, подробно описанной в **Задаче №1**):

1. $\sigma_1 = x_1 + x_2 + x_3 = 0$
2. $\sigma_2 = x_1x_2 + x_2x_3 + x_1x_3 = p$
3. $\sigma_3 = x_1x_2x_3 = -q$

Старшим членом всего f будет $L_0 = (x_1)^2 \cdot (x_2)^2 \cdot (x_1)^2 = x_1^4x_2^2 \simeq \sigma_1^2\sigma_2^2$. Следующий по старшинству член оставшейся части: $L_1 = x_1^4x_2x_3 \simeq \sigma_1^3\sigma_3$. Следующий по старшинству член оставшейся части: $L_2 = x_1^3x_2^3 \simeq \sigma_2^3$. Следующий по старшинству член оставшейся части: $L_3 = x_1^3x_2^2x_3 \simeq \sigma_1\sigma_2\sigma_3$. Последний возможный старший член оставшейся части: $L_4 = x_1^2x_2^2x_3^2 \simeq \sigma_3^2$. Тогда $D(f) = \sigma_1^2\sigma_2^2 + \alpha\sigma_1^3\sigma_3 + \beta\sigma_2^3 + \gamma\sigma_1\sigma_2\sigma_3 + \delta\sigma_3^2$.

Теперь будем подставлять различные значения переменных x_1, x_2, x_3 и наблюдать за изменением значений симметрических слагаемых и самого многочлена $D(f)$.

x_1	x_2	x_3	$\sigma_1^2\sigma_2^2$	$\sigma_1^3\sigma_3$	σ_2^3	$\sigma_1\sigma_2\sigma_3$	σ_3^2	$D(f)$
1	-1	0	0	0	-1	0	0	4
1	1	-2	0	0	-27	0	4	0
1	1	-1	1	-1	-1	1	1	0
1	1	1	81	27	27	9	1	0

Подставив значения симметрических многочленов, получим систему с четырьмя неизвестными:

$$\begin{cases} 4 = -\beta \Rightarrow \beta = -4 \\ 0 = -27\beta + 4\delta \Rightarrow 4\delta = -4 \cdot 27 \Rightarrow \delta = -27 \\ 0 = 1 - \alpha - \beta + \gamma + \delta \Rightarrow \alpha = 1 + 4 - 27 + \gamma = \gamma - 22 \Rightarrow \alpha = 18 - 22 = -4 \\ 0 = 81 + 27\alpha + 27\beta + 9\gamma + \delta = 81 + 27\gamma - 22 \cdot 27 - 27 \cdot 4 + 9\gamma - 27 \Rightarrow 648 = 36\gamma \Rightarrow \gamma = 18 \end{cases}$$

Таким образом, $D(f) = \sigma_1^2\sigma_2^2 - 4\sigma_1^3\sigma_3 - 4\sigma_2^3 + 18\sigma_1\sigma_2\sigma_3 - 27\sigma_3^2$. – общий вид многочлена. Подставим теперь известные значения элементарных симметрических: $\sigma_1 = 0$, $\sigma_2 = p$, $\sigma_3 = -q$. Тогда $D(f) = -4\sigma_2^3 - 27\sigma_3^2 = -4p^3 - 27q^2$.

По следствию из определения дискриминанта, многочлен имеет кратный корень тогда и только тогда, когда его дискриминант равен 0.

Воспользуемся полученным результатом общего вида дискриминатна и подставим значения $p = -\lambda$ и $q = 2$, при этом приравняв к нулю:

$$D(x^3 - \lambda x + 2) = -4 \cdot (-\lambda)^3 - 27 \cdot (2)^2 = 4\lambda^3 - 108 = 0 \Rightarrow \lambda^3 = 27 \Rightarrow \lambda \in \left\{\sqrt[3]{27}\right\}$$

Получается, λ принимает значения всех кубических корней из 27. Заметим, что $27 = 27e^{2\pi i}$. Тогда $\lambda \in \left\{\sqrt[3]{27}\right\} = \left\{\sqrt[3]{27} \cdot e^{\frac{2\pi k}{3}i}\right\} = \left\{3e^{\frac{2\pi k}{3}i},\ k \in \{0,\ 1,\ 2\}\right\}$. Но тогда λ принимает значения $\lambda_1 = 3e^0 = 3$, $\lambda_2 = 3e^{\frac{2\pi}{3}i}$, $\lambda_3 = 3e^{\frac{4\pi}{3}i}$.

Таким образом, комплексные значения, при которых многочлен $x^3 - \lambda x + 2$ имеет кратный комплексный корень: $\lambda \in \left\{3,\ 3e^{\frac{2\pi}{3}i},\ 3e^{\frac{4\pi}{3}i}\right\}$.

Q.E.D.

9 Семинарское занятие №9

9.1 Многочлен и его корень

Задача №4. *Пусть α – комплексный корень многочлена x^2+x+1. Представьте элемент*

$$\frac{\alpha^3+2\alpha^2+\alpha}{\alpha^3-2\alpha+2} \in \mathbb{Q}(\alpha)$$

в виде $f(\alpha)$, где $f(x) \in \mathbb{Q}[x]$ и $deg\big[f(x)\big] \leqslant 1$.

Решение. Так как α – корень x^2+x+1, то $\alpha^2+\alpha+1=0$. Выделим из числителя и знаменателя $\frac{\alpha^3+2\alpha^2+\alpha}{\alpha^3-2\alpha+2}$ данный многочлен, так как $h(\alpha)\cdot(\alpha^2+\alpha+1)=0 \ \forall \ h(x) \in \mathbb{Q}[x]$.

$$\begin{array}{r|l} \alpha^3+2\alpha^2+\alpha+0 & \alpha^2+\alpha+1 \\ \underline{\alpha^3+\alpha^2+\alpha} & \\ \alpha^2+0+0 & \\ \underline{\alpha^2+\alpha+1} & \\ -\alpha-1 & \end{array}$$

Остаток: $-\alpha-1$.

$$\begin{array}{r|l} \alpha^3+0-2\alpha+2 & \alpha^2+\alpha+1 \\ \underline{\alpha^3+\alpha^2+\alpha} & \\ -\alpha^2-3\alpha+2 & \\ \underline{-\alpha^2-\alpha-1} & \\ -2\alpha+3 & \end{array}$$

Остаток: $-2\alpha+3$.

Наша дробь примет вид:

$$f(\alpha)=\frac{-\alpha-1}{-2\alpha+3}=\frac{\alpha+1}{2\alpha-3}$$

Однако, нам необходим многочлен с рациональными коэффициентами, а не дробь. Тогда найдём элемент, обратный к знаменателю, ибо $h(x)/g(x)=h(x)\cdot g^{-1}(x)$.
Обозначим $g(\alpha)=2\alpha-3$.

Пусть $u=u(\alpha)=g^{-1}(\alpha)$. В этом случае по определению: $g\cdot u=1$. Воспользуемся методом неопределённых коэффициентов и применим следующий трюк:

$$1=g\cdot u=(2\alpha-3)\cdot u+(\alpha^2+\alpha+1)\cdot v,\ v\in\mathbb{Q}[\alpha]$$

– фактически мы прибавили 0, и равенство сохранилось. Заметим, что
$deg\big[g(\alpha)\big]=1$, $deg\big[\alpha^2+\alpha+1\big]=2$ и при этом степени числителя и знаменателя исходной дроби были равны 3. Тогда степень каждого из слагаемых правой части в вышеуказанном равенстве должна не превосходить 3, причём $deg\big[u\big] \leqslant deg\big[g\big]$, так как в противном случае, будь $deg\big[u\big]$ хотя бы 2, из неё можно было бы выделить нулевую компоненту вида $h(\alpha)\cdot(\alpha^2+\alpha+1)$ – но её мы уже учли во втором слагаемом. Отсюда $deg\big[u(\alpha)\big] \leqslant 1$ и $deg\big[v(\alpha)\big] \leqslant 1$, то есть $u=b\alpha+c$ и $v=x\alpha+y$, b, c, x, $y \in \mathbb{Q}$. Уравнение примет вид:

$$\begin{gathered} 1=(2\alpha-3)\cdot(b\alpha+c)+(\alpha^2+\alpha+1)\cdot(x\alpha+y)= \\ =2b\alpha^2-3b\alpha+2c\alpha-3c+x\alpha^3+x\alpha^2+x\alpha+y\alpha^2+y\alpha+y= \\ =x\alpha^3+(2b+x+y)\alpha^2+(-3b+2c+x+y)\alpha+(-3c+y)= \\ =0\cdot\alpha^3+0\cdot\alpha^2+0\cdot\alpha+1 \end{gathered}$$

Получаем систему на 4 неизвестных:

$$\begin{cases} x=0 \\ 2b+x+y=0 \Rightarrow y=-2b \Rightarrow y=\frac{4}{19} \\ -3b+2c+x+y=0 \Rightarrow -3b+2c-2b=0 \Rightarrow c=\frac{5}{2}b \Rightarrow c=-\frac{5}{19} \\ -3c+y=1 \Rightarrow -\frac{15}{2}b-2b=1 \Rightarrow -\frac{19}{2}b=1 \Rightarrow b=-\frac{2}{19} \end{cases}$$

Итого:

$$1 = (2\alpha - 3) \cdot \big(-\frac{2}{19}\alpha - \frac{5}{19}\big) + (\alpha^2 + \alpha + 1) \cdot \big(0 + \frac{4}{19}\big) \Longrightarrow u(\alpha) = -\frac{2}{19}\alpha - \frac{5}{19} = g^{-1}(\alpha)$$

Значит,

$$f(\alpha) = \frac{\alpha + 1}{2\alpha - 3} = (\alpha + 1) \cdot \big(-\frac{2}{19}\alpha - \frac{5}{19}\big) = -\frac{2}{19}\alpha^2 - \frac{2}{19}\alpha - \frac{5}{19}\alpha - \frac{5}{19} =$$
$$= -\frac{2}{19}\alpha^2 - \frac{7}{19}\alpha - \frac{5}{19} = -\frac{1}{19}(2\alpha^2 + 7\alpha + 5)$$

Однако, в этом многочлене также содержится некая часть вида $h(\alpha) \cdot (\alpha^2 + \alpha + 1) = 0$. Поделим $f(\alpha)$ с остатком на $\alpha^2 + \alpha + 1$:

$$\begin{array}{r|l} 2\alpha^2 + 7\alpha + 5 & \alpha^2 + \alpha + 1 \\ \hline 2\alpha^2 + 2\alpha + 2 & 2 \\ \hline 5\alpha + 3 & \end{array}$$

Остаток: $5\alpha + 3$.

Таким образом,

$$f(\alpha) = -\frac{1}{19}(5\alpha + 3)$$

Замечание. *В задаче №2 Домашнего задания алгоритм действий аналогичный. Будьте внимательны со степенями u и v. Уверяю вас, в решении системы на коэффициенты, ровно как и в итоговом ответе, всё получится целое.*

Q.E.D.

9.2 Минимальный многочлен

Задача №6. *Найдите минимальный многочлен для числа $\sqrt{2} + \sqrt{3}$ над $\mathbb{Q}$.*

Решение. Минимальным многочленом элемента $\alpha \in F$ над подполем K называется ненулевой многочлен $h(x) \in K[x]$ наименьшей степени, для которого $h(\alpha) = 0$.

Пусть $\alpha = \sqrt{2} + \sqrt{3}$. Будем рассматривать степени данного уравнения, постепенно избавляясь от иррациональности.

$$\alpha^2 = 2 + 2\sqrt{6} + 3 = 5 + 2\sqrt{6} \Rightarrow \sqrt{6} = \frac{\alpha^2 - 5}{2}$$
$$6 = \frac{(\alpha^2 - 5)^2}{4} \Rightarrow 0 = \frac{(\alpha^2 - 5)^2}{4} - 6$$

В таком случае, для многочлена

$$f(x) = \frac{(x^2 - 5)^2}{4} - 6$$

число α будет являться корнем.

Докажем, что данный многочлен – минимальный для α.

Предположим, что данный многочлен не является минимальным. В таком случае существует некий $g(x)$ такой, что $deg\big[g(x)\big] \in \{1,\ 2,\ 3\}$ и $g(\alpha) = 0$. Стоит отметить, что если $deg\big[f(x)\big] > deg\big[g(x)\big]$ и $f(\alpha) = 0 = g(\alpha)$, то $g(x) \mid f(x)$.

Если $deg\big[g(x)\big] = 1$, то $g(\alpha) = x \cdot (\sqrt{2} + \sqrt{3}) + y$, $x,\ y \in \mathbb{Q}$ – ясно, что ни при каких коэффициентах из $\mathbb{Q}$ данный многочлен не будет принадлежать $\mathbb{Q}[x]$. Значит, $deg\big[g(x)\big] \neq 1$. Отсюда же следует, что $deg\big[g(x)\big] \neq 3$, так как в противном случае из многочлена третьей степени можно выделить линейный сомножитель $w(x)$, на который $f(x)$ должен делиться – возвращаемся к случаю $deg\big[g(x)\big] = 1$, только теперь для $w(x)$.

Значит, если $g(x)$ и существует, то $deg\big[g(x)\big] = 2$.

Предложение. *Пусть $\alpha \in F$ – алгебраический элемент над K и n – степень его минимального многочлена над K. Тогда*

$$K(\alpha) = \{\beta_0 + \beta_1\alpha + \ldots + \beta_{n-1}\alpha^{n-1} \mid \beta_0, \ \ldots \ , \beta_{n-1} \in K\}$$
$$K(\alpha) = \Big\{\frac{f(\alpha)}{g(\alpha)} \mid f(x),\, g(x) \in K[x],\, f(\alpha) \neq 0\Big\}$$

Кроме того, элементы $1,\ \alpha,\ \alpha^2,\ \ldots\ ,\ \alpha^{n-1}$ *линейно независимы над* K.
В частности, $\big[K(\alpha) : K\big] = n$. *Иными словами, степень поля расширения равна степени минимального многочлена и любой элемент из поля расширения представим в виде линейной комбинации степеней* α.

Полагая $g(x)$ существующим, мы тем самым утверждаем, что степень расширения поля равна 2. В таком случае любая максимальная система из линейно независимых элементов $\mathbb{Q}(\alpha)$ должна состоять ровно из 2-х элементов.

Заметим, что

$$\frac{1}{\alpha} = \frac{1}{\sqrt{2}+\sqrt{3}} = \frac{\sqrt{2}-\sqrt{3}}{2-3} = -\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\alpha)$$

Тогда рассмотрим элементы:

$$1 \in \mathbb{Q}(\alpha)$$
$$\alpha + (-\sqrt{2}+\sqrt{3}) = 2\sqrt{3} \in \mathbb{Q}(\alpha)$$
$$-\alpha + (-\sqrt{2}+\sqrt{3}) = -2\sqrt{2} \in \mathbb{Q}(\alpha)$$

Легко заметить, что элементы $1,\ -2\sqrt{2},\ 2\sqrt{3}$ являются линейно независимыми над $\mathbb{Q}$. Выходит, мы получили линейно независимую систему из 3-х элементов. Но по предположению, степень расширения поля равна 2, и максимальный размер любой системы из линейно независимых элементов равен 2 – пришли к противоречию. Значит, $deg\big[g(x)\big] \geqslant 3$.

Ранее было доказано, что случай $deg\big[g(x)\big] = 3$ не возможен. Но тогда минимальная степень $g(x)$ равна 4, и степень расширения поля не меньше 4. Но в таком случае многочлен

$$f(x) = \frac{(x^2-5)^2}{4} - 6$$

имеющий степень 4, подходит и является минимальным для α.

Замечание. *В задаче №3 Домашнего задания ровно то же самое с точностью до замены цифр и знаков.*

Q.E.D.

9.3 Поле разложения

Задача №7. *Найдите степень поля разложения многочлена* $x^4 - 2$ *над* $\mathbb{Q}$.

Решение. Определение: Пусть K – некоторое поле и $f(x) \in K[x]$. Полем разложения многочлена $f(x)$ называется такое расширение F поля K, что

1. многочлен $f(x)$ разлагается над F на линейные множители
2. корни многочлена $f(x)$ не лежат ни в каком собственном подполе поля F, содержащим K

Корнями нашего многочлена являются корни 4-й степени из 2,
а именно: $\sqrt[4]{2},\ -\sqrt[4]{2},\ i\sqrt[4]{2},\ -i\sqrt[4]{2}$.

Обозначим как $\alpha_1,\ \alpha_2,\ \alpha_3,\ \alpha_4$ соответствующие корни многочлена $x^4 - 2$.

Возьмём первый корень: $\alpha_1 = \sqrt[4]{2}$. Найдём его минимальный многочлен над $\mathbb{Q}$. Заметим, что $x^4 - 2$ является минимальным многочленом для α_1 – в противном случае существовал бы $g(x) \in \mathbb{Q}[x]$, такой, что $deg\big[g(x)\big] \in \{1,\ 2,\ 3\}$ и $g(\alpha_1) = 0$. Путём нехитрых рассуждений, аналогичных проведённым в предыдущей задаче, легко увидеть, что такого многочлена с рациональными коэффициентами попросту нет. Тогда степень расширения поля $\big[\mathbb{Q}(\alpha_1) : \mathbb{Q}\big] = 4$.

По определению поля, если $\alpha \in F$, то и $-\alpha \in F$. Тогда $-\alpha_1 = \alpha_2 \in \mathbb{Q}(\alpha_1)$.

Теперь возьмём третий корень: $\alpha_3 = i\sqrt[4]{2}$. Найдём его минимальный многочлен над $\mathbb{Q}(\alpha_1)$. Стоит отметить, что любой элемент в $\mathbb{Q}(\alpha_1)$ является линейной комбинацией степеней α_1. В таком случае можно обозначить $\alpha_3 = i\sqrt[4]{2} = i\alpha_1$.

Заметим, что многочлен $(x-i\alpha_1)(x-\overline{i\alpha_1}) = x^2-(i\alpha_1+\overline{i\alpha_1})x+i\alpha_1\cdot\overline{i\alpha_1}$ – многочлен с коэффициентами из $\mathbb{Q}(\alpha_1)$:

$$\begin{gathered}(x - i\alpha_1)(x - \overline{i\alpha_1}) = x^2 - (i\alpha_1 + \overline{i\alpha_1})x + i\alpha_1 \cdot \overline{i\alpha_1} = \\ = x^2 - (0) + (i\sqrt[4]{2} \cdot (-i\sqrt[4]{2})) = \\ = x^2 + \sqrt{2}\end{gathered}$$

Он является минимальным, поскольку любой многочлен первой степени $g(x) = bx + c$, b, $c \in \mathbb{Q}(\alpha_1)$, такой, что $g(\alpha_3) = 0$, очевидно, не может иметь все коэффициенты из $\mathbb{Q}(\alpha_1)$. Тогда степень расширения поля $\big[\mathbb{Q}(\alpha_3) : \mathbb{Q}(\alpha_1)\big] = \big[\mathbb{Q}(i\alpha_1) : \mathbb{Q}(\alpha_1)\big] = 2$.

По определению поля, если $\alpha \in F$, то и $-\alpha \in F$. Тогда $-\alpha_3 = \alpha_4 \in \mathbb{Q}(\alpha_3)$.

Таким образом, все корни многочлена $x^4 - 2$ лежат в $\mathbb{Q}(\alpha_3)$. По определению поля разложения, все корни $x^4 - 2$ должны лежать в таком поле. Но тогда $\mathbb{Q}(\alpha_3)$ и есть поле разложения многочлена $x^4 - 2$ по построению, причём пункт 2 определения следует из определения минимального многочлена.

Таким образом, поле разложения $x^4 - 2$ совпадает с полем расширения $\mathbb{Q}(\alpha_3)$.

Сначала мы расширили $\mathbb{Q}$ до $\mathbb{Q}(\alpha_1)$, потом расширили $\mathbb{Q}(\alpha_1)$ до $\mathbb{Q}(\alpha_3)$. В таком случае:

$$\big[\mathbb{Q}(\alpha_3) : \mathbb{Q}\big] = \big[\mathbb{Q}(\alpha_1) : \mathbb{Q}\big] \cdot \big[\mathbb{Q}(\alpha_3) : \mathbb{Q}(\alpha_1)\big] = 4 \cdot 2 = 8$$

и степень поля разложения многочлена $x^4 - 2$ над $\mathbb{Q}$ также равна 8.

Замечание. *В задаче №4 Домашнего задания стоит воспользоваться не только тем, что если $\alpha \in F$, то и $-\alpha \in F$, но и другим свойством поля:*
если $\alpha \in F$, то и $\alpha^n \in F$ $\forall$ $n \in \mathbb{N}$.

Важно понимать, как именно надо строить минимальный многочлен для расширения поля. В частности, с комплексными числами чаще всего можно сразу переходить к многочлену с сопряжённым, получая коэффициенты в исходном поле. Если вам повезёт, то можно будет обойтись одним расширением, поэтому не забывайте проверять свойства поля на элементах.

Q.E.D.