Методика решений задач из контрольной

Солонков Денис, Недолужко Андрей, Семенов Михаил. 161 группа

12 апреля 2018 г.

1 Группы порядка x, в которых нет элемента порядка k

Рассмотрим конкретный пример: Перечислить все абелевы группы порядка 252, в которых нет элемента порядка 4.

Напомним, что в курсе лекций существовала следующая теорема:

Теорема 1.1. Всякая конечная группа A разлагается в прямую сумму примарных подгрупп, то есть:

$$A \cong \mathbb{Z}_{p_1^{k_1}} \oplus \ldots \oplus \mathbb{Z}_{p_n^{k_n}}$$

Где p_i - простые числа, не обязательно различные, а k_i натуральные числа.

Разложим размер нашей группы 252 на простые множители:

$$252 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 7$$

Исходя из этого разложения и теоремы выше, можно понять, что:

$$A \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7$$
$$A \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_7$$
$$A \cong \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7$$
$$A \cong \mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_7$$

Сразу видно, что последние 2 варианта нам не подходят, так что остается только внимательно посмотреть на первые 2 варианта. Если:

$$A \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7$$

Так как размеры всех этих подгрупп простые числа, то и порядки всех элементов внутри подгрупп также равны размерностям этих подгрупп. Значит, мы никак не получим порядок 4. Такая группа нам подходит. Посмотрим на вторую:

$$A \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_7$$

Тут опять же все ясно. Во всех группах, кроме $\mathbb{Z}_9$ порядки равны размерности, а в $\mathbb{Z}_9$ порядки равны либо 3, либо 9, но 4 мы никак не получим.

Второй вариант

$$A \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7$$
$$A \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_7$$
$$A \cong \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7$$
$$A \cong \mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_7$$

Второй и четвёртый стулья нам не подходят, комфортно обустраиваемся на первом и третьем. Данные варианты действительно подойдут, потому что в каждой порядок произвольного элемента - это НОК порядков соответствующих "координат" данного элемента. Ну и понятно, что девять мы никак не получим.

2 Разложить факторгруппу в прямую сумму циклических групп

Тут мы будем очень сильно пользоваться теоремой о согласованный базисах. Напомним ее:

Теорема 2.1. Для всякой подгруппы N свободной абелевой группы L ранга n найдется такой базис $e_1, \ldots, e_n$ группы L и такие натуральные числа $u_1, \ldots, u_m$, что $u_1e_1, \ldots, u_me_m$ является базисом подгруппы N и при этом $u_i | u_{i+1}$.

TODO: расписать теоретический метод поиска согласованного базиса.

Решим эту задачу на примере. Пусть A - свободная абелева группа с базисом e_1, e_2, e_3, а B ее подгруппа, порожденная элементами:

$$f_1 = 2e_1 + 3e_2 + 7e_3$$
$$f_2 = e_1 - e_2 + 5e_3$$
$$f_3 = 5e_1 - 3e_2 + 5e_3$$

Запишем это в качестве матрицы и начнем проводить всякие преобразования строк и столбцов, главное, чтобы они были обратимы.

$$M = \begin{pmatrix} 2 & 1 & 5 \\ 3 & -1 & -3 \\ 7 & 5 & 5 \end{pmatrix} \sim \begin{pmatrix} 2 & 1 & 5 \\ 1 & -2 & -8 \\ 7 & 5 & 5 \end{pmatrix} \sim \begin{pmatrix} 1 & -2 & -8 \\ 2 & 1 & 5 \\ 7 & 5 & 5 \end{pmatrix} \sim \begin{pmatrix} 1 & -2 & -8 \\ 0 & 5 & 21 \\ 0 & 19 & 61 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 5 & 21 \\ 0 & 19 & 61 \end{pmatrix} \sim$$
$$\sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 5 & 21 \\ 0 & 4 & -2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 23 \\ 0 & 4 & -2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 23 \\ 0 & 0 & -94 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 94 \end{pmatrix}$$

Итого получилось, что мы можем выбрать такой базис e_1', e_2', e_3' в A, что наша подгруппа порождается элементами $e_1', e_2', 94e_3'$. Теперь скажем следующее:

$$A \cong \mathbb{Z}^3$$
$$B \cong \mathbb{Z} \oplus \mathbb{Z} \oplus 94\mathbb{Z}$$
$$A/B \cong (\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z})/(\mathbb{Z} \oplus \mathbb{Z} \oplus 94\mathbb{Z})$$

И у нас есть теорема, что если мы берем фактор группу от вот таких вот прямых суммах в скобках, то мы можем раскрыть это взятие фактор группы по стандартным правилам

$$A/B \cong (\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z})/(\mathbb{Z} \oplus \mathbb{Z} \oplus 94\mathbb{Z}) \cong \mathbb{Z}/\mathbb{Z} \oplus \mathbb{Z}/\mathbb{Z} \oplus \mathbb{Z}/94\mathbb{Z} \cong \{0\} \cong \{0\} \cong \mathbb{Z}_{94} \cong \mathbb{Z}_{94}$$

Что от нас и требовалось.

Второй вариант

$$M = \begin{pmatrix} 2 & 3 & 7 \\ 1 & -1 & 5 \\ 5 & -3 & 5 \end{pmatrix} = \begin{pmatrix} 1 & -1 & 5 \\ 2 & 3 & 7 \\ 5 & -3 & 5 \end{pmatrix} = \begin{pmatrix} 1 & -1 & 5 \\ 0 & 5 & -3 \\ 0 & 2 & -20 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 5 & -3 \\ 0 & 2 & -20 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 5 & -3 \\ 0 & 2 & -20 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 37 \\ 0 & 2 & -20 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 30 \\ 0 & 0 & -94 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 94 \end{pmatrix} \Rightarrow \mathbb{Z}_{94}$$

Какое совпадение!

3 Найти нормализатор подгруппы

Итак, аккуратно посмотрим на то, как будет выглядить произведение gHg^{-1} для произвольного g.

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$g^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Обратную матрицу я нашел по формуле из линала. Так как определитель у нее 1, то там фигня, на которую мы домножаем также будет единичной. А теперь честно распишем произведение:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} at & bt^{-1} \\ ct & dt^{-1} \end{pmatrix} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} adt - bct^{-1} & -abt + abt^{-1} \\ cdt - cdt^{-1} & -bct + adt^{-1} \end{pmatrix}$$

Далее предполагается, что исходная матрица не единична, то есть $t \neq t^{-1}$ (единичная матрица, понятно дело, является стабилизатором).

$$abt = abt^{-1}$$
$$cdt = cdt^{-1}$$

(это получается из того, что второй и третий элемент матрицы равны нулю)

Заметим, что эти уравнения накладывают все условия на матрицу g. Действительно, матрицы из H - диагональные матрицы с единичным детерминантом. Диагональность мы только что потребовали, а **детерминант будет равен единице по свойству произведения детерминантов**.

Собственно, либо $a = 0$, либо $b = 0$, а также либо $c = 0$, либо $d = 0$.

Пусть $a = 0$. Тогда $c \neq 0$ (в противном случае матрица g не принадлежит группе $SL_n(\mathbb{R}_2)$, поскольку её детерминант равен нулю), следовательно $d = 0$.

Аналогично, если $b = 0$, то $c = 0$.

Причём поскольку g имеет единичный детерминант.

Почти ответ:

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} or \begin{pmatrix} 0 & a \\ -a^{-1} & 0 \end{pmatrix}$$

Так мы доказали, что для вышеупомянутых матриц $gHg^{-1} \subset H$. Давайте покажем строгое равенство.

Это просто!

Давайте подставим в качестве матрицы g матрицу первого типа из ответа. Получим

$$\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}$$

то есть матрица из h перейдёт просто сама в себя. Значит, подставляя разные h, мы получим всё множество H.

Аналогично для второго типа:

$$\begin{pmatrix} -t^{-1} & 0 \\ 0 & -t \end{pmatrix}$$

То есть мы получили обратную матрицу к исходной. $H^{-1} = H$.

4 Найти сумму кубов корней, или еще какая-нибудь фигня с суммой многочлена от корней

Тут все очень упирается на то, что многочлен, с которым мы работаем является симметрическим. Если он не симметрический, то мы проиграли. Если же он симметрический, то мы обмажемся симметрическим разложением, которое проще всего показать на примере. Итак, мы хотим посчитать сумму кубов корней многочлена $f(x) = 7x^4 - 14x^3 - 7x + 2$. Обозначим за α_i соответствующий корень. Нас интересует следующая штука, от которой мы можем найти симметрическое разложение:

$$\alpha_1^3 + \alpha_2^3 + \alpha_3^3 + \alpha_4^3$$

Напомним, как надо искать симметрическое разложение. Для начала найдем максимальный одночлен. В нашем многочлене он представляет из себя α_1^3. Теперь найдем все остальные одночлены, которые удовлетворяют следующему набору свойств:

1. Степени переменных не возрастают. То есть, $\alpha_1^3\alpha_2^2\alpha_3^1$ подходит под это свойство, а вот $\alpha_1\alpha_4^3$ нет

2. Сумма степеней переменных равна сумме степеней максимального одночлена, в нашем случае 3.

3. Он лексиграфически меньше максимального одночлена.

Выпишем такие одночлены и также правее них выпишем такой одночлен из элементарных симметрических, что максимальный одночлен такого произведение симметрических равен штуке слева:

$$\alpha_1^3 \Rightarrow \sigma_1^3$$
$$\alpha_1^2\alpha_2 \Rightarrow \sigma_1\sigma_2$$
$$\alpha_1\alpha_2\alpha_3 \Rightarrow \sigma_3$$

И теперь по доказанной на лекции теореме утверждается, что наш многочлен представляет из себя линейную комбинацию этих σ_i, то есть:

$$h(x) = \alpha_1^3 + \alpha_2^3 + \alpha_3^3 + \alpha_4^3 = \beta_1\sigma_1^3 + \beta_2\sigma_1\sigma_2 + \beta_3\sigma_3$$

Чтобы найти значения β_i, просто подставим очень хорошие значения в $h(x)$. То есть:

$$h(1,0,0,0) = 1 = \beta_1$$
$$h = \sigma_1^3 + \beta_2\sigma_1\sigma_2 + \beta_3\sigma_3$$
$$h(1,1,0,0) = 2 = 8 + \beta_2 2$$
$$\beta_2 = -3$$
$$h = \sigma_1^3 - 3\sigma_1\sigma_2 + \beta_3\sigma_3$$
$$h(1,1,1,0) = 3 = 27 - 27 + \beta_3$$
$$\beta_3 = 3$$
$$h = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$$

А теперь, вспомним теорему Виета. Напомним, что наш многочлен равен $x^4 - 2x^3 - x + \frac{2}{7}$. По теореме Виета:

$$\sigma_1 = -2$$
$$\sigma_2 = 0$$
$$\sigma_3 = -1$$

Значит, искомое нами число есть:

$$-8 - 3 = 11$$

Второй вариант Воспользуемся решением выше, и выразим новые элементарные симметрические многочлены (обозначим их как γ_i) через старые (новые - это которые от корней многочлена, который мы хотим построить, а старые - это которые уже есть).

Запишем уравнение в каноническом виде

$$x^3 - 4/3x^2 + 2x + 10/3 = 0$$

Следовательно, старые элементарные симметрические многочлены равны

$$\sigma_1 = (-1)^1 \cdot (-4/3) = 4/3$$
$$\sigma_2 = (-1)^2 \cdot 2 = 2$$
$$\sigma_3 = (-1)^3 \cdot 10/3 = -10/3$$

Теперь выразим новые элементарные симметрические многочлены через старые.

$$\gamma_1 = x_1^2 + x_2^2 + x_3^2 = \sigma_1^2 - 2\sigma_2 = 16/9 - 4 = -5$$

С γ_2 просто не получается, давайте честно сделаем.
Старший член - $x_1^2 x_2^2 \leftrightarrow \sigma_2^2$.
Все одночлены степени четыре, лексикографически меньшие старшего члена:

$$x_1^2 x_2 x_3 \leftrightarrow \sigma_1 \sigma_3$$

Значит

$$\gamma_2 = a \cdot \sigma_2^2 + b \cdot \sigma_1 \sigma_3$$

Найдём a и b, подставляя различные значения x_1, x_2, x_3 :

$$\begin{cases} \gamma_2(1,1,0) = 1 \\ \sigma_2(1,1,0) = 1 \\ \sigma_3(1,1,0) = 0 \\ \sigma_1(1,1,0) = 2 \end{cases} \Rightarrow 1 = a \cdot 1 \Rightarrow a = 1$$

$$\begin{cases} \gamma_2(1,1,1) = 3 \\ \sigma_2(1,1,1) = 3 \\ \sigma_3(1,1,1) = 1 \\ \sigma_1(1,1,1) = 3 \end{cases} \Rightarrow 3 = a \cdot 9 + b \cdot 3 \Rightarrow b = -2$$

Следовательно,

$$\gamma_2 = \sigma_2^2 - 2\sigma_3\sigma_1 = 4 + 80/9 = 116/90$$

Наконец

$$\gamma_3 = \sigma_3^2 = 100/9$$

Следовательно, итоговый многочлен равен

$$x^3 - 100/9x^2 + 116/9x + 5 = 0$$

5 Алгоритм Евклида и много боли

Мы хотим втащить расширенный алгоритм Евклида для многочленов f, g Будем строить табличку Семенова со столбцами u, v, z и поддерживать в ней инвариант, что $uf + vg = z$. Заметим, что умножение строки на многочлен не нарушает инвариант, как и сложение двух строк. Значит, мы можем прокрутить алгоритм Евклида, используя эту табличку и получить u, v автоматом:

u	v	z
1	0	$x^5 + x^4 + x^3 + 5x^2 + 5x + 5$
0	1	$x^4 - 2x^3 + 5x - 10$
1	$-x - 3$	$7x^3 + 35$
$-\frac{x}{y} + \frac{2}{7}$	$x + 4$	0

Итого мы получили, что

$$f + (-x - 3)g = 7x^3 + 35$$
$$\frac{1}{7}f + \frac{1}{7}(-x - 3)g = x^3 + 5$$

Что и является нашим нодом.

6 Убираем корни из знаменателя

Для начала представим что мы умеем находим линейное разложение НОДа знаменателя и многочлена корнем которого является α. То есть пусть наша дробь имеет вид $\frac{g(\alpha)}{h(\alpha)}$, и $q(\alpha) = 0$, где q наш полином. Тогда есть такие $u, v : h(x)u(x) + v(x)q(x) = (h, q)$ Теперь полезно рассмотреть два случая.

Случай первый $(h, q)(\alpha) = 0$ Тогда мы можем считать что $q = (h, q)$. Но тогда знаменатель равен нулю, противоречие.

Случай второй $(h, q)(\alpha) \neq 0$. Тогда мы можем считать, что $q' = q/(h, q)$. Но тогда $q'(\alpha) = 0$. И мы имеем $u'(x)h(x) + v'(x)q'(x) = 1$.

Далее все просто:

$$\frac{g(\alpha)}{h(\alpha)} = \frac{g(\alpha)u'(\alpha)}{h(\alpha)u'(\alpha)} = \frac{g(\alpha)u'(\alpha)}{1 - v'(\alpha)q'(\alpha)} = \frac{g(\alpha)u'(\alpha)}{1} = g(\alpha)u'(\alpha)$$

Осталось разделить ответ с остатком на $q'(\alpha)$ и степень нового ответа будет строго меньше чем $degq'$.

Заметим, что для счастья нам нужен только $u'(\alpha)$.

Начинаем обмазываться чиселками. Юзаем табличку, утверждается, что один из столбцов нам не нужен(ну и выбросим его).

u	z	$debug$
1	x^7+1	$-$
0	x^4+x+2	x^3-1
1	x^3+x	x
$-x$	$-x^2+x+2$	$-x-1$
$1-x-x^2$	$x+2$	$-x$
$-x^3-x^2+x$	2	
x^3+x^2-x	1	

Возможно тут есть бага, но числа не нужны.
P.S. У этого полинома нет корней можно ничего не делать, приятного дня.