ДЗ 10. Симметрические многочлены и расширения полей.

Задачи

Задача 1. Выразить мономиальную функцию

$$\sum_{i \neq j} x_i^4 x_j$$

через элементарные симметрические. Число переменных конечно, но произвольно. Заметьте, что это не влияет на вид ответа.

Задача 2. Выразите через элементарные симметрические полиномы

$$(x_1 + x_2)(x_1 + x_3)(x_1 + x_4)(x_2 + x_3)(x_2 + x_4)(x_3 + x_4)$$

Задача 3 (2 балла)**.** Найдите коэффициенты многочлена $p(x) \in \mathbb{Q}[x]$, которому удовлетворяет элемент $x_1^2 + x_1$, если x_1 есть корень уравнения $x^4 + x + 1$.

Задача 4. Найдите результант двух многочленов $x^3 - 3x^2 + 2x + 1$ и $2x^2 - x - 1$.

Задача 5. Найдите $D(x^3 + 2x^2 + x + 1)$.

Задача 6. Покажите, что

$$D(x^n + ax + b) = (-1)^{\frac{n(n-1)}{2}}((n^n)b^{n-1} + (-1)^{n-1}(n-1)^n a^n).$$

Теория

Предложение. *Пусть L конечное расширение K. Для любого элемента $\beta \in L$ существует многочлен $g(x) \in K[x]$, такой что $g(\beta) = 0$ и $\deg g(x) \leq \deg p(x)$.*

Доказательство. Рассмотрим набор $1, \beta, \beta^2, \ldots, \beta^k$. Пусть k наименьшее такое, что этот набор линейно зависим. Тогда $k \leq n$ из-за ограничения на размерность. Рассмотрим нетривиальную линейную комбинацию, которая равна 0

$$a_k\beta^k + a_{k-1}\beta^{k-1} + \cdots + a_0 = 0,$$

$a_i \in K$. Это равенство говорит, что многочлен $g(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_0$ обнуляется на β.

Мы стартовали с задачи нахождения уравнения для элемента из $\beta \in K[\alpha_1, \ldots, \alpha_n]$, где $\alpha_1, \ldots, \alpha_n$ — все корни некоторого многочлена $p(x) \in K[x]$.

Оказалось, что формулу довольно легко написать. А именно, если $\beta = f(\alpha_1, \ldots, \alpha_n)$, где $f \in K[x_1, \ldots, x_n]$ — многочлен, то подойдёт

$$g(x) = \prod_{\tau \in S_n} (x - f(\alpha_{\tau(1)}, \ldots, \alpha_{\tau(n)})).$$

Действительно, ясно, что β есть корень этого многочлена. Вопрос — почему его коэффициенты из K? Ответ: потому что они есть симметрические функции (над K) от корней многочлена $p(x)$ и, следовательно, полиномиально (над K) выражаются через коэффициенты $p(x)$.

Определение 1. Функция $\sigma_k(x_1, \ldots, x_n) = \sum_{1 \leq i_1 < \cdots < i_k \leq n} x_{i_1} \ldots x_{i_k}$ называется элементарной однородной степени k симметрической функцией от переменных $x_1, \ldots, x_n$. Если многочлен $p(x) = (x - x_1)\ldots(x - x_n) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, то $a_i = (-1)^{n-i}\sigma_{n-i}(x_1, \ldots, x_n)$.

Теорема 1. Пусть $f(x_1, \ldots, x_n)$ — симметрический многочлен из $R[x_1, \ldots, x_n]$ (R можно взять произвольным коммутативным кольцом, нас в основном будет интересовать случай, когда R — поле или кольцо $\mathbb{Z}$). Тогда существует единственный многочлен $g(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$, что $g(\sigma_1, \ldots, \sigma_n) = f(x_1, \ldots, x_n)$, а

$$\sigma_k(x_1, \ldots, x_n) = \sum_{1 \leq i_1 < \cdots < i_k \leq n} x_{i_1} \ldots x_{i_k}$$

Доказательство. Совершенно понятно, что теорему можно доказывать по отдельности для однородных многочленов фиксированной степени l. Теперь необходимо ввести упорядочивание на мономах. Если многочлен однородный степени l, то любой моном, который входит в его представление имеет вид $x_1^{\lambda_1}\dots x_n^{\lambda_n}$ где $\sum\lambda_i = l$. Как обычно будем обозначать за λ набор из степеней $(\lambda_1,\dots,\lambda_n)$, а соответствующий моном за x^λ. Видно, что мономы соответствуют упорядоченным разбиениям числа l на слагаемые. Будем говорить, что два разбиения $\lambda > \mu$, если $\lambda_1 = \mu_1,\dots,\lambda_s = \mu_s, \lambda_{s+1} > \mu_{s+1}$.

Теперь будем убирать из f самые большие мономы. Если старший моном соответствовал разбиению $\lambda = (\lambda_1,\dots,\lambda_n)$, то $\lambda_i \geq \lambda_{i+1}$ (из-за симметричности f). Тогда из f надо вычесть

$$\sigma_1^{\lambda_1-\lambda_2}\dots\sigma_{n-1}^{\lambda_{n-1}-\lambda_n}\sigma_n^{\lambda_n}$$

с подходящим коэффициентом. И т.д. □

Замечание. Функция $g(x) = \prod_{\tau\in S_n}(x - f(\alpha_{\tau(1)},\dots,\alpha_{\tau(n)}))$ хороша всем, кроме того, что её степень $n!$. Если многочлен f специального вида, то можно обойтись функцией меньшей степени. Например, если $f(x_1,\dots,x_n) = x_1^s$, то достаточно взять $g(x) = \prod_{i=1}^n(x - x_i^s)$.

Отдельно стоит вопрос, какие ещё симметрические функции, (кроме элементарных) задают значения всех остальных симметрических функций?

Определение 2. Новым важным примером симметрических многочленов являются суммы степеней

$$s_k(x_1,\dots,x_n) = x_1^k + \dots + x_n^k$$

Для этих функций справедливы тождества Ньютона, которые связывают их с элементарными симметрическими:

Лемма 1. Степенные суммы и элементарные симметрические многочлены связаны тождествами

$$0 = (-1)^n n\sigma_n + \sum_{k=0}^{n-1}(-1)^k\sigma_k s_{n-k}$$

Доказательство. Рассмотрим равенство

$$(x - x_1)\dots(x - x_n) = x^n + \sum(-1)^{n-i}\sigma_{n-i}x^i.$$

Подставим в это равенство $x = x_j$. Получим

$$0 = x_j^n + \sum(-1)^{n-i}\sigma_{n-i}x_j^i.$$

Просуммируем по всем j. Получим

$$0 = s_n + \sum_{i\neq 0}(-1)^{n-i}\sigma_{n-i}s_i + (-1)^n n\sigma_n$$

Это доказывает равенство, когда число переменных равно номеру σ_n. Подставив переменные $x_{k+1},\dots,x_n$ равные 0 в это равенство получим его для k переменных $k < n$.

Теперь предположим, что $k > n$. Проверим, что справа и слева однинаковые мономы входят с одинаковым коэффициентом.

Заметим, что в каждом мономе заведомо участвует не более n различных переменных так степень каждого монома ровно n. Пусть мы хотим проверить наличие справа и слева одинакового числа мономов в записи которых участвуют переменные $x_{i_1},\dots,x_{i_n}$. Подставим вместо всех остальных переменных 0. Понятно, что с искомым мономом ничего не произойдёт. С другой стороны после такой подстановки и переобозначения переменных мы приходим к уже доказанному равенству, когда $k = n$. □

Кроме сумм степеней встречаются так же полные однородные симметрические многочлены степени k.

Определение 3. Полным однородным симметрическим многочленом от переменных $x_1,\dots,x_n$ степени k называется

$$p_k(x_1,\dots,x_n) = \sum_{\substack{\lambda_1+\dots+\lambda_n=k\\ \text{различные разбиения}}} x_1^{\lambda_1}\dots x_n^{\lambda_n}.$$

Мы про них ничего не говорили. Они – альтернатива элементарным симметрическим – все другие так же выражаются через них. Для них есть тождества типа тождеств Ньютона, связывающие их со степенными суммами.

Важный пример симметрических многочленов — мономиальные функции. Их много. Они хороши тем, что образуют базис пространства всех симметрических многочленов (в отличие от элементарных, степенных, полных однородных).

Определение 4. Пусть $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ — разбиение числа n на слагаемые.

$$m_\lambda = \sum_{\substack{\text{по неповторяющимся} \\ \text{мономам}}} x_{\tau(1)}^{\lambda_1} \dots x_{\tau(n)}^{\lambda_n}.$$

Замечание. Степенные суммы и элементарные симметрические многочлены являются частным случаем мономиальных.

Всю эту технику можно применить к решению систем уравнений, в которые переменные входят в симметрично. Например, если у вас есть система

$$\begin{cases} x+y+z=a \\ xy+yz+zx=b \\ xyz=c, \end{cases}$$

то элементы x, y, z являются корнями $x^3 - ax^2 + bx - c$. В частности, система

$$\begin{cases} x+y+z=6 \\ xy+yz+zx=11 \\ xyz=6, \end{cases}$$

имеет корнями всевозможные перестановки $(1, 2, 3)$.

А ещё техника симметрических многочленов позволяет считать разные выражения от корней многочленов, которые имеют определённый смысл. Например,

Определение 5. Пусть f и g – два многочлена со старшими коэффициентами a_n и b_m, тогда

$$Res(f,g) = a_n^m b_m^n \prod (x_i - y_j),$$

где x_i – все корни f с учётом кратности, а y_j – корни g.

Это определение корректно, потому что перед нами написан симметричный многочлен по переменным x_i и y_j и, следовательно, он выражается через элементарные симметрические функции, то есть является многочленом от $\frac{a_i}{a_n}$ и $\frac{b_j}{b_m}$. На самом деле степени a_n и b_m вначале подобраны так, что это многочлен именно от a_i и b_j. Точнее справедлива теорема:

Теорема 2. Пусть многочлен $f(x) = a_0 + \cdots + a_n x^n$, а $g(x) = b_0 + \cdots + b_m x^m$. Тогда результант есть определитель квадратной матрицы размера $n + m$

$$Res(f,g) = \det S = \det \begin{pmatrix} a_n & a_{n-1} & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & a_n & a_{n-1} & \cdots & a_0 & \cdots & 0 \\ & & & & & & \\ 0 & \cdots & a_n & a_{n-1} & a_{n-2} & \cdots & a_0 \\ b_m & \cdots & b_1 & b_0 & 0 & \cdots & 0 \\ & & & & & & \\ 0 & \cdots & 0 & b_m & \cdots & b_1 & b_0 \end{pmatrix}.$$

Эта матрица называется матрицей Сильвестра.

Доказательство. Рассмотрим отображение из $K[x]_{\leq m-1} \times K[x]_{\leq n-1} \to K[x]_{\leq n+m-1}$, заданное по правилу

$$(a(x), b(x)) \to a(x)f(x) + b(x)g(x).$$

Очевидно, матрицей этого отображения в стандартном базисе является транспонированная матрица Сильвестра. Когда это отображение вырождено? Тогда и только тогда, когда есть многочлены маленьких степеней, что $a(x)f(x) = -b(x)g(x)$. Это происходит тогда и только тогда, когда у многочленов f и g есть общий множитель. С другой стороны результант зануляется в той же ситуации. Докажем, что $Res(f,g) = \det S$, как многочлены от x_i, y_j используя то, что $\det S$ зануляется тогда и только тогда, когда у f, g есть общий корень над алгебраическим замыканием поля.

Поделим $p(x_1 \dots, x_n, y_1, \dots, y_m) = \det S$ на $(x_i - y_j)$ с остатком как многочлен от x_i

$$p = (x_i - y_j)q + r(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n, y_1, \dots, y_m).$$

В остатке стоит многочлен r степени 0 по x_i, то есть от x_i не зависящий. Подставляя справа и слева $x_i = y_j$ получаем, что $r = 0$, то есть $\det S \vdots (x_i - y_j)$. Тогда $\det S \vdots \prod (x_i - y_j)$. Осталось сравнить степени и старшие коэффициенты. $\square$

Как всегда такое представление ответа хорошо теоретически — это означает, что результант имеет смысл над любым кольцом. Мы уже знаем, что означает, что результант обращается в 0 над полем. Это значит, что у многочленов f и g есть общий корень в алгебраическом замыкании, то есть общий множитель над K.

Что значит равенство нулю результанта по y для двух многочленов $f(x,y)$ и $g(x,y)$ из $K[x,y]$? Их результант это многочлен $h(x)$. Рассмотрим точку x_0. Допустим, что старшие коэффициенты f и g не обращаются в 0 в точке x_0. Тогда равенство нулю результанта $h(x_0)$ – это равенство нулю результанта многочленов $f(x_0,y)$ и $g(x_0,y)$, что означает, что у последних есть общий корень y_0. То есть у системы $f=g=0$ есть корень (x_0,y_0). Таким образом корни результанта – это просто x-координаты решений системы, или точки, в которых старший коэффициент многочленов обращается в 0.

А что можно вывести из того факта, что у $Res(f,g)=n$ для двух многочленов из $\mathbb{Z}[x]$? Разложим n на простые множители. Получим $n=p_1^{\alpha_1}\dots p_k^{\alpha_k}$. Допустим, что p_i не делит старшие коэффициенты f и g. Тогда $0=Res(f,g)\bmod p_i$ есть $Res(\overline{f},\overline{g})$ и следовательно по модулю p_i у многочленов есть общий корень и обратно.

Выделим несколько свойств результанта, которые позволяют его считать.

Лемма 2. Пусть $f(x)=a_0+\dots+a_nx^n$, а $g(x)=b_0+\dots+b_mx^m$. Тогда

$$Res(f,g)=b_m^n\prod f(y_j)=(-1)^{mn}a_n^m\prod g(x_i).$$

Кроме того, если $f=gq+r$, где $\deg r=k$, то

$$Res(f,g)=(-1)^{(n-k)m}b_m^{n-k}Res(r,g).$$

Определение 6. Дискриминантом многочлена $f=a_0+\dots+a_nx^n$ называется выражение

$$D(f)=a_n^{2n-2}\prod_{i\neq j}(x_i-x_j)^2.$$

Лемма 3. Имеет место равенство $Res(f,f')=(-1)^{\frac{n(n-1)}{2}}a_nD(f)$.

Примеры:
1) $D(x^2+ax+b)=-4b+a^2$.
2) $D(x^3+ax+b)=-27b^2-4a^3$.

Новая теория

Понятие дискриминанта оказывается очень важным, когда речь идёт про расширения полей. А именно,

Определение 7. Пусть L – конечное расширение поля K. Тогда $Disc(L/K)$ называется элемент факторгруппы $K^*/(K^*)^2$ равный $\det \mathrm{Tr}_{L/K}$.

Действительно, если мы заменим координаты, то матрица квадратичной формы поменяется $C^\top AC$, а её определитель поменяется на квадрат. Осталось только понять, как этот дискриминант связан с дискриминантом многочлена.

Лемма 4. Пусть $L=K[x]/f$, где f – сепарабельный многочлен (без кратных корней над замыканием) со старшим коэффициентом 1. Тогда $Disc(L/K)=D(f)$.

Доказательство. Выберем базис $1,x,\dots,x^{n-1}$. Теперь неплохо бы было посчитать в этом базисе $Disc(L/K)$. Для этого надо понять, что такое $\mathrm{Tr}(x^k)$. Перейдём к алгебраическому замыканию. Оператор домножения на x имеет собственными числами все корни $x_1,\dots,x_k$ многочлена $f(x)$. Тогда след его k-ой степени – это $s_k(x)=x_1^k+\dots+x_n^k$. Заметим тогда, что получившаяся матрица имеет вид $B^\top B$, где B – это матрица Вандермонда для x_i. □

Если наше базовое поле – это $\mathbb{Q}$, то понятие дискриминанта можно уточнить. А именно, внутри $\mathbb{Q}$ есть подкольцо $\mathbb{Z}$, а внутри любого расширения L есть кольцо целых $\mathcal{O}_L=\{a\in L\,|\,a \text{ цел над } \mathbb{Z}\}$, то есть существует многочлен $p(x)\in\mathbb{Z}[x]$ со старшим коэффициентом 1, что $p(a)=0$.

Факт. $\mathcal{O}_L$ – подкольцо в L и является конечнопорождённой абелевой группой ранга, равного степени расширения $L/\mathbb{Q}$.

Определение 8. Тогда определим целое число $Disc_L=\det \mathrm{Tr}_{\mathcal{O}_L}$, то есть определитель матрицы составленной из $\mathrm{Tr}(e_ie_j)$, где e_i – базис $\mathcal{O}_L$, как абелевой группы.

Лемма 5. Дискриминант определён однозначно.

Доказательство. Любая матрица замены C целочисленна и обратима. Тогда её определитель равен ± 1. Тогда его квадрат и вовсе единица. Тогда $\det(C^\top AC) = (\det C)^2 \det A = \det A$, где A – матрица для формы следа в исходном базисе. □

Замечание. Пусть есть решётка $\mathbb{Z}^n$ с квадратичной формой q и в ней подгруппа полного ранга M. Тогда определитель $\det q|_M = [\mathbb{Z}^n : M]^2 \cdot \det q$.

Следствие 1. Пусть $L = \mathbb{Q}[x]/f(x)$, где $f(x)$ – многочлен со старшим коэффициентом 1. Тогда $D(f) = k^2 Disc_L$ для некоторого k.

Дискриминант расширения наряду со степенью расширения является очень сильным инвариантом, но нас прежде всего будет интересовать следующий факт:

Факт. Пусть имеется башня полей $\mathbb{Q} \subseteq K \subseteq L$. Тогда $Disc_L \vdots Disc_K$.

Следствие 2. Если $L = \mathbb{Q}[x]/f(x)$, а $K = \mathbb{Q}[x]/g(x)$, где $f, g \in \mathbb{Z}[x]$ со старшим коэффициентом 1 и при этом $D(g) = p^s u$, где s – нечётное, а p – простое, (u, p), а $D(f) \not\vdots p$. Тогда у многочлена g нет корней в L.

Доказательство. Если у многочлена g есть корень в L, то поле K вкладывается в L. Заметим, что $Disc_K \vdots p$, а $Disc_L \not\vdots p$. Противоречие с фактом. □

Надо заметить, что указанное следствие далеко не самый очевидный способ доказать отсутствие корней. Наиболее простой критерий вытекает из теоремы о башне полей.

Теорема 3 (Теорема о башне полей.)**.** Пусть есть башня расширений полей $K \subseteq L \subseteq M$. Тогда $[M : K] = [M : L][L : K]$.

Замечание. Пусть есть башня полей $K \subseteq L \subseteq M$, и $x \in L$. Тогда $\mathrm{Tr}_{M/K}(x) = [M : L] \mathrm{Tr}_{L/K}(x)$.

Доказательство. Пусть e_i – базис L над K, а f_j – базис M над L. Тогда $e_i f_j$ – базис M над K. Но матрица домножения на x в таком базисе – это блочнодиагональная матрица с матрицей домножения на x на L в блоках на диагонали. □

Замечание. Радикалом называется корень уравнения $x^l - a = 0$. Если $a \in \mathbb{Q}$ – не есть k-ая степень, где $k|l$, то соответствующий многочлен неприводим над $\mathbb{Q}$. Следовательно след такого радикала всегда 0 (он ноль в наименьшем расширении, содержащем x, так как равен коэффициенту минимального многочлена, а в остальных 0 по предыдущему замечанию).

Теперь можно доказать простую теорему.

Теорема 4 (Теорема о линейной независимости радикалов)**.** Пусть даны числа $a_i = \sqrt[k_i]{\frac{d_i}{r_i}} \in \mathbb{C}$, где $(d_i, r_i) = 1$, $d_i \neq d_j$ или $r_i \neq r_j$ и при этом r_i, d_i – без квадратов. Тогда они линейно независимы над $\mathbb{Q}$.

Доказательство. Пусть есть нетривиальная линейная комбинация $\sum \lambda_i a_i = 0$. Пусть $\lambda_1 = 1$. Поделим всё выражение на a_1. Получим $1 = -\sum \lambda_i \frac{a_i}{a_1}$. Заметим, что все числа в последней сумме не лежат в $\mathbb{Q}$ и удовлетворяют уравнению вида $x^s = d$. Рассмотрим конечное подрасширение M в $\mathbb{C}$, которое их содержит. Тогда $\mathrm{Tr}_{M/\mathbb{Q}}(-\sum \lambda_i \frac{a_i}{a_1}) = 0$, а с другой стороны это $\mathrm{Tr}\, 1$, то есть степень расширения. □