I. Инварианты конечных групп

1. Разные задачи

Все группы предполагаются конечными и все алгебры и векторные пространства рассматриваются над полем $\mathbb{C}$.

1. Приведите пример подалгебры $S \subset \mathbb{C}[x, y]$, которая не конечно порождена.

Определение. Группа G называется *линейно редуктивной*, если каждое конечномерное представление V группы G вполне приводимо. Т.е. у любого подпредставления $V' \subset V$ существутет дополнительное подпредставление $V'' \subset V$, т.ч. $V = V' \oplus V''$. Представление V называется *неприводимым*, если $V \neq 0$ у него нет нетривиальных подпредставлений.

2. Пусть G линейно редуктивная группа. (а) Докажите, что любое представление группы G раскладывается в прямую сумму неприводимых. (б) Если V, W два неприводимых представления, докажите что пространство G-морфизмов $Hom_G(V, W)$ равно нулю, если $V \ncong W$, и равно $\mathbb{C}$, если $V \cong W$.

3. Докажите, что группа G линейно редуктивна тогда и только тогда, когда в любом ее конечномерном представлении V существует единственный проектор $\pi = \pi_V : V \to V^G$ на подпространство G-инвариантнов $V^G \subset V$, такой что π коммутирует с действием G. (Подсказка. Допустим, что для каждого V существует такой проектор π_V. (1) Докажите сначала, что V раскладывается в прямую сумму G-модулей $V = ker(\pi_V) \oplus V^G$, так, что

$$Hom_G(ker(\pi_V), V^G) = 0$$

(2) Покажите далее, что если $\alpha : V \to W$ морфизм представлений, то $\pi_W \cdot \alpha = \alpha \cdot \pi_V$. В частности, если α сюръективен, то $\alpha : V^G \to W^G$ тоже сюръективен. (3) Пусть теперь $V' \subset V$ подпредставление. Рассмотрите индуцированный морфизм векторных пространств $\beta : Hom_{\mathbb{C}}(V, V') \to Hom_{\mathbb{C}}(V', V')$. Введите на этих пространствах структуру представления группы G так, что β - морфизм представлений. Тогда элемент $id \in Hom_{\mathbb{C}}(V', V')^G$ равен $\beta(\pi)$ для некорого $\pi \in Hom_{\mathbb{C}}(V, V')^G$. Получаем разложение представления $V = V' \oplus ker(\pi)$.)

4. Докажите, что любая конечная группа линейно редуктивна.

5. Пусть $V = \mathbb{C}^n$ - перестановочное представление симметрической группы S_n. Рассмотрим V как представление альтернированной подгруппы $A_n \subset S_n$. Опишите кольцо инвариантов $\mathbb{C}[V]^{A_n} \subset \mathbb{C}[V]$. Подсказка: пусть $x_1, ..., x_n$ стандартные линейные функции на V. Докажите, что определитель Вандермонда

$$\Delta = \det \begin{bmatrix} 1 & 1 \\ x_1 & x_n \\ \vdots & \vdots \\ x_1^{n-1} & x_n^{n-1} \end{bmatrix} = \prod_{j<i}(x_i - x_j)$$

принадлежит кольцу $\mathbb{C}[V]^{A_n}$.

6. Пусть $V = \mathbb{C}^n$ - перестановочное представление симметрической группы S_n. Рассмотрим подпространство

$$H = \{\Sigma a_i e_i \mid \Sigma a_i = 0\}$$

Очевидно, что S_n сохраняет H. Опишите подалгебру инвариантов $\mathbb{C}[H]^{S_n} \subset \mathbb{C}[H]$.

7. Пусть p простое число, и G группа из p элементов. Пусть

$$V = \mathbb{C}[G] = \bigoplus_{g \in G} \mathbb{C}g$$

регулярное представление G. Используя формулу Мольена, вычислите ряд Пуанкаре $P_{\mathbb{C}[V]^G}(t)$.

8. Положим $V = \mathbb{C}^2$ и пусть $G = Q_8 \subset Gl_2(\mathbb{C})$ кватернионная группа из 8 элементов, порожденная матрицами

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

(1) Используя формулу Мольена, вычислите ряд Пуанкаре $P_{\mathbb{C}[V]^G}(t)$.

(2) Докажите, что подалгебра G-инвариантов $\mathbb{C}[V]^G \subset \mathbb{C}[V]$ порождена многочленами

$$x^4 + y^4, \quad x^2y^2, \quad x^5y - xy^5$$

9. Диэдральная группа $G = D_{2r} \subset Gl_2(\mathbb{R})$ порядка $2k$ порождена матрицами

$$R = \begin{pmatrix} \cos\frac{2\pi}{k} & -\sin\frac{2\pi}{k} \\ \sin\frac{2\pi}{k} & \cos\frac{2\pi}{k} \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Таким образом, G действует на пространстве $V = \mathbb{R}^2$.

(1) Используя формулу Мольена, докажите формулу для ряда Пуанкаре

$$P_{\mathbb{R}[V]^G}(1) = \frac{1}{(1-t^2)(1-t^k)}$$

(2) Докажите, что подалгебра инвариантов $\mathbb{R}[V]^G \subset \mathbb{C}[V] = \mathbb{R}[x, y]$ свободно порождена многочленами

$$x^2 + y^2, \quad x^k + y^k$$

В частности, алгебра $\mathbb{R}[V]^G$ - это кольцо многочленов от двух переменных.

2. Псевдоотражения и формула Мольена

Пусть V - представление размерности n конечной группы G. По формуле Мольена

$$P_{\mathbb{C}[V]^G} = \frac{1}{|G|}\sum_{g\in G}\frac{1}{\det(1-gt)}$$

$$= \frac{1}{|G|}\left(\frac{1}{\det(1-t)} + \sum_{g\neq 1}\frac{1}{\det(1-gt)}\right)$$

Таким образом, разложение рациональной функции $P_{\mathbb{C}[V]^G}$ в ряд Лорана в точке $t = 1$ имеет вид

$$P_{\mathbb{C}[V]^G} = \frac{\frac{1}{|G|}}{(1-t)^n} + \frac{*}{(1-t)^{n-1}} + \cdots \tag{1}$$

Знак * в формуле можно вычислить через число псевдоотражений, содержащихся в группе G.

Определение. Пусть даны конечномерное пространство V и конечная подгруппа $G \subset Gl(V)$. Элемент $g \in G$ называется *псевдоотражением*, если $g \neq 1$ и собственные значения g - это $\{1, 1, ..., 1, \lambda\}$ $(\lambda \neq 1)$.

1. Пусть группа G содержит $s(G)$ различных псевдоотражений. Докажите, что ряд Пуанкаре $P_{\mathbb{C}[V]^G}$ имеет вид

$$P_{\mathbb{C}[V]^G} = \frac{1}{|G|}\left(\frac{1}{(1-t)^n} + \frac{\frac{|s(G)|}{2}}{(1-t)^{n-1}} + \cdots\right)$$

2. Пусть $V \simeq \mathbb{C}^n$ и $G \subset Gl_n(\mathbb{C})$ конечная группа. Пусть даны однородные инвариантные многочлены $f_1, \cdots, f_n \in \mathbb{C}[V]^G$, $\deg(f_i) = d_i$ со следующими свойствами.

(i) $\prod_{i=1}^n d_i = |G|$,

(ii) $f_1, \cdots, f_n$ алгебраически независимы.
Докажите тогда, что $|s(G)| \geq \sum_{i=1}^n (d_i - 1)$.
Подсказка: Докажите сначала, что

$$P_{\mathbb{C}[f_1,\cdots f_n]}(t) = \frac{1}{d_1 \cdots d_n}\left(\frac{1}{(1-t)^n} + \frac{\Sigma(d_i-1)}{2(1-t)^{n-1}} + \cdots\right)$$

Теперь, из условия (i) следует, что

$$\Delta(t) := P_{\mathbb{C}[V]^G} - P_{\mathbb{C}[f_1,\cdots f_n]}(t)$$

имеет полюс порядка не больше $n-1$. Т.к. все коэффициенты степенного ряда $\Delta(t)$ не отрицательны, то значение функции $(1-t)^{n-1}\Delta(t)$ в $t=1$ также не отрицательно.

3. Выведите из предыдущей задачи следующее заключение: пусть дополнительно выполнено равенство

$$\mathbb{C}[V]^G = \mathbb{C}[f_1, ..., f_n]$$

Тогда имеем равенство

$$|s(G)| = \sum_{i=1}^n (d_i - 1)$$

3. Инварианты группы, порожденной псевдоотражениями

Теорема 3.1. *Пусть даны конечномерное пространство V и конечная подгруппа $G \subset Gl(V)$, $\mathbb{C}[V]^G \subset \mathbb{C}[V]$ - подкольцо инвариантов. Следующие условия эквивалентны:*

(1) G порождена преводотражениями.

(2) $\mathbb{C}[V]$ - свободный градуированный $\mathbb{C}[V]^G$ - модуль.

(3) Алгебра $\mathbb{C}[V]^G$ порождена однородными элементами, которые алгебраически независимы.

Доказательство этой теоремы будет получено в серии задач. Обозначим алгебру $\mathbb{C}[V]$ через S.

1. Пусть $R \subset S$ градуированная подалгебра, $R_+ \subset R$ - однородный идеал в R состоящий из всех элементов положительной степени. Рассмотрим однородный идеал $I := R_+S \subset S$. Пусть $\{s_\alpha\}$ множество однородных елементов в S такое, что классы $\{s_\alpha + I\}$ образуют $\mathbb{C}$-базис пространства S/I. Тогда множество $\{s_\alpha\}$ порождает S как R-модуль.

Псевдодифференцирования Шевалле. В одной из следующих задач нам понадобится понятие (псевдо)дифференцирования, связанного с псевдоотражением. А именно, пусть $s \in Gl(V)$ псевдоотражение с собственными значениями $(1, \cdots, 1, \lambda_s)$. Тогда $H_s := \ker(s-1) \subset V$ - это гиперплоскость в V; выберем $0 \neq x_s \in V$, т.ч. $sx_s = \lambda_s x_s$. Тогда для любого $v \in V$ выполнено

$$s(v) = v + l_s(v)x_s$$

где $l_s : V \to \mathbb{C}$ - линейный функционал, т.ч. $H_s = \ker l_s$ и $l_s(x_s) = \lambda_s x_s$. Рассмотрим оператор $s-1$ на V и на S. Тогда $(s-1)H_s = 0$ and $(s-1)x_s = \lambda_s x_s - x_s \neq 0$. Если $f \in \mathbb{C}[V]$, тогда при $u \in H_s$

$$(sf - f)(u) = f(s^{-1}u) - f(u) = f(u) - f(u) = 0$$

и, значит, l_s делит $sf - f$ в кольце $\mathbb{C}[V]$. Определим $\Delta_s(f)$ формулой

$$sf - f = \Delta_s(f)l_s$$

Заметим, что Δ_s зависит от выбора x_s и l_x, поэтому корректно определено только с точностью до умножения на скаляр.

2. Проверить следующие свойства псевдодифференцирования Δ_s.
(а) $\Delta_s : S_d \to S_{d-1}$, т.е. Δ_s понижает степень многочлена на 1.
(б) Для любых $f, h \in S$ выполняется равенство:

$$\Delta_s(fh) = f\Delta_s(h) + \Delta_s(f)h + l_s\Delta_s(f)\Delta_s(h)$$

(в) Функция $f \in S$ сохраняется псевдоотражением s тогда и только тогда, когда $\Delta_s(f) = 0$.
(г) Отображение $\Delta_s : S \to S$ линейно над подкольцом $S^G \subset S$.

3. Пусть группа G порождена псевдоотражениями. В задаче 1 возьмем $R = S^G$. Пусть $x_i \in S^G$, $y_i \in S$ $(1 \leq i \leq m)$ однородные элементы и выполнено соотношение

$$x_1y_1 + ... + x_my_m = 0 \qquad (2)$$

Если при этом $x_1 \in S^Gx_2 + ... + S^Gx_m$, то $y_1 \in I$.
Подсказка. Использовать индукцию по степени многочлена y_1 с применением операторов Δ_s к уравнению (2) для всех псевдоотражений $s \in G$.

4. В обозначениях предыдущей задачи пусть $y_1, ..., y_m$ - однородные элементы кольца S такие, что их классы по модулю идеала I образуют $\mathbb{C}$-базис пространства S/I. Тогда $y_1, ..., y_m$ линейно независимы над S^G.

5. Вывести из предыдущих задач импликацию (1) $\Rightarrow$ (2) теоремы.

Импликация (2) $\Rightarrow$ (3) следует из следующей задачи.

6. Пусть дана градуированная подалгебра $R \subset S$, такая, что S - конечно порожденный **свободный** градуированный R-модуль. Тогда R - это градуированное кольцо многочленов от n переменных.
Подсказка. Сначала докажите, что алгебра R конечно порождена. Далее, пусть $R_+ \subset R$ - максимальный однородный идеал в R с минимальным набором однородных образующих $\{f_1, \cdots, f_m\}$. Тогда $\{f_1, \cdots, f_m\}$ порождают алгебру R. Главный шаг: доказать, что $\{f_1, \cdots, f_m\}$ алгебраически независимы; это можно будет разобрать в классе.

Доказательство импликации (3) $\Rightarrow$ (1):

Допустим, что $S^G = \mathbb{C}[f_1, \cdots, f_n]$, где f_i однородный многочлен степени d_i. Т.к. степень трансцендентности поля частных кольца S^G над $\mathbb{C}$ равна n, то $\{f_1, \cdots, f_n\}$ алгебраически независимы. Значит, ряд Пуанкаре равен

$$P_{S^G}(t) = \prod_{i=1}^{n}(1 - t^{d_i})^{-1}$$

Можно считать, что $G \neq 1$ и, значит не все d_i равны 1.

7. Докажите, что $|G| = d_1 \cdots d_n$.
Подсказка. Вычислите значение $(1-t)^n P_{S^G}(t)$ в $t = 1$ и воспользуйтесь формулой (1).

Значит, можно воспользоваться формулой

$$|s(G)| = \sum_{i=1}^{n}(d_i - 1)$$

из задачи 3 в предыдущем разделе и заключить, что группа G содержит псевдоотражения. Пусть $H \subset G$ подгруппа, порожденная всеми псевдоотражениями в G. Тогда по уже доказанной импликации (1) $\Rightarrow$ (3) в теореме получаем, что $S^H = \mathbb{C}[h_1, \cdots h_n]$, где $\{h_1, \cdots, h_n\}$ однородные алгебраически независимые многочлены, степеней $e_1, \cdots, e_n$ соответственно. Можно считать, что

$$d_1 \leq d_2 \leq \cdots \leq d_n, \quad e_1 \leq e_2 \leq \cdots \leq e_n$$

Из задачи 7 следует, что

$$\prod_{i=1}^{n} e_i = |H| \leq |G| = \prod_{i=1}^{n} d_i$$

Поэтому достаточно доказать, что $e_i = d_i$ для всех i.

Снова по задаче 3 из предыдущего раздела заключаем, что

$$|s(H)| = \sum_{i=1}^{n}(e_i - 1)$$

Но т.к. $s(H) = s(G)$, то $\sum e_i = \sum d_i$. Поэтому достаточно показать, что $e_i \leq d_i$ для всех i.

Имеется включение $S^G \subset S^H$. Поэтому для каждого $i = 1, \cdots, n$ существует единственный многочлен $P_i \in \mathbb{C}[T_1, \cdots, T_n]$, т.ч. $f_i = P_i(h_1, \cdots, h_n)$. Зафиксируем индекс i. Т.к. фкнкции $f_1, \cdots f_i$ алгебраически независимы, то в многочлены $P_1, \cdots, P_i$ не могут входить только переменные $T_1, \cdots, T_{i-1}$. значит при некоторых $j \leq i$ и $l \geq i$ переменная T_l входит в многочлен P_j. Отсюда следует искомое неравенство

$$d_i \geq d_l \geq e_j \geq e_i$$

Теорема полностью доказана.

В следующей задаче подводятся итоги нашего изучения инвариатнов конечных групп, порожденных псевдоотражениями.

8. Пусть $V = \mathbb{C}^n$ и $G \subset Gl(V)$ конечная группа, порожденная псевдоотражениями, $S = \mathbb{C}[V]$. Тогда алгебра инвариантов $S^G \subset S$ порождена n алгебраически независимыми однородными многочленами $\{f_1, \cdots, f_n\}$. Если $\deg f_i = d_i$, то

$$|G| = \prod d_i$$

и $\sum(d_i - 1) = s(G)$ - число псевдоотражений в группе G.

II. Инварианты алгебраических групп.

1. Пусть $\mathbf{O}_n \subset Gl_n(\mathbb{C})$ ортогональная группа, действующая на пространстве $V = \mathbb{C}^n$. По определению, группа $\mathbf{O}_n$ сохраняет многочлен

$$D = x_1^2 + \cdots + x_n^2 \in \mathbb{C}[V]$$

Докажите следующие утверждения: (а) каждая гиперповерхность ненулевого уровня $\{D = c \neq 0\} \subset V$ - это одна $\mathbf{O}_n$-орбита. (Подсказка. Воспользуйтесь следующей теоремой Витта: Пусть V векторное пространство с невырожденной симметрической формой, и пусть даны два подпространства $L, L' \subset V$. Тогда любая изометрия $L \xrightarrow{\sim} L'$ продолжается до изометрии $V \xrightarrow{\sim} V$.) (б) алгебра инвариантов $\mathbb{C}[V]^{\mathbf{O}_n}$ это $\mathbb{C}[D]$ - алгебра многочленов от одной переменной D; (в) гиперповерхность нулевого уровня $\{D = 0\} \subset V$ (нуль-конус) состоит из двух $\mathbf{O}_n$-орбит.

2. (а) Пусть группа $Gl_n(\mathbb{C})$ действует на пространстве W симметрических $n \times n$ матриц: $g \cdot A := gAg^t$. Докажите, что у этого действия конечное число орбит. Опишите орбиты. Подажите, что стабилизатор единичной матрицы - это ортогональная подгруппа $\mathbf{O}_n \subset Gl_n$. (б) Заменим группу Gl_n на Sl_n. Проверьте, что тогда функция $det : W \to \mathbb{C}$ инвариантна, и $\mathbb{C}[W]^{Sl_n} = \mathbb{C}[det]$. (Подсказка Докажите, что для любой $A \in W$, $det(A) = \delta \neq 0$, орбита A содержит дигональную матрицу с собственными значениями $(\delta, 1, \cdots 1)$.)

3. Инварианты системы векторов. Пусть группа Sl_n действует обычным образом на $V = \mathbb{C}^n$ и диагональным образом на прямой сумме $V^{\oplus m} = V_m$. Будем изображать векторы из пространства V столбцами, а элементы из V_m - $n \times m$-матрицами M. Нас интересует алгебра инвариантов $\mathbb{C}[V_m]^{Sl_n}$.
$m < n$. Докажите, что $\mathbb{C}[V_m]^{Sl_n} = \mathbb{C}$.
$m = n$. Докажите, что $\mathbb{C}[V_m]^{Sl_n} = \mathbb{C}[det]$, где $det : V_n \to \mathbb{C}$ - определитель. (Подсказка. Пусть $e_1, \cdots, e_n$ - базис в V. Покажите, что орбита любой матрицы $M \in V_n$, $det(M) \neq 0$ пересекает прямую $L = \{(te_1, e_2, \cdots, e_n) \mid t \in \mathbb{C}\}$.)
$m > n$. Зафиксируем индексы $0 \leq i_1 < \cdots < i_n \leq m$. Если $M \in V_m$, обозначим через $det_{i_1,\cdots,i_n}(M)$ определитель квадратной матрицы, состоящей из столбцов в M с номерами $i_1, \cdots, i_n$. Докажите, что всевозможные функции $det_{i_1,\cdots,i_n}$ порождают алгебру инвариантов $\mathbb{C}[V_m]^{Sl_n}$, т.е. $\mathbb{C}[V_m]^{Sl_n} = \mathbb{C}[det_{i_1,\cdots,i_n}]_{i_1,\ldots,i_n}$. (Обозначит кольцо $\mathbb{C}[det_{i_1,\cdots,i_n}]_{i_1,\ldots,i_n}$ через D.) (Подсказка. Группа Gl_m действует на

пространстве V_m умножением справа:

$$A \cdot M := MA^t, \quad A \in Gl_m$$

Это действие коммутирует с действием Sl_n, поэтому Gl_m действует на кольце инвариантов $\mathbb{C}[V_m]^{Sl_n}$. Легко видеть, что это действие Gl_m сохраняет подкольцо $D \subset \mathbb{C}[V_m]^{Sl_n}$. Пусть $U_m \subset Gl_m$ максимальная унипотентная подгруппа, состоящая из верхнетреугольных матриц с единицами на диагонали. Из общей теории представлений группы Gl_m следует (можно будет обсудить в классе), что для доказательства равенства $D = \mathbb{C}[V_m]^{Sl_n}$ достаточно показать, что любая функция $f \in \mathbb{C}[V_m]^{Sl_n}$, инвариантная относительно U_m, принадлежит D.

Группа U_m действует на матрицу $M = (v_1, \cdots v_m)$, прибавляя к каждому из векторов $(v_1, \cdots, v_m)$ произвольную линейную комбинацию предыдущих. Отсюда следует, что любая U_m-инвариантная функция на V_m определяется своими значениями на матрицах $M = (v_1, \cdots, v_n, 0 \cdots, 0)$. Поэтому любая $f \in \mathbb{C}[V_m]^{Sl_n}$, инвариантная относительно U_m, принадлежит $\mathbb{C}[V_n]^{Sl_n}$, и мы уже знаем, что $\mathbb{C}[V_n]^{Sl_n} = \mathbb{C}[det_{1,2,\cdots n}] \subset B$.)

Вывести из доказанного, что нуль-конус в V_m состоит из матриц ранга $< n$.

4. Рассмотрим проективную прямую $\mathbf{P}^1$ как проективизацию плоскости $\mathbb{C}^2$. Т.е. точка в $\mathbf{P}^1$ определяется ненулевым вектором $v \in \mathbb{C}^2$, и при этом пропорциональные вектора соответствуют одной и той же точке в $\mathbf{P}^1$. Известно, что группа автоморфизмов $\mathbf{P}^1$ - это PGl_2, т.е. фактор Gl_2 по своему центру. Заметим, что гомоморфизм групп $Sl_2 \to PGl_2$ - это двулистное накрытие. (а) Докажите, что действие PGl_2 на $\mathbf{P}^1$ 3-транзитивно, т.е. PGl_2 действует транзитивно на тройках упорядоченных точек в $\mathbf{P}^1$.

(б) Пусть даны 4 различные точки (p_1, p_2, p_3, p_4) на $\mathbf{P}^1$. Выберем подъем $v_i \in \mathbb{C}^2$ точки p_i и рассмотрим 2×4 матрицу $M = [v_1, v_2, v_3, v_4]$. Двойное соотношение $[p_1, p_2, p_3, p_4]$ определяется как величина

$$[p_1, p_2, p_3, p_4] = det_{12}(M) det_{23}(M)^{-1} det_{24}(M) det_{14}(M)^{-1}$$

где функции det_{ij} были определены в предыдущей задаче. (Двойное соотношение может принимать значение ∞.) Докажите, что двойное соотношение корректно определено, т.е. не зависит от выбора подъема точек p_i.

(в) Докажите, что 2 упорядоченных набора из 4 точек на $\mathbf{P}^1$ лежат в одной PGl_2-орбите, тогда и только тогда, когда их двойные соотношения совпадают.

5. Инварианты эллиптических кривых. Известно, что любую эллиптическую кривую (т.е. гладкую проективную кривую рода один) можно представить в виде двулистного накрытия $\mathbf{P}^1$, разветвленного в четырех точках $\{p_1, p_2, p_3, p_4\}$. При этом две эллиптические кривые изоморфны тогда и только тогда, когда соответствующие (неупорядочные) наборы точек лежат в одной PGl_2-орбите. Из предыдущей задачи мы знаем, что двойное соотношение ρ - единственный PGl_2-инвариант упорядочного набора из четырех точек. (а) Проверьте, что при всевозможных перестановках точек оно принимает значения

$$\rho,\ \rho^{-1},\ 1-\rho,\ 1-\rho^{-1},\ (1-\rho)^{-1},\ (1-\rho^{-1})^{-1}$$

(б) Докажите, что j-инвариант

$$j = \frac{(\rho^2-\rho+1)^3}{\rho^2(\rho-1)^2}$$

классифицирует эллиптические кривые, т.е. такие кривые E_1, E_2 изоморфны, тогда и только тогда, когда $j(E_1) = j(E_2)$.