Лекция 4. Гипотеза Морделла, Лемма Рота.

0.8 Гипотеза Морделла

Гипотеза 0.31 *Число рациональных точек на кривой рода* ≤ 2 *конечно.*

В этой части мы обсудим лемму Зигеля и лемму Рота, доказательство которой обобщается в некотором смысле для гипотезы Морделла.

0.9 Лемма Зигеля и Рота

Обозначения

Класс эквивалентности абсолютных значений поля k называется местом числового поля k.

Для числового поля k, множество M_k — множество всех вложений k, это объединение множества вещественных, комплексных и неархимедовых мест. Вещественные и комплексные места находятся во взаимно-однозначном соответствии с соответствующими вложениями в R и парами $(\sigma, \bar{\sigma})$ вложений в C. Множество неархимедовых мест находятся в соответствии с множеством ненулевых простых идеалов в кольце целых $\mathcal{O}_K$ поля k. Для каждого $v \in M_k$ мы определяем норму:

$$||\cdot||_v = |\sigma(x)|, |\sigma(x)^2|, x^{-ef},$$

где первая норма по вещественным вложениям, вторая — по комплексным, третье, если v $\mathfrak{p}$-адично, где $\mathfrak{p}$ разветлено с порядком e над рациональными простым p и f степень расширения поля частных.

Заметим, что $||\cdot||_v$ называются нормами, а не абсолютными значениями, так как оно не удовлетворяет неравенству треугольника, когда v комплексно.

В таком определении у нас есть формула произведения

$$\prod_{v \in M_k} ||x||_v = 1$$

для всех x.

И пусть $N_v = 1, 2$ или 0 в зависимости от того, является v вещественным, комплексным, или неархимедовым.

Тогда

$$\sum_{v \in M_k} N_v = [k : Q]$$

и

$$||a_1 + ... + a_n||_v \leq n^{N_v} max||a_1||_v, ..., ||a_n||_v$$

для всех $n \in N$ и $a_1, ..., a_k \in k$.

Наконец, снова будем рассматривать логарифмические высоты, в частности, высота в точке $P \in P^n$ с однородными координатами $[x_0 : ... : x_n]$ равна

$$h(P) = \frac{1}{[k:Q]} \sum_{v \in M-k} logmax||x_0||_v, ..., ||x_n||_v$$

Лемма Зигеля

Лемма 0.32 *(Зигель). Пусть $A \quad M \times N$ матрица с $M < N$ и целыми коэффициентами, имеющими абсолютное значение не более Q. Тогда существует ненулевой вектор $x = (x_1, ..., x_n) \in Z^N$ с $Ax = 0$, такой что*

$$|x_i| \leq [(NQ)^{N/(M-N)}] =: Z, \quad i = 1, ..., N$$

Доказательство:

Число целых точек в прямоугольнике $0 \leq x_i \leq Z$ равно $(Z+1)N$. С другой стороны, для всех $j = 1, ..., N$ и для всех таких x, j-ая координата y_j вектора $y = Ax$ лежит в интервале $[-n_j QZ, (N - n_j)QZ]$, где $n_j \quad$ это число отрицательных чисел в j-ой строке матрицы A. Значит существует максимум

$$(NQZ + 1)^M < (Z + 1)^N$$

возможных значений Ax. Поэтому существует вектора $x_1 \neq x_2$ с коэффициентами из нужного диапазона и такие что $Ax_1 = Ax_2$. Тогда, легко видеть, что $x = x_1 - x_2$ удовлетворяет условиям леммы.

Напомним, кольцо целых числового поля $K \quad$ это кольцо целых элементов, содержащихся в K. При этом целым называется корень приведённого многочлена с целыми коэффициентами.

Лемма Зигеля арифметико-геометрическая, все результаты могут быть сделаны в контексте кольца R_S, которое получается локализацией кольца R целых поля K по конечному множеству мест S поля K.

Лемма Рота

Вспомним классическую теорему Лиувилля.

Теорема 0.33 *(Liouville) Пусть $\alpha \in R$ алгебраическое иррациональное число степени d над полем Q. Тогда существует эффективно вычислимая константа $c(\alpha)$, такая что для всех $p/q \in Q$*

$$|p/q - \alpha| > c/q^d$$

Доказательство проходит в несколько шагов. В начале выбирается многочлен $f(x)$, который зануляется в α. Этот многочлен единственен, если мы потребуем его неприводимости над целыми числами (с положительным старшим коэффициентом).

Далее, $f(p/q) \neq 0$. Более того, $f(p/q) \geq 1/q^d$

Завершается доказательство тем, что можно показать, что

$$f(p/q) \leq b(\alpha)|p/q - \alpha|$$

для явной константы $b(\alpha)$, заданной условием $|p/q - \alpha| \leq 1$.

Константа из теоремы Лиувилля это $max(1, 1/2b(\alpha))$

Теорема 0.34 *Для заданного алгебраического числа $\alpha \in \bar{Q}$, вещественного C и $\epsilon > 0$ есть только конечное число пар взаимно простых чисел, таких что*

$$|\frac{p}{q} - \alpha| \leq \frac{C}{|q|^{2+\epsilon}}$$

Доказательство:

Начнём доказательство леммы Рота. Помимо леммы Зигеля нам понадобится ещё несколько вспомогательных утверждений.

Следующее утверждение говорит, что большинство значений $i_1/d_1 + \Delta\Delta\Delta + i_n/d_n$ с $0 \leq i_h \leq d_h (h = 1, ..., m)$ близки к $n/2$.

Лемма 0.35 *Пусть $d_1, ..., d_n$ целые и не менее чем 1 и пусть $\epsilon > 0$. Число множеств целых $(i_1, ..., i_n)$, которые удовлетворяют $0 \leq i_j \leq d_j$ и*

$$|\sum_{h=1}^{n} \frac{i_h}{d_h} - \frac{n}{2}| \geq \epsilon n$$

не более чем

$(d_1 + 1)...(d_n + 1)/(4n\epsilon^2)$.

Доказательство леммы:

Рассмотрим величины i_j как независимые случайные величины, такие что i_j равномерно распределены на $0, ..., d_h$.

Определем случайную величину $X = \sum_{h=1}^{n} i_h/d_h$.

Тогда ожидание X равно $\mu = n/2$ и вариация

$$\sigma^2 = Var(i_1/d_1) + ... + Var(i_n/d_n)$$

.

Мы имеем

$$Var(i_h/d_h) = \sum_{i_h=0}^{d_h} (i_h/d_h - 1/2)^2/(d_h + 1) = \frac{2d_h + 1}{6d_h} - 1/4 \leq 1/4$$

Значит, $\sigma^2 \leq n/4$. По колмогоровскому обобщению неравенства Чебышёва имеем

$$Prob(|X - \mu| \geq c) \leq \sigma^2/c^2.$$

Значит,

$$Prob(|X - n/2| \geq \epsilon m) \leq \frac{1}{4m\epsilon^2}$$

Лемма доказана.

Теперь хочется определить порядок зануления многочлена в данной точке, часто смотрят на наименьшее $(i_1 + ... + i_n)$, когда соответствующая частная производная не обращается в ноль, но нам необходимо смотреть на многочлены с разными степенями по переменным, поэтому нужно ввести степени. Так Рот определил индекс в данной точке с весом.

Определение 0.36 *Для многочлена $P(X_1, ..., X_n) \in Z[X_1, ..., X_n]$ и $i = (i_1, ...i_n) \in Z^n_{\geq 0}$ зададим*

$$P_i(X_1, ..., X_n) = \frac{1}{i_1!...i_n!} \frac{\partial^{i_1}}{\partial X_1^{i_1}} \cdots \frac{\partial^{i_n}}{\partial X_1^{i_n}} P(X)$$

$$= \sum_{l_h \geq 0} \prod_h C_{i_h}^{j_h} C(j_1, ..., j_n) \prod_h X_h^{j_h - i_h}$$

Пусть $\alpha_1, ..., \alpha_n \in C$ и $d_1, ..., d_n$ положительные целые. Тогда индекс многочлена P в $\alpha = (\alpha_1, ..., \alpha_n)$ с весами $d_1, ..., d_n$ это

$$t(P, \alpha, d_1, ..., d_n) = min \sum_{i=1}^{n} \frac{l_i}{d_i} | P_i(\alpha) \neq 0$$

Заметим, что $t(PQ) = t(P) + t(Q)$ и $t(P + Q) \geq min(t(P), t(Q))$.

Теперь покажем, как строить многочлен с большим индексом в заданной точке. Для многочлена P обозначим максимум модулей коэффициентов за $|P|$.

Лемма 0.37 *(теорема об индексе). Предположим, что α алгебраическое целое степени $d \geq 2$. Пусть $\epsilon > 0$ и пусть n целое с условием $n \geq d/2\epsilon^2$. Пусть $d_1, ..., d_n$ положительные целые. Тогда есть многочлен P, не равный тождественно нулю, что*

(i) $deg(P) \leq d_i$ *в* $X - i$

(ii)

$$t(P, (\alpha, ..., \alpha), d_1, ..., d_n) \geq n(1 - \epsilon)/2$$

(iii) $|P| \leq C_1^{d_1 + ... + d_n}$

Запишем $P = \sum_{j_1=0}^{d_1} ... \sum_{j_n=0}^{d_n} z(j_1,..,j_n) X_1^{j_1} \cdot \cdot \cdot X_n^{j_n}$, где z целые, которые должны быть определены так, чтобы (ii) выполнялось, т.е. $P_i(\alpha) = 0$ для $i_1/d_1 + ... + i_n/d_n \leq b(1-\epsilon)/2$.

Соберём все эти условия в одно

$$A_0 z + \alpha A_1 z + ... + \alpha^{d_1+d_n} A_{d_1+...+d_n} z = 0,$$

где A_i это $M \times N$ матрицы с целыми коэффициентами и условием $|A_i| \leq 4^{d_1+...+d_n}$, где $N = (d_1+1)...(d_n+1)$ и M число наборов i, что $i_1/d_1 + ... + i_n/d_n \leq n(1-\epsilon)/2$.

Так как α алгебраическое число степени d, поэтому есть

$$B_0 z + ... + \alpha^{d-1} B_{b-1} z = 0,$$

где B_i $M \times N$ матрицы с целыми коэффициентами и условием $|A_i| \leq C_2^{d_1+...+d_n}$.

Так как $\alpha, ..., \alpha^{d-1}$ линейно независимы над Z имеем $B_0 z = 0, ..., B_{d-1} z = 0$. Значит, $Bz = 0$, где B матрица размера $dM \times N$ с $|B| \leq C_2^{d_1+...+d_n}$

По комбинаторной лемме выше

$$M \leq \frac{(d_1+1)...(d_h+1}{4m\epsilon^2} = \frac{N}{4m\epsilon^2} \leq \frac{N}{2d}.$$

Тогда по лемме Зигеля существует ненулевой целый вектор z, такой что $Bz = 0$ и

$$|z| \leq (N|B|)^{dM/(N-dM)} \leq N|B| \leq C_3^{d_1+...+d_n}.$$

Константы C_1, C_2, C_3 зависят только от α. Лемма доказана.

Следующая лемма даёт критерий достаточности для многочлена, чтобы он имел небольшой индекс по отношени. к вектору $(p_1/q_1, ..., p_n/q_n)$ и $(d_1, ..., d_n)$.

Лемма 0.38 *(Рот)*

Пусть $n \geq 1$ положительное целое и $\epsilon > 0$. Тогда существует число $C_4 = C_4(m, \epsilon) > 1$ со следующим свойством:

пусть d_j $(j = 1, ..., n)$ целые и $d_h \geq C_4 d_{h+1}, h = 1, ..., n-1$. Пусть $(p_1, q_1), ..., (p_n, q_n)$ пары взаимно простых чисел с $q_h^{d_h} \geq q_1^{d_1}$ и $q_h \geq 2^{2mC_4}, h = 1, ..., n$. Пусть $P(X_1, .., X_n)$ не равен тождественно нулю и степень по каждой X_h не более d_h с условием

$$|P|^{C_4} \leq q_1^{d_1}$$

Тогда

$$t = t(P, (p_1/q_1, ..., p_n/q_n), d_1, .., d_n) \leq \epsilon$$

Доказательство этой технической леммы мы пропустим, оно есть в книжках, например, Лэнга.

Наконец-то мы можем приступить к доказательству непосредственно основного утверждения. Допустим, от противного, что неравенство

$$|\frac{p}{q} - \alpha| \leq \frac{C}{|q|^{2+\delta}}$$

выполнено для бесконечного числа пар (p, q). Без потери общности предположим, что α алгебраическое целое степени $d \geq 2$ с $;|\alpha| < 1$. Также предположим, что $0 < \delta < 1/2$.

Шаг 1. Выбор подходящих точек p_h/q_h.

Пусть P многочлен построенный в теореме об индексе для $\alpha, \epsilon = \delta/2, n > d/2\epsilon^2$ и произвольных $d_1, ..., d_n$. Тогда P имеет индекс $> n(1-\epsilon)/2$ в точке $(\alpha, ..., \alpha)$ и с весом $(d_1, ..., d_n)$.

Для начала выберем решения так:

(1) Выберем (p_1, q_1) так чтобы

$$q_1 > max((6C_1)^{1/\epsilon}, C_1^m, 2^{2mC_4}),$$

где C_1 константа, которая возникала в теореме об индексе, а C_4 в лемме Рота (промежуточной).

(2) Теперь выберем $(p_2, q_2), ...(p_n, q_n)$ такие что

$$q_{h+1} > q_h^{(1+\epsilon)C_4}, 1 \leq h \leq n-1$$

(3) Выберем теперь d_1 так что

$$q_1^{\epsilon d_1} \geq q_h$$

(4) для номеров 2,..., n выберем

$$q_1^{d_1} \leq q_h^{d_h} < q_1^{d_1(1+\epsilon)}$$

это возможно так как $q_1^{\epsilon d_1} \geq q_n \geq q_h$

Простая проверка показывает, что промежуточная лемма Рота в этих условиях выполнена.

Шаг 2. Воспользуемся разложением Тейлора и покажем, что $P(p_1/q_1, ..., p_n/q_n) = 0$.

На самом деле, можно доказать больший результат, а именно, что индекс многочлена больше ϵ в точке $(p_1/q_1, ..., p_n/q_n)$ и $(d_1, ..., d_n)$. Для этого докажем, что для каждого i с

$$i_1/d_1 + ... + i_n/d_n < \epsilon$$

имеем $P_i(p_1/q_1, ..., p_n/q_n) = 0$.

Заметим, что

$$P_i(\alpha) = \sum_j P_j(0) C_{i_1}^{j_1} ... C_{i_n}^{j_n} \alpha^{j_1 - i_1} ... \alpha^{j_n - i_n},$$

откуда, используя $|\alpha| < 1$

$$|P_i(\alpha)| \leq |P| max_j C_{i_1}^{j_1} ... C_{i_n} \leq (2C_1)^{d_1 + ... + d_n} \leq (2C_1)^{nd_1},$$

где максимум продолжается на те j с $j_h \leq d_h$.
Разложим $P_i(X)$ в ряд Тейлора вокруг $(\alpha, ..., \alpha)$,

$$P_i(X) = \sum_j P_j(\alpha) C_{i_1}^{j_1} ... C_{i_n}^{j_n} (X_1 - \alpha)^{j_1 - i_1} ... (X_n - \alpha)^{j_n - i_n}$$

по конструкции P (условие (ii) в теореме об индексе)

$$t(P, (\alpha, .., \alpha), d_1, .., d_n) \geq n(1 - \epsilon)/2$$

Значит, $P_j(\alpha) = 0$, если $j_1/d_1 + ... j_n/d_n \leq n(1 - \epsilon)/2$, т.е. безусловно, если $(j_1 - i_1)/d_1 + ... + (j_n - i_n)/d_n \leq n(1 - 3\epsilon)/2$. Более того,

$$\sum_j P_j(\alpha) C_{i_1}^{j_1} ... C_{i_n}^{j_n} \leq (2C_1)^{nd_1} \sum_j 2^{j_1 + ... + j_n} \leq (6C_1)^{nd_1}$$

Значит, для

$$F(X) := P_i(X) = \sum_{(l) \geq 0} F^{(l)}(\alpha, ..., \alpha)(X - \alpha)^{(l)}$$

мы получаем, что все члены ноль, кроме тех, что отвечают $(j_1 - i_1)/d_1 + ... + (j_n - i_n)/d_n \geq n(1 - 3\epsilon)/2$ и

$$\sum_j |F^{(l)}(\alpha, ..., \alpha)| \leq (6C_1)^{nd_1}$$

Будем ставить (*), если выполнено $(j_1 - i_1)/d_1 + ... + (j_n - i_n)/d_n \geq n(1 - 3\epsilon)/2$
Из этого следует, что

$$\log |F(p_1/q_1, ..., p_n/q_n)| \leq (6C_1)^{nd_1} max^*_{(l)} \prod_h |\frac{p_h}{q_h} - \alpha|^{l_h}$$

$$\leq (6C_1)^{nd_1} max^*_l (\prod q_h^{l_h/d_h})^{-2-\delta} \leq (6C_1)^{nd_1} max^*_l (q_1^{d_1})^{(l_1/d_1 + ... + l_n/d_n)(-2-\delta)}$$

$$\leq (q_1)^{\epsilon n d_1} (q_1^{d_1})^{-n(1-3\epsilon)(1+\delta/2)} \leq (q_1^{d_1} ... q_h^{d_h})^{(\epsilon - n(1-3\epsilon)(1+\delta/2)/(1+\epsilon)} < (q_1^{d_1} ... q_h^{d_h})^{-1}.$$

С другой стороны, $|F(p_1/q_1, ..., p_n/q_n)|$ рациональное число с определителем, который делит $q_1^{d_1} ... q_h^{d_h}$. Таким образом,

$$P_i(p_1/q_1, ..., p_n/q_n) = F(p_1/q_1, ..., p_n/q_n) = 0$$

Шаг 3. Заключение шага 2 противоречит промежуточной лемме Рота. Так что это доказательство леммы Рота. □