SPRING 2006 Analysis

Russian Language EXAM

2. РЕГУЛЯРНЫЕ ЗНАЧЕНИЯ

Литература: Дж. Милнор, Топология с дифференциальной точки зрения, в книге: Дж. Милнор и А. Уоллес, Дифференциальная топология, начальный курс, «Мир», М., 1972, стр. 177-267.

Р. Нарасимхан, Анализ на действительных и комплексных многообразиях, «Мир», М., 1971.

С. Стернберг, Лекции по дифференциальной геометрии, «Мир», М., 1970.

Цель настоящей главы — доказать следующую теорему:

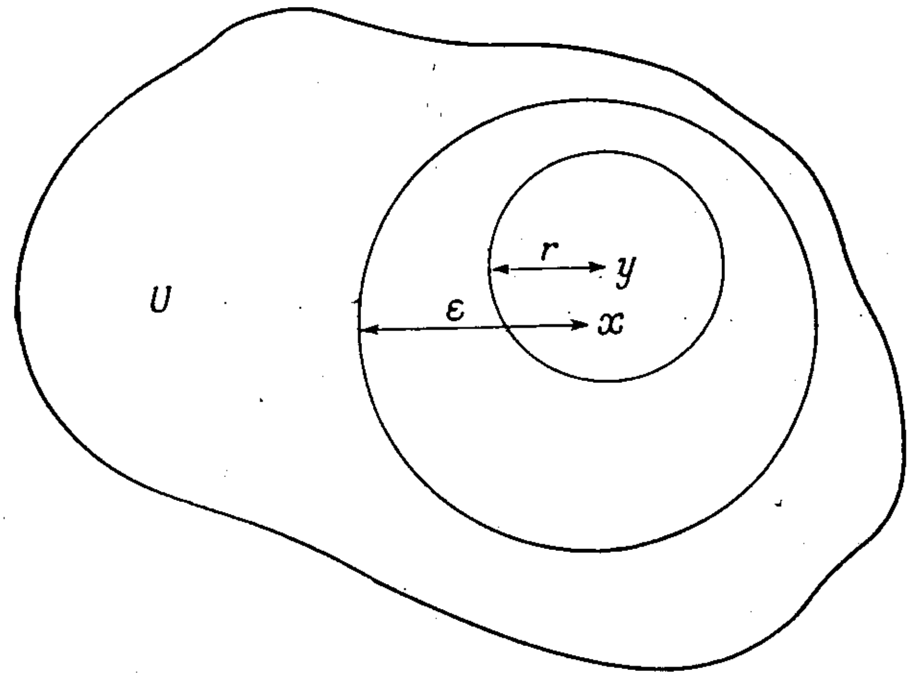
2.1. Теорема Сарда. *Мера Лебега множества критических значений дифференцируемого отображения равна нулю.*

Определение множества нулевой меры Лебега будет дано ниже. А сейчас выведем некоторые следствия из сформулированной теоремы. Пусть $f\colon \mathbf{R}^n \to \mathbf{R}^m$ — дифференцируемое отображение. Тогда для почти всех точек $b \in \mathbf{R}^m$ (т. е. всюду, кроме множества меры нуль) верно следующее утверждение: множество $f^{-1}\{b\} \subset \mathbf{R}^n$ — дифференцируемое подмногообразие размерности $n-m$. Иными словами:

При заданном $f = (f_1, \ldots, f_m)$ для почти всех $b_i \in \mathbf{R}$, $1 \leqslant i \leqslant m$, система нелинейных уравнений $f_i(x) = b_i$, $x \in \mathbf{R}^n$, $1 \leqslant i \leqslant m$, имеет в качестве множества решений $(n-m)$-мерное многообразие.

2.2. Вспомогательное утверждение. Пусть $\{K_n\}_{n \in \mathbf{N}}$ — множество всех шаров в $\mathbf{R}^m$, имеющих рациональный радиус и рациональные координаты центра (таких шаров счетное число!). Тогда *если $U \subset \mathbf{R}^m$ — открытое подмножество, то $U = \bigcup_{i \in T} K_i$ для некоторого подмножества $T \subset \mathbf{N}$.*

Доказательство. Пусть $x \in U$ и $\varepsilon > 0$ столь мало, что ε-окрестность точки x содержится в U. Возьмем шар K_l с рациональным центром y, удовлетворяющим условию $|x-y|<\varepsilon/3$, и рациональным радиусом r, удовлетворяющим условию $|x-y|<r<2\varepsilon/3$. ∎



Вот следствие из этого утверждения.

2.3. Замечание. *Пусть X — произвольное подмножество в $\mathbb{R}^n$ и $\{U_\lambda\}_{\lambda\in\Lambda}$ — семейство открытых множеств в $\mathbb{R}^n$, такое, что $X\subset\bigcup\limits_{\lambda\in\Lambda}U_\lambda$. Тогда существует счетное множество $\Gamma\subset\Lambda$, такое, что $X\subset\bigcup\limits_{\lambda\in\Gamma}U_\lambda$.*

Доказательство. Множество X содержится в объединении тех шаров K_p, каждый из которых содержится по меньшей мере в одном из множеств U_λ. Таких K_p — счетное число. Выберем для каждого из них множество $U_{\lambda(p)}$, удовлетворяющее условию $K_p\subset U_{\lambda(p)}$. Тогда X содержится в объединении таких $U_{\lambda(p)}$. ∎

2.4. Определение. Множество $C\subset\mathbb{R}^n$ имеет *меру нуль*, если для любого $\varepsilon>0$ существует последовательность кубов $W_i\subset\mathbb{R}^n$, такая, что

$$C\subset\bigcup_{i=1}^{\infty}W_i \quad \text{и} \quad \sum_{i=1}^{\infty}|W_i|<\varepsilon.$$

Здесь через $|W_i|$ обозначен объем куба W_i, т. е. $|W_i| = a^n$, где a — длина ребра W_i.

2.5. Ясно, что *если* $C = \bigcup_{\nu=1}^{\infty} C_\nu$ *и каждое из множеств* C_ν *имеет меру нуль, то и множество* C *имеет меру нуль*. Действительно,

$$C_\nu \subset \bigcup_{i=1}^{\infty} W_i^\nu, \qquad \text{где} \quad \sum_{i=1}^{\infty} |W_i^\nu| < \frac{\varepsilon}{2^\nu},$$

откуда следует, что

$$C \subset \bigcup_{i,\nu} W_i^\nu, \qquad \text{где} \quad \sum_{i,\nu} |W_i^\nu| < \sum_\nu \frac{\varepsilon}{2^\nu} = \varepsilon.$$

Аналогичные рассуждения показывают, что для определения множеств меры нуль годятся как открытые, так и замкнутые W_i, а вместо кубов можно брать шары, параллелепипеды и т. д.

2.6. Лемма. *Если множество* $C \subset \mathbf{R}^n$ *имеет меру нуль и* $f\colon C \to \mathbf{R}^n$ — *дифференцируемое отображение, то множество* $f(C)$ *имеет меру нуль.*

Доказательство. Выберем открытое множество U, содержащее C, и дифференцируемое отображение $F\colon U \to \mathbf{R}^n$, такое, что $F|C = f$. Поскольку U является объединением счетного числа замкнутых шаров, без ограничения общности можно считать, что C содержится в некотором компактном шаре и что покрывающие C кубы также содержатся в (несколько большем) компактном шаре K, который в свою очередь содержится в U.

Положим теперь

$$b = \max\left\{\left|\frac{\partial F_i}{\partial x_j}(x)\right| \,\Big|\, x \in K\right\}.$$

Если длина ребра куба W равна a, то $|x_i - x_i^0| \leqslant a$ для $x \in W$, откуда

$$|F_i(x) - F_i(x^0)| \leqslant b \cdot n \cdot a.$$

Algebra

V

ГЛАВА

ТЕОРИЯ ГАЛУА

В этой главе мы применим аппарат бимодулей и тензорных произведений к изучению расширений поля K, т. е. к теории Галуа.

§ 1. Элементы теории полей

Далее нам понадобятся некоторые известные результаты о строении полей и их расширений.

Пусть K — произвольное поле. Напомним, что *характеристикой* поля K называется наименьшее натуральное число p, для которого

$$p1 = \underbrace{1 + 1 + \ldots + 1}_{p \text{ раз}} = 0 \quad \text{(если такое число существует).}$$

Если такого числа нет, т. е. $m1 \neq 0$ ни для какого m, говорят, что K — поле характеристики 0. Поскольку из равенства $p = mn$, очевидно, следует, что $p1 = (m1)(n1)$, характеристика поля — всегда простое число (или 0).

Предположим, что K — поле характеристики 0. Тогда из $n \neq m$ следует, что $n1 \neq m1$, и мы можем, отождествляя элемент $n1$ с числом n, считать, что K содержит множество натуральных чисел. Обозначая далее $(-n)1 = -n1$ и отождествляя $-n1$ с числом $-n$, мы можем рассматривать и совокупность целых чисел как подмножество (подкольцо) поля K. Наконец, рассматривая отношения $n1/m1$, мы можем вложить в K все поле рациональных чисел $\mathbf{Q}$.

Если поле K — простой характеристики p, положение еще проще: легко видеть, что в этом случае элементы вида $n1$, где $0 \leqslant n < p$, сами образуют подполе, изоморфное полю $\mathbf{F}(p)$ вычетов по модулю p.

Очевидно, поля $\mathbf{Q}$ и $\mathbf{F}(p)$ уже не содержат собственных подполей. Поля, обладающие этим свойством, называются *простыми*. Итогом наших рассуждений является следующая теорема.

Теорема 1.1. *Всякое поле K содержит простое подполе, изоморфное либо $\mathbf{Q}$ (если K — характеристики 0), либо $\mathbf{F}(p)$ (если K — характеристики $p > 0$).*

Следствие 1.2. *Если поле K конечно, то число элементов в нем равно p^n, где p — простое число.*

Доказательство. Характеристика конечного поля всегда отлична от нуля, т. е. $K \supset \mathbf{F}(p)$ для некоторого простого p. Но тогда K — конечное расширение $\mathbf{F}(p)$. Выбирая в нем базис, мы сразу получаем, что K состоит из p^n элементов, где $n = [K : F(p)]$.

Нас будут интересовать в основном конечные расширения фиксированного поля K. Важнейшую роль при построении и исследовании таких расширений играет следующий результат.

Теорема 1.3 (Кронекер). *Пусть $p(x)$ — неприводимый многочлен над полем K, $(p(x))$ — идеал в $K[x]$, состоящий из многочленов, кратных $p(x)$: $(p(x)) = \{p(x)g(x) \mid g(x) \in K[x]\}$. Тогда $K[x]/(p(x))$ есть поле, в котором многочлен $p(x)$ имеет корень. Наоборот, если L — расширение поля K, в котором $p(x)$ имеет корень a, то $K[a] \simeq K[x]/(p(x))$.*

Доказательство. Обозначим $I = (p(x))$ и рассмотрим в факторалгебре $K[x]/I$ класс $\bar{x} = x + I$. Из определения действий в факторалгебре следует, что $p(\bar{x}) = p(x) + I = 0$, т. е. $\bar{x}$ — корень $p(x)$. Остается проверить, что $K[x]/I$ есть поле.

Пусть $\bar{f} = f(x) + I$ — ненулевой класс $K[x]/I$, т. е. $f(x) \notin I$. Тогда многочлены $f(x)$ и $p(x)$ взаимно просты. Потому $1 = f(x)h(x) + p(x)g(x)$, где $h(x)$ и $g(x)$ — некоторые многочлены. Обозначим $\bar{h} = h(x) + I$, получаем, что $\bar{f}\bar{h} = 1$ в факторалгебре $K[x]/I$.

Наоборот, пусть L — расширение поля K, $a \in L$ — корень $p(x)$. Тогда $p(x) = m_a(x)$. Определяя гомоморфизм $\varphi : K[x] \to L$ формулой $\varphi(f(x)) = f(a)$, из теоремы о гомоморфизме находим, что $K[a] \simeq K[x]/I$.

Заметим, что расширение $K[x]/I$ — конечное: если степень $p(x)$ равна n, то легко проверить, что $1, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{n-1}$ — базис $K[x]/I$.

Из теоремы Кронекера можно получить такое важное следствие. Пусть $f(x)$ — произвольный многочлен над полем K, $p(x)$ — его неприводимый множитель. Тогда в поле $K_1 = K[x]/(p(x))$ многочлен $p(x)$, а потому и $f(x)$ имеет корень a_1, откуда по теореме Безу $f(x) = (x - a_1) f_1(x)$. Продолжая этот процесс, мы построим цепочку конечных расширений[9] $K \subset K_1 \subset K_2 \subset \ldots$, такую, что в K_i многочлен $f(x)$ имеет i корней (с учетом кратности). Отсюда следует, что если $f(x)$ — степени n, то в поле K_n он разложится на линейные множители.

Говорят, что L — поле разложения многочлена $f(x)$, если в нем $f(x)$ разлагается на линейные множители, но ни в каком его собственном подполе $f(x)$ не разлагается на линейные множители.

Теорема 1.4. *Для любого многочлена $f(x) \in K[x]$ существует поле разложения L и любые два поля разложения изоморфны.*

Доказательство. Существование поля разложения следует из изложенного выше. Его единственность мы будем доказывать индукцией по степени n многочлена $f(x)$. База индукции, $n = 1$, тривиальна: здесь автоматически $L = K$.

Пусть $f(x)$ — многочлен степени n, L и L' — его поля разложения, $p(x)$ — неприводимый (над K) множитель $f(x)$. Тогда $p(x)$ имеет корень a в поле L и корень a' в поле L'. Из теоремы Кронекера следует, что поля $K[a]$ и $K[a']$ изоморфны. Отождествляя их, можно считать, что L и L' содержат общее подполе $K_1 = K[a]$.

[9] Заметим, что в этой цепочке включения не обязаны быть строгими. Например, если $p(x)$ — линейный многочлен, то уже $K_1 = K$.

Но тогда L и L' — расширения поля K_1. Более того, это поля разложения над K_1 многочлена $f_1(x) = f(x)/(x - a)$ степени $n - 1$. По индукционному предположению $L \simeq L'$, что и требовалось доказать.

Покажем, что поле разложения L — также конечное расширение основного поля K. Поскольку L — подполе поля K_n, получающегося из K цепочкой конечных расширений, наше утверждение является частным случаем следующего результата.

Теорема 1.5. *Если $K = K_0 \subset K_1 \subset \ldots \subset K_{n-1} \subset K_n$ — цепочка полей, в которой K_{i+1} — конечное расширение K_i для любого i, то K_n — конечное расширение K и $[K_n : K] = \prod_{i=1}^{n} [K_i : K_{i-1}]$.*

Доказательство, очевидно, достаточно провести для случая $n = 2$: общий результат получается отсюда по индукции.

Итак, пусть $K \subset F \subset L$, причем $[F:K] = n$ и $[L:F] = m$. Выберем базис $\{a_1, \ldots, a_n\}$ поля F над K и базис $\{b_1, \ldots, b_m\}$ поля L над F. Тогда всякий элемент F имеет вид $\sum_{i=1}^{n} \alpha_i a_i$, где $\alpha_i \in K$, а всякий элемент поля L — вид $\sum_{j=1}^{m} \beta_j b_j$, где $\beta_j \in F$. Но, расписывая $\beta_j = \sum_{i=1}^{n} \alpha_{ij} a_i$, $\alpha_{ij} \in K$, мы получим $\sum_{j=1}^{m} \beta_j b_j = \sum_{i,j} \alpha_{ij} a_i b_j$, $\alpha_{ij} \in K$, т. е. $\{a_i b_j\}$ — система образующих векторного пространства L над полем K.

С другой стороны, если $\sum_{i,j} \alpha_{ij} a_i \beta_j = 0$, то из линейной независимости $\{b_j\}$ над F следует, что $\sum_{i=1}^{n} \alpha_{ij} a_i = 0$ для любого j, откуда, ввиду линейной независимости a_i над K, $\alpha_{ij} = 0$ для всех i, j, т. е. элементы $a_i b_j$ линейно независимы над K. Итак, мы построим базис $\{a_i b_j\}$ поля L над K, состоящий из nm элементов, что и доказывает теорему.

§ 2. Конечные поля. Теорема Веддербёрна

Применим полученные ранее результаты для описания конечных полей (и даже всех конечных тел!). Докажем вначале одну лемму о коммутативных группах.

Лемма 2.1. *Если в коммутативной группе G есть элементы порядков m и n, то в G есть и элемент порядка k, где k — наименьшее общее кратное m и n.*

Доказательство. Пусть x — элемент порядка m, y — элемент порядка n. Если m и n взаимно просты, то $k = mn$ и $(xy)^k = x^k y^k = 1$. Наоборот, если $(xy)^l = 1$, то $x^l = y^{-l}$ и элементы x^l и y^l имеют одинаковый порядок. Но порядок элемента x^l

ОБЫКНОВЕННЫЕ РАЗНОСТНЫЕ УРАВНЕНИЯ

Diff. eq.

ГЛАВА 1
РАЗНОСТНЫЕ УРАВНЕНИЯ ПЕРВОГО И ВТОРОГО ПОРЯДКА ПРИМЕРЫ РАЗНОСТНЫХ СХЕМ

§ 1. Простейшие разностные уравнения

1. Разностные уравнения. Для дифференциального уравнения первого порядка

$$u'(x) + A\,u(x) = f(x)$$

мы построили во введении две разностные схемы:

$$\frac{u(x+h) - u(x)}{h} + A\,u(x) = f(x),$$

$$\frac{u(x+h) - u(x-h)}{2h} + A\,u(x) = f(x),$$

которые можно записать соответственно в виде

$$-\frac{1-Ah}{h}\,u(x) + \frac{1}{h}\,u(x+h) = f(x), \qquad (1)$$

$$-\frac{1}{2h}\,u(x-h) + A\,u(x) + \frac{1}{2h}\,u(x+h) = f(x). \qquad (2)$$

Для дифференциального уравнения второго порядка

$$u''(x) + A\,u'(x) + B\,u(x) = f(x)$$

во введении было построено разностное уравнение

$$\frac{u(x+h) - 2u(x) + u(x-h)}{h^2} + A\,\frac{u(x+h) - u(x-h)}{2h} + B\,u(x) = f(x),$$

или, в другой записи,

$$\frac{1}{h^2}\left(1 - \frac{Ah}{2}\right)u(x-h) - \frac{1}{h^2}(2 - Bh^2)\,u(x) + {} + \frac{1}{h^2}\left(1 + \frac{Ah}{2}\right)u(x+h) = f(x). \qquad (3)$$

Приведенные здесь примеры разностных уравнений, приближающих простейшие дифференциальные, принадлежат к одному из следующих двух видов:

$$a\,u(x)+b\,u(x+h)=f(x), \tag{1'}$$

$$a\,u(x-h)+b\,u(x)+c\,u(x+h)=f(x). \tag{2'}$$

Если последовательность точек, делящих ось Ox на отрезки длины h, занумеровать слева направо так, чтобы $x_n=x_{n-1}+h$, и обозначить $u(x_n)$ через u_n, а $f(x_n)$ через f_n, то мы можем переписать наши разностные схемы в виде уравнений

$$au_n+bu_{n+1}=f_n, \tag{4}$$

$$au_{n-1}+bu_n+cu_{n+1}=f_n. \tag{5}$$

В §§ 1—4 мы займемся изучением разностных уравнений вида (4) и (5), причем не будем интересоваться, являются ли эти уравнения разностными схемами для каких-либо дифференциальных уравнений.

В уравнениях (4) и (5) неизвестные u_n образуют последовательность $\{u_n\}$:

$$\ldots,\ u_{-3},\ u_{-2},\ u_{-1},\ u_0,\ u_1,\ u_2\ u_3,\ \ldots$$

Мы будем часто сопоставлять эту последовательность с последовательностью точек, занумерованных числами

$$\ldots,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ \ldots,$$

или, как иногда говорят, с сеткой.

Последовательность $\{u_n\}$ можно считать функцией u, заданной в точках сетки. Тогда u_k есть значение сеточной функции u в точке, имеющей номер k. На рис. 1 приведен график некоторой сеточной функции u. Этот график есть совокупность точек $(x_k,\ u_k)$ на плоскости Oxu.

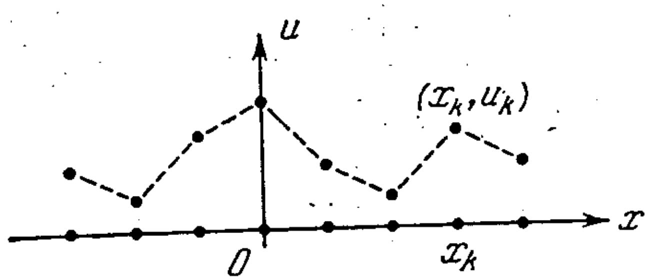


Рис. 1.

После того как мы отказались от рассмотрения связи разностных уравнений с дифференциальными, нам вовсе не обязательно считать, что расстояние между двумя соседними точками равно h. Можно выбрать его произвольным, например равным единице, а в качестве x_0 взять точку нуль. Тогда сеточная функция u будет определена в точках с целыми координатами $x_k=k$.

Будем считать для простоты, что коэффициенты a, b, c уравнений (4), (5) постоянны. Говоря, что изучаемые уравнения являются уравнениями с постоянными коэффициентами, мы имеем в виду независимость этих коэффициентов от номера n; например, уравнение

$$u_{n-1}+5\sqrt{n}\,u_n+u_{n+1}=0$$

не является уравнением с постоянными коэффициентами.

Мы будем рассматривать только такие уравнения (4), у которых a и b отличны от нуля. В уравнении (5) отличными от нуля будем считать коэффициенты a и c.

Последовательность $\{f_n\}$ называется *правой частью* рассматриваемых уравнений.

Если предполагать, что последовательность $\{u_n\}$ определена во всех целых точках n, $-\infty<n<\infty$, и не накладывать на эту последовательность никаких дальнейших ограничений, то легко видеть, что уравнения (4) и (5) имеют много решений. Например, уравнение $qu_n-u_{n+1}=0$ допускает как решение $u_n\equiv 0$, так и решение $u_n=q^n$.

Чтобы выделить единственное решение уравнения (4)

$$au_n+bu_{n+1}=f_n,$$

достаточно задать значение этого решения в какой-нибудь одной целой точке m, т. е. задать u_m. В самом деле, уравнение (4) можно записать в виде рекуррентной формулы

$$u_{n+1}=\frac{1}{b}(f_n-au_n),$$

из которой при $n=m$, $m+1$, ... последовательно определяются u_{m+1}, u_{m+2}, ..., т. е. все u_n при $n>m$. Записывая уравнение в виде другой рекуррентной формулы:

$$u_{n-1}=\frac{1}{a}(f_n-bu_n),$$

мы таким же путем определим все u_n при $n<m$.

Для выделения единственного решения уравнения (5)

$$au_{n-1}+bu_n+cu_{n+1}=f_n$$

достаточно задать произвольно значения u в каких-нибудь двух последовательных целых точках, например задать значения u_{m-1} и u_m. Доказательство немедленно следует из того, что рассматриваемое уравнение может быть переписано в виде следующих двух рекуррентных формул:

$$u_{n+1}=\frac{1}{c}(f_n-bu_n-au_{n-1}),$$

$$u_{n-1}=\frac{1}{a}(f_n-bu_n-cu_{n+1}).$$