Независимый Московский Университет, весна 2020

ПЕРЕСЕЧЕНИЯ В ПРОСТРАНСТВАХ МОДУЛЕЙ КРИВЫХ

Лекция 1 (13 февраля 2020)
Пространство модулей кривых как множество

В этой лекции мы определим предварительное понятие алгебраической кривой и опишем множество всех кривых с точностью до некоторого отношения эквивалентности.

1.0. Глобальные поля

1.0.0. Основное поле. Работаем над основным алгебраически замкнутым полем

$$\Bbbk = \overline{\Bbbk}.$$

Во многих случаях оно произвольно; в некоторых случаях рассмотрения упрощаются в предположениях вроде $\mathrm{char}(\Bbbk) \neq 2, 3$.

Некоторые *трансцендентные* методы имеют смысл лишь при $\Bbbk = \mathbb{C}$; обоснование некоторых результатов существенно упрощается в этом предположении.

1.0.1. Расширения основного поля. В современной математике весьма распространены специфические связи между геометрическими и алгебраическими объектами. Так, компактам сопоставляются банаховы алгебры непрерывных функций на них (Гельфанд-Наймарк), коммутативным кольцам – их спектры (Гротендик); различные варианты этих соответствий определяют эквивалентности подходящих категорий.

В нашем случае удобно начать с алгебраических объектов.

Пусть

$$\mathcal{K} \supset \Bbbk$$

конечнопорождённое расширение полей степени трансцендентности 1.

Отметим, что приведённые условия не следуют друг из друга.

$\Bbbk(x,y) \supset \Bbbk$ – конечнопорождённое расширение степение трансцендентности 2.
$\mathbb{C}(x, x^{\frac{1}{2}}, x^{\frac{1}{4}}, x^{\frac{1}{8}}, \dots) \supset \mathbb{C}$ – расширение степени трансцендентности 1, не являющееся конечнопорождённым.

1.0.2. Простейший пример: поле $\Bbbk(x)$. Это *–поле рациональных функций одной переменной*

$$\mathcal{K} = \Bbbk(x).$$

ВНИМАНИЕ К ОБОЗНАЧЕНИЯМ! Скоро для *кривой* $\mathbf{X}$ (это понятие БУДЕТ определено) через

$$\mathcal{K} = \Bbbk(\mathbf{X})$$

будет обозначаться *поле рациональных функций* на этой кривой. Оба обозначения настолько стандартны, что от них невозможно отклониться. Так что лишь внимание к контекстам и **фонтам** позволит избежать недоразумений.

1.0.3. Нормирования. Мы следуем [**Серр1968**]. Введём упорядоченную полугруппу

$$(\mathbb{Z} \coprod \{\infty\}, +, \leq),$$

в которой подразумевается $\mathbb{Z} + \infty = \{\infty\}, \mathbb{Z} < \infty$.

Нормирование произвольного[1] поля $\mathcal{K}$ есть эпиморфизм полугрупп

$$v : (\mathcal{K}, \cdot) \twoheadrightarrow (\mathbb{Z} \coprod \{\infty\}, +),$$

удовлетворяющий аксиомам

$$v(x) = \infty \iff x = 0; \tag{**1.0.3a**}$$

$$v|_{\mathcal{K}^\times} : \mathcal{K}^\times \twoheadrightarrow \mathbb{Z} - \text{морфизм групп}; \tag{**1.0.3b**}$$

$$v(x+y) \geq \min\{v(x), v(y)\}. \tag{**1.0.3c**}$$

Введём не вполне стандартное обозначение

$$\mathrm{Val}(\mathcal{K}) := \Big\{\text{нормирования } \mathcal{K} \twoheadrightarrow \big(\mathbb{Z} \coprod \{\infty\}\big)\Big\}.$$

Теорема Островского описывает все нормирования поля рациональных чисел – их оказывается по одному на каждое простое число

$$\mathrm{Val}(\mathbb{Q}) = \{v_p \mid p - \text{простое}\},$$

где $v_p\big(p^n \frac{a}{b}\big) = n$ при $a, b \in \mathbb{Z}, a\mathbb{Z} + p\mathbb{Z} = b\mathbb{Z} + p\mathbb{Z} = \mathbb{Z}, n \in \mathbb{Z}$.

---

[1] аксиомы, которые сейчас будут сформулированы, временно не подразумевают выделенного подполя $\Bbbk \subset \mathcal{K}$

В наших основных рассмотрениях фигурирует основное поле $\Bbbk \subset \mathcal{K}$, и к перечисленным трём аксиомам добавляется четвёртая:

$$v|_{\Bbbk^\times} \equiv 0. \qquad (\mathbf{1.0.3d})$$

Нормирования поля $\mathcal{K}$, удовлетворяющие этому условию, называются нормированиями *над* $\Bbbk$. Обозначение:

$$\mathrm{Val}_{\Bbbk}(\mathcal{K}) := \{v \in \mathrm{Val}(\mathcal{K}) \mid v|_{\Bbbk^\times} \equiv 0\}.$$

Это понятие может показаться не вполне естественным; мы, однако, постепенно с ним освоимся, учась на некоторых примерах думать о нормированиях как о *точках*.

1.0.4 Нормирования поля $\Bbbk(x)$. Для любого $\alpha \in \Bbbk$ имеется нормирование "порядок нуля или полюса в α". Оно обозначается ord_α и однозначно определяется тем, что для любых многочленов $A, B \in \Bbbk[x]$, удовлетворяющих $A(\alpha)B(\alpha) \neq 0$ и любого $n \in \mathbb{N}$, имеет место равенство

$$\mathrm{ord}_\alpha\Big((x-\alpha)^n \frac{A}{B}\Big) = n;$$

это нормирование надо доопределить, положив $\mathrm{ord}_\alpha(0) := \infty$.

Ещё одно нормирование будет обозначаться ord_∞; оно определяется тем, что

$$\mathrm{ord}_\infty(x) = -1$$

и, следовательно, нормирования ненулевых рациональных функций определяются формулой

$$\mathrm{ord}_\infty\Big(\frac{A}{B}\Big) := -\deg(A) + \deg(B).$$

Теорема. *Нормирования поля $\Bbbk(x)$ исчерпываются указанными нормированиями:*

$$\mathrm{Val}_{\Bbbk}\big(\Bbbk(x)\big) = \{\mathrm{ord}_\alpha \mid \alpha \in \Bbbk\} \coprod \{\mathrm{ord}_\infty\}.$$

Доказательство. Пусть $v : \Bbbk(x)^\times \to \mathbb{Z}$ – нормирование. Рассмотрим две возможности.

(1) $\exists \alpha \in \Bbbk; v(x-\alpha) > 0$. Тогда такая α единственна: если бы нашлась $\beta \neq \alpha$, удовлетворяющая $v(x-\beta) > 0$, то мы бы немедленно пришли к противоречию

$$0 = v\big((x-\alpha) + (\beta - x)\big) \geq_{(1.0.3d)} \min(v(x-\alpha), v(x-\beta)) > 0.$$

Далее,

$$v(x-\alpha) = 1,$$

поскольку иначе, в случае $v(x-\alpha) = d > 1$ в силу (1.0.3b) выполнялось бы включение $v\big((x-\alpha)^n\big) \in d\mathbb{Z}$ для любых $n \in \mathbb{Z} \setminus \{0\}$, и поэтому, так как любой многочлен $P \in \Bbbk[x]$ степени $n > 0$ представим в виде $P = c_0 + \sum_{i=1}^n c_i(x-\alpha)^i$, где $c_0, c_1, \ldots, c_n \in \Bbbk$ и $c_n \neq 0$, оказалось бы (с помощью известной леммы: *если для $a, b \in \mathcal{K}$ выполнено $v(a) \neq v(b)$*, то $v(a+b) = \min\big(v(a), v(b)\big)$), что $v(P) = d\min\{i | c_i \neq 0\} \in d\mathbb{Z}$, а тогда и все значения нормирования v будут делиться на d, вопреки предположению о его сюръективности.

Отсюда нетрудно вывести равенство $v = \mathrm{ord}_\alpha$.

(2) $\forall \alpha \in \Bbbk; v(x-\alpha) \leq 0$. Как и в случае (1), легко убедиться, что $\forall \alpha \in \Bbbk; v(x-\alpha) = -1$ и вывести отсюда, что для любого многочлена $P \in \Bbbk[x]$ имеет место равенство $v(P) = -\deg P$. Это и означает, что $v = \mathrm{ord}_\infty$.■

1.1. Что такое алгебраическая кривая?

1.1.0. Многочлены и множества их нулей. Процитируем определение из самого начала замечательного учебника [**Шафаревич2007**]:

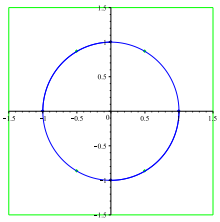
> *плоской алгебраической кривой* называется множество всех точек, координаты которых удовлетворяют уравнению
>
> $$f(x, y) = 0,$$
>
> где $f(x, y)$ – многочлен с коэффициентами из $\Bbbk$.

Читатель, которого устраивает это определение[2], может продолжить чтение. А если читателя что-то в нём смущает (например, что x – не тот, что в предыдущих подразделах...), то, возможно, ему/ей имеет смысл предварительно просмотреть Приложение.

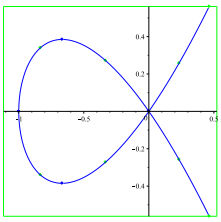
То, что в этом подразделе будет называться *кривой,* правильнее называть (плоской) *аффинной кривой*; в дальнейшем мы будем заниматься другими кривыми.

Уравнения кривых часто записываются в виде $\mathsf{A} = \mathsf{B}$; при этом подразумевается равносильность этой записи и $\mathsf{A} - \mathsf{B} = 0$.

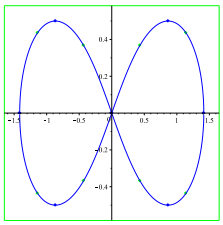
У некоторых кривых (вместе с уравнениями!) есть общепринятые имена; они обычно связываются с образами вещественных кривых – класса, которым мы заниматься в основном не будем. Например,



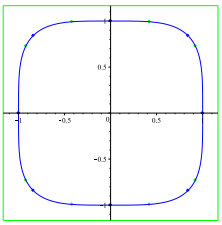
Окружность
$x^2 + y^2 = 1$



Декартов лист
$y^2 = x^3 + x^2$



Лемниската Бернулли
$(x^2 + y^2)^2 = 2(x^2 - y^2)$



Квартика Ферма
$x^4 + y^4 = 1$

[2] меня в студенческие годы оно вполне устраивало...

Не все классические алгебраические кривые – плоские. Например, *эллиптические* кривые возникли при изучении длин дуг *эллипсов*

$$\frac{X^2}{a^2}+\frac{Y^2}{b^2}=1.$$

С нашей точки зрения сами эллипсы малоинтересны и не отличаются от окружности (хотя в 17-м веке эти кривые считались бы разными). Однако их длины, выражаемые после параметризации ($X=a\cos t, Y=b\sin t$) с учётом равенства *квадратичных дифференциалов*

$$(\mathrm{d}\ell)^2:=(\mathrm{d}X)^2+(\mathrm{d}Y)^2=\big(a^2\sin^2 t+b^2\cos^2 t\big)(\mathrm{d}t)^2$$

к *эллиптическому интегралу*

$$\int \mathrm{d}\ell=\int\sqrt{a^2\sin^2 t+b^2\cos^2 t}\;\mathrm{d}t,$$

не берущемуся в элементарных функциях и сыгравшему значительную роль в развитии математики 18 и 19 веков. Введя новые переменные[3]

$$\xi:=\cos t,\ \eta:=\sin t,\ \zeta:=\sqrt{b^2\cos^2 t+a^2\sin^2 t},$$

рассматриваемый интеграл можно переписать в виде *рационального* интеграла

$$\int\zeta\mathrm{d}\arcsin\eta=\int\zeta\frac{\mathrm{d}\eta}{\sqrt{1-\eta^2}}=\int\zeta\frac{\mathrm{d}\eta}{\xi}$$

на кривой, заданной двумя уравнениями в трёхмерном пространстве с координатами ξ,η,ζ

$$\begin{cases}\xi^2+\eta^2=1\\ \zeta^2=b^2\xi^2+a^2\eta^2\end{cases}$$

Выражаясь профессионально, мы представили эллиптическую кривую как *пересечение двух квадрик.*

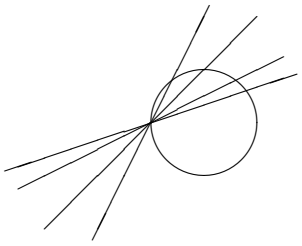
1.1.1. Какие кривые одинаковы? Несомненно одинаковы кривые, переводимые друг в друга *взаимно обратными полиномиальными* преобразованиями – например, любой *график многочлена* $y=f(x)$ переходит в прямую при преобразовании $(x,y)\mapsto(x,y-f(x))$, тогда как обратное преобразование имеет вид $(x,y)\mapsto(x,y+f(x))$. Это отношение эквивалентности на множестве кривых, однако, для нас слишком тонко. Введём более грубое отношение, начав с трёх примеров.

Рациональная параметризация окружности. Снова рассмотрим окружность, заданную уравнением

$$x^2+y^2=1 \tag{1.1.1a}$$

и построим *пучок прямых* через точку $(x,y)=(-1,0)$:

[3] мы используем не очень удобные и не самые традиционные обозначения переменных, поскольку в дальнейшем будем преобразовывать полученные формулы с использованием более стандартных координат



Уравнения этих прямых –

$$y = t(x+1),$$

где $t \in \Bbbk$. Подставляя это соотношение в уравнение окружности, получаем

$$x^2 + [t(x+1)]^2 = 1; \tag{1.1.1b}$$

рассмотрим его как квадратное уравнение относительно x с коэффициентами в $\Bbbk(t)$. Поскольку $x = -1$ является одним из корней этого уравнения, мы знаем без всяких вычислений, что другой корень (являющийся x-координатой пересечения окружности с прямой, проходящей через точку $(x, y) = (-1, 0)$) и имеющей "наклон" t) зависит от t *рационально.*

Действительно, находим

$$x = \frac{1-t^2}{1+t^2},\ y = \frac{2t}{1+t^2}; \tag{1.1.1c}$$

таким образом, любое $t \in \Bbbk$ даёт точку на окружности. Например, при характеристике $\mathrm{char}(\Bbbk) \notin \{2, 5\}$ выбор $t = \frac{1}{2}$ даёт "хорошо известную" (*египетскую*) точку $(x, y) = (\frac{3}{5}, \frac{4}{5})$.

Более того, *все* рациональные точки на окружности, кроме одной, получаются таким образом; действительно, если $(x, y) \neq (-1, 0)$ лежит на окружности, то

$$t = \frac{y}{x+1} \tag{1.1.1d}$$

есть не что иное, как "наклон" прямой из рассмотренного пучка.

Уравнения (1.1.1c) и (0.0.0d) определяют *бирациональный изоморфизм* окружности, заданной уравнением (1.1.1a), и прямой, параметризованной переменной t.

Рациональная параметризация декартова листа. Напомним уравнение этой кривой[4]:

$$y^2 = x^3 + x^2 \tag{1.1.1e}$$

Здесь требуемое преобразование строится даже проще, чем в предыдущем примере: пучок прямых

$$y = tx \tag{1.1.1f}$$

проходит через *особую точку* кривой (это понятие будет обсуждаться ниже; полезно увидеть эту особую точку на изображённой выше вещественной картинке). Подстановка (1.1.1f) в (1.1.1e) даёт $t^2x^2 = x^3 + x^2$, или после сокращения на x^2

$$x = t^2 - 1,\ y = t^3 - t \tag{1.1.1g}$$

[4] с этого примера начинается учебник [**Шафаревич2007**]

– это и есть искомая параметризация декартова листа. Важно отметить, что она "склеивает" точки $t = \pm 1$. Однако это – снова *бирациональный изоморфизм*, поскольку в силу (1.1.1f) обратное преобразование задаётся формулой $t = \frac{y}{x}$.

Разные канонические виды эллиптических кривых. Мы начинали с реализации кривой, ответственной за длины дуг эллипса $\frac{X^2}{a^2} + \frac{Y^2}{b^2} = 1$, и эта эллиптическая кривая была реализована как пересечение двух пространственных квадрик (над $\mathbb{R}$ – цилиндра и конуса)

$$\begin{cases} \xi^2 + \eta^2 = 1 \\ b^2\xi^2 + a^2\eta^2 = \zeta^2 \end{cases}, \tag{1.1.1h}$$

вторая из которых зависит от "полуосей" a и b эллипса.

Нетрудно проверить, что в новых координатах

$$\xi = \frac{1-u^2}{1+u^2}, \eta = \frac{2u}{1+u^2}, \zeta = \frac{bv}{1+u^2} \tag{1.1.1i}$$

(в первых двух компонентах читатель узнает "тригонометрическую" замену (1.1.1c) в изменённых обозначениях) два уравнения (1.1.1h) превращаются в одно

$$v^2 = u^4 + \frac{4a^2 - 2b^2}{b^2}u^2 + 1 \tag{1.1.1j}$$

– если ввести "эксцентриситет"

$$e := \sqrt{1 - \frac{b^2}{a^2}},$$

то оно превращается в

$$v^2 = \Big(u^2 + \frac{1-e}{1+e}\Big)\Big(u^2 + \frac{1+e}{1-e}\Big). \tag{1.1.1j$'$}$$

Обратное к (1.1.1i) преобразование имеет вид

$$u = \frac{\eta}{\xi + 1}, v = \frac{\zeta}{b}\Big(1 + \frac{\eta^2}{(\xi+1)^2}\Big) \tag{1.1.1k}$$

Заметим, что преобразования (1.1.1i) и (1.1.1k) не определены в лежащих на рассматриваемых кривых точках ($\xi = -1, \eta = 0, \zeta = \pm b$) пространственной кривой и $\big(u = \pm\mathrm{i}, v = \pm\frac{2e\mathrm{i}}{\sqrt{1-e^2}}\big)$ плоской.

Наконец, отметим, что кривая (1.1.1j') бирационально изоморфна кривой (1.1.1j')

$$y^2 = x(x-e)\big(x - \frac{1}{e}\big) \tag{1.1.1l}$$

– приведём одну компоненту преобразования, $u = -\mathrm{i}\sqrt{\frac{1-e}{1+e}}\frac{x+1}{x-1}$, предоставляя читателю найти остальные три. Полученные преобразования тоже окажутся определёнными не всюду. Преимущество кривой ((1.1.1l)) перед (1.1.1j') скажется при вложении аффинной плоскости в проективную.

***

Итак, на нескольких примерах мы познакомились понятиями *бирациональных преобразований* и *бирационального изоморфизма* кривых. Точного определения этих понятий, требующего (на данном уровне рассмотрения) большого количества промежуточных обозначений, мы приводить не будем, отсылая читателя к [**Шафаревич2007**].

Отметим, однако, несколько моментов.

(а) Бирациональный изоморфизм кривых будет для нас основным; пространства модулей кривых будут состоять именно из классов бирациональной изоморфности кривых.
(б) Его точное определение будет дано вскоре.
(в) Аффинные кривые не будут играть существенной роли в курсе. Интуитивно их следует воспринимать как *полные кривые с проколами*. Читатели, владеющие комплексным анализом и двумерной топологией, сумеют сформулировать точное утверждение.
(г) Одно из не очень приятных свойств рассмотренных примеров заключалось в том, что рассмотренные преобразования было "не совсем" отображениями. Когда мы перейдём к полным кривым, всюду-определённость отображений будет восстановлена; тогда же мы перейдём от бирациональных изоморфизмов к *бирегулярным*.
(д) Кривые, допускающие рациональную параметризацию, называются *рациональными*; они бирационально изоморфны прямой; лингвисты бывают шокированы, узнав, что есть области математики, представители которых не различают прямых и окружностей. Серьёзный же вопрос: *существуют ли нерациональные кривые*?

Ответ – ДА, и с одним их множеством мы уже встретились: эллиптические кривые не рациональны. Когда мы освоим понятие *рода* кривой, обоснование будет мгновенно: род рациональной кривой равен 0, а эллиптической – 1. В самом начале [**Шафаревич2007**] устанавливается нерациональность ещё одной эллиптической кривой, так называемой *кубики Ферма*, определяемой уравнением $x^3 + y^3 = 1$.

1.1.2. Абстрактные, вложенные и погружённые кривые. Опять введём эти фундаментальные понятия предварительно и на примерах.

Введём временное обозначение для (аффинной) *прямой*

$$\mathbf{L} := \{t | t \in \Bbbk\}.$$

Можно было бы подумать, что просто $\mathbf{L} = \Bbbk$, но для нас $\Bbbk$ – множество с операциями, а $\mathbf{L}$ – "просто" множество, структуру (*окольцованного пространства*) на котором мы введём позже.

Введём также постоянное обозначение для *аффинной плоскости*

$$\mathbf{A}_2(\Bbbk) := \Bbbk \times \Bbbk,$$

к которому относятся те же замечания.

Надо научиться думать об $\mathbf{L}$ как об *абстрактной*, никуда не вложенной, кривой (прямой). Рассмотренные нами примеры окружности и декартова листа надо понимать как два отображения

$$\mathbf{L} \setminus \{\pm\mathbf{i}\} \longrightarrow \mathbf{A}_2(\Bbbk) : t \mapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$$

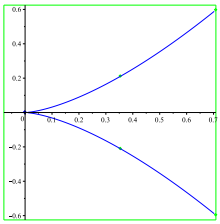
и

$$\mathbf{L} \longrightarrow \mathbf{A}_2(\Bbbk) : t \mapsto (t^2-1, t^3-t).$$

Первое из них является *вложением* (не-определённость которого в двух точках пройдёт при переходе от аффинной геометрии к проективной), а второе – *погружением* (поскольку склеивает точки $t = \pm 1$).

Складывающееся представление о том, что вложение – это инъективное отображение абстрактной кривой в плоскость, требует некоторой корректировки. Рассмотрим ещё одну классическую кривую, *полукубическую параболу*, задаваемую в аффинной плоскости уравнением

$$y^2 = x^3$$



Она допускает очевидную инъективную параметризацию

$$\mathbf{L} \longrightarrow \mathbf{A}_2(\Bbbk) : t \mapsto (t^2, t^3)$$

(обратное преобразование выглядит, как и в случае декартова листа, просто: $t = \frac{y}{x}$), которая, однако, является погружением, а не вложением. Причина кроется в *особой точке* $(x = 0, y = 0)$, но мы откладываем обсуждение этого понятия.

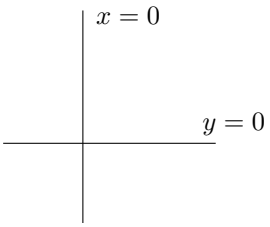
1.2. Поля рациональных функций на кривых

1.2.0. Важное обозначение. Для многочлена $f \in \Bbbk[x, y] \setminus \Bbbk$ положительной степени мы теперь определяемую им кривую будем иногда называть *множеством* его *нулей* и обозначать

$$\mathrm{zer}_f := \{(\mathrm{x}, \mathrm{y}) \in \mathbf{A}_2(\Bbbk) \mid \quad f(\mathrm{x}, \mathrm{y}) = 0\}.$$

Нестандартный шрифт для x, y комментируется в Приложении. Отметим, что традиционно – см., например, [**Манин2012**]) – используется менее мнемоничное обозначение $\mathrm{V}(f) \equiv \mathrm{zer}_f$, по-видимому, от слова *variety*.

1.2.1. Неприводимые плоские кривые. Начнём опять с простого примера: кривая, заданная уравнением $xy = 0$



является объединением двух кривых, поскольку многочлен $xy \in \Bbbk[x, y]$ *приводим*. Напомним общее определение:

многочлен $f \in \Bbbk[x, y]$ называется *неприводимым,* если он не может быть представлен как произведение многочленов меньших степеней, то есть из равенства $f = f_1 f_2$, где $f_1, f_2 \in \Bbbk[x, y]$ следует, что либо $f_1 \in \Bbbk$, либо $f_2 \in \Bbbk$. В силу очевидной формулы

$$\mathrm{zer}_{f_1 f_2} = \mathrm{zer}_{f_1} \bigcup \mathrm{zer}_{f_2}$$

неприводимость многочлена $f \in \Bbbk[x, y]$ равносильна *невозможности представить кривую* zer_f *в виде объединения строго содержащихся в ней кривых.* Кривые, обладающие таким свойством, сами называются *неприводимыми.*

Все рассмотренные в предыдущем разделе кривые были неприводимы, хотя мы специально этого не оговаривали. В этом же разделе неприводимость кривых окажется весьма существенной.

Иногда кажется соблазнительным вовсе отказаться в алгебро-геометрических курсах от рассмотрения приводимых многообразий – ведь приводимые многообразия распадаются в объединения неприводимых. Однако часто, в том числе в нашем курсе, многообразия рассматриваются не только индивидуально, но и в *семействах*; и часто встречаются семейства, почти все члены которых неприводимы, но некоторые приводимы. Таково (очевидно) семейство гипербол $xy = c$ и (тоже очевидно, если видеть то, что в 19-м веке называлось *мнимым*) семейство окружностей $x^2 + y^2 = r^2$.

1.2.2. Кольца регулярных функций на кривых. Если рассматривать кольцо $\Bbbk[x, y]$ как кольцо *полиномиальных функций* $\mathbf{A}_2(\Bbbk) \to \Bbbk$, то для непостоянного многочлена $f \in \Bbbk[x, y] \setminus \Bbbk$ порождённый им идеал

$$\langle f \rangle := f\Bbbk[x, y] \lhd \Bbbk[x, y]$$

следует интерпретировать как множество этих функций, обращающихся в 0 на кривой zer_f. Элементы *фактор-кольца* $\frac{\Bbbk[x,y]}{\langle f \rangle}$ интерпретируются как *регулярные (полиномиальные) функции на* zer_f.

Если ввести обозначение

$$\mathbf{X} := \mathrm{zer}_f,$$

то это фактор-кольцо оказывается одним из самых главных объектов коммутативной алгебры $\approx$ *аффинной* алгебраической геометрии

$$\Bbbk[\mathbf{X}] := \frac{\Bbbk[x, y]}{\langle f \rangle}$$

Если непостоянный многочлен $f \in \Bbbk[x,y] \setminus \Bbbk$ неприводим, то порождённый им идеал $\langle f \rangle$ *прост* (см. [**АтьяМакдональд1972**]).

В этом случае кольцо $\Bbbk[\mathbf{X}]$ не имеет делителей нуля.

1.2.3. Поля рациональных функций на неприводимых кривых. Итак, в случае неприводимой кривой $\mathbf{X}$ определено (см. [**АтьяМакдональд1972**]) *поле частных*[5]

$$\Bbbk(\mathbf{X}) := \text{ff}\Big(\Bbbk[\mathbf{X}]\Big).$$

Эти поля и будут основными в нашем подходе к классификации алгебраических кривых над полем $\Bbbk$. Класс этих полей был введён в начале лекции; оказывается, он охватывает поля рациональных функций на ВСЕХ кривых.

Теорема. *(а) Если многочлен $f \in \Bbbk[x,y] \setminus \Bbbk$ неприводим, то поле*

$$\Bbbk(\mathrm{zer}_f) \supset \Bbbk$$

является конечнопорождённым расширением поля $\Bbbk$ степени трансцендентности 1.
(б) Наоборот, если $\mathcal{K} \supset \Bbbk$ – конечнопорождённое расширение полей степени трансцендентности 1*, то найдётся неприводимый многочлен $f \in \Bbbk[x,y]$, для которого $\mathcal{K} \simeq \Bbbk(\mathrm{zer}_f)$.*

О доказательствах. (а) Поскольку поле $\mathcal{K}$ порождено над $\Bbbk$ всего двумя элементами x и y, конечнопорождённость сомнений не вызывает. Остаётся показать, что любые два элемента $u, v \in \mathcal{K}$ удовлетворяют нетривиальному полиномиальному соотношению с коэффициентами из $\Bbbk$. Это геометрически очевидно: снова обозначив $\mathbf{X} := \mathrm{zer}_f$ и представив u, v как (классы эквивалентности) рациональных функций от x, y, отметим, что знаменатели этих функций имеют не более конечного множества нулей на $\mathbf{X}$, и потому определено *рациональное* (то есть определённое вне конечного множества точек и задаваемое рациональными функциями) отображение

$$u \times v : \mathbf{X} \dashrightarrow \mathbf{A}_2(\Bbbk).$$

Образ этого отображения – плоская кривая (см. [**Шафаревич2007**], где, правда, соответствующее утверждение устанавливается для проективных кривых, но нужное нам утверждение из него вытекает), а это и означает, что u и v связаны полиномиальным соотношением.

(б) Не сразу очевидно, что поле $\mathcal{K}$ поля $\Bbbk(\mathbf{X})$, порождённое конечным множеством образующих, может быть порождено всего двумя образующими.

Начало доказательства таково. Выберем $x \in (\mathcal{K} \setminus \Bbbk)$. Если $\mathcal{K} \setminus \Bbbk(x)$, то больше ничего доказывать не надо. В противном случае расширение $\mathcal{K} \supset \Bbbk(x)$ конечно и, если оно *сепарабельно*, то по теореме *о примитивном элементе* (см.

[5] мы используем иногда встречающееся в современной литературе обозначение ff для fraction field

[**Варден1975**]) найдётся такой $y \in \mathcal{K}$, что $\mathcal{K} = \Bbbk(x)(y) = \Bbbk(x,y)$. Общее геометрическое доказательство снова можно найти в [**Шафаревич2007**] (кривая $\mathbf{X}$ сначала помещается в многомерное пространство, а затем проектируется оттуда на плоскость). ■

1.3. Объединение $\mathcal{M}(\Bbbk)$ всех пространств модулей

1.3.0. Окончательное определение бирационального изоморфизма. Мы уже знакомы с понятием бирационального изоморфизма на примерах аффинных кривых (которые в дальнейшем будут играть в основном вспомогательную роль, а фигурировали по историческим и методическим причинам).

Теперь введём основное, точное и окончательное определение. Две неприводимые аффинные кривые $\mathbf{X}_1 \subset \mathbf{A}_2(\Bbbk)$ и $\mathbf{X}_2 \subset \mathbf{A}_2(\Bbbk)$ *бирационально изоморфны*,

$$\mathbf{X}_1 \simeq \mathbf{X}_2,$$

если поля рациональных функций на них $\mathcal{K}_1 = \Bbbk(\mathbf{X}_1)$ и $\mathcal{K}_2 = \Bbbk(\mathbf{X}_2)$ *изоморфны над полем констант*:

$$\mathcal{K}_1 \simeq_{\Bbbk} \mathcal{K}_2.$$

Несколько комментариев к этому определению.

(а) Поля $\mathcal{K}_1 \supset \Bbbk$ и $\mathcal{K}_2 \supset \Bbbk$ называются *изоморфными над* $\Bbbk$, если существует изоморфизм

$$\iota : \mathcal{K}_1 \xrightarrow{\simeq} \mathcal{K}_2,$$

тождественный на $\Bbbk$. Предостережение: в случае $\Bbbk = \mathbb{C}$ изоморфизм полей

$$\mathfrak{ff}\Big(\frac{\mathbb{C}[z,w]}{\langle -w^2 + z^3 + \mathrm{i}z + 1\rangle}\Big) \xrightarrow{\simeq} \Big(\frac{\mathbb{C}[z,w]}{\langle -w^2 + z^3 - \mathrm{i}z + 1\rangle}\Big),$$

определённый сопоставлением $(z.w) \mapsto (\overline{z}, \overline{w})$, не является изоморфизмом над $\mathbb{C}$.
(б) Поскольку главным содержанием этой лекции является связь между многочленами $f \in \Bbbk[x,y]$ и определёнными ими множествами нулей zer_f, более естественным могло бы показаться определение определение бирациональных изоморфизмов в терминах $\mathrm{zer}_{f_1} \simeq \mathrm{zer}_{f_2}$ (нетрудно, впрочем, убедиться, что многочлен $f \in \Bbbk[x,y]\setminus\Bbbk$ определяется множеством своих нулей zer_f однозначно с точностью до $\Bbbk^\times$-пропорциональности). Однако мы предпочли использовать обозначения вида $\mathcal{K} = \Bbbk(\mathbf{X})$, подчёркивающее связь кривой и для рациональных функций на ней; в дальнейшем мы будем придерживаться словосочетания $\mathbf{X}$ – *модель* (пока *плоская аффинная*) поля $\mathcal{K} = \Bbbk(\mathbf{X})$.
(в) Это же обозначение будет сохранено при более широком понимании понятия "кривая" $\mathbf{X}$, которое, однако, не потребует расширения класса рассматриваемых полей $\mathcal{K}$. Во всех случаях будут фигурировать множества $U \subset \mathbf{X}$, получаемые выбрасыванием из $\mathbf{X}$ конечных (иногда пустых) множеств точек, таких, что $\mathcal{K} = \mathfrak{ff}\big(\Bbbk[U]\big)$.

1.3.1. Определение множества $\mathcal{M}(\Bbbk)$. Здесь нам полезно будет обозначение

для уже фигурировавшего множества *неприводимых* многочленов

$$\Bbbk_{\mathrm{irr}}[x,y] \subset \Bbbk[x,y].$$

На всякий случай, введя для $d \in \mathbb{N}_{>0}$ обозначение

$$\Bbbk[x,y]_d := \Big\{ \sum_{i+j=d} a_{ij} x^i y^j \mid a_{ij} \in \Bbbk, \exists i \in \{0,\dots,d\} : a_{i,d-i} \neq 0 \Big\}.$$

для множества многочленов степени d, уточним

$$\Bbbk_{\mathrm{irr}}[x,y] := \Bbbk[x,y] \setminus \Big(\{0\} \coprod \coprod_{d_1,d_2 \in \mathbb{N}_{>0}} \Bbbk[x,y]_{d_1} \cdot \Bbbk[x,y]_{d_2} \Big).$$

Теперь мы готовы ввести главный объект настоящей лекции

$$\boxed{\mathcal{M}(\Bbbk) := \frac{\{\mathrm{zer}_f \mid f \in \Bbbk_{\mathrm{irr}}[x,y]\}}{\simeq}}$$

Пространство модулей (всех) кривых – это множество плоских аффинных кривых с точностью до бирационального изоморфизма.

По определению, это множество снабжено сюръекцией

$$\Bbbk_{\mathrm{irr}}[x,y] \twoheadrightarrow \mathcal{M}(\Bbbk).$$

1.3.2. Заключение. Мы определили пространство модулей кривых как множество; предстоит определить на этом множестве ряд структур. Окажется, что единственный дискретный инвариант в мире кривых, род, разбивает пространство модулей на подмножества, наделёнными естественной (хотя потребовался чуть ли не век, чтобы выработать строгие определения) структурой конечномерных алгебраических многообразий.

Задача ближайших лекций – ввести эти структуры.

Приложение: что такое многочлен?

Вопрос может показаться несколько обидным для человека для человека хотя бы со средним образованием. И даже студентам младших курсов современных (механико-) математических факультетов любых университетов известно определение-обозначение

$$\Bbbk[x,y] := \Big\{ \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} x^i y^j \mid m,n \in \mathbb{N}, a_{ij} \in \Bbbk \Big\}$$

(мы тоже им пользовались).

Однако не вполне ясны ответы на следующие **вопросы**:

- Что такое $x, y, \dots$?

  Вот мы определяем окружность: $\mathbf{S}^1 := \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 1\}$. Здесь явно $x \in \mathbb{R}$ и $y \in \mathbb{R}$ – например, мы радостно находим точку на окружности $(x,y) = (\frac{3}{5}, \frac{4}{5}) \in \mathbf{S}^1$.

С другой стороны, когда мы определяем *кольцо регулярных функций на окружности* $\mathbb{R}[\mathbf{S}^1] := \frac{\mathbb{R}[x,y]}{\langle x^2+y^2-1\rangle}$, то явно $x, y : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ – *абсцисса* и *ордината*, вещественнозначные функции на вещественной плоскости.

•Что такое f?

В частности, какая запись правильнее:

$$f \text{ или } f(x,y) \in \Bbbk[x,y]?$$

В первом случае f – элемент кольца полиномов, во втором – функция двух переменных $\Bbbk \times \Bbbk \to \Bbbk$. Кстати, над конечными полями многочлен и определяемая им функция – разные объекты, например, над $\mathbb{F}_p$ многочлен $x^p = x$ тождественно равен нулю.

•Что такое $\Bbbk[x,y]$? Определение было дано, так что уточним вопрос: *какова роль букв x, y в определении кольца* $\Bbbk[x,y]$?

Проще обсудить этот вопрос для кольца многочленов одной переменной

$$\Bbbk[x] := \{a_0 + a_1 x + a_2 x^2 + \dots\} \longleftrightarrow \{(a_0, a_1, a_2, \dots)\}$$

– действительно, почему бы не отождествить многочлен с последовательностью его коэффициентов?

После такого отождествления сложение в кольце $\Bbbk[x]$ оказывается очевидным (покоэффициентным), а умножение – неочевидным и определяемым формулой[6]

$$(a_0, a_1, a_2, \dots)(b_0, b_1, b_2, \dots) := (a_0 b_0, a_0 b_1 + a_1 b_0, a_0 b_2 + a_1 b_1 + a_2 b_0, \dots);$$

именно для обоснования этой формулы нужно вернуться к традиционным многочленам, и тогда формула

$$(a_0 + a_1 x + a_2 x^2 + \dots)(b_0 + b_1 x + b_2 x^2 + \dots) =$$

$$+ a_0 b_0 + (a_0 b_1 + a_1 b_0) x + (a_0 b_2 + a_1 b_1 + a_2 b_0) x^2 + \dots$$

следует из *дистрибутивности...*– но ГДЕ? Мы ведь в процессе построения умножения в ещё не определённом кольце!

Таким образом, буква x в кольце $\Bbbk[x]$ играет некоторую символическую роль, всего лишь обосновывая своеобразное умножение. Не вполне ясно, кольца $\Bbbk[x]$ и $\Bbbk[y]$ – изоморфные кольца или одно и то же кольцо с использованием разных букв для обоснования естественности определения умножения...

Те же проблемы действуют и в кольцах $\Bbbk[x,y] := \Bbbk[x][y]$ и т. п.

***

Теоретически можно было бы предложить следующие **ответы**:

• Кольца $\Bbbk[x]$, $\Bbbk[x,y]$, ... и поля $\Bbbk(x)$, $\Bbbk(x,y)$, ... считать известными и понятными; не вдаваться в обсуждение фигурирующих в них букв.

---

[6] эта формула называется *свёрткой*, а само определение (правда, не в кольце многочленов $\Bbbk[x]$, а в большем кольце *формальных степенных рядов* $\Bbbk[[x]]$) сводится к построению *полугруппового кольца* $\Bbbk[\mathbb{N}^+]$/ Конструкция немного проясняется, если отождествить аддитивный моноид $\mathbb{N}^+$ с мультипликативным $\{x^n \mid n \in \mathbb{N}\}$.

• Использовать возможности TeXa для различения разновидностей использования традиционных букв, например

$$x, y, \dots \in \Bbbk(x, y, \dots) \text{ для переменных;}$$

$$\mathrm{x}, \mathbf{y}, \dots \in \Bbbk \text{ для констант;}$$

$$\mathsf{x}, \mathsf{y}, \dots \in \Bbbk \text{ для символов.}$$

• Считать основным обозначение $f \in \Bbbk[x, y]$, а для соответствующих полиномиальных функций использовать какое-нибудь обозначение вроде

$$\underline{f} : \Bbbk \times \Bbbk \longrightarrow \Bbbk : (\mathrm{x}, \mathbf{y}) \mapsto \underline{f}(\mathrm{x}, \mathbf{y}).$$

Однако за такими обозначениями было бы трудно следить, и их использование неоправданно отклонялось бы от традиций современной алгебро-геометрической литературы. Поэтому мы пойдём другим путём.

***

Будем в основном следовать традициям (понимая буквы в зависимости от контекста). Но подойдём к кольцам многочленов с позиций **универсальной алгебры.**

Напомним соответствующее (взрослое) определение. Для множества *переменных* $\mathcal{X}$ (типичные примеры: $\mathcal{X} = \{x\}$, $\mathcal{X} = \{x, y\}$, ...) вводится категория (см. [**Ленг1968**], [**Маклейн2004**])

$$^{[\mathcal{X}]}\Bbbk := \{\{(A, \iota) \mid\mid A \in\in \Bbbk\text{-}\mathcal{ALG}, \iota : \mathcal{X} \dashrightarrow A\}\},$$

объекты которой – пары ($\Bbbk$-алгебра A, отображение множеств $\iota : \mathcal{X} \dashrightarrow A$), а

$$\mathrm{Mor}\big((A, \iota), (A', \iota')\big) := \{\alpha : A \to A' \mid \iota' \circ \alpha = \iota\}.$$

Кольцо многочленов – начальный объект этой категории. Здесь снова возникает проблема обозначений, потому что хочется обозначить первую компоненту этого объекта $\Bbbk[\mathcal{X}]$, но такое обозначение очевидно конфликтовало бы с уже принятыми $\Bbbk[x]$, $\Bbbk[x, y]$ и т.д. Здесь мы, однако, позволим себе использовать чисто TeXовский трюк – нестандартный размер скобок[7] (обсуждаемая конструкция больше не будет фигурировать в курсе).

Итак, обозначаем начальный объект категории $^{[\mathcal{X}]}\Bbbk$ через

$$\Big(\Bbbk\Big[\mathcal{X}\Big], \iota_{\mathcal{X}}\Big).$$

Тогда для любого объекта $(A, \iota) \in\in^{[\mathcal{X}]} \Bbbk$ определён морфизм $\alpha : \Bbbk\Big[\mathcal{X}\Big] \to A$, удовлетворяющий $\alpha \circ \iota_{\mathcal{X}} = \iota$. Особенно важен случай $A = \Bbbk$; обозначим вторую компоненту этого объекта plug. Это – подстановка "числовых" значений на места переменных; в отвергнутых выше нетрадиционных обозначениях можно было бы использовать запись $\mathsf{plug} : \mathcal{X} \to \Bbbk : x \mapsto \mathrm{x}, \dots$. Если ещё обозначить $\alpha = \mathsf{eval} : \Bbbk\Big[\mathcal{X}\Big] \to \Bbbk$, то $\mathsf{eval} \circ \iota_{\mathcal{X}} = \mathsf{plug}$ – это и есть процедура вычисления значения многочлена при подстановке числовых значений на место переменных.

---

[7] по принятому соглашению $\Bbbk[x] = \Bbbk\Big[\{x\}\Big]$. Такого рода обозначение необходимо было бы при построении алгебраического замыкания поля, где используется $\Bbbk\Big[\mathcal{X}\Big] = \Bbbk\Big[\Bbbk_{\mathrm{irr}}[x]\Big]$.

Но работать в таких громоздких обозначениях, конечно, невозможно. Поэтому, доказав, что $\iota_{\mathcal{X}}$ инъективно, мы вложим с его помощью $\mathcal{X}$ в $\Bbbk\Big[\mathcal{X}\Big]$ и затем для $f \in \Bbbk\Big[\mathcal{X}\Big]$ и $x \in \mathcal{X}$ введём полузаконное сокращение

$$f(x) := \mathsf{eval}(f),$$

реализующее отображение "значение многочлена" $\Bbbk\Big[\mathcal{X}\Big] \times \Bbbk^{\mathcal{X}} \to \Bbbk$.

Список литературы

[**АтьяМакдональд1972**] М. Атья, И. Макдональд, *Введение в коммутативную алгебру.* МЦНМО, 2012.

[**Варден1975**] Ван дер Варден, *Алгебра.* — М:, Наука, 1975.

[**Ленг1968**] С. Ленг, *Алгебра.* — М:, Мир, 1968.

[**Маклейн2004**] С. Маклейн, *Категории для работающего математика.* М., ФИЗМАТЛИТ, 2004.

[**Манин2012**] Ю.И. Манин, *Введение в теорию схем и квантовые группы.* МЦНМО, 2012.

[**Серр1968**] Ж.-П. Серр, *Алгебраические группы и поля классов.* Перев. с франц. — М.: Мир, 1968.

[**Шафаревич2007**] И.Р. Шафаревич, *Основы алгебраической геометрии.* МЦНМО, 2007.