09.8.7 / 09.10.30

Лекция 2 (21 сентября 2009)
Ньютон и эллиптические кривые (II).

2.0. Сводка результатов лекции 1. Мы ввели (вслед за Ньютоном...) несколько алгебраических кривых и дифференциалов на них, интегралы от которых имеют физический или геометрический смысл. Соберём их в таблицу.

Кривая	Уравнение или система	Дифференциал	Смысл интеграла
(1.8.1)	$\frac{1}{\rho^2} = 2E + \frac{2\gamma}{r} - \frac{\Sigma^2}{r^2}$	$\rho \mathrm{d}r$	время
(1.12.4)	$\zeta^2 = (1-\xi^2)(1+\epsilon^2-2\epsilon\xi)$	$r_0 \cdot \frac{1-2\epsilon\xi+\epsilon^2}{(1-\epsilon\xi)^2} \cdot \frac{\mathrm{d}\xi}{\zeta}$	путь
(1.13.3),(1.13.4)	$\begin{cases} \xi^2+\eta^2=1 \\ (1-\xi^2)(1+\epsilon^2-2\epsilon\xi)=\zeta^2 \end{cases}$	$\frac{\mathrm{d}\xi}{\eta}$ $\sqrt{\frac{r_0^3}{\gamma}} \cdot \frac{\mathrm{d}\xi}{\eta(1-\epsilon\xi)^2}$ $r_0 \frac{\mathrm{d}\xi}{(1-\epsilon\xi)^2}$	угол время расст. до Солнца
(1.14.1),(1.15.2)	$\begin{cases} \frac{X^2}{a^2}+\frac{Y^2}{b^2}=1 \\ X^2+Y^2+Z^2=a^2+b^2 \end{cases}$	$\frac{b}{a}\frac{Z\mathrm{d}X}{Y}$	длина
(1.16.7)	$v^2 = 1+(4\frac{a^2}{b^2}-2)u^2+u^4$	$2b\frac{v\mathrm{d}u}{(1+u^2)^2}$	длина
(1.18.2)	$V^2 = (1+U^2)(1+\frac{a^2}{b^2}U^2)$	$b\frac{V\mathrm{d}U}{(1+U^2)^2}$	длина

Одна из важных черт всех этих дифференциалов заключается в том, что, за исключением (1.8.1), *при общих значениях параметров* они *не* интегрируются в элементарных функциях. Простейшее объяснение этого явления: кривая (1.8.1) над полем комплексных чисел гомеоморфна проколотой сфере (её *род* равен нулю), тогда как остальные кривые гомеоморфны проколотому тору (имеют *род* один). Подробнее о топологии комплексных кривых мы поговорим в лекции ???.

Рассмотренные нами пять кривых рода 1 заданы четырьмя разными способами: (1.12.4) – как плоская кубическая кривой, (1.13.4),(1.13.4) – как пересечение *цилиндра над кубической кривой* со сферой, (1.14.1),(1.15.2)

– как пересечение двух квадрик, а кривые (1.16.7) и (1.18.2) – как плоские *квартики,* т.е. кривые степени 4, специального (лежандрова) вида.

В задачах 2.1.,2.2,2.3 вам предлагается убедиться в том, что все эти кривые преобразуются в плоские кубические, чем и объясняется основной предмет сегодняшней лекции.

2.1. Классификация эллиптических интегралов. Мы сформулируем классические результаты в классической терминологии, следуя в основном **[ГурвицКурант1968,** стр. 247-252**]**, однако будем пользоваться обозначениями, по возможности совместимыми с нашими рассмотрениями. Кроме того, фактическое интегрирование мы отложим до лекции ???, а сейчас речь пойдёт о *неопределённом* интегрировании. Таким образом, приводимые результаты относятся по существу к *дифференциальной алгебре* и имеют смысл над произвольным полем.

Итак, под *эллиптическим интегралом* мы будем понимать неопределённый интеграл вида

$$\int R(x,y)\mathrm{d}x, \qquad (\mathbf{2.1.1})$$

где x и y предполагаются связанными полиномиальным соотношением

$$y^2 = F(x); \qquad (\mathbf{2.1.2})$$

здесь $F \in \mathbb{C}[x]$ – ненулевой многочлен третьей или четвёртой степени без кратный корней (при наличии кратных корней интеграл (2.1.1) берётся в элементарных функциях), а $R \in \mathbb{C}[x,y]$ – произвольная рациональная функция, знаменатель которой не обращается тождественно в ноль на кривой (2.1.2).

В самодостаточном виде интеграл (2.1.1), разумеется, имеет вид

$$\int R(x,\sqrt{F(x)})\mathrm{d}x; \qquad (\mathbf{2.1.3})$$

очевидный недостаток этой записи заключается в том, что в комплексной области требуются оговорки о выборе значения квадратного корня. С принятой нами точки зрения (неопределённого интегрирования, или дифференциальной алгебры) проблем не возникает: корень из многочлена – это просто элемент алгебраической структуры с известными

правилами возведения в квадрат и дифференцирования. Мы будем пользоваться обеими записями, приписывая многочлену F индекс 3 или 4, означающий его степень, в тех случаях, когда эта степень существенна.

Теперь мы готовы к введению классической терминологии – не вполне, увы, совпадающей с применяемой во многих справочниках, но по существу равносильной ей.

Интеграл (2.1.1) называется интегралом *первого рода,* если он преобразуется к интегралу вида

$$\int \frac{\mathrm{d}x}{y} = \int \frac{\mathrm{d}x}{\sqrt{F(x)}}, \qquad (\mathbf{2.1.4})$$

интегралом *второго рода,* если преобразуется к интегралу вида

$$\int \frac{x\mathrm{d}x}{y} = \int \frac{x\mathrm{d}x}{\sqrt{F_3(x)}}, \qquad (\mathbf{2.1.5})$$

и интегралом *третьего рода,* если преобразуется к интегралу вида

$$\int \frac{x\mathrm{d}x}{y} = \int \frac{x\mathrm{d}x}{\sqrt{F_4(x)}}. \qquad (\mathbf{2.1.6})$$

Теорема. *Любой эллиптический интеграл представим в виде суммы четырёх*

$$\int_0 + \int_1 + \int_2 + \int_3, \qquad (\mathbf{2.1.7})$$

где $\int_0$ *является элементарной функцией, а интегралы* $\int_{1,2,3}$ *являются интегралами соответственно первого, второго и третьего рода.*

Доказательство существенно более общей теоремы будет проведено современными средствами в лекции ???; тогда же рассмотренные нами интегралы будут приведены к указанному виду.

Замечание. Некоторые интегралы третьего рода, обнаруженные Н.-Х.Абелем, берутся в элементарных функциях. Мы поговорим о них в лекции ???.

КЛАССИФИКАЦИЯ КУБИЧЕСКИХ КРИВЫХ ПО НЬЮТОНУ

The chief Properties of the Conic Sections are everywhere treated of by Geometers; and of the same Nature are the Properties of the Curves of the Second Gender...

If, of the equation $ax^3 + bxx + cx + d$ *all the Roots... are real and unequal, then the Figure is a diverging Parabola of the form of a Bell, with an oval...*

I. Newton

2.2. Алгебро-геометрическое введение. Традиционная алгебраическая геометрия изучает множества, задаваемые системами полиномиальных уравнений. В разные эпохи популярны были разные кольца (или полукольца) и поля, из которых брались коэффициентов полиномов и в которых решались системы уравнений. Иногда такие выборы представлялись очевидными; например, Ньютон изучал *плоские вещественные кривые* , т.е. множества вещественных решений одного полиномиального уравнения с двумя неизвестными.

Уже в первой половине девятнадцатого века математики начали чувствовать ограничительность вещественной математики – например, офицер наполеоновской армии Ж.-В. Понселе в 1814 году в саратовском плену понял, что для лучшего понимания геометрии треугольника следует рассматривать *мнимые* точки пересечения вписанной и описанной окружностей. Кроме того, стало ясно, что все плоские окружности проходят через *бесконечные мнимые* точки. Начиная примерно с середины девятнадцатого века обычным стало рассматривать системы *однородных* полиномиальных уравнений в комплексном пространстве и изучать их комплексные решения.

В двадцатом веке естественной постепенно стала представляться замена поля комплексных чисел на произвольное алгебраически замкнутое поле $\Bbbk$. Таким образом, естественная арена традиционной алгебраической

геометрии – n-мерное проективное пространство $\mathbb{P}_n(\Bbbk)$; мы будем пользоваться в нём однородными координатами $(x_0 : x_1 : \cdots : x_n)$. Итак, изучаемые множества суть пересечения *гиперповерхностей,* т.е. множеств (классов пропорциональности ненулевых) решений уравнений вида

$$\sum_{i_0+\cdots+i_d=0} c_{i_0\ldots i_d} x_0^{i_0} \ldots x_n^{i_d} = 0;$$

здесь подразумевается, что все коэффициенты $c_{i_0\ldots i_d}$ лежат в $\Bbbk$ и что не все они одновременно равны нулю. Число d называется *степенью* гиперповерхности, а сама гиперповерхность называется $(n-1)$-мерной.

2.3. Плоские кубические кривые. Выбор $(n = 2, d = 3)$ даёт простейший истинно нетривиальный алгебро-геометрический объект. Действительно, случай $n = 1$ даёт гиперповерхности, состоящие из конечного числа точек, а случай $d = 1$ – гиперплоскости. Выбор $d = 2$ приводит к изучению *квадрик,* и, хотя их теория достаточно интересна (см., например, **[ГриффитсХаррис198?**, т.2., стр.???**]**), они весьма похожи на проективные пространства: проектирование из любой точки квадрики на любую гиперплоскость, не содержащую этой точки, определяет *почти* изоморфизм (*бирациональный* изоморфизм, т.е. изоморфизм вне множества положительной коразмерности) квадрики с гиперплоскостью. Таким образом, степень $d = 3$ – наименьшая, от которой можно ждать интересной алгебраической геометрии, и в наименьшей разумной размерности $n = 2$ эти ожидания вполне оправдываются.

Итак, *плоская кубика* задаётся в $\mathbb{P}_n(\Bbbk)$ уравнением

$$\begin{gathered} 0 = \sum_{i_0+i_1+i_2=3} c_{i_0 i_1 i_2} x_0^{i_0} x_1^{i_1} x_2^{i_2} = \\ = c_{300}x_0^3 + \\ + c_{210}x_0^2x_1 + c_{201}x_0^2x_2 + \\ + c_{120}x_0x_1^2 + c_{111}x_0x_1x_2 + c_{102}x_0x_2^2 + \\ + c_{030}x_1^3 + c_{021}x_1^2x_2 + c_{012}x_1x_2^2 + c_{003}x_2^3. \end{gathered} \qquad (\mathbf{2.3.0})$$

От десяти коэффициентов $c_{300}, \ldots, c_{003}$) для начала требуется лишь то, чтобы они не обращались в ноль все одновременно; поскольку при умножении всех коэффициентов на одну и ту же ненулевую константу кривая

не меняется, можно считать, что

$$(c_{300} : \cdots : c_{003}) \in \mathbb{P}_9(\Bbbk).$$

Таким образом, мы работаем с *девятипараметрическим* семейством плоских кубик.

2.4. Проективные преобразования. На проективной плоскости $\mathbb{P}_2(\Bbbk)$ действует *группа проективных преобразований*

$$\mathsf{PGL}_3(\Bbbk) := \frac{\mathsf{GL}_3(\Bbbk)}{\Bbbk^\times},$$

где мультипликативная группа поля $\Bbbk^\times$ подразумевается вложенной в группу $\mathsf{GL}_3(\Bbbk)$ как группа диагональных (скалярных) матриц, а матрицы из $\mathsf{GL}_3(\Bbbk)$ действуют на тройках координат обычным образом.

Действуя на точках проективной плоскости $\mathbb{P}_2(\Bbbk)$, группа $\mathsf{PGL}_3(\Bbbk)$ действует и на её подмножествах, переводя, в частности, кубики в кубики (постарайтесь очень подробно объяснить себе, почему). Кубики, переводимые друг в друга проективными преобразованиями, называются *проективно эквивалентными;* очевидно, все *внутренние* свойства проективно эквивалентных кубик совпадают.

Таким образом, на девятимерном множестве кубик $\mathbb{P}_9(\Bbbk)$ действует восьмимерная группа $\mathsf{PGL}_3(\Bbbk)$, а нас интересует фактор-множество множества кубик по этому действию – естественно ожидать, что оно окажется одномерным.

Однако у рассматриваемого действия группы на проективном пространстве имеются "плохие" орбиты: например, произведение трёх линейных форм задаёт треугольник. Нас же в основном интересуют *неприводимые гладкие* кубики – хотя, как мы увидим, для лучшего понимания некоторых вопросов полезно рассматривать их вырождения.

Полный анализ всех типов орбит и их взаимного расположения можно найти, например, в книге **[Крафт2000].**

Условие гладкости общей кубики (2.3.0) весьма громоздко, и мы его не

приводим; оно является "кубическим" аналогом условия невырожденности матрицы квадратичной формы, определяющей конику.

Для решения этой и других связанных с кубиками задач надо найти *удобные* системы координат; этот вопрос является аналогом приведения квадратичной формы к *сумме квадратов.*

Предварительно мы обсудим явление, представляющее самостоятельный интерес и отсутствующее в случае коник.

2.5. Перегибы плоских кубик. По определению, гладкая точка кубической кривой называется её *точкой перегиба,* если касательная в этой точке имеет с кривой *трёхкратное* касание. Это определение подразумевает, что точка не лежит на компоненте, являющейся прямой (для кубик наличие такой компоненты равносильно приводимости).

Гессианом однородной формы от трёх переменных называется определитель матрицы, составленной из вторых частных производных формы – см., например, **[Клейн1989]**. Вырожденным кубикам посвящаются задачи 2.7. и 2.8., а мы в дальнейшем будем предполагать, что рассматриваемые кубики неприводимы. В этом случае можно установить, что *кубика пересекается с кривой, определённой обращением в ноль её гессиана, по крайней мере в трёх и не более чем в девяти точках.*

Более того, как хорошо известно, *точки перегиба неприводимой плоской кубики определяются обращением в ноль гессиана определяющей её формы* – см. **[Клейн1989]**. Таким образом, на неприводимой плоской кубике имеется по крайней мере три точки перегиба.

2.6. Помещение прямой перегиба в бесконечность. Пусть прямая перегиба является "бесконечной", т.е. задаётся уравнением $x_0 = 0$, и пусть точка перегиба на ней имеет координаты $(0 : 0 : 1)$. Тогда можно положить $(c_{030} : c_{021} : c_{012} : c_{003}) = (1 : 0 : 0 : 0)$, и уравнение (2.3.0) примет вид

$$\begin{gathered} 0 = c_{300}x_0^3 + \\ + c_{210}x_0^2x_1 + c_{201}x_0^2x_2 + \\ + c_{120}x_0x_1^2 + c_{111}x_0x_1x_2 + c_{102}x_0x_2^2 + x_1^3. \end{gathered} \qquad (\mathbf{2.6.1})$$

Перейдём к аффинным координатам

$$x = \frac{x_1}{x_0}, y = \frac{y_1}{x_0}; \qquad (\mathbf{2.6.2})$$

после деления на x_0^3 уравнение (2.6.1) превратится в

$$0 = c_{300} + c_{210}x + c_{201}y + c_{120}x^2 + c_{111}xy + c_{102}y^2 + x^3. \qquad (\mathbf{2.6.3})$$

Заметим, что в случае $c_{102} = 0$ уравнение (2.6.2) разрешимо относительно координаты y и потому задаёт *рациональную* кривую. Пренебрежём этим случаем и предположим, что $c_{102} \neq 0$; воспользовавшись масштабным преобразованием по y (мы работаем над алгебраически замкнутым полем!), будем считать, что $c_{102} = -1$. Уравнение (2.6.2) станет равносильно уравнению

$$y^2 = c_{300} + c_{210}x + c_{201}y + c_{120}x^2 + c_{111}xy + x^3. \qquad (\mathbf{2.6.4})$$

Следуя Джону Тейту (см. **[Silverman1986]**), введём новые обозначения

$$a_1 := -c_{111}, a_2 := c_{120}, a_3 := -c_{201}, a_4 := c_{210}, a_6 = c_{300} \qquad (\mathbf{2.6.5})$$

и преобразуем уравнение (2.6.4) в так называемое *минимальное уравнение Вейерштрасса-Тейта*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \qquad (\mathbf{2.6.6})$$

Коэффициенты $a_1, \ldots, a_6$ пронумерованы в нём так, чтобы преобразованию координат $x \leftarrow \lambda^2 x, y \leftarrow \lambda^3 y$ сопутствовало преобразование коэффициентов $a_k \leftarrow \lambda^k a_k$ (уравнение (2.6.6) умножится при таких преобразованиях на λ^6).

Минимальное уравнение Вейерштрасса-Тейта используется для исследования кубических кривых над *произвольными* полями (любых характеристик) и, видимо, над всеми полями разом не допускает дальнейших упрощений; во всяком случае, современной математике такие упрощения неизвестны. Для нас, однако, интересующихся в основном алгебраической геометрией над $\mathbb{C}$, это уравнение является лишь промежуточным этапом на пути к гораздо более коротким уравнениям.

2.7. Дальнейшие преобразования и подсчёт параметров. Мы начинали с десятипараметрического семейства уравнений плоских кубик, наборы коэффициентов которых пробегали *девятимерное проективное* пространство; на множестве этих уравнений действовала *восьмимерная* група преобразований координат.

Теперь у нас остались коэффициенты a_1, a_2, a_3, a_4, a_6, пробегающие *пятимерное аффинное* пространство; аффинность возникла в результате выбранных нормировок (два коэффициента были приравнены нами к ± 1). Естественно ожидать, что на оставшихся коэффициентах действует *четырёхмерная* група преобразований координат.

Действительно, вид минимальных уравнений Вейерштрасса-Тейта (2.6.6) сохраняется при преобразованиях

$$x \leftarrow \lambda^2 x + \kappa,$$

$$y \leftarrow \lambda^3 y + \mu x + \nu.$$

С помощью этих преобразований мы вскоре сведём над $\mathbb{C}$ уравнение (2.6.6) к одной из канонических форм.

2.8. Гладкость. Уравнение Вейерштрасса-Тейта уже достаточно просто, чтобы условие гладкости задаваемой им кривой можно было выписать явно. Действительно, (единственная) точка нашей кубики на бесконечной прямой является точкой перегиба, т.е. заведомо имеет касательную (саму бесконечную прямую); поэтому достаточно проверить, что особых точек кубики нет на конечной части плоскости, т.е. уравнение кривой и две его частные производные не обращаются одновременно в ноль.

Иначе говоря, наша кубика гладка тогда и только тогда, когда система уравнений

$$\begin{cases} y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 & (\mathbf{2.8.0}) \\ a_1y = 3x^2 + 2a_2x + a_4 & (\mathbf{2.8.1}) \\ 2y + a_1x + a_3 = 0 & (\mathbf{2.8.2}) \end{cases}$$

несовместна. Выразив y через x из уравнения (2.8.2) (это можно сделать лишь при $\mathrm{char}\Bbbk \neq 2$!), мы сведём условие гладкости кубики к отсут-

ствию общих корней двух многочленов от x, т.е. к необращению в ноль соответствующего результанта. Вычисление (с помощью MAPLE...) даёт

$$0 \neq 3\,{a_1}^2{a_2}^2a_6 - \frac{9}{4}\,a_6{a_1}^3a_3 + \frac{15}{8}\,{a_1}^2a_4{a_3}^2 - \frac{1}{2}\,{a_1}^2{a_4}^2a_2 - \frac{1}{16}\,{a_1}^5a_4a_3 -$$
$$-\frac{9}{2}\,{a_3}^2a_2a_4 - \frac{9}{4}\,{a_3}^3a_2a_1 + \frac{1}{2}\,{a_2}^2{a_1}^2{a_3}^2 + \frac{1}{16}\,a_2{a_1}^4{a_3}^2 - \frac{9}{2}\,{a_1}^2a_4a_6 -$$
$$-18\,a_6a_2a_4 + \frac{3}{4}\,a_2{a_1}^4a_6 + 6\,a_1a_3{a_4}^2 - \frac{1}{16}\,{a_1}^4{a_4}^2 + \frac{27}{2}\,{a_3}^2a_6 - \frac{1}{16}\,{a_3}^3{a_1}^3 + 27\,{a_6}^2 -$$
$$-{a_2}^2{a_4}^2 + {a_2}^3{a_3}^2 + 4\,{a_2}^3a_6 + \frac{1}{16}\,{a_1}^6a_6 + 4\,{a_4}^3 - \frac{1}{2}\,{a_1}^3a_4a_2a_3 -$$
$$-{a_2}^2a_4a_1a_3 - 9\,a_6a_2a_1a_3 + \frac{27}{16}\,{a_3}^4.$$

2.9. Нормальная форма Вейерштрасса. Главный шаг в упрощении уравнения (2.6.6.) – уничтожение *перекрёстного членаа*$_1xy$. При $\mathrm{char}\Bbbk \neq 2$ оно достигается преобразованием

$$y \leftarrow y - \frac{a_1}{2}x.$$

Остальные преобразования проводятся независимо по x и y и при $\mathrm{char}\Bbbk \neq 2, 3$ обычным образом превращают уравнение в

$$y^2 = x^3 + ax + b; \qquad (\mathbf{2.9.0})$$

по причинам, которые будут объяснены в лекции ???, его принято записывать в виде

$$y^2 = 4x^3 - g_2x - g_3, \qquad (\mathbf{2.9.1})$$

который и называется *вейерштрассовой нормальной формой.*

Условие *гладкости* кривой сводится теперь к отсутствию кратных корней у правой части уравнения (2.9.1), которое равносильно

$$0 \neq g_2^3 - 27g_3^2. \qquad (\mathbf{2.9.2})$$

2.10. Инварианты. Уравнение (2.9.1) всё ещё зависит от двух параметров, а не от одного; это объясняется тем, что от группы преобразований исходного уравнения осталась однопараметрическая группа

$$x \leftarrow \lambda^2x,\ y \leftarrow \lambda^3y,\ g_2 \leftarrow \lambda^4g_2,\ g_3 \leftarrow \lambda^6g_3.$$

Традиционными инвариантами *гладкой* кубики относительно этой последней группы преобразований являются два отличающиеся в 1728 раз числа:

$$J := \frac{g_2^3}{g_2^3 - 27g_3^2} \qquad (\mathbf{2.10.1})$$

и

$$j = 1728J. \qquad (\mathbf{2.10.2})$$

Заметим, что в силу (2.9.2) оба инварианты определены для всех *гладких* кубик. Анализ инварианта (2.10.1) и появление (2.10.2) мы отложим до лекции ???. Часто рассматривается также инвариант

$$1 - J = \frac{27g_3^2}{g_2^3 - 27g_3^2}. \qquad (\mathbf{2.10.3})$$

2.11. Об универсальном семействе кубик. Хотелось бы избавиться от последней неоднозначности параметров в уравнении (2.9.1) и написать уравнение такого однопараметрического семейства кубик, чтобы каждая кубика с данным инвариантом входила в это семейство, причём только однажды.

Это, однако, невозможно: мешают кривые с *симметриями.* Лучшее, что можно сделать – ввести семейство Вейерштрасса-Тейта, в которое входят все гладкие кубики, кроме двух:

$$y^2 + xy = x^3 - \frac{36x + 1}{j - 1728} \text{ при } j \neq 0, 1728. \qquad (\mathbf{2.10.4})$$

Кубики со значениями инвариантов $j = 0$ и $j = 1728$ надо задавать отдельно: уравнениями

$$y^2 + y = x^3 \qquad (\mathbf{2.10.5})$$

(см. задачи 2.11 и 2.12) и

$$y^2 = x^3 + x. \qquad (\mathbf{2.10.6})$$

2.12. Групповой закон на гладких проективных кубиках. Пусть

$$C \subset \mathbb{P}_2(\Bbbk)$$

– гладкая проективная кубика, а

$$L \subset \mathbb{P}_2(\Bbbk)$$

– прямая. Имеются лишь следующие три возможности их взаимного расположения:

•$\#(C \cap L) = 3$, это – так называемый случай *общего положения*;
•$\#(C \cap L) = 2$, и прямая L касается кубики C в одной из точек пересечения;
•$\#(C \cap L) = 1$, и прямая L является прямой перегиба кубики C.

В соответствии с этими возможностями мы будем рассматривать на кубике C бинарные *ассоциативные* операции $\oplus$ с нейтральным элементом $\underline{0}$, обладающие следующими свойствами, формулируемыми относительно *произвольной* прямой L:

• если $\#(C \cap L) = 3$ и $C \cap L = \{P_1, P_2, P_3\}$, то

$$P_1 \oplus P_2 \oplus P_3 = \underline{0};$$

• если $\#(C \cap L) = 2$ и $C \cap L = \{P_1, P_2\}$, причём прямая L касается кубики C в точке P_1, то

$$P_1 \oplus P_1 \oplus P_2 = \underline{0};$$

• если $\#(C \cap L) = 1$ и $C \cap L = \{P\}$, то

$$P \oplus P \oplus P = \underline{0}.$$

Для того, чтобы фиксировать на гладкой проективной кубике *групповую* операцию $\oplus$, необходимо "назначить" нейтральный элемент $\underline{0}$. Оказывается, за нейтральный элемент может быть принята любая точка

$$\underline{0} \in C,$$

и это однозначно определяет операцию $\oplus$. Действительно, *взятие обратного*

$$P \mapsto \ominus P$$

в общем положении однозначно определяется условием коллинеарности точек $\underline{0}, P$ и $\ominus P$; в случаях необщего положения вносятся очевидные изменения. Теперь операция

$$(P, Q) \mapsto P \oplus Q$$

в общем положении однозначно определяется условием коллинеарности точек P, Q и $\ominus(P \oplus Q)$, а в случаях необщего положения доопределяется соответствующими изменениями или *по непрерывности.* .

Коммутативность введённой операции $\oplus$ на кубике C с (произвольно) выделенной точкой $\underline{0}$ очевидна; нетривиальным фактом, как это ни странно, является её ассоциативность. Мы можем свести проверку ассоциативности $\oplus$ к проверке (весьма громоздкого) алгебраического тождества; поскольку рассмотренные геометрические конструкции, очевидно, не зависят от выбора координат, достаточно проверить ассоциативность $\oplus$ в любой из введённых нормальных форм. Это предлагается проделать в задачах 2.14 и 2.15.

В лекциях ?? и ??? будут даны другие определения операции $\oplus$, при которых ассоциативность будет очевидна.

ЗАДАЧИ

2.1. Воспользовавшись уравнением (1.13.3), разрешите уравнение (1.13.4) относительно ξ. Подставив результат в (1.13.3), получите полиномиальное соотношение между η и ζ. Далее, воспользовавшись заменами

$$\eta = \frac{\left(1-\epsilon^2\right) v}{2\epsilon u^2},\ \zeta = \frac{\left(1-e^2\right)^{3/2} v}{2\epsilon u^3},$$

преобразуйте кривую к лежандроподобному виду. Проверьте обратимость проведённого преобразования.

2.2. Воспользовавшись тем, что гладкая квадрика в проективном пространстве над алгебраически замкнутым полем (например, над $\mathbb{C}$) двумя способами представима как объединение семейств своих прямолинейных образующих (и потому *изоморфна* произведению двух проективных прямых), реализуйте *общее* пересечение двух квадрик как двулистное накрытие проективной прямой, разветвлённое в четырёх точках. Представьте любое такое накрытие в виде кривой, заданной лежандроподобным уравнением. Примените полученные результаты, преобразовав кривую (1.14.1)-(1.15.2) к лежанрову виду (эти формулы можно также извлечь из лекции 1).

2.3. Пусть над произвольным алгебраически замкнутым полем $\Bbbk$ (например, над $\Bbbk = \mathbb{C}$) кривая задана *гиперэллиптическим* уравнением

$$V^2 = F(U),$$

где $F \in \Bbbk[U]$ – многочлен *чётной* степени (есть причины обозначить её $2g+2$) без кратных корней. Примените к координате U дробно-линейное преобразование, переводящее один из корней многочлена F в бесконечность. Покажите, что в результате этого преобразования та же кривая может быть задано уравнением

$$v^2 = f(u),$$

где $f \in \Bbbk[u]$ – теперь многочлен *нечётной* степени $2g+1$. Примените полученный результат к преобразованию лежандроподобных кривых в гладкие (проективные!) кубические кривые.

2.4. Найдите площадь фигуры, ограниченной *овалом* (т.е. компонентой связности, гомеоморфной окружности) плоской вещественной кривой, заданной уравнением

$$y^2 = x^3 - x.$$

2.5. Докажите, что, если в уравнении кубики $\sum_{i_0+i_1+i_2=3} c_{i_0 i_1 i_2} x_0^{i_0} x_1^{i_1} x_2^{i_2} = 0$ лишь один из коэффициентов $c_{i_0 i_1 i_2}$ отличен от нуля, то кубика является объединением прямых, а если лишь два, то кубика особа.

2.6. Докажите, что при $\mathrm{char}\Bbbk \neq 3$ *кубика Ферма,* задаваемая уравнением $x_1^3 + x_2^3 = x_0^3$, не допускает *полиномиальной униформизации,* т.е. не существует *непостоянных* многочленов $X_0, X_1, X_2 \in \Bbbk[t]$, удовлетворяющих этому уравнению. Отдельно разберите случай $\mathrm{char}\Bbbk = 3$.

Решение этой задачи можно найти в книге **[Шафаревич1972].** Сформулируйте и докажите аналогичное утверждение для *кубики Клейна,* задаваемой уравнением $x_0 x_1^2 + x_1 x_2^2 + x_2 x_0^2 = 0$.

2.7. Докажите, что гессиан формы, определяющей кубику, тождественно равен нулю тогда и только тогда, когда кубика является объединением прямых.

2.8. Докажите, что гессиан формы, определяющей приводимую кубику, приводим. Верно ли обратное?

2.9. Приведите к вейерштрассовой нормальной форме *кубику Ферма* (см. задачу 2.7).

2.10. Приведите к вейерштрассовой нормальной форме кубику, заданную уравнением (2.10.4)

$$y^2 + xy = x^3 - \frac{36x + 1}{j - 1728}$$

и вычислите её $j-$инвариант. Рассмотрите случаи всевозможных характеристик основного поля.

2.11. Проанализируйте кубику, заданную уравнением

$$y^2 + xy = x^3 + \frac{36x + 1}{1728}$$

при соответствующих ограничениях на характеристику основного поля.

2.12. Приведите к вейерштрассовой нормальной форме кубику, заданную уравнением (2.10.5)

$$y^2 + y = x^3$$

и вычислите её $j-$инвариант. Рассмотрите случаи всевозможных характеристик основного поля.

2.13. Приведите к вейерштрассовой нормальной форме кубику, заданную уравнением (2.10.6)

$$y^2 = x^3 + x$$

и вычислите её $j-$инвариант. Рассмотрите случаи всевозможных характеристик основного поля.

2.14. Найдите явный вид сложения на кубике в вейерштрассовой нормальной форме с бесконечной точкой, принятой за нейтральный элемент.

Указание. Начните с использования теоремы Виета для выражения $x(P_1 \oplus P_2)$ через $x(P_1)$ и $x(P_2)$.

2.15. Пользуясь результатами задачи 2.14, проверьте ассоциативность сложения на гладкой проективной кубике. Она окажется установленной в характеристиках, отличных от 2 и 3; чтобы проверить ассоциативность во *всех* характеристиках, попытайтесь проделать аналогичные действия для кривых в форме Вейерштрасса-Тейта.