

Независимый Московский Университет, осень 2020

Г.Б. Шабат,

ПЕРЕСЕЧЕНИЯ В ПРОСТРАНСТВАХ МОДУЛЕЙ КРИВЫХ-2

Лекция 1 (10 сентября 2020)

Пространства модулей кривых малых родов

1.0. Напоминания	1
...1.0.0. Обозначения	1
...1.0.1. Линейные расслоения и пространства Римана-Роха	2
...1.0.2. Теорема Римана-Роха	4
1.1. Кривые родов 0 и 1	4
...1.1.0. \mathcal{M}_0	4
...1.1.1. \mathcal{M}_1	5
1.2. О геометрической теории инвариантов	8
Литература	9

В этой лекции начинается обзор геометрии пространств модулей кривых над произвольным алгебраически замкнутым полем. Мы будем свободно пользоваться алгебро-геометрическими понятиями в объеме книг [Манин2012] и [Шафаревич2007]. Работая с кривыми, мы в основном следуем [Серп1968].

1.0. Напоминания

1.0.0. Обозначения. Основное поле $\mathbb{k} = \bar{\mathbb{k}}$ предполагается алгебраически замкнутым. Обычно мы работаем над $\mathbb{k} = \mathbb{C}$ и иногда над $\mathbb{k} = \bar{\mathbb{Q}}$ или $\mathbb{k} = \bar{\mathbb{F}}_p$, но сегодня \mathbb{k} произвольно.

Иногда поле для данной *схемы* (или, иногда точнее, для *функционала*) является "переменным", и тогда оно при необходимости указывается в скобках, как в случае *проективного пространства* $\mathbf{P}_n(\mathbb{k})$. Для нас наиболее важны примеры пространств *модулей*¹ \mathcal{M}_g , а функциональность будет проявляться в очевидных включениях вроде

$$\mathcal{M}_g(\bar{\mathbb{Q}}) \subset \mathcal{M}_g(\mathbb{C}).$$

Под *кривой* по умолчанию будет пониматься *неприводимая* (и, следовательно, *связная*) *полная гладкая* кривая над \mathbb{k} . Важную роль играет *поле рациональных функций* $\mathbb{k}(\mathbf{X})$, снабжённое для всех точек $P \in \mathbf{X}$ *нормированием* $\text{ord}_P : \mathbb{k}(\mathbf{X})^\times \rightarrow \mathbb{Z}$.

По каждой кривой \mathbf{X} строится частично упорядоченная свободная абелева группа *дивизоров* $\text{Div}(\mathbf{X})$, порождённая её точками:

$$\text{Div}(\mathbf{X}) := \bigoplus_{P \in \mathbf{X}} \mathbb{Z} P.$$

¹поскольку никаких других мы рассматривать не собираемся, слово *кривых* в сочетании *пространство модулей кривых* мы отныне будем опускать

Определён морфизм групп

$$\text{div} : \mathbb{k}(\mathbf{X})^\times \longrightarrow \text{Div}(\mathbf{X}) : f \mapsto \sum_{P \in \mathbf{X}} \text{ord}_P(f),$$

с помощью которого строится важнейший инвариант

$$\text{Pic}(\mathbf{X}) := \frac{\text{Div}(\mathbf{X})}{\text{div}(\mathbb{k}(\mathbf{X})^\times)}.$$

Дивизоры, лежащие образе морфизма div , называются *главными*. Два дивизора, отличающиеся на главный, называются *линейно эквивалентными*; для двух дивизоров $D_1, D_2 \in \text{Div}(\mathbf{X})$ их линейная эквивалентность, то есть принадлежность $D_1 - D_2 \in \text{div}(\mathbb{k}(\mathbf{X}))$, записывается в виде $D_1 \equiv D_2$.

Определён также морфизм групп

$$\deg : \text{Div}(\mathbf{X}) \longrightarrow \mathbb{Z} : \sum_{P \in \mathbf{X}} n_P P \mapsto \sum_{P \in \mathbf{X}} n_P.$$

Совсем другое отображение с тем же обозначением²:

$$\deg : \mathbb{k}(\mathbf{X}) \setminus \mathbb{k} \rightarrow \mathbb{N} : x \mapsto [\mathbb{k}(\mathbf{X}) : \mathbb{k}(x)]$$

сопоставляет непостоянной рациональной функции на кривой её *степень*, то есть (если понимать функцию как морфизм $\mathbf{X} \rightarrow \mathbf{P}_1$) мощность почти всех линий уровня.

Структура (абстрактной) алгебраической кривой \mathbf{X} , как и других алгебраических многообразий, которые нам встречаются, задаётся *структурным пучком* $\mathcal{O}_{\mathbf{X}}$, сопоставляющим каждому открытому множеству $U \subset \mathbf{X}$ конечно порождённую \mathbb{k} -алгебру $\mathcal{O}(U) \subseteq \mathbb{k}(\mathbf{X})$ функций, регулярных на U .

1.0.1. Линейные расслоения и пространства Римана-Роха. Все регулярные функции на полных кривых постоянны. Чтобы исследовать кривые с помощью функций на них, приходится ослабить требование регулярности. Это делается одним из двух, на первый взгляд разных, способов:

- Разрешить *полюса*; это заменяет функции на *почти функции*, то есть функции, определённые вне конечных множеств точек (их, впрочем, полезно считать всюду определёнными *накрытиями* проективной прямой $\mathbf{P}_1(\mathbb{k}) \simeq \mathbb{k} \coprod \{\infty\}$, но на множествах накрытий нет традиционных алгебраических структур);
- Относиться к обычным функциям как к *сечениям тривиального линейного расслоения*; тогда среди *нетривиальных* найдутся расслоения с достаточно богатыми запасами сечений.

Указанные подходы оказываются по существу равносильными. Линейные расслоения на кривой \mathbf{X} параметризуются дивизорами $D \in \text{Div}(\mathbf{X})$: если в покрытии $\mathbf{X} = \bigcup_{i \in I} U_i$ дивизор задаётся локальными уравнениями $D|_{U_i} = \text{div}(f_i) \cap U_i$, то расслоение L_D задаётся функциями перехода $t_{ij} = \frac{f_i}{f_j}$; важно подчеркнуть,

²используемые шрифты для аргументов, будем надеяться, предотвратят недоразумения...

что $t_{ij} \in \mathcal{O}^\times(U_{ij})$. Сечения такого расслоения задаются наборами регулярных функций $s_i \in \mathcal{O}(U_i)$, удовлетворяющих на пересечениях соотношениям $s_j = s_i t_{ij}$. Поскольку полюса рациональных функций можно "гасить" функциями перехода (которые могут иметь нули на множествах $U_i \setminus U_{ij}$), не всюду (а *почти всюду...*) определённые рациональные функции таким образом превращаются во всюду определённые сечения линейных расслоений.

Линейно эквивалентные дивизоры определяют *изоморфные* расслоения: если $D_1 \equiv D_2$, то $L_{D_1} \simeq L_{D_2}$.

Каждому линейному расслоению $L \xrightarrow{\pi} X$ сопоставляется пучок его *сечений*

$$\mathcal{L} : U \mapsto \{s : U \rightarrow L \mid \pi \circ s = \text{id}_U\}.$$

Естественно определяются *рациональные* сечения таких пучков³. Для множества всех таких сечений, обладающего структурой 1-мерного векторного пространства над $\mathbb{k}(X)$, общепринятого обозначения не выработано, и мы будем его использовать лишь в специальных случаях, а сейчас лишь ответим, что для такого ненулевого сечения $s : X \dashrightarrow L$ с помощью локальных координат определяется дивизор $\text{div}(s) \in \text{Div}(X)$.

Среди линейных расслоений над данной кривой X , помимо тривиального, выделяются *касательное* и *кокасательное*. Функции перехода для них при наличии *локальных параметров* $x_i \in \mathcal{O}(U_i)$ задаются выражениями $(\frac{dx_i}{dx_j})^{\pm 1}$, понимаемыми, как в анализе. Сечения этих расслоений интерпретируются как *дифференцирования* и *дифференциалы*. Пучок сечений кокасательного расслоения обозначается Ω_X^1 . Пространство его сечений, то есть *абелевых дифференциалов*, обозначается $\Omega^1[X]$. Размерность этого пространства – одно из определений *рода* кривой,

$$g_X := \dim_{\mathbb{k}} \Omega^1[X].$$

Пространство рациональных сечений кокасательного расслоения обозначается $\Omega^1(X)$; его элементы тоже называются *абелевыми дифференциалами* (классически – *первого, второго и третьего рода*⁴)

Поскольку для любых ненулевых дифференциалов $\omega_1, \omega_2 \in \Omega^1(X) \setminus \{0\}$ их отношение – ненулевая рациональная функция $\frac{\omega_1}{\omega_2} \in \mathbb{k}(X)^\times$, их дивизоры $\omega_1 \equiv \omega_2$ линейно эквивалентны. Класс этой линейной эквивалентности называется *каноническим классом* кривой и будет обозначаться $K_X \in \text{Pic}(X)$ или просто

$$K \in \text{Pic}(X).$$

Любой представитель канонического класса, далее называемый просто *каноническим*, будет традиционно обозначаться

$$K \in \text{Div}(X);$$

³Инвариантное определение см. в [Серр1968].

⁴в других языках терминологической коллизии не происходит: например, по-английски *род кривой* – это *genus of the curve*, а *дифференциал третьего рода* – это *differential of the third kind*.

иначе говоря, для любого $\omega \in \Omega^1(\mathbf{X}) \setminus \{0\}$ законно обозначение $\operatorname{div}(\omega) = K$.

Если $g_{\mathbf{X}} = g$, то

$$\deg K = 2g - 2.$$

Для каждого дивизора $D \in \operatorname{Div}(\mathbf{X})$ строится конечномерное над \mathbb{k} пространство Римана-Роха

$$L(D) := \{x \in \mathbb{k}(\mathbf{X}) \mid \operatorname{div}(x) + D \geq 0\};$$

важнейший инвариант дивизора – *размерность* этого пространства

$$\ell(D) := \dim_{\mathbb{k}} L(D).$$

В случае *очень обильного* дивизора любой базис $\langle x_0, \dots, x_n \rangle = L(D)$ определяет вложение

$$\iota_D = (x_0 : \dots : x_n) : \mathbf{X} \hookrightarrow \mathbf{P}_n,$$

которое считается зависящим только от дивизора D , поскольку при смене базиса пространства $L(D)$ образ кривой $\iota_D(\mathbf{X})$ изменится лишь на проективное преобразование.

1.0.2. Теорема Римана-Роха. *Пусть \mathbf{X} – кривая рода g , на ней дан произвольный дивизор $D \in \operatorname{Div}(\mathbf{X})$ и канонический дивизор K . Тогда*

$$\boxed{\ell(D) - \ell(D - K) = d - g + 1} \quad (1.0.2a)$$

Следствие. *В условиях теоремы выполняется неравенство Римана-Роха*

$$\ell(D) \geq d - g + 1 \quad (1.0.2b)$$

Следствие. *В условиях теоремы если $d \geq 2g - 1$, то*

$$\ell(D) = d - g + 1 \quad (1.0.2c)$$

При ссылке на любое из этих утверждений мы иногда будем пользоваться аббревиатурой RR.

1.1. Пространства модулей малых родов

1.1.0. \mathcal{M}_0 . Здесь нет интересной геометрии, поскольку для любого \mathbb{k} пространство $\mathcal{M}_0(\mathbb{k})$ одноточечно. Однако оно нам ещё пригодится при обсуждении *комбинаторных* пространств модулей.

Проанализируем кривые рода 0 с помощью теоремы Римана-Роха. Пусть \mathbf{X} – такая кривая; выберем на ней произвольную точку, которую в соответствии с традицией обозначим $\underline{\infty} \in \mathbf{X}$. Согласно RR,

$$\ell(\underline{\infty}) = 2,$$

поэтому найдётся

$$x \in L(\underline{\infty}) \setminus \mathbb{k}.$$

Поскольку⁵ $\deg(x) = 1$, функция x осуществляет биекцию кривых

$$\mathbf{X} \xrightarrow{\sim} \mathbf{P}_1(\mathbb{k})$$

⁵решите задачу 1.1

и изоморфизм полей

$$\mathbb{k}(\mathbf{X}) \simeq \mathbb{k}(x).$$

1.1.1. \mathcal{M}_1 . Пусть \mathbf{X} – кривая рода 1. Снова выберем на ней произвольную точку, которую снова обозначим $\underline{\infty} \in \mathbf{X}$ (поскольку будем называть *бесконечной*). По теореме Римана-Роха

$$\ell(2\underline{\infty}) = 2 \text{ и } \ell(3\underline{\infty}) = 3,$$

поэтому найдутся

$$x \in L(2\underline{\infty}) \setminus \ell(2\underline{\infty})$$

и

$$y \in L(3\underline{\infty}) \setminus \mathbb{k}.$$

Тогда семь функций (одна из которых – константа)

$$x^3, y^2, xy, x^2, y, x, 1$$

имеют в $\underline{\infty}$ полюса не выше шестого порядка, то есть

$$\{x^3, y^2, xy, x^2, y, x, 1\} \subset L(6\underline{\infty}).$$

Но по теореме Римана-Роха $\dim L(6\underline{\infty}) = 6$, так что эти семь функций связаны нетривиальным линейным соотношением; предварительно запишем его в виде

$$ax^3 + by^2 + cxy + dx^2 + ey + fx + g = 0. \quad (1.1.1a)$$

Заметим, что $ab \neq 0$ – решите задачу **1.2**. В силу этого соотношение (1.1.1a) можно переписать в *форме Тейта*, имеющей глубокий арифметический смысл (см. [Silverman2009], стр. 46):

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \quad (1.1.1b)$$

Для всех возможных основных полей более компактной записи, видимо, не существует. Однако при $\text{char}(\mathbb{k}) \notin \{2, 3\}$ (далее принимаем это предположение) линейными заменами функций x, y уравнение может быть сильно упрощено: (см. [Silverman2009], стр. 48). Введём обозначение для получаемой плоской аффинной кривой (такие кривые по историческим причинам называются *эллиптическими*)

$$\dot{\mathbf{E}}_{c_1, c_2} : y^2 = x^3 - 27c_4x - 54c_6. \quad (1.1.1c)$$

Это кривая $\dot{\mathbf{E}}_{c_1, c_2} \subset \mathbf{A}_2(\mathbb{k})$ гладка тогда и только тогда, когда

$$c_4^3 \neq c_6^2 \quad (1.1.1d)$$

– см. задачу **1.3**.

Введём также обозначение для *проколотой* (абстрактной!) кривой

$$\dot{\mathbf{X}} := \mathbf{X} \setminus \{\underline{\infty}\};$$

нами построен морфизм

$$(x, y) : \dot{\mathbf{X}} \longrightarrow \dot{\mathbf{E}}_{c_1, c_2}.$$

На самом деле это – *изоморфизм*⁶, но убедиться в этом удобнее, перейдя к дополнению и проективизации.

⁶ Я благодарен слушателю курса А. Молякову, указавшему на необходимость обоснования этого.

Вложив обычным образом аффинную плоскость в проективную

$$\mathbf{A}_2(\mathbb{k}) \hookrightarrow \mathbf{P}_2(\mathbb{k}) : (x, y) \mapsto (x : y : 1),$$

получим замыкание аффинной кривой $\dot{\mathbf{E}}_{c_1, c_2} \hookrightarrow \mathbf{E}_{c_1, c_2} \subset \mathbf{P}_2(\mathbb{k})$, где проективная кривая задана однородным уравнением

$$\mathbf{E}_{c_1, c_2} : y^2 z = x^3 - 27c_4 xz^2 - 54c_6 z^3; \quad (1.1.1e)$$

нетрудно убедиться, что эта кривая остаётся гладкой при условии (1.1.1d). Она имеет род 1, поскольку на ней есть регулярный дифференциал $\frac{dx}{y}$ без нулей и полюсов (начинающим рекомендуется тщательно проверить это). Теперь определён морфизм полных кривых

$$(x : y : 1) : \mathbf{X} \longrightarrow \mathbf{E}_{c_1, c_2};$$

в том, что это – изоморфизм, предлагается убедиться в упражнении (1.4).

Нами (при упрощающем предположении $\text{char}(\mathbb{k}) \notin \{2, 3\}$) установлен следующий результат.

Теорема. *Любая кривая рода 1 изоморфна гладкой плоской кубике.* ■

Однако для применения этого результата к полному описанию пространства модулей \mathcal{M}_1 надо ещё освоить множество всех (или почти всех) кубик.

Всякая ли кубика – неприводимая кривая рода 1? Разумеется, нет: например, уравнение $xyz = 0$ в $\mathbf{P}_2(\mathbb{k})$ задаёт объединение трёх прямых. Надо придать точный смысл ощущению того, что этот пример исключителен.

Самая общая кубика в $\mathbf{P}_2(\mathbb{k})$ задаётся уравнением

$$\sum_{i+j+k=3} a_{ijk} x^i y^j z^k = 0, \quad (1.1.1f)$$

где $(a_{300}, \dots, a_{003}) \neq (0, \dots, 0)$. Поскольку коэффициенты уравнения (1.1.1f) имеют смысл лишь с точностью до общей пропорциональности, правильно считать, что кубики параметризуются точками проективного пространства

$$(a_{300} : \dots : a_{003}) \in \mathbf{P}_9(\mathbb{k}).$$

Из этого пространства следует выбросить множество наборов коэффициентов $(a_{300} : \dots : a_{003})$, задающих особые, приводимые... или ещё хуже того (например, *трёхкратная прямая*, задаваемая уравнением $x^3 = 0$), кривые. В задачах 1.5. и 1.6. предлагается доказать, что для гладкости кубики достаточно, чтобы набор коэффициентов не лежал на некоторой гиперповерхности $\mathbf{Sing} \subset \mathbf{P}_9(\mathbb{k})$, и что для любой гладкой кубики на проективной плоскости найдётся *прямая перегиба*, то есть прямая, пересекающая кубику (*трёхкратно*) в единственной точке.

Практически работать с уравнением (1.1.1f) невозможно, и подбираются такие координаты, в которых уравнение выглядит компактнее – выше мы обсуждали такие действия с семичленными уравнениями (1.1.1a) и (1.1.1b). Сейчас мы

(единственный раз!) распишем 10-членное уравнение (1.1.1f)

$$\begin{aligned} & a_{300}x^3 + \\ & + a_{210}x^2y + a_{201}x^2z + \\ & + a_{120}xy^2 + a_{111}xyz + a_{102}xz^2 + \\ & + a_{030}y^3 + a_{021}y^2z + a_{012}yz^2 + a_{003}z^3 = 0 \end{aligned} \quad (1.1.1f')$$

и выберем координаты так, чтобы прямая " $z = 0$ " оказалась прямой перегиба. Пересечение этой прямой с кубикой "(1.1.1f')" задаётся уравнением

$$a_{300}x^3 + a_{210}x^2y + a_{120}xy^2 + a_{030}y^3 = 0. \quad (1.1.1g)$$

Мы требуем, чтобы у этого уравнения был только один (трёхкратный) корень — скажем, $(0:1:0)$; это равносильно равенствам

$$a_{210} = a_{120} = a_{030} = 0.$$

Подстановка этих равенств в 10-членное уравнение (1.1.1f') превращает его в 7-членное

$$a_{300}x^3 + a_{201}x^2z + a_{111}xyz + a_{102}xz^2 + a_{021}y^2z + a_{012}yz^2 + a_{003}z^3 = 0. \quad (1.1.1h)$$

Если положить в нём $z = 1$, то есть рассмотреть на аффинной плоскости вне "бесконечной" прямой " $z = 0$ ", то получится уравнение

$$a_{300}x^3 + a_{201}x^2 + a_{111}xy + a_{102}x + a_{021}y^2 + a_{012}y + a_{003} = 0, \quad (1.1.1i)$$

почти совпадающее с рассмотренным выше (1.1.1a).

Остается, как и при анализе того уравнения, убедиться, что $a_{300}a_{021} \neq 0$. Но равенство $a_{300} = 0$ превратило бы кубику в конику (точнее, проективная кубика представляла бы собой объединение коники с "бесконечной" прямой), а в случае $a_{021} = 0$ уравнение (1.1.1i) можно было бы решить относительно y , и кубика оказалось бы рациональной вопреки предположению $g = 0$.

Итак, мы привели произвольную гладкую кубику к уже рассмотренному выше виду. Чтобы окончательно осознать структуру пространства модулей $\mathcal{M}_1(\mathbb{k})$, осталось осознать два обстоятельства:

- Выбор координат в $\mathbf{P}_2(\mathbb{k})$ соответствует действию группы $\mathrm{PGL}_3(\mathbb{k})$ на $\mathbf{P}_2(\mathbb{k})$;
- Изоморфные кубики проективно эквивалентны.

(Желательно, чтобы второе стало очевидно. Все наши действия с абстрактными кривыми носят линейно-алгебраический характер вроде выборов базисов в конечномерных пространствах и потому выражаемы через действие $\mathrm{PGL}_3(\mathbb{k})$).

Опустив некоторые детали, мы пришли к главному выводу:

$$\boxed{\mathcal{M}_1(\mathbb{k}) \simeq \frac{\mathbf{P}_9(\mathbb{k}) \setminus \mathbf{Sing}}{\mathrm{PGL}_3(\mathbb{k})}}$$

Хотя мы еще не ввели на множестве $\mathcal{M}_1(\mathbb{k})$ никакой структуры, интуитивно ясное следствие заключается в том, что

$$\dim_{\mathbb{k}} \mathcal{M}_1(\mathbb{k}) = \dim_{\mathbb{k}} (\mathbf{P}_9(\mathbb{k})) - \dim_{\mathbb{k}} (\mathrm{PGL}_3(\mathbb{k})) = 9 - 8 = 1.$$

1.2. О геометрической теории инвариантов

Общематематическая проблема теории инвариантов возникает, когда задано действие группы на множестве

$$G : \mathcal{Z}$$

и требуется в том или ином смысле описать фактор-множество

$$\frac{\mathcal{Z}}{G}.$$

Как правило, и на множестве, и на группе имеются какие-то *структуры* (обычно – одинаковые), и отображения, задающие группу и её действие, то есть

$$\begin{aligned} G \times G &\longrightarrow G : (g_1, g_2) \mapsto g_1 g_2, \\ G &\longrightarrow G : g \mapsto g^{-1} \end{aligned}$$

и

$$G \times \mathcal{Z} \longrightarrow \mathcal{Z} : (g, z) \mapsto g \cdot z,$$

имеющиеся структуры *уважают*. Одна из основных проблем теории: в какой мере на фактор-множество $\frac{\mathcal{Z}}{G}$ переносится та же структура?

Инвариантами кратко называются *G*-инвариантные *функции* на \mathcal{Z} .

В интересующих нас случаях и множество, и группа наделены структурой алгебраических многообразий. Оказывается, полностью на фактор-множество это структура переносится далеко не всегда; простейший пример –

$$G = \mathbb{k}^\times, \mathcal{Z} = \mathbb{k},$$

а действие определяется умножением. Фактор-множество $\frac{\mathcal{Z}}{G}$ двухэлементно и в очень сильном смысле *неотделимо*. Вряд ли на нём можно ввести разумную структуру алгебраического многообразия.

Это нежелательное явление подсказывает способ его преодоления: выбросить ПЛОХИЕ орбиты, то есть выделить (как можно большее) G-инвариантное подмножество

$$\mathcal{Z}^{\text{good}} \subseteq \mathcal{Z},$$

такое, что фактор-множество $\frac{\mathcal{Z}^{\text{good}}}{G}$ всеми желательными свойствами. Потом, правда, часто оказывается, что о выброшенных плохих орбитах приходится вспомнить, вводить $\frac{\mathcal{Z}^{\text{bad}}}{G}$ и приделывать его, как обычно говорят, "на границу" множества $\frac{\mathcal{Z}^{\text{good}}}{G}$. Именно это последнее действие характерно для геометрической теории инвариантов. Она представляет собой огромный раздел математики, восходящий к чудовищным ручным вычислениям классиков XIX-го века. По геометрической теории инвариантов имеется обширная современная литература, из которой можно порекомендовать, например, книгу [Dolgachev2003], в которой нужные нам примеры подробно разобраны, в том числе с исторической точки зрения.

Мы сегодня поработали с простейшим (с точки зрения пространств модулей) случаем

$$\mathcal{Z} = \mathbf{P}_9(\mathbb{k}), G = \mathsf{PGL}(\mathbb{k});$$

множество $\mathcal{Z}^{\text{good}} = \mathbf{P}_9(\mathbb{k}) \setminus \mathbf{Sing}$ состояло из уравнений гладких кубик. В следующей лекции мы разберём этот пример более подробно.

СПИСОК ЛИТЕРАТУРЫ

- [Dolgachev2003] Igor Dolgachev, *Lectures on Invariant Theory*. Cambridge University Press, 2003.
- [Silverman2009] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*. Springer, 2009.
- [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.