

Алгебраическая геометрия

Предисловие

Конспект написан по материалам лекций, прочитанных А.С. Сивацким студентам бакалавриата «Математика» и магистратуры «Современная математика» факультета Математики и Компьютерных наук СПбГУ. В конспекте присутствуют материалы спецкурса «Основы алгебраической геометрии, часть I».

Конспект набран Матвеем Магиным, редактировался Леонидом Данилевичем. Как и в любом большом тексте, в нём наверняка присутствуют опечатки и неточности. Если Вы хотите сообщить о них, Вы можете написать составителю на электронную почту matheusz.magin@gmail.com.

Составитель признателен коллегам, сообщавшим об опечатках и неточностях.

Исходные файлы конспекта Вы можете найти в проекте по адресу

<https://www.overleaf.com/read/fcnprfmdmqm#81c360>.

Содержание

1	Аффинные многообразия	3
1.1	Введение. Аффинные алгебраические многообразия. Идеалы, неприводимые многообразия.	3
1.2	Разложение в неприводимые компоненты	6
1.3	Размерность аффинного многообразия	8
1.4	Регулярные функции	11
1.5	Морфизмы алгебраических многообразий	13
1.6	Антиэквивалентность $\text{Aff}^{\text{op}} \cong \mathbb{k}\text{-Alg}$	14
1.7	Рациональные функции	16
1.8	Главные аффинные окрестности	16
1.9	Эквивалентные определения размерности неприводимого аффинного многообразия	18
1.10	Прямое произведение многообразий и его первые приложения	19
1.11	О количестве порождающих идеала	21
2	Проективные многообразия	24
2.1	Проективные многообразия	24
2.2	Проективное замыкание аффинного многообразия	28
2.3	Прямое произведение проективных многообразий	29
2.4	Замкнутость образа проективного многообразия	32
2.5	Рациональные отображения многообразий	35
2.6	Бирациональная эквивалентность	37
2.7	Рациональные многообразия	38
3	Локальные кольца	40
3.1	Локальное кольцо в точке	40
3.2	Касательное пространство	43
3.3	Разложение в ряд Тейлора	46

3.4	Локальное кольцо точки на неособой кривой. Индексы ветвления и степень инерции.	49
3.5	Конечные морфизмы и нормализация многообразия	50
3.6	Морфизмы между неособыми кривыми	54
3.7	Морфизмы между неособыми проективными неприводимыми кривыми	55
4	Дивизоры	56
4.1	Дивизоры Вейля	56
4.2	Дивизоры форм	60
4.3	Дивизоры на эллиптических кривых.	61
4.4	Групповой закон для точек эллиптической кривой	63
5	Приложение: альтернативное доказательство того, что степень главного дивизора равна нулю	66
5.1	План доказательства	66
5.2	Аппроксимационная теорема. Оценка в одну сторону	66
5.3	Пространство функций, ассоциированное с дивизором. Оценка в другую сторону	68
6	Приложение: компендиум по коммутативной алгебре	70

1 Аффинные многообразия

1.1 Введение. Аффинные алгебраические многообразия. Идеалы, неприводимые многообразия.

Прежде всего отметим, что в данном курсе будет изучаться (квази)аффинная и (квази)проективная алгебраическая геометрия и речь пойдет о (квази)аффинных и (квази)проективных многообразиях.

Пусть \mathbb{k} — алгебраически замкнутое поле, через $\mathbb{A}_{\mathbb{k}}^n = \mathbb{A}^n$ мы будем обозначать \mathbb{k}^n , рассматриваемое как множество, и будем называть это множество *n -мерным аффинным пространством* над \mathbb{k} . Определим на нём топологию.

Определение 1. Рассмотрим $T \subset \mathbb{k}[x_1, \dots, x_n]$ и определим

$$Z(T) \stackrel{\text{def}}{=} \{(a_1, \dots, a_n) \in \mathbb{A}_{\mathbb{k}}^n \mid f(a_1, \dots, a_n) = 0 \quad \forall f \in T\}.$$

Замечание 1. В случае $T = \emptyset$ естественно полагать $Z(T) = \mathbb{A}_{\mathbb{k}}^n$. Кроме того, сразу заметим, что $Z((1)) = \emptyset$.

Замечание 2. Пусть $I = (T)$ — идеал, порождённый множеством T . В этом случае $Z(T) = Z(I)$, так как если (a_1, \dots, a_n) является нулём для всех элементов идеала, то для $T \subset I$ уж тем более, и, кроме того, если (a_1, \dots, a_n) является общим нулём многочленов из T , то многочлен $f \in I$ мы можем представить в виде

$$f = \sum g_i h_i, \quad h_i \in T, \quad g_i \in \mathbb{k}[x_1, \dots, x_n]$$

откуда ясно, что $f(a_1, \dots, a_n) = 0$.

Отсюда ясно, что достаточно рассматривать не произвольные подмножества $\mathbb{k}[x_1, \dots, x_n]$, а идеалы этого кольца.

Определение 2. Введём на $\mathbb{A}_{\mathbb{k}}^n$ *топологию Зарисского* следующим образом: объявим замкнутыми все множества вида $Z(T)$ для некоторого T .

Покажем, что это действительно топология.

1. Ясно, что $Z(T_1) \cup Z(T_2) = Z(T_1 T_2)$, где $T_1 T_2 = \{f_1 f_2 \mid f_1 \in T_1, f_2 \in T_2\}$.

Совсем очевидно, что левая часть лежит в правой. Обратно, пусть $f_1 f_2(a_1, \dots, a_n) = 0 \quad \forall f_1 \in T_1, f_2 \in T_2$. Раз $f_1 f_2(a_1, \dots, a_n) = 0$, то хотя бы один многочлен из произведения зануляется.

2. Кроме того, ясно, что $\bigcap_{i \in I} Z(T_i) = Z(\bigcup_{i \in I} T_i)$.

Пример 1. Рассмотрим $\mathbb{A}_{\mathbb{k}}^1$. Какими могут быть замкнутые множества? Пусть $I = (T)$. Так как $\mathbb{k}[x]$ — область главных идеалов, то и идеал I — главный.

- Если $I = 0$ то $Z(I) = \mathbb{A}^1$ — замкнутое.
- Если $I = (1)$, то $Z(T) = \emptyset$.
- Если, наконец, $I = (f)$, f необратим, то в силу алгебраической замкнутости $\mathbb{k} : f(x) = (x - a_1) \cdot \dots \cdot (x - a_n)$, откуда $Z(T) = \{a_1, \dots, a_n\}$ — конечный набор точек.

С другой стороны, если у нас есть конечное множество $\{a_1, \dots, a_n\} \subset \mathbb{A}_{\mathbb{K}}^1$, то оно является множеством нулей многочлена

$$f(x) = \prod_{i=1}^n (x - a_i).$$

Таким образом, замкнутые подмножества аффинной прямой — в точности все конечные подмножества $\mathbb{A}_{\mathbb{K}}^1$, пустое и сама прямая $\mathbb{A}_{\mathbb{K}}^1$. Отсюда сразу видно, что любые два открытых подмножества пересекаются и топология Зарисского не хаусдорфова. Хаусдорфовости не будет и в общем случае, что показывает, что интуицию из топологии, скажем, на \mathbb{R}^n , надо перенимать с осторожностью.

Определение 3. Пусть X — топологическое пространство, $Y \subset X$, $Y \neq \emptyset$. Y называется *неприводимым*, если из равенства $Y = Y_1 \cup Y_2$, где Y_i замкнуты в Y , следует, что $Y_1 = Y$ или $Y_2 = Y$.

То есть, неприводимые множества — в точности те, которые нельзя представить в виде объединения двух меньших замкнутых подмножеств.

Пример 2. Аффинная прямая $\mathbb{A}_{\mathbb{K}}^1$ неприводима (просто из соображений мощности).

Теперь докажем такой общетопологический факт:

Предложение 1. *Непустое открытое подмножество неприводимого — неприводимо и плотно. Замыкание неприводимого множества неприводимо.*

Доказательство. Пусть $U \subset Y$ — открытое подмножество. Покажем, что оно неприводимо. Пусть

$$U = (U \cap F_1) \cup (U \cap F_2), \quad F_1, F_2 \text{ замкнуты в } Y.$$

Тогда $Y = F_1 \cup F_2 \cup (Y \setminus U)$, а так как Y — неприводимо, Y совпадает с каким-то из этих множеств. С $Y \setminus U$ оно совпасть не может, так как $U \neq \emptyset$. Значит, $Y = F_i \implies U \cap F_i = U \cap Y = U$, что мы и хотели.

Теперь докажем, что $\overline{U} = Y$. Действительно, $Y = (Y \setminus U) \cup \overline{U}$ и из неприводимости Y и непустоты U следует, что $\overline{U} = Y$. \square

Определение 4. Замкнутые непустые подмножества в $\mathbb{A}_{\mathbb{K}}^n$ мы будем называть *аффинными алгебраическими многообразиями*¹.

Пример 3. Рассмотрим $\mathbb{A}^1 \setminus \{0\}$. Это множество не является замкнутым в нашей топологии. С другой стороны, есть взаимно-однозначное соответствие между этим множеством и множеством $\{(x, y) \in \mathbb{A}^2 \mid xy - 1 = 0\}$, которое является аффинным многообразием.

В одну сторону нам надо сделать проекцию графика гиперболы на горизонтальную ось: $(x, y) \mapsto x \in \mathbb{A}^1 \setminus \{0\}$, а в обратную сторону, мы можем отобразить $\mathbb{A}^1 \setminus \{0\} \ni x \mapsto (x, x^{-1})$.

Замечание 3. Пример выше наводит на мысль о том, что наше определение не достаточно общее. Довольно скоро мы его обобщим. Вообще говоря, в данном конспекте под словом *многообразие* будет пониматься самое общее, что введено к данному моменту курса.

¹Отметим, что в книге Хартсхорна все аффинные алгебраические многообразия предполагаются неприводимыми.

Определение 5. Рассмотрим произвольное подмножество $Y \subset \mathbb{A}_{\mathbb{k}}^n$, положим

$$I(Y) \stackrel{\text{def}}{=} \{f \in \mathbb{k}[x_1, \dots, x_n] \mid f(y) = 0 \quad \forall y \in Y\}.$$

Совершенно ясно, что $I(Y)$ — идеал. Кроме того, отметим, что для $Y = \mathbb{A}_{\mathbb{k}}^n : I(Y) = 0$, а для $Y = \emptyset : I(Y) = (1)$. Таким образом, у нас есть отображения

$$\mathbb{k}[x_1, \dots, x_n] \supset T \mapsto Z(T), \quad \mathbb{A}_{\mathbb{k}}^n \supset Y \mapsto I(Y).$$

Предложение 2. *Определённые выше отображения имеют следующие свойства:*

1. Если $T_1 \subset T_2$, где $T_1, T_2 \subset \mathbb{k}[x_1, \dots, x_n]$, то $Z(T_1) \supset Z(T_2)$.
2. Если $Y_1 \subset Y_2 \subset \mathbb{A}_{\mathbb{k}}^n$, то $I(Y_1) \supset I(Y_2)$.
3. $I(Y_1 \cup Y_2) = I(Y_1) \cap I(Y_2)$.
4. Пусть $Y \subset \mathbb{A}_{\mathbb{k}}^n$, тогда $Z(I(Y)) = \bar{Y}$.
5. Пусть $I \leq \mathbb{k}[x_1, \dots, x_n]$, тогда $I(Z(I)) = \sqrt{I}$.

Доказательство. Первые три пункта очевидны.

Четвёртый пункт следует просто из определений. С одной стороны, ясно, что $Y \subset Z(I(Y))$. С другой стороны, пусть $T = Z(\mathfrak{a})$ — произвольное замкнутое множество, содержащее Y . Раз $Y \subset T$, то легко проверить, что $\mathfrak{a} \subset I(Y)$ ². Пункт 1 влечёт $T = Z(\mathfrak{a}) \supset Z(I(Y))$, что по произвольности T даёт искомое.

Пятый пункт — в точности (сильная) теорема Гильберта о нулях 33. □

Предложение 3. *Отображения $Y \mapsto I(Y)$ устанавливает взаимно-однозначное соответствие между аффинными многообразиями в $\mathbb{A}_{\mathbb{k}}^n$ и радикальными идеалами кольца многочленов $\mathbb{k}[x_1, \dots, x_n]$.*

При этом, неприводимым аффинным многообразиям соответствуют простые идеалы и наоборот.

Доказательство. Четвёртый и пятый пункты предыдущего предложения 2 как раз означают то, что отображения Z и I взаимно обратные

Пусть теперь Y неприводимо. Покажем, что $I(Y)$ — простой идеал. Рассмотрим $f, g \in \mathbb{k}[x_1, \dots, x_n]$, пусть $fg \in I(Y)$. Заметим, что

$$Y = (Y \cap Z(f)) \cup (Y \cap Z(g)),$$

значит, одно из этих множеств совпадает с Y . Пусть, например, $Y = Y \cap Z(f) \implies Y \subset Z(f) \implies f \in I(Y)$.

Наоборот, предположим, что $I(Y)$ — простой идеал. Пусть $Y = Y_1 \cup Y_2$, тогда

$$I(Y) = I(Y_1) \cap I(Y_2) \supset I(Y_1)I(Y_2).$$

Так как идеал простой, не умаляя общности, $I(Y_1) \subset I(Y) \implies Y \subset Y_1 \implies Y = Y_1$, что мы и хотели. □

²А именно: $\forall f \in \mathfrak{a} : f(T) = f(Z(\mathfrak{a})) = 0$, откуда $f(Y) = 0$, то есть $f \in I(Y)$.

Посмотрим, куда при этом соответствии переходят точки (одноточечные подмножества $\mathbb{A}_{\mathbb{k}}^n$). Пусть $P = (a_1, \dots, a_n)$. Множество $\{P\}$ замкнуто, так как оно равняется $Z((x_1 - a_1, \dots, x_n - a_n))$.

Из обращения включений в 2 понятно, что точки — минимальные замкнутые множества — соответствуют максимальным идеалам кольца $\mathbb{k}[x_1, \dots, x_n]$.

Слабая теорема Гильберта о нулях 34 говорит, что все максимальные идеалы $\mathbb{k}[x_1, \dots, x_n]$ имеют вид $(x_1 - a_1, \dots, x_n - a_n)$, то есть других максимальных идеалов нет, все соответствуют точкам. Тем самым, имеется биекция

$$\text{точки } \mathbb{A}_{\mathbb{k}}^n \longleftrightarrow \text{Specm}(\mathbb{k}[x_1, \dots, x_n]).$$

1.2 Разложение в неприводимые компоненты

Определение 6. Топологическое пространство X называется *нётеровым*, если оно удовлетворяет ДСС для замкнутых множеств. Иными словами, всякая цепочка $Z_0 \supset Z_1 \supset Z_2 \supset \dots$ стабилизируется: $\exists n \in \mathbb{N} : Z_n = Z_{n+1} = \dots$.

Или же, еще более иными словами, в любом семействе замкнутых множеств содержится минимальный (по включению) элемент.

Пример 4. $\mathbb{A}_{\mathbb{k}}^n$ является нётеровым, так как по теореме Гильберта о базисе $\mathbb{k}[x_1, \dots, x_n]$ — нётерово кольцо.

В самом деле, если $Z_0 \supset Z_1 \supset \dots$, то $I(Z_0) \subset I(Z_1) \subset \dots$. Так как $\mathbb{k}[x_1, \dots, x_n]$ — нётерово, $\exists m : I(Z_m) = I(Z_{m+1}) = \dots$, и, применяя Z , мы имеем $Z_m = Z_{m+1} = \dots$.

Теорема 1. Пусть X — нётерово пространство, $Y \subset X$ — замкнутое. Тогда существует единственное разложение $Y = Y_1 \cup Y_2 \cup \dots \cup Y_m$, где Y_i — замкнутые неприводимые множества и $\forall i, j : Y_i \not\subset Y_j$.

Доказательство. Существование. Пусть существуют замкнутые множества Y , не разлагающиеся в объединение неприводимых. В силу нётеровости пространства, мы можем выбрать минимальное множество с таким свойством и обозначить его за Y .

Совершенно ясно, что оно не может быть неприводимым. Тем самым его можно представить в виде $Y = T_1 \cup T_2$, где T_1, T_2 — замкнутые и не совпадают с Y . Так как $T_1, T_2 \subset Y$, а Y — минимальное из тех, что не разложить, то T_i мы уже можем представить в виде объединения неприводимых, а значит, и Y , что даёт нам противоречие.

Единственность. Пусть $Y = Y_1 \cup Y_2 \cup \dots \cup Y_m = Y'_1 \cup \dots \cup Y'_s$. Тогда

$$Y_1 = \bigcup_i (Y_1 \cap Y'_i) \implies Y_1 \subset Y'_i.$$

Проводя аналогичное рассуждение для Y'_i , мы получаем, что $Y'_i \subset Y_j$ для некоторого j . Но, так как, в силу посылки теоремы, между компонентами не может быть включений, то $j = 1$ и $Y_1 = Y'_i$. Повторяя аналогичный аргумент с остальными индексами, получаем единственность. \square

Определение 7. Замкнутые неприводимые множества Y_i , определённые в теореме выше, называют *неприводимыми компонентами* Y .

Пусть теперь Y — аффинное алгебраическое многообразие. Так как оно вложено в некоторое \mathbb{A}^n , то оно также раскладывается в объединение неприводимых компонент.

Итак, пусть $Y = Y_1 \cup \dots \cup Y_m$, тогда $I(Y) \subset I(Y_i)$, а $I(Y_i)$ — простые идеалы (так как Y_i неприводимы).

Предложение 4. Идеалы $I(Y_i)$ — в точности наименьшие простые идеалы, содержащие $I(Y)$.

Доказательство. Пусть $T \subset Y$ — неприводимое подмножество, тогда

$$T = \bigcup_{i=1}^m (T \cap Y_i) \implies T \subset Y_i.$$

Пусть $Y = Z(I)$, а $Y_i = Z(\mathfrak{p}_i)$, $I \subset \mathfrak{p}_i \in \text{Spec}(\mathbb{k}[x_1, \dots, x_n])$.

Предположим, что $I \subset \mathfrak{p} \subsetneq \mathfrak{p}_i$ для некоторого $\mathfrak{p} \in \text{Spec}(\mathbb{k}[x_1, \dots, x_n])$. Тогда $Z(\mathfrak{p}) \subset Y$ — неприводимое подмножество, и как проверено выше, $Z(\mathfrak{p}) \subset Z(\mathfrak{p}_j)$ для некоторого \mathfrak{p}_j . Но отсюда сразу следует

$$\underbrace{Z(\mathfrak{p}_j)}_{=Y_j} \subsetneq \underbrace{Z(\mathfrak{p}_i)}_{=Y_i},$$

что даёт нам противоречие.

Теперь, возьмём произвольный минимальный простой идеал $\mathfrak{p} \supset I$ и покажем, что он даст нам неприводимую компоненту (т.е., что он будет совпадать с одним из \mathfrak{p}_i).

В самом деле, для некоторого i мы имеем $Z(\mathfrak{p}) \subset Z(\mathfrak{p}_i) \implies \mathfrak{p}_i \subset \mathfrak{p}$, откуда по минимальности \mathfrak{p} мы имеем $\mathfrak{p}_i = \mathfrak{p}$. \square

Дадим теперь следующее определение:

Определение 8. Пусть Y — аффинное многообразие. Его *аффинным координатным кольцом* мы будем называть $A(Y) = \mathbb{k}[x_1, \dots, x_n]/I(Y)$.

Домашнее задание 1. Задачи:

1. Любое подпространство нётерова пространства нётерово.
2. Нётерово пространство квазикompактно³.
3. Имеется отображение $f: \mathbb{A}^2 \rightarrow \mathbb{A}^2$, $f(x, y) = (x, xy)$. Вычислить образ и определить, будет ли этот образ $f(\mathbb{A}^2)$ открытым/замкнутым/плотным подмножеством в \mathbb{A}^2 .
4. Пусть $f: \mathbb{A}^3 \rightarrow \mathbb{A}^3$, $f(x, y, z) = (x, xy, xyz)$. Вычислить образ и определить, будет ли этот образ $f(\mathbb{A}^3)$ открытым/замкнутым/плотным подмножеством в \mathbb{A}^3 .
5. Пусть $Y \subset \mathbb{A}^3$, $Y = Z(x^2 - yz, xz - x)$.
6. Найти неприводимые компоненты Y .
7. Вычислить неприводимые компоненты $Y = Z(y^2 - xz, z^2 - y^3)$.
8. Рассмотрим $Y = \{(t^3, t^4, t^5) \in \mathbb{A}_{\mathbb{k}}^3\}$.
 - (a) Y — аффинное многообразие в \mathbb{A}^3 .
 - (b) Докажите, что $I(Y)$ порождается тремя элементами и найдите их.

³То есть из всякого открытого покрытия можно выделить конечное подпокрытие. Слово квазикompактность выдумали, чтобы не путать с обычной компактностью, которую иногда определяют так, что компакт по определению хаусдорфов.

(с) Докажите, что $I(Y)$ не порождается двумя элементами.

9. Рассмотрим $Y = Z(y^2 - x^3)$ и аффинное координатное кольцо $A(Y) = \mathbb{k}[x, y]/I(Y)$. Докажите, что поле частных этого кольца изоморфно $\mathbb{k}[k](t)$. Выясните, является ли кольцо $A(Y)$ целозамкнутым.

1.3 Размерность аффинного многообразия

Пусть X — произвольное топологическое пространство. Тогда его размерность $\dim X$ определяется аналогично размерности Крулля для кольца в коммутативной алгебре. А именно, рассматривается максимальная длина убывающей цепочки непустых замкнутых неприводимых множеств:

$$X_0 \supsetneq X_1 \supsetneq X_2 \dots \supsetneq X_n.$$

и размерностью X называется такое максимально возможное n .

Предложение 5. Пусть Y — многообразие, а $A(Y)$ — его координатное кольцо. Тогда

$$\dim Y = \dim A(Y).$$

Доказательство. Замкнутые неприводимые подмножества $Y \subset \mathbb{A}^n$ соответствуют простым идеалам кольца $\mathbb{k}[x_1, \dots, x_n]$, содержащим $I(Y)$, а они, в свою очередь, соответствуют простым идеалам координатного кольца $A(Y) = \mathbb{k}[x_1, \dots, x_n]/I(Y)$. Значит, $\dim Y$ равна наибольшей из длин цепочек отличных друг от друга простых идеалов в $A(Y)$, то есть размерности Крулля $A(Y)$. \square

Это предложение показывает, что результаты из теории размерности нётеровых колец весьма-весьма полезны в алгебраической геометрии.

Вычислим теперь размерности каких-то базовых пространств. В \mathbb{A}^n легко найти цепочку замкнутых подмножеств $\mathbb{A}^n \supset Z(x_1) \supset Z(x_1, x_2) \supset \dots \supset Z(x_1, \dots, x_n)$, но доказать, что большей цепочки нет, сильно сложнее.

Чтобы сделать это, докажем следующую теорему из коммутативной алгебры:

Теорема 2. Пусть B — конечно порождённая \mathbb{k} -алгебра. Если B — область целостности, то $\dim(B) = \text{trdeg}_{\mathbb{k}}(\text{Frac}(B))$ (где $\text{Frac}(B)$ — поле частных \mathbb{k} -алгебры B).

Доказательство. Будем вести индукцию по $\text{trdeg}_{\mathbb{k}}(\text{Frac}(B))$.

Случай $\text{trdeg}_{\mathbb{k}}(\text{Frac}(B)) = 0$ тривиален — в таком случае расширение $\text{Frac}(B)/\mathbb{k}$ чисто алгебраическое, и из алгебраической замкнутости \mathbb{k} : $\text{Frac}(B) = \mathbb{k}$. Но раз B — \mathbb{k} -алгебра, то $B = \mathbb{k}$, и, разумеется, $\dim B = 0$.

Теперь пусть $\text{trdeg}_{\mathbb{k}}(\text{Frac}(B)) > 0$. Согласно лемме Нётер о нормализации 31, внутри B содержится подкольцо $A \subset B$, изоморфное кольцу многочленов $A \cong \mathbb{k}[x_1, \dots, x_m]$, и включение $A \subset B$ конечно. Так как при целом (тем более при конечном) расширении размерность не меняется, то $\dim A = \dim B$. С другой стороны, раз $A \subset B$ конечно, то расширение полей частных алгебраическое, откуда $\text{trdeg}_{\mathbb{k}}(\text{Frac}(A)) = \text{trdeg}_{\mathbb{k}}(\text{Frac}(B))$, значит, достаточно доказать посылку теоремы лишь для кольца многочленов $A = \mathbb{k}[x_1, \dots, x_m]$.

Выберем цепочку простых идеалов $0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_n \subset A$, где $n = \dim A$ (мы ещё не доказали, что размерность A равна количеству переменных m , и пока лишь очевидно, что $n \geq m$). Докажем следующую лемму:

Лемма 1. Пусть A — факториальная область целостности, и $\mathfrak{p}_1 \subset A$ — простой идеал высоты 1. Тогда $\mathfrak{p}_1 = (p)$ — главный идеал для некоторого неприводимого $p \in A$.

Доказательство. Так как $\mathfrak{p}_1 \neq 0$, то $\exists 0 \neq f \in \mathfrak{p}_1$. Он раскладывается на неприводимые множители, и из простоты \mathfrak{p}_1 , хотя бы один из этих множителей (пусть p) лежит внутри \mathfrak{p}_1 . Получается, идеал $(p) \subset \mathfrak{p}_1$ — тоже простой, и из максимальной цепочки $\mathfrak{p}_1 = (p)$. \square

Отфакторизуем кольцо многочленов A по \mathfrak{p}_1 , и посмотрим, что получится.

Идеал \mathfrak{p}_1 — высоты 1 (так как цепочка максимальна), откуда в силу леммы $\mathfrak{p}_1 = (p)$, и пусть без потери общности x_1 входит в p нетривиальным образом. Тогда образы x_2, \dots, x_m внутри $\text{Frac}(A/(p))$ образуют базис трансцендентности (очевидно, что они порождают всё поле частных $\text{Frac}(A/(p))$, а независимость даже и не пригодится). Тем самым, $\text{trdeg}_{\mathbb{K}} \text{Frac}(A/(p)) \leq m - 1$, откуда по индукции $\dim A/(p) = m - 1$. Но цепочка $0 = \mathfrak{p}_1/(p) \subsetneq \dots \subsetneq \mathfrak{p}_n/(p)$ внутри $A/(p)$ имеет длину $n - 1$, откуда $n - 1 \leq m - 1$, и мы доказали обратное неравенство. \square

Пример 5. Отсюда мы сразу получаем, что $\dim \mathbb{A}^n = \dim \mathbb{K}[x_1, \dots, x_n] = n$.

Определение 9. *Аффинная алгебра* — это координатное кольцо некоторого аффинного многообразия.

Замечание 4. Эквивалентно можно говорить, что аффинная алгебра — это конечно порождённая редуцированная алгебра. В самом деле, координатное кольцо любого аффинного многообразия — это факторкольцо $\mathbb{K}[x_1, \dots, x_n]$ по радикальному идеалу, оно конечно порождено над \mathbb{K} и редуцировано. Обратно, любое конечно порождённое над \mathbb{K} кольцо представимо в виде факторкольца кольца многочленов, а редуцированность означает, что идеал, по которому происходит факторизация, радикален.

Теорема 3. Пусть B — целостная аффинная алгебра над \mathbb{K} (или, что эквивалентно, конечно порождённая целостная \mathbb{K} -алгебра), а $\mathfrak{p} \in \text{Spec } B$. Тогда

$$\text{ht } \mathfrak{p} + \dim B/\mathfrak{p} = \dim B.$$

Доказательство. Будем вести индукцию по $\dim B$. База ($\dim B = 0$) очевидна.

Рассмотрим два варианта — сначала равенство B кольцу многочленов, потом общий случай.

I. Пусть $B = \mathbb{K}[x_1, \dots, x_n]$, $\dim B = n$. Возьмём $\mathfrak{p} \in \text{Spec } B$, $\text{ht } \mathfrak{p} = m$, то есть

$$0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \dots \subsetneq \mathfrak{p}_m = \mathfrak{p}.$$

Тогда $\text{ht } \mathfrak{p}_1 = 1$, и идеал $\mathfrak{p}_1 = (p)$ — главный в силу леммы 1

Отфакторизуем по (p) : $\mathfrak{p}/(p) \subseteq B/(p)$, $\mathfrak{p}/(p) \in \text{Spec } B/(p)$. Так как (p) — главный идеал, то по предыдущей теореме 2: $\dim B/(p) = \dim B - 1$ (несложно предъявить базис трансцендентности $\text{Frac}(B/(p))$), значит, мы можем применить индукционное предположение:

$$\text{ht } \mathfrak{p}/(p) + \dim B/\mathfrak{p} = \dim B - 1.$$

Докажем, что $\text{ht } \mathfrak{p}/(p) = \text{ht } \mathfrak{p} - 1$. Очевидно, что $\text{ht } \mathfrak{p}/(p) \geq \text{ht } \mathfrak{p} - 1$. С другой стороны, если $\pi: B \rightarrow B/(p)$, то всякая цепочка для $\mathfrak{p}/(p)$

$$0 \subsetneq \mathfrak{q}_1 \subsetneq \dots \subsetneq \mathfrak{q}_s = \mathfrak{p}/(p),$$

поднимается до цепочки для \mathfrak{p} :

$$0 \subsetneq (\mathfrak{q}) \subsetneq \pi^{-1}(0) \subsetneq \pi^{-1}(\mathfrak{q}_1) \subsetneq \dots \subsetneq \pi^{-1}(\mathfrak{q}_s) = \mathfrak{p}.$$

II. Пусть B — произвольная конечно порождённая целостная \mathbb{k} -алгебра. По лемме Нётер о нормализации B — целое расширение $A = \mathbb{k}[x_1, \dots, x_n]$, $\dim B = \dim A$. Далее по теореме о спуске для $\mathfrak{q} \in \text{Spec } B$ мы имеем $\text{ht } \mathfrak{q} \geq \text{ht}(\mathfrak{q} \cap A)$. Кроме того, расширение

$$A/(\mathfrak{q} \cap A) \hookrightarrow B/\mathfrak{q}$$

тоже целое, откуда $\dim A/(\mathfrak{q} \cap A) = \dim B/\mathfrak{q}$. Получается, мы имеем

$$\dim B/\mathfrak{q} + \text{ht } \mathfrak{q} \geq \dim(A/\mathfrak{q} \cap A) + \text{ht}(\mathfrak{q} \cap A)$$

По пункту I, правая часть равна $\dim A = \dim B$, то есть мы показали, что

$$\dim B/\mathfrak{q} + \text{ht } \mathfrak{q} \geq \dim B.$$

Но неравенство в другую сторону очевидно. □

Следствие 1. Пусть B — целостная конечно порождённая алгебра, $f \in B$, $f \neq 0$ и f необратим. Пусть \mathfrak{p} — минимальный простой идеал, содержащий f . Тогда

$$\dim B/\mathfrak{p} = \dim B - 1.$$

Доказательство. По теореме 3 мы имеем

$$\text{ht } \mathfrak{p} + \dim B/\mathfrak{p} = \dim B.$$

Но, по теореме Крулля о главных идеалах (hauptidealsatz), $\text{ht } \mathfrak{p} = 1$, откуда мы имеем нужное. □

Переформулируем это на алгебро-геометрический язык:

Определение 10. (Необязательно неприводимая) *гиперповерхность* в \mathbb{A}^n — множество вида $Z(f)$, где $f \in \mathbb{k}[x_1, \dots, x_n]$ необратим, $f \neq 0$.

Следствие 2. Пересечение неприводимого многообразия X с гиперповерхностью $Z(f)$ имеет размерность каждой компоненты хотя бы $\dim X - 1$.

Доказательство. Пусть $X \subset \mathbb{A}^n$ задаётся идеалом $I(X)$. Его размерность — размерность координатного кольца $A(X) = \mathbb{k}[x_1, \dots, x_n]/I(X)$. При этом координатное кольцо пересечения — это $A(X \cap Z(f)) = \mathbb{k}[x_1, \dots, x_n]/\sqrt{I(X) + (f)} = A(X)/\sqrt{(f)}$. Так как X неприводимо, то $I(X)$ прост, откуда $A(X)$ целостно.

При этом неприводимые компоненты $A(X \cap Z(f))$ — максимальные неприводимые замкнутые подмножества — соответствуют минимальным простым идеалам $A(X \cap Z(f))$, которые в свою очередь отвечают минимальным простым идеалам $A(X)$, содержащим образ f . Если образ f внутри $A(X)$ обратим, то этих идеалов нет (с геометрической точки зрения, пересечение $X \cap Z(f)$ пусто). Иначе f необратим, и применимо следствие 1: ясно, что если неприводимая компонента $X \cap Z(f)$ отвечает простому идеалу $\mathfrak{p} \supset (f)$, то её размерность равна размерности её координатного кольца $A(X)/\mathfrak{p}$. □

Отсюда получаем вот такое следствие:

Предложение 6. Пусть X неприводимо. Тогда все неприводимые компоненты $Z(I(X) + (f_1, \dots, f_m))$ имеют размерность хотя бы $\dim X - m$.

Следствие 3. Пусть $f_1, \dots, f_m \in \mathbb{k}[x_1, \dots, x_n]$, $m < n$ и $f_1(0) = \dots = f_m(0) = 0$. Тогда система

$$\begin{cases} f_1 = 0 \\ \vdots \\ f_m = 0 \end{cases}$$

имеет ненулевое решение.

Доказательство. Пространство переменных — аффинное пространство $\mathbb{A}_{\mathbb{k}}^n$. Пространство решений — замкнутое множество $Z(f_1, \dots, f_m)$. По условию $(0, \dots, 0) \in Z(f_1, \dots, f_m)$.

В силу предыдущего предложения (применённого к $X = \mathbb{A}_{\mathbb{k}}^n$), размерность компоненты $Z(f_1, \dots, f_m)$, содержащей $(0, \dots, 0)$, хотя бы 1, что согласно геометрическому определению размерности означает, что там есть ещё хотя бы одна точка (из неприводимости их даже бесконечно много). \square

1.4 Регулярные функции

Определение 11. Будем говорить, что X — *квазиаффинное многообразие*, если X — открытое подмножество аффинного многообразия.

Определение 12. Пусть $X \subset \mathbb{A}_{\mathbb{k}}^n$ — квазиаффинное. Будем говорить, что отображение $f: X \rightarrow \mathbb{k}$ — регулярное в точке p , если существует окрестность $U \subset X$, $U \ni p$ и многочлены $g, h \in A = \mathbb{k}[x_1, \dots, x_n]$ такие, что

- h не имеет нулей в U ,
- $f|_U = g/h$.

Функция $f: X \rightarrow \mathbb{k}$ называется *регулярной* на X , если она регулярна в каждой точке X .

Регулярные функции на X образуют кольцо, которое мы будем обозначать $\mathcal{O}(X)$.

Замечание 5. Например, все многочлены — регулярные функции на \mathbb{A}^n .

Теорема 4. Пусть X — аффинное многообразие. Тогда

$$\mathcal{O}(X) \cong A(X) = \mathbb{k}[x_1, \dots, x_n]/I(X).$$

Доказательство. Сначала отметим, что каждый многочлен очевидно определяет регулярную функцию на \mathbb{A}^n , а значит и на X . Так мы строим гомоморфизм

$$\alpha: \mathbb{k}[x_1, \dots, x_n] \rightarrow \mathcal{O}(X), \quad f \mapsto f.$$

Но, его ядро — это в точности $I(X)$:

$$\text{Ker } \alpha = \{f \in \mathbb{k}[x_1, \dots, x_n]: f|_X = 0\} = I(X).$$

Значит, у нас есть инъективный гомоморфизм $A(X) \hookrightarrow \mathcal{O}(X)$. Покажем, что он сюръективен.

Рассмотрим $f \in \mathcal{O}(X)$. По определению, у любой точки $x \in X$ существует окрестность U_x и многочлены p_x, q_x такие, что $q_x f = p_x$ в U_x , причём q_x не обращается в 0 на U_x . Так как $X \setminus U_x$ замкнуто, $X \setminus U_x = Z(\mathfrak{a})$ для некоторого идеала $\mathfrak{a} \subseteq \mathbb{k}[x_1, \dots, x_n]$ и легко видеть, что

$$Z(\mathfrak{a}) \subset X = Z(I(X)) \implies I(X) \subset \mathfrak{a}.$$

Значит, если мы возьмём $s \in \mathfrak{a} \setminus I(X)$, мы получим, что

$$s \cdot q_x \cdot f = s \cdot p_x \quad \text{на всём } X, \text{ так как}$$

- $s \in \mathfrak{a} = I(X \setminus U_x)$, что значит, что $s|_{X \setminus U_x} = 0$ и на $X \setminus U_x$ это равенство превращается в $0 = 0$.
- А на U_x это равенство получается домножением $q_x f = p_x$ на s .

Причём, выберем s так, чтоб $s(x) \neq 0$. Мы можем так сделать, так как если нет, то

$$\begin{cases} \forall s \in \mathfrak{a} \setminus I(X) & s(x) = 0 \\ \forall s \in I(X) & s(x) = 0 \end{cases} \implies \forall s \in \mathfrak{a} \quad s(x) = 0,$$

но отсюда получается, что $x \in Z(\mathfrak{a}) = X \setminus U_x$ (а это абсурдно).

Итак, выбрав такой s , мы построили для любой точки x многочлены p'_x и q'_x такие, что

$$\forall y \in X \quad q'_x(y)f(y) = p'_x(y) \text{ и } q'_x(x) \neq 0.$$

Теперь рассмотрим идеал $\sum_{x \in X} (q'_x) + I(X)$ в кольце $\mathbb{k}[x_1, \dots, x_n]$ и покажем, что он совпадает со всем кольцом. Предположим противное, то есть он содержится в некотором максимальном идеале $\mathfrak{m} \in \text{Spec}(\mathbb{k}[x_1, \dots, x_n])$. Но в таком случае

$$Z\left(\sum_{x \in X} (q'_x) + I(X)\right) \supset Z(\mathfrak{m}) = \text{pt} \in \mathbb{A}^n \implies \forall x \in X : q'_x(\text{pt}) = 0, \quad \forall h \in I(X) : h(\text{pt}) = 0.$$

Это даёт противоречие, так как

- Если $\text{pt} \notin X$, то не может быть такого, что $\forall h \in I(X) : h(\text{pt}) = 0$.
- Если же $\text{pt} \in X$, то по построению $q'_{\text{pt}}(\text{pt}) \neq 0$.

Итак, мы показали, что

$$\sum_{x \in X} (q'_x) + I(X) = (1) \implies \sum_{x \in X} (\overline{q'_x}) = (\overline{1}) \text{ в } A(X),$$

откуда существуют $\overline{\ell_{x_i}} \in A(X)$ такие, что

$$\sum_{i=1}^N \overline{\ell_{x_i}} \cdot \overline{q'_{x_i}} = \overline{1} \quad \text{на } X.$$

Но, ранее мы показали, что $q'_x \overline{f} = p'_x$ на X . Домножая сумму выше на \overline{f} , мы получаем, что

$$\sum_{i=1}^N \overline{\ell_{x_i}} \cdot \overline{p'_{x_i}} = \overline{f} \in A(X).$$

Таким образом, мы построили для каждой регулярной функции прообраз в $A(X)$. □

Предложение 7. Регулярная функция $f: X \rightarrow \mathbb{k}$ непрерывна, если отождествить \mathbb{k} с \mathbb{A}^1 с топологией Зарисского.

Доказательство. Докажем сначала такую лемму из общей топологии:

Лемма 2. Пусть X — топологическое пространство, $T \subset X$, а U_i — открытое покрытие X . Утверждается, что T замкнуто в X тогда и только тогда, когда $\forall i: T \cap U_i$ замкнуто в U_i .

Доказательство. В самом деле,

$$V = X \setminus T = \bigcup_i (U_i \setminus T) = \bigcup_i \underbrace{(U_i \setminus (T \cap U_i))}_{\text{открытое}}. \quad \square$$

Достаточно показать, что прообраз замкнутого множества замкнут. Как мы видели, замкнутые множества в \mathbb{A}^1 — конечные наборы точек, поэтому достаточно показать, что

$$\forall a \in \mathbb{k} \quad f^{-1}(a) = \{P \in X \mid f(P) = a\} \text{ — замкнуто.}$$

Как мы видели в лемме, это достаточно проверять локально. Пусть U — открытое множество, на котором f можно представить в виде g/h , где $g, h \in \mathbb{k}[x_1, \dots, x_n]$ и h не имеет нулей в U . Тогда

$$f^{-1}(a) \cap U = \{P \in U \mid g(P)/h(P) = a\}, \quad \text{но } g(P)/h(P) = a \iff (g - ah)(P) = 0,$$

откуда $f^{-1}(a) \cap U = Z(g - ah) \cap U$ — замкнуто в U . □

1.5 Морфизмы алгебраических многообразий

Определение 13. Пусть X, Y — квазиаффинные многообразия; $\varphi: X \rightarrow Y$ — морфизм, если

1. φ непрерывно;
2. Для каждого открытого $V \subset Y$ и каждой регулярной функции $f: V \rightarrow \mathbb{k}$ её пулбэк $\varphi^*(f) = f \circ \varphi: \varphi^{-1}(V) \rightarrow \mathbb{k}$ — регулярная функция.

Замечание 6. В частности, теперь у нас определено понятие изоморфизма многообразий. Отметим, что изоморфизм обязательно является биективным и непрерывным в обе стороны морфизмом, однако биективный и бинепрерывный морфизм может и не быть изоморфизмом.

Предложение 8. Квазиаффинные многообразия (и морфизмы, определенные как в 13) образуют категорию, которую мы будем обозначать $\mathbf{qAff}_{\mathbb{k}}$.

Предложение 9. Пусть X — квазиаффинное многообразие, $Y \subset \mathbb{A}_{\mathbb{k}}^n$ — тоже квазиаффинное многообразие. В таком случае $\psi: X \rightarrow Y$ является морфизмом в точности тогда и только тогда, когда функции

$$\psi^*(x_i): X \xrightarrow{\psi} Y \xrightarrow{x_i} \mathbb{k}$$

являются регулярными на X .

Доказательство. Если ψ — морфизм, то эти функции регулярны просто по определению морфизма. Теперь докажем утверждение в обратную сторону.

Покажем непрерывность. Возьмём замкнутое $T \subset Y$ и проверим, что $\psi^{-1}(T)$ замкнуто. Достаточно проверить это локально, то есть в окрестности любой точки. Возьмём произвольную точку $x \in X$ и докажем, что существует такая окрестность $U_x \ni x$, что $U_x \cap \psi^{-1}(T)$ замкнуто в U_x .

Так как функции $\psi^*(x_i): X \rightarrow \mathbb{k}$ регулярны, то в некоторой окрестности⁴ x мы можем представить отображение ψ в виде

$$(x_1, \dots, x_m) \mapsto \left(\frac{f_1(x_1, \dots, x_m)}{g_1(x_1, \dots, x_m)}, \dots, \frac{f_n(x_1, \dots, x_m)}{g_n(x_1, \dots, x_m)} \right)$$

Если T задаётся многочленами F_1, \dots, F_k , то есть $T = \{y \in Y \mid F_1(y) = \dots = F_k(y) = 0\}$, то

$$\psi^{-1}(T) \cap U_x = \left\{ (x_1, \dots, x_m) \mid F_1 \left(\frac{f_1}{g_1}(x_1, \dots, x_m), \dots, \frac{f_n}{g_n}(x_1, \dots, x_m) \right) = \dots = 0 \right\},$$

откуда $\psi^{-1}(T) \cap U_x$ замкнуто в U_x .

Теперь надо проверить второе условие. Его также можно проверять локально. Возьмём открытое $U \subset Y$ и рассмотрим на нём регулярную функцию f . Покажем, что $f \circ \psi$ регулярна на $\psi^{-1}(U)$. Мы можем покрыть U окрестностями, на которых f представляется, как отношение многочленов: пусть $U = \bigcup U_i$ и

$$f|_{U_i} = \frac{g_i}{h_i}.$$

Теперь достаточно доказать, что $\psi^*(f|_{U_i})$ регулярны на $\psi^{-1}(U_i)$, а для этого достаточно доказать, что $\psi^*(g_i)$ и $\psi^*(h_i)$ регулярны. Но, это очевидно, так как по условию $\psi^*(x_i)$ регулярны, а g_i и h_i — многочлены от x_i . \square

1.6 Антиэквивалентность $\text{Aff}^{\text{op}} \cong \mathbb{k}\text{-Alg}$

Предложение 10. Пусть X, Y — многообразия, причем Y — аффинное. Имеется естественное биективное отображение (изоморфизм бифункторов)

$$\text{Hom}_{\text{qAff}}(X, Y) \xrightarrow{\sim} \text{Hom}_{\mathbb{k}\text{-Alg}}(A(Y), \mathcal{O}(X)).$$

Естественность тут понимается в обычном смысле: а именно, если у нас есть морфизм $X_1 \rightarrow X_2$, то мы получим коммутативную диаграмму:

$$\begin{array}{ccc} \text{Hom}_{\text{qAff}}(X_2, Y) & \xleftarrow{\sim} & \text{Hom}_{\mathbb{k}\text{-Alg}}(A(Y), \mathcal{O}(X_2)) \\ \downarrow & & \downarrow \\ \text{Hom}_{\text{qAff}}(X_1, Y) & \xleftarrow{\sim} & \text{Hom}_{\mathbb{k}\text{-Alg}}(A(Y), \mathcal{O}(X_1)) \end{array}$$

И, если же у нас есть морфизм $Y_1 \rightarrow Y_2$, то мы получим коммутативную диаграмму:

⁴Достаточно взять окрестность из определения для каждой из координат и пересечь их.

$$\begin{array}{ccc}
\mathrm{Hom}_{\mathbf{qAff}}(X, Y_1) & \xleftarrow{\sim} & \mathrm{Hom}_{\mathbf{k-Alg}}(A(Y_1), \mathcal{O}(X)) \\
\downarrow & & \downarrow \\
\mathrm{Hom}_{\mathbf{qAff}}(X, Y_2) & \xleftarrow{\sim} & \mathrm{Hom}_{\mathbf{k-Alg}}(A(Y_2), \mathcal{O}(X))
\end{array}$$

Доказательство. Пусть задан морфизм $\varphi: X \rightarrow Y$, он переводит регулярные функции на Y в регулярные функции на X (при помощи пуллбека). Значит, он индуцирует отображение $\varphi^*: \mathcal{O}(Y) \rightarrow \mathcal{O}(X)$:

$$f \in \mathcal{O}(Y), \quad f \mapsto \varphi^*(f) \in \mathcal{O}(X).$$

Совершенно ясно, что это отображение является гомоморфизмом \mathbf{k} -алгебр. По теореме 4, $\mathcal{O}(Y) \cong A(Y)$, так что мы получаем гомоморфизм $A(Y) \rightarrow \mathcal{O}(X)$.

Теперь построим обратное отображение. Пусть задан гомоморфизм \mathbf{k} -алгебр $h: A(Y) \rightarrow \mathcal{O}(X)$. Y — аффинное, так что $A(Y) = \mathbf{k}[x_1, \dots, x_n]/I(Y)$. Рассмотрим $\xi_i = h(\overline{x_i}) \in \mathcal{O}(X)$. Эти функции определены на всём X , так что мы можем определить отображение

$$\psi: X \rightarrow \mathbb{A}^n, \quad \psi(P) = (\xi_1(P), \dots, \xi_n(P)).$$

Покажем, что на самом деле ψ действует в Y . Так как $Y = Z(I(Y))$, достаточно показать, что $\forall f \in I(Y), \forall P \in X : f(\psi(P)) = 0$. Так как f — многочлен, а h — гомоморфизм \mathbf{k} -алгебр,

$$f(\psi(P)) = f((\xi_1(P), \dots, \xi_n(P))) = h(f(\overline{x_1}, \dots, \overline{x_n}))(P) = 0,$$

так как $f \in I(Y)$. Так по гомоморфизму \mathbf{k} -алгебр $h: A(Y) \rightarrow \mathcal{O}(X)$ мы построили отображение $\psi: X \rightarrow Y$. То, что ψ — морфизм, напрямую вытекает из предложения 9.

Дальше в качестве упражнения идёт проверка того, что построенные отображения $\mathrm{Hom}_{\mathbf{qAff}}(X, Y) \xrightarrow{\sim} \mathrm{Hom}_{\mathbf{k-Alg}}(A(Y), \mathcal{O}(X))$ взаимно обратны.

Естественность данного изоморфизма оставляется в качестве упражнения. \square

Заметим, что если оба многообразия аффинные, то мы получаем соответствие (естественный изоморфизм)

$$\mathrm{Hom}_{\mathbf{Aff}}(X, Y) \xrightarrow{\sim} \mathrm{Hom}_{\mathbf{k-Alg}}(A(Y), A(X)).$$

То есть, мы получаем (контравариантный) функтор $\mathrm{Aff}_{\mathbf{k}}^{\mathrm{op}} \rightarrow \mathbf{k-Alg}$ (где алгебры конечно порождённые и редуцированные⁵):

$$A: \mathrm{Aff}_{\mathbf{k}}^{\mathrm{op}} \rightarrow \mathbf{k-Alg}, \quad X \mapsto A(X).$$

Кроме того, мы видели, что есть и обратный функтор: если $A \in \mathbf{k-Alg}$, то мы можем рассмотреть аффинное многообразие X' такое, что $A(X') \cong A$ и сопоставить $A \rightarrow X'$. Например, можно представить $A \cong \mathbf{k}[x_1, \dots, x_N]/I$, и тогда $X' = Z(I) \subset \mathbb{A}_{\mathbf{k}}^N$.

Этот функтор задан корректно, в частности, если взять другое многообразие X такое, что $A(X) \cong A(X')$, то изоморфизм алгебр будет индуцировать и изоморфизм многообразий $X \cong X'$ (так как функтор переводит изоморфизмы в изоморфизмы).

Таким образом, мы доказали такую теорему:

⁵Других в этом конспекте не встретится.

Теорема 5. Категория аффинных многообразий Aff антиэквивалентна категории конечно порождённых редуцированных \mathbb{k} -алгебр.

Переводя это на существенно менее изысканный язык, мы получаем такое следствие

Следствие 4. Аффинные многообразия X и Y изоморфны тогда и только тогда, когда их аффинные координатные кольца $A(X)$ и $A(Y)$ изоморфны как \mathbb{k} -алгебры.

1.7 Рациональные функции

Определение 14. Пусть X — неприводимое аффинное многообразие, U, V — непустые открытые подмножества, а f и g — регулярные функции на U и V соответственно. В таком случае будем говорить, что $(U, f) \sim (V, g)$ если $f = g$ на $U \cap V$.

Класс эквивалентности по этому отношению мы будем называть *рациональной функцией*.

Областью определения данной рациональной функции называется объединение всех U таких, что данная функция эквивалентна (U, f) для некоторой $f : U \rightarrow \mathbb{k}$.

Замечание 7. Множество всех рациональных функций на X образует поле, которое мы будем обозначать через $\mathbb{k}(X)$.

Проверим, что это в самом деле поле. Так как X неприводимо, любые два непустых открытых подмножества X имеют непустое пересечение (по 1), и мы можем определить сложение и умножение, превратив $\mathbb{k}(X)$ в кольцо. Кроме того, если $(U, f) \in K(X)$ и $f \neq 0$, то мы можем ограничить f на открытое множество $V = U \setminus (U \cap Z(f))$, на котором f не имеет нулей, и тогда $1/f$ регулярна на V , и пара $(V, 1/f)$ будет обратным элементом к (U, f) .

Отметим, что для неприводимого аффинного многообразия X определение поля рациональных функций $\mathbb{k}(X)$ можно дать несколько иначе по сравнению с определением 14.

Так как X неприводимо, то координатное кольцо $A(X)$ целостно, и мы можем рассматривать его поле частных. Кроме того, рассматривая очевидное (инъективное) отображение

$$A(X) \rightarrow \mathbb{k}(X).$$

мы получаем и вложение полей $\text{Frac}(A(X)) \hookrightarrow \mathbb{k}(X)$. Вложение полей инъективно всегда; сюръективность следует из определения регулярной функции: на некоторой окрестности $U \subset X$ регулярная функция представима в виде частного многочленов g/h , значит, она эквивалентна рациональной функции $(U, g/h)$, которая безусловно лежит в образе $\text{Frac}(A(X))$. Тем самым, это изоморфизм.

1.8 Главные аффинные окрестности

Определение 15. Главным открытым множествами (или, аффинными окрестностями) в \mathbb{A}^n называют множества вида

$$D(f) \stackrel{\text{def}}{=} \mathbb{A}^n \setminus Z(f),$$

где f — некоторый многочлен из $\mathbb{k}[x_1, \dots, x_n]$.

Пусть X — аффинное многообразие, $\bar{f} \in A(X) = \mathbb{k}[x_1, \dots, x_n]/I(X)$. Определим

$$D(\bar{f}) \stackrel{\text{def}}{=} D(f) \cap X = X \setminus Z(\bar{f}).$$

Ясно, что определение корректно, так как утверждение $f(x) = 0$ для точки $x \in X$ не зависит от выбора представителя f класса \bar{f} .

Замечание 8. Ясно, что если $f = 1$, то $D(f) = \mathbb{A}^n$, откуда $D(\bar{f}) = X$.

Для краткости обозначим $A = A(X)$ и рассмотрим главную локализацию

$$A_{\bar{f}} = S^{-1}A, \text{ где } S = \{\bar{f}^n \mid n \in \mathbb{N}\}.$$

Замечание 9. Отметим, что возможен случай, когда $A_{\bar{f}} = 0$, но тогда $\exists k: \bar{f}^k = 0$, а так как $I(X)$ — радикальный идеал, это равносильно тому, что $\bar{f} = 0$, что равносильно тому, что $f \in I(X)$, то есть

$$D(\bar{f}) = X \setminus Z(\bar{f}) = \emptyset.$$

В случае, когда $D(\bar{f}) \neq \emptyset$, мы получаем гомоморфизм колец

$$A_{\bar{f}} \rightarrow \mathcal{O}(D(\bar{f})), \quad \frac{\bar{a}}{\bar{f}^k} \mapsto \text{функция } \frac{\bar{a}}{\bar{f}^k}$$

- Этот гомоморфизм инъективен:

$$\frac{\bar{a}}{\bar{f}^k} \Big|_{D(\bar{f})} = 0 \implies \bar{a}|_{D(\bar{f})} = 0 \implies \bar{a} \cdot \bar{f}|_X = 0 \implies af \in I(X) \implies \bar{a}\bar{f} = 0 \in A(X),$$

откуда $\bar{a}/\bar{f}^k = 0$ в локализации $A(X)_{\bar{f}}$.

- Кроме того, он сюръективен. Пусть $r \in \mathcal{O}(D(\bar{f}))$, то есть

$$\forall x \in D(\bar{f}) \quad \exists \text{ окрестность } U_x \ni x, \bar{g}_x, \bar{h}_x \in A(X): r\bar{h}_x = \bar{g}_x \text{ на } U_x$$

и h_x не имеет нулей в U_x .

Выбирая многочлен $s_x \in A(X)$, не равный нулю в точке x , но обращающийся в ноль на дополнении $D(\bar{f})$, мы можем полагать, что наше равенство выполнено на всём X (см. доказательство теоремы 4). Не умаляя общности, будем считать так изначально.

- Заметим, что

$$Z\left(\sum_{x \in D(\bar{f})} (h_x) + I(X)\right) \subset Z(f),$$

так как если $y \in Z\left(\sum_{x \in D(\bar{f})} (h_x) + I(X)\right)$, то $y \in X \setminus D(\bar{f}) = X \cap Z(f)$.

- Получается,

$$\sqrt{(f)} \subset \sqrt{\sum_{x \in D(\bar{f})} (h_x) + I(X)} \implies f^m \in \sum_{x \in D(\bar{f})} (h_x) + I(X) \implies \bar{f}^m \in \sum_{x \in D(\bar{f})} (h_x)$$

Значит, мы можем представить \bar{f}^m в виде

$$\bar{f}^m = \sum_{i=1}^N \overline{h_{x_i}} \cdot \bar{\ell}_i, \quad x_i \in D(\bar{f}).$$

Наконец, домножая это равенство на r мы получаем

$$\bar{f}^m r = \sum_{i=1}^N \overline{g_{x_i} \ell_{x_i}} \implies r = \frac{\bar{a}}{\bar{f}^m} \in A_{\bar{f}}.$$

Таким образом, мы доказали такое предложение:

Предложение 11. $A(X)_{\bar{f}} \cong \mathcal{O}(D(\bar{f}))$.

Полезно также рассмотреть альтернативное доказательство этого факта.

Альтернативное доказательство предложения 11. Рассмотрим отображение

$$A_{\bar{f}} \xrightarrow{\sim} A[t]/(\bar{f}t - 1), \quad \frac{a}{\bar{f}^k} \mapsto \bar{a}t^k.$$

Это изоморфизм, в чём легко убедиться, используя универсальные свойства, определяющие локализацию и кольцо многочленов. Кроме того,

$$A = \mathbb{k}[x_1, \dots, x_n]/I(X) \implies A[t]/(\bar{f}t - 1) \cong \mathbb{k}[x_1, \dots, x_n, t]/(I(X) + (\bar{f}t - 1)),$$

откуда видно, что $A_{\bar{f}}$ — это координатное кольцо многообразия

$$Y = \{(x_1, \dots, x_n, t) \in \mathbb{A}_{\mathbb{k}}^{n+1} \mid (x_1, \dots, x_n) \in X, \quad f(x_1, \dots, x_n)t - 1 = 0\}.$$

Рассмотрим коммутативную диаграмму колец:

$$\begin{array}{ccc} A(X)_{\bar{f}} & \xrightarrow{\sim} & A(X)[t]/(\bar{f}t - 1) \\ \downarrow \text{---} & & \downarrow \sim \\ \mathcal{O}(D(\bar{f})) & \xrightarrow{\sim} & \mathcal{O}(Y) \end{array}$$

Нижняя горизонтальная стрелка получается из того, что $Y \xrightarrow{\sim} D(\bar{f})$ посредством (взаимно обратных) отображений

$$(x_1, \dots, x_n, t) \mapsto (x_1, \dots, x_n), \quad (x_1, \dots, x_n) \mapsto (x_1, \dots, x_n, 1/f(x_1, \dots, x_n))$$

Так как горизонтальные и правая вертикальная стрелка — изоморфизмы, левая вертикальная стрелка — тоже изоморфизм. \square

1.9 Эквивалентные определения размерности неприводимого аффинного многообразия

Предложение 12. Пусть X — неприводимое квазиаффинное многообразие, $U \subset X$ — открытое подмножество. В таком случае $\dim U = \dim X$.

Доказательство. **I.** Пусть X — аффинное. Так как U открытое,

$$\begin{aligned} U = X \setminus Z(\overline{f_1}, \dots, \overline{f_n}) \supset X \setminus Z(\overline{f_1}) = D(\overline{f_1}) \implies D(\overline{f_1}) \subset U \subset X \implies \\ \implies \dim D(\overline{f_1}) \leq \dim U \leq \dim X. \end{aligned}$$

Но, как мы знаем из предложения 11 и теоремы 2, $\dim D(\overline{f_1}) = \dim A(X)_{\overline{f_1}} = \text{tr. deg}_{\mathbb{k}} \text{Frac}(A(X)_{\overline{f_1}})$. Осталось заметить, что поля частных $A(X)_{\overline{f_1}}$ и $A(X)$ совпадают, откуда мы заключаем, что $\dim U = \dim X$.

II. Пусть X квазиаффинное. Имеют место включения $U \subset X \subset \overline{X}$, где \overline{X} — аффинное. Так как U — открытое подмножество \overline{X} , по пункту I мы имеем

$$\dim U = \dim \overline{X}.$$

С другой стороны, $\dim U \leq \dim X \leq \dim \overline{X}$, откуда мы получили нужное. \square

Замечание 10. Пусть X — квазиаффинное многообразие. Тогда $\dim X$ — наибольшая из размерностей его неприводимых компонент.

1.10 Прямое произведение многообразий и его первые приложения

Пусть $X \subset \mathbb{A}^m$, $Y \subset \mathbb{A}^n$ — аффинные многообразия. Пусть $X = Z(f_1, \dots, f_k)$, $Y = Z(g_1, \dots, g_\ell)$, тогда

$$X \times Y = \{(x_1, \dots, x_m, y_1, \dots, y_n) \mid f_i(x_1, \dots, x_m) = 0, g_j(y_1, \dots, y_n) = 0 \ \forall i, j\}.$$

То есть, прямое произведение естественно снабжается структурой аффинного многообразия в $\mathbb{A}^{m \times n}$. Позже мы докажем, что это произведение в категорном смысле.

Также видно, что если X и Y — квазиаффинные, то их прямое произведение тоже квазиаффинное.

Предложение 13. Пусть $X \subset \mathbb{A}^m$, $Y \subset \mathbb{A}^n$ — неприводимые аффинные многообразия, тогда $X \times Y$ — неприводимое аффинное многообразие в $\mathbb{A}^m \times \mathbb{A}^n$.

Доказательство. Предположим противное, то есть, что

$$X \times Y = Z_1 \cup Z_2, \quad Z_i \neq X \times Y.$$

Ясно, что $\forall x \in X : \{x\} \times Y \cong Y$ — неприводимое, откуда $\{x\} \times Y \subset Z_1$ или $\{x\} \times Y \subset Z_2$. Но отсюда

$$X = X_1 \cup X_2, \quad X_j = \{x \mid \{x\} \times Y \subset Z_j\}.$$

Покажем, что множества X_1 и X_2 замкнутые. Для этого достаточно заметить, что

$$X_1 = \bigcap_{y \in Y} X_y, \quad \text{где } X_y = \{x \in X \mid (x, y) \in Z_1\},$$

а X_y — замкнуты, так как если $Z_1 = Z(f_1(x, y), \dots, f_k(x, y))$, то

$$X_{\tilde{y}} = Z(f_1(x, \tilde{y}), \dots, f_k(x, \tilde{y})).$$

В дальнейшем мы увидим, что вложение $X \rightarrow X \times Y, x \mapsto (x, \tilde{y})$ непрерывно, откуда сразу будет следовать, что $X_{\tilde{y}}$ замкнуто — это прообраз Z_1 при таком вложении.

Так или иначе, мы приходим к противоречию, так как из неприводимости X следует, что $X \subset X_1$ или $X \subset X_2$, откуда $X \times Y = Z_1$ или $X \times Y = Z_2$ (что противоречит нашему предположению). \square

Предложение 14. Пусть X, Y — неприводимые аффинные многообразия. Тогда $\dim(X \times Y) = \dim X + \dim Y$.

Доказательство. Пусть $\dim X = r, \dim Y = s$. Поле функций $\mathbb{k}(X)$ порождается ровно r алгебраически независимыми координатными функциями u_1, \dots, u_r . Аналогично, $\mathbb{k}(Y)$ порождается координатными функциями v_1, \dots, v_s и они алгебраически независимы. Совершенно ясно, что

$$\dim(X \times Y) = \text{trdeg}(\mathbb{k}(X \times Y)) \leq r + s.$$

Остаётся показать, что система $(u_1, \dots, u_r, v_1, \dots, v_s)$ будет алгебраически независимой в $\mathbb{k}(X \times Y)$.

Предположим, что

$$\sum f_{i_1 i_2 \dots i_r}(v_1, \dots, v_s) u_1^{i_1} \cdot \dots \cdot u_r^{i_r} = 0.$$

Подставляя $a_i \in \mathbb{k}$, мы получаем полиномиальное соотношение на u_i :

$$\sum f_{i_1 i_2 \dots i_r}(a_1, \dots, a_s) u_1^{i_1} \cdot \dots \cdot u_r^{i_r} = 0,$$

а так как u_i алгебраически независимы, отсюда следует, что $f_{i_1 \dots i_r}(a_1, \dots, a_s) = 0$. По произвольности набора a_1, \dots, a_s , мы получаем, что $f_{i_1 i_2 \dots i_r}(v_1, \dots, v_s) = 0$, но так как v_i алгебраически независимы, отсюда следует, что $f_{i_1 \dots i_r} = 0$, что и требовалось. \square

Замечание 11. Здесь мы по существу использовали, что для аффинных $\mathbb{k}(X) = \text{Frac}(A(X))$.

Обсудим, что происходит в случае приводимых многообразий. Если

$$X = \bigcup_i X_i, Y = \bigcup_j Y_j \quad X_i, Y_j \text{ — неприводимые,}$$

то $\dim X = \max \dim X_i$, а $\dim Y = \max \dim Y_j$. Несложно предъявить разложение $X \times Y$ в неприводимые:

$$X \times Y = \bigcup X_i \times Y_j$$

Таким образом, мы получили, что

Предложение 15. Пусть X, Y — многообразия, тогда $\dim(X \times Y) = \dim X + \dim Y$.

Теорема 6. Пусть $Y, Z \subset \mathbb{A}_{\mathbb{k}}^n$ — неприводимые аффинные многообразия, $\dim Y = r, \dim Z = s$. Тогда любая компонента $Y \cap Z$ имеет размерность $\geq r + s - n$.

Доказательство. Рассмотрим диагональное вложение

$$\Delta: \mathbb{A}^n \rightarrow \mathbb{A}^n \times \mathbb{A}^n = \mathbb{A}^{2n}, x \mapsto (x, x).$$

Образ $\Delta(\mathbb{A}^n)$ замкнут в \mathbb{A}^{2n} , так как он задаётся вот такой системой уравнений:

$$\begin{cases} y_1 = y_{n+1} \\ y_2 = y_{n+2} \\ \vdots \\ y_n = y_{2n} \end{cases} \quad (1)$$

Заметим, что имеет место изоморфизм

$$Y \cap Z \xrightarrow{\sim} \Delta(\mathbb{A}^n) \cap (Y \times Z).$$

Так как при изоморфизме неприводимые компоненты переходят в неприводимые компоненты, размерности неприводимых компонент левой и правой частей равны. Заметим, что $\Delta(\mathbb{A}^n)$ — пересечение n гиперповерхностей (как видно из 1). Пользуясь теоремой 6 (и тем фактом, что $\dim Y \times Z = r + s$), мы получаем нужное. \square

Заметим, что в процессе доказательства мы установили, что $D(\bar{f})$ изоморфно аффинному подмногообразию в \mathbb{A}^{n+1} .

Упражнение 1. Если X, Y — аффинные, то $A(X \times Y) \cong A(X) \otimes_{\mathbb{k}} A(Y)$.

Замечание 12. Из упражнения выше следует, что над алгебраически замкнутым полем тензорное произведение целостных конечно порождённых алгебр — целостная конечно порождённая алгебра. Если поле не алгебраически замкнутое, то это не обязательно так.

1.11 О количестве порождающих идеала

Для алгебраического многообразия $X \subset \mathbb{A}_{\mathbb{k}}^n$ разумно задать вопрос о минимальном количестве образующих, задающих идеал $I(X) \subseteq \mathbb{k}[x_1, \dots, x_n]$. Будем считать, что X неприводимо, то есть $I(X) \subseteq \mathbb{k}[x_1, \dots, x_n]$ прост.

- Если $X \subset \mathbb{A}^1$, то любой идеал в $\mathbb{k}[x]$ главный, откуда достаточно одной образующей.
- В \mathbb{A}^2 есть идеалы высоты 0, 1, 2. Высоты 0 — только нулевой идеал, все идеалы высоты 1 — главные 1, а идеалы высоты 2 — максимальные, то есть $(x_1 - a_1, x_2 - a_2)$, отвечающие точкам.
- В \mathbb{A}^3 для высоты 2 уже всё сложно: $\forall n \in \mathbb{N} : \exists \mathfrak{p} \in \mathbb{k}[x, y, z]$: число образующих \mathfrak{p} хотя бы n .

Сейчас мы докажем, однако, что любое многообразие в n -мерном аффинном пространстве можно задать n уравнениями, или как пересечение n гиперповерхностей. Это не противоречит написанному выше, так как данные n образующих будут задавать не сам идеал $I(X)$, а некоторый J , такой, что $\sqrt{J} = I(X)$.

Лемма 3. Пусть R — нётерово кольцо. Следующие условия верны:

1. Любой минимальный простой идеал состоит из делителей нуля.

2. Множество всех делителей нуля нётерова кольца R представляет собой объединение конечного числа простых идеалов \mathfrak{p}_i , а $\mathfrak{p}_i = \text{Ann}(a_i)$ для некоторого $a_i \in R$.
3. Пусть R — нётерово кольцо, причем любой его элемент либо обратим, либо делитель нуля и вдобавок R редуцировано (т.е. $\text{NRad}(R) = 0$). Тогда $\dim R = 0$ (т.е. R — артиново кольцо).

Доказательство. Докажем сначала **первый пункт**. Пусть \mathfrak{p} — минимальный простой идеал. Так как в кольце $R_{\mathfrak{p}}$ идеал $\mathfrak{p}R_{\mathfrak{p}}$ максимальный, то

$$\text{NRad}(R_{\mathfrak{p}}) = \mathfrak{p}R_{\mathfrak{p}}.$$

Так $R_{\mathfrak{p}}$ нётерово (локализация нётерова кольца нётерова), значит идеал конечно порождён: $\mathfrak{p}R_{\mathfrak{p}} = (e_1, \dots, e_n)$. Если $\forall j : e_j^m = 0$, то

$$\text{NRad}(R_{\mathfrak{p}})^{nm} = 0.$$

Значит, $\forall a \in \mathfrak{p} : a^{nm} = 0$ в кольце $R_{\mathfrak{p}}$. Тогда $\exists s \in \mathfrak{p} : a^N s = 0$ в R , значит a — делитель нуля.

Второй пункт был в курсе коммутативной алгебры — это факт про примарное разложение идеала $0 \leq R$.

Теперь докажем **третий** пункт. Возьмём $\mathfrak{m} \in \text{Specm } R$, он полностью состоит из делителей нуля. По пункту 2:

$$\mathfrak{m} \subset \bigcup_{i=1}^m \mathfrak{p}_i \implies \mathfrak{m} \subset \mathfrak{p}_i \implies \mathfrak{m} = \mathfrak{p}_i.$$

Тем самым, $\mathfrak{m} = \text{Ann}(a)$ для некоторого $a \in R$. Предположим, что существует $\mathfrak{p} \subsetneq \mathfrak{m}$. Рассмотрим два случая:

1. $a \in \mathfrak{m}$. Значит, $a \in \text{Ann}(a)$, то есть $a^2 = 0$, но это противоречит тому, что $\text{NRad}(R) = 0$.
2. $a \notin \mathfrak{m}$. Возьмём $b \in \mathfrak{m} \setminus \mathfrak{p}$. Заметим, что $ab = 0$, причём $a \notin \mathfrak{p}, b \notin \mathfrak{p}$. Получили противоречие с тем, что идеал \mathfrak{p} простой. \square

Теорема 7. Пусть R — нётерово кольцо, а $S = R[x]$. Пусть $\dim R = d - 1$, $d \geq 1$, а $I \leq S$. Тогда $\exists f_1, \dots, f_d \in I$:

$$\sqrt{I} = \sqrt{(f_1, \dots, f_d)}.$$

Доказательство. Пусть $d = 1$, тогда $\dim R = 0$ и $R/\text{NRad}(R)$ — редуцированное артиново кольцо, то есть прямая сумма конечного числа полей

$$R/\text{NRad}(R) = K_1 \oplus K_2 \oplus \dots \oplus K_n.$$

С другой стороны, легко проверить, что $\text{NRad}(R[x]) = \text{NRad}(R)[x]$. Но тогда мы получаем, что

$$S/\text{NRad}(S) \cong K_1[x] \oplus \dots \oplus K_n[x],$$

а справа написано кольцо главных идеалов. В частности, идеал $(I + \text{NRad}(S))/\text{NRad}(S)$ главный, пусть он порождается $f \in I$. То есть в кольце S :

$$I + \text{NRad}(S) = (f) + \text{NRad}(S) \implies \sqrt{I} = \sqrt{I + \text{NRad}(S)} = \sqrt{(f) + \text{NRad}(S)} = \sqrt{(f)}.$$

Поясним равенство $\sqrt{I} = \sqrt{I + \text{NRad}(S)}$. Включение (\subset) очевидно, докажем включение (\supset) . Пусть $x \in \sqrt{I + \text{NRad}(S)}$, тогда $x^m = a + b$, где $a \in I$, $b \in \text{NRad}(S)$. Так как $b^N = 0$ для некоторого N , а $(x^m)^N \in I$, то $x \in \sqrt{I}$.

Тем самым, база индукции доказана, $\sqrt{I} = \sqrt{(f)}$.

Сделаем теперь **переход** $d - 1 \mapsto d$. Так как при факторизации по $\text{NRad}(R)$ размерность не меняется, а $\sqrt{I} = \sqrt{I + \text{NRad}(S)}$, то не умаляя общности мы можем полагать, что с самого начала кольцо редуцированное.

Рассмотрим U — множество всех не делителей нуля в R . Это мультипликативная система, можно рассмотреть локализацию $U^{-1}R = R[U^{-1}]$. Заметим, что в $R[U^{-1}]$ любой элемент либо обратим, либо является делителем нуля. По лемме 3 это кольцо будет редуцированным нётеровым кольцом размерности 0, то есть произведением конечного числа полей. Тогда

$$S[U^{-1}] = \prod K_i[x],$$

в частности, это кольцо главных идеалов. Пусть $I \cdot S[U^{-1}] = (f_1)$, где $f_1 \in I$.

В силу конечной порождённости $I \trianglelefteq S$, $\exists r \in U: rI \subset (f_1) \trianglelefteq S^6$. Так как r — не делитель нуля, то он не лежит в объединении всех минимальных простых идеалов кольца R (тут мы вновь пользуемся леммой 3). Перейдём к фактору и покажем, что

$$\dim R/(r) \leq d - 2$$

Пойдём от противного: пусть $\dim R/(r) \geq d - 1$, то есть имеется цепочка

$$\mathfrak{p}_0/(r) \subsetneq \mathfrak{p}_1/(r) \subsetneq \dots \subsetneq \mathfrak{p}_{d-1}/(r).$$

Поднимаясь к исходному кольцу, мы получаем такую цепочку:

$$(r) \subset \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_{d-1}.$$

Теперь видно, что идеал \mathfrak{p}_0 не может быть минимальным (так как r не лежит ни в каком минимальном), а значит, мы можем увеличить цепочку и получить противоречие.

Теперь мы можем применить к кольцу $R/(r)$ индукционное предположение: $\exists \overline{f_2}, \dots, \overline{f_d} \in I + (r)/(r)$:

$$\sqrt{I + (r)/(r)} = \sqrt{(\overline{f_1}, \dots, \overline{f_d})}.$$

Можно считать, что $f_2, \dots, f_d \in I$. Теперь остается проверить только, что

$$\sqrt{I} = \sqrt{(f_1, \dots, f_d)}.$$

По построению $f_1, f_2, \dots, f_d \in I$, проверим включение в обратную сторону. Действительно, если $x \in \sqrt{I}$, то $x^k \in I$, а кроме того, $\overline{x^m} \in \sqrt{(\overline{f_2}, \dots, \overline{f_d})} \cdot S/(r)$, то есть $x^m \in (r, f_2, \dots, f_d)$.

Перемножая, получаем $x^{k+m} \in x^m I \in (r, f_2, \dots, f_d)I$, но так как $rI \subset (f_1)$, то $x^{k+m} \in (f_1, \dots, f_d)$. \square

⁶Надо выразить образующие I в виде $\frac{a_i}{r_i} \cdot f_1$, где $r_i \in U$, и тогда в качестве r подойдёт произведение r_i . Стоит заметить, что локализация по U инъективна, так как в U нет делителей нуля.

Применим эту теорему.

Пусть $X \subset \mathbb{A}^n$ — аффинное многообразие, тогда $I(X) \subset S = \mathbb{k}[x_1, \dots, x_{n-1}][x_n] = R[x]$, $\dim R = n - 1$. По предыдущей теореме мы можем найти f_1, \dots, f_d такие, что

$$\sqrt{I(X)} = I(X) = \sqrt{(f_1, \dots, f_d)}.$$

Ясно, что $X = Z(I) = Z(\sqrt{(f_1, \dots, f_d)}) = Z(f_1, \dots, f_d)$, чего мы и хотели.

Следствие 5. В \mathbb{A}^n любое аффинное многообразие задаётся не более чем n уравнениями.

2 Проективные многообразия

2.1 Проективные многообразия

Пусть \mathbb{k} — наше базовое алгебраически замкнутое поле, определим проективное пространство $\mathbb{P}^n = \mathbb{P}_{\mathbb{k}}^n$. Как множество, это, разумеется, $(\mathbb{k}^{n+1} \setminus \{0\}) / \sim$ — кортежи, в которых хотя бы один элемент ненулевой, отфакторизованные по гомотетиям с коэффициентами из \mathbb{k} .

В этом контексте кольцо многочленов $S = \mathbb{k}[x_0, x_1, \dots, x_n]$ мы будем рассматривать, как градуированное кольцо. Для этого вкратце напомним терминологию:

Определение 16. Кольцо S называется *градуированным*⁷, если оно обладает разложением в прямую сумму

$$S = \bigoplus_{d \geq 0} S_d$$

абелевых групп S_d таких, что $S_d \cdot S_e \subset S_{d+e}$, индекс d пробегает \mathbb{N}_0 . Элементы из S_d мы будем называть *однородными степени d* .

Идеал $\mathfrak{a} \subset S$ мы будем называть *однородным*, если он представляется в виде

$$\mathfrak{a} = \bigoplus_{d \geq 0} (\mathfrak{a} \cap S_d).$$

Приведём несколько полезных фактов про однородные идеалы:

- Идеал однородный тогда и только тогда, когда он может быть порождён однородными элементами.
- Сумма, произведение, пересечение однородных идеалов, а также радикал однородного идеала однородны.
- Однородный идеал \mathfrak{a} простой тогда и только тогда, когда для любых двух *однородных* f, g из условия fg следует, что либо $f \in \mathfrak{a}$, либо $g \in \mathfrak{a}$.

Кольцо $S = \mathbb{k}[x_0, x_1, \dots, x_n]$ мы превратим в градуированное так: обозначим за S_d множество всех линейных комбинаций с коэффициентами из \mathbb{k} одночленов полной степени d (одночленов вида $x_0^{d_0} \cdot \dots \cdot x_n^{d_n}$, где $d_0 + \dots + d_n = d$).

⁷Если точнее, $\mathbb{N}_{\geq 0}$ -градуированным.

Кроме того, многочлены мы уже не можем рассматривать как функции на \mathbb{P}^n ввиду неоднозначности координатных представлений точек \mathbb{P}^n . Тем не менее, если f — однородный многочлен, то свойство f обращаться в 0 зависит только от класса эквивалентности (a_0, \dots, a_n) . Тем, самым, для однородного многочлена f имеет смысл говорить о множестве

$$Z(f) \stackrel{\text{def}}{=} \{P \in \mathbb{P}^n \mid f(P) = 0\}.$$

Соответственно, для любого множества T однородных элементов мы определяем

$$Z(T) \stackrel{\text{def}}{=} \{P \in \mathbb{P}^n \mid f(P) = 0 \quad \forall f \in T\}.$$

Если \mathfrak{a} — однородный идеал в S , то определим $Z(\mathfrak{a})$, как $Z(\mathfrak{a}) = Z(T)$, где T — множество всех однородных элементов из \mathfrak{a} . В силу нётеровости кольца S любое множество однородных элементов T содержит такое конечное подмножество f_1, \dots, f_r , что $(T) = (f_1, \dots, f_r)$.

Определение 17. Подмножество проективного пространства $Y \subset \mathbb{P}^n$ называется *проективным алгебраическим многообразием*, если существует такое множество $T \subset S$ однородных элементов, что $Y = Z(T)$.

Таким образом, мы можем задать на \mathbb{P}^n топологию Зарисского, объявив замкнутыми алгебраические многообразия.

Определение 18. Также, для любого $Y \subset \mathbb{P}^n$ определим его *однородный идеал* $I(Y) \subset S$, как идеал, порождённый множеством однородных элементов $f \in S$ таких, что $f(P) = 0$ для всех $P \in Y$. *Однородное координатное кольцо* $S(Y)$ проективного многообразия Y определим как факторкольцо $S(Y) = S/I(Y)$.

Упражнение 2. Пусть $S = \mathbb{k}[x_1, \dots, x_n]$, обозначим за S^h множество однородных многочленов. Докажите, что

1. Если $T_1 \subset T_2 \subset S^h$, то $Z(T_2) \subset Z(T_1)$.
2. Если $Y_1 \subset Y_2 \subset \mathbb{P}^n$, то $I(Y_2) \subset I(Y_1)$.
3. $I(Y_1 \cup Y_2) = I(Y_1) \cap I(Y_2)$.
4. Пусть $I \subset S$ — однородный идеал, $Z(I) \neq \emptyset$. Тогда $I(Z(I)) = \sqrt{I}$.
5. Пусть $I \subset S$ — однородный идеал. Тогда следующие условия равносильны:
 - (a) $Z(I) = \emptyset$
 - (b) $\sqrt{I} = (1)$ или $\sqrt{I} = S^+ = \bigoplus_{d>0} S_d$
 - (c) $S_d \subset I$ для некоторого d .

Теорема 8 (Однородный Nullstellensatz). Пусть $I \subset \mathbb{k}[x_0, \dots, x_n]$ — однородный идеал, а $f \in \mathbb{k}[x_0, \dots, x_n]$ — однородный элемент положительной степени. Если $\forall P \in Z(I) \subset \mathbb{P}^n : f(P) = 0$, то $\exists m : f^m \in I$.

Это теорема легко сводится к аффинному случаю.

Определение 19. *Квазипроективным многообразием* мы будем называть открытое подмножество проективного многообразия.

Наша дальнейшая цель состоит в том, чтоб показать, что n -мерное проективное пространство обладает открытым покрытием, состоящим из n -мерных аффинных пространств. И, как весьма полезное следствие, что *всякое проективное/квазипроективное многообразие обладает открытым покрытием состоящие из аффинных многообразий* (это очень удобно, если мы доказываем что-то локально).

Пусть $H_i = Z(x_i)$ — координатные гиперплоскости. Рассмотрим множества

$$U_i = \mathbb{P}^n \setminus H_i = \{(x_0 : \dots : x_n) \in \mathbb{P}^n \mid x_i \neq 0\}.$$

Совершенно ясно, что \mathbb{P}^n покрывается квазиаффинными U_i (так как у любой точки хотя бы одна из однородных координат отлична от нуля). Рассмотрим отображение

$$\varphi_i: U_i \rightarrow \mathbb{A}^n, \quad (a_0 : \dots : a_n) \mapsto \left(\frac{a_0}{a_i} : \dots : \frac{a_n}{a_i} \right).$$

Отметим, что это отображение определено корректно, так как частное a_j/a_i не зависит от выбора однородных координат.

Предложение 16. *Отображение φ_i осуществляет гомеоморфизм $U_i \xrightarrow{\sim} \mathbb{A}^n$.*

Доказательство. Очевидно, что оно биективно. Достаточно показать, что замкнутые множества в U_i соответствуют замкнутым множествам в \mathbb{A}^n . Не умаляя общности, $i = 0$, $U_0 = U$, $\varphi_0 = \varphi$.

Пусть $A = \mathbb{k}[y_1, \dots, y_n]$. Рассмотрим отображения

$$\alpha: S^h \rightarrow A, \quad \alpha(f) = f(1, y_1, \dots, y_n), \quad \beta: A \rightarrow S^h, \quad \beta(g) = x_0^{\deg g} \cdot g\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right).$$

Пусть $Y \subset U$ — замкнутое подмножество. Тогда \bar{Y} (тут замыкание берётся в \mathbb{P}^n) — проективное многообразие, то есть $\bar{Y} = Z(T)$ для некоторого $T \subset S^h$. Положим $T' = \alpha(T)$. Непосредственно проверяется, что $\varphi(Y) = Z(T')$. И обратно, если W — замкнутое подмножество в \mathbb{A}^n , то $W = Z(T')$ для некоторого $T' \subset A$ и легко проверить, что

$$\varphi^{-1}(W) = Z(\beta(T')) \cap U.$$

Значит и φ и φ^{-1} замкнутые, что и требовалось. \square

Следствие 6. *Пусть Y — проективное (квазипроективное) многообразие. Тогда Y покрывается открытыми множествами $Y \cap U_i$, гомеоморфными аффинным (квазиаффинным) многообразиям, причем гомеоморфизм осуществляется определённым выше отображением φ_i .*

Замечание 13. На самом деле, даже квазипроективное многообразие покрывается аффинными картами. Для доказательства этого утверждения надо вспомнить, что у каждой точки квазиаффинного многообразия имеется главная аффинная окрестность. В случае, если надо, из квазикомпактности этих окрестностей можно выбрать конечное количество.

Определение 20. Пусть X — квазипроективное многообразие. Функция $f: X \rightarrow \mathbb{k}$ называется *регулярной* в точке $P \in Y$, если существует такая открытая окрестность $U \subset X$ точки P и такие **однородные** многочлены $g, h \in \mathbb{k}[x_0, \dots, x_n]$ **одной и той же степени**, что

- h не имеет нулей в U .
- $f = g/h$ в U .

Функция f *регулярна на Y* , если она регулярна в каждой точке Y .

Замечание 14. Отметим, что в этом случае сами g и h не являются функциями на \mathbb{P}^n , но вот их отношение (при $h \neq 0$) определено корректно, так как они имеют одинаковую степень однородности.

Пример 6. Например, если $X = U_0$, то функция $f(x_0, \dots, x_n) = x_1/x_0$ регулярна на X .

Определение морфизма на квазипроективные многообразия переносится без изменений:

Определение 21. Пусть X, Y — квазипроективные многообразия, $\varphi: X \rightarrow Y$ — *морфизм*, если

1. φ непрерывно.
2. Для каждого открытого $V \subset Y$ и каждой регулярной функции $f: V \rightarrow \mathbb{k}$ её пулбек $\varphi^*(f) = f \circ \varphi: \varphi^{-1}(V) \rightarrow \mathbb{k}$ — регулярная функция.

Предложение 17. Пусть $U_i \subset \mathbb{P}^n$ — определённое выше открытое множество. Отображение $\varphi_i: U_i \rightarrow \mathbb{A}^n$ определённое выше является изоморфизмом.

Доказательство. Выше мы уже показали, что это отображение — гомеоморфизм. Теперь нужно показать, что на каждом открытом множестве регулярные функции этих многообразий совпадают. Регулярные функции на U_i локально представляются в виде отношений однородных многочленов от x_0, \dots, x_n одинаковой степени, а на \mathbb{A}^n — в виде отношений многочленов от y_1, \dots, y_n . Легко видеть, что они отождествляются с помощью отображений α и β , определённых в доказательстве 16. \square

Пусть f — регулярная функция на всём \mathbb{P}^n . Тогда $f|_{U_i}$ — регулярная функция на U_i , а так как U_i (по утверждению выше) отождествляется с \mathbb{A}^n , $f|_{U_i}$ отождествляется с регулярной функции на \mathbb{A}^n (причем, при помощи определённых нами выше отображений). Тем самым, $f|_{U_i}$ — многочлен от переменных $\frac{x_j}{x_i}$, $j \neq i$. Значит, мы можем представить её в виде

$$f = \frac{r_i(x_0, \dots, x_n)}{x_i^m},$$

где r_i — многочлен.

Посмотрим, что происходит на пересечениях. Например,

$$\text{на } U_0 \cap U_1: \frac{r_0(x_0, \dots, x_n)}{x_0^m} = \frac{r_1(x_0, \dots, x_n)}{x_1^k}$$

Это равенство имеет вид везде, где $x_0, x_1 \neq 0$, легко видеть, что это означает равенство элементов $\mathbb{k}(x_0, \dots, x_n)$. Используя единственность разложения на множители, получаем, что $m = k = 0$, значит, и степень числителя тоже нулевая. Тем самым, функция равна какой-то константе, а на пересечениях константы согласованы. Получаем, что функция f постоянна. Итак, мы доказали такое утверждение:

Предложение 18. *Всякая регулярная функция $f : \mathbb{P}^n \rightarrow \mathbb{k}$ постоянна.*

Можно провести аналогию между этим утверждением и теоремой Лиувилля из комплексного анализа.

Предложение 19. *Любое квазиаффинное многообразие изоморфно некоторому квазипроективному.*

Доказательство. Как мы видели, у нас есть изоморфизм $\mathbb{A}^n \xrightarrow{\sim} U_0$. Причём, при отображении в эту сторону многочлены гомогенизировались:

$$f(y_1, \dots, y_n) \mapsto f^h(x_0, \dots, x_n) = x_0^{\deg f} f\left(\frac{x_0}{x_1}, \dots, \frac{x_n}{x_0}\right).$$

Получаем следующую коммутативную диаграмму:

$$\begin{array}{ccc} \mathbb{A}^n & \xrightarrow{\sim} & U_0 \\ \uparrow & & \uparrow \\ Z(f) & \dashrightarrow & Z(f^h) \end{array}$$

Значит и соответствующие открытые куски будут изоморфны. \square

Это предложение говорит, что все определённые нами многообразия — (квази)аффинные и (квази)проективные — на деле являются квазипроективными, и в дальнейшем мы будем использовать квазипроективные многообразия, как наиболее общий вид алгебраического многообразия.

Пример 7. Рассмотрим кривую в $C \subset \mathbb{P}^2$, $C = Z(y^2 - xz)$. Рассмотрим отображения

$$\mathbb{P}^1 \rightarrow C, (s : t) \mapsto (s^2 : st : t^2), \quad C \rightarrow \mathbb{P}^1, (x : y : z) \mapsto \begin{cases} (x : y), & x \neq 0 \\ (y : z), & z \neq 0 \end{cases}.$$

Видно, что эти отображения — взаимно обратные морфизмы, то есть задают изоморфизм C и \mathbb{P}^1 . Однако однородные координатные кольца у этих многообразий — это $S(\mathbb{P}^1) = \mathbb{k}[x, y]$ и $S(C) = \mathbb{k}[x, y, z]/(y^2 - xz)$, а они не изоморфны. Например, можно доказать, что первое факториально, а второе — нет.

Это наводит нас на мысль о том, что для проективных многообразий нам нужен другой структурный инвариант.

В качестве такого инварианта подойдут локальные кольца точек многообразия — их правда будет не по одному на каждое многообразие, а по одному на каждую точку многообразия. Локальные кольца будут обсуждаться чуть позже 3.

2.2 Проективное замыкание аффинного многообразия

Пусть $T \subset \mathbb{A}^n$ — замкнутое подмножество, попробуем найти $\overline{T} \subset \mathbb{P}^n$.

Первое, что приходит в голову — это просто взять гомогенизацию многочленов, которыми задаётся T . Оказывается, это не всегда даст $\overline{T} \subset \mathbb{P}^n$, что иллюстрируется следующим примером:

Пример 8. Пусть $T = Z(y - x^2, z - xy) \subset \mathbb{A}^3$. Гомогенизируя эти многочлены, получаем

$$\mathbb{P}^3 \supset Z(yw - x^2, zw - xy) \supsetneq Z(yw - x^2, zw - xy, y^2 - xz) = \{(st^2 : s^2t : s^3 : t^3) \mid (s : t) \in \mathbb{P}^1\}T.$$

Включение строгое, так как в левой части ещё лежит точка $(x : y : z : w) = (0 : 1 : 0 : 0)$, то есть

$$Z(yw - x^2, zw - xy) = \{(st^2 : s^2t : s^3 : t^3) \mid (s : t) \in \mathbb{P}^1\} \cup \{(0 : 1 : 0 : 0)\}.$$

Однако оказывается, что если гомогенизировать не только образующие идеала, а все содержащиеся в нём многочлены, то гомогенизация всё-таки получится.

Упражнение 3. Пусть $T \subset \mathbb{A}^n$. Тогда $\bar{T} = Z(\langle f^h \rangle_{f \in I(T)})$. При этом, если T неприводимо, то \bar{T} — (однозначно определённое) замкнутое неприводимое множество $R \subset \mathbb{P}^n : R \cap \mathbb{A} = T$.

Упражнение 4. Пусть X — квазипроективное многообразие, а Y — аффинное. Упражнение состоит в том, чтобы проследить, что доказательство предложения 10 работает и в этом случае, то есть по-прежнему $\text{Hom}_{\mathbf{qProj}}(X, Y) \xrightarrow{\sim} \text{Hom}_{\mathbf{k-Alg}}(A(Y), \mathcal{O}_X)$.

2.3 Прямое произведение проективных многообразий

В этом параграфе мы построим произведение квазипроективных многообразий, как квазипроективное подмногообразие в \mathbb{P}^N для некоторого N ⁸

Рассмотрим сначала $X = \mathbb{P}^n$, $Y = \mathbb{P}^m$. Построим вложение

$$\psi : \mathbb{P}^n \times \mathbb{P}^m \rightarrow \mathbb{P}^{(n+1)(m+1)-1}$$

следующим образом. Пусть $x = (u_0 : \dots : u_n) \in \mathbb{P}^n$, $y = (v_0 : \dots : v_m) \in \mathbb{P}^m$, положим

$$\psi(x \times y) = (\dots : w_{ij} : \dots), \text{ где } w_{ij} = u_i v_j.$$

Обозначим $T = \psi(\mathbb{P}^n \times \mathbb{P}^m)$. Во-первых, покажем, что T — замкнутое множество в $\mathbb{P}^{(n+1)(m+1)-1}$, для этого выпишем его уравнения:

$$w_{ij}w_{k\ell} = w_{kj}w_{i\ell}, \quad i, k = 0, \dots, n, \quad j, \ell = 0, \dots, m. \quad (2)$$

Действительно, подставим:

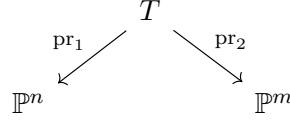
$$(u_i v_j)(u_k v_\ell) = (u_k v_j)(u_i v_\ell),$$

что выполнено. С другой же стороны, если w_{ij} удовлетворяют уравнениям (2) и, к примеру, $w_{00} \neq 0$, то, полагая $k = \ell = 0$, мы получаем, что

$$(\dots : w_{ij} : \dots) = \psi(x, y),$$

где $x = (w_{00}, \dots, w_{n0})$, $y = (w_{00}, \dots, w_{0m})$ (так мы заодно проверили, что отображение биективно). Строгая проверка того, что ψ — изоморфизм на образ, задаваемый уравнениями (2), остаётся в качестве упражнения. Это вложение называется *вложением Сегре*. Итак, T — проективное многообразие. Построим теперь проекции:

⁸Тут можно дописать всякой идеологии, я это позже сделаю возможно.



Если $\exists i: u_{ij} \neq 0$:

$$\text{pr}_1(\dots: w_{ij} : \dots) = (w_{0j} : w_{1j} : \dots : w_{nj}) = (u_0 v_j : u_1 v_j : \dots : u_n v_j) = (u_0 : \dots : u_n).$$

И, если $\exists j: u_{ij} \neq 0$:

$$\text{pr}_2(\dots: w_{ij} : \dots) = (w_{i0} : w_{i1} : \dots : w_{im}) = (u_i v_0 : u_i v_1 : \dots : u_i v_m) = (v_0 : \dots : v_m).$$

Независимость определения этих отображений от выбора индекса ненулевого элемента обеспечивается уравнениями (2).

Замечание 15. Отметим, что pr_1, pr_2 — морфизмы проективных многообразий.

Итак, у нас есть композиция

$$\mathbb{P}^m \times \mathbb{P}^n \xrightarrow{\psi} T \xrightarrow{\text{pr}_1 \times \text{pr}_2} \mathbb{P}^m \times \mathbb{P}^n.$$

Посмотрим, что произойдёт, если мы рассмотрим $T \xrightarrow{\text{pr}_1 \times \text{pr}_2} \mathbb{P}^m \times \mathbb{P}^n \xrightarrow{\psi} \mathbb{P}^{(n+1)(m+1)-1}$:

$$(\dots: w_{ij} : \dots) \mapsto (w_{0j} : w_{1j} : \dots : w_{nj} : w_{i0} : w_{i1} : \dots : w_{im}) \mapsto (w_{j0} w_{i0} : w_{j0} w_{i1} : \dots : w_{j0} w_{im} : w_{1j} w_{i0} : \dots),$$

И, нетрудно показать, что полученный объект снова удовлетворяет уравнениям для T .

Определение 22. Пусть $X \subset \mathbb{P}^n, Y \subset \mathbb{P}^m$ — квазипроjektивные многообразия, а $\psi: \mathbb{P}^n \times \mathbb{P}^m \rightarrow \mathbb{P}^{(n+1)(m+1)-1}$ — вложение Сегре.

Определим *прямое произведение* X и Y следующим образом:

$$X \times Y \stackrel{\text{def}}{=} \psi(X \times Y),$$

где в правой части равенства подразумевается теоретико-множественное декартово произведение.

Предложение 20. *Определение выше корректно, то есть $X \times Y$ является квазипроjektивным подмногообразием в $\mathbb{P}^{(n+1)(m+1)-1}$.*

Доказательство. I. Пусть сначала $X \subset \mathbb{P}^m$ и $Y \subset \mathbb{P}^n$ — проективные. Пусть X задаётся семейством уравнений $\{F_i(x_0 : \dots : x_m)\}_i$, а Y — семейством уравнений $\{G_j(y_0 : \dots : y_n)\}_j$. Пусть $x_0^{k_0} \dots x_m^{k_m}$ — какой-то моном из F_i , $k_0 + \dots + k_m = N$, тогда

$$x_0^{k_0} \dots x_m^{k_m} \cdot y_0^N = (x_0 y_0)^{k_0} \dots (x_m y_0)^{k_m} = w_{00}^{k_0} \dots w_{m0}^{k_m}.$$

Аналогично мы можем сделать с любым мономом. Значит, $F_i \cdot y_0^N$ — однородный многочлен от w_{ij} . Также мы можем рассмотреть и $G_j x_i^M$. Так мы получаем систему из уравнений

$$\begin{cases} F_i(x_0 : \dots : x_m) y_k^N = 0 \\ \vdots \\ G_j(y_0 : \dots : y_n) x_r^N = 0 \end{cases}, \quad 0 \leq k \leq n, \quad 0 \leq r \leq m.$$

При желании, N тут можно полагать одним и тем же, выбирая максимальное.

Далее проверка, что эта система задаёт $\psi(X \times Y)$, как проективное подмногообразие в $\mathbb{P}^{(n+1)(m+1)-1}$.

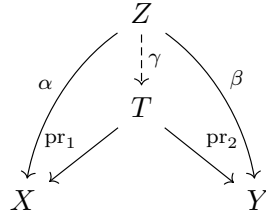
II. Теперь пусть X, Y — квазипроективные. Пусть $Y \subset Y'$, $X \subset X'$, где X', Y' — проективные. По определению $X = X' \cap U$, $Y = Y' \cap V$, где $U \subset \mathbb{P}^m$, $V \subset \mathbb{P}^n$ — открытые подмножества. Так как ψ инъективно (это мы видели в начале параграфа), то

$$\psi(X \times Y) = \psi(X' \times Y') \setminus (\psi(X' \times (Y' \setminus V)) \cup \psi((X' \setminus U) \times Y')).$$

Заметим, что каждое из множеств в правой части замкнуто, откуда видно, что $\psi(X \times Y)$ — открытое подмножество $\psi(X' \times Y')$, то есть квазипроективное подмногообразие в $\mathbb{P}^{(n+1)(m+1)-1}$. \square

Предложение 21. Построенное нами выше произведение является произведением в категорном смысле.

Доказательство. Мы хотим построить стрелку $\gamma: Z \rightarrow T$, замыкающую диаграмму и показать её единственность:



Единственность очевидна сразу, так как T также будет произведением в категории **Set** (откуда ясно, что на уровне множеств таких стрелок не более одной). Так вот, в качестве стрелки γ возьмём стрелку, замыкающую диаграмму в категории **Set** и покажем, что она годится. Проверять, что это морфизм квазипроективных многообразий, мы будем локально.

Рассмотрим $z \in Z$, не умаляя общности $\alpha(z)$ и $\beta(z)$ лежат в таких аффинных картах, что первая координата у них ненулевая. В окрестности $U \ni z$:

$$\begin{aligned} \alpha(z') &= (1 : f_1(z') : \dots : f_m(z')), \text{ где } f_i \text{ регулярны в } U; \\ \beta(z') &= (1 : g_1(z') : \dots : g_n(z')), \text{ где } g_j \text{ регулярны в } U. \end{aligned}$$

Получается,

$$\gamma(z') = (1 : g_1(z') : \dots : g_n(z') : f_1(z') : f_1(z') \cdot g_1(z') : \dots : f_i(z')g_j(z') : \dots)$$

будем морфизмом (так как произведение регулярных функций регулярно); \square

Замечание 16. В дальнейшем, мы будем писать $\mathbb{P}^n \times \mathbb{P}^m$ вместо $\psi(\mathbb{P}^n \times \mathbb{P}^m)$, и вообще $X \times Y$ вместо $\psi(X \times Y)$.

Изучим теперь, как устроены подмногообразия $X \subset \mathbb{P}^m \times \mathbb{P}^n$.

Пусть X задаётся уравнениями $F_i(w_{00} : \dots : w_{nm}) = 0$, где F_i — однородные многочлены. После подстановки $w_{ij} = u_i \cdot v_j$ мы получим систему

$$G_i(u_0 : \dots : u_n; v_0 : \dots : v_m) = 0,$$

где G_i однородны как по u_i , так и по v_j , причём степени однородности обеих систем переменных совпадают. В то же время ясно, что многочлен с таким свойством однородности всегда может быть представлен, как многочлен от произведений $u_i v_j$. Однако, если уравнения однородны как по u_i , так и по v_j , то они всегда определяют в $\mathbb{P}^n \times \mathbb{P}^m$ алгебраическое подмногообразие, даже если степени однородности были разными. Действительно, если $G(u_0 : \dots : u_n; v_0 : \dots : v_m)$ имеет степень однородности r по u_i и s по v_j (и, например, $r > s$), то

$$G = 0 \iff \begin{cases} v_0^{r-s} G = 0 \\ \vdots \\ v_m^{r-s} G = 0 \end{cases}.$$

Давайте также разберёмся с этим вопросом для $\mathbb{P}^n \times \mathbb{A}^m$. Пусть $\mathbb{A}^m \hookrightarrow U_0 \subset \mathbb{P}^m$, тут оно задаётся $v_0 \neq 0$. Уравнения замкнутого подмножества в $\mathbb{P}^n \times \mathbb{A}^m$ имеют вид

$$G_i(u_0 : \dots : u_n; v_0 : \dots : v_m) = 0.$$

Пусть степень однородности G_i по v_0, \dots, v_m равна r_i . Поделив уравнение на $v_0^{r_i}$ и положив $y_i = v_i/v_0$ мы получим набор уравнений

$$g_i(u_0 : \dots : u_n; y_1 : \dots : y_m) = 0,$$

где g_i однородны по u_0, \dots, u_n и, вообще говоря, неоднородны по y_1, \dots, y_m . Таким образом, мы доказали такую теорему:

Теорема 9. *Подмножество $X \subset \mathbb{P}^n \times \mathbb{P}^m$ тогда и только тогда замкнуто, когда оно задаётся системой уравнений*

$$G_i(u_0 : \dots : u_n; v_0 : \dots : v_m) = 0$$

однородных по каждой системе переменных u_i и v_j в отдельности.

Каждое замкнутое подмножество в $\mathbb{P}^n \times \mathbb{A}^m$ задаётся системой уравнений

$$g_i(u_0 : \dots : u_n; y_1 : \dots : y_m) = 0,$$

однородных по переменным u_0, \dots, u_n .

Аналогично дело обстоит с $\mathbb{P}^{n_1} \times \dots \times \mathbb{P}^{n_k}$.

2.4 Замкнутость образа проективного многообразия

В этом параграфе мы докажем следующее замечательное утверждение:

Теорема 10. *Пусть $X \in \text{Proj}$, $Y \in \text{qProj}$, а $f : X \rightarrow Y$ — регулярное отображение. Тогда $f(X)$ замкнут в Y .*

Прежде чем приступать к доказательству, убедимся в необычайной полезности этого утверждения. Например, из него мы сразу получаем вот такое следствие:

Следствие 7. Пусть X — неприводимое проективное многообразие. Тогда $\mathcal{O}(X) \cong \mathbb{k}$.

Доказательство. Пусть $f: X \rightarrow \mathbb{A}^1$ — регулярная функция. Так как $f(X)$ замкнут (по теореме 10) и неприводим, либо $f(X) = \mathbb{A}^1$, либо $f(X) = \text{pt}$ (в этом случае мы всё доказали). Предположим, что $f(X) = \mathbb{A}^1$. Рассмотрим сквозное отображение

$$X \xrightarrow{f} \mathbb{A}^1 \hookrightarrow \mathbb{P}^1$$

и назовём его g . Получается, что если $f(X) = \mathbb{A}^1$, то $g(X) = \mathbb{P}^1 \setminus \text{pt}$, но оно не замкнуто в \mathbb{P}^1 (что приводит нас к противоречию с теоремой 10). \square

Замечание 17. Можно думать, что эта теорема является алгебраизацией утверждения о том, что голоморфная на всей римановой поверхности функция без полюсов постоянна.

Замечание 18. Также видно, что в 7 можно требовать от X только связности (разбив на неприводимые компоненты).

Доказательство теоремы 10. Отображение f мы можем разложить в композицию двух:

$$X \xrightarrow{\Gamma_f} X \times Y \xrightarrow{\text{pr}_2} Y, \quad x \mapsto (x, f(x)) \mapsto f(x).$$

Достаточно доказать, что

1. $\Gamma_f(X)$ замкнут в $X \times Y$,
2. pr_2 переводит замкнутые множества в замкнутые.

Докажем сначала **первое**. Выделим это в отдельную лемму:

Лемма 4 (О замкнутом графике). Для всякого морфизма $f: X \rightarrow Y$ его график $\Gamma_f(X)$ замкнут в $X \times Y$.

Доказательство леммы. Рассмотрим диагональный морфизм $\Delta: Y \rightarrow Y \times Y$. Достаточно проверить, что $\Delta(Y)$ замкнут в $Y \times Y$, так как если мы это докажем, то можно рассмотреть

$$X \times Y \xrightarrow{(f, \text{id})} Y \times Y$$

и так как $\Gamma_f(X) = (f, \text{id})^{-1}(\Delta(Y))$, то из замкнутости $\Delta(Y)$ будет следовать замкнутость графика (просто по непрерывности).

Предположим сначала, что Y аффинное. В этом случае всё просто: $\Delta(Y) = \Delta(\mathbb{A}^n) \cap (Y \times Y)$ и оба пересекемых множества очевидно замкнуты.

Если же Y произвольное, покроем его аффинными: $Y \subset \bigcup U_i$, тогда $\Delta(Y \times Y) \subset \bigcup U_i \times U_i$ и чтобы показать, что $\Delta(Y)$ замкнуто, нам достаточно убедиться, что $\Delta(Y) \cap (U_i \times U_i)$ замкнуто для всех i . Но это очевидно, так как

$$\Delta(Y) \cap (U_i \times U_i) = \Delta(U_i),$$

а $\Delta(U_i)$ замкнуто по первому шагу доказательства. \square

Теперь покажем **второе**.

Прежде всего, можно считать, что $X = \mathbb{P}^n$, так как для произвольного X можно рассматривать композицию

$$X \times Y \hookrightarrow \mathbb{P}^n \times Y \rightarrow Y,$$

применить теорему для неё и из этого всё будет следовать.

Покрывая Y аффинными, мы понимаем, что достаточно доказать теорему для случая

$$\mathbb{P}^n \times \mathbb{A}^m \rightarrow \mathbb{A}^m.$$

А в этом случае работать существенно проще, так как (из теоремы 9) мы знаем полное описание замкнутых множеств. Все они имеют вид

$$T = \{(u, y) \mid g_i(u, y) = 0, 1 \leq i \leq t\} \rightsquigarrow \text{pr}(T) = \{y \in \mathbb{A}^m \mid \exists u \in \mathbb{P}^n g_i(u, y) = 0, 1 \leq i \leq t\},$$

где g_i — однородный многочлен по u .

Пусть $y \in \mathbb{A}^m$. Равенство $g_i(u, y) = 0$ для всех $1 \leq i \leq t$ выполнено на некотором замкнутом множестве в \mathbb{P}^n , и $y \in \text{pr}_2(T)$ если и только если оно непусто. Согласно однородной теореме Гильберта о нулях (пусть $I^s = (u_0, \dots, u_n)^s \subseteq \mathbb{K}[u_0, \dots, u_n]$),

$$y \in \text{pr}_2(T) \iff \forall s : (g_1(u, y), \dots, g_t(u, y)) \not\in I^s,$$

Тем самым, проекцию можно задать в виде

$$\text{pr}(T) = \bigcap_s \{y \in \mathbb{A}^m \mid I^s \not\subset (g_1(u, y), \dots, g_t(u, y))\}. \quad (3)$$

Получается, достаточно доказать, что каждое пересеканное множество замкнуто. По этому поводу зафиксируем s . Пусть $k_i = \deg_u(g_i)$, $\{M^{(\alpha)}\}_{(\alpha \in \mathbb{N}^{n+1}, \sum \alpha_j = s)}$ — все мономы степени s ⁹. Посмотрим, что означает условие, противоположное к условию (3):

$$I^s \subset (g_1(u, y), \dots, g_t(u, y)) \iff \forall \alpha : M^{(\alpha)} = \sum g_i(u, y) F_{i,\alpha}(u) \quad (*)$$

а F_i однородные по переменным u_i . Можно считать, что для всех i, α : $\deg F_{i,\alpha} = s - k_i$, или же $F_{i,\alpha} = 0$ (в частности, если $s < k_i$, то $F_{i,\alpha} = 0$)¹⁰. Теперь рассмотрим $\{N_i^{(\beta)}\}_\beta$ — все мономы (от переменных u_i) степени $s - k_i$. Условие (*) означает, что все $M^{(\alpha)}$ — всевозможные линейные комбинации $g_i(u, y) N_i^{(\beta)}$. Иными словами (пусть S — пространство однородных многочленов от u степени s),

$$S = \text{span}\{g_i(u, y) N_i^{(\beta)}\},$$

Теперь ясно, что

$$I^s \not\subset (g_1(u, y), \dots, g_t(u, y)) \iff S \neq \text{span}\{g_i(u, y) N_i^{(\beta)}\} \iff \text{rank } A < \dim_{\mathbb{K}} S,$$

где A — матрица, состоящая из коэффициентов $g_i(u, y) N_i^{(\beta)}$. Ясно, что при фиксированном y это полиномиальное условие (обнуление всех определителей подматриц размера $\dim_{\mathbb{K}} S \times \dim_{\mathbb{K}} S$), так что мы показали замкнутость. \square

Следствие 8. Пусть $X \in \text{Proj}$, $Y \in \text{qProj}$, а $f: X \rightarrow Y$ — морфизм. Пусть $Z \subset X$ — замкнутое подмножество. Тогда $f(Z)$ замкнуто в Y .

⁹Например, при $n = 2$ есть такой моном: $M^{(2,3,1)} = u_0^2 u_1^3 u_2$

¹⁰Если равенство имеет место, и от всех $F_{i,\alpha}$ оставить только однородные компоненты данной степени, то равенство сохранится.

2.5 Рациональные отображения многообразий

Лемма 5. Пусть X, Y — многообразия, причём X неприводимо, а φ, ψ — морфизмы из X в Y . Предположим, что существует такое непустое открытое множество $U \subset X$, что $\varphi|_U = \psi|_U$. Тогда $\varphi = \psi$.

Доказательство. Пусть $Y \subset \mathbb{P}^n$ для некоторого n . Беря композиции морфизмов φ и ψ с вложением $Y \rightarrow \mathbb{P}^n$, мы сводим всё к случаю $Y = \mathbb{P}^n$. Рассмотрим $\mathbb{P}^n \times \mathbb{P}^n$ со структурой проективного многообразия, определяемой вложением Сегре (см. 2.3). Морфизмы φ и ψ определяют морфизм

$$X \xrightarrow{\varphi \times \psi} \mathbb{P}^n \times \mathbb{P}^n.$$

Рассмотрим диагональ $\Delta \subset \mathbb{P}^n \times \mathbb{P}^n$. Она (как и в аффинном случае) замкнуто, так как представляется уравнениями

$$x_i y_j = x_j y_i, \quad i, j = 0, \dots, n.$$

По предположению $(\varphi \times \psi)(U) \subset \Delta$, но U плотно в X (так как X неприводимо), а Δ замкнуто, откуда мы имеем $(\varphi \times \psi)(X) \subset \Delta$, то есть $\varphi = \psi$. \square

Определение 23. Пусть X, Y — многообразия, X неприводимо. Рассмотрим множество пар (U, f) , где $U \subset X$ — открытое, а $f: U \rightarrow Y$ — морфизм. На этом множестве мы можем ввести такое отношение эквивалентности:

$$(U_1, f_1) \sim (U_2, f_2) \Leftrightarrow f_1|_{U_1 \cap U_2} = f_2|_{U_1 \cap U_2}.$$

Класс эквивалентности по этому отношению называется *рациональным отображением* и обозначается $f: X \dashrightarrow Y$.

Из всех пар (U, f) мы можем выбрать такую, для которой открытое множество U максимально. Это множество U мы будем называть *областью регулярности* рационального отображения.

Замечание 19. То, что описанное выше отношение — отношение эквивалентности, следует из леммы 5. В частности, любые два $U_1, U_2 \subset X$ имеют непустое пересечение, так как X неприводимо.

Замечание 20. Область регулярности определена корректно: пара (U, f) с максимальным U единственна (она же будет парой с наибольшей U). Это верно, так как два эквивалентных рациональных отображения (U_1, f_1) и (U_2, f_2) можно «объединить» — они же совпадают на пересечении. Строгая проверка остаётся в качестве упражнения.

Определение 24. Рациональное отображение $f: X \dashrightarrow Y$ называется *доминантным*, если для некоторой пары (U, f) : $f(U)$ плотно в Y .

Замечание 21. Если образ плотен для какой-то пары, то это так и для всех (тоже по лемме 5).

Композицию рациональных отображений определить не всегда возможно (по понятным причинам), а вот с доминантными рациональными отображениями дело обстоит лучше.

Пусть у нас есть доминантные рациональные отображения $X \dashrightarrow Y \dashrightarrow Z$ и они представляются морфизмами $f: U \rightarrow Y$ и $g: V \rightarrow Z$. Так как f доминантно, $f(U) \cap V \neq \emptyset$, откуда $W = f^{-1}(V) \cap U \neq \emptyset$. Определим $g \circ f: X \dashrightarrow Z$ как класс эквивалентности пары $(W, g \circ f|_W)$.

Отметим также, что композиция доминантных отображений является доминантной. Действительно, предположим противное, а именно, что образ W под действием композиции попадает в некоторое замкнутое $T \subsetneq Z$. Но $f(W) \subsetneq g^{-1}(T) \subsetneq Y$, а это противоречит доминантности.

Значит, квазипроективные многообразия с доминантными рациональными морфизмами образуют категорию.

Кроме того, доминантное рациональное отображение $\varphi: X \dashrightarrow Y$ индуцирует гомоморфизм полей рациональных функций

$$\varphi^*: \mathbb{k}(Y) \rightarrow \mathbb{k}(X)$$

Действительно, пусть φ представлено парой (U, φ_U) и пусть $f \in \mathbb{k}(Y)$ — рациональная функция, представленная парой (V, f) , где f регулярна на V . Поскольку $\varphi_U(U)$ плотно в Y , оно пересекается с V и $\varphi_U^{-1}(V)$ — непустое открытое подмножество X , так что $f \circ \varphi_U$ — регулярная функция на $\varphi_U^{-1}(V)$ (а регулярна она, так как φ_U — морфизм). Она представляет некоторую рациональную функцию на X .

$$\varphi_U^{-1}(V) \xrightarrow{\varphi_U} V \xrightarrow{f} \mathbb{k}.$$

Таким образом, мы построили отображение

$$\mathbb{k}(Y) \rightarrow \mathbb{k}(X), \quad f \mapsto \varphi^*(f).$$

Пусть \mathcal{C} — категория неприводимых многообразий с доминантными рациональными отображениями, а \mathcal{D} — категория конечно порождённых расширений поля \mathbb{k} .

Теорема 11. *Для любых неприводимых многообразий X, Y приведённая выше конструкция осуществляет биективное соответствие между*

- *множеством доминантных рациональных отображений $X \rightarrow Y$*
- *множеством гомоморфизмов \mathbb{k} -алгебр $\mathbb{k}(Y) \rightarrow \mathbb{k}(X)$.*

Более этого, это соответствие осуществляет антиэквивалентность категорий \mathcal{C} и \mathcal{D} :

$$\mathcal{F}: \mathcal{C} \rightarrow \mathcal{D}, \quad X \mapsto \mathbb{k}(X).$$

Доказательство. Построим отображение обратное тому, что было приведено ранее.

Пусть $\theta: \mathbb{k}(Y) \rightarrow \mathbb{k}(X)$ — гомоморфизм \mathbb{k} -алгебр. Надо построить соответствующее ему доминантное рациональное отображение $X \dashrightarrow Y$.

Выберем внутри Y аффинное открытое подмножество, без потери общности Y можно заменить на него (не поменяются ни поле функций на Y , ни множество доминантных рациональных отображений $X \dashrightarrow Y$). Итак, Y — аффинное, пусть $A(Y)$ — его аффинное координатное кольцо, а y_1, \dots, y_n — его образующие, как \mathbb{k} -алгебры. Тогда $\theta(y_1), \dots, \theta(y_n)$ являются рациональными функциями на X . Выберем открытое множество $U \subset X$ так, чтобы все функции $\theta(y_i)$ были регулярными на U . В таком случае θ определяет инъективный гомоморфизм \mathbb{k} -алгебр

$$A(Y) \rightarrow \mathcal{O}(U).$$

По теореме 10 ему соответствует морфизм $\varphi: U \rightarrow Y$, который определяет доминантное¹¹ рациональное отображение $X \dashrightarrow Y$.

¹¹ Оно будет доминантным, так как иначе отображение $A(Y) \rightarrow \mathcal{O}(U)$ не инъективно.

Теперь убедимся, что мы действительно построили антиэквивалентность категорий. Надо проверить, что для любого неприводимого многообразия Y поле рациональных функций $\mathbb{k}(Y)$ конечно порождено над \mathbb{k} и обратно, что всякое конечно порождённое расширение K/\mathbb{k} является полем рациональных функций $K = \mathbb{k}(Y)$ некоторого неприводимого многообразия Y .

Пусть Y — неприводимое многообразие, тогда $\mathbb{k}(Y) = \mathbb{k}(U)$ для любого открытого подмногожества $U \subset Y$, так что опять же можно полагать Y аффинным. В этом случае $\mathbb{k}(Y) \cong \text{Frac } A(Y)$ и, как следствие, оно является конечно порождённым расширением поля \mathbb{k} степени трансцендентности $\dim Y$.

С другой стороны, пусть K — конечно порождённое расширение поля \mathbb{k} , а $y_1, \dots, y_n \in K$ — система образующих. Пусть B — подалгебра в K , порождённая y_1, \dots, y_n над \mathbb{k} . B является фактором кольца многочленов $\mathbb{k}[x_1, \dots, x_n]$ по некоторому идеалу I , так что $B \cong A(Y)$ для $Y = Z(I) \subset \mathbb{A}^n$. Y будет неприводимым, так как $A(Y)$ целостное. Значит, $K \cong \mathbb{k}(Y)$ и теорема доказана. \square

Переводя это на существенно менее изысканный язык, мы получаем такое следствие:

Следствие 9. *Неприводимые многообразия X и Y бирационально эквивалентны тогда и только тогда, когда их поля рациональных функций $\mathbb{k}(X)$ и $\mathbb{k}(Y)$ изоморфны как \mathbb{k} -алгебры.*

2.6 Бирациональная эквивалентность

Определение 25. *Бирациональным отображением $\varphi: X \rightarrow Y$ называется (доминантное) рациональное отображение, которое обладает обратным, т.е. таким (доминантным) рациональным отображением $\psi: Y \rightarrow X$, что $\psi \circ \varphi = \text{id}_X$, $\varphi \circ \psi = \text{id}_Y$. Многообразия X и Y называются бирационально эквивалентными, если существует хотя бы одно бирациональное отображение $X \rightarrow Y$.*

Следствие 10. *Для любых двух неприводимых многообразий X и Y следующие условия эквивалентны:*

1. X и Y бирационально эквивалентны,
2. существуют открытые подмножества $U \subset X$ и $V \subset Y$ такие, что U изоморфно V ,
3. $\mathbb{k}(X) \cong \mathbb{k}(Y)$ в категории \mathbb{k} -алгебр.

Доказательство. Сначала докажем (1) \implies (2). Пусть $\varphi: X \rightarrow Y$ и $\psi: Y \rightarrow X$ — бирациональные отображения. Пусть φ представлено парой (U, φ) , а ψ — парой (V, ψ) . Тогда отображение $\psi \circ \varphi$ представляется парой $(\varphi^{-1}(V), \psi \circ \varphi)$, а так как $\psi \circ \varphi = \text{id}_X$ как рациональное отображение, $\psi \circ \varphi$ тождественно на $\varphi^{-1}(V)$. Аналогично, $\varphi \circ \psi$ тождественно на $\psi^{-1}(U)$. Получается, $\varphi^{-1}(\psi^{-1}(U)) \subset X$ и $\psi^{-1}(\varphi^{-1}(U)) \subset Y$ — изоморфные открытые подмножества (изоморфизм осуществляется посредством отображений φ и ψ).

Утверждение (2) \implies (3) следует из определения полей функций:

$$\mathbb{k}(U) \cong \mathbb{k}(X), \quad \mathbb{k}(V) \cong \mathbb{k}(Y), \quad \mathbb{k}(U) \cong \mathbb{k}(V) \implies \mathbb{k}(X) \cong \mathbb{k}(Y).$$

Утверждение (3) \implies (1) напрямую следует из теоремы 11. \square

Теперь докажем какой-нибудь результат про бирациональную эквивалентность. Напомним несколько фактов из алгебры:

Теорема 12 (О примитивном элементе). Пусть L — конечное сепарабельное расширение поля K . Тогда существует элемент $\alpha \in L$, порождающий поле L , как расширение над K . Более того, если β_1, \dots, β_n — произвольная система образующих L/K и поле K бесконечно, то α можно выбрать α в виде линейной комбинации $\alpha = c_1\beta_1 + \dots + c_n\beta_n$ элементов β_i с коэффициентами $c_i \in K$.

Определение 26. Расширение K/\mathbb{k} называется *сепарабельно порожждённым*, если существует такой базис трансцендентности $\{x_i\}$ в K/\mathbb{k} , что поле K является сепарабельным алгебраическим расширением поля $\mathbb{k}(\{x_i\})$. В таком случае $\{x_i\}$ называется *сепарабельным базисом трансцендентности*.

Теорема 13. Пусть K/\mathbb{k} — конечно порождённое и сепарабельно порождённое расширение поля \mathbb{k} . Тогда всякое множество образующих расширения K/\mathbb{k} содержит подмножество, являющееся сепарабельным базисом трансцендентности.

Теорема 14. Пусть \mathbb{k} — алгебраически замкнутое поле. Тогда любое конечно порождённое расширение K/\mathbb{k} является сепарабельно порождённым.

Предложение 22. Всякое неприводимое многообразие X размерности r бирационально эквивалентно гиперповерхности $Y \subset \mathbb{P}^{r+1}$.

Доказательство. Начнём с того, что поле функций $\mathbb{k}(X)$ является конечно порождённым расширением поля \mathbb{k} . По теореме 14 оно сепарабельно порождено над \mathbb{k} . Значит, существует базис трансцендентности $x_1, \dots, x_r \in \mathbb{k}(X)$ такой, что $\mathbb{k}(X)$ — конечное сепарабельное расширение $\mathbb{k}(x_1, \dots, x_r)$. Теперь по теореме о примитивном элементе 12 существует $y \in \mathbb{k}(X)$ такой, что $K = \mathbb{k}(y, x_1, \dots, x_r)$. Элемент y алгебраичен над \mathbb{k} , то есть удовлетворяет некоторому полиномиальному уравнению с коэффициентами из поля рациональных функций от переменных $\mathbb{k}(x_1, \dots, x_r)$. Домножая на знаменатели, мы получим

$$f(y, x_1, \dots, x_r) = 0,$$

где f — некоторый неприводимый многочлен. Теперь легко видеть, что он определяет гиперповерхность в \mathbb{A}^{r+1} с полем функций $\mathbb{k}(X)$, а отсюда, по теореме 11, она бирационально эквивалентна X . Проективное замыкание этой гиперповерхности и есть требуемая гиперповерхность $Y \subset \mathbb{P}^{r+1}$. \square

2.7 Рациональные многообразия

Определение 27. *Рациональным многообразием* мы будем называть многообразие, бирационально изоморфное проективному пространству. Эквивалентно (по теореме 11), можно говорить, что это многообразие, поле функций которого изоморфно $\mathbb{k}(t_1, \dots, t_n)$.

Пример 9. Например, окружность $x^2 + y^2 = 1$ является рациональным многообразием. Действительно, так как поле алгебраически замкнуто,

$$x^2 + y^2 = (x + iy)(x - iy) = st$$

и окружность задаётся как $st = 1$. Её аффинная алгебра — это $\mathbb{k}[s, t]/(st - 1) = \mathbb{k}(s, s^{-1})$. Видно, что $\mathbb{k}(X) \cong \mathbb{k}(t)$.

А знаем ли мы многообразия, которые не являются рациональными? Рассмотрим *эллиптическую кривую*

$$y^2 = x^3 + ax + b,$$

с условием, что $x^3 + ax + b$ не имеет кратных корней и $\text{char } \mathbb{k} \neq 2, 3$. Условие про кратные корни гарантировано, например, тем, что $4a^3 + 27b^2 \neq 0$.

Линейной заменой переменной x , уравнение сводится к виду

$$y^2 = x(x - 1)(x - \alpha), \quad \alpha \neq 0.$$

Покажем, что эта кривая не является рациональной. Посмотрим на проективное замыкание этой кривой, для этого нужно взять гомогенизацию этого многочлена:

$$y^2 z = x^3 + axz^2 + bz^3.$$

Несложно видеть, что проективное замыкание отличается от самой кривой лишь одной бесконечно удалённой точкой: в карте $z \neq 0$ лежат все аффинные точки, а $z = 0$ даёт одну бесконечно удалённую точку $(0 : 1 : 0)$.

Так как аффинная кривая содержится в проективной, как открытое подмножество, то поля функций у них совпадают. Отсюда в частности следует, что если мы докажем, что аффинная кривая не рациональна, то мы получим, что её проективизация не изоморфна \mathbb{P}^1 .

То, что аффинная кривая не рациональна, будем доказывать от противного. Предположим, что $\mathbb{k}(X) \cong \mathbb{k}(t)$, и

$$y \leftrightarrow \frac{p_1(t)}{p_2(t)}, \quad x \leftrightarrow \frac{q_1(t)}{q_2(t)}.$$

Не умаляя общности, $(p_1, p_2) = (q_1, q_2) = 1$. Должно быть выполнено соотношение

$$\frac{p_1^2}{p_2^2} = \frac{q_1}{q_2} \left(\frac{q_1}{q_2} - 1 \right) \left(\frac{q_1}{q_2} - \alpha \right) \rightsquigarrow p_1^2 \cdot q_2^3 = p_2^2 q_1 (q_1 - q_2) (q_1 - \alpha q_2).$$

Отсюда $p_2^2 : q_2^3$ и $q_2^3 : p_2^2$, то есть они пропорциональны, а именно $q_2^3/p_2^2 = c \in \mathbb{k}$. Получаем

$$cp_1^2 = q_1(q_1 - q_2)(q_1 - \alpha q_2)$$

и подправляя p_1 и p_2 правильным образом на константный множитель, можно считать $c = 1$. В силу взаимной простоты множителей, мы получаем, что q_1 , $q_1 - q_2$, $q_1 - \alpha q_2$ — квадраты. При этом q_2 — тоже квадрат, так как $q_2^3 = p_2^2$.

Получается, в некотором двумерном \mathbb{k} -подпространстве $\mathbb{k}[t]$ нашлось четыре различных (не совпадающих даже с точностью до ассоциированности) квадрата. Несложно придумать три квадрата, лежащих в двумерном пространстве — скажем, подойдут $(x^2 - y^2)^2$, $(x^2 + y^2)^2$, $x^2 y^2$, но, предложение ниже говорит, что, оказывается, четырёх таких квадратов найти не получится.

Предложение 23. Пусть Q_1, Q_2 — два взаимно простых многочлена. В пространстве $\text{span}_{\mathbb{k}}(Q_1, Q_2)$ нет четырёх ненулевых квадратов (разумеется, различных с точностью до ассоциированности).

Доказательство. Пусть $R_1, R_2 \in \text{span}_{\mathbb{K}}(Q_1, Q_2)$ непропорциональные квадраты. Так как они непропорциональны, $\text{span}_{\mathbb{K}}(R_1, R_2) = \text{span}_{\mathbb{K}}(Q_1, Q_2)$. Оставшиеся два квадрата можно записать в виде $\alpha_1 R_1 - \alpha_2 R_2$ и $\beta_1 R_1 - \beta_2 R_2$. Пусть $R_1 = S_1^2$, $R_2 = S_2^2$ и

$$\begin{aligned}\alpha_1 R_1 - \alpha_2 R_2 &= (\sqrt{\alpha_1} S_1 + \sqrt{\alpha_2} S_2)(\sqrt{\alpha_1} S_1 - \sqrt{\alpha_2} S_2) \\ \beta_1 R_1 - \beta_2 R_2 &= (\sqrt{\beta_1} S_1 + \sqrt{\beta_2} S_2)(\sqrt{\beta_1} S_1 - \sqrt{\beta_2} S_2)\end{aligned}$$

Так как $(S_1, S_2) = 1$, значит взаимно просты и правые части равенств, а отсюда $\sqrt{\alpha_1} S_1 + \sqrt{\alpha_2} S_2$, $\sqrt{\alpha_1} S_1 - \sqrt{\alpha_2} S_2$, $\sqrt{\beta_1} S_1 + \sqrt{\beta_2} S_2$, $\sqrt{\beta_1} S_1 - \sqrt{\beta_2} S_2$ — квадраты.

Выберем изначально Q_1, Q_2 с наименьшим максимумом степеней; выкладка выше показывает возможность бесконечного спуска, то есть противоречие. \square

Следствие 11. *Эллиптическая кривая (кривая вида $\{y^2 = x^3 + ax + b\}$ при $4a^3 + 27b^2 \neq 0$, $\text{char } \mathbb{K} \neq 2, 3$) не рациональна.*

Замечание 22. Альтернативное доказательство этого факта использует то, что бирациональные морфизмы между неособыми проективными кривыми продолжаются до регулярных, а отсутствие изоморфизма на уровне Proj доказывать проще. Об этом написано в 3.6.

3 Локальные кольца

3.1 Локальное кольцо в точке

Определение 28. Пусть X — квазипроективное многообразие, $P \in X$, а $\mathcal{O}(X)$ — его кольцо регулярных функций. Для точки P определим её *локальное кольцо* \mathcal{O}_P , как

$$\mathcal{O}_P = \varinjlim_{U \ni P} \mathcal{O}(U).$$

Говоря более изысканно, это кольцо ростков регулярных функций на X в окрестности P . Или, иными словами, элемент \mathcal{O}_P — это пара (U, f) , где U — открытая окрестность P в X , а f — регулярная функция на U , причём пары (U, f) и (V, g) отождествляются, если $f = g$ на $U \cap V$.

Отметим, что кольцо \mathcal{O}_P на самом деле является локальным кольцом: его единственный максимальный идеал \mathfrak{m}_P состоит из всех ростков регулярных функций, обращающихся в нуль в точке P . В самом деле, если $f(P) \neq 0$, то $1/f$ регулярна в некоторой окрестности P и f обратима в \mathcal{O}_P . Раз всё вне \mathfrak{m}_P обратимо, то \mathfrak{m}_P — единственный максимальный идеал. Также несложно видеть, что поле вычетов $\mathcal{O}_P/\mathfrak{m}_P \cong \mathbb{K}$.

Пусть A — локальное кольцо, \mathfrak{m} — его максимальный идеал. Тогда $\mathfrak{m}/\mathfrak{m}^2$ — векторное пространство над A/\mathfrak{m} .

Доказательство следующей леммы предоставляется читателю как упражнение, она будет использоваться в дальнейшем.

Лемма 6. Пусть A — коммутативное кольцо, I_1, \dots, I_n — набор идеалов ($n \geq 2$), причем среди них есть не более двух **не** простых. И пусть

$$J \leq A, \quad J \subset I_1 \cup \dots \cup I_n.$$

Тогда $J \subset I_k$ для некоторого k .

Упражнение 5. Локальное кольцо точки $P = (0, 0)$ для кривой $X = Z(y^2 - x^3)$ не является дискретно нормированным.

Пример 10. Нетрудно заметить, что в случае упражнения выше у нас всё устроено так:

$$\dim X = 1, \quad \mathfrak{m} = (x, y), \quad \dim_{\mathbb{K}} \mathfrak{m}_P / \mathfrak{m}_P^2 = 2.$$

Возводя в степень максимальный идеал это кольца можно заметить интересную вещь:

$$\mathfrak{m}^3 = (x^3, x^2y, xy^2, y^3) = (y^2, x^2y) \subset (y) \implies \mathfrak{m}^3 \subset (y) \subset \mathfrak{m}$$

Это явление имеет такое коммутативно алгебраическое происхождение:

Теорема 15. Пусть A — нётерово локальное кольцо. Тогда $\dim A < \infty$ и она равна такому минимальному d , для которого $\exists k \in \mathbb{N}$, $x_1, x_2, \dots, x_d \in \mathfrak{m}$ такие, что

$$\mathfrak{m}^k \subset (x_1, \dots, x_d) \subset \mathfrak{m}.$$

Доказательство. Мы будем доказывать эту теорему для колец геометрического происхождения, то есть колец вида \mathcal{O}_P . Зафиксируем d и предположим, что для некоторого $k \in \mathbb{N}$ мы имеем

$$\mathfrak{m}_P^k \subset (x_1, \dots, x_d) \subset \mathfrak{m}.$$

Шаг 1. Покажем сначала, что в таком случае $\dim \mathcal{O}_P \leq d$.

Для начала обоснуем, почему можно считать, что X неприводимо, и, следовательно, \mathcal{O}_P целостно. Как копредел, локальное кольцо зависит только от окрестности точки P , так что без потери общности можно считать, что X аффинно. В аффинном случае \mathcal{O}_P — локализация $A(X)$ в максимальном идеале \mathfrak{m}_P . Любая максимальная цепочка идеалов в \mathcal{O}_P длины $\dim \mathcal{O}_P$ начинается в каком-то минимальном простом идеале \mathcal{O}_P , он же — минимальный простой идеал $A(X)$, содержащийся в \mathfrak{m}_P . Такие идеалы отвечают неприводимым компонентам X , содержащим точку P , откуда видно, что при замене X на ту неприводимую компоненту, содержащую точку P , которая имеет максимальную размерность, $\dim \mathcal{O}_P$ не поменяется.

Итак, можно считать, что $X = \operatorname{Spec} A$ аффинно и неприводимо, следовательно, локальное кольцо $\mathcal{O}_P = A_{\mathfrak{m}_P}$ целостно.

Далее представим максимальную локализацию, как копредел главных: $\mathcal{O}_P = \varinjlim_{a(P) \neq 0} A_a$, и в соответствии с этим докажем вот такую лемму:

Лемма 7. Пусть I, J — идеалы в целостном нётеровом кольце A , $\mathfrak{m} \in \operatorname{Spec} A$ и $I_{\mathfrak{m}} \subset J_{\mathfrak{m}}$. Тогда существует $a \in A \setminus \mathfrak{m}$ такой, что $I_a \subset J_a$.

Доказательство леммы. Рассмотрим короткую точную последовательность

$$0 \rightarrow J \rightarrow I + J \rightarrow (I + J)/J \rightarrow 0.$$

Так как локализация — это точный функтор, точной будет и последовательность

$$0 \rightarrow J_{\mathfrak{m}} \xrightarrow{\sim} (I + J)_{\mathfrak{m}} \rightarrow ((I + J)/J)_{\mathfrak{m}} \rightarrow 0.$$

Тогда, так как $I_{\mathfrak{m}} \subset J_{\mathfrak{m}}$, вторая слева стрелка — изоморфизм, откуда $((I + J)/J)_{\mathfrak{m}} = 0$. Рассмотрим конечно порождённый A -модуль $M = (I + J)/J$. Так как $M_{\mathfrak{m}} = 0$, существует $a \in A \setminus \mathfrak{m}$ такой, что $M_a = 0$, то есть $((I + J)/J)_a = 0$. Но последовательность

$$0 \rightarrow J_a \xrightarrow{\sim} (I + J)_a \rightarrow ((I + J)/J)_a \rightarrow 0 \iff 0 \rightarrow J_a \xrightarrow{\sim} (I + J)_a \rightarrow 0$$

также точна, откуда $I_a \subset J_a$. □

Применяя эту лемму к $\mathcal{O}_P = A_{\mathfrak{m}_P}$ мы получаем, что $\exists b \in A \setminus \mathfrak{m}_P$: в кольце $B = A_b$ имеется включение идеалов

$$\mathfrak{m}_P^k \subset (x_1, \dots, x_d) \subset \mathfrak{m}_P.$$

Беря радикалы, получаем

$$\mathfrak{m}_P \subset \sqrt{(x_1, \dots, x_d)} \subset \mathfrak{m}_P,$$

откуда по теореме Гильберта о нулях $\{P\} = Z(x_1, \dots, x_d) \cap \text{Specm } B$. Предполагая $\dim \mathcal{O}_P > d$, мы приходим к противоречию, так как $Z(x_1, \dots, x_d)$ — это пересечение d гиперповерхностей, а оно либо пустое, либо размерности $\dim \mathcal{O}_P - d > 0$.

Шаг 2. Покажем, что для $d = \dim \mathcal{O}_P$ существует натуральное k такое, что

$$\mathfrak{m}_P^k \subset (x_1, \dots, x_d).$$

Будем доказывать это индукцией по d .

База. Случай $d = 0$ очевиден, так как кольцо \mathcal{O}_P локальное, откуда $\text{Rad}(\mathcal{O}_P) = \mathfrak{m}_P$, но в артиновом кольце радикал Джекобсона нильпотентен, то есть для некоторого N : $\mathfrak{m}_P^N = 0$ и условие будет выполнено.

Переход. Рассмотрим элемент x_1 , не лежащий в объединении минимальных простых идеалов. Как мы видели при доказательстве теоремы 7,

$$\dim \mathcal{O}_P/(x_1) \leq \dim \mathcal{O}_P - 1,$$

так как если у нас есть максимальная цепочка вложенных простых $\overline{\mathfrak{p}}_0 \subset \dots \subset \overline{\mathfrak{p}}_n \leq \mathcal{O}_P/(x_1)$, то цепочка $\mathfrak{p}_0 \subset \dots \subset \mathfrak{p}_n \leq \mathcal{O}_P$ уже не будет максимальной, так как идеал \mathfrak{p}_0 не минимальный. По индукционному предположению существует k такое, что

$$\mathfrak{m}_P^k/(x_1) \subset (\overline{x_2}, \dots, \overline{x_d}) \subset \mathfrak{m}_P/(x_1) \implies \mathfrak{m}_P^k \subset (x_1, x_2, \dots, x_d) \subset \mathfrak{m}_P.$$

Тот факт, что не лежащий в объединении минимальных простых идеалов x найдётся, остаётся в качестве упражнения; подсказка — использовать 6. Заметим, что при факторизации по (x_1) кольцо остаётся максимальной локализацией аффинной \mathbb{k} -алгебры, то есть кольцом вида \mathcal{O}_P . □

Замечание 23. Комментарий про $\dim A < \infty$ тут по существу, так как произвольное нётерово кольцо, вообще говоря, не обязано быть конечномерным. Однако в нашем случае колец \mathcal{O}_P сразу очевидно, что $\dim \mathcal{O}_P < \infty$, как размерность максимальной неприводимой компоненты, содержащей точку P .

Следствие 12 (Из теоремы 15). Пусть A — нётерово локальное кольцо с максимальным идеалом \mathfrak{m} . Тогда

$$\dim A \leq \dim_{A/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2.$$

Доказательство. Пусть $\overline{x_1}, \dots, \overline{x_n}$ — базис $\mathfrak{m}/\mathfrak{m}^2$. Тогда по предложению 31 мы имеем $(x_1, \dots, x_n) = \mathfrak{m}$, а тогда $\mathfrak{m} \subset (x_1, \dots, x_n) \subset \mathfrak{m}$. Но тогда по теореме 15 мы имеем $\dim A \leq n$. \square

Применяя это к кольцу \mathcal{O}_P , мы получаем, что

$$\dim \mathcal{O}_P \leq \dim_{\mathbb{k}} \mathfrak{m}_P / \mathfrak{m}_P^2.$$

Это наводит на мысль, что полезно рассматривать следующие объекты:

Определение 29. Пусть A — локальное кольцо с максимальным идеалом \mathfrak{m} . Оно называется *регулярным*, если $\dim A = \dim_{\mathbb{k}} \mathfrak{m}/\mathfrak{m}^2$.

Нам понадобятся следующие факты о регулярных локальных кольцах:

1. Регулярное локальное кольцо целостное — будет доказано здесь 16.
2. Регулярное локальное кольцо факториально — доказано не будет, вариант идеи возможного доказательства приводится после теоремы 18. Там же приведён альтернативный аргумент, о целостности локального кольца.
3. Любая локализация регулярного локального кольца относительно простого идеала — тоже регулярное локальное кольцо ??.

Перед тем, как доказывать эти факты, введём объект, который в принципе мотивирует изучение регулярных колец (то есть поймём, что условие регулярности означает геометрически).

3.2 Касательное пространство

Определение 30. Пусть $X \subset \mathbb{A}^n$ — аффинное многообразие, $I(X) = (f_1, \dots, f_m)$, $P \in X$. Пространство решений системы линейных уравнений относительно (t_1, \dots, t_n)

$$\begin{cases} \frac{\partial f_1}{\partial x_1}(P)t_1 + \dots + \frac{\partial f_1}{\partial x_n}(P)t_n = 0 \\ \vdots \\ \frac{\partial f_m}{\partial x_1}(P)t_1 + \dots + \frac{\partial f_m}{\partial x_n}(P)t_n = 0 \end{cases} \quad (4)$$

называется *касательным пространством к многообразию X в точке P* . Будем его обозначать $T_P X$.

Данное определение понятным образом соотносится с определением касательного пространства в анализе. Однако у него есть некоторые недостатки — зависимость определения от выбора образующих идеала и зависимость от выбора объемлющего пространства. Сейчас с этим сейчас поборемся.

Замечание 24. Определение корректно, то есть оно не зависит от выбора образующих в идеале $I(X)$.

Доказательство. Возьмём $f \in I(X)$ и разложим его по образующим

$$f = f_1 g_1 + \dots + f_m g_m.$$

Теперь продифференцируем:

$$\frac{\partial f}{\partial x_1}(P) = \sum_{j=1}^m \left(\frac{\partial f_j}{\partial x_1}(P) \cdot g_j(P) + \underbrace{f_j(P)}_{=0, \text{ т.к. } f_j \in I(X)} \cdot \frac{\partial g_j}{\partial x_1}(P) \right) = \sum_{j=1}^m \frac{\partial f_j}{\partial x_1}(P) \cdot g_j(P).$$

Тогда отсюда мы заключаем, что

$$\sum_i \frac{\partial f}{\partial x_i} t_i = \sum_{i,j} \frac{\partial f_j}{\partial x_i}(P) g_j(P) t_i = \sum_j g_j(P) \cdot \left(\sum_i \frac{\partial f_j}{\partial x_i}(P) \cdot t_i \right)$$

Теперь заметим, что если (t_1, \dots, t_n) удовлетворяют системе 4, то каждое слагаемое будет равно нулю. Значит, можно определять касательное пространство более инвариантно: записать бесконечную систему таких уравнений по всем элементам $f \in I(X)$, и результат не поменяется. \square

Проверим независимость определения касательного пространства от объемлющего пространства, дав эквивалентное функториальное определение. Для этого рассмотрим билинейное спаривание

$$\mathfrak{m}_P / \mathfrak{m}_P^2 \times T_P X \rightarrow \mathbb{k}, \quad (\bar{g}, (t_1, \dots, t_n)) \mapsto \sum_i \frac{\partial g}{\partial x_i}(P) t_i \in \mathbb{k}.$$

С производными многочленов выше по тексту проблем не было, а в данном месте придётся пояснить, что означают производные элементов локального кольца.

- Для начала поднимемся в объемлющее пространство — для функции $\bar{g} \in A(X) = \mathbb{k}[x_1, \dots, x_n]/I(X)$ можно рассмотреть прообраз $g \in \mathbb{k}[x_1, \dots, x_n]$. Заметим, что $\frac{\partial g}{\partial x_i}(P)$ **зависит** от выбора представителя \bar{g} , но — удивительное дело — если $(t_1, \dots, t_n) \in T_P X$, то сумма $\sum_i \frac{\partial g}{\partial x_i}(P) t_i$ от выбора представителя \bar{g} уже не зависит — для всякого $g \in I(X)$ эта сумма равна нулю по определению касательного пространства.
- Пусть $g \in \mathcal{O}_P$, то есть в окрестности точки P функция g равна отношению регулярных на X функций: $g = r/s$. Определим $\frac{\partial g}{\partial x_i}(P) := \frac{\frac{\partial r}{\partial x_i}(P) \cdot s(P) - r(P) \cdot \frac{\partial s}{\partial x_i}(P)}{s(P)^2}$ в соответствии с формулой $g' = \frac{r's - rs'}{s^2}$. В анализе данная формула означала предел приращения функции по отношению к приращению аргумента, но тут такие инфинитезимальные разговоры обосновать сложнее, поэтому предлагается поверить (или проверить), что определение корректно (не зависит от выбора представления $g = r/s$, и удовлетворяет тем же свойствам, что и удовлетворяла обычная производная — скажем, $(fg)' = f'g + fg'$).
- Наконец, если $\bar{g}_1 = \bar{g}_2 \in \mathfrak{m}_P / \mathfrak{m}_P^2$, то $g_1 - g_2 = h \in \mathfrak{m}_P^2$. Тогда

$$h = \sum_j \ell_j \ell'_j, \text{ где } \ell_j, \ell'_j \in \mathfrak{m}_P \implies \frac{\partial h}{\partial x_i}(P) = \sum_j \left(\ell_j(P) \frac{\partial \ell'_j}{\partial x_i}(P) + \frac{\partial \ell_j}{\partial x_i}(P) \cdot \ell'_j(P) \right) = 0.$$

Теперь наконец покажем, что оно невырождено.

- Зафиксируем $(t_1, \dots, t_n) \in T_P X$. Предположим, что

$$\forall g \in \mathfrak{m}_P : \sum_i \frac{\partial g}{\partial x_i}(P) t_i = 0.$$

Пусть $P = (p_1, \dots, p_n)$. Принимая $g = x_i - p_i \in \mathfrak{m}_P$, получаем из равенства выше, что $t_i = 0 \ \forall i$.

- Теперь зафиксируем $g \in \mathfrak{m}_P \subset \mathcal{O}_P \subset \mathbb{K}(x_1, \dots, x_n)$. Предположим, что

$$\sum_i \frac{\partial g}{\partial x_i}(P) \cdot t_i = 0 \quad \forall (t_1, \dots, t_n) \in T_P X.$$

Это уравнение является следствием уравнений для касательного пространства, откуда

$$\sum_i \frac{\partial g}{\partial x_i}(P) t_i = \alpha_1 \ell_1 + \dots + \alpha_m \ell_m, \text{ где } \ell_j = \sum_i \frac{\partial f_j}{\partial x_i}(P) t_i.$$

Приравнивая коэффициенты при t_i слева и справа мы получаем, что

$$\frac{\partial g}{\partial x_i}(P) = \alpha_1 \frac{\partial f_1}{\partial x_i}(P) + \dots + \alpha_m \frac{\partial f_m}{\partial x_i}(P) \ \forall i \implies \frac{\partial(g - \sum \alpha_j f_j)}{\partial x_i}(P) = 0.$$

Положим $\tilde{g} = g - \sum \alpha_j f_j$ и разложим \tilde{g} по формуле Тейлора в точке P :

$$\tilde{g}(x_1, \dots, x_n) = \underbrace{\tilde{g}(p_1, \dots, p_n)}_{=0} + \sum_i \underbrace{\frac{\partial \tilde{g}}{\partial x_i}(P)}_{=0} \cdot (x_i - p_i) + \varepsilon, \quad \varepsilon \in \mathfrak{m}_P^2,$$

(такое разложение очевидно для многочленов, и его можно проверить для рациональных функций), откуда $\tilde{g} = 0$ в $\mathfrak{m}_P / \mathfrak{m}_P^2$. С другой стороны, $\sum \alpha_j f_j \equiv 0$ на X , откуда $g \in \mathfrak{m}_P^2$, то есть $\tilde{g} = 0$ в $\mathfrak{m}_P / \mathfrak{m}_P^2$, что и требовалось доказать.

Значит, мы только что доказали, что имеет место изоморфизм

$$T_P X \cong (\mathfrak{m}_P / \mathfrak{m}_P^2)^*.$$

Это замечательное наблюдение позволяет нам распространить понятие касательного пространства с аффинного многообразия на произвольное квазипроективное:

Определение 31. Пусть $X \in \mathbf{qProj}$ а $P \in X$. Касательным пространством к X в точке P мы будем называть векторное пространство

$$T_P X \stackrel{\text{def}}{=} (\mathfrak{m}_P / \mathfrak{m}_P^2)^*.$$

Замечание 25. Так как идеал \mathfrak{m}_P конечно порождён, то это пространство всегда конечномерное.

Теорема 16. Регулярное локальное кольцо геометрического происхождения является областью целостности.

Доказательство. Будем вести индукцию по $\dim R$.

База. Пусть $\dim R = 0$. Тогда, так как R регулярно,

$$\dim R = \dim_{\mathbb{k}} \mathfrak{m}_P / \mathfrak{m}_P^2 = 0 \iff \mathfrak{m}_P = \mathfrak{m}_P^2.$$

Так как R — нётерово кольцо размерности 0, оно артиново, а отсюда (и из того факта, что оно локальное) $\mathfrak{m}_P = \text{Rad}(R) = \text{NRad}(R)$, откуда существует такое n , что $\mathfrak{m}_P^n = 0$, но тогда $\mathfrak{m}_P = 0$, то есть R — поле.

Переход. Пусть $\dim R \geq 1$. Рассмотрим элемент $x \in \mathfrak{m} \setminus \mathfrak{m}^2$, не лежащий в объединении минимальных простых. Такой существует, так как в противном случае

$$\mathfrak{m} = \bigcup_{\mathfrak{p} \text{ — минимальный простой}} \mathfrak{p} \cup \mathfrak{m}^2 \xrightarrow{6} \mathfrak{m} \subset \mathfrak{p} \text{ или } \mathfrak{m} \subset \mathfrak{m}^2.$$

В первом случае $\dim R = 0$. Во втором случае по лемме Накаямы 30: $\mathfrak{m} = 0$, откуда R — поле.

Теперь рассмотрим кольцо $S = R/(x)$. Ясно (см. 7), что $\dim S \leq \dim R - 1$. Пусть $\dim S = d$. Тогда согласно 15: $\exists x_1, \dots, x_d \in R, k \in \mathbb{N}$:

$$\overline{\mathfrak{m}^k} \subset (\overline{x_1}, \dots, \overline{x_d}) \subset \overline{\mathfrak{m}} \implies \mathfrak{m}^k \subset (x, x_1, \dots, x_d) \subset \mathfrak{m},$$

откуда опять же по 15, $\dim R \leq \dim S + 1$, то есть имеет место равенство $\dim S = \dim R - 1$. Теперь убедимся, что S — регулярное локальное кольцо. Оно локальное с единственным идеалом $\overline{\mathfrak{m}}$, откуда

$$\dim S \leq \dim_{\mathbb{k}} \overline{\mathfrak{m}} / \overline{\mathfrak{m}}^2.$$

С другой стороны, мы имеем

$$\dim_{\mathbb{k}} \overline{\mathfrak{m}} / \overline{\mathfrak{m}}^2 \leq \dim_{\mathbb{k}} \mathfrak{m} / \mathfrak{m}^2 - 1 = \dim R - 1 = \dim S,$$

так как отображение $\mathfrak{m} / \mathfrak{m}^2 \hookrightarrow \mathfrak{m} / (\mathfrak{m}^2 + (x))$ имеет нетривиальное ядро. Значит, кольцо S регулярно. По индукционному предположению S — область целостности, откуда $(x) \subset R$ — простой идеал. Так как x не лежит ни в одном минимальном простом идеале, существует $\mathfrak{p} \in \text{Spec } R$ такой, что $\mathfrak{p} \subseteq (x)$. Рассмотрим $y \in \mathfrak{p}$, тогда $y = ax$ для некоторого $a \in R$. Но, так как $x \notin \mathfrak{p}$, отсюда $a \in \mathfrak{p}$. То есть $\mathfrak{p} = (x)\mathfrak{p}$, откуда по лемме Накаямы 30: $\mathfrak{p} = 0$, то есть R — область целостности. \square

Определение 32. Пусть X — многообразие, $P \in X$. Точка P называется *неособой*, если \mathcal{O}_P регулярно. Многообразие X называется *неособым*, если каждая его точка неособая. Точка, в которой локальное кольцо нерегулярно, называется *особой точкой*.

В случае $\mathbb{k} = \mathbb{k}^{\text{alg}}$ также есть следующие синонимичные понятия: *точки гладкости* (синоним неособой точки), многообразие — *гладкое*, если все его точки — точки гладкости, а в противном случае многообразие содержит *точки негладкости*.

3.3 Разложение в ряд Тейлора

Пусть X — многообразие, $P \in X$. Возьмём $f \in \mathcal{O}_P$, тогда ясно, что $f - f(P) \in \mathfrak{m}_P$. Так как идеал \mathfrak{m}_P конечно порождён, мы можем выбрать какую-то систему образующих $\mathfrak{m}_P = (u_1, \dots, u_n)$. Тогда

$$f - f(P) = g_1 u_1 + \dots + g_n u_n, \quad g_i \in \mathcal{O}_P.$$

Аналогично, $g_i \in g_i(P) + \mathfrak{m}_P$, тогда

$$f - f(P) - \sum_{i=1}^n g_i(P)u_i \in \mathfrak{m}_P^2 \implies f - f(P) - \sum_{i=1}^n g_i(P)u_i = \sum_{i,j=1}^n h_{ij}u_iu_j, \quad h_{i,j} \in \mathcal{O}_P.$$

Продолжая в том же духе мы получаем, что

$$\forall g \in \mathcal{O}_P : \exists F_0 + F_1 + \dots \in \mathbb{k}[[x_1, \dots, x_n]] : f - \sum_{i=0}^s F_i(u_1, \dots, u_n) \in \mathfrak{m}_P^{s+1} \quad \forall s \in \mathbb{N},$$

где F_i — однородный многочлен степени i от переменных x_1, \dots, x_n .

Определение 33. Полученное выше представление и называется *рядом Тейлора* для функции f относительно системы локальных параметров u_1, \dots, u_n .

Ответим сразу на естественный вопрос о единственности такого представления.

Теорема 17. Пусть X — многообразие, $P \in X$ — неособая точка, а $\dim \mathcal{O}_P = n$. Выберем систему образующих $\mathfrak{m} = (u_1, \dots, u_n)$ и рассмотрим функцию $f \in \mathcal{O}_P$. Тогда существует единственный ряд Тейлора для функции f относительно системы (u_1, \dots, u_n) .

Доказательство. Докажем сначала вот такую лемму:

Лемма 8. Пусть F — s -форма от x_1, \dots, x_n с коэффициентами из поля \mathbb{k} . Предположим, что $F(u_1, \dots, u_n) \in \mathfrak{m}_P^{s+1}$. Тогда $F \equiv 0$.

Доказательство леммы. 1) Предположим сначала, что $F(0, \dots, 0, 1) = [u_n^s]F \neq 0$. Так как $a_n u_n^s + \dots \in \mathfrak{m}_P^{s+1}$, $a_n u_n^s + \dots = G(u_1, \dots, u_n)$, где G — форма степени s с коэффициентами из \mathfrak{m}_P .

$$G(u_1, \dots, u_n) = H_0 u_n^s + H_1 u_n^{s-1} + \dots + H_s, \quad \text{где}$$

H_i — форма от x_1, \dots, x_{n-1} степени i . Тогда

$$\left(\underbrace{a_n}_{\in \mathbb{k}^\times} - \underbrace{H_0(u_1, \dots, u_{n-1})}_{\in \mathfrak{m}_P} \right) u_n^s \in (u_1, \dots, u_{n-1}) \implies u_n^s \in (u_1, \dots, u_{n-1}),$$

так как $\left(\underbrace{a_n}_{\in \mathbb{k}^\times} - \underbrace{H_0(u_1, \dots, u_{n-1})}_{\in \mathfrak{m}_P} \right) \in \mathcal{O}_P^*$. Значит, мы получаем

$$\mathfrak{m}_P^s \subset (u_1, \dots, u_{n-1}) \subset \mathfrak{m}_P,$$

но тогда по лемме 15 мы имеем $\dim \mathcal{O}_P = n - 1$, что приводит к противоречию.

2) В общем случае сделаем замену переменных: возьмём

$$G(u_1, \dots, u_n) = F(\alpha_{11}u_1 + \dots + \alpha_{1n}u_n, \dots, \alpha_{n1}u_1 + \dots + \alpha_{nn}u_n)$$

где $(\alpha_{ij}) \in \text{GL}_n(\mathbb{k})$ и

$$G(0, \dots, 0, 1) = F(\alpha_{1n}, \dots, \alpha_{nn}) \neq 0$$

и таким образом сведём ситуацию к 1). □

Теперь докажем теорему. Так как нас интересует лишь вопрос единственности, достаточно показать, что у нулевой функции ряд Тейлора также будет нулевым. Пусть $F_0 + F_1 + \dots$ — ряд Тейлора для нуля. Так как функция 0 (очевидно) обнуляется в точке P , из определения и леммы мы имеем

$$F_0(u_1, \dots, u_n) \in \mathfrak{m}_P, \implies F_0 \equiv 0.$$

Пусть теперь $s = 1$. Тогда, так как $F_0 = 0$, отсюда

$$F_1(u_1, \dots, u_n) \in \mathfrak{m}_P^2 \implies F_1 \equiv 0$$

по лемме. Продолжая пользоваться леммой мы получаем, что $F_j \equiv 0$. \square

Итак, выбор системы образующих $\mathfrak{m}_P = (u_1, \dots, u_n)$ определяет гомоморфизм

$$\tau: \mathcal{O}_P \rightarrow \mathbb{k}[[x_1, \dots, x_n]].$$

Естественно задуматься о том, каково его ядро. Нетрудно видеть, что

$$\tau(f) = 0 \iff f \in \bigcap_{s \in \mathbb{N}} \mathfrak{m}^s,$$

что мотивирует изучить, как устроен идеал справа. Оказывается, в нашем случае он устроен не слишком уж сложно.

Теорема 18. Пусть A — локальное нётерово кольцо с максимальным идеалом \mathfrak{m} . Тогда

$$\bigcap_{s \in \mathbb{N}} \mathfrak{m}^s = 0.$$

Доказательство. Рассмотрим $\alpha \in \bigcap_{s \in \mathbb{N}} \mathfrak{m}^s$. Для каждого $k \in \mathbb{N}$ найдётся такой F_k , что $\alpha = F_k(u_1, \dots, u_n)$, где F_k — однородный многочлен из $A[x_1, \dots, x_n]$ степени k .

Так как $A[x_1, \dots, x_n]$ нётерово, то по теореме Гильберта о базисе: $\exists s \in \mathbb{N}$:

$$(F_1, F_2, \dots, F_k, \dots) = (F_1, \dots, F_s).$$

Но это в частности значит, что

$$F_{s+1} = G_1 F_1 + \dots + G_s F_s, \quad G_i \in A[x_1, \dots, x_n], \deg G_i = s + 1 - i$$

и G_i однородные. Подставляя u_1, \dots, u_n , получаем:

$$\alpha = F_{s+1}(u_1, \dots, u_n) = \alpha(G_1(u) + \dots + G_s(u)) \implies \alpha = \alpha\beta, \beta \in \mathfrak{m}.$$

Тем самым, $\alpha(1 - \beta) = 0$, и сокращая на $1 - \beta$ — обратимый элемент A — мы получаем $\alpha = 0$. \square

Таким образом, как мы видим, ядро построенного выше гомоморфизма тривиально и $\mathcal{O}_P \hookrightarrow \mathbb{k}[[x_1, \dots, x_n]]$, откуда сразу следует целостность кольца \mathcal{O}_P . Таким же образом можно пытаться доказать факториальность \mathcal{O}_P . Однако, во-первых, надо начать с доказательства факториальности $\mathbb{k}[[x_1, \dots, x_n]]$, а, во-вторых, подкольцо факториального кольца совсем не обязано быть факториальным, так что нужны дополнительные слова.

Отметим также, что из леммы 8 можно извлечь достаточно полезное следствие. А именно, рассмотрим градуированное кольцо

$$\bigoplus_{k=0}^{\infty} \mathfrak{m}_P^k / \mathfrak{m}_P^{k+1}.$$

В случае, если P — неособая точка, мы можем рассмотреть гомоморфизм

$$\mathbb{k}[[x_1, \dots, x_n]] \rightarrow \bigoplus_{k=0}^{\infty} \mathfrak{m}_P^k / \mathfrak{m}_P^{k+1}, \quad x_i \mapsto u_i.$$

Из леммы следует, что это мономорфизм, а сюръективность очевидна. Значит, мы доказали такое следствие.

Следствие 13. Пусть $P \in X$ — неособая точка. Тогда имеет место следующий изоморфизм \mathbb{k} -алгебр:

$$\bigoplus_{k=0}^{\infty} \mathfrak{m}_P^k / \mathfrak{m}_P^{k+1} \cong \mathbb{k}[[x_1, \dots, x_n]]$$

В частности, отсюда следует, что на неособом многообразии градуированная алгебра

$$\bigoplus_{k=0}^{\infty} \mathfrak{m}_P^k / \mathfrak{m}_P^{k+1}$$

не зависит от выбора точки P (что вообще говоря неочевидно).

3.4 Локальное кольцо точки на неособой кривой. Индексы ветвления и степень инерции.

Рассмотрим неособую проективную кривую X и точку $P \in X$. Мы знаем, что в силу того, что кривая неособая, $\dim \mathcal{O}_P = \dim_{\mathbb{k}} \mathfrak{m}_P / \mathfrak{m}_P^2$, а из этого условия по лемме Накаямы следует, что идеал \mathfrak{m}_P главный.

Кольцо \mathcal{O}_P в этом случае — дискретно нормированное кольцо и с каждой точкой кривой у нас ассоциировано нормирование v_P поля $\mathbb{k}(X)$.

Пусть теперь $\varphi: Y \rightarrow X$ — морфизм неособых кривых и $\varphi^{-1}(P) = \{Q_1, \dots, Q_n\}$. Попробуем понять, как же связаны нормирования v_P и v_{Q_i} . Ясно, что в этом случае для любой точки Q_i есть расширение колец $\varphi^*: \mathcal{O}_P \rightarrow \mathcal{O}_{Q_i}$ и $\mathfrak{m}_P \subset \mathfrak{m}_{Q_i}$, $\mathfrak{m}_P = \mathfrak{m}_{Q_i} \cap \mathcal{O}_P$. И видно, что в этой ситуации нормирования v_{Q_i} *продолжают* нормирование v_P . Действительно, мы можем рассмотреть функцию

$$\psi: \mathcal{O}_P \rightarrow \mathbb{Z}, \psi(f) = v_{Q_i}(\varphi^*(f))$$

для которой легко проверить, что $\psi(f \cdot g) = \psi(f) + \psi(g)$ и $\psi(f + g) \geq \min(\psi(f), \psi(g))$. Возможно, ψ не сюръективна, но так как $f(P) = 0 \iff \varphi^*(f)(P) = 0$, то $\psi(f) > 0 \iff v_P(f) > 0$. Отсюда ясно, что $\exists e > 0$:

$$v_{Q_i} = e \cdot v_P.$$

Число e в этом контексте называют *индексом ветвления* и обозначают $e = e(\mathcal{O}_{Q_i} / \mathcal{O}_P)$. Сразу видно, что индекс ветвления можно вычислить вот так:

$$v_{Q_i}(\pi_P) = e(\mathcal{O}_{Q_i} / \mathcal{O}_P),$$

где $(\pi_P) = \mathfrak{m}_P$ — локальный параметр для кольца \mathcal{O}_P . Или, иными словами, такой элемент, что $v_P(\pi_P) = 1$.

Теорема 19. Оказывается, в такой ситуации $e_1 + \dots + e_n = [\mathbb{k}(Y) : \mathbb{k}(X)]$ ¹².

3.5 Конечные морфизмы и нормализация многообразия

Теорема 20. Пусть L/K — сепарабельное конечное расширение, кольцо $A \subset K$ и $K = \text{Frac}(A)$. Пусть $B = \text{Int}_L A$ и предположим, что A нётерово и целозамкнуто¹³ (в своём поле частных). Тогда B — конечно порождённый A -модуль.

Доказательство. Это доказывается стандартным образом.

Во-первых, из следующей несложной леммы очевидно, что $L = \text{Frac}(B)$.

Лемма 9. Для любого $x \in L$ существует $a \in A^\times$: $ax \in B$.

Доказательство. Так как расширение L/K конечно, то x алгебраичен над K . Значит, имеется зависимость $x^n + c_{n-1}x^{n-1} + \dots + c_0 = 0$ для некоторых $c_i \in K$. Домножая на знаменатели, получим зависимость вида $a_n x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$ для некоторых $a_i \in A$, причём $a_n \neq 0$. Видно, что $a_n x^n$ — целый над A элемент (чтобы явно получить зависимость, надо уравнение домножить на a_n^{n-1}). \square

Возьмём $\{\omega_i\}_{i=1}^n$ — базис L/K , причём выберем $\omega_i \in B$ (что возможно по лемме 9). Рассмотрим билинейную форму следа

$$L \times L \rightarrow K, \quad (x, y) \mapsto \text{Tr}(xy).$$

Из курса теории полей известно, что так как расширение сепарабельно, то эта форма невырождена. Возьмём двойственный базис к ω_i , то есть рассмотрим такой набор $\{\omega_i^*\}$, что

$$\text{Tr}(\omega_i \omega_j^*) = \begin{cases} 1, & i = j \\ 0, & \text{иначе.} \end{cases}$$

Имеем следующие включения

$$A\omega_1 \oplus \dots \oplus A\omega_n \subset B \subset A\omega_1^* \oplus \dots \oplus A\omega_n^*.$$

Первое включение очевидно, докажем второе. Пусть $b = a_1\omega_1^* + \dots + a_n\omega_n^*$, где $a_i \in K$, мы покажем, что $a_i \in A$. С одной стороны,

$$a_i = \text{Tr}(b\omega_i).$$

Пусть $G = \{\sigma : L \rightarrow K^{\text{alg}}\}$ — все вложения L в K^{alg} . Если α цел над A , то $\sigma\alpha$ цел над A (это тривиальная проверка), а тогда и $\text{Tr}(\alpha)$ цел над A , так как

$$\text{Tr}(\alpha) = \sum_{\sigma \in G} \sigma\alpha.$$

¹²Об этом написано в книге «Алгебраическая Геометрия» Хартсхорна, Г. 2, §6, предложение 6.9. Это верно, если $\varphi : Y \rightarrow X$ — конечный морфизм, и доказательство этого, насколько понимает редактор, идёт ниже, вплоть до 22

¹³также говорят нормально; A — область целостности, так что нормальность и целозамкнутость — синонимы.

Так как $\text{Tr}(b\omega_i) \in K$ цело над A , то из целозамкнутости A : $a_i = \text{Tr}(b\omega_i) \in A$. Мы получили, что B — подмодуль конечно порождённого модуля над нётеровым кольцом, откуда B — конечно порождённый A -модуль. \square

Теперь опустим требование сепарабельности расширения ценой конкретизации ситуации: в дальнейшем A будет не произвольной нётеровой областью целостности, а целостной аффинной \mathbb{k} -алгеброй.

Теорема 21. Пусть A — целостная аффинная алгебра, $K = \text{Frac}(A)$, а L/K — конечное расширение. Обозначим $B = \text{Int}_L A$. Тогда B — конечно порождённый A -модуль.

Доказательство. По лемме Нётер о нормализации, A — конечное расширение кольца многочленов $\mathbb{k}[x_1, \dots, x_n]$. Так как B цело на A , оно цело и над $\mathbb{k}[x_1, \dots, x_n]$, откуда $B = \text{Int}_L \mathbb{k}[x_1, \dots, x_n]$.

Кроме того, расширение $L/\text{Frac}(\mathbb{k}[x_1, \dots, x_n])$ конечное (это следует из такой леммы):

Лемма 10. Пусть $\varphi: A \hookrightarrow B$ — конечное расширение. Тогда расширение $\text{Frac}(B)/\text{Frac}(A)$ конечное.

Доказательство. Рассмотрим мультипликативное подмножество $S = A \setminus \{0\}$. Согласно 29, $\text{Frac}(A) = S^{-1}A \hookrightarrow \varphi(S)^{-1}B$ конечное. С другой стороны, так как $\varphi(S)^{-1}B$ — конечная область целостности над полем $\text{Frac}(A)$, оно является полем 30, в которое вкладывается B . Согласно универсальному свойству поля частных оно совпадает с $\text{Frac}(B)$, и мы получили, что расширение $\text{Frac}(B)/\text{Frac}(A)$ конечное. \square

Из этих рассуждений следует, что мы без ограничений общности можем полагать, что $A = \mathbb{k}[x_1, \dots, x_n]$.

Кроме того, без ограничений общности мы можем полагать, что расширение L/K нормальное, так как если мы перейдём к нормальному замыканию \tilde{L}/K и докажем теорему для него и для $\tilde{B} = \text{Int}_{\tilde{L}} A \supset B$, то мы докажем теорему и для B .

Пусть $G = \{\sigma: L \rightarrow K^{\text{alg}}\}$. Так как L/K нормально, то $\forall \sigma \in G: \sigma(L) \subset L$ и мы можем рассмотреть башню расширений:

$$\begin{array}{c} L \\ | \\ L^G = F \\ | \\ K \end{array}$$

где верхний этаж — расширение Галуа, а нижний — чисто несепарабельное расширение¹⁴.

¹⁴В характеристике 0 все расширения сепарабельны; там окажется $F = K$.

Введём соответствующие кольца целых $\mathcal{O}_L = \text{Int}_L A$ и $\mathcal{O}_F = \text{Int}_F A$. Они образуют башню расширений колец

$$\begin{array}{c} \mathcal{O}_L = \text{Int}_L A \\ | \\ \mathcal{O}_F = \text{Int}_F A \\ | \\ A \end{array}$$

Так как расширение L/F сепарабельно, а \mathcal{O}_F целозамкнуто, то мы можем применить теорему 20 и получить, что \mathcal{O}_L — конечно порождённый \mathcal{O}_F -модуль.

Далее, из общей теории полей следует, что чисто несепарабельное расширение устроено следующим образом:

$$F = \mathbb{k}\left(y^{\frac{1}{p^{m_1}}}, \dots, y^{\frac{1}{p^{m_s}}}\right), \text{ где } y_i \in A, p = \text{char } \mathbb{k}.$$

Возьмём $m = \max m_i$, запишем $y_i = \sum_I a_I x^I$ (где I — мультииндекс), и извлечём корень

$$y_i^{\frac{1}{p^m}} = \sum a_I^{\frac{1}{p^m}} x^{I/p^m}, \quad (5)$$

так как в характеристике p :

$$\left(\sum a_I^{\frac{1}{p^m}} x^{\frac{I}{p^m}}\right)^{p^m} = \sum \left(a_I^{\frac{1}{p^m}} x^{\frac{I}{p^m}}\right)^{p^m}$$

а так как поле \mathbb{k} алгебраически замкнуто, то все $a_I^{\frac{1}{p^m}} \in \mathbb{k}$. Итак, из (5) следует, что

$$F \subset \mathbb{k}\left(x_1^{\frac{1}{p^m}}, \dots, x_n^{\frac{1}{p^m}}\right).$$

Тем самым, если мы докажем теорему для $\mathbb{k}\left(x_1^{\frac{1}{p^m}}, \dots, x_n^{\frac{1}{p^m}}\right)$, то мы докажем её и для F , так что далее без ограничений общности можно полагать, что

$$F = \mathbb{k}\left(x_1^{\frac{1}{p^m}}, \dots, x_n^{\frac{1}{p^m}}\right).$$

Теперь убедимся, что $\mathcal{O}_F = \mathbb{k}\left[x_1^{\frac{1}{p^m}}, \dots, x_n^{\frac{1}{p^m}}\right] =: R$. Включение $R \subset \mathcal{O}_F$ очевидно. Пусть $\alpha \in \mathcal{O}_F$, то есть α цел над A , значит он цел и над R , откуда $\alpha \in R$ (так как R целозамкнуто и расширение R/A конечно¹⁵).

Итак, мы показали, что \mathcal{O}_F/R конечно (а так как R/A конечно и $\mathcal{O}_L/\mathcal{O}_F$ конечно), из этого следует теорема. \square

Определение 34. Если в предыдущей теореме $L = K$, то B называется *нормализацией* A .

¹⁵Его базис состоит из мономов вида $x_1^{k_1/p^m} \cdot \dots \cdot x_n^{k_n/p^m}$ по $0 \leq k_i \leq p^m - 1$

Пример 11. Пусть $A = \mathbb{k}[x, y]/(y^2 - x^3)$. Это кольцо не целозамкнуто: $(\frac{y}{x})^2 = x$, но $\frac{y}{x} \notin A$. Обозначая $t := \frac{y}{x}$, видим наличие вложения $A \hookrightarrow \mathbb{k}[t]$, $x \mapsto t^2, y \mapsto t^3$. При этом $\mathbb{k}[t]$ — конечный A -модуль, и $\mathbb{k}[t]$ уже целозамкнуто. Можно показать, что $\mathbb{k}[t]$ — нормализация A .

Замечание 26. Отметим, что в этом случае B является аффинной \mathbb{k} -алгеброй, так как она целостна, и к тому же — конечно порождённый модуль над какой-то другой аффинной \mathbb{k} -алгеброй.

Определение 35. Пусть X — аффинное многообразие. Тогда X называется *нормальным*, если $X = \text{Specm}(A)$, где A — нормальное.

Таким образом, аффинное многообразие X может быть нормальным, а может — не быть. Во втором случае теорема 21 говорит, что существует аффинное нормальное многообразие Y , и конечный морфизм (вложение) $A(X) \rightarrow A(Y)$. Он, кстати, порождает $Y \rightarrow X$ в силу антиэквивалентности категорий.

Теперь обобщим данную ситуацию на случай произвольных (необязательно аффинных) многообразий.

Определение 36. Пусть $\varphi: Y \rightarrow X$ — морфизм многообразий. Предположим, что у любой точки $x \in X$ есть такая аффинная окрестность U_x , что $\varphi^{-1}(U_x) \cong V_x$, где $V_x \subset Y$ — аффинная, и расширение $A(U_x) \hookrightarrow A(V_x)$ конечно. Тогда φ называется *конечным морфизмом*.

Определение 37. Неприводимое многообразие X ¹⁶ называют *нормальным*, если $\forall P \in X$: кольцо \mathcal{O}_P нормально.

Предложение 24. *Предыдущие два определения нормальности согласованы.*

Доказательство. Нам нужно доказать следующее утверждение: A нормально, если и только если $\forall \mathfrak{m} \in \text{Specm}(A)$ кольцо $A_{\mathfrak{m}}$ нормально (для целостного кольца A).

Легко убедиться, что любая локализация целозамкнутого кольца целозамкнута.

Обратно, покажем, что $A = \bigcap_{\mathfrak{m} \in \text{Specm}(A)} A_{\mathfrak{m}}$. Включение слева направо очевидно. Пусть $x \in \bigcap_{\mathfrak{m} \in \text{Specm}(A)} A_{\mathfrak{m}}$. Рассмотрим множество $I := \{a \in A \mid xa \in A\}$, очевидно, что это идеал. При этом для всякого $\mathfrak{m} \in A : x \in A_{\mathfrak{m}}$, так что x представим в виде r/s , где $s \notin \mathfrak{m}$, откуда $I \not\subseteq \mathfrak{m}$. Тем самым, $I = (1)$, то есть $x \in A$.

Так как каждое кольцо в правой части целозамкнуто, и само A целозамкнуто. \square

Замечание 27. Тем самым, X нормально, если локальное кольцо в каждой точке нормально. Понятно, что достаточно требовать существования покрытия аффинными картами, такого, что аффинная алгебра каждой карты нормальна.

Замечание 28. Если X — неособое (гладкое) многообразие, то все его локальные кольца регуляры. Можно доказать, что регулярное кольцо факториально, а факториальное кольцо очевидным образом нормально.

Тем самым, все неособые многообразия нормальны.

Обратное неверно: конус $\{x^2 + y^2 = z^2\} \subset \mathbb{A}^3$ — нормальное многообразие, но имеет особенность в $(0, 0, 0)$.

¹⁶Уже не обязательно аффинное

3.6 Морфизмы между неособыми кривыми

Предложение 25. Пусть X — неособая неприводимая кривая, пусть у нас есть рациональное отображение $f: X \dashrightarrow \mathbb{P}^n$. Тогда оно регулярно во всех точках.

Доказательство. Действительно, рассмотрим открытое $U \subset X$, на котором f — (регулярный) морфизм. Уменьшая окрестность U , можно считать, что $f(U)$ попадает в аффинную карту: если рассмотреть f , как отображение $U \rightarrow \mathbb{A}_0^n \subset \mathbb{P}^n$, то f мы можем записать, как

$$u \mapsto (1 : f_1(u) : f_2(u) : \dots : f_n(u)) = (f_0(u) : f_1(u) : f_2(u) : \dots : f_n(u)), \quad f_i \text{ — регулярны на } U.$$

Тогда $f_i \in \mathbb{k}(X)$. Рассмотрим $P \in X$, понятно, что $\mathcal{O}_P \subset \mathbb{k}(X)$. Так как кривая X неособая, то \mathcal{O}_P — дискретно нормированное кольцо. Обозначим соответствующее дискретное нормирование за v_P , пусть $k_i = v_P(f_i)$, а $k = \min_i \{k_i\}$. В силу симметрии, мы можем считать, что минимум достигается при $i = 0$. Тогда мы можем записать каждую функцию, как

$$f_i = t^{k_i} g_i,$$

где t — локальный параметр, то есть образующая \mathfrak{m}_P (или же, такой элемент, что $v_P(t) = 1$), и $v_P(g_i) = 0$. Разделим каждую координату на t^{k_0} . Так мы получим эквивалентное рациональное отображение $X \dashrightarrow Y$, имеющее вид

$$u \mapsto (g_0(u) : t^{k_1-k_0} g_1(u) : \dots : t^{k_n-k_0} g_n(u)).$$

Заметим, что $v_P(g_0) = 0$, то есть $g_0 \in \mathcal{O}_P^*$, то есть $g_0 \notin \mathfrak{m}_P$. Это означает, что g_0 определена в точке P и не обращается в 0 в ней (и даже в некоторой окрестности этой точки). Для остальных i мы получаем, что $v_P(g_i) \geq 0 \implies g_i \in \mathcal{O}_P$, то есть они регулярны в некоторой окрестности P . Тем самым, отображение определено в некоторой окрестности точки P и точка P является точкой регулярности (так как в её окрестности не все координаты равны нулю). По произвольности точки P мы имеем нужное. \square

При помощи этого утверждения также можно доказать, что эллиптическая кривая не бирационально изоморфна \mathbb{P}^1 .

Предположим противное, пусть у нас есть рациональное отображение $C \dashrightarrow \mathbb{P}^1$, и обратное ему $\mathbb{P}^1 \dashrightarrow C$. В силу предыдущего предложения мы можем полагать, что оба эти отображения — регулярные морфизмы. Получили композицию

$$C \xrightarrow{f} \mathbb{P}^1 \xrightarrow{g} C,$$

где f, g — регулярные изоморфизмы, причём на некотором открытом множестве $g \circ f = \text{id}$ и $f \circ g = \text{id}$.

Лемма 11. Если $h_1, h_2: X \rightarrow Y$ — морфизмы, X неприводимо и h_1 совпадает с h_2 на некотором открытом $U \subset X$, то $h_1 = h_2$.

Доказательство. Рассмотрим диагональное $X \xrightarrow{h_1 \times h_2} Y \times Y$. По условию $(h_1 \times h_2)(U) \subset \Delta(Y)$, а в силу плотности $U \subset X$ и замкнутости диагонали, $(h_1 \times h_2)(X) \subset \Delta(Y)$. \square

Итак, из бирациональной эквивалентности неособых проективных кривых $C \cong \mathbb{P}^1$ получается обычный изоморфизм $C \cong \mathbb{P}^1$ в категории Proj . Так как группа автоморфизмов \mathbb{P}^1 действует на ней транзитивно, то не умаляя общности, можно считать, что $\infty \mapsto \infty$. Выкидывая бесконечно удалённые точки, достаточно доказывать, что аффинная эллиптическая кривая не может быть изоморфна \mathbb{A}^1 . Чтобы доказать это, можно посмотреть на кольца регулярных функций — оказывается, кольцо регулярных функций на эллиптической кривой не факториально.

3.7 Морфизмы между неособыми проективными неприводимыми кривыми

Пусть $f : Y \rightarrow X$ — морфизм между неособыми проективными неприводимыми кривыми.

Образ $f(Y) \subset X$ замкнут, и отбрасывая неинтересный случай одноточечного образа, получаем $f(Y) = X$. Морфизм алгебраических многообразий f индуцирует морфизм полей частных $\mathbb{k}(X) \rightarrow \mathbb{k}(Y)$. Так как $\text{tr. deg}_{\mathbb{k}} \mathbb{k}(X) = \text{tr. deg}_{\mathbb{k}} \mathbb{k}(Y) = 1$, то расширение алгебраично. В силу конечной порождённости обоих полей над \mathbb{k} (это поля частных аффинных алгебр) получаем, что расширение полей конечно.

Покроем X аффинными картами: $X = \bigcup_i \text{Specm } A_i$.

Теорема 22. *Оказывается, $f^{-1}(\text{Specm } A_i) \cong \text{Specm Int}_{\mathbb{k}(Y)} A_i$.*

Доказательство. Пусть $A = A_i$, положим $B := \text{Int}_{\mathbb{k}(Y)} A$. Мы находимся в ситуации 21, значит, B — нормальная целостная аффинная алгебра, конечная над A , причём $\text{Frac}(B) \cong \mathbb{k}(Y)$. В силу антиэквивалентности категорий, существует бирациональный изоморфизм $\varphi : \text{Specm } B \dashrightarrow Y$.

Ещё раз используя, что $\text{Frac}(B) \cong \mathbb{k}(Y)$, получаем в силу 2, $\dim B = 1$, и в силу нормальности B — дедекиндово кольцо. Значит, $\text{Specm } B$ — неособая кривая¹⁷, и φ продолжается до регулярного морфизма $\varphi : \text{Specm } B \rightarrow Y$.

Следующим шагом покажем, что этот морфизм $\varphi : \text{Specm } B \rightarrow Y$ — изоморфизм на образ.

- В силу того, что $\varphi : \text{Specm } B \dashrightarrow Y$ — бирациональный изоморфизм, существует рациональный морфизм $\varphi^{-1} : Y \rightarrow \text{Specm } B$. Пусть $\text{Specm } B \subset \mathbb{A}^n$, в таком случае можно скомпоновать φ^{-1} с координатными проекциями $\pi_j : \mathbb{A}^n \rightarrow \mathbb{k}$, и получить координатное задание: $\varphi^{-1}(y) = (g_1(y), \dots, g_n(y))$, где $g_i \in \mathbb{k}(Y)$ — рациональные функции.
- Чтобы проверить наличие обратного регулярного отображения, необходимо убедиться, что все g_i регулярны во всех точках $\text{Im } \varphi$. Выберем какую-нибудь точку $y_0 = \varphi(x_0)$, и проверим регулярность g_i в ней. Предположим противное: $v_{y_0}(g_i) < 0$, то есть $\frac{1}{g_i} \in \mathfrak{m}_{y_0}$. Ясно, что $\varphi^*(\mathfrak{m}_{y_0}) \subset \mathfrak{m}_{x_0}$, тем самым, получаем, что $\frac{1}{\pi_i} = \varphi^*\left(\frac{1}{g_i}\right) \in \mathfrak{m}_{x_0}$, то есть $v_{x_0}(\pi_i) < 0$. Но координатная проекция π_i регулярна в точке x_0 , откуда мы получаем противоречие.
- Итак, $\varphi^{-1} : \text{Im } \varphi \rightarrow \text{Specm } B$ — обратный к φ регулярный морфизм. То, что они действительно взаимно обратны, следует, например, из 11.

В дальнейшем можем отождествить $\text{Specm } B$ с $\text{Im } \varphi$, и рассматривать $\text{Specm } B \subset Y$. Теперь приступим к доказательству теоремы: проверим, что $\text{Specm } B = f^{-1}(\text{Specm } A)$.

- Зафиксируем точку $P \in \text{Specm } A$, и пусть точки $Q_1, \dots, Q_m \in \text{Specm } B$ — её прообразы относительно f . Отображение f^* задаёт морфизмы $f^* : \mathcal{O}_P \rightarrow \mathcal{O}_{Q_i}$, и мы оказываемся в ситуации теоремы 19. А именно, определены индексы ветвления $e_i = e(\mathcal{O}_{Q_i}/\mathcal{O}_P)$, и теорема говорит, что $e_1 + \dots + e_m = [\mathbb{k}(Y) : \mathbb{k}(X)]$.

¹⁷ дедекиндовость можно было и не упоминать, это сразу следует из нормальности B .

- Пойдём от противного: пусть $\exists Q \notin \text{Specm } B : f(Q) = P$. Тут тоже есть $f^* : \mathcal{O}_P \rightarrow \mathcal{O}_Q$, и опять же есть индекс ветвления $e = e(\mathcal{O}_Q/c\mathcal{O}_P)$. Получим противоречие, показав, что $s := e + e_1 + \dots + e_m \leq [\mathbb{k}(Y) : \mathbb{k}(X)]$. Дальше идёт рассуждение, идентичное доказательству теоремы 25, и так как оно там оформлено более аккуратно, то закончим доказательство ссылкой.

□

4 Дивизоры

4.1 Дивизоры Вейля

Начнём с такого примера:

Пример 12. Как мы увидим через секунду, все нормирования на $\mathbb{k}(t) = \mathbb{k}(\mathbb{P}^1)$, тривиальные на \mathbb{k} , соответствуют точкам $\alpha \in \mathbb{k}$ и ∞ . Если говорить конкретнее, то любая рациональная функция на \mathbb{P}^1 имеет вид

$$f(t) = C \cdot \frac{(t - \alpha_1)^{k_1} \cdot \dots \cdot (t - \alpha_m)^{k_m}}{(t - \beta_1)^{s_1} \cdot \dots \cdot (t - \beta_n)^{s_n}}$$

и тогда мы имеем

$$v_\gamma(f) = \begin{cases} 0, & \gamma \neq \alpha_j, \beta_j \\ k_i & \gamma = \alpha_i \\ s_j, & \gamma = \beta_j \end{cases}, \quad v_\infty = s_1 + \dots + s_n - k_1 - \dots - k_m.$$

В частности мы видим, что

$$\forall f \in \mathbb{k}(\mathbb{P}^1) \quad \sum_{P \in \mathbb{P}^1} v_P(f) = 0.$$

Это наблюдение можно обобщить на произвольную неособую проективную кривую X .

Предложение 26. Все нормирования на $\mathbb{k}(t)$, тривиальные на \mathbb{k} , имеют такой вид.

Доказательство. Пусть v — нормирование на $\mathbb{k}(t)$. Выберем $f \in \mathbb{k}(X)$ такой, что $v(f) \neq 0$, и разложим f на неприводимые: $f = (t - \alpha_1)^{n_1} \cdot \dots \cdot (t - \alpha_n)^{n_k}$, где $n_1, \dots, n_k \in \mathbb{Z}$. Так как $v(f) \neq 0$, то найдётся множитель $t - \alpha$ такой, что $v(t - \alpha) \neq 0$. В силу 28, $v(t - \beta) = \min\{v(t - \alpha), 0\}$ для $\beta \neq \alpha$. Отсюда мы получаем все нормирования на $\mathbb{k}(t)$ — если $v(t - \alpha) > 0$, то будет нормирование в α , иначе нормирование на бесконечности. □

Пусть X — неособая проективная кривая (и в дальнейшем всегда так).

Определение 38. Дивизор на X — это формальная целочисленная линейная комбинация $\sum_{P \in X} n_P \cdot P$, где $n_P \in \mathbb{Z}$, и почти все из них равны нулю.

Иными словами, группа дивизоров $\text{Div}(X)$ на кривой X — это свободная абелева группа, порожденная точками кривой.

Рассмотрим произвольную рациональную функцию $f \in \mathbb{k}(X)^*$; в кольце \mathcal{O}_P она представима в виде $f = z_P^{v_P(f)} \cdot f_0$, где $(z_P) = \mathfrak{m}_P$ — локальный параметр, а $f_0 \in \mathcal{O}_P^*$ (так как кривая неособая и локальное кольцо каждой точки регулярно).

Определение 39. Пусть $f \in \mathbb{k}(X)^*$ — ненулевая рациональная функция на кривой X . Её *дивизором* называют

$$\operatorname{div}(f) = \sum_{p \in X} v_p(f) \cdot p$$

А *дивизором нулей* и *дивизором полюсов* называют соответственно

$$\operatorname{div}(f)_0 = \sum_{p \in X, v_p(f) > 0} v_p(f) \cdot p, \quad \operatorname{div}(f)_\infty = - \sum_{p \in X, v_p(f) < 0} v_p(f) \cdot p.$$

Замечание 29. Нетрудно видеть, что $\operatorname{div}(f)_\infty = \operatorname{div}(1/f)_0$ и $\operatorname{div}(f) = \operatorname{div}(f)_0 - \operatorname{div}(f)_\infty$.

Замечание 30. Определение корректно, то есть в суммах конечное число ненулевых слагаемых. Проверим это: пусть $U \subset X$ — область регулярности f . Множество нулей $\{f = 0\}$ замкнуто внутри U , значит, оно разбивается на конечное множество неприводимых компонент. Так как $f \neq 0$, то $\dim\{f = 0\} < 1$, и неприводимые компоненты — точки. Тем самым, сумма в определении дивизора нулей действительно конечна. Аналогично поступаем с суммой в определении дивизора полюсов.

Определение 40. Степенью $\deg D$ дивизора D называется сумма его кратностей.

Пример 13. Пусть X — неособая неприводимая проективная кривая, $f \in \mathbb{k}(X)^*$. Рассмотрим морфизм полей $\mathbb{k}(t) \rightarrow \mathbb{k}(X)$, $t \mapsto f$. Ему соответствует некоторое доминантное рациональное отображение $X \rightarrow \mathbb{P}^1$. Мы доказывали в 25, что это отображение будет регулярным во всех точках. Рассмотрим точку $P = 0 \in \mathbb{P}^1$ и $Q_i \in X$ такие, что $Q_i \mapsto P$ (то есть $f(Q_i) = 0$). Тогда $v_{Q_i}(f) = e_i v_P(t) = e_i$. В силу 19,

$$\sum_i e_i = [\mathbb{k}(X) : \mathbb{k}(f)].$$

С другой стороны, $\{Q_i\} = \{Q \in X \mid v_Q(f) > 0\}$, то есть дивизор нулей функции f имеет вид

$$\sum v_{Q_i}(f) \cdot Q_i,$$

откуда мы в частности получаем, что $\deg(\operatorname{div}(f)_0) = [\mathbb{k}(X) : \mathbb{k}(f)]$.

Предложение 27. Пусть X — неособая проективная неприводимая кривая, $f \in \mathbb{k}(X)^\times$. Тогда $\operatorname{div}(f)$ — главный, то есть $\deg(\operatorname{div}(f)_0) = \deg(\operatorname{div}(f)_\infty)$.

Доказательство. Согласно примеру выше, $\deg(\operatorname{div}(f)_0) = [\mathbb{k}(X) : \mathbb{k}(f)]$. Аналогично $\deg(\operatorname{div}(f)_\infty) = \deg(\operatorname{div}(1/f)_0) = [\mathbb{k}(X) : \mathbb{k}(1/f)] = [\mathbb{k}(X) : \mathbb{k}(f)]$. \square

Доказательство выше использует недоказанную¹⁸ теорему 19, опирающуюся на сложную технику конечных морфизмов, и в связи с этим в следующем семестре лектор приводит другое доказательство. Его можно найти в приложении 5.

Ясно, что $\operatorname{div}(fg) = \operatorname{div}(f) + \operatorname{div}(g)$, в связи с чём главные дивизоры образуют подгруппу $\operatorname{PDiv}(X)$ в группе всех дивизоров $\operatorname{Div}(X)$. Факторгруппу $\operatorname{Div}(X)/\operatorname{PDiv}(X)$ называют *группой классов дивизоров*, и обозначают $\operatorname{Cl}(X)$.

¹⁸насколько редактор понимает

Пример 14. Пусть X — проективная неособая неприводимая кривая. Отображение степени $\deg : \text{Div}(X) \rightarrow \mathbb{Z}$ пропускается через фактор, так как все главные дивизоры имеют степень 0.

В случае $X = \mathbb{P}^1$ это оказывается изоморфизмом (то есть $\deg : \text{Cl}(X) \xrightarrow{\sim} \mathbb{Z}$), что ясно из явного вида нормирований на $\mathbb{k}(t)$.

Пусть X — неособое неприводимое многообразие, $C \subset X$ — неприводимое подмногообразие коразмерности 1. Можно определить локальное кольцо по отношению к C (по аналогии с локальным кольцом точки):

$$\mathcal{O}_C \subset \mathbb{k}(X), \quad \mathcal{O}_C = \left\{ \frac{f}{g} \mid g|_C \neq 0 \right\}.$$

Тут мы подразумеваем, что g не обращается **тождественно** в 0 на C . Видно, что в случае одноточечного $C = P$ это определение совпадает с определением локального кольца точки.

Предположим, что X — аффинное многообразие с аффинной алгеброй $A = A(X)$. В этом случае подмногообразие C соответствует некоторому простому идеалу $\mathfrak{p} \subset A$ высоты 1. Тогда $\mathcal{O}_C = A_{\mathfrak{p}}$ (тот факт, что знаменатель не обращается тождественно в 0 на C , означает как раз, что он не лежит в идеале \mathfrak{p}).

Теперь возьмём $\mathfrak{p} \subset \mathfrak{m} \subset A$. Максимальный идеал \mathfrak{m} соответствует какой-то точке C и ясно, что $A_{\mathfrak{p}}$ получается локализацией кольца $A_{\mathfrak{m}}$. X неособое, так что $A_{\mathfrak{m}}$ регулярно. Идеал $\mathfrak{p}A_{\mathfrak{m}}$ — высоты 1. Регулярное локальное кольцо факториально¹⁹, а в факториальном локальном кольце простой идеал высоты 1 является главным: 1. Значит, $\mathfrak{p}A_{\mathfrak{m}}$ — главный идеал, тогда $\mathfrak{p}A_{\mathfrak{p}}$ — главный, а это говорит нам, что кольцо $A_{\mathfrak{p}}$ является дискретно нормированным.

Дальше всё некоторое время идёт по аналогии с одномерным случаем кривой.

Определение 41. Пусть X — неособое многообразие. Тогда *группа дивизоров* $\text{Div}(X)$ — свободная абелева группа, образующими которой являются неособые подмногообразия размерности 1.

Пусть $D \in \text{Div}(X)$ — дивизор, $D = \sum_{Z \subset X} n_Z \cdot Z$. Его *носителем* мы будем называть

$$\text{supp } D = \bigcup_{Z \subset X: n_Z \neq 0} Z.$$

Определение 42. Пусть $f \in \mathbb{k}(X)^*$. Тогда её *дивизором* мы будем называть

$$\text{div}(f) = \sum_{C \subset X, \text{codim } C=1} v_C(f) \cdot C$$

где сумма идёт по всем неприводимым C . Дивизоры такого вида мы будем называть *главными*. Нетрудно заметить, что они образуют подгруппу в $\text{Div}(X)$, её мы обозначим через $\text{PDiv}(X)$.

Замечание 31. Это определение корректно, так как для заданной функции $f \in \mathbb{k}(X)$ существует лишь конечное число неособых неприводимых подмногообразий C коразмерности таких, что $v_C(f) > 0$.

Рассмотрим сначала случай, когда X аффинно и $f \in A(X)$. В таком случае, просто по определению, если C не является компонентой $Z(f)$, то $v_C(f) = 0$. Покажем, что таких C , что $v_C(f) > 0$ конечное число. Пусть C соответствует идеалу \mathfrak{p} высоты 1, тогда

$$v_C(f) > 0 \iff f \in \mathfrak{p}.$$

¹⁹что мы не доказывали, но обсуждается в 18.

Рассмотрим $\mathfrak{p}/(f) \subset A/(f)$. Заметим, что если $\mathfrak{p}, \mathfrak{q} \trianglelefteq A$, причём $f \in \mathfrak{q}$, \mathfrak{p} и $\mathfrak{q} \neq \mathfrak{p}$, то $\mathfrak{p}/(f) \neq \mathfrak{q}/(f)$. Тогда нам достаточно доказать, что в $A/(f)$ конечное число минимальных простых идеалов (что правда в любом нётеровом кольце).

Если же X всё ещё аффинно, но $f \in \mathbb{k}(X)$, $f = g/h$, где $g, h \in A(X)$, то мы видим, что $v_C(f) = v_C(g) - v_C(h)$, и всё сводится к случаю $f \in A(X)$.

В произвольном случае мы покроем $X = \bigcup U_i$ аффинными (конечным числом) и всякое C пересекается хоть с одним из U_i . При этом пересечение имеет ту же размерность, что и C , так как оно — открытое подмножество C . Тем самым, дивизор функции опять же определён корректно.

Определение 43. Группой классов дивизоров мы будем называть группу $\text{Cl}(X) = \text{Div}(X)/\text{PDiv}(X)$.

Определение 44. Как и в случае кривых, степень $\deg D$ дивизора $D \in \text{Div}(X)$ называется сумма его кратностей.

Определение 45. Пусть Z — неприводимое неособое подмногообразие в X коразмерности 1. Тогда ему соответствует дивизор $1 \cdot Z$. Простыми мы будем называть дивизоры такого вида.

Пусть $U \subset X$ — открытое подмножество, $Z = X \setminus U$. Можно определить отображение

$$\text{Div}(X) \rightarrow \text{Div}(U).$$

Зададим его на образующих: пусть $T \subset X$ — простой дивизор, тогда если $T \cap U = \emptyset$, отправим его в 0, а если $T \cap U \neq \emptyset$, то $T \cap U$ — простой дивизор в U и мы отправим T в $T \cap U$. Отметим также, что с главными дивизорами при этом отображении происходит также понятная вещь:

$$\text{div}(f) \mapsto \text{div}(f|_U).$$

Значит, мы получили корректно определённое отображение $\text{Cl}(X) \rightarrow \text{Cl}(U)$. Заметим теперь, что так как отображение $\text{Div}(X) \twoheadrightarrow \text{Div}(U)$ сюръективно, отображение $\text{Cl}(X) \twoheadrightarrow \text{Cl}(U)$ также сюръективно. Вычислим его ядро. Предположим, что $\sum n_i Z_i \in \text{Ker}(\text{Cl}(X) \rightarrow \text{Cl}(U))$, это означает, что он перешёл в $\text{div}(f)$ для некоторой рациональной $f \in \mathbb{k}(U)$. Эту f можно рассматривать и как элемент $\mathbb{k}(X)$, то есть $\sum n_i Z_i - \text{div}(f) \mapsto 0$ при отображении $\text{Div}(X) \rightarrow \text{Div}(U)$. Но, если $Z_1 \cap U \neq \emptyset, Z_2 \cap U \neq \emptyset$, и оказалось, что $Z_1 \cap U \neq Z_2 \cap U$, то, конечно, $Z_1 = Z_2$. Отсюда следует, что ядро состоит из тех неприводимых подмногообразий коразмерности 1, которые не пересекаются с U . А это в точности неприводимые компоненты $Z = X \setminus U$ коразмерности 1 (в X).

Таким образом, $\text{Ker}(\text{Cl}(X) \twoheadrightarrow \text{Cl}(U)) = \mathbb{Z}^m$, где m — количество неприводимых компонент Z коразмерности 1 в X . В частности, у нас есть точная последовательность

$$\mathbb{Z}^m \rightarrow \text{Cl}(X) \rightarrow \text{Cl}(U) \rightarrow 0.$$

Пример 15. Это наблюдение уже позволяет вычислить группу классов дивизоров для чего-нибудь.

1. Рассмотрим $X = \mathbb{A}^n$ и простой дивизор $T \subset X$. Подмногообразия в \mathbb{A}^n коразмерности 1 соответствуют простым идеалам высоты 1 в факториальном кольце $\mathbb{k}[x_1, \dots, x_n]$, согласно 1, эти идеалы главные. Таким образом, T задаётся одним уравнением: $T = Z(f)$, но тогда $T = \text{div}(f)$ и T главный. Значит, все простые дивизоры главные, откуда следует, что $\text{Cl}(\mathbb{A}^n) = 0$.

2. Теперь рассмотрим $X = \mathbb{P}^n$ и $U = \mathbb{A}^n$, Тогда, так как $X \setminus U = \mathbb{P}^{n-1}$, мы получаем

$$\mathbb{Z} \hookrightarrow \text{Cl } \mathbb{P}^n \rightarrow \text{Cl } \mathbb{A}^n \rightarrow 0,$$

а так как левое отображение инъективно (так как дивизор функции не может состоять только из $\mathbb{P}^n \setminus \mathbb{A}^n$: на \mathbb{A}^n регулярная функция без нулей постоянна)

$$0 \rightarrow \mathbb{Z} \rightarrow \text{Cl } \mathbb{P}^n \rightarrow \underbrace{\text{Cl } \mathbb{A}^n}_{=0} \rightarrow 0,$$

мы имеем $\text{Cl } \mathbb{P}^n \cong \mathbb{Z}$.

Определение 46. Дивизор называется *эффективным* или *неотрицательным*, если все его кратности неотрицательны. В таком случае мы пишем $D \geq 0$.

Замечание 32. Заметим, что если f регулярна, то $\text{div}(f) \geq 0$.

Оказывается, верно и обратное.

Теорема 23. Пусть X — неособое многообразие, $f \in \mathbb{k}(X)$, причём $\text{div}(f) \geq 0$. Тогда f регулярна на X .

Доказательство. Будем проверять регулярность f в каждой точке X . Без потери общности, X можно заменить на аффинную окрестность, пусть A — аффинное координатное кольцо X .

Выберем точку $P \in X$, которой соответствует идеал $\mathfrak{m} \trianglelefteq A$, и воспользуемся тем, что $\mathcal{O}_P = A_{\mathfrak{m}}$ факториально. В его поле частных $f = u \cdot \pi_1^{n_1} \cdot \dots \cdot \pi_k^{n_k}$, где $u \in \mathcal{O}_P^\times$ все $\pi_i \in \mathcal{O}_P$ неприводимы, а $n_i \in \mathbb{Z}$.

Убедимся, что все $n_j \geq 0$, зафиксируем некоторый $j = 1..k$. Так как π_j — неприводимый элемент $A_{\mathfrak{m}}$, то (π_j) — простой идеал высоты 1 в этом кольце. Он соответствует неприводимой компоненте X , содержащей точку P . Остальные $\pi_{j'}$ соответствуют другим неприводимым компонентам, и при локализации по идеалу (π_j) перейдёт в обратимые элементы. Тем самым, $v_{Z(\pi_j)}(f) = n_j$, и так как $\text{div}(f) \geq 0$, то $n_j \geq 0$. \square

Посчитаем группу классов дивизоров для некоторых произведений. Например, $\mathbb{A}^1 \times \mathbb{A}^1 \subset \mathbb{P}^1 \times \mathbb{A}^1$ — открытое подмногообразие. Значит, имеет место точная последовательность $\mathbb{Z} \rightarrow \text{Cl}(\mathbb{P}^1 \times \mathbb{A}^1) \rightarrow \text{Cl}(\mathbb{A}^1 \times \mathbb{A}^1) \rightarrow 0$.

Покажем, что левая стрелка всё-таки инъективна. Пусть $Z = (\mathbb{P}^1 \times \mathbb{A}^1) \setminus (\mathbb{A}^1 \times \mathbb{A}^1) = \text{pt} \times \mathbb{A}^1$, и пусть $Z \cdot n = \text{div}(f)$ для некоторой $f \in \mathbb{k}(\mathbb{P}^1 \times \mathbb{A}^1)$, $n \geq 0$. Тогда f регулярна (по только что доказанной теореме) на всём $\mathbb{P}^1 \times \mathbb{A}^1$.

Пусть $x \in \mathbb{A}^1$, положим $g_x(t) = f(t, x)$. Это регулярная функция $\mathbb{P}^1 \rightarrow \mathbb{k}$, значит, она постоянна, то есть $f(t, x) = h(x)$. Однако $f(t, x)|_{\text{pt} \times \mathbb{A}^1} = 0$, откуда $h = 0$. Тем самым, $\text{Cl}(\mathbb{P}^1 \times \mathbb{A}^1) = \mathbb{Z}$.

Аналогично можно вложить открыто $\mathbb{A}^1 \times \mathbb{P}^1 \rightarrow \mathbb{P}^1 \times \mathbb{P}^1$. На $\mathbb{P}^1 \times \mathbb{P}^1$ тоже нет регулярных функций, значит, $\text{Cl}(\mathbb{P}^1 \times \mathbb{P}^1) = \mathbb{Z} \oplus \mathbb{Z}$.

4.2 Дивизоры форм

Пусть $X \subset \mathbb{P}^N$ — многообразие, F — форма (однородный многочлен). Определим дивизор формы F .

Рассмотрим неприводимое подмногообразие $C \subset X$ коразмерности 1. Выберем форму G той же степени, что и F так, чтоб $G|_C \neq 0$ (т.е. не обращается в 0 полностью). Рассмотрим функцию F/G (так как это частное двух форм, это функция) и положим

$$v_C(F) \stackrel{\text{def}}{=} v_C\left(\frac{F}{G}\right).$$

Замечание 33. Покажем, что это определение корректно. Возьмём две формы G_1 и G_2 , удовлетворяющие этим условиям, тогда

$$v_C\left(\frac{F}{G_2}\right) = v_C\left(\frac{F}{G_1}\right) + v_C\left(\frac{G_1}{G_2}\right), \text{ но } v_C\left(\frac{G_1}{G_2}\right) = 0,$$

откуда мы получаем нужное.

Определим *дивизор формы F* как

$$\text{div}(F) = \sum_{C \subset X} v_C(F) \cdot C,$$

где сумма, как и ранее, берётся по всем неприводимым подмногообразиям коразмерности 1. В качестве упражнения читателям остаётся убедиться, что эта сумма финитна, как и раньше.

Пусть теперь X кривая. Тогда мы можем определить *степень дивизора* формы F следующим образом:

$$\deg \text{div}(F) = \sum_{C \subset X} v_C(F).$$

Рассмотрим две формы F_1, F_2 такие, что $\deg F_1 = \deg F_2$. У нас есть очевидное равенство

$$\text{div}(F_1) = \text{div}(F_2) + \text{div}\left(\frac{F_1}{F_2}\right),$$

и применяя степень мы получаем, что

$$\deg \text{div}(F_1) = \deg \text{div}(F_2).$$

Это позволяет построить отображение $\mathbb{Z} \rightarrow \text{Cl}(X)$, отправляющее в $n \mapsto \text{div}(F)$, где F — произвольная форма степени n . Так как отображение стреляет в $\text{Cl}(X)$, то есть дивизоры функций нулевые, это определение корректно.

4.3 Дивизоры на эллиптических кривых.

Для иллюстрации вычислим дивизор линейной формы на эллиптической кривой.

Эллиптическая кривая задаётся уравнением

$$y^2 = x^3 + ax + b, \quad a, b \neq 0, \quad 4a^3 + 27b^3 \neq 0.$$

Приравняв обе производные по x и по y к нулю, и решая полученную систему, несложно убедиться, что эта кривая неособая.

Можно рассмотреть точку $P(x_1, y_1) \in C$ и вычислить локальный параметр для кольца \mathcal{O}_P (то есть образующую максимального идеала \mathfrak{m}_P). Для этого надо рассмотреть следующие два случая²⁰

²⁰Но вообще данные выкладки нам не пригодятся, будет достаточно лишь то, что локальные кольца регулярны, в чём мы уже убедились, дифференцируя.

1. Пусть $y_1 \neq 0$. Тогда покажем, что $x - x_1$ — локальный параметр для кольца \mathcal{O}_P . Ясно, что $\mathfrak{m}_P = (x - x_1, y - y_1)$. Попробуем получить одну образующую вместо двух.

$$\begin{cases} y^2 = x^3 + ax + b \\ y_1^2 = x_1^3 + ax_1 + b \end{cases} \implies (y - y_1)(y + y_1) = (x - x_1)(x^2 + xx_1 + x_1^2 + a)$$

$$y - y_1 = \frac{(x - x_1)(x^2 + xx_1 + x_1^2 + a)}{y + y_1}.$$

Тогда достаточно показать, что $y + y_1 \notin \mathfrak{m}_P$. Действительно, если $y + y_1 \in \mathfrak{m}_P$, тогда $y_1 \in \mathfrak{m}_P$, а это возможно тогда и только тогда, когда $y_1 = 0$ (а мы предположили, что это не так).

2. Пусть $y_1 = 0$, тогда локальным параметром будет y .

$$x_1^3 + ax_1 + b = 0 \implies y^2 = (x - x_1)(x^2 + xx_1 + x_1^2 + a) \implies x - x_1 = \frac{y^2}{x^2 + xx_1 + x_1^2 + a}.$$

Покажем, что $x^2 + xx_1 + x_1^2 + a \notin \mathfrak{m}_P$.

$$x^2 + xx_1 + x_1^2 + a \equiv 3x_1^2 + a \pmod{\mathfrak{m}_P}.$$

То есть $3x_1^2 + a = 0$, $y_1 = 0$. Но это противоречит тому, что точка $P(x_1, y_1)$ неособая, а именно, тому, что у уравнения $x^3 + ax + b$ нет кратных корней. В самом деле, если $3x_1^2 + a = 0$ выполняется вместе с $x_1^3 + ax_1 + b = 0$, то есть многочлен зануляется вместе со своей производной, то корень не простой, а с кратностью.

Вычислим степень дивизора линейной формы. Оказывается, что удобнее всего пересекать эллиптическую кривую с бесконечно удалённой прямой, так что проективизируем её. Уравнение проективизации

$$X: \{y^2z = x^3 + axz^2 + bz^3\},$$

и бесконечно удалённая точка соответствует $z = 0$. Такая одна — с координатами $(0 : 1 : 0)$.

Через эту точку проходит прямая $z = 0$, которая и есть та пресловутая бесконечно удалённая прямая. Пересечение с ней всего одно — точка P_0 , и чтобы найти дивизор бесконечно удалённой прямой, надо всего лишь посчитать кратность точки P_0 в этом пересечении.

Будем действовать по определению: чтобы найти дивизор формы, надо превратить эту форму в функцию, деля на другую форму, ненулевую в рассматриваемой точке. В нашем случае, конечно, делить будем на y . Для вычисления дивизора функции $\frac{z}{y}$, поделим уравнение кривой на y^3 , получая

$$\frac{z}{y} = \left(\frac{x}{y}\right)^3 + a\frac{x}{y}\left(\frac{z}{y}\right)^2 + b\left(\frac{z}{y}\right)^3.$$

Обозначим $x/y = x_1$, $z/y = z_1$. В них

$$z_1 = x_1^3 + ax_1z_1^2 + bz_1^3,$$

а P_0 имеет координаты $(0, 0)$. Производная по z_1 в этой точке ненулевая, то есть, точка неособая (это важно, ведь почти все результаты мы доказывали для неособых кривых).

Локальный параметр здесь — x_1 , так как можно выразить

$$z_1 = \frac{x_1^3}{1 - bz_1^2 - ax_1z_1}$$

где числитель — единица по модулю \mathfrak{m}_{P_0} , то есть обратим в \mathcal{O}_{P_0} .

Итак, функция z_1 имеет кратность 3 в точке P_0 , что и следовало ожидать — уравнение эллиптической кривой имеет степень 3.

Тем самым, дивизор любой другой линейной формы F на данной кривой будет тоже равен 3. В частности, если прямая $F = 0$ пересекает эллиптическую кривую в трёх точках, то дивизор соответствующей формы будет просто суммой этих точек — нужно назначить трём точкам положительные целые кратности так, чтобы сумма была равна трём, и науке известен всего один способ сделать это.

4.4 Групповой закон для точек эллиптической кривой

Пусть X — неособая проективная кривая. Мы знаем, что в этом случае любой главный дивизор имеет степень 0, а значит, мы можем рассмотреть отображение

$$\mathrm{Cl}(X) \xrightarrow{\deg} \mathbb{Z} \rightarrow 0$$

и, обозначая его ядро через $\mathrm{Cl}^0(X)$ написать короткую точную последовательность

$$0 \rightarrow \mathrm{Cl}^0(X) \rightarrow \mathrm{Cl}(X) \xrightarrow{\deg} \mathbb{Z} \rightarrow 0$$

Пусть $X \subset \mathbb{P}^2$ — эллиптическая кривая $y^2z = x^3 + axz^2 + bz^3$, рассмотрим отображение

$$\varphi: X \rightarrow \mathrm{Cl}^0(X), \quad P \mapsto [P] - [P_0],$$

где P_0 — это бесконечно удалённая точка²¹. Посредством этого отображения хочется определить сложение точек на эллиптической кривой, перенося структуру абелевой группы с $\mathrm{Cl}^0(X)$ на саму кривую X . Для этого надо проверить, что φ — биекция.

Теорема 24. *Отображение $\varphi: X \rightarrow \mathrm{Cl}^0(X)$, $P \mapsto [P] - [P_0]$ взаимно однозначно.*

Доказательство. Докажем сначала вот такую лемму:

Лемма 12. Пусть X — неособая проективная кривая, на которой есть две различные точки $P \neq Q$ такие, что $(P - Q)$ — главный дивизор. Тогда $X = \mathbb{P}^1$.

Доказательство. Пусть $P - Q = \mathrm{div}(f)$. Но тогда $P = \mathrm{div}(f)_0$, $\mathrm{div}(f)_\infty = Q$. Рассмотрим отображение $X \rightarrow \mathbb{P}^1$, которое даёт нам расширение полей $t \mapsto f$, $\mathbb{k}(X)/\mathbb{k}(f)$ и при этом $[\mathbb{k}(X) : \mathbb{k}(f)] = \deg \mathrm{div}(f)_0 = 1$. Оно влечёт $\mathbb{k}(X) = \mathbb{k}(f) = \mathbb{k}(t)$, то есть X — рациональная кривая. \square

²¹Точки в группе классов дивизоров мы вдруг стали брать в квадратные скобки, потому что на самой кривой появилось сложение, и не хочется их перепутать.

Так как мы доказывали, что эллиптическая кривая рационально не изоморфна \mathbb{P}^1 , то отсюда следует инъективность отображения:

Инъективность. Предположим, что $[P] - [P_0] = [Q] - [P_0]$ в $\text{Cl}^0(X)$. Тогда $[P] - [Q] = 0$, то есть $P - Q$ — главный дивизор. По доказанной лемме имеет место бирациональный изоморфизм $X \cong \mathbb{P}^1$ и мы пришли к противоречию.

Сюръективность. Рассмотрим $\sum n_i [P_i] \in \text{Cl}^0(X)$. Так как сумма коэффициентов равна нулю,

$$\sum n_i [P_i] = \sum n_i ([P_i] - [P_0])$$

Будем доказывать, что для любых $n_i \in \mathbb{Z}$

$$\sum n_i ([P_i] - [P_0]) = [S] - [P_0] \in \text{Cl}^0(X) \quad (\text{divisor})$$

для некоторой $S \in X$. Сначала покажем, что можно считать, что все $n_i > 0$. Пусть некоторый $n_i < 0$, то есть в сумму входит $[P_0] - [P_i]$ с положительным коэффициентом. Проведём вертикальную прямую $x = \text{const}$ через точку P_i на эллиптической кривой. Ей соответствует форма $x - \text{const} \cdot z$, которая пересечёт кривую в точке P_i , в бесконечно удалённой точке, и ещё в точке, симметричной точке P_i относительно оси абсцисс, назовём её P'_i . Получается, в $\text{Cl}^0(X)$ имеет место равенство

$$[P_i] + [P'_i] + [P_0] = 3[P_0]$$

из которого следует $[P_0] - [P_i] = [P'_i] - [P_0]$. Получается, можно привести дивизор (??) к виду, где все $n_i > 0$, не меняя при этом сумму модулей n_i .

Теперь рассмотрим дивизор

$$[P_1] - [P_0] + [P_2] - [P_0] \quad (6)$$

Проведём прямую через точки P_1 и P_2 ²², то есть найдём форму, обнуляющуюся в этих точках. Её дивизор имеет степень 3, то есть равен $[P_1] + [P_2] + [P_3]$ для некоторой третьей точки $P_3 \in X$. Получается,

$$[P_1] + [P_2] + [P_3] = 3[P_0] \text{ в } \text{Cl}(X),$$

и дивизор $([P_1] - [P_0]) + ([P_2] - [P_0])$ оказался равен дивизору $([P_0] - [P_3])$. С отрицательными кратностями мы уже поборолись раньше. Таким образом, дивизор в конце концов приводится к виду $[S] - [P_0]$, чем доказывается сюръективность. \square

Немного порефлексируем над тем, что мы доказали.

Чтобы сложить две точки $P, Q \in X$ на эллиптической кривой, мы пишем дивизор $([P] - [P_0]) + ([Q] - [P_0])$, и, проводя прямую через P и Q , находим точку R , такую, что дивизор равен $[P_0] - [R]$. Дальше R отражается относительно оси абсцисс, и получается $[R'] - [P_0]$.

Тем самым, точки на эллиптической кривой можно складывать так: для точек $P_1, P_2 \in X$, рассмотрим прямую, проходящую через них. Эта прямая пересечёт эллиптическую кривую в третьей точке, её мы симметрично отразим относительно оси абсцисс и объявим результатом сложения то, что получилось. Однако проверить ассоциативность данного определения весьма непросто, а наш подход позволяет это увидеть сразу.

²²В случае $P_1 = P_2$ подойдёт касательная, но нужны дополнительные слова, почему это так.

Замечание 34. Пусть $U \subset X$ — аффинная часть эллиптической кривой. Имеет место точная последовательность

$$\mathbb{Z} \rightarrow \mathrm{Cl} X \rightarrow \mathrm{Cl} U \rightarrow 0$$

и как мы только что убедились, $\mathrm{card}(\mathrm{Cl} X) = \mathrm{card}(X) = \mathrm{card}(\mathbb{k})$. Несложно проверить, что от выкидывания одной точки ничего не поменяется, то есть $\mathrm{card}(\mathrm{Cl} U) = |\mathbb{k}|$, а аффинное координатное кольцо $A(U)$ получилось дедекиндовым кольцом со сколь угодно большой по мощности группой классов. Где вы ещё такое увидите?

5 Приложение: альтернативное доказательство того, что степень главного дивизора равна нулю

Данный вариант доказательства был прочитан в следующем семестре, и включён в данный конспект просто по приколу.

5.1 План доказательства

Пусть X — неособая неприводимая проективная кривая, $f \in \mathbb{k}(X)^*$, и предположим, что $f \notin \mathbb{k}$ (случай $f \in \mathbb{k}$ неинтересен, там $\operatorname{div}(f) = 0$).

Разложим дивизор f в сумму дивизоров нулей и полюсов:

$$\operatorname{div}(f) = \sum_{P \in X, v_P(f) > 0} v_P(f) \cdot P + \sum_{P \in X, v_P(f) < 0} v_P(f) \cdot P.$$

Пусть $0 = Q \in \mathbb{P}^1$, заметим, что $\{P \in X \mid v_P(f) > 0\} = \{P \in X \mid f(x) = 0\} = f^{-1}(Q)$. Более того, несложно в аналогичных терминах выразить нормирования $v_P(f)$. Дело в том, что нормирования v_P на X продолжают нормирование v_Q на \mathbb{P}^1 , о чём немножко говорится здесь 3.4, откуда $v_P(f) = e(P/Q) \cdot \underbrace{v_Q(t)}_1$, где $t \in \mathbb{k}(\mathbb{P}^1)$ — рациональная функция координаты.

В дальнейшем мы стремимся доказать, что

$$\sum_{P \in f^{-1}(Q)} e(P/Q) = [\mathbb{k}(X) : \mathbb{k}(f)].$$

Как только мы это докажем, станет понятно, что дивизор функции — главный, так как слева в равенстве стоит $\deg \operatorname{div}(f)_0$. По той же причине окажется, что $\deg \operatorname{div}(f)_\infty = \deg \operatorname{div}(1/f)_0 = [\mathbb{k}(X) : \mathbb{k}(1/f)] = [\mathbb{k}(X) : \mathbb{k}(f)]$, а то, что степени дивизоров нулей и полюсов совпадают как раз и является тем, что мы хотим доказать.

5.2 Аппроксимационная теорема. Оценка в одну сторону

Пусть K — поле.

Определение 47. Сюръективный гомоморфизм абелевых групп $v : K^\times \rightarrow \mathbb{Z}$ называют *нормированием* на K , если $\forall f, g \in K^\times : v(f+g) \geq \min\{v(f), v(g)\}$.

Если вдруг оказалось, что $f+g=0$, то нельзя говорить о $v(f+g)$; удобно определить $v(0) = \infty$, в таком случае формула останется верной.

Предложение 28. Пусть $f, g \in K, v(f) \neq v(g)$. Тогда $v(f+g) = \min\{v(f), v(g)\}$.

Доказательство. Ясно, что $v(-1) = 0$, так как -1 имеет конечный порядок в K^\times , откуда $\forall h \in K : v(h) = v(-h)$.

Без потери общности $v(f) < v(g)$. Предположим противное: $v(f+g) > v(f)$. Запишем $v(f) = v((f+g) - g) \geq \min\{v(f+g), v(g)\} > v(f)$, получая противоречие. \square

Определение 48. Элемент $x \in K^\times$ имеет нуль в v , если $v(x) > 0$.

Определение 49. Элемент $x \in K^\times$ имеет полюс в v , если $v(x) < 0$.

Предложение 29. Пусть K — поле, и v_1, \dots, v_n — различные нормирования на K . Тогда $\exists x \in K$: x имеет нуль в v_1 , и полюса в остальных нормированиях.

Доказательство. Пусть сначала $n = 2$. Так как нормирования различны, то $\mathcal{O}_{v_1} \neq \mathcal{O}_{v_2}$, тем самым, $\exists y \in \mathcal{O}_{v_1} \setminus \mathcal{O}_{v_2}$, $z \in \mathcal{O}_{v_2} \setminus \mathcal{O}_{v_1}$. Легко проверить, что $x := \frac{y}{z}$ подходит.

Теперь докажем общий случай по индукции. Согласно индукционному предположению, $\exists y, z \in K^\times$ такие, что y имеет нуль в v_1 , и полюса в v_2, \dots, v_{n-1} , а z имеет нуль в v_1 , и полюс в v_n .

Пусть $m \in \mathbb{N}$, утверждается, что $x := y + z^m$ подойдёт при достаточно больших m . В самом деле $v_1(y + z^m) \geq \min\{v_1(y), m \cdot v_1(z)\} > 0$, и $v_k(y + z^m) \geq \min\{v_k(y), m \cdot v_k(z)\}$, причём равенство достигается в случае $v_k(y) \neq m \cdot v_k(z)$. Понятно, что при достаточно больших m будет именно этот случай. \square

Следствие 14. Рассмотрим элемент $z := \frac{1}{1+x^k}$. Это такой элемент, что z имеет нуль порядка хотя бы k в нормированиях v_2, \dots, v_n , и $z - 1$ имеет нуль порядка хотя бы k в v_1 .

Следствие 15. Пусть $a_1, \dots, a_m \in K$, $N \in \mathbb{N}$. Тогда $\exists y \in K$: $v_i(y - a_i) \geq N$.

Доказательство. Для каждого $i = 1..m$ выберем свой z_i так, что $v_i(z_i - 1) \geq N$, и $v_j(z_i) \geq N$.

Теперь $y := \sum_{i=1}^m a_i z_i$ подойдёт. \square

Следствие 16 (Аппроксимационная теорема). Пусть $n_1, \dots, n_m \in \mathbb{Z}$ — целые числа, v_1, \dots, v_m — различные нормирования на K . Тогда $\exists x \in K^\times$: $v_i(x) = n_i$.

Доказательство. Выберем a_i так, что $v_i(a_i) = n_i$, и применим предыдущее следствие для $N > n_1, \dots, n_m$. Так как $v_i(y - a_i) > v_i(a_i)$, то согласно 28, $v_i(a_i) = v_i(y)$. \square

Пусть E/K — конечное расширение полей, v — нормирование на K , w — нормирование на E .

Определение 50. Говорят, что w *продолжает* нормирование v , если существует $e \in \mathbb{N}$, называемое *индексом ветвления*, такое, что $\forall x \in K^\times$: $w(x) = e \cdot v(x)$.

Теорема 25. Пусть E/K — конечное расширение полей, v — нормирование на K , нормирования w_1, \dots, w_m на E различны и продолжают v , а соответствующие индексы ветвления равны e_1, \dots, e_m . Тогда $e_1 + \dots + e_m \leq [E : K]$; в частности, возможных продолжений лишь конечное число.

Доказательство. Согласно аппроксимационной теореме, для каждого $i = 1..m$ можно выбрать $\pi_i \in E$ так, что $w_i(\pi_i) = 1$, $w_j(\pi_i) > e_j$.

Утверждается, что система $\bigsqcup_{i=1}^m \{\pi_i^1, \dots, \pi_i^{e_i}\}$ из $e_1 + \dots + e_m$ элементов линейно независима над K . Ясно, что для доказательства теоремы достаточно это проверить.

Пойдём от противного: пусть есть линейная зависимость вида $\sum_{i=1}^m \sum_{j=1}^{e_i} a_{ij} \pi_i^j = 0$, где $a_{ij} \in K$ не все равны нулю. Так как a_{ij} можно одновременно домножать на любой элемент поля, то можно считать, что все ненулевые a_{ij} таковы, что $v(a_{ij}) \geq 0$, причём (без потери общности) $w(a_{1t}) = 0$, и t выбрано минимально возможным.

Переносим $a_{1t}e_1^t$ в правую часть равенства, получаем

$$\sum_{i=2}^m \sum_{j=1}^{e_i} a_{ij} \pi_i^j + \sum_{\substack{j=1..e_1 \\ j \neq t}} a_{1j} e_1^j = a_{1t} e_1^t$$

Применяя w_1 к данному равенству, получаем противоречие — нормирование правой части равно $w_1(e_1^t) = t$, а нормирование суммы в левой части не меньше минимума нормирований слагаемых. Для $i > 1$: $w_1(a_{ij} \pi_i^j) \geq j w_1(\pi_i) > e_1$, а для $i = 1$ пишется следующая оценка:

$$w_1(a_{1j} \pi_1^j) = e_1 \cdot v(a_{1j}) + j \cdot \underbrace{w_1(\pi_1)}_1,$$

что при $j < t$ хотя бы $e_1 + j > e_1 \geq t$, а при $j > t$ — хотя бы $j > t$. \square

Следствие 17. В ситуации вложения полей, осуществляемого рациональной функцией f , получается

$$\sum_{P \in f^{-1}(Q)} e(P/Q) \leq [\mathbb{k}(X) : \mathbb{k}(f)],$$

так как ясно, что нормирования, отвечающие различным точкам X , различны.

5.3 Пространство функций, ассоциированное с дивизором. Оценка в другую сторону

Пусть $D \in \text{Div}(X)$ — произвольный дивизор на проективной неособой неприводимой кривой X .

Определение 51. Говорят, что D неотрицательный, если он имеет вид $\sum_P n_P \cdot P$ для некоторых $n_P \geq 0$. Пишут $D \geq 0$.

Введём пространство функций, ассоциированное с дивизором

$$\mathcal{L}(D) \stackrel{\text{def}}{=} \{f \in \mathbb{k}(X)^\times \mid \text{div}(f) + D \geq 0\} \cup \{0\}.$$

Несложно проверить, что $\mathcal{L}(D)$ замкнуто относительно сложения и умножения на скаляр из \mathbb{k} . В самом деле, если $f, g \in \mathcal{L}(D)$, то проверка того, что $f + g \in \mathcal{L}(D)$, поточечна:

$$\forall P \in X : \begin{cases} v_P(f) + n_P \geq 0 \\ v_P(g) + n_P \geq 0 \end{cases} \Rightarrow \min\{v_P(f), v_P(g)\} + n_P \geq 0.$$

Теорема 26. Пространство $\mathcal{L}(D)$ конечномерно над \mathbb{k} . Обозначим $l(D) := \dim_{\mathbb{k}} \mathcal{L}(D) < \infty$. Помимо этого, утверждается, что $l(D) \leq \deg D + 1$, если $D \geq 0$.

Доказательство. Без потери общности $D \geq 0$ — в противном случае надо доказать лишь конечномерность, и понятно, что $\mathcal{L}(D) \subset \mathcal{L}(D_+)^{23}$, так что можно заменить D на D_+ .

²³Пусть $D = \sum n_P \cdot P$, тогда $D_+ \stackrel{\text{def}}{=} \sum \max\{n_P, 0\} \cdot P$.

Будем действовать по индукции по $\deg D$. База — нулевой дивизор $D = 0$. В таком случае $\mathcal{L}(D)$ — регулярные везде на X функции. Согласно 7, это только константы, откуда действительно $l(D) = 1 \leq \deg D + 1$.

Теперь совершим переход. $D \neq 0$, значит, существует точка $x \in \operatorname{supp} D \stackrel{\text{def}}{=} \{x \in X | n_x \neq 0\}$. Можно записать $D = r \cdot x + D_1$, где $x \notin \operatorname{supp} D_1$; обозначим $D' = (r - 1) \cdot x + D_1$. Пусть t — локальный параметр в точке x , то есть $\mathfrak{m}_x = (t)$.

Устроим линейное отображение $\mathcal{L}(D) \rightarrow \mathbb{k}, f \mapsto (t^r f)(x)$. Не факт, что оно сюръективно, но определено оно корректно, и его ядро равно $\mathcal{L}(D')$. По индукционному предположению $\dim \mathcal{L}(D') \leq \deg D$, и по теореме о размерности ядра и образа всё получается. \square

Замечание 35. Предположим, что равенство $\deg \operatorname{div}(f)_0 = [\mathbb{k}(X) : \mathbb{k}(f)]$ уже доказано. Рассмотрим точку $x \in X$, и соответствующий ей дивизор $D = x$.

Выберем $f \in \mathcal{L}(D)$ так, что $f \notin \mathbb{k}$. Если такая f нашлась, то $\deg \operatorname{div}(f)_\infty = 1$, откуда $[\mathbb{k}(X) : \mathbb{k}(1/f)] = 1$. Иными словами, $\mathbb{k}(X) = \mathbb{k}(1/f)$, или $\mathbb{k}(X)$ — чисто трансцендентное расширение X , значит, кривая X рациональна.

Но есть и нерациональные кривые, и для них получается, что $l(D) = 1$ при одноточечном $D = x$. Просматривая доказательство, видно, что в случае нерациональной кривой утверждение можно усилить: $l(D) \leq \max\{\deg D, 1\}$.

Итак, пусть $f \in \mathbb{k}(X)$, $f \notin \mathbb{k}$. Обозначим $n := [\mathbb{k}(X) : \mathbb{k}(f)]$, и выберем базис $\mathbb{k}(X)$ над $\mathbb{k}(f)$, пусть он называется z_1, \dots, z_n . Расширение $[\mathbb{k}(X) : \mathbb{k}(f)]$ алгебраично, откуда все z_i алгебраичны над $\mathbb{k}(f)$. Домножая их на подходящий элемент $\mathbb{k}(f)$, можем считать, что все z_i целы над $\mathbb{k}[f]$, то есть каждый z_i удовлетворяет полиномиальному уравнению вида

$$z_i^m + a_i \cdot z_i^{m-1} + \dots + a_0 = 0, \quad a_i \in \mathbb{k}[f].$$

Пусть в точке $P \in X$: $\operatorname{div}(z_i)$ имеет отрицательный коэффициент, то есть $v_P(z_i) < 0$. Предположение $v_P(f) \geq 0$ влечёт противоречие, так как в этом случае $v_P(a_i) \geq 0$, и v_P выдаёт разные результаты на левой и правой частях равенства $-z_i^m = a_i \cdot z_i^{m-1} + \dots + a_0$. Тем самым, $v_P(f) < 0$, и из финитности дивизора: $\exists N \in \mathbb{N} : \forall M > N : \operatorname{div}(z_i) + M \cdot \operatorname{div}(f)_\infty \geq 0$. Эту константу N можно выбрать универсально одной для всех z_i .

Осталось заметить, что $\bigsqcup_{i=1}^n \{z_i \cdot f^s\}_{s=1}^{M-N} \subset \mathcal{L}(M \cdot \operatorname{div}(f)_\infty)$. Все эти функции внутри $\mathbb{k}(X)$ являются \mathbb{k} -линейно независимыми, так как степени f^s независимы внутри $\mathbb{k}[f]$, а z_i — базис $\mathbb{k}(f)$ -векторного пространства.

В силу только что доказанной теоремы 26, $(M - N) \cdot n \leq M \cdot \deg \operatorname{div}(f)_\infty$. Деля на M , и устремляя его к бесконечности, мы получаем искомое $n \leq \deg \operatorname{div}(f)_\infty$.

6 Приложение: компендиум по коммутативной алгебре

В данном приложении собраны некоторые утверждения из коммутативной алгебры, на которые опирался курс.

Лемма Накаямы

Теорема 27 (Лемма Накаямы). Пусть M — конечно порождённый R -модуль, $I \trianglelefteq R$ — идеал. Предположим, что $M = IM$. Тогда $\exists a \in I : \forall t \in M \quad at = t$

Доказательство. $\text{id}_M(M) = IM \implies$, а значит, по теореме Гамильтона-Кэли $\exists p(t) = t^n + \alpha_{n-1}t^{n-1} + \dots + \alpha_0$, $\alpha_i \in I : p(\text{id}_M) = 0$. Тогда

$$\text{id}_M(1 + \alpha_{n-1} + \dots + \alpha_0) = 0 \implies \text{id}_M(-(\alpha_{n-1} + \dots + \alpha_0)) = 1.$$

Тогда $a = -(\alpha_{n-1} + \dots + \alpha_0)$ подходит. В самом деле,

$$at = \text{id}_M(t) = t \quad \forall t \in M.$$

□

Предложение 30. В частности, если A — локальное кольцо, $\mathfrak{m} \trianglelefteq A$ — максимальный идеал, а M — конечно порождённый A -модуль, то $\mathfrak{m}M = M \iff M = 0$.

Доказательство. Помимо того, что это прямое следствие предыдущего (с одной стороны, в локальном кольце $a - 1$ обратимо, с другой стороны $\forall t \in M : (a - 1)t = 0$), это можно доказывать и независимо.

А именно, пусть $M = \text{span}\{m_1, \dots, m_k\}$, где k выбрано наименьшим. Согласно посылке предложения, $m_1 \in \mathfrak{m} \cdot \text{span}\{m_1, \dots, m_k\}$, то есть $m_1 = \sum_{i=1}^k m_i \alpha_i$, где $\alpha_i \in \mathfrak{m}$. Отсюда $m_1(1 - \alpha_1) = \sum_{i=2}^k m_i \alpha_i$, и сокращая на $1 - \alpha_1$, получаем, что систему образующих модуля можно уменьшить.

□

Предложение 31. Пусть A — локальное кольцо, $\mathfrak{m} \trianglelefteq A$ — максимальный идеал, и имеется набор $x_i \in \mathfrak{m}$ таких, что $(\overline{x_1}, \dots, \overline{x_k}) = \mathfrak{m}/\mathfrak{m}^2$. Тогда $(x_1, \dots, x_k) = \mathfrak{m}$.

Доказательство. Рассмотрим модуль $M = \mathfrak{m}/(x_1, \dots, x_k)$. По лемме Накаямы

$$M = 0 \iff \mathfrak{m}M = M \iff \mathfrak{m}^2 + (x_1, \dots, x_k) = \mathfrak{m},$$

что как равносильно тому, что $(\overline{x_1}, \dots, \overline{x_k})$ — система образующих $\mathfrak{m}/\mathfrak{m}^2$.

□

Теорема о подъёме и теорема о спуске

Теорема 28 (О спуске). Пусть $A \subset B$ — целостные, включение — целое расширение колец, и A — целозамкнуто. Пусть $\mathfrak{q}_m \in \text{Spec } B$, $\mathfrak{p}_m \in \text{Spec } A$ — простые, причём $\mathfrak{q}_m \cap A = \mathfrak{p}_m$. Тогда для любой цепочки простых идеалов

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \dots \subset \mathfrak{p}_m \subset A$$

существует цепочка простых идеалов

$$\mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \dots \subset \mathfrak{q}_m \subset B : \mathfrak{q}_i \cap A = \mathfrak{p}_i.$$

Целые и конечные расширения

Теорема 29. Пусть $R \subset A$ — целое (конечное) включение колец, и $\varphi : R \rightarrow B$ — гомоморфизм колец. Тогда $B \rightarrow A \otimes_R B$ — тоже целое (конечное) включение колец.

- В частности, для всякой мультипликативной системы $S \subset A$: $S^{-1}R \subset S^{-1}A$ цело (конечно).
- В частности, для всякого идеала $I \trianglelefteq R$: гомоморфизм $R/I \rightarrow A/IA$ цел (конечен)²⁴.
- Как следствие предыдущего, для всякого идеала $I \trianglelefteq A$: $R/(I \cap R) \subset A/I$ цело (конечно).

Теорема 30. Пусть $R \subset A$ — целое (конечное) включение областей целостности. Тогда R поле если и только если A — поле.

Теорема 31 (Лемма Нётер о нормализации). Пусть B — конечно-порожденная \mathbb{k} -алгебра. Тогда B — конечное расширение кольца многочленов $\mathbb{k}[x_1, \dots, x_n]$ для некоторого n .

Теорема 32 (Сохранение размерности при целом расширении). Пусть $A \subset B$ — целое включение колец. Тогда $\dim A = \dim B$.

Теорема Гильберта о нулях

Теорема 33 (Теорема Гильберта о нулях, (strong) nullstellensatz). Пусть $\mathbb{k} = \mathbb{k}^{alg}$, $I \trianglelefteq F[t_1, \dots, t_n]$, а $f \in \mathbb{k}[x_1, \dots, x_n]$. Тогда $f(Z(I)) = 0 \Leftrightarrow f \in \sqrt{I}$. Иными словами, $I(Z(I)) = \sqrt{I}$.

Теорема 34 (Слабая теорема Гильберта о нулях, weak nullstellensatz). Пусть $\mathbb{k} = \mathbb{k}^{alg}$, $\mathfrak{m} \trianglelefteq F[t_1, \dots, t_n]$ — максимальный идеал. Тогда $\exists a_1, \dots, a_n \in \mathbb{k} : \mathfrak{m} = (x_1 - a_1, \dots, x_n - a_n)$.

Теория размерности.

Теорема 35 (Теорема Крулля о главных идеалах, hauptidealsatz). Пусть A — нётерово кольцо, а $f \in A$ — элемент, не являющийся ни делителем нуля, ни обратимым. Тогда высота каждого минимального простого идеала \mathfrak{p} , содержащего f равна 1. Т.е.

$$\forall \mathfrak{p} \in \text{Спец } A : (f) \subset \mathfrak{p} \quad \text{ht } \mathfrak{p} = 1.$$

²⁴В данном случае гомоморфизм $R/I \rightarrow A/IA$ не обязан быть инъективным, поэтому включение внезапно поменялось на морфизм. Суть та же — A/IA будет цело (конечно) над образом R/I внутри себя.