Лекция 1.

Понятие аффинного алгебраического многообразия. Словарь алгебра/геометрия: максимальный и простой спектры, теорема Гильберта о нулях, топология Зарисского. Кратные пересечения и результант.

Напомним, что *аффинное алгебраическое подмножество* n-мерного аффинного пространства $\mathbb{A}^n$ над полем k – это подмножество $V \subset \mathbb{A}^n$ общих нулей какого-то конечного набора полиномиальных фунцкий $f_1, \dots, f_m \in k[x_1, \dots, x_n]$ на $\mathbb{A}^n$. Аффинные алгебраические множества это базовый объект изучения алгебраической геометрии, но использовать буквально это определение неудобно. Во-первых, одно и то же со всех точек зрения множество может быть задано разными наборами уравнений. Во-вторых, конкретное вложение $V \to \mathbb{A}^n$ не очень существенно: мы видели на примерах, что разные подмножества разных пространств иногда можно естественным образом отождествить, так что по сути мы имеем один и тот же объект (самый очевидный пример – это просто координатная гиперплоскость в $\mathbb{A}^n$, которая с любой точки зрения есть ни что иное, как аффинное пространство меньшей размерности).

Для решения первой проблемы, вводят понятие идеала.

Определение 1.1. *Идеалом* $\mathfrak{a} \subset A$ (коммутативного) кольца A называется подмножество в A, замкнутое относительно сложения/вычитания и умножения на элементы A: если $f \in \mathfrak{a}$, $a \in A$, то $fa \in \mathfrak{a}$. Для любого набора $f_1, \dots, f_m \in A$, *идеал, порожденный* $f_1, \dots, f_m$ это множество линейных комбинаций $a_1 f_1 + \dots + a_m f_m$; он обозначается $(f_1, \dots, f_m) \subset A$. Идеал $\mathfrak{a}$ *собственный*, если $\mathfrak{a} \neq A$.

Упражнение 1.1. *Проверьте, что* $(f_1, \dots, f_m) \subset A$ *– действительно идеал. Приведите пример идеала, порожденного двумя разными наборами своих элементов.*

Если алгебраическое подмножество $V \subset \mathbb{A}^n$ задано полиномами $f_1, \dots, f_m \in k[x_1, \dots, x_n]$, то ясно, что любая линейная комбинация этих полиномов тоже обращается в 0 на V – поэтому V есть множество общих нулей идеала $\mathfrak{a} = (f_1, \dots, f_n) \in A$ и не зависит от выбора образующих $f_1, \dots, f_m$. Так мы и будем определять алгебраические подмножества.

Определение 1.2. *Алгебраическое подмножество* $V = V(\mathfrak{a}) \subset \mathbb{A}^n$, соответствующее идеалу $\mathfrak{a} \subset k[x_1, \dots, x_n]$, это множество общих нулей всех элементов $a \in \mathfrak{a}$.

Теперь мы хотим решить вторую проблему – определить базовый объект алгебраической геометрии инвариантно, без связи с конкретным вложением $V \subset \mathbb{A}^n$. Пока что, наше $V(\mathfrak{a})$ это просто множество, без какой-либо дополнительной структуры. Что взять в качестве дополнительной структуры? *Алгебраической*, или *полиномиальной* функцией на $V(\mathfrak{a}) \subset \mathbb{A}^n$ естественно называть такую функцию, которая получается ограничением полиномиальной функции $f \in k[x_1, \dots, x_n]$ на A^n на наше подмножество $V(\mathfrak{a})$. По определению, функции $f \in \mathfrak{a}$ ограничиваются на $V(\mathfrak{a})$ нулем; руководствуясь этим, вводят такое определение.

Определение 1.3. *Кольцом (алгебраических) функций* на алгебраическом множестве $V(\mathfrak{a})$ называется факторкольцо $A = k[x_1, \dots, x_n]/\mathfrak{a}$.

Ясно, что кольцо функций – это внутренний инвариант алгебраического множества: при любом разумном определении алгебраической структуры на множестве $V(\mathfrak{a})$, мы должны уметь восстановить по ней кольцо $A = k[x_1, \dots, x_n]/\mathfrak{a}$. Оказывается, однако, что этого *и достаточно*, и более того, кольцо A это на самом деле первичный объект: в частности, множество $V(\mathfrak{a})$ восстанавливается по кольцу A. Вот как это делается.

Определение 1.4. Идеал $\mathfrak{m} \subset A$ называется *максимальным*, если это максимальный элемент в множестве всех собственных идеалов A, упорядоченных по включению – иными словами, если какой-то собственный идеал $\mathfrak{m}' \subset A$ содержит $\mathfrak{m}$, то $\mathfrak{m} = \mathfrak{m}'$.

Упражнение 1.2. *Идеал $\mathfrak{m} \subset A$ максимальный тогда и только тогда, когда $A/\mathfrak{m}$ – поле.*

Определение 1.5. Поле $A/\mathfrak{m}$ называется *полем вычетов* максимального идеала $\mathfrak{m}$.

Напомним, что по Лемме Цорна из теории множеств, если в частично упорядоченном множестве X любая возрастающая последовательность $x_1 \leq x_2 \leq \dots$ ограничена сверху каким-то элементом $x \in X$, $x_i \leq x$, то в X есть хотя бы один максимальный элемент. Для любого идеала $\mathfrak{a} \in A$ множество собственных идеалов в A, содержащих $\mathfrak{a}$, очевидным образом удовлетворяет условию Леммы Цорна – объединение последовательности вложенных собственных идеалов это идеал. Поэтому любой идеал $\mathfrak{a} \subset A$ содержится в максимальном идеале $\mathfrak{m} \subset A$.

Упражнение 1.3. *Почему объединение последовательности вложенных собственных идеалов* – собственный *идеал?*

Определение 1.6. *Максимальным спектром* $\operatorname{Max}(A)$ кольца A называется множество его максимальных идеалов.

Упражнение 1.4. *Если $\mathfrak{a} \subset k[x_1, \dots, x_n]$ – максимальный идеал, то $V(\mathfrak{a}) \subset \mathbb{A}^n$ либо состоит из одной точки, либо пусто.*

Предложение 1.7. *Пусть A – коммутативное кольцо, представленное как*

$$A = k[x_1, \dots, x_n]/\mathfrak{a},$$

факторкольцо алгебры полиномов от n переменных над полем k по идеалу $\mathfrak{a} \subset k[x_1, \dots, x_n]$. Обозначим через $\operatorname{Max}_k(A) \subset \operatorname{Max}(A)$ подмножество, состоящее из макисмальных идеалов с полем вычетов k. Тогда существует естественное отождествление $\operatorname{Max}_k(A) \cong V(\mathfrak{a})$.

Доказательство. Для любой точки $x \in \mathbb{A}^n$, множество полиномов, обращающихся в ноль в x, очевидно есть собственный идеал $\mathfrak{m}_x \subset k[x_1, \dots, x_n]$, причем $k[x_1, \dots, x_n]/\mathfrak{m}_x$ изоморфно полю k, так что этот идеал максимальный и лежит в $\operatorname{Max}_k(A)$. При этом $x \in V(\mathfrak{a})$ тогда и только тогда, когда $\mathfrak{a} \subset \mathfrak{m}_x$. Такие идеалы, в свою очередь, соответствуют идеалам факторкольца $k[x_1, \dots, x_n]/\mathfrak{a}$. Таким образом, получаем соответствие "точки $V(\mathfrak{a})$" $\Rightarrow$ "идеалы из $\operatorname{Max}_k(k[x_1, \dots, x_n])$, содержащие $\mathfrak{a}$ $\Leftrightarrow$ "идеалы из $Max_k(A)$". Надо доказать, что это соответствие биективно – любой максимальный идеал $k[x_1, \dots, x_n]$ с полем вычетов k происходит из точки $\mathbb{A}^n$. Иными словами, мы хотим доказать, что если в Упражении 1.4 $\mathfrak{a} \in \operatorname{Max}_k(A)$, то $V(\mathfrak{a})$ не может быть пусто – оно всегда состоит из одной точки. В самом деле, любой $\mathfrak{m} \in \operatorname{Max}_k(k[x_1, \dots, x_n])$ по определению есть ядро отображения $\varphi : k[x_1, \dots, x_n] \to k \cong k[x_1, \dots, x_n]/\mathfrak{m}$, и легко видеть, что $\mathfrak{m} = \mathfrak{m}_x$, где $x \in \mathbb{A}^n$ имеет координаты $\varphi(x_1), \dots, \varphi(x_n)$. $\square$

Тем самым, множество $V(\mathfrak{a})$ полностью восстанавливается по соответствующему кольцу функций $A = k[x_1, \dots, x_n]/\mathfrak{a}$. Заметим при этом, что A содержит *строго больше* информации, чем соответствующее алгебраическое множество $V(\mathfrak{a}) \subset \mathbb{A}^n$. А именно, рассмотрим например идеал $\mathfrak{a} = (x^2) \subset k[x]$. Тогда $V(\mathfrak{a})$ состоит из одной точки $0 \in \mathbb{A}^1$, но $A = k[x]/x^2$ это не поле k – в нем есть еще элемент x; хотя $x^2 = 0$ в A, само x нулю не равно. Неформально, идеалу $\mathfrak{a}$ соответствует точка 0, "взятая с кратностью 2". На уровне множеств, хорошо ввести кратности трудно; а вот кольцо функций A помнит про кратности автоматически.

Поэтому с чисто формальной точки зрения, удобно считать именно конечно порожденные алгебры над полем k первичным объектом, и под аффинным алгебраическим многообразием над полем k понимать именно его алгебру функций.

Исторически, при первых попытках формального обоснования алгебраической геометрии (А. Вейль, О. Зарисски) так и делали. Однако это не вполне идеально: хотя зависимость от явного вложения в $\mathbb{A}^n$ из определения пропадает – выбор вложения это просто выбор образующих алгебры – остается зависимость от основного поля k. Все было бы ничего, если бы существовало "самое маленькое" поле k, которое вкладывалось бы в любое другое – но такого поля очевидно нет; в любое кольцо вкладывается кольцо $\mathbb{Z}$, но это не поле, в нем в самом много идеалов, и, как мы увидим в дальнейшем, с точки зрения алгебраической геометрии $\mathbb{Z}$ имеет размерность один. Таким образом, тривиальное алгебраическое многообразие – одна точка – получается над каждым полем свое; а если бороться с этим, объявив точкой $\mathbb{Z}$, то точка получается какая-то одномерная.

Кроме того, даже если рассматривать только поля характеристики 0, которые все содержат $\mathbb{Q}$, часто полезно рассматривать одно и то же многообразие – например аффинное пространство – над разными полями. Если выбор поля зашит в определение, переход от одного поля к другому получается неуклюжим.

При этом с начала XX века было известно, что если базовое поле k алгебраически замкнуто, то оно тоже восстанавливается по кольцу A. А именно, имеет место следующий замечательный результат Д. Гильберта.

Теорема 1.8 (Теорема Гильберта о нулях, алгебраическая версия). *Пусть расширение K поля k порождено как k-алгебра конечным числом элементов $x_1, \dots, x_n \in K$. Тогда K алгебраично над k.*

Доказательство. Напомним, что если поле $k' \supset k$ – расширение поля k, порожденное одним элементом $\alpha \in k'$, то возможны две ситуации: или α удовлетворяет какому-то алгебраическому уравнению $P(\alpha) = 0$, $P \in k[x]$ – тогда говорят, что α алгебраичен на k – или такого соотношения нет, и тогда говорят, что α трансцедентен над k. В первом случае можно выбрать полином $P(x)$ наименьшей возможной степени, скажем d, и тогда $k' = k[x]/P(x)$ есть d-мерное векторное пространство над k с базисом $1, \alpha, \dots, \alpha^{d-1}$. Во втором случае, k' изоморфно полю рациональных функций $k(x)$ от одной переменной над k.

Изменяя при необходимости порядок образующих $x_1, \dots, x_n \in K$, добьемся того, чтобы x_i, $i \leq r$ были трансцедентны над $k(x_1, \dots, x_{i-1})$, так что K содержит подполе $K_0 = k(x_1, \dots, x_r)$, а при $r < i \leq n$ элемент x_i алгебраичен над $K_{i-r} = K\langle x_{r+1}, \dots, x_{i-1}\rangle \subset K$, скажем степени d_i. Иными словами, существуют такие полиномы $P_i \in K_0[x_{r+1}, \dots, x_{i-1}]$ степени d_i по последней переменной, что $P_i(x_{r+1}, \dots, x_i) = 0$. Этих полиномов конечное число, а их коэффициенты – рациональные функции от $x_1, \dots, x_r$. Поэтому есть такое $g \in k[x_1, \dots, x_r]$, что $gP_i \in k[x_1, \dots, x_{i-1}]$. Иными словами, если мы рассмотрим подкольцо $B = k\langle x_1, \dots, x_r, g^{-1}\rangle \subset K_0$, то все P_i это полиномы с коэффициентами из B.

Упражнение 1.5. *Поле K, рассмотренное как модуль над $B \subset K$ – это свободный модуль ранга $d_r \dots d_n$ с базисом*

$$\prod_{r<i\leq n} x_i^{e_i}, \qquad 0 \leq e_i < d_i.$$

В силу этого упражнения, если B содержит собственный идеал $I \subset B$, то $IK \subset K$ – тоже собственный идеал, чего не может быть, т.к. K поле. Поэтому B тоже поле. Причем поскольку $B \subset K_0 = k(x_1, \dots, x_r)$, а все образующие $x_1, \dots, x_r$ лежат в B, то $B = K_0 = k(x_1, \dots, x_r$. Иными словами, любую рациональную функцию от $x_1, \dots, x_r$ можно выразить как полином от $x_1, \dots, x_r$ и еще одной образующей g^{-1}. Если $r \geq 1$, это невозможно – всегда существует полином $f \in k[x_1, \dots, x_r]$, который взаимно прост с g, и функцию f^{-1} представить в таком виде нельзя. □

Следствие 1.9. *Если алгебра A конечно порождена над алгебраически замкнутым полем k, то* $\mathrm{Max}_k(A) = \mathrm{Max}(A)$. □

Следствие 1.10 (Теорема Гильберта о нулях.). *Пусть $\mathfrak{a} \subset k[x_1, \dots, x_n]$ – идеал в алгебре полиномов над лагебраически замкнутым полем k. Тогда если $V(\mathfrak{a})$ пусто, то $\mathfrak{a} = k[x_1, \dots, x_n]$.*

Доказательство. Идеал $\mathfrak{a}$ содержится в каком-то максимальном идеале $\mathfrak{m} \subset k[x_1, \dots, x_n]$. Поскольку k алгебраически замкнуто, $\mathfrak{m} \in \mathrm{Max}_k(k[x_1, \dots, x_n])$, и по Предложению 1.7, $V(\mathfrak{a}) \supset V(\mathfrak{m})$ содержит точку. □

Замечание 1.11. Кроме всего прочего, теорема Гильберта о нулях показывает, что выйти из класса конечно порожденных алгебр над фиксированным полем k очень легко – уже поле рациональных функций $k(x)$ не конечно порождено.

Одним из новшеств А. Гротендика было следующее решение: для того, чтобы теория была естественной, в качестве базовых объектов алгебраической геометрии надо допускать *любые* кольца – даже такие, которые совершенно не выглядят геометрически (например, кольцо $\mathbb{Z}$).

Определение 1.12. *Аффинной схемой* называется коммутативное кольцо A.

Таким образом, аффинная алгебраическая геометрия по существу эквивалентна коммутативной алгебре, т.е. теории коммутативных колец. Мы доказываем утверждения про кольца, используя интуицию, полученную из геометрической картинки. В начале 50х годов эта точка зрения была совершенно дикой; но со временем она вошла в обиход, и оказалась вполне плодотворной – даже в теории чисел, которая сейчас воспринимается как алгебраическая геометрия над $\mathbb{Z}$ или даже алгебраическая геометрия самого $\mathbb{Z}$.

Конечно, буквально Определения 1.12 у Гротендика нет – оно слишком тавтологично. Гротендик определяет *схемы*, объекты изучения алгебраической геометрии. Схемы склеиваются из кусков, называемых аффинными, и соответствующих коммутативным кольцам – подобно тому, как проективное пространство склеивается из аффинных карт. Мы все это будем изучать через несколько лекций; по процедура склейки требует некоторой техники, которая пока совершенно несущественна: прежде чем склеивать, надо изучить сами аффинные куски. Поэтому пока что мы будем заниматься только аффинной алгебраической геометрией, или, что то же самое, коммутативной алгеброй. Помимо доказательства некоторых важных теорем, наша цель – наработать словарь, позволяющий переводить алгебраические понятия на геометрический язык, и наоборот.

Нулевую строку словаря мы уже ввели в декларативном порядке – постановили, что аффинная схема есть коммутативное кольцо.

В соответствии с современной категорной идеологией, как только мы определили какие-то математические объекты, надо определить отображения между ними. Поскольку мы мыслим элементы кольца A как функции, пускай в обобщенном смысле, на соответствующей аффинной схеме, отображение схем это просто отображение колец, но действующее в другую сторону: отображение из схемы, заданной кольцом B, в схему, заданную кольцом A, это то же самое, что отображение из кольца A в кольцо B.

Под множеством точек схемы, отвечающей кольцу A, было бы естественно понимать множество $\mathrm{Max}(A)$, но здесь есть проблема – это множество плохо ведет себя при отображениях. А именно, если $\mathfrak{a} \in B$ – идеал, а $f : A \to B$ – отображение колец, то $f^{-1}(\mathfrak{a}) \subset A$ конечно тоже идеал; но если $\mathfrak{a} \in B$ – максимальный идеал, то $f^{-1}(\mathfrak{a})$ не обязан быть максимальным! Например, пусть $A = k[x]$ – кольцо полиномов над полен k, а $B = k(x)$ – кольцо рациональных функций. Тогда $0 \in k(x)$ – максимальный идеал в B, но никак не в A. Для борьбы с этим, Гротендик расширяет рассматриваемый класс идеалов.

Определение 1.13. Собственный идеал $\mathfrak{a} \in A$ называется *простым*, если $A/\mathfrak{a}$ не содержит делителей нуля – иными словами, если $ab \in \mathfrak{a}$, то или a, или b тоже лежат в $\mathfrak{a}$.

Определение 1.14. Множество простых идеалов кольца A называется его *спектром* и обозначается $\mathrm{Spec}(A)$.

Упражнение 1.6. *Если $f : A \to B$ – гомоморфизм колец, а $\mathfrak{p} subset B$ – простой идеал, то $f^{-1}(\mathfrak{p}) \subset A$ – тоже простой идеал.*

Таким образом, каждому отображению колец $f : A \to B$ отвечает отображение множеств $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$. Множество $\mathrm{Spec}(A)$ понимается как множество точек соотвествующей аффинной схемы. Да и саму схему by abuse of notation обозначают $\mathrm{Spec}(A)$.

Если мы занимаемся аффинной алгебраической геометрией над $\mathbb{C}$, т.е. рассматриваем аффинное пространство $\mathbb{A}^n_{\mathbb{C}}$, мы интуитивно полагаем, что для его точек есть какое-то понятие близости, какая-то топология. Однако важно понимать, что все это вещи совершенно не алгебраические: в алгебраической геометрии, никакого способа увидеть естественную топологию на множестве $\mathrm{Max}(\mathbb{C}[x_1, \dots, x_n])$ *нет.* Рассматривая только полиномиальные функции, мы не можем сказать, что две точки близки. Все, что мы можем сказать, это что они лежат в одном алгебраическом подмножестве. Тем не менее, формализовать это последнее обстоятельство оказывается полезным, и для этого можно употребить, пусть и не по назначению, обычное определение топологического пространства.

Определение 1.15. *Топология Зарисского* на множестве $\mathrm{Spec}(A)$ задается так: замкнутые подмножества $V(\mathfrak{a}) \subset \mathrm{Spec}(A)$ соответствуют идеалам $\mathfrak{a} \in A$ и состоят из всех простых идеалов $\mathfrak{p} \in \mathrm{Spec}\, A$, содержащих $\mathfrak{a}$.

Упражнение 1.7. *Проверьте, что это действительно задает топологию. Для этого проверьте, что $V(\mathfrak{a}_1) \cap V(\mathfrak{a}_2) = V(\mathfrak{a}_1 + \mathfrak{a}_2)$ и что $V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2) = V(\mathfrak{a}_1 \cap \mathfrak{a}_2)$.*

Подчеркнем еще раз: топология Зарисского это топология в чисто формальном смысле, и к обычной топологии она имеет очень слабое отношение. В частности, большинство привычных дополнительных аксиом для топологии Зарисского неверны. Так, она нехаусдорфова, и даже не удовлетворяет свойству T_1: не все точки замкнуты. Это непривычно, но не плохо: наоборот, топология Зарисского помогает отделить "настоящие" точки из $\mathrm{Max}(A) \subset \mathrm{Spec}(A)$ от тех, которые мы добавили в спектр по формальным причинам.

Упражнение 1.8. *Точка $x \in \mathrm{Spec}(A)$ замкнута тогда и только тогда, когда $x \in Max(A)$.*

Упражнение 1.9. *Опишите топологические пространства $\mathrm{Spec}\, \mathbb{Z}$ и $\mathrm{Spec}\, k[x]$, k – алгебраически замкнутое поле и $\mathbb{R}$.*

Определение 1.16. Замкнутое подмножество $V \subset X$ топологического пространства X называется *неприводимым* если его нельзя представить в виде объединения двух непустых собственных замкнутых подмножеств $X_1, X_2 \subset X$.

Упражнение 1.10. *Пусть топологическое пространство X хаусдорфово. Найдите все неприводимые замкнутые подмножества X.*

Упражнение 1.11. *Пусть $\mathfrak{a} \subset A$ – простой идеал. Докажите, что $V(\mathfrak{a}) \subset \operatorname{Spec}(A)$ неприводимо, и совпадает с замыканием точки $\mathfrak{a} \in \operatorname{Spec}(A)$.*

Определение 1.17. В такой ситуации, говорят, что $\mathfrak{a}$ есть *общая точка* неприводимого подмножества $V(\mathfrak{a}) \subset \operatorname{Spec}(A)$.

Впоследствии мы увидим, что при некоторых разумных предположениях конечности на A обратное тоже верно – любое неприводимое замкнутое подмножество в $\operatorname{Spec}(A)$ есть замыкание своей "общей точки" $\mathfrak{a} \in \operatorname{Spec}(A)$. Таким образом, при переходе от $\operatorname{Max}(A)$ к $\operatorname{Spec}(A)$ мы добавляем по одной "общей" точке для каждого неприводимого алгебраического подмножества.

Как и в случае $A = k[x_1, \ldots, x_n]$, разные идеалы $\mathfrak{a}_1, \mathfrak{a}_2 \subset A$ могут задавать одно и то же подмножество $V(\mathfrak{a}_1) = V(\mathfrak{a}_2) \subset \operatorname{Spec}(A)$ – факторкольцо $A/\mathfrak{a}$ хранит больше информации, чем подмножество $V(\mathfrak{a})$. Поэтому вводят следующее определение.

Определение 1.18. Отображение схем $\operatorname{Spec} B \to \operatorname{Spec} A$ называется *замкнутым вложением*, если соответствующее отображение колец $A \to B$ сюръективно, т.е. B отождествлено с факторкольцом $A/\mathfrak{a}$ по какому-то идеалу $\mathfrak{a} \in A$. В такой ситуации говорят, что $\operatorname{Spec} B$ – *замкнутая подсхема* схемы $\operatorname{Spec} A$, *заданная идеалом* $\mathfrak{a} \subset A$ (и пишут $\operatorname{Spec}(B) \subset \operatorname{Spec}(A)$).

Когда хотят подчеркнуть, что рассматривается не просто подмножество $V(\mathfrak{a}) \subset \operatorname{Spec}(A)$, а именно подсхема $\operatorname{Spec}(A/\mathfrak{a}) \subset \operatorname{Spec}(A)$, иногда говорят, что множество нулей идеала $\mathfrak{a}$ рассматривается "со схемной структурой".

Говорят, что идеалы $\mathfrak{a}_1, \mathfrak{a}_2 \subset A$ *взаимно просты*, если $\mathfrak{a}_1 + \mathfrak{a}_2 = A$. Геометрически, это значит, что подмножества $V(\mathfrak{a}_1), V(\mathfrak{a}_2) \subset A$ не пересекаются. *Несвязным объединением* схем $\operatorname{Spec}(A)$ и $\operatorname{Spec}(B)$ называется схема

$$\operatorname{Spec}(A) \coprod \operatorname{Spec}(B) = \operatorname{Spec}(A \oplus B).$$

Хотелось бы верить, что наш язык достаточно точен, и отражает тот очевидный геометрический факт, что объединение нескольких попарно непересекающихся подмножеств изоморфно их абстрактному несвязному объединению. Это действительно так.

Упражнение 1.12 (Китайская теорема он остатках.). *Пусть $\mathfrak{a}_1, \ldots, \mathfrak{a}_m \subset A$ – попарно взаимно простые идеалы. Тогда $A/(\mathfrak{a}_1 \cap \cdots \cap \ldots \mathfrak{a}_m) \cong (A/\mathfrak{a}_1) \oplus \cdots \oplus (A/\mathfrak{a}_m)$.*

В следующей лекции мы продолжим сегодняшний перевод простых геометрических понятий на алгебраический язык (и в частности, узнаем, чему в алгебре отвечают *открытые* по Зарисскому подмножества). Пока что, подведем итог – вот изученный сегодня словарь.

Алгебра	Геометрия
Коммутативное кольцо A	Аффинная схема $\operatorname{Spec}(A)$
Гомоморфизм $A \to B$	Отображение схем $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$
Идеал $\mathfrak{a} \subset A$	Замкнутое подмножество $V(\mathfrak{a}) \subset \operatorname{Spec}(A)$
Сумма идеалов $\mathfrak{a}_1 + \mathfrak{a}_1$	Пересечение $V(\mathfrak{a}_1) \cap V(\mathfrak{a}_2)$
Пересечение идеалов $\mathfrak{a}_1 \cap \mathfrak{a}_2$	Объединение $V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2)$
Факторкольцо $A/\mathfrak{a}$	Замкнутая подсхема $\operatorname{Spec}(A/\mathfrak{a}) \subset \operatorname{Spec}(A)$
Сюръективное отображение $A \to B$	Замкнутое вложение $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$
Простой идеал $\mathfrak{p} \subset A$	Точка $\mathfrak{p} \in \operatorname{Spec}(A)$, такая что $V(\mathfrak{p}) = \overline{\{\mathfrak{p}\}}$; общая точка $V(\mathfrak{p})$
Максимальный идеал $\mathfrak{m} \subset A$	Замкнутая точка $\mathfrak{m} \in \operatorname{Spec}(A)$

А теперь, чтобы не было так скучно, попробуем применить наш формализм к чему-нибудь конкретному – а именно, к теореме Безу. Саму теорему Безу мы не докажем, поскольку для этого нужны проективные многообразия, а у нас пока есть только аффинные. Но мы разберемся с кратностями пересечения, и покажем, откуда появляется результант.

Нульмерной схемой над алгебраически замкнутым полем k будем называть спектр $\mathrm{Spec}(A)$ такой k-алгебры A, что A конечномерно как векторное пространство над k. Размерность $\mathsf{dim}_k A$ будем называть *длиной* нульмерной схемы $\mathrm{Spec}(A)$. Если $A = k \oplus \cdots \oplus k$, то $\mathrm{Spec}(A)$ – несвязное объединение m точек $\mathrm{Spec}(k)$, и длина $\mathrm{Spec}(A)$ – это как раз число m. Если $B = k[x]$ и $\mathrm{Spec}\, A = \mathrm{Spec}(k[x]/(P(x)))$ – подсхема нулей полинома $P(x)$, то длина $\mathrm{Spec}\, A$ – число нулей полинома

Рассмотрим аффинную плоскость $\mathbb{A}^2 = \mathrm{Spec}\, k[x, y]$ над k. Пусть заданы два полинома $P(x, y)$, $Q(x, y)$ степеней n и m. Обозначим через $A = k[x, y]/(P(x, y))$, $B = k[x, y]/(Q(x, y))$ факторкольца по идеалам, порожденным $P(x, y)$ и $Q(x, y)$. Будем говорить, что замкнутые подсхемы $\mathrm{Spec}\, A, \mathrm{Spec}\, B \subset \mathbb{A}^2$ *не имеют общих компонент*, если их пересечение $\mathrm{Spec}\, A \cap \mathrm{Spec}\, B = \mathrm{Spec}\, k[x, y]/(P(x, y), Q(x, y)) \subset \mathbb{A}^2$ – нульмерная подсхема. Обозначим

$$C = k[x, y]/(P(x, y)Q(x, y))$$

(теоретико-множественно, $\mathrm{Spec}\, C$ это объединение $\mathrm{Spec}\, B \subset \mathbb{A}^2$ и $\mathrm{Spec}\, A \subset \mathbb{A}^2$.

Лемма 1.19. *Заменами переменных вида $x \mapsto x + \alpha y$, $y \mapsto y$ можно добиться того, что алгебры A, B и C – совбодные модули над кольцом $k[x]$ рангов n, m, $n + m$.*

Доказательство. Чтобы A было свободным модулем, достаточно добиться того, чтобы коэффициент при y^n в $P(x, y)$ был ненулевым – тогда A это модуль с базисом $1, y, y^2, \ldots, y^{n-1}$. Аналогично, достаточно добиться того, чтобы коэффициенты при старшей степени y в $Q(x, y)$ и $P(x, y)Q(x, y)$ были ненулевыми. Все эти коэффициенты – нетривиальные полиномы от α, т.е. “плохих” значений α – конечное число. Поскольку алгебраически замкнутое поле бесконечно, существует хорошее α. $\square$

Рассмотрим теперь отображение $\varphi : A \oplus B \to C$, заданное как $\varphi(\langle a, b\rangle) = Q(x, y)a + P(x, y)b$. Легко видеть, что образ этого отображения – идеал $(P(x, y), Q(x, y)) \subset C$; поэтому его коядро – как раз $k[x, y]/(P(x, y), Q(x, y))$, кольцо функций на пересечении $\mathrm{Spec}\, A \cap \mathrm{Spec}\, B$, которое мы хотим изучить. С другой стороны, $A \oplus B$ и C – свободные модули над $k[x]$ ранга $n + m$, т.е. φ – матрица размера $(n + m) \times (n + m)$ из элементов кольца $k[x]$.

Упражнение 1.13. *Любую матрицу нам кольцом $k[x]$ можно элементарными преобразованиями по строкам и столбцам привести к диагональному виду.*

Аффинная версия теоремы Безу, которую мы хотим доказать, такая.

Теорема 1.20. *Длина нульмерной схемы* $\mathrm{Spec}\, A \cap \mathrm{Spec}\, B$ *равна степени полинома* $\mathsf{det}\, \varphi \in k[x]$.

Доказательство. Более общо, мы докажем, что если дана матрица φ размера $l \times l$ над кольцом $k[x]$, причем коядро отображения $\varphi : k[x]^{\oplus l} \to k[x]^{\oplus l}$ конечномерно над k, то размерность этого коядра равна степени полинома $\mathsf{det}\, \varphi$.

Действительно, поскольку элементарные преобразования обратимы и не меняют определитель, можно воспользоваться Упражнением 1.13 и привести φ к диагональному виду, с какими-то полиномами $\varphi_1, \ldots \varphi_l$ на диагонали. Тогда $\mathsf{Coker}\, \varphi = \mathsf{Coker}\, \varphi_1 \oplus \cdots \oplus \mathsf{Coker}\, \varphi_l$, а $\mathsf{det}\, \varphi = \varphi_1 \cdot \cdots \cdot \varphi_l$. $\square$

Если расписать явно определитель $\mathsf{det}\, \varphi$, получится результант.