Лекция 2.

Открытые по Зарисскому множества, локализация, локальные кольца. Модули и операции над ними. Тензорные произведения. Неразветвленные накрытия, теория Галуа.

На прошлой лекции мы обсуждали понятие алгебраического многообразия. Напомним вкратце основые идеи. Любой геометрический объект в математике можно исследовать двумя способами. Во-первых, можно думать про него как про множество, множество точек. Во-вторых, можно рассматривать набор заданных на нем функций. Функции можно складывать и перемножать, так что они образуют кольцо. По функции f и точке x можно построить число – вычислить значение $f(x)$ функции в точке. При этом операция вычисления довольно симметрична. Можно считать, что задано множество точек, а функция – это то, что сопоставляет точке число; а можно, наоборот, считать, что задано кольцо функций, а точка – это то, что сопоставляет функции число. Иными словами, точка x задает гомоморфизм вычисления ev_x из кольца функций в числа.

Какой из этих двойственных подходов выбрать, это вопрос удобства. На прошлой лекции мы выяснили, что в алгебраической геометрии множество точек – недостаточно тонкая вещь, и не улавливает всей геометрической структуры (например, потому, что у точек алгебраического множества естественным образом могут быть кратности). Поэтому при исследовании по крайней мере аффинных многообразий в качестве первичного объекта берут кольцо функций. Оказывается при этом, что годится любое кольцо – на любое коммутативное кольцо A можно смотреть как на геометрический объект и исследовать его, используя геометрическую интуицию. Тогда точка этого объекта – это любой гомоморфизм из кольца A в числа. Числа здесь понимаются как элементы поля, причем, чтобы теория получилась естественной, какое именно поле лучше не выбирать, а рассматривать все.

Определение 2.1. *Точкой* кольца A со значениями в поле K называется гомоморфизм $A \to K$.

На самом деле, оказывается полезным даже еще ослабить это определение, и не требовать, чтобы K было полем – т.е. под числами тоже понимать элементы любого коммутативного кольца. Но нам пока такая точка зрения не понадобится. Напротив, даже гомоморфизм $A \to K$ для нас пока будет лишним данным, и вместо того, что помнить весь гомоморфизм, мы будем помнить его ядро $\mathfrak{p} \subset A$ – простой идеал кольца A. Множество всех простых идеалов A называется *спектром* A и обозначается $\operatorname{Spec} A$.

На прошлой лекции мы описали множество $\operatorname{Spec} A$ в простых случаях, а также ввели на нем некоторую топологию, называемую топологией Зарисского. А именно, замкнутые по Зарисскому подмножества в $\operatorname{Spec}(A)$ – это множества $V(\mathfrak{a}) \subset \operatorname{Spec}(A)$ всех простых идеалов, содержащих данный идеал $\mathfrak{a} \subset A$. Топология Зарисского, напомним, весьма противоречит обычной интуиции – она нехаусдорфова и т.д. Вот, чтобы вспомнить о чем речь, простая и полезная Лемма.

Лемма 2.2. *Если $\mathfrak{a} \subset A$ – ненулевой идеал в кольце A без делителей нуля, то замкнутое подмножество $V(\mathfrak{a}) \subset \operatorname{Spec} A$ нигде не плотно.*

Доказательство. По определению, надо доказать, что для любого непустого открытого $U \subset \operatorname{Spec} A$ существует такое непустое открытое $U_1 \subset U$, что $U_1 \cap V(\mathfrak{a}) = \emptyset$. Действительно, раз U открыто, дополнение $\operatorname{Spec} A \setminus U$ имеет вид $V(\mathfrak{a}_1)$, а раз U непусто, $\mathfrak{a}_1 \subset A$ – ненулевой идеал. Тогда, поскольку в A нет делителей нуля, $\mathfrak{a} \cap \mathfrak{a}_1 \subset A$ – тоже ненулевой идеал, а потому $\operatorname{Spec} A \setminus V(\mathfrak{a} \cap \mathfrak{a}_1)$ в свою очередь непусто. Вот его и можно взять в качестве U_1. $\square$

Обсудим теперь, какие подмножества в этой топологии открыты.

Пусть дано кольцо A и элемент $f \in A$. Тогда можно “формально обратить f” – а именно, рассмотреть факторкольцо кольца многочленов $A[x]$ по идеалу, порожденному $fx - 1 \in A[x]$. Это факторкольцо обозначается $A[f^{-1}]$ и называется *локализацией* кольца A по степеням элемента $f \in A$. В явном виде, элементы $A[f^{-1}]$ это классы эквивалентности формальных выражений $a \cdot f^{-n}$, где $a \in A$, а n – неотрицательное целое число, по следующему отношению эквивалентности: $af^{m_1} \cdot f^{-(n+m_1)} \sim af^{m_2} \cdot f^{-(n+m_2)}$. Операции на этих элементах задаются так:

$$a \cdot f^{-n} + b \cdot f^{-m} = (af^m + bf^n) \cdot f^{-(n+m)} \qquad (a \cdot f^{-n})(b \cdot f^{-m}) = ab \cdot f^{-(n+m)}.$$

Упражнение 2.1. *Проверьте, что эти формулы совместимы с отношением эквивалентности.*

Упражнение 2.2. *Опишите кольцо $A[f^{-1}]$ в следующих частных случаях: (1) $f \in A$ обратим, (2) $f \in A$ нильпотентный ($f^n = 0$ для достаточно большого n).*

Любой идеал $\mathfrak{a} \subset A$ очевидным образом дает идеал $\mathfrak{a}[f^{-1}] \subset A[f^{-1}]$; наоборот, любой идеал $\mathfrak{a} \subset A[f^{-1}]$ дает идеал $\varphi^{-1}(\mathfrak{a}) \subset A$ – прообраз $\mathfrak{a}$ при естественном отображении $\varphi : A \to A[f^{-1}]$.

Упражнение 2.3. *Проверьте, что идеал $\mathfrak{a}[f^{-1}] \subset A[f^{-1}]$ собственный тогда и только тогда, когда $\mathfrak{a} \subset A$ собственный и не содержит никакой степени f^n. Проверьте также, что для любого идеала $\mathfrak{b} \subset A[f^{-1}]$ имеем $\mathfrak{b} = \varphi^{-1}(\mathfrak{b})[f^{-1}]$.*

Заметим, что если идеал $\mathfrak{a} \subset A$ простой, то по определению, если он содержит f^n, то он содержит и само f. Поэтому возможны только два варианта: или простой идеал $\mathfrak{p} \subset A$ содержит f, или $\mathfrak{p}[f^{-1}] \subset A[f^{-1}]$ – собственный идеал. Легко видеть, что он также и простой, причем $\mathfrak{p} = \varphi^{-1}(\mathfrak{p}[f^{-1}])$. Таким образом, имеем естественнное отождествление $\operatorname{Spec} A[f^{-1}] \cong \operatorname{Spec} A \setminus V((f))$ – спектр $A[f^{-1}]$ отождествлен с дополнением к множеству $V((f)) \subset \operatorname{Spec}(A)$ нулей элемента $a \in A$.

Упражнение 2.4. *Проверьте, что это отождествление – гомеоморфизм между спектром $\operatorname{Spec} A[f^{-1}]$ и открытым подмножеством $\operatorname{Spec} A \setminus V((f)) \subset \operatorname{Spec} A$ с индуцированной топологией.*

Итак, дополнение к замкнутому подмножеству $V((f)) \subset \operatorname{Spec} A$ – спектр локализации $A[f^{-1}]$.

Лемма 2.3. *Открытые подмножества вида $\operatorname{Spec} A[f^{-1}] \subset \operatorname{Spec} A$ образуют базу топологии Зарисского на $\operatorname{Spec} A$.*

Доказательство. Возьмем произвольное открытое $U \subset \operatorname{Spec} A$, дополнение к замкнутому $V(\mathfrak{a}) \subset \operatorname{Spec} A$, множеству нулей идеала $\mathfrak{a} \subset A$. По определению, надо доказать, что U есть объединение множеств вида $\operatorname{Spec} A[f^{-1}]$. Иными словами, пусть $x \in U$ любая точка; надо найти такое $f \in A$, что $x \in \operatorname{Spec} A[f^{-1}] \subset U$. Поскольку $x \in U$, соответствующий простой идеал $\mathfrak{p} \subset A$ не содержит $\mathfrak{a} \subset A$. Возьмем $f \in \mathfrak{a}$, не лежащее в $\mathfrak{p}$. Тогда $\operatorname{Spec} A[f^{-1}] \subset U$, а раз f не лежит в $\mathfrak{p}$, $x \in \operatorname{Spec} A[f^{-1}]$. $\square$

Конструкцию локализации полезно обобщить. *Мультипликативной системой* $S \subset A$ будем называть любое подмножество, замкнутое относительно умножения (например, все степени какого-то элемента $f \in A$).

Определение 2.4. *Локализацией* $A[S^{-1}]$ кольца A по мультипликативной системе S называется множество классов эквивалентности формальных выражений вида $a \cdot s^{-1}$, $a \in A$, $s \in S$, по отношению эквивалентности $as_1 \cdot (s_1 s)^{-1} \sim as_2 \cdot (s_2 s)^{-1}$. Операции в $A[S^{-1}]$ задаются равенствами

$$a_1 \cdot s_1^{-1} + a_2 \cdot s_2^{-1} = (a_1 s_2 + a_2 s_1) \cdot (s_1 s_2)^{-1} \qquad (a_1 \cdot s_1^{-1})(a_2 \cdot s_2^{-1}) = a_1 a_2 \cdot (s_1 s_2)^{-1}.$$

Упражнение 2.5. *Докажите, что естественное отображение* $\operatorname{Spec} A[S^{-1}] \to \operatorname{Spec} A$ *инъективно, и является гомеоморфизмом на свой образ.*

Если мультипликативная система $S \subset A$ конечно порождена – т.е. все $s \in S$ представляются как произведения некоторого конечного набора образующих $s_1, \dots, s_n \in S$ – то $\operatorname{Spec} A[S^{-1}] \subset \operatorname{Spec} A$ открыто. В общем случае это не так – $\operatorname{Spec} A[S^{-1}]$ есть пересечение открытых множеств, но, возможно, бесконечного их числа. Экстремальный пример здесь такой: пусть A *область целостности*, т.е. кольцо без делителей нуля. Тогда $S = A \setminus \{0\}$, множество всех ненулевых элементов A, образует мультипликативную систему, и легко видеть, что $A[S^{-1}]$ есть поле. Это поле называется *полем частных* кольца A.

Упражнение 2.6. *Чему равны поля частных колец* $\mathbb{Z}$, $k[x]$?

При этом если K – поле частных A, то $\operatorname{Spec} K \subset \operatorname{Spec} A$ – это одна точка, а именно, общая точка $\operatorname{Spec} A$ (отвечающая нулевому идеалу $\{0\} \subset A$).

Более общо, пусть $x \in \operatorname{Spec} A$ – точка, отвечающая простому идеалу $\mathfrak{p} \subset A$. Тогда $S_x = A \setminus \mathfrak{p}$ – мультипликативная система.

Определение 2.5. Локализация $A[S_x^{-1}]$ называется *локальным кольцом* схемы $\operatorname{Spec} A$ в точке $x \in A$ и обозначается $A_{\mathfrak{p}}$.

Упражнение 2.7. *Проверьте, что* $\mathfrak{p}A_{\mathfrak{p}} \subset A_{\mathfrak{p}}$ *– максимальный идеал, и что других максимальных идеалов в кольце* $A_{\mathfrak{p}}$ *нет.*

Упражнение 2.8. *Опишите локальное кольцо* $\mathbb{Z}_{(p)}$, p *– простое число.*

Геометрически, $\operatorname{Spec} A_{\mathfrak{p}} \subset \operatorname{Spec} A$ – это пересечение всех открытых подмножеств в $\operatorname{Spec} A$, которые содержат точку x. Важно помнить и понимать, что в силу особенностей топологии Зарисского, это совсем не только точка x! Абстрагируя эту ситуацию, вводят следующее.

Определение 2.6. Кольцо A называется *локальным*, если в нем есть единственный максимальный идеал $\mathfrak{m} \subset A$; поле вычетов $A/\mathfrak{m}$ называется полем вычетов локального кольца A.

Упражнение 2.9. *Докажите, что в локальном кольце* A *любой элемент* $a \in A$, *не лежащий в максимальном идеале* $\mathfrak{m} \subset A$, *обратим.*

Спектр локального кольца, таким образом, содержит только одну замкнутую точку (и, вообще говоря, довольно много незамкнутых). Это наилучшее приближение к “маленькой окрестности точки”, которое можно получить алгебраическими средствами. Разумеется, это очень грубое приближение. В частности, интуитивно маленькие окрестности точек хорошего – скажем, в каком-то смысле гладкого – многообразия должны быть все одинаковые, такие как у точки в аффинном пространстве; а локальных колец бывает очень много, и мы скоро увидим, что они разные даже для очень хороших многообразий. Но тем не менее, рассматривать локальные кольца часто очень полезно.

Дальше мы изучим, чему на алгебраическом языке отвечает произведение многообразий; но прежде чем сделать это, нам понадобится вспомнить некоторые факты о модулях над кольцом. Напомним, что модулем M над кольцом A называется группа M, снабженная дополнительной операцией умножения на элементы A: для любых $m \in M$, $a \in A$ задано произведение $am \in M$, причем выполнены аксиомы ассоциативности и дистрибутивности. Если A поле, то модуль над A это то же самое, что векторное пространство; в общем случае, все обычные операции линейной алгебры – взятие образа, ядра, коядра, прямой суммы – тоже имеют смысл, с тем же определением. Само A это очевидно модуль над собой. Прямая сумма $A^{\oplus n}$ какого-то количества копий A – возможно, бесконечного – называется *свободным A-модулем.*

Любой модуль над полем свободен (любое векторное пространство имеет базис). Однако для произвольного кольца это не так. Помимо свободных модулей, важные примеры это идеалы $\mathfrak{a} \subset A$ (иными словами, подмодули A) и факторы по ним $A/\mathfrak{a}$ (фактормодули A). Бывает, что идеалы на самом деле тоже свободны.

Упражнение 2.10. *Кольцо называется* кольцом главных идеалов*, если любой идеал $\mathfrak{a} \subset A$ порожден одним элементом $a \in A$. Докажите, что $k[x]$ и $\mathbb{Z}$ – кольца главных идеалов, и что любой ненулевой идеал $\mathfrak{a} \subset A$, рассмотренный как A-модуль, изоморфен A.*

Но в общем случае это не так. Например, в некоторый момент мы докажем, что для общего кубического многочлена $f(x, y)$, факторкольцо $k[x, y]/(f(x, y))$ не есть кольцо главных идеалов (это открыл, по-видимому, Абель).

Тем не менее, с модулями можно делать многое из того, что делают с идеалами. Например, их можно локализовать: если дан модуль M над кольцом A и мультипликативная система $S \subset A$, то локализация $M[S^{-1}]$ определяется как множество классов эквивалентности формальных выражений $m \cdot s^{-1}$, $m \in M$, $s \in S$, причем отношение эквивалентности и операции на $M[S^{-1}]$ задаются ровно теми же формулами, что для колец (проверьте, что все хорошо определено). Если $S = A \setminus \mathfrak{p}$ для простого идеала $\mathfrak{p} \subset A$, то локализация $M[S^{-1}]$ обозначается через $M_{\mathfrak{p}}$.

Упражнение 2.11. *Последовательность*

$$M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3$$

модулей и отображений называется точной*, если $\operatorname{Ker} \varphi_2 = \operatorname{Im} \varphi_1$ (в частности, $\varphi_2 \circ \varphi_1 = 0$). Докажите, что если дана точная последовательность A-модулей и мультипликативная система $S \subset A$, то последовательность локализаций*

$$M_1[S^{-1}] \xrightarrow{\varphi_1} M_2[S^{-1}] \xrightarrow{\varphi_2} M_3[S^{-1}]$$

тоже точна. Докажите также, что $(M_1 \oplus M_2)[S^{-1}] \cong M_1[S^{-1}] \oplus M_2[S^{-1}]$.

Чтобы получить какое-то представление о том, какие воообще говоря бывают модули, изучим модули над кольцом $k[x]$ полиномов от одной переменной.

Определение 2.7. Модуль M над кольцом A называется *конечно порожденным*, если существует сюръективное отображение $A^{\oplus n} \to M$, n положительное целое число (иными словами, можно выбрать такие элементы $m_1, \dots, m_n \in M$, что любой $m \in M$ есть линейная комбинация $m_1, \dots, m_n$ с коэффициентами из A). Конечно порожденный модуль M называется *конечно представимым*, если можно так выбрать сюръекцию $A^{\oplus n} \to M$, что ее ядро тоже конечно порождено.

Предложение 2.8. *Любой конечно представимый модуль M над кольцом $k[x]$ полиномов от одной переменной над полем k есть прямая сумма модулей вида $k[x]/(P(x))$, $P(x) \in k[x]$.*

Модуль имеет вид $k[x]/(P(x))$ тогда и только тогда, когда он порожден одним элемнтом; такой модуль называется циклическим. Поэтому это Предложение еще формулируют так: конечно представимый модуль над $k[x]$ есть сумма циклических.

Доказательство. По определению, M есть коядро отображения $\varphi : A^{\oplus m} \to A^{\oplus n}$. Зададим это отображение матрицей размера $m \times n$ и воспольуемся Упражнением 1.13. Легко видеть, что элементарные преобразования не меняют коядро; поэтому мы может предполагать, что φ – диагональная матрица, а в таком случае утверждение очевидно. □

Упражнение 2.12. *Докажите, что без предложения конечной представимости это неверно (рассмотрите $k[x, x^{-1}]$ как модуль над $k[x]$, и, применив к нему локализацию, перейдите к векторным пространствам на полем частных $k(x)$).*

Следствие 2.9 (Жорданова нормальная форма). *Любой эндоморфизм $A : V \to V$ конечномерного векторного пространства над алгебраически замкнутым полем k имеет жорданову нормальную форму.*

Доказательство. Рассмотрим V как $k[x]$-модуль – а именно, заставим x действовать с помощью эндоморфизма A. Тогда легко видеть, что V конечно представимо (например, V есть коядро отображения $k[x]^n \to k[x]^n$, заданного матрицей $x\,\mathsf{Id} - A$, где n – размерность пространства V). Поэтому V есть сумма циклических модулей, и достаточно доказать, что циклический модуль $k[x]/(P(x))$ имеет жорданову нормальную форму. А это очевидно – достаточно разложить на множители полином $P(x)$. □

Между прочим, именно поэтому множество простых идеалов называют *спектром*: это далекое обощение понятия спектра линейного оператора, т.е. набора его собственных значений.

Следующее утверждение доказывается аналогичным трюком, и, хотя оно совсем простое, применяется необычайно часто.

Лемма 2.10 (Лемма Накаямы). *Пусть M – конечно порожденный модуль над локальным кольцом A, и пусть $\mathfrak{m} \subset A$ – максимальный идеал. Тогда если $\mathfrak{m}M = M$, то $M = 0$.*

Доказательство. Выберем образующие $m_1, \dots, m_n \in M$. Поскольку $M = \mathfrak{m}M$, имеем $m_i = \sum m_j a_{ij}$ для каких-то $a_{ij} \in \mathfrak{m}$, т.е. $\sum m_j a'_{ij} = 0$, причем $a'_{ij} = \delta_{ij} - a_{ij} = \delta_{ij} \mod \mathfrak{m}$. Образуем из a'_{ij} квадратную матрицу A размера $n \times n$, и рассмотрим соотвествующее отображение $A : M^{\oplus n} \to M^{\oplus n}$. Тогда $A(\langle 0, \dots, m_i, \dots, 0\rangle) = 0$. Если B – матрица из главных миноров матрицы A, то BA – диагональная матрица, причем на диагонали стоит $\det A$. Тогда тем более $BA(\langle 0, \dots, m_i, \dots, 0\rangle) = 0$, т.е. $\det A m_i = 0$, а значит, $\det A$ действует нулем на M. Но $\det A = 1 \mod \mathfrak{m}$, а стало быть, обратим. □

Следствие 2.11. *Если элементы $m_1, \dots, m_n \in M$ конечно порожденного модуля M над локальным кольцом A порождают векторное пространство $M/\mathfrak{m}M$, то они порождают и сам M.*

Доказательство. Пусть $M' \subset M$ – подмодуль, порожденный $m_1, \dots, m_n$; легко видеть, что фактормодуль $M'' = M/M'$ удовлетворяет $\mathfrak{m}M'' = M''$. □

Введем теперь еще одну операцию линейной алгебры, которая также имеет смысл для модулей, и крайне важна – тензорное произведение.

Определение 2.12. *Тензорным произведением* модулей M_1, M_2 над кольцом A называется модуль, порожденный формальными выражениями вида $m_1 \otimes m_2$, $m_1 \in M_1$, $m_2 \in M_2$, с соотношениями

$$am_1 \otimes m_2 = a(m_1 \otimes m_2) \qquad (m_1 + m_1') \otimes m_2 = m_1 \otimes m_1 + m_1' \otimes m_2,$$

плюс те же соотношения по второму сомножителю. Тензорное произведение обозначается $M_1 \otimes_A M_2$, или – редко, когда нет риска перепутать – просто $M_1 \otimes M_2$.

Это определение довольно формально, его надо хорошо осознать; в частности, надо решить следующее упражнение.

Упражнение 2.13. *Вычислить тензорное произведение $M_1 \otimes_A M_2$ в следующих ситуациях:*

(i) $M_1 = A^{\otimes n}$, $M_2 = A^{\otimes m}$,

(ii) $M_1 = A^{\otimes n}$, M_2 *любой,*

(iii) $A = \mathbb{Z}$, $M_1 = \mathbb{Z}/2\mathbb{Z}$, $M_2 = \mathbb{Z}/n\mathbb{Z}$,

(iv) $A = \mathbb{Z}$, $M_1 = \mathbb{Q}$, $M_2 = \mathbb{Z}/n\mathbb{Z}$,

(v) A *любое,* $M_1 = A/\mathfrak{a}_1$, $M_2 = A/\mathfrak{a}_2$, $\mathfrak{a}_1$ *и* $\mathfrak{a}_2$ *взаимно просты.*

Упражнение 2.14. *Докажите, что для любого модуля M над кольцом A и любой мультипликативной системы $S \subset A$ имеется изоморфизм $M[S^{-1}] \cong M \otimes_A A[S^{-1}]$.*

Нам потребуется следующее наблюдение. Пусть даны кольца A, B и отображение $A \to B$. Тогда B – и более того, любой B-модуль – естественным образом можно рассматривать как модуль над A. Наоборот, если дан A-модуль M, то тензорное произведение $M \otimes_A B$ естественным образом есть модуль над B: B действует умножениями на второй множитель.

Упражнение 2.15. *Вычислите $A^{\oplus n} \otimes_A B$.*

Упражнение 2.16. *Докажите, что для любого A-модуля M и B-модуля N имеется естественный изоморфизм групп*

$$\mathsf{Hom}_A(A, B) \cong \mathsf{Hom}_B(M \otimes_A B, N). \tag{2.1}$$

Заметим, что (2.1) можно использовать как *определение* тензорного произведения (но тогда надо доказывать, что тензорное произведение существует).

Если же нам дано кольцо A и *два* кольца B_1, B_2 с отображениями $A \to B_1$, $A \to B_2$, то тензорное произведение $B_1 \otimes_A B_2$ имеет естественную структуру *кольца*: тензорные произведения $b_1 \otimes b_2 \in B_1 \otimes_A B_2$ можно перемножать почленно. При этом мы тоже имеем естественное отображение $A \to B_1 \otimes_A B_2$.

Геометрически, в такой ситуации говорят, что $\operatorname{Spec} B_1$ и $\operatorname{Spec} B_2$ это *схемы над* $\operatorname{Spec} A$ – имея в виду, что заданы отображения $\operatorname{Spec} B_1 \to \operatorname{Spec} A$, $\operatorname{Spec} B_2 \to \operatorname{Spec} A$.

Определение 2.13. Схема $\operatorname{Spec}(B_1 \otimes_A B_2)$ называется *расслоенным произведением* $\operatorname{Spec} B_1$ и $\operatorname{Spec} B_2$ над $\operatorname{Spec} A$ и обозначается $\operatorname{Spec} B_1 \times_{\operatorname{Spec}_A} \operatorname{Spec} B_2$.

Определение 2.14. Чему равно расслоенное произведение $\operatorname{Spec} \mathbb{C} \times_{\operatorname{Spec} \mathbb{R}} \operatorname{Spec} \mathbb{C}$?

Геометрически, расслоенным произведением $X_1 \times_Y X_2$ множеств X_1, X_2 над множеством Y – т.е. множеств X_1, X_2, снабженных отображениями $\pi_1 : X_1 \to Y$, $\pi_2 : X_2 \to Y$ – называется подмножество в $X_1 \times X_2$, состоящее из пар точек $\langle x_1, x_2 \rangle$, $x_1 \in X$, $x_2 \in X_2$ таких, что $\pi_1(x_1) = \pi_2(x_2)$. Алгебраически, это формализуется с помощью тензорного произведения. При этом из-за того, что в алгебраической геометрии нет выделенной абстрактной "точки" – единственная схема, в которую любая другая отображается канонически, это $\operatorname{Spec} \mathbb{Z}$, которое однако никак не точка – понятие расслоенного произведения важнее, чем просто произведение. Это часть общей идеологии (тоже гротендиковской): в алгебраической геометрии надо все утверждения рассматривать относительно, т.е. доказывать их не для просто схемы X, а для схемы X над "базовой" схемой Y. В случае, когда $Y = \operatorname{Spec} k$ – спектр поля, схемы над Y называются для простоты схемами над k.

Отметим, что хотя понятие произведения правильно отображает геометрическую интуицию, оно плохо согласовано с нашим – весьма расширенным – определением того, что такое множество точек. Как говорят американцы, win some, lose some.

Упражнение 2.17. *Докажите, что* $\mathbb{A}^n_k \times_k \mathbb{A}^m_k = \mathbb{A}^{n+m}_k$ *(здесь* $\mathbb{A}^l_k = \operatorname{Spec} k[x_1, \dots, x_l]$ *–* l*-мерное аффинное пространство над полем* k*.*

Упражнение 2.18. *Приведите пример таких схем* $\operatorname{Spec} A_1$, $\operatorname{Spec} A_2$ *над полем* k*, что*

$$\operatorname{Spec}(A_1 \otimes_k A_2) \neq (\operatorname{Spec} A_1) \times (\operatorname{Spec} A_1)$$

(здесь произведение справа понимается как произведение множества точек).

Попробуем теперь применить развитую абстрактную технику для того, чтобы изучить конкретный геометрический объект – разветвленные (и неразветвленные) накрытия.

Определение 2.15. Говорят, что модуль M над кольцом A *локально свободный ранга* n, если для любого простого идеала $\mathfrak{p} \subset A$, $M_{\mathfrak{p}} \cong A_{\mathfrak{p}}^{\oplus n}$.

Мы будем называть морфизм схем $X = \operatorname{Spec} B \to Y = \operatorname{Spec} A$ n*-листным разветвленным накрытием*, или *разветвленным накрытием степени* n, если B – локально свободный A-модуль ранга n. Стандартный пример такой ситуации следующий.

Упражнение 2.19. *Пусть* $B = A[x]/(P(x))$*, где* $P(x)$ *– какой-то полином с коэффициентами из* A *и обратимым старшим коэффициентом. Докажите, что* $\operatorname{Spec} B \to \operatorname{Spec} A$ *– разветвленное накрытие, Какова его степень?*

Мы сначала изучим просто накрытия, неразветвленные, а потом (уже не на этой лекции) изучим ветвление.

В топологии, отображение $f : X \to Y$ хаусдорфовых топологических пространств называется n-листным накрытием, если у каждой точки $y \in Y$ есть такая окрестность $U \subset Y$, что $f^{-1}(U)$ – несвязное объединение n копий U. Эквивалентно, у каждой точки n прообразов, и каждая точка $x \in X$ имеет такую окрестность $U_x \subset X$, что $f : U_x \to f(U_x)$ – гомеоморфизм. В алгебраической геометрии окрестностей слишком мало, но это определение можно пересказать так, что оно будет иметь алгебраический смысл. А именно, рассмотрим произведение $X \times X$, и объединим все окрестности U_x в одну окрестность $U \subset X \times X$ диагонали $X \subset X \times X$. Тогда то условие, что f взаимно-однозначно на U_x, перескажется так: $U \cap X \times_Y X$ есть сама диагональ. Иными словами, диагональ $X \subset X \times_Y X$ открыта в индуцированной топологии. Поскольку X хаусдорфово, она еще и замкнута, а потому является компонентой связности $X \times_Y X$.

Определение 2.16. Морфизм схем $X \to Y$ называется *неразветвленным* если диагональ $X \subset X \times_Y X$ – компонента связности $X \times_Y X$ (иными словами, существует изоморфизм $X \times_Y X \cong X \coprod X'$, где X' – какая-то схема.

Важным частным случаем неразветвленного накрытия является следующее.

Определение 2.17. Морфизм схем $X \to Y$ называется (неразветвленным) *накрытием Галуа* если это n-листное неразветвленное накрытие, и более того, произведение $X \times_Y X$ разлагается в несвязное объединение n схем,

$$X \times_Y X = \coprod_{1 \le i \le n} X_i,$$

причем X_1 это диагональ, и для каждого i проекция $X_i \to X$ на первый сомножитель – изоморфизм.

Это важно вот почему. Любая замкнутая подсхема $X' \subset X \times_Y X$, для которой проекция $X' \to X$ – изоморфизм, есть график какого-то отображения $g : X \to X$ (коммутирующего с проекцией $X \to Y$). Тем самым, если $X \to Y$ – накрытие Галуа, имеем n отображений $g_i : X \to X$. Легко проверить, что график композиции есть пересечение графиков, и поскольку все X_i – компоненты связности, отображения g_i образуют конечную группу G порядка n. Эта группа G называется *группой Галуа* накрытия $X \to Y$. Легко видеть, что множество точек Y отождествляется с множеством G-орбит на множестве точек X; и во всяких других смыслах Y есть фактор X по действию G.

Для простоты, будем теперь работать локально – предположим, что A – локальное кольцо с максимальным идеалом $\mathfrak{m} \subset A$ (и тогда, по нашему предположению, $B = A^{\oplus n}$ как A-модуль). Вот что происходит при накрытии Галуа с кольцом функций.

Лемма 2.18. *Пусть A – локальное кольцо, и пусть $X = \operatorname{Spec} B \to Y = \operatorname{Spec} A$ – накрытие Галуа с группой Галуа G. Тогда $A \subset B$ совпадает с подкольцом $A^G \subset A$ G-инвариантных элементов. Кроме того, B изоморфно $A[G]$ как A-модуль с действием G ($A[G]$ это прямая сумма $|G|$ копий A, на которых G действует перестановками).*

Доказательство. Очевидно, что $A \subset B^G$; надо доказать, что это изоморфизм. По определению G, имеем $B = (B \otimes_A B)^G$, где G действует на второй сомножитель. Но поскольку $B = A^{\oplus n}$ как A-модуль, $B \otimes_A B = A^{\oplus n} \otimes_A B = B^{\oplus n}$, и $(B \otimes_A B)^G = (B^{\oplus n})^G = (B^G)^{\oplus n}$. Поэтому $B = A^{\oplus n} = (B^G)^{\oplus n}$, а стало быть, $A = B^G$. Далее, по определению $B[G] \cong B \otimes_A B$, где G действует на второй сомножитель, и это отображение коммутирует с действием G по первому сомножителю. Переходя к G-инвариантам, получаем изоморфизм $A[G] \cong B$. □

Пусть теперь дано просто неразветвленное n-листное накрытие $X \to Y$. Оказывается, что его можно полностью изучить с помощью накрытий Галуа. А именно, во-первых, имеем следующее наблюдение.

Лемма 2.19. *Пусть дана последовательность схем и разветвленных накрытий $\widetilde{X} \to X \to Y$, причем $\widetilde{X} \to Y$ – неразветвленное накрытие Галуа с группой G, а $\widetilde{X} \to X$ сюръективно. Тогда $\widetilde{X} \to X$ – накрытие Галуа с группой $H \subset G$.*

Доказательство. Расслоенное произведение $\widetilde{X} \times_X \widetilde{X}$ это по определению замкнутая подсхема в $\widetilde{X} \times_Y \widetilde{X}$; поэтому это объединение некоторых из связных компонент $\widetilde{X} \times_Y \widetilde{X}$. □

Тем самым, для любого накрытия Галуа $\widetilde{X}/Y$ “промежуточные” накрытия X/Y нумеруются подгруппами в G.

Далее, рассмотрим n-кратное произведение $X^n_Y = X \times_Y X \times_Y \cdots \times_Y X$. Тогда по индукции оно разлагается в несвязное объединение разных диагоналей (диагональ это подсхема, заданная условиями вида “координаты 1-я, 13-я и 42-я равны”). В частности, имеется открыто-замкнутая подсхема $\widetilde{X} \subset X^n_Y$ которая есть дополнение *ко всем* диагоналям – все координаты попарно не равны.

Упражнение 2.20. *Докажите, что $\widetilde{X} \to Y$ – $n!$-листное разветвленное накрытие, а $\widetilde{X} \to X$ – $(n-1)!$-листное разветвленное накрытие. Указание: сначала рассмотрите случай, когда A – поле; чтобы доказать, что модуль локально тривиален в общем случае, используйте Лемму Накаямы.*

Заметим теперь, что симметрическая группа S_n действует на $\widetilde{X}$, это действие совместимо с проекцией на Y, и в S_n как раз $n!$ элементов, т.е. она транзитивно переставляет листы накрытия; таким образом, $\widetilde{X} \to Y$ – накрытие Галуа с группой $G = S_n$. Аналогично, $H = S_{n-1} \subset G$ переставляет листы накрытия $\widetilde{X} \to X$, и оно тем самым есть накрытие Галуа с группой H.

В классической теории Галуа рассматривают только такие накрытия $X \to Y$, что само X связно; поэтому наше $\widetilde{X}$ не годится, и надо заменить его на его компоненту связности $\widetilde{X}_0$ (любую – они все одинаковые, потому что их переставляет симметрическая группа). Группа Галуа G тогда будет подгруппой в S_n, сохраняющей $\widetilde{X}_0$, а $H = S_{n-1} \cap G \subset S_n$. Все остальное останется как прежде. Таким образом, любое неразветвленное накрытие $X = \operatorname{Spec} B \to Y = \operatorname{Spec} A$ спектра локального кольца A выглядит так: имеется накрытие Галуа $\widetilde{X} = \operatorname{Spec} \widetilde{B} \to Y$ с группой Галуа G, подгруппа $H \subset G$, и $X = \widetilde{X}/H$ – т.е. $B = \widetilde{B}^H$, и $\widetilde{X} \to X$ – накрытие Галуа с группой H.

На следующей лекции мы выясним, как из локальной информации получать глобальную, как измерять ветвление, и когда, в частности, накрытие $\operatorname{Spec} A[x]/(P(x)) \to \operatorname{Spec} A$ неразветвлено.