Лекция 3.

Приведенные и неприводимые схемы, области целостности. Нетеровы модули и кольца. Теорема Гильберта о базисе. Размерность по Круллю (определение). Ассоциированные идеалы, примарные разложения. Плоские модули (определение). Ветвление и дискриминант.

Чтобы продолжить изучение аффинной алгебраической геометрии, нам нужно ввести некоторые ограничения на рассматриваемые кольца. Во-первых, для удобства вводятся следующие понятия.

Определение 3.1. Аффинная схема $X = \operatorname{Spec} A$ называется *приведенной*, если в кольце A нет нильпотентных элементов. Аффинная схема называется *неприводимой*, если X неприводимо как топологическое пространство (с топологией Зарисского).

Упражнение 3.1. *Докажите, что множество нильпотентных элементов кольца A – идеал (этот идеал называется* нильрадикалом *кольца). Докажите, что если $J \subset A$ – нильрадикал, то $\operatorname{Spec} A/J$ – приведенная схема.*

Схема $\operatorname{Spec} A/J$ иногда – очень редко по-русски, чаще по-английски – называется *редукцией* схемы $X = \operatorname{Spec} A$ и обозначается X_{red}. Надо сказать, что “приведенный” по-английски будет “reduced” (а “неприводимый” – “irreducible”).

Лемма 3.2. *Нильрадикал $J \subset A$ кольца A равен пересечению всех его простых идеалов.*

Доказательство. По определению, любой нильпотентный элемент лежит в любом простом идеале. Наоборот, пусть дан элемент $a \in A$. Локализация $A[a^{-1}]$ равна нулю тогда и только тогда, когда a нильпотентен (условие “$1 \sim 0$ в $A[a^{-1}]$ тавтологически эквивалентно $a^n = 0$). Если это не так, то $A[a^{-1}]$ содержит нетривиальный максимальный идеал $\mathfrak{m} \subset A[a^{-1}]$; пересечение $\mathfrak{m} \cap A$ тогда – нетривиальный простой идеал в A, не содержащий a. ☐

Замечание 3.3. Под “пересечением” здесь, by abuse of notation, понимается прооообраз $\mathfrak{m} \subset A[a^{-1}]$ при каноническом отображении $A \to A[a^{-1}]$. Мы иногда и впредь будем говорить про “пересечение $I \cap A \subset A$, имея в виду прообраз идеала $I \subset B$ в каком-то кольце B при заданном отображении $A \to B$.

Следствие 3.4. *Схема $X = \operatorname{Spec} A$ приведенная и неприводимая тогда и только тогда, когда в кольце A нет делителей нуля.*

Доказательство. Если в кольце нет делителей нуля, то там тем более нет нильпотентов, и кроме того, $\{0\} \subset A$ – простой идеал. Легко видеть – и мы это уже обсуждали на Лекции 1 – что $\operatorname{Spec} A$ есть замыкание соотв. своей точки, а потому неприводимо.

В обратную сторону, пусть X неприводима и приведена, и пусть даны $a, b \in A$ с $ab = 0$. Тогда $\operatorname{Spec} A = V((a) \cup V((b))$. Поскольку X неприводимо, $V((a)) = V((b)) = \operatorname{Spec} A$, т.е. любой простой идеал $\mathfrak{p} \subset A$ содержит a (и b). Поэтому оба нильпотентны. ☐

Определение 3.5. Кольцо без делителей нуля называется *областью целостности*, или *целым кольцом* (по-английски domain), а его спектр – *целой схемой.*

Неформально-геометрически, приведенные подсхемы в $\mathbb{A}^n$ это подсхемы “без кратных точек”, а неприводимые – это подсхемы, состоящие из одной компоненты. Как мы видели, избавиться от кратностей можно с помощью канонической операции редукции. Геометрически понятно, что любую приведенную подсхему в $\mathbb{A}^n$ можно, далее, разложить в объединение неприводимых компонент, причем конечного их числа. Но это надо доказывать; более того, если вместо $\mathbb{A}^n$ взять любую аффинную схему X, то это *неверно* – нужно налагать на кольцо какое-то разумное условие конечности. Как показывает практика, правильное условие следующее.

Определение 3.6. Модуль M над кольцом A называется *нетеровым*, если любая возрастающая цепочка подмодулей $M_0 \subset M_1 \subset \dots \subset M$ стабилизируется на конечном шаге, $M_n = M_{n+1}$ для всех n больших некоторой константы N. Кольцо A называется *нетеровым*, есло оно нетерово как модуль над собой (иными словами, любая цепочка идеалов $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \dots \subset A$ стабилизируется на конечном шаге).

Упражнение 3.2. *Любой подмодуль и фактормодуль нетерова модуля тоже нетеров. Наоборот, если $M' \subset M$ и M/M' нетеровы, то M нетеров.*

Упражнение 3.3. *Конечно-порожденный модуль M над нетеровым кольцом A нетеров, нетеров модуль M над нетеровым кольцом A конечно порожден. И оба они конечно представимы.*

Упражнение 3.4. *Если кольцо A нетерово, то любое его факторкольцо $A/\mathfrak{a}$ нетерово. Кроме того, любая локализация $A[S^{-1}]$ тоже нетерова (докажите сначала, что любой идеал $\mathfrak{a} \subset A[S^{-1}]$ имеет вид $(\mathfrak{a} \cap A)[S^{-1}]$).*

Упражнение 3.5. *Кольцо A нетерово тогда и только тогда, когда любой идеал $I \subset A$ конечно порожден.*

Ключевое утверждение, которое показывает осмысленность понятия нетеровости, это естественно нетеровость кольца полиномов $k[x_1, \dots, x_n]$. Это выводится очевидной индукцией из следующего фундаментального факта.

Теорема 3.7 (Теорема Гильберта о базисе.). *Если A – нетерово кольцо, то кольцо полиномов $A[x]$ тоже нетерово.*

Прежде чем доказывать это, расскажем немного про историю. В конце 19го века была модная наука “теория инвариантов” – люди рассматривали алгебру полиномов $k[x_1, \dots, x_n]$, брали какую-то группу G – скажем, конечную – которая как-то действует на векторном пространстве с базисом $x_1, \dots, x_n$, и пытались выразить все “инвариантные многочлены” – в современной терминологии, элементы подкольца $k[x_1, \dots, x_n]^G$ – через некоторый конечный базовый набор. Самая известная теорема такого рода – это что все симметрические многочлены, т.е. инварианты симметрической группы S_n, переставляющей $x_1, \dots, x_n$, выражаются как полиномы от n штук элементарных симметрических полиномов, по одному в каждой степени от 1 до n. Гильберт начал было тоже заниматься этой наукой, но в некоторый момент решил разом закрыть ее – доказать, что конечный набор элементарных полиномов существует для любой группы (причем явно его не выписывая). Это по-видимому одно из первых в математике “доказательств существования”, совершенно неконструктивных (надо сказать что многие, например Кронекер, даже отказывались признавать это доказательством). Ключевой момент в рассуждении Гильберта – это что любой идеал в кольце полиномов конечно порожден. Затем, при аксиоматизации абстрактной алгебры, придумали определение с цепочками, и назвали его в честь Эмми Нетер.

Доказательство. Для любого идеала $I \subset A[x]$, $I^{(n)} = (I \cap x^n A[x]) \mod x^{n+1}$ – идеал в A, причем $I^{(n)} \subset I^{(n+1)}$. Поскольку A нетерово, цепочка идеалов $I^{(n)}$ стабилизируется на каком-то конечном шаге N. Обозначим

$$I^{(\infty)} = I^{(N)} = \bigcup I^{(n)}.$$

Более того, если $I_0 \subset I_1$, то $I_0^{(\infty)} \subset I_1^{(\infty)}$. Поэтому если дана возрастающая цепочка идеалов $I_0 \subset I_1 \subset \cdots \subset A[x]$, то цепочка $I_k^{(\infty)}$ стабилизируется. Выкидывая конечное число элементов, можем считать, что $I_k^{(\infty)} = I_0^{(\infty)} = I_0^{(N)}$. Тогда по определению, для любого $k \geq 0$ и $n \geq N$

$$I_0 \cap x^n A[x] \subset I_k \cap x^n A[x],$$

причем по модулю x^{n+1}, $I_0 \cap x^n A[x] \subset I_k \cap x^n A[x] \subset I_0^{(\infty)}$, и левая часть в этом включении равна правой. Стало быть, обе они равны средней. По индукции, $I_0 \cap x^N A[x] = I_k \cap x^N A[x]$. Поэтому для того, чтобы доказать, что цепочка I_k стабилизируется, достаточно доказать, что стабилизируется цепочка $I_k/(I_k \cap x^N A[x]) \subset A[x]/x^N$. Но $A[x]/x^N$ – конечно-порожденный A-модуль. □

Упражнение 3.6. *Пусть A – нетерово кольцо; докажите, что кольцо формальных рядов $A[[x]]$ тоже нетерово.*

Таким образом, нетеровость сохраняется при переходе к факторкольцам, конечно порожденным алгебрам, локализациям, и даже кольцам формальных рядов. Практически все теоремы алгебраической геометрии требуют предположения нетеровости (хотя и не строго все – иногда, особенно в последнее время, приходится рассматривать и ненетеровы кольца).

Упражнение 3.7. *Пусть $B \subset A$ – подкольцо нетерова кольцо A. Верно ли, что B нетерово? (Рассмотрите, например, $A = k[x, y]$).*

Покажем, что для нетерова кольца A, $\operatorname{Spec} A$ состоит из конечного числа неприводимых компонент.

Лемма 3.8. *Если A – нетерово кольцо, то $X = \operatorname{Spec} A$ есть объединение конечного числа неприводимых замкнутых подмножеств $X_i \subset X$ (называемых* неприводимыми компонентами *X).*

Доказательство. Т.к. кольцо A нетерово, то любая убывающая последовательность $Z_0 \supset Z_1 \supset \cdots \subset X$ стабилизируетыса на конечном шаге (говорят, что X *нетерово топологическое пространство*). Рассмотрим совокупность замкнутых подмножеств в X, которые *нельзя* представить как объединение конечного числа неприводимых замкнутых подмножеств. Тогда в силу нетеровости, эта совокупность, будучи упорядочена по включению, удовлетворяет условию Леммы Цорна. Поэтому, если такие множества вообще есть, то есть и минимальное такое подмножество $Z \subset X$. Оно по условию приводимо, $Z = Z_1 \cup Z_2$, а так как оно минимально, Z_1 и Z_2 уже разлагаются в конечное объединение. Противоречие. □

Надо сказать, что нетеровость дает больше – для спектров нетеровых колец можно построить разумную теорию *размерности* (и по крайней мере локальные кольца будут конечномерны). Это сделал Крулль. Определение следующее.

Определение 3.9. *Размерностью* (круллевской) нетерова кольца A называется максимальная длина цепочки $\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \cdots \subset \mathfrak{p}_n$ вложенных попарно различных простых идеалов в A. *Высотой* простого идеала $\mathfrak{p} \subset A$ называется максимальная длина такой цепочки, строго лежащей в $\mathfrak{p}$.

Таким образом, высота минимального простого идеала равна 0 – такие идеалы отвечают неприводимым компонентам $\operatorname{Spec} A$. Идеалы высоты n отвечают подмногообразиям коразмерности n, и определение Крулля фактически основана на следующем геометрически очевидном наблюдении: если одно неприводимое множество содержит другое, то его размерность должна быть строго больше. Размерность кольца обозначается $\mathsf{dim}\, A$, а высота идеала обозначается $\mathsf{ht}\,\mathfrak{p}$. Формально, легко видеть, что $\mathsf{ht}\,\mathfrak{p} = \mathsf{dim}\, A_{\mathfrak{p}}$. К сожалению, это *все*, что легко видеть – и то, что размерность конечна, и то, что например $\mathsf{dim}\, \mathbb{A}^n = n$, надо доказывать, развив некоторую теорию. Мы этим займемся через некоторое время; но определение размерности полезно продумать уже сейчас.

Упражнение 3.8. *Докажите, что* $\mathsf{dim}\, Z$ *и* $\mathsf{dim}\, k[x]$, k *– поле, обе равны* 1.

Изучим теперь нетеровы модули. Идеальным результатом здесь была бы версия Предложения 2.8: каждый конечно порожденный модуль над нетеровым кольцом разлагается в прямую сумму циклических. Геометрически, модуль “разлагается по точкам спектра”. Ничего подобного в общем случае нет – кольцо полиномов $k[x]$ слишком хорошее (например, имеет размерность 1). Но кое-какие геометрические инварианты по модулю построить можно.

Определение 3.10. *Аннулятором* элемента $m \in M$ A-модуля M называется идеал $\mathsf{Ann}(m) \subset A$ таких элементов $a \in A$, что $am = 0$. *Аннулятором* $\mathsf{Ann}\, M$ всего модуля M называется пересечение $\cap_m \mathsf{Ann}(m) \subset A$. *Носителем* $\operatorname{Supp} M \subset \operatorname{Spec} A$ называется замкнутое подмножество, определенное идеалом $\mathsf{Ann}\, M$.

Поскольку $\mathsf{Ann}\, M$ – идеал, носитель $\operatorname{Supp} M$ имеет также некоторую схемную структуру, но она малоосмыслена. Более полезное понятие такое.

Определение 3.11. Простой идеал $\mathfrak{p} \subset A$ называется *ассоциированным идеалом* для M если $\mathfrak{p} = \mathsf{Ann}(m, M)$ для какого-то $m \in M$. Множество ассоциированных простых идеалов обозначается $\operatorname{Ass}(M)$.

Если A – нетерово кольцо, то множество идеалов вида $\mathsf{Ann}(m, M)$, $m \in M$ очевидным образом удовлетворяет условию Леммы Цорна, а потому имеет максимальные элементы.

Упражнение 3.9. *Любой максимальный элемент множества идеалов* $\mathsf{Ann}(m, M)$, $m \in M$ *– простой идеал. Идеал* $\mathfrak{p} \subset A$ *просто тогда и только тогда, когда* $\mathsf{Ann}(a, A/\mathfrak{p}) = \mathfrak{p}$ *для любого* $a \in A/\mathfrak{p}$, $a \neq 0$.

Таким образом, множество $\operatorname{Ass}(M)$ для модуля M над нетеровым кольцом по крайней мере непусто. На самом деле, некоторые ассоциированные идеалы видны по носителю.

Лемма 3.12. *Минимальные (по включению) элементы множества* $\operatorname{Ass}(M)$ *совпадают с общими точками неприводимых компонент носителя* $\operatorname{Supp}(M)$.

Доказательство. Заменяя A на $A/\mathsf{Ann}(M)$, можем считать, что $\mathsf{Ann}(M) = 0$ и $\operatorname{Supp} M = \operatorname{Spec} A$. Тогда неприводимые компоненты $\operatorname{Spec} A$ отвечают минимальным простым идеалам A, и любой ассоциированный простой идеал содержит хотя бы один минимальный. Таким образом, достаточно доказать, что любой минимальный идеал ассоциированный. Действительно, пусть $\mathfrak{p} \subset A$ – минимальный простой идеал. Тогда, поскольку $\mathsf{Ann}(M) = 0$, локализация $M_{\mathfrak{p}}$ не обращается в ноль, т.е. есть такое $m \in M$, что $\mathsf{Ann}(m, M) \subset \mathfrak{p}$. Рассматривая все такие m, упорядочивая $\mathsf{Ann}(m, M)$ по включению, и беря максимальный $\mathsf{Ann}(m, M)$, заключаем, что есть простой идеал $\mathfrak{p}' = \mathsf{Ann}(m', M) \subset \mathfrak{p}$. Поскольку $\mathfrak{p}$ – минимальный простой идеал, имеем $\mathfrak{p} = \mathfrak{p}'$. $\square$

Определение 3.13. Неминимальные ассоциированные идеалы $\mathfrak{p} \in \mathrm{Ass}(M)$ называются *вложенными.*

Таким образом, множество $\mathrm{Ass}(M)$ это более тонкий инвариант, чем носитель – оно содержит и вложенные идеалы (кстати, "вложенные" здесь относится к соответствующим точкам $\mathrm{Supp}(M)$).

Докажем теперь, что в нетеровой ситуации множество $\mathrm{Ass}(M)$ конечно.

Лемма 3.14. *Пусть M – конечно-порожденный модуль над нетеровым кольцом A. Тогда на M существует конечная фильтрация F_iM, все присоединенные градуированные факторы $\mathsf{gr}_i^F M$ которой имеют вид $A/\mathfrak{p}_i$, $\mathfrak{p}_i$ простой.*

Доказательство. Объясним сначала терминологию. Фильтрацией (возрастающей) на модуле M называется набор подмодулей F_iM, причем $F_iM \subset F_{i+1}M$. Присоединенные градуирвоанные факторы фильтрации – это модули $\mathsf{gr}_i^F M = F_{i+1}M/F_iM$. Эта терминология совершенно общая, бывает и для векторных пространств, и для других "линейно-алгебраических" объектов – ее надо запомнить.

Доказательство же проводится элементарной индукцией. Берем любое $\mathfrak{p}_0 \in \mathrm{Ass}(M)$, так что $\mathfrak{p}_0 = \mathsf{Ann}(m, M)$, и полагаем $F_0M = A \cdot m \subset M$. Легко видеть, что $F_0M \cong A/\mathfrak{p}_0$. Далее заменяем M на M/F_0M. Фильтрация конечна в силу нетеровости. □

Упражнение 3.10. *Пусть $M' \subset M$ – два модуля. Докажите, что* $\mathrm{Ass}(M) \subset \mathrm{Ass}(M') \cup \mathrm{Ass}(M/M')$. *Выведите отсюда и из Леммы* 3.14, *что множество* $\mathrm{Ass}(M)$ *для конечно-порожденного модуля M над нетеровым кольцом A конечно.*

Хочется думать, что идеалы $\mathfrak{p}_0$, появляющиеся в Лемме 3.14, это как раз ассоциированные простые идеалы M. Однако это не так – их, вообще говоря, появляется больше. Доказывать мы это сейчас не будем, но приведем следующее рассуждение. Если модуль M над областью целостности A локально тривиальный, то $\mathsf{Ann}(M) = 0$ (почему?). Тогда $\mathrm{Ass}(M)$ состоит из нулевого идеала. Но, как мы вскоре докажем, если мы модуль допускал фильтрацию F_iM с $\mathsf{gr}_i^F = A$, то он был бы тривиальным, а не только локально тривиальным. То, что происходит, описано в следующем упражнении.

Упражнение 3.11. *В ситуации Упражнения* 3.10, *приведите пример, когда объединение множеств* $\mathrm{Ass}(M')$ *и* $\mathrm{Ass}(M/M')$ *строго больше, чем* $\mathrm{Ass}(M)$ *(положите, например, $A = \mathbb{Z}$, $M = \mathbb{Z}$).*

Даже если новых простых идеалов при переходе к $\mathsf{gr}_\bullet^F M$ не появляется, у нас все равно есть не разложение в прямую сумму, а только фильтрация. Какие-то теоремы о разложении тоже можно доказать, но они довольно слабые, и применяются редко. Важное понятие здесь такое.

Определение 3.15. Пусть $\mathfrak{p} \subset A$ – простой идеал. Говорят, что подмодуль $M' \subset M$ – в частности, идеал $\mathfrak{a} \subset A$ – *примарный, отвечающий* $\mathfrak{p}$, если $\mathrm{Ass}(M/M') = \{\mathfrak{p}\}$.

Упражнение 3.12. *Пусть A – нетерово локальное кольцо с максимальным идеалом $\mathfrak{m} \subset A$. Докажите, что идеал $\mathfrak{a} \subset A$ примарный тогда и только тогда, когда $\mathfrak{m}^n \subset \mathfrak{a}$ для какого-то $n \geq 1$.*

Типичная "теорема о примарном разложении" выглядит так.

Предложение 3.16. *Пусть M – конечно-порожденный модуль над нетеровым кольцом A, а $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ – все ассоциированные с ним идеалы. Тогда существует вложение*

$$M \hookrightarrow \bigoplus_{1 \le i \le n} M/N_i,$$

где $N_i \subset M$ – примарный подмодуль, отвечающий $\mathfrak{p}_i$, причем ни одно из слагаемых в правой части нельзя исключить.

Доказательство. Будем говорить, что подмодуль $N \subset M$ неразложимый, если его нельзя представить как пересечение $N = N_1 \cap N_2$ собственных подмодулей $N_1, N_2 \subset M$. Неразложимый подмодуль, очевидно, примарен (если у фактора M/N два разных ассоциированных идеала $\mathfrak{p}_1$, $\mathfrak{p}_2$, то в нем есть по крайней мере два разных собственных подмодуля $(A/\mathfrak{p}_1), (A/\mathfrak{p}_2) \subset M/N$. Т.к. M нетеров, $0 \subset M$ можно представить как конечное пересечение $N_1 \cap \dots \cap N_m$ неразложимых собственных подмодулей $N_i \subset M$, причем так, что ни один из них нельзя исключить. Тогда $M \subset \bigoplus(M/N_i)$, поэтому $\mathrm{Ass}(M) \subset \cup_i Ass(M/N_i)$, и осталось доказать, что это равенство – простой идеал $\mathfrak{p}_i$, ассоциированный с каждым из M/N_i, ассоциирован также и с M. Действительно, переставляя слагаемые, видим, что достаточно проверить $i = 1$. Поскольку в разложении $N_1 \cap \dots \cap N_m = 0$ ничего нельзя исключить, отображение

$$\varphi : M \to \bigoplus_{i \ge 2} M/N_i$$

уже не вложение. Его ядро $\mathsf{Ker}\,\varphi$ тогда вкладывается в M/N_1, в силу чего $\mathrm{Ass}(\mathsf{Ker}\,\varphi) \subset \mathrm{Ass}(M/N_1) = \{\mathfrak{p}_1\}$, $\mathfrak{p}_1$ ассоциирован с $\mathsf{Ker}\,\varphi$, а следовательно, и с $M \supset \mathsf{Ker}\,\varphi$. □

Такого типа теоремы обобщают соответствующие утверждения про идеалы, которые в свою очередь происходят из теории чисел – заменяя элементы кольца $a \in A$ на соответствующие идеалы $(a) \subset A$, люди пытались восстановить в произвольном кольце алгебраических чисел разложение на простые множители. Примарный идеал – это обобщение идеала вида $(p^n) \subset \mathbb{Z}$, p простое (термин происходит оттуда же – по-английски примарный будет primary, а простой – prime). Но со временем вся эта деятельность заглохла, и кажется, особо глубокого смысла в ней нет.

Последнее, что хотелось бы сегодня рассказать про модули – это про понятие *плоского модуля.* Пусть M – модуль над кольцом A, и пусть для простоты A – область целостности. Если M локально тривиальный, то $\mathsf{Ann}(M) = 0$, и $\mathrm{Ass}(M)$ состоит только из нулевого идеала $0 \subset A$. Однако же обратное, хотя и верно для $k[x]$ и других хороших колец, в общем случае ни в коем случае неверно – есть огромный зазор между модулями M с нулевым аннулятором (они называются *модули без кручения*) и локально-тривиальными модулями. Чтобы удобным образом охарактеризовать локально-тривиальные модули, применяют методы гомологической алгебры. Главное определение такое.

Определение 3.17. Модуль M над кольцом A называется *плоским*, если для любой точной последовательности

$$N_1 \longrightarrow N_2 \longrightarrow N_3$$

последовательность

$$N_1 \otimes M \longrightarrow N_2 \otimes M \longrightarrow N_3 \otimes M$$

тоже точна.

Напомним, что (Упражнение 2.11) слова “последовательность точна” означают, что образ левого отображения равен ядру правого. Из того же упражнения следует, что для любой мультипликативной системы S, $A[S^{-1}]$ – плоский A-модуль. Нетрудно также показать, что локально-тривиальный модуль тоже плоский. A priori непонятно, почему плоскость это разумное свойство, и какое отношение имеют точные последовательности к интересующим нас конкретным геометрическим вещам. Оказывается, однако, что свойства точности можно эффективно контролировать – имеется мощный систематический формализм, который позволяет многие вещи поссчитать. В частности, довольно часто нетрудно доказать, что тот или иной модуль плоский. А с другой стороны, можно доказать, например, что любой конечно-порожденный плоский модуль локально тривиален. К сожалению, все эти утверждения несложные, но только после того, как построена некоторая отдельная наука. Мы это сделаем, но через некоторое время. Пока что, полезно запомнить определение плоскости, иметь в виду что это разумное понятие, а реально воспринимать "плоскость" конечно-порожденного модуля как другое название для локальной тривиальности.

Поговорим теперь о разветвленных накрытиях. Напомним, что *развевленным накрытием* степени n аффинной схемы $Y = \operatorname{Spec} A$ мы называли такую схему X/Y, $X = \operatorname{Spec} B$, что B – локально тривиальный A-модуль ранга n. Накрытие называлось *неразветвленным*, если $X \times_Y X$ разлагается в несвязное объединение $X \times_Y X = X \coprod X'$ диагонали и какой-то схемы X'. Неразвевленное накрытие называется *накрытием Галуа*, если $X \times_Y X$ разлагается и дальше, в объединение n штук схем X_i, которые все изоморфны X. Напомним также, что мы, для простоты, работаем локально по Y, т.е. предполагаем, что A – локальное кольцо с максимальным идеалом $\mathfrak{m} \subset A$ (и соответственно, $B = A^n$ как A-модуль).

Сегодня мы выведем некоторый критерий неразветвленности (и способ измерять ветвление). Для этого удобно воспользоваться следующей линейной алгеброй. Пусть $M \cong A^n$ – свободный модуль над кольцом A. Будем говорить, что билинейная форма $Q : M \otimes_A M \to A$ *невырождена*, если соответствующее отображение $M \to M^*$ обратимо (здесь M^* – двойственный модуль, т.е. множество всех A-линейных отображений $M \to A$; легко видеть, что это A-модуль, и раз $M \cong A^n$, то M^* тоже свободный ранга n). Выбирая изоморфизм $M \cong A^n$, т.е. базис в M, формы Q можно записать матрицей; тогда $\mathsf{det}\, Q \in A$ – детерминант этой матрицы – есть также детерминант отображения $M \to M^*$, а потому форма Q невырождена тогда и только тогда, когда $\mathsf{det}\, Q$ обратим.

Важно понимать, что $\mathsf{det}\, Q$ зависит от выбора базиса в M, так что он *не определен однозначно.* Однако переход к другому базису задается матрицей, детерминант которй обратим. Поэтому *идеал* $(\mathsf{det}\, Q) \subset A$ уже определен однозначно (в инвариантных терминах, это есть образ канонического отображения $\mathsf{det}_A(M) \otimes \mathsf{det}_A(M) \to A$, полученного из отображения $\mathsf{det}(Q) : \mathsf{det}_A(M) \to \mathsf{det}_A(M^*) = \mathsf{det}_A(M)^*$; $\mathsf{det}_A M$ значит старшую внешнюю степень свободного модуля M). Форма невырождена тогда и только тогда, когда $(\mathsf{det}\, Q) = A$.

Упражнение 3.13. *Пусть M – свободный A-модуль, снабженный невырожденной билинейной формой Q, и пусть $\varphi : M \to M_1$ – сюръективный гомоморфизм на свободный A-модуль M_1. Тогда существует ортогональное разложение $M = \mathsf{Ker}\, \varphi \oplus M'$ по отношению к Q, и φ отождествляет M' и M_1.*

Рассмотрим теперь разветвленное накрытие $X = \operatorname{Spec} B \to Y = \operatorname{Spec} A$. По нашим предположениям, $B = A^n$ – свободный A-модуль. На нем можно канонически ввести билинейную форму Q, положив

$$Q(b_1, b_2) = \mathsf{tr}(b_1 b_2)$$

(здесь $b_1 b_2$ – вернее, умножение на него – понимается как эндоморфизм свободного A-модуля B, а tr – это его след). Эта форма очевидно обладает следующим дополнительным свойством:

$$Q(b_1 b_2, b_3) = Q(b_1, b_2 b_3). \tag{3.1}$$

Детерминант этой формы Q – вернее, соответствующий идеал в A – называется *дискриминантом* накрытия X/Y и обозначается $\mathsf{disc}(B/A) \subset A$.

Лемма 3.18. *Накрытие X/Y неразветвлено тогда и только тогда, когда форма* $\mathsf{tr}(b_1 b_2)$ *невырождена, т.е.* $\mathsf{disc}(B/A) = A$.

Доказательство. Если следовая форма B/A невырождена, то следовая форма $(B \otimes_A B)/B$ тоже невырождена (их детерминанты тождественно равны). Поэтому имеем ортогональное разложение $B \otimes_A B = B \oplus \mathsf{Ker}\,\varphi$, где $\varphi : B \otimes_A B \to B$ – отображение умножения (геометрически, вложение диагонали). Из (3.1) немедленно следует, что это разложение в сумму подалгебр, т.е. накрытие X/Y неразветвлено.

Пусть теперь накрытиес неразветвлено. Представим его как фактор накрытия Галуа $\widetilde{X} \to Y$ – иными словами, выберем такое накрытие Галуа $\widetilde{X}/Y$, что $\widetilde{X} \times_Y X$ есть несвязное объединение n копий $\widetilde{X}$ (почему это можно сделать, мы обсуждали в прошлый раз). Тогда дискриминант X/Y тождественно такой же, как дискриминант $\widetilde{X} \times_Y X$ над $\widetilde{X}$, и он обратим, поскольку следовая форма n копий $\widetilde{X}$ представляется, очевидно, единичной матрицей. □

Название "дискриминант" берется из частного случая $B = A[x]/(P(x))$, где $P(x)$ – многочлен степени n с обратимым старшим членом. Тогда у нас есть готовый базис $1, x, \dots, x^{n-1}$ в B, и $\mathsf{disc}\, B/A$ можно понимать как элемент кольца A; причем понятно, что он задается явной универсальной формулой от коэффициентов полинома $P(x)$. Нам эта формула не понадобится (если хотите, можете проверить что для квадратичного многочлена $x^2 + px + q$ получается, с точностью до знака, $p^2 - 4q$). Заметим только, что если $P(x)$ разложен на линейные множители, $P(x) = (x - \alpha_1) \cdots (x - \alpha_n)$, то можно выписать дискриминант в другом естественном базисе и получить, что – с точностью до обратимого элемента кольца A – имеем

$$\mathsf{disc}\, P(x) = \mathsf{disc}\, B/A = \prod_{i \neq j} (\alpha_i - \alpha_j).$$

Т.е. – как и должно быть из геометрических соображений – дискримимант равен нулю тогда и только тогда, когда у $P(x)$ есть кратные корни. Отметим также, что наличие кратных корней можно проверять по другому – кратный корень $P(x)$ это общий корень $P(x)$ и производной $P'(x)$, поэтому можно взять результант $\mathsf{Res}(P(x), P'(x))$. Оказывается, что получится то же самое – с точностью до знакае имеем $\mathsf{disc}\, P(x) = \mathsf{Res}(P(x), P'(x))$. Это можно доказывать либо честно, либо с помощью обманного трюка – свести все к ситуации, когда A поле, затем заменить его на такое расширение, что $P(x)$ разлагается на линейные множители, и сравнить формулы: для любых $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$, $g(x) = (x - \beta_1) \cdots (x - \beta_m)$ имеем

$$\mathsf{Res}(f(x), g(x)) = \prod_{i,j} (\alpha_i - \beta_j) = \pm \prod_i g(\alpha_i),$$

а потому

$$\mathsf{Res}(P(x), P'(x)) = \pm \prod_i P'(\alpha_i) = \pm \prod_i \prod_{j \neq i} (\alpha_i - \alpha_j) = \mathsf{disc}\, P(x).$$

Нам это все пока не понадобится. Отметим на будущее две вещи: (1) в науке про ветвление появляется производная $P'(x)$, как мы в дальнейшем увидим, появляется она по делу, и (2) если A поле характеристики 0, а $P(x)$ – неприводимый многочлен (так что B тоже поле), то производная $P'(x)$ имеет меньшую степень, чем $P(x)$, а потому $P(x)$ и $P'(x)$ должны быть взаимно просты. Поэтому автоматически $\mathsf{Res}(P(x), P'(x)) \neq 0$, и B/A неразветвлено (в науке про поля традиционно говорят "сепарабельно"). Но в характеристике p этот трюк не проходит, в силу следующего восхитительного явления – производная $P'(x)$ может быть тавтологически равна нулю! А именно, если $P(x) = x^p$ – или, более общо, $P(x) = Q(x^p)$ для какого-то полинома $Q(x)$ – то $P'(x)$ это полином, все коэффициенты которого делятся на p, а потому обращаются в ноль.

Упражнение 3.14. *Пусть* $k = (\mathbb{Z}/p\mathbb{Z})(t)$ *– поле рациональных* $(\mathbb{Z}/p\mathbb{Z})$*-значных функций от одной переменной, и пусть* $k' = k[x]/(x^p - t)$ *–* p*-листное накрытие* k*. Докажите, что* k' *поле, и вычислите* $k' \otimes_k k'$ *(в частности, выясните, сколько точек у* $\operatorname{Spec}(k' \otimes_k k')$*). Чему равна следовая форма* $\mathsf{tr}(b_1 b_2)$ *на* k'/k*?*

Приведем теперь более геометрический пример ветвления. А именно, положим $A = k[t]$, причем будем считать, что $\mathsf{char}\, k$ не делит число n, и положим $B = A[x]/(x^n - t)$. Иными словами, мы добавили к A корень n-й степени из t.

Упражнение 3.15. *Докажите, что* $\operatorname{Spec} B \otimes_A B$ *это объединение* n *прямых, каждая из которых изоморфна* $\operatorname{Spec} B$*.*

Таким образом, B/A разветвлено, но тем не менее ведет себя в точности как накрытие Галуа – $\operatorname{Spec} B \otimes_A B$ разлагается в объединение n копий $\operatorname{Spec} B$! Только для накрытий Галуа объединение было несвязным, и n копий $\operatorname{Spec} B$ были компонентами связности; а здесь они пересекаются, и это только неприводимые компоненты. Тем не менее, они все равно графики отображений $g_i : B \to B$.

Упражнение 3.16. *В описываемом примере, проверьте, что отображения* g_i *образуют группу* $\mathbb{Z}/n\mathbb{Z}$*, и что* $B = A[\mathbb{Z}/n\mathbb{Z}]$ *как* A*-модуль с действием* $\mathbb{Z}/n\mathbb{Z}$*.*

Мы видим, по крайней мере некоторые факты теории Галуа верны и для разветвленных накрытий. Оказывается, что (1) верно довольно много, и (2) рассмотренный пример в значительной степени общий – например, если перейти к кольцу $k[[t]]$ формальных рядов от t и наложить некоторые разумные условия на кольцо B, то оно *всегда* будет иметь вид $A[x]/(x^n - t)$. Но это мы обсудим в следующий раз.