Лекция 19.

Род кривой. Теорема Римана–Роха. Теорема Гурвица. Гиперэллиптические кривые. Каноническое вложение. Эллиптические кривые.

Род кривой

Пусть X — проективная схема над полем k. Тогда $H^0(X, \mathcal{O}_X)$ — коммутативная алгебра над k, причем конечномерная в силу проективности схемы X. Заметим, что если схема X целая, то алгебра $H^0(X, \mathcal{O}_X)$ не имеет делителей нуля, значит является полем K, конечным расширением поля k. В этом случае всякое локальное кольцо схемы X имеет естественную структуру K-алгебры, то есть X является схемой над K, а струтурный морфизм $X \to \operatorname{Spec} k$ представляется в виде композиции $X \to \operatorname{Spec} K \to \operatorname{Spec} k$ (факторизация Штейна!). Если расширение K/k нетривиально, то при переходе от X к $X \otimes \overline{k}$, наша схема перестает быть связной (если K/k сепарабельно), или приобретает нильпотенты (если K/k чисто несапарабельно), или происходит и то и другое.

Определение 19.1. Схема X называется *геометрически связной* (*геометрически приведенной*, *геометрически целой*, и т.д.), если схема $X \otimes \overline{k}$ связна (приведена, цела и т.д.).

Напомним, что кривой называется геометрически целая отделимая одномерная схема над полем k. В прошлом семестре мы доказали, что всякая собственная кривая проективна.

Определение 19.2. *Арифметический род* кривой C — это число $p_a(C) = \dim H^1(C, \mathcal{O}_C)$. *Геометрический род* кривой C — это число $p_g(C) = \dim H^0(C, \Omega_C)$.

Лемма 19.3. *Если C — неособая проективная кривая, то $p_a(C) = p_g(C)$.*

Доказательство. Это непосредственно следует из двойственности Серра. □

Так как арифметический род гладкой проективной кривой равен геометрическому роду, его называют также просто *родом* и обозначают g. Род кривой — важнейший (и, более того, единственный) ее дискретный инвариант. Заметим, что род — всегда неотрицателен!

Важнейшим вычислительным средством изучения кривых является следующая

Теорема 19.4 (теорема Римана–Роха). *Пусть D — дивизор на гладкой проективной кривой C рода g над полем k. Тогда*

$$\dim_k H^0(C, \mathcal{O}_C(D)) - \dim_k H^1(C, \mathcal{O}_C) = \deg D + 1 - g.$$

Доказательство. Пусть вначале $D = 0$. Тогда $\mathcal{O}_C(D) = \mathcal{O}_C$, $H^0(C, \mathcal{O}_C) = k$ (так как C геометрически цела и проективна) и $\dim H^1(C, \mathcal{O}_C) = p_a(C) = g$ по определению рода, поэтому требуемое равенство очевидно выполняется.

Пусть теперь D — произвольный дивизор и P — точка кривой C. Рассматривая точку P как дивизор, получаем обратимый пучок $\mathcal{O}_C(P)$ и его регулярное сечение $s \in H^0(C, \mathcal{O}_C(P))$, дивизор которого совпадает с P. Сечение s задает гомоморфизм $\mathcal{O}_C(-P) \to \mathcal{O}_C$. Легко видеть, что он является вложением, а его коядро — структурный пучок точки P. Иначе говоря, имеем точную последовательность

$$0 \to \mathcal{O}_C(-P) \to \mathcal{O}_C \to \mathcal{O}_P \to 0.$$

Подкручивая ее на обратимый пучок $\mathcal{O}_C(D)$, получаем точную последовательность

$$(*) \qquad 0 \to \mathcal{O}_C(D-P) \to \mathcal{O}_C(D) \to \mathcal{O}_P \to 0$$

(заметим, что $\mathcal{O}_P \otimes \mathcal{O}_C(D) \cong \mathcal{O}_P$, так как пучок $\mathcal{O}_C(D)$ в окрестности точки P изоморфен пучку $\mathcal{O}_C$). Заметим, что $H^1(C, \mathcal{O}_P) = H^1(P, \mathcal{O}_P) = 0$, $H^0(C, \mathcal{O}_P) = k(P)$. В частности, $\chi(\mathcal{O}_P) = \mathsf{dim}_k\, k(P) = \mathsf{deg}\, P$, следовательно, $\chi(\mathcal{O}_C(D)) = \chi(\mathcal{O}_C(D-P)) + \mathsf{deg}\, P$. Итак, мы видим, что теорема Римана–Роха для дивизора D выполняется тогда и только тогда, когда она выполняется длядивизора $D - P$. Остается заметить, что всякий дивизор получается из нулевого конечным числом операций прибавления или убавления точки. □

Упражнение 19.1. *Покажите, что* $\mathsf{dim}\, H^0(C, \mathcal{O}_C(D)) \le \mathsf{deg}\, D + 1 - g$.

Замечание 19.5. Из точной последовательности когомологий последовательности $(*)$

$$0 \to H^0(C, \mathcal{O}_C(D-P)) \to H^0(C, \mathcal{O}_C(D)) \to k(P) \to H^1(C, \mathcal{O}_C(D-P)) \to H^1(C, \mathcal{O}_C(D)) \to 0$$

следует, что $\mathsf{dim}\, H^0(C, \mathcal{O}_C(D)) - \mathsf{deg}\, k(P)/k \le \mathsf{dim}\, H^0(C, \mathcal{O}_C(D-P)) \le \mathsf{dim}\, H^0(C, \mathcal{O}_C(D))$ и $\mathsf{dim}\, H^1(C, \mathcal{O}_C(D)) \le \mathsf{dim}\, H^1(C, \mathcal{O}_C(D-P)) \le \mathsf{dim}\, H^1(C, \mathcal{O}_C(D)) + \mathsf{deg}\, k(P)/k$. В частности, если k алгебраически замкнуто (и, значит, $k(P) = k$), то

$$\begin{array}{lll} \text{либо } \mathsf{dim}\, H^0(C,\mathcal{O}_C(D-P)) = \mathsf{dim}\, H^0(C,\mathcal{O}_C(D)) - 1 & \text{и} & \mathsf{dim}\, H^1(C,\mathcal{O}_C(D-P)) = \mathsf{dim}\, H^1(C,\mathcal{O}_C(D)), \\ \text{либо } \mathsf{dim}\, H^0(C,\mathcal{O}_C(D-P)) = \mathsf{dim}\, H^0(C,\mathcal{O}_C(D)) & \text{и} & \mathsf{dim}\, H^1(C,\mathcal{O}_C(D-P)) = \mathsf{dim}\, H^1(C,\mathcal{O}_C(D)) + 1. \end{array}$$

Напомним, что каноническим дивизором называется такой дивизор K, что $\mathcal{O}(K) \cong \omega$.

Следствие 19.6. *Пусть* K_C *— канонический дивизор на кривой* C. *Тогда* $\mathsf{deg}\, K_C = 2g - 2$.

Доказательство. По двойственности Серра $\mathsf{dim}\, H^0(C, \mathcal{O}_C(K_C)) = g$, $\mathsf{dim}\, H^1(C, \mathcal{O}_C(K_C)) = 1$, поэтому $\chi(\mathcal{O}_C(K_C)) = g - 1$. Остается воспользоваться теоремой Римана–Роха. □

Сформулированная нами теорема Римана–Роха является частным случаем общей теоремы Римана–Роха–Хирцебруха, вычисляющей эйлерову характеристику произвольного когерентного пучка на гладком проективном многообразии через топологические инварианты пучка (характер Черна) и топологические инварианты многообразия (класс Тодда касательного расслоения).

Теорема Гурвица

Как вычислить род кривой? Ясно, что ответ на этот вопрос зависит от того, как задана кривая. Основные способы — это представление кривой в виде накрытия другой кривой, либо вложение в многообразие большей размерности. Сегодня мы изучим первый способ.

Пусть $f : X \to Y$ — конечный морфизм кривых. Так как он автоматически доминантен, ему соответствует вложение полей $K(Y) \subset K(X)$, причем $\mathsf{deg}\, f = \mathsf{deg}\, K(X)/K(Y)$. Накрытие f называется *сепарабельным*, если сепарабельно расширение полей $K(X)/K(Y)$. Ясно, что в характеристике 0 всякое накрытие сепарабельно, а в характеристике p степень любого чисто несепарабельного накрытия равна p^n.

Упражнение 19.2. *Покажите, что если* $K(X)/K(Y)$ *чисто немепарабельное расширение, то* $f : X \to Y$ *— степень морфизма Фробениуса. В частности,* $X \cong Y$ *и* $g(X) = g(Y)$.

Лемма 19.7. *Пусть* $f : X \to Y$ *— сепарабельный конечный морфизм кривых. Тогда последовательность пучков*

$$0 \to f^*\Omega_Y \to \Omega_X \to \Omega_{X/Y} \to 0$$

точна. В частности, $\Omega_{X/Y}$ *— пучок кручения на* X.

Доказательство. Пучки $f^*\Omega_Y$ и Ω_X обратимы, так как X и Y гладкие и X приведена. Поэтому достаточно проверить, что морфизм $f^*\Omega_Y \to \Omega_X$ нетривиален в общей точке. Но в общей точке последовательность имеет вид

$$\Omega_{K(Y)/k} \otimes_{K(Y)} K(X) \to \Omega_{K(X)/k} \to \Omega_{K(X)/K(Y)} \to 0,$$

причем $\Omega_{K(X)/K(Y)} = 0$ так как расширение $K(X)/K(Y)$ конечно и сепарабельно. Следовательно, интересующий нас морфизм сюръективен, а значит и нетривиален. $\square$

Итак, чтобы найти связь между пучками Ω_X и $f^*\Omega_Y$ надо описать пучок относительных дифференциалов. Предположим, что поле k алгебраически замкнуто. Пусть $x \in X$, $y = f(x) \in Y$ — замкнутые точки, а $t \in \mathcal{O}_{X,x}$ и $u \in \mathcal{O}_{Y,y}$ — униформизующие. Тогда $f^*u = at^e$, где e — целое число, а a — обратимый элемент в $\mathcal{O}_{X,x}$. Напомним, что e называется индексом ветвления морфизма f в точке x. Если характеристика поля k положительна и делит индекс ветвления e, говорят что ветвление *сильное* (иначе говорят, что ветвление *слабое*).

Лемма 19.8. *Слой пучка $\Omega_{X/Y}$ в замкнутой точке $x \in X$ является циклическим модулем, $\Omega_{X/Y,x} \cong \mathcal{O}_{X,x}/\mathfrak{m}_x^r$, причем $r = e-1$, если ветвление слабое, и $r \ge e$, если ветвление сильное.*

Доказательство. Ясно, что $\Omega_{X,x} \cong \mathcal{O}_{X,x}dt$, $(f^*\Omega_Y)_x \cong \mathcal{O}_{X,x}du$. Остается заметить, что $du = d(at^e) = eat^{e-1}dt + t^e da$. $\square$

Дивизор $R = \sum_{P \in X} r_P P$, где r_P — длина $\mathcal{O}_{X,P}$-модуля $\Omega_{X/Y,P}$ называется *дивизором ветвления* морфизма f (сумма конечна, так как $r_P \ne 0$ только для $P \in \operatorname{supp} \Omega_{X/Y}$, а носитель когерентного пучка — замкнутое множество).

Теорема 19.9 (Теорема Гурвица). *Пусть $f : X \to Y$ — сепарабельное накрытие степени n кривых над алгебраически замкнутым полем. Тогда*

$$K_X = f^*K_Y + R.$$

В частности,

$$2g(X) - 2 = n(2g(Y) - 2) + \mathsf{deg}\, R.$$

Доказательство. Подкрутим точную последовательность леммы 19.7 на пучок Ω_X^{-1}:

$$0 \to \Omega_X^{-1} \otimes f^*\Omega_Y \to \mathcal{O}_X \to \Omega_X^{-1} \otimes \Omega_{X/Y} \to 0.$$

Из леммы 19.8 следует, что $\Omega_X^{-1} \otimes \Omega_{X/Y} \cong \mathcal{O}_R$, значит $\Omega_X^{-1} \otimes f^*\Omega_Y \cong \mathcal{O}_X(-R)$, откуда получаем первое равенство. Сравнивая степени и пользуясь тем, что при обратном образе степень дивизора умножается на степень морфизма, получаем второе равентство. $\square$

Замечание 19.10. Ясно, что теорема Гурвица выполняется и над незамкнутыми полями — весь вопрос здесь в вычислении дивизора ветвления через индексы ветвления в точках. Ясно, что надо учитывать возникающие расширения полей $k(x)/k(y)$. Если, например, расширение $k(x)/k(y)$ сепарабельно, то при переходе от k к $\overline{k}$ точка x распадается на $\mathsf{deg}\, k(x)/k(y)$ точек с равными индексами ветвления, а если расширение $k(x)/k(y)$ чисто несепарабельно, то при переходе к $\overline{k}$ в точке x возникает дополнительное сильное ветвление.

Упражнение 19.3. *Сформулируйте и докажите теорему Гурвица над незамкнутым полем.*

Из теоремы Гурвица вытекает множество следствий.

Упражнение 19.4. *Пусть $f : X \to Y$ — этальное накрытие степени n. Покажите, что $g(X) = ng(Y) - n + 1$. В частности, не существует этальных накрытий над $\mathbb{P}^1$.*

Следствие 19.11 (теорема Люрота). *Если $f : \mathbb{P}^1 \to C$ — накрытие, то $g(C) = 0$.*

Доказательство. Раскладывая расширение $K(\mathbb{P}^1)/K(C)$ на чисто несепарабельное и сепарабельное расширения, и пользуясь упражнением 19.2, сводим все к случаю чисто сепарабельного расширения. В этом случае из теоремы Гурвица следует, что $g(C) = 0$, так как $\deg R \geq 0$. □

Упражнение 19.5. *Пусть X — кривая рода 1. Если $f : X \to Y$ — накрытие, то либо $g(Y) = 0$, либо $g(Y) = 1$ и f — этальный морфизм.*

Обильность дивизоров на кривой

Теорема Римана–Роха вычисляет эйлерову характеристику обратимого пучка. Простые дополнительные соображения в некоторых случаях позволяют явно вычислить все его когомологии.

Лемма 19.12. *Пусть D — дивизор на кривой C. Если $\deg D < 0$, то $H^0(C, \mathcal{O}_C(D)) = 0$. Если $\deg D = 0$ и $D \not\sim 0$, то $H^0(C, \mathcal{O}(D)) = 0$.*

Доказательство. Пусть $H^0(C, \mathcal{O}_C(D)) \neq 0$. Пусть s — нетривиальное сечение пучка $\mathcal{O}_C(D)$ и D' — его дивизор нулей. Тогда $D' \geq 0$ и $D' \sim D$. Значит $\deg D = \deg D' \geq 0$. Причем если $\deg D = 0$, то $\deg D' = 0$, следовательно $D' = 0$. □

Следствие 19.13. *Если $\deg D > 2g-2$, то $H^1(C, \mathcal{O}_C(D)) = 0$. Если $\deg D = 2g-2$ и $D \not\sim K_C$, то $H^1(C, \mathcal{O}(D)) = 0$.*

Доказательство. Согласно двойственности Серра $H^k(C, \mathcal{O}_C(D)) \cong H^{1-k}(C, \mathcal{O}_C(D)^{-1} \otimes \omega_C)^*$, но $\mathcal{O}_C(D)^{-1} \otimes \omega_X \cong \mathcal{O}_C(K_C - D)$ и $\deg(K_C - D) = 2g - 2 - \deg D$. □

Дивизор D на кривой C называется *неспециальным*, если $H^1(C, \mathcal{O}_C(D)) = 0$. Только что мы проверили, что всякий дивизор степени $\geq 2g - 1$ неспециален. Заметим, что для неспециальных дивизоров теорема Римана–Роха вычисляет размерность пространства глобальных сечений.

Лемма 19.14. *Пусть D — дивизор на кривой рода g. Рассмотрим полную линейную систему $|D|$. Если $\deg D \geq 2g$, то $|D|$ не имеет базисных точек. Если $\deg D \geq 2g + 1$, то $|D|$ очень обильна.*

Упражнение 19.6. *Пусть δ — линейная система на схеме X. Докажите, что δ не имеет базисных точек (очень обильна) тогда и только тогда, когда она не имеет базисных точек (очень обильна) на схеме $X \otimes \overline{k}$.*

Доказательство. В силу упражнения можно считать поле k алгебраически замкнутым. Пусть P — базисная точка линейной системы $|D|$, то есть всякий дивизор, линейно эквивалентный D проходит через P. Значит $\dim H^0(C, \mathcal{O}_C(D - P)) \geq \dim H^0(C, \mathcal{O}_C(D))$. Но при $\deg D \geq 2g$ оба дивизора D и $D - P$ неспециальны, поэтому приведенное неравенство противоречит теореме Римана–Роха.

Предположим теперь, что линейная система $|D|$ не имеет базисных точек, но не разделяет точки P и Q, то есть всякий дивизор, линейно эквивалентный D и проходящий, например, через P проходит и через Q. Значит $\dim H^0(C, \mathcal{O}_C(D-P-Q)) \geq \dim H^0(C, \mathcal{O}_C(D-P))$. Но при $\deg D \geq 2g+1$ оба дивизора $D-P$ и $D-P-Q$ неспециальны, поэтому приведенное неравенство противоречит теореме Римана–Роха.

Наконец, пусть линейная система не разделяет касательные векторы в точке P, то есть всякий дивизор, линейно эквивалентный D и проходящий через P имеет в точке P кратность ≥ 2. Значит $\dim H^0(C, \mathcal{O}_C(D-2P)) \geq \dim H^0(C, \mathcal{O}_C(D-P))$. Но при $\deg D \geq 2g+1$ оба дивизора $D-2P$ и $D-P$ неспециальны, поэтому приведенное неравенство противоречит теореме Римана–Роха. □

Полученные результаты уже позволяют ответить на первые классификационные вопросы.

Лемма 19.15. *Пусть C кривая рода 0 над алгебраически замкнутым полем. Тогда $C \cong \mathbb{P}^1$.*

Доказательство. Пусть D — дивизор степени 1 на C (например, $D = P$). Так как $1 = 2g+1$, дивизор D очень обилен, причем $\dim H^0(C, \mathcal{O}_C(D)) = \deg D + 1 - g = 2$, следовательно получаем морфизм $f : C \to \mathbb{P}^1$, такой что $f^*\mathcal{O}_{\mathbb{P}^1}(1) \cong \mathcal{O}_C(D)$. Так как при обратном образе относительно конечного морфизма степень обратимого пучка умножается на степень расширения полей, то $\deg K(C)/K(\mathbb{P}^1) = 1$, значит $K(C) = K(\mathbb{P}^1)$, то есть $C = \mathbb{P}^1$, так как гладкая проективная кривая однозначно определяется своим полем функций. □

Упражнение 19.7. *Пусть $C \subset \mathbb{P}^2_k$ — коника, не имеющая точек над полем k. Покажите, что род C равен нулю, но $C \ncong \mathbb{P}^1_k$. Проверьте, что любая кривая рода нуль изоморфна конике (указание: $\deg(-K_C) = 2$).*

Всякая кривая рода 1 называется *эллиптической кривой.* В дальнейшем мы увидим, что существуют разные эллиптические кривые даже над алгебраически замкнутым полем.

Упражнение 19.8. *Покажите, что кривая рода 1 над алгебраически замкнутым полем*
(i) представляется как двулистное накрытие $\mathbb{P}^1$;
(ii) изоморфна кубической кривой в $\mathbb{P}^2$.

Дивизор D называется *подвижным,* если $\dim H^0(C, \mathcal{O}_C(D)) \geq 2$. Пусть C — кривая рода $g \geq 1$. Ясно, что никакой дивизор D степени 1 на кривой C не может быть подвижным (иначе $C \cong \mathbb{P}^1$).

Лемма 19.16. *Пусть D — дивизор степени 2 на кривой C рода $g \geq 1$. Если D подвижен, то линейная система $|D|$ не имеет базисных точек.*

Доказательство. Можно считать, что поле k алгебраически замкнуто и надо проверить, что $\dim H^0(C, \mathcal{O}_C(D-P)) \leq 1$. Но если $\dim H^0(C, \mathcal{O}_C(D-P)) \geq 2$, то $D-P$ был бы подвижным дивизором степени 1, что невозможно так как $g \geq 1$. □

Заметим, что $\dim H^0(C, \mathcal{O}_C(D)) \leq 2$ для всякого дивизора степени 2 на кривой рода ≥ 1 (иначе над полем $\overline{k}$ дивизор $D-P$ был бы подвижным дивизором степени 1). Таким образом, всякий подвижный дивизор D степени 2 на кривой C рода ≥ 1 задает отображение $C \to \mathbb{P}^1$, которое, как легко видеть, является двулистным накрытием.

Определение 19.17. Кривая C рода $g \geq 2$ называется *гиперэллиптической*, если существует двулистное накрытие $C \to \mathbb{P}^1$.

Только что мы показали, что кривая гиперэллиптична тогда и только тогда, когда на ней существует подвижный дивизор степени 2.

Упражнение 19.9. *Покажите, что любая кривая рода 2 гиперэллиптична.*

Теорема 19.18. *Пусть C — кривая рода $g \geq 2$. Канонический дивизор K_C на C очень обилен тогда и только тогда, когда C не гиперэллиптична.*

Доказательство. Как показано в лемме 19.14 достаточно проверить, что

$$\dim H^0(C, \mathcal{O}_C(K_C - P)) = g - 1 \quad \text{и} \quad \dim H^0(C, \mathcal{O}_C(K_C - P - Q)) = g - 2$$

для всех точек $P, Q \in C \otimes \overline{k}$. В самом деле, если $\dim H^0(C, \mathcal{O}_C(K_C - P)) = g$, то по теореме Римана–Роха и двойственности Серра $\dim H^0(C, \mathcal{O}_C(P)) = \dim H^1(C, \mathcal{O}_C(K_C - P)) = 2$, то есть P является подвижным дивизором степени 1 на C, что невозможно, так как $g \geq 2$. Аналогично, если $\dim H^0(C, \mathcal{O}_C(K_C - P - Q)) = g-1$, то $P+Q$ является подвижным дивизором степени 2 на C, что равносильно гиперэллиптичности кривой. □

Пусть C — негиперэллиптическая кривая рода g. Линейная система $|K_C|$ задает вложение кривой C в $\mathbb{P}^{g-1}$. Ее образ называется *канонически вложенной кривой*, или просто *канонической кривой.*

Упражнение 19.10 (геометрическая теорема Римана–Роха). *Пусть $C \subset \mathbb{P}^{g-1}$ — каноническая кривая рода g. Покажите, что $\dim |P_1 + P_2 + \dots + P_r| + \dim\langle P_1, P_2, \dots, P_r\rangle = r - 1$, где $\langle P_1, P_2, \dots, P_r\rangle$ — линейная оболочка точек $P_1, P_2, \dots, P_r$ в $\mathbb{P}^{g-1}$.*

Упражнение 19.11. *Покажите, что любые два подвижных дивизора степени 2 на гиперэллиптической кривой линейно эквивалентны.*

Упражнение 19.12 (геометрическая теорема Римана–Роха). *Пусть C — гиперэллиптическая кривая рода g. Покажите, что $|K_C|$ не имеет базисных точек, а отображение, задаваемое этой линейной системой является композицией двулистного накрытия $C \to \mathbb{P}^1$ и вложения Веронезе $\mathbb{P}^1 \to \mathbb{P}^{g-1}$.*

Эллиптические кривые

В отличии от кривых рода 0, которые над алгебраически замкнутым полем все изоморфны $\mathbb{P}^1$, эллиптические кривые бывают разными над любым полем. Ограничимся для простоты случаем поля k, $\operatorname{char} k \neq 2$.

Примером кривой является двулистное накрытие $\mathbb{P}^1$ разветвленное в четырех точках. Заметим, что множество всех четверок попарно различных точек проективной прямой — четырехмерное алгебраическое многообразие. Факторизуя его по группе $\operatorname{Aut} \mathbb{P}^1 = \mathrm{P}GL_2$, которая трехмерна, получаем одномерный фактор, который параметризует множество всех эллиптических кривых. Конечно, чтобы это рассуждение сделать строгим, нужно кое-что доказать.

Лемма 19.19. *Пусть C — эллиптическая кривая и $P \in C$. Существует единственное разветвленное в точке P двулистное накрытие $C \to \mathbb{P}^1$.*

Доказательство. Ясно, что такое накрытие должно задаваться подсистемой линейной системы $|2P|$, поэтому достаточно проверить, что $\dim H^0(C, \mathcal{O}_C(2P)) = 2$ и что система $|2P|$ не имеет базисных точек. Но это действительно так, поскольку $\deg(2P) = 2 = 2g$. □

Лемма 19.20. *Для любых точек $P, P' \in C$ существует инволюция σ кривой C, такая что $\sigma(P) = P'$. В частности группа $\operatorname{Aut} C$ действует на множестве точек транзитивно.*

Доказательство. Так же как и в предыдущей лемме проверяем, что отображение, задаваемое линейной системой $|P+P'|$ является двулистным накрытием $\mathbb{P}^1$. Значит поле $K(C)$ является расширением степени 2 поля $K(\mathbb{P}^1)$. Пусть σ — автоморфизм поля $K(C)$ над $K(\mathbb{P}^1)$. Ясно, что он действует на C и переводит P в P'. □

Предложение 19.21. *Пусть $f : C \to \mathbb{P}^1$ и $f' : C' \to \mathbb{P}^1$ — двулистные накрытия, разветвленные в точках P_1, P_2, P_3, P_4 и P_1', P_2', P_3', P_4' соответственно. Кривые C и C' изоморфны тогда и только тогда, когда существует автоморфизм $g \in \mathsf{Aut}\,\mathbb{P}^1$, такой что $g(f(P_i)) = f'(P_i')$ для всех i.*

Доказательство. Предположим вначале, что кривые изоморфны, то есть будем считать, что $C' = C$. Применяя, если нужно, автоморфизм, можно считать, что $P_1' = P_1$. Так как накрытия f и f' оба разветвлены в точке P_1, они эквивалентны, то есть отличаются на автоморфизм $g \in \mathsf{Aut}\,\mathbb{P}^1$. Ясно, что этот изоморфизм нам и нужен.

Обратно, надо показать, что эллиптическая кривая C однозначно определяется своими точками ветвления. Выберем координаты на $\mathbb{P}^1$ так, чтобы точками ветвления были точки $0, 1, \infty$ и λ. Так как поле $K(C)$ является расширением степени 2 поля $K(\mathbb{P}^1) = k(x)$, то можно представить его в виде $K(C) = k(x)[y]/(y^2 - f(x))$, где $f(x) \in k[x]$ не имеет кратных корней. Непосредственное вычисление (мы его проделывали в прошлом семестре) показывает, что морфизм $C \to \mathbb{P}^1$ разветвлен над корнями многочлена $f(x)$, а если $\mathsf{deg}\, f(x)$ нечетна, то еще и над точкой ∞. Значит в нашем случае кривая задается уравнением $y^2 = x(x-1)(x-\lambda)$. □

Упражнение 19.13. *Покажите, что любые четыре точки на $\mathbb{P}^1$ автоморфизмом перевести в точки $0, 1, \lambda, \infty$. Проверьте, что точки $0, 1, \lambda, \infty$ переводятся автоморфизмом в $0, 1, \mu, \infty$ тогда и только тогда, когда $\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2} = \frac{(\mu^2-\mu+1)^3}{\mu^2(\mu-1)^2}$.*

Пусть C — эллиптическая кривая. Представим ее в виде двулистного накрытия $\mathbb{P}^1$, а координату на $\mathbb{P}^1$ выберем так, чтобы точками ветвления были точки $0, 1, \lambda, \infty$. Сопоставим кривой C число

$$j(C) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda-1)^2}.$$

Оно называется j-инвариантом эллиптической кривой C. Приведенные выше рассуждения доказывают

Теорема 19.22. *Эллиптические кривые C и C' изоморфны тогда и только тогда, когда $j(C) = j(C')$.*

Таким образом, множество всех эллиптических кривых отождествляется со множеством всех значений j-инварианта, который, как легко видеть, может принимать любые значения.

Упражнение 19.14. *Пусть $\mathsf{char}\, k \neq 2, 3$. Покажите, что группа автоморфизмов эллиптической кривой, сохраняющих точку P, имеет порядок*

- *6, если $j = 1728$,*
- *4, если $j = 0$,* и
- *2, если $j \neq 0, 1728$.*

Напоследок покажем, что всякая эллиптическая кривая обладает структурой группы.

Предложение 19.23. *Пусть $P_0 \in C$. Отображение $P \to \mathcal{O}_C(P - P_0)$ задает изоморфизм множества точек кривой C на группу $\mathrm{Pic}^0(C)$ обратимых пучков степени 0.*

Доказательство. Инъективность: если $\mathcal{O}_C(P - P_0) \cong \mathcal{O}_C(P' - P_0)$, то $P - P_0 \sim P' - P_0$, то есть $P \sim P'$. Но тогда $|P|$ — подвижная линейная система степени 1, что невозможно.

Сюръективность: пусть $\mathcal{L}$ — линейное расслоение степени 0. По теореме Римана–Роха $\chi(\mathcal{L}(P_0)) = \mathsf{deg}(\mathcal{L}(P_0)) = 1$, значит пучок $\mathcal{L}(P_0)$ обладает регулярным сечением, которое должно иметь ровно один нуль (так как $\mathsf{deg}\,\mathcal{L}(P_0) = 1$). Значит $\mathcal{L}(P_0) \cong \mathcal{O}_C(P)$, то есть $\mathcal{L} \cong \mathcal{O}_C(P - P_0)$. □

На самом деле, группа $\mathrm{Pic}^0(X)$ обладает естественной структурой схемы для любого проективного многообразия X (она является групповой схемой), а построенное нами отображение $C \to \mathrm{Pic}^0(C)$ является изоморфизмом схем.