

Лекция 1

Павел Владимирович Снурницын

15 декабря 2025 г.

1 Введение

Курс «Арифметика-III: Римановы поверхности и алгебраические кривые» является продолжением следующих двух курсов:

1. «Арифметика-I: Основы алгебраической теории чисел». Курс представляет собой введение в теорию чисел, начиная от делимости, сравнений, квадратичных вычетов и заканчивая полями алгебраических чисел и полями p -аддитических чисел;
2. «Арифметика II: Решётки и формы». В рамках курса рассматривались рациональные евклидовы решетки и квадратичные и модулярные формы.

Несмотря на то, что данный курс является продолжением этой серии, большая часть материала не связана с содержанием предыдущих курсов.

Чтобы создать общую картину курса и мотивировать слушателей, предложим несколько утверждений и определений.

Для начала рассмотрим **решётку** $L \subset \mathbb{C}$, то есть множество

$$L = \{z = n\omega_1 + m\omega_2 : n, m \in \mathbb{Z}, \omega_1, \omega_2 \in \mathbb{C}\}.$$

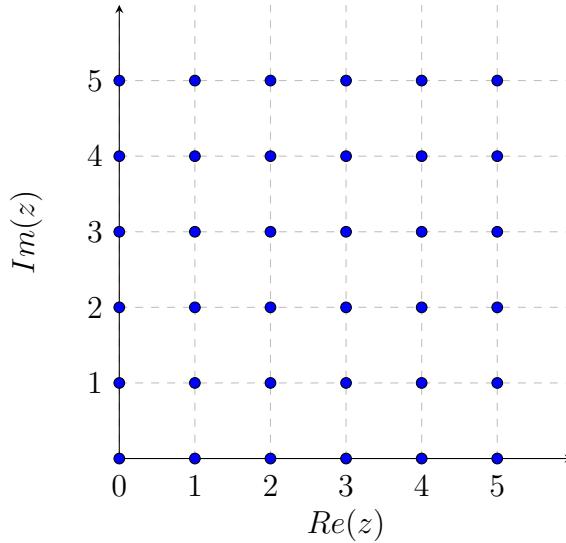


Рис. 1: Решетка для $\omega_1 = 1$ и $\omega_2 = i$

Фактор-пространство по этой решетке \mathbb{C}/L определяется так называемым **фундаментальным параллелепипедом** $P = \{z = x + iy: 0 \leq x \leq 1, 0 \leq y \leq 1\}$, так как любое комплексное число $z \in \mathbb{C}$ представимо в виде суммы: $z = \omega + p$, где $\omega \in L$, а $p \in P$.

Теперь «склеим» противолежащие стороны нашего фундаментального параллелепипеда. «Склейив» первую пару сторон, увидим полый круговой цилиндр. Окружности на концах полого цилиндра будут второй парой противолежащих сторон. «Склейив» вторую пару, получим **топ**:

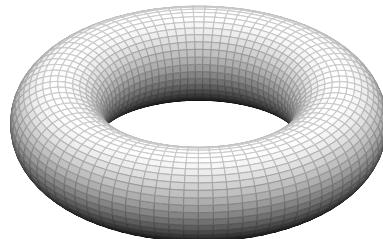


Рис. 2: Топ, полученный из фундаментального параллелепипеда

Забегая вперед, полученная нами поверхность имеет **топологический род 1**.

Теперь рассмотрим следующую группу целочисленных невырожденных матриц:

$$\Gamma = SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc = 1; a, b, c, d \in \mathbb{Z} \right\}.$$

Эта группа действует в верхней комплексной полуплоскости:

$$\mathbb{H} = \{z \in \mathbb{C} : Im(z) > 0\}$$

Опишем её действие:

$$\gamma \cdot z = \gamma z = \begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \begin{pmatrix} az+b \\ cz+d \end{pmatrix}.$$

Модулярной функцией называется функция, обладающая «хорошими» свойствами симметрии относительно данного действия, например

$$f(\gamma z) = (cz + d)^k f(z),$$

где k – некоторое целое число.

Рассмотрим разбиение \mathbb{H} на фактор-множества при действии Γ :

$$\mathbb{H}/\Gamma \sim D.$$

Множество D называется **фундаментальной областью**. Она задает поверхность, имеющую **топологический род 0**. Примечательно, что если рассмотреть подгруппу Γ , то есть некоторую группу Γ' , то задаваемая ей поверхность будет иметь **топологический род $g \geq 0$** . Род g имеет важную роль в исследовании модулярных функций.

Далее рассмотрим конечное поле \mathbb{F}_q из $q = p^n$ элементов, где p – простое число. Пусть $f(x, y) \in \mathbb{F}_q[x, y]$ – многочлен от двух переменных с коэффициентами из этого поля. Данный многочлен задает некоторую кривую. Обозначим через N_m число точек на этой кривой, то есть множество решений уравнения

$$f(x, y) = 0,$$

принадлежащих **проективному пространству** $\mathbb{P}^2(\mathbb{F}_q)$ (формально определим позднее). Для N_m верна теорема:

Теорема 1 (Хассе-Вейль).

$$|N_m - (q^n + 1)| \leq 2gq^{n/2},$$

где g – алгебраический род кривой $f = 0$.

Данный курс имеет целью раскрыть данную теорию и показать, как эти вопросы связаны через алгебраическую геометрию и теорию Римановых поверхностей.

2 Римановы поверхности (РП). Введение.

Определим основные объекты и понятия.

Определение 1. Пусть X – множество. Говорят, что на X задана структура топологического пространства, если $\forall x \in X$ задано непустое множество подмножеств X , обозначаемое $\mathcal{U}(x) \neq \emptyset$, и

1. $\forall U \in \mathcal{U}(x): x \in U;$
2. $U, V \in \mathcal{U}(x) \implies U \cap V \in \mathcal{U}(x);$
3. $U \in \mathcal{U}(x), V \subset X, x \in V \text{ и } U \subset V \implies V \in \mathcal{U}(x);$
4. $U \in \mathcal{U}(x), \dot{U} = \{z \in U: U \in \mathcal{U}(z)\} \in \mathcal{U}(x).$

Существует более полезное определение:

Определение 2. Топологическим пространством называется пара (X, T) , где T – множество подмножеств X , называемое системой открытых множеств, и удовлетворяющее:

1. $\emptyset, X \subset T;$
2. $\forall (U_\alpha) \in T: \bigcup_\alpha U_\alpha \in T;$
3. $\forall (U_i)_{i=1}^n, U_i \in T, \bigcap_{i=1}^n U_i \in T$

Примеры:

1. Множество \mathbb{C} является топологическим пространством с системой открытых множеств в виде окрестностей $|z| < \varepsilon$;
2. \mathbb{R}^2 является топологическим пространством с системой открытых множеств в виде окрестностей $\sqrt{x^2 + y^2} < \varepsilon$.

Определение 3. Пусть X, Y – топологические пространства. Отображение $f: X \rightarrow Y$ называется непрерывным, если $\forall x \in X: \forall V \in \mathcal{U}(f(x))$ (в топологии Y) $\exists U \in \mathcal{U}(x)$ (в топологии X) такое, что $f(U) \subset V$.

Определение 4. Отображение $f: X \rightarrow Y$ называется открытым, если для любого открытого множества U множество $f(U)$ открытое (в топологии Y).

Определение 5. Если $f: X \rightarrow Y$ – непрерывно и биективно, то f называется гомеоморфизмом.

Определение 6. Пусть X – топологическое пространство, $U \subset X$ – открытое множество, $V \subset \mathbb{C}$ – открытое множество. Гомеоморфизм $\phi: U \rightarrow V$ называется комплексной картой. Если для некоторой $p \in U$: $\phi(p) = 0$, то p называется центром карты.

Комплексную карту можно представлять себе как некоторую «локальную координату».

Примеры:

1. Пусть $X = \mathbb{R}^2$, $U \subset X$ – открытое подмножество. Тогда отображение $\phi_U(x, y) = x + iy$ будет комплексной картой.
2. Можно предложить другое отображение:

$$\phi_U(x, y) = \frac{x}{1 + \sqrt{x^2 + y^2}} + i \frac{y}{1 + \sqrt{x^2 + y^2}},$$

которое также будет картой.

Определение 7. Две карты на X : $\phi_1: U_1 \rightarrow V_1$ и $\phi_2: U_2 \rightarrow V_2$ называются совместимыми, если либо $U_1 \cap U_2 = \emptyset$, либо $T = \phi_2 \circ \phi_1^{-1}$, $T: \phi_1(U_1 \cap U_2) \rightarrow \phi_2(U_1 \cap U_2)$ является голоморфной, то есть комплексно дифференцируемой функцией в окрестности любой точки рассматриваемой области.

Функция T называется функцией склейки. Она отвечает за совпадение карт на пересечении областей определения.

Заметим, что если ψ – карта, задающая отображение из подмножества \mathbb{C} в подмножество \mathbb{C} , то композиция $\phi \circ \psi$ по сути осуществляет замену координат.

Лемма 1. Пусть T – функция склейки. Тогда её производная $T' = \frac{dT}{dz} \neq 0$ в области определения T .

Доказательство. Так как T – голоморфная, то существует обратная функция $S = T^{-1}$. При этом $S \circ T$ является тождественной функцией, поэтому для любого z из области определения T верно $S \circ T(z) = z$, но тогда

$$(S \circ T(z))' = S'(T(z)) \cdot T'(z) = 1,$$

поэтому $T'(z)$ не может равняться нулю. \square

Следствие 1. Пусть ϕ, ψ – две карты, $z_0 = \phi(p)$, $w_0 = \psi(p)$, где p – точка, в которой обе карты определены. Тогда ряд Тейлора для функции склейки имеет вид:

$$z = T(w) = z_0 + \sum_{n=1}^{\infty} a_n (w - w_0)^n, a_1 \neq 0.$$

Последнее неравенство является следствием леммы.

Упражнение. Докажите, что не совместимы две карты:

$$\phi_U(x, y) = x + iy,$$

$$\phi_U(x, y) = \frac{x}{1 + \sqrt{x^2 + y^2}} + i \frac{y}{1 + \sqrt{x^2 + y^2}}.$$

Определение 8. Комплексным атласом \mathcal{A} на X называется набор

$$\mathcal{A} = \{\phi_\alpha: U_\alpha \rightarrow V_\alpha\},$$

для которого

1. $\forall \alpha, \beta: \phi_\alpha$ и ϕ_β совместимы;
2. $\bigcup_\alpha U_\alpha = X$.

Далее будем обозначать $T_{\alpha\beta} = \phi_\beta \circ \phi_\alpha^{-1}$, то есть соответствующую функцию склейки.

Примеры

1. Сфера в \mathbb{R}^3 , которую обозначают

$$S^2 = \{(x_1, x_2, x_3) \in \mathbb{R}^3: x_1^2 + x_2^2 + x_3^2 = 1\}.$$

Рассмотрим \mathbb{R}^2 как плоскость, вложенную в \mathbb{R}^3 , то есть $\mathbb{R}^2 = \{(x_1, x_2, 0)\}$ и одновременно как \mathbb{C} . Определим проекцию из точки $(0, 0, 1)$ (полюса сферы):

$$\phi(x_1, x_2, x_3) = \frac{x_1}{1 - x_3} + i \frac{x_2}{1 - x_3}.$$

Данное отображение определено везде, кроме самого полюса. Аналитически можно описать прообраз:

$$\phi^{-1}(z) = \left(\frac{2\operatorname{Re}(z)}{|z|^2 + 1}, \frac{2\operatorname{Im}(z)}{|z|^2 + 1}, \frac{|z|^2 - 1}{|z|^2 + 1} \right).$$

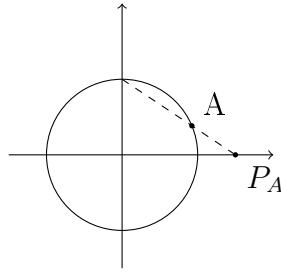


Рис. 3: Проекция точки A сферы на плоскость

Проекция из $(0, 0, -1)$ имеет вид

$$\psi(x_1, x_2, x_3) = \frac{x_1}{1 + x_3} - i \frac{x_2}{1 + x_3}.$$

Тогда функция склейки для ϕ и ψ равна $T(z) = \frac{1}{z}$.
Множество $\{\phi, \psi\}$ задает комплексный атлас на S^2 .

Определение 9. Два атласа \mathcal{A}_1 и \mathcal{A}_2 называются эквивалентными, если $\forall \phi_\alpha \in \mathcal{A}_1, \forall \phi_\beta \in \mathcal{A}_2$ карты ϕ_α и ϕ_β совместны.

Определение 10. Класс эквивалентности комплексного атласа называется комплексной структурой.

Определение 11. Топологическое пространство X называется Хаусдорфовым, если $\forall x, y \in X, x \neq y: \exists U, V$ – окрестности x и y , соответственно, такие, что $U \cap V = \emptyset$.

Определение 12. Топологическое пространство X называется пространством со счетной базой, если в системе открытых множеств T можно выделить счетное число подмножеств, которое порождает T .

Определение 13. Пространство X называется связным, если \nexists открытые непустые подмножества U_1, U_2 множества X , для которых $X = U_1 \cup U_2$ и $U_1 \cap U_2 = \emptyset$.

Определение 14. X называется Римановой поверхностью (РП), если

1. X – связное Хаусдорфово топологическое пространство со счетной базой;
2. на X задана комплексная структура.

Примеры

1. $X = S^2$ с картами $\{\phi, \psi\}$ является Римановой поверхностью. Будем называть её сферой Римана (Римановой сферой). Иногда про сферу Римана говорят, что она описывает множество $\mathbb{C} \cup \{\infty\} = \mathbb{C}_\infty$, где бесконечно удаленным точкам соответствуют полюса сферы.

Предложение 1. Как задать Риманову поверхность на множестве X ? Для этого нужно:

1. счетное покрытие (U_α) : $\bigcup_\alpha U_\alpha = X$;
2. $\forall \alpha$ определим биекцию $\phi_\alpha: U_\alpha \rightarrow V_\alpha \subseteq \mathbb{C}$, где V_α – открытые множества, а для биекций верно:
 - (a) $\forall \alpha, \beta: \phi_\alpha(U_\alpha \cap U_\beta)$ – открытое в V_α ;
 - (b) $\forall \alpha, \beta: \phi_\alpha, \phi_\beta$ – совместимые;
 - (c) топология на X связна и Хаусдорфова.

Теперь определим проективное пространство, которое было упомянуто во введении:

Определение 15. Если \mathbb{C}^{n+1} – комплексное векторное пространство, то можно определить отношение эквивалентности ненулевых векторов:

$$(z_0, z_1, \dots, z_n) \sim (z'_0, z'_1, \dots, z'_n),$$

если $\exists \lambda \neq 0 \in \mathbb{C}: \forall i \in \overline{0, n}$ верно $z_i = \lambda z'_i$. Тогда проективное пространство определяется, как

$$\mathbb{P}^n(\mathbb{C}^n) = \mathbb{C}^{n+1} / \sim.$$

Через \mathbb{C}^{n+1} будем обозначать аффинное пространство соответствующей размерности: $\mathbb{C}^{n+1} = \mathbb{A}^{n+1}(\mathbb{C})$.

Пока мы работаем только с комплексными координатами, будем обозначать $\mathbb{P}^n = \mathbb{P}^n(\mathbb{C})$. Элементы \mathbb{P}^n обычно обозначают через представителей классов эквивалентности: $[z_0: z_1: \dots: z_n] = [\lambda z_0: \lambda z_1: \dots: \lambda z_n]$.

Далее покажем, что на \mathbb{P}^1 можно определить структуру Римановой поверхности.

Пусть

$$U_0 = \{[z_0: z_1]: z_0 \neq 0\},$$

$$U_1 = \{[z_0: z_1]: z_1 \neq 0\}.$$

$\{U_0, U_1\}$ образуют покрытие \mathbb{P}^1 , то есть $\mathbb{P}^1 = U_0 \cup U_1$.

Зададим отображения:

$$\phi_0: U_0 \rightarrow \mathbb{C},$$

$$\phi_1: U_1 \rightarrow \mathbb{C}$$

следующего вида:

$$\phi_0([z_0: z_1]) = \frac{z_1}{z_0},$$

$$\phi_1([z_0: z_1]) = \frac{z_0}{z_1}.$$

При этом $\phi(U_0 \cap U_1) = \mathbb{C}^* = \mathbb{C} \setminus \{0\}$ – открытое в обычной топологии \mathbb{C} .

Далее для функции склейки:

$$T = (\phi_1 \circ \phi_0^{-1})(z) = \frac{1}{z}.$$

На \mathbb{C}^* данная функция голоморфна, поэтому ϕ_0 и ϕ_1 совместны. Получаем, что $\{\phi_0, \phi_1\}$ – атлас.

Заметим, что U_0 и U_1 связны. Их пересечение $U_0 \cap U_1$ тоже связно, поэтому $\mathbb{P}^1 = U_1 \cup U_2$ связно.

Докажем Хаусдорфовость. Пусть $p, q \in \mathbb{P}^1$. Если $p, q \in U_i, i \in \{0, 1\}$ то отделимость следует из отделимости \mathbb{C} . Пусть $p \in U_0 \setminus U_1$ и $q \in U_1 \setminus U_0$. Тогда $p = [1: 0]$ и $q = [0: 1]$. Рассмотрим $D = \{|z| < 1, z \in \mathbb{C}\}$. Имеем $p \in \phi_0^{-1}(D)$ и $q \in \phi_1^{-1}(D)$, а также $\phi_0^{-1}(D) \cap \phi_1^{-1}(D) = \emptyset$, так как $T(D) = \{|z| > 1\}$.

Заметим, что для замкнутого диска $\overline{D} = \{|z| \leq 1\}$:

$$\mathbb{P}^1 = \phi_0^{-1}(\overline{D}) \cup \phi_1^{-1}(\overline{D}).$$

Рассмотрим еще одно топологическое понятие:

Определение 16. *X называется компактом, если из любого покрытия (U_α) можно выделить конечное подпокрытие.*

Тогда \mathbb{P}^1 является компактом.

Замечание 1. Для римановых поверхностей существует более общее понятие n -мерных комплексных многообразий: пусть задано топологическое пространство X , n -мерные комплексные карты $\phi: U \rightarrow V$, где $U \subset X$, а V – открытое подмножество \mathbb{C}^n . Тогда также \mathbb{P}^n – n -мерное комплексное многообразие, а карты являются отображениями вида:

$$\phi_i = \{[z_0 : \dots : z_n] : z_i \neq 0\} \rightarrow \left(\frac{z_0}{z_i}, \dots, \hat{i}, \dots, \frac{z_n}{z_i} \right).$$

Вернемся к понятию решетки, то есть множества вида

$$L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2,$$

где ω_1, ω_2 – линейно независимые комплексные числа. Основной параллелепипед решетки – это множество

$$P = \{\lambda_1\omega_1 + \lambda_2\omega_2 : 0 \leq \lambda_i \leq 1\}.$$

Рассмотрим фактор-пространство $X = \mathbb{C}/L$. По сути, так как любое комплексное число z представляется в виде $z = p + \omega$, где $p \in P, \omega \in L$, то класс эквивалентности по этому фактору имеет вид $[z] = p = (z \bmod L)$ или в обозначениях естественной проекции – $\pi(z)$. Используя эту проекцию, можно задать естественную топологию на X – топологию фактор-пространства, то есть $U \subset X$ – открытое тогда и только тогда, когда $\pi^{-1}(U)$ открыто в \mathbb{C} . При этом π непрерывно в этой топологии, а X связно, так как связно \mathbb{C} .

Лемма 2. *Верны следующие утверждения:*

1. Для любого открытого множества $U \subset X$ существует открытое $V \subset \mathbb{C}$, $\pi(U) = V$;

2. π – открытое отображение (переводит открытые множества в открытые).

Доказательство оставляется читателю в качестве упражнения.

Так как $\pi: P \rightarrow X$, то есть это сюръекция и P – компактное множество, то X также является компактным множеством.

Далее решетка L является дискретным множеством, то есть $\exists \varepsilon > 0$: $\forall \omega \in L \setminus \{0\}$ верно $|\omega| > 2\varepsilon$. Возьмем $D_{z_0} = \{|z - z_0| < \varepsilon\}$. Любые $z_1, z_2 \in D_{z_0}$ удовлетворяют $z_1 \neq z_2 \pmod{L}$. Теперь карты можно определить, как

$$\forall z_0 \in \mathbb{C}, \phi_{z_0}: \pi(D_{z_0}) \rightarrow D_{z_0}.$$

По сути эти карты – прообразы ограничения (сужения) π на D_{z_0} , то есть $\phi_{z_0} = (\pi|_{D_{z_0}})^{-1}$. Геометрически это означает, что либо z_0 полностью лежит с окрестностью внутри параллелепипеда, либо её окрестность «раскинута» по разным «частям» параллелепипеда.

Рассмотрим вопрос совместности $\phi_1 = \phi_{z_1}$ и $\phi_2 = \phi_{z_2}$. Пусть $U = \pi(D_{z_1}) \cap \pi(D_{z_2}) \neq \emptyset$. Для функции склейки

$$T(z) = \phi_2(\phi_1^{-1}(z)) = \phi_2(\pi(z))$$

можно записать

$$\pi(T(z)) = \pi(z).$$

Получаем, что z и $T(z)$ лежат в одном классе решетки, но тогда $T(z) - z = \omega = \omega(z)$. Функция $\omega(z)$ есть отображение $\phi_1(U) \rightarrow L$. Можно заметить, что ω непрерывна, так как непрерывны ϕ , T . При этом L – дискретное множество, поэтому $\omega(z)$ локально постоянна, то есть на $\phi_1(U)$ верно $T(z) = z + \omega$, где ω – константа. Из этого следует, что T – это просто «сдвиг» на ω и тогда данная функция голоморфна.

3 Род и число Эйлера

Неформально говоря, род поверхности – это число её «дырок» или «ручек».

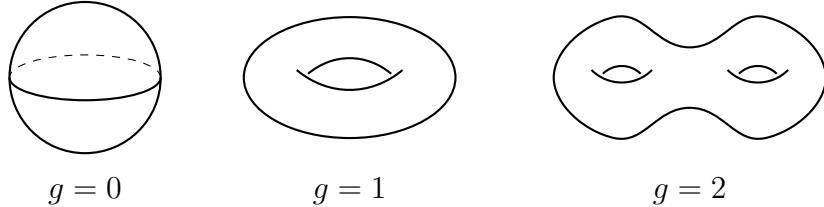


Рис. 4: Поверхности различных родов g

Определение 17. Пусть X – это комплексное двумерное многообразие. Триангуляцией X называется разбиение $X = \bigcup_{i=1}^n T_i$: T_i – замкнуто, гомеоморфно треугольнику и $T_i \cap T_j \in \{\emptyset, \text{вершина}, \text{ребро}\} \forall i \neq j$.

Определение 18. Пусть T – триангуляция X . Эйлеровой характеристикой называется $\chi(T) = v - e + t$, где v, e, t – число, соответственно, вершин, рёбер и треугольников в триангуляции.

Лемма 3 (без доказательства). $\chi(T)$ не зависит от T , то есть $\chi = \chi(X)$.

Определение 19. Топологическим родом X назовем число

$$g(X) = \frac{1}{2}(2 - \chi(X)).$$

Наше изначальное понимание топологического рода было связано со следующей теоремой:

Теорема 2 (без доказательства). Всякое комплексное ориентируемое многообразие гомеоморфно сфере с g ручками, где g – топологический род.

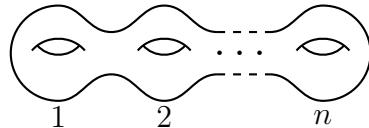


Рис. 5: Вид X при $g = n$

Примеры:

1. Разобьем сферу на «треугольные» поверхности следующим образом:

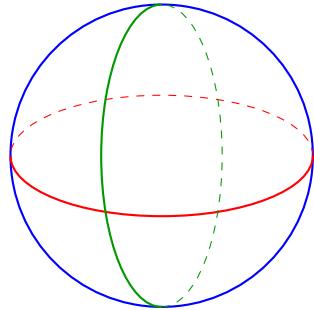


Рис. 6: Разбиение сферы на триангуляции

Здесь триангуляции – это поверхности, ограниченные тремя дугами разного цвета. Посчитаем Эйлерову характеристику: $\chi = 6 - 12 + 8 = 2$. Тогда род $g = 0$.

2. В случае тора достаточно вспомнить, что тор можно «вытянуть» в прямоугольник и далее разбить его на треугольники, учитывая, что противолежащие стороны прямоугольника отождествляются на торе. Подсчет топологического рода далее производится аналогично сфере.

Теорема 3 (то, что нам нужно из топологии). *Если X – Риманова поверхность, то X гомеоморфно обобщенному тору рода $g \geq 0$.*

4 Аффинные кривые

Рассмотрим некоторые понятия алгебраической геометрии.

Определение 20. Пусть $f \in \mathbb{C}[z, w]$ (многочлен от двух переменных).
Множество

$$X_f = \{(z, w) \in \mathbb{C}^2 : f(z, w) = 0\}$$

называется аффинной кривой над \mathbb{C} .

Определение 21. X_f или f называется невырожденной (неособенной) кривой в точке $p \in X_f$, если

$$\frac{\delta f}{\delta z}(p) \neq 0$$

или

$$\frac{\delta f}{\delta w}(p) \neq 0.$$

Если X_f невырождена в каждой точке $p \in X_f$, то X_f называют гладкой аффинной кривой.

Теорема 4 (без доказательства). Если f – неприводимый многочлен, то X_f – Риманова поверхность.

Основная сложность доказательства теоремы выше состоит в доказательстве связности.

Пример. Рассмотрим многочлен $f = w^2 - h(z)$. Если f – неприводимый, то решения уравнения $w^2 = h(z)$ задают Риманову поверхность. Утверждается, что f неприводим над \mathbb{C} тогда и только тогда, когда h не является полным квадратом.

В частности, при $\deg h = 3$ получим **эллиптическую кривую**. При $\deg h > 3$ получим **гиперэллиптическую кривую**.

5 Проективные кривые

Определение 22. Пусть $F(x, y, z)$ – однородный многочлен степени d ($F \in \mathbb{C}[x, y, z]_d$), то есть $F(\lambda x, \lambda y, \lambda z) = \lambda^d F(x, y, z)$. Множество

$$X_F = \{[x: y: z] \in \mathbb{P}^2 : F(x, y, z) = 0\}$$

будем называть проективной кривой.

Аналогично аффинным кривым определяются невырожденности X_F и F , а также верна теорема:

Теорема 5 (без доказательства). Если F – невырожденный многочлен, то X_F – компактная Риманова поверхность.

Кроме того, верна следующая теорема:

Теорема 6 (без доказательства). *Если F – невырожденный многочлен, а также однородный многочлен степени d , то*

$$g(X_F) = \frac{(d-1)(d-2)}{2}.$$

Пример. Эллиптическая кривая имеет степень 3, откуда по теореме выше её род g равен 1.