Contents

1 Elliptic curves

1.1 Reduction of Weierstrass equations

In this subsection, we want to investigate the important constants of elliptic curves such as c_4, c_6, Δ, j by calculating equations with hands.

Step 1. The Riemann-Roch theorem proves that every curve of genus 1 with a specified base point can be described by the first kind of Weierstrass equation. Explicitly, the first form of Weierstrass equation is

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1}$$

Step 2. *Elimination of xy and y.* Factorize the left hand side

$$y\,(y + a_1x + a_3) = x^3 + a_2x^2 + a_4x + a_6.$$

By translation

$$\boxed{x \mapsto x, \qquad y \mapsto y - \tfrac{1}{2}(a_1x + a_3)}$$

we have

$$\begin{aligned} y^2 - (\tfrac{1}{2}(a_1x + a_3))^2 = x^3 + a_2x^2 + a_4x + a_6,& \\ y^2 &= x^3 + (\tfrac{1}{4}a_1^2 + a_2)x^2 + (\tfrac{1}{2}a_1a_3 + a_4)x + (\tfrac{1}{4}a_3^2 + a_6), \\ y^2 &= x^3 + \frac{1}{4}(a_1^2 + 4a_2)x^2 + \frac{1}{2}(a_1a_2 + 2a_4)x + \frac{1}{4}(a_3^2 + 4a_6). \end{aligned}$$

Introduce new coefficients b to write it as

$$y^2 = x^3 + \frac{1}{4}b_2x^2 + \frac{1}{2}b_4x + \frac{1}{4}b_6.$$

By scaling

$$\boxed{x \mapsto x, \qquad y \mapsto \tfrac{1}{2}y}$$

we get

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6. \tag{2}$$

Step 3. *Elimination of x^2.* By translation

$$\boxed{x \mapsto x - \tfrac{1}{12}b_2}$$

we have

$$\begin{aligned}y^2 = 4\left(x^3 - 3\cdot\frac{1}{12}b_2x^2 + 3\cdot\frac{1}{12^2}b_2^2x - \frac{1}{12^3}b_2^3\right)\\ +b_2\left(x^2 - 2\cdot\frac{1}{12}b_2x + \frac{1}{12^2}b_2^2\right)\\ +2b_4\left(x - \frac{1}{12}b_2\right)\\ +b_6,\end{aligned}$$

so

$$\begin{aligned}y^2 &= 4x^3 + \left(4\cdot 3\cdot\frac{1}{12^2}b_2^2 - 2\cdot\frac{1}{12}b_2^2 + 2b_4\right)x + \left(-4\cdot\frac{1}{12^3}b_2^3 + \frac{1}{12^2}b_2^3 - 2\cdot\frac{1}{12}b_2b_4 + b_6\right)\\ &= 4x^3 + \frac{1}{12}\left(-b_2^2 + 24b_4\right)x + \frac{1}{216}\left(b_2^3 - 36b_2b_4 + 216b_6\right).\end{aligned}$$

Write it as

$$y^2 = 4x^3 - \frac{1}{12}c_4x - \frac{1}{216}c_6.$$

We want to match the coefficients of y^2 and x^3 but also want the coefficients of c_4x and c_6 to be integers. Iterative scaling implies

$$\begin{aligned}x\mapsto\tfrac{1}{6}x: &\qquad 216y^2 = 4x^3 - 3c_4x - c_6\\ y\mapsto\tfrac{1}{36}y: &\qquad y^2 = 24x^3 - 18c_4x - 6c_6\\ x\mapsto\tfrac{1}{6}x: &\qquad 9y^2 = x^3 - 27c_4x - 54c_6\\ y\mapsto\tfrac{1}{3}y: &\qquad y^2 = x^3 - 27c_4x - 54c_6.\end{aligned}$$

Thus, we get the famous third form of Weierstrass equation:

$$y^2 = x^3 - 27c_4x - 54c_6. \tag{3}$$

Theorem 1.1. *Let*

$$E : y^2 = x^3 - Ax - B.$$

TFAE:

(1) *A point (x, y) is a singular point of E.*

(2) *$y = 0$ and x is a double root of $x^3 - Ax - B$.*

(3) *$\Delta = 0$.*

Proof. (1)⇒(2) $\partial_y f = 0$ implies $y = 0$. $f = \partial_x f = 0$ implies x is a double root of $x^3 - Ax - B$. A determines whether x is either cusp of node. □

2 Algebraic integer

2.1 Quadratic integer

Theorem 2.1. *Every quadratic field is of the form $\mathbb{Q}(\sqrt{d})$ for a square-free d.*

Theorem 2.2. *Let d be a square-free.*

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z} + \sqrt{d}\mathbb{Z} & , d \equiv 2, 3 \pmod 4 \\ \mathbb{Z} + \dfrac{1+\sqrt{d}}{2}\mathbb{Z} & , d \equiv 1 \pmod 4 \end{cases}$$

$$\Delta_{\mathbb{Q}(\sqrt{d})} = \begin{cases} 4d & , d \equiv 2, 3 \pmod 4 \\ d & , d \equiv 1 \pmod 4 \end{cases}$$

Example 2.1.

$$\Delta_{\mathbb{Q}(i)} = -4, \quad \Delta_{\mathbb{Q}(\sqrt{2})} = 8, \quad \Delta_{\mathbb{Q}(\gamma)} = 5, \quad \Delta_{\mathbb{Q}(\omega)} = -3$$

where $\gamma := \frac{1+\sqrt{5}}{2}$ and $\omega = \zeta_3$.

Theorem 2.3. *Let $\theta^3 = hk^2$ for h, k square-free's.*

$$\mathcal{O}_{\mathbb{Q}(\theta)} = \begin{cases} \mathbb{Z} + \theta\mathbb{Z} + \dfrac{\theta^2}{k}\mathbb{Z} & , m \not\equiv \pm 1 \pmod 9 \\ \mathbb{Z} + \theta\mathbb{Z} + \dfrac{\theta^2 \pm \theta k + k^2}{3k}\mathbb{Z} & , m \equiv \pm 1 \pmod 9 \end{cases}$$

Corollary 2.4. *If θ^3 is a square free integer, then*

$$\mathcal{O}_{\mathbb{Q}(\theta)} = \mathbb{Z}[\theta].$$

2.2 Integral basis

Theorem 2.5. *Let $\alpha \in K$. $Tr_K(\alpha) \in \mathbb{Z}$ if $\alpha \in \mathcal{O}_K$. $N_K(\alpha) \in \mathbb{Z}$ if and only if $\alpha \in \mathcal{O}_K$.*

Theorem 2.6. *Let $\{\omega_1, \cdots, \omega_n\}$ be a basis of K over $\mathbb{Q}$. If $\Delta(\omega_1, \cdots, \omega_n)$ is square-free, then $\{\omega_1, \cdots, \omega_n\}$ is an integral basis.*

Theorem 2.7. *Let $\{\omega_1, \cdots, \omega_n\}$ be a basis of K over $\mathbb{Q}$ consisting of algebraic integers. If $p^2 \mid \Delta$ and it is not an integral basis, then there is a nonzero algebraic integer of the form*

$$\frac{1}{p}\sum_{i=1}^{n} \lambda_i \omega_i.$$

2.3 Fractional ideals

Theorem 2.8. *Every fractional ideal of K is a free $\mathbb{Z}$-module with rank $[K : \mathbb{Q}]$.*

Proof. This theorem holds because $K/\mathbb{Q}$ is separable and $\mathbb{Z}$ is a PID. $\square$

2.4 Frobenius element

Consider an abelian extension L/K. Let $\mathfrak{p}$ be a prime in $\mathcal{O}_K$. Since L/K is Galois, the followings do not depend on the choice of $\mathfrak{P}$ over $\mathfrak{p}$.

Lemma 2.9. *The following sequence of abelian groups is exact:*

$$0 \longrightarrow I(\mathfrak{P}|\mathfrak{p}) \longrightarrow D(\mathfrak{P}|\mathfrak{p}) \longrightarrow \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p})) \longrightarrow 0,$$

where $k(\mathfrak{P}) := \mathcal{O}_L/\mathfrak{P}$ and $k(\mathfrak{p}) := \mathcal{O}_K/\mathfrak{p}$ are residue fields.

The Frobenius element is defined as an element of $D(\mathfrak{P}|\mathfrak{p})/I(\mathfrak{P}|\mathfrak{p}) \cong \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$, which is a cyclic group.

Definition 2.1. For an unramified prime $\mathfrak{p} \subset \mathcal{O}_K$ so that $I(\mathfrak{P}|\mathfrak{p})$ is trivial, the Frobenius element $\phi(\mathfrak{P}|\mathfrak{p}) \in \mathrm{Gal}(L/K)$ is defined by

$$\phi_{\mathfrak{P}|\mathfrak{p}}(\mathfrak{P}) = \mathfrak{P}, \quad \text{and} \quad \phi_{\mathfrak{P}|\mathfrak{p}}(x) \equiv x^{|\mathcal{O}_K/\mathfrak{p}|} \pmod{\mathfrak{P}} \quad \text{for} \quad x \in \mathcal{O}_L.$$

The first condition is equivalent to $\phi_{\mathfrak{P}|\mathfrak{p}} \in D(\mathfrak{P}|\mathfrak{p})$. In fact, the Frobenius element is in fact a generator of the cyclic group $D(\mathfrak{P}|\mathfrak{p}) \cong \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$ by the Galois theory of finite fields.

Remark. Fermat's little theorem states

$$\phi_{\mathfrak{P}|\mathfrak{p}}(x) \equiv x \pmod{\mathfrak{p}}, for x \in \mathcal{O}_K,$$

which means $\phi_{\mathfrak{P}|\mathfrak{p}}$ fixes the field $\mathcal{O}_K/\mathfrak{p}$ so that $\phi_{\mathfrak{P}|\mathfrak{p}} \in \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$.

2.5 Quadratic Dirichlet character

Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic field with discriminant D and $L = \mathbb{Q}(\zeta_D)$ be the cyclotomic field for $\zeta_D = e^{\frac{2\pi i}{D}}$.

$$\begin{array}{ccccccc} D(\mathfrak{P}/p) & \subset & \mathrm{Gal}(L/\mathbb{Q}) & \cong & (\mathbb{Z}/D\mathbb{Z})^\times & \qquad & L = \mathbb{Q}(\zeta_D) \\ & & \Big\downarrow q & & \Big\downarrow \chi_K = (\frac{D}{\cdot}) & & \\ D(\mathfrak{p}/p) & \subset & \mathrm{Gal}(K/\mathbb{Q}) & \cong & \{\pm 1\} & & K = \mathbb{Q}(\sqrt{D}). \end{array}$$

For $p \nmid D$ so that p is unramified, let $\sigma_p := (\zeta_D \mapsto \zeta_D^p) \in \mathrm{Gal}(L/\mathbb{Q})$. Then, what is $\sigma_p|_K$ in $\mathrm{Gal}(K/\mathbb{Q})$. In other words, for $\sigma_p(\zeta_D) = \zeta_D^p$ which is true: $\sigma_p(\sqrt{D}) = \pm\sqrt{D}$?

Note that σ satisfies the condition to be the Frobenius element: $\sigma_p = \phi_{\mathfrak{P}|p}$. Therefore, $q(\phi_{\mathfrak{P}|p}) = \phi_{\mathfrak{p}|p} = \sigma_p|_K$ is also a Frobenius element. There are only two cases:

(1) If $f = |D(\mathfrak{p}/p)| = 1$, then $\sigma|_K$ is the identity, so $\chi_K(p) = 1$

(2) If $f = |D(\mathfrak{p}/p)| = 2$, then $\sigma|_K$ is not trivial, so $\chi_K(p) = -1$

Artin reciprocity: $(\mathbb{Z}/D\mathbb{Z})^\times$ is extended to I_K^S.

3 Diophantine equations

3.1 Quadratic equation on a plane

Ellipse is reduced by finitely many computations.

Especially for hyperbola, here is a strategy to use infinite descent.

(1) Let midpoint to be origin.

(2) Find the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ preserving the image of hyperbola(which would be isomorphic to $\mathbb{Z}$).

(3) Find an impossible region.

(4) Assume a solution and reduce it to the either impossible region or the ground solution.

Example 3.1 (Pell's equation)**.** Consider

$$x^2 - 2y^2 = 1.$$

A generator of hyperbola generating group is $g = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}$. It has a ground solution $(1, 0)$ and impossible region $1 < x < 3$. If (a, b) is a solution with $a > 0$, then we can find n such that $g^n(a, b)$ is in the region $[1, 3)$. The possible case is $g^n(a, b) = (1, 0)$.

Example 3.2 (IMO 1988, the last problem)**.** Consider a family of equations

$$x^2 + y^2 - kxy - k = 0.$$

By the vieta jumping, a generator is $g : (a, b) \mapsto (b, kb - a)$. It has an impossible region $xy < 0 : x^2 + y^2 - kxy - k \geq x^2 + y^2 > 0$. If (a, b) is a solution with $a > b$, then we can find n such that $g^n(a, b)$ is in the region $xy \leq 0$. Only possible case is $g^n(a, b) = (\sqrt{k}, 0)$ or $g^n(a, b) = (0, -\sqrt{k})$. In ohter words, the equation has a solution iff k is a perfect square.

3.2 The Mordell equations

(The reciprocity laws let us learn not only which prime splits, but also which prime factors a given polynomial has.)

$$y^2 = x^3 + k$$

There are two strategies for the Mordell equations:

- $x^2 - 2x + 4$ has a prime factor of the form $4k + 3$
- $x^3 = N(y - a)$ for some a.

First case: $k = 7, -5, -6, 45, 6, 46, -24, -3, -9, -12$.

Example 3.3. Solve $y^2 = x^3 + 7$.

Proof. Taking mod 8, x is odd and y is even. Consider

$$y^2 + 1 = (x + 2)(x^2 - 2x + 4).$$

Since

$$x^2 - 2x + 4 = (x - 1)^2 + 3,$$

there is a prime $p \equiv 3 \pmod 4$ that divides the right hand side. Taking mod p, we have

$$y^2 \equiv -1 \pmod p,$$

which is impossible. Therefore, the equation has no solutions. $\square$

Example 3.4. Solve $y^2 = x^3 - 2$.

Proof. Taking mod 8, x and y are odd. Consider a ring of algebraic integers $\mathbb{Z}[\sqrt{-2}]$. We have

$$N(y - \sqrt{-2}) = (y - \sqrt{-2})(y + \sqrt{-2}) = x^3.$$

For a common divisor δ of $y \pm \sqrt{-2}$, we have

$$N(\delta) \mid N((y - \sqrt{-2}) - (y + \sqrt{-2})) = N(2\sqrt{-2}) = |(2\sqrt{-2})(-2\sqrt{-2})| = 8.$$

On the other hand,

$$N(\delta) \mid x^3 \equiv 1 \pmod 2,$$

so $N(\delta) = 1$ and δ is a unit. Thus, $y \pm \sqrt{-2}$ are relatively prime. Since the units in $\mathbb{Z}[\sqrt{-2}]$ are ± 1, which are cubes, $y \pm \sqrt{-2}$ are cubics in $\mathbb{Z}[\sqrt{-2}]$.

Let

$$y + \sqrt{-2} = (a + b\sqrt{-2})^3 = a(a^2 - 6b^2) + b(3a^2 - 2b^2)\sqrt{-2},$$

so that $1 = b(3a^2 - 2b^2)$. We can conclude $b = \pm 1$. The possible solutions are $(x, y) = (3, \pm 5)$, which are in fact solutions. $\square$

4 The local-global principle

4.1 The local fields

Let $f \in \mathbb{Z}[x]$.

Does $f = 0$ have a solution in $\mathbb{Z}$?

Does $f = 0$ have a solution in $\mathbb{Z}/(p^n)$ for all n?

Does $f = 0$ have a solution in $\mathbb{Z}_p$?

In the first place, here is the algebraic definition.

Definition 4.1. Let $p \in \mathbb{Z}$ be a prime. The ring of the p-adic integers $\mathbb{Z}_p$ is defined by the inverse limit:

$$\mathbb{Z}_p := \varprojlim_{n\in\mathbb{N}} \mathbb{F}_{p^n} \longrightarrow \cdots \longrightarrow \mathbb{Z}/(p^3) \longrightarrow \mathbb{Z}/(p^2) \longrightarrow \mathbb{F}_p.$$

Definition 4.2. $\mathbb{Q}_p = \operatorname{Frac}\mathbb{Z}_p$.

Secondly, here is the analytic definition.

Definition 4.3. Let $p \in \mathbb{Z}$ be a prime. Define a absolute value $|\cdot|_p$ on $\mathbb{Q}$ by $|p^m a|_p = \frac{1}{p^m}$. The local field $\mathbb{Q}_p$ is defined by the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

Definition 4.4. $\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$.

Example 4.1. Observe

$$\begin{aligned} 3^{-1} &\equiv 2_5 \pmod 5 \\ &\equiv 32_5 \pmod{5^2} \\ &\equiv 132_5 \pmod{5^3} \\ &\equiv 1313132_5 \pmod 5^7 \cdots . \end{aligned}$$

Therefore, we can write

$$3^{-1} = \overline{13}2_5 = 2 + 3p + p^2 + 3p^3 + p^4 + \cdots$$

for $p = 5$. Since there is no negative power of 5, 3^{-1} is a p-adic integer for $p = 5$.

Example 4.2.

$$\begin{aligned} 7 &\equiv 1_3^2 \pmod 3 \\ &\equiv 111_3^2 \pmod{3^3} \\ &\equiv 20111_3^2 \pmod{3^5} \\ &\equiv 120020111_3^2 \pmod{3^9} \cdots . \end{aligned}$$

Therefore, we can write

$$\sqrt{7} = \cdots 120020111_3 = 1 + p + p^2 + 2p^4 + 2p^7 + p^8 + \cdots$$

for $p = 3$. Since there is no negative power of 3, $\sqrt{7}$ is a p-adic integer for $p = 3$.

There are some pathological and interesting phenomena in local fields. Actually note that the values of $|\cdot|_p$ are totally disconnected.

Theorem 4.1. *The absolute value $|\cdot|_p$ is nonarchimedean: it satisfies $|x+y|_p \leq \max\{|x|_p, |y|_p\}$.*

Proof. Trivial. $\square$

Theorem 4.2. *Every triangle in $\mathbb{Q}_p$ is isosceles.*

Theorem 4.3. *$\mathbb{Z}_p$ is a discrete valuation ring: it is local PID.*

Proof. asdf $\square$

Theorem 4.4. *$\mathbb{Z}_p$ is open and compact. Hence $\mathbb{Q}_p$ is locally compact Hausdorff.*

Proof. $\mathbb{Z}_p$ is open clearly. Let us show limit point compactness. Let $A \subset \mathbb{Z}_p$ be infinite. Since $\mathbb{Z}_p$ is a finite union of cosets $p\mathbb{Z}_p$, there is α_0 such that $A \cap (\alpha_0 + p\mathbb{Z}_p)$ is infinite. Inductively, since

$$\alpha_n + p^{n+1}\mathbb{Z}_p = \bigcup_{1 \leq x < p} (\alpha_n + xp^{n+1} + p^{n+2}\mathbb{Z}_p),$$

we can choose α_{n+1} such that $\alpha_n \equiv \alpha_{n+1} \pmod{p^{n+1}}$ and $A \cap (\alpha_{n+1} + p^{n+2}\mathbb{Z}_p)$ is infinite. The sequence $\{\alpha_n\}$ is Cauchy, and the limit is clearly in $\mathbb{Z}_p$. $\square$

4.2 Hensel's lemma

Theorem 4.5 (Hensel's lemma)**.** *Let $f \in \mathbb{Z}_p[x]$. If f has a simple solution in $\mathbb{F}_p$, then f has a solution in $\mathbb{Z}_p$.*

Proof. asdf $\square$

Remark. Hensel's lemma says: for X a scheme over $\mathbb{Z}_p$, X is smooth iff $X(\mathbb{Z}_p) \twoheadrightarrow X(\mathbb{F}_p)$....???

Example 4.3. $f(x) = x^p - x$ is factorized linearly in $\mathbb{Z}_p[x]$.

4.3 Sums of two squares

Theorem 4.6 (Euler)**.** *A positive integer m can be written as a sum of two squares if and only if $v_p(m)$ is even for all primes $p \equiv 3 \pmod 4$.*

Lemma 4.7. *Let p be a prime with $p \equiv 1 \pmod 4$. Every p-adic integer is a sum of two squares of p-adic integers.*

5 Ultrafilter

Theorem 5.1. *Let $\mathcal{U}$ be an ultrafilter on a set S and X be a compact space. For $f\colon S \to X$, the limit $\mathcal{U}$-$\lim f$ always exists.*

Theorem 5.2. *Let $X = \prod_{\alpha\in\mathcal{A}} X_\alpha$ be a product space of compact spaces X_α. A net $\{f_d\}_{d\in\mathcal{D}}$ on X has a convergent subnet.*

Proof 1. Use Tychonoff. Compactness and net compactness are equivalent. □

Proof 2. It is a proof without Tychonoff. Let $\mathcal{U}$ be a ultrafilter on a set $\mathcal{D}$ contatining all $\uparrow d$. Define a directed set $\mathcal{E} = \{(d, U) \in \mathcal{D} \times \mathcal{U} : d \in U\}$ as $(d, U) \prec (d', U')$ for $U \supset U'$. Let $f\colon \mathcal{E} \to X$ be a net defined by $f_{(d,U)} = f_d$.

By the previous theorem, $\mathcal{U}$-$\lim \pi_\alpha f_d$ exsits for each α. Define $f \in X$ such that $\pi_\alpha f = \mathcal{U}$-$\lim \pi_\alpha f_d$. Let $G = \prod_\alpha G_\alpha \subset X$ be any open neighborhood of f where $G_\alpha = X_\alpha$ except finite. Then G_α is an open neighborhood of $\pi_\alpha f$ so that we have $U_\alpha := \{d : \pi_\alpha f_d \in G_\alpha\} \in \mathcal{U}$ by definition of convergence with ultrafilter.9 Since $U_\alpha = \mathcal{D}$ except finites, we can take an upper bound $U_0 \in \mathcal{U}$. Then, by taking any $d_0 \in U_0$, we have $f_{(d,U)} \in G$ for every $(d, U) \succ (d_0, U_0)$. This means $f = \lim_\mathcal{E} f_{(d,U)}$, so we can say $\lim_\mathcal{E} f_{(d,U)}$ exists.

□

6 Universal coefficient theorem

Lemma 6.1. *Suppose we have a flat resolution*

$$0 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow A \longrightarrow 0.$$

Then, we have a exact sequence

$$\cdots \longrightarrow 0 \longrightarrow \mathrm{Tor}_1^R(A,B) \longrightarrow P_1 \otimes B \longrightarrow P_0 \otimes B \longrightarrow A \otimes B \longrightarrow 0.$$

Theorem 6.2. *Let R be a PID. Let $C_\bullet$ be a chain complex of flat R-modules and G be a R-module. Then, we have a short exact sequence*

$$0 \longrightarrow H_n(C) \otimes G \longrightarrow H_n(C;G) \longrightarrow \mathrm{Tor}(H_{n-1}(C),G) \longrightarrow 0,$$

which splits, but not naturally.

Proof 1. We have a short exact sequence of chain complexes

$$0 \longrightarrow Z_\bullet \longrightarrow C_\bullet \longrightarrow B_{\bullet-1} \longrightarrow 0$$

where every morphism in $Z_\bullet$ and $B_\bullet$ are zero. Since modules in $B_{\bullet-1}$ are flat, we have a short exact sequence

$$0 \longrightarrow Z_\bullet \otimes G \longrightarrow C_\bullet \otimes G \longrightarrow B_{\bullet-1} \otimes G \longrightarrow 0$$

and the associated long exact sequence

$$\cdots \longrightarrow H_n(B;G) \longrightarrow H_n(Z;G) \longrightarrow H_n(C;G) \longrightarrow H_{n-1}(B;G) \longrightarrow H_{n-1}(Z;G) \longrightarrow \cdots$$

where the connecting homomomorphisms are of the form $(i_n \colon B_n \to Z_n) \otimes 1_G$ (It is better to think diagram chasing than a natural construction). Since morhpisms in B and Z are zero (if it is not, then the short exact sequence of chain complexes are not exact, we have

$$\cdots \longrightarrow B_n \otimes G \longrightarrow Z_n \otimes G \longrightarrow H_n(C;G) \longrightarrow B_{n-1} \otimes G \longrightarrow Z_{n-1} \otimes G \longrightarrow \cdots.$$

Since

$$0 \longrightarrow \mathrm{Tor}_1^R(H_n,G) \longrightarrow B_n \otimes G \longrightarrow Z_n \otimes G \longrightarrow H_n \otimes G \longrightarrow 0$$

for all n, the exact sequence splits into short exact sequence by images

$$0 \longrightarrow H_n \otimes G \longrightarrow H_n(C;G) \longrightarrow \mathrm{Tor}_1^R(H_{n-1},G) \longrightarrow 0.$$

For splitting, □

Proof 2. Since R is PID, we can construct a flat resolution of G

$$0 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow G \longrightarrow 0.$$

Since modules in $C_\bullet$ are flat so that the tensor product functors are exact and $P_1 \to P_0$ and $P_0 \to G$ induce the chain maps, we have a short exact sequence of chain complexes

$$0 \longrightarrow C_\bullet \otimes P_1 \longrightarrow C_\bullet \otimes P_0 \longrightarrow C_\bullet \otimes G \longrightarrow 0.$$

Then, we have the associated long exact sequence

$$\cdots \longrightarrow H_n(C; P_1) \longrightarrow H_n(C; P_0) \longrightarrow H_n(C; G) \longrightarrow H_{n-1}(C; P_1) \longrightarrow H_{n-1}(C; P_0) \longrightarrow \cdots$$

Since flat tensor product functor commutes with homology funtor from chain complexes, we have

$$\cdots \longrightarrow H_n \otimes P_1 \longrightarrow H_n \otimes P_0 \longrightarrow H_n(C; G) \longrightarrow H_{n-1} \otimes P_1 \longrightarrow H_{n-1} \otimes P_0 \longrightarrow \cdots.$$

Since

$$0 \longrightarrow \operatorname{Tor}_1^R(G, H_n) \longrightarrow H_n \otimes P_1 \longrightarrow H_n \otimes P_0 \longrightarrow H_n \otimes G \longrightarrow 0$$

for all n, the exact sequence splits into short exact sequence by images

$$0 \longrightarrow H_n \otimes G \longrightarrow H_n(C; G) \longrightarrow \operatorname{Tor}_1^R(G, H_{n-1}) \longrightarrow 0.$$

$\square$

Proof 3. (??) By tensoring G, we get the following diagram.

$$\begin{tikzcd}
H_n \otimes G \arrow[dr] & & & & H_{n-1} \otimes G \\
& \operatorname{coker} \partial_{n+1} \otimes G \arrow[ddr, two heads] & & \ker \partial_{n-1} \otimes G \arrow[ur, two heads] \arrow[dr] & \\
C_n \otimes G \arrow[ur, two heads] \arrow[drr, two heads] & & & & C_{n-1} \otimes G \\
& & \operatorname{im} \partial_n \otimes G \arrow[uur] \arrow[urr] & & \\
& \operatorname{Tor}_1(H_{n-1}, G) \arrow[ur, tail] & & &
\end{tikzcd}$$

Every aligned set of consecutive arrows indicates an exact sequence. Notice that epimorphisms and cokernals are preserved, but monomorphisms and kernels are not. Especially, $\operatorname{coker} \partial_{n+1} \otimes G = \operatorname{coker}(\partial_{n+1} \otimes 1_G)$ is important.

Consider the following diagram.

$$\begin{tikzcd}
H_n(C;G) \arrow[dr, tail] & H_n \otimes G \arrow[d] & & & \\
& \operatorname{coker} \partial_{n+1} \otimes G \arrow[dd, two heads] \arrow[ddrr, two heads] & & \ker \partial_{n-1} \otimes G \arrow[dr, "\text{monic!}"] & \\
& & & & C_{n-1} \otimes G \\
& \operatorname{im} \partial_n \otimes G \arrow[uurr] & & \operatorname{im}(\partial_n \otimes 1_G) \arrow[uu, tail, dashed] \arrow[ur, tail] & \\
\operatorname{Tor}_1(H_{n-1}, G) \arrow[uur, tail] & & & &
\end{tikzcd}$$

Since $\ker \partial_{n-1}$ is free,

If we show $\operatorname{im}(\partial_n \otimes 1_G) \to \ker \partial_{n-1} \otimes G$ is monic, then we can get

$$\begin{aligned}
H_n(C;G) &= \ker(\operatorname{coker} \partial_{n+1} \otimes G \to \operatorname{im}(\partial_n \otimes 1_G)) \\
&= \ker(\operatorname{coker} \partial_{n+1} \otimes G \to \ker \partial_{n-1} \otimes G).
\end{aligned}$$

□

7 Fundamental differential geometry

7.1 Manifold and Atlas

Definition 7.1. A *locally Euclidean space* M of dimension m is a Hausdorff topological space M for which each point $x \in M$ has a neighborhood U homeomorphic to an open subset of $\mathbb{R}^d$.

Definition 7.2. A *manifold* is a locally Euclidean space satisfying the one of following equivalent conditions: second countability, blabla

Definition 7.3. A *chart* or a *coordinate system* for a locally Euclidean space is a map φ is a homeomorphism from an open set $U \subset M$ to an open subset of $\mathbb{R}^d$. A chart is often written by a pair (U, φ).

Definition 7.4. An *atlas* $\mathcal{F}$ is a collection $\mathcal{F} = \{(U_\alpha, \varphi_\alpha) \mid \alpha \in A\}$ of charts on M such that $\bigcup_{\alpha \in A} U_\alpha = M$.

Definition 7.5. A *differentiable maifold* is a manifold on which a differentiable structure is equipped.

The definition of differentiable structure will be given in the next subsection. Actually, a differentiable structure can be defined for a locally Euclidean space.

7.2 Definition of Differentiable Structure

Definition 7.6. An atlas $\mathcal{F}$ is called *differentiable* if any two charts $\varphi_\alpha, \varphi_\beta \in \mathcal{F}$ is *compatible*: each *transition function* $\tau_{\alpha\beta} \colon \varphi_\alpha(U_\alpha \cap U_\beta) \to \varphi_\beta(U_\alpha \cap U_\beta)$ which is defined by $\tau_{\alpha\beta} = \varphi_\beta \circ \varphi_\alpha^{-1}$ is differentiable.

It is called a *gluing condition*.

Definition 7.7. For two differentiable atlases $\mathcal{F}, \mathcal{F}'$, the two atlases are *equivalent* if $\mathcal{F} \cup \mathcal{F}'$ is also differentiable.

Definition 7.8. An differentiable atlas $\mathcal{F}$ is called *maximal* if the following holds: if a chart (U, φ) is compatible to all charts in $\mathcal{F}$, then $(U, \varphi) \in \mathcal{F}$.

Definition 7.9. A *differentiable structure* on M is a maximal differentiable atlas.

To differentiate a function on a flexible manofold, first we should define the differentiability of a function. A differentiable structure, which is usually defined by a maximal differentiable atlas, is roughly a collection of differentiable functions on M. When the charts is already equipped on M, it is natural to define a function $f \colon M \to \mathbb{R}$ differentiable if the functions $f \circ \varphi^{-1} \colon \mathbb{R}^d \to \mathbb{R}$ is differentiable.

The gluing condition makes the differentiable function for a chart is also differentiable for any charts because $f \circ \varphi_\alpha^{-1} = (f \circ \varphi_\beta^{-1}) \circ (\varphi_\beta \circ \varphi_\alpha^{-1}) = (f \circ \varphi_\beta^{-1}) \circ \tau_{\alpha\beta}$. If a function f is differentiable on an atlas $\mathcal{F}$, then f is also differentiable on any atlases which is equivalent to $\mathcal{F}$ by the definition of the equivalence relation for differential atlases. We can construct the equivalence classes respected to this equivalence relation.

Therefore, we want to define a differentiable structure as a one of the equivalence classes. However the differentiable structure is frequently defined as a maximal atlas for the convenience since each equivalence class is determined by a unique maximal atlas.

Example 7.1. While the circle S^1 has a unique smooth structure, S^7 has 28 smooth structures. The number of smooth structures on S^4 is still unknown.

Definition 7.10. A continuous function $f\colon M \to N$ is differentiable if $\psi \circ f \circ \varphi^{-1}$ is differentiable for charts φ, ψ on M, N respectively.

7.3 Curves

Definition 7.11. For $f\colon M \to \mathbb{R}$ and (U, ϕ) a chart,

$$df\left(\frac{\partial}{\partial x^\mu}\right) := \frac{\partial f \circ \phi^{-1}}{\partial x^\mu}.$$

Definition 7.12. Let $\gamma\colon I \to M$ be a smooth curve. Then, $\dot{\gamma}(t)$ is defined by a tangent vector at $\gamma(t)$ such that

$$\dot{\gamma}(t) := d\gamma\left(\frac{\partial}{\partial t}\right).$$

Let $\phi\colon M \to N$ be a smoth map. Then, $\phi(t)$ can refer to a curve on N such that

$$\phi(t) := \phi(\gamma(t)).$$

Let $f\colon M \to \mathbb{R}$ be a smooth function. Then, $\dot{f}(t)$ is defined by a function $\mathbb{R} \to \mathbb{R}$ such that

$$\dot{f}(t) := \frac{d}{dt} f \circ \gamma.$$

Proposition 7.1. *Let $\gamma\colon I \to M$ be a smooth curve on a manifold M. The notation $\dot{\gamma}^\mu$ is not confusing thanks to*

$$(\dot{\gamma})^\mu = (\dot{\gamma^\mu}).$$

In other words,

$$dx^\mu(\dot{\gamma}) = \frac{d}{dt} x^\mu \circ \gamma.$$

7.4 Connection computation

$$\begin{aligned}\nabla_X Y &= X^\mu \nabla_\mu (Y^\nu \partial_\nu) \\ &= X^\mu (\nabla_\mu Y^\nu)\partial_\nu + X^\mu Y^\nu (\nabla_\mu \partial_\nu) \\ &= X^\mu \left(\frac{\partial Y^\nu}{\partial x^\mu}\right)\partial_\nu + X^\mu Y^\nu (\Gamma^\lambda_{\mu\nu}\partial_\lambda) \\ &= X^\mu \left(\frac{\partial Y^\nu}{\partial x^\mu} + \Gamma^\nu_{\mu\lambda} Y^\lambda\right)\partial_\nu.\end{aligned}$$

The covariant derivative $\nabla_X Y$ does not depend on derivatives of X^μ.

$$Y^\nu_{,\mu} = \nabla_\mu Y^\nu = \frac{\partial Y^\nu}{\partial x^\mu}, \qquad Y^\nu_{;\mu} = (\nabla_\mu Y)^\nu = \frac{\partial Y^\nu}{\partial x^\mu} + \Gamma^\nu_{\mu\lambda} Y^\lambda.$$

Theorem 7.2. *For Levi-civita connection for g,*

$$\Gamma^l_{ij} = \frac{1}{2}(\partial_i g_{jk} + \partial_j g_{ki} - \partial_k g_{ij}).$$

Proof.

$$\begin{aligned}(\nabla_i g)_{jk} &= \partial_i g_{jk} - \Gamma^l_{ij} g_{lk} - \Gamma^l_{ik} g_{jl} \\ (\nabla_j g)_{kl} &= \partial_j g_{kl} - \Gamma^l_{jk} g_{li} - \Gamma^l_{ji} g_{kl} \\ (\nabla_k g)_{ij} &= \partial_k g_{ij} - \Gamma^l_{ki} g_{lj} - \Gamma^l_{kj} g_{il}\end{aligned}$$

If ∇ is a Levi-civita connection, then $\nabla g = 0$ and $\Gamma^k_{ij} = \Gamma^k_{ji}$. Thus,

$$\Gamma^l_{ij} g_{kl} = \frac{1}{2}(\partial_i g_{jk} + \partial_j g_{ki} - \partial_k g_{ij}).$$

$$\Gamma^l_{ij} = \frac{1}{2} g^{kl}(\partial_i g_{jk} + \partial_j g_{ki} - \partial_k g_{ij}).$$

□

7.5 Geodesic equation

Theorem 7.3. *If c is a geodesic curve, then components of c satisfies a second-order differential equation*

$$\frac{d^2\gamma^\mu}{dt^2} + \Gamma^\mu_{\nu\lambda}\frac{d\gamma^\nu}{dt}\frac{d\gamma^\lambda}{dt} = 0.$$

Proof. Note

$$0 = \nabla_{\dot\gamma}\dot\gamma = \dot\gamma^\mu \nabla_\mu (\dot\gamma^\lambda \partial_\lambda) = (\dot\gamma^\nu \partial_\nu \dot\gamma^\mu + \dot\gamma^\nu \dot\gamma^\lambda \Gamma^\mu_{\nu\lambda})\partial_\mu.$$

Since
$$\dot{\gamma}^\nu \partial_\nu \dot{\gamma}^\mu = \dot{\gamma}(\dot{\gamma}^\mu) = d\dot{\gamma}^\mu(\dot{\gamma}) = d\dot{\gamma}^\mu \circ d\gamma \left(\frac{\partial}{\partial t}\right) = d\dot{\gamma}^\mu \left(\frac{\partial}{\partial t}\right) = \ddot{\gamma}^\mu,$$
we get a second-order differential equation
$$\frac{d^2\gamma^\mu}{dt^2} + \Gamma^\mu_{\nu\lambda}\frac{d\gamma^\nu}{dt}\frac{d\gamma^\lambda}{dt} = 0$$
for each μ. $\square$

8 Vector calculus on spherical coordinates

$$
\begin{array}{rcccccccl}
V & = & (V_r, V_\theta, V_\phi) & & & & & & \\
& = & V_r & \widehat{r} & + & V_\theta & \widehat{\theta} & + & V_\phi \quad \widehat{\phi} \qquad \text{(normalized coords)} \\
& = & V_r & \frac{\partial}{\partial r} & + & \frac{1}{r}\, V_\theta & \frac{\partial}{\partial \theta} & + & \frac{1}{r\sin\theta}\, V_\phi \quad \frac{\partial}{\partial \phi} \qquad (\Gamma(TM)) \\
& = & V_r & dr & + & r\, V_\theta & d\theta & + & r\sin\theta\, V_\phi \quad d\phi \qquad (\Omega^1(M)) \\
& = & r^2\sin\theta\, V_r & d\theta\wedge d\phi & + & r\sin\theta\, V_\theta & d\phi\wedge dr & + & r\, V_\phi \quad dr\wedge d\theta \qquad (\Omega^2(M)).
\end{array}
$$

$$\nabla\cdot V = \frac{1}{r^2\sin\theta}\left[\frac{\partial}{\partial r}\left(r^2\sin\theta\, V_r\right) + \frac{\partial}{\partial\theta}\left(r\sin\theta\, V_\theta\right) + \frac{\partial}{\partial\phi}\left(r\, V_\phi\right)\right]$$

$$\Delta u = \frac{1}{r^2\sin\theta}\left[\frac{\partial}{\partial r}\left(r^2\sin\theta\frac{\partial}{\partial r}u\right) + \frac{\partial}{\partial\theta}\left(\sin\theta\frac{\partial}{\partial\theta}u\right) + \frac{\partial}{\partial\phi}\left(\frac{1}{\sin\theta}\frac{\partial}{\partial\phi}u\right)\right]$$

Let (ξ,η,ζ) be an orthogonal coordinate that is *not* normalized. Then,

$$\sharp = g = \mathrm{diag}(\|\partial_\xi\|^2, \|\partial_\eta\|^2, \|\partial_\zeta\|^2)$$

$$\widehat{x} = \|\partial_x\|^{-1}\;\partial_x = \|\partial_x\|\; dx = \|\partial_y\|\|\partial_z\|\; dy\wedge dz$$

In other words, we get the normalized differential forms in sphereical coordinates as follows:

$$dr,\quad r\,d\theta,\quad r\sin\theta\,d\phi,\quad (r\,d\theta)\wedge(r\sin\theta\,d\phi),\quad (r\sin\theta\,d\phi)\wedge(dr),\quad (dr)\wedge(r\,d\theta).$$

$$\mathrm{grad}:\nabla = \left[\;\frac{1}{\|\partial_x\|}\frac{\partial}{\partial x}\cdot - \;,\; \frac{1}{\|\partial_y\|}\frac{\partial}{\partial y}\cdot - \;,\; \frac{1}{\|\partial_z\|}\frac{\partial}{\partial z}\cdot - \;\right]$$

$$
\begin{aligned}
\mathrm{curl}:\nabla = \Bigg[\; & \frac{1}{\|\partial_y\|\|\partial_z\|}\left(\frac{\partial}{\partial y}(\|\partial_z\|\cdot -) - \frac{\partial}{\partial z}(\|\partial_y\|\cdot -)\right)\;, \\
& \frac{1}{\|\partial_z\|\|\partial_x\|}\left(\frac{\partial}{\partial z}(\|\partial_x\|\cdot -) - \frac{\partial}{\partial x}(\|\partial_z\|\cdot -)\right)\;, \\
& \frac{1}{\|\partial_x\|\|\partial_y\|}\left(\frac{\partial}{\partial x}(\|\partial_y\|\cdot -) - \frac{\partial}{\partial y}(\|\partial_x\|\cdot -)\right)\;\Bigg]
\end{aligned}
$$

$$\mathrm{div}:\nabla = \frac{1}{\|\partial_x\|\|\partial_y\|\|\partial_z\|}\left[\;\frac{\partial}{\partial x}(\|\partial_y\|\|\partial_z\|\cdot -)\;,\;\frac{\partial}{\partial y}(\|\partial_z\|\|\partial_x\|\cdot -)\;,\;\frac{\partial}{\partial z}(\|\partial_x\|\|\partial_y\|\cdot -)\;\right]$$

$$\Delta = \frac{1}{\|\partial_x\|\|\partial_y\|\|\partial_z\|}\left[\;\frac{\partial}{\partial x}\left(\frac{\|\partial_y\|\|\partial_z\|}{\|\partial_x\|}\frac{\partial}{\partial x}\right) + \frac{\partial}{\partial y}\left(\frac{\|\partial_z\|\|\partial_x\|}{\|\partial_y\|}\frac{\partial}{\partial y}\right) + \frac{\partial}{\partial z}\left(\frac{\|\partial_x\|\|\partial_y\|}{\|\partial_z\|}\frac{\partial}{\partial z}\right)\;\right]$$

$$\mathrm{grad} = \frac{1}{\|\cdot\|^1}\,(\nabla)\,\|\cdot\|^0$$

$$\mathrm{curl} = \frac{1}{\|\cdot\|^2}\,(\nabla\times)\,\|\cdot\|^1$$

$$\mathrm{div} = \frac{1}{\|\cdot\|^3}\,(\nabla\cdot)\,\|\cdot\|^2$$

9 Bundles

Show that S^n has a nonvanishing vector field if and only if n is odd.

Solution. Since S^n is embedded in $\mathbb{R}^{n+1}$, the tangent bundle TS^n can be considered as an embedded manifold in $S^n \times \mathbb{R}^{n+1}$ which consists of (x, v) such that $\langle x, x\rangle = 1$ and $\langle x, v\rangle = 0$, where the inner product is the standard one of $\mathbb{R}^{n+1}$.

Suppose n is odd. We have a vector field $(x_1, x_2, \cdots, x_{n+1}; x_2, -x_1, \cdots, -x_n)$ which is nonvanishing.

Conversely, suppose we have a nonvanishing vector field X. Consider a map

$$\phi : S^n \xrightarrow{X} TS^n \to S^n \times \mathbb{R}^{n+1} \xrightarrow{\phi} \mathbb{R}^{n+1} \to S^n.$$

The last map can be defined since X is nowhere zero. Since this map satisfies $\langle x, \phi(x)\rangle = 0$ for all $x \in S^n$, we can define homotopies from ϕ to the identity map and the antipodal map respectively. Therefore, the antipodal map must have positive degree, $+1$, so n is odd. □

Proposition 9.1. *Independent commuting vector fields are realized as partial derivatives in a chart.*

Proposition 9.2. *Let $\{\partial_1, \cdots, \partial_k\}$ be an independent involutive vector fields. We can find independent commuting $\{\partial_{k+1}, \cdots, \partial_n\}$ such that union is independent. (Maybe)*

Proposition 9.3. *Let $\{\partial_1, \cdots, \partial_k\}$ be an independent commuting vector fields. We can find independent commuting $\{\partial_{k+1}, \cdots, \partial_n\}$ such that union is independent and commuting. (Maybe)*

The following theorem says that image of immersion is equivalent to kernel of submersion.

Proposition 9.4. *An immersed manifold is locally an inverse image of a regular value.*

Proposition 9.5. *A closed submanifold with trivial normal bundle is globally an inverse image of a regular value.*

Proof. It uses tubular neighborhood. Pontryagin construction? □

Proposition 9.6. *An immersed manifold is locally a linear subspace in a chart.*

Proposition 9.7. *Distinct two points on a connected manifold are connected by embedded curve.*

Proof. Let $\gamma : I \to M$ be a curve connecting the given two points, say p, q.

*Step [.1]*Constructing a piecewise linear curve For $t \in I$, take a convex chart U_t at $\gamma(t)$. Since I is compact, we can choose a finite $\{t_i\}_i$ such that $\bigcup_i \gamma^{-1}(U_{t_i}) = I$. This implies $\operatorname{im}\gamma \subset \bigcup_i U_{t_i}$. Reorganize indices such that $\gamma(t_1) = p$, $\gamma(t_n) = q$, and $U_{t_i} \cap U_{t_{i+1}} \neq \varnothing$ for all $1 \leq i \leq n-1$. It is possible since the graph with $V = \{i\}_i$ and $E = \{(i,j) : U_{t_i} \cap U_{t_j} \neq \varnothing$ is connected. Choose $p_i \in U_{t_i} \cap U_{t_{i+1}}$ such that they are all dis for $1 \leq i \leq n-1$ and let $p_0 = p$, $p_n = q$.

How can we treat intersections?

Therefore, we get a piecewise linear curve which has no self intersection from p to q.

*Step [.2]*Smoothing the curve □

Proposition 9.8. *Let M is an embedded manifold with boundary in N. Any kind of sections on M can be extended on N.*

Proposition 9.9. *Every ring homomorphism $C^\infty(M) \to \mathbb{R}$ is obtained by an evaluation at a point of M.*

Proof. Suppose $\phi : C^\infty(M) \to \mathbb{R}$ is not an evaluation. Let h be a positive exhaustion function. Take a compact set $K := h^{-1}([0, \phi(h)])$. For every $p \in K$, we can find $f_p \in C^\infty(M)$ such that $\phi(f_p) \neq f_p(p)$ by the assumption. Summing $(f_p - \phi(f_p))^2$ finitely on K and applying the extreme value theorem, we obtain a function $f \in C^\infty(M)$ such that $f \geq 0$, $f|_K > 1$, and $\phi(f) = 0$. Then, the function $h + \phi(h)f - \phi(h)$ is in kernel of ϕ although it is strictly positive and thereby a unit. It is a contradiction. □

Proposition 9.10. *The set of points that is geodesically connected to a point is open.*

10 Some problems

Problems I made:

1. Let f be C^2 with $f''(c) \neq 0$. Defined a function ξ such that $f(x) - f(c) = f'(\xi(x))(x - c)$ with $|\xi - c| \leq |x - c|$, show that $\xi'(c) = 1/2$.

2. Let f be a C^2 function such that $f(0) = f(1) = 0$. Show that $\|f\| \leq \frac{1}{8}\|f''\|$.

3. Show that a measurable subset of $\mathbb{R}$ with positive measure contains an arbitrarily long subsequence of an arithmetic progression.

4. Show that there is no continuous bijection from $[0, 1]^2 \setminus \{p\}$ to $[0, 1]^2$.

---

1. Show that for a nonnegative sequence a_n if $\sum a_n$ diverges then $\sum \frac{a_n}{1+a_n}$ also diverges.

2. Show that if both limits of a function and its derivative exist at infinity then the former is 0.

3. Show that every real sequence has a monotonic subsequence that converges to the limit superior of the supersequence.

4. Show that if a decreasing nonnegative sequence a_n converges to 0 and satisfies $S_n \leq 1 + na_n$ then S_n is bounded by 1.

5. Show that the set of local minima of a convex function is connected.

6. Show that a smooth function such that for each x there is n having the nth derivative vanish is a polynomial.

7. Show that if a continuously differentiable f satisfies $f(x) \neq 0$ for $f'(x) = 0$, then in a bounded set there are only finite points at which f vanishes.

8. Let a function f be differentiable. For $a < a' < b < b'$ show that there exist $a < c < b$ and $a' < c' < b'$ such that $f(b) - f(a) = f'(c)(b - a)$ and $f(b') - f(a') = f'(c')(b' - a')$.

9. Show that if $xf'(x)$ is bounded and $x^{-1}\int_0^x f \to L$ then $f(x) \to L$ as $x \to \infty$.

10. Show that if a sequence of real functions $f_n \colon [0, 1] \to [0, 1]$ satisfies $|f(x) - f(y)| \leq |x - y|$ whenever $|x - y| \geq \frac{1}{n}$, then the sequence has a uniformly convergent subsequence.

11. (Flett)

12. Let f be a differentiable function with $f(0) = 0$. Show that there is $c \in (0, 1)$ such that $cf(c) = (1 - c)f'(c)$.

13. Find the value of $\lim_{n\to\infty} \frac{1}{n} \left(\sum_{k=1}^{n} \frac{1}{n} f\left(\frac{k}{n}\right) - \int_0^1 f(x)\, dx \right)$.

---

14. Let f be a continuous function. Show that f(x)=c cannot have exactly two solutions for every c.

15. Show that a continuous function that takes on no value more than twice takes on some value exactly once.

16. Let f be a function that has the intermediate value property. Show that if the preimage of every singleton is closed, then f is continuous.

---

17. Show that if a holomorphic function has positive real parts on the open unit disk then $|f'(0)| < 2 \operatorname{Re} f(0)$.

18. Show that if at least one coefficient in the power series of a holomorphic function at each point is 0 then the function is a polynomial.

19. Show that if a holomorphic function on a domain containing the closed unit disk is injective on the unit circle then so is on the disk.

20. Show that for a holomorphic function f and every z_0 in the domain there are $z_1 \neq z_2$ such that $\frac{f(z_1)-f(z_2)}{z_1-z_2} = f'(z_0)$.

21. For two linearly independent entire functions, show that one cannot dominate the other.

22. Show that uniform limit of injective holomorphic function is either constant or injective.

23. Suppose the set of points in a domain $U \subset \mathbb{C}$ at which a sequence of bounded holomorphic functions (f_n) converges has a limit point. Show that (f_n) compactly converges.

---

24. Show that normal nilpotent matrix equals zero.

25. Show that two matrices AB and BA have same nonzero eigenvalues whose both multiplicities are coincide blabla...

26. Show that if A is a square matrix whose characteristic polynomial is minimal then a matrix commuting A is a polynomial in A.

27. Show that if two by two integer matrix is a root of unity then its order divides 12.

28. Show that a finite symmetric group has two generators.

29. Show that a nontrivial normalizer of a p-group meets its center out of identity.

30. Show that a proper subgroup of a finite p-group is a proper subgroup of its normalizer. In particular, every finite p-group is nilpotent.

31. Show that the complement of a saturated monoid in a commutative ring is a union of prime ideals.

32. Show that the Galois group of a quintic over $\mathbb{Q}$ having exactly three real roots is isomorphic to S_5.

33. Show that if $A^\circ \in B$ and B is closed, then $(A \cup B)^\circ \subset B$.

34. Show that the tangent space of the unitary group at the identity is identified with the space of skew Hermitian matrices.

35. Prove the Jacobi formula for matrix.

36. Show that S^3 and T^2 are parallelizable.

37. Show that $\mathbb{R}P^n = S^n/Z_2$ is orientable if and only if n is odd.