Contents

1 Fock space reading notes

1.1 Closed operators

Definition 1.1. An operator A is said to be *closable* if

$$x_n \text{ and } Ax_n \text{ are Cauchy} \quad \Longrightarrow \quad \lim_{n\to\infty} Ax_n = A \lim_{n\to\infty} x_n.$$

Note that the opposite direction is always true.

1.1.1 Properties of closed operators

For closed operators, we introduce a new norm.

Theorem 1.1. *Let A, B be closed operators between Banach spaces. Then, $A+B$ is closed iff*

$$\|Ax\| + \|Bx\| \lesssim \|(A+B)x\| + \|x\|$$

for $x \in D(A) \cap D(B)$, i.e. A and B are $A+B$-bounded. It is paraphrased by

$$\|x\|_A + \|x\|_B \sim \|x\|_{A+B}.$$

Proof. ($\Leftarrow$) Suppose $(x_n, (A+B)x_n)$ is Cauchy. Then, the inequality gives that Ax_n and Bx_n are Cauchy. Since A and B are closed, we have $\lim Ax_n = A \lim x_n$ and $\lim Bx_n = B \lim x_n$. So $\lim(A+B)x_n = \lim Ax_n + \lim Bx_n = A \lim x_n + B \lim x_n = (A+B) \lim x_n$.

($\Rightarrow$) □

Theorem 1.2. *Let A be a closed, and B be a closable operator between Banach spaces with $D(A) \subset D(B)$. Then, $A+B$ is closed if*

$$\|Bx\| \le \alpha\|Ax\| + c\|x\|$$

for some $\alpha < 1$.

Proof.

$$\|Ax\| \le \|(A+B)x\| + \|Bx\| \le \|(A+B)x\| + \alpha\|Ax\| + c\|x\|$$

implies

$$\|Ax\| \lesssim \|(A+B)x\| + \|x\|.$$

□

Proposition 1.3 (Closed graph theorem)**.** *For $T \in D_{cl}(X, Y)$,*

$$T \text{ is unbounded} \quad \Longleftrightarrow \quad T \text{ is not everywhere defined.}$$

Closed operators,

(1) provide with the optimal extended domain for adjoint operators,

(2) have maximal essential domains,

(3) are closed under invertibility,

(4) do not distinguish everywhere defined denslely defined, since everywhere definedness is equivalent to boundedness.

1.1.2 Decomposition of spectrum for closed operators

Note that since decomposition of spectrum is orginated for application to quantum mechanics, this traditional definition is usually for closed operators. Even though the following definitions can be applied for non-closable operators, but it does not make sense in any senses. So, every operator in this subsection is assumed to be *closed*.

Let $X = Y$ in order to see $L(X, Y)$ as a ring. Let $B(X) \subset D(X) \subset L(X)$ be the spaces of *everywhere defined operators, densely defined operators, and just linear operators* respectively. Note that $D(X)$ is not a vector space. For $T \in L(X)$,

$$\lambda \begin{cases} \text{is in } \rho(T) \\ \text{is in } \sigma_c(T) \\ \text{is in } \sigma_r(T) \\ \text{is in } \sigma_p(T) \end{cases} \qquad \textit{iff} \qquad R_\lambda(T) \begin{cases} \in B(X) \\ \in D(X) \setminus B(X) \\ \in L(X) \setminus D(X) \\ \text{cannot be defined.} \end{cases} .$$

Discrete spectrum is defined to consist of scalars having finite dimensional eigenspace and is isolated from any other elements in spectrum.

1.2 Densly defined operators

1.2.1 Adjoint

Adjoint is defined for densely defined operators: For Banach spaces, we have

$$\mathrm{adj} : D(X, Y) \to L_{cl}(Y^*, X^*)$$

that is not injetcive. (I don't know it's surjective)

For reflexive Y, we have

$$\mathrm{adj} : D_{cl}(X, Y) \to D_{cl}(Y^*, X^*)$$

that is inj? surj?

For reflexive X, we have

$$adj : D_{closable}(X) \Rightarrow D_{cl}(X^*).$$

For $f : X \to Y$, "I" define the predicate $f : A \Rightarrow B$ by

$$f(A) = B \quad \text{and} \quad A = f^{-1}(B).$$

Theorem 1.4. *The adjoint $B_{cl}(H) \overset{\sim}{\to} B_{cl}(H)$ can be extended to $D_{cl}(H) \overset{\sim}{\to} D_{cl}(H)$.*

Theorem 1.5. *For $T \in D_{cl}(H)$, $H = \ker T \oplus \overline{\operatorname{im} T^*}$.*

The space D_{cl} is optimized when we think adjoints for reflexive spacse.

unitarily equivalence can defined for $T_1 \in L(H_1)$ and $T_2 \in L(H_2)$.

1.3 Self-adjoint operators

Definition 1.2. Let $T \in L(H)$ be satisfy $T \subset T^*$, i.e. $\langle Tx, y\rangle = \langle x, Ty\rangle$ for all $x, y \in D(T)$. Then, we have definitions by the following diagram:

$$\begin{tikzcd}
 & & \text{Bounded self-adjoint} \arrow[d] \\
\text{Hermitian} \arrow[urr, dashed, bend left, "\text{everywhere defined}"] \arrow[r, dashed, bend right, "\text{densely defined}"'] & \text{Symmetric} \arrow[l] \arrow[r, dashed, bend right, "D(T) = D(T^*)"'] & \text{Self-adjoint} \arrow[l]
\end{tikzcd}$$

Proposition 1.6. *Hermitian iff the numerical range is in $\mathbb{R}$.*

Proposition 1.7. *A symmetric operator is closable.*

Proof. Since T is dense and $T \subset T^*$, T^* is dense. Therefore, T is closable. $\square$

2 Vector calculus on spherical coordinates

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

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

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

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

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

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

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

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

$$\begin{aligned}
\text{grad} : \nabla &= \left[\ \frac{1}{\|\partial_x\|}\frac{\partial}{\partial x}\cdot - \ ,\ \frac{1}{\|\partial_y\|}\frac{\partial}{\partial y}\cdot - \ ,\ \frac{1}{\|\partial_z\|}\frac{\partial}{\partial z}\cdot - \ \right] \\
\text{curl} : \nabla &= \left[\ \frac{1}{\|\partial_y\|\|\partial_z\|}\left(\frac{\partial}{\partial y}(\|\partial_z\|\cdot -) - \frac{\partial}{\partial z}(\|\partial_y\|\cdot -)\right)\ ,\right. \\
&\qquad \frac{1}{\|\partial_z\|\|\partial_x\|}\left(\frac{\partial}{\partial z}(\|\partial_x\|\cdot -) - \frac{\partial}{\partial x}(\|\partial_z\|\cdot -)\right)\ , \\
&\qquad \left.\frac{1}{\|\partial_x\|\|\partial_y\|}\left(\frac{\partial}{\partial x}(\|\partial_y\|\cdot -) - \frac{\partial}{\partial y}(\|\partial_x\|\cdot -)\right)\ \right] \\
\text{div} : \nabla &= \frac{1}{\|\partial_x\|\|\partial_y\|\|\partial_z\|}\left[\ \frac{\partial}{\partial x}(\|\partial_y\|\|\partial_z\|\cdot -)\ ,\ \frac{\partial}{\partial y}(\|\partial_z\|\|\partial_x\|\cdot -)\ ,\ \frac{\partial}{\partial z}(\|\partial_x\|\|\partial_y\|\cdot -)\ \right] \\
\Delta &= \frac{1}{\|\partial_x\|\|\partial_y\|\|\partial_z\|}\left[\ \frac{\partial}{\partial x}\left(\frac{\|\partial_y\|\|\partial_z\|}{\|\partial_x\|}\frac{\partial}{\partial x}\right) + \frac{\partial}{\partial y}\left(\frac{\|\partial_z\|\|\partial_x\|}{\|\partial_y\|}\frac{\partial}{\partial y}\right) + \frac{\partial}{\partial z}\left(\frac{\|\partial_x\|\|\partial_y\|}{\|\partial_z\|}\frac{\partial}{\partial z}\right)\ \right]
\end{aligned}$$

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

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

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

3 Statements in functional analysis and general topology

Function analysis:

- Every seperable Banach space is linearly isomorphic and homeomorphic. But there are two non-isomorphic Banach spaces.
- open mapping theorem -¿ continuous embedding is really an embedding.
- $D(\Omega)$ is defined by a *countable stict* inductive limit of $D_K(\Omega)$, $K \subset \Omega$ compact. Hence it is not metrizable by the Baire category theorem. (Here strict means that whenever $\alpha < \beta$ the induced topology by $\mathcal{T}_\beta$ coincides with $\mathcal{T}_\alpha$)
- A net $(\phi_d)_d$ in $D(\Omega)$ converges if and only if there is a compact K such that $\phi_d \in D_K(\Omega)$ for all d and ϕ_d converges uniformly.
- Th integration with a locally integrable function is a distribution. This kind of distribution is called *regular*. The nonregular distribution such as δ is called *singular*.
- D' is equipped with the weak* topology.
- $\frac{\partial}{\partial x} \colon D' \to D'$ is continuous. They commute (Schwarz theorem holds).
- $D \to S \to L^p$ are continuous (immersion) but not imply closed subspaces (embedding).

General topology:

- $H \subset \mathbb{C}$ and $H \subset \widehat{\mathbb{C}}$ have distinct Cauchy structures which give a same topology. In addition, the latter is precompact while the former is not.

4 Algebraic closure

Theorem 4.1. *Every field has an algebraic closure.*

Proof. Let F be a field.

Step 1: Construct an algebraically closed field containing F.. Let S be a set of irreducibles or nonconstants in $F[x]$.(anyone is fine) Define $R := F[\{x_p\}_{p \in S}]$. Let I be an ideal in R generated by $p(x_p)$ as p runs through all S. It has a maximal ideal $\mathfrak{m} \supset I$.

Define $K_1 := R/\mathfrak{m}$. Every nonconstant $f \in F[x]$ has a root in K_1. (In fact, this K_1 is already algebraically closed, but it's hard to prove.) Construct $K_2, \cdots$ such that every nonconstant $f \in K_n[x]$ has a root in K_{n+1}. Define $K = \lim_{\to} K_n$. Then, K is algebraically closed.

Step 2: Construct the algebraic closure of F.. Let $\overline{F}$ be the set of all algebraic elements of K over F. Then, this is the algebraic closure. $\square$

5 Space curve theory

Definition 5.1. Let α be a curve.

$$\mathbf{T} := \frac{\alpha'}{\|\alpha'\|}, \quad \mathbf{N} := \frac{\mathbf{T}'}{\|\mathbf{T}'\|}, \quad \mathbf{B} := \mathbf{T} \times \mathbf{N}.$$

Proposition 5.1. *$\mathbf{T}', \mathbf{B}', \mathbf{N}$ are collinear.*

Definition 5.2.

$$s(t) := \int_0^t \|\alpha'\|, \quad \kappa := \frac{d\mathbf{T}}{ds} \cdot \mathbf{N}, \quad \tau := -\frac{d\mathbf{B}}{ds} \cdot \mathbf{N}.$$

Theorem 5.2 (Frenet-Serret formula)**.** *Let α be a unit speed curve.*

$$\begin{pmatrix} \mathbf{T}' \\ \mathbf{N}' \\ \mathbf{B}' \end{pmatrix} = \begin{pmatrix} 0 & \kappa & 0 \\ -\kappa & 0 & \tau \\ 0 & -\tau & 0 \end{pmatrix} \begin{pmatrix} \mathbf{T} \\ \mathbf{N} \\ \mathbf{B} \end{pmatrix}.$$

Theorem 5.3. *Let α be a unit speed curve.*

$$\begin{aligned} \alpha' &= \mathbf{T} \\ \alpha'' &= \kappa \mathbf{N} \\ \alpha''' &= -\kappa^2 \mathbf{T} + \kappa' \mathbf{N} + \kappa\tau \mathbf{B} \end{aligned}$$

$$\kappa = \|\alpha''\|, \quad \tau \frac{[\alpha'\alpha''\alpha''']}{\kappa^2}.$$

Theorem 5.4. *Let α be a curve.*

$$\begin{aligned} \alpha' &= s'\mathbf{T} \\ \alpha'' &= s''\mathbf{T} + s'^2\kappa\mathbf{N} \\ \alpha''' &= (s''' - s'^3\kappa^2)\mathbf{T} + (3s's''\kappa + s'^2\kappa')\mathbf{N} + s'^3\kappa\tau\mathbf{B} \end{aligned}$$

$$\kappa = \frac{\|\alpha' \times \alpha''\|}{\|\alpha'\|^3}, \quad \tau = \frac{[\alpha'\alpha''\alpha''']}{\|\alpha' \times \alpha''\|}.$$

Problem solving strategy:

- Represent α and its derivatives over the Frenet basis.
-

Uniqueness: The Frene-Serret formula is an ODE for the vector (of vectors) $(\mathbf{T}, \mathbf{N}, \mathbf{B})$. After showing this equation preserves orthonormality, obtain α by integratin $\mathbf{T}$. The skew-symmetry implies that $\|\mathbf{T}\|^2 + \|\mathbf{N}\|^2 + \|\mathbf{B}\|^2$ is constant.

6 Algebraic integer

6.1 Quadratic integer

Theorem 6.1. *Every quadratic field is of the form $\mathbb{Q}(\sqrt{d})$ for a square-free d.*

Theorem 6.2. *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 6.3.

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

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

Theorem 6.4. *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 6.5. *If θ^3 is a square free integer, then*

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

6.2 Integral basis

Theorem 6.6. *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 6.7. *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 6.8. *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*

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

6.3 Fractional ideals

Theorem 6.9. *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. $\square$

6.4 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 6.10. *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 6.1. 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

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

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

6.5 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 $\zeta_D = e^{\frac{2\pi i}{D}}$.

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

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.

7 Diophantine equations

7.1 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 7.1 (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 7.2 (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.

7.2 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 7.3. 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. □

Example 7.4. 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. □

8 The local-global principle

8.1 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 8.1. 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 8.2. $\mathbb{Q}_p = \operatorname{Frac} \mathbb{Z}_p$.

Secondly, here is the analytic definition.

Definition 8.3. 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 8.4. $\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$.

Example 8.1. 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 8.2.

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

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

Proof. Trivial. $\square$

Theorem 8.4. *Every triangle in $\mathbb{Q}_p$ is isosceles.*

Theorem 8.5. *$\mathbb{Z}_p$ is a discrete valuation ring: it is local PID.*

Proof. asdf $\square$

Theorem 8.6. *$\mathbb{Z}_p$ 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

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

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 $\mathbb{Z}_p$. $\square$

8.2 Hensel's lemma

Theorem 8.7 (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 8.8. $f(x) = x^p - x$ is factorized linearly in $\mathbb{Z}_p[x]$.

8.3 Sums of two squares

Theorem 8.9 (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 8.10. *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.*

9 Ultrafilter

Theorem 9.1. *Let $\mathcal{U}$ be an ultrafilter on a set S and X be a compact space. For $f: S \to X$, the limit $\mathcal{U}$-$\lim f$ always exists.*

Theorem 9.2. *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 $f: \mathcal{E} \to X$ 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.

□

10 Universal coefficient theorem

Lemma 10.1. *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 10.2. *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

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

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

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

$\square$

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

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

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.

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

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

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

□

11 Estimates

Theorem 11.1. *The following series diverges:*

$$\sum_{n=1}^{\infty} \frac{1}{n^{1+|\sin n|}}.$$

Proof. Let $A_k := [1, 2^k] \cap \{x : |\sin x| < \frac{1}{k}\}$. Divide the unit circle $\mathbb{R}/2\pi\mathbb{Z}$ by $7k$ uniform arcs. There are at least $2^k/7k$ integers that are not exceed 2^k and are in a same arc. Let S be the integers and x_0 be the smallest element. Since, $|x - x_0| \pmod{2\pi} < \frac{2\pi}{7k}$ for $x \in S$,

$$|\sin(x - x_0)| < |x - x_0| \pmod{2\pi} < \frac{2\pi}{7k} < \frac{1}{k}.$$

Also, $1 \le x - x_0 \le x \le 2^k$, $x - x_0 \in A_k$.

$$|A_k| \ge \frac{2^k}{7k}.$$

Therefore,

$$\begin{aligned}
\sum_{n=1}^{\infty} \frac{1}{n^{1+|\sin n|}} &\ge \sum_{n \in A_N} \frac{1}{n^{1+|\sin n|}} \\
&\ge \sum_{k=1}^{N} (|A_k| - |A_{k-1}|) \frac{1}{2^{k+1}} \\
&= \sum_{k=1}^{N} \frac{|A_k|}{2^{k+1}} - \sum_{k=1}^{N-1} \frac{|A_k|}{2^{k+2}} \\
&= \frac{|A_N|}{2^{N+1}} + \sum_{k=1}^{N-1} \frac{|A_k|}{2^{k+2}} \\
&> \sum_{k=1}^{N} \frac{2^k}{2^{k+2}} \frac{1}{7k} \\
&= \frac{1}{28} \sum_{k=1}^{N} \frac{1}{k} \\
&\to \infty.
\end{aligned}$$

□

Theorem 11.2. *If $|xf'(x)| \le M$ and $\frac{1}{x}\int_0^x f(y)\,dy \to L$, then $f(x) \to L$ as $x \to \infty$.*

Proof. Since

$$\begin{aligned}
\left| f(x) - \frac{F(x) - F(a)}{x - a} \right| &\le \frac{1}{x - a} \int_a^x |f(x) - f(y)|\,dy \\
&= \frac{1}{x - a} \int_a^x (x - y)|f'(c)|\,dy \\
&\le \frac{M}{x - a} \int_a^x \frac{x - y}{c}\,dy \\
&\le M \frac{x - a}{a}
\end{aligned}$$

by the mean value theorem and

$$f(x) - L = \left[f(x) - \frac{F(x) - F(a)}{x - a}\right] + \frac{x}{x-a}\left[\frac{F(x)}{x} - L\right] + \frac{a}{x-a}\left[\frac{F(a)}{a} - L\right],$$

we have for any $\varepsilon > 0$

$$\limsup_{x \to \infty} |f(x) - L| \leq \varepsilon$$

where a is defined by $\frac{x-a}{a} = \frac{\varepsilon}{M}$. $\square$

12 Action

Definition

- $G \curvearrowright X$
  - fcn $G \times X \to X$: compatibility, identity
  - hom $\rho\colon G \to \mathrm{Sym}(X)$ or $\mathrm{Aut}(X)$
  - funtor from G

  nt) X is called G-set.

  nt) ρ is called permutation repr.

  $*$ right action is a contravariant functor.

- $\mathrm{Stab}_G(x) = G_x$, $\mathrm{Orb}_G(x) = G.x$
  - Orbit-stabilizer theorem

    pf) quotient with $-.x\colon G \to X$.

    $*$ this is not the first isom.

  $*$ stabilizer is also called isotropy group.

- Faithfulness, Transitivity

Useful Actions

$*$ these actions are on $P(G)$.

- Left Multiplication
  - $\mathrm{Stab}(A) = AA^{-1}$

  eg) $G \curvearrowright G/H$, for $H \leq G$

  $\ker \rho = \bigcap xHx^{-1} = \mathrm{Core}_G(H)$

- Conjugation
  - $\mathrm{Stab}(A) = N_G(A)$

  eg) $G \curvearrowright \{\{h\} : h \in H\}$, for $H \lhd G$

  $\ker \rho = C_G(H)$, $\mathrm{im}\,\rho \subset \mathrm{Aut}(H)$

  eg) $G \curvearrowright \mathrm{Syl}_p$

  $*$ conjugation is an isomorphism.

Sylow Theorem

- $\mathrm{Syl}_p \neq \varnothing$
- $n_p = kp + 1 \mid \left[G : \overline{P}\right]$

- $G \curvearrowright \mathrm{Syl}_p$ transitive

  pf) four actions by conjugation:

  $$G \curvearrowright G, \quad \overline{P}, G, P \curvearrowright \mathrm{Orb}_G(\overline{P}).$$

EXERCISES

13 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.