LaTeX M1 NOTE II

X

January 29, 2026

Github: https://github.com/Baudelaireee/Notebook

Contents

1 Some linear algebra

This section can be seen as a breif review of linear agebra, it mainly focus on something related to lie theory and representation theory.

1.1 Decomposition of endomorphisms

Theorem 1.1 (Real-Polar decomposition)**.**
For any real endomorphism $A \in \mathrm{GL}_n(\mathbb{R})$, there exists a unique orthogonal endomorphism $O \in O(n)$ and a unique symmetric positive definite endomorphism $P \in S_n^{++}(\mathbb{R})$ such that

$$A = OP$$

Proof. Here is the outline of the proof:
(1) A **lemma** about the existence of square root are needed here: If $A \in S_n^+(\mathbb{R})$, then there exists a (unique) $B \in S_n^+(\mathbb{R})$ such that $B^2 = A$.
(2) Prove that A^tA is (semi-definite) positive, thus by the lemma there exist a (unique) squar root $P = \sqrt{A^tA}$, and we prove that P is positive definite.
(3) Define $O = AP^{-1}$, and prove that O is orthogonal.
(4) Prove the uniqueness of the decompoistion.

Here is the details:
(1) By real-spectral theorem, there exists $O \in O(n)$ such that

$$A = ODO^T, \quad D = \mathrm{dig}(\lambda_1, ..., \lambda_n)$$

where $\lambda_i \geq 0$ are the eigenvalues of A, and we set $\Sigma = \mathrm{dig}(\sqrt{\lambda_1}, ..., \sqrt{\lambda_n})$ such that

$$A = (O\Sigma O^T)^2$$

which shows that $B = O\Sigma O^T$ is a (unique) square root of A and it is positive since $\sqrt{\lambda_i} \geq 0$.

(2) A^TA is clearly symmetric, and it is positive since

$$x^T(A^TA)x = \|Ax\| \geq 0$$

for any $x \in \mathbb{R}^n$ under the common inner product, and A is invertible such that $\|Ax\| = 0$ if and only if $x = 0$, thus A^TA is positive definite, so does its square root (the eignevalues is strictly positive).

(3) $P^{-1} = (P^{-1})^T$ since P is symmetric, so we have

$$O^TO = (P^{-1})^TA^TAP^{-1} = (P^{-1})^TP^2P^{-1} = I$$

(4) Suppose that there eixsts another decomposition $A = O_0P_0$, then we have

$$A^TA = P_0^TO_0^TO_0P_0 = P_0^2$$

so P_0 is the positive square root of A^TA, if the uniqueness of (1) is proved, we can finish the proof, but here we give another proof of the uniqueness only under the existence of the

square root: we have $O_0^{-1}O = P_0P^{-1}$, so it is easy to check that P_0P^{-1} is **orthogonal**; notice that P_0 and A^TA commute, and there exists a polynomial f such that

$$f(A^TA) = P$$

it can be done by using lagrange interpolation, thus P_0 and P commute as two symmetric matrix, then P and P_0 can be diagonalized simultaneously by one orthogonal H such that

$$P = HDH^T \quad P_0 = HD_0H^T$$

where $D = \mathrm{dig}(\lambda_1, ..., \lambda_n)$ and $D_0 = \mathrm{dig}(\mu_1, ..., \mu_n)$, thus

$$P_0P^{-1} = HD_0^{-1}DH^T$$

it is **symmetric and positive definite** since $D_0^{-1}D$ is digonal with positive entries, thus $P_0P^{-1} \in O(n) \cap S_n^{++}(\mathbb{R}) = \{I\}$, which implies that $P_0 = P$ and $O_0 = O$. □

Theorem 1.2 (Complex-Polar decomposition)**.**
For any complex endomorphism $A \in \mathrm{GL}_n(\mathbb{C})$, there exists a unique unitary endomorphism $U \in U(n)$ and a unique hermitian positive definite endomorphism $P \in H_n^{++}(\mathbb{C})$ such that

$$A = UP$$

The proof is similar to the real case, we set $P = \sqrt{A^*A}$ and $U = AP^{-1}$, and the lemma is based on the complex-spectral theorem for normal opreator: The postive Hermitian endomorphism has a unique positive Hermitian square root.

Remark 1.1. In particular, if $n = 1$, we have the polar decompistion in $\mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^*$ by

$$z = |z|e^{iArg(z)}$$

it is easy to see that $U(1) \cong \mathbb{S}^1$, it is the original ideal of the decomposition. Similarly, in the real case, we can embed $\mathbb{C}$ into $\mathrm{GL}_2(\mathbb{R})$ by

$$a + ib \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

and we have the polar decomposition for the matrix form of complex numbers:

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} \sqrt{a^2+b^2} & 0 \\ 0 & \sqrt{a^2+b^2} \end{pmatrix} \begin{pmatrix} \frac{a}{\sqrt{a^2+b^2}} & -\frac{b}{\sqrt{a^2+b^2}} \\ \frac{b}{\sqrt{a^2+b^2}} & \frac{a}{\sqrt{a^2+b^2}} \end{pmatrix}$$

Another useful decomposition is QR decomoposition, which is also called as Gram-Schimidt decompoistion. Suppose that

2 Exponential map

Remember that $M_n(K) \cong K^{n^2}$ for any field (even any ring), in particualr we consider $K = \mathbb{C}$ or $\mathbb{R}$, then the space of endomorphisms or matirces is just a finite-dimensional

vector space over the field, so we can define the typical norm on it:

$$\|A\| = \sqrt{\sum_{i,j} |a_{ij}|^2} \quad \text{(euclidean norm)}$$
$$\|A\|_\infty = \max_{i,j} |a_{ij}| \quad \text{(Max norm)}$$
$$\|A\|_1 = \sum_{i,j} |a_{ij}| \quad \text{(Sum norm)}$$

Moreover, we can consider the norm of $M_n(K)$ from another view, we view it as the linear continous operator inside K^n, hence in particular the norm of K^n can induce the norm of operator:

$$\|A\|_{op} = \sup_{x \in K^n - \{0\}} \frac{\|Ax\|}{\|x\|}$$

Anyway, the space of endomrphisms on finitie-dimensional vector space or the matrix space is still finite-dimensional, as a Banach space, all the norms on $M_n(K)$ is equivalent, with the basic knowledge of topology on it, we can talk about some whether some series in analysis makes sense or not, in particular, exponential map:

Definition 2.1. For a matrix $A \in M_n(K)$, the exponential of A is defined by

$$\exp(A) = \sum_{k \geq 0} \frac{A^k}{k!}$$

or sometimes we denote it by e^A.

The definition is analogous to the exponential map in $\mathbb{C}$, and we can verify that it is well-defined for any A by

$$\|\exp(A)\| \leq \sum_{k \geq 0} \frac{\|A\|^k}{k!} = \exp(\|A\|) < +\infty$$

so exponential map still makes sense for linear algebra! Some algebraic properties can be conclude to handle different calculation, and they are important.

Proposition 2.1.

3 Toplogical Groups

3.1 Basic properties

Group and Topological space is two different objects, group is algebraic structure, topological space is geometric structure, but it is not strange to combine them together.

Definition 3.1. A **topological group** is a object $(G, \mathcal{T}, \cdot)$ such that

- $(G, \cdot)$ is a group
- $(G, \mathcal{T})$ is a topological space
- The group structure is compatible with topological structure, i.e. multiplication

$$m : G \times G \to G, \quad (x, y) \mapsto x \cdot y$$

and inverse

$$i : G \to G, \quad x \mapsto x^{-1}$$

are continuous maps.

With the basic definition, we can talk about the properties of topological groups, here is a useful lemma, it shows that the topological group is **homogeneous**, i.e. the local topology is same at any point.

Lemma 3.1. Let G be a topological group, then for any $g \in G$, we define **left translation** and **right translation** by

$$L_g : G \to G, \quad x \mapsto gx$$
$$R_g : G \to G, \quad x \mapsto xg$$

Then both L_g and R_g are homeomorphisms on G.

Proof. It is easy to verify that $L_{gh} = L_g \circ L_h$, and $R_{gh} = R_h \circ R_g$, then we have

$$L_g^{-1} = L_{g^{-1}}, \quad R_g^{-1} = R_{g^{-1}}$$

and we can check the continuity of L_g and R_g by composition. □

It is an important in the following proofs of properties, we first talk about the basic properties of topological groups.

Proposition 3.2. Let G be a topological group, then

(1) each open subgroup $H < G$ is also closed.

(2) each closed subgroup $H < G$ with finite index is also open.

Proof. The subgroup H gives a partition of G by left cosets:

$$G = \bigsqcup_{g \in \mathcal{S}} gH$$

with $\mathcal{S} \subset G$ the set of representatives in G/H, and we fix the representatives for H be e, then

$$G - H = \bigsqcup_{g \in S - \{e\}} gH$$

If H is open, then by translation each gH is also open, thus the union of open sets $G - H$ is also open, hence H is closed, which finishes that proof of (1). For the statement (2), the finite index shows that $\mathcal{S}$ is finite, and we suppose that the index is n. If $n = 1$, then $H = G$ is open clearly; otherwise, we can deduce that $G - H$ is the finite union of closed sets gH with $g \in \mathcal{S} - \{e\}$, thus it is closed, it can be done similarly by translation, hence H is open sice $G - H$ is closed. □

Then it is the **separation** of topological groups.

Proposition 3.3. Let G be a topological groups, then the following statements are equivalent:

(1) G is Hausdorff (T2).

(2) The singleton $\{e\}$ is closed in G.

(3) G is T1.

Proof. (3) implies (2) is clear, since T1 space makes all singletons closed; (1) implies (3) is just the implication from strong to weak separation axiom.

(2) implies (1): G is Hausdorff if and only if the diagonal set

$$\Delta = \{(g, g) \in G \times G \mid g \in G\}$$

is closed under the product topology, and topolgical group induces a continous map $f(x, y) = xy^{-1}$ for any $(x, y) \in G \times G$, then $\Delta = f^{-1}(\{e\})$ is closed by continuity. □

Corollary 3.4. Let G be a topological group and $H < G$ be a subgroup, then the quotient space G/H is **Hausdorff** if and only if H is **closed** in G.

Another topological properties is about **connectness**:

Proposition 3.5. Let G be a topological group, then

(1) If G is connected, then any open set containing e generates G.

(2) The connected component G_0 of identity $e \in G$ is a **closed normal subgroup** of G, and each connected component of G is homeomorphic to G_0 by translation.

Proof. (1) We denote $\langle A \rangle$ be the subgroup generated by $A \subset G$, and we take A be an open set containing e, we will prove that $\langle A \rangle$ is open and closed, by the connectness of G, which implies that $\langle A \rangle = G$. It is clear that

$$\bigcup_{x \in \langle A \rangle} xA \subset \langle A \rangle$$

conversely, for any $a \in \langle A \rangle$, we have $a = ae$ with $e \in A$, so a is in the union such that we can replace the inculsion by equality. Notice that $xA = L_x(A)$ is open since A is open, so $\langle A \rangle$ is also open as the union of open sets; By the propoistion 3.2, $\langle A \rangle$ is also closed since it is open subgroup, hence we finish the proof of (1).

(2) Any connected component is closed in general topology, which can be proved by contradition to $G_0 \subsetneq \overline{G_0}$. To prove that G_0 is a subgroup, we take a continous map $f(x, y) = xy^{-1}$ on $G \times G$, then $f(G_0 \times G_0)$ is connected since the finite product of connected spaces is connected, and we notice that $a = f(a, e)$ for any $a \in G_0$, so $G_0 \subset f(G_0 \times G_0)$ and then we can take equality by the maximality of connected component, and it shows that G_0 is exactly a subgroup.

To prove the normality, we take the conjugation map for any $g \in G$:

$$\sigma_g : G \to G, \quad x \mapsto gxg^{-1}$$

it is homeomorphism by composition $\sigma_g = L_g \circ R_g^{-1}$. Here $\sigma_g(e) = e$ and the image is also connected, so $\sigma_g(G_0) \subset G_0$ by the maximality of connected component, so it must be normal. □

Notice that if $H < G$ is a subgroup, then it induces a natural equivalence relation on G by left cosets:

$$x \sim y \iff x = yh, \text{ for some } h \in H$$

similarly we can define right cosets here, and then it gives a quotient space $G/\sim$ and we denote it by G/H, and it is natrually endowed with the quoitent topology with a (continous) quoitent map:

$$\pi : G \to G/H, \quad g \mapsto gH$$

In particular, if H is a normal subgroup, then G/H is exactly a topological group by UPQ:

$$\begin{array}{ccc} G \times G & \xrightarrow{f} & G \\ {\scriptstyle \pi\times\pi}\downarrow & & \downarrow{\scriptstyle \pi} \\ G/N \times G/N & \xrightarrow{f_{G/N}} & G/N \end{array}$$

with $f(g, h) = gh^{-1}$, so it gives the continuity of group opreation. However, it is not so easy to talk about the the topology of quoitent space G/H directly, it is better to see the quotient space as a **homogeneous space** under the action of G, hence we need to talk about acion of the topological group:

Definition 3.2. Let G be a topological group and X be a topological space, a continous action of G on X is a well-defined action in the sense of group together with a continous operation, that means there exists a continous map

$$\phi : G \times X \to X, \quad (g, x) \mapsto g \cdot x$$

such that for any $g, h \in G$ and $x \in X$, we have

(1) $e \cdot x = x$

(2) $g \cdot (h \cdot x) = (gh) \cdot x$

In the context of toplogical groups or Lie groups, we alwasys omit "continous" when it comes to actions, it is a convention sometimes in the liter

ature. It is similar to the algebraic action, we can define **stabilizer** of a point $x \in G$

$$I_x = \{g \in G \mid g \cdot x = x\}$$

It is sometimes called **isotropy group** at x, and it can be written as the preimage

$$I_x = \phi_x^{-1}(\{x\}), \quad \phi_x(g) = g \cdot x$$

with ϕ_x a continous map by fixing variable, hence the isotropy group is always a **closed subgroup** of G if X is Hausdorff (T1 is enough, but manifold makes sense). Similarly, we can define **orbit** of x by

$$Gx = O_x = \{g \cdot x \mid g \in G\}$$

which is the image of ϕ_x on the contrary, hence it gives a natural bijection

Lemma 3.6 (stabilizer-orbit)**.**
Let G be a compact group and X be a Hausdorff space, If G acts continously on X, then for any $x \in G$, there exists a homemomorphism $G/I_x \cong Gx$.

Proof. The proof is just based on the universal property of quotient space, and the stablizier-orbit theorem in group theory, we just need to check the natural bijection induced by ϕ_x is indeed a homemomorphism. □

In particular, the orbit gives a equivalence reliation on X by

$$x \sim y \iff y = g \cdot x, \text{ for some } g \in G$$

hence it gives a quotient space denoted by X/G and we call it **orbit space**, it is natrually endowed with the quoitent topology with a (continous) quoitent map:

$$\pi : X \to X/G, x \mapsto Gx$$

the following lemma is useful and important, it shows that the topology of group action is well-behaved from the view of techinc:

Lemma 3.7. The natural quotient map $\pi : X \to G/X$ is open.

Proof. Suppose that U is an open set of X, then we can prove

$$\pi^{-1}(\pi(U)) = \bigsqcup_{g \in G} gU$$

and then by translation each gU is open, so we can finish the proof by the definition of quotient topology that $\pi(U)$ is open if its preimage is open. □

Then we can conclude

Proposition 3.8. Let G be a topological group and H be a subgroup, then

(1) H is closed if and only if G/H is Hausdorff.

(2) If G is connected, then G/H is connected.

(3) If G/H and H are both connected, then G is connected.

Proof. □

Neighborhood system

As we have mentioned before, topological group is a homogeneous space, so the local topology at one point can be translated to generate the global topology, for some convenience, we always study the local topology at identity of the group.

Formally, for any group G we define the **neighborhood system** (at x) to be the collection of subsets containing x, denoted by $\mathcal{V}_x$:

$$A \in \mathcal{V}_x \iff x \in A \wedge A \subset G$$

Hence we can induce a topology on G by neighborhood system (i.e. determine the open voisinage of identity).

Proposition 3.9. Let G be a group with $\mathcal{V}_e$ as the neighborhood system at identity e, if $\mathcal{V}_e$ satisfies the following conditions:

1. For any $U, V \in \mathcal{V}_e$, there exists $W \in \mathcal{V}_e$ such that
$$W \subset U \cap V.$$
2. If $a \in U \in \mathcal{V}_e$, then there exists $V \in \mathcal{V}_e$ such that
$$Va \subset U.$$
3. For each $U \in \mathcal{V}_e$, there exists $V \in \mathcal{V}_e$ such that
$$V^{-1}V \subset U.$$
4. For each $U \in \mathcal{V}_e$ and each $x \in G$, there exists $V \in \mathcal{V}_e$ such that
$$x^{-1}Vx \subset U.$$

then there exist a unique topology $\mathcal{T}$ such that $\mathcal{V}_e$ is the set of all open voisinage of e, and $(G, \mathcal{T})$ is a topological group.

Proof. The topology $\mathcal{T}$ is uniquely defined by translation:

$$\mathcal{B} = \{gU \mid g \in G, U \in \mathcal{V}_e\}$$

we just need to prove that $\mathcal{B}$ is the topology basis. Notice the condition (1) and (2) ensure that $\mathcal{B}$ generates a topology, the condition (3) is the requirement of continuity of multiplication and inverse; finally, the condition (4) is obligator for non-abelian group to ensure the continuity. □

In partiuclar, we can naturally choose subgroup as the element in the system, the condition can be simplified as following:

Corollary 3.10. Let G be a group with $\mathcal{U}$ as a collection of subgroups of G, if $\mathcal{U}$ satisfies the following conditions:

1. For any $U, V \in \mathcal{U}$, there exists $W \in \mathcal{U}$ such that
$$W \subset U \cap V.$$
2. For each $U \in \mathcal{U}$ and each $x \in G$, there exists $V \in \mathcal{U}$ such that
$$x^{-1}Vx \subset U.$$

then there exist a unique topology $\mathcal{T}$ such that $\mathcal{U}$ is a basis of open voisinage of e, and $(G, \mathcal{T})$ is a topological group.

Here are some classic examples of topological groups constructed by neighborhood system:

Example 3.1. We consider the usual topology on $\mathbb{Q}$, then the completion of $\mathbb{Q}$ is just $\mathbb{R}$, it is another method to construct real number (see in Bourkabi's book). We review that we always write the viosinage of 0 as the form of $(-\varepsilon, \varepsilon)$, which motivates us to consider the system of subgroup:
$$\mathcal{U} = \{\frac{1}{n}\mathbb{Z} \mid n \in \mathbb{N}^*\}$$
pay attention to the choices here! We can not take $n\mathbb{Z}$ to be an open set (consider it in $\mathbb{R}$, it is closed and not open). Then we can verify the topology induced by $\mathcal{U}$ is just the subspace topology induced by $\mathbb{R}$, i.e. it induces a usual absolute value on field $\mathbb{Q}$:
$$|x|_\infty = \begin{cases} x & x \geq 0 \\ -x & x \leq 0 \end{cases}$$

It is natural to ask that can we define other topological stucture on $\mathbb{Q}$ such that we can get other different completion? The answer is yes, and a classic example is the $p-adic$ **number field.**

Example 3.2. We fix a prime number p and then we can define a subgroup
$$\mathbb{Z}_{(p)} = \{\frac{m}{n} \mid m, n \in \mathbb{Z}, p \nmid n\}$$
and we let $\mathcal{U} = \{p^t\mathbb{Z}_{(p)} \mid t \in \mathbb{Z}\}$ to be the collection of subgroups, which generates an unique toplogy (verify!). Notice that we have a unique chain in the system:
$$\ldots p^2\mathbb{Z}_{(p)} \subset p\mathbb{Z}_{(p)} \subset \mathbb{Z}_{(p)} \subset p^{-1}\mathbb{Z}_{(p)} \subset p^{-2}\mathbb{Z}_{(p)} \subset \ldots$$
motivates from the above example, we consider each subgroup gives a method to measure the size of an elemnt is some sense, for example we consider the following number when $p = 3$:
$$1, \quad 4, \quad \frac{1}{2}, \quad \frac{2}{5}$$

they are all in $\mathbb{Z}_{(p)}$, and we consider the distance of them to 0 can be bounded by α (consider $(-\varepsilon, \varepsilon)$ gives the set of all elements with distance to 0 less than ε), and then we consider some other numbers:

$$\frac{1}{3}, \quad \frac{2}{3}, \quad \frac{7}{6}$$

they are all in $\frac{1}{3}\mathbb{Z}_{(p)}$ but not in $\mathbb{Z}_{(3)}$, so we can think that their distance to 0 is bouned by β, and it is natural to give a realtion $\alpha < \beta$, which motivates us to give a new method to consider the metric on $\mathbb{Q}$ by conisder the local factorization of p.

Hence we can define something to denote α and β just now:

$$v_p : \mathbb{Z} - \{0\} \to \mathbb{N}, \quad m \mapsto \max\{k : p^k | m\}$$

for example $v_3(6) = 2$, $v_3(-2) = 0$. Then the method of measuring can be extended to $\mathbb{Q}$ as following:

$$v_p : \mathbb{Z} - \{0\} \to \mathbb{Z}, \quad \frac{m}{n} \mapsto v_p(m) - v_p(n)$$

And we make a convention that $v_p(0) = +\infty$, it is called **p-adic valustion**. for example $v_3(\frac{1}{3}) = -1$, $v_3(\frac{9}{2}) = 2$. Then we can get a measure of number

$$p^k\mathbb{Z}_{(p)} \iff \{x \in \mathbb{Q} \mid v_p(x) \geq p^k\}$$

but a question occurs here is that $v_3(1) = 0$ and $v_3(\frac{1}{3}) = -1$, as what we discussed just now, actually we hope the measure of 1 should be less than the measure of $\frac{1}{3}$ (here $0 > -1$), hence the valuation v_p can not be treated as the absolute value directly, hence we modify it as following:

$$|-|_p : \mathbb{Q} \to \mathbb{R}_+, \quad x \mapsto \frac{1}{e^{v_p(x)}}$$

the convention just now forces $|0|_p = 0$, and again we can get a clear measure of numbers:

$$x \in p^k\mathbb{Z}_{(p)} \iff |x|_p \leq e^{-k}$$

hence $|1|_3 < |\frac{1}{3}|_3$, which admits our original idea.

Remark 3.1. it is just a short introduction of p-adic number from the view of topologyical group, and here are sommething to supplement if to go deeper:

(1) The metric of is induced by the absolute value:

$$d(x, y) = |x - y|_p$$

we can verify that is a **ultrametric (non-archimedean metric)**, i.e. a metric satifying the strong triangle inequality:

$$d(x.z) \leq \max d(x, y), d(y, z), \quad \forall x, y, z \in \mathbb{Q}$$

which induces different analysis structure on $\mathbb{Q}$.

(2) Same situation with $\mathbb{Q}$ equipped by the usual absolute value, $(\mathbb{Q}, |-|_p)$ is not complete as a metric space, we can complete it to get the **p-adic number field** $\mathbb{Q}_p$.

(The completion process is same with what we do for the real number, and we can prove that the completion is unique up to isometry.)

(3) By **Ostrowski's theorem**, any non-trival absolute value on $\mathbb{Q}$ is equivalent to either the usual absolute value or some p-adic absolute value. In detail, if $|-|$ is a non-trival absolute value on $\mathbb{Q}$, then either there is some $c > 0$ such that

$$|x| = |x|_\infty^c, \quad \forall x \in \mathbb{Q}$$

or there is some prime p and some $c > 0$ such that

$$|x| = |x|_p^c, \quad \forall x \in \mathbb{Q}$$

3.2 Homogeneous Spaces

Review that a group action $G \circlearrowright X$ is **transtive** if for any $x, y \in X$, there exists $g \in G$ such that $g \cdot x = y$, i.e. there is only one orbit.

Definition 3.3. A **homogeneous space** is a Hausdorff topological space X with a transtive continous action of a group G, in particular, we call it **G-homogeneous space** to emphasize the acting group G.

3.3 The Pontryagin Duality

We consider the category of locally compact abelian groups:

$$\textbf{LCA} \;\Big|\; \begin{array}{l}\text{objects: locally compact abelian groups } (G,+)\\ \text{morphisms: continuous group homomorphisms}\end{array}$$

without talking about the topology of the group, we can simiarly consider the pure algebraic structure:

$$\textbf{Ab} \;\Big|\; \begin{array}{l}\text{objects: abelian group } (G,+)\\ \text{morphisms: group homomorphisms}\end{array}$$

Clearly it is same as category of $\mathbb{Z}$-modules, hence it is an abelian category with tools of homological algebra, so we can choose a certain objects of abelian groups to construct a duality.

$$\hat{G} := \mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{R}/\mathbb{Z})$$

Clearly, $\mathbb{R}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module, hence the Hom-functor will keep exactness. In particular, it will have a good behavior when group is finite.

Proposition 3.11. If G is a finite abelian group, then $\hat{G}$ is isomorphic to G.

Proof. □

However, the duality fails when G is infinite. For example, if $G = \mathbb{Z}$, then $\hat{\mathbb{Z}} \cong \mathbb{R}/\mathbb{Z}$, but if we take dual again

$$\hat{\mathbb{R}/\mathbb{Z}} = \mathrm{End}_{\mathbb{Z}}(\mathbb{R}/\mathbb{Z}) \cong \prod_p \mathbb{Z}_p$$

clearly it is larger than $\mathbb{Z}$, hence it actually fails to be a duality. What we have done is to give a exact restriction on the categroy of abelian groups to make the duality work: It depends on the topology of the group, so we need to consider the topology of the dual group firstly. Formally, we define dual group as following:

Definition 3.4. Let $G \in \textbf{LCA}$, we define its **dual group** as G^* or $\hat{G}$ by

$$G^* := \mathrm{Hom}_{\textbf{LCA}}(G, \mathbb{S}^1)$$

i.e. the group of continous group homomorphism from G to the circle group ($\mathbb{S}^1 \cong \mathbb{R}/\mathbb{Z}$). Among G^*, the elelment are called **characters** of G, and we usually denote it by

$$\chi : G \to \mathbb{S}^1$$

with operation defined by pointwise multiplication:

$$(\chi_1 + \chi_2)(g) := \chi_1(g) \cdot \chi_2(g)$$

Generally a Hom-functor is not necessary to keep category itself, it will maps to a category of sets, so we should verify that LCA is a good condition to make the functor closed.

Lemma 3.12. Let $G \in \mathbf{LCA}$, then its dual group G^* endowed with the compact-open topology is a locally compact abelian group, in particular

$$V(K,\varepsilon) = \{\chi \in G^* : \chi(K) \subset U_\varepsilon\}$$

for any compact subset $K \subset G$ and $U_\varepsilon = \{e^{it} \mid t \in (-\varepsilon, \varepsilon)\}$, it forms a neighborhood basis of $0 \in G^*$.

Proof. It is easy to verify that G^* is indeed a abelian group under defined opreation, to verify it is a topological group, we need to verify the family $\mathcal{B}$ of all $V(K, varepsilon)$ forms a neighborhood basis of identity of G^*: (1) zero character $g \mapsto 1$ is in any set clearly; (2) $V(K,r) \cap V(L,t) = V(K \cup L, \min(r,t))$, so it is stable under finite intersection; (3) $-V(K,\varepsilon) = V(K,\varepsilon)$ since $U_\varepsilon^{-1} = U_\varepsilon$; (4) $V(K,r)+V(L,t)$ is the subset of $V(K \cup L, r+t)$, so it is stable under opreation. Hence it forms a neighborhood system of identity by (1)-(4).

Finally, we need to verify that G^* is locally compact by Ascoli's theorem... □

Remark 3.2. In particular, we denot evalution map by

$$\mathrm{ev} : G \times G^* \to \mathbb{S}^1, \quad (g,\chi) \mapsto \chi(g)$$

the compact-open topology is **the coarsest topology** such that the evaluation map is continuous (page 43 [1]).

A convention is that G^* always means the dual group with compact-open topology, so we finish the level of objects in the category, and then it is naturally to consider the functoriality, or the level of morphisms.

Lemma 3.13. Let $G, H \in \mathbf{LCA}$, and $f : G \to H$ be a continuous group homomorphism, then it induces a natrual map

$$f^* : H^* \to G^*, \quad \chi \mapsto \chi \circ f$$

which is a continuous (under the compact-open topology) group homomorphism.

Proof. For any two characters $\chi_1, \chi_2 \in H^*$, we have

$$f^*(\chi_1 + \chi_2)(g) = (\chi_1 + \chi_2)(f(g)) = \chi_1(f(g)) \cdot \chi_2(f(g)) = f^*(\chi_1)(g) \cdot f^*(\chi_2)(g)$$

for any $g \in G$, so $f^*(\chi_1 + \chi_2) = f^*(\chi_1) + f^*(\chi_2)$ it is a group homomorphism. To prove the continuity, we take a basic open set $V_G(K,\varepsilon)$, then

$$\begin{aligned}(f^*)^{-1}(V_G(K,\varepsilon)) &= \{\chi \in H^* \mid \chi \circ f \in V_G(K,\varepsilon)\} \\ &= \{\chi \in H^* \mid \chi(f(K)) \subset U_\varepsilon\} \\ &= V_H(f(K),\varepsilon)\end{aligned}$$

here $f(K)$ is compact since f is continous, so the preimage of any voisinage of identity is open, hence f^* is continous by translation. □

It is easy to verify that $(f \circ g)^* = f^* \circ g^*$, hence we have constructed a contravariant functor insider the category **LCA**.

Lemma 3.14. If $f : G \to H$ is a surjective continuous group homomorphism, then $f^* : H^* \to G^*$ is injective; If $f : G \to H$ is both injective and open, then $f^* : H^* \to G^*$ is surjective.

Proof. If f is surjective, we take any $\chi_1, \chi_2 \in H^*$ such that $f^*(\chi_1) = f^*(\chi_2)$, we assume that $\chi_1 \neq \chi_2$, then there exists $h \in H$ such that $\chi_1(h) \neq \chi_2(h)$, since f is surjective, there exists $g \in G$ such that $f(g) = h$, hence $f^*(\chi_1)(g) \neq f^*(\chi_2)(g)$, so it is absurd.

If f is injective, then injective module $\mathbb{S}^1$ allows us to extend a charcter $\chi : G \to \mathbb{S}^1$ to $\tilde{\chi} : H \to \mathbb{S}^1$ such that $\tilde{\chi} \circ f = \chi$. We need to verify the continuity of $\tilde{\chi}$: notice that f is open, so $f(G)$ is the open subgroup of H, hence we can prove that $\tilde{\chi}$ is continous on $f(G)$, then we can conclue that $\tilde{\chi}$ is continous on H by translation (a group homomorphism is continous on some open subgroup, then the morphism is just continous). □

Theorem 3.1 (Pontryagin-Van Kampen,1934)**.**
Let $G \in \mathbf{LCA}$ and G^* be its dual group, then evluation map gives a natural ismoprhism in **LCA** by fixing one variable:

$$\mathrm{ev} : G \to (G^*)^*, \quad g \mapsto \mathrm{ev}_g$$

where $\mathrm{ev}_g : G^* \to \mathbb{S}^1$ is defined by $\mathrm{ev}_g(\chi) = \chi(g)$.

Proof. □

Here is the slogan of the duality:

every LCA-group is the dual group of its dual group.

The conclusion is similar with the finite-dimension vector space, hence it will be a strong tool to study the structure of LCA-groups and the analysis on it. In the sense of category theory, the Pontryagin duality is a contravariant equivalence with inverse itself:

$$(-)^* : \mathbf{LCA} \to (\mathbf{LCA})^{op}$$

Consequences

It is wonderful to see what we can get from the duality, we make a convention that G in this section always means a LCA-group.

Proposition 3.15. In the sense of topological isomophism

$$G_1 \oplus G_2 \cong G_1 \times G_2$$

and

$$(G_1 \times G_2)^* \cong G_1^* \times G_2^*$$

Proof. In the sense of category of abelian groups, we have

$$(G_1 \times G_2)^* \cong G_1^* \oplus G_2^* \cong G_1^* \times G_2^*$$

So we just need to verify the isomophism is homemomorphism under the compact-open topology. □

Proposition 3.16. If G is compact, then G^* is discrete; If G is discrete, then G^* is compact.

Proof. □

Proposition 3.17. If G is compact group, then

- G is metrizable if and only if G^* is countable.

- G is connected if and only if G^* is torsion-free.

4 Field and Galois Theory

To study the structure of the field, consider a natural map: Let K be a field

$$\phi : \mathbb{Z} \to K, \quad 1 \mapsto 1_K$$

It is a well-defined homomorphism, which invites a ideal of $\mathbb{Z}$

$$\ker \phi = \{n \in \mathbb{Z} | n \cdot 1_k = 0_k\}$$

By the structure of $\mathbb{Z}$, so there exists a integer $p \in \mathbb{Z}$ such that $\ker \phi = p\mathbb{Z}$,which gives the definition of the characteristic of the field.

Definition 4.1. For any field K, we define $\mathrm{char}(K)$ be the characteristic of the field: either 0 or the smallest integer $n \in \mathbb{N}$ such that $n \cdot 1_k = 0$, by the natural map equivalently

$$\begin{cases} \mathrm{char}(K) = 0 \iff \mathrm{im}\phi \cong \mathbb{Z} \\ \mathrm{char}(K) = p \iff \mathrm{im}\phi \cong \mathbb{Z}/p\mathbb{Z} \end{cases}$$

The characteristic of a field is either zero or a prime number. Suppose that $\mathrm{char}(K) = p \neq 0$, if $p = ab$ is not a prime, then we will get two zero divisor $a \cdot 1_K$ and $b \cdot 1_K$, but a field can not conatain any zero divisor, so p must be prime. An amazing thing in a field (or ring) with non-zero characteristic p is that we can write a equation

$$(x + y)^p = x^p + y^p$$

it has an interesting name: **freshman's dream**, this is an equality that would be written by someone who has studied very little mathematics or is just beginning to learn it.

Another natural map is **Frobenius endomorphism**, let K be a field with non-zero characteristic p, then we define

$$\sigma : K \to K, \quad x \mapsto x^p$$

It is a well-defined injective field homomorphism, so it is a endomorphism, but it is not necessary surjective.

Example 4.1. Consier $K = \mathbb{F}_p(x)$ a field of rational functions. $\mathrm{char}(K) = p$ since $\mathrm{im}\phi = \mathbb{F}_p$, and it is easy to observe that there exists no $f \in \mathbb{F}_p(x)$ such that $f^p(x) = x$, so the Frobenius map here is not surjective.

A good case is finite field, in that case frobenius endomorphism is furthermore a automorphism, so the frobenius map will be in galois group and it reflects the structure of the finite field.

4.1 Finite extension and splitting Field

For the beginning, notice a classic isomorphism:

$$\mathbb{R}[X]/(X - a) \cong \mathbb{R}$$

For any $a \in \mathbb{R}$, and we review the isomorphism given in complex number field:

$$\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$$

Clearly, $\mathbb{C}$ is a larger field containning $\mathbb{R}$, but we wonder how we can get it from the algebra structure. Here it motivates us to consider the question from the polynoimal structure defined on a field. Firstly we need some lemmas, it is very clear after commutative ring:

Lemma 4.1. Let L be a field containning K as a subfield, then L is a vector space over K.

This lemma allows us to give a rough classification of field extension:

Definition 4.2. If L is a field containing K as a subfield.

- L/K or $K \subset L$ is denoted a **field extension** of K.
- L/K is a **finite extension** if L is a finite-dimensional vector space over K. The **degree** of the finite extension is defined as $[L : K] := \dim_K L$.
- $a \in L$ is **algebraic** over K if there exists a non-zero polynomial $f \in K[X]$ such that $f(a) = 0$, L/K is an **algebraic extension** if every element in L is algebraic over K.
- a is **transcendental** over K if it is not algebraic over K.

Another lemma is the key to construction of field, the reason is that in a PID ring a ideal is maximal if and only if it is generated by an irreducible element.

Lemma 4.2. If K a field and $p \in K[X]$, then p is irreducible if and only if $K[X]/(p)$ is a field.

Hence the a contrsuction of field extension can be given by the quotient of polynoimal ring over a field by a good choice of ideal:

Proposition 4.3. Let K be a field and I be a principl ideal generated by a monic irreducible polynoimal $p \in K[X]$ of degree d, Let $L = K[X]/I$, then
(1) L is a field and K can be embedded in L , so K can be identified as a subfield of L.
(2) p has a root β in L, exactly $\beta = X + I \in L$
(3) If $g \in K[X]$ and β is a root of g in L, then $p|g$.
(4) p is the unique monic irreducible polynoimal in $K[X]$ having β as a root in L.
(5) L can be viewed as a K-vector space with the basis $\{1, \beta, ..., \beta^{d-1}\}$.

Proof. (1) L is a field by above lemma, and we consider an embedding $i(a) = a + I$ for any $a \in K$, clearly it is injective and actually it is $\pi|_K$, where π is the canoncial map from $K[x]$ to $K[x]/I$.

(2) Suppose $p(x) = a_0 + ... + a_d x^d$, then in L, we have

$$\begin{aligned} p(\beta) &= a_0 + a_1\beta + ... + a_d\beta^d \\ &= a_0 + a_1(X + I) + ... + a_d(X + I)^d \\ &= a_0 + a_1(X + I) + ... + a_d(X^d + I) \\ &= p(X) + I = I \end{aligned}$$

Here $p(X) \in I$ and I is the zero element in L.

(3) If p does not divide g, then $gcd(p, g) = 1$ since p is irreducible, so PID ring $K[X]$ imples the existence of r, t in $K[X]$ such that

$$1 = s(x)p(x) + t(x)g(x)$$

put $x = \beta$ in L, then $1 = 0$ leads to a contradiction.

(4) immediately from (3). For (5) we use euclidean divison for polynoimal, any $f \in K[X]$, there exists $q, r \in K[X]$ with $\deg r < d$ such that $f(x) = q(x)p(x) + r(x)$, then $f + I = r + I$ in L, and if $r(x) = b_0 + ... + b_k x^k$, $k < d$, by opreations of ideal

$$r + I = b_0 + b_1\beta + ... + b_k\beta^k$$

so $\{1, \beta, ..., \beta^{d-1}\}$ spans L. They are linearly independent because if we assume they are linearly dependent, that means there exists a polynoimal $h \in K[X]$ of degree $< d$ such that h has β as the root, but by (3) we know that $p|h$, which leads to a contradiction since $d = \deg p \leq \deg h$. □

Review the example in the beginning, the complex number field can also be constructed by adjoining element i to $\mathbb{R}$ such that $i^2 + 1 = 0$, and we alaways write a complex number of the form $a + ib$ with a, b real numbers, which is another construction of field extension, and more generally we have the following proposition:

Proposition 4.4. Let K be a field and $f \in K[X]$ irreducible, adjoin element $c \notin K$ such that c is a root of f, then $K[c]$ is a field containning K as a subfield, and it can be written as $K(c)$.

$$K(c) = \{a_0 + a_1 c + ... + a_k c^k | a_1, ..., a_k \in K, k = \deg f - 1\}$$

Proof. $K[c]$ naturally is a ring with same identity with K, so we just need to find the inverse. For any polynoimal $p \in K[X]$ with degree less than $\deg f$, it is co-prime with f since f is irreducible, so by Bezout's theorem for polynoimal, there exists $r, t \in K[X]$ such that

$$p(x)r(x) + t(x)f(x) = 1$$

hence we take $x = c$ then immediately $p(c)r(c) = 1$, so in $K[c]$ we find the inverse of $p(c)$. and notice that $K[c]$ is a field garantee any rational polynoimal can have the form of polynoimal, so $K[c] = K(c)$ evidently. □

Here we find two method to extension the field, the first method is consider the quotient of polynomial ring, and we can embed K into it; the second is more direct, we just add some element in the field.

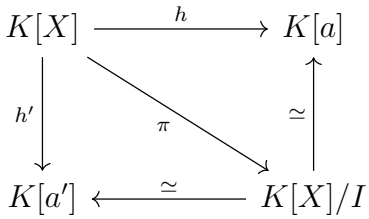
Theorem 4.1 (Structure of field extension)**.**
Let L/K be field extension of K and $a \in L$ is algebraic, then
(1) There exists a unique **monic** irreducible polynoimal in $K[X]$ having a as a root, formally we call it **minimal polynoimal** of a over K, and denote it by Π_a.
(2) If $I = (\Pi_a)$, then there exists an isomorphism

$$\phi : K[X]/I \to K(a)$$

with $X + I \mapsto a$ and $c + I \mapsto c$ for all $c \in K$.
(3) Let L'/K is another field extension and $a' \in L'$ is also a root of Π_a, then there exists an isomrphism $\psi : K(a) \to K(a')$ such that $\psi|_K = \mathrm{id}_K$ and $\psi(a) = a'$.

Proof. It needs to consider the **valuation map**, we define $h : K[X] \to L$ by $p \mapsto p(a)$, then clearly $\ker h$ contains all polynoimals having a as a root, then notice that $K[X]$ is a principal ideal ring, so $\ker h$ must be the form (p) with monic $p \in K[X]$. By first

isomorphism theorem, we know that $K[X]/I \cong K(a)$, then by Lemma 4.2 p must be irreducible, hence we prove (1) and (2), and we can draw commute diagram to finish (3):



where $h'(p) = p(a')$, and π is the canoncial map. □

Remark 4.1. The theorem shows a induction

$$\{\text{algebraic elements in } L/K\} \rightsquigarrow \{\text{monic irreducible polynoimal over } K\}$$

conversely it is not right since the field extension may be not enough large, which refers the **"closure"** in the sense of algebraic element. For statement (3), a simple example is $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(-\sqrt{2})$, and monic irreducible polynoimal $X^2 - 2 \in \mathbb{Q}[X]$.

Example 4.1. We consider the field extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, here the minimal polynoimal of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $X^3 - 2$, we can sovle it in $\mathbb{C}$ with roots:

$$\sqrt[3]{2}, \quad \sqrt[3]{2}\omega, \quad \sqrt[3]{2}\omega^2 \quad \text{with } \omega = e^{2\pi i/3}$$

by above theorem we can connclude $\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}(\sqrt[3]{2}\omega) \cong \mathbb{Q}(\sqrt[3]{2}\omega^2)$, and it also implies a **question**: quotient ring such as $\mathbb{Q}[X]/(X^3 - 2)$ can not construct a field containing all roots of irreducible polynoimal such as $X^3 - 2$.

But we can construct a larger field since $\mathbb{Q}(\sqrt[3]{2})$ has been a field: equivalently, we can adjoin ω to $\mathbb{Q}(\sqrt[3]{2})$, or consider the irreducible polynoimal $X^2 + X + 1$ over $\mathbb{Q}(\sqrt[3]{2})$, then we can get a larger field $\mathbb{Q}(\sqrt[3]{2}, \omega)$ containing all roots of $X^3 - 2$.

For a polynoimal $f \in K[X]$, we say f **splits** over K if there exists $c, a_1, \ldots, a_n \in K$ such that f can be factorized as linear terms:

$$f(x) = c(x - a_1)(x - a_2) \cdots (x - a_n)$$

above examples motivates us to construct a larger field containing all roots of a polynoimal:

Theorem 4.5 (splitting field)**.**
Let K be a field and $f \in K[X]$ with degree $n \geq 1$, then there exists a smallest field extension L/K such that f splits over L, and it is unique up to isomorphism, formally such a field extension is called **splitting field** of f over K.

Proof. □

Theorem 4.6 (Kronecker)**.** If K is a field and $f \in K[X]$, then there exists a field L containing K as a subfield and with $f(X)$ a product of linear polynomial in $K[X]$.

By Kronecker's theorme, we deduce a larger field where f can be decomposed completlely, so it is meaningful to define the field

Definition 4.3. Let L/K be a field and $f \in K[X]$.

- f splits over L/K if there exists $c, a_1, ...a_n \in K$ such that

$$f(x) = c(x - a_1) \cdots (x - a_n)$$

with $n = \deg f$.

- L/K is called a splitting field of f over K if it is the smallest field such that f splits.

The existence of the splitting field is ensured by above theorem, since for any $f \in K[X]$, we can obtain a field extension L/K such that f splits, and then $K(a_1, ..., a_n) \subset L$ as a splittin field.