Reading Notes for
Representation Theory: A First Course

Zhi Wang

September 20, 2021

Contents

0 Notes and Definitions

0.1 Notes

0.2 Prerequisites for Chapter 1

0.2.1 Matrix

Definition (matrix)**.** For any positive integers m, n, k, a $m \times n$ **matrix** whose entries are from a ring R, is an element in $R^{m\times n}$, on which the matrix addition is defined as element-wise ring addition operation, and matrix multiplication $\cdot_L \colon R^{m\times n} \times R^{n\times k} \to R^{m\times k}$ and $\cdot_R \colon R^{k\times m} \times R^{m\times n} \to R^{k\times n}$ are defined as

$$(AB)_{ik} = \sum_{j=1}^{n} A_{ij} B_{jk},$$

where, for example, $(AB)_{ik}$, A_{ij}, and B_{jk} are the (ik)-th, (ij)-th, and (jk)-th element of matrices $\mathbf{AB}$, $\mathbf{A}$, and $\mathbf{B}$, respectively, and $\mathbf{A} \in R^{m\times n}, \mathbf{B} \in R^{n\times k}$.

The summation is valid as the addition operation in the ring is commutative and associative.

Definition (square matrix)**.** An $n \times n$ matrix is named as a **square matrix** of order n.

Definition (main diagonal)**.** The **main diagonal** of a matrix $\mathbf{A}$ is the list of entries A_{ij} (meaning the (ij)-the element in the matrix $\mathbf{A}$) where $i = j$.

Definition (identity matrix)**.** The **identity matrix** $\mathbf{I}_n$ over a ring R of size n is the $n \times n$ matrix in which all the elements on the main diagonal are equal to the multiplicative identity in R and all other elements are equal to the additive identity in R.

Proposition 0.1. *The set of square matrices of a specific order with entries in a ring forms a ring under matrix addition and matrix multiplication.*

Proof. It is an Abelian group under matrix addition as it is element-wise ring addition which itself forms an Abelian group.

Since matrix multiplication of two square matrices of the same size n is still a square matrix of order n, the set is a magma under matrix multiplication.

Let $\mathbf{A}$ be any square matrices over ring R of order n, we have

$$\begin{aligned}(AI)_{ik} &= \sum_{j=1}^{n} A_{ij} I_{jk} = A_{ik}, \\ (IA)_{ik} &= \sum_{j=1}^{n} I_{ij} A_{jk} = A_{ik},\end{aligned} \tag{0.1}$$

because any element in R multiplied by the additive identity is the additive identity, and any element in R added to the additive identity or multiplied by the multiplicative identity is itself.

The equation (0.1) shows that the identity matrix $\mathbf{I}_n$ of size n is the identity under matrix multiplication of square matrices of order n. The set now becomes a unital magma under matrix multiplication.

Now consider any three matrices $\mathbf{A}, \mathbf{B}, \mathbf{C} \in R^{n \times n}$. We have

$$\begin{aligned}((AB)C)_{ps} &= \sum_{r=1}^{n} \left(\sum_{q=1}^{n} A_{pq} B_{qr} \right) C_{rs}, \\ (A(BC))_{ps} &= \sum_{q=1}^{n} A_{pq} \left(\sum_{r=1}^{n} B_{qr} C_{rs} \right).\end{aligned} \tag{0.2}$$

Since multiplication is distributive with respect to addition in the ring R, and addition is commutative and associative, both in (0.2) are equal to

$$\sum_{q=1}^{n} \sum_{r=1}^{n} A_{pq} B_{qr} C_{rs}.$$

Therefore, matrix multiplication is associative. The set is a monoid under matrix multiplication.

We have left to prove matrix multiplication is distributive with respect to its addition. Given three matrices $\mathbf{A}, \mathbf{B}, \mathbf{C} \in R^{n \times n}$,

$$\begin{aligned}(A(B+C))_{ij} &= \sum_{k=1}^{n} A_{ik} \left(B_{kj} + C_{kj} \right) = \sum_{k=1}^{n} A_{ik} B_{kj} + \sum_{k=1}^{n} A_{ik} C_{kj}, \\ ((B+C)A)_{ij} &= \sum_{k=1}^{n} \left(B_{ik} + C_{ik} \right) A_{kj} = \sum_{k=1}^{n} B_{ik} A_{kj} + \sum_{k=1}^{n} C_{ik} A_{kj},\end{aligned} \tag{0.3}$$

which is also supported by multiplication being distributive with respect to addition in the ring R, and addition being commutative and associative.

In conclusion, the set of all matrices in $R^{n \times n}$ forms a ring.

□

Definition (matrix ring)**.** A **matrix ring** $\mathrm{M}_n(R)$ is the set of $n \times n$ matrices with entries in the ring R.

Definition (matrix algebra)**.** When R is a commutative ring, the matrix ring $\mathrm{M}_n(R)$ is a unital associative algebra over R (section 3.1.3.1), and may be called a **matrix algebra**.

Definition (invertible matrix)**.** An $n \times n$ matrix $\mathbf{A}$ over ring R is **invertible** if there exists an $n \times n$ matrix $\mathbf{B}$ over the same ring such that

$$\mathbf{AB} = \mathbf{BA} = \mathbf{I}_n,$$

where $\mathbf{I}_n$ denotes the $n \times n$ identity matrix.

Proposition 0.2. *The set of all invertible matrices of a specific size forms a group under matrix multiplication.*

Proof. Given two invertible matrices $\mathbf{A}, \mathbf{B} \in \mathrm{M}_n(R)$, since $\mathbf{I}_n$ is the multiplicative identity in $\mathrm{M}_n(R)$, and matrix multiplication is associative, we have

$$(\mathbf{AB})(\mathbf{DC}) = (\mathbf{DC})(\mathbf{AB}) = \mathbf{I}_n, \tag{0.4}$$

where $\mathbf{C}$ is any matrix such that $\mathbf{AC} = \mathbf{CA} = \mathbf{I}_n$ and $\mathbf{D}$ is any matrix such that $\mathbf{BD} = \mathbf{DB} = \mathbf{I}_n$. Therefore $\mathbf{AB}$ is invertible too.

Since $\mathbf{I}_n$ is the multiplicative identity, we have

$$\mathbf{I}_n\mathbf{I}_n = \mathbf{I}_n,$$

proving its invertible property.

Associativity inherits from $\mathrm{M}_n(R)$.

For any invertible matrix $\mathbf{A} \in \mathrm{M}_n(R)$, if $\mathbf{AB} = \mathbf{BA} = \mathbf{I}_n$ where $\mathbf{B} \in \mathrm{M}_n(R)$, then $\mathbf{B}$ is invertible as well (from the definition). □

0.2.2 Homomorphism, Isomorphism, and Automorphism

Definition (homomorphism)**.** A **homomorphism** is a *structure-preserving* map between two algebraic structures *of the same type*.

A homomorphism from A to B, where A and B are algebraic structures of the same type, is a map $f\colon A \to B$ that preserves every operation μ of arity k, defined on both A and B, such that

$$f\left(\mu_A\left(a_1, \ldots, a_k\right)\right) = \mu_B\left(f\left(a_1\right), \ldots, f\left(a_k\right)\right), \tag{0.5}$$

for all elements $a_1, ..., a_k$ in A. This includes 0-ary operations, i.e., the constants (e.g., the identity element) as well.

Definition (isomorphism)**.** An **isomorphism** is defined as a *bijective homomorphism*.

Definition (endomorphism)**.** An **endomorphism** is a homomorphism from a mathematical object to itself.

Remark. The set of all endomorphisms of X forms a monoid, the full transformation monoid, and denoted $\mathrm{End}(X)$.

Definition (automorphism)**.** An **automorphism** is an *isomorphic endomorphism*.

Proposition 0.3. *The set of all automorphism of an algebraic structure forms a group (if it is a set).*

Proof. There is a trivial automorphism which maps every object in the structure to itself, which is the identity element of the group.

The transitivity of mapping guarantees that the multiplication of two automorphisms is automorphism and that it is associative.

An automorphism is bijective, from which the inverse operation can be defined. □

0.2.3 General Linear Group

Definition (general linear group)**.** The **general linear group** of degree n over any ring R, is the set of $n \times n$ invertible matrices with entries from R. It is typically denoted as $\mathrm{GL}_n(R)$ or $\mathrm{GL}(n, R)$.

Definition (general linear group of a module)**.** The **general linear group of a module** M is *its automorphism group*, denoted as $\mathrm{GL}(M)$.

Proposition 0.4. *Given a ring R, the general linear group $\mathrm{GL}(n, R)$ is isomorphic to the general linear group of a free R-module of rank n.*

Proof. Every element in a free R-module M of rank n can be represented uniquely by a basis set E. Therefore, any automorphism $T \in \mathrm{GL}(M)$ can be represented uniquely (given the basis set E) as

$$T(e_i) = \sum_{j=1}^{n} t_i^{\ j} e_j, \tag{0.6}$$

where $(e_1, e_2, \ldots, e_n)$ is one permutation of the basis set E, and $t_i^{\ j} \in R$ are the coefficients uniquely determined by T and E. There is a unique matrix $\mathbf{T}$ whose (ij)-th element is $t_i^{\ j}$. In this way, we have defined a mapping

$f\colon \mathrm{GL}(M) \to \mathrm{M}_n(R)$ such that $f(T) \coloneqq \mathbf{T}$, based on a specific permutation of E. Given the mapping f, the equation (0.6) can be rewritten as

$$T(e_i) = \sum_{j=1}^{n} (f(T))_i^{\ j}\, e_j. \tag{0.7}$$

As T is a bijection, for each e_i, there must be unique element e_i^{-1} uniquely represented as

$$T^{-1}(e_i) = e_i^{-1} = \sum_{j=1}^{n} s_i^{\ j} e_j, \tag{0.8}$$

such that

$$T(e_i^{-1}) = e_i. \tag{0.9}$$

From the definition of f (see (0.6)), we see that $f(T^{-1}) = \mathbf{S}$ where the (ij)-th element of $\mathbf{S}$ is $s_i^{\ j}$.

Since T is a homomorphism from V to V, plug (0.6) and (0.8) into (0.9)

$$\begin{aligned} e_i &= T\left(\sum_{j=1}^{n} s_i^{\ j} e_j\right) \\ &= \sum_{j=1}^{n} s_i^{\ j} T(e_j) \\ &= \sum_{j=1}^{n} s_i^{\ j} \left(\sum_{k=1}^{n} t_j^{\ k} e_k\right). \end{aligned} \tag{0.10}$$

Given the distributivity of scalar multiplication with respect to addition operation in the module as well as the ring addition, the compatibility of scalar multiplication with ring multiplication, and the commutativity and associativity of addition operation in the module, we have

$$e_i = \sum_{k=1}^{n} \left(\sum_{j=1}^{n} s_i^{\ j} t_j^{\ k}\right) e_k. \tag{0.11}$$

Since e_i and e_k are elements in the basis set, the coefficient $\sum_{j=1}^{n} s_i^{\ j} t_j^{\ k}$ must be equal to the (ik)-th element in a identity matrix $\mathbf{I}_n$, which can be expressed by

$$f(T^{-1}) f(T) = \mathbf{ST} = \mathbf{I}_n. \tag{0.12}$$

Similarly,

$$f(T) f(T^{-1}) = f((T^{-1})^{-1}) f(T^{-1}) = \mathbf{I}_n.$$

Therefore $f(T)$ is invertible, i.e., f is a mapping from $\mathrm{GL}(M)$ to $\mathrm{GL}(n, R)$.

Given an invertible matrix $\mathbf{A} \in \mathrm{GL}(n, R)$ whose (ij)-th element is ${a_i}^j$, we construct a mapping $A\colon M \to M$ such that

$$A(x) \coloneqq \sum_{j=1}^{n} \left(\sum_{i=1}^{n} x^i {a_i}^j \right) e_j, \tag{0.13}$$

for each $x \in M$ uniquely represented as

$$x = \sum_{i=1}^{n} x^i e_i. \tag{0.14}$$

We now prove A is a homomorphism:

$$\begin{aligned} A(0_M) &= \sum_{j=1}^{n} \left(\sum_{i=1}^{n} 0_R {a_i}^j \right) e_j \\ &= \sum_{j=1}^{n} \left(\sum_{i=1}^{n} 0_R \right) e_j \\ &= \sum_{j=1}^{n} 0_R e_j \\ &= 0_M, \end{aligned} \tag{0.15}$$

where 0_M and 0_R are the additive identities in module M and ring R, respectively. Because

$$x + y = \sum_{i=1}^{n} x^i e_i + \sum_{i=1}^{n} y^i e_i = \sum_{i=1}^{n} \left(x^i + y^i \right) e_i,$$

we have

$$\begin{aligned} A(x) + A(y) &= \sum_{j=1}^{n} \left(\sum_{i=1}^{n} x^i {a_i}^j \right) e_j + \sum_{j=1}^{n} \left(\sum_{i=1}^{n} y^i {a_i}^j \right) e_j \\ &= \sum_{j=1}^{n} \left(\sum_{i=1}^{n} x^i {a_i}^j + \sum_{i=1}^{n} y^i {a_i}^j \right) e_j \\ &= \sum_{j=1}^{n} \left(\sum_{i=1}^{n} \left(x^i + y^i \right) {a_i}^j \right) e_j \\ &= A(x + y), \end{aligned} \tag{0.16}$$

where an arbitrary $y \in M$ can be represented as $y = \sum_{i=1}^{n} y^i e_i$. Because

$$rx = r \sum_{i=1}^{n} x^i e_i = \sum_{i=1}^{n} r \left(x^i e_i \right) = \sum_{i=1}^{n} \left(r x^i \right) e_i,$$

we have

$$\begin{aligned} rA(x) &= r \sum_{j=1}^{n} \left(\sum_{i=1}^{n} x^i {a_i}^j \right) e_j \\ &= \sum_{j=1}^{n} \left(\sum_{i=1}^{n} \left(r x^i \right) {a_i}^j \right) e_j \\ &= A(rx), \end{aligned} \tag{0.17}$$

where r is an arbitrary number in ring R. Up till now, we have shown A is a homomorphism.

Denote the (ij)-th element of $\mathbf{B} = \mathbf{A}^{-1}$ as ${b_i}^j$, a homomorphism $B \colon M \to M$ can be constructed similarly:

$$B(x) \coloneqq \sum_{j=1}^{n} \left(\sum_{i=1}^{n} x^i {b_i}^j \right) e_j. \tag{0.18}$$

Note that $\mathbf{AB} = \mathbf{I}_n$, therefore by plugging (0.13) into (0.18), we have

$$\begin{aligned} B(A(x)) &= \sum_{j=1}^{n} \left(\sum_{i=1}^{n} \left(\sum_{k=1}^{n} x^k {a_k}^i \right) {b_i}^j \right) e_j \\ &= \sum_{j=1}^{n} \left(\sum_{k=1}^{n} x^k \left(\sum_{i=1}^{n} {a_k}^i {b_i}^j \right) \right) e_j \\ &= \sum_{j=1}^{n} \left(\sum_{k=1}^{n} x^k {\delta_k}^j \right) e_j \\ &= \sum_{j=1}^{n} x^j e_j \\ &= x, \end{aligned} \tag{0.19}$$

where δ is the Kronecker delta notation. ${\delta_k}^j$ is equal to (kj)-th element of $\mathbf{I}_n$.

Since $\mathbf{B}^{-1} = \mathbf{A}$, we can derive that

$$A(B(x)) = x.$$

Therefore, both A and B are automorphic mappings. Hence, we have constructed a mapping $g\colon \mathrm{GL}(n,R) \to \mathrm{GL}(M)$ such that $g(\mathbf{A}) \coloneqq A$, and we have shown that

$$g(\mathbf{A}^{-1}) = g(\mathbf{B}) = B = A^{-1} = (g(\mathbf{A}))^{-1}.$$

The definition (0.13) can now be rewritten as

$$g(\mathbf{A})(x) = \sum_{j=1}^{n} \left(\sum_{i=1}^{n} x^i {a_i}^j \right) e_j. \tag{0.20}$$

Next, we want to demonstrate that g is the inverse of f.

For any $T \in \mathrm{GL}(M)$, because T is a homomorphism, we can apply and (0.14), (0.7), and (0.20) to get

$$\begin{aligned} T(x) &= \sum_{i=1}^{n} x^i T(e_i) \\ &= \sum_{i=1}^{n} x^i \sum_{j=1}^{n} (f(T))_i{}^j \, e_j \\ &= \sum_{j=1}^{n} \left(\sum_{i=1}^{n} x^i (f(T))_i{}^j \right) e_j \\ &= g(f(T))(x). \end{aligned} \tag{0.21}$$

Consider any $\mathbf{A} \in \mathrm{GL}(n,R)$. Set x to e_i in (0.20) and compare it with (0.7) by setting $T = g(\mathbf{A})$:

$$\sum_{j=1}^{n} \left(\sum_{k=1}^{n} (e_i)^k {a_k}^j \right) e_j = g(\mathbf{A})(e_i) = \sum_{j=1}^{n} (f(g(\mathbf{A})))_i{}^j \, e_j. \tag{0.22}$$

Due to the unique representation, the coefficient must be consistent

$$(f(g(\mathbf{A})))_i{}^j = \sum_{k=1}^{n} (e_i)^k {a_k}^j = {a_i}^j. \tag{0.23}$$

Therefore, f and g are bijections and $g = f^{-1}$.

Consider the g transform of an identity matrix by plugging $\mathbf{I}_n$ into (0.20):

$$g(\mathbf{I}_n)(x) = \sum_{j=1}^{n} \left(\sum_{i=1}^{n} x^i {\delta_i}^j \right) e_j = \sum_{j=1}^{n} x^j e_j = x. \tag{0.24}$$

Therefore, g preserves the identity element.

Finally, consider matrix $\mathbf{A}, \mathbf{B} \in \mathrm{GL}(n, R)$, and apply (0.20) repeatedly

$$\begin{aligned} g(\mathbf{B})(g(\mathbf{A})(x)) &= \sum_{j=1}^{n} \left(\sum_{i=1}^{n} \left(g(\mathbf{A})(x) \right)^i b_i^{\ j} \right) e_j \\ &= \sum_{j=1}^{n} \left(\sum_{i=1}^{n} \left(\sum_{k=1}^{n} x^k a_k^{\ i} \right) b_i^{\ j} \right) e_j \\ &= \sum_{j=1}^{n} \left(\sum_{k=1}^{n} x^k \left(\sum_{i=1}^{n} a_k^{\ i} b_i^{\ j} \right) \right) e_j \\ &= g(\mathbf{AB})(x). \end{aligned} \tag{0.25}$$

Therefore, g preserves multiplication. (If $(g(\mathbf{A})g(\mathbf{B}))(x) \coloneqq g(\mathbf{A})(g(\mathbf{B})(x))$, then transpose every matrix mentioned above.)

Does the ring need to be commutative? □

Definition (general linear group of a vector space)**.** The **general linear group of a vector space** V is *its automorphism group*, denoted as $\mathrm{GL}(V)$.

Corollary 0.5. *The general linear group* $\mathrm{GL}(n, F)$ *is isomorphic to the general linear group of a vector space over field* F *of rank* n*.*

Proof. A field is also a commutative ring. A vector space is also a module. A vector space over field F of rank n has a basis set of cardinality n. Also the meaning of automorphism for a vector space is the same as that for a module because they share the same set of axioms. □

0.2.4 Commutative Diagram

Definition (category)**.** A **category** C is a collection of

- a class $\mathrm{ob}(C)$ of **objects**,
- a class $\hom(C)$ of **morphisms**, or arrows, or maps between the objects,
- a **domain**, or source object class function $\mathrm{dom}\colon \hom(C) \to \mathrm{ob}(C)$,
- a **codomain**, or target object class function $\mathrm{cod}\colon \hom(C) \to \mathrm{ob}(C)$,
- for every three objects a, b and c, a **binary operation** $\circ\colon \hom(a, b) \times \hom(b, c) \to \hom(a, c)$, called **composition of morphisms**, such that the following axioms hold:

– (associativity)

$$\begin{aligned}&\forall f \in \hom(a,b) \forall g \in \hom(b,c) \forall h \in \hom(c,d)\\ &[h \circ (g \circ f) = (h \circ g) \circ f],\end{aligned} \tag{0.26}$$

– (identity)

$$\begin{aligned}&\forall x \in \mathrm{ob}(C) \exists 1_x \in \hom(x,x)\\ &[\forall a \in \mathrm{ob}(C) \forall f \in \hom(a,x)(1_x \circ f = f)\\ &\wedge \forall b \in \mathrm{ob}(C) \forall g \in \hom(x,b)(g \circ 1_x = g)].\end{aligned} \tag{0.27}$$

1_x is sometimes written as id_x as well.

Here $\hom(a,b)$ (or $\hom_C(a,b)$) denotes the subclass of morphisms f in $\hom(C)$ such that $\mathrm{dom}(f) = a$ and $\mathrm{cod}(f) = b$. Such morphisms are often written as $f\colon a \to b$.

Definition (functor)**.** A (covariant) **functor** associates two categories while preserving identity morphisms and composition of morphisms. Let C and D be categories. A functor F from C to D is a mapping containing

- $F\colon \mathrm{ob}(C) \to \mathrm{ob}(D)$,
- $F_{X,Y}\colon \hom_C(X,Y) \to \hom_D(F(X),F(Y))$, $\forall X \in \mathrm{ob}(C) \forall Y \in \mathrm{ob}(C)$, such that

  –

  $$\forall X \in \mathrm{ob}(C)[F_{X,X}(1_X) = 1_{F(X)}], \tag{0.28}$$

  –

  $$\begin{aligned}&\forall X \in \mathrm{ob}(C) \forall Y \in \mathrm{ob}(C) \forall Z \in \mathrm{ob}(C)\\ &[\forall f \in \hom_C(X,Y) \forall g \in \hom_C(Y,Z)\\ &(F_{X,Z}(g \circ_C f) = F_{Y,Z}(g) \circ_D F_{X,Y}(f))].\end{aligned} \tag{0.29}$$

Definition (diagram)**.** A **diagram** D of type J in a category C is a (covariant) *functor* $D\colon J \to C$, where J is called the index category or the scheme of the diagram D. We can think it as a "subset" of a category? We draw the category J as a backbone and fill with elements in C.

Definition (commutative diagram)**.** A **commutative diagram** is a diagram such that all directed paths in the diagram with the same start and endpoints lead to the same result.

1 Representations of Finite Groups

1.1 Definitions

1.1.1 Basic Linear Algebra

Definition (linear map)**.** A **linear map** is a *homomorphism* between vector spaces.

Proposition 1.1. *Given vector spaces V, W over field F, the space of all linear maps from $V \to W$, denoted as* $\mathrm{Hom}(V, W)$*, forms a vector space over F.*

Proof. $\forall f, g \in \mathrm{Hom}(V, W), a, b, c \in F, v, v' \in V$,

$$\begin{aligned} (f+g)(v) &\coloneqq f(v) + g(v), \\ (af)(v) &\coloneqq af(v). \end{aligned} \tag{1.1}$$

Following the definition,

$$\begin{aligned} (f+g)(av+bv') &= af(v) + bf(v') + ag(v) + bg(v') \\ &= a(f+g)(v) + b(f+g)(v'), \\ (cf)(av+bv') &= caf(v) + cbf(v')) \\ &= a(cf)(v) + b(cf)(v). \end{aligned} \tag{1.2}$$

Thus, $f+g, cf \in \mathrm{Hom}(V, W)$. This requires commutative scalar multiplication. □

Definition (kernel)**.** The **kernel** of a linear map $\varphi\colon V \to W$ is a subspace in V $\ker \varphi = \{\, v \in V \mid \varphi(v) = 0_W \,\}$.

Definition (image)**.** The **image** of a linear map $\varphi\colon V \to W$ is a subspace in W $\operatorname{im} \varphi = \{\, w \in W \mid \exists v \in V[\varphi(v) = w] \,\}$.

Definition (cokernel)**.** The **cokernel** of a linear map $\varphi\colon V \to W$ is a quotient vector space $W/\operatorname{im} \varphi$.

Definition (dual space)**.** Given any vector space V over a field F, the (algebraic) **dual space** V^* is defined as the set of all linear maps $\varphi\colon V \to F$ equipped with

$$\begin{aligned} (\varphi + \psi)(x) &= \varphi(x) + \psi(x), \\ (a\varphi)(x) &= a\left(\varphi(x)\right), \end{aligned}$$

$\forall \varphi, \psi \in V^*, x \in V, a \in F$.

Corollary 1.2. *The dual space forms a vector space.*

Definition (transpose)**.** The **transpose** or dual $f^*\colon W^* \to V^*$ of a linear map $f\colon V \to W$ is defined by

$$f^*(\varphi) = \varphi \circ f,\ \forall \varphi \in W^*.$$

$f^*(\varphi) \in V^*$ is called the **pullback** of φ along f. In this book, it is denoted as ${}^t f$.

Proposition 1.3. *The transpose of a linear map is also a linear map.*

Proof.

$$\begin{aligned} f^*(a\varphi + b\psi)(v) &= (a\varphi + b\psi)(f(v)) \\ &= a\varphi(f(v)) + b\psi(f(v)) \\ &= af^*(\varphi)(v) + bf^*(\psi)(v) \\ &= (af^*(\varphi) + bf^*(\psi))(v). \end{aligned} \tag{1.3}$$

□

1.1.2 Main Text

Definition (representation)**.** A **representation** of a finite group G on a finite-dimensional vector space V is a homomorphism $\rho\colon G \to \mathrm{GL}(V)$. If we call V a representation of G, it is actually saying that V equipped with ρ, the latter of which gives V the structure of a G-module, a representation.

Definition (G-module linear map)**.** A **map** φ between two representations V with ρ and W with σ of the same group G is a linear map $\varphi\colon V \to W$ such that

$$\forall g \in G[\varphi \circ \rho(g) = \sigma(g) \circ \varphi].$$

It can be called a G-linear map.

Theorem 1.4. *Kernel, image, and cokernel of a linear map are also G-modules.*

This is equivalent to that

$$\begin{aligned} &\forall g \in G[\rho(g)(\ker \varphi) = \ker \varphi], \\ &\forall g \in G[\sigma(g)(\operatorname{im} \varphi) = \operatorname{im} \varphi], \\ &\forall g \in G[\sigma(g)(\operatorname{coker} \varphi) = \operatorname{coker} \varphi]. \end{aligned} \tag{1.4}$$

Definition (subrepresentation)**.** A **subrepresentation** of a representation ρ of group G on vector space V is the same representation on a vector subspace W of V such that

$$\forall g \in G \forall w \in W[\rho(g)(w) \in W].$$

Corollary 1.5. *Kernel, image, cokernel of a G-linear map are all subrepresentations.*

Exercise 1.1. The dual representation ρ^* of representation ρ of a group G on a vector space V over field F is given by

$$\rho^*(g) = {}^t\rho(g^{-1}), \forall g \in G.$$

Proof.

$$\begin{aligned}[\rho^*(g)(v^*)][\rho(g)(v)] &= [v^* \circ \rho(g^{-1})](\rho(g))(v) \\ &= v^*\{[\rho(g^{-1}) \circ \rho(g)](v)\}.\end{aligned} \tag{1.5}$$

Since g is a homomorphism, this becomes

$$\begin{aligned}[\rho^*(g)(v^*)][\rho(g)(v)] &= v^*\{[(\rho(g))^{-1} \circ \rho(g)](v)\} \\ &= v^*(v).\end{aligned} \tag{1.6}$$

Therefore the pairing is preserved. □

Lemma 1.6. *A vector space V over field F is isomorphic to* $\mathrm{Hom}(F, V)$.

Proof. Let $f\colon V \to \mathrm{Hom}(F, V)$ such that $f(v)(a) \coloneqq av$, $\forall a \in F, v \in V$. Easy to show that $f(v)$ and f are linear maps.

Let $g\colon \mathrm{Hom}(F, V) \to V$ such that $g(\varphi) \coloneqq \varphi(1_F), \forall \varphi \in \mathrm{Hom}(F, V)$. Easy to prove g is a linear map too.

$$g(f(v)) = f(v)(1_F) = 1_F v = v.$$

$$f(g(\varphi))(a) = a\varphi(1_F) = \varphi(a1_F) = \varphi(a).$$

Therefore, f and g are isomorphisms. □

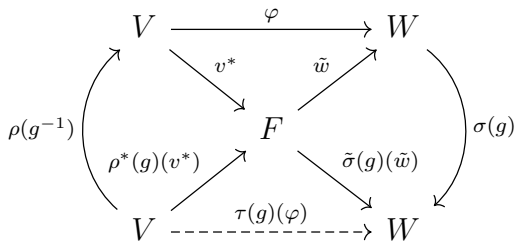
Proposition 1.7. *Given three finite-dimensional vector spaces U, V, W over the same field, the tensor product* $\mathrm{Hom}(U, V) \otimes \mathrm{Hom}(V, W)$ *is isomorphic to* $\mathrm{Hom}(U, W)$.

Proof. TODO □

Proposition 1.8. *Representation on* $\mathrm{Hom}(V, W)$ *can be viewed as the representation on* $V^* \otimes W$*.*

Proof. Any element in $V^* \otimes W$ can be represented as finite sum of pure tensors, each of which can be represented as $v^* \otimes w$ and is isomorphic to $\varphi = \tilde{w} \circ v^*$, where $v^* \in \mathrm{Hom}(V, F)$ and $\tilde{w} \in \mathrm{Hom}(F, W)$, the latter of which is isomorphic to $w \in W$.

Given any representation ρ on V and σ on W, the representations ρ^* on V^* and $\tilde{\sigma}$ on $\mathrm{Hom}(F, W)$ can be generated. Thus, the following commutative diagram can be constructed for representation τ on $\mathrm{Hom}(V, W)$ as the composite of two representations:



□

Lemma 1.9. *Composition of finite linear mappings is linear mapping.*

Proof. Given vector spaces U, V, W over field F and linear mappings $f \in \mathrm{Hom}(U, V), g \in \mathrm{Hom}(V, W)$, for any $u, u' \in U$, $a, b \in F$,

$$\begin{aligned} g \circ f(au + bu') &= g(af(u) + bf(u')) \\ &= ag \circ f(u) + bg \circ f(u'). \end{aligned} \tag{1.7}$$

□

Proposition 1.10. *Given a group* G *and a field* F*, representations* ρ *on* V *and* σ *on* W *generates a representation on* $\mathrm{Hom}(V, W)$*.*

Proof. Define $\tau \colon G \to \mathrm{GL}(\mathrm{Hom}(V, W))$ as

$$\tau(g)(\varphi) \coloneqq \sigma(g) \circ \varphi \circ \rho(g^{-1}), \forall \varphi \in \mathrm{Hom}(V, W).$$

$\because \sigma(g) \in \mathrm{Hom}(W, W), \varphi \in \mathrm{Hom}(V, W), \rho(g^{-1}) \in \mathrm{Hom}(V, V)$,
$\therefore \tau(g)(\varphi) \in \mathrm{Hom}(V, W)$.

$$\begin{aligned} \tau(g)(a\varphi + b\psi) &= \sigma(g) \circ (a\varphi + b\psi) \circ \rho(g^{-1}) \\ &= a[\sigma(g) \circ \varphi \circ \rho(g^{-1})] + b[\sigma(g) \circ \psi \circ \rho(g^{-1})] \\ &= a[\tau(g)(\varphi)] + b[\tau(g)(\psi)]. \end{aligned} \tag{1.8}$$

Therefore $\tau(g) \in \mathrm{GL}(\mathrm{Hom}(V,W))$. The operation in $\mathrm{GL}(\mathrm{Hom}(V,W))$ is also defined above

$$\tau(g)(a\varphi + b\psi) = (a\tau(g) + b\tau(g))(\psi).$$

Since the inverse of the identity id_G in the group is still itself, and ρ, σ preserves identity.

$$\begin{aligned} \tau(\mathrm{id}_G)(\varphi) &= \sigma(\mathrm{id}_G) \circ \varphi \circ \rho(\mathrm{id}_G) \\ &= \mathrm{id}_W \circ \varphi \circ \mathrm{id}_V \\ &= \varphi. \end{aligned} \tag{1.9}$$

Therefore τ preserves identity.

Since the inverse of inverse is it self, and ρ, σ preserves inverse.

$$\begin{aligned} \tau(g) \circ \tau(g^{-1})(\varphi) &= \sigma(g) \circ \sigma(g^{-1}) \circ \varphi \circ \rho(g) \circ \rho(g^{-1}) \\ &= \sigma(g) \circ \sigma^{-1}(g) \circ \varphi \circ \rho^{-1}(g^{-1}) \circ \rho(g^{-1}) \\ &= \mathrm{id}_W \circ \varphi \circ \mathrm{id}_V \\ &= \varphi. \end{aligned} \tag{1.10}$$

Similarly

$$\tau(g^{-1}) \circ \tau(g)(\varphi) = \varphi.$$

If $\rho(g) \circ \rho(h) = \rho(gh)$, $\sigma(g) \circ \sigma(h) = \sigma(gh)$, then

$$\begin{aligned} \tau(g) \circ \tau(h)(\varphi) &= \sigma(g) \circ \sigma(h) \circ \varphi \circ \rho(h^{-1}) \circ \rho(g^{-1}) \\ &= \sigma(gh) \circ \varphi \circ \rho((gh)^{-1}) \\ &= \tau(gh)(\varphi). \end{aligned} \tag{1.11}$$

□

Exercise 1.2. The space of G-linear maps forms the maximum trivial sub-representation on $\mathrm{Hom}(V,W)$.

Proof. Compare the two diagrams. □

Exercise* 1.3. $\bigwedge^k V$

$$\bigwedge^k$$

TODO

Definition (permutation representation)**.** Let V be the vector space with a finite basis $\{ e_x \mid x \in X \}$, and let G act on V by

$$g \cdot e_x = e_{gx}.$$

This is called a **permutation representation**.

Remark. If a vector is represented by the basis as

$$x = (x^1, x^2, \ldots, x^n),$$

then $g \cdot x$ will be

$$g \cdot x = (x^{g^{-1}(1)}, x^{g^{-1}(2)}, \ldots, x^{g^{-1}(n)}).$$

Definition (regular representation)**.** The **regular representation** of a group G, denoted R_G or R, is the permutation representation on the group itself.

Remark. If a vector is represented by the basis as

$$x = (x^1, x^2, \ldots, x^{|G|}),$$

then $g \cdot x$ will be

$$g \cdot x = (x^{g^{-1}(1)}, x^{g^{-1}(2)}, \ldots, x^{g^{-1}(|G|)}).$$

Exercise* 1.4. TODO

1.2 Complete Reducibility; Schur's Lemma

Proposition in Book 1.5. *Given a representation ρ on V of a finite group G, if the subspace W of V satisfies $\forall g \in G \forall w \in W[\rho(g)(w) \in W]$, then there is another subrepresentation W' of V, so that $V = W \oplus W'$.*

Note that the decomposition of a vector space into direct sum of two is not unique. The projection onto one depends on the other one.

Consider a group of two elements, the non-identity element of which is represented in the $V = \mathbb{R}^4$ as

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{1.12}$$

If W is the first two dimensions in V, and U is the last two dimensions. Then the projection π_0 is given by:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}. \tag{1.13}$$

The other projection π is constructed as:

$$\pi = \frac{1}{2}\pi_0 + \frac{1}{2}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\pi_0 \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \pi_0. \tag{1.14}$$

Therefore the kernel of π, which is just U, is another subrepresentation of G. Note that elements in U are not invariant under G.

Consider another representation of the same group on $V = \mathbb{R}^3$, where the non-identity element is represented as

$$\begin{pmatrix} -1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Consider the subspace $W = \{\, [a, 0, 0] \mid a \in F \,\}$ and its complementary space $U = \{\, [0, b, c] \mid b, c \in F \,\}$. Then,

$$\pi_0 = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}, \tag{1.15}$$

and

$$\pi = \frac{1}{2}\pi_0 + \frac{1}{2}(-1)\,\pi_0 \begin{pmatrix} -1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -1 & 0 \end{pmatrix}.$$

The kernel is $W = \{\, [a, a, c] \mid a, c \in F \,\}$.

Proposition 1.11. *There is a Hermitian inner product on a finite representation that is preserved by the finite group.*

Proof. For a n-dimensional vector space V over complex number, it is always possible to find a basis set, based on which the Hermitian inner product H_0 is defined as

$$H_0(v, w) = \sum_{i=1}^{n} \overline{v^i} w^i,$$

where $v = \sum_{i=1}^{n} (v^i) e_i$, $w = \sum_{i=1}^{n} (w^i) e_i$ are their representations in the basis set $\{e_1, e_2, \ldots, e_n\}$.

Now we introduce the G-invariant binary operation $H \colon V \times V \to \mathbb{C}$ as

$$H(v, w) \coloneqq \sum_{g \in G} H_0(gv, gw).$$

We need to show this is a valid Hermitian product as follows.

- Linearity: holds because g is isomorphism and summation is linear operation.
- Conjugate symmetry: holds for similar reasons.
- Positive definiteness: holds for similar reasons ($gv = 0 \iff v = 0$).

This is G-invariant because any $h \in G$ acting on the group to the right simply permutes. □

Corollary in Book 1.6. *Complete reducibility.*

Note also that this argument would fail if the vector space V was over a field of finite characteristic since it might then be the case that $\pi(v) = 0$ for $v \in W$.
`https://en.wikipedia.org/wiki/Modular_representation_theory`

Lemma in Book 1.7. *Schur's Lemma.*

Proposition in Book 1.8. *Unique decomposition.*

Equation in Book 1.9.

$$V = a_1 V_1 \oplus \cdots \oplus a_k V_k.$$

1.3 Examples: Abelian Groups; $\mathfrak{S}_3$

Definition (center)**.** The **center** of a group is the set of elements that commute with every element in the group G, denoted as $\mathrm{Z}(G)$.

Theorem 1.12. *$\rho(g)$ is G-linear iff $g \in \mathrm{Z}(G)$.*

Proposition 1.13. *Any irreducible complex representation of an Abelian group is 1-dimensional.*

Proof. Any representation $\rho(g)$ must be G-linear map as the center of an Abelian group is the group itself. From Schur's Lemma this is proved. □

Definition (symmetric group)**.** The **symmetric group** $\mathfrak{S}_n$ defined over any set of cardinality n is the group whose elements are all the bijections from the set to itself.

Theorem 1.14. $|\mathfrak{S}_n| = n!$.

Proposition 1.15. *The $\mathfrak{S}_3$ group is isomorphic to C_{3v} group where the principal axis is along $[1, 1, 1]$.*

Definition (alternating representation)**.** The **alternating representation** of a symmetric group is a one-dimensional representation given by

$$gv = \operatorname{sgn}(g)v,$$

where sgn is 1 if g is an even permutation or -1 otherwise.

Definition (transposition)**.** A **transposition** is a permutation which exchanges two elements and keeps all others fixed.

Exercise 1.10. Ez to show the standard representation is valid.

Exercise 1.11. $\operatorname{Sym}^2 V$ has three basis:

$$\alpha \otimes \alpha, \frac{1}{2}(\alpha \otimes \beta + \beta \otimes \alpha), \beta \otimes \beta.$$

Therefore it is isomorphic to $U \oplus V$.

$\operatorname{Sym}^3 V$ has four. $\alpha^{\otimes 3}$ and $\beta^{\otimes 3}$ both have eigenvalue of 1 for τ. $\alpha^{\otimes 2}\beta$ and $\alpha\beta^{\otimes 2}$ are ω, ω^2 respectively. Since $\alpha^{\otimes 3}$ and $\beta^{\otimes 3}$ are linearly independent, $\operatorname{Sym}^3 V$ is isomorphic to $U \oplus U' \oplus V$.

Exercise 1.12. (a) The representation in the textbook

$$g(z_1, z_2, z_3) = (z_{g^{-1}(1)}, z_{g^{-1}(2)}, z_{g^{-1}(3)}).$$

has a basis set of

$$\{(1, 1, 1), \alpha, \beta\}.$$

Therefore it is $U \oplus V$.

Similarly, the **regular representation** is

$$g(z_1, z_2, z_3, z_4, z_5, z_6) = (z_{g^{-1}(1)}, z_{g^{-1}(2)}, z_{g^{-1}(3)}, z_{g^{-1}(4)}, z_{g^{-1}(5)}, z_{g^{-1}(6)}),$$

where the index 1 to 6 represents a permutation of the group, and the function is left multiplication.

Define the order as $1, \tau, \tau^2, \sigma, \tau\sigma, \sigma\tau$. Apparently, $(1, 1, 1, 1, 1, 1)$ and $(1, 1, 1, -1, -1, -1)$ forms basis for U and U'. Since the aforementioned permutation left-multiplied by τ^{-1} becomes $\tau^2, 1, \tau, \sigma\tau, \sigma, \tau\sigma$, τ has two eigenvectors of eigenvalue ω:

$$\alpha \oplus 0, 0 \oplus \alpha.$$

Similarly, τ has two eigenvectors of eigenvalue ω^2:

$$\beta \oplus 0, 0 \oplus \beta.$$

Therefore,

$$R \cong U \oplus U' \oplus V^{\oplus 2}.$$

(b) The basis in $\mathrm{Sym}^k V$ has bases (starting from $\alpha^{\otimes k}$ to $\beta^{\otimes k}$) of eigenvalues for τ of

$$\omega^k, \omega^{k+1}, \dots \omega^{2k}.$$

For $\mathrm{Sym}^{k+6} V$, it effectively add two sets of permutation of $1, \omega, \omega^2$ to the end of the above list. This corresponds to $U \oplus U' \oplus V^{\oplus 2} \cong R$. Therefore $\mathrm{Sym}^{k+6} V \cong \mathrm{Sym}^k V \oplus R$.

Below is the representation from $k = 1$ to 6:

k	1	2	3	4	5	6
$\mathrm{Sym}^k V$	V	$U \oplus V$	$U \oplus U' \oplus V$	$U \oplus V^{\oplus 2}$	R	$U \oplus R$

For $k = 2n$ there is always an additional U because the basis $\alpha^{\otimes n} \otimes \beta^{\otimes n}$ is symmetric (eigenvalue=1) with respect to τ.

Exercise* 1.13. For $\mathrm{Sym}^3 V$ the eigenvalues are $1, \omega, \omega^2, 1$, therefore $\mathrm{Sym}^2(\mathrm{Sym}^3 V)$ have three sets of ω, ω^2 and four 1s. The four 1s becomes a pair of $U \oplus U'$:

$$\{\alpha^6 + \beta^6, \alpha^6 - \beta^6\},$$

and two Us:

$$\{\alpha^3\beta^3 + \beta^3\alpha^3\}, \{(\alpha^2\beta)(\beta^2\alpha)\}.$$

Hence,

$$\mathrm{Sym}^2(\mathrm{Sym}^3 V) \cong U^3 \oplus U' \oplus V^3.$$

For $\mathrm{Sym}^3(\mathrm{Sym}^2 V)$, the eigenvalues are the same, except that the two Us are

$$\{(\alpha \otimes \beta + \beta \otimes \alpha)^{\otimes 3}\}, \{(\alpha^2)(\alpha\beta)(\beta^2)\}.$$

Is $\mathrm{Sym}^m(\mathrm{Sym}^n V)$ isomorphic to $\mathrm{Sym}^n(\mathrm{Sym}^m V)$?

Exercise* 1.14. There is a *unique* Hermitian inner product, up to scalars, for an irreducible representation of a finite group.

Proof. We have shown there is at least some Hermitian inner product in 1.11, say H for any finite representation.

Given a basis set $E = \{e_1, e_2, \dots, e_n\}$ of the n-dimensional vector space V, the representation $\rho\colon G \to \mathrm{GL}(V)$ can be represented as the $\mathbf{G}$ matrix:

$$\rho(g)(e_i) = \sum_{j=1}^{n} e_j G^j{}_i, \ \forall g \in G, i \in \mathbb{Z}_n.$$

The Hermitian inner product H can be represented similarly as the $\mathbf{H}$ matrix

$$H^i{}_j = H(e_i, e_j),\ \forall i, j \in \mathbb{Z}_n.$$

The invariance of H is represented as

$$\begin{aligned} H^i{}_j &= H\left(\rho(g)(e_i), \rho(g)(e_j)\right) = H\left(\sum_{r=1}^{n} e_r G^r{}_i, \sum_{s=1}^{n} e_s G^s{}_j\right) \\ &= \sum_{r=1}^{n}\sum_{s=1}^{n} (G^r{}_i)^* H^r{}_s G^s{}_j, \end{aligned}$$

$\forall g \in G$. This is to say,

$$\mathbf{G}^\dagger \mathbf{H} \mathbf{G} = \mathbf{H}.$$

Since H is positive definite, so is $\mathbf{H}$. Therefore, there is a unique Cholesky decomposition

$$\mathbf{H} = \mathbf{L}\mathbf{L}^\dagger,$$

where $\mathbf{L}$ is a lower triangular matrix with positive diagonal.

If H' is another one for the representation V of group G, we can construct and decompose the matrix similarly as

$$\mathbf{H}' = \mathbf{L}'\mathbf{L}'^\dagger,$$

where $\mathbf{L}'$ is a lower triangular matrix with positive diagonal uniquely determined by H'.

Since lower triangular matrix with positive diagonal is invertible, there is always a invertible matrix $\mathbf{Q} = (\mathbf{L}'\mathbf{L}^{-1})^\dagger$ such that

$$\mathbf{Q}^\dagger \mathbf{H} \mathbf{Q} = \mathbf{H}'.$$

Therefore, we have built an automorphism $\varphi\colon V \to V$ such that $H(\varphi(v), \varphi(w)) = H'(v, w)$.

Schur's Lemma indicates that φ must be a scalar multiplied by identity transform, proving the uniqueness of Hermitian inner product.

□

2 Characters

2.1 Characters

Definition (order)**.** The **order** of an element g in a group is a positive integer n such that g^n is the identity element.

Proposition 2.1. *All elements in a finite group must have an order.*

Proof. Otherwise the group would be infinite. □

Proposition 2.2. *The eigenvalues of the representation of an element in a finite group must be n-th roots of unity, where n is the order of the element.*

Proof. Because for any element g in the group, g^n is the identity, whose eigenvalues are 1. □

Proposition in Book 2.1.

$$\chi_{V\oplus W} = \chi_V + \chi_W, \chi_{V\otimes W} = \chi_V\chi_W, \chi_{V^*} = \bar{\chi}_V, ...$$

Exercise 2.2. $\sum_{i\le j}\lambda_i\lambda_j = \frac{(\sum\lambda_i)^2+\sum\lambda_i^2}{2}$.

Exercise* 2.3. For a specific element $g \in G$, where G is the group, if its eigenvalues in a n-dimensional representation V is $\{\lambda_i\}$, define a function $f\colon \mathbb{Z}^+ \to \mathbb{C}$ as

$$f(m) \coloneqq \chi_V(g^m) = \sum_{i=1}^{n}\lambda_i^m.$$

Denote the character of $\bigwedge^k V$ in n-dimensional space as $L(n,k)$. If we know $L(n,k-1)$, consider multiplying it by the character:

$$f(1)L(n,k-1) = kL(n,k) + f(2)L(n-1,k-2). \tag{2.1}$$

When the additional term in $f(1)$ does not duplicate with any term in $L(n,k-1)$, it becomes a term in $L(n,k)$, but it has k duplicity as the new term can be multiplied in any position.

If $\lambda_{p_1}\lambda_{p_2}\lambda_{p_k}$ is a term in $L(n,k)$, with $p_1 < p_2 < \cdots < p_k$, there is k possibilities to get it from multiplying $L(n,k-1)$ by $f(1)$:

$L(n,k-1)$														
$f(1)$	p_1	p_2	...	p_k	p_1	p_2	...	p_k	...	...	p_1	p_2	...	p_k

The other term on the right hand side of (2.1) is the situation where the index in $f(1)$ overlaps with one in $L(n,k-1)$. In this case, you can reduce it as a sum of λ_i^2 multiplied by the product of $k-2$ non-repeating indices sampled in a $k-1$ dimensional space (because one dimensional is occupied by the λ_i^2 term).

Similarly, we can rewrite the $kL(n,k)$ term as $f(1)L(n-1,k-1)$. By the same procedure of deriving (2.1), we can also write down the formula to calculate $L(n-1,k-p)$ terms:

$$f(p)L(n-1,k-p) = f(p)L(n,k-p) - f(p+1)L(n-1,k-p-1). \quad (2.2)$$

Therefore, we can plug (2.2) into (2.1)

$$L(n,k) = \frac{1}{k}\left[\sum_{p=1}^{k}(-1)^{p+1}f(p)L(n,k-p)\right], \quad (2.3)$$

where $L(n,0) = 1$.

Now we can write it down explicitly:

$$\begin{aligned}
\chi_{\bigwedge^1 V}(g) &= \chi_V(g),\\
\chi_{\bigwedge^2 V}(g) &= \frac{1}{2}\left[(\chi_V(g))^2 - \chi_V(g^2)\right],\\
\chi_{\bigwedge^3 V}(g) &= \frac{\chi_V(g)}{6}\left[(\chi_V(g))^2 - \chi_V(g^2)\right] - \frac{\chi_V(g^2)}{3}\chi_V(g) + \frac{\chi_V(g^3)}{3},\\
&= \frac{(\chi_V(g))^3}{6} - \frac{\chi_V(g)\chi_V(g^2)}{2} + \frac{\chi_V(g^3)}{3},\\
L(n,4) &= \frac{1}{4!}\left[f^4(1) - 6f^2(1)f(2) + 3f^2(2) + 8f(1)f(3) - 6f(4)\right].
\end{aligned} \quad (2.4)$$

Equation for $\mathrm{Sym}^k V$.

Definition (characteristic polynomial)**.** The **characteristic polynomial** of an $n \times n$ matrix $\mathbf{A}$, denoted by $p_A(t)$, is the polynomial defined by

$$p_A(t) = \det(t\mathbf{I}_n - \mathbf{A}).$$

Proposition 2.3. *The characteristic polynomial of* $\mathbf{A} \in \mathrm{M}_n(\mathbb{C})$ *is*

$$p_A(t) = \prod_{i}^{n}(t - \lambda_i),$$

where λ_i *are eigenvalues of* $\mathbf{A}$*.*

Proof. $\mathbb{C}$ is algebraically closed. □

Exercise* 2.4. Given an n-dimensional space V, in the characteristic polynomial of $\rho(g) \in \mathrm{GL}(V)$, the coefficient of t^{n-k} is $(-1)^k \chi_{\bigwedge^k V}(g)$.

Exercise 2.5. The representation is a matrix of $|X|$ 1's, which is on the main diagonal if element in X is fixed by g, or elsewhere otherwise.

Therefore $\chi_V(g) = \mathrm{Tr}(\rho(g))$ counts the number of nonzero elements on the main diagonal, i.e., the number of fixed elements.

Example in Book 2.6. Character table of $\mathfrak{S}_3$.

Exercise* 2.7. See the character table

	1	3	2
$\mathfrak{S}_3$	1	(12)	(123)
V	2	0	-1
$V \otimes V$	4	0	1

The character of $V^{\otimes n}$ is $(2^n, 0, (-1)^n)$, therefore

$$V^{\otimes n} \cong U^{\oplus \frac{2^{n-1}+(-1)^n}{3}} \oplus U'^{\oplus \frac{2^{n-1}+(-1)^n}{3}} \oplus V^{\oplus \frac{2^n-(-1)^n}{3}}.$$

2.2 The first projection formula and its consequences

Proposition in Book 2.8. *The map* $\varphi = \frac{1}{|G|}\sum_{g\in G} \rho(g)$ *is a projection of* V ***onto*** $V^G = \{\, v \in V \mid \forall g \in G[\rho(g)(v) = v] \,\}$.

Equation in Book 2.9. $\dim V^G = \mathrm{Tr}(\varphi)$.

Proof. $\because \varphi \circ \varphi = \varphi$, $\therefore$ the eigenvalues must be either 0 or 1. The trace is just the sum of all eigenvalues. But φ maps *onto* V^G. Therefore, the number of nonzero eigenvalues must be equal to $\dim V^G$. □

Equation in Book 2.10.

$$\frac{1}{|G|}\sum_{g\in G} \overline{\chi_V(g)}\chi_W(g) = \delta_{VW}.$$

Definition (conjugacy class)**.** Given a group G, the equivalence class that contains the element $a \in G$ is

$$\mathrm{Cl}(a) = \left\{ gag^{-1} : g \in G \right\}$$

and is called the **conjugacy class** of a.

Definition (class function)**.** A **class function** is a *function on a group* G that is constant on the conjugacy classes of G.

Equation in Book 2.11.

$$(\alpha, \beta) = \frac{1}{|G|} \sum_{g \in G} \overline{\alpha(g)} \beta(g).$$

Theorem in Book 2.12. *In terms of this Hermitian inner product, the characters of the irreducible representations of* G *are orthonormal.*

Corollary in Book 2.13. *The number of irreducible representations of* G *is less than or equal to the number of conjugacy classes.*

Corollary in Book 2.14. *Any representation is determined by its character.*

Corollary in Book 2.15. *A representation* V *is irreducible if and only if* $(\chi_V, \chi_V) = 1$.

Corollary in Book 2.16. *The multiplicity* a_i *of* V_i *in* V *is the Hermitian inner product of* χ_V *with* χ_{V_i} *i.e.,* $a_i = (\chi_V, \chi_{V_i})$.

Equation in Book 2.17.

$$R = \bigoplus V_i^{\oplus \dim V_i},$$

where R is the regular representation.

Corollary in Book 2.18. *Any irreducible representation* V *of* G *appears in the regular representation* $\dim V$ *times.*

Equation in Book 2.19.

$$|G| = \dim R = \sum_i \dim \left(V_i\right)^2.$$

Equation in Book 2.20.

$$0 = \sum_{V_i} (\dim V_i) \cdot \chi_{V_i}(g),$$

if $g \neq e$.

Definition (class number)**.** The **class number** of a group is the number of distinct (nonequivalent) conjugacy classes.

Exercise 2.21. Assuming the class number is the number of unique irreducible representations.

$$\sum_{\chi} \overline{\chi(g)}\chi(h) = \frac{|G|}{c(g)}\delta_{gh},$$

where $c(g)$ is the cardinality of the conjugacy classes of $g \in G$, and δ is the Kronecker delta.

Proof. Since the class number is the number of unique irreducible representations, the character table forms a unitary matrix.

If $\mathcal{G}$ is the set of all conjugacy classes in group G, the class number of which is $m = |\mathcal{G}|$, denote $[g]$ as the conjugacy class of $g \in G$, and define an $m \times m$ matrix $\mathbf{X} \in \mathrm{M}_m(\mathbb{C})$ such that the (ij)-th element is

$$X_{ij} = \sqrt{\frac{c(g_i)}{|G|}}\chi_{V_j}(g_i),$$

where V_j is the j-th unique irreducible representation, and $[g_i]$ is the i-th nonequivalent conjugacy classes (g_i can be any element in the class without changing the result, as both χ and c are class functions).

We can show that $\mathbf{X}$ is unitary from (2.10)

$$(\mathbf{X}^\dagger\mathbf{X})_{ij} = \sum_{k=1}^{m} \overline{X_{ki}}X_{kj} = \sum_{[g]\in\mathcal{G}} \frac{c(g)}{|G|}\overline{\chi_{V_i}(g)}\chi_{V_j}(g) = \delta_{ij}, \tag{2.5}$$

where δ is the Kronecker delta notation.

Therefore,

$$\delta_{ij} = (\mathbf{X}\mathbf{X}^\dagger)_{ij} = \sum_{k=1}^{m} X_{ik}\overline{X_{jk}} = \frac{\sqrt{c(g_i)c(g_j)}}{|G|}\sum_{\chi} \chi(g_i)\overline{\chi(g_j)}. \tag{2.6}$$

Set $g = g_j$ and $h = g_i$. When $g \neq h$, the equation is zero, and therefore $\frac{\sqrt{c(g_i)c(g_j)}}{|G|}$ can be replaced by any constant. When $g = h$, $\frac{\sqrt{c(g_i)c(g_j)}}{|G|} = \frac{c(g)}{|G|}$. □

2.3 Examples: $\mathfrak{S}_4$ and $\mathfrak{A}_4$

2.3.1 Basic Group Theory

2.3.1.1 Generated Subgroup

Definition (generated subgroup)**.** The **subgroup generated by a subset** of a group is the smallest subgroup containing every element of the subset.

Remark. The subgroup generated by a subset S of a group G is expressed by

$$\langle S \rangle = \{ \prod_{i=1}^{n} s_i^{k_i} \in G \mid n \in \mathbb{Z}^+, s_i \in S, k_i \in \{-1, 1\} \}.$$

Theorem 2.4. *$\langle S \rangle$ is the intersection over all subgroups containing the elements of S.*

Proposition 2.5. *The subgroup generated by a subset S of a finite group G is expressed by*

$$\langle S \rangle = \{ \prod_{i=1}^{n} s_i \in G \mid n \in \mathbb{Z}^+, s_i \in S \}.$$

Proof. This is true because any element in a finite group has a finite order, i.e., the inverse of an element can be expressed by a power of the element. □

Definition (generating set)**.** A **generating set of a group** is a subset of the group such that every element of the group can be expressed as a combination (under the group operation) of finitely many elements of the subset and their inverses.

Remark. This is equivalent to saying that, the subset S of a group G is its **generating set** if and only if

$$\forall g \in G \left[g = \prod_{i=1}^{n} s_i^{k_i} \right],$$

where $s_i \in S$ and k_i is either 1 or -1.

Remark. A subgroup generated by an element g in a *finite* group G is expressed by

$$\langle g \rangle = \{ g^n \in G \mid n \in \mathbb{N} \}.$$

$|\langle g \rangle|$ is the order of g.

2.3.1.2 Group Action and Orbits

Definition (group action)**.** If G is a group with identity element e, and X is a set, then a (left) **group action** α of G on X is a function $\alpha \colon G \times X \to X$, that satisfies the following two axioms:

- Identity:

$$\alpha(e, x) = x, \ \ \forall x \in X.$$

- Compatibility:

$$\alpha\left(g, \alpha\left(h, x\right)\right) = \alpha\left(gh, x\right), \ \ \forall g, h \in G, \forall x \in X.$$

The group G is said to act on X (from the left). A set X together with an action of G is called a (left) G-set. $\alpha(g, x)$ is alternatively denoted as $g \cdot x$.

Definition (orbit)**.** Consider a group G acting on a set X. The **orbit** of an element $x \in X$ is the set of elements in X to which x can be moved by the elements of G. The orbit of x is denoted by $G \cdot x$:

$$G \cdot x = \left\{g \cdot x \in X \mid g \in G\right\}.$$

2.3.1.3 Cyclic Permutation

Definition (cycle)**.** The **cycles** of a permutation π of a finite set S correspond bijectively to the orbits of the subgroup generated by π acting on S.

Or equivalently:

Definition (k-cycle)**.** If a permutation π of a finite set X permutes the subset $S = \{s_1, s_2, \ldots, s_k\}$ of X in the way:

$$\pi(s_i) = s_{i+1}, \ \forall i \in \mathbb{Z}_k,$$

where s_{k+1} is set as s_1, we say this is a k**-cycle** of the permutation π, denoted as $(s_1 s_2 \ldots s_k)$. The subset S is the **orbit** of the cycle.

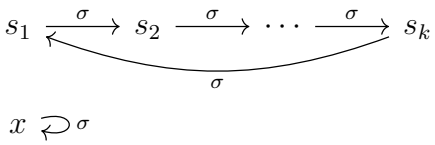
Remark. This expression is not unique since c_1 can be chosen to be any element of the subset.

Definition (cyclic permutation)**.** A permutation σ of a set X, viewed as a bijective function $\sigma\colon X \to X$, is called **cyclic** if the action on X of the subgroup generated by σ has at most one orbit with more than a single element.

Or equivalently:

Definition (cyclic permutation, alt)**.** A permutation is called a **cyclic permutation** *if and only if* it has at most one single nontrivial cycle (a cycle of length larger than 1).

Remark. A permutation σ acting on X is cyclic if and only if there is a subset $S = \{s_1, s_2, \ldots, s_k\}$ of X such that the following relationship holds (x must be satisfied for all elements of X not in S).



Definition (disjoint cycles)**.** Two cycles are called **disjoint** if their orbits are disjoint.

Proposition 2.6. *Disjoint cycles are commutative.*

Proof. Since the cycle acts on non-orbit elements as identity morphism, which commutes with any elements in the permutation group, disjoint cycles are commutative.

Given two disjoint cycles $\sigma = (s_1 s_2 \dots s_p)$ and $\pi = (t_1 t_2 \dots t_q)$,

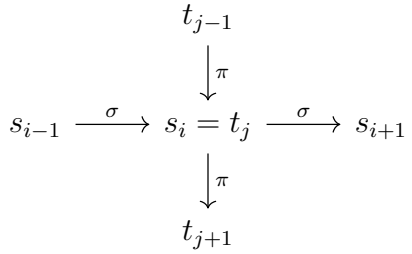
$$\begin{aligned}\pi(\sigma(t_i)) &= \sigma(\pi(t_i)) = t_{i+1},\\ \pi(\sigma(s_j)) &= \sigma(\pi(s_j)) = s_{j+1},\\ \pi(\sigma(x)) &= \sigma(\pi(x)) = x,\end{aligned}$$

where x is an element in neither orbits. □

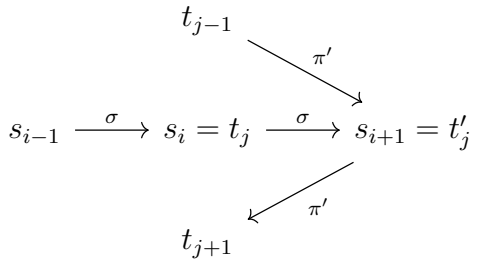
Theorem 2.7. *Any permutation can be expressed as product of disjoint cycles.*

Proposition 2.8. *If the intersection of orbits of two cycles, σ and π, is a singleton $\{s_i = t_j\}$, then $\sigma \circ \pi \circ \sigma^{-1}$ is still a cycle, whose orbit is that of π shifted by one element, from the s_i to $\sigma(s_i)$.*

Proof. Consider the following cycles $\sigma = (s_1 s_2 \dots s_p)$ and $\pi = (t_1 t_2 \dots t_q)$,



If $\pi' = \sigma \circ \pi \circ \sigma^{-1}$, then



□

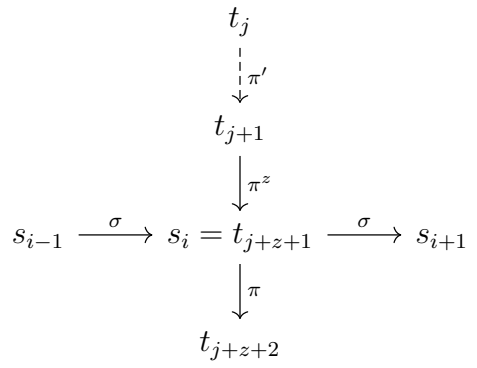
Proposition 2.9. *Given a cycle $\pi = (t_1 t_2 \dots t_k)$ acting on a set and an arbitrary permutation σ acting on the same set X, $\pi' = \sigma \circ \pi \circ \sigma^{-1}$ is still a k-cycle expressed as $(\sigma(t_1)\sigma(t_2)\dots\sigma(t_k))$.*

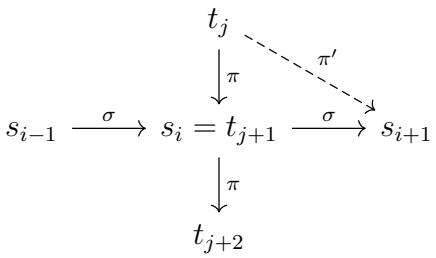
Proof. First, there is no repeating element in $(\sigma(t_1)\sigma(t_2)\dots\sigma(t_k))$ because σ is a permutation.

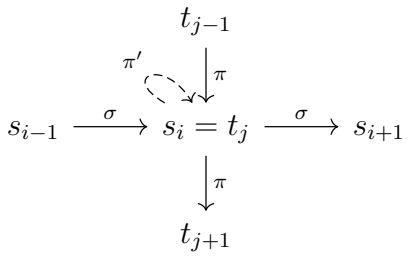
Second, $\pi'(\sigma(t_j)) = \sigma \circ \pi \circ \sigma^{-1} \circ \sigma(t_j) = \sigma(t_{j+1})$.

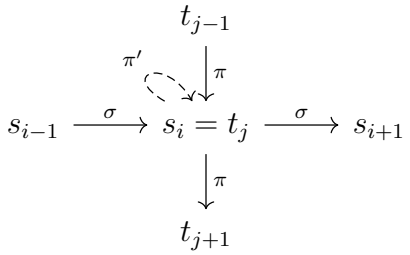
Third, if $\pi \circ \sigma^{-1}(x) \neq \sigma^{-1}(x)$, then $\sigma^{-1}(x)$ must be in the orbit of π, i.e., be one of t_j, in which case, x must be one of $\sigma(t_j)$. If x cannot be expressed as $\sigma(t_j)$, then $\pi'(x) = \sigma \circ \sigma^{-1}(x) = x$. □

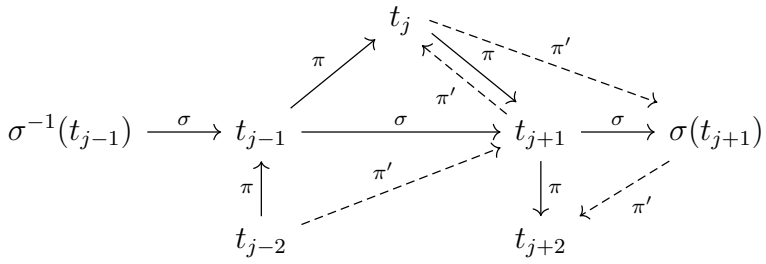
Corollary 2.10. *Given two cycles, σ and π, the latter of which is a k-cycle, then $\sigma \circ \pi \circ \sigma^{-1}$ is still a k-cycle.*

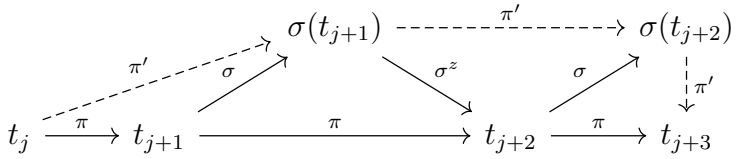



t_j
π'
π
s_{i-1}
σ
$s_i = t_{j+1}$
σ
s_{i+1}
π
t_{j+2}


t_{j-1}
π'
π
s_{i-1}
σ
$s_i = t_j$
σ
s_{i+1}
π
t_{j+1}


t_{j-1}
π'
π
s_{i-1}
σ
$s_i = t_j$
σ
s_{i+1}
π
t_{j+1}


t_j
π
π
π'
π'
$\sigma^{-1}(t_{j-1})$
σ
t_{j-1}
σ
t_{j+1}
σ
$\sigma(t_{j+1})$
π
π'
π
π'
t_{j-2}
t_{j+2}



Proposition 2.11. *The set of all k-cycles in a permutation group forms a conjugacy class.*

Proof. 1-cycles are trivial permutations, i.e., the identity element, which itself forms a conjugacy class.

Any group element can be expressed as product of cycles (2.7), each of which transforms a k-cycle to a k-cycle (see 2.10). Therefore, the conjugacy class is a subset of all k-cycles.

Any k-cycle can be transformed from another k-cycle by changing each of its orbit (see 2.8). Given $\sigma = (s_1 s_2 \dots s_k)$ and $\pi = (t_1 t_2 \dots t_k)$,

$$\sigma = \rho \circ \pi \circ \rho^{-1},$$

where

$$\rho = (t_1 s_1) \circ (t_2 s_2) \circ \cdots \circ (t_k s_k).$$

Note that if $t_i = s_i$, $(t_i s_i)$ becomes the identity, which does not affect the conclusion. Therefore, the set of all k-cycles is a subset of the conjugacy class. □

2.3.2 Main Text

Definition (partition)**.** A **partition** of a positive integer n, also called an integer partition, is a way of writing n as a sum of positive integers.

Proposition 2.12. *For any positive integer d, there is a bijection mapping from partitions of d onto conjugacy classes of $\mathfrak{S}_d$.*

Proof. Any permutation acting on set X is product of disjoint cycles (2.7). If the union of orbits of multiplicands does not equal to X, it can be always completed by adding identities, whose orbit is a singleton.

Therefore, any permutation σ can be represented as product of disjoint cycles, whose orbits cover the whole set X:

$$\sigma = \prod_i (s_{i,1}\ s_{i,2}\ \dots\ s_{i,k_i}),$$

where

$$\sum_i k_i = |X| = d,$$

and $s_{i,j} = s_{m,n} \iff (i = m \wedge j = n)$.

Given any permutation π (2.9),

$$\pi \circ \sigma \circ \pi^{-1} = \prod_i \pi \circ (s_{i,1}\, s_{i,2}\, \ldots\, s_{i,k_i}) \circ \pi^{-1} = \prod_i (\pi(s_{i,1})\, \pi(s_{i,2})\, \ldots\, \pi(s_{i,k_i})). \tag{2.7}$$

Since π is a permutation, we have $\pi(s_{i,j}) = \pi(s_{m,n}) \iff (i = m \wedge j = n)$. Therefore, this does not change the pattern (k_i).

Given another permutation expressed by $\prod_i (p_{i,1}\, p_{i,2}\, \ldots\, p_{i,k_i})$, possibly with different permutation of (k_i). Since disjoint cycles are commutative (2.6), the order of multiplication does not matter, therefore you can always align the (k_i) to make them consistent. Since $p_{i,j} = p_{m,n} \iff (i = m \wedge j = n)$, we can always find a permutation π such that $\pi(s_{i,j}) = p_{i,j}$, in which way equation (2.7) holds.

Now we have proved that each conjugacy class is completely determined by (k_i). Also, each partition of d corresponds to a pattern (k_i). Therefore, the bijection exists. □

Corollary 2.13. *The class number of $\mathfrak{S}_d$ is the partition function of d.*

Exercise 2.22. The cardinality of the conjugacy class of $\mathfrak{S}_d$ given by the partition (k_i) is

$$\frac{d!}{\prod_{j=1}^{d} m_j! \prod_i k_i},$$

where m_j is the cardinality of set $\{i \in \mathbb{Z}^+ | k_i = j\}$.

Corollary 2.14.

$$\sum_{j=1}^{d} j m_j = \sum_i k_i = d.$$

Corollary 2.15.

$$\frac{d!}{\prod_{j=1}^{d} m_j! \prod_i k_i} = \frac{d!}{\prod_{j=1}^{d} j^{m_j} m_j!}.$$

Corollary 2.16.

$$\sum_{\mathbf{k} \in p(d)} \frac{1}{\prod_{j=1}^{d} j^{m_j} m_j!} = 1.$$

Proof. The disjoint union of all conjugacy classes should be the group itself, whose size is $d!$ (1.14). □

Proposition 2.17. *The alternating representation is a representation for all symmetric groups.*

Proof. The multiplication of odd/even permutations is homomorphic to multiplication of odd/even numbers. □

Definition (standard representation)**.** The **standard representation** of a symmetric group $\mathfrak{S}_d$ $(d > 1)$ is the quotient of permutation representation on $\mathbb{C}^d$ by the trivial representation.

Remark.

$$\mathbb{C}^d \cong U \oplus V,$$

where U is the trivial representation and V is the standard representation.

Proposition 2.18. *Standard representation is irreducible.*

Proof. From 2.5 we know the character of the permutation representation is

$$\chi_{\mathbb{C}^d}(k_i) = m_1(k_i),$$

where $m_j(k_i)$ is the cardinality of set $\{i \in \mathbb{Z}^+ | k_i = j\}$.

Therefore the character of the standard representation V is

$$\chi_V(k_i) = m_1(k_i) - 1. \tag{2.8}$$

The squared norm (2.11) of the representation is

$$(\chi_V, \chi_V) = \frac{1}{d!} \sum_{\mathbf{k} \in p(d)} \frac{d!}{\prod_{j=1}^{d} j^{m_j} m_j!} (m_1 - 1)^2. \tag{2.9}$$

Consider the form

$$f(d, s) = \sum_{\mathbf{k} \in p(d)} \left[\frac{1}{\prod_{j=1}^{d} j^{m_j} m_j!} \prod_{r=0}^{s} (m_1 - r) \right], \tag{2.10}$$

where s is a natural number smaller than d.

The term $\prod_{r=0}^{s}(m_1 - p)$ selects all $\mathbf{k}$ with $m_1 > s$. This always exists because there is a partition of d with $m_j = \delta_{1j} d$ and $s < d$.

Since $\sum_{j=1}^{d} j m_j = d$, if $m_1 > s$, then $\sum_{j=2}^{d} j m_j < d - s$ (note that $d > 1$). Therefore $m_j = 0$ for all $j \geq \max(d - s, 2)$.

Therefore (since $d > 1$, $(m_1 - s - 1)!$ is defined) (2.10) is

$$f(d,s) = \sum_{\mathbf{k}\in p(d), m_1 > s} \left[\frac{1}{(m_1 - s - 1)! \prod_{j=2}^{d-s-1} j^{m_j} m_j!} \right], \tag{2.11}$$

where the product evaluates to 1 if $d - s - 1 < 2$.

Perform the following replacement:

$$\begin{aligned} d' &= \max(1, d - s - 1) = d - s - 1 + \delta_s^{d-1}, \\ m'_j &= m_j, \forall j > 1 \\ m'_1 &= m_1 - s - 1 + \delta_s^{d-1}. \end{aligned} \tag{2.12}$$

Easy to show that $\sum_{j=1}^{d'} j m'_j = \sum_{j=1}^{d} j m'_j = d'$.

Since $1^{m'_1} = 1$, $0! = 1!$, (2.11) can be rewritten as (using 2.16)

$$\begin{aligned} f(d,s) &= \sum_{\mathbf{k}\in p(d), m_1 > s} \left[\frac{1}{\prod_{j=1}^{d'} j^{m'_j} m'_j!} \right] \\ &= \sum_{\mathbf{k}\in p(d')} \left[\frac{1}{\prod_{j=1}^{d'} j^{m'_j} m'_j!} \right] \\ &= 1. \end{aligned} \tag{2.13}$$

By using (2.13), (2.9) reduces to (note that $d > 1$)

$$(\chi_V, \chi_V) = f(d,1) - f(d,0) + 1 = 1.$$

From 2.15, we know V is irreducible. □

Remark. Alternatively, we can separate $s = d - 1$ case from the $s < d - 1$ cases.

If $s = d - 1$, then $m_1 = d$ and all other m's must be zero.

$$f(d, d-1) = \frac{1}{0!} = 1. \tag{2.14}$$

If $s < d - 1$, then $d - s \geq 2$. Everything becomes normal.

Corollary 2.19. *The character of the standard representation V is*

$$\chi_V(k_i) = m(k_i) - 1. \tag{2.15}$$

where $m(k_i)$ is the cardinality of set $\{i \in \mathbb{Z}^+ | k_i = 1\}$, i.e., the number of disjoint trivial cycles in the conjugacy class.

Proof. See 2.18. □

Proposition 2.20. *The character of a 1-dimensional representation of a finite group is roots of unity.*

Proof. The character is the eigenvalue of the linear map representing the group element. Therefore, it must be a root of unity. □

Corollary 2.21. *For any 1-dimensional (irreducible) representation L, there must be another 1-dimensional representation L^* such that $L^* \otimes L \cong L \otimes L^* \cong U$, where U is the trivial representation.*

Proposition 2.22. *The tensor product of an irreducible representation with a 1-dimensional representation is irreducible.*

Proof. See the proof for more general cases here. Here we provide a proof for the finite case.

Let V be an irreducible representation of any finite group G and let L be a 1-dimensional representation. If $\oplus_i W_i \cong V \otimes L$, where W_i are proper nonzero subrepresentations (and not the only one), then $\oplus_i (W_i \otimes L^*) \cong V$, and $W_i \otimes L^*$ are proper nonzero subrepresentations, contradicting with the definition of irreducibility.

The similar conclusion holds for $L \otimes V$. □

Exercise 2.23. Verify character table of $\mathfrak{S}_4$...

Proposition 2.23. *If $\chi_V(g) = \chi_V(e)$, where e is the identity in the group, then g is represented as identity matrix in V.*

Proof. Character is sum of eigenvalues, which are roots of unity. Therefore the eigenvalues must be all 1's.

Since the representation are unitary matrix (2.27), it must be identity matrix.

$\chi_V(e)$ is the dimension of the representation V. □

Definition (normal subgroup)**.** A **normal subgroup** is a subgroup that is invariant under conjugation by members of the group of which it is a part.

Remark. N is a normal subgroup of G iff N is a subgroup and

$$\forall g \in G \forall n \in N [gng^{-1} \in N].$$

Proposition 2.24. *The elements whose representation is identity matrix forms a normal subgroup.*

Proof. They form a subgroup, because e is represented as identity matrix, identity matrix multiplied by identity matrix is identity matrix, the inverse of an identity matrix is an identity matrix.

They form a normal subgroup, because identity matrix commutes with any other matrix in the same matrix ring. Therefore,

$$\rho(gng^{-1}) = \rho(g)\rho(n)\rho(g)^{-1} = \rho(e).$$

□

Definition (coset)**.** Let H be a subgroup of the group G. Given an element g of G, the **left cosets** of H in G are

$$gH = \{\, gh \mid h \in H \,\}.$$

The **right cosets** are

$$Hg = \{\, hg \mid h \in H \,\}.$$

Definition (quotient group)**.** Let N be a normal subgroup of a group G. The **quotient group** G/N is the set of all left cosets of N in G.

Remark.

$$G/N = \{\, aN \mid a \in G \,\} = \{\, \{\, an \mid n \in N \,\} \mid a \in G \,\}.$$

Theorem 2.25. *If N is a normal subgroup of a group G, a representation is trivial on N if and only if it factors through the quotient.*

Remark. Given a normal subgroup N of group G whose representation is ρ,

$$\forall g \in G \forall n \in N[\rho(gn) = \rho(g)]$$

is equivalent to

$$\forall n \in N[\rho(n) = \rho(e)],$$

where e is the identity element.

Example in Book 2.24. The group of rigid motions of a cube is the symmetric group on four letters; $\mathfrak{S}_4$ acts on the cube via its action on the four long diagonals. $\mathfrak{S}_3$ acts on the cube via its action on the axis connecting centers of opposite faces.

The $\mathfrak{S}_4$ group is isomorphic to the T_d point group: `http://symmetry.jacobs-university.de/cgi-bin/group.cgi?group=902&option=4`.

This correspond to the permutation of four vertices of a tetrahedron.

T_d	E	C_3	C_2	S_4	σ_d
$\mathfrak{S}_4$	1	(123)	(12)(34)	(1234)	(12)

Exercise* 2.25. Decompose the permutation representation of $\mathfrak{S}_4$ on (i) the vertices and (ii) the edges of the cube.

Definition (alternating group)**.** An **alternating group** is the group of even permutations of a finite set.

Exercise 2.26. The character table for $\mathfrak{A}_4$:

	1	4	4	3
$\mathfrak{A}_4$	1	(123)	(132)	(12)(34)
U	1	1	1	1
U'	1	ω	ω^2	1
U''	1	ω^2	ω	1
V	3	0	0	-1

The $\mathfrak{A}_4$ group is isomorphic to the T point group: `http://symmetry.jacobs-university.de/cgi-bin/group.cgi?group=900&option=4`.

Exercise 2.27. U, V are preserved, W is decomposed. $U \cong U'$, $V \cong V'$.

2.4 More projection formulas; more consequences

2.4.1 Main Text

Proposition in Book 2.28. *Given a finite group G whose representation $\rho\colon G \to \mathrm{GL}(V)$ is automorphism on a finite-dimensional vector space V over $\mathbb{C}$, and $\alpha\colon G \to \mathbb{C}$, let $\varphi_{\alpha,V} \in \mathrm{End}(V)$ be*

$$\varphi_{\alpha,V} = \sum_{g\in G} \alpha(g)\rho(g).$$

Then

$$\forall V \forall \rho \forall h \in G[\varphi_{\alpha,V} \circ \rho(h) = \rho(h) \circ \varphi_{\alpha,V}]$$

is equivalent to

$$\forall g \in G \forall h \in G[\alpha(g) = \alpha(hgh^{-1})].$$

Exercise 2.29. For any $v \in V$, because hgh^{-1} is just a permutation of g, ρ is homomorphism, and α maps to a scalar,

$$\begin{aligned}
\varphi_{\alpha,V} \circ \rho(h)(v) &= \sum_{g\in G} \alpha(g)\rho(g) \circ \rho(h)(v) \\
&= \sum_{g\in G} \alpha(hgh^{-1})\rho(hg(h^{-1})) \circ \rho(h)(v) \\
&= \rho(h) \left(\sum_{g\in G} \alpha(hgh^{-1})\rho(g) \circ \rho(h^{-1}) \circ \rho(h)(v) \right) \\
&= \rho(h) \left(\sum_{g\in G} \alpha(hgh^{-1})\rho(g)(v) \right).
\end{aligned} \tag{2.16}$$

At the same time,

$$\rho(h) \circ \varphi_{\alpha,V}(v) = \rho(h) \left(\sum_{g\in G} \alpha(g)\rho(g)(v) \right). \tag{2.17}$$

Therefore, by comparing (2.16) with (2.17)

$$\alpha(hgh^{-1}) = \alpha(g) \implies \varphi_{\alpha,V} \circ \rho(h) = \rho(h) \circ \varphi_{\alpha,V}.$$

Let V be $\mathbb{C}^{|G|}$, the space of complex valued functions on G and ρ the regular representation R of G. If v is one of the basis in V, then $\rho(g)(v)$ generates a complete basis set because $\rho(g)$ permutes the basis.

Equalize (2.16) with (2.17) and perform left action $\rho(h^{-1})$, it becomes

$$\sum_{g\in G} \alpha(hgh^{-1})\rho(g)(v) = \sum_{g\in G} \alpha(g)\rho(g)(v),$$

for which to hold the coefficients must be consistent.

Therefore,

$$\varphi_{\alpha,\mathbb{C}^{|G|}} \circ R(h) = R(h) \circ \varphi_{\alpha,\mathbb{C}^{|G|}} \implies \alpha(hgh^{-1}) = \alpha(g).$$

Proposition in Book 2.30. *N(irreducible representation) = N(conjugacy class).*

Equivalently, the characters of irreducible representations form an orthonormal basis for class functions on the group.

Remark. $\varphi_{\alpha,V}$ is G-like linear map from irreducible representation V to V, therefore $\varphi_{\alpha,V} = \lambda \cdot \mathrm{id}$ from Schur's Lemma (1.7).

Since $\varphi_{\alpha,V}$ is zero for all irreducible representations, and any representation is finite direct sum of irreducible representations, $\therefore\ \varphi_{\alpha,V} = 0$ for all representations.

Definition (free abelian group)**.** A **free abelian group** is an abelian group with a basis.

Remark. If B forms a basis of a free abelian group G, then any $g \in G$ can be uniquely represented as (assuming multiplication is the group operation)

$$g = \prod_{b \in B'} b^{g_b},$$

where B' is a finite subset of B and g_b are nonzero integers.

Proposition 2.26. *The set of all isomorphism classes of representations of a finite group forms a free commutative monoid.*

Proof. Direct sum is commutative. The irreducible representations form a complete basis set. The coefficient is the duplicity (non-negative). Also: 1.8. □

Definition (representation ring)**.** The **representation ring** $R(G)$ of a group G is a ring whose elements are the formal differences of isomorphism classes of finite dimensional linear representations of the group. For the ring structure, addition is given by the *direct sum* of representations, and multiplication by their *tensor product*.

Definition (virtual representation)**.** Elements of a representation ring are called **virtual representations**.

Remark. A free abelian group whose basis set is all isomorphism classes of representations can be constructed as

$$\{ \sum_{i=1}^{n} a_i V_i \},$$

where $a_i \in \mathbb{Z}$ and V_i are isomorphism classes of finite representations of the group.

The representation ring of a finite group can be constructed as this free abelian group mod out the subgroup generated by elements of the form $V + W - (V \oplus W)$ (coefficients are 1, 1, and -1).

Alternatively, the representation ring of a finite group can be constructed as

$$\{ \sum_{i=1}^{n} a_i U_i \},$$

where $a_i \in \mathbb{Z}$ and U_i are isomorphism classes of irreducible representations of the group.

Remark. Representations have non-negative coefficients but virtual representations are allowed to have *negative coefficients*.

Remark. The virtual representation can be defined as a set of ordered pairs of two finite representations

$$[U, V] = \{ (U', V') \mid U \oplus V' \cong U' \oplus V \}.$$

The addition is defined as

$$[U, V] + [U', V'] = [U \oplus U', V \oplus V'].$$

The multiplication is defined as

$$[U, V] \cdot [U', V'] = [(U \otimes U') \oplus (V \otimes V'), (U \otimes V') \oplus (V \otimes U')].$$

Easy to show that these operations are well-defined, i.e., not depending on the two representations in the bracket.

Definition (virtual character)**.** The character χ defines a ring homomorphism $R(G) \to \mathbb{C}_{\text{class}}(G)$, where $\mathbb{C}_{\text{class}}(G)$ is the set of all class functions on group G. The image of χ is **virtual character**.

Remark. The virtual character induces an isomorphism

$$\chi_{\mathbb{C}} \colon R(G) \otimes \mathbb{C} \to \mathbb{C}_{\text{class}}(G).$$

Remark.

$$\mathbb{Z} \times \mathbb{C} \cong \mathbb{C}?$$

Equation in Book 2.31.

$$\psi_V.$$

Equation in Book 2.32.

$$\pi_i = \frac{\dim V_i}{|G|} \sum_{g \in G} \overline{\chi_{V_i}(g)} \cdot g$$

is the linear projection of $\bigoplus_j V_j^{\oplus a_j}$ *onto* $V_i^{\oplus a_i}$.

Exercise* 2.33. (a) Given two virtual representations V, W,

$$(V, W) = \dim \mathrm{Hom}_G(V, W)$$

is true because $\mathrm{Hom}_G(V, W)$ is the set of G-module maps from V to W, whose dimension is, from Schur's lemma, the Hermitian inner product.

If $V = \sum_i a_i U_i$ and $W = \sum_i b_i U_i$, where U_i are irreducible representations, then

$$(V, W) = \sum_i \overline{a_i} b_i.$$

(b) True because coefficients must be integers.

(c)

$$(W, V^* \otimes U) = \frac{1}{|G|} \sum_{g \in G} \overline{\chi_W(g) \chi_V(g)} \chi_U(g) = (V \otimes W, U).$$

If this happens, then

$$\dim W \leq \dim V^* \otimes U = \dim V \dim U.$$

Exercise* 2.34. Consider any $h \in G$

$$h^{-1} \cdot L(hv) = \frac{1}{|G|} \sum_{g \in G} h^{-1} g^{-1} \cdot L_0(gh \cdot v) = L(v),$$

because gh is just a permutation of g. Therefore L is G-module map, which, per Schur's lemma, is $\lambda \delta_{VW} \cdot \mathrm{id}$.

If $V \cong W$, λ can be calculated from trace because $L = \lambda \cdot \mathrm{id}$:

$$\begin{aligned} \lambda &= \frac{\mathrm{tr}(L)}{\dim(V)} \\ &= \frac{1}{|G| \dim(V)} \sum_{g \in G} \mathrm{tr}(g^{-1} L_0 g) \\ &= \frac{1}{|G| \dim(V)} \sum_{g \in G} \mathrm{tr}(L_0) \\ &= \frac{\mathrm{tr}(L_0)}{\dim(V)}. \end{aligned} \tag{2.18}$$

Proposition 2.27. *Any finite representation can be represented as a unitary matrix.*

Proof. Irreducible representations are represented by unitary matrices: we have shown here (1.14) that for any finite representation, we can construct a Hermitian inner product such that

$$\mathbf{G}^\dagger \mathbf{H} \mathbf{G} = \mathbf{H}.$$

We can also perform Cholesky decomposition

$$\mathbf{H} = \mathbf{L}\mathbf{L}^\dagger,$$

where $\mathbf{L}$ is a invertible lower triangular matrix.

Therefore, the automorphism G can also be represented as a unitary matrix $\mathbf{U}$:

$$\mathbf{U} = \mathbf{L}^\dagger \mathbf{G} (\mathbf{L}^{-1})^\dagger,$$

such that $\mathbf{U}^\dagger \mathbf{U} = \mathbf{I}$ ($\mathbf{U}$ is invertible because so is $\mathbf{G}$). □

Corollary 2.28. *Any irreducible representation can be uniquely represented as a unitary matrix (up to a scalar factor of root of unity).*

Proof. The Hermitian inner product and the Cholesky decomposition are unique.

All elements have the same "phase" because it comes from $\mathbf{L}$, not $\mathbf{G}$. □

Corollary 2.29. *Any irreducible representation can be uniquely represented as a unitary matrix if the identity element in the group is represented as identity matrix.*

Exercise* 2.35. Represent all irreducible representations as unitary matrices. Rewrite 2.34 into matrix form:

$$\frac{1}{|G|} \sum_{g \in G} \mathbf{G}(g^{-1}; W) \mathbf{L} \mathbf{G}(g; V) = \delta_{VW} \frac{\operatorname{tr}(\mathbf{L})}{\dim(V)} \mathbf{I}. \tag{2.19}$$

Since the representation is homomorphic and unitary, it becomes (in scalar form):

$$\frac{1}{|G|} \sum_{g \in G} \sum_{k=1}^{\dim(W)} \sum_{l=1}^{\dim(V)} \overline{G_{ki}(g; W)} L_{kl} G_{lj}(g; V) = \delta_{VW} \frac{\operatorname{tr}(\mathbf{L})}{\dim(V)} \delta_{ij}. \tag{2.20}$$

Now let $\mathbf{L}$ be a single-entry matrix with the nonzero entry at position rs, i.e.,

$$L_{kl} = \delta_{kr} \delta_{ls}.$$

Then,

$$\frac{1}{|G|}\sum_{g\in G}\overline{G_{ri}(g;W)}G_{sj}(g;V)=\delta_{VW}\frac{\delta_{rs}}{\dim(V)}\delta_{ij}. \tag{2.21}$$

Therefore, the matrix entries of these representations $G_{sj}(g;V)$ are orthogonal.

Since (2.19)

$$|G|=\sum_i \dim\left(V_i\right)^2,$$

these entries form a complete orthogonal basis set.

$$\{\sqrt{\dim(V)}G_{ij}(g;V)\}$$

should form a orthonormal basis set given the Hermitian inner product (2.11).

Exercise* 2.36. $V_1\boxtimes V_2$ is irreducible *if and only if* V_1 and V_2 are irreducible.

Proof.

$$\begin{aligned}(\chi_{V_1\boxtimes V_2},\chi_{V_1\boxtimes V_2}) &= \frac{1}{|G_1\times G_2|}\sum_{g_1\times g_2\in G_1\times G_2}\overline{\chi_{V_1\boxtimes V_2}(g_1\times g_2)}\chi_{V_1\boxtimes V_2}(g_1\times g_2)\\ &= \frac{1}{|G_1|\,|G_2|}\sum_{g_1\in G_1}\sum_{g_2\in G_2}\overline{\chi_{V_1}(g_1)\chi_{V_2}(g_2)}\chi_{V_1}(g_1)\chi_{V_2}(g_2)\\ &= \left(\chi_{V_1},\chi_{V_1}\right)\left(\chi_{V_2},\chi_{V_2}\right).\end{aligned}$$

Since Hermitian inner product is positive integer, QED. □

Definition (faithful representation)**.** If a representation $\rho\colon G\to \mathrm{GL}(V)$ is injective, it is called **faithful**.

Proposition 2.30. *The following statements are equivalent for representations of a finite group*

- *A representation is faithful.*
- $\chi(g)=\chi(e)\iff g=e$.
- *The normal subgroup of trivial representations contains only the identity.*

Proof. If a representation is not faithful, i.e., if $\rho(g)=\rho(h)$ for $g\neq h$, then $\rho(gh^{-1})=\mathrm{id}$ but $gh^{-1}\neq e$ (otherwise $g=h$).

Reversely, if $\rho(g)=\mathrm{id}$ for $g\neq e$, then $\rho(h)=\rho(gh)$ and $h\neq gh$.

Since eigenvalues of the representation of a finite group must be roots of unity (otherwise the group would be infinite) and any group element can be represented as a unitary matrix (and therefore diagonalizable) (see 2.27),

$$\chi(g) = \chi(e) = \dim(V)$$

is true if and only if

$$\rho(g) = \mathrm{id}\,.$$

□

Exercise* 2.37. Any irreducible representation is contained in some tensor power of a faithful representation.

Proof. Let V be the faithful representation and U be the irreducible representation. Then let $a_n = (\chi_U, \chi_{V^{\otimes n}}) = (\chi_U, \chi_V^n)$.

Consider the power series

$$\begin{aligned}\sum_{n=1} a_n t^n &= \frac{1}{|G|}\sum_{n=1}^{\infty}\sum_{C} |C|\,\overline{\chi_U(C)}(\chi_V(C))^n t^n \\ &= \frac{1}{|G|}\sum_{C,\chi_V(C)\neq 0} |C|\,\overline{\chi_U(C)}\left[\frac{1}{1-\chi_V(C)t} - 1\right].\end{aligned} \tag{2.22}$$

Since $\chi_V(e) \neq 0$, $\chi_U(e) \neq 0$, $|[e]| \neq 0$, it is nonzero when $C = [e]$.

Also, $\chi_V(C) = \dim(V)$ only for $C = [e]$ (2.30), therefore other terms cannot cancel out the $[e]$ term.

In conclusion, the right-hand side is a nontrivial rational function of t; in particular a_n cannot be zero for all positive n. □

Definition (support)**.** Given an algebraic structure M with (additive) identity, denoted 0_M, the (set-theoretic) **support** of a function $f\colon X \to M$, where X is a set, is the set

$$\mathrm{supp}(f) = \{\, x \in X \mid f(x) \neq 0_M \,\}\,.$$

Definition (group ring)**.** Let G be a group, written multiplicatively, and let R be a ring. The **group ring** of G over R, denoted $R[G]$, is the set of mappings $f\colon G \to R$ of finite support. For $g \in G$, $r \in R[G]$, and $s \in R[G]$,

$$\begin{aligned}(r+s)(g) &= r(g) + s(g), \\ (rs)(g) &= \sum_{h\in\mathrm{supp}(r)} r(h)s(h^{-1}g).\end{aligned} \tag{2.23}$$

Remark. $r + s$ has finite support as both r and s have finite support.

Since both r and s have finite support, the set

$$\{\,(g,h) \mid r(h)s(h^{-1}g) \neq 0\,\} = \{\,(g',h) \mid r(h)s(g') \neq 0\,\},$$

where $g' = h^{-1}g$ (because the left action of h^{-1} is bijective), is the Cartesian product of two supports. Therefore, rs has finite support.

Remark. The group ring is also a free module, with scalar product defined as ($\alpha \in R$)

$$(\alpha \cdot r)(g) = \alpha \cdot (r(g)).$$

Obviously the product defined this way has finite support.

The basis of the module is the image set of e

$$E = \{\,e(g) \in R[G] \mid g \in G\,\},$$

where $e\colon G \to R[G]$ is a group homomorphism (easy to show from the definition of multiplication in group ring) such that $e(g)(h) = \delta_{gh}$.

Any element r in the group ring can be represented uniquely as a finite sum

$$r = \sum_{g \in \operatorname{supp}(r)} r(g) \cdot e(g).$$

Remark. The multiplicative unity in the group ring is $e(1_G)$ where 1_G is the unity in G.

Definition (center of a ring)**.** The **center of a ring** R is the subring $\mathrm{Z}(R)$

$$\{\,r \in R \mid \forall s \in R[rs = sr]\,\}.$$

Proposition 2.31. *The center of a group ring over a commutative ring is the set of class functions with finite support.*

Proof. Given $r \in R(G)$, $r \in \mathrm{Z}(R(G))$ is equivalent to that

$$\begin{aligned} rs &= \left[\sum_{g \in \operatorname{supp}(r)} r(g) \cdot e(g)\right]\left[\sum_{h \in \operatorname{supp}(s)} s(h) \cdot e(h)\right] \\ &= \left[\sum_{h \in \operatorname{supp}(s)} s(h) \cdot e(h)\right]\left[\sum_{g \in \operatorname{supp}(r)} r(g) \cdot e(g)\right] = sr \end{aligned} \tag{2.24}$$

holds for any $s \in R(G)$.

Especially, when $s = e(h)$ for any $h \in G$, we can multiply $e(h^{-1})$ on the left of (2.24):

$$\sum_{g \in \mathrm{supp}(r)} r(g)e(h^{-1}gh) = \sum_{g \in \mathrm{supp}(r)} r(g)e(h^{-1}hg) = \sum_{g \in \mathrm{supp}(r)} r(g)e(g). \tag{2.25}$$

Let $g' = h^{-1}gh$, then

$$\sum_{hg'h^{-1} \in \mathrm{supp}(r)} r(hg'h^{-1})e(g') = \sum_{g \in \mathrm{supp}(r)} r(g)e(g). \tag{2.26}$$

Since $e(g)$ forms the basis set of the group ring, this equality holds if and only if

$$r(hgh^{-1}) = r(g), \forall g \in G.$$

Therefore $\mathrm{Z}(R(G)) \subseteq R_{\mathrm{class}}(G)$, where $R_{\mathrm{class}}(G)$ denotes the set of R-valued class functions on G with finite support.

Next, if $r \in R_{\mathrm{class}}(G)$, then for any $s \in R(G)$ and any $g \in G$,

$$\begin{aligned}
(sr)(g) &= \sum_{h \in \mathrm{supp}(s)} s(h)r(h^{-1}g) \\
&= \sum_{h^{-1}g \in \mathrm{supp}(s)} s(h^{-1}g)r(g^{-1}hg), \\
(rs)(g) &= \sum_{h \in \mathrm{supp}(r)} r(h)s(h^{-1}g) \\
&= \sum_{h \in \mathrm{supp}(r)} r(g^{-1}hg)s(h^{-1}g) \\
&= \sum_{h^{-1}g \in \mathrm{supp}(s)} r(g^{-1}hg)s(h^{-1}g).
\end{aligned} \tag{2.27}$$

Since the ring R is commutative, we have $sr = rs$. □

Corollary 2.32. *The map $\alpha \mapsto \alpha \cdot e(1_G)$ is a ring homomorphism from a commutative ring R to the $\mathrm{Z}(R(G))$*

Proof. Since the conjugacy class of 1_G is a singleton,

$$(\alpha \cdot e(1_G))(g) = \alpha \cdot e(1_G)(g) = \begin{cases} \alpha & g = 1_G \\ 0 & g \neq 1_G \end{cases},$$

therefore this is a class function with finite support, i.e., in the center of $R(G)$. □

Definition (group algebra)**.** If the ring is commutative then the group ring is also referred to as a **group algebra**.

Remark. This is a unital associative algebra (section 3.1.3.1).

Definition (monic polynomial)**.** A **monic polynomial** is a single-variable polynomial (that is, a univariate polynomial) in which the leading coefficient (the nonzero coefficient of highest degree) is equal to 1.

Definition (algebraic integer)**.** An **algebraic integer** is a complex number that is a root of some monic polynomial with integer coefficients.

$\mathbb{C}$ is the union of all number fields because $\mathbb{C}$ is algebraically closed? The set of all quaternions is not a field because the multiplication is non-commutative.

Theorem 2.33. *Given $\alpha \in K$ where K is a (algebraic) number field, α is an **algebraic integer** if and only if there exists a monic polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.*

Theorem 2.34. *The set of all algebraic integers is a commutative subring of $\mathbb{C}$ (or the number field, e.g., $\mathbb{Q}(i)$).*

Proof. TODO □

Proposition 2.35. *If the set of all algebraic integers is denoted $\overline{\mathbb{Z}}$, then*

$$\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}.$$

Proof. Let $c = p/q \in \overline{\mathbb{Z}}$ where $p \in \mathbb{Z}$, $q \in \mathbb{Z}^+$, and p is coprime with q. From the definition of algebraic integer, there exists a monic polynomial of degree n (i.e., $a_n = 1$):

$$f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x],$$

such that $f(c) = 0$.

Apparently $n > 0$, therefore

$$a_0 = -\frac{p^n + \sum_{i=1}^{n-1} a_i p^i q^{n-i}}{q^n}.$$

Because p and q are coprime integers, we have $q \nmid p^n$. But $q \mid \sum_{i=1}^{n-1} a_i p^i q^{n-i}$ (the summation evaluates zero if $n = 1$), resulting in

$$q \nmid \left(p^n + \sum_{i=1}^{n-1} a_i p^i q^{n-i} \right).$$

Therefore, for $a_0 \in \mathbb{Z}$, q must be 1. □

Proposition 2.36. *The complex conjugate of an algebraic integer is an algebraic integer.*

Proof. Given any

$$f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x],$$

we have

$$\overline{f(x)} = \sum_{i=0}^{n} \overline{a_i x^i} = \sum_{i=0}^{n} a_i \overline{x^i} = \sum_{i=0}^{n} a_i \overline{x}^i = f(\overline{x}).$$

□

Exercise* 2.38. The dimension of an irreducible representation of a finite group divides the order of the group.

Proof. Denote the group as G, the vector space as V, the irreducible representation as ρ. Given a conjugacy class $C \subseteq G$, construct $\varphi \in \mathrm{End}(V)$ as

$$\varphi = \sum_{g \in C} \rho(g).$$

This is a G-map (2.28). From Schur's lemma,

$$\varphi = \lambda_C \cdot \mathrm{id},$$

where λ_C is a scalar.

We also see that

$$\lambda_C \cdot \dim(V) = \mathrm{tr}(\varphi) = |C| \cdot \chi_V(C).$$

`https://math.stackexchange.com/questions/243221/proofs-that-the-degree-of-an-ir`
TODO □

Exercise* 2.39. TODO

2.4.2 More on Category Theory

Definition (product category)**.** The **product category** $C \times D$ of two categories C and D has:

- as objects:

$$\forall A \in \mathrm{ob}(C) \forall B \in \mathrm{ob}(D)[\exists!(A, B) \in \mathrm{ob}(C \times D)];$$

- as arrows:

  $$\forall f \in \hom_C(A_1, A_2) \forall g \in \hom_D(B_1, B_2)[\exists!(f, g) \in \hom_{C\times D}((A_1, B_1), (A_2, B_2))];$$

- as composition:

  $$[(f_2, g_2) \circ_{C\times D} (f_1, g_1) = (f_2 \circ_C f_1, g_2 \circ_D g_1)];$$

- as identities:

  $$\forall A \in \mathrm{ob}(C) \forall B \in \mathrm{ob}(D)[1_{(A,B)} = (1_A, 1_B)].$$

Definition (multifunctor)**.** A **multifunctor** is a functor whose domain is a product category of n categories. It is called a **bifunctor** if $n = 2$.

Definition (natural transformation)**.** If F and G are functors between the categories C and D, then a **natural transformation** η from F to G is a family of morphisms in category D that satisfies two requirements.

- The natural transformation must associate $\eta_X \in \hom_D(F(X), G(X))$ to every object $X \in \mathrm{ob}(C)$, the former of which is called the **component** of η at X.
- The following diagram must commute $\forall X, Y \in \mathrm{ob}(C), \forall f \in \hom_C(X, Y)$ (If both F and G are contravariant, the vertical arrows in this diagram are reversed.):

$$\begin{array}{ccc} X & & F(X) \xrightarrow{\eta_X} G(X) \\ \downarrow f & & \downarrow F(f) \qquad \downarrow G(f) \\ Y & & F(Y) \xrightarrow{\eta_Y} G(Y) \end{array}$$

This is denoted as $\eta \colon F \to G$ or $\eta \colon F \implies G$. Alternatively, we say the family of morphisms $\eta_X \colon F(X) \to G(X)$ is **natural** in X.

Natural transformation can be viewed as a family of morphisms indexed by a category.

Definition (monoidal category)**.** A **monoidal category** is a category $\mathbf{C}$ equipped with a monoidal structure, consisting of the following:

- a bifunctor $\otimes\colon \mathbf{C}\times\mathbf{C}\to\mathbf{C}$ called the tensor product or monoidal product,
- an object I called the unit object or identity object,
- three natural isomorphisms subject to certain coherence conditions expressing the fact that the tensor operation $\otimes$
  - is *associative*: there is a natural (in each of three arguments $A, B, C \in \mathrm{ob}(\mathbf{C})$) isomorphism α, called associator, with components $\alpha_{A,B,C}\colon A\otimes (B\otimes C)\cong (A\otimes B)\otimes C$,
  - has I as *left and right identity*: there are two natural isomorphisms λ and ρ, respectively called left and right unitor, with components ($A\in\mathrm{ob}(\mathbf{C})$) $\lambda_A\colon I\otimes A\cong A$ and $\rho_A\colon A\otimes I\cong A$.

Definition (center of a monoidal category)**.** The **center of a monoidal category** $(\mathcal{C},\otimes,I)$, denoted $\mathcal{Z}(\mathcal{C})$, is the category whose objects are pairs (A,u) consisting of an object $A\in\mathrm{ob}(\mathcal{C})$ and an isomorphism $u_X\colon A\otimes X\cong X\otimes A$ which is natural in X, such that the following diagram commutes

$$\begin{array}{ccccc} A\otimes(X\otimes Y) & \xrightarrow{\alpha_{A,X,Y}} & (A\otimes X)\otimes Y & \xrightarrow{u_X\otimes 1_Y} & (X\otimes A)\otimes Y \\ \Big\downarrow{\scriptstyle u_{X\otimes Y}} & & & & \Big\downarrow{\scriptstyle \alpha^{-1}_{X,A,Y}} \\ (X\otimes Y)\otimes A & \xleftarrow[\alpha_{X,Y,A}]{} & X\otimes(Y\otimes A) & \xleftarrow[1_X\otimes u_Y]{} & X\otimes(A\otimes Y) \end{array}$$

Test: section 2.1

3 Examples; Induced Representations; Group Algebras; Real Representations

3.1 Examples: $\mathfrak{S}_5$ and $\mathfrak{A}_5$

3.1.1 Main Text

Exercise 3.1. Calculate and show the irreducibility of V and V'.

Proposition 3.1. *One-dimensional representations of $\mathfrak{S}_d$ are trivial on normal subgroups whose quotient group is cyclic and not order 2.*

Proof. This is obvious when the cyclic subgroup is trivial.

If $k > 2$, where k is the order of the cyclic subgroup, denote the 1d representation as U.

All of the non identity elements in the cyclic subgroup correspond to $(12\dots k)$ in $\mathfrak{S}_d$, which is within the same conjugacy class. Therefore they must have the same character in the cyclic subgroup.

A 1d representation must be irreducible, but the only irreducible representation in the cyclic subgroup satisfying such condition is the trivial one.

□

There are no more one-dimensional representations, since these are trivial on normal subgroups whose quotient group is cyclic, and $\mathfrak{A}_5$ is the only such subgroup.

Why: From the decomposition $V \oplus U = \mathbb{C}^5$, we have also $\bigwedge^4 V = \bigwedge^5 \mathbb{C}^5 = U'$, and $V^* = V$.

How is this a perfect paring

$$V \times \bigwedge^3 V \to \bigwedge^4 V.$$

No additional requirement for characters?

Exercise 3.2. (i)

$$V \otimes V - \bigwedge^2 V = (10, 4, 1, 0, 0, 2, 1).$$

(ii)

$$(\chi_{\mathrm{Sym}^2 V}, \chi_{\mathrm{Sym}^2 V}) = \frac{100 + 160 + 20 + 60 + 20}{5!} = 3.$$

(iii)

$$(\chi_{\mathrm{Sym}^2 V}, \chi_U) = (\chi_{\mathrm{Sym}^2 V}, \chi_V) = 1.$$

Exercise 3.3.

$$\begin{aligned} W \otimes W &= (25, 1, 1, 1, 0, 1, 1), \\ \bigwedge^2 W &= (10, -2, 1, 1, 0, -2, 1), \end{aligned} \tag{3.1}$$

TODO

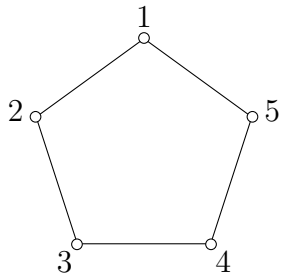
Exercise 3.4. $(a_{1,1}a_{1,2}\dots a_{1,b_1})\dots(a_{k,1}a_{k,2}\dots a_{k,b_k})$ to $(12\dots b_1)\dots(d - b_k + 1\dots d)$

TODO

Exercise* 3.5. TODO

Represent $\mathfrak{A}_5$ or $\mathfrak{S}_5$ as motions of an icosahedron (or, equivalently, of a dodecahedron)

and confirm that Note that the two representations $\mathfrak{A}_5 \to \mathrm{GL}_3(\mathbb{R})$ corresponding to Y and Z have the same image, but (as you can see from the fact that their characters differ only on the conjugacy classes of (12345) and (21345) differ by an *outer* automorphism of $\mathfrak{A}_5$.

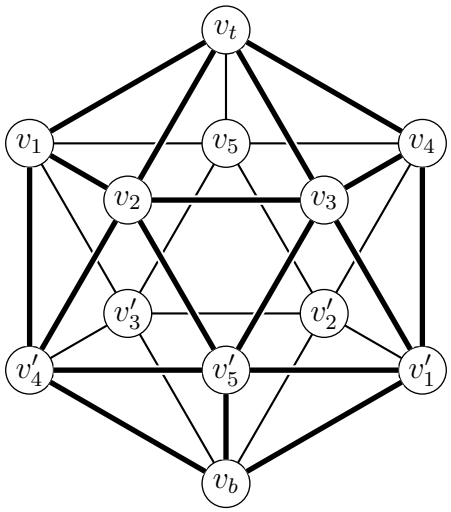


$\mathfrak{A}_5$ can be viewed as a subgroup of I_h point group (and isomorphic to I point group), where (123) correspond to C_3, (12)(34) to C_2, (12345) to C_5, and (21345) $\sim$ (13524) to C_5^2.

I_h point group: `http://symmetry.jacobs-university.de/cgi-bin/group.cgi?group=906&option=4`

I point group:`http://symmetry.jacobs-university.de/cgi-bin/group.cgi?group=905&option=4`

The $\mathfrak{A}_5$ group permutes the diagonals connecting v_i with v_i' in the following icosahedron.



If abc are three neighboring numbers, then (abc) corresponds to the rotation of 60 or 120 degrees along the axis connecting the center of faces (v_t, v_d, v_e) and

(v_b, v'_d, v'_e). Otherwise, it is the rotation along the axis connecting the center of (v_a, v_b, v_c) and (v'_a, v'_b, v'_c).

There are 10 sets of opposite faces and each set have C_3 and C_3^2 rotations. In total, it is 20.

Exercise 3.6. TODO

Definition (dihedral group)**.** The **dihedral group** D_{2n} is defined to be the group of isometries of a regular n-gon in the plane.

Remark. D_{2n} consists of n rotations ($r_0 = e, r_1, \ldots, r_{n-1}$, with r_i meaning counter-clockwise rotation by $\frac{2\pi i}{n}$) and n reflections, $s_0, s_1, \ldots, s_{n-1}$, where the line of symmetry of s_i is rotating $\frac{\pi i}{n}$ counter-clockwise from that of s_0.

Remark. If the order of elements denoting the composition is right to left (e.g., $s_2 s_1$ is the reflection s_1 followed by the reflection s_2), then

$$\begin{aligned} r_i r_j &= r_{(i+j) \bmod n}, \\ r_i s_j &= s_{(i+j) \bmod n}, \\ s_i r_j &= s_{(i-j) \bmod n}, \\ s_i s_j &= r_{(i-j) \bmod n}. \end{aligned} \tag{3.2}$$

From the multiplication rules, the inverses are

$$\begin{aligned} r_i^{-1} &= r_{(-i) \bmod n}, \\ s_i^{-1} &= s_i. \end{aligned} \tag{3.3}$$

Proposition 3.2. *All rotational operations in D_{2n} form a cyclic (and Abelian) group of order n.*

Proposition 3.3. *The conjugacy classes in D_{2n} are*

$$\begin{aligned} [r_i] &= \{\, r_{i'} \in D_{2n} \mid (i - i') \mid n \vee (i + i') \mid n \,\}, \\ [s_i] &= \{\, s_{i'} \in D_{2n} \mid 2 \mid (i - i') \vee 2 \nmid n \,\}. \end{aligned} \tag{3.4}$$

Remark. The rotational operation is only conjugate with its inverse. All reflections are conjugate if n is odd. If n is even, odd-indexed reflections form one conjugacy class and even-indexed ones another.

Proof.

$$r_j r_i r_{-j} = r_i, s_j r_i s_j = s_j s_{i+j} = r_{-j}.$$

$$r_j s_i r_{-j} = s_{i+j} r_{-j} = s_{i-2j}, s_j s_i s_j = r_{j-i} s_j = s_{2j-i}.$$

□

Exercise 3.7. TODO

Exercise 3.8. For any D_{2n}, there is a trivial representation U corresponding the trivial representation of the cyclic group.

There is another representation U' derived from the same trivial representation of the cyclic subgroup, where all reflections are represented as -1. Easy to show this satisfies group homomorphism from (3.2).

If n is even, there is a alternating representation in the cyclic group ($k = \frac{n}{2}$):

$$\chi_V(r_j) = \mathrm{e}^{\frac{2\pi ijk}{n}} = (-1)^j.$$

The representation for reflections could be either

$$\chi_V(s_i) = (-1)^i,$$

or

$$\chi_{V'}(s_i) = (-1)^{i+1}.$$

Easy to show this satisfies group homomorphism from (3.2):

$$\begin{aligned}
\chi(r_i)\chi(r_j) &= (-1)^i(-1)^j = (-1)^{i+j} = \chi(r_{i+j}),\\
\chi(r_i)\chi(s_j) &= (-1)^i(-1)^{j+k} = (-1)^{(i+j)+k} = \chi(s_{i+j}),\\
\chi(s_i)\chi(r_j) &= (-1)^{i+k}(-1)^j = (-1)^{i+j+k-2j} = \chi(s_{i-j}),\\
\chi(s_i)\chi(s_j) &= (-1)^{i+k}(-1)^{j+k} = (-1)^{i+j+2k-2(k+j)} = (-1)^{i-j} = \chi(r_{i-j}).
\end{aligned}$$

where χ could be either χ_V or $\chi_{V'}$ depending on k being 0 or 1.

Such representation does not exist for odd n because the modulo-n operation does not keep the parity if n is odd.

For other representations in the cyclic subgroup, $\chi(r_i) = \overline{\chi(r_{-i})} \neq \chi(r_{-i})$. Therefore, it must be direct sum of two 1-d representations:

$$\rho_k(r_j) = \begin{pmatrix} \mathrm{e}^{\frac{2\pi ijk}{n}} & 0 \\ 0 & \mathrm{e}^{-\frac{2\pi ijk}{n}} \end{pmatrix}.$$

The representation for s_0 is the second Pauli matrix:

$$\rho_k(s_0) = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},$$

which generates representations for other reflections from (3.2):

$$\rho_k(s_j) = \begin{pmatrix} 0 & -i\mathrm{e}^{\frac{2\pi ijk}{n}} \\ i\mathrm{e}^{-\frac{2\pi ijk}{n}} & 0 \end{pmatrix}.$$

Easy to show $\rho_k\colon D_{2n} \to \mathrm{GL}_2(\mathbb{C})$ is group homomorphism from (3.2). Also $\rho_k(r_{n+j}) = \rho_k(r_j), \rho_k(s_{n+j}) = \rho_k(s_j)$ for all $k \in \mathbb{Z}$.

It can be proved that $(\chi_k, \chi_k) = 1$ for $0 < k < n/2$.

If n is odd, let $n = 2m+1$ where $m \in \mathbb{N}$. The character table for D_{2n} is

	1	2	$\dots$	2	$2m+1$
D_{4m+2}	e	r_1	$\dots$	r_m	s_0
U	1	1	$\dots$	1	1
U'	1	1	$\dots$	1	-1
W_1	2	$2\cos\left(\frac{2\pi}{2m+1}\right)$	$\dots$	$2\cos\left(\frac{2m\pi}{2m+1}\right)$	0
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
W_k	2	$2\cos\left(\frac{2k\pi}{2m+1}\right)$	$\dots$	$2\cos\left(\frac{2mk\pi}{2m+1}\right)$	0
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
W_m	2	$2\cos\left(\frac{2m\pi}{2m+1}\right)$	$\dots$	$2\cos\left(\frac{2m^2\pi}{2m+1}\right)$	0

If $n = 2m$ where $m \in \mathbb{Z}^+$, the character table is

	1	2	$\dots$	2	1	m	m
D_{4m}	e	r_1	$\dots$	r_{m-1}	r_m	s_0	s_1
U	1	1	$\dots$	1	1	1	1
U'	1	1	$\dots$	1	1	-1	-1
V	1	-1	$\dots$	$(-1)^{m-1}$	$(-1)^m$	1	-1
V'	1	-1	$\dots$	$(-1)^{m-1}$	$(-1)^m$	-1	1
W_1	2	$2\cos\left(\frac{\pi}{m}\right)$	$\dots$	$2\cos\left(\frac{(m-1)\pi}{m}\right)$	-2	0	0
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
W_k	2	$2\cos\left(\frac{k\pi}{m}\right)$	$\dots$	$2\cos\left(\frac{(m-1)k\pi}{m}\right)$	$2\cdot(-1)^k$	0	0
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
W_{m-1}	2	$2\cos\left(\frac{(m-1)\pi}{m}\right)$	$\dots$	$2\cos\left(\frac{(m-1)^2\pi}{m}\right)$	$2\cdot(-1)^{m-1}$	0	0

Exercise 3.9. (b) Assume $m > 0$.

From 3.29 and 3.30, the following relation is a multiplicative group homomorphism ρ (and another one ρ' if m is even) and thus gives a representation $\mathcal{H} = \mathbb{C}^{2^{\lceil m/2\rceil - 1}}$ (and another one $\mathcal{H}'$ if m is even):

$$H_{2n+1} \subseteq \mathrm{Cl}^{[0]}_{2n+1}(\mathbb{C}) \cong \mathrm{Cl}_{2n}(\mathbb{C}) \cong \mathrm{M}_{2^n}(\mathbb{C}) \supseteq \mathrm{GL}(\mathbb{C}^{2^n}),$$
$$H_{2n} \subseteq \mathrm{Cl}^{[0]}_{2n}(\mathbb{C}) \cong \mathrm{Cl}_{2n-1}(\mathbb{C}) \cong \mathrm{M}_{2^{n-1}}(\mathbb{C}) \oplus \mathrm{M}_{2^{n-1}}(\mathbb{C}) \supseteq 2\,\mathrm{GL}(\mathbb{C}^{2^{n-1}}),$$

where the multiplication by 2 means direct sum.

From 3.44, we know that elements not in the center are paired as $\{\pm\varepsilon_I\}$ in the conjugacy class. Therefore, if $\varepsilon_I \notin \mathrm{Z}(H_m)$, then (since ρ and Tr preserve scalar multiplication)

$$\chi_{\mathcal{H}}(-\varepsilon_I) = \mathrm{Tr}(\rho(-\varepsilon_I)) = -\mathrm{Tr}(\rho(\varepsilon_I)) = -\chi_{\mathcal{H}}(\varepsilon_I),$$

but two sides must be equal because χ is a class function. Therefore

$$\varepsilon_I \notin \mathrm{Z}(H_m) \implies \chi_{\mathcal{H}}(\pm\varepsilon_I) = 0.$$

Similar for $\mathcal{H}'$ if m is even.

We already know from (3.9) that

$$\chi_{\mathcal{H}}(1) = \chi_{\mathcal{H}'}(1) = \dim \mathcal{H} = 2^{\lceil m/2 \rceil - 1}.$$

And from homomorphism:

$$\chi_{\mathcal{H}}(-1) = \chi_{\mathcal{H}'}(-1) = -\chi_{\mathcal{H}}(1) = -2^{\lceil m/2 \rceil - 1}.$$

Therefore, for $m = 2n+1$, (rewrite $\mathcal{H}$ as S and ε_I as v_I)

	1	1	2	…
H_{2n+1}	1	-1	$\pm v_I$	…
S	2^n	-2^n	0	…

This is an irreducible representation because

$$(\chi_S, \chi_S) = \frac{1}{2^{2n+1}}((2^n)^2 + (-2^n)^2) = 1.$$

For $m = 2n$, the pseudoscalar $\varepsilon_{\mathbb{Z}_m}$ is mapped to the pseudoscalar $\varepsilon_{\mathbb{Z}_{m+1}}$ in $H_{2n+1}(\mathbb{C})$ (Can be mapped to $-\varepsilon_{\mathbb{Z}_{m+1}}$ as well?), and therefore the representation can be calculated from (3.9) (assuming ρ takes the upper left block and ρ' the lower right):

$$\rho(\varepsilon_{\mathbb{Z}_m}) = \left[\prod_{i=1}^{2n} \varphi_{2n}(\mathbf{e}_i)\right] i^{n+1} \left[\prod_{i=1}^{2n} \varphi_{2n}(\mathbf{e}_i)\right] = -(-i)^{n+1}\mathbf{I}_{2^{n-1}}.$$

Note that $\rho(\mathbf{e}_{2n}) = i^{n+1}\left[\prod_{i=1}^{2n} \varphi_{2n}(\mathbf{e}_i)\right]$ and

$$i^{n+1}\rho(\varepsilon_{\mathbb{Z}_m}) = \rho(\mathbf{e}_{2n})\rho(\mathbf{e}_{2n}) = -\mathbf{I}_{2^{n-1}}.$$

For lower right block:

$$\rho'(\varepsilon_{\mathbb{Z}_m}) = \left[\prod_{i=1}^{2n} -\varphi_{2n}(\mathbf{e}_i)\right](-i^{n+1})\left[\prod_{i=1}^{2n}\varphi_{2n}(\mathbf{e}_i)\right] = (-i)^{n+1}\mathbf{I}_{2^{n-1}}.$$

Therefore we can calculate the character table (as ρ is homomorphism): (take ρ as S^+, ρ' as S^-, $\varepsilon_{\mathbb{Z}_m}$ as $v_{\{1,\ldots,2n\}}$ and ε_I as v_I)

	1	1	1	1	2	...
H_{2n}	1	-1	$v_{\{1,\ldots,2n\}}$	$-v_{\{1,\ldots,2n\}}$	$\pm v_I$	...
S^+	2^{n-1}	-2^{n-1}	$(-2i)^{n-1}$	$-(-2i)^{n-1}$	0	...
S^-	2^{n-1}	-2^{n-1}	$-(-2i)^{n-1}$	$(-2i)^{n-1}$	0	...

They are irreducible representations because

$$(\chi_{S^-}, \chi_{S^-}) = (\chi_{S^+}, \chi_{S^+}) = \frac{1}{2^{2n}}(4(2^{n-1})^2) = 1.$$

(c) From 3.42 and 3.44, we know that there are $2^{2n}+1$ conjugacy classes for H_{2n+1} and $2^{2n-1}+2$ for H_{2n}. Since the order of H_m is $2\cdot 2^{m-1} = 2^m$ (3.20), all remaining irreducible representations must be one-dimensional because we found

- one 2^n-dimensional irreducible representation for H_{2n+1},

$$2^{2n+1} = 2^{2n}\cdot 1^2 + 1\cdot(2^n)^2,$$

- two 2^{n-1}-dimensional irreducible representations for H_{2n},

$$2^{2n} = 2^{2n-1}\cdot 1^2 + 2\cdot(2^{n-1})^2.$$

Also, the subgroup $\{\pm 1\}$ is in the center of H_m, and therefore a normal subgroup. Therefore, the quotient group $H_m/\{\pm 1\}$ exists. It is a Boolean group (elementary Abelian 2-group) isomorphic to a group $\mathcal{G}(H_m)$ of diagonal matrices with ± 1 diagonal entries and determinant 1 (3.41).

Therefore it has $|H_m/\{\pm 1\}| = 2^{m-1}$ 1-d irreducible representations which are also 1-d representations in H_m because elements in the same conjugacy class are mapped to the same element in the quotient subgroup. In this way, we have found all irreducible representations of H_m.

Given any subset A of $\mathbb{Z}_{m-1}$ (there are 2^{m-1} such subsets), we can construct the character tables (3.36):

	1	1	2	…
H_{2n+1}	1	-1	$\pm v_I$	…
U_A	1	1	$(-1)^{\lvert A\cap I\rvert}$	…
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$
S	2^n	-2^n	0	…

	1	1	1	1	2	…
H_{2n}	1	-1	$v_{\{1,\dots,2n\}}$	$-v_{\{1,\dots,2n\}}$	$\pm v_I$	…
U_A	1	1	$(-1)^{\lvert A\rvert}$	$(-1)^{\lvert A\rvert}$	$(-1)^{\lvert A\cap I\rvert}$	…
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$
S^+	2^{n-1}	-2^{n-1}	$(-2i)^{n-1}$	$-(-2i)^{n-1}$	0	…
S^-	2^{n-1}	-2^{n-1}	$-(-2i)^{n-1}$	$(-2i)^{n-1}$	0	…

We see that $U_\varnothing$ is the trivial representation.
(a) Below are some examples (subscript in concise notation)

	1	1
H_1	1	-1
U	1	1
S	1	-1

	1	1	1	1
H_2	1	-1	$v_{\{1,2\}}$	$-v_{\{1,2\}}$
U	1	1	1	1
U'	1	1	-1	-1
S^+	1	-1	1	-1
S^-	1	-1	-1	1

	1	1	2	2	2
H_3	1	-1	v_{23}	v_{31}	v_{12}
U	1	1	1	1	1
U_1	1	1	1	-1	-1
U_2	1	1	-1	1	-1
$U_3 = U_{12}$	1	1	-1	-1	1
S	2	-2	0	0	0

	1	1	2	2	2	2	2	2	2	2
H_4	1	-1	v_{1234}	$-v_{1234}$	v_{12}	v_{23}	v_{34}	v_{41}	v_{13}	v_{24}
U	1	1	1	1	1	1	1	1	1	1
U_1	1	1	-1	-1	-1	1	1	-1	-1	1
U_2	1	1	-1	-1	-1	-1	1	1	1	-1
U_3	1	1	-1	-1	1	-1	-1	1	-1	1
U_{12}	1	1	1	1	1	-1	1	-1	-1	-1
U_{23}	1	1	1	1	-1	1	-1	1	-1	-1
U_{123}	1	1	-1	-1	1	1	-1	-1	1	-1
S^+	2	-2	$-2i$	$2i$	0	0	0	0	0	0
S^-	2	-2	$2i$	$-2i$	0	0	0	0	0	0

H_5	1	-1	15	25	35	45	12	13	14	23	24	34	235	245	345	12345	1234
{}	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
{1}	1	1	-1	1	1	1	-1	-1	-1	1	1	1	-1	-1	-1	1	-1
{2}	1	1	1	-1	1	1	-1	1	1	-1	-1	1	-1	-1	1	-1	-1
{3}	1	1	1	1	-1	1	1	-1	1	-1	1	-1	-1	1	-1	-1	-1
{4}	1	1	1	1	1	-1	1	1	-1	1	-1	-1	1	-1	-1	-1	-1
{1, 2}	1	1	-1	-1	1	1	1	-1	-1	-1	-1	1	1	1	-1	-1	1
{1, 3}	1	1	-1	1	-1	1	-1	1	-1	-1	1	-1	1	-1	1	-1	1
{1, 4}	1	1	-1	1	1	-1	-1	-1	1	1	-1	-1	-1	1	1	-1	1
{2, 3}	1	1	1	-1	-1	1	-1	-1	1	1	-1	-1	1	-1	-1	1	1
{2, 4}	1	1	1	-1	1	-1	-1	1	-1	-1	1	-1	-1	1	-1	1	1
{3, 4}	1	1	1	1	-1	-1	1	-1	-1	-1	-1	1	-1	-1	1	1	1
{1, 2, 3}	1	1	-1	-1	-1	1	1	1	-1	1	-1	-1	-1	1	1	1	-1
{1, 2, 4}	1	1	-1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	1	1	-1
{1, 3, 4}	1	1	-1	1	-1	-1	-1	1	1	-1	-1	1	1	1	-1	1	-1
{2, 3, 4}	1	1	1	-1	-1	-1	-1	-1	-1	1	1	1	1	1	1	-1	-1
{1, 2, 3, 4}	1	1	-1	-1	-1	-1	1	1	1	1	1	1	-1	-1	-1	-1	1
S	4	-4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

H_6	1	−1	ω	$-\omega$	16	26	36	46	56	12	13	14	15	23	24	25	34	35	45	123456	124566	125566	134566	135566	145566	234566	235566	245566	345566	12345	12346	12356	12456	13456	23456
{}	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
{1}	1	1	−1	−1	−1	1	1	1	1	−1	−1	−1	−1	1	1	1	1	1	1	−1	−1	−1	−1	−1	−1	1	1	1	1	−1	−1	−1	−1	−1	1
{2}	1	1	−1	−1	1	−1	1	1	1	−1	1	1	1	−1	−1	−1	1	1	1	−1	−1	−1	1	1	1	−1	−1	−1	1	−1	−1	−1	−1	1	−1
{3}	1	1	−1	−1	1	1	−1	1	1	1	−1	1	1	−1	1	1	−1	−1	1	−1	1	1	−1	−1	1	−1	−1	1	−1	−1	−1	1	−1	−1	−1
{4}	1	1	−1	−1	1	1	1	−1	1	1	1	−1	1	1	−1	1	−1	1	−1	1	−1	1	−1	1	−1	1	−1	−1	1	−1	−1	−1	1	−1	−1
{5}	1	1	−1	−1	1	1	1	1	−1	1	1	1	−1	1	1	−1	1	−1	−1	1	1	−1	1	−1	−1	1	1	−1	−1	−1	−1	−1	1	−1	−1
{1, 2}	1	1	1	1	−1	−1	1	1	1	1	−1	−1	−1	−1	−1	1	1	1	1	1	1	1	−1	−1	−1	−1	−1	1	1	1	1	−1	−1	−1	−1
{1, 3}	1	1	1	1	−1	1	−1	1	1	−1	1	−1	−1	−1	1	1	−1	−1	1	1	−1	1	1	−1	−1	−1	1	−1	1	1	−1	1	−1	1	−1
{1, 4}	1	1	1	1	−1	1	1	−1	1	−1	−1	1	−1	1	−1	1	−1	1	−1	−1	1	−1	1	−1	1	−1	1	−1	−1	1	−1	1	1	−1	−1
{1, 5}	1	1	1	1	−1	1	1	1	−1	−1	−1	−1	1	1	1	−1	1	−1	−1	−1	1	1	1	−1	−1	−1	−1	1	1	1	1	−1	−1	1	−1
{2, 3}	1	1	1	1	1	−1	−1	1	1	−1	−1	1	1	1	−1	−1	−1	−1	1	1	−1	−1	−1	−1	1	1	1	−1	−1	1	1	−1	−1	1	1
{2, 4}	1	1	1	1	1	−1	1	−1	1	−1	1	−1	1	−1	1	−1	−1	1	−1	−1	1	−1	−1	1	−1	1	−1	1	−1	1	−1	1	−1	1	1
{2, 5}	1	1	1	1	1	−1	1	1	−1	−1	1	1	−1	−1	−1	1	1	−1	−1	−1	1	1	−1	−1	1	1	−1	−1	1	1	−1	−1	1	1	1
{3, 4}	1	1	1	1	1	1	−1	−1	1	1	−1	−1	1	−1	−1	1	1	−1	−1	−1	−1	1	1	−1	−1	1	−1	−1	1	1	−1	−1	1	1	1
{3, 5}	1	1	1	1	1	1	−1	1	−1	1	−1	1	−1	−1	1	−1	−1	1	−1	−1	1	−1	−1	1	−1	−1	1	−1	−1	1	−1	1	−1	1	1
{4, 5}	1	1	1	1	1	1	1	−1	−1	1	1	−1	−1	1	−1	−1	−1	−1	1	1	1	−1	−1	−1	−1	1	1	−1	−1	−1	−1	1	1	1	1
{1, 2, 3}	1	1	−1	−1	−1	−1	−1	1	1	1	1	−1	−1	1	−1	−1	−1	−1	1	−1	1	1	1	1	−1	1	1	−1	−1	−1	−1	1	1	1	1
{1, 2, 4}	1	1	−1	−1	−1	−1	1	−1	1	1	−1	1	−1	−1	1	−1	−1	1	−1	1	−1	1	1	−1	1	1	−1	1	1	−1	−1	−1	−1	1	1	1
{1, 2, 5}	1	1	−1	−1	−1	−1	1	1	−1	1	−1	−1	1	1	−1	−1	1	1	−1	1	−1	−1	1	1	−1	1	1	−1	−1	1	1	−1	−1	1	1
{1, 3, 4}	1	1	−1	−1	−1	1	−1	−1	1	−1	1	1	−1	−1	−1	1	1	−1	−1	1	1	−1	−1	1	1	1	−1	−1	1	−1	1	1	−1	1	1
{1, 3, 5}	1	1	−1	−1	−1	1	−1	1	−1	−1	1	−1	1	−1	1	−1	−1	1	−1	1	−1	1	1	−1	1	−1	1	−1	1	1	−1	1	−1	1	1
{1, 4, 5}	1	1	−1	−1	−1	1	1	−1	−1	−1	1	1	1	−1	−1	−1	1	1	1	−1	1	1	1	−1	−1	−1	1	1	1	1	−1	−1	1	1	1
{2, 3, 4}	1	1	−1	−1	1	−1	−1	−1	1	−1	−1	−1	1	1	1	−1	1	−1	−1	1	1	−1	1	−1	−1	−1	1	1	1	−1	1	1	1	−1	−1
{2, 3, 5}	1	1	−1	−1	1	−1	−1	1	−1	−1	−1	1	−1	1	−1	1	−1	1	−1	1	−1	1	−1	1	−1	1	−1	1	1	1	−1	1	1	−1	−1
{2, 4, 5}	1	1	−1	−1	1	−1	1	−1	−1	−1	1	−1	−1	−1	1	1	−1	−1	1	−1	1	−1	−1	1	1	1	−1	−1	1	1	−1	1	−1	1	−1
{3, 4, 5}	1	1	−1	−1	1	1	−1	−1	−1	1	−1	−1	−1	−1	−1	−1	1	1	1	−1	−1	−1	1	1	1	1	1	−1	1	1	1	−1	−1	−1	−1
{1, 2, 3, 4}	1	1	1	1	−1	−1	−1	−1	1	1	1	1	−1	1	1	−1	1	−1	−1	−1	−1	1	−1	1	1	−1	1	1	1	1	−1	−1	−1	−1	1
{1, 2, 3, 5}	1	1	1	1	−1	−1	−1	1	−1	1	1	−1	1	1	−1	1	−1	1	−1	−1	1	−1	−1	1	1	−1	1	1	−1	1	−1	1	−1	−1	−1
{1, 2, 4, 5}	1	1	1	1	−1	−1	1	−1	−1	1	−1	1	1	−1	1	1	−1	−1	1	1	−1	−1	1	1	−1	1	1	−1	1	−1	−1	−1	1	−1	−1
{1, 3, 4, 5}	1	1	1	1	−1	1	−1	−1	−1	−1	1	1	1	−1	−1	−1	1	1	1	1	1	−1	−1	−1	1	1	1	−1	−1	−1	−1	1	−1	1	−1
{2, 3, 4, 5}	1	1	1	1	1	−1	−1	−1	−1	−1	−1	−1	1	1	1	1	1	1	1	1	−1	−1	−1	−1	−1	−1	1	1	1	1	−1	−1	−1	−1	1
{1, 2, 3, 4, 5}	1	1	−1	−1	−1	−1	−1	−1	−1	1	1	1	1	1	1	1	1	1	1	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1	1	1	1	1	1	1
S_-	4	−4	−4	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S_+	4	−4	4	−4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Exercise 3.10. TODO

Exercise 3.11. TODO

`https://people.maths.bris.ac.uk/~matyd/GroupNames/1/He3.html`

3.1.2 Quadratic Form

Definition (characteristic)**.** The **characteristic** of a ring R, often denoted $\text{char}(R)$, is defined to be the smallest number of times one must use the ring's multiplicative identity (1) in a sum to get the additive identity (0). If this sum never reaches the additive identity the ring is said to have characteristic zero.

Remark. Equivalently, $\text{char}(R)$ of a ring R is the smallest positive number n such that $\underbrace{1 + \cdots + 1}_{n \text{ summands}} = 0$ if such a number n exists, and 0 otherwise.

Definition (quadratic form)**.** A **quadratic form** $Q\colon V \to K$ on a vector space V over a field K of arbitrary characteristic is a map from V to K such that

- $Q(a \cdot v) = a^2 Q(v), \forall a \in K, v \in V$,

- $\Psi\colon V\times V\to K$ defined as $\Psi(u,v)\coloneqq Q(u+v)-Q(u)-Q(v)$ is bilinear.

Ψ is called the **bilinear form associated to** Q.

See more in *Quadratic Forms in Infinite Dimensional Vector Spaces* by Herbert Gross (1979), pp 354–355.

Proposition 3.4. *The bilinear form associated to a quadratic form is a symmetric form, i.e.,* $\Psi(u,v)=\Psi(v,u)$.

Proof. This is true due to the additive commutativity in K and V. □

Proposition 3.5. *Given a symmetric bilinear form* $\Phi\colon V\times V\to K$, $Q\colon V\to K$ *defined as* $v\mapsto\Phi(v,v)$ *is a quadratic form.*

Proof. The first condition holds due to bilinear property of Φ.

The bilinear form Ψ associated to Q is $\Psi(u,v)=\Phi(u+v,u+v)-\Phi(u,u)-\Phi(v,v)=2\Phi(u,v)$ (the last step is a result of bilinear property and symmetric property of Φ) where 2 is defined as $1+1$ in K. □

Remark. This is used to construct quadratic form for a commutative ring as well (see `https://en.wikipedia.org/wiki/Quadratic_form#Generalization`).

Proposition 3.6. *For any field of non-2 characteristic, there is a unique quadratic form whose associated bilinear form is a given symmetric bilinear form.*

Proof. Given a symmetric bilinear form $\Psi\colon V\times V\to K$, where V is a vector field over field K in which $1+1\neq 0$, one can construct $Q\colon V\times V\to K$:

$$Q(v)=(1+1)^{-1}\cdot\Psi(v,v).$$

From the bilinearity of Ψ, we get the first requirement of quadratic form. For the second one, consider

$$Q(u+v)-Q(u)-Q(v)=(1+1)^{-1}\cdot[\Psi(u+v,u+v)-\Psi(u,u)-\Psi(v,v)]=\Psi(u,v).$$

Similar to the proof in 3.5.

If Q' is a quadratic form whose associated bilinear form is Ψ, then

$$\Psi(v,v)=Q'(2v)-2Q'(v)=2\cdot(2-1)Q'(v)=2Q'(v),$$

indicating $Q=Q'$. □

Corollary 3.7. *If* Q *is a quadratic form and* Ψ *is the bilinear form associated to* Q*, then*

$$\Psi(v,v)=(1+1)Q(v).$$

Corollary 3.8. *For a finite-dimensional vector space over a field of characteristic not 2, it suffices to specify the bilinear form on the basis set for uniquely determining a quadratic form.*

Proof. There is always a basis set for a finite dimensional vector field and all elements are represented uniquely as the linear combination of bases. □

3.1.3 Clifford Algebra

3.1.3.1 Definition of Clifford algebra

Definition (unital associative algebra)**.** Let R be a commutative ring. A **unital associative R-algebra** is a ring that is also an R-module in such a way that the ring addition and the module addition are the same operation, and scalar multiplication satisfies

$$r \cdot (xy) = (r \cdot x)y = x(r \cdot y),$$

for all $r \in R$ and $x, y \in A$.

Remark. A unital associative R-algebra A is equipped with three operations:

- ring addition $+\colon A \times A \to A$,
- ring multiplication $\cdot\colon A \times A \to A$,
- scalar multiplication $\cdot\colon R \times A \to A$.

Remark. In the definition, the requirement of R-module is same as the definition of a vector space.

The distributivity axiom for the ring combined with the compatibility with scalars $r \cdot (xy) = (r \cdot x)y = x(r \cdot y)$ consists of additional requirement for an algebra (see `https://en.wikipedia.org/wiki/Algebra_over_a_field#Definition`).

The algebra being a ring means it is unital (the multiplicative identity of the ring) and associative (in terms of ring/algebra multiplication).

Remark. Equivalently, a **unital associative algebra** A is a *ring* together with a *ring homomorphism* from a commutative ring R to the center of A.

Proof. Given a scalar multiplication, one can define such a mapping $\eta\colon R \to A$ as

$$\eta(r) = r \cdot I,$$

where $r \in R$, and I is the multiplicative identity in A.

This is a ring homomorphism:

Distributivity of module multiplication with respect to addition in R
$\eta(r+s) = (r+s)\cdot I = r\cdot I + s\cdot I = \eta(r) + \eta(s)$,
Compatibility of scalar multiplication with multiplication in R
Multiplicative identity in A
Compatibility of scalar multiplication with multiplication in A
$\eta(r\cdot s) = (r\cdot s)\cdot I = r\cdot(s\cdot I) = r\cdot(I\cdot(s\cdot I)) = (r\cdot I)\cdot(s\cdot I) = \eta(r)\cdot\eta(s)$,
Identity element of scalar multiplication
$\eta(1) = 1\cdot I = I$,

where $1 \in R$ is the multiplicative identity of R.

$$\begin{aligned}
(r\cdot I)\cdot x &= r\cdot(I\cdot x) && \text{Identity element of scalar multiplication (left)}\\
&= r\cdot(x\cdot I) && \text{Multiplicative identity in } A\\
&= x\cdot(r\cdot I), && \text{Identity element of scalar multiplication (right)}
\end{aligned}$$

$\forall r \in R, x \in A$. Therefore, $\eta(R) \subseteq \mathrm{Z}(A)$.

In contrast, given a ring homomorphism $\eta\colon R \to \mathrm{Z}(A)$, one can define scalar multiplication $\cdot\colon R \to A$ as

$$r\cdot x = \eta(r)\cdot x,$$

satisfying all axioms of an R-module. For example:

$$\begin{aligned}
(r\cdot s)\cdot x &= \eta(r\cdot s)\cdot x && \text{Definition of scalar multiplication}\\
&= (\eta(r)\cdot\eta(s))\cdot x && \text{Ring homomorphism}\\
&= \eta(r)\cdot(\eta(s)\cdot x) && \text{Multiplicative associativity in } A\\
&= r\cdot(s\cdot x). && \text{Definition of scalar multiplication}
\end{aligned}$$

Others can be done similarly with ring homomorphism, and distributivity or multiplicative identity in A.

The compatibility of scalar multiplication with multiplication in A requires the property of ring homomorphism, multiplicative associativity in A, and the fact that $\eta(r)$ commutes with any element in A. □

Definition (Clifford algebra)**.** Given a vector space V over a field K, equipped with a quadratic form $Q\colon V \to K$, the **Clifford algebra** $\mathrm{Cl}(V, Q)$ is the

quotient algebra of the tensor algebra $T(V)$ by the two-sided ideal I_Q generated by all elements of the form

$$v \otimes v - Q(v) \cdot 1, \forall v \in V,$$

where 1 is the multiplicative identity in $T(V)$.

Remark.

$$I_Q = \{ \sum_{i=1}^{m} x_i \otimes [v_i \otimes v_i - Q(v_i) \cdot 1] \otimes y_i \mid m \in \mathbb{N}, v_i \in V, x_i, y_i \in T(V) \} . \tag{3.5}$$

3.1.3.2 Structure of Clifford algebra

Proposition 3.9. $\mathrm{Cl}(V,Q) \cong K \oplus V \oplus W$, *where* $W = \bigoplus_{n>1} V^{\otimes n}/I_Q$.

Proof. Given any $a, b \in K$, if $a - b \in I_Q$, then all terms must have either x_i or y_i being zero, otherwise there will be second order term $v_i \otimes v_i$. This means $a - b = 0$, i.e., every element in K form a equivalent class (as a singleton) in K/I_Q.

Similar for $v, u \in V$. □

Therefore we can use elements in K and V to represent elements in the subspace of $\mathrm{Cl}(V,Q)$.

Proposition 3.10. *For a finite dimensional vector space V with basis set $(e_i)_{i \in I}$, the basis of* $\mathrm{Cl}(V,Q)$ *is of form*

$$\prod_{i \in I' \subseteq I} e_i = \prod_{i=1}^{|I'|} e_{l_i},$$

given a strict partial order $<$ on I, i.e., $l_1 < l_2 < \cdots < l_{|I'|}$. The product evaluates 1 (the multiplicative identity) if $I' = \varnothing$.

Proof. We have $\bigotimes_{i=1}^{m} e_i$ as the basis of $T(V)$. From 3.12 and 3.13, $e_i \cdot e_j, e_j \cdot c_i, 1$ are linearly dependent, and so are $e_i \cdot e_i, 1$. □

Proposition 3.11. *The dimension of the Clifford algebra on an n-dimensional vector space is 2^n.*

Proof. There is a bijection from the basis set of the Clifford algebra onto the power set of the basis set of the vector space. □

3.1.3.3 Multiplication in Clifford algebra

Proposition 3.12. *For any* $v \in V \subseteq \mathrm{Cl}(V, Q)$, $v^2 = Q(v)$.

Proof. $v^2 - Q(v) \in I_Q$. □

Proposition 3.13. *The anticommutator in* $\mathrm{Cl}(V, Q)$ *is given by*

$$[u, v]_+ = u \cdot v + v \cdot u = \Psi(u, v) \cdot 1, \forall u, v \in V,$$

where $\Psi(u, v) = Q(u + v) - Q(u) - Q(v)$ *is the bilinear form associated to* Q *and* 1 *is the multiplicative identity in* $\mathrm{Cl}(V, Q)$.

Proof. $[u, v]_+ = (u + v)^2 - u^2 - v^2 = Q(u + v) - Q(u) - Q(v) = \Psi(u, v)$. □

3.1.3.4 Grading

3.1.3.4.1 Superalgebra

Definition (graded ring)**.** A **graded ring** is a ring R that is decomposed into a direct sum

$$R = \bigoplus_{n=0}^{\infty} R_n = R_0 \oplus R_1 \oplus R_2 \oplus \cdots$$

of additive groups $R_0, R_1, \ldots$, such that $R_m R_n \subseteq R_{m+n}$ for all nonnegative integers m and n.

Definition (superalgebra)**.** A **superalgebra** is a $\mathbb{Z}_2$-graded algebra.

Let R be a commutative ring, a **superalgebra** A over R is an R-module with direct sum decomposition into two submodules, A_0 and A_1:

$$A = A_0 \oplus A_1,$$

together with a bilinear multiplication $A \times A \to A$ such that

$$A_i A_j \subseteq A_{i+j}, \forall i, j \in \mathbb{Z}_2.$$

Remark. Module + bilinear multiplication are the basic axioms for algebra.

Definition (even subalgebra)**.** The submodule A_0 in above definition forms an ordinary algebra over R, and thus called a **even subalgebra**.

Remark. A_0 is an algebra because $A_0 A_0 \subseteq A_{0+0} = A_0$.

3.1.3.4.2 Division ring

Definition (division ring)**.** A **division ring** is a nonzero ring in which every nonzero element a has a multiplicative inverse.

Remark. A noncommutative division ring is a "noncommutative field". A commutative division ring is a field.

Definition (proper zero divisor)**.** Let $(R, +, \cdot)$ be a ring. A **proper (left) zero divisor** of R is an element $x \in R^*$ such that:

$$\exists y \in R^*[x \cdot y = 0],$$

where R^* is defined as $R \setminus \{ 0 \}$.

Proposition 3.14. *Division ring has no proper zero divisors.*

Proof. See `https://proofwiki.org/wiki/Division_Ring_has_No_Proper_Zero_Divisors`

By definition of division ring $(R, +, \cdot)$, every element $x \in R^* = R \setminus \{ 0 \}$ has an element y such that:

$$y \cdot x = x \cdot y = 1.$$

That is, by definition, every element of R^* is a unit of R. The result follows from *Unit of Ring is not Zero Divisor*. □

Corollary 3.15. *If $a, b \in R$ where R is a division ring and $ab = 0$, then $a = 0$ or $b = 0$.*

Lemma 3.16. *If any $a \in R$, where R is a division ring, satisfies $a^2 = 1$, then $a = 1$ or $a = -1$.*

Proof.

$$\begin{aligned} a^2 = 1 &\iff a^2 + a = a + 1 && \text{Commutative addition} \\ &\iff a(a+1) = 1(a+1) && \text{Multiplicative identity and distributivity} \quad (3.6) \\ &\iff (a-1)(a+1) = 0 && \text{Additive inverse and distributivity} \end{aligned}$$

□

Lemma 3.17. *Given a division ring R whose characteristic is not 2, $2^{-1} + 2^{-1} = 1$.*

Proof.

$$2^{-1} + 2^{-1} = (1+1) \cdot 2^{-1} = 1.$$

□

3.1.3.4.3 Clifford algebra as superalgebra

Lemma 3.18. *Given a field K whose characteristic is not 2, a vector space V over K, and an involutory linear map $f\colon V \to V$, V can be decomposed into eigenspaces of f of eigenvalues 1 and -1.*

Remark. This is to say, if $f \in \mathrm{GL}(V)$ and $f \circ f = \mathrm{id}_V$, then $V = V_1 \oplus V_{-1}$, where V_1 and V_{-1} are K-subspaces: $V_i = \{\, x \in V \mid f(x) = i \cdot x \,\}$.

Proof. Since the characteristic of field K is not 2, any $x \in V$ can be decomposed into

$$x = g(x) + h(x),$$

where $g\colon V \to V$ and $h\colon V \to V$ are endomorphisms given by

$$\begin{aligned} g(x) &= 2^{-1}x + 2^{-1}f(x), \\ h(x) &= 2^{-1}x - 2^{-1}f(x). \end{aligned}$$

They are homomorphisms

- for vector addition: because f is automorphism as well as additive commutativity and distributivity of vector space
- for scalar multiplication: because f is automorphism, compatibility of scalar multiplication with field multiplication, and commutative multiplication in field.

Note that $g(ax) \neq ag(x)$ if K is noncommutative division ring.

Therefore, the images of g and h are subspaces of V:

$$\begin{aligned} U = \mathrm{im}(g) &= \{\, g(x) \in V \mid x \in V \,\}, \\ W = \mathrm{im}(h) &= \{\, h(x) \in V \mid x \in V \,\}. \end{aligned}$$

Next, we show they are eigenspaces. As f is involution and homomorphism and vector addition is commutative, as well as distributivity in vector space, we have

$$\begin{aligned} f(g(x)) &= 2^{-1}f(x) + 2^{-1}x = g(x), \\ f(h(x)) &= 2^{-1}f(x) - 2^{-1}x = -h(x), \end{aligned}$$

indicating $U \subseteq V_1, W \subseteq V_{-1}$.

For any $x \in V_i$, by definition of eigenspace, we have

$$f(x) = ix,$$

therefore

$$2^{-1}x + i2^{-1}f(x) = 2^{-1}(1+i^2)x = x,$$

if $i^2 = 1$, i.e., $i \in \{\, 1, -1 \,\}$. Therefore $U = V_1, W = V_{-1}$.

To conclude the proof, we need to show $U \cap W = \{\, 0 \,\}$. If $v, w \in V$ such that $g(v) = h(w)$, then

$$h(w) = g(v) = f(g(v)) = f(h(w)) = -h(w),$$

indicating $2h(w) = 0$. Since the characteristic of K is not 2, we have $g(v) = h(w) = 0$. □

Remark. An involution might not be an automorphism. For example, $\alpha\colon \mathbb{Z}_2 \to \mathbb{Z}_2$ given by

$$0 \mapsto 1, 1 \mapsto 0,$$

is an involution but not automorphism.

Proposition 3.19. *A Clifford algebra over a field of which characteristic is not 2 is a superalgebra.*

Proof. The linear map on V defined by $v \mapsto -v$ (reflection through the origin) preserves the quadratic form Q and so by the universal property of Clifford algebras (the linear map) extends to an algebra automorphism:

$$\alpha : \mathrm{Cl}(V, Q) \to \mathrm{Cl}(V, Q),$$

i.e., $\forall v_{ij} \in V$,

$$\begin{aligned}
&\alpha(\{\, x \in T(V) \mid \left(x - \sum_{j=1}^{k} \bigotimes_{i=1}^{m_j} v_{ij} \right) \in I_Q \,\}) \\
&= \{\, x \in T(V) \mid \left(x - \sum_{j=1}^{k} \bigotimes_{i=1}^{m_j} (-v_{ij}) \right) \in I_Q \,\}.
\end{aligned}$$

Such α is well-defined bijection because (from (3.5))

$$\left[\sum_{j=1}^{k}\bigotimes_{i=1}^{m_j} v_{ij} - \sum_{j=1}^{k'}\bigotimes_{i=1}^{m'_j} v'_{ij}\right] \in I_Q$$

$$\iff \left[\sum_{j=1}^{k}\bigotimes_{i=1}^{m_j} v_{ij} - \sum_{j=1}^{k'}\bigotimes_{i=1}^{m'_j} v'_{ij}\right] = \sum_{i=1}^{m} x_i \otimes [v_i \otimes v_i - Q(v_i)\cdot 1] \otimes y_i$$

$$\iff \left[\sum_{j=1}^{k}\bigotimes_{i=1}^{m_j} (-v_{ij}) - \sum_{j=1}^{k'}\bigotimes_{i=1}^{m'_j} (-v'_{ij})\right] = (-1)^2 \sum_{i=1}^{m} x'_i \otimes [v_i \otimes v_i - Q(v_i)\cdot 1] \otimes y'_i$$

$$\iff \left[\sum_{j=1}^{k}\bigotimes_{i=1}^{m_j} (-v_{ij}) - \sum_{j=1}^{k'}\bigotimes_{i=1}^{m'_j} (-v'_{ij})\right] \in I_Q$$

Since α is an involution (i.e., it squares to the identity) one can decompose $\mathrm{Cl}(V,Q)$ into positive and negative eigenspaces of α:

$$\mathrm{Cl}(V,Q) = \mathrm{Cl}^{[0]}(V,Q) \oplus \mathrm{Cl}^{[1]}(V,Q), \tag{3.7}$$

where

$$\mathrm{Cl}^{[i]}(V,Q) = \{\, x \in \mathrm{Cl}(V,Q) \mid \alpha(x) = (-1)^i x \,\}, \forall i \in \mathbb{Z}. \tag{3.8}$$

Note that $[i] \in \mathbb{Z}_2$.

Given $x \in \mathrm{Cl}^{[i]}(V,Q)$ and $y \in \mathrm{Cl}^{[i]}(V,Q)$, since α is homomorphism and the algebra multiplication is compatible with scalar multiplication,

$$\alpha(xy) = \alpha(x)\alpha(y) = ((-1)^i x)((-1)^j y) = (-1)^{i+j}(xy).$$

Therefore, $xy \in \mathrm{Cl}^{[i+j]}(V,Q)$, i.e.,

$$\mathrm{Cl}^{[i]}(V,Q)\,\mathrm{Cl}^{[j]}(V,Q) \subseteq \mathrm{Cl}^{[i+j]}(V,Q).$$

□

Proposition 3.20. *The dimensionality of the even subalgebra of a Clifford algebra* $\mathrm{Cl}(V,Q)$ *generated by an* n*-dimensional vector space* V *(*$n > 0$*) is* 2^{n-1}.

Proof. By binomial theorem, the dimensionality of the even subalgebra is (because $n > 0$)

$$\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2k} = \frac{1}{2}\left[\sum_{i=0}^{n}\binom{n}{i} + \sum_{i=0}^{n}(-1)^i\binom{n}{i}\right] = \frac{1}{2}[(1+1)^n + (1+(-1))^n] = 2^{n-1}.$$

□

3.1.4 Special Clifford Algebras

3.1.4.1 Finite real and complex Clifford algebras Given a field K, an n-dimensional K-vector space V, with basis set $(e_1, e_2, \ldots, e_n)$, and the quadratic form $Q\colon V \times V \to K$:

$$Q\left(\sum_{i=1}^{n} x_i e_i\right) = \sum_{i=1}^{p} x_i^2 - \sum_{j=1}^{q} x_{p+j}^2,$$

the Clifford algebra $\mathrm{Cl}(V, Q)$ is denoted $\mathrm{Cl}_{p,q}(K)$.

Such a (finite) basis set can always be found for $K = \mathbb{R}$ by orthogonal diagonalization as long as Q is nondegenerate.

If $K = \mathbb{C}$, and Q nondegenerate, then q can always be set to zero by choosing appropriate basis set (multiplying by i).

See more: `https://en.wikipedia.org/wiki/Classification_of_Clifford_algebras#Classification`

`https://en.wikipedia.org/wiki/Clifford_algebra#Examples:_real_and_complex_Clifford_algebras`

3.1.4.2 Clifford algebras of negative quadratic form Given a field K of which the characteristic is not 2, one can construct a Clifford algebra $C_n = \mathrm{Cl}(V, Q)$, where $V = K^n$ is an n-dimensional K-vector space, with basis set $(e_1, e_2, \ldots, e_n)$, and the quadratic form $Q\colon V \times V \to K$ is given by its associated bilinear form $\Psi\colon V \times V \to K$,

$$\Psi(e_i, e_j) = -2\delta_{ij}.$$

Proposition 3.21. $e_i^2 = -1, e_i e_j = -e_j e_i$ *if* $i \neq j$.

Proposition 3.22. $\left(\sum_{i=1}^{n} x_i e_i\right)^2 = -\sum_{i=1}^{n} x_i^2$.

Proposition 3.23. $C_n = \mathrm{Cl}_{0,n}(K)$.

Proposition 3.24. $C_0(K) \cong K$.

Proposition 3.25. $C_1(\mathbb{R}) \cong \mathbb{C}$.

Proof. $e_1 \cong i$. □

Proposition 3.26. $C_2(\mathbb{R}) \cong \mathbb{H}$, *where* $\mathbb{H}$ *is the set of quaternions.*

Proof. $e_1 \cong i, e_2 \cong j, e_1 e_2 \cong k$. □

Proposition 3.27. $C_3(\mathbb{R}) \cong \mathbb{H} \oplus \mathbb{H}$.

Proof. TODO □

Proposition 3.28. $C_3^{[0]}(\mathbb{R}) \cong \mathbb{H}$.

Proof. $1 \cong 1, e_2e_3 \cong i, e_3e_1 \cong j, e_1e_2 \cong k$. □

See *Linear Algebra and its Applications* Volume 128, January 1990, Pages 51–63. *Matrix representations of Clifford algebras* by Gerald N. Hile and Pertti Lounesto.

Theorem 3.29.

$$\mathrm{Cl}_{2n}(\mathbb{C}) \cong \mathrm{M}_{2^n}(\mathbb{C}), \mathrm{Cl}_{2n+1}(\mathbb{C}) \cong \mathrm{M}_{2^n}(\mathbb{C}) \oplus \mathrm{M}_{2^n}(\mathbb{C}).$$

The isomorphism can be represented as the algebra homomorphism $\varphi_m\colon \mathrm{Cl}_{0,m}(\mathbb{C}) \to \mathrm{M}_{2^{\lceil m/2 \rceil}}(\mathbb{C})$*, which is given recursively: (the* $\prod$ *evaluates 1 if* $n = 0$*)*

$$\begin{aligned}
\varphi_m(1) &= \mathbf{I}_{2^{\lceil m/2 \rceil}}, \\
\varphi_{2n+1}(\mathbf{e}_j) &= \begin{pmatrix} \varphi_{2n}(\mathbf{e}_j) & 0 \\ 0 & -\varphi_{2n}(\mathbf{e}_j) \end{pmatrix}, \forall j \in \mathbb{Z}_{2n}, \\
\varphi_{2n+1}(\mathbf{e}_{2n+1}) &= i^{n+1} \begin{pmatrix} \prod_{j=1}^{2n} \varphi_{2n}(\mathbf{e}_j) & 0 \\ 0 & -\prod_{j=1}^{2n} \varphi_{2n}(\mathbf{e}_j) \end{pmatrix}, \\
\varphi_{2n+2}(\mathbf{e}_j) &= \varphi_{2n+1}(\mathbf{e}_j), \forall j \in \mathbb{Z}_{2n+1}, \\
\varphi_{2n+2}(\mathbf{e}_{2n+2}) &= \begin{pmatrix} 0 & \mathbf{I}_{2^n} \\ -\mathbf{I}_{2^n} & 0 \end{pmatrix}.
\end{aligned} \tag{3.9}$$

Remark. Easy to show that

$$\varphi_m(\mathbf{e}_j)\varphi_m(\mathbf{e}_j) = -\mathbf{I}_{2^{\lceil m/2 \rceil}} = \varphi_m(-1), \forall m \in \mathbb{Z}^+, \forall j \in \mathbb{Z}_m.$$

For example,

$$[\varphi_{2n+1}(\mathbf{e}_{2n+1})]^2 = (-1)^{n+1} \operatorname{diag}(\omega, (-1)^2\omega),$$

where

$$\begin{aligned}
\omega &= \prod_{j=1}^{2n} \varphi_{2n}(\mathbf{e}_j) \prod_{j=1}^{2n} \varphi_{2n}(\mathbf{e}_j) \\
&= (-1)^{n(2n-1)} \prod_{j=1}^{2n} [\varphi_{2n}(\mathbf{e}_j)]^2 \\
&= (-1)^{n(2n-1)} (-1)^{2n} \mathbf{I}_{2^n}.
\end{aligned}$$

Therefore,

$$\left[\varphi_{2n+1}(\mathbf{e}_{2n+1})\right]^2 = (-1)^{2n^2+2n+1}\mathbf{I}_{2^{n+1}} = \varphi_{2n+1}(-1).$$

Remark. Examples:

$$\begin{aligned} \varphi_0(1) &= \begin{pmatrix} 1 \end{pmatrix}. \\ \varphi_1(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, &\varphi_1(\mathbf{e}_1) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}. \end{aligned} \tag{3.10}$$

define real/complex/quaternion/Octonion ($\mathbb{O}$, looks like not)? as even sub-algebra

$\mathrm{Cl}_{n+2}(\mathbb{C}) \cong \mathrm{Cl}_n(\mathbb{C}) \otimes \mathrm{Cl}_2(\mathbb{C})$
simple ring/ semisimple/ central simple/ Wedderburn–Artin theorem
pin/spin group
The even subalgebra $\mathrm{Cl}^{[0]}(V, Q)$ of a Clifford algebra is itself isomorphic to a Clifford algebra.

Theorem 3.30.

$$\mathrm{Cl}^{[0]}_{0,n}(\mathbb{C}) \cong \mathrm{Cl}_{0,n-1}(\mathbb{C}).$$

Proof. TODO □

3.1.5 Elementary Abelian Group

Definition (p-group)**.** Given a prime number p, a **p-group** is a group in which the order of every element is a power of p.

Definition (elementary abelian group)**.** Given a prime number p, an **elementary abelian group** (or **elementary abelian p-group**) is an abelian group in which every nontrivial element has order p.

Definition (Boolean group)**.** An elementary abelian 2-group is called a **Boolean group**.

Theorem 3.31. *In general, a (possibly infinite) elementary abelian p-group is a direct sum of cyclic groups of order p.*

`https://en.wikipedia.org/wiki/Elementary_abelian_group`

Corollary 3.32. *The order of finite elementary abelian p-group is power of p.*

`https://proofwiki.org/wiki/Order_of_Boolean_Group_is_Power_of_2`

Theorem 3.33. *Any finite Boolean algebra is isomorphic to the Boolean algebra of the power set of a finite set.*

`https://en.wikipedia.org/wiki/Power_set#Properties`

Proposition 3.34. *Any finite Boolean group $\mathbb{Z}_2^n \cong \mathcal{P}(\mathbb{Z}_n)$ has the character table, given $A, I \subseteq \mathbb{Z}_n$:*

	1	$\dots$
$\mathbb{Z}_2^n$	A	$\dots$
U_I	$(-1)^{\lvert A \cap I \rvert}$	$\dots$
$\vdots$	$\vdots$	$\ddots$

Proof. This is a group homomorphism because

$$\begin{aligned} U_I(A)U_I(B) &= (-1)^{|A\cap I|}(-1)^{|B\cap I|} \\ &= (-1)^{|(A\setminus B)\cap I|+|A\cap B\cap I|}(-1)^{|(B\setminus A)\cap I|+|B\cap A\cap I|} \\ &= (-1)^{|(A\setminus B)\cap I|+|(B\setminus A)\cap I|} \\ &= (-1)^{|(A\triangle B)\cap I|} \\ &= U_I(A\triangle B), \end{aligned}$$

where $\triangle$ is the symmetric difference, the multiplication in the Boolean group.

There is no repeating representations in the table, i.e.,

$$\forall I, J \subseteq \mathbb{Z}_n \exists A \subseteq \mathbb{Z}_n [I \neq J \implies U_I(A) \neq U_J(A)].$$

Since $I \neq J$, $I\triangle J$ must be nonempty. Let A be the singleton of any element in $I\triangle J$ and the above relation holds.

Since there are 2^n ways to pick I, which is equal to the $|\mathbb{Z}_2^n|$, the above table is the complete character table. □

Proposition 3.35. *The set of all subsets with even cardinality of a finite nonempty set of cardinality $n > 0$, without loss of generality, $\mathbb{Z}_n$, forms a Boolean group under symmetric difference and is isomorphic to $\mathcal{P}(\mathbb{Z}_{n-1})$ through*

$$A \mapsto A \setminus \{ n \},$$

where $\{ n \} = \mathbb{Z}_n \setminus \mathbb{Z}_{n-1}$.

Proof. It is obvious to be a Boolean group.

The map is bijective because any set $B \subseteq \mathbb{Z}_{n-1}$ can and can only be mapped by B if $|B|$ is even or $B \cup \{ n \}$ if $|B|$ is odd.

It is group homomorphism because for any sets $A, B \subseteq \mathbb{Z}_n$, we have

$$(A \setminus \{ n \})\triangle(B \setminus \{ n \}) = (A\triangle B) \setminus \{ n \}.$$

□

Corollary 3.36. *The above group has the character table, given $A \subseteq \mathbb{Z}_n$ such that $2 \mid |A|$, and $I \subseteq \mathbb{Z}_{n-1}$:*

	1	$\dots$
$\mathcal{P}^{[0]}(Z_n)$	A	$\dots$
U_I	$(-1)^{\lvert A\cap I\rvert}$	$\dots$
$\vdots$	$\vdots$	$\ddots$

Proof. Because

$$(A \setminus \{ n \}) \cap I = A \cap I.$$

□

Remark. The idea of Boolean group can be generalized into a Boolean algebra.

Consider the subalgebra B_n of diagonal matrices in the matrix algebra $\mathrm{M}_n(\mathbb{F}_2)$, if we assign 0 to False and 1 to True, then matrix addition is XOR, while matrix multiplication is AND.

If we instead assign 1 to False and 0 to True, then matrix addition is "==" or $\iff$, and the matrix multiplication is OR.

Similarly, one can construct diagonal matrices with entries in $\{ 1, -1 \}$. If we assign 1 to False and -1 to True, then matrix multiplication is XOR, element-wise max is AND, and they form a Boolean algebra as does B_n. Additionally, element-wise min is OR.

A Boolean algebra generally has two sets of algebra structure. Below is a table of summarizing it. **The identities are parenthesized after the operations. The identity of Algebra2 $+$ is always that of Algebra $\times$ and the identity of Algebra2 $\times$ is always that of Algebra $+$.** Note that T is True and F is False.

	Algebra $+$	Algebra $\times$	Algebra2 $+$	Algebra2 $\times$
n-tuples of T/F	XOR (F^n)	AND (T^n)	$\iff$	OR
Diagonal $\mathrm{M}_n(\mathbb{F}_2)$	Mat $+$ ($\mathbf{0}$)	Mat $*$ ($\mathbf{I}_n$)	Kronecker δ	max
Diag $\mathrm{M}_n(\{ 1, -1 \})$	Mat $*$ ($\mathbf{I}_n$)	max ($-\mathbf{I}_n$)	Mat $-A * B$	min
Power set $\mathcal{P}(X)$	$\triangle$ ($\varnothing$)	$\cap$ (X)	$(A \cap B) \cup (A \cup B)^c$	$\cup$

Stone's representation theorem for Boolean algebras: **Any Boolean algebra is isomorphic to a subalgebra of some poser set algebra.**

3.1.6 Boolean group and Clifford algebra

3.1.6.1 Group homomorphism to Boolean group Consider the group homomorphism from a multiplicative group in Clifford algebra to a Boolean group.

Given

- a field K of which the characteristic is not 2 (and denote $K \setminus \{0\}$ as K^*),
- an m-dimensional vector space V over K with basis $E = \{ \mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_m \}$,
- and a quadratic form $Q \colon V \times V \to K$ generated by its associated bilinear form $(\mathbf{e}_i, \mathbf{e}_j) \mapsto 2a_i\delta_{ij}$ where $a_i \in K^*$,

the union set of the subspaces spanned by each one of the bases of the Clifford algebra $\mathrm{Cl}(V,Q)$, excluding 0, forms a *multiplicative group*:

$$\{ \left[c \bigotimes_{i=1}^{n} \mathbf{v}_i \right] \in \mathrm{Cl}(V,Q) \mid c \in K^*, n \in \mathbb{N}, \mathbf{v}_i \in E \} \subseteq \mathrm{Cl}(V,Q),$$

or more explicitly (given the two-sided ideal I_Q)

$$\{ \{ \lambda \in T(V) \mid (\lambda - c \bigotimes_{i=1}^{n} \mathbf{v}_i) \in I_Q \} \in \mathrm{Cl}(V,Q) \mid c \in K^*, n \in \mathbb{N}, \mathbf{v}_i \in E \},$$

where $\bigotimes$ evaluates to 1 if $n = 0$. Its cardinality is $2^m(|K| - 1)$.

The group, denoted G_m, can be expressed as (if the algebra multiplication in $\mathrm{Cl}(V,Q)$ is $\cdot$ which can be omitted)

$$G_m = \{ c \prod_{i=1}^{k} \mathbf{e}_{r_i} \mid c \in K^*, k \in [0,m] \cap \mathbb{Z}, 1 \le r_1 < \cdots < r_k \le m \},$$

where $\prod$ evaluates 1 if $k = 0$. Denote $\prod_i \mathbf{e}_{r_i}$ as ε_I if $I = \{ 1 \le r_1 < \cdots < r_k \le m \}$ and $\varepsilon_\varnothing = 1$.

This is a group because it has

- closed multiplication: as
  - $\mathbf{e}_i^2 = a_i \neq 0$,
  - $\mathbf{e}_i \mathbf{e}_j = -\mathbf{e}_j \mathbf{e}_i \neq 0$ if $i \neq j$, which is a basis of $\mathrm{Cl}(V,Q)$;
- multiplicative associativity: because Clifford algebra is associative;
- identity element: since the multiplicative identity 1 in Clifford algebra is itself a nonzero basis of $\mathrm{Cl}(V,Q)$;
- multiplicative inverse: because given any $c \in K^*$ and any ordered index set $I \subseteq \mathbb{Z}_m$

  $$\left(c \prod_{i \in I} \mathbf{e}_i \right)^{-1} = c^{-1} \prod_{i \in I'} a_i^{-1} \mathbf{e}_i,$$

  where I' is the reverse of I.
  If the index set is sorted, $I = \{ 1 \le r_1 < r_2 \cdots < r_k \le m \}$, then

  $$\left(c \prod_{i=1}^{k} \mathbf{e}_{r_i} \right)^{-1} = c^{-1} \prod_{j=k}^{1} a_j^{-1} \mathbf{e}_{r_j} = c^{-1} (-1)^{\frac{k(k-1)}{2}} \prod_{i=1}^{k} a_i^{-1} \mathbf{e}_{r_i},$$

  as a result of $\frac{1}{a_i} \mathbf{e}_i \mathbf{e}_i = 1$.

There is a **group homomorphism** $\mathcal{G}$ from G_m to the group $\mathrm{GL}(m, K)$, which maps elements of form

$$c\prod_{i=1}^{k}\mathbf{e}_{r_i},$$

given $c \in K^*, k \in \mathbb{N}$ and the sorted index set $I = \{\, 1 \leq r_1 < r_2 \cdots < r_k \leq m \,\}$, to a diagonal matrix in $\mathrm{GL}(m, K)$ whose main diagonal is -1 for r_i-th entry and 1 otherwise.

Easy to show this is a group homomorphism, because if r_i-th basis shows up in both multiplicands, it disappears in the product, as shown in $\mathrm{GL}(m, K)$ that $(-1)(-1) = 1$. Similar for other cases.

The image of $\mathcal{G}$ is a Boolean group and $|\mathrm{im}\,\mathcal{G}| = 2^m$.

3.1.6.2 Commutativity Note that G_m is generally noncommutative.

Given $\alpha, \beta \in G_m$ expressed as

$$\alpha = c\varepsilon_A, \beta = c'\varepsilon_B,$$

we consider the relation between $\alpha\beta$ and $\beta\alpha$.

We can always permute A and B while changing signs of c and c' to keep α and β unchanged. Let all elements in $A \cap B$ be on the right hand side of ε_A and left hand side of ε_B, and align them in reverse order, such that they will disappear directly after multiplication without having to permute, then

$$\alpha\beta = \left(cc' \prod_{i \in A \cap B} a_i\right) \varepsilon_{A \triangle B},$$

where $\triangle$ is the "order-keeping" symmetric difference.

Now calculate $\beta\alpha$. First, all elements in $A \cap B$ need to be moved from one end to the other end. Denote $k = |A|, l = |B|, p = |A \cap B|$, then the transposition must be done

$$\sum_{r=1}^{p}(k - r) + \sum_{r=1}^{p}(l - r) = p(k + l) - p(p + 1)$$

times. Also, when switching from $\varepsilon_{A \triangle B}$ to $\varepsilon_{B \triangle A}$, the basis must transpose

$$|A \setminus B|\,|B \setminus A| = (k - p)(l - p)$$

times. Therefore the total transposition is

$$pk + pl - p^2 - p + kl - pk - pl + p^2 = kl - p$$

times. Therefore

$$\beta\alpha = (-1)^{|A||B| - |A \cap B|}\alpha\beta. \tag{3.11}$$

Proposition 3.37. *The cardinality of any conjugacy class in G_m is at most 2.*

Proof. Because after swapping the multiplication order, you get either the original product or it multiplied by -1. □

Corollary 3.38. *The conjugacy classes of G_m are singletons $\{\lambda\}$ for $\lambda \in \mathrm{Z}(G_m)$ and $\{\pm\sigma\}$ for $\sigma \notin \mathrm{Z}(G_m)$.*

3.1.6.3 Center of G_m

Proposition 3.39. *Given any $k \in \mathbb{N}$,*

$$\begin{aligned}\mathrm{Z}(G_{2k}) &= K^* \\ \mathrm{Z}(G_{2k+1}) &= K^* \cup \{\, c \prod_{i=1}^{2k+1} \mathbf{e}_i \mid c \in K^* \,\}.\end{aligned}$$

Proof. From (3.11), we know that $\alpha = c\varepsilon_A$ commutes with other elements in the group G_m if $|A| = 0$ because $|A \cap B| \leq |A| = 0$.

If $|A| = m \neq 0$ where $m = \dim V$, then $|A \cap B| = |B|$, so

$$\beta\alpha = (-1)^{(m-1)|B|}\alpha\beta. \tag{3.12}$$

If m is even, then $m \geq 2$, therefore we can let $|B| = 1$ such that α does not commute with β. However, if m is odd, then α is in the center.

For $0 < |A| < m$, we can let B consist of one element of A (because $|A| > 0$) and one not belonging to A (which can always be done since $|A| < m$), then

$$(-1)^{|A||B|-|A\cap B|} = (-1)^{|A|2-1} = -1 \neq 1. \tag{3.13}$$

□

Corollary 3.40.

$$\mathrm{Z}(\mathrm{Cl}(V,Q)) = \{\, 0 \,\} \cup \mathrm{Z}(G_m).$$

3.1.6.4 Even subalgebra and Boolean group Next, consider the group homomorphism from group in the even subalgebra to a Boolean group.

The subset $G_m^{[0]}$ of G_m, constructed as

$$\begin{aligned}G_m^{[0]} &= G_m \cap \mathrm{Cl}^{[0]}(V,Q) \\ &= \{\, c \prod_{i=1}^{k} \mathbf{e}_{r_i} \mid c \in K^*, k \in [0,m] \cap 2\mathbb{Z}, 1 \leq r_1 < \cdots < r_k \leq m \,\},\end{aligned} \tag{3.14}$$

is also a multiplicative group because the multiplication is closed: $\mathbf{e}_i^2 = a_i \neq 0$, meaning the change of number of basis is always even.

Proposition 3.41. *$\mathcal{G}$ is still a group homomorphism. The image are diagonal matrices with ± 1 diagonal entries and $+1$ determinant.*

Proposition 3.42. *Given any $k \in \mathbb{N}$,*

$$\mathrm{Z}(G^{[0]}_{2k}) = K^* \cup \{\, c \prod_{i=1}^{2k} \mathbf{e}_i \mid c \in K^* \,\},$$
$$\mathrm{Z}(G^{[0]}_{2k+1}) = K^*.$$

Proof. See (3.12) and (3.13). $|B|$ is always even in even subalgebra. and $\prod_{i=1}^{2k+1} \mathbf{e}_i$ is not in the even subalgebra. □

Proposition 3.43. *The cardinality of any conjugacy class in $G^{[0]}_m$ is at most 2.*

Proof. Because it is a subgroup of G_m. □

Corollary 3.44. *The conjugacy classes of $G^{[0]}_m$ are singletons $\{\, \lambda \,\}$ for $\lambda \in \mathrm{Z}(G^{[0]}_m)$ and $\{\, \pm\sigma \,\}$ for $\sigma \notin \mathrm{Z}(G^{[0]}_m)$.*

3.1.6.5 $\mathrm{Cl}_{p,q}$ and Boolean group For $\mathrm{Cl}_{p,q}(K)$, i.e.,

$$Q\left(\sum_{k=1}^{p+q} z_i \mathbf{e}_i\right) = \sum_{i=1}^{p} z_i^2 - \sum_{j=1}^{q} z_{p+j}^2,$$

construct groups

$$H_{p,q} = \{\, c\varepsilon_I \in \mathrm{Cl}_{p,q}(K) \mid c \in \{\, 1, -1 \,\}, I \subseteq \mathbb{Z}_{p+q} \,\},$$

and

$$H^{[0]}_{p,q} = H_{p,q} \cap \mathrm{Cl}^{[0]}_{p,q}(K) = \{\, c\varepsilon_I \in \mathrm{Cl}^{[0]}_{p,q}(K) \mid c \in \{\, 1, -1 \,\}, I \subseteq \mathbb{Z}_{p+q} \,\}.$$

They are groups because

- $\mathbf{e}_i^2 \in \{\, 1, -1 \,\}$,
- $-1 \in \{\, 1, -1 \,\}$,
- $\{\, 1, -1 \,\}$ is a multiplicative group inside K.

$\mathcal{G}$ is still a group homomorphism.
$H^{[0]}_{0,m}$ is H_m in the book (3.9). $\mathcal{G}(H^{[0]}_{0,m})$ is the abelian 2-group in the book.

3.2 Exterior powers of the standard representation of $\mathfrak{S}_d$

Lemma 3.45. *For $d > 1$, the count for even permutations is equal to that of odd permutations in $\mathfrak{S}_d$.*

Proof. For any two elements a, b (since $d = |X| \geq 2$) in the set X being permuted, one can construct a mapping from even permutations to odd permutations by transposition of these two elements.

Any odd permutation has its inverse image by transposition of a and b. Its inverse image is also unique, and therefore the mapping is bijective. QED. □

Proposition in Book 3.12. *Exterior power $\bigwedge^k V$ of standard representation is irreducible.*

Remark.

$$\bigwedge^k \mathbb{C}^d = \bigoplus_{i=0}^{k} \bigwedge^{k-i} V \otimes \bigwedge^i U,$$

but $\bigwedge^i U$ are trivial spaces for $i > 1$ ($\because \dim U = 1$).

Since U is trivial representation, i.e., all group elements are represented as 1 (multiplicative identity), the tensor product of U with any representation does not change the representation.

$\bigwedge^0 W = U$ for any representation W?

For $k = 0$, $\bigwedge^k V = U$ is irreducible. For $k > 0$, both $\bigwedge^k V$ and $\bigwedge^{k-1} V$ are not zero representations, so $\forall 1 \leq k \leq d-1[(\chi, \chi) = 2] \implies$ both of the right hand side are irreducible.

All possible sets B forms the basis for $\bigwedge^k \mathbb{C}^d$. Since $G = \mathfrak{S}_d$ acts on the basis of $\bigwedge^k \mathbb{C}^d$ as permutation (with possible multiplication by 1), from 2.5 we know the character for $g \in G$ in $\bigwedge^k \mathbb{C}^d$ is the number of basis fixed by g. But even if $g(B) = B$, it might permutes it. As transposition change the sign, all odd permutations should be multiplied by -1. Therefore,

$$\chi(g) = \sum_{g(B)=B} \operatorname{sgn} g|_B,$$

where $g|_B$ denotes the permutation of the set B determined by g.

If $k - l = 0$, then $B = C$. If $k - l = 1$, then there are

$$\binom{k}{k-1}\binom{d-k}{1}$$

ways to choose C given a set B. The original equation becomes

$$\frac{1}{d!}\binom{d}{k}\binom{k}{k-1}\binom{d-k}{1}(k-1)!(d-k-1)!=1.$$

Note that when $k=1$, $\bigwedge^k V = V$. This is an extension of 2.18.

Remark. Every irreducible real representation admits an inner product (unique, up to scalars) invariant under the group action (corollary from 1.14).

3.3 Induced representations

3.3.1 Cosets

See the definition in 2.3.2.

Lemma 3.46. *Given subgroup H of group G and $g \in G$, then*

$$g \in gH.$$

Proof. The identity e of G is also in H, therefore $g = ge \in gH$. □

Lemma 3.47. *Given subgroup H of group G, then the union of all left cosets is the original group G.*

Proof. For any $x \in G$ and there exists a left coset xH containing x because 3.46. □

Lemma 3.48. *Given subgroup H of group G and $g \in G$, then*

$$g' \in gH \iff g^{-1}g' \in H \iff (g')^{-1}g \in H.$$

Proof.

$$g' \in gH \iff \exists h \in H[g' = gh] \iff \exists h \in H[g^{-1}g' = h] \iff g^{-1}g' \in H.$$

The second half holds because any element in H has its inverse and $(g^{-1}g')^{-1} = (g')^{-1}g$. □

Lemma 3.49. *There is a bijection from the subgroup to any left coset.*

Proof. Given subgroup H of group G and $g \in G$, there is a mapping $\varphi\colon H \to gH$:

$$\varphi(h) = gh.$$

This is surjective because for any $gh' \in gH$, we have $\varphi(h') = gh'$.

This is injective because if $h \neq h'$, but $\varphi(h) = \varphi(h')$, then $h = g^{-1}gh = g^{-1}\varphi(h) = g^{-1}\varphi(h') = g^{-1}gh' = h'$, which is contradicting.

□

Lemma 3.50. *Given subgroup H of group G, $g \in G$, and a left coset σ, then*

$$g \in \sigma \iff \sigma = gH.$$

Proof. $\sigma = gH \implies g \in \sigma$ due to 3.46.

If $g \in \sigma$, let σ be $g'H$ where $g' \in G$, i.e., $g \in g'H$. Then from 3.48, $(g')^{-1}g \in H$ and $g^{-1}g' \in H$. Hence, for any $x \in G$,

$$\begin{aligned} x \in gH &\iff \exists h \in H[x = gh = g'(g')^{-1}gh] \\ &\implies \exists h \in H \exists h' \in H[x = g'h' \wedge h' = ((g')^{-1}g)h] \\ &\implies x \in g'H, \\ x \in g'H &\iff \exists h' \in H[x = g'h' = gg^{-1}g'h'] \\ &\implies \exists h' \in H \exists h \in H[x = gh \wedge h = (g^{-1}g')h'] \\ &\implies x \in gH. \end{aligned}$$

□

Corollary 3.51. *Given subgroup H of group G and a left coset σ, then*

$$\forall g \in G \forall g' \in G[gH = g'H \iff g^{-1}g' \in H \iff (g')^{-1}g \in H].$$

Proof. Let $\sigma = gH$ and apply 3.50

$$gH = g'H \iff g' \in gH.$$

From 3.48 we get the second half. □

Lemma 3.52. *Different left cosets are disjoint.*

Proof. Given subgroup H of group G and $g \in G$, we have shown in 3.50 that if $x \in gH$, then $xH = gH$.

For any $x \in G \setminus gH$ (if any), if $\exists h, h' \in H[xh = gh']$, then $x = gh'h^{-1} \in gH$ because $h'h^{-1} \in H$. This contradicts with $x \notin gH$. Therefore $xH \cap gH = \varnothing$.

Now we have considered all possible cosets, and they are either same cosets or disjoint cosets. □

Definition (quotient set of group over subgroup)**.** The **quotient set** of a group G over its subgroup H is the set of all left cosets:

$$G/H \coloneqq \{\, gH \in \mathcal{P}(G) \mid g \in G \,\}.$$

Proposition 3.53. *Given H as a subgroup of a group G,*

$$\exists \sigma \in G/H(x \in \sigma \wedge y \in \sigma) \iff x^{-1}y \in H \iff y^{-1}x \in H.$$

Proof. From 3.50,

$$\exists \sigma \in G/H(x \in \sigma \wedge y \in \sigma) \iff \exists \sigma \in G/H(xH = \sigma = yH).$$

Since $xH \in G/H, yH \in G/H$,

$$\exists \sigma \in G/H(xH = \sigma = yH) \iff xH = yH.$$

With 3.51, we finish the proof. □

Definition (left action of group on quotient set)**.** Given group G and its subgroup H, the **left action of G on G/H** is:

$$g(\sigma) = \{\, gg_\sigma \in G \mid g_\sigma \in \sigma \,\},$$

for any $\sigma \in G/H$.

Proposition 3.54. *Given subgroup H of group G,*

$$\forall g \in G \forall \sigma \in G/H \forall g_\sigma \in \sigma [g(\sigma) = (gg_\sigma)H].$$

Proof. Since (3.53)

$$g'_\sigma \in \sigma \wedge g_\sigma \in \sigma \implies g_\sigma^{-1} g'_\sigma \in H,$$

and ($g_\sigma H = \sigma$, 3.50)

$$\forall h \in H \exists g'_\sigma = g_\sigma h \in \sigma (g_\sigma^{-1} g'_\sigma = h),$$

we have

$$\begin{aligned} x \in g(\sigma) &\iff \exists g'_\sigma \in \sigma (gg'_\sigma = x) \\ &\iff \exists h \in H \exists g'_\sigma \in \sigma (gg_\sigma h = x \wedge g_\sigma^{-1} g'_\sigma = h) \\ &\iff \exists h \in H (gg_\sigma h = x) \\ &\iff x \in (gg_\sigma)H. \end{aligned}$$

□

Corollary 3.55. *Given subgroup H of group G and $g, g' \in G$,*

$$g(g'H) = (gg')H.$$

Proof. we have $g' \in g'H$ (3.46), from 3.54 this is proved. □

Corollary 3.56. *The above definition is a valid left action.*

Proof. For any $g_\sigma \in \sigma$, from 3.54 and 3.55

$$g(g'(\sigma)) = g((g'g_\sigma)H) = (g(g'g_\sigma))H = ((gg')g_\sigma)H = (gg')(\sigma).$$

□

Remark. Since $g'(g(\sigma)) = (g'g)(\sigma)$ (3.56), and $g(H) = (ge)H = gH$ (since $e \in H$ and 3.54) there is no ambiguity in writing $g(\sigma)$ as $g\sigma$.

Proposition 3.57. *The left action of a group on the quotient set of the group over its subgroup is a bijection.*

Remark. Given group G and its subgroup H, any $g \in G$ gives rise to a bijection $\alpha(g)\colon G/H \to G/H$.

Proof. Given any $x, y \in G$, if $g(xH) = g(yH)$, then $(gx)H = (gy)H$ (3.55). Therefore $(gy)^{-1}(gx) = y^{-1}x \in H$ (3.51). Applying 3.51 again and we get $xH = yH$. Therefore g is injection.

For any $\sigma \in G/H$, we take $g_\sigma \in \sigma$, $\because g^{-1}g_\sigma \in G, \therefore (g^{-1}g_\sigma)H \in G/H$, then (3.55, 3.50)

$$g((g^{-1}g_\sigma)H) = (g(g^{-1}g_\sigma))H = g_\sigma H = \sigma.$$

Therefore g is a surjection. □

Definition (index)**.** The **index** of a subgroup H in a group G is the number of left cosets of H in G, denoted $|G : H|$ or $[G : H]$ or $(G : H)$.

Remark. By definition, it is the cardinality of G/H.

Proposition 3.58.

$$|G| = |G : H||H|.$$

Proof. Because G is the disjoint union of the left cosets (3.52, 3.47) and because each left coset has the same size as H (3.49), the index is related to the orders of the two groups by the formula. □

Proposition 3.59. *Given a group G and its subgroup H, the product of two cosets $\rho, \sigma \in G/H$ defined as*

$$\{\, xy \in G \mid x \in \rho, y \in \sigma \,\},$$

is a left coset for all $\rho, \sigma \in G/H$ if and only if H is a normal subgroup.

Proof. Let $a \in \rho, b \in \sigma$. Then the element in the product set is $ahbh'$, where $h, h' \in H$. This is a coset if and only if (3.53)

$$\forall h_1, h_2, h_3, h_4 \in H[(ah_1bh_2)^{-1}(ah_3bh_4) \in H].$$

Let $h_1 = h_2 = h_4 = e$, the identity in G (and H), then $b^{-1}h_3b \in H$ is required for all $h_3 \in H$. Since the union of all cosets is G (3.47), this is to say

$$\forall g \in G[ghg^{-1} \in H],$$

where $g = b^{-1}$.

If H is a normal subgroup, then

$$(ah_1bh_2)^{-1}(ah_3bh_4) = h_2^{-1}(b^{-1}(h_1^{-1}h_3)b)h_4 \in H.$$

□

3.3.2 Main Text

Definition (induced representation)**.** Given H as a *subgroup* of group G and representation V of G, if W as a subspace of V is a *subrepresentation* of $\mathrm{Res}^G_H V$, i.e., $\forall h \in H[h(W) = W]$, then

$$\forall g \in G \forall x \in gH \exists h \in H[x(W) = (gh)(W) = g(h(W)) = g(W)].$$

Therefore we define $\sigma = gH$ acting on W as

$$\sigma(W) \coloneqq g(W),$$

for any $g \in \sigma$. Denote the set of all left cosets $\{\, gH \mid g \in G \,\}$ as G/H, then **representation** V is **induced** by W if every element in V can be written *uniquely as a sum* of elements in such translates of W, i.e.,

$$V = \bigoplus_{\sigma \in G/H} \sigma(W).$$

Example in Book 3.13. The left action of G on G/H is:

$$g(\sigma) = (gg_\sigma)H = \{\, gg_\sigma h \in G \mid h \in H \,\},$$

where $\sigma = g_\sigma H \in G/H$.

Its restriction in W (since e_H is the only basis) is:

$$h(H) = (h \cdot 1)H = hH = H \implies h(e_H) = e_H,$$

because $h \in H$ and H has closed multiplication. Therefore W is a subrepresentation of H. It is trivial because $\forall h \in H[h(H) = H]$.

If $\sigma = g_\sigma H$, then

$$\sigma(W) = g_\sigma(W) = \mathbb{C} \cdot e_{g_\sigma(1 \cdot H)} = \mathbb{C} \cdot e_\sigma.$$

Therefore (since all σ's form the basis of V)

$$V = \bigoplus_{\sigma \in G/H} \mathbb{C} \cdot e_\sigma = \bigoplus_{\sigma \in G/H} \sigma(W),$$

which satisfies the definition of induced representation.

Example in Book 3.14. Given a subgroup H of group G, the regular representation R_H of H is a restriction of R_G, i.e.,

$$R_H(h)(e_{h'}) = e_{hh'} = R_G(h)(e_{h'}), \forall h, h' \in H,$$

and therefore a subrepresentation.

Express W as linear combination of bases:

$$W = \bigoplus_{h \in H} \mathbb{C} \cdot e_h.$$

If $g_\sigma \in \sigma \in G/H$, then (the last two equality signs are results of 3.49 and 3.50)

$$\sigma(W) = g_\sigma(W) = \bigoplus_{h \in H} \mathbb{C} \cdot e_{g_\sigma h} = \bigoplus_{g \in g_\sigma H} \mathbb{C} \cdot e_g = \bigoplus_{g \in \sigma} \mathbb{C} \cdot e_g.$$

Then (a result of 3.52 and 3.47)

$$\bigoplus_{\sigma \in G/H} \sigma(W) = \bigoplus_{\sigma \in G/H} \bigoplus_{g \in \sigma} \mathbb{C} \cdot e_g = \bigoplus_{g \in G} \mathbb{C} \cdot e_g = V.$$

Therefore, V is induced by W.

Proposition 3.60. *Given a representation W of H as a subgroup of G, the induced representation V exists and is unique up to isomorphism.*

Proof. Given a subgroup H of group G and a representation of H: $(W, \rho_W \colon H \to \mathrm{GL}(W))$, we can define copies of W by introducing isomorphisms

$$I_H^\sigma(W) = W^\sigma$$

for each $\sigma \in G/H$, with I_H^H being the identity map, i.e.,

$$\begin{aligned} W^H &= W, \\ I_H^H(w) &= w, \forall w \in W. \end{aligned} \tag{3.15}$$

Easy to show composites $I_{\sigma'}^\sigma = I_H^\sigma \circ \left(I_H^{\sigma'}\right)^{-1}$ are also isomorphisms. It is easy to show that the inverse function is given by $\left(I_{\sigma'}^\sigma\right)^{-1} = I_\sigma^{\sigma'}$.

Then the vector space V over the same field can be constructed as

$$V = \bigoplus_{\sigma \in G/H} W^\sigma,$$

and define $P^\sigma \colon V \to W^\sigma$ as the projection from V onto W^σ, and the injection $I_\sigma \colon W^\sigma \to V$.

Next we define some $\varphi \colon G/H \to G$ such that

$$\varphi(\sigma) \coloneqq \begin{cases} e & \sigma = H \\ g_\sigma \in \sigma & \sigma \neq H \end{cases}, \tag{3.16}$$

where e is the identity in G (and H). There might be multiple ways to define φ by picking different g_σ for each coset $\sigma \in G/H$, but we will show they generate isomorphic representations. Now we choose them arbitrarily and fix it in the following discussion.

$\because e \in H, \therefore \varphi(\sigma) \in \sigma$. As a result of (3.50),

$$\varphi(\sigma) H = \sigma. \tag{3.17}$$

Given φ, we **define** $\rho_V \colon G \to \mathrm{GL}(V)$ such that for all $g \in G$ ($\rho_V(g)$ is a linear map because all components are linear maps),

$$\rho_V(g) = \sum_{\sigma \in G/H} I_{\tau_\sigma} \circ I_H^{\tau_\sigma} \circ \rho_W(h_\sigma) \circ I_\sigma^H \circ P^\sigma,$$

where

$$\begin{aligned} \tau_\sigma &= (g\varphi(\sigma))H \in G/H, \\ h_\sigma &= (\varphi(\tau_\sigma))^{-1} g \varphi(\sigma) \in H. \end{aligned}$$

$h_\sigma \in H$ because $g\varphi(\sigma) \in \tau_\sigma$ (3.46) and $\tau_\sigma = \varphi(\tau_\sigma)H$ ((3.17)) and 3.48. Therefore $\rho_W(h_\sigma)$ is well-defined.

We then show ρ_V is a **group homomorphism**.

Since $\tau_\sigma = (g\varphi(\sigma))H = g(\varphi(\sigma)H) = g(\sigma)$ is an action (3.55, (3.17)), for a given $g \in G$, the map $\sigma \mapsto \tau_\sigma$ is a bijection $G/H \to G/H$.

Therefore we can rewrite (use φ_σ as a short notation of $\varphi(\sigma)$ and $g\sigma$ for $g(\sigma)$ (3.3.1)):

$$\begin{aligned} h_\sigma &= \varphi_{g\sigma}^{-1} g \varphi_\sigma, \\ \rho_V(g) &= \sum_{\sigma \in G/H} I_{g\sigma} \circ I_H^{g\sigma} \circ \rho_W(\varphi_{g\sigma}^{-1} g \varphi_\sigma) \circ I_\sigma^H \circ P^\sigma. \end{aligned} \tag{3.18}$$

$$V \xrightarrow{P^\sigma} W^\sigma \xrightarrow{I_\sigma^H} W \xrightarrow{\rho_W(\varphi_{g\sigma}^{-1} g \varphi_\sigma)} W \xrightarrow{I_H^{g\sigma}} W^{g\sigma} \xrightarrow{I_{g\sigma}} V$$

Since P is projection, we have

$$I_{\sigma'}^H \circ P^{\sigma'} \circ I_\sigma \circ I_H^\sigma = \mathrm{id}_W \, \delta_{\sigma\sigma'}.$$

Therefore (bijection + projection),

$$\begin{aligned} \rho_V(g')\rho_V(g) &= \sum_{\sigma' \in G/H} I_{g'\sigma'} \circ I_H^{g'\sigma'} \circ \rho_W(h'_{\sigma'}) \circ I_{\sigma'}^H \circ P^{\sigma'} \\ &\quad \sum_{\sigma \in G/H} I_{g\sigma} \circ I_H^{g\sigma} \circ \rho_W(h_\sigma) \circ I_\sigma^H \circ P^\sigma \\ &= \sum_{\sigma \in G/H} I_{g'g\sigma} \circ I_H^{g'g\sigma} \circ \rho_W(h'_{g\sigma}) \circ \rho_W(h_\sigma) \circ I_\sigma^H \circ P^\sigma. \end{aligned}$$

Since ρ_W is a group homomorphism (also (3.18)),

$$\rho_W(h'_{g\sigma}) \circ \rho_W(h_\sigma) = \rho_W(\varphi_{g'g\sigma}^{-1} g' \varphi_{g\sigma}) \circ \rho_W(\varphi_{g\sigma}^{-1} g \varphi_\sigma) = \rho_W(\varphi_{g'g\sigma}^{-1} g' g \varphi_\sigma)$$

Therefore

$$\rho_V(g')\rho_V(g) = \rho_V(g'g),$$

i.e., ρ_V **is a representation** of G on V.

Next, we show (W, ρ_W) is a **subrepresentation** of (V, ρ_V).

For all $h \in H, w \in W$, the projection returns zero unless σ is H:

$$P^\sigma(w) = w\delta_{H\sigma}. \tag{3.19}$$

Therefore,

$$\begin{aligned}\rho_V(h)(w) &= \sum_{\sigma\in G/H} I_{h\sigma}\circ I_H^{h\sigma}\circ\rho_W(\varphi_{h\sigma}^{-1}h\varphi_\sigma)\circ I_\sigma^H\circ P^\sigma(w).\\ &= I_{hH}\circ I_H^{hH}\circ\rho_W(\varphi_{hH}^{-1}h\varphi_H)\circ I_H^H(w)\end{aligned}$$

But $h\in H$, so $hH=H$ (3.50). From (3.16), we know $\varphi_H=\varphi_{hH}=e$. And I_H^{hH} is identity map (see (3.15)) Therefore,

$$\rho_V(h)(w)=I_H\circ\rho_W(h)(e^{-1}we)=\rho_W(h)(w). \tag{3.20}$$

We then show (V,ρ_V) is the **induced representation**.

For $w\in W$ and $\sigma'\in G/H$, from (3.19) and (3.17) and (3.16) and (3.15),

$$\begin{aligned}\rho_V(\varphi_{\sigma'})(w) &= \sum_{\sigma\in G/H} I_{\varphi_{\sigma'}\sigma}\circ I_H^{\varphi_{\sigma'}\sigma}\circ\rho_W(\varphi_{\varphi_{\sigma'}\sigma}^{-1}\varphi_{\sigma'}\varphi_\sigma)\circ I_\sigma^H\circ P^\sigma(w)\\ &= I_{\varphi(\sigma')H}\circ I_H^{\varphi(\sigma')H}\circ\rho_W(\varphi_{\varphi(\sigma')H}^{-1}\varphi_{\sigma'}\varphi_H)\circ I_H^H(w)\\ &= I_{\sigma'}\circ I_H^{\sigma'}\circ\rho_W(\varphi_{\sigma'}^{-1}\varphi_{\sigma'}e)(w)\\ &= I_H^{\sigma'}(w).\end{aligned} \tag{3.21}$$

Therefore,

$$V=\bigoplus_{\sigma'\in G/H} W^{\sigma'}=\bigoplus_{\sigma'\in G/H}\rho_V(\varphi_{\sigma'})(W)=\bigoplus_{\sigma'\in G/H}\sigma'(W).$$

Finally we prove the **uniqueness**.

If there is another induced representation $(V',\rho_{V'})$, then it must satisfy:

$$V'=\bigoplus_{\sigma\in G/H} W_{V'}^\sigma=\bigoplus_{\sigma\in G/H}\rho_{V'}(\varphi_\sigma)(W),$$

and $\rho_{V'}(\varphi_\sigma)$ is an isomorphism from W onto $W_{V'}^\sigma$ (because $\rho_{V'}(\varphi_\sigma)(W)=W_{V'}^\sigma$ and $\rho_{V'}(\varphi_\sigma)$ is an isomorphism from V' to V').

Since it is direct sum, there exist a unique linear combination for each $v'\in V'$:

$$v'=\sum_{\sigma\in G/H} v'_\sigma=\sum_{\sigma\in G/H}\rho_{V'}(\varphi_\sigma)(w_\sigma),$$

where $v'_\sigma\in W_{V'}^\sigma$ and $w_\sigma=(\rho_{V'}(\varphi_\sigma))^{-1}(v'_\sigma)\in W$.

Then ($\rho_{V'}$ is group homomorphism)

$$\rho_{V'}(g)\rho_{V'}(\varphi_\sigma)=\rho_{V'}(g\varphi_\sigma),$$

and similarly (since W is subrepresentation of V')

$$\rho_{V'}(g\varphi_\sigma) = \rho_{V'}(\varphi_{g\sigma})\rho_{V'}(h_\sigma) = \rho_{V'}(\varphi_{g\sigma})\rho_W(h_\sigma),$$

where h_σ is given in (3.18).

Since (3.17) and 3.54,

$$\varphi_{g\sigma} \in g\sigma = g\varphi_\sigma H,$$

$\therefore h_\sigma = \varphi_{g\sigma}^{-1} g\varphi_\sigma \in H$ (3.48).

.

Unique

□

Example in Book 3.15.

$$W = \bigoplus_i W_i \implies \operatorname{Ind} W = \bigoplus_i \operatorname{Ind} W_i.$$

Exercise 3.16. TODO

(a)

$$U \otimes \operatorname{Ind} W = \operatorname{Ind}(\operatorname{Res}(U) \otimes W).$$

When W is trivial representation, $\operatorname{Ind}(\operatorname{Res}(U)) = U \otimes P$ (3.13).

(b) ...

Proposition in Book 3.17.

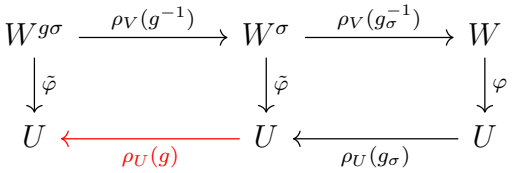
$$\operatorname{Hom}_H(W, \operatorname{Res} U) = \operatorname{Hom}_G(\operatorname{Ind} W, U)$$

Proof. Let $V = \operatorname{Ind} W$, the following diagram commutes (with W^σ denoting $\sigma(W)$)

$$\begin{array}{ccccc} W^\sigma & \xrightarrow{\rho_V(g_\sigma^{-1})} & W & \xrightarrow{\rho_W(h)} & W \\ \downarrow{\scriptstyle \tilde{\varphi}} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi} \\ U & \xleftarrow[\rho_U(g_\sigma)]{} & U & \xleftarrow[\rho_U(h^{-1})]{} & U \end{array}$$

The left part is the definition of $\tilde{\sigma}$. The right part is the fact that φ is H module. The combination shows that such $\tilde{\sigma}$ is independent on the choice of the representative g_σ for any coset σ.

From Equation 3.3.2, we know that any $g \in G$ maps W^σ to $W^{g\sigma}$. Therefore the following diagram commutes



The right half is the definition of $\tilde{\varphi}$ on W^{σ}, the combination is its definition on $W^{g\sigma}$ (note $\rho_V(g_\sigma^{-1}) \circ \rho_V(g^{-1}) = \rho_V((gg_\sigma)^{-1})$ and $gg_\sigma \in (gg_\sigma)H = g\sigma$ (3.46, 3.54) therefore representing $g\sigma$). This proves the left half, i.e., $\tilde{\varphi}$ is G-module. □

Equation in Book 3.18. Given $s \in \sigma$, 3.54 gives $g\sigma = gsH$, and 3.50 gives $\sigma = sH$. Therefore 3.51

$$g\sigma = \sigma \iff gsH = sH \iff s^{-1}gs \in H.$$

Hence

$$\chi_{\operatorname{Ind} W}(g) = \sum_{g\sigma=\sigma} \chi_W(s^{-1}gs).$$

Exercise 3.19. (a) TODO
(b) 3.58, $\chi_W(D_i) = 1$ and $\sum_{i=1}^{r} |D_i| = |C \cap H|$.

Corollary in Book 3.20. *Frobenius Reciprocity*
TODO

Remark. It suffices by linearity to prove this when W and V are irreducible because both Ind and Res are group homomorphisms of representation rings (i.e., preserve direct sum) and because the Hermitian inner product is bilinear when the scalar multiplication only involves integers (as required in representation ring).

Example in Book 3.21.

$$\begin{aligned}(\operatorname{Ind} V_2, U_3) &= (V_2, U_2) = 0,\\ (\operatorname{Ind} V_2, U_3') &= (V_2, V_2) = 1,\\ (\operatorname{Ind} V_2, V_3) &= (V_2, U_2 \oplus V_2) = 1.\end{aligned}$$

Example in Book 3.22.

$$(\operatorname{Ind} V_3, U_4) = (V_3, U_3) = 0,$$

TODO

Exercise 3.23. (i) Since (1234) has order of 4, the subgroup H is

$$\{\, e, (1234), (13)(24), (1432) \,\}.$$

This is a cyclic group, and therefore has four irreducible representations C_0, C_1, C_2, C_3:

	1	1	1	1
H	e	(1234)	$(13)(24)$	(1432)
C_0	1	1	1	1
C_1	1	i	-1	$-i$
C_2	1	-1	1	-1
C_3	1	$-i$	-1	i

From the character table of $\mathfrak{S}_4$ we see that

$$\begin{aligned}
\operatorname{Res} U &= (1,1,1,1) = C_0,\\
\operatorname{Res} U' &= (1,-1,1,-1) = C_2,\\
\operatorname{Res} V &= (3,-1,-1,-1) = C_1 \oplus C_2 \oplus C_3,\\
\operatorname{Res} V' &= (3,1,-1,1) = C_0 \oplus C_1 \oplus C_3,\\
\operatorname{Res} W &= (2,0,2,0) = C_0 \oplus C_2.
\end{aligned}$$

Therefore

$$\operatorname{Ind} C_1 = V \oplus V'.$$

(ii) Denote $\omega = \mathrm{e}^{2\pi i/3}$, then

	1	1	1
H	e	(123)	(132)
C_0	1	1	1
C_1	1	ω	$\overline{\omega}$
C_2	1	$\overline{\omega}$	ω

From the character table of $\mathfrak{S}_4$ we see that

$$\begin{aligned}
\operatorname{Res} U &= (1,1,1) = C_0,\\
\operatorname{Res} U' &= (1,1,1) = C_0,\\
\operatorname{Res} V &= (3,0,0) = C_0 \oplus C_1 \oplus C_2,\\
\operatorname{Res} V' &= (3,0,0) = C_0 \oplus C_1 \oplus C_2,\\
\operatorname{Res} W &= (2,-1,-1) = C_1 \oplus C_2.
\end{aligned}$$

Therefore

$$\operatorname{Ind} C_1 = V \oplus V' \oplus W.$$

Exercise 3.24. TODO

Lemma 3.61. *For U as a representation of group G, $\operatorname{Res} U$ as its restriction in subgroup H is irreducible if and only if the multiplicity of U in $\operatorname{Ind}\operatorname{Res} U$ is 1.*

Proof. Applying Frobenius Reciprocity ($W = \operatorname{Res} U$):

$$\operatorname{Res} U \text{ is irreducible} \iff (\operatorname{Ind}\operatorname{Res} U, U) = (\operatorname{Res} U, \operatorname{Res} U) = 1$$

□

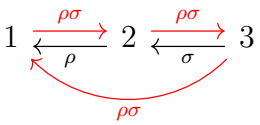
Lemma 3.62.

$$(12) = (21).$$

Lemma 3.63.

$$\begin{aligned} (12) \circ (23) &= (123), \\ (23) \circ (12) &= (321). \end{aligned} \tag{3.22}$$

Proof. Let ρ be the left operand and σ the right. See the followings:

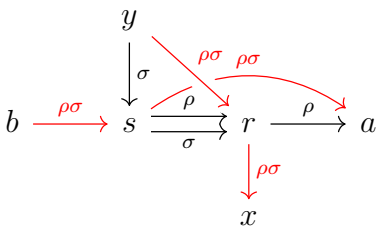


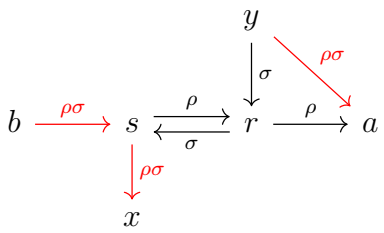
□

Lemma 3.64.

$$\begin{aligned} (ra \ldots bs)(rx \ldots ys) &= (a \cdots bs)(rx \cdots y), \\ (ra \ldots bs)(sx \ldots yr) &= (a \ldots bsx \ldots y). \end{aligned} \tag{3.23}$$

Proof. Let ρ be the left operand and σ the right. See the followings:





□

Remark.

$$\begin{aligned}(145)(26843) &= (514)(43268) = (5143268),\\ (1286347)(529460) &= (7128634)(460529) = (71286)(634)(46)(60529)\\ &= (71286)(34)(60529) = (34)(71286)(60529)\\ &= (34)(712)(286)(6052)(29)\\ &= (34)(8605)(712)(29)\\ &= (34)(8605)(7129).\end{aligned} \tag{3.24}$$

Lemma 3.65. *If a conjugacy class C of group G is disjoint with a subgroup H of G, then*

$$\chi_{\operatorname{Ind} W}(C) = 0,$$

for any representation W of H.

Lemma 3.66. *If a conjugacy class C of group G satisfies $C \subseteq H$ where H is a subgroup of G, then for any representation U of G,*

$$\chi_{\operatorname{Ind}\operatorname{Res} U}(C) = [G : H]\chi_U(C).$$

Proof. By definition of subset and set intersection:

$$C \subseteq H \iff C = C \cap H.$$

Therefore

$$\frac{\chi_{\operatorname{Ind}\operatorname{Res} U}(C)}{[G:H]} = \sum_i \frac{|D_i|}{|C|}\chi_{\operatorname{Res} U}(D_i) = \sum_i \frac{|D_i|}{|C|}\chi_U(C) = \frac{|C \cap H|}{|C|}\chi_U(C) = \chi_U(C).$$

□

Lemma 3.67. $\operatorname{Ind} W$ *is irreducible in G if and only if (by setting $U = \operatorname{Ind} W$ in Frobenius Reciprocity)*

$$(\chi_W, \chi_{\operatorname{Res}\operatorname{Ind} W})_H = 1.$$

Exercise* 3.25. TODO

From 3.61 ($G = \mathfrak{S}_d$, $H = \mathfrak{A}_d$)

$$\operatorname{Res} U \text{ is irreducible} \iff \chi(\operatorname{Ind}\operatorname{Res} U, U) = 1.$$

If C_0 is a class of even permutations (i.e., $\sum(j-1)$ is even, where j is the number of indices in each parenthesis (orbit)), since $C_0 \subseteq H$, then

$$\chi_{\operatorname{Ind}\operatorname{Res} U}(C_0) = 2\chi_U(C_0).$$

If C_1 is a class of odd permutations, since $C_1 \cap H = \varnothing$,then

$$\chi_{\operatorname{Ind}\operatorname{Res} U}(C_1) = 0.$$

Therefore, U is irreducible, if and only if

$$\frac{1}{|G|}\sum_{C_0} 2\,|C_0|\,\overline{\chi_U(C_0)}\chi_U(C_0) = 1.$$

This can be rewritten as

$$(\chi_{W\otimes U}, \chi_U) = 1,$$

where $\chi_W(C_0) = 2, \chi_W(C_1) = 0$, i.e., $W = A \oplus A'$, where A is the trivial representation and A' is the alternating representation.

Therefore $W \otimes U = U \oplus U'$ where $U' = U \otimes A'$. If the Hermitian inner product is 1, U must be irreducible, otherwise $(\chi_U, \chi_U) > 1$. The other condition is $U \neq U'$ (because U' is tensor product of irreducible representation and 1-d representation, and thus a irreducible representation).

In conclusion, $\operatorname{Res} U$ **is irreducible if and only if** U **is irreducible and there is a conjugacy class** C **of odd permutations in** G **such that** $\chi_U(C) \neq 0$**.**

For a representation W of H, $\operatorname{Ind} W$ is irreducible in G if and only if

$$(\chi_W, \chi_{\operatorname{Res}\operatorname{Ind} W})_H = 1.$$

$$\chi_{\operatorname{Res}\operatorname{Ind} W}(C) = \chi_{\operatorname{Ind} W}(C) = 2\sum_i \frac{|D_i|}{|C|}\chi_W(D_i).$$

$$(\chi_W, \chi_{\operatorname{Res}\operatorname{Ind} W})_H = \frac{1}{|H|}\sum_C \sum_j \overline{\chi_W(D_j)} \cdot 2\sum_i \frac{|D_i|}{|C|}\chi_W(D_i).$$

Note that if there are at most 2 D_i's for each C, and they have the same size.

TODO: Should be those irreducible representations with different characters in D_i's (split conjugacy classes)

Remark. Since there are no classes with both even and odd permutations, and the number of even and odd permutations are the same, we have $\sum_{C_0} 2\,|C_0| = \sum_{C_0} |C_0| + \sum_{C_1} |C_1| = |G|$, and hence the Ind Res of trivial representation contains 1 of its copy.

Exercise* 3.26. TODO

Theorem in Book 3.27. *TODO*

Theorem in Book 3.28. *TODO*

3.4 The group algebra

3.4.1 G-module

Given a vector space V over field K, the set of all endomorphisms on V forms a unital associative algebra $(\mathrm{End}(V), +, \cdot, \circ)$. The multiplicative identity is the identity map, id_V.

If we have a group G with a representation $\rho\colon G \to \mathrm{GL}(V)$, the $K[G]$-module $(M, +, \cdot, \circ, *)$ given by this representation is a subalgebra of $\mathrm{End}(V)$ as well as a 1-d free module given by basis (id_V) and scalar multiplication

$$e_g * \mathrm{id}_V = \rho(g),$$

where e_g is the basis of $K[G]$. Due to the distributivity, the scalar multiplication by any element in $K[G]$ is given by

$$\alpha * \mathrm{id}_V = \sum_{g\in G} [a_g \cdot \rho(g)],$$

where $\alpha = \sum_{g\in G} a_g e_g \in K[G]$. By definition of a free module, all elements in the $K[G]$-module M can be uniquely expressed in this way.

If $\alpha = \sum_{g\in G} a_g e_g$, and $\beta = \sum_{h\in G} b_h e_h$, then the scalar multiplication $*\colon K[G] \times M \to M$ can be expressed as

$$\alpha * (\beta * \mathrm{id}_V) = (\alpha\beta) * \mathrm{id}_V = \sum_{g\in G}\sum_{h\in G} [(a_g b_h) \cdot \rho(gh)].$$

The vector addition $+\colon M \times M \to M$ and scalar multiplication by K, $\cdot\colon K \times M \to M$ and composite $\circ\colon M \times M \to M$ are inherited from $\mathrm{End}(V)$. Easy to prove these operations are closed within M and compatible with other operations.

Notably, the multiplicative identity e_e in the group algebra $K[G]$ where e is the identity in G gives the following property:

$$e_e * \mathrm{id}_V = \rho(e) = \mathrm{id}_V,$$

which is why id_V is chosen as the basis.

3.4.2 Regular Representation

Given a field K, the regular representation of a group G is an injection $\rho\colon G \to K[G]$ acting on $K[G]$ by algebra multiplication.

The group homomorphism ρ is given by

$$\rho(g) = e_g,$$

where e_g is the basis in $K[G]$. The left action on $K[G]$ is the algebra multiplication, i.e.,

$$\rho(g)\left(\sum_{h\in G} a_h e_h\right) = e_g\left(\sum_{h\in G} a_h e_h\right) = \sum_{h\in G}\left(a_h e_{gh}\right),$$

for any $\sum_{h\in G} a_h e_h \in K[G]$.

The $K[G]$-module is $K[G]$ itself, with e_e as the basis, i.e., $\mathrm{id}_{K[G]}$. The scalar multiplication $*\colon K[G] \times K[G] \to K[G]$ is the same as the algebra multiplication.

3.4.3 Semisimple Module

Definition (simple modules)**.** The **simple modules** over a ring R are the (left or right) modules over R that are non-zero and have no non-zero proper submodules.

Definition (semisimple module)**.** A module over a (not necessarily commutative) ring is said to be **semisimple** (or completely reducible) if it is the direct sum of simple (irreducible) submodules.

3.4.4 Idempotent

Definition. An **idempotent element**, or simply an idempotent, of a ring is an element a such that $a^2 = a$.

3.4.5 Main Text

The algebra homomorphism to End(V) because 0 is in the group algebra (and GL(V) does not form an algebra).

The image of the algebra homomorphism should also be an algebra, and therefore a ring. This ring form a module over itself. For a specific vector space V, there might be different representation ρ of the group G. TRUE??? TODO...

Then all of the irreducible representations of lower than dim V should form of the basis of the $\mathbb{C}[G]$-module in End(V).

Proposition in Book 3.29.

$$\mathbb{C}[G] \cong \bigoplus_i \mathrm{End}(W_i).$$

Remark. Regular representation is permutation representation, and therefore it is identity map only for e (the identity in group), i.e., faithful representation (2.30). TODO

too many details... TODO

Exercise* 3.30. TODO

Exercise 3.31. See the definition of group ring.

Exercise* 3.32. Fourier transform TODO

Exercise* 3.33. $n \times n$ matrix. TODO

3.5 Real representations and representations over subfields of $\mathbb{C}$

Exercise* 3.34. See 3.9 and 3.8.

	1	1	2	2	2
D_8	e	r_2	r_1	s_0	s_1
U	1	1	1	1	1
U'	1	1	1	-1	-1
V	1	1	-1	1	-1
V'	1	1	-1	-1	1
W_1	2	-2	0	0	0

	1	1	2	2	2
G	1	-1	$\pm i$	$\pm j$	$\pm k$
U	1	1	1	1	1
U_1	1	1	1	-1	-1
U_2	1	1	-1	1	-1
U_3	1	1	-1	-1	1
S	2	-2	0	0	0

Lemma in Book 3.35. *An irreducible representation V of G is real if and only if there is a nondegenerate symmetric bilinear form B on V preserved by G. TODO*

Remark. Since the bilinear form and Hermitian form are nondegenerate, by definition it generates isomorphisms form vector space to dual space.

Since B and H are G-invariant,

$$H(g\varphi(x), gy) = H(\varphi(x), y) = B(x, y) = B(gx, gy) = H(\varphi(gx), gy).$$

Therefore φ is G-module map.

$$H(\varphi(ix), y) = B(ix, y) = iB(x, y) = iH(\varphi(x), y) = H(-i\varphi(x), y).$$

Definition in Book 3.36. TODO **quaternionic representation**

Theorem in Book 3.37. *TODO (1) Complex*
(2) Real
(3) Quaternionic

Exercise 3.38. Irreducible:

$$\frac{1}{|G|}\sum_{g\in G}\chi_V(g^2).$$

If $|G|$ is odd, It also implies that if the order of G is odd, all nontrivial representations must be complex?? because the summation is even? or $\mathrm{Sym}^2 = \bigwedge^2$?

Exercise 3.39. TODO

Exercise 3.40. TODO

Exercise* 3.41. TODO

Exercise* 3.42. TODO

Exercise* 3.43. TODO

3.5.1 Representations over Subfields of $\mathbb{C}$ in General

Exercise* 3.44. TODO

Exercise* 3.45. TODO

4 Representations of $\mathfrak{S}_d$: Young Diagrams and Frobenius's Character Formula

4.1 Statements of the results

4.1.1 Partition Function

Definition (partition function)**.** The **partition function** $p(d)$ of d the number partitions of d: $d = \lambda_1 + \cdots + \lambda_k$, where $\lambda_1 \geq \cdots \geq \lambda_k \geq 1$.

Remark. Let $p_k(d)$ be the number of partitions of d with integers no less than k, then $p(d) = p_1(d)$.

We can derive the recursive relation: $p_k(d) = p_{k+1}(d) + p_k(d-k)$ because the number of partitions with some k's is $p_k(d-k)$ and the number of partitions without any k's is $p_{k+1}(d)$.

`https://en.wikipedia.org/wiki/Partition_function_(number_theory)#Generating_function`

$$\sum_{n=0}^{\infty} p(n)x^n = \prod_{k=1}^{\infty}\left(\frac{1}{1-x^k}\right) = \prod_{k=1}^{\infty}\sum_{j=0}^{\infty} x^{kj}.$$

The equality between the products on the first and second lines of this formula is obtained by expanding each factor $1/(1-x^k)$ into the geometric series. To see that the expanded product equals the sum on the first line, apply the distributive law to the product. This expands the product into a sum of monomials of the form $x^{a_1}x^{2a_2}x^{3a_3}\cdots$ for some sequence of coefficients a_i, only finitely many of which can be non-zero. The exponent of the term is $n = \sum ia_i$, and this sum can be interpreted as a representation of n as a partition into a_i copies of each number i. Therefore, the number of terms of the product that have exponent n is exactly $p(n)$, the same as the coefficient of x^n in the sum on the left. Therefore, the sum equals the product.

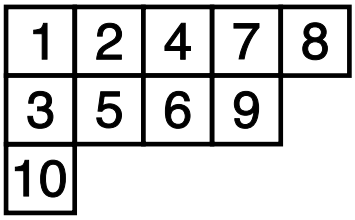
4.1.2 Young diagram

Definition (Young diagram)**.** A **Young diagram** (also called a Ferrers diagram, particularly when represented using dots) is a finite collection of boxes,

or cells, arranged in left-justified rows, with the row lengths in non-increasing order.

Definition (Young tableau)**.** A **Young tableau** is obtained by filling in the boxes of the Young diagram with numbers $1, 2, \ldots, d$ where d is the number of boxes.

Definition (standard tableau)**.** A tableau is called **standard** if the entries in each row and each column are increasing.



Definition (involution numbers)**.** The number of distinct standard Young tableaux on n entries is given by the **involution numbers**

$$1, 1, 2, 4, 10, 26, 76, 232, 764, 2620, 9496, \ldots.$$

Definition (semistandard tableau)**.** A tableau is called **semistandard**, or column strict, if the entries weakly increase along each row and strictly increase down each column.

1	2	2	4	7
3	5	6	9	
8				

Definition (weight of tableau)**.** Recording the number of times each number appears in a tableau gives a sequence known as the **weight of the tableau**.

Remark. The standard Young tableaux are precisely the semistandard tableaux of weight $(1, 1, \ldots, 1)$, which requires every integer up to n to occur exactly once.

4.1.3 G-module continued

Given a group G and a field K, there exists a unital associative algebra $(K[G], +, \cdot, *)$ of K-valued functions on G with finite support.

For any $\lambda \in K[G]$, one can construct an endomorphism on the group algebra $K[G]$

$$\alpha \mapsto \alpha * \lambda, \forall \alpha \in K[G].$$

The image of such endomorphism is a linear subspace $(V_\lambda, +, \cdot)$ of $K[G]$ over K:

$$V_\lambda = \{\, \alpha * \lambda \in K[G] \mid \alpha \in K[G] \,\}.$$

The regular representation $\rho\colon G \to K[G]$ of the group:

$$\rho(g) = e_g,$$

acts on V_λ same as the algebra multiplication:

$$\rho(g)(\alpha * \lambda) = e_g * \alpha * \lambda, \forall \alpha * \lambda \in V_\lambda.$$

For any $\alpha * \lambda \in V_\lambda$, and $\beta \in K[G]$,

$$\beta * (\alpha * \lambda) = (\beta * \alpha) * \lambda \in V_\lambda.$$

Therefore $\rho(g)(V_\lambda) = V_\lambda$, i.e., $\rho(g) \in \mathrm{End}(V_\lambda)$.

For any $\alpha * \lambda \in V_\lambda$ and $g \in G$, there exist $\gamma = e_{g^{-1}} * \alpha * \lambda \in V_\lambda$ such that

$$\rho(g)(\gamma) = \alpha * \lambda,$$

so $\rho(g) \in \mathrm{GL}(V_\lambda)$ is an isomorphism. And thus it is a representation on V_λ.

4.1.4 Main Text

Young diagrams can be used to describe projection operators for the regular representation, which will then give the irreducible representations of $\mathfrak{S}_d$.

If $\mathbb{Z}_d = \bigcup_i \lambda_i$ and λ_i also represents the index set represented by the i-th row of the Young tableau, then

$$g \in P_\lambda \iff \forall \lambda_i [g(\lambda_i) = \lambda_i].$$

For example, given the following tableau,

1	2	4	7	8
3	5	6	9	
10				

we have

$$\lambda_1 = \{\, 1, 2, 4, 7, 8 \,\}, \lambda_2 = \{\, 3, 5, 6, 9 \,\}, \lambda_3 = \{\, 10 \,\}.$$

Then $(12478)(396) \in P_\lambda$ but $(13) \notin P_\lambda$.

$$|P| = \prod_i |\lambda_i|!.$$

Equation in Book 4.1. For a partition λ, define two elements in $\mathbb{C}[\mathfrak{S}_d]$:

$$a_\lambda = \sum_{g \in P} e_g, b_\lambda = \sum_{g \in Q} \operatorname{sgn}(g) e_g.$$

a_λ averages out everything within each row in the permutation representation $\mathbb{C}^d$ with basis $(e_1, e_2, \ldots, e_d)$:

$$\sum_{k=1}^{d} x_k e_k \mapsto |P| \sum_i \left(\frac{1}{|\lambda_i|} \sum_{j \in \lambda_i} x_j \right) \sum_{k \in \lambda_i} e_k.$$

a_λ acting on $V^{\otimes d} = \bigotimes_i V^{\otimes \lambda_i}$ as permutation within each $V^{\otimes \lambda_i}$ and then average them out, making it a symmetric tensor product space:

$$V^{\otimes d} \xrightarrow{a_\lambda} \bigotimes_i \operatorname{Sym}^{\lambda_i} V$$

Similarly, sgn gives the exterior product.

Equation in Book 4.2.

$$c_\lambda = a_\lambda b_\lambda.$$

Theorem in Book 4.3. *Irreducible representation of $\mathfrak{S}_d \sim$ partition of $d \sim$ conjugacy class of $\mathfrak{S}_d$.*

Proposition 4.1. *The following Young diagram corresponds to the alternating representation of $\mathfrak{S}_d$.*

1
2
⋮
d

Proof. Let $G = \mathfrak{S}_d$. Then

$$\begin{aligned} P &= \{\, e \,\}, \\ Q &= G, \\ a &= 1, \\ b &= \sum_{g \in G} \operatorname{sgn}(g) e_g, \\ c &= \sum_{g \in G} \operatorname{sgn}(g) e_g, \\ \mathbb{C}[G] \cdot c &= \sum_{h \in G} \sum_{g \in G} w_h \operatorname{sgn}(g) e_{hg} \\ &= \sum_{h \in G} w_h \operatorname{sgn}(h^{-1}) \sum_{g' \in G} \operatorname{sgn}(g') e_{g'} \\ &= \mathbb{C} \cdot \sum_{g' \in G} \operatorname{sgn}(g') e_{g'}, \end{aligned} \tag{4.1}$$

where $g' = hg$.

For a permutation $p \in \mathfrak{S}_d$ and $x \in \mathbb{C}$,

$$\begin{aligned} e_p \cdot x \cdot \sum_{g' \in G} \operatorname{sgn}(g') e_{g'} &= \operatorname{sgn}(p^{-1}) \cdot x \cdot \sum_{g'' \in G} \operatorname{sgn}(g'') e_{g''} \\ &= \operatorname{sgn}(p) \cdot x \cdot \sum_{g'' \in G} \operatorname{sgn}(g'') e_{g''} \\ &= \begin{cases} x \cdot \sum_{g'' \in G} \operatorname{sgn}(g'') e_{g''} & p \in \mathfrak{A}_d \\ -x \cdot \sum_{g'' \in G} \operatorname{sgn}(g'') e_{g''} & p \notin \mathfrak{A}_d \end{cases}, \end{aligned}$$

where $g'' = pg'$. This is the alternating representation. □

Lemma 4.2.

$$\begin{aligned} P_\lambda &= Q_{\lambda'}, \\ Q_\lambda &= P_{\lambda'}. \end{aligned} \tag{4.2}$$

Definition (tensor product of representations)**.** If V_1, V_2 are linear representations of a group G, then their tensor product is the tensor product of vector spaces $V_1 \otimes V_2$ with the linear action of G uniquely determined by the condition that

$$g \cdot (v_1 \otimes v_2) = (g \cdot v_1) \otimes (g \cdot v_2).$$

Exercise* 4.4. (a) TODO

(b) $(Aa_\lambda)b_\lambda = A(a_\lambda b_\lambda)$.

$(Ab_\lambda)a_\lambda = A(b_\lambda a_\lambda)$.

And from(a): $A(b_\lambda a_\lambda) \cong A(a_\lambda b_\lambda)$.

(c) TODO, maybe using $c_\lambda^2 = nc_\lambda$? Let $G = \mathfrak{S}_d$. Then

$$\begin{aligned} V_\lambda = Aa_\lambda b_\lambda &= A \sum_{a\in P_\lambda} e_a \sum_{b\in Q_\lambda} \operatorname{sgn}(b) e_b, \\ U' &= \mathbb{C}\cdot \sum_{g\in G} \operatorname{sgn}(g) e_g, \\ \therefore V_\lambda \otimes U' &= A \sum_{a\in P_\lambda}\sum_{b\in Q_\lambda}\sum_{g\in G} \operatorname{sgn}(b)\operatorname{sgn}(g) e_a e_b \otimes e_g, \end{aligned} \tag{4.3}$$

Since $g \mapsto \operatorname{sgn}(g)$ and $g \mapsto e_g$ are group homomorphisms, and left action of ab on G permutes the group, and $\operatorname{sgn}(a) = \operatorname{sgn}(a^{-1})$, we have ($g' = abg$)

$$V_\lambda \otimes U' = A \sum_{a\in P_\lambda}\sum_{b\in Q_\lambda}\sum_{g'\in G} \operatorname{sgn}(a)\operatorname{sgn}(g') e_a e_b \otimes e_{b^{-1}a^{-1}g'}.$$

Consider the left action of e_h on the tensor product space:

$$\alpha \sum_{a\in P_\lambda}\sum_{b\in Q_\lambda}\sum_{g'\in G} \operatorname{sgn}(a)\operatorname{sgn}(g') e_{hab} \otimes e_{h(ab)^{-1}g'} \tag{4.4}$$

Note that $P_\lambda = Q_{\lambda'}$ and $Q_\lambda = P_{\lambda'}$,

$$V_{\lambda'} = Aa_{\lambda'}b_{\lambda'} \cong Ab_{\lambda'}a_{\lambda'} = A \sum_{a\in Q_{\lambda'}} \operatorname{sgn}(a) e_a \sum_{b\in P_{\lambda'}} e_b = A \sum_{a\in P_\lambda}\sum_{b\in Q_\lambda} \operatorname{sgn}(a) e_{ab}, \tag{4.5}$$

Exercise 4.5. All trivial and alternating representations are already derived.

$\mathfrak{S}_2$

See text.

$\mathfrak{S}_3$

For the standard representation:

1	2
3	

$$
\begin{aligned}
P &= \{\,(1),(12)\,\},\\
Q &= \{\,(1),(13)\,\},\\
a_\lambda &= 1 + e_{(12)},\\
b_\lambda &= 1 - e_{(13)},\\
c_\lambda = a_\lambda b_\lambda &= 1 + e_{(12)} - e_{(13)} - e_{(132)},\\
e_{(12)}c_\lambda &= e_{(12)} + 1 - e_{(132)} - e_{(13)} = c_\lambda,\\
e_{(123)}c_\lambda &= e_{(123)} + e_{(13)} - e_{(23)} - 1,\\
e_{(13)}c_\lambda &= e_{(123)}e_{(12)}c_\lambda = e_{(123)}c_\lambda,\\
e_{(23)}c_\lambda &= e_{(23)} + e_{(132)} - e_{(123)} - e_{(12)} = -(1+e_{(13)})c_\lambda,\\
e_{(132)}c_\lambda &= e_{(23)}e_{(12)}c_\lambda = -(1+e_{(13)})c_\lambda.
\end{aligned}
\tag{4.6}
$$

Therefore, c_λ and $e_{(13)}c_\lambda$ form the basis.

$$
\begin{aligned}
e_{(12)}\begin{pmatrix}1\\ e_{(13)}\end{pmatrix}c_\lambda &= \begin{pmatrix}e_{(12)}\\ e_{(132)}\end{pmatrix}c_\lambda = \begin{pmatrix}1 & 0\\ -1 & -1\end{pmatrix}\begin{pmatrix}1\\ e_{(13)}\end{pmatrix}c_\lambda,\\
e_{(123)}\begin{pmatrix}1\\ e_{(13)}\end{pmatrix}c_\lambda &= \begin{pmatrix}e_{(123)}\\ e_{(23)}\end{pmatrix}c_\lambda = \begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix}\begin{pmatrix}1\\ e_{(13)}\end{pmatrix}c_\lambda.
\end{aligned}
\tag{4.7}
$$

So $\mathrm{Tr}(e_{(12)}) = 0, \mathrm{Tr}(e_{(123)}) = -1$.

$\mathfrak{S}_4, \mathfrak{S}_5$: TODO

Exercise* 4.6. $\bigwedge^s V \sim$ a hook.

Equation in Book 4.7.

$$
\begin{aligned}
P_j(x) &= \sum_{i=1}^{k} x_k^j,\\
\Delta(x) &= \prod_{i<j}(x_i - x_j).
\end{aligned}
$$

Equation in Book 4.8.

$$
f(x) = \sum_{l_1}\cdots\sum_{l_k}[f(x)]_{(l_1,\ldots,l_k)}\prod_{j=1}^{k} x_j^{l_j}.
$$

Equation in Book 4.9.

$$
l_j = \lambda_j + k - j.
$$

Equation in Book 4.10.

$$\chi_\lambda(C_{\mathbf{i}}) = \left[\Delta(x)\prod_{j=1}^{d} P_j(x)^{i_j}\right]_{(l_1,\ldots,l_k)}.$$

For the following Young diagram:

1	2
3	4
5	

$$d = 5, \lambda = (2,2,1), k = 3, l = (4,3,1).$$

If we want to calculate the character of (123), then $\mathbf{i} = (2,0,1,0,0)$. Hence we calculate the coefficient:

$$[(x_1 - x_2)(x_2 - x_3)(x_1 - x_3)(x_1 + x_2 + x_3)^2(x_1^3 + x_2^3 + x_3^3)]_{(4,3,1)},$$

which gives

$$\chi_{(2,2,1)}(C_{\mathbf{i}}) = -1.$$

```
(x - y) (y - z) (x - z) (x + y + z)^2 (x^3 + y^3 + z^3) // Expand
```

```
x^7 y + x^6 y^2 - x^5 y^3 + x^3 y^5 - x^2 y^6 - x y^7 - x^7 z - x^4 y^3 z +
 x^3 y^4 z + y^7 z - x^6 z^2 + y^6 z^2 + x^5 z^3 + x^4 y z^3 - x y^4 z^3 - y^5 z^3 -
 x^3 y z^4 + x y^3 z^4 - x^3 z^5 + y^3 z^5 + x^2 z^6 - y^2 z^6 + x z^7 - y z^7
```

This corresponds to W.

Schur polynomials

Vandermonde determinant

Equation in Book 4.11.

$$\dim V_\lambda = \frac{d!}{\prod_{j=1}^{k} l_j!}\prod_{i<j\le k}(l_i - l_j).$$

Definition (hook length)**.** The **hook length** of a box in a Young diagram is the number of squares directly below or directly to the right of the box, including the box once.

In the following diagram, each box is labeled by its hook length:

6	4	3	1
4	2	1	
1			

Equation in Book 4.12.

$$\dim V_\lambda = \frac{d!}{\prod_{j=1}^{d} L_j},$$

where L is the hook length.

Exercise* 4.13. TODO

Exercise* 4.14. TODO

Exercise* 4.15. TODO

Exercise* 4.16. TODO

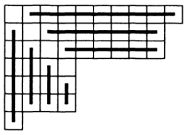
Exercise 4.17. TODO

Equation in Book 4.18. TODO

$$\chi_\lambda((12\dots m)).$$

Definition (rank, characteristics).

Define the *rank* r of a partition to be the length of the diagonal of its Young diagram, and let a_i and b_i be the number of boxes below and to the right of the ith box of the diagonal, reading from lower right to upper left. Frobenius called $\begin{pmatrix} a_1 a_2 \dots a_r \\ b_1 b_2 \dots b_r \end{pmatrix}$ the *characteristics* of the partition. (Many writers now use a reverse notation for the characteristics, writing $(b_r, \dots, b_1 | a_r, \dots, a_r)$ instead.) For the partition (10, 9, 9, 4, 4, 4, 1):



$r = 4$

characteristics $= \begin{pmatrix} 2 & 3 & 4 & 6 \\ 0 & 6 & 7 & 9 \end{pmatrix}$

Exercise* 4.19. TODO

Exercise* 4.20. TODO

4.2 Irreducible representations of $\mathfrak{S}_d$

TODO

4.3 Proof of Frobenius's formula

TODO

5 Representations of $\mathfrak{A}_d$ and $\mathrm{GL}_2(\mathbb{F}_q)$

5.1 Representations of $\mathfrak{A}_d$

5.1.1 Basic Property of Subgroup of Index 2, Normal Subgroup

Lemma 5.1. *If H is a subgroup of G with index 2, then*

$$\begin{aligned} h, h' \in H &\implies hh' \in H, \\ s \in G \setminus H &\iff s^{-1} \in G \setminus H, \\ r, s \in G \setminus H &\implies rs \in H, \\ s \in G \setminus H \wedge h \in H &\implies sh \notin H \wedge hs \notin H. \end{aligned} \tag{5.1}$$

Proof. The first relation is a result of closed multiplication in the group H.

G can be divided into two disjoint left cosets: H and $G \setminus H$ (definition of index, 3.47, 3.52).

Since $s \in G \setminus H$ and $G \setminus H$ is a left coset, $\therefore sH = G \setminus H$ (3.50). If $s^{-1} \in H$, then by definition of coset, $e = ss^{-1} \in sH = G \setminus H$, which contradicts with $e \in H$. Therefore $s^{-1} \notin H$. Since $(s^{-1})^{-1} = s$, the reverse is also true.

If $r, s \in G \setminus H$, then $r^{-1} \in G \setminus H$. From 3.51, we know $rs = (r^{-1})^{-1}s \in H$.

The last equation is a result of disjoint left/right cosets. □

Proposition 5.2. *A subgroup of index 2 is always normal.*

Proof. Let G be a group and H be its subgroup of index 2.

Since H is a group, $\therefore h, h' \in H \implies hh'h^{-1} \in H$.

If $s \in G \setminus H, h \in H$, then (5.1)

$$s^{-1} \in G \setminus H, sh \in G \setminus H,$$

leading to (5.1)

$$shs^{-1} \in H.$$

□

Remark. Alternatively, $G \setminus H = sH = Hs \implies H$ commutes with any $s \notin H$.
`https://crypto.stanford.edu/pbc/notes/group/normal.html`

Proposition 5.3. *If N is a normal subgroup of G, then the conjugacy classes of G must be either subset of N or subset of $G \setminus N$.*

Proof. If $n \in N$, then from definition of normal subgroup, $\forall g \in G[gng^{-1} \in N]$.

If $s \in G \setminus N$ but $\exists g \in G[gsg^{-1} \in N]$. Let $n' = gsg^{-1} \in N$, then $s = hn'h^{-1} \in N$ where $h = g^{-1} \in G$, which is contradicting. □

Corollary 5.4. *Let G be a group and H be its subgroup of index 2. The conjugacy classes of G must be either subset of H or subset of $G \setminus H$.*

Proof. 5.3, 5.2. □

Proposition 5.5. *Let G be a group and H be its subgroup of index 2. Then any conjugacy class C of G is either a conjugacy class of H or the union of two conjugacy classes of H of equal size.*

Proof. TODO □

5.1.2 Main Text

Definition (nontrivial representation)**.** Given a subgroup H of group G with index 2, the **nontrivial representation** of G obtained from the two representations of G/H, denoted U', is

$$\chi_{U'}(g) = \begin{cases} 1 & g \in H \\ -1 & g \notin H \end{cases}.$$

Remark. This is a valid representation due to 5.1.

This is the **alternating representation** in $\mathfrak{S}_d$.

Definition (conjugate representation)**.** If W is any representation of H as a subgroup of G with index 2, there is a **conjugate representation** W' defined as

$$\chi_{W'}(h) = \chi_W(tht^{-1}),$$

where $t \in G \setminus H$.

Proposition 5.6. *Conjugate representation is unique up to isomorphism.*

Proof.

$$tht^{-1} \in H$$

because 5.2.

TODO: Prove conjugate representation *is* a representation of H.

Given $\chi_{W'}(h) = \chi_W(tht^{-1})$, and $\chi_{W''}(h) = \chi_W(shs^{-1})$, where $t, s \in G \setminus H$.

Then $t^{-1}s \in H$ (5.1), denoted as $n = t^{-1}s$, i.e., $s = tn$.

Therefore

$$\chi_{W''}(h) = \chi_W((tn)h(tn)^{-1}) = \chi_W(t(nhn^{-1})t^{-1}) = \chi_{W'}(nhn^{-1}) = \chi_{W'}(h),$$

because nhn^{-1} and h are in the same conjugacy class of H. □

Proposition 5.7. *A representation is self-conjugate if and only if it is a restriction.*

Proof. If W as a representation of H (a subgroup of G of index 2) is a restriction of V, a representation of G, then W must be self-conjugate because for any $t \in G \setminus H, h \in H$,

$$\chi_W(tht^{-1}) = \chi_V(tht^{-1}) = \chi_V(h) = \chi_W(h)$$

as tht^{-1} and h are in the same conjugate class of G.

If W as a representation of H is self-conjugate, then for any $g \in G, h \in H$ ($ghg^{-1} \in H$ because 5.2),

$$f(ghg^{-1}) = 2\chi_W(ghg^{-1}) = 2\chi_W(h) = f(h),$$

where f is a class function of G

$$f(g) = \begin{cases} 2\chi_W(g) & g \in H \\ 0 & g \notin H \end{cases},$$

which is possible because 5.4.

Prove this: f is the character of $\operatorname{Ind} W$ and it is direct sum of two representations whose restriction is W. □

Proposition 5.8. *If U is a representation of group G and W a representation of subgroup H of index 2, then*

$$\operatorname{Ind}(\operatorname{Res}(U)) = U \oplus U'.$$

Proof. From Exercise 3.16(a), we know that

$$\operatorname{Ind}(\operatorname{Res}(U)) = U \otimes P,$$

where P is the permutation representation of G on G/H.

For $h \in H$, since $hH = H$ (3.50) and $h(G \setminus H) = G \setminus H$ (5.1), $\chi_P(h) = 2$.

For $t \in G \setminus H$, since $tH = G \setminus H, t(G \setminus H) = H$ (5.1), $\chi_P(t) = 0$.

Therefore $P = T \oplus T'$, where T is the trivial representation and T' is the alternating representation. Hence, $\operatorname{Ind}(\operatorname{Res}(U)) = U \oplus U'$ where $U' = U \otimes T'$. □

Proposition in Book 5.1. *Let V be an irreducible representation of G, and let W be the restriction of V to H. Then exactly one of the following holds:*
...

Proof. Since V is irreducible representation of G we have $(\chi_V, \chi_V)_G = 1$. As H has index 2,

$$2\,|H| = |G| = \sum_{h\in H} |\chi_V(h)|^2 + \sum_{t\notin H} |\chi_V(t)|^2$$

But

$$\sum_{h\in H} |\chi_V(h)|^2 = \sum_{h\in H} |\chi_W(h)|^2 = |H|\,(\chi_W, \chi_W)_H$$

is multiple of $|H|$.

The multiple must be 1 or 2, because both terms are non-negative and their sum is $2\,|H|$.

- If $\sum_{h\in H} |\chi_V(h)|^2 = |H|$, then W is a irreducible representation because $(\chi_W, \chi_W)_H = 1$. In this case

  $$\sum_{t\notin H} |\chi_V(t)|^2 = |H| > 0 \implies \exists t \notin H[\chi_V(t) \neq 0]$$

  which means V is not isomorphic to $V' = V \otimes U'$ where U' is the alternating representation.

  W is self-conjugate because 5.7. $\operatorname{Ind} W = \operatorname{Ind}\operatorname{Res} V = V \oplus V'$ because 5.8.

- If $\sum_{h\in H} |\chi_V(h)|^2 = |G|$, then W is a direct sum of two irreducible representations because $(\chi_W, \chi_W)_H = 2$. Then W is a direct sum of two different irreducible representations (Exercise 2.33(b)). In this case

  $$\sum_{t\notin H} |\chi_V(t)|^2 = 0 \implies \forall t \notin H[\chi_V(t) = 0]$$

  which means V is isomorphic to $V' = V \otimes U'$ where U' is the alternating representation.

  Let $W = W' \oplus W''$, prove W' is conjugate to W''.

  Prove $\operatorname{Res}(\operatorname{Ind} W)$ is the direct sum of W and its conjugate (Exercise 3.19)

  Prove $V \cong \operatorname{Ind} W' \cong \operatorname{Ind} W''$.

  Prove Each irreducible representation of H arises uniquely in this way

□

Exercise* 5.2. TODO

TODO till end of subchapter

Proposition in Book 5.3. *TODO*

Exercise* 5.4. TODO

Exercise* 5.5. TODO

5.2 Representations of $\mathrm{GL}_2(\mathbb{F}_q)$ and $\mathrm{SL}_2(\mathbb{F}_q)$

5.2.1 Finite Field

Definition (prime power)**.** A **prime power** is a positive integer power of a single prime number.

Definition (Galois field)**.** A **finite field** or **Galois field** is a field that contains a finite number of elements.

Theorem 5.9. *A finite field of order q exists if and only if q is a prime power p^k (where p is a prime number and k is a positive integer).*

Theorem 5.10. *All fields of the same order are isomorphic. Moreover, a field cannot contain two different finite subfields with the same order.*

Remark. One may therefore identify all finite fields with the same order, and they are unambiguously denoted $\mathbb{F}_q$, F_q or $\mathrm{GF}(q)$.

Theorem 5.11. *The characteristic of the field $\mathbb{F}_{p^k}$ (p as a prime number and k a positive integer) is p.*

Remark. Finite field of characteristic p is $\mathbb{F}_{p^k}$ where k is a positive integer. It can be constructed as the quotient polynomial ring

$$\sum_{i=0}^{k-1} a_i x^i \in \mathbb{F}_p[x]/(P),$$

where $a_i \in \mathbb{F}_p$ and (P) is the two-sided ideal generated from an irreducible polynomial of degree k in $\mathbb{F}_p[x]$.

For example,

$$\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1),$$
$$\mathbb{F}_{p^2} = \mathbb{F}_p[x]/(x^2 + 1),$$

where p is an odd prime here.

Proposition 5.12. *If q is odd, $\mathbb{F}_q^*$ contains half of elements with square roots, and exactly 2 square roots. If q is even, every element in $\mathbb{F}_q$ has a unique square root.*

Proof. $x^2 = y^2 \implies x = y \vee x = -y$.

For odd q, $x \neq -x \iff x \neq 0$. So $x \sim -x$ forms a equivalence relation and thus equivalence classes in $\mathbb{F}_q^*$. Every equivalence class has a distinct (unique) square, therefore exactly half of the multiplicative group must have exactly 2 square roots.

For even q, $x = -x$ (because q must be a power of 2, so the field must have characteristic of 2). So $x \sim -x$ forms a equivalence relation and thus equivalence classes (as a singleton) in $\mathbb{F}_q$. Every equivalence class has a distinct (unique) square, therefore all elements in the field must have exactly 1 square root. □

Remark. Also see this proof.

Theorem 5.13. *The multiplicative group of a finite field is a cyclic group.*

Definition (primitive element)**.** A **primitive element** of a finite field $\mathbb{F}_q$ is a generator of the multiplicative group of the field,

Theorem 5.14. *Primitive element must exist. Given $\alpha \in \mathbb{F}_q$, below statements are equivalent.*

- *α is a primitive element.*
- *α is a primitive $(q-1)$th root of unity.*
- *Each non-zero element of $\mathbb{F}_q$ can be written as α^i for some integer i.*

Definition (Euler's totient function)**.** The **Euler's totient function** $\phi\colon \mathbb{Z}^+ \to \mathbb{Z}^+$ is defined as $\phi(m)$ counting the positive integers less than or equal to m which are relatively prime to m.

Theorem 5.15. *A finite cyclic group of order m contains $\phi(m)$ generators.*

Corollary 5.16. *The number of primitive elements in a finite field $\mathbb{F}_q$ is $\phi(q-1)$, where ϕ is Euler's totient function.*

Proposition 5.17. *A primitive element of an odd-order finite field does not have square root.*

Proof. Let ε be the primitive element and assume α as its square root.

Then $\alpha^{q-1} = \varepsilon^{(q-1)/2} = 1$ (property of cyclic group and q is odd) which contradicts with the definition of primitive element (primitive $(q-1)$th root of unity). □

Proposition 5.18. *A primitive element of an odd-order finite field $\mathbb{F}_q$ has two square roots in $\mathbb{F}_{q^{2n}}$ where n is a positive number.*

Proof. Let ε be the primitive element in $\mathbb{F}_q$ and κ be the primitive element in $\mathbb{F}_{q^{2n}}$.

Therefore,

$$\kappa^{q^{2n}-1} = (\kappa^m)^{q-1} = 1 = \varepsilon^{q-1},$$

where

$$m = \sum_{i=0}^{2n-1} q^i$$

is an even number (since q is odd and number of terms is even).

Since both are primitive root of unity,

$$\varepsilon = \kappa^m.$$

Because m is even, ε must have square root(s). □

5.2.2 Linear Groups

Definition (special linear group)**.** The **special linear group** $\mathrm{SL}(n, F)$ or $\mathrm{SL}_n(F)$ of degree n over a field F is the set of $n \times n$ matrices with determinant 1, with the group operations of ordinary matrix multiplication and matrix inversion.

Theorem 5.19. *The special linear group is the normal subgroup of the general linear group given by the kernel of the determinant*

$$\det\colon \mathrm{GL}(n, F) \to F \setminus \{\, 0 \,\}.$$

Theorem 5.20. *The center of a group is always a normal subgroup.*

Definition (projective space)**.** Given a vector space V over a field K, the **projective space** $\mathrm{P}(V)$ is the set of equivalence classes of $V^* = V \setminus \{\, \mathbf{0} \,\}$ under the equivalence relation $\sim$ defined by $x \sim y$ if there is a nonzero element λ of $K^* = K \setminus \{\, 0 \,\}$ such that $x = \lambda y$. Explicitly:

$$\mathrm{P}(V) = \{\, \{\, \lambda x \in V^* \mid \lambda \in K^* \,\} \in \mathcal{P}(V^*) \mid x \in V^* \,\}.$$

Remark. It can be viewed as a sphere in the V^* space? Every element of the projective space is corresponding to a projective line in V^*.

Definition (projective linear group)**.** The **projective (general) linear group** is the quotient group

$$\mathrm{PGL}(V) = \mathrm{GL}(V)/\,\mathrm{Z}(V),$$

where $\mathrm{GL}(V)$ is the general linear group of vector space V and $\mathrm{Z}(V)$ is the normal subgroup of all nonzero scalar transformations of V

Remark. PGL is the induced action of the general linear group of a vector space V on the associated projective space $\mathrm{P}(V)$. $\mathrm{Z}(V)$ are quotiented out because they act trivially on the projective space and they form the kernel of the action.

Theorem 5.21. $\mathrm{Z}(V)$ *is the center of* $\mathrm{GL}(V)$.

Definition (projective special linear group)**.** The **projective special linear group** is defined as

$$\mathrm{PSL}(V) = \mathrm{SL}(V)/\,\mathrm{SZ}(V),$$

where $\mathrm{SL}(V)$ is the special linear group over a vector space V and $\mathrm{SZ}(V)$ is the subgroup of scalar transformations with unit determinant.

Remark. PSL is the induced action of the special linear group on the associated projective space.

Theorem 5.22. $\mathrm{SZ}(V)$ *is the center of* $\mathrm{SL}(V)$.

Theorem 5.23. $\mathrm{SZ}(V)$ *is the group of* n*th roots of unity in* F*, where* n *is the dimension of* V *over field* F*.*

General linear group can be considered as moving the axes and rulers on the axes.

5.2.3 Main Text

5.2.3.1 Introduction

Definition (GL2Fq)**.** $\mathrm{GL}_2(\mathbb{F}_q)$ is the group of invertible 2×2 matrices with entries in the finite field $\mathbb{F}_q$ with q elements, where q is a prime power.

Definition (simple group)**.** A **simple group** is a nontrivial group whose only normal subgroups are the trivial group and the group itself.

Similar to irreducible representation?

5.2.3.2 Borel Subgroup

5.2.3.2.1 Cardinality The Borel subgroup B of $G = \mathrm{GL}_2(\mathbb{F}_q)$ has cardinality:

$$|B| = q(q-1)^2,$$

because in the form

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix},$$

$a \neq 0, d \neq 0$ (otherwise not invertible).

5.2.3.2.2 Non-normal Subgroup Given any $g \in G$, $x \in B$,

$$(gxg^{-1})_{21} = \sum_i \sum_j g_{2i} x_{ij} (g^{-1})_{j1} = g_{21} x_{11} (g^{-1})_{11} + \sum_i g_{2i} x_{i2} (g^{-1})_{21}$$

since $x_{21} = 0$ but this is not necessarily 0. Therefore Borel subgroup is **not a normal subgroup** of G.

If $x_{11} = x_{22} = 1$, then

$$(gxg^{-1})_{21} = g_{21}(g^{-1})_{11} + g_{22}(g^{-1})_{21} + g_{21}x_{12}(g^{-1})_{22} = g_{21}x_{12}(g^{-1})_{22} = \frac{x_{12}g_{21}g_{11}}{\det g}.$$

Therefore

$$N = \{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \}$$

is **a subgroup but not normal subgroup** of $\mathrm{SL}_2(\mathbb{F}_q)$.

For example, if $x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in N, g = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_q)$, then $g^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_q)$, and $gxg^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix} \notin B$ (it becomes $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ if q is power of 2).

5.2.3.2.3 Conjugacy classes of Borel subgroup Given $x = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in B$ and $s = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} \in B$, we have (since $d' \neq 0$)

$$sxs^{-1} = \begin{pmatrix} a & \frac{b'(d-a)+a'b}{d'} \\ 0 & d \end{pmatrix}.$$

Therefore there are three types of conjugacy classes. For any $b'' \in \mathbb{F}_q$, if we want $sxs^{-1} = \begin{pmatrix} a & b'' \\ 0 & d \end{pmatrix}$, then

Table 1: Conjugacy classes of the Borel subgroup

Representative	Num Elements in Class	Num Classes
$a'_x = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}, x \neq 0$	1	$q-1$
$b'_x = \begin{pmatrix} x & b \\ 0 & x \end{pmatrix}, x \neq 0, b \neq 0$	$q-1$	$q-1$
$c'_{x,y} = \begin{pmatrix} x & b \\ 0 & y \end{pmatrix}, xy \neq 0, x \neq y$	q	$(q-1)(q-2)$

1. if $a \neq d$, then $a' = a - d, b' = b + b'', d' = d - a$.
2. if $a = d, b \neq 0, b'' \neq 0$, then $a' = b'', b' = 0, d' = b$.
3. if $a = d, b = b'' = 0$, then $a' = d' = 1, b' = 0$.

Therefore the number of conjugacy classes is $q(q-1)$ and total number of elements is $q(q-1)^2$.

The conjugacy classes of B is summarized in Table **??**.

5.2.3.3 Projective Line Based on the definition of projective space, the **finite projective line** $L_{(1:0)}$, as an element of the projective space, is a subset of the 2-dimensional vector space $\mathbb{F}_q^2$ such that

$$L_{(1:0)} = \{\, (a, 0) \in \mathbb{F}_q^2 \mid a \neq 0 \,\}.$$

5.2.3.4 Transitive Group Action

Definition (transitive group action)**.** The **action** of group G on set X is called **transitive** if X is non-empty and if for each pair x, y in X there exists a g in G such that $gx = y$, i.e.,

$$X \neq \varnothing \wedge \forall x \in X \forall y \in X \exists g \in G[gx = y].$$

Based on the definition of projective space, Any element $x \in \mathbb{P}^1(\mathbb{F}_q)$ can be expressed as

$$x = \{\, a(x_1, x_2) \mid a \in \mathbb{F}_q^* \,\},$$

where $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{\, 0 \,\}$ and $x_1 x_2 \neq 0$.

$G = \mathrm{GL}_2(\mathbb{F}_q)$ acts transitively on $\mathbb{P}^1(\mathbb{F}_q)$. This is because G are isomorphisms (and therefore maps projective line onto projective line) and G contains all isomorphisms (and therefore for any $x, y \in \mathbb{P}^1(\mathbb{F}_q)$ there exists a mapping $g \in G$ from x onto y).

5.2.3.5 Isotropy Group

Definition (isotropy group)**.** An **isotropy group** is the group of isomorphisms from any object to itself in a groupoid. An isotropy representation is a representation of an isotropy group.

For any $x = (r, 0), y = (s, 0) \in L_{(1:0)}$, $gx = y \implies g \in B$, because $0 = y_2 = g_{21}x_1 + g_{22}x_2 = g_{21}x_1$ but $x_1 = r \neq 0$. Therefore B contains the isotropy group on $L_{(1:0)}$.

Given any $g = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in B$ and $x = (r, 0) \in L_{(1:0)}$, we have $gx = (ar, 0) \in L_{(1:0)}$ because $a \neq 0, r \neq 0$.

Also, B acts transitively on $L_{(1:0)}$. For any $x = (r, 0), y = (s, 0) \in L_{(1:0)}$, we have $g \in B$ such that $gx = y$, given

$$g = \begin{pmatrix} s/r & 0 \\ 0 & 1 \end{pmatrix},$$

because $r \neq 0, s \neq 0$.

Therefore, $BL_{(1:0)} = L_{(1:0)}$, concluding that B is the isotropy group acting on $L_{(1:0)}$.

5.2.3.6 The Order of G The order of G is the product of the cardinality of $\mathbb{P}^1(\mathbb{F}_q)$ multiplied by the order of the isotropy group on one element in $\mathbb{P}^1(\mathbb{F}_q)$.

Since $\mathbb{F}_q^*$ is a multiplicative group,

$$\therefore a(1, x) = (1, y) \iff a = 1 \implies x = y,$$

where $a, x, y \in \mathbb{F}_q$.

Therefore, $(1, x) \in \mathbb{F}_q^2$ are q representatives of q different projective lines in the space $\mathbb{P}^1(\mathbb{F}_q)$.

Since $\mathbb{F}_q^*$ is a multiplicative group (meaning, multiplicative inverse exists), any vector in $\mathbb{F}_q^2$ with nonzero first coordinate is a scalar product of a nonzero scalar with one of the vectors of form $(1, x)$.

Easy to prove that $(0, 1)$ is the last remaining equivalent class in $\mathbb{P}^1(\mathbb{F}_q)$, so

$$\left|\mathbb{P}^1(\mathbb{F}_q)\right| = q + 1,$$

and therefore

$$|G| = |B| \left|\mathbb{P}^1(\mathbb{F}_q)\right| = (q-1)^2 q(q+1).$$

5.2.3.7 Field Extension

Definition (field extension)**.** If K is a subfield of L, then L is an **extension field** or simply extension of K, and this pair of fields is a **field extension**. Such a field extension is denoted L/K (read as "L over K").

Definition (intermediate field)**.** If L is an extension of F, which is in turn an extension of K, then F is said to be an **intermediate field** (or intermediate extension or subextension) of L/K.

Theorem 5.24. *Given a field extension L/K, the larger field L is a K-vector space. The dimension of this vector space is called the degree of the extension and is denoted by $[L : K]$.*

5.2.3.8 The Cyclic Subgroup

Theorem 5.25. *Any finite group has some cyclic subgroup.*

Proposition 5.26. *Let ε be a primitive element of an odd-order finite field $\mathbb{F}_q$. Then one of the square roots of ε together with 1 forms the basis of $\mathbb{F}_{q^2} = \mathbb{F}_q(1, \sqrt{\varepsilon})$.*

Proof. Clearly $\mathbb{F}_q$ is a subfield of $\mathbb{F}_{q^2}$ (need proof) and therefore $\mathbb{F}_{q^2}/\mathbb{F}_q$ is a field extension, and the $\mathbb{F}_{q^2}$ can be viewed as a 2-dimensional vector space over $\mathbb{F}_q$.

Since $\mathbb{F}_q^*$ is a cyclic group, it must have a multiplicative generator (primitive element), denoted ε. Since it is a generator, it must not have square root in $\mathbb{F}_q$ if q is odd (5.17).

Denote one of its square root in $\mathbb{F}_{q^2}$ as $\sqrt{\varepsilon}$ (existence: 5.18) and therefore this combined with 1 form a basis of the vector space $\mathbb{F}_{q^2}$. □

Remark. Note, it is possible that -1 has (two) square root(s) in a odd-order finite field (e.g., $\mathbb{F}_9$, see this, $b^2 = e^2 = 2 = -1$).

Proposition 5.27. *Given odd q and $x, y \in \mathbb{F}_q$ but $x \neq 0 \vee y \neq 0$,*

$$x + y\sqrt{\varepsilon} \mapsto \begin{pmatrix} x & \varepsilon y \\ y & x \end{pmatrix}$$

is a group isomorphism from $\mathbb{F}_{q^2}^*$ onto $K \subseteq \mathrm{GL}_2(\mathbb{F}_q)$.

Proof. First prove $\mathbf{A} = \begin{pmatrix} x & \varepsilon y \\ y & x \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$.

Note that

$$\det \mathbf{A} = x^2 - \varepsilon y^2$$

which becomes nonzero if either x or y is zero (the other must be nonzero, and $\varepsilon \neq 0$).

Since ε is a primitive $(q-1)$th root of unity, where $q-1$ is even, $\therefore$ odd power of ε is not 1.

If $x \neq 0, y \neq 0$, then

$$\det \mathbf{A} = x^2 - \varepsilon y^2 = \varepsilon^{2r} - \varepsilon^{2s+1} = \varepsilon^{2r}(1 - \varepsilon^{2s-2r+1}) \neq 0,$$

because $2s - 2r + 1$ is odd ($\implies 1 - \varepsilon^{2s-2r+1} \neq 0$) and $\varepsilon \neq 0$ ($\implies \varepsilon^{2r} \neq 0$), $x \neq 0, y \neq 0$ ($\implies$ x, y can be expressed as power of the multiplicative generator ε). Therefore $\mathbf{A} \in \mathrm{GL}_2(\mathbb{F}_q)$.

Since $(1, \sqrt{\varepsilon})$ forms a basis of $\mathbb{F}_{q^2}$, the coefficients x, y are unique, $\therefore$ this map is injective. Therefore it is a bijection onto its image.

Below shows this is a group homomorphism.

$$\begin{aligned} &(x + y\sqrt{\varepsilon})(u + v\sqrt{\varepsilon}) = (xu + yv\varepsilon) + (xv + yu)\sqrt{\varepsilon} \\ \mapsto &\begin{pmatrix} xu + yv\varepsilon & \varepsilon(xv + yu) \\ xv + yu & xu + yv\varepsilon \end{pmatrix} = \begin{pmatrix} x & \varepsilon y \\ y & x \end{pmatrix} \begin{pmatrix} u & \varepsilon v \\ v & u \end{pmatrix} \end{aligned}$$

□

5.2.3.9 Conjugacy classes in G

Remark. Conjugacy classes in G:

1. $a_x \in \mathrm{Z}(G)$ so their conjugacy classes are singletons (note $x \neq 0$).
2. Given $a \neq 0$,

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \begin{pmatrix} x & 1 \\ 0 & x \end{pmatrix} \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}^{-1} = \begin{pmatrix} ax & a + bx \\ 0 & ax \end{pmatrix} \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}^{-1} = \begin{pmatrix} x & 1 \\ 0 & x \end{pmatrix}.$$

   And only matrices of this form (which forms a subgroup) will keep b_x $(x \neq 0)$ as it is. Therefore the cardinality of the conjugacy class is the index of this subgroup:

$$\frac{|G|}{q(q-1)} = q^2 - 1.$$

3. Similarly the isotropy group for $c_{x,y}$ ($xy \neq 0, x \neq y$) is D (invertible diagonal matrices, order $(q-1)^2$),

4. and the isotropy group for $d_{x,y}$ ($y \neq 0, x \in \mathbb{F}_q$) is K.

To see that the classes are disjoint, consider the eigenvalues and the Jordan canonical forms. JCF in finite field?

5.2.3.10 The q-dimensional Irreducible Representation V

Proposition 5.28. *Any permutation representation of a finite group contains a trivial representation.*

Proof. Let the group G acts on X, then below is a trivial representation (R is a ring, e_x is the basis of free R-module of R-valued functions on X):

$$\sum_{x \in X} e_x$$

because it is not changed by any action of G. □

Remark. The permutation representation of G on $P = \mathbb{P}^1(\mathbb{F}_q)$ has dimension $q+1$.

Let $\alpha = \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{F}_q^2 \setminus \{ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \}$ and $[\alpha] \in \mathbb{P}^1(\mathbb{F}_q)$, we can calculate that

1. $$a_x \alpha = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} xa \\ xb \end{pmatrix} \in [\alpha] .$$

2. $$b_x \alpha = \begin{pmatrix} x & 1 \\ 0 & x \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} xa + b \\ xb \end{pmatrix} \implies (\forall b_x \alpha \in [\alpha] \leftrightarrow b = 0)$$

3. $$c_{x,y} \alpha = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} xa \\ yb \end{pmatrix} \implies (\forall c_{x,y} \alpha \in [\alpha] \leftrightarrow ab = 0)$$

4. $$d_{x,y} \alpha = \begin{pmatrix} x & \varepsilon y \\ y & x \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} xa + \varepsilon yb \\ ya + xb \end{pmatrix} \implies (\neg \forall d_{x,y} \alpha \in [\alpha])$$

Then (since the character is the number of basis fixed by the permutation action) we have the row of P:

size of the conjugacy class	1	q^2-1	q^2+q	q^2-q
number of classes	$q-1$	$q-1$	$\frac{(q-1)(q-2)}{2}$	$\frac{q(q-1)}{2}$
G	a_x	b_x	$c_{x,y}$	$d_{x,y}$
P	$q+1$	1	2	0
V	q	0	1	-1

By removing the trivial representation in P, the complementary q-dimensional representation V has character one less than that of P (see table above).

$$
\begin{aligned}
&(\chi_V, \chi_V) \\
&= \frac{1}{(q-1)^2 q(q+1)} \left(q^2(q-1) + \frac{(q-1)(q-2)(q^2+q)}{2} + \frac{q(q-1)(q^2-q)}{2} \right) \\
&= \frac{1}{(q-1)(q+1)} \left(q + \frac{(q-2)(q+1)}{2} + \frac{q^2-q}{2} \right) \\
&= 1.
\end{aligned}
$$

Therefore V is irreducible.

5.2.3.11 1-dimensional Representations

Remark. Since $\mathbb{F}_q^*$ is a cyclic group of order $q-1$ (5.13), it has $q-1$ 1-d representations $\alpha \colon \mathbb{F}_q^* \to \mathbb{C}^*$

For each α, we have a one-dimensional representation U_α of G defined by $U_\alpha(g) = \alpha(\det(g))$.

$\det(g) \in \mathbb{F}_q^*$ because g is invertible (i.e., $g \in \mathrm{GL}_2(\mathbb{F}_q)$), therefore $\alpha(\det(g))$ is well defined.

$U_\alpha(g) \in \mathrm{GL}(\mathbb{C}) = \mathbb{C}^*$ because α maps into $\mathbb{C}^*$.

It is a group homomorphism because both α and det are group homomorphisms:

$$U_\alpha(gh) = \alpha(\det(gh)) = \alpha(\det(g)\det(h)) = \alpha(\det(g))\alpha(\det(h)) = U_\alpha(g)U_\alpha(h).$$

By calculating the determinant of each conjugacy class, we get the explicit expression for U_α.

5.2.3.12 Field Norm

Definition (field norm)**.** Given a finite field extension L/K and an element $a \in L$, the mapping $x \mapsto ax$ is a K-linear map of the vector space L into itself (i.e., endomorphism).

Express this linear map in terms of $\mathrm{M}([L:K], K)$. The determinant of such matrix is defined as **field norm**.

Remark. Let $\xi = x + y\sqrt{\varepsilon} \in \mathbb{F}_{q^2}^*$ and $\lambda = u + v\sqrt{\varepsilon} \in \mathbb{F}_{q^2}$, then

$$\begin{aligned}\xi\lambda &= (xu + yv\varepsilon) + (xv + yu)\sqrt{\varepsilon} \\ &\mapsto \begin{pmatrix} xu + yv\varepsilon \\ xv + yu \end{pmatrix} = \begin{pmatrix} x & \varepsilon y \\ y & x \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix},\end{aligned}$$

Therefore the field norm of $\lambda \mapsto \xi\lambda$ is the determinant of $d_{x,y}$.

Theorem 5.29. *Let $L = \mathbb{F}_{q^n}$ be a finite extension of a finite field $K = \mathbb{F}_q$, then*

$$\mathrm{Norm}_{L/K}(\alpha) = \alpha \cdot \alpha^q \cdot \alpha^{q^2} \cdots \alpha^{q^{n-1}} = \alpha^{(q^n-1)/(q-1)}.$$

Additionally,

$$\begin{aligned}&\forall \alpha \in L, \quad \mathrm{Norm}_{L/K}(\alpha^q) = \mathrm{Norm}_{L/K}(\alpha), \\ &\forall a \in K, \quad \mathrm{Norm}_{L/K}(a) = a^n.\end{aligned} \tag{5.2}$$

Remark. Since L/K is a Galois extension, if $\alpha \in L$, then the norm of α is the product of all the Galois conjugates of α.

Remark. Applying above formula, we get

$$x^2 - \varepsilon y^2 = \xi^{q+1}. \tag{5.3}$$

5.2.3.13 1-dimensional Representation of Borel Subgroup Given two representations $\alpha, \beta \colon \mathbb{F}_q^* \to \mathbb{C}^*$ of $\mathbb{F}_q^*$, the mapping

$$W'_{\alpha,\beta} \colon \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mapsto \alpha(a)\beta(d)$$

1. is well-defined because $a \neq 0, d \neq 0$;
2. is in $\mathrm{GL}(\mathbb{C}) = \mathbb{C}^*$ because $\mathbb{C}^*$ has closed multiplication;
3. is a group homomorphism because
   - the diagonal is simply piecewise-multiplied,
   - α, β are group homomorphisms.
   - $\mathbb{C}^*$ is abelian multiplicative group.

5.2.3.14 Induced Representation of the 1-d Representation of the Borel Subgroup

See Table **??** for conjugacy classes of the Borel subgroup.

Each a_x, b_x class bijectively corresponds to the a'_x, b'_x class respectively, with possibly reduced elements. $[c_{x,y}] = [c_{y,x}]$ is split into two different conjugacy classes in the Borel subgroup.

Denote $W_{\alpha,\beta}$ as the induced representation of the above 1-d representation of the Borel subgroup. From Exercise 3.19 ($d_{x,y}$ is not in the subgroup B):

$$\begin{aligned}
\chi_{W_{\alpha,\beta}}(a_x) &= \frac{|G|}{|B|}\frac{1}{1}W'_{\alpha,\beta}(\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}) \\
&= (q+1)\alpha(x)\beta(x), \\
\chi_{W_{\alpha,\beta}}(b_x) &= \frac{|G|}{|B|}\frac{q-1}{q^2-1}W'_{\alpha,\beta}(\begin{pmatrix} x & 1 \\ 0 & x \end{pmatrix}) \\
&= \alpha(x)\beta(x), \\
\chi_{W_{\alpha,\beta}}(c_{x,y}) &= \frac{|G|}{|B|}\frac{q}{q^2+q}\left[W'_{\alpha,\beta}(\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}) + W'_{\alpha,\beta}(\begin{pmatrix} y & 0 \\ 0 & x \end{pmatrix})\right] \\
&= \alpha(x)\beta(y) + \alpha(y)\beta(x), \\
\chi_{W_{\alpha,\beta}}(d_{x,y}) &= 0.
\end{aligned}$$

By calculating the inner product, We see from this that $W_{\alpha,\beta} \cong W_{\beta,\alpha}$, that $W_{\alpha,\beta} \cong U_\alpha \oplus V_\alpha$, and that for $\alpha \neq \beta$, the representation is irreducible. This gives $(q-1)(q-2)/2$ (because there are $q-1$ different α) more irreducible representations, of dimension $q+1$ (because $\alpha(1) = \beta(1) = 1$).

5.2.3.15 Induced Representations from K

5.2.3.15.1 Conjugacy classes of K

Let $\varphi\colon K \to \mathbb{C}^*$ be one of the q^2-1 one-dimensional representations of $\mathbb{F}^*_{q^2} \cong K$.

We see that

1. a_x is unchanged in K ($y = 0$),
2. b_x disappears in K ($0\varepsilon = 0 \neq 1$),
3. $c_{x,y}$ disappears in K (main diagonal entries not equal),
4. $[d_{x,y}] = [d_{x,-y}]$ is split to two singleton classes in K.

This tallies to $(q-1) + 2(\frac{q(q-1)}{2}) = q^2 - 1 = |K|$ elements.

5.2.3.15.2 Induced representation From Exercise 3.19,

$$\begin{aligned}
\chi_{\operatorname{Ind}\varphi}(a_x) &= \frac{|G|}{|K|}\frac{1}{1}\varphi(a_x) \\
&= q(q-1)\varphi(x) \\
\chi_{\operatorname{Ind}\varphi}(b_x) &= \chi_{\operatorname{Ind}\varphi}(c_{x,y}) = 0 \\
\chi_{\operatorname{Ind}\varphi}(d_{x,y}) &= \frac{|G|}{|K|}\frac{1}{q^2-q}(\varphi(d_{x,y}) + \varphi(d_{y,x})) \\
&= \varphi(x+y\sqrt{\varepsilon}) + \varphi(x-y\sqrt{\varepsilon}) \\
&= \varphi(\xi) + \varphi(\xi^q)
\end{aligned}$$

Note that the last equality is because ((5.3))

$$\xi(x-y\sqrt{\varepsilon}) = (x+y\sqrt{\varepsilon})(x-y\sqrt{\varepsilon}) = x^2 - \varepsilon y^2 = \xi^{q+1}. \tag{5.4}$$

5.2.3.15.3 Representations of K Note that $\varphi_k(j) = \mathrm{e}^{\frac{2\pi ijk}{q^2-1}}$. If $\varphi^q = \varphi$, then $\varphi^{q-1} = \mathrm{e}^{\frac{2\pi ijk}{q+1}} = 1$.

This means $q+1 \mid k \iff \varphi^q = \varphi$.

Therefore there are $\frac{q^2-1}{q+1} = q-1$ representations such that $\varphi = \varphi^q$ and $q^2 - 1 - (q-1) = q(q-1)$ representations such that $\varphi \neq \varphi^q$.

5.2.3.15.4 Isomorphic representations Since $x \in \mathbb{F}_q^*$ is in a cyclic group of order $q-1$, therefore $x^q = x$.

Since $(x+y\sqrt{\varepsilon})^q = x - y\sqrt{\varepsilon}$ ((5.4)), by replacement $y \mapsto -y$, we have $(x-y\sqrt{\varepsilon})^q = x + y\sqrt{\varepsilon}$, and therefore $(\xi^q)^q = \xi$. This also comes from the fact that $\mathbb{F}_{q^2}^*$ is a cyclic group of order q^2-1.

Therefore the mapping $\varphi^q \colon \alpha \mapsto \varphi(\alpha)^q$ gives an induced representation isomorphic to $\operatorname{Ind}\varphi$.

Therefore there are $q-1$ representations $\operatorname{Ind}\varphi$ where $\varphi = \varphi^q$ and $\frac{q(q-1)}{2}$ representations $\operatorname{Ind}\varphi$ where $\varphi \neq \varphi^q$.

However, they are not irreducible representations.

5.2.3.16 Remaining Irreducible Representations Let

$$V \otimes W_{\alpha,1} \cong X_\varphi \oplus W_{\alpha,1} \oplus \operatorname{Ind}\varphi,$$

where $\varphi \neq \varphi^q$ and $\alpha = \operatorname{Res}\varphi$ is the restricted representation from $\mathbb{F}_{q^2}^*$ to $\mathbb{F}_q^*$, so $\alpha(x) = \varphi(x), \forall x \in \mathbb{F}_q^*$.

Therefore

size of the conjugacy class	1	q^2-1	q^2+q	q^2-q
number of classes	$q-1$	$q-1$	$\frac{(q-1)(q-2)}{2}$	$\frac{q(q-1)}{2}$
G	a_x	b_x	$c_{x,y}$	$d_{x,y}$
V	q	0	1	-1
$W_{\alpha,1}$	$(q+1)\varphi(x)$	$\varphi(x)$	$\varphi(x)+1$	0
$V\otimes W_{\alpha,1}$	$q(q+1)\varphi(x)$	0	$\varphi(x)+1$	0
$\operatorname{Ind}\varphi$	$q(q-1)\varphi(x)$	0	0	$\varphi(\xi)+\varphi(\xi)^q$
X_φ	$(q-1)\varphi(x)$	$-\varphi(x)$	0	$-(\varphi(\xi)+\varphi(\xi^q))$

And we can show X_φ is irreducible if $\varphi\neq\varphi^q$.

5.2.3.17 Character Table Given that

- ε is a primitive element (5.2.1) in $\mathbb{F}_q^*$;
- $\xi=x+y\sqrt{\varepsilon}\in\mathbb{F}_{q^2}^*$ where $x,y\in\mathbb{F}_q$ has the properties

$$\begin{aligned}\xi^q&=x-y\sqrt{\varepsilon},\\ \xi^{q+1}&=x^2-\varepsilon y^2\in\mathbb{F}_q^*,\end{aligned}\tag{5.5}$$

  (see (5.3), (5.4));
- $\alpha,\beta\colon\mathbb{F}_q^*\to\mathbb{C}^*$ are two different one-dimensional representations of the multiplicative cyclic group $\mathbb{F}_q^*$;
- $\varphi\colon\mathbb{F}_{q^2}^*\to\mathbb{C}^*$ is a one-dimensional representation of the multiplicative cyclic group $\mathbb{F}_{q^2}^*$ such that $\varphi\neq\varphi^q$;
- representative matrices

$$a_x=\begin{pmatrix}x&0\\0&x\end{pmatrix},b_x=\begin{pmatrix}x&1\\0&x\end{pmatrix},c_{x,y}=\begin{pmatrix}x&0\\0&y\end{pmatrix},d_{x,y}=\begin{pmatrix}x&\varepsilon y\\y&x\end{pmatrix}$$

  for conjugacy classes of $\mathrm{GL}_2(\mathbb{F}_q)$;

below is the character table of $\mathrm{GL}_2(\mathbb{F}_q)$:

	Size conj class	1	q^2-1	q^2+q	q^2-q
	Num columns	$q-1$	$q-1$	$\frac{(q-1)(q-2)}{2}$	$\frac{q(q-1)}{2}$
	$\mathrm{GL}_2(\mathbb{F}_q)$	a_x	b_x	$[c_{x,y}]=[c_{y,x}]$	$[d_{x,y}]=[d_{x,-y}]$
Num rows		$x\neq0$	$x\neq0$	$xy\neq0$	$y\neq0$
$q-1$	U_α	$\alpha(x^2)$	$\alpha(x^2)$	$\alpha(xy)$	$\alpha(\xi^{q+1})$
$q-1$	V_α	$q\alpha(x^2)$	0	$\alpha(xy)$	$-\alpha(\xi^{q+1})$
$\frac{(q-1)(q-2)}{2}$	$W_{\alpha,\beta}\cong W_{\beta,\alpha}$	$(q+1)\alpha(x)\beta(y)$	$\alpha(x)\beta(y)$	$\alpha(x)\beta(y)+\alpha(y)\beta(x)$	0
$\frac{q(q-1)}{2}$	$X_\varphi\cong X_{\varphi^q}$	$(q-1)\varphi(x)$	$-\varphi(x)$	0	$-(\varphi(\xi)+\varphi(\xi^q))$

Clearly the number of rows matches the number of columns. The total dimensionality sums up to

$$(q-1)\cdot 1^2+(q-1)\cdot q^2+\frac{(q-1)(q-2)}{2}\cdot(q+1)^2+\frac{q(q-1)}{2}\cdot(q-1)^2=|G|\,.$$

5.2.3.18 The remaining part of the section

TODO till end of chapter

Exercise 5.6. TODO

Exercise 5.7. TODO

Exercise 5.8. TODO

Exercise* 5.9. TODO

Exercise 5.10. TODO

Exercise* 5.11. TODO

6 Weyl's Construction

6.1 Schur functors and their characters

6.1.1 Introduction

The group $\mathrm{GL}(V)$ acts on $V\otimes V$, and this is, as we shall soon see, the decomposition of $V\otimes V$ into a direct sum of irreducible $\mathrm{GL}(V)$-representations.

We shall see that this other space is a sum of two copies of an irreducible $\mathrm{GL}(V)$-representation.

$\mathrm{Sym}^d V$ and $\bigwedge^d V$ are images of symmetrizing operators from $V^{\otimes d}$ to itself: see 4.1.4.

$a_{(d)}$ maps $V^{\otimes d}$ to $\mathrm{Sym}^d V$ and $b_{(1,\dots,1)}$ maps it to $\bigwedge^d V$.

6.1.2 Right Action on Tensor Space

In subsubsection 4.1.3, given a commutative ring K and a group G, $\lambda\in K[G]$ defines a right action as well as an endomorphism on the group algebra $(K[G],+,\cdot,*)$

$$\alpha\mapsto\alpha*\lambda,\forall\alpha\in K[G],$$

whose image is a linear subspace $(V_\lambda,+,\cdot)$ of $K[G]$ over K:

$$V_\lambda=\{\,\alpha*\lambda\in K[G]\mid\alpha\in K[G]\,\}\,.$$

Similarly, for $V^{\otimes d}$, we can define a right action of a permutation $\sigma \in \mathfrak{S}_d$ such that

$$(\sum_i \bigotimes_{j=1}^{d} v_{i,j})\sigma = \sum_i \bigotimes_{j=1}^{d} v_{i,\sigma(j)},$$

given any $v_{i,j} \in V$.

TODO: above might be wrong

TODO: need to check: Is this a valid right action?

$$xe = x$$

$$x(\rho\sigma) = (x\rho)\sigma$$

Is it a well defined action?

$$((av_1 + bv_2) \otimes (cw_1 + dw_2))\rho = (acv_1 \otimes w_1 + adv_1 \otimes w_2 + bcv_2 \otimes w_1 + bdv_2 \otimes w_2)\rho$$

Is it a linear map?

$$(av + bw)\sigma = a((v)\sigma) + b((w)\sigma)$$

Is it mapping into itself?

TODO: this chapter is skipped

Is this a functor? Is this a module?

Wikipedia

6.2 The proofs

TODO: skipped

7 Lie Groups

7.0 Basic Topology

7.0.1 Hierarchy of Topological Spaces

7.0.1.1 Topological Space

7.0.1.1.1 Definition

Definition (topological space)**.** A **topological space** is an ordered pair $(X, \tau \subseteq \mathcal{P}(X))$, where X is a set and τ is a collection of subsets of X, satisfying the following axioms:

- empty set and X are open:

$$\varnothing \in \tau \wedge X \in \tau,$$

- the union of open sets is open:

$$\forall \sigma [\sigma \subseteq \tau \implies \bigcup \sigma \in \tau],$$

- the intersection of finite open sets is open:

$$\forall \sigma [(\sigma \subseteq \tau \wedge \sigma \neq \varnothing \wedge |\sigma| < \aleph_0) \implies \bigcap \sigma \in \tau].$$

The elements of τ are called **open sets** and the collection τ is called a **topology** on X. A subset $C \subseteq X$ is said to be **closed** in (X, τ) if and only if its complement $X \setminus C$ is an element of τ, i.e., an open set.

Alternatively, a **topological space** is a set of **points**, along with a set of **neighbourhoods** for each point, satisfying a set of *axioms* relating points and neighbourhoods.

Remark. It can be viewed as how we group things together? Some intuition.

7.0.1.1.2 Neighbourhood, Base

Definition (neighbourhood of a set)**.** An **neighbourhood of a subset** S of a topological space (X, τ) is a subset N such that either one of the equivalent conditions hold

- $\exists U \in \tau [A \subseteq U \subseteq N]$.
- it is a neighbourhood of all the points in S.
- S is a subset of the interior $\mathring{N}$ of N,

Definition (neighbourhood of a point)**.** An **neighbourhood of point** x in topological space (X, τ) is a subset N such that

- either
$$\exists U \in \tau[x \in U \subseteq N],$$
- or N is a neighbourhood of set $\{ x \}$.

Definition (base)**.** A **base** or basis for the topology τ of a topological space (X, τ) is a family $\mathcal{B} \subseteq \tau$ such that every open set of the topology is equal to a union of some sub-family of $\mathcal{B}$.

Equivalently, $\mathcal{B}$ is a base of topology (X, τ) iff

$$\forall S[S \in \tau \iff \exists \mathcal{A} \subseteq \mathcal{B}(S = \bigcup \mathcal{A})].$$

Remark. $\mathcal{B} \subseteq \tau$ is induced from the above formula.

Definition (local base)**.** Given a topological space (X, τ), a **local base** for a point $x \in X$ is a collection of neighbourhoods $\mathcal{B}_x \subseteq \mathcal{N}_x$ such that all neighbourhoods U_x of x is a superset of some set B in $\mathcal{B}_x$:

$$\forall B \in \mathcal{B}_x \exists U_x \in \tau[x \in U_x \subseteq B] \wedge \forall U_x \in \tau \exists B \in \mathcal{B}_x[x \in U_x \implies B \subseteq U_x].$$

Equivalently,

$$\forall U_x[x \in U_x \in \tau \iff \exists B \in \mathcal{B}_x(B \subseteq U_x)].$$

7.0.1.1.3 Continuity

Definition (continuous function)**.** A **function** from a topological space (X, σ) to a topological space (Y, τ) is **continuous** if and only if *the inverse image for every open set is open*, i.e.,

$$\forall S \in \tau[\{ x \in X \mid f(x) \in S \} \in \sigma].$$

Theorem 7.1. *A continuous function $(X, \tau_X) \to (Y, \tau_Y)$ stays continuous if the topology τ_Y is replaced by a coarser topology and/or τ_X is replaced by a finer topology.*

Definition (continuity at a point)**.** Given two topological spaces (X, σ) and (Y, τ), A function $f\colon X \to Y$ is continuous at a point $x \in X$ if and only if $f^{-1}(V)$ is a neighborhood of x for every neighborhood V of $f(x)$ in Y, i.e.,

$$\forall V \in \tau \exists U \in \sigma[f(x) \in V \implies x \in U \subseteq f^{-1}(V)].$$

Theorem 7.2. *A function is continuous at every point if and only if it is a continuous function.*

Remark. Because an open set is a set that is a neighborhood of all its points.

Theorem 7.3. *The preimage of continuous function on a closed set is closed.*

Definition (open map)**.** A map is called an **open map** or a strongly open map if it maps open subsets of its domain to open subsets of its codomain.

Definition (homeomorphism)**.** A function between two topological spaces is a **homeomorphism** if it is *bijective* and both *the function and its inverse are continuous*, i.e., given $f\colon (X, \sigma) \to (Y, \tau)$, f is homeomorphism if and only if

- it is injective and surjective

  $$\forall x \in X \forall x' \in X[f(x) = f(x') \implies x = x'] \wedge \forall y \in Y \exists x \in X[f(x) = y],$$

- it is continuous

  $$\forall T \in \tau[\{\, x \in X \mid f(x) \in T \,\} \in \sigma],$$

- it is a strongly open map

  $$\forall S \in \sigma[\{\, f(x) \in Y \mid x \in S \,\} \in \tau].$$

7.0.1.1.4 Limit

Definition (limit point)**.** Given a topological space (X, τ), a point $x \in X$ is a **limit point** or cluster point or accumulation point of a subset $S \subseteq X$ if every (open) neighbourhood of x contains at least one point of S different from x itself, i.e.,

$$\forall U \in \tau[x \in U \implies \exists y \in U \cap S(x \neq y)].$$

Definition (limit of a sequence)**.** A point $x \in X$ of the topological space (X, τ) is a **limit** or limit point of the sequence $(x_n)_{n\in\mathbb{N}}$ if for every (open) neighbourhood U of x, there exists some $N \in \mathbb{N}$ such that for every $n \geq N$, $x_n \in U$, i.e.,

$$\forall U \in \tau[x \in U \implies \exists N \in \mathbb{N} \forall n \in \mathbb{N}(n \geq N \implies x_n \in U)].$$

Definition (adherent point)**.** An **adherent point** of a subset A of a topological space (X, τ), is a point $x \in X$ such that

$$\forall U \in \tau[x \in U \implies U \cap A \notin \varnothing].$$

Remark. This definition differs from that of a limit point, in that for a limit point it is required that every neighborhood of x contains at least one point of A **different from** x.

Thus every limit point is an adherent point, but the converse is not true. An adherent point of A is either a limit point of A or an element of A (or both).

Definition (isolated point)**.** An adherent point which is not a limit point is an **isolated point**.

7.0.1.1.5 Closure

Definition (closure)**.** The **closure** of a subset S of a topological space (X, τ), denoted by $\mathrm{cl}_{(X,\tau)} S$ or possibly by $\mathrm{cl}_X S, \mathrm{cl}\, S, \overline{S}, S^-$, can be defined using any of the following equivalent definitions: it is

- the set of all adherent points of S,
- the set S combined with all of its limit points,
- the intersection of all closed sets containing S,
- the smallest closed set containing S,
- the union of S and its boundary ∂S,

7.0.1.2 Metric Space

7.0.1.2.1 Definition

Definition (metric space)**.** A **metric space** is an ordered pair $(M, d\colon M \to \mathbb{R}_0^+)$ such that $\forall x, y, z \in M$, the following holds:

- identity of indiscernibles:

$$d(x, y) = 0 \iff x = y,$$

- symmetry:

$$d(x, y) = d(y, x),$$

- triangle inequality:

$$d(x, z) \leq d(x, y) + d(y, z).$$

d is called the **metric** on M.

7.0.1.2.2 Metric Topology

Definition (open ball)**.** Let (M, d) be a metric space. The **open (metric) ball** of radius $r \in \mathbb{R}^+$ centered at a point $p \in M$, usually denoted by $B_r(p)$ or $B(p; r)$, is defined by

$$B_r(p) = \{\, x \in M \mid d(x, p) < r \,\}.$$

Definition (metric topology)**.** The **metric topology** of a metric space (M, d) is the topology whose base is the set σ of all open balls

$$\sigma = \{\, B_r(p) \in \mathcal{P}(M) \mid r \in \mathbb{R}^+, p \in M \,\},$$

i.e., the metric topology τ is given by

$$\tau = \{\, \mathcal{S} \in \mathcal{P}(M) \mid \exists \sigma' [\sigma' \subseteq \sigma \wedge \mathcal{S} = \bigcup \sigma'] \,\},$$

or more explicitly

$$\tau = \{\, \mathcal{S} \in \mathcal{P}(M) \mid \exists \sigma' \forall \mathcal{T} \in \sigma' \exists r \in \mathbb{R}^+ \exists p \in M [\mathcal{T} = B_r(p) \wedge \mathcal{S} = \bigcup \sigma'] \,\}.$$

Remark. The metric topology on a metric space (M, d) is the coarsest topology on M relative to which the metric d is a continuous map from the product of M with itself to the non-negative real numbers.

7.0.1.2.3 Complete Metric Space

Definition (Cauchy sequence)**.** A sequence $(x_n)_{n\in\mathbb{N}}$ in a metric space (X, τ, d) is called **Cauchy** if for every positive real number $r > 0$ there is a positive integer $N \in \mathbb{Z}^+$ such that for all positive integers $m, n > N$, $d(x_m, x_n) < r$, i.e.,

$$\forall r \in \mathbb{R}^+ \exists N \in \mathbb{Z}^+ \forall m \in \mathbb{Z}^+ \forall n \in \mathbb{Z}^+ [(m > N \wedge n > N) \implies d(x_m, x_n) < r].$$

Definition (complete metric space)**.** A metric space (M, τ, d) is called **complete** (or a Cauchy space) if every Cauchy sequence $(x_n)_{n\in\mathbb{N}}$ of points in M has a limit x that is also in M.

Equivalently, given the class $\mathcal{C}$ of all Cauchy sequences in (M, d), the metric space is complete if and only if

$$\forall (x_n)_{n\in\mathbb{N}} \in \mathcal{C} \exists x \in M \forall \varepsilon \in \mathbb{R}^+ \exists N \in \mathbb{N} \forall n \in \mathbb{N} [n \geq N \implies d(x_n, x) < \varepsilon].$$

7.0.1.3 Normed Vector Space

Definition (normed vector space)**.** A **normed vector space** or normed space is a vector space $(V, +, \cdot, \|\cdot\| : V \to \mathbb{R}_0^+)$ over K (either $\mathbb{R}$ or $\mathbb{C}$), on which the norm $\|\cdot\|$, $\forall x \in V, a \in K$, has the following properties:

- $$\|x\| \geq 0,$$
- $$\|x\| = 0 \iff x = \mathbf{0},$$
- $$\|ax\| = |a| \|x\|,$$
- $$\|x + y\| \leq \|x\| + \|y\|.$$

Definition (norm induced metric)**.** The norm in a normed space $(V, +, \cdot, \|\cdot\|)$ induces its **(norm) induced metric**, by the formula

$$d(x, y) = \|y - x\|, \forall x, y \in V.$$

Therefore, a normed space can be expanded to $(V, +, \cdot, \tau, d, \|\cdot\|)$.

7.0.1.4 Inner Product Space

Definition (inner product space)**.** An **inner product space** is a vector space $(V, +, \cdot)$ over the field K (either $\mathbb{R}$ or $\mathbb{C}$) together with a positive-definite Hermitian form

$$\langle \cdot\,,\, \cdot \rangle \colon V \times V \to K.$$

Explicitly, $\forall a \in K, x, y, z \in V$

$$\begin{aligned} \langle ax, y\rangle &= a\langle x, y\rangle, \\ \langle x + y, z\rangle &= \langle x, z\rangle + \langle y, z\rangle, \\ \langle x, y\rangle &= \overline{\langle y, x\rangle}, \\ x \neq \mathbf{0} &\implies \langle x, x\rangle \in \mathbb{R}^+. \end{aligned}$$

Definition (canonical norm)**.** Every inner product space $(V, +, \cdot, \langle \cdot\,,\, \cdot \rangle)$ induces a norm, called its **canonical norm**, that is defined by

$$\|x\| = \sqrt{\langle x, x\rangle}, \forall x \in V.$$

Therefore, it can be expanded as $(V, +, \cdot, \tau, d, \|\cdot\|, \langle \cdot\,,\, \cdot \rangle)$.

7.0.1.5 Hilbert Space

7.0.1.5.1 Definition

Definition (Hilbert space)**.** A **Hilbert space** is a real or complex inner product space that is also a complete metric space with respect to the distance function induced by the inner product.

Theorem 7.4. *Finite-dimensional inner product spaces over $\mathbb{R}$ or $\mathbb{C}$ are metrically complete, and therefore Hilbert spaces.*

Remark. Inner product space can be a vector space over any quadratically closed subfield of $\mathbb{R}$ or $\mathbb{C}$. However, finite-dimensional inner product spaces over a proper subfield of $\mathbb{C}$ (that is, neither $\mathbb{R}$ nor $\mathbb{C}$) are not metrically complete.

7.0.1.5.2 Euclidean Space

Definition (Euclidean space)**.** A finite dimensional real inner product space is called a **Euclidean space**.

Remark. The definition is from *Introduction to Hilbert Spaces with Applications*, Second Edition by L. Debnath and P. Mikusinski, 1999. Page 92.

Corollary 7.5. *Each Euclidean space is complete, and therefore a real Hilbert space, i.e., a complete inner product space over* $\mathbb{R}$.

Proposition 7.6. *For any n-dimensional* ***Euclidean space***

$$(\mathbb{R}^n, +, \cdot, \tau, d, \|\cdot\|, \langle\,\cdot\,,\,\cdot\,\rangle),$$

there must be a basis such that

$$\begin{aligned}\langle x, y\rangle &= \sum_{i=1}^{n} x_i y_i,\\ \|x\| &= \sqrt{\sum_{i=1}^{n} x_i^2},\\ d(x,y) &= \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2},\end{aligned}$$

and

$$\begin{aligned}\tau = \{\mathcal{S} \in \mathcal{P}(\mathbb{R}^n) | \exists \sigma' \forall \mathcal{T} \in \sigma' \exists r \in \mathbb{R}^+ \exists p \in \mathbb{R}^n\\ [\mathcal{T} = \{\, x \in \mathbb{R}^n \mid \sum_{i=1}^{n} (x_i - p_i)^2 < r^2 \,\} \wedge \mathcal{S} = \bigcup \sigma']\},\end{aligned}$$

Proof. This is trivial if $n = 0$.

If $n > 0$, then pick any nonzero vector $x \in \mathbb{R}^n \setminus \{\, \mathbf{0} \,\}$ and set the first basis as $(x \neq \mathbf{0} \implies \|x\| \neq 0)$

$$e_1 = \frac{x}{\|x\|} \notin \{\, \mathbf{0} \,\},$$

therefore

$$\langle e_1, e_1\rangle = \frac{\langle x, x\rangle}{\|x\|^2} = 1,$$

by definition of the canonical norm.

If we get $(e_1, \dots, e_k)$ $(k < n)$ orthonormal basis such that $\langle e_i, e_j \rangle = \delta_{ij}$, then pick any vector from $x_{k+1} \in \mathbb{R}^n \setminus \operatorname{span}(e_1, \dots, e_k)$ (which must exist because $k < n$) and set

$$e'_{k+1} = x_{k+1} - \sum_{i=1}^{k} \langle x_{k+1}, e_i \rangle e_i \neq \mathbf{0},$$

$$e_{k+1} = \frac{e'_{k+1}}{\left\| e'_{k+1} \right\|} \notin \operatorname{span}(e_1, \dots, e_k).$$

$e'_{k+1} \neq \mathbf{0}$ because $x_{k+1} \notin \operatorname{span}(e_1, \dots, e_k)$. $e_{k+1} \notin \operatorname{span}(e_1, \dots, e_k)$ because $x_{k+1} \notin \operatorname{span}(e_1, \dots, e_k)$ and $\frac{1}{\left\| e'_{k+1} \right\|} \neq 0$.

Add e_{k+1} to the basis. Therefore $\langle e_{k+1}, e_{k+1} \rangle = 1$ (see above for e_1) and $\forall j \leq k$,

$$\begin{aligned}
\langle e_j, e_{k+1} \rangle = \langle e_{k+1}, e_j \rangle &= \frac{1}{\left\| e'_{k+1} \right\|} \left(\langle x_{k+1}, e_j \rangle - \sum_{i=1}^{k} \langle x_{k+1}, e_i \rangle \langle e_i, e_j \rangle \right) \\
&= \frac{1}{\left\| e'_{k+1} \right\|} \left(\langle x_{k+1}, e_j \rangle - \sum_{i=1}^{k} \langle x_{k+1}, e_i \rangle \delta_{ij} \right) \\
&= \frac{1}{\left\| e'_{k+1} \right\|} \left(\langle x_{k+1}, e_j \rangle - \langle x_{k+1}, e_j \rangle \right) \\
&= 0 \in \mathbb{R}.
\end{aligned}$$

Therefore $\langle e_i, e_j \rangle = \delta_{ij}$ holds up to $k + 1$.

This process ends when $k = n$. And we get a complete orthonormal basis. Any two vectors $x, y \in \mathbb{R}^n$ can be expressed as the unique linear combination of the basis:

$$x = \sum_{i=1}^{n} x_i e_i, y = \sum_{i=1}^{n} y_i e_i,$$

and from the orthonormal property and the Hermitian property of inner product, we get

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i,$$

since $y_i \in \mathbb{R}$. □

Remark. Actually, all Hilber spaces can be described this way. See 7.32.

Definition (Euclidean topology)**.** The τ defined in the above Euclidean space is called the **Euclidean topology**.

Proposition 7.7. *The real matrix algebra* $(\mathrm{M}_n(\mathbb{R}), +, \cdot, *)$ *can be defined as an* n^2*-dimensional real Hilbert space*

$$(\mathrm{M}_n(\mathbb{R}), +, \cdot, *, \tau, d, \|\cdot\|, \langle\cdot\,,\,\cdot\rangle)$$

with the inner product:

$$\langle A, B\rangle = \mathrm{tr}(AB^\intercal).$$

Proof. This is because

$$\begin{aligned}\mathrm{tr}(A+B) &= \mathrm{tr}(A) + \mathrm{tr}(B),\\ \mathrm{tr}(cA) &= c\,\mathrm{tr}(A),\\ \mathrm{tr}(A^\intercal) &= \mathrm{tr}(A),\\ \mathrm{tr}(P^{-1}AP) &= \mathrm{tr}(A).\end{aligned}$$

Therefore we have

$$\mathrm{tr}(BA^\intercal) = \mathrm{tr}((AB^\intercal)^\intercal) = \mathrm{tr}(AB^\intercal) \in \mathbb{R}.$$

and

$$\mathrm{tr}(AA^\intercal) = \mathrm{tr}(AA^\dagger) = \mathrm{tr}(QUQ^\dagger QU^\dagger Q^\dagger) = \mathrm{tr}(UU^\dagger) = \sum_{i=1}^{n}\sum_{k=1}^{n} U_{ik}\overline{U_{ik}},$$

where U is an upper triangular matrix and Q is a unitary matrix. This is done by Schur decomposition.

Therefore

$$\langle A, A\rangle = 0 \iff U = 0 \iff A = 0.$$

□

Remark. $\mathrm{tr}(AB^\intercal) = \sum_{i=1}^{n}\sum_{k=1}^{n} A_{ik}B_{ik}$. Therefore $\mathrm{M}_n(\mathbb{R}) \cong \mathbb{R}^{n^2}$.

7.0.2 Separation Axioms

7.0.2.1 Hausdorff Space

Definition (Hausdorff space)**.** A **Hausdorff space** or a T_2 space is a topological space satisfying the Hausdorff axiom (T_2 axiom), i.e., *any two distinct points possess disjoint neighbourhoods.*

Explicitly, a topological space (X, τ) is Hausdorff if and only if

$$\forall x, y \in X[x \neq y \implies \exists U_x, V_y \in \tau(x \in U_x \wedge y \in V_y \wedge U_x \cap V_y = \varnothing)].$$

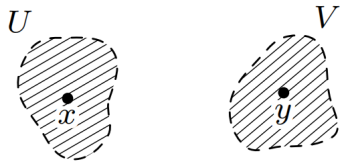


Figure 1: Hausdorff space

Theorem 7.8. *Any metric space is Hausdorff.*

Theorem 7.9. *A space X is Hausdorff iff*

$$\forall x \in X[\{ x \} = \bigcap_{U \ni x} \overline{U}],$$

where $\overline{U}$ is the closure of U.

Theorem 7.10. *In a Hausdorff space any sequence has at most one limit.*

Definition (hereditary properties)**.** A topological property is **hereditary** if it carries over from a space to its subspaces, i.e., if a space X has this property, then each subspace of X also has it.

Theorem 7.11. *The property of being a Hausdorff space is hereditary, i.e., each subspace of a Hausdorff space is Hausdorff.*

7.0.2.2 Topological Distinguishability and Separated Sets

Definition (topological distinguishability)**.** Given a topological space (X, τ) and $x, y \in X$, below statements are equivalent:

- x and y are **topologically distinguishable**,
- x and y do not have the same open neighbourhoods,
- at least one of them has a neighbourhood that is not a neighbourhood of the other,
- there is an open set that one point belongs to but the other point does not:

$$\exists U \in \tau[x \in U \iff y \notin U].$$

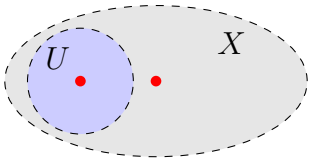


Figure 2: Topologically distinguishable points

Definition (separated sets)**.** Given a topological space (X, τ) and $A, B \subseteq X$, they are (from weaker to stronger condition)

1. **disjoint** iff
$$A \cap B = \varnothing;$$

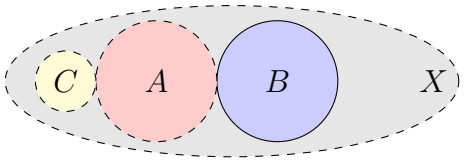


Figure 3: Disjoint sets

2. **separated** iff
$$A \cap \overline{B} = B \cap \overline{A} = \varnothing;$$

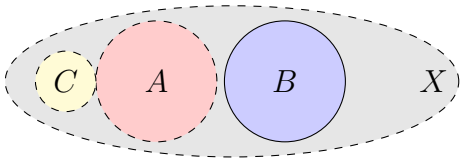


Figure 4: Separated sets

3. **separated by neighbourhoods** iff there are (open) neighbourhoods U of A and V of B such that U and V are disjoint:
$$\exists U, V \in \tau [A \subseteq U \wedge B \subseteq V \wedge U \cap V = \varnothing].$$

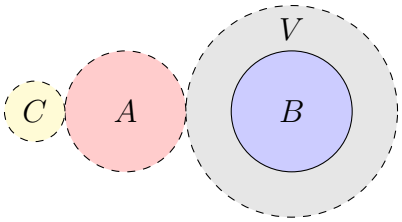


Figure 5: Separated by neighbourhoods

4. **separated by closed neighbourhoods** iff there is a closed neighbourhood U of A and a closed neighbourhood V of B such that U and V are disjoint:

$$\exists U \exists V \exists U_o, V_o \in \tau [X \setminus U \in \tau \wedge X \setminus V \in \tau \\ \wedge A \subseteq U_o \subseteq U \wedge B \subseteq V_o \subseteq V \wedge U \cap V = \varnothing],$$

or equivalently

$$\exists U_o, V_o, U^c, V^c \in \tau [A \subseteq U_o \wedge U_o \cap U^c = \varnothing \wedge B \subseteq V_o \wedge V_o \cap V^c = \varnothing \\ \wedge U^c \cup V^c = X],$$

which, geometrically, implies that there is a "wall" separating open neighbourhoods U_o and V_o.

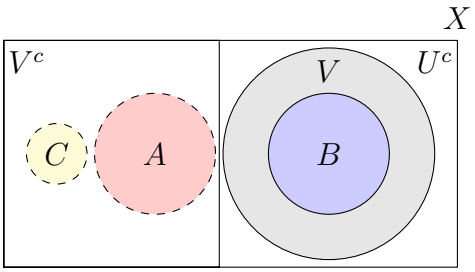


Figure 6: Separated by closed neighbourhoods

It can also be simplified using closure:

$$\exists U, V \in \tau [A \subseteq U \wedge B \subseteq V \wedge \overline{U} \cap \overline{V} = \varnothing].$$

5. **separated by a function** iff there exists a *continuous* function $f \colon X \to \mathbb{R}$ such that $f(A) = \{ 0 \}$ and $f(B) = \{ 1 \}$.

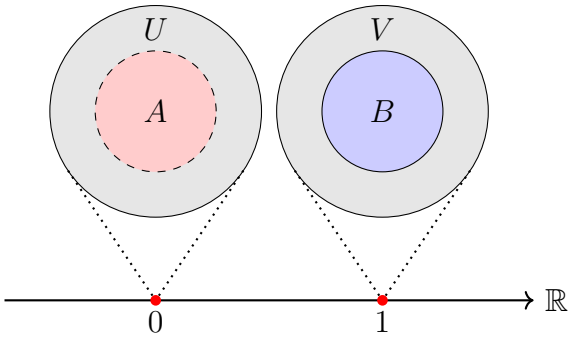


Figure 7: Separated by a function (U and V are zero sets)

6. **precisely separated by a function** if there exists a continuous function $f\colon X \to \mathbb{R}$ such that $f^{-1}(\{\,0\,\}) = A$ and $f^{-1}(\{\,1\,\}) = B$.

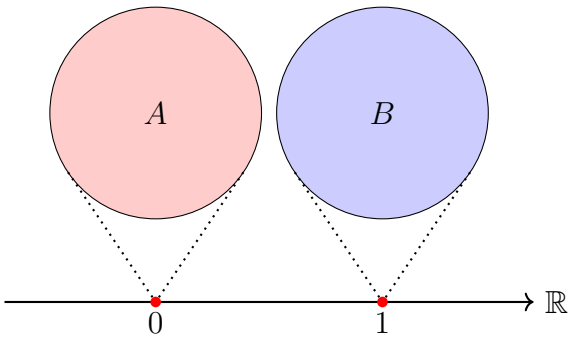


Figure 8: Precisely separated by a function (A and B are zero sets)

Definition (separated points)**.** Given a topological space (X, τ) and $x, y \in X$, below statements are equivalent:

- x and y are **separated**,
- $\{\,x\,\}$ and $\{\,y\,\}$ are separated,
- each of them has a neighbourhood that is not a neighbourhood of the other,
- $$\exists U_x, V_y \in \tau[x \in U_x \wedge x \notin V_y \wedge y \in V_y \wedge y \notin U_x].$$

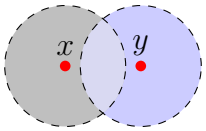


Figure 9: Separated points

Remark.

$$\{ x \} \cap \overline{\{ y \}} = \varnothing \iff x \notin \overline{\{ y \}} \iff U_x \subseteq X \setminus \overline{\{ y \}} \iff y \notin U_x \in \tau. \tag{7.1}$$

Proposition 7.12. *Two points x, y are not separated, iff for each neighbourhood U_x of x and each neighbourhood V_y of y, either one of them is a neighbourhood of both points.*

Proof. Given a topological space (X, τ) and two points $x, y \in X$ that are not separated, from definition of separated points, we get

$$\forall U_x, V_y \in \tau [x \notin U_x \vee x \in V_y \vee y \notin V_y \vee y \in U_x],$$

which is equivalent to

$$\forall U_x, V_y \in \tau [(x \in U_x \wedge y \in V_y) \implies (x \in V_y \vee y \in U_x)].$$

□

7.0.2.3 Hierarchy of Separation Axioms

7.0.2.3.1 Definition

Definition (separation axioms without T0)**.** Given a topological space X,

- X is R_0, or **symmetric**, if any two topologically distinguishable points in X are separated.
- X is R_1, or **preregular**, if any two topologically distinguishable points in X are separated by neighbourhoods.
- X is **regular** if any closed set $F \subseteq X$ and any point $x \in X \setminus F$ are separated by neighbourhoods.
- X is **completely regular** if any closed set $F \subseteq X$ and any point $x \in X \setminus F$ are separated by a continuous function.

- X is **normal** if any two disjoint closed subsets of X are separated by neighbourhoods.
- X is **normal regular** if it is both R_0 and normal. Every normal regular space is regular.
- X is **completely normal** if any two separated sets are separated by neighbourhoods.
- X is a G_δ space if every closed set is a G_δ set.
- X is **perfectly normal** if any two disjoint closed sets are precisely separated by a continuous function.

Remark. For perfectly normal space, see this for more equivalent definition: 7.26.

Definition (separation axioms)**.** Given a topological space (X, τ),

- X is T_0, or **Kolmogorov**, if any two distinct points in X are topologically distinguishable:
$$\forall x, y \in X[x \neq y \implies \exists U \in \tau(x \in U \iff y \notin U)].$$
- X is T_1, or **accessible**, if any two distinct points in X are separated. Equivalently, every single-point set is a closed set.
- X is **Hausdorff**, or T_2, if any two distinct points in X are separated by neighbourhoods.
- X is $T_{2\frac{1}{2}}$, or **Urysohn**, if any two distinct points in X are separated by closed neighbourhoods.
- X is **completely Hausdorff**, or completely T_2, if any two distinct points in X are separated by a continuous function.
- X is **regular Hausdorff**, or T_3, if it is both T_0 and regular.
- X is **Tychonoff**, or $T_{3\frac{1}{2}}$, if it is both T_0 and completely regular.
- X is **normal Hausdorff**, or T_4, if it is both T_1 and normal.
- X is **completely normal Hausdorff**, or T_5, if it is both completely normal and T_1.
- X is **perfectly normal Hausdorff**, or T_6, if it is both perfectly normal and T_1.

7.0.2.3.2 Properties

Lemma 7.13. *A topological space (X, τ) is not T_0 iff*

$$\exists x, y \in X[x \neq y \wedge \forall U \in \tau(X \in U \iff y \in U)].$$

Proposition 7.14. *For any nonempty T_0 topological space (X, τ) and $y \notin X$, one can always construct a non-T_0 space $(X \cup \{ y \}, \tau')$.*

Proof. Pick an arbitrary $x \in X$ and replace each of the open set $U \ni x$ with $U \cup \{ y \}$. Easy to prove the new collection of open sets is a topology on $X \cup \{ y \}$ in which x and y are not topologically distinguishable: □

Theorem 7.15. *Given a topological space (X, τ), the following statements are equivalent:*

- *X is regular topological space,*
- *any closed set $F \subseteq X$ and any point $x \in X \setminus F \in \tau$ are separated by **closed** neighbourhoods,*
- *given any point $x \in X$ and neighbourhood G of x, there is a closed neighbourhood E of x that is a subset of G,*
- *the closed neighbourhoods of each point in a topological space form a local base at that point.*

Theorem 7.16. *A topological space is normal if and only if any two disjoint closed sets can be separated by **a continuous function**.*

Theorem 7.17. *Given a topological space (X, τ), the following statements are equivalent:*

- *X is completely normal, i.e., every two separated sets can be separated by neighbourhoods,*
- *every subspace of X with subspace topology is a normal space,*
- *every open subset of X is normal with the subspace topology.*

Theorem 7.18. *Any T_1 topological real or complex vector space of dimension $n < \infty$ is homeomorphic to a finite dimensional Hilbert space.*

Remark. Are all topological (finite-dim) real vector spaces homeomorphic to a coordinate space?

See e.g. Rudin, Functional analysis, theorem 1.21.

Also: Is Rudin wrong? When is a finite dimensional topological vector space homeomorphic to coordinate space?

7.0.2.3.3 Visualization of Hierarchy

See Figure 10.

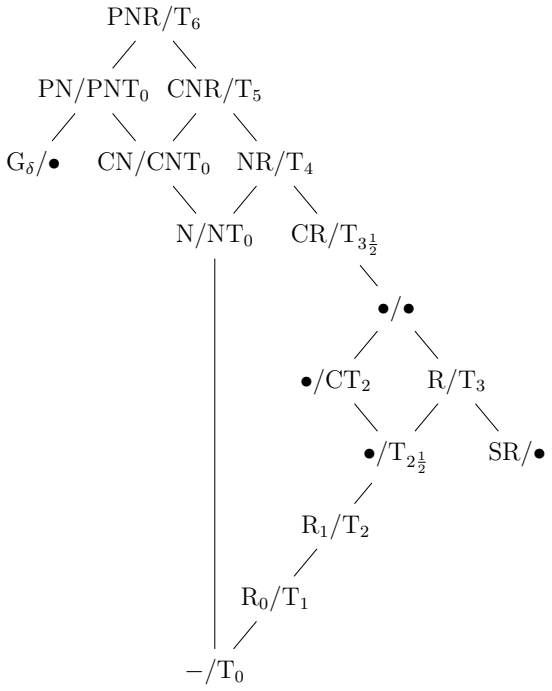
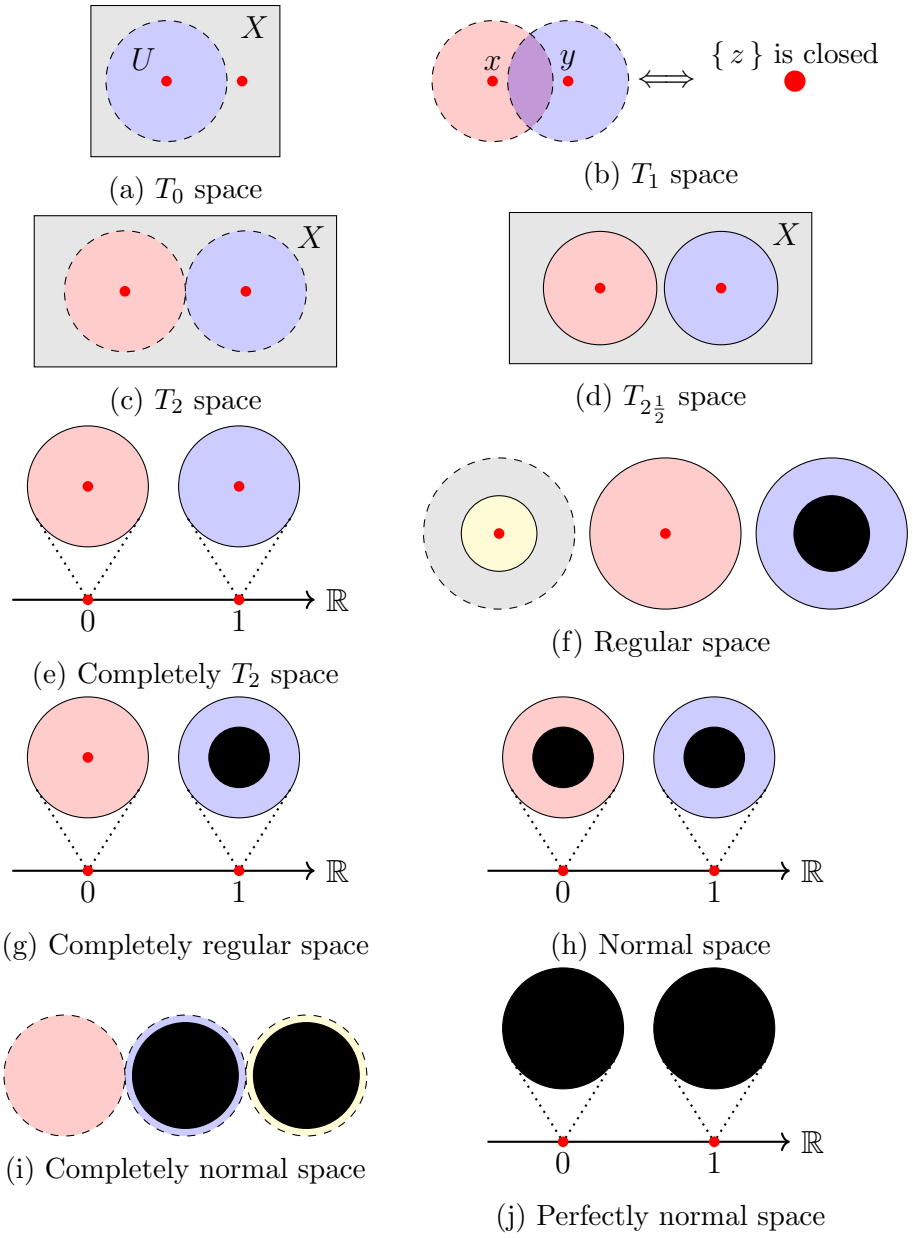


Figure 10: Hierarchy of separation axioms (SR=semiregular, iff, regular open sets (sets equal to the interiors of their closures) form a base).
Upper $\implies$ lower.
Left $+T_0$ $\iff$ Right.
N $+T_1$ $\iff$ T.
*N $+R_0$ $\iff$ *NR.
N $+G_\delta$ $\iff$ PN.

7.0.2.3.4 Visualization of Separation Axioms

See Figure 11.



(a) T_0 space

(b) T_1 space

(c) T_2 space

(d) $T_{2\frac{1}{2}}$ space

(e) Completely T_2 space

(f) Regular space

(g) Completely regular space

(h) Normal space

(i) Completely normal space

(j) Perfectly normal space

Figure 11: Visualized separation axiom.

More visualization: 1 , 2.

7.0.2.4 Metrizable Spaces

7.0.2.4.1 Definition

Definition (metrizable space)**.** A **metrizable space** is a topological space that is homeomorphic to a metric space.

Remark. Equivalently, a topological space (X, τ) is said to be metrizable if there is a metric $d\colon X \times X \to \mathbb{R}_0^+$ such that the topology induced by d is τ.

7.0.2.4.2 Necessary Condition: T_6

Theorem 7.19. *All metrizable spaces are perfectly normal Hausdorff (T_6).*

Remark. See this thread for details.

Definition (Gdelta set)**.** A G_δ **set** is a countable intersection of open sets.

Remark. Given a topology (X, τ), a set $A \subseteq X$ is G_δ iff

$$\exists \sigma \subseteq \tau [|\sigma| \leq \aleph_0 \wedge A = \bigcap \sigma]. \tag{7.2}$$

Corollary 7.20. *Open sets are G_δ.*

Proof. By definition. □

Theorem 7.21. *Given a topological space (X, τ) and a function f from X to a metric space, the set of points where such a function f is continuous is G_δ.*

Theorem 7.22. *For any G_δ subset $A \subseteq \mathbb{R}$, there is a function $f\colon \mathbb{R} \to \mathbb{R}$ that is continuous exactly at the points in A, i.e., f is continuous at x iff $x \in A$.*

Corollary 7.23. *It is possible for the irrationals to be the set of continuity points of a function, but it is impossible to construct a function that is continuous only on the rational numbers.*

Definition (Thomae's function)**.** The **Thomae's function** $f\colon \mathbb{R} \to \mathbb{R}$ is defined as

$$f(x) = \begin{cases} \frac{1}{q} & \exists p \in \mathbb{Z} \exists q \in \mathbb{N} [\gcd(p, q) = 1, x = p/q] \\ 0 & \text{otherwise} \end{cases}. \tag{7.3}$$

Theorem 7.24. *The Thomae's function is discontinuous at all rational numbers, continuous at all irrational numbers, and nowhere differentiable.*

Definition (zero set)**.** The **zero set** of a real-valued function $f\colon X \to \mathbb{R}$ is $f^{-1}(\{0\})$, i.e., the inverse image of $\{0\}$ in X.

Theorem 7.25. *The zero set of every real-valued continuous function is a G_δ set.*

Remark. Since zero set is the intersection of the open sets

$$\{\, x \in X \mid -1/n < f(x) < 1/n \,\}, \forall n \in \mathbb{Z}^+.$$

Theorem 7.26. *Given a topological space (X, τ), below are equivalent statements:*

- *X is perfectly normal;*
- *X is normal and every closed set is a G_δ set;*
- *Every closed set in X is a zero set of a real-valued continuous function, i.e.,*

  $$\forall U \in \tau \exists f \in \mathcal{C}^0(X, \mathbb{R}) \forall x \in X [f(x) = 0 \iff x \in X \setminus U],$$

  where $\mathcal{C}^0(X, \mathbb{R})$ denotes the class of real-valued continuous functions on X.

Remark. See this question: Why are these two definitions of a perfectly normal space equivalent?

Corollary 7.27. *In a metrizable space, every closed set is a G_δ set.*

Proof. Metrizable $\implies$ T_6 $\implies$ perfectly normal $\iff$ closed set is zero set. And zero set is G_δ. □

7.0.2.4.3 Sufficient Conditions

Theorem 7.28. *Every Hausdorff second-countable regular space is metrizable.*

Theorem 7.29. *A topological space is metrizable if and only if it is regular, Hausdorff and has a σ-locally finite base. A σ-locally finite base is a base which is a union of countably many locally finite collections of open sets.*

7.0.3 Compactness

7.0.3.1 Paracompactness and Compactness

Definition (cover)**.** A **cover** of a set X is a collection of sets whose union contains X. In symbols, $\mathcal{U}$ is a cover of X iff

$$X \subseteq \bigcup \mathcal{U}.$$

Definition (open cover)**.** A cover $\mathcal{U}$ of a topological space (X, τ) is **open** if all its members are open sets, i.e.,

$$\forall U \in \mathcal{U}[U \in \tau].$$

Definition (refinement of a cover)**.** A **refinement of a cover** of a set X is a new cover of the same set such that every set in the new cover is a subset of some set in the old cover. In symbols, $\mathcal{V}$ is a refinement of the cover $\mathcal{U}$ if and only if,

$$X \subseteq \bigcup \mathcal{V} \wedge \forall V \in \mathcal{V} \exists U \in \mathcal{U}[V \subseteq U].$$

Definition (open refinement)**.** An **open refinement of a cover** of a topological space (X, τ) is a refinement that is also an open cover. In symbols, $\mathcal{V}$ is a open refinement of the cover $\mathcal{U}$ if and only if,

$$X \subseteq \bigcup \mathcal{V} \wedge \forall V \in \mathcal{V}[V \in \tau \wedge \exists U \in \mathcal{U}(V \subseteq U)].$$

Definition (locally finite open cover)**.** An open cover of a topological space (X, τ) is **locally finite** if every point of the space has a neighborhood that intersects only finitely many sets in the cover. In symbols, $\mathcal{U}$ is locally finite if and only if,

$$\forall x \in X \exists V_x \in \tau[x \in V_x \wedge |\{\, U \in \mathcal{U} \mid U \cap V_x \neq \varnothing \,\}| < \aleph_0].$$

Definition (paracompact space)**.** A **paracompact space** is a topological space in which every open cover has an open refinement that is locally finite.

Remark. A topological space (X, τ) is paracompact iff

$$\forall \mathcal{U} \in \mathcal{P}(\tau)[X = \bigcup \mathcal{U} \implies \exists \mathcal{V} \in \mathcal{P}(\tau)\big(X = \bigcup \mathcal{V} \wedge \forall V \in \mathcal{V} \exists U \in \mathcal{U}(V \subseteq U) \wedge \forall x \in X \exists W_x \in \tau(x \in W_x \wedge |\{\, V \in \mathcal{V} \mid V \cap W_x \neq \varnothing \,\}| \in \mathbb{N})\big)].$$

Definition (subcover)**.** A **subcover** of a cover $\mathcal{C}$ of X is a subset of $\mathcal{C}$ that still covers the set X.

Remark. Every subcover is also a refinement, but the opposite is not always true.

Definition (compact space)**.** A topological space (X, τ) is **compact** if every open cover of X has a finite subcover, i.e.,

$$\forall \mathcal{U} \subseteq \tau[X = \bigcup \mathcal{U} \implies \exists \mathcal{V} \subseteq \mathcal{U}\big(X = \bigcup \mathcal{V} \wedge |\mathcal{V}| \in \mathbb{N}\big)]. \tag{7.4}$$

Remark. Compactness means "small" because you can describe the whole space finitely.

7.0.3.2 Other Compactness

Definition (point-finite cover)**.** A cover $\mathcal{U}$ of X is said to be point-finite if every point of X is contained in only finitely many sets in the cover, i.e.,

$$X \subseteq \bigcup \mathcal{U} \wedge \forall x \in X[|\{\, U \in \mathcal{U} \mid x \in U \,\}| \in \mathbb{N}].$$

Remark. A cover is point-finite if it is locally finite, though the converse is not necessarily true.

Definition (list of compactness)**.** A topological space (X, τ) is

- **sequentially compact** if every sequence of points in X has a convergent subsequence converging to a point in X,
- **limit point compact** if every infinite subset of X has a limit point in X,
- **countably compact** if every countable open cover has a finite subcover,
- **compact** if every open cover has a finite subcover,
- **Lindelöf** if every open cover has a countable subcover,
- **metacompact** if every open cover has a point-finite open refinement,
- **paracompact** if every open cover admits a locally finite open refinement.

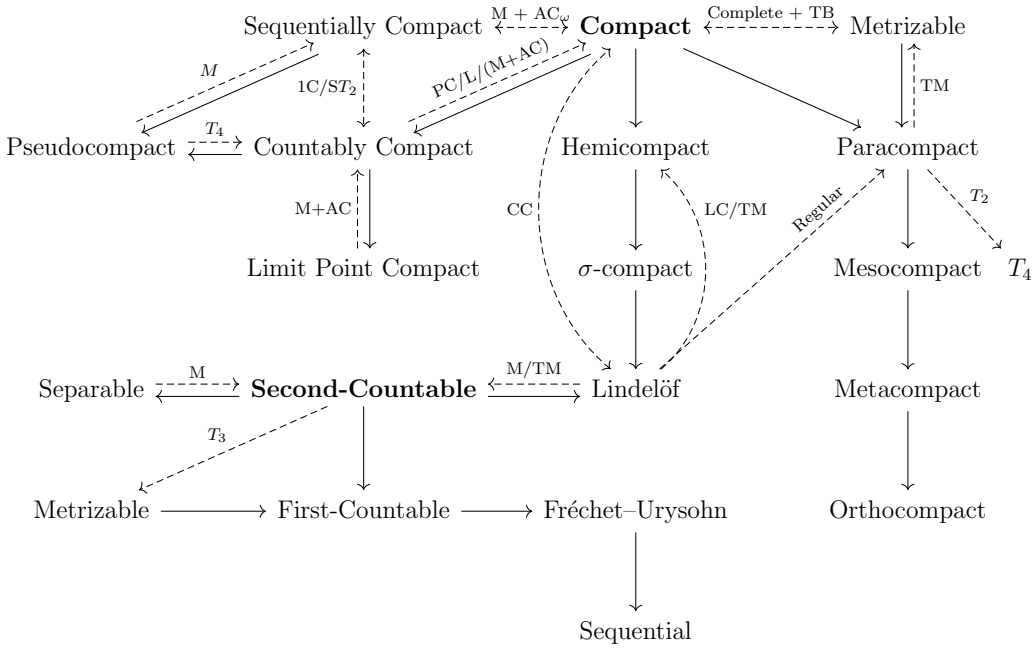


Figure 12: Hierarchy of compactness/countability:
solid line = unconditional, dashed line = conditional,
M = metrizable, L = Lindelöf, CC = countably compact, PC = paracompact, LC = locally compact, AC = axiom of choice, TB = totally bounded, ST_2 = sequential Hausdorff, 1C = first countable, TM = topological manifold (locally Euclidean T_2)

7.0.4 Countability Axioms

Definition (dense)**.** Let A and B be two sets in a topological space (X, τ). We call A is **dense** in B if the one of following equivalent conditions holds

- B is a subset of the closure of A, i.e., $B \subseteq \overline{A}$,
- points in B are adherent points of A, i.e., either in A or a limit point of A,
- all open neighbourhoods of $x \in B$ intersects with A, i.e.,

$$\forall x \in B \forall U \in \tau [x \in U \implies A \cap U \neq \varnothing],$$

- all open sets intersecting with B must also intersect A, i.e.,

$$\forall U \in \tau [B \cap U \neq \varnothing \implies A \cap U \neq \varnothing].$$

A is **everywhere dense** or simply dense (in X) iff $\overline{A} = X$, i.e.,

$$\forall U \in \tau [U \neq \varnothing \implies A \cap U \neq \varnothing].$$

Remark. Below shows the equivalence.

$$\forall x \in B \forall U \in \tau [x \in U \implies A \cap U \neq \varnothing],$$

iff (exchanging $\forall$)

$$\forall U \in \tau \forall x \in B [x \in U \implies A \cap U \neq \varnothing],$$

iff (definition of qualified $\forall$ and set intersection)

$$\forall U \in \tau \forall x [x \in B \cap U \implies A \cap U \neq \varnothing],$$

iff (right hand side is free of x, see 7.30)

$$\forall U \in \tau [\exists x \in B \cap U \implies A \cap U \neq \varnothing],$$

iff (definition and uniqueness of empty set)

$$\forall U \in \tau [B \cap U \neq \varnothing \implies A \cap U \neq \varnothing].$$

Proposition 7.30. *Given wff $\varphi(x)$ and wff ψ free of x, we have*

$$\forall x\big(\varphi(x) \implies \psi\big) \iff \exists x\varphi(x) \implies \psi.$$

Proof. Given wff $\varphi(x)$ and wff ψ free of x, we have

$$\forall x\big(\varphi(x) \implies \psi\big)$$

iff (definition of $\implies$)

$$\forall x\big(\neg\varphi(x) \vee \psi\big)$$

iff (ψ is free of x)

$$\big(\forall x\neg\varphi(x)\big) \vee \psi$$

iff (definition of $\forall$)

$$\big(\neg\exists x\varphi(x)\big) \vee \psi$$

iff (definition of $\implies$)

$$\exists x\varphi(x) \implies \psi.$$

□

Definition (countability axioms)**.** A topological space (X, τ) is called

- **sequential**: a set is open if every sequence convergent to a point in the set is eventually in the set,
- **first-countable**: every point has a countable local base,

$$\forall x \in X\exists\mathcal{B}_x\Big[\big(\,|\mathcal{B}_x| \leq \aleph_0\big) \wedge \forall U_x\big(x \in U_x \in \tau \iff \exists B \in \mathcal{B}_x(B \subseteq U_x)\big)\Big],$$

- **second-countable**: the topology has a countable base,

$$\exists\mathcal{B}\Big[\big(\,|\mathcal{B}| \leq \aleph_0\big) \wedge \forall S\big(S \in \tau \iff \exists\mathcal{A} \subseteq \mathcal{B}(S = \bigcup\mathcal{A})\big)\Big],$$

- **separable**: there exists a countable dense subset, i.e., there exists a sequence $\{\,x_n\,\}_{n=1}^{\infty}$ of elements of the space such that every nonempty open subset of the space contains at least one element of the sequence, or symbolically,

$$\exists S[|S| \leq \aleph_0 \wedge \forall U \in \tau\exists x \in S(U = \varnothing \vee x \in U)].$$

7.0.5 More on Metric Space

Theorem 7.31. *Any separable inner product space has an orthonormal basis.*

Remark. Use an infinite-dimensional analog of the Gram–Schmidt process to show this.

Theorem 7.32. *Any complete inner product space has an orthonormal basis.*

Remark. Use the Hausdorff maximal principle and the fact that in a complete inner product space orthogonal projection onto linear subspaces is well-defined to show this.

Theorem 7.33. *Every metric space admits partitions of unity.*

Theorem 7.34. *Every continuous real-valued function defined on a closed subset of a metric space can be extended to a continuous map on the whole space (Tietze extension theorem).*

Theorem 7.35. *Every real-valued Lipschitz-continuous map defined on a subset of a metric space can be extended to a Lipschitz-continuous map on the whole space.*

7.0.6 Connectedness

Definition (connected space)**.** For a topological space (X, τ) the following conditions are equivalent:

- X is **connected**, that is, it cannot be divided into two disjoint non-empty open sets:

$$\neg\exists A, B \in \tau [A \neq \varnothing \wedge B \neq \varnothing \wedge A \cup B = X \wedge A \cap B = \varnothing].$$

- X cannot be divided into two disjoint non-empty closed sets.
- X The only subsets of X which are both open and closed (clopen sets) are X and the empty set:

$$A \in \tau \wedge X \setminus A \in \tau \iff A \in \{ \varnothing, X \}.$$

- The only subsets of X with empty boundary are X and the empty set.
- X cannot be written as the union of two non-empty separated sets (sets for which each is disjoint from the other's closure).

- All continuous functions from X to $\{0,1\}$ are constant, $\{0,1\}$ is the two-point space endowed with the discrete topology.

Definition (connected components)**.** The maximal connected subsets (ordered by inclusion) of a non-empty topological space are called the **connected components** of the space.

Theorem 7.36. *The components of any topological space form a partition of the space: they are disjoint, non-empty, and their union is the whole space. Every component is a closed subset of the original space.*

Definition (path)**.** A **path** from a point x to a point y in a topological space X is a continuous function $f\colon [0,1] \to X$ with $f(0) = x, f(1) = y$.

Definition. A path-component of X is an equivalence class of X under the equivalence relation which makes x equivalent to y if there is a path from x to y, i.e.,

$$x \sim y \iff \exists f \in \mathcal{C}^0([0,1], X)[f(0) = x \wedge f(1) = y],$$

where $\mathcal{C}^0([0,1], X)$ is the class of all continuous function from $[0,1]$ to X.

Definition (path-connected space)**.** The space X is said to be path-connected (or pathwise connected or 0-connected) if there is exactly one path-component, i.e., if there is a path joining any two points in X.

Theorem 7.37. *A path-connected space is connected.*

Remark. Every path-connected space is connected. The converse is not always true: examples of connected spaces that are not path-connected include the extended long line L^* and the topologist's sine curve.

7.0.7 Manifold

7.0.7.1 Locally Euclidean Space

Definition (locally Euclidean)**.** A topological space (X, τ) is called **locally Euclidean** if every point in X has a neighborhood homeomorphic to an Euclidean space.

Remark. Given a topological space (X, τ), below statements are equivalent

- X is locally Euclidean,
- each point in X has an (open) neighborhood homeomorphic to an open neighborhood in Euclidean space,

- every point in X has a neighborhood homeomorphic to an open ball in some Euclidean space,
- each point in X has a neighborhood homeomorphic to the unit ball in an Euclidean space:

$$\{\,(x_1, x_2, \ldots, x_n) \in \mathbb{R}^n \mid x_1^2 + x_2^2 + \cdots + x_n^2 < 1\,\},$$

for some $n \in \mathbb{Z}^+$.

7.0.7.2 Topological Manifold

Definition (topological manifold)**.** A **topological manifold** is a locally Euclidean Hausdorff space.

Remark. In some pages, second countability is required.

Second countable and Hausdorff are point-set conditions; second countable excludes spaces which are in some sense "too large" such as the long line, while Hausdorff excludes spaces such as "the line with two origins".

Also see this: When (why) did we allow manifolds to be non-Hausdorff and/or non-second countable?

Definition (pure manifold)**.** If the dimensionality of the Euclidean space n is fixed for all points, then we call it a **pure manifold**, or an n-manifold.

Remark. The disjoint union of a sphere and a line in three-dimensional space is not a pure manifold. Since dimension is a local invariant (i.e. the map sending each point to the dimension of its neighbourhood over which a chart is defined, is locally constant), each connected component has a fixed dimension.

Definition (dimensionality of manifold)**.** The **dimensionality of a pure manifold** is the dimensionality, n, of the Euclidean space $\mathbb{R}^n$ to which the manifold is locally homeomorphic.

Theorem 7.38. *A manifold need not be connected, but every manifold M is a disjoint union of connected manifolds. These are just the connected components of M, which are open sets since manifolds are locally-connected. Being locally path connected, a manifold is path-connected if and only if it is connected. It follows that the path-components are the same as the components.*

7.0.7.3 Examples

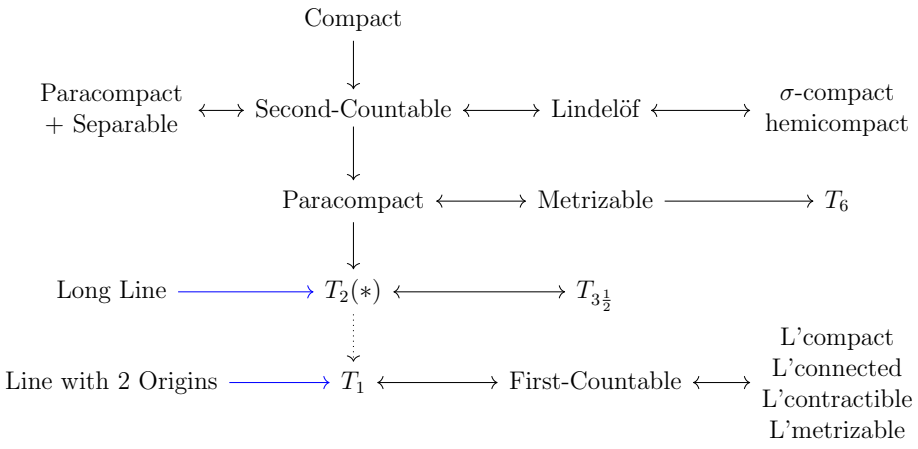


Figure 13: Hierarchy of manifolds. Any manifold above T_2 assumes T_2, whereas those below are necessary conditions of a locally Euclidean space. A Property starting with "L" indicates it is a local property.

7.0.7.3.1 Line with two origins

Definition (line with two origins)**. Line with two origins**, or bug-eyed line is the quotient space of two copies of the real line

$$\mathbb{R} \times \{ a \} \cup \mathbb{R} \times \{ b \}, (a \neq b),$$

with the equivalence relation

$$(x, a) \sim (x, b) \text{ if } x \neq 0.$$

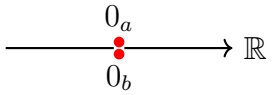


Figure 14: Line with two origins

Remark. Equivalently, this is the topological space

$$(\mathbb{R} \cup \{ 0' \}, \tau_{\mathbb{R}} \cup \{ U \triangle \{ 0, 0' \} \mid 0 \in U \in \tau \} \cup \{ U \cup \{ 0' \} \mid 0 \in U \in \tau \}),$$

where $\tau_{\mathbb{R}}$ is the Euclidean topology on $\mathbb{R}$ and $0' \notin \mathbb{R}$ is any mathematical object as a copy of $0 \in \mathbb{R}$.

This is a topology with two origins, 0 and $0'$. Each origin looks similar to the origin in $\mathbb{R}$, except that neighbourhoods contained both origins are added to the topology.

Proposition 7.39. *The line with two origins is T_1 but not T_2.*

Proof. There are neighbourhoods containing only one origin but not the other, so two origins are separated.

Since the open balls at either origin form a local base at that origin, the neighbourhood of 0 must contain

$$(-\varepsilon, \varepsilon)$$

and the neighbourhood of $0'$ must contain

$$(-\varepsilon', \varepsilon') \triangle \{ 0, 0' \}$$

where $\varepsilon, \varepsilon' > 0$ are positive real numbers. Then the intersection of both neighbourhoods must contain nonempty subset

$$(-\varepsilon_m, \varepsilon_m) \setminus \{ 0 \}$$

where $\varepsilon_m = \min(\varepsilon, \varepsilon')$. Therefore, two origins are not separated by neighbourhood. □

Proposition 7.40. *The line with two origins is locally Euclidean.*

Proof. Every point has a neighbourhood, containing at most one origin, locally homeomorphic to $\mathbb{R}$. □

7.0.7.3.2 Long line

Definition (order topology)**.** An **order topology**, or interval topology, defined on a *totally ordered set* with *at least two elements* is the topology whose base consists of open rays and open intervals.

Remark. Given a set X with strict total order $<$, if $|X| \geq 2$, then a base for the order topology is

$$\begin{aligned} &\{ \{ x \in X \mid a < x \} \in \mathcal{P}(X) \mid a \in X \} \\ \cup &\{ \{ x \in X \mid x < b \} \in \mathcal{P}(X) \mid b \in X \} \\ \cup &\{ \{ x \in X \mid a < x < b \} \in \mathcal{P}(X) \mid a, b \in X \}. \end{aligned} \tag{7.5}$$

Definition (closed long ray)**.** The **closed long ray** L is defined as the Cartesian product of the first uncountable ordinal ω_1 with the half-open interval $[0, 1)$, equipped with the order topology that arises from the lexicographical order on $\omega_1 \times [0, 1)$.

Remark. The closed long ray consists of an uncountable number of copies of $[0, 1)$ "pasted together" end-to-end.

It can be viewed as the "shortest line segment of uncountable length" (?).

The closed ray $[0, +\infty) \subseteq \mathbb{R}$ can be viewed as $\omega \times [0, 1)$ where ω is the first infinite ordinal.

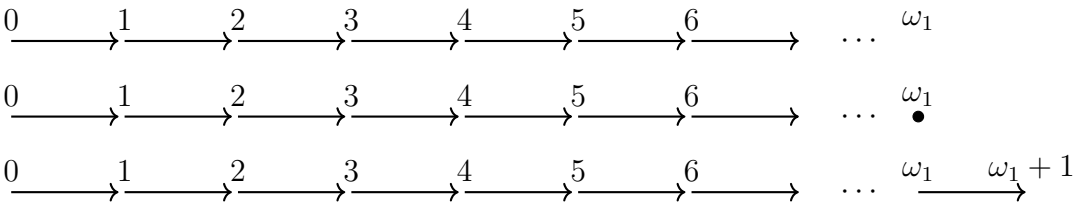


Figure 15: Above: the closed long ray.
Middle: the closed extended long ray.
Below: a ray too long to be locally Euclidean.

Definition (long line)**.** The **long line** can be constructed as the order topology on the disjoint union of the reversed **open long ray** ("reversed" means the order is reversed, "open" means the smallest element $(0, 0)$ is removed) and the (not reversed) closed long ray, totally ordered by letting the points of the latter be greater than the points of the former.

Remark. Intuitively, this is obtained by putting together a long ray in each direction.

Definition (extended long line)**.** The (closed) **extended long ray**, L^*, is obtained as the one-point compactification of L by adjoining an additional element to the right end of L.
One can similarly define the **extended long line** by adding two elements to the long line, one at each end.

Lemma 7.41. *Given two ordinal numbers α, β,*

$$\alpha < \beta \iff \alpha \in \beta.$$

Lemma 7.42. *The order topology on $\alpha \times [0, 1)$ is homeomorphic to $[0, 1)$ iff α is countable.*

Proposition 7.43. *The long line is locally homeomorphic to $\mathbb{R}$, but if we tried to glue together more than ω_1 copies of $[0, 1)$, the resulting space would no longer be locally homeomorphic to $\mathbb{R}$.*

Proof. See this for the proof.

We only need to prove local homeomorphism at $\langle \lambda, 0 \rangle$ where λ is a limit ordinal. Since $\lambda \in \omega_1$, we know $\lambda < \omega_1$ (7.41). Meanwhile, ω_1 is the *first* uncountable ordinal, meaning λ must be countable ordinal. Therefore $\lambda \times [0, 1)$ is homeomorphic to $[0, 1)$ (7.42).

For $(\omega_1 + 1) \times [0, 1)$, since $\omega_1 \in (\omega_1 + 1)$ is an uncountable limit point, no neighbourhood of $\langle \omega_1, 0 \rangle$ is homeomorphic to $\mathbb{R}$. □

Remark. The long ray is sequentially compact but not Lindelöf.

Other properties of (possibly extended) long rays and lines:

- are T_4 spaces;
- have the same cardinality as the real line, yet they are "much longer";
- are locally compact;
- is not metrizable.

Properties of (non-extended) long line or ray:

- is not paracompact;
- is path-connected, locally path-connected and simply connected but not contractible;
- is first-countable but not second countable and not separable.

Every connected (non-empty) one-dimensional (not necessarily separable) topological manifold possibly with boundary, is homeomorphic to either one of them

- the circle,
- the closed interval, the open interval (real line), the half-open interval,
- the closed long ray, the open long ray, or the long line.

There are $2^{\aleph_1}$ pairwise non-diffeomorphic smooth structures on the long line.

The extended long line is connected but "too long" to be path-connected.

7.0.7.3.3 "Abnormal" manifold See this thread.

Let $L_+ = \omega_1 \times [0,1) \setminus \langle 0,0 \rangle$ be the open long ray, and set $\Omega = \{ \langle \alpha, 0 \rangle \in L_+ \mid \alpha \in \omega_1 \}$. Take $M = L_+ \times (-1,1) \setminus \Omega \times \{ 0 \}$. Then M is a 2-manifold since Ω is closed in L_+. But the two closed sets $A = \bigcup_{\alpha \in \omega_1} \{ \langle \alpha, 0 \rangle \} \times (0,1)$ and $B = (L_+ \setminus \Omega) \times \{ 0 \}$ cannot be separated by disjoint open sets.

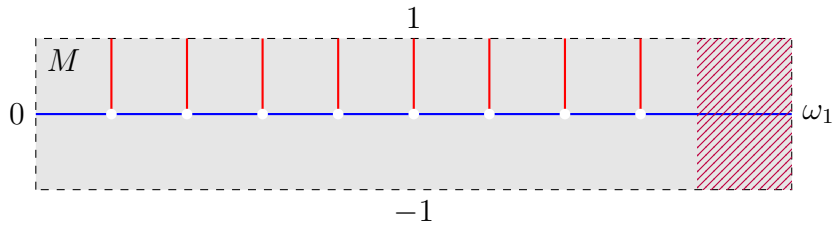


Figure 16: A T_2 locally Euclidean space that is not T_4. Red vertical lines are A and blue horizontal line is B.

7.0.7.4 Atlas

Definition (Euclidean neighborhoods)**.** In a locally Euclidean space, the neighbourhoods homeomorphic to an open subset of an Euclidean space are called **Euclidean neighborhoods**.

Theorem 7.44. *A topological space is locally Euclidean if and only if it can be covered by Euclidean neighborhoods.*

Definition (coordinate chart)**.** For any Euclidean neighborhood U, a homeomorphism $\varphi \colon U \to \varphi(U) \in \tau(\mathbb{R}^n)$ is called a **coordinate chart** on U.

Definition (atlas)**.** An **atlas** for a locally Euclidean space M is an indexed family

$$\{ (U_\alpha, \varphi_\alpha) \mid \alpha \in I \}$$

of charts on M which covers M (that is, $\bigcup_{\alpha \in I} U_\alpha = M$).

Definition (adequate atlas)**.** An atlas $(U_i, \varphi_i)_{i \in I}$ on an n-dimensional manifold M is called an **adequate atlas** if *all* the following conditions hold:

- the image of each chart is either the Euclidean space $\mathbb{R}^n$ or the closed half space $\mathbb{R}^n_+$,
- $(U_i)_{i \in I}$ is a locally finite open cover of M,
- $M = \bigcup_{i \in I} \varphi_i^{-1}(B_1)$, where B_1 is the unit open ball centered at the origin.

Theorem 7.45. *Any cover $\mathcal{V}$ of a* ***second-countable*** *manifold admits an adequate atlas $(U_i, \varphi_i)_{i\in I}$ such that $\mathcal{U} = (U_i)_{i\in I}$ is a refinement of $\mathcal{V}$.*

Proof. J. Dugundji, Topology. Allyn and Bacon, Boston, 1966. XI, P241, Theorem 7.2

7.2 Theorem The following three properties are equivalent:

(1). Y is σ-compact.

(2). Y can be represented as $Y = \bigcup_1^\infty U_i$, where each U_i is a relatively compact open set, and $\bar{U}_i \subset U_{i+1}$ for each $i \in Z^+$.

(3). Y is a Lindelöf locally compact space.

Proof: (1) $\Rightarrow$ (2). We have $Y = \bigcup_1^\infty C_i$ where each C_i is compact. Since Y is locally compact, there is [**6.2**(3)] a relatively compact open $U_1 \supset C_1$ and, proceeding inductively, we choose U_n to be a relatively compact open set containing the compact $\bar{U}_{n-1} \cup C_n$. The sets $\{U_n \mid n \in Z^+\}$ evidently satisfy the requirements.

(2) $\Rightarrow$ (3). Let $\{V_\alpha \mid \alpha \in \mathscr{A}\}$ be any open covering of Y. For each $i \in Z^+$, extract finitely many sets $\{V_{ij} \mid 1 \leqslant j \leqslant n(i)\}$ to cover $\bar{U}_i$; then the family $\{V_{ij} \mid 1 \leqslant j \leqslant n(i),\ i \in Z^+\}$ is a countable subcovering.

(3) $\rightarrow$ (1). Let $\{V(y) \mid y \in Y\}$ be a covering by relatively compact nbds, and extract a countable subcovering.

Kosinski, Antoni A. (1993). Differential manifolds. Academic Press, Inc. I, P5, Definition 2.1

(2.1) ***Definition*** An atlas $\{U_\alpha, h_\alpha\}$ on M is said to be *adequate* if it is locally finite, $h_\alpha(U_\alpha) = \mathbf{R}^m$ or $\mathbf{R}^m_+$ and $\bigcup_\alpha h_\alpha^{-1}(\mathring{D}^m) = M$.

I, P6, Theorem 2.2

(2.2) Theorem *Let $\mathcal{V} = \{V_\beta\}$ be a covering of M. Then there is an adequate atlas $\{U_\alpha, h_\alpha\}$ such that $\{U_\alpha\}$ is a refinement of $\mathcal{V}$.*

In particular, it follows that a smooth manifold is paracompact.

Proof Since M is locally compact, Hausdorff, and second countable, we obtain easily (*cf.* [Du,XI,7.2]) that there is a sequence $\{K_i\}$, $i = 1, 2, \ldots$, of open subspaces of M, with compact closures, and such that $\bar{K}_i \subset K_{i+1}$ and $\bigcup_i K_i = M$. We also set $K_0 = K_{-1} = \emptyset$.

We construct now the desired refinement in stages; the ith stage is as follows: Let $p \in \bar{K}_i - K_{i-1}$ and suppose that $p \in V_\beta$. Let (U_p, h_p) be a chart such that $h_p(U_p) = \mathbf{R}^n$, $h_p(p) = \mathbf{0}$, and $U_p \subset (K_{i+1} - \bar{K}_{i-2}) \cap V_\beta$.

Now, $\bar{K}_i - K_{i-1}$ is compact, and the sets $h_p^{-1}(\mathring{D}^m)$ cover it. Hence there is a finite family that does the same; let $U_1^i, \ldots, U_{k_i}^i$ be the corresponding

charts. Then the family $\mathcal{U} = \{U_j^i\}$, $i = 1, 2 \ldots, j = 1, 2, \ldots, k_i$ is locally finite: Every point of M is contained in one of the open sets K_i and each such set intersects—at most—only the U_j^m with $m \leq i + 2$. It is clear that $\mathcal{U}$ is a refinement of $\mathcal{V}$ and an adequate atlas. □

□

Remark. Since σ-compactness is equivalent to second-countability in topological manifold, the proof given here can not be applied to paracompact manifolds.

Definition (transition map)**.** Suppose that $(U_\alpha, \varphi_\alpha)$ and (U_β, φ_β) are two charts for a manifold M such that $U_\alpha \cap U_\beta$ is non-empty. The **transition map** $\tau_{\alpha,\beta} \colon \varphi_\alpha(U_\alpha \cap U_\beta) \to \varphi_\beta(U_\alpha \cap U_\beta)$ is the map defined by

$$\tau_{\alpha,\beta} = \varphi_\beta \circ \varphi_\alpha^{-1}.$$

Proposition 7.46. *Transition map is homeomorphism between open subsets of Euclidean spaces.*

Proof. Since composition and inverse of homeomorphism is homeomorphism. □

7.0.7.5 Differential Manifold

Definition (differentiability class)**.** Given a function f, it is (from weaker to stronger condition)

1. of **(differentiability) class** C^r if the derivatives $f', f'', ..., f^{(r)}$ exist and are continuous;
2. infinitely differentiable, **smooth**, or of class C^∞, if it is C^r for all natural numbers r;
3. of class C^ω, or **analytic**, if f is smooth and if its Taylor series expansion around any point in its domain converges to the function in some neighborhood of the point.

Remark. $C^\omega \subsetneqq C^\infty \subsetneqq \dots C^1 \subsetneqq C^0$.

Definition (differential atlas)**.** An atlas is called C^r if all transition maps in the atlas is C^r.

Corollary 7.47. *All atlases are C^0.*

Definition (compatible atlases)**.** Two C^r atlases are (C^r-)compatible iff the union is still a C^r atlas, i.e., the transition maps between them are C^r.

Remark. See this for more information: Can't understand the definition of equivalence of topological atlas.

Corollary 7.48. *All atlases are C^0-compatible.*

Theorem 7.49. *Compatibility of atlases is a equivalence relation.*

Definition (maximal atlas)**.** The **maximal atlas** of an atlas is the equivalence class of the atlas, i.e., the union of all atlases compatible to a given one.

Remark. Kosinski, Antoni A. (1993). Differential manifolds. Academic Press, Inc. I, P2, Definition 1.1:

Two different atlases may yield the same result. They certainly will if they are compatible, in the sense that their union is an atlas. This relation of compatibility is an equivalence relation; hence every atlas is contained in a maximal one: the union of all atlases compatible with it.

Wikipedia says "Unlike an ordinary atlas, the maximal atlas of a given manifold is unique."

In general, this is not true. See this question: Is the maximal atlas for a topological manifold unique?

However, the maximal atlas of a given manifold *equipped with some differential atlas* should be unique per Zorn's lemma.

Remark 3.2.2 *Every atlas $\mathcal{A}$ determines a unique maximal atlas $\mathcal{A}_{max}$. Hence, for practical purposes it is enough to just specify an atlas.*

Proof. Recall Zorn's lemma: If a poset (partially ordered set) P has the property that every chain in P has an upper bound in P, then P contains a maximal element.

Now the set P of all atlases containing a given atlas $\mathcal{A}$ is partially ordered by inclusion. Given a chain $\mathcal{A}_j$ in P the set $\bigcup_\alpha A_\alpha \in P$. Hence Zorn's lemma implies that there is a maximal atlas containing $\mathcal{A}$. ■

Definition (differential manifold)**.** A maximal C^r atlas on a manifold M is called a C^r **structure**. A **differential manifold** M of class C^r consists of a *(preferably second countable)* Hausdorff topological space M and a C^r structure on it.

Below are aliases of different types of differential manifold.

Differentiability	Atlas type	Structure type	Manifold type
C^∞	smooth atlas	smooth structure	**smooth manifold**
C^ω	analytic atlas	analytic structure	**analytic manifold**

Remark. There are some benefits of enforcing second countability:

Is an immersed submanifold second-countable?

When (why) did we allow manifolds to be non-Hausdorff and/or non-second countable?

Corollary 7.50. *A differential manifold is a (possibly second-countable) topological manifold, i.e., the existence of an atlas grants its locally Euclidean property.*

Theorem 7.51. *Every C^r structure, if $r \geq 1$, contains a smooth structure.*

Proof. See H. Whitney, Differentiable manifolds. Ann. of Math. 37 (1936), 645-680. □

7.0.7.6 Complex Manifold

Definition (complex chart)**.** Given a neighborhood U of a topological space, a homeomorphism $\varphi\colon U \to \varphi(U) \in \tau(\mathbb{C}^n)$ to a open subset of a finite dimensional Hilbert space is a (complex) **chart** on U.

Definition (holomorphic function)**.** A **holomorphic function** is a complex-valued function of one or more complex variables that is complex differentiable in a neighbourhood of each point in a domain in complex coordinate space $\mathbb{C}^n$.

Theorem 7.52. *All holomorphic functions are complex analytic functions, and vice versa.*

Definition (biholomorphically compatible charts)**.** Two overlapping charts $(U_\alpha, \varphi_\alpha)$ and (U_β, φ_β) are called **biholomorphically compatible** if the transition map

$$\tau_{\alpha,\beta} \colon \varphi_\alpha(U_\alpha \cap U_\beta) \to \varphi_\beta(U_\alpha \cap U_\beta)$$

defined by

$$\tau_{\alpha,\beta} = \varphi_\beta \circ \varphi_\alpha^{-1}$$

is biholomorphic, i.e., holomorphic, bijective and possessing a holomorphic inverse.

Definition (holomorphic atlas)**.** Given a topological space X, an **holomorphic atlas**, if existent, is an indexed family

$$\{\, (U_\alpha, \varphi_\alpha) \mid \alpha \in I \,\}$$

of pairwise biholomorphically compatible (complex) charts on X which covers X (that is, $\bigcup_{\alpha \in I} U_\alpha = X$).

Remark. There is a unique maximal atlas for a given atlas. But, unlike real charts, the codomain of charts actually matters, as an open ball in $\mathbb{R}^n$ is not holomorphic to $\mathbb{R}^n$.

Definition (complex manifold)**.** A **complex manifold** is a Hausdorff topological space M equipped with a complex structure, i.e., a maximal holomorphic atlas.

Lemma 7.53. *The space $\mathbb{R}^{2n}$ is homeomorphic to $\mathbb{C}^n$.*

Proof. Choose a orthonormal basis $(e_k)_{k=1,\dots,2n}$ for $\mathbb{R}^{2n}$ and $(e'_k)_{k=1,\dots,n}$ for $\mathbb{C}^n$, which always exists due to 7.32, then the inner product in $\mathbb{R}^{2n}$ is expressed as

$$\langle x, y \rangle = \sum_{i=1}^{2n} x_i y_i,$$

and the inner product in $\mathbb{C}^n$ is

$$\langle x, y\rangle = \sum_{i=1}^{n} x_i \overline{y_i},$$

then the map

$$\sum_{k=1}^{n} x_k e_k + x_{k+n} e_{k+n} \mapsto \sum_{k=1}^{n} (x_k + x_{k+n} i) e'_k$$

is a homeomorphism. □

Corollary 7.54. *All complex manifolds are locally Euclidean.*

Confirm "local compactness" is not needed here.

7.0.7.7 Diffeomorphism

Definition (differentiable at a point)**.** Given two C^k $(r \leq k)$ manifolds, M_1 and M_2, a map $f\colon M_1 \to M_2$ is called **differentiable (or C^r) at a point** $p \in M_1$ iff there is a chart (U_1, φ_1) in M_1 and a chart (U_2, φ_2) in M_2 and $U \subseteq M_1$ such that

$$p \in U \wedge f(p) \in f(U) \wedge U \subseteq U_1 \wedge f(U) \subseteq U_2$$

and the map from an open set of a finite-dimensional Hilbert space onto an open set of a finite-dimensional Hilbert space

$$\varphi_2 \circ f \circ \varphi_1^{-1}\colon \varphi_1(U) \to \varphi_2(f(U))$$

is differentiable or C^r at point $\varphi_1(p)$.

$$\begin{array}{ccc} U \subseteq U_1 \subseteq M_1 & \xrightarrow{\quad f \quad} & f(U) \subseteq U_2 \subseteq M_2 \\ {\scriptstyle \varphi_1^{-1}}\uparrow & & \downarrow{\scriptstyle \varphi_2} \\ \varphi_1(U) \subseteq K^{n_1} & \xrightarrow{\quad \varphi_2 \circ f \circ \varphi_1^{-1} \quad} & \varphi_2(f(U)) \subseteq K^{n_2} \end{array}$$

Remark. One can choose $U = f^{-1}(U_2) \cap U_1$. Or choose $U = U_1$ by enforcing $f(U_1) \subseteq U_2$.

In general, there will be many available charts; however, the definition of differentiability does not depend on the choice of chart at p. It follows from the chain rule applied to the transition functions between one chart and another that if f is differentiable in any particular chart at p, then it is differentiable in all charts at p.

Definition (differentiable map)**.** A map is called **differentiable (or C^r)** if it is differentiable (or C^r) at all points in the domain.

Definition (differentiable function)**.** A **differentiable function** on a differential manifold is a differential map from the manifold to $\mathbb{R}^n$ or $\mathbb{C}^n$.

Definition (diffeomorphism)**.** A (C^r-)**diffeomorphism** f is a bijection such that both f and f^{-1} are (C^r-)differentiable. Two differential manifolds are (C^r-)**diffeomorphic** if there is a (C^r-)diffeomorphism between them.

Remark. All concept above can be generalized to holomorphic maps.

7.0.7.8 Tangent Space From now on, every manifold/mapping/atlas is assumed the same class of smoothness, being either C^r with $r \geq 1$, smooth, analytic, or holomorphic. For the sake of simplicity, the term "differentiable" is adopted to represent all these cases unless specified explicitly, i.e., assuming at least C^1.

Definition (differentiable curve)**.** A **differentiable curve** on a real differential manifold M is a differentiable map from a non-empty (preferably connected) real 1-manifold to M

Remark. The domain is usually set as an interval in $\mathbb{R}$.

Definition (holomorphic curve)**.** A **holomorphic curve** in a complex manifold M is a non-constant holomorphic map f from the complex plane to M.

Remark. Note that $\mathbb{C}$ is not holomorphic to an open ball.

Definition (initialized differential curve)**.** Given a real differentiable manifold $(M, \tau, \mathcal{A})$ and a point $x \in M$, a **differentiable curve initialized at** x is a differentiable curve $\gamma\colon (-1, 1) \to M$ such that $\gamma(0) = x$.

Remark. We need some special treatment for complex manifolds.

Remark. Initialized differential curve might also be defined in this way:

Given a real differentiable manifold $(M, \tau, \mathcal{A})$ and a point $x \in M$, pick a coordinate chart $(\varphi\colon U \to \mathbb{R}^n)$ from the atlas $\mathcal{A}$, where U is an open neighbourhood of x (that is, $x \in U \in \tau$). Let $\gamma\colon (-1, 1) \to U$ be a mapping such that $\gamma(0) = x$ and that $\varphi \circ \gamma\colon (-1, 1) \to \mathbb{R}^n$ is differentiable, then γ is a **differentiable curve initialized at** x.

The codomain is dependent on the choice of the coordinate chart, and the algebra of differentiable curves initialized at a given point defined this way might be smaller than allowing the codomain to be the whole manifold (?

need proof!). (even though the image is restricted within a path-connected component (?) but there might not be a single coordinate chart covering the whole path-connected component, or is there???)

However, when considering local property, it should be equivalent to allowing the codomain to be the whole manifold.

Definition (tangent space)**.** Given a real differentiable manifold $(M, \tau, \mathcal{A})$ and a point $x \in M$, pick a coordinate chart $(\varphi\colon U \to \mathbb{R}^n)$ from the atlas $\mathcal{A}$, where U is an open neighbourhood of x (that is, $x \in U \in \tau$). Let $\gamma_1, \gamma_2\colon (-1, 1) \to M$ be two differentiable curves initialized at x ($\gamma_1(0) = x = \gamma_2(0)$), they are said to be **equivalent at** 0 if and only if the derivatives of $\varphi \circ \gamma_1|_{\gamma_1^{-1}(U)}$ and $\varphi \circ \gamma_2|_{\gamma_2^{-1}(U)}$ at 0 coincide.

The quotient space of all differentiable curves initialized at x by this equivalence relation is the **tangent space** of M at x, denoted T_xM, and equivalence classes in the tangent space are known as **tangent vectors** of M at x, denoted $\gamma'(0)$.

One can define a bijective linear map $\mathrm{d}\varphi_x\colon T_xM \to \mathbb{R}^n$ as

$$\mathrm{d}\varphi_x(\gamma'(0)) = \frac{\mathrm{d}}{\mathrm{d}t}[\varphi \circ \gamma(t)]\bigg|_{t=0},$$

where $\gamma \in \gamma'(0)$ is a curve in the equivalence class.

Remark. The definition does not depend on the choice of coordinate chart.

Definition. directional derivative

TODO, structure sheaf

7.0.8 Sheaf and Germ

7.0.8.1 Category Theory Continued See Commutative Diagram and More on Category Theory for background.

7.0.8.1.1 Category of Sets

Definition (partial function)**.** A **partial function** f from a set X to a set Y is a function $S \to Y$, where $S \subseteq X$ is called the **domain of definition** of f. If $S = X$, f is said to be **total**.

Definition (category of sets)**.** The **category of sets**, denoted as **Set**, is the category whose objects are sets. The morphisms from A to B are the (total) functions from A to B, and the composition of morphisms is the composition of functions.

Definition (category of algebraic structure)**.** The category of some algebraic structure is the category whose objects are structures of a given kind, and morphisms are homomorphisms.

Remark. For example,

- **Grp** is the category of groups with group homomorphisms;
- **Ab** is the category of Abelian groups with group homomorphisms;
- **Ring** is the category whose objects are rings (with identity) and whose morphisms are ring homomorphisms;
- K-**Vect** is the category of all vector spaces over a field K as objects, and K-linear maps as morphisms.
- **Top** is the category whose objects are topological spaces and whose morphisms are continuous maps;
- $\mathbf{Man}^p$ is the category of C^p-manifolds and whose morphisms are C^p-differentiable maps; C^p-manifolds on spaces in a fixed category A, denoted $\mathbf{Man}^p(A)$, C^p-manifolds modeled on a fixed space E denoted $\mathbf{Man}^p(E)$ are also categories.

7.0.8.1.2 Category of Open Sets

Definition (category of open sets)**.** If X is a topological space, then the **open sets** in X form a partially ordered set $\mathrm{Open}(X)$ under inclusion.
Explicitly, $\mathrm{Open}(X)$ is formed by adding a single morphism $U \to V$ if and only if $U \subseteq V$.

Definition (proper class)**.** A **class** is a collection of sets built from

$$\{\, x \mid \varphi \,\},$$

where x are sets and φ is some rule (e.g., well-formed formula) restricting the selection of x.
A class that is not a set (informally in Zermelo–Fraenkel) is called a **proper class**.

Definition (small category)**.** A category C is called **small** if both $\mathrm{ob}(C)$ and $\hom(C)$ are not proper classes, and **large** otherwise.
A **locally small category** is a category such that for all objects a and b, the hom-class $\hom(a, b)$ is a set, called a **homset**.

Lemma 7.55. *Poset is small category.*

Corollary 7.56. *Category of open sets is small.*

7.0.8.1.3 Sheaf

Definition (opposite category)**.** The **opposite category** or dual category C^{op} of a given category C is formed by reversing the morphisms, i.e., interchanging the source and target of each morphism.

Proposition 7.57. *Doing the reversal twice yields the original category, so the opposite of an opposite category is the original category itself. In symbols,*

$$(C^{\mathrm{op}})^{\mathrm{op}} = C.$$

Proposition 7.58. *Opposite preserves products:*

$$(C \times D)^{\mathrm{op}} \cong C^{\mathrm{op}} \times D^{\mathrm{op}}.$$

Opposite preserves functors:

$$(\mathcal{F}(C, D))^{\mathrm{op}} \cong \mathcal{F}(C^{\mathrm{op}}, D^{\mathrm{op}}).$$

Opposite preserves slices:

$$(F \downarrow G)^{op} \cong (G^{op} \downarrow F^{op}).$$

Definition (contravariant functor)**.** A **contravariant functor**, or a cofunctor, associates two categories by "turning morphisms around" and "reversing the composition".

Let C and D be categories. A functor F from C to D is a mapping containing

- $F\colon \mathrm{ob}(C) \to \mathrm{ob}(D)$,
- $\forall X, Y \in \mathrm{ob}(C)$, $F_{X,Y}\colon \hom_C(X, Y) \to \hom_D(F(Y), F(X))$ such that
  - $$\forall X \in \mathrm{ob}(C)[F_{X,X}(1_X) = 1_{F(X)}], \tag{7.6}$$
  - $$\begin{aligned} &\forall X, Y, Z \in \mathrm{ob}(C) \\ &\Big[\forall f \in \hom_C(X, Y) \forall g \in \hom_C(Y, Z) \\ &\big(F_{X,Z}(g \circ_C f) = F_{X,Y}(f) \circ_D F_{Y,Z}(g)\big)\Big]. \end{aligned} \tag{7.7}$$

Remark. Note that one can also define a contravariant functor as a covariant functor on the opposite category.

Definition (presheaf on category)**.** A **presheaf on a category** C is a functor from its opposite category C^{op} to a category J, usually being the category of sets, **Set**. It is contravariant on C.

Definition (presheaf on a topological space)**.** A **presheaf on a topological space** is

$$C^{\mathrm{op}} \to \mathbf{Set},$$

where C is the poset of open sets in a topological space. In general **Set** can be replaced by any category.

Remark. Explicitly, given a topological space $(X, \mathcal{T})$, *a presheaf of sets* $\mathscr{F}$ on X consists of the following

- a set $\mathscr{F}(U)$ for each $U \in \tau$; $\mathscr{F}(U)$ is called the **sections** of $\mathscr{F}$ over U; $\mathscr{F}(X)$ is the **global sections** of $\mathscr{F}$;
- a function $\mathrm{Res}_V^U \colon \mathscr{F}(U) \to \mathscr{F}(V)$ for each pair of open sets $V \subseteq U$, usually called a **restriction morphism**; if $s \in \mathscr{F}(U)$, then denote $s|_V \coloneqq \mathrm{Res}_V^U(s)$.

such that

- For every open set $U \in \tau$, the restriction morphism $\mathrm{Res}_U^U \colon \mathscr{F}(U) \to \mathscr{F}(U)$ is the identity morphism on $\mathscr{F}(U)$.
- For any three open sets $W \subseteq V \subseteq U$, the composite $\mathrm{Res}_W^V \circ \mathrm{Res}_V^U = \mathrm{Res}_W^U$.

For instance, by assigning to every open set U the associative algebra of real-valued continuous functions on U, one obtains a presheaf of algebras on X.

Definition (sheaf)**.** A **sheaf** $\mathscr{F}$ on a topological space $(X, \mathcal{T})$ is a presheaf where *compatible sections can be uniquely glued together*, i.e., it follows the two axioms below
($\forall$ open set $U \in \mathcal{T}$ and $\forall$ open cover $\mathcal{U} \subseteq \mathcal{T}$ of U such that $\bigcup \mathcal{U} = U$):

- locality:
$$\forall U_i \in \mathcal{U}\big(s|_{U_i} = t|_{U_i}\big) \implies s = t.$$
- gluing/concatenation/collation:
$$\exists \sigma \in \prod_{U_k \in \mathcal{U}} \mathscr{F}(U_k) \forall U_i, U_j \in \mathcal{U}\big[\sigma(U_i)|_{U_i \cap U_j} = \sigma(U_j)|_{U_i \cap U_j}\big]$$
$$\implies \exists s \in \mathscr{F}(U) \forall U_i \in \mathcal{U}\big[s|_{U_i} = \sigma(U_i)\big],$$

where the Cartesian product is defined as

$$\prod_{U_k \in \mathcal{U}} \mathscr{F}(U_k) = \{\, \sigma : \mathcal{U} \to \bigcup \mathscr{F}(\mathcal{U}) \mid \forall U_k \in \mathcal{U}\big(\sigma(U_k) \in \mathscr{F}(U_k)\big) \,\}\,.$$

Remark. The locality axiom indicates the uniqueness, i.e., a section over any open set U is uniquely determined by its restriction to smaller open sets (covering U).

The image of σ, sections $s_i = \sigma(U_i) \in \mathscr{F}(U_i)$, are called **compatible** if the gluing condition is satisfied. The axiom claims the existence of a glued section.

Remark. Without using the notation of Cartesian product, the gluing axiom can be rewritten as

$$\begin{aligned}
&\exists\big(\sigma : \mathcal{U} \to \bigcup \mathscr{F}(\mathcal{U})\big) \forall U_i, U_j \in \mathcal{U} \\
&\big[\sigma(U_i) \in \mathscr{F}(U_i) \wedge \sigma(U_j) \in \mathscr{F}(U_j) \wedge \sigma(U_i)|_{U_i \cap U_j} = \sigma(U_j)|_{U_i \cap U_j}\big] \\
&\quad \implies \exists s \in \mathscr{F}(U) \forall U_i \in \mathcal{U}\big[s|_{U_i} = \sigma(U_i)\big].
\end{aligned}$$

Definition (structure sheaf of manifold)**.** On an C^k-manifold M, the sheaf of C^j-differentiable functions $\mathcal{O}_M^j$ (with $j \leq k$) is a sheaf of unital associative algebra over K (with K being either $\mathbb{R}$ or $\mathbb{C}$). Its sections on some open set U are the C^j-functions $U \to K$. For $j = k$, this sheaf is called the **structure sheaf** and is denoted $\mathcal{O}_M$.

Remark. The nonzero C^k functions also form a sheaf of Abelian groups, denoted $\mathcal{O}_X^\times$.

7.0.8.2 Stalk and Germ

Definition (stalk)**.** Given a topological space (X, τ), the **stalk** of presheaf $\mathcal{F}$ at $x \in X$, usually denoted $\mathcal{F}_x$, is:

$$\mathcal{F}_x \coloneqq \varinjlim_{U \ni x} \mathcal{F}(U),$$

where the direct limit is indexed over all the open neighbourhoods of x, with order relation induced by reverse inclusion ($U \leq V$ iff $V \subseteq U$). Explicitly, this is the disjoint union over an equivalence relation

$$\mathcal{F}_x = \bigsqcup_{U \ni x} \mathcal{F}(U) \Big/ \sim,$$

where

$$\forall s \in \mathcal{F}(U) \forall t \in \mathcal{F}(V)[s \sim t \iff \exists W \subseteq U \cap V(x \in W \in \tau \wedge s|_W = t|_W)],$$

i.e., two sections are considered equivalent if the restrictions of the two sections coincide on some open neighborhood of x.

Remark. Let M be a complex manifold of dimension n and $x \in M$. Then

$$\mathcal{O}_{X,x} \cong \mathbb{C}[z_1, \ldots, z_n]$$

is the ring of convergent power series: If $\varphi \colon U \to V \subseteq \mathbb{C}^n$ is a chart around x with $\varphi(x) = 0$, then any $f_x \in \mathcal{F}_x$ can be mapped to the Taylor series expansion of $f_x \circ \varphi^{-1}$. On the other hand, any holomorphic function is locally determined by its Taylor series.

Definition (germ)**.** The canonical map

$$\mathcal{F}(U) \to \mathcal{F}_x, s \mapsto s_x \coloneqq [s]$$

is a homomorphism. We call s_x the **germ** of s in x.

7.0.8.3 Holomorphic Tangent Space

Definition (holomorphic tangent space)**.** Let $(M, \tau, \mathcal{A})$ be a complex manifold and $x \in M$ be a point in the manifold. On the stalk $\mathcal{O}_{M,x}$ of the structure sheave $\mathcal{O}_M$ of unital associative algebra of holomorphic functions from open sets to $\mathbb{C}$, the set of all linear maps satisfying the Leibniz identity

$$T_x M = \{\, D \colon \mathcal{O}_{M,x} \to \mathbb{C} \mid \forall f, g \in \mathcal{O}_{M,x}[D(fg) = D(f) \cdot g(x) + D(g) \cdot f(x)] \,\}$$

is called the **holomorphic tangent space** of M at x. It is a $\mathbb{C}$-vector space.

Remark. Tangent space of a real differential manifold can be defined similarly, equivalent to the previous definition.

7.0.9 Lie Group

7.0.9.1 Product Manifold

Definition (Cartesian product)**.** If I is any index set, and $\{\, X_i \,\}_{i \in I}$ is a family of sets indexed by I, then the **Cartesian product** of the sets in $\{\, X_i \,\}_{i \in I}$ is defined to be

$$\prod_{i \in I} X_i = \left\{ f \colon I \to \bigcup_{i \in I} X_i \;\middle|\; \forall i \in I \Big(f(i) \in X_i \Big) \right\},$$

that is, the set of all functions defined on the index set such that the value of the function at a particular index i is an element of X_i.

Definition (canonical projection)**.** If I is any (nonempty) index set, and $\{ X_i \}_{i \in I}$ is a family of sets indexed by I, then given any $i \in I$, the canonical projection

$$p_i \colon \prod_{i \in I} X_i \to X_i$$

is defined as

$$p_i(f) = f(i).$$

Definition (product topology)**.** Let I be some non-empty index set and for every index $i \in I$, X_i be a topological space. Given the Cartesian product of the sets X_i

$$X \coloneqq \prod_{i \in I} X_i,$$

equipped with the canonical projections

$$p_i : X \to X_i,$$

the **product topology** on X is defined to be the coarsest topology (i.e., the topology with the fewest open sets) for which all the projections p_i are continuous. The Cartesian product X endowed with the product topology is called the **product space**.

Remark. For example, consider two topological spaces (X, σ) and (Y, τ), In the product space $(X \times Y, \rho)$, we have canonical projections

$$\forall b \in Y, (a, b) \mapsto a,$$

which must be continuous, i.e.,

$$\mathcal{S} = \{ S \times Y \mid S \in \sigma \} \subseteq \rho.$$

Similarly,

$$\mathcal{T} = \{ X \times T \mid T \in \tau \} \subseteq \rho.$$

Since the intersection of two open sets is open, we have

$$\{ S \times T \mid S \in \sigma, T \in \tau \} \subseteq \rho.$$

Since the union of open sets is open, we have

$$\{\bigcup_{i\in I}(S_i\times T_i)\mid (S_i,T_i)_{i\in I}\subseteq \sigma\times\tau\}\subseteq\rho.$$

Since the product topology is defined as the coarsest topology satisfying the above condition, we obtain

$$\rho=\{\bigcup_{i\in I}(S_i\times T_i)\mid (S_i,T_i)_{i\in I}\subseteq \sigma\times\tau\},$$

i.e., open sets in product topology are the unions of Cartesian products of open sets.

This can be generalized to finite product of topological spaces (because finite intersection of open sets is still open set). Given spaces $(X_1,\tau_1),\ldots,(X_n,\tau_n)$ where $n\in\mathbb{Z}^+$, the product topology is

$$\{\bigcup_{i\in I}\prod_{j=1}^{n}S_{ij}\mid S_{ij}\in\tau_j\}.$$

For infinite Cartesian product of $(X_j,\tau_j)_{j\in J}$, a base consists of

$$\prod_{j\in J}S_j$$

where S_j is X_j except finite number of them is allowed to be an open subset of X_j.

If the number of open sets is allowed to be infinite, then the topology is called the **box topology**, which is finer than the product topology.

Proposition 7.59. *If P is the product space of spaces $(X_\lambda)_{\lambda\in\Lambda}$, then for any partition of the index set Λ into two subsets Λ_1 and Λ_2 ($\Lambda=\Lambda_1\cup\Lambda_2,\Lambda_1\cap\Lambda_2=\varnothing$), and any $f_2\in\prod_{\lambda\in\Lambda_2}X_\lambda$, the mapping*

$$\mathcal{I}\colon\prod_{\lambda\in\Lambda_1}X_\lambda\to\prod_{\lambda\in\Lambda}X_\lambda, f_1\mapsto f$$

such that

$$f(\lambda)=\begin{cases}f_1(\lambda) & (\lambda\in\Lambda_1)\\ f_2(\lambda) & (\lambda\in\Lambda_2)\end{cases}.$$

is a continuous injection.

Proof. Any open set A in the product space $P = \prod_{\lambda\in\Lambda} X_\lambda$ is an union

$$A = \bigcup_{\gamma\in\Gamma} \prod_{\lambda\in\Lambda} S_{\gamma\lambda} = \bigcup_{\gamma\in\Gamma} \mathscr{P}\left[\left(\prod_{\lambda\in\Lambda_1} S_{\gamma\lambda}\right) \times \left(\prod_{\lambda\in\Lambda_2} S_{\gamma\lambda}\right)\right],$$

where for each γ there are finite sets in $S_{\gamma\lambda}$ is an open subset of X_λ (others must be X_λ) (let's call it "finite support") and $\mathscr{P}$ is a permutation function. Since $(S_{\gamma\lambda})_{\lambda\in\Lambda}$ has finite support iff both $(S_{\gamma\lambda})_{\lambda\in\Lambda_1}$ and $(S_{\gamma\lambda})_{\lambda\in\Lambda_2}$ have finite support, therefore such partition is valid.

Partition Γ into two subsets Γ_1 and Γ_2 such that

$$f_2 \in \prod_{\lambda\in\Lambda_2} S_{\gamma\lambda} \iff \gamma \in \Gamma_1.$$

Then the preimage of A is the same as the preimage of A'

$$A' = \bigcup_{\gamma\in\Gamma_1} \mathscr{P}\left[\left(\prod_{\lambda\in\Lambda_1} S_{\gamma\lambda}\right) \times \left(\prod_{\lambda\in\Lambda_2} S_{\gamma\lambda}\right)\right].$$

That is to say, the preimage is

$$\mathcal{I}^{-1}(A) = \mathcal{I}^{-1}(A') = \bigcup_{\gamma\in\Gamma_1} \left(\prod_{\lambda\in\Lambda_1} S_{\gamma\lambda}\right),$$

which is an open set because $(S_{\gamma\lambda})_{\lambda\in\Gamma_1}$ has finite support.

Therefore $\mathcal{I}$ is a continuous function. From the property of Cartesian product, we know it is injection. □

Corollary 7.60. *Given $f_2 \in \prod_{\lambda\in\Lambda_2} X_\lambda$, the cross section (or slice) of an open set $A \subseteq \prod_{\lambda\in\Lambda} X_\lambda$ in the product space into some smaller product space*

$$\{\, f_1 \in \prod_{\lambda\in\Lambda_1} X_\lambda \mid f \in A \wedge f(\lambda) = \begin{cases} f_1(\lambda) & (\lambda \in \Lambda_1) \\ f_2(\lambda) & (\lambda \in \Lambda_2) \end{cases} \}$$

is open.

Corollary 7.61. *If X and Y are topological spaces, and $x_0 \in X, y_0 \in Y$, then*

$$f_{x_0} \colon Y \to X \times Y, y \mapsto (x_0, y)$$

and

$$f_{y_0} \colon X \to X \times Y, x \mapsto (x, y_0)$$

are continuous injections. If A is an open set in $X \times Y$, then

$$\{\, x \in X \mid (x, y_0) \in A \,\}$$

and

$$\{\, y \in Y \mid (x_0, y) \in A \,\}$$

are open sets in X, Y, respectively.

Proposition 7.62. *If $f\colon X_1 \to X_2$ is continuous, then*

$$f_1\colon X_1 \times Y \to X_2 \times Y\colon (x, y) \mapsto (f(x), y)$$

and

$$f_2\colon W \times X_1 \to W \times X_2\colon (w, x) \mapsto (w, f(x))$$

are continuous for any topological spaces W, Y.

Proof. The open set in $X_2 \times Y$ is a union

$$A = \bigcup_{i \in I} (S_i \times T_i)$$

where S_i are open sets in X_2 and T_i are open sets in Y.

Therefore the preimage

$$f_1^{-1}(A) = \bigcup_{i \in I} f_1^{-1}(S_i \times T_i) = \bigcup_{i \in I} f^{-1}(S_i) \times T_i$$

is open in $X_1 \times Y$ because $f^{-1}(S_i)$ is open in X_1.

f_2 is continuous for similar reasons. □

Definition (product manifold)**.** The **product manifold** is the Cartesian product of manifolds.

Its point set is the Cartesian product of point sets. Its topology is the product topology, and a Cartesian product of charts is a chart for the product manifold. An atlas for the product manifold can be constructed using atlases for its factors.

7.0.9.2 Definition of Lie Group

Definition (Lie group)**.** A real (or complex) **Lie group** is a group G that is also a finite-dimensional real (or complex) smooth manifold, in which the mapping from the product manifold $G \times G$ to G

$$(x, y) \mapsto x^{-1} y,$$

is smooth (or holomorphic).

Remark. Lie group is a tuple (with K being either $\mathbb{R}$ or $\mathbb{C}$)

$$(G, \cdot \colon G \times G \to G, (\bullet)^{-1} \colon G \to G, \tau \in \mathcal{P}(\mathcal{P}(G)), I, \mathcal{A} = (U_i, \varphi_i \colon U_i \to K^{n_i})_{i \in I})$$

satisfying the following axioms
$(\exists! e \in G, \forall x, y, z \in G, \forall \mathcal{S} \subseteq \tau, \forall (V, \psi \colon V \to K^{n'}))$:

- it is a Hausdorff topological space, i.e.,

$$\begin{aligned} \{ \varnothing, G \} \subseteq & \tau, \\ \bigcup \mathcal{S} \in & \tau, \\ |\mathcal{S}| \in \mathbb{Z}^+ \implies & \bigcap \mathcal{S} \in \tau, \\ x \neq y \implies & \exists N_x, N_y \in \tau \\ & \Big(x \in N_x \wedge y \in N_y \wedge N_x \cap N_y = \varnothing \Big); \end{aligned} \tag{7.8}$$

- it contains a smooth or complex structure, i.e.,

$$\begin{aligned} & \bigcup_{j \in I} U_j = G, \\ & (V, \psi \colon V \to K^{n'}) \in \mathcal{A} \iff \\ & \Big(V \in \tau \wedge \forall p, q \in V \big(p = q \iff \psi(p) = \psi(q) \big) \\ & \wedge \forall S \subseteq V \big(S \in \tau \iff \psi(S) \in \mathcal{T}(K^{n'}) \big) \\ & \wedge \forall i \in I \big((\psi \circ \varphi_i^{-1}) \text{ and } (\varphi_i \circ \psi^{-1}) \text{ are smooth/holomorphic} \big) \Big); \end{aligned} \tag{7.9}$$

- it is a group, i.e.,

$$\begin{aligned} (x \cdot y) \cdot z &= x \cdot (y \cdot z), \\ e \cdot x &= x \cdot e = x, \\ (x)^{-1} \cdot x &= x \cdot (x)^{-1} = e; \end{aligned} \tag{7.10}$$

- the group operations are smooth/holomorphic, i.e.,

$$\begin{aligned} & \exists j, k, l \in I \Big[x \in U_j \wedge y \in U_k \wedge (x)^{-1} \cdot y \in U_l \wedge \\ & \Big(\varphi_l \circ \big((p, q) \mapsto (p)^{-1} \cdot q \big) \circ (\varphi_j \times \varphi_k)^{-1} \Big) \text{ is smooth/holomorphic} \Big], \end{aligned} \tag{7.11}$$

where $\mathcal{T}(K^{n'})$ retrieves the metric topology on a n'-dimensional Hilbert space $K^{n'}$ (7.6). $n', n_i \in \mathbb{N}$.

Remark. The last two group axioms can be rewritten without assuming the uniqueness of identity:

$$\begin{aligned}&\exists e \in G \forall u \in G[e \cdot u = u \cdot e = u],\\ &\exists w \in G \forall v \in G\Big((w \cdot x) \cdot v = v \cdot (w \cdot x)\\ &\qquad\qquad = (x \cdot w) \cdot v = v \cdot (x \cdot w)\Big);\end{aligned} \tag{7.12}$$

The iff in the second half of smooth/complex structure condition indicates $\mathcal{A}$ is maximal atlas.

$V \in \tau$ is required to make sure the image is an open set.

Condition

$$\bigcup_{j \in I} U_j = G$$

is redundant since it is equivalent to

$$\forall x \in G \exists j \in I(x \in U_j).$$

Remark. One may add more properties to the Lie group, like paracompactness

$$\begin{aligned}\forall \mathcal{U} \subseteq \tau\Big[G = \bigcup \mathcal{U} \implies\\ \exists \mathcal{V} \subseteq \tau\big(G = \bigcup \mathcal{V} \wedge \forall V \in \mathcal{V} \exists U \in \mathcal{U}(V \subseteq U)\\ \wedge \forall x \in G \exists W_x \in \tau(x \in W_x \wedge |\{\, V \in \mathcal{V} \mid V \cap W_x \neq \varnothing \,\}| \in \mathbb{N})\\ \big)\Big],\end{aligned}$$

or a stronger condition, second countability,

$$\exists \mathcal{B}\Big[\big(|\mathcal{B}| \leq \aleph_0\big) \wedge \forall S\big(S \in \tau \iff \exists \mathcal{A} \subseteq \mathcal{B}(S = \bigcup \mathcal{A})\big)\Big].$$

A compact Lie group satisfies

$$\forall \mathcal{U} \subseteq \tau[G = \bigcup \mathcal{U} \implies \exists \mathcal{V} \subseteq \mathcal{U}\big(G = \bigcup \mathcal{V} \wedge |\mathcal{V}| \in \mathbb{N}\big)]. \tag{7.13}$$

7.0.10 Algebraic Variety

7.0.10.1 Group Actions

See 2.3.1.2 for the definition of group action.

Definition (types of actions)**.** The group action of G on set X is called:

- **Transitive** if

$$X \neq \varnothing \wedge \forall x, y \in X \exists g \in G[gx = y].$$

- **Faithful** (or effective) if

$$\forall g, h \in G \exists x \in X [g = h \iff gx = hx],$$

or equivalently

$$\forall g \in G \exists x \in X [g = e \iff gx = x],$$

or, different elements of G induce different permutations of X. (see 2.30)

- **Free** (or semiregular or fixed point-free) if,

$$\forall g, h \in G [\exists x \in X (gx = hx) \implies g = h],$$

or equivalently

$$\forall g \in G [\exists x \in X (gx = x) \implies g = e],$$

or, by applying 7.30 and the fact that $ex = x$, equivalently

$$\forall g \in G \forall x \in X [g = e \iff gx = x].$$

- **Regular** (or simply transitive or sharply transitive) if it is both transitive and free, i.e.,

$$X \neq \varnothing \wedge \forall x, y \in X \exists! g \in G [gx = y].$$

- n**-transitive** if

$$\begin{aligned} &|X| \geq n \wedge \forall (x_i)_{i \in \mathbb{Z}_n}, (y_i)_{i \in \mathbb{Z}_n} \in X^n \\ &\Big[\forall i, j \in \mathbb{Z}_n \big(i = j \iff (x_i = x_j \wedge y_i = y_j)\big) \\ &\implies \exists g \in G \forall i \in \mathbb{Z}_n \big(g x_i = y_i\big)\Big]. \end{aligned}$$

A 2-transitive action is also called **doubly transitive**, a 3-transitive action is also called **triply transitive**, and so on.

- **Sharply** n**-transitive** if there is exactly one such g:

$$\begin{aligned} &|X| \geq n \wedge \forall (x_i)_{i \in \mathbb{Z}_n}, (y_i)_{i \in \mathbb{Z}_n} \in X^n \\ &\Big[\forall i, j \in \mathbb{Z}_n \big(i = j \iff (x_i = x_j \wedge y_i = y_j)\big) \\ &\implies \exists! g \in G \forall i \in \mathbb{Z}_n \big(g x_i = y_i\big)\Big]. \end{aligned}$$

- **Locally free** if (G, τ) is a topological group and

$$\exists U \in \tau \forall g \in U \forall x \in X [e \in U \wedge (gx = x \iff g = e)].$$

Definition (principal homogeneous space)**.** If G is a regular group action on set X, then X is called a **principal homogeneous space** for G or a G-torsor.

Proposition 7.63. *A free action on a non-empty set is faithful, and locally free (topological group).*

Proof. Because $ex = x$ is guaranteed by definition, and forall implies exists for nonempty set.

It is locally free because the topological group G contains the identity and it is an open set. □

Proposition 7.64. *The action of any group G on itself by left multiplication is regular, and thus faithful as well.*

Proposition 7.65. *The action of the symmetric group $\mathfrak{S}_n$ on a set with n elements is always n-transitive; the action of the alternating group $\mathfrak{A}_n$ is $(n-2)$-transitive.*

Proposition 7.66. *Group G is a regular action on set X iff the map $G \to X$*

$$g \mapsto gx$$

is bijective for all $x \in X$.

Proof. G is regular action on X
iff (by definition)

$$X \neq \varnothing \wedge \forall x, y \in X \exists! g \in G [gx = y].$$

iff (by definition of $\exists!$)

$$X \neq \varnothing \wedge \forall x, y \in X \exists g \in G \forall h \in G [hx = y \iff g = h].$$

TODO □

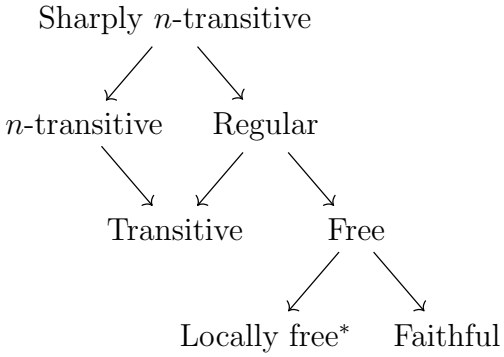


Figure 17: Hierarchy of group actions on *non-empty* set. $n > 1$.
*For topological group.

7.0.10.2 Affine Space

Definition (affine space)**.** An **affine space** is a principal homogeneous space A for the action of the additive group of a vector space $\overrightarrow{A}$.

The elements of the affine space A are called **points**. The vector space $\overrightarrow{A}$ is said to be **associated** to the affine space, and its elements are called **vectors**, **translations**, or sometimes free vectors.

Remark. A should be nonempty.

If the group action is defined as the right action:

$$+ \colon A \times \overrightarrow{A} \to A,$$

then it is equivalent to say this action + satisfies
$(\forall v, w \in \overrightarrow{A}, \forall a \in A)$

- Right identity:
$$a + \mathbf{0} = a,$$
where $\mathbf{0}$ is the zero vector in $\overrightarrow{A}$.
- Associativity:
$$(a + v) + w = a + (v + w).$$
- Regular action: the map
$$\begin{aligned} &\overrightarrow{A} \to A, \\ &v' \mapsto a + v', \end{aligned}$$

is a bijection.

Right identity and Associativity claims $+$ is a right action. Therefore $A \to A \colon a \mapsto a + v$ is bijection for any $v \in \overrightarrow{A}$.

For the map between affine space A and the associated vector space $\overrightarrow{A}$, see 7.66. For any $a, b \in A$, $\exists! v \in \overrightarrow{A}$, such that $a + v = b$. Such v is denoted $b - a$.

Affine space can be considered as a space "parallel to" the associated vector space. It can be thought of a space where only subtraction is well-defined.

Proposition 7.67. *The second Weyl's axiom:* $(c - b) + (b - a) = (c - a)$.

7.0.10.3 Affine Variety and Zariski Topology

Definition (affine variety)**.** For an *algebraically closed field* K and a natural number n, let $\mathbb{A}^n$ be an affine space to which an n-dimensional K-vector space is associated. That is to say, $\mathbb{A}^n$ is formed by the n-tuples of elements of K.

Let S be a set of multivariate polynomials in $x_1, \ldots, x_n$ with coefficients in K, i.e., $S \subseteq K[x_1, \ldots, x_n]$, define the zero-locus $\mathrm{Z}(S)$ to be intersection of zero sets of the functions in S, that is to say

$$\mathrm{Z}(S) \coloneqq \{\, (x_1, \ldots, x_n) \in \mathbb{A}^n \mid \forall f \in S[f(x_1, \ldots, x_n) = 0] \,\}.$$

This is called an **affine algebraic set**. An affine algebraic set $\mathrm{Z}(S)$ is called **irreducible** if it is nonempty and cannot be written as the union of two proper algebraic subsets, i.e.,

$$\begin{aligned} &\mathrm{Z}(S) \neq \varnothing \wedge \neg \exists S_1, S_2 \subseteq K[x_1, \ldots, x_n] \\ &\Big(\mathrm{Z}(S_1) \neq \mathrm{Z}(S) \wedge \mathrm{Z}(S_2) \neq \mathrm{Z}(S) \wedge \mathrm{Z}(S_1) \cup \mathrm{Z}(S_2) = \mathrm{Z}(S) \Big). \end{aligned} \tag{7.14}$$

Depending on author, **affine variety** might be defined as affine algebraic set or irreducible affine algebraic set.

Definition (ideal operations)**.** The **sum and product of ideals** I and J are defined as

$$I + J \coloneqq \{\, a + b \mid a \in I, b \in J \,\}, IJ \coloneqq \{\, \sum_{(a,b) \in S} ab \mid S \subseteq I \times J, |S| \in \mathbb{Z}^+ \,\},$$

where $I \times J$ is the Cartesian product. I and J are called **comaximal** ideals if $I + J = R$.

Remark. $I + J$ is the smallest ideal containing $I \cup J$, $IJ \subseteq I \cap J$.

Proposition 7.68. *Given two ideals I, J of a commutative ring R,*

$$I + J = R \implies IJ = I \cap J.$$

Proof.

$$\because 1 \in I + J = R, \therefore \exists i \in I, j \in J[i + j = 1].$$

Hence, $\forall x \in I \cap J$,

$$x = x \cdot 1 = x \cdot (i + j) = i \cdot x + x \cdot j \in IJ.$$

□

Definition (Zariski topology)**.** The **Zariski topology** on an affine space is the topology in which closed sets are the affine algebraic sets.
The Zariski topology on an affine algebraic set is the subspace topology inherited from the Zariski topology on an affine space.

Remark. This is a valid topology because

- Empty set and the affine space are affine algebraic sets.

$$\mathrm{Z}(K[x_1, \ldots, x_n]) = \mathrm{Z}(\{\, 1 \,\}) = \varnothing, \mathrm{Z}(\varnothing) = \mathrm{Z}(\{\, 0 \,\}) = \mathbb{A}^n.$$

- $\mathrm{Z}(S) = \mathrm{Z}(I_S)$ where $I_S \subseteq K[x_1, \ldots, x_n]$ is the ideal generated by S.
- Given two ideals $I, J \subseteq K[x_1, \ldots, x_n]$,

$$\mathrm{Z}(I) \cup \mathrm{Z}(J) = \mathrm{Z}(IJ), \mathrm{Z}(I) \cap \mathrm{Z}(J) = \mathrm{Z}(I + J).$$

Proposition 7.69. *Affine variety is a T_1 space.*

Proof. Let $(c_1, c_2, \ldots, c_n) \in V \subseteq \mathbb{A}^n$ be a point in an affine space V over K. Then the zero locus of the set of polynomials $\{\, (x_1 - c_1), \ldots, (x_n - c_n) \,\} \subseteq K[x_1, \ldots, x_n]$ is a singleton $\{\, (c_1, c_2, \ldots, c_n) \,\}$.

Therefore, any singleton in an affine variety is a closed set, i.e., it is T_1 space (7.0.2.3.1). □

Remark. Affine variety is not T_2.

The Zariski topology on a commutative ring (that is, the prime spectrum of a ring) is T_0 but not, in general, T_1.

Definition (coordinate ring)**.** Given an affine space $\mathbb{A}^n$ and an affine algebraic set $V \subseteq \mathbb{A}^n$ over an algebraically closed field K, the ideal

$$I(V) = \{\, f \in K[x_1, \ldots, x_n] \mid \forall x \in V[f(x) = 0] \,\}$$

consists of all polynomial functions vanishing on V, and thus the zero locus of $I(V)$ is V itself.

$$\mathrm{Z}(I(V)) = V.$$

The **coordinate ring** of V is the quotient algebra:

$$K[x_1, \ldots, x_n]/I(V).$$

Elements in the coordinate ring are called **regular functions**.

Remark. A regular function on a variety can be viewed as an analytical total function. See Wolfram Math World.

Definition (regular map)**.** If X and Y are affine varieties as closed subvarieties of $\mathbb{A}^n$ and $\mathbb{A}^m$, then a regular map $f\colon X \to Y$ is the restriction of a polynomial map $\mathbb{A}^n \to \mathbb{A}^m$. Explicitly, let $\mathcal{O}_X(X)$ be the coordinate ring of X, then the regular maps are elements of the Cartesian product

$$(\mathcal{O}_X(X))^n$$

such that the image is a subset of Y.

Remark. A regular function can also be viewed as a regular map to $\mathbb{A}^1$.

Definition (structure sheaf of affine variety)**.** The **structure sheaf $\mathcal{O}_X$ of affine variety** X over K is a sheaf of K-algebras such that the section $\mathcal{O}_X(U)$ over a closed subset $U \subseteq X$ is the ring of regular functions on U.

Remark. Therefore, the coordinate ring consists of the global sections of the structure sheaf.

7.0.10.4 Scheme

See more in OSCAR MICHEL, AN INTRODUCTION TO THE ZARISKI TOPOLOGY.

7.0.10.4.1 Prime Spectrum

Definition (maximal ideal)**.** An ideal I is a **maximal ideal** of a ring R if there are no other ideals contained between I and R.

Definition (prime ideal)**.** An ideal P of a commutative ring R is prime if

$$P \neq R \wedge \forall a, b \in R[ab \in P \implies (a \in P \vee b \in P)].$$

Remark. This generalizes the following property of prime numbers: if p is a prime number and if $p|ab, a, b \in \mathbb{Z}$, then $p|a \vee p|b$. We can therefore say:
a positive integer n is a prime number if and only if $n\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$.

Theorem 7.70. *Non-trivial commutative ring with unity has non-empty prime spectrum.*

Definition (integral domain)**.** An **integral domain** R can be defined equivalently as

- a nonzero commutative ring in which the product of any two nonzero elements is nonzero:

  $$\exists x \in R\Big[x \neq 0\Big] \wedge \forall x, y \in R\Big[\big(xy = yx\big) \wedge \big((xy = 0) \iff (x = 0 \vee y = 0)\big)\Big];$$

- a nonzero commutative ring with no nonzero zero divisors;
- a commutative ring in which the zero ideal $\{\, 0 \,\}$ is a prime ideal;
- a ring for which the set of nonzero elements is a commutative monoid under multiplication;
- a ring that is isomorphic to a subring of a field.

Theorem 7.71. *An integral domain R has no nonzero nilpotent elements:*

$$\forall x \in R[x = 0 \iff \exists n \in \mathbb{Z}^+(x^n = 0)].$$

Definition (prime spectrum)**.** The (prime) **spectrum** of a ring R is the set of all prime ideals of R, and is usually denoted by $\operatorname{Spec} R$.

Definition (Zariski topology on spectrum)**.** The **Zariski topology on the spectrum** of a commutative ring R is the topology for which the closed sets are

$$V(I) = \{\, P \in \operatorname{Spec}(R) \mid I \subseteq P \,\},$$

where I is an ideal, i.e., a close set is a set of all prime ideals containing some ideal.

Theorem 7.72. *The Zariski topology on a spectrum is compact and T_0 and spectral.*

Definition (nilpotent ideal)**.** A **nilpotent ideal** is an ideal I such that

$$\exists n \in \mathbb{Z}^+[I^n = \{\, 0 \,\}].$$

Definition (nil ideal)**.** A **nil ideal** is an ideal I of ring R such that

$$\forall x \in R[x \in I \implies \exists n \in \mathbb{Z}^+(x^n = 0)].$$

The **nilradical** of a ring R is $\mathrm{rad}(\{\, 0 \,\}; R)$, defined as

$$\forall x \in R[x \in \mathrm{rad}(\{\, 0 \,\}; R) \iff \exists n \in \mathbb{Z}^+(x^n = 0)].$$

7.0.10.4.2 Collection of Theorems

Definition (irreducible space)**.** A topological space (X, τ) is **irreducible** or **hyperconnected** if it cannot be written as the union of two nonempty proper closed subsets of X, i.e., (τ is the collection of open sets)

$$\forall A, B \in \tau \setminus \{\, \varnothing, X \,\}\, [A \cap B \neq \varnothing].$$

Remark. Note that a topological space (X, τ) is connected iff

$$\forall A, B \in \tau \setminus \{\, \varnothing \,\}\, [A \cup B \neq X \vee A \cap B \neq \varnothing].$$

Therefore, a nonempty irreducible space is connected.

Theorem 7.73. *Given a commutative ring R and its ideal I, let*

- $\mathrm{Ideal}(R)$ *be the set of all ideals of R,*
- $\mathrm{Spec}(R)$ *be the set of all prime ideals of R,*
- $\mathrm{mSpec}(R)$ *be the set of all maximal ideals of R,*
- $V_i(I; R) = \{\, J \in \mathrm{Ideal}(R) \mid I \subseteq J \,\}$,

- $V(I;R) = \{\, P \in \mathrm{Spec}(R) \mid I \subseteq P \,\}$,
- $V_m(I;R) = \{\, M \in \mathrm{mSpec}(R) \mid I \subseteq M \,\}$,
- *the radical of* I *be* $\mathrm{rad}(I;R) = \{\, r \in R \mid \exists n \in \mathbb{Z}^+[r^n \in I] \,\}$,
- **NZComRing** *be the category of non-trivial commutative rings.*

Then $\forall R, S \in \mathbf{NZComRing}, \forall \varphi \in \hom(R,S), \forall I, J \in \mathrm{Ideal}(R), \forall K \in$

$\mathrm{Ideal}(S), \forall P \in \mathrm{Spec}(R), \forall Q \in \mathrm{Spec}(S),$

$$\begin{aligned}
\ker(\varphi) &\in \mathrm{Ideal}(R),\\
\mathrm{im}(\varphi) &\cong R/\ker(\varphi) \in \mathbf{NZComRing},\\
\varphi^{-1}(K) &\in \mathrm{Ideal}(R),\\
\varphi(I) &\in \mathrm{Ideal}(\mathrm{im}(\varphi)),\\
V_i(I;R) &\cong \mathrm{Ideal}(R/I),\\
I \neq R &\iff \exists M \in \mathrm{mSpec}(R)[I \subseteq M],\\
I = R &\iff 1 \in I,\\
R \in \mathbf{Field} &\iff \mathrm{Ideal}(R) = \{\{0\}, R\}\\
&\iff \{0\} \in \mathrm{mSpec}(R),\\
I \in \mathrm{mSpec}(R) &\iff R/I \in \mathbf{Field},\\
I \in \mathrm{Spec}(R) &\iff R/I \in \mathbf{IntegralDomain},\\
\varphi^{-1}(Q) &\in \mathrm{Spec}(R),\\
IJ \subseteq P &\iff I \subseteq P \vee J \subseteq P,\\
I \subseteq \mathrm{rad}(I;R) &\in \mathrm{Ideal}(R),\\
\mathrm{rad}(\{0\};R) &\subseteq P,\\
\mathrm{mSpec}(R) &\subseteq \mathrm{Spec}(R) \subseteq \mathrm{Ideal}(R),\\
V(I;R) = \varnothing &\iff I = R,\\
V(I;R) = \{I\} &\iff I \in \mathrm{mSpec}(R),\\
V(I;R) &= V(\mathrm{rad}(I;R);R),\\
V(I;R) = V(J;R) &\iff \mathrm{rad}(I;R) = \mathrm{rad}(J;R),\\
\mathrm{Spec}(R) &\in \mathbf{CompactSpace},\\
\big(\varphi^*\colon Q \mapsto \varphi^{-1}(Q)\big) &\in \mathcal{C}^0\big(\mathrm{Spec}(S) \to \mathrm{Spec}(R)\big),\\
\Big(\mathcal{P}(R) \supseteq Q' \mapsto \bigcup Q' \subseteq R\Big) &\in \mathbf{Homeo}\big(\mathrm{Spec}(R/I) \to V(I;R) \subseteq \mathrm{Spec}(R)\big),\\
\mathrm{Spec}(R) &\cong \mathrm{Spec}(R/\mathrm{rad}(\{0\};R)),\\
\mathrm{Spec}(R \times S) &\cong \mathrm{Spec}(R) \sqcup \mathrm{Spec}(S),\\
\mathrm{Spec}(R)\ \textit{disconnected} &\iff \exists R_1, R_2 \in \mathbf{NZComRing}[R \cong R_1 \times R_2],\\
\mathrm{rad}(\{0\};R) \in \mathrm{Spec}(R) &\iff \mathrm{Spec}(R)\ \textit{irreducible},\\
R \in \mathbf{IntegralDomain} &\iff \mathrm{Spec}(R)\ \textit{irreducible} \wedge \mathrm{rad}(\{0\};R) = \{0\},
\end{aligned} \tag{7.15}$$

Proof. Prove

$$\varphi(I) \in \mathrm{Ideal}(\mathrm{im}(\varphi)).$$

First prove $\varphi(I)$ is a subgroup of $\mathrm{im}(\varphi)$ under addition.

By definition,

$$\varphi(I) \subseteq \mathrm{im}(\varphi).$$

Since φ is ring homomorphism,

$$0 \in I \wedge \varphi(0) = 0 \implies 0 \in \varphi(I),$$
$$\forall a, b \in R[a + b \in I \implies \varphi(a) + \varphi(b) = \varphi(a + b) \in \varphi(I)].$$

Therefore $\varphi(I)$ is a subgroup of $\mathrm{im}(\varphi)$ under addition.

Next prove it is an ideal of $\mathrm{im}(\varphi)$.

By definition of image,

$$\forall s \in \mathrm{im}(\varphi) \exists a \in R[\varphi(a) = s].$$

Therefore,

$$\forall a \in R[\varphi(a)\varphi(I) = \varphi(aI) \subseteq \varphi(I)].$$

□

7.0.10.4.3 Scheme

Definition (ringed space)**.** A **ringed space** $(X, \mathcal{O}_X)$ is a topological space X together with a sheaf of rings $\mathcal{O}_X$ on X, called the structure sheaf of X.

Definition (locally ringed space)**.** A locally ringed space is a ringed space $(X, \mathcal{O}_X)$ such that all stalks of are local rings (i.e., they have unique maximal ideals).

Remark. An arbitrary topological space X can be considered a locally ringed space by taking $\mathcal{O}_X$ to be the sheaf of real-valued (or complex-valued) continuous functions on open subsets of X.

Manifolds and varieties are locally ringed space too.

Definition (affine scheme)**.** TODO

Remark. Affine variety is affine scheme?

7.0.11 TODO

`https://en.wikipedia.org/wiki/Immersion_(mathematics)`
`https://en.wikipedia.org/wiki/Partition_of_unity`
`https://en.wikipedia.org/wiki/Diffeomorphism`
Directional differentiation

Tangent vector and the differential
Definition of tangent space and differentiation in local coordinates
Partitions of unity
Tangent bundle
Cotangent bundle
Tensor bundle
Frame bundle
Jet bundles
Calculus on manifolds
(Pseudo-)Riemannian manifolds
Symplectic manifolds
Lie groups

7.1 Lie groups: definitions

a map of connected Lie groups $\varphi\colon G \to H$ is a surjective map of groups is equivalent to saying that the differential $d\varphi$ is surjective at every point.

7.2 Examples of Lie groups

7.3 Two constructions

8 Lie Algebras and Lie Groups

8.0 Topological Group

Definition (topological group)**.** A **topological group**, G, is a topological space that is also a group such that the map

$$G \times G \to G, (x, y) \mapsto x^{-1}y$$

is continuous.

Remark. The preimage of $(x, y) \mapsto z$, where $z = x^{-1}y$, is

$$\{\, (x, xz) \mid x \in G \,\}$$

which is bijectively corresponding to the right coset Gz. Therefore we can write down a formal definition without terminologies.

A topological group is a tuple

$$\big(G, \cdot \colon G \times G \to G, (\bullet)^{-1} \colon G \to G, \tau \in \mathcal{P}(\mathcal{P}(G))\big)$$

satisfying the following axioms
$(\exists! e \in G, \forall x, y, z \in G, \forall S \in \tau, \forall \mathcal{S} \subseteq \tau)$:

- it is a topological space, i.e.,

$$\begin{aligned} \{ \varnothing, G \} \subseteq & \tau, \\ \bigcup \mathcal{S} \in & \tau, \\ |\mathcal{S}| \in \mathbb{Z}^+ \implies & \bigcap \mathcal{S} \in \tau; \end{aligned} \tag{8.1}$$

- it is a group, i.e.,

$$\begin{aligned} (x \cdot y) \cdot z &= x \cdot (y \cdot z), \\ e \cdot x &= x \cdot e = x, \\ (x)^{-1} \cdot x &= x \cdot (x)^{-1} = e; \end{aligned} \tag{8.2}$$

- the group operations are continuous, i.e., $\exists (P_i, Q_i)_{i \in I} \subseteq (\tau \times \tau)$ such that

$$\forall p \forall q \big[(p \in G \wedge q \in S) \iff \exists i \in I (p \in P_i \wedge p \cdot q \in Q_i) \big].$$

Remark. The last equation can be simplified as

$$\{ (p, p \cdot q) \mid p \in G, q \in S \} = \bigcup_{i \in I} (P_i \times Q_i). \tag{8.3}$$

Lemma 8.1. *Let G be a topological group and $x, y, r \in G$. The multiplication $(x, y) \mapsto xy$, $(x, y) \mapsto xy^{-1}$ are continuous, the left multiplication $s \mapsto rs$, right multiplication $s \mapsto sr$, and inversion $s \mapsto s^{-1}$, are self-homeomorphisms of G.*

Proof. If $e \in G$ is the identity, then due to 7.61,

$$s \mapsto (s, e) \mapsto s^{-1} e = s^{-1}$$

is a continuous map (the composition of continuous maps is continuous). Since $(s^{-1})^{-1} = s$ and this is unique, the inverse map

$$s^{-1} \mapsto (s^{-1})^{-1} = s$$

is also well-defined and continuous. Therefore the inversion is self-homeomorphism.

And hence the following mappings are well-defined and continuous (7.62):

$$\begin{aligned}(x,y) &\mapsto (x^{-1},y) \mapsto (x^{-1})^{-1}y = xy,\\ (x,y) &\mapsto (x,y^{-1}) \mapsto xy^{-1},\\ s &\mapsto (r,s) \mapsto rs,\\ s &\mapsto (s,r) \mapsto sr,\\ rs &\mapsto (r^{-1},rs) \mapsto r^{-1}rs = s,\\ sr &\mapsto (sr,r^{-1}) \mapsto srr^{-1} = s.\end{aligned}$$

□

Remark. If G is a group equipped with some topology, such self-homeomorphism property does not guarantee G be a topological group. Therefore all topological groups are semitopological groups but the converse does not hold.

Definition (semitopological group)**.** A **semitopological group** G is a topological space that is also a group such that

$$g_1 : G \times G \to G : (x,y) \mapsto xy$$

is continuous with respect to both x and y.

Lemma 8.2. *Let G be a topological group. If $U \subseteq G$ is open and $V \subseteq G$ is any subset of G, then*

$$UV = \{\, uv \in G \mid u \in U, v \in V \,\}$$

and

$$VU = \{\, vu \in G \mid u \in U, v \in V \,\}$$

are open in G.

Proof. Given any $v \in V$, $v^{-1} \in G$, $\therefore$ the mappings below are homeomorphisms on G:

$$x \mapsto xv^{-1}, x \mapsto v^{-1}x.$$

The preimage of an open set U for both mappings are

$$Uv = \{\, uv \mid u \in U \,\}, vU = \{\, vu \mid u \in U \,\},$$

respectively. So they must be open in G.

Since

$$UV = \bigcup_{v \in V} Uv, VU = \bigcup_{v \in V} vU,$$

and union of open sets is open, $\therefore UV$ and VU are open in G. □

Remark. See more about topological group here.

Theorem 8.3. *The identity component of a topological or algebraic group is a closed normal subgroup.*

Proof. It is closed since components are always closed. It is a subgroup since multiplication and inversion in a topological or algebraic group are continuous maps by definition. Moreover, for any continuous automorphism a of G we have $a(G^0) = G^0$. Thus, G^0 is a characteristic subgroup of G, so it is normal. □

Remark. The identity component need not be open. However, the identity component of a locally path-connected space (for instance a Lie group) is always open.

Proposition 8.4. *Any neighbourhood of the identity of a topological group generates a non-empty clopen set.*

Proof. See this proof.

Since $u \mapsto u^{-1}$ is homeomorphism (8.1) (and therefore open map), U being open implies that U^{-1} is open, and therefore $gU^{-1} = \{ g \} U^{-1}$ is open (8.2). the identity is in U and therefore in U^{-1}, so $g \in gU^{-1}$. □

Corollary 8.5. *Any neighbourhood of the identity of a topological group generates the identity component of a Lie group or the whole group if it is connected.*

8.1 Lie Algebras: Motivation and Definition

Exercise 8.1. See 8.5.

Remark. See also: a neighbourhood of identity U generates G where G is a connected lie group.

8.2 Examples of Lie algebras

8.3 The exponential map