Group Theory: Notes and Annotations

Shi Feng

1 Equivalence

Let $\sim$ denote the relation of equivalence " = " in a set S, then $\sim$ satisfies

1. reflexivity: $(\forall a \in S)\ a \sim a$
2. symmetry: $(\forall a \in S)(\forall b \in S)\ a \sim b \ \Rightarrow \ b \sim a$
3. transitivity: $(\forall a \in S\ )(\forall b \in S\ )(\forall c \in S)$, $(a \sim b$ and $b \sim c) \Rightarrow a \sim c$

Another way to define equivalence is by partition. Namely partition and equivalence are the same thing. A partition of S is a family of disjoint nonempty subsets of S, whose union is S, with every subset called the equivalence class:

$$[a]_\sim \equiv \{b \in S | b \sim a\}.$$

where we have used a as a representation of an equivalent class in which a is a member. Then all the equivalence classes form a partition set $\mathcal{P}_\sim$.

Example 1: The prototype example is $=$, which can be defined such that all three properties are met:

$$\{(a,b) \in S \times S | a = b\} = \{(a,a) | a \in S\} \subseteq S \times S.$$

in which every equivalent class has only one element.

Example 2: Another common example in Group is the equivalence defined by a similarity transformation $ag_1a^{-1} = g_2 \quad \Leftrightarrow \quad g_1 \sim g_2$, where $a, g_i \in G$. Apparently it satisfies reflexivity and symmetry. Here we show the transitivity: suppose we have

$$ag_1a^{-1} = g_2, \ \ bg_2b^{-1} = g_3.$$

where $a, b, g_i \in G$. That is $g_1 \sim g_2, \ \ g_2 \sim g_3$. Then we have

$$ag_1a^{-1} = g_2 = b^{-1}g_3b \ \ \Rightarrow \ \ (ba)g_1(ba)^{-1} = g_3 \ \ \Rightarrow \ \ g_1 \sim g_3.$$

Hence the transitivity is proved. The partition by equivalent classes depends on the details of group structure.

Example 3: $a \equiv b(mod\ n)$ is an equivalence relation. The proof is trivial using $n|a-b$:
$a \equiv b(mod\ n) \ \Rightarrow \ a - b = \beta n$, $b \equiv c(mod\ n) \ \Rightarrow \ b - c = \gamma n$, where $\beta, \gamma \in \mathbb{Z}$, hence

$$a - c = \beta n + \gamma n = (\beta + \gamma)n \in \mathbb{Z} \ \ \Rightarrow \ \ n|a-c.$$

so we proved the transitivity.

Definition 1.1. The *Quotient* of the set S with respect to the equivalence relation $\sim$ is the set

$$S/\sim \equiv \mathcal{P}_{\sim}.$$

of equivalent classes of elements of S wrt $\sim$.

Example 4: Take $S = \mathbb{Z}$ and let $\sim$ defined by

$$a \sim b \quad \Leftrightarrow \quad a - b \text{ is even.}$$

Then by definition we have

$$\mathbb{Z}/\sim = \{[0]_{\sim}, [1]_{\sim}\}.$$

where $[0]_{\sim} \equiv \{0, 2, 4, \ldots\}$ and $[1]_{\sim} \equiv \{1, 3, 5, \ldots\}$.

2 Morphism

Let group G act on two sets M_1 and M_2. For all $a \in G$ and $m_1 \in M_1$, we call the map $f : M_1 \to M_2$ a G-morphism if

$$f(am_1) = af(m_1).$$

As an example, let M_1 be some point set on which the group G acts. Let $M_2 = Subg(G)$ be the set of all subgroups of G, on which the group G acts by conjugation. Then the map $f : M_1 \to M_2,\ f(m) \equiv G_m$ is a G-morphism.

Proof. It's easy to see that

$$f(am) = G_{am} = aG_m a^{-1} = af(m).$$

that is, M_1 and M_2 has "essentially" the same structure defined by the action of G and linked to eached other by the G-morphism f. □

Another example, let $G \times M$ (to be identified as M_1) denote the Cartesian product of G and M so that $G \times M$ consists of all pairs of (b, m) with $b \in G,\ m \in M$. Let $\forall a \in G$ act on this $G \times M$ by

$$a(b, m) = (aba^{-1}, am).$$

and act on itself by conjugation aba^{-1}. Relative two this $M_1 \equiv G \times M$ and the group action, we can define two simple G-morphisms: $\theta : G \times M \to M$ and $\tau : G \times M \to G$, defined respectively by

$$\theta(b, m) = m, \quad \tau(b, m) = b.$$

Proof. for any $a \in G$ and $(b, m) \in G \times M$:

$$\theta[a(b, m)] = \theta(aba^{-1}, am) = am = a\theta(b, m).$$

similarly

$$\tau[a(b, m)] = \tau(aba^{-1}, m) = aba^{-1} = a\tau(b, m).$$

Indeed these two maps defines two G-mophisms. □

Furthermore, let $Z \subset G \times M$ be the subset consisting of all pairs (b, m) such that $bm = m$:

$$Z = \{(b, m) | bm = m, b \in G, m \in M\} = \bigcup_{m \in M} G_m \times \{m\}.$$

Note that Z is closed under the action of $\forall a \in G$, thas is, Z is carried into itself, as a set, by $\forall a \in G$. To see this, let $(b, m) \in Z$, recall that $G_{am} = aG_m a^{-1}$, we immediately have

$$a(b, m) = (aba^{-1}, am) = G_{am} \times \{am\} \in Z.$$

so we can as well write $aZ = Z$, $\forall a \in G$. With this subset Z we can define two fabration ρ, σ as restrictions of θ, τ.

Let $\rho : Z \to M$ denote the restriction of θ to the subdomain $Z \subset G \times M$. Let $\sigma : Z \to G$ denote the restriction of τ to the subdomain of $Z \subset G \times M$. So we have two fabrations (S.Sternberg P.25). For a fixed point $m \in M$, the inverse image i.e. $\rho^{-1}(m)$ is precisely the set of all (a, m), $a \in G_m$, or equivalently:

$$\rho^{-1}(m) = \{(a, m) | a \in G_m\} = G_m \times \{m\}.$$

Similarly, the inverse map $\sigma^{-1}(a)$ consists of all pairs (a, m) where $m \in FP(a)$ lies in the set of fixed points of a ($am = m$):

$$\sigma^{-1}(a) = \{(a, m) | m \in FP(a)\} = \{a\} \times FP(a).$$

We say Z is fibered over M. The fiber over a point $m \in M$ being its isotropy group G_m. Z is also a fiber over G. The fiber over $a \in G$ being its fixed point set $FP(a)$.

Note that the identity $e \in G_m$ for all $m \in M$, that is $\{e\} \times M \subset Z$. For the convenience of derivation of a useful formula, we would like to remove this trival action. This is simply done by defining a new subset $Y \subset Z$:

$$Y = \{(a, m) | am = m, a \neq e, a \in G, m \in M\} = Z - \{e\} \times M.$$

We can count the number of elements in Y in two ways, given Y is a finite set. Using the fibration over G we have

$$\#Y = \sum_{a \neq e} \#FP(a).$$

(One may worry about that there might be an overlap between FP(a) and FP(b) thus induces a double counting. This is ruled out by the fact that $(a, m) \neq (b, m)$ even though m is a common FP of a and b).

On the other hand, denote $P \subset M$ such that $\forall m \in P$, $\exists a \neq e \in G$, $am = m$. (The purpose of defining P is to shed off those points $(a, m) \in G \times M$ in which m has a trivial isotropy group $G_m = \{e\}$ that has been excluded in Y). Then using the fibration over M we have

$$\#Y = \sum_{m \in P} (\#G_m - 1)$$

where -1 is because we removed (e, m) for every isotropy group $G_m, m \in P$. We can simplify this expression by *re-grouping* of elements in P. Note that if

$m \in P$ i.e. there is an isotropy group $G_m \neq \{e\} \subset G$, then for $\forall a \in G$ we must have $am \in P$, since $G_{am} = aG_m a^{-1}$ (it's simple yet necessary to show that for $m \in P$ and $G_m = \{b\}$ we have $aba^{-1} \neq e$), that is, the entire orbit of m under G is within P. However, this orbit does not necessarily fully cover P because there could be $n \in P$ that is not reachable by $G \cdot m$, i.e. it could be for some $m, n \in P$, $\nexists a \in G$, $am = n$. Then we need to include this n as well as its orbit $G \cdot n$ into P. we can repeat this process orbit by orbit until all elements in P is covered. Suppose there are r orbits that together fully and tightly cover P, then

$$P = P_1 \cup P_2 \cup \ldots \cup P_r.$$

where P_i labels different orbits that do not overlap. Note that $\#G_m = const$ on each orbit, $\#G_{am} = G_m$ and $\#G/\#G_m$ is the number of elements in an orbit. We conclude

$$\#Y = \sum_{\text{orbits}} \frac{\#G}{\#G_m}(\#G_m - 1).$$

Thus

$$\boxed{\sum_{a \neq e} \#FP(a) = \sum_{\text{orbits}} \frac{\#G}{\#G_m}(\#G_m - 1)}.$$

3 Classification of the finite subgroups of $SO(3)$

Let G be a finite subgroup of $SO(3)$. Then each $a \neq e$ in G leaves precisely one line of vectors fixed in 3D space, that is, infinite FPs along the lines.

Now we restrict the discussion to the unite sphere $\mathbb{S}^2$. In $\mathbb{S}^2$ there are just 2 intersections with the line of FPs, so there are just 2 FPs in this case. Using notations in previous section, that is $\forall a \in G$ and $a \neq e$, we must have $\#FP(a) = 2$. Hence

$$\#Y = \sum_{a \neq e} \#FP(a) = 2(\#G - 1) \tag{3.1}$$

in which $\#G - 1$ comes from $\sum_{a \neq e}$ and the factor of 2 comes from $\#FP(a) = 2$. For convenience let us use the following convetion

$$\begin{aligned} n &= \#G \\ r &= \#(\text{orbits of } G \text{ on } P) \\ n_i &= \#G_m, \ m \in i\text{-th orbit} \end{aligned}$$

then we have

$$2(n-1) = \sum_{i=1}^{r} \frac{n}{n_i}(n_i - 1) \tag{3.2}$$

if devided by $n = \#G$

$$\boxed{2 - \frac{2}{n} = r - \sum_{i=1}^{r} \frac{1}{n_i}} \tag{3.3}$$

This is very important since it imposes strong restrictions on n, r, n_i.

Notice that since $G_m \neq \{e\}$ of $m \in P$, hence $n_i = \#G_m \geq 2$. Then the above equation gives

$$2 - \frac{2}{n} = r - \sum_{i=1}^{r} \frac{1}{n_i} > r - \frac{r}{2} \quad \Rightarrow \quad r < 4 \tag{3.4}$$

Therefore there are at most $r = 3$ orbits on P. Furthermore, note that $n_i \leq n$, thus if $r = 1$:

$$2 - \frac{2}{n} = 1 - \frac{1}{n_1} \tag{3.5}$$

which is equivalent to $n_1 = n/(2-n)$ whose only solution is $n_1 = n = 1$. This is just the trivial $G = \{e\}$. Hence the only non-trivial choice is $r = 2, 3$.

3.1 $r = 2$

From Eq.(3.3) we have

$$\frac{2}{n} = \frac{1}{n_1} + \frac{1}{n_2} \tag{3.6}$$

since $n_i \leq n$, the only solution is $n_1 = n_2 = n$. That is, the finite group G in this case has the same amount of elements of 2 isotropy groups defined on 2 separate orbits. It is readily to infer this is just the group C_n for which $\#G_m = \#G$ for each pole. Thus all rotations are about a same axis through angle $2\pi/n$.

3.2 $r = 3$

4 Topological space

Metric spaces $\subset$ manifolds $\subset$ topological spaces.

Definition 4.1. Let X be any set and $\mathcal{T} = \{U_i | i \in I\}$ denote a certain collection of subsets of X (I can be perceived as a not-disjoint partition). Then pair $(X, \mathcal{T})$ is a topological space if $\mathcal{T}$ satiesfies the following:

(1) $\emptyset$, $X \in \mathcal{T}$

(2) For any subset $J \subseteq I$ (finite or infinite), the family $\{U_j | j \in J\}$ satisfies $\bigcup_j U_{j\in J} \in \mathcal{T}$. In other words, union of members of $\mathcal{T}$ still belongs to $\mathcal{T}$

(3) For any finite subset $K \subseteq I$, the family $\{U_k | k \in K\}$ satisfies $\bigcap_{k\in K} U_k \in \mathcal{T}$. In other words, the intersection of any finite number of members of $\mathcal{T}$ still belongs to $\mathcal{T}$

Then U_is are called the open sets (recursive def: a collection of sets are called open sets if there $\cap/\cup$ with other open sets remains open), and $\mathcal{T}$ is said to give a topology to X.

5 $R_\theta \in SO(2)$

The typical representation of R_θ is

$$R_\theta \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x\cos\theta - y\sin\theta \\ x\sin\theta + y\cos\theta \end{pmatrix} \tag{5.1}$$

each rotation R_θ of $\mathbb{R}^2$ can be represented by the complex number

$$z_\theta = \cos\theta + i\sin\theta \tag{5.2}$$

this is clear if we multiply an arbitrary point $(x, y) = x + iy$ by z_θ

$$\begin{aligned} z_\theta(x+iy) &= (\cos\theta + i\sin\theta)(x+iy) \\ &= x\cos\theta - y\sin\theta + i(x\sin\theta + y\cos\theta) \\ &= (x\cos\theta - y\sin\theta,\ x\sin\theta + y\cos\theta) \end{aligned} \tag{5.3}$$

compare with Eq.(5.1) we see that z_θ is exactly the rotation R_θ in the form $U(1)$. This is actually a concrete example of Unitary theorem that all groups have unitary representation. It is very helpful since any combination of rotations in 2d $R_\phi R_\theta$ can be represented by the multiplication of 2 complex exponentials $z_\phi z_\theta = z_{\phi+\theta}$. So we have

$$z_{\theta+\phi} = \cos(\theta+\phi) + i\sin(\theta+\phi) = z_\theta z_\phi = (\cos\theta + i\sin\theta)(\cos\phi + i\sin\phi) \tag{5.4}$$

thus we can verify the following by comparing real and imaginary parts:

$$\cos(\theta+\phi) = \cos\theta\cos\phi - \sin\theta\sin\phi \tag{5.5}$$

$$\sin(\theta+\phi) = \sin\theta\cos\phi + \cos\theta\sin\phi \tag{5.6}$$

6 Quotient Group

Def. For any subgroup $H \subseteq G$, *the set of left cosets* is denoted by

$$G/H = \{gH | g \in G\} \tag{6.1}$$

Def. N is called a normal subgroup of G, denoted by $N \trianglelefteq G$, if $gN = Ng,\ \ \forall g \in G$, or equivalently, $gNg^{-1} = N,\ \ \forall g \in G$. (Note this doesn't mean $n \in N$ and $g \in G$ have to commute, since the def is valid upto a permutation).

Theorem 6.1. *If $N \trianglelefteq G$ then G/N forms a group known as the quotient group with $(xN)(yN) = (xy)N,\ \ \forall x, y \in G$.*

Proof. **1.Nicity for all Coset Representitives**

First of all we need to show that this operatrion is well-defined. This theorem means: (coset1)(coset2) = (coset3), but the equivalence of cosets has a "gauge dof", which can be seen from the following: Suppose $x_1N = x_2N$, and $y_1N = y_2N$. That means

$$x_1^{-1}x_2 \in N, \quad y_1^{-1}y_2 \in N$$

also since N is a normal subgroup of G, we have $N = x_1Nx_1^{-1} = x_1(x_1^{-1}x_2)x_1^{-1} = x_2x_1^{-1}$. So the above equation can be extended to

$$x_1^{-1}x_2,\ x_2x^{-1} \in N \tag{6.2}$$

$$y_1^{-1}y_2,\ y_2y_1^{-1} \in N \tag{6.3}$$

so we need to show this "gauge dof (coset representatives)" does not undermine the validit of the theorem. To do this, we see that the theorem is equivalent to

$$\begin{aligned} (x_1N)(y_1N) &= (x_1y_1)N = (x_1y_1y_1^{-1}y_2)N = (x_1y_2)N \\ &= N(x_1y_2) = N(x_2x_1^{-1}x_1y_2) = N(x_2y_2) \\ &= (x_2y_2)N \end{aligned} \tag{6.4}$$

where in the 2nd line we used the commutation for normal subgroup N.
Identity: Identity can be defined by $eN \equiv e$. It can be shown by:

$$(xN)(eN) = (xe)N = xN.$$

therefore eN can be identified as the identity.

Inverses:

$$(xN)^{-1} = x^{-1}N.$$

This can be seen from the following:

$$(xN)^{-1}(xN) \equiv (x^{-1}N)(xN) = (x^{-1}x)N = eN.$$

from previous argument eN is identified as the identity, thus QED. □

Example: The $n = 3$ Dihedral group is $D_3 = \{e, r, r^2, f, fr, fr^2\}$, where r denotes rotation, f denote reflection. It has subgroup $R = \{e, r, r^2\}$. What is the quotient D_3/R?

Solution: First of all we need to show that $R \trianglelefteq D_3$.

7 Homomorphisms

We will present the relation between $SL(2, \mathbb{C})$ and Lorentz group as an example of homomorphisms. Let $M = \mathbb{R}^4$ be the 4-d Minkowski space with Lorentz metric:

$$\|x\|^2 = x_0^2 - x_1^2 - x_2^2 - x_3^2, \text{ with } x = \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} \tag{7.1}$$

that is, M is the ordinary Minkowski space of special relativity, and we have chosen the speed of light to be unity. A Lorentz transformation, B, is a linear transformation of M into itself which preserves the Lorentz metric:

$$\|Bx\|^2 = \|x\|^2, \text{ for all } x \in M \tag{7.2}$$

We let L denote the group of all Lorentz transformations, and call it Lorentz group.

We now decribe a homomorphism from $SL(2, \mathbb{C})$ to L. For this purpose we shall identity every point x in M with a 2-by-2 self-adjoint matrix:

$$x := \begin{pmatrix} x_0 + x_3 & x_1 - ix_2 \\ x_1 + ix_2 & x_0 - x_3 \end{pmatrix} = x_0 \mathbb{1} + x_1\sigma_1 + x_2\sigma_2 + x_3\sigma_3 \tag{7.3}$$

which satisfies $x^\dagger = x$ and $\det(x) = \|x\|^2 = x_0^2 - x_1^2 - x_2^2 - x_3^2$. In this notation, we have $x_0 = 1/2\,\mathrm{tr}(x)$, $x_3 = 1/2\tilde{\mathrm{tr}}(x)$ where $\tilde{tr}$ means the difference of the diagonal.

Now let A be any $2 - by - 2$ matrix. We define the action of the matrix A on the self-adjoint matrix x by

$$x \to AxA^\dagger \equiv \phi(A)x$$

where we denoted the corresponding concrete action on the vector x by $\phi(A)x$. The nicity can be seen from the fact

$$\left(AxA^\dagger\right)^\dagger = A^{\dagger\dagger}x^\dagger A^\dagger = AxA^\dagger.$$

so the new $AxA^\dagger$ is also self-adjoint. Notice also that

$$\left\|\phi(A)x\right\|^2 = \det\left(AxA^\dagger\right) = \left|\det(A)\right|^2 \det(x) \tag{7.4}$$

is $A \in SL(2,\mathbb{C})$, then

$$\left\|\phi(A)x\right\|^2 = \left\|x\right\|^2 \tag{7.5}$$

Therefore if A is in $SL(2,\mathbb{C})$, $\phi(A)$ represents a Lorentz transformation. Notice also that

$$ABx(AB)^\dagger = ABxB^\dagger A^\dagger = A(BxB^\dagger)A^\dagger.$$

so that

$$\phi(AB)x = \phi(A)\phi(B)x \tag{7.6}$$

Thus ϕ is a homomorphism! Also note that $\phi(-A) = \phi(A)$ so this map is not one-to-one, i.e. $\pm A$ shall be mapped to the same Lorentz transformation by ϕ.

8 Euler angles

To prove Euler's description we first introduce a useful lemma

Lemma 8.1. *Let m be a point of M and let a be an element of G. Then we can relate two isotropy group by*

$$G_{am} = aG_m a^{-1} \tag{8.1}$$

that is, a group element $c \in G_{am}$ if and only if $c = aba^{-1}$ for $b \in G_m$. And conversely $G_m = a^{-1}G_{am}a$.

Proof. If $b \in G_m$, then $bm = m$. Then $\forall a \in G$ we have

$$am = abm = ab(a^{-1}a)m = (aba^{-1})am \tag{8.2}$$

Thus we conclude $aba^{-1} \in G_{am}$ for $\forall b \in G_m, a \in G$. This also indicates $\#G_{am} = \#G_m$. □

Now let us get back to Euler anlges:

Theorem 8.2. *Euler's description of an arbitrary element $R \in SO(3)$ is that any such element can be factorized as the product of three rotations*

$$R = R^z_\phi R^y_\theta R^z_\psi$$

Note here we are talking about the rotation of a point instead of a rigid body, so we only need rotation about 2 independent axes.

Proof. For simplicity, let n denote the north pole on a sphere. We can move the north pole to an arbitrary point p on the sphere by $p = Rn$. If some other $B \in SO(3)$ also gives the same effect, we have

$$p = Bn = Rn.$$

hence we must have $R = CB$ where $C \in SO(3)$ satisfies $CBn = Bn$. In other words, $C \in SO(3)_{Rn} = SO(3)_{Bn}$, thus C is a rotation about the axis through $p = Rn$. It is easy to see a *trivial* path (call it B) by which we can get n at north pole to any position p by 2 subsequent rotation

$$Rn = R^z_\phi R^y_\theta n.$$

that is, $Rn = Bn = R^z_\phi R^y_\theta n$. But this means $R = CB$ where $C \in SO(3)_{Bn}$. By Lemma.8.1 we have

$$C = BDB^{-1} \quad \text{for } \forall D \in SO(3)_n.$$

Thus

$$R = CB = BDB^{-1}B = BD = R^z_\phi R^y_\theta R^z_\psi.$$

□

9 Topology of SU(2) and SO(3)

10 Useful drosophilas

10.1 Z_N

The two square roots of 1, namely $\{1, -1\}$, form the primary representation of group Z_2 under ordinary multiplication.

The three cube roots of 1 form the $Z_3 = \{1, \omega, \omega^2\}$ with $\omega = e^{2\pi i/3}$

$Z_4 = \{1, i, -1, -i\}$, or $\{1, \omega, \omega^2, \omega^3\}$ with $\omega = e^{i\pi/2}$

More generally, $Z_N = \{e^{i2\pi j/N} : j = 0, 1, 2, \ldots, N-1\}$

10.2 Permutation S_n

Consider $g \in S_5$:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{pmatrix}.$$

which reads: $1 \to 4,\ 2 \to 1,\ 3 \to 5,\ 4 \to 2,\ 5 \to 3$. One can imagine that the 1st row being labels of 5 distinct balls, 2nd row being lables of boxes into which the balls are to be placed. We put the balls into boxes according to the rule and then relabel the balls with labels of boxes. Note that this $g \in S_5$ is equalent to: $1 \to 4 \to 2 \to 1$ and $3 \to 5 \to 3$. A more compact notation is $g = (142)(35)$, where

$$\begin{aligned} (142) &\equiv 1 \to 4 \to 2 \to 1 \\ (35) &\equiv 3 \to 5 \to 3 \end{aligned}$$

This notation is called cyclic permutation, which is a natural way of constructing/describing a permutation, and more conceptually handy compared to the matrix notation. Generally: $(a_1 a_2 \dots a_k)$ permutes by $a_1 \to a_2 \to a_3 \to \dots \to a_k \to a_1$. A cycle of length 2 is called a transposition, or an exchange. The notation of any k-cycle can be cyclically move around without changing anything. e.g. $(35) = (53)$, $(142) = (421) = (214)$.

Any elements in a permutation group can be written as the product of such cycles of various lengths, including cycles of length 1 (untouched by permutation), with none of the cycles containing any number in common. Note that the 1-cycle is trivial and does nothing. Hence it is usually ommitted. e.g.

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix} \equiv (25)(1)(3)(4) \equiv (25).$$

Theorem 10.1. *Any permutation can be written as a product of of 2-cycles, i.e. exchanges.*

in otherwords, exchanges can be viewed as basic building blocks of permutations. e.g.

$$(14)(42) = \begin{pmatrix} 1 & 2 & 4 \\ 4 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 4 \\ 1 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 \\ 1 & 4 & 2 \\ 4 & 1 & 2 \end{pmatrix} = (142).$$

in the last equality we need only compare labels on the 1st and 3rd rows. so $g = (14)(42)(35) = (142)(35)$.

10.3 A_4

A_4 is even permutations group of four objects.

11 Lagrange's theorem

Let a group G with n elements have a subgroup H with m elements. Then m is a factor of n, i.e. n/m is an integer.

Proof:

Let the elements of subgroup H be $\{h_1, h_2, \dots, h_m\}$. Let $g_1 \in G$ but $g_1 \notin H$. Now consider the list:

$$\{h_1 g_1, h_2 g_1, \dots, h_m g_1\} = \{h_1, h_2, \dots, h_m\} g_1 \equiv H g_1.$$

Note that this set is NOT a group ($h_i g_1 = I \in H \;\Rightarrow\; g = h_i^{-1} \in H$. But we assumed $g_1 \notin H$. So the set doesn't have identity element, thus not a group).

Lemma A: elements on the list Hg_1 are all different from one another.

Proof by contradiction: For $a \neq b$, $h_a g_1 = h_b g_1 \;\Rightarrow\; h_1 = h_b$ which is ruled out by the assumption that H being a subgroup. (This is also true for a generic group G and $g_1 \in G$, that in Gg_1 all elements must be distrinct. It leads to the rearrangement or cyclic theorem)

Lemma B: $H \cap Hg_1 = \emptyset$

In other words the two list have no common elements. Proof by contradiction: For some a, b, $h_a g_1 = h_b \quad \Rightarrow \quad g_1 = h_a^{-1} h_b \in G$, which contradicts the assumption that $g_1 \notin H$.

Now consider the following approach: remove from G all elements in Hg_1, call the remains $R_1 := G/Hg_1$. Then pick some $g_2 \in S_1$, and make Hg_2 in which all elements are distinct (*Lemma A*) and shares no elements with H (*Lemma B*). Remove Hg_2 from R_1 and we are left with $R_2 := R_1/Hg_2$. We can repeat this process, until there is no group element left. Repeated k times, we end up with k distinct lists. That is $m/n = k \in \mathcal{Z}$.

Not that since $I \in H$, $Ig_i = g_i \in Hg_i$ is always removed. This forbids any leftover elements in the process.

11.1 An intuitive picture

Let G be a finite group and $m \in M$ is a point in space M. We define the *orbit of m under G* as

$$G \cdot m = \{am \mid a \in G\}$$

Given any point $m \in M$ we can consider the subset G_m of G consisting of those $a \in G$ which satisfy $am = m$, i.e. the point m remains invariant under these operations. It is simple to see that such a subset forms a subgroup of G because

1. $\mathbb{1}m = m$, G_m has an identity element.
2. if $am = m$, then $a^{-1}m = m \;\Rightarrow\; a^{-1} \in G_m$. So all elements in G_m have inverse.
3. if $am = m,\ bm = m$, then $(ab)m = m$. That is $\forall a, b \in G$ and $a \neq b$, we have $ab \in G$. Hence the closure condition is met.

We call such a subgroup G_m of G the *isotropy group of m*.

Now let $\#G$ denote the number of elements in G. Let $m \in M$ be a point of interest, and consider the orbit of m under G which contains $\#(G \cdot m)$ elements. Let $n \neq m$ belong to the orbit of m, that is, $n \in G \cdot m$ with $n = am$ for some $a \in G$. We would like to know the number of elements in G which can map m to n.

If $n = bm$ for some other group element b as well, then we must have

$$n = bm = am \quad \Rightarrow \quad m = a^{-1}bm, \quad \Rightarrow \quad a^{-1}b \in G_m.$$

This means that *to each element n there are exactly $\#G_m$ group elements that map m into n.* Too see this, one can think of the following:

$$m = G_m \cdot m = a^{-1}(aG_m) \cdot m.$$

so we can simply pick an element b from the coset $aG_m \cap G_m = \emptyset$ that must satisfy $n = bm$, and there has to be $\#G_m$ of them. So we conclude, there are $\#G_m$ of ways to carry $m \in M$ into an arbitrary orbital element $n \in G \cdot m$.

Furthermore, every element of G carries m into some *points* $n_i = a_j m$. According to the argument we just made, for each *unique* $n_i \in Gm$, there will be $\#G_m$ a_js that map m into n_i. so we have

$$\#G = \#(G \cdot m)\#G_m \tag{11.1}$$

The dummy diagram is shown below:
This is a concrete example of Lagrange's theorem.

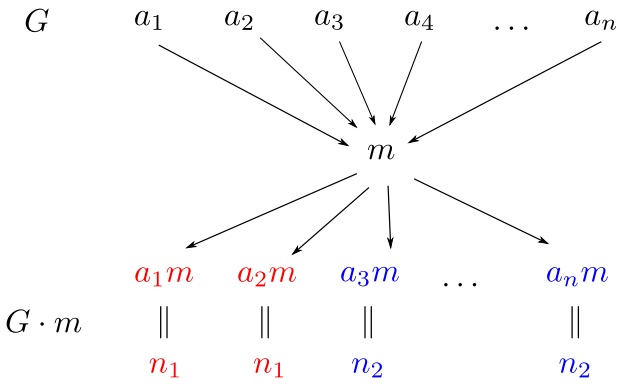

Figure 1: Mapped points n_i of m by G. Note that n_i of the same index (color) should be counted only once in $\cdot m$.

12 Unitary theorem

Finite groups have unitary representations: $D^\dagger(g)D(g) = I$ *for all* g *and all representation*

Intuitive picture:

Suppose the representation $D(g)$ is 1-by-1, that is a generic complex number $re^{i\theta}$. If we keep mutiplying g by itself, then at some step k we must go back to identity. By representation it is $D(g^k) = D(g)^k = r^k e^{ik\theta} \equiv 1$. The last equivalence cannot be true unless $r = 1$; that is, $D(g)$ is unitary representation.

Proof of Unitary theorem:

Lemma 12.1. *Rearrangement Lemma: [Ch.I.1, Zee]:*

$$\sum_{g\in G} f(g) = \sum_{g\in G} f(g'g) = \sum_{g\in G} f(gg') = \sum_{g\in G} f(g)f(g') \tag{12.1}$$

with this lemma we're ready to prove the theorem. Suppose that a given representation $\tilde{D}(g)$ is *non-unitary*. Define:

$$H = \sum_{g\in G} \tilde{D}(g)^\dagger \tilde{D}(g) \tag{12.2}$$

Note that $H^\dagger = H$, so that H is Hermitian. For any g' we have:

$$\begin{aligned}\tilde{D}(g')^\dagger H \tilde{D}(g') &= \sum_{g\in G} \tilde{D}(g')^\dagger \tilde{D}(g)^\dagger \tilde{D}(g)\tilde{D}(g') \\ &= \sum_{g\in G} \left[\tilde{D}(g)\tilde{D}(g')\right]^\dagger \tilde{D}(g)\tilde{D}(g') \\ &= \sum_{g\in G} \left[\tilde{D}(gg')\right]^\dagger \tilde{D}(gg') \\ &= H\end{aligned} \tag{12.3}$$

where in the last step we used the rearrangement lemma.

Since H is Hermitian, there must be a unitary matrix W such that $\rho^2 = W^\dagger H W$ is diagonal and real. We now show that the diagonal elements are not only real but also *positive*.

Lemma 12.2. *For any matrix M, the matrix $M^\dagger M$ has non-negative eigenvalues*

Proof. Let x be an arbitrary non-zero eigenvector of $M^\dagger M$, we must have $\|x\| \geq 0$. Now we are interested its eigenvalue λ.

$$\lambda\|x\| = \langle \lambda x, x\rangle = \left\langle M^\dagger M x, x\right\rangle = \langle Mx, Mx\rangle \geq 0 \tag{12.4}$$

Hence we must have $\lambda \geq 0$ □

Let ψ be the column vector with 1 in the jth entry and 0 everywhere else. Then:

$$\begin{aligned}(\rho)^2_{jj} = \psi^\dagger \rho^2 \psi = \psi^\dagger W^\dagger H W \psi &= \sum_{g\in G} (\psi^\dagger W^\dagger)\tilde{D}(g)^\dagger \tilde{D}(g)(W\psi) \\ = \sum_{g\in G} \phi(g)^\dagger \phi(g) &= \sum_{g\in G} |\phi(g)|^2 > 0\end{aligned} \tag{12.5}$$

where we have defined $\phi(g) := \tilde{D}(g)W\psi$. Note that it cannot equal zero, in which case the group would be trivial that all $D(g) = 0$. Thus the matrix H, and hence ρ^2 must have non-negative eigenvalues. Now we know ρ^2 is positive definite, so we can safely take its squareroot and get an invertable matrix ρ.

Finally, we can define our unitary representation and show it is indeed unitary. Define representation $D(g)$ as:

$$D(g) \equiv \rho W^\dagger \tilde{D}(g) W \rho^{-1} \tag{12.6}$$

so that:

$$\begin{aligned}D(g)^\dagger D(g) &= \rho^{-1} W^\dagger \tilde{D}(g)^\dagger W \rho^2 W^\dagger \tilde{D}(g) W \rho^{-1} \\ &= \rho^{-1} W^\dagger \left[\tilde{D}(g)^\dagger H \tilde{D}(g)\right] W \rho^{-1} \\ &= \rho^{-1} W^\dagger H W \rho^{-1} \\ &= \rho^{-1}\rho^2\rho^{-1} = I\end{aligned} \tag{12.7}$$

that is $D(g)^\dagger = D(g)^{-1}$, so that $D(g)$ defined is unitary.

13 Schur's Lemma

Let $D(g)$ be an irreducible representation of a finite group G, and if there is some matrix A such that $AD(g) = D(g)A$ for all group elements g, then we must have $A = \lambda I$ for some constant λ.

Interpretation:

If we're given a bunch of matrices D_1, $D_2, \ldots$, D_n, the identity matrix I must commutes with all these matrices. This, of course, is the trivial case. But it is also quite possible to find a matrix A that is not the identity. Schur's lemma says that we cannot find such an A if D_i are matrices that furnishing an irreducibable representation of a group.

A small lemma: *A can be taken to be Hermitian with no loss of generality.*

To see this, recall that $D(g)$ can be made a unitary representation while retains its irreducibility. We can take the following hermitian conjugate:

$$AD(g) = D(g)A \quad \Rightarrow \quad D(g)^\dagger A^\dagger = A^\dagger D(g)^\dagger.$$

since $D(g)$ is unitary, this can be rewritten as:

$$D(g)^{-1} A^\dagger = A^\dagger D(g)^{-1}.$$

and hence

$$A^\dagger D(g) = D(g) A^\dagger.$$

Add and subtracting the 1st and 3rd row:

$$(A + A^\dagger) D(g) = D(g)(A + A^\dagger).$$

$$i(A - A^\dagger) D(g) = D(g) i(A - A^\dagger).$$

hence the statement of Schur's lemma also holds for the two hermitian matrices: $(A+A^\dagger)$ and $i(A-A^\dagger)$. Thus, we might as well focus on such Hermitian matrices, and rename A to H to indicate its hermiticity.

Proof:

We want to prove that if $D(g)$ is irreducible, and if $HD(g) = D(g)H$ for all g, then $H = \lambda I$ for some constant λ.

Since H is hermitean, it can be diagonalized by unitary matrix W: $H = W^\dagger H' W$ where H' is diagonal matrix. Hence the statement of the theorem becomes:

$$(W^\dagger H' W) D(g) = D(g)(W^\dagger H' W).$$

we can as well transform $D(g)$ into the new basis such that: $D(g) = W^\dagger D'(g) W$. Thus:

$$(W^\dagger H' W)(W^\dagger D'(g) W) = (W^\dagger D'(g) W)(W^\dagger H' W).$$

so that

$$H' D'(g) = D'(g) H'.$$

since it is an equivalent statement as the original, we will drop the primes here.

Now take the (i,j) component of the above equation:

$$(HD(g))^i_j = (D(g)H)^i_j \,.$$

noting that H is diagonal, we must have:

$$H^i_i D^i_j(g) = D^i_j(g) H^j_j \quad \Rightarrow \quad (H^i_i - H^j_j) D^i_j = 0.$$

Hence, unless $D^i_j(g) = 0$ is for all g, we must have $H^i_i = H^j_j$, which is a matrix proportional to identity. Note the "unless" statement is essential (a synonym) for the condition: "if $D(g)$ is irreducible".

Theorem 13.1. *all irreducible representations of an abelian group are 1-dimensional.*

Proof. □

14 the Great Orthogonality Theorem

Given a d-dimensional irreducible representation $D(g)$ of a finite group G, we have:

$$\sum_{g\in G} D^\dagger(g)^i_j \; D(g)^k_l = \frac{N(G)}{d} \delta^i_l \; \delta^k_j \tag{14.1}$$

with $N(G)$ the number of group elements.

Check:
Let us set $j = k$ and evaluate the L.H.S.

$$\sum_{g\in G} D^\dagger(g)^i_j \; D(g)^j_l = \sum_{g\in G} \delta^i_l = N(G)\delta^i_l \tag{14.2}$$

where we assumed D is unitary. The R.H.S. is:

$$\frac{N(G)}{d} \delta^i_l \delta^j_j = \frac{N(G)}{d} \delta^i_l \times d = N(G)\delta^i_l \tag{14.3}$$

so that the equation holds.

Proof:
Construct the matrix A:

$$A = \sum_{g\in G} D^\dagger(g) X D(g) \tag{14.4}$$

for some arbitrary matrix X. Now we calculate $D^\dagger(g)AD(g)$:

$$\begin{aligned} D^\dagger(g)AD(g) &= D^\dagger(g) \left[\sum_{g'\in G} D^\dagger(g') X D(g') \right] D(g) \\ &= \sum_{g'\in G} D^\dagger(g'g) X D(g'g) = A \end{aligned} \tag{14.5}$$

where in the last step we used the rearrangement lemma. Now look at the two ends in the above equation, we have:

$$AD(g) = D(g)A \tag{14.6}$$

since $D(g)$ is assumed to be d-dimensional irreducible representation, by Schur's lemma we must have $A = \lambda I_d$. Then the trace of A gives:

$$\operatorname{Tr} A = \lambda d = \sum_{g\in G} \operatorname{Tr}\big(D^\dagger(g) X D(g)\big) = N(G) \operatorname{Tr} X \tag{14.7}$$

which determines λ:

$$\lambda = \frac{N(G)}{d} \operatorname{Tr} X \tag{14.8}$$

By far it is for any X. We now choose $X^j_k = 1$ for a particular (j,k) and 0 elsewhere. Therefore the trace becomes:

$$\operatorname{Tr} X = \delta^k_j \tag{14.9}$$

and an arbitrary element of A becomes:

$$\begin{aligned} A^i_l &= \sum_{g\in G} \big(D^\dagger(g) X D(g)\big)^i_l = \sum_{g\in G} D^\dagger(g)^i_j (X^j_m \delta_{k,m}) D(g)^m_l \\ &= \sum_{g\in G} D^\dagger(g)^i_j D(g)^k_l \\ &= \lambda \delta^i_l = \frac{N(G)}{d} \operatorname{Tr} X \delta^i_l = \frac{N(G)}{d} \delta^i_l \delta^k_j \end{aligned} \tag{14.10}$$

That is:

$$\sum_{g\in G} D^\dagger(g)^i_j D(g)^k_l = \frac{N(G)}{d} \delta^i_l \, \delta^k_j \tag{14.11}$$

Q.E.D.

14.1 A simple application: Pauli identity

The great orthoganality theorm(GOT) can be used to prove a useful identity in pauli algebra:

$$\sum_{a=1,2,3} \sigma^a_{\alpha\beta} \sigma^a_{\gamma\delta} = 2\delta_{\alpha\delta}\delta_{\beta\gamma} - \delta_{\alpha\beta}\delta_{\gamma\delta} \tag{14.12}$$

where σ are pauli matrices. Note that 2-by-2 Pauli matrices belongs to irreducible representation of SU(2), so we can apply the theorem directly to Pauli group:

$$G_P = \{\pm I, \pm\sigma^x, \pm\sigma^y, \pm\sigma^z, \pm iI, \pm i\sigma^x, \pm i\sigma^y, \pm i\sigma^z\} \tag{14.13}$$

Now we apply the GOT:

$$\sum_{g\in G_P} D^\dagger(g)_{\alpha\beta} D(g)_{\gamma\delta} = 8\delta_{\alpha\delta} \, \delta_{\gamma\beta} \tag{14.14}$$

Note that $\pm$ and i has no effect on the L.H.S. due to the mutiplication with the complex conjuate, the summation $\sum_{g\in G_p}$ can be divided into 4 identity sums, of which we are interested the subset $P = \{I, \sigma^x, \sigma^y, \sigma^z\}$. This gives us:

$$\sum_{g\in P} D^\dagger(g)_{\alpha\beta} D(g)_{\gamma\delta} = 2\delta_{\alpha\delta}\delta_{\gamma\beta} \tag{14.15}$$

we can separate out the identity I out of the sum, that is, whcih gives us $\delta_{\alpha\beta}\delta_{\gamma\delta}$ on the L.H.S., and write the representation explicit by pauli matrices σ:

$$\delta_{\alpha\beta}\delta_{\gamma\delta} + \sum_a \sigma^a_{\alpha\beta}\sigma^a_{\gamma\delta} = 2\delta_{\alpha\delta}\delta_{\gamma\beta} \tag{14.16}$$

rearrange and we have the desired form:

$$\sum_{a=1,2,3} \sigma^a_{\alpha\beta}\sigma^a_{\gamma\delta} = 2\delta_{\alpha\delta}\delta_{\beta\gamma} - \delta_{\alpha\beta}\delta_{\gamma\delta} \tag{14.17}$$

Q.E.D.

14.2 Different irreducible representations are orthogonal

We would like to show that

$$\sum_g D^{(r)\dagger}(g)^\mu_\nu D^{(s)}(g)^k_l = 0 \tag{14.18}$$

if $r \neq s$ are two different representation.