代数0H：邱宇

Reference book: Artin. Algebra

1. Symmetry&Groups

1.1 3维空间的正多面体

1.1.1 CW-复形

X上的一个胞腔复形是指一个子集族$\{e_\alpha^n, \alpha \in J_n\}$

且每个e_α^n称为一个n-胞腔。全体n-胞腔构成的子集族为n-骨架K^n，设它们中所有元素的并集$|K^n|$视为X的子空间。称边界$\partial e_\alpha^n = e_\alpha^n \cap |K^{n-1}|$，于是也可定义胞腔的内部。

且子集族满足$X = \cup e_\alpha^n = |K|$且$Inte_\alpha^n \cap Inte_\beta^m = \phi \; unless (n, \alpha) = (m, \beta)$

且每个胞腔e_α^n和它的边界偶存在一个满态射$f : (D^n, S^{n-1}) \to (e_\alpha^n, \partial e_\alpha^n)$，且它限制在$D^n - S^{n-1}$上是到内部$Inte_\alpha^n$的同胚。于是每个胞腔都是紧的。

称e_β^m是e_α^n的一个immediate face，若前者与后者的内部的交为空（要么指标完全相同，要么前者维度更低）。如果两个胞腔能通过有限的immediate face关系形成一个immediate face链，则称前者为后者的面。面关系下的极大元称为主胞腔。

若胞腔复形满足：a. 闭包有限(C)：每个胞腔有有限个接触面；b. 弱拓扑(W)：$S \subseteq X$闭 $\iff$ 它与任意胞腔的交集是这个胞腔的闭集，则称为CW复形。

*Hatcher - Algebra Topology*给出了等价的定义。

(1) Start with a discrete set X^0, whose points are regarded as 0-cells.

(2) Inductively, form the ***n*-skeleton** X^n from X^{n-1} by attaching n-cells e^n_α via maps $\varphi_\alpha : S^{n-1} \to X^{n-1}$. This means that X^n is the quotient space of the disjoint union $X^{n-1} \coprod_\alpha D^n_\alpha$ of X^{n-1} with a collection of n-disks D^n_α under the identifications $x \sim \varphi_\alpha(x)$ for $x \in \partial D^n_\alpha$. Thus as a set, $X^n = X^{n-1} \coprod_\alpha e^n_\alpha$ where each e^n_α is an open n-disk.

(3) One can either stop this inductive process at a finite stage, setting $X = X^n$ for some $n < \infty$, or one can continue indefinitely, setting $X = \bigcup_n X^n$. In the latter case X is given the weak topology: A set $A \subset X$ is open (or closed) iff $A \cap X^n$ is open (or closed) in X^n for each n.

A space X constructed in this way is called a **cell complex** or **CW complex**. The explanation of the letters 'CW' is given in the Appendix, where a number of basic topological properties of cell complexes are proved. The reader who wonders about various point-set topological questions lurking in the background of the following discussion should consult the Appendix for details.

要从这个定义得到上文中定义的对空间偶的映射f，只需要考虑如下的特征映射：

After these examples we return now to general theory. Each cell e^n_α in a cell complex X has a **characteristic map** $\Phi_\alpha : D^n_\alpha \to X$ which extends the attaching map φ_α and is a homeomorphism from the interior of D^n_α onto e^n_α. Namely, we can take Φ_α to be the composition $D^n_\alpha \hookrightarrow X^{n-1} \coprod_\alpha D^n_\alpha \to X^n \hookrightarrow X$ where the middle map is the quotient map defining X^n. For example, in the canonical cell structure on S^n described in Example 0.3, a characteristic map for the n-cell is the quotient map $D^n \to S^n$ collapsing ∂D^n to a point. For $\mathbb{R}P^n$ a characteristic map for the cell e^i is the quotient map $D^i \to \mathbb{R}P^i \subset \mathbb{R}P^n$ identifying antipodal points of ∂D^i, and similarly for $\mathbb{C}P^n$.

欧拉示性数$\chi = 2 - 2g - b$，对于CW复形$\chi = \sum(-1)^j |X^j|$

这有两个方式证明：一是利用同调：$|X^j|$实际上是同调群维数的差，另一是利用拓扑：考虑复形的加细（与多边形的情况类似），但是这两个证明无论详细写出哪一个都会使内容失控，因此略去。

1.1.2 Rigid Built

一个多面体(Polytope)是一个CW复形，且满足任何j-胞腔都在$\mathbb{R}^n$的一个$j-$仿射子空间内。

Convexity：Omitted.

Isometric maps：Omitted

正多面体：一个多面体是正多面体如果对于每条胞腔升链之间都有等距变换。

Now we consider the classification:

存在性略(However the verifications become increasingly complicated as the dimension rises. For example:)

例子 1.13. 考虑四维空间中的如下600个点：

- 下列坐标的所有置换得到的坐标：

$$\begin{cases}(0,0,\pm 2,\pm 2),\\(\pm 1,\pm 1,\pm 1,\pm\sqrt{5}),\\(\pm\phi^{-2},\pm\phi,\pm\phi,\pm\phi),\\(\pm\phi^{-1},\pm\phi^{-1},\pm\phi^{-1},\pm\phi^{2}).\end{cases}$$

- 下列坐标的所有偶置换得到的坐标：

$$\begin{cases}(0,\pm\phi^{-2},\pm 1,\pm\phi^{2}),\\(0,\pm\phi^{-1},\pm\phi,\pm\sqrt{5}),\\(\pm\phi^{-1},\pm 1,\pm\phi,\pm 2).\end{cases}$$

证明这些点生成的凸包是一个正则胞腔（120-胞腔）。

分类的唯一性：

引理：$\frac{1}{p}+\frac{1}{q}+\frac{1}{r}>1$的正整数解为$(1,\cdots,\cdots);(2,2,\cdots);(2,3,3\ or\ 4\ or\ 5)$

定理：三维空间中仅有5种正多面体。

a. 这个多面体的每个2-胞腔都是一个2维polygon：n-gon（$n\geq 3$）

b. 每个顶点均在m条棱中（$m\geq 3$）

$\{(f,e):e\in\partial f\}$，于是$2E=n\cdot F$

$\{(v,e):v\in\partial e\}$，于是$2E=m\cdot V$，但$V-E+F=2$，于是
$\frac{1}{m}+\frac{1}{n}=\frac{1}{2}+\frac{1}{E}\implies\frac{1}{2}+\frac{1}{m}+\frac{1}{n}=1+\frac{1}{E}$

这个方程有意义的解数有限。

1.1.3 Another perspective: Spherical Tiling

We first admit this theorem: **(Gauss-Bonnet) For a sphere triangle ABC,** $Area(ABC)=A+B+C-\pi$

Now we construct a spherical tiling from a regular convex polyton: Imagine a light origin located at the geometric center of the polyton. One can seperate the face of the polyton into triangles by connecting the center of the face and the midpoint of the edge, thus we get a triangular separation of the entire surface.

Now we project these triangles (by the light origin) to the circumscribed sphere (assuming the sphere to be the unit sphere) then we get a spherical tiling. Each part of it is a sphere triangle.

Because of the Area formula: the area of each part is
$\frac{\pi}{2} + \frac{2\pi}{2m} + \frac{2\pi}{2n} - \pi = \pi(\frac{1}{m} + \frac{1}{n} - \frac{1}{2})$. Trivial that the tiling contains $4E$ parts, thus the area of each part is $4\pi/4E$ (Same notation)

Now we get $\frac{1}{m} + \frac{1}{n} = \frac{1}{2} + \frac{1}{E} \implies \frac{1}{2} + \frac{1}{m} + \frac{1}{n} = 1 + \frac{1}{E}$ which is exactly what we have just achieved in the previous section!

Have a closer look on each part of the tiling, every solutions of the equation $\iff$ a spherical tiling. Moreover, the Gauss-Bonnet theorem implies a well-known result: the relation between $A + B + C$and π is determined by the principle curvature integrated over the manifold.

2. Group: the measure of symmetrics

First we give a definition while lack of rigorous: the Symmetric group of an object X is the set
$Sym(X) := \{f : X \to X, f\ bijective,\ preserving\ the\ intrinsic\ properties\ of\ X\}$

Ex.

$X = Set$, which does not have any extra structure, it simply becomes the "well-known" symmetric groups.

$X = Vector\ Space$, it has a linear structure, so $Sym(X) \in \mathrm{Hom}(X, X) = \mathrm{End}(X)$

$X = Topology$, then f has to be up to isotopic

From this we can see the important structure of groups, now we give the exact definition.

Def:(Group) A set with a binary operation, satisfying certain axioms (omitted)

Ex. $\mathbb{Z} = (\mathbb{Z}, +)$

Def:(Order) The order of an element a is the minimum $m \in \mathbb{Z}^+ \ s.t. \ a^m = e$

Ex. $(\mu_5, \cdot) \overset{not\ mentioned\ yet!}{\cong} (\mathbb{Z}_5, +) \cong C_5$, the last group is cyclic group.

We have infinite cyclic group $(C_\infty, \cdot) = (\mathbb{Z}, +)$

However, in the finite situations $C_n \cong Sym^+(n-gon)$ (+ means the bijection keeps the orientation)

This doesn't hold when $n \to \infty$ since $Sym^+(Circle) = \mathbb{R}/\mathbb{Z}$.

Def:(Center) The center of a group is the elements that is commutive to every element in the group.

$C(G) = G \iff G \ abelian.$

2.1 Group Homomorphism

Group Homomorphism is the map between groups preserving group structure:

Def:(Group Hom.) A map$\varphi : G_1 \to G_2 \ s.t. \ \varphi(ab) = \varphi(a)\varphi(b)$

Rmk: Group Hom. keeps the identity units and inverse.

Ex.

$\sigma : S_n \to \mu_2$

$\varphi(\mathbb{R}, +) \to (\mathbb{R}^+, \cdot) : \ x \mapsto e^x$

$\det : GL(n, F) \to (\mathbb{R}^*, \cdot)$

Def: Injective, Surjective, Bijective: Omitted

Def: Isomorphism = Inj+Surj - Homomorphism

Def: Isomorphic : Two groups are called isomorphic iff a isomorphism exists.

Def: Automorphism: Isomorphism from a group G to itself.

2.2 Subgroup, Normal Subgroup, Quotient

Def: A subgroup is a subset which has the operation inherited from the orignal group, and satisfies the group axioms.

Judgement: $H \leq G \iff HH^{-1} \subseteq H$

Prop. $finite\ H_i \leq G \implies \cap H_i \leq G$

Generating: The smallest subgroup containing a certain set.

Def: (Kernel) $\varphi : G \to H,\ \ker \varphi := \varphi^{-1}(e_H)$

$\ker \varphi \leq G; (actually \quad \ker \varphi \trianglelefteq G)$
$\varphi\ inj \iff \ker = e_G$

Ex. $\det : GL(n, \mathbb{R}) \to (\mathbb{R}^*, \cdot)$, hence $\ker \det = SL(n, \mathbb{R})$

However quotient of a subgroup does not necessarily have a group structure. This motivates us to define the following.

Def(Coset): $aH = \{ah | h \in H\}$

Easy to find that the cosets leads to a equivalent relation.

$G = \coprod_{a \in G/\sim} aH = \coprod_{a \in G/\sim} Ha$ Hence $|H| \mid |G|$

Def(Norm. SubGrp.): $H \leq G$ **normal** $\iff \forall a \in G, aH = Ha \iff a^{-1}Ha = H$

This necessary to ensure $aH \cdot bH = abH$

Now we can introduce a group structure on the quotient. It becomes a quotient group G/H

Rmk. By moduling the left cosets equivalent relation $\sim_L$, we can only get a quotient $(G/H)_l$ but not a quotient group.

Ex. There exists a subgroup which isn't a normal subgroup in D_{2n}

In the finite case: $|G/H| = |G|/|H|$ (**Do not use this to prove Lagarange theorem!!!**)

2.3 Isomorphism Theorem

1^{st} isomorphism theorem: Fundamental Thm.

One-line description: $\mathrm{Im}\varphi \cong G/\ker\varphi$

One-line Proof: $a\ker\varphi \mapsto a$

2^{nd} isomorphism theorem: Corresponding Thm.

$N \trianglelefteq G, N \leq M \leq G$ corresponds with a subgroup in G/N. Proof: Obvious.

3^{rd} isomorphism thorem: Intersection and Product.

$N \trianglelefteq G, H \leq G$, then $NH \leq G, N \cap H \trianglelefteq H, N \trianglelefteq NH, NH/N \cong H/(N \cap H)$

(Alt. Version $N \trianglelefteq M \trianglelefteq G : G/M \cong (G/N)/(M/N)$)

2.4 Rigid Body Motion

Def($\mathbb{R}^n$ case):

A translation $T_{\vec{v}}(\vec{x}) = \vec{x} + \vec{v}$

A rotation R **is given by an** $A \in SO(n)$

An orthognal transformation is the linear transformation which satisfies $A^T = A^{-1}$

**A reflection is given by reflecting over a hyperplane$0 \in P \subseteq \mathbb{R}^n$, $\dim P = n - 1$

Trivial that an orthognal transformation is always isometric.

Thm. Isometric map$\varphi : \mathbb{R}^n \to \mathbb{R}^n$ can always be represented as the composition of translations, rotations, and reflections.

Pf: Wlog let $\varphi(0) = 0$, then $\varphi \in O(n)$

Consider the orthonormal basis e_i, easy to find $\varphi(e_i)$ are still orthonormal basis.

To show that φ is always linear (or affine when considering the transition), we have $||\varphi(au + bv) - a\varphi(u) - b\varphi(v)||^2 \overset{\varphi \; keeps \; inner \; product}{=\!=\!=} ||(au + bv) - au - bv||^2 = 0$

(The inner product preserving leads from $< f(x), f(y) >= \frac{||f(x)+f(y)||^2 - ||f(x)-f(y)||^2}{4}$)

Consider several examples on R^3

(Euler) For a sphere triangle XYZ **on the unit sphere: and the inner angle** α, β, γ**,** $R_z(2\gamma) \circ R_y(2\beta) \circ R_x(2\alpha) = id$

Lem: $R_y(2\beta) = F_{xy} \circ F_{yz}$ where F_{xy} denotes the reflection over the plane span $< x, y >$ and $\beta = \angle(xy, yz)$

Pf: Consider $\forall \; plane \; P \perp y$

Hence the main theroem is completed, since $R_z(2\gamma) \circ R_y(2\beta) \circ R_x(2\alpha) = F_{xz} \circ F_{yz} \circ F_{yz} \circ F_{yx} \circ F_{yx} \circ F_{xz} = id$

$A \in Isom(\mathbb{R}^n)$, then A is the product of at most $n+1$ reflections.

Pf: Select a reflection such that $0 \mapsto \varphi(0)$

And select n reflections such that $e_i \mapsto \varphi(e_i)$

Classification of finite group $SO(3)$

2.5 Presentation

(Free Group) Omitted

Suppose $G =< X >$, exists a group hom. $G \to F_X$, Thus $G \cong F_X / \ker \varphi$

The kernel is known as the relation. The relation itself has a set of generated relations, thus $G \cong F_X/(R)$

For example $D_n =< a, b > /(a^n = 1, b^2 = 1, abab = 1)$

The key is: why does the dihedral group was determined by this set of relations?

Cayley Graph $CG(G)$ with respect to a set X of generators is a directed graph whose vertices are the elements of the group G, the edges are $\{g \xrightarrow{x} gx\},\ x \in X$

Example $CG(F_X)$, $X = \{a, b\}$ is a $(2,2)-$regular tree.

$CG(C_n =< a >)\ wrt\ a$ is a cycle.

$CG(D_n =< a, b > /(a^n = 1, b^2 = 1, abab = 1))\ wrt\ \{a, b\}$ is a graph with two opposite direction cycle.

$CG(T = A_4 =< x, y > /(x^2 = 1, y^3 = 1, (xy)^3) = 1)\ x = (12)(34)\ y = (123)$

Rmk. X is a set of generator $\iff$ $CG(G)$ wrt X Connected.

Von Dyck Group $D(p,q,r) =< x,y,z > /(x^p = y^q = z^r = xyz = 1)$ Finite $\iff$ $1/p + 1/q + 1/r > 1$

Sketch.

$(\Longleftarrow)$ Direct check.

$(\Longrightarrow)$ If $1/p + 1/q + 1/r < 1$ for instance $(2,3,7)$. From previous tiling discussions, there is a hyperbolic tiling X and its symmetry group actually has three elements $x,y,z\ s.t.\ x^2 = y^3 = z^7 = xyz = 1$, thus exists a group hom. $D(2,3,7) \to Sym(X)$. However $Sym(X)$ is already infinite, thus $D(2,3,7)$ infinite.

(We now see this is also related with the finite subgroup of $SO(3)$)

2.6 Group Actions

G acts on X: $(g,x) \mapsto gx$**, call** X **a** $G-$**set (and a group homomorphism** $G \to Sym(X)$**)**

To say it percisely: we need $(e,x) \mapsto x, (g,(h,x)) \mapsto (gh,x)$

Example S_n, A_n acts on $[1n]$

H subgroup acts on G: Left times, Right times, Conjugates.

Cayley: $G \hookrightarrow S_n$: trivial.

Orbit, Stablizer: $Orb(x) = \{gx | g \in G\}, Stab(x) = \{g | gx = x\}$

Orbit is a equiv. relation. Thus, $X = \coprod Orb(x)$, take $X/G = \{Orb\}$

$Stab(x) \leq G$ and $G/Stab(x)$ (Cosets L/R) Correspondence to elements of $Orb(x)$, ($gStab(x) \leftrightarrow gx$)in particular $|G/Stab(x)| = |Orb(x)|, |Stab(x)| = |G|/|Orb(x)|$

Call a group action transitive if $Orb(x) = X$

Thm. Burnside: A finite group G acts on X, let $X^g = \{x | gx = x\}$

$|X/G| = \frac{1}{|G|} \sum |X^g|$

Proof:

Calculate $\#\{(g, x) | gx = x\}$.

$\sum |Stab(x)| = \sum_{X/G} \sum_{x \in Orb} |Stab(x)| = |X/G||G|$

On the other hand, $\sum |Stab(x)| = \sum |X^g|$

Finite Subgroup of $SO(3)$: C_n, D_n, T, O, I

Pf: Existence omitted.

Let $G \leq SO(3)$,

Take $\mathscr{A} = \{axis\ of\ rotations\ in\ G\}, P = \{polars\ of\ A \in \mathscr{A}\ on\ the\ sphere\ S^2\}$

Claim: G acts on P: $G(A)$ is the axis of $g^{-1}R_A g$

Thus $P = \coprod Orb$, take $|Orb| = o_i, |Stab| = r_i \geq 2$

Count $\{(g, p) | g(p) = p, g \neq 1\}$

Every g fixes exactly 2 polars (unless) : $2|G| - 2$

On the other hand $\# = \sum_{p \in P} (r_p - 1) = \sum_{i=1}^m o_i(r_i - 1) = m|G| - \sum_{i=1}^m \frac{|G|}{r_i}$

$\sum_{i=1}^m 1/r_i = m - 2 + 2/|G|$

One can easily find the only possible cases are $m = 2\ and\ 3$

https://groupprops.subwiki.org/wiki/Classification_of_finite_subgroups_of_SO(3,R)

2.7 Conjugate Classes

Group G acts on itself, with action $(g, a) \mapsto gag^{-1}$

$Cl(a) = \{a^g | g \in G\}, Cl(e) = \{e\}$. If G Abelian, $Cl(g) = \{g\}$. If $G = GL(n)$, $Cl = Similarity$

$Cl(a) = |G|/|Z(a)|$ $(Z(a) = Stab(a))$

Class Equation:

$$G = \coprod Cl_\alpha = \overset{length\ 1\ orbit}{|Z(G)|} + \sum_{Cl_\alpha \geq 2} |Cl_\alpha|$$

Example:

1. Take $G = D_8, 8 = \overset{e}{1} + \overset{\omega^2}{1} + \overset{\omega^{\pm 1}}{2} + 2 + 2$
2. If G is a $p-$group, $|Z(G)| \neq 1$: trivial from the Class Equation.
3. A_5 simple. (View A_5 as the sym. of 12-gon)
   $60 = 1 + \overset{Edge:\pi}{15} + \overset{Vertices:\pm\pi/3}{20} + (\overset{Faces:\pm\pi/5\ or\ \pm 2\pi/5}{12 + 12})$

However, normal subgroups must be the union of the classes. While $60/(1 + 15) \notin \mathbb{Z}$ etc.

4. Class Equations for S_n.

2 permutations are in the same class $\iff$ they have the same type: only need to observe $(123)^g = (g(1)g(2)g(3))$

For example: types of S_4 are $(1^4), (1^2 2), (13), (2^2), (4)$

5. $A_4 : 1 + 4 + 4 + 3$
6. A_n Simple. $(n \geq 5)$

Proof: $n \leq 5$ checked.

Suppose A_m checked, for A_{m+1}

Since A_{m+1} acts on $[1\ m+1]$, $Stab(t) \cong A_m$ simple.

Consider $N \trianglelefteq A_{m+1}$: $N \cap Stab(t) \trianglelefteq Stab(t)$

case 1. $\exists t$, $N \cap Stab(t) = Stab(t)$

$\forall (ijk)\ and\ (ijk)^t \in Stab(t) \subseteq N \implies N = A_{m+1}\ (i,j,k \neq t)$

The implication comes from conjugating t and you can get all 3-cycles. (rather than those who does not contains t)

case 2. $\forall t\ N \cap Stab(t) = 1$

Take $\phi \subseteq N$

2.1 If $\phi = (12)(34)\cdots$

$[(123)^{-1}, \phi] = (14)(23)\cdots \in Stab(t)$, since $m \geq 5$, one can always find a t to cause a contradiction.(Contradiction comes from $[(123)^{-1}\phi(123)]\phi^{-1} \in N$)

2.2 If $\phi = (123)\cdots$

$[(12j)^{-1}, \phi] = (1j2)(23\phi(j))$ Get the contradiction similarly.

Another Proof: Artin.

Key is about the 3-cycles.

2.8 Filtration/Series, Solvable

Subnormal series: $1 = N_0 \triangleleft N_1 \triangleleft \cdots \triangleleft N_l = G$, define its factors are N_{i+1}/N_i

If the factors are simple, we call the series a composite series.

We can always get a composite series in a finite group G: find maximal proper normal subgroups.

Thm. (Jordan-Holder, Schreier refinement)

Schreier refinement has a elegant proof by using Zassenhaus lemma. Apply Schreier refinement on two distinct compositew series we directly get Jordan-Holder theorem.

(Solvable Group) Group G solvable if exists abelian-factor subnormal series.

G solvable, if the derived series(quotienting commutator $[G,G]$) descend to 1

Solvable is closed under taking subgroups/quotient group/extension: $N, G/N$

Proof:

1. $N^{(k)} \hookrightarrow G^{(k)}$
2. $G^{(k)} \twoheadrightarrow (G/N)^{(k)}$
3. Consider surjective group homomorphism $\varphi : G \to G/N$, since G/N Solvable, $\exists n, \varphi(G^{(n)}) = (G/N)^{(n)} = 1$, thus $G^{(n)} \leq N$, the rest can be deduced from the solvability of N.

Example/Propopsition:

$S_{n\geq 5}$ is unsolvable: Consider its derived series: $S_n \to A_n \to A_n \to \cdots$

2.9 Practice: Rubik's Cube

Take group $G_0 =< U, D, L, R, F, B >$, where e stands for the standard cases. Trivially $G \hookrightarrow S_{54}$

We have to relate the product of $U, D \cdots$ with the state of the cube.

Assume the cube's center are fixed. Each corner has 3 states($twist^3 = 1$), each edge has 2 states ($flip^2 = 1$)

Structure Theorem: $G_0 \cong (\mathbb{Z}_3^7 \times \mathbb{Z}_2^{11}) \rtimes [(A_8 \times A_{12}) \rtimes \mathbb{Z}_2]$

First we discuss about the semi-direct product. (See the reference article about the relation between the presentation of linear functions and semi-direct product.)

We are familiar with the inner semi-product:
$H \leq G, N \trianglelefteq G, H \cap N = 1, G = NH, then\ G = N \rtimes H$

In this case $H \cong G/N$. Moreover, the short exact series(SES) $1 \to N \hookrightarrow G \to H \to 1$ right splits.

(Examples: $1 \to C_n \to D_{2n} \to \mu_2 \to 1$; $T(n) \triangleleft Isom(n), Isom(n)/T(n) \cong O(n)$, is $Isom = T \rtimes O$?)

(Examples: Klein Bottle $\pi_1(KB) =< a, b > /(aba^{-1}b)$, one can easily get the split SES $1 \to < b > \to \pi_1 \to < a > \to 1\ \pi_1 = \mathbb{Z} \rtimes \mathbb{Z}, \varphi :< a > \to Aut(< b >), b^{a^s} := b^{(-1)^s}$)

(Question: $\mathbb{Z}_4 = \mathbb{Z}_2 \rtimes \mathbb{Z}_2\ s.d.prod$? No! It's not! ; $1 \to \mathbb{Z}_4 \to Q_8 \to \mathbb{Z}_2 \to 1$ Splits? No!)

Now we give the prrof of magic cube group structure theorem.

1. $(7 \to 1)$ Assign each corner an index. $\forall g, h \in G_0$, define
   $Co(g, h) = \#twists = \sum Co^i(g, h) \in \mathbb{Z}/3\mathbb{Z}$

Here Co^i denotes the twists of $i - corner$ (the difference between the start and end states on $i - corner$)

Conclusion: $Co(g, h) = 0$: It suffices to check generator $U, D\ etc.$ cases.

Corollary: Given the position and orientations of 7 corners, the last corner is determined.

2. $(11 \to 1)$ Similar.

3. Position of edges is in S_{12}, position of corners is in S_8

Thus exists group homomorphisms $G \to S_{12}(S_8)$, we claim $\sigma(e_{12})\sigma(c_8) = 1, where\ e_{12} \cdots are\ the\ images\ in\ S_{12}(or\ S_8)$. (This can be checked over the generator cases)

Thus we cannot exchange a pair ofcorners without exchanging edge.

4. $(\pm twists)\ \forall$ 2 corners(or edges), exists a method that only twisting them(opposite orientation) without making other changes. (The existences can be deduced from magic cube techiniques)
5. $(3-cycle)$ 3-cycle of corners and edges.(This is about positions) (similar to 4: exists a method that only circulating 3 corners etc.)
6. (Main theorem)

6a. $O_0 = \mathbb{Z}_3^7 \times \mathbb{Z}_2^{11} \lhd G_0$ (This can be deduced from 1,2. Normality is trivial: this subgroup is only about orientation, without changing the block's positions)

6b. Consider G_0/O_0, this group is only about positioning. (Orientation free)

Obvious that $G_0/O_0 \to S_{12} \times S_8$ (3. Indicates that A_{12}, A_8 Exists in G_0/O_0)

Since the existence of $3-cycle$ algorithm and A_n is generated by the 3-cycles. We get $A_{12} \times A_8 \lhd G_0/O_0$

Take parity function $\sigma \cdot \sigma : (G_0/O_0)/(A_{12} \times A_8) \to C_2 \times C_2$, From 3. we know the remaining part is a cyclic group $\mathbb{Z}_2 = \{(1,1),(-1,-1)\}$

Methods and Techniques:

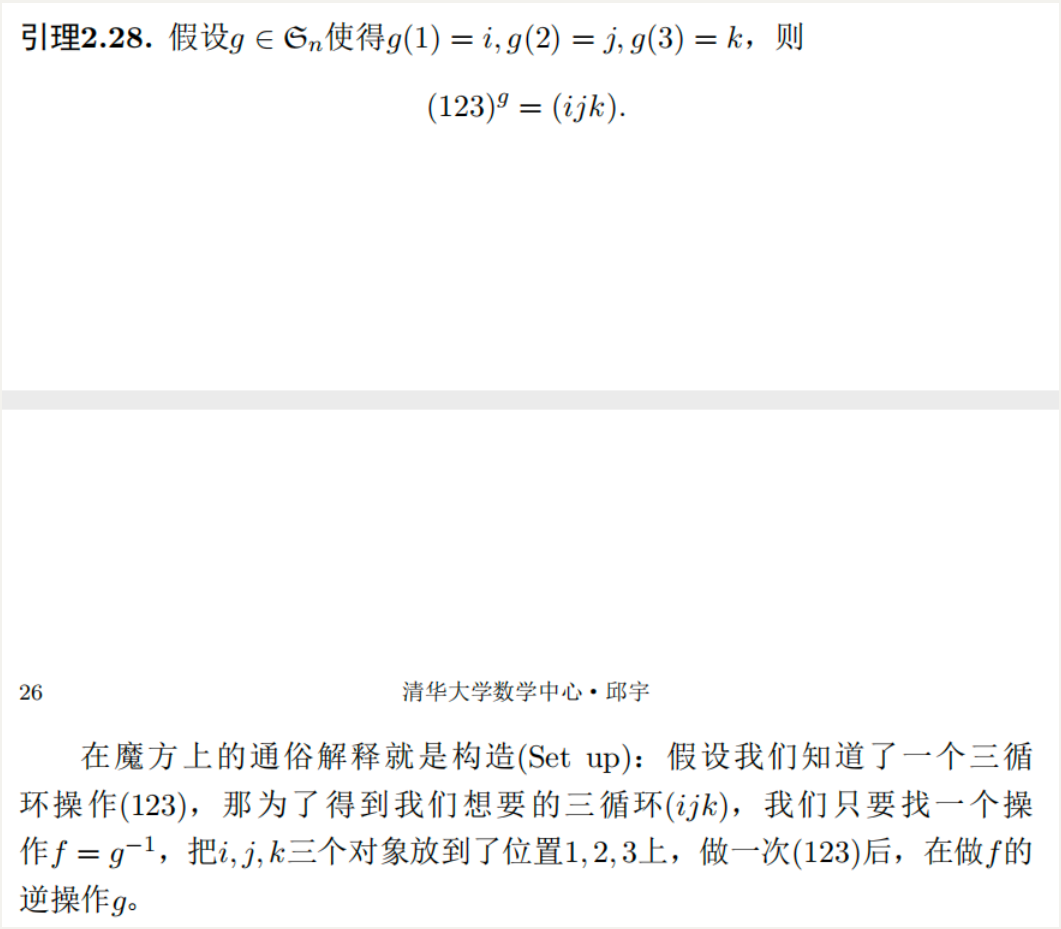
1. Commutators $[a,b] = aba^{-1}b^{-1}$

$S_0 = [U^{-1}, R]$, then $\mathrm{ord} S_0 = 6$

Through practice, we discover that:

S_0^3 =Double 2-cycles of Corners; S_0^2 =3-cycles of Edges.

2. Conjugating plays an important role: S_0^3 usually does not exchange the exact 3 corners that we want to exchange. (Here the conjugating element g can change other blocks)



引理2.28. 假设$g \in \mathfrak{S}_n$使得$g(1) = i, g(2) = j, g(3) = k$，则

$$(123)^g = (ijk).$$

在魔方上的通俗解释就是构造(Set up)：假设我们知道了一个三循环操作(123)，那为了得到我们想要的三循环(ijk)，我们只要找一个操作$f = g^{-1}$，把i, j, k三个对象放到了位置$1, 2, 3$上，做一次(123)后，在做f的逆操作g。

Thus through S_0^2, S_0^3, one can complete the positioning stuff.

3. About orientations: S_0^2 also changes the orientations.

2.10 Some other topics

2.10a $SU(2), SO(3)$

$U(n) = \{M \in Mat_n(\mathbb{C}) | M\overline{M^t} = I_n\}$

$SU(n)$ satisifies the SES $1 \to SU(n) \to U(n) \to U(1) \to 1$

$SU(2) = \{\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} | |\alpha|^2 + |\beta|^2 = 1\}$, thus $SU(2) \cong S^3$

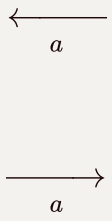
Recall $S^3 \cong \mathbb{R}Q_8$, and $\mathbb{R}^3 \cong \mathbb{R} < i, j, k >$

For any element $q \in \mathbb{R}^3$, we have a group homomorphism $\varphi_q : v \mapsto qvq^{-1}$

Thm. $\exists$ **group homomorphism** $\Phi : SU(2) \to SO(3)$**, with** $\ker \Phi = \pm I_2$

Proof: Define Φ as $q \mapsto \varphi = R_v(2\theta)$ (where $v = (b, c, d), \cos\theta = a, \sin\theta = \pm|v|$)

Def: $\mathbb{R}P^n = \P\mathbb{R}^{n+1}$, thus $\mathbb{R}P^1 = \mathbb{R}^2/\sim = S^1/\sim (v \sim -v)$ (glue diametrical point)

$\mathbb{R}P^2 =$ 

(Ignore the upper hemisphere)($\pi_1\mathbb{R}P^2 =< a, b > /abab, g = 1$)

$\mathbb{C}P^1 \cong \bar{\mathbb{C}}$

Recall $S^n \cong \overline{\mathbb{R}^n}$, (Stereographic Projection)(球极)

We call the operation $\mathbb{R}^n \to \overline{\mathbb{R}^n} \cong S_n$ one-point compactrfication.

This a geometric/topological point of view.

Lem. $\mathbb{R}P^3 = S^3/\sim = B_1(0)/\sim (v \sim -v) \to SO(3)$

The last corresponding is $\vec{v} \to R_v(||v||\pi)$

($SU(2) \cong S_3$, thus the kernel is $\pm I_2$)

2.10b Hopf fibration

The goal is to get a fibration $S_2 \times S_1 \to S_3$: S_2 base space, S_1 fiber type.

$S_2 \cong \mathbb{C}P^1 = [z_1 : z_2]$

Since $S_3 = \{||z_1||^2 + ||z_2||^2 = 1\}$, we define the projection $S_3 \to S_2$ to be $(z_1, z_2) \to [z_1 : z_2]$

Let $z_j = r_j e^{i\theta_j}, r_1^2 + r_2^2 = 1$, thus the projection $p(z_1, z_2) = \frac{r_1}{r_2} e^{i\pi(\theta_1 - \theta_2)}$

Fix $\rho = r_1/r_2, T_\rho = \{(z_1, z_2)\ s.t.\ p(z_1, z_2) = \rho \cdot e^{i\pi \cdot something}\}$

From previous conditions, $T_\rho \cong S_1 \times S_2$, which is a bunch of fiber.

This is more or less the view of fibration, however, $T_0 = S^1$ in xy-plane, $T_\infty = z - axis$, the fiber $p^{-1}(\rho e^{i\pi\theta})$, which is part of T_ρ

2.10c Conjugation class of $SU(2)$

$SU(2) = \cup_{|a| \leq 1} Cl(a)$,

where $Cl(a) = \{\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} | with\ tr = 2a\}$

Since $trAMA^{-1} = trM$, it can be checked it is indeed an conjugation class.

Each $Cl(a) \cong S^2$

3. Linear Representation of Finite Groups

(Def: Representation) A representation of a group G on V is a Group homomorphism $\rho : G \to GL(V)$, (thus V is a representation of G)

Or saying more explicitly, it is a group action $G \times V \to V$, preserving linear structure, namely $g(\sum \lambda_i v_i) = \sum \lambda_i g(v_i)$

In linear algebra, we usually use matrix form to represent $GL(V)$, namely $GL(n, \mathbb{C})$ (resp. a certain set of basis)

(Def: Hom. between Representations) A homomorphism between two representation is a linear map φ, such that following graph commutes:

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & W \\ {\scriptstyle \rho_V}\downarrow & & \downarrow{\scriptstyle \rho_W} \\ V & \xrightarrow{\varphi} & W \end{array}$$

If φ is a isomorphism, call the representation isomorphic.

Call the set of homomorphism between representation $Hom_G(V, W)$

Namely, $Rep^n = Hom(G, GL(n, \mathbb{C}))/GL(n, \mathbb{C})$

(Def: Sub rep.) Sub rep. V' of V is a subspace such that $\rho_g(V') \subseteq V'$

(Def: D.S./D.P.) $g(v \otimes w) = g(v) \otimes g(w)$ etc.

Example: A representation: $C_\infty \to GL(V)$, the image of its generator can be selected arbitrary. $na \mapsto nA$

Example: A representation: $C_t \to GL(V)$, generator $a \mapsto A$, $A^t = I_n$

Example: G a finite abelian group: $\forall a \in G, \rho(a)$ is a diagnol matrix.

Lemma. If A, B diagonalizable, then A, B can be simultaniously diagonalizable $\iff AB = BA$

Proof:

Suppose $A_{n\times n}, B_{m\times m}$

Thus, A, B Diagonalizable $\iff C = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ diagonalizable.

(Only need to check the $\Leftarrow$ Direction: Suppose $D = SCS^{-1}, S = \begin{pmatrix} x_1 & \cdots & x_{m+n} \\ y_1 & \cdots & y_{m+n} \end{pmatrix}$,
$Ax = xD_A, By = yD_B$, namely $x_{,i}$, y_i are eigen vectors, thus
$rankS \leq n + m = rankX + rankY \leq n + m$ which leads to the equality, thus diagonalizable)

Thus in the lemma $\Rightarrow$ direction is trivial.

$\Leftarrow$ If $A^P = D_A = diag\{\lambda_i I_{m_i}\}$

$AB = BA \iff D_A B^P = B^P D_A$, expanding in block matrix one can get
$B^P = \begin{pmatrix} B_{m_1} & \cdots & O \\ \cdots & \cdots & \cdots \\ O & \cdots & B_{m_l} \end{pmatrix}$

Since B^P diagonal, suppose $(B^P)^Q$ Diagonal, and $(A^P)^Q$ diagonal obviously, thus we get the conclusion.

(Another Proof: $AB = BA \implies A, B$ have common eigen vectors)

Back to the representation of finite Abelian group.

Since commutative, we can find a basis such that the image of every elements is a diagonla matrix, namely $g(e_i) = \lambda(g, i)e_i$

Thus as an representation $V = \mathbb{C} < e_1 > \oplus \cdots \oplus \mathbb{C} < e_n >$

(Def. irreducible) A rep. of G is irreducible, if $\nexists$ non-trivial subrep.

(The 1-dim case $\rho : G \to GL(\mathbb{C}) = \mathbb{C}^*$ is called character)

(Def. Permutation rep.) $\rho_S : S_n \to GL(V) : \rho_S(\sigma)(e_i) = e_{\sigma(i)}$

(Def. Regular rep.) If $|G| = n$, exists a regular rep.
$\rho_{rep} : G \to GL(V), g \mapsto \rho(g)(e_h) = e_{gh}$**, where the basis of V is $\{e_i | i \in G\}$**

Regular rep. is not irreducible.

Take $\mathbb{C} < \bar{e} = \sum e_g >= V_0$ is a non-trival subrep.

(Def.) Exists a rep. on $Hom_{\mathbb{C}}(V, W)$

For any $\varphi \in Hom_{\mathbb{C}}(V, W), g(\varphi) = \rho_W(g) \circ \varphi \circ \rho_V^{-1}(g)$

(Def. Unitary Rep.) $U(n) = \{M \in Mat(\mathbb{C}) | MM^* = I_n\}$**, call a rep unitary if** $ImG \subseteq U(n)$**.**

(A Hermitian form on V is a bilinear form on complex linear space)

(Def.) $T \in GL(V)$ **is unitary w.r.t.**$<,>$ **if** $< T(v), T(w) >=< v, w >$**, calling this unitary form** $U(V)$

(The $U(n)$ Case is w.r.t. standard Hermitian form)

Calling $W \subseteq V$ G-stable if $G(W) \subseteq W$

Calling Hermitian form $<,>$ G-stable if $< g(v), g(w) >=< v, w >$

(Thm. Weyl's Unitary Trick) If $|G| < +\infty, \forall V, \rho$, then $\exists$ a G-stable Hermitian form $<,>_G$, such that $\rho(G) \subseteq U(V)$

Proof:

$\forall <,>$: Take the $< v, w >_G = \frac{1}{|G|} \sum_{g \in G} < g(v), g(w) >$

(Thm. Maschke) $|G| < \infty$,every rep. of G is the direct sum of irreducible rep.

Proof:

Lemma(Artin 10.3.4): V is a Hermetian space, ρ is an unitary rep. on it. Suppose W is $G-$ invariant subspace, then $W_\perp$ is also $G-$Invariant. ρ Is the direct sum of ρ_W and $\rho_{W^\perp}$

Lm pf: Take $v \in W^\perp, < w, g(v) >=< g^{-1}(w), v >= 0$

Lm alt. Pf: Take $V = W \oplus W''$, $\exists$ projection $\pi : V \to W, \pi|_W = id$.

Let $\pi_G = \frac{1}{G} \sum_{g \in G} g \pi g^{-1}$. Then it is also a projection, and commutes with every element of $h \in G$.

Then kernel $W' = \ker \pi_G$ is $G-$Invariant, and
$W' \cap W = \{0\}, \dim W' + \dim W = \dim V$; thus we get a direct $G-$invariant sum decomposition.

Back to the Maschke Proof, take the $G - stable$ Hermitian form, and from Lemma we know if one factor V is not irreducible, then we can decomposite $V = W \oplus W^\perp$

(Schur's Lemma)

Lem. V irreducible, $f \in End_G(V) = Hom_G(V, V) \implies f = \lambda \cdot Id$

Pf: $\exists \lambda \neq 0$ Eigenvalue, E_λ Is eigenspace, then E_λ is $G-$inv.

$f - \lambda \cdot Id \in End_G(V) \implies \ker = V$. $f(g(v)) = g(\lambda(v)) = \lambda g(v)$.

Cor. V, W Irreducible, $f \in Hom_G(V, W)$ where V, W is irreducibe.

Then either

(The Uniqness of Maschke's Theorem) Suppose we have $V = \oplus_{W_k \in irr} W_k^{\otimes m_k}$, $V' = \oplus_{W_k' \in irr} W_k'^{\oplus m_k'}$

$\phi \in Hom_G(V, V')$, Schur Lemma guarentee that for each factor, $\phi(V_k) \subseteq V_k'$, thus uniquness.

$Irr(S_3)$

$\rho_0 = Trivial\ rep.\ , \rho_{\pm} = \sigma(g) \in \mathbb{C}^*$

$\rho : S_n \to GL(\mathbb{C}, n = \oplus \mathbb{C} < e_i >)$ a permutation rep.

Take $\mathbb{C}^n = V = W \oplus \mathbb{C} < \sum e_i >$ recalling that latter part is $G-$invariant.

Take $n = 3, W = \mathbb{C} < e_1 - e_2 > \oplus \mathbb{C} < e_2 - e_3 > \oplus \mathbb{C} < e_1 + e_2 + e_3 >$

Ignore the last part,
$\phi = (123), \phi(e_{1-2}) = (e_{2-3}); \tau(23) = \tau(e_{2-3}) = e_{1-3} = e_{1-2} + e_{2-3}$

Thus under the base e_{1-2}, e_{2-3}, we indeed get a irreducible rep.

$$\phi \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \tau \mapsto \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$$

Another rep. with a direct geometry view:

$$\phi \mapsto \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}, \tau \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

or another one:

$$\phi \mapsto \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix}, \tau \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

These 3 rep. are all the same, call it ρ_{st}.

(By changing basis)

Lem. $\forall (V, \rho)$ **of** S_3**,** $\rho = \rho_0^{\oplus ?} \oplus \rho_{\pm}^{\oplus ?} \oplus \rho_{st}^{\oplus ?}$

$\rho(\phi)^3 = id$, thus with eigen value $1, \omega, \omega^2$

Then $V = V(1) \oplus V(\omega) \oplus V(\omega^2)$

$\tau \phi \tau^{-1} = \phi^{-1}, \tau(V(\omega^j)) = \omega^{-j}$

$V(1) = V(1)^+ \oplus V(1)^- = V_0^{\oplus ?} \oplus V_{\pm}^{\oplus ?}$

Tensor Product

The basis of $V \otimes W$ is $e_i \otimes f_j$.

Pf: Span is trivial, suppose $\sum \lambda_{ij} e_i \otimes f_j = 0$

Take $e_i^* : V \to \mathbb{C}, e_s \mapsto \delta_{is}$

And we get $e_i^* \otimes f_j^* : V \otimes W \to \mathbb{C}$

Thus from this characterize map, we can get each $\lambda_{ij} = 0$

Facts: $U \otimes (V \otimes W) = (U \otimes V) \otimes W$

$(U \oplus V) \otimes W = (U \otimes W) \oplus (V \otimes W)$

$\exists isomorphism, W \otimes V^* = Hom(V, W)$

Pf: $w \otimes f \mapsto (w \otimes f)(v) = f(v)w$

$A \in End(V), B \in End(W) \implies A \otimes B \in End(V \otimes W)$ (If written in matrix form, it is indeed the matrix tensor perform)

$detA \otimes B = (detA)^{dimB}(detB)^{dimA}$

$Sym^n V =< \frac{1}{n!} \sum_{\sigma \in S_n} \sigma(e_1 \otimes \cdots \otimes e_n) >$

Character Theory

(Class Function) $G = \coprod C_i$**(Conjugation Class)**

A class function $\Phi : G \to \mathbb{C}, \Phi(g) = \Phi(hgh^{-1})$, thus it is a function of class, namely $\Phi(G) =< 1_{C_i} >$, where $1_{C_i}(C_j) = \delta_{ij}$

($\Phi(G)$ denotes the linear space of class functions)

Lemma: $\exists$Hernitian form $<,>$ on $\Phi(G)$: Take $< \Phi, \Phi' >= \frac{1}{|G|} \sum \Phi(g)\overline{\Phi'(g)}$

(Character) A character of representation (ρ, V) **is** $\chi_\rho : G \to \mathbb{C} : g \mapsto tr\rho(g)$

(不选择det是因为它丢失的信息太多了)

($tr\rho(g)$ well-defined, since changing basis does not change trace.)

Lemma: $\chi_\rho \in \Phi(G)$, since conjuating does not change trace.

If ρ irreducible, say χ_ρ is called an irreducible character.(?)

Lemma(Properties)

1. $\chi(1) = \dim V$
2. $\chi \in \Phi(G)$
3. $\chi(g^{-1}) = \overline{\chi(g)}$
4. $\chi_{V^*}(g) = \chi(g^{-1})$
5. $\chi_{V \oplus W} = \chi_V + \chi_W$
6. $\chi_{V \otimes W} = \chi_V \cdot \chi_W$

(Main Theorem) $\Phi(G) =< \chi_\rho | \rho \in Irr(G) >$

In particular, this admits a normal orthogonal basis. (Here the inner product is induced from the previous Hermitian form $< \Phi, \Phi' >= \frac{1}{|G|} \sum \Phi(g)\overline{\Phi'(g)})$

Proof:

Let $\phi \in Hom_{\mathbb{C}}(V, W)$ (irreducible rep. V, W)

We get an averaging rep. Hom. $\underline{\phi} = \frac{1}{|G|} \sum \rho_W(g) \circ \phi \circ \rho_v(g)^{-1}$

Cor. $V \ncong W \implies \underline{\phi} = 0$ (Schur Lemma.) $\sum B_g M A_g^{-1} = 0$

$V = W : tr\underline{\phi} = \lambda \cdot \dim V = tr\phi$.(Since $\lambda \cdot I_n$)

Orthogonal relation:

$< \chi_V, \chi_W >= 0, V \ncong W \in Irr(G)$

Proof: $< \chi_V, \chi_W >= \frac{1}{|G|} \sum trA_g trB_{g^{-1}} = (use\ Artin\ Lem.10.8.1) = 0$

$< \chi_V, \chi_V >= 1$

Proof: Use Previous result ($V = W : tr\underline{\phi} = \lambda \cdot \dim V = tr\phi$.(Since $\lambda \cdot I_n$))

Complete:

$\Phi(G) = span < \chi_\rho | \rho \in Irr >$

Proof:

If exists another Φ, such that $< \Phi, \chi_i >= 0$

Take $T_\rho = \frac{1}{|G|} \sum \overline{\Phi(g)} \rho(g) \in Hom_{\mathbb{C}}(V, V)$

Then it is an element of $Hom_G(V, V)$

Consider regular rep. We get $\chi_{reg}(1) = |G|, otherwise\ 0$

$< \chi_V, \chi_{reg} >= \frac{1}{|G|} \sum \chi_V(g) \chi_{reg}(g) = \chi_V(1) = \dim V$

Consider $\rho_{reg} = \oplus \rho_i u^{d_i}$, thus $d_i = \dim V_i$

If ρ Irreducible, $T_\rho = 0$, thus $T_{\rho_{reg}} = 0$

Then $T_{\rho_{reg}} = \frac{1}{|G|} \sum \overline{\Phi(g)} e_g = 0$, thus $\Phi = 0$

Thus Completeness.

Cor. $\#Conj.Class = \#Irr(G)$

From the maschke theorem $\rho = \oplus \rho_i^{n_i}$, right inner producting ρ_i one get $n_i =< \rho, \rho_i >$

Thus $V \cong_G W \iff \chi_V = \chi_W$

$\rho \in Irr(G) \iff ||\rho|| = 1$

Character Table. Column: Conjugating Class; Row: Irreducible Rep. The element: the value.

S_3 :

S_3	(1)	(123)	(23)
χ	1	1	-1
$\chi_{\pm}$	1	1	-1
χ_{st}	2	-1	0

列正交:

$\sum \chi_i(C_t)\chi(C_s) = \delta_{st}(|G|/|C_s|)$

See Notetakers version.

Recall $\mathbb{C}[G]$ is not only a vector space, but also a group algebra. Since the topic we are discussing about is representations $G \to GL(V)$. We claim this has a correspondence with representation of $\mathbb{C}[G]$.

Lemma. $\rho : G \to GL(V) \iff \rho : \mathbb{C}[G] \to GL(V)$

Proof: $\Longrightarrow$ Through linear extension; $\Longleftarrow$ Through restriction.

Theorem. $|G| < +\infty$, exists an algebra isomorphism:

$\mathbb{C}[G] \overset{\widetilde{\rho}=\oplus\rho_i}{\longrightarrow} \oplus End_{\mathbb{C}}(V_i) : \varphi \mapsto (\rho_V(\varphi))$

Proof: ?(Serre 6.2 V_i stands for irreducible representation)

Serre 6.5 (About integralilty of d_i)

Lifting of Reps of Quotient group

$G \longrightarrow G/N \longrightarrow GL(V)$ induces a representation from the quotient group rep.

Take the composed representation to be $\widetilde{\rho} = \pi \circ \rho$

$\widetilde{\chi}(1) = \dim V = \chi(1); \chi \in Irr(G/N) \iff \widetilde{\chi} \in Irr(G)$

Proof:
$< \widetilde{\chi}, \widetilde{\chi} >= \frac{1}{|G|} \sum \widetilde{\chi}(g)\overline{\widetilde{\chi}(g)} = \frac{1}{|G|} \sum |N| \chi(gN)\overline{\chi(gN)} = \frac{|N|}{|G|} \sum \chi(h)\overline{\chi(h)} =< \chi, \chi >$

Define $\ker \chi = \chi^{-1}(\chi(1))$, recall $\ker \rho = \rho^{-1}(id)$

$\ker \chi = \ker \rho$

Proof: $|\chi(g)| = \chi(1) \iff \rho_g = \lambda \cdot I$: Consider the diagonalization of ρ_g.

If $\rho_g = Id, \chi(g) = \chi(1)$; if $\chi(g) = \chi(1) \implies \rho_g = \lambda \cdot Id \& \lambda = 1 \implies \rho_g = Id$

Cor. $\ker \chi \lhd G$

$\widetilde{\chi} \in Rep(G), \widetilde{\chi} is\ a\ lift\ of\ G/N \iff N \trianglelefteq \ker \widetilde{\chi}$.($\widetilde{\chi}$在陪集上取值相同)

Thm. $\exists 1-1$Correspondence: $Rep(G/N) \leftrightarrow \{\rho \in Rep(G) | N \trianglelefteq \ker \rho\}$

(This correspondence can be restricted to irreducible representation)

Prop. $N = \cap_{\substack{\chi \in Irr(G) \\ N \trianglelefteq \ker \chi}} \ker \chi$

Proof: $\cap_{\chi \in Irr(G)} \ker \chi = e \ \cap \ker \chi_{irr} \subseteq \ker(\sum c_i \chi_i) = \ker 1_{C_1} = 1$

Consider the lifting.

Cor. G is simple $\iff$ $\forall$non trivial $\chi \in Irr(G), \ker \chi = 1$

Examples.

$A_4' = [A_4, A_4] = \{(12)(34), (13)(24), (14)(23), 1\}, A_4/A_4' \cong C_3$

From character table of C_3, we get character table of A_4.

S_4 :

Still use the previous subgroups, $S_4/A_4' \cong S_3$, conduct the similar process

Similarly $Z(\chi) = \{g || \chi(g)| = \chi(1)\}, Z(G) = \cap_{irr} Z(\chi)$

Linear Characater

A character χ is linear if $\chi(1) = 1$

$LC(G) = \{\chi \ linear\}$

Lemma $G' \trianglelefteq \ker \chi (\forall \chi \in LC(G))$

More precisely, $LC(G) = Lifts\ of\ Irr(G/G'), |LC(G)| = \#Irr(G/G') = |G/G'|$

$\Theta \in LC(G), \chi \in \chi_{Irr(G)} \implies \Theta \cdot \chi \in \chi_{Irr(G)}$

(Computing its inner product implies a direct proof)

D_{2n}

Tensor product of characters

Given 2 representations, we can get a tensor product representation via tensor product.

$\chi_{V \otimes W} = \chi_V \cdot \chi_W$

$< \chi_{V_1 \otimes W_1}, \chi_{V_2 \otimes W_2} > = < \chi_{V_1}, \chi_{V_2} > \cdot < \chi_{W_1}, \chi_{W_2} >$

Cor. $\chi_{Irr(G \times H)} = \chi_{Irr(G)} \cdot \chi_{Irr(H)}$

Def. $G \to G \times G \to GL(V \otimes W)$

□

4. Mckay Correspondence

Directed Graph.

Given a group $|G| < +\infty$, fix a $\rho \in Rep(G), MG(G, \rho) = \begin{cases} MG_0 & = Irr(G) \\ MG_1 & = \{\rho_i \xrightarrow{a_{ij}} \rho_j\} \end{cases}$

(Here a_ij denote the mutiple number of edges)

$a_{ij} = \dim Hom(V \otimes V_i, V_j) = < \chi\chi_i, \chi_j >$

Take $\Gamma(G) = MG(G < SU(2), \rho_{nat})$

Lemma. $a_{ij} = a_{ji}$ provided that $\chi(g) = \overline{\chi(g)}$. (Or saying self-dual)

$$\frac{1}{|G|}\sum \chi(g)\chi_i(g)\overline{\chi_j(g)} = \frac{1}{|G|}\sum \chi(g^{-1})\chi_i(g^{-1})\overline{\chi_j(g^{-1})} = \frac{1}{|G|}\sum \chi(g)\chi_j(g)\overline{\chi_i(g)}$$

对于$\Gamma(G)$，取Cartan 矩阵$C = (c_{ij} = 2\delta_{ij} - a_{ij})_{|G|\times|G|}$。Here
$a_{ij} = \dim Hom_G(V_i \otimes V, V_j)$

C和Γ互相决定了对方。

$$G \overset{finite}{<} SU(2), G\ abelian \iff G = C_n \iff V_N\ reducible$$

Ex. $\Gamma(C_n) = n - Polygon.$

Lemma. $2d_i = \sum a_{ij}d_i$

Lemma. $a_{ij} = a_{ji}; a_{ii} = 0$

Lemma. Γ is connected graph.

Pf: 1. Induction. $v_i \in \Gamma_0 \iff v_i$ is a summand of $V^{\otimes m}$,

Suppose $\exists v_i \notin \Gamma_0, < \chi_i, \chi_v^m >= 0$

However $< \chi_i, \chi_v^m >= \frac{1}{|G|}\sum \chi_i(g)\overline{\chi_v(g)^m}, \chi_v(g) = \begin{cases} \pm 2 & \pm I \\ 2\Re(\lambda) & O/W \end{cases}$

Thus, $\chi_i(I) + \chi_i(-I)(-1)^m + \sum \chi_i(g)|\overline{\chi_v(g)}/2|^m = 0$

Let $m \to \infty$, one get $\chi_i(I) = \chi_i(-I) = 0$

Thus contradiction.

Lemma. $a_{ij} \leq 1$ provided that $G \neq C_1\ or\ C_2$.

Pf: If $\exists a_{ij} \geq 2$.

$2(d_i + d_j) = \sum a_{ik} d_i + a_{jk} d_k = 2(d_i + d_j) + etc. \implies G = C_1 \ or \ C_2.$

Thm. Classification.

$\widetilde{A_n}, \widetilde{D_n}, \widetilde{\widetilde{E_{6,7,8}}} (Exceptional \ Graphs)$

These are called Euclidean type(Since it corresponds to 3d polygon)

Dynkin (Spherical Type): Finiteness

Dynkin (Euclidean Type): Tame

Dynkin (Hyperbolic Type): Wild

Given a connected graph Γ, Cartan matrix C. Say vertex set $\Gamma_0 = \{0, \cdots, n\}$.

Def.

Quadratic Form $q(\alpha) = \sum \alpha_i^2 - \sum_{i \leq j} c_{ij} \alpha_i \alpha_j$; Bilinear Form
$(\alpha, \beta) = q(\alpha + \beta) - q(\alpha) - q(\beta) = \alpha^T C \beta.$

Particularly $q(\alpha) = \frac{1}{2}(\alpha, \alpha).$

Def. Under the condition of q semi-positive determined, let radical
$rad(q) = \{\alpha | (\alpha, -) = 0\}.$

Theorem. $P.D. \iff Dynkin; S.P.D. - P.D. \iff Euclidean$

Pf: Say $\alpha \geq \beta$ if $\alpha_i \geq \beta_i, \forall i.$ α sincere if $\prod \alpha_i \neq 0$.

Lemma. If $\exists 0 \neq \beta \geq 0, s.t. \ \beta \in rad(q)$, then β is sincere.

If q is S.P.D., then $rad(q) = \{\mathbb{Q}\beta\} \cap \mathbb{Z}^{n+1}$

Rmk. For Euclidean Γ, $\exists \beta = (d_i) \in rad(q_\Gamma)$.

Proof: $(\beta, -) = 0$. Since $(\beta, \rho_i) = 0$, $(2 - 2a_{ij})\beta_i = \sum a_{ij}\beta_j$

If $\beta_i = 0$, $\sum a_{ij}\beta_j = 0$: $a_j = 0 \; if \beta_j \neq 0$

Since Γ conn. $\beta = 0$, contradiction.

Thus β sincere.

$q(\alpha) = \sum_i (1 - a_{ii})\alpha_i^2 - \sum_{i<j} c_{ij}\alpha_i\alpha_j \overset{Computation}{=\!=\!=} \sum_{i<j} a_{ij}\frac{\beta_i\beta_j}{2}(\frac{\alpha_i}{\beta_i} - \frac{\alpha_j}{\beta_j})^2$

Thus q S.P.D., $q(\alpha) = 0 \iff \alpha, \beta \; proportional$.(Since all connected)

In such case, define $\Delta = \{\alpha \in \mathbb{Z}^{n+1} | q(\alpha) \leq 1\}$ set of roots.

Here real roots $q(\alpha) = 1$,imaginary roots $q(\alpha) = 0$.

If not $Dynkin/Euclidean$, then $\exists \alpha \geq 0, q(\alpha) < 0 \wedge (\alpha, e_i) \leq 0 \forall i$

Fact. $\exists \Gamma^* \subseteq \Gamma; \Gamma : \widetilde{ADE}$.

Let$d^* \in rad(q_{\Gamma^*}), \alpha = 2d^* + e_i$.
$q(\alpha) = \frac{1}{2}(\alpha, \alpha) = 2(d^*, d^*) + 2(d^*, e_i) + \frac{1}{2}(e_i, e_i) < 0$

Thus not $D/E \implies$ not $P.D./S.P.D.$

Previously we get $E \implies S.P.D.$

Only need to show $D \implies P.D.$: since $q(\alpha) = 0 \implies \alpha = (d_i)$

Calculate all roots of A_n, D_n

Summing up: ADE Phenomenon.

$\forall \Gamma, q_\Gamma \ pos. \ def. \iff \Gamma \ Dynkin; S.P.D. - P.D. \iff Euclidean$

This is a purely combinatoric stuff. However this phenomenon has a relation with other branches.

Remark. $Dynkin \iff Spherical; Euclidean \iff Euclidean$

$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\} = \Gamma(2,2,2)$ a binary dihedral group.

Its Mckay graph is exactly $\widetilde{D_4}$

$\Gamma(BD_{2n})$

$SO(3), SU(2).$

Recall $SU(2) \to SO(3), \Phi(q) = \phi_q$, then $\phi^{-1}(R_v(\theta)) = \pm(\cos\theta/2 + \sin\theta/2 \cdot \frac{v}{||v||})$

Since $2I$ is the inverse image of I under the map Φ, one can easily get:
$2I = \{\pm 1\} \sqcup \{\pm(\cos k\pi/3 + \sin k\pi/3 \cdot v_i/||v_i||\} \sqcup \{\pm(v_i + v_j)/||v_i + v_j||\}$
$$\sqcup \{\pm \cos k\pi/5 + \sin k\pi/5 \cdot \sum_5 v_i / || \sum_5 v_i ||\}$$

(Note that $Sp(1) = SU(2)$)

Thus using this fact $2I, 2O, 2T$ can be written down explicitly.

BI	1	-1	$\pm x$	y	$-y$	z	$-z$	z^2	$-z^2$
$\tilde{\chi}_0$									
$\tilde{\chi}_{st}$									
$\tilde{\chi}_n$									
$\tilde{\chi}_n^{\sigma}$									
χ_5									
χ_N									
χ_2									
χ_4									
χ_6									

5. Ellipse Cubic Equation & Elliptic Curves

Elliptic Integrals

Def.(Ellipse) $x^2/a^2 + y^2/b^2 = 1$

Arc length.

$$C = 4\int_0^{\pi/2} \sqrt{a^2\cos^2 t + b^2 \sin^2 t}\mathrm{d}t$$
$$= 4a\int_0^{\pi/2} (1-\lambda \sin^2 t)^{1/2}\mathrm{d}t$$
$$= 4a\int_0^{\pi/2} \sum_{n=0}^{\infty} \binom{1/2}{n} (-\lambda \sin^2 t)^n \mathrm{d}t$$

Recall(?) $F(i,j,k;\nu) = \sum_{n=0}^{\infty} \frac{(i)_n (j)_n}{n!(k)_n}\nu^n$

Thus combining with the Wallis Formula we get $C = 2\pi a F(1/2, -1/2, 1; \lambda)$, where $\lambda = c^2/a^2$.

However $F(i,j,2j;4h/(1+h)^2) = F(i, i-j+1/2, j+1/2; h)$

Thus $C = \pi(a+b)F(-1/2, 1/2, 1; h)$

Remark. Kepler $\pi(a+b)$; Euler $2\pi\sqrt{(a^2+b^2)/2}$; Ramanujan $\pi(3(a+b)-\sqrt{(a+3b)(b+3a)})$

$$\frac{1}{4}C_{a,b}=\int_0^1\sqrt{\frac{a^2-c^2\sin^2 t}{1-\sin^2 t}}\mathrm{d}\sin t=a\int_0^1\sqrt{\frac{1-\lambda s^2}{1-s^2}}\mathrm{d}s$$

$\frac{1}{2}C_{a,b}=\int_{1-\lambda^2}^1\frac{x\mathrm{d}x}{\sqrt{x(x-1)(x-(1-\lambda^2))}}$, where the right hand side integral is called 2nd type Elliptic Integral. (1st type can be achieved by deleting the x over the fraction line)

Cubic Equation

Given a cubic equation over $\mathbb{R}$, it can be deduced into a normal form $(x\to x-a_1/3a_0):x^3+ax+b=0$

Cardano's trick:

Say a root $x=u+v$,
$(u+v)^3+a(u+v)+b=0\implies u^3+v^3+(3uv+a)(u+v)+b=0$

Let $3uv+a=0$ we get $u^3+v^3=-b\wedge(uv)^3=(-a/3)^3$

Thus $u^3,v^3=-b/2\pm\sqrt{\frac{\Delta}{108}}$. Here $\Delta=-(4a^3+27b^2)$, then we get the result

Elliptic Curves

Consider the curve $y^2=x^3+ax+b$ (From previous discussion we have already noticed its importance), and we expect it to be defined over $\mathbb{C}$.

Def.(Elliptic Curves) Elliptic Curves is a projective algebra curve (in $\mathbb{C}P^2$) of genus 1 with a specified point $O=\{0:1:0\}$, and it is not singular.

Plane projective curve $C_f/\mathbb{k}$ is more and less projective varieties. (Here $C_f \subseteq \mathbb{C}P^2$)

Say the variety singular at a point p, if $\dfrac{\partial f}{\partial x} = \dfrac{\partial f}{\partial y} = \dfrac{\partial f}{\partial z} = 0$.

Its quite hard to show the equivlance of previous 2 definitions of elliptic curves. But we can check for curve $y^2 = x^3 + ax + b$, it satisfies the second definitions.

Remark. In general $f(x, y) = \sum a_{ij} x^i y^j$,
$NP(f) = Newton\ Polytope = convex\ hall\ of\ (i, j)$

Genus of Algebraic Varieties: $Genus\ C_f = \#interior\ lattice\ points\ in\ NP(f)$

Singular Example. Singular case: $y^2 = x^3$

Theorem. (Abel Group Structure on Elliptic Curves) $\exists$ an abelian group structure on Elliptic Curve:

1. $Unit = 0 = Infinity\ Point = O, P = P + O = O + P$

2. If $P = (x_P : y_P : 1)$**, then inverse element** $-P = (x_P : -y_P : 1)$

3. $P + Q + R = 0 \iff P, Q, R$ **colinear, namely we define** $P + Q = -R$**.**

Proof:

$P = (x_P, y_P); Q = (x_Q, y_Q)$, take $s = \dfrac{y_P - y_Q}{x_P - x_Q}$ then
$R = (s^2 - x_P - x_Q, y_P + s(x_R - x_P))$

When $x_P = x_Q, y_P = -y_Q$, through definition we immediately get $R = O$

When $x_P = x_Q, y_P = y_Q$, namely $Q \to P$, through taking limits we immediately get the result, where s is the slope of tangent $\dfrac{3x_P^2 + a}{2y_P}$.

Associative Law.

$(P + Q) + R = P + (Q + R)$, verified by direct calculation.

Ossia:

Say $P + Q = A, Q + R = B$.

We want to show $-T = B + P, -S = A + R$ are same points.

Suppose $S \neq T$, we say 3 lines $l_1 = (Q, P, -A); l_2 = (R, S, A); l_3 = (-B, B, O)$,
$m_1 = (Q, R, -B); m_2 = (P, T, B); m_3 = (-A, A, O)$

Say $\tilde{l} = \prod l_i, \tilde{m} = \prod m_i$, since $S \neq T, \tilde{l}(T) \neq 0, \tilde{m}(S) \neq 0$

Let Vector Space $V = \{cubic\ homogenous\ poly.\ in\ \mathbb{C}[x, y, z]\}$, $\dim V = 10$.

WLOG we let P, Q, R generic. Consider
$W = subspace\ of\ V\ such\ that\ it\ vanishes\ at\ \pm A, \pm B, P, Q, R, O$

$\dim W = 10 - 8 = 2, \tilde{l}, \tilde{m} \in W$, and $\tilde{l}, \tilde{m}$ are linear independent. (Consider its value on S, T.)

Thus $W = \text{span} < \tilde{l}, \tilde{m} >$

However $f(x, y, z) = x^3 + axz^3 + bz^3 - y^2z \in W$

Thus $f = \lambda\tilde{l} + \mu\tilde{m}$, as $S, T \in f$, i.e. $f(S), f(T) = 0$, thus $\lambda, \mu = 0$, Contradiction!

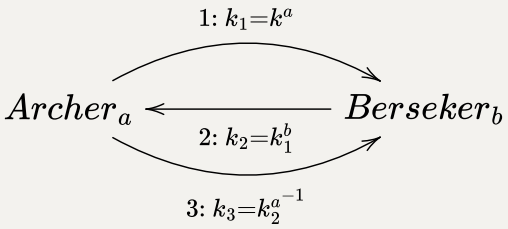
Remark. Theorem also holds over a general field $\mathbb{K}$: especially a finite field.

For example $y^2 = x^3 - 2x/(\mathbb{Z}/11\mathbb{Z})$,
$E = \{(0, 0); \infty; (2, \pm 2); (4, \pm 1); (5, \pm 4); (8, \pm 1); (10, \pm 1)\}$, i.e. $|E| = 12$.

$$(5,7)+(8,10)=(10,-1)$$

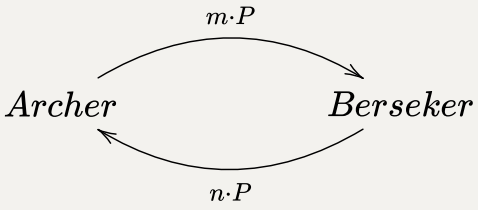
Elliptic Cryptography

Diffre-Hellmen Key-Exchange Protocol.(DHKE)



Transfer information k from Archer to Berseker, where Archer owns a private key a, Berseker owns a private key b. Berseker decode information through $k=k_3^{b^{-1}}$.

Ellip. Agreement on a key: Given a elliptic curve $E: y^2=x^3+ax+b/(\mathbb{Z}/p)$.



Initial point P and the Elliptic Curve and the prime number p are public. $m,n\in\mathbb{Z}$ are resp. Archer and Berseker's private key, they send $m\cdot P, n\cdot P$ to each other, and they can now own the same key $k=(mn)\cdot P$.

Now Archer and Berseker safely own the key without letting others now. Through the same key Archer and Berseker can safely transfer information. (For example Archer sends $k\cdot information$, Bersecker decode it by dividing k.)

Complex Toris

Given a lattice $\Lambda=\{\mathbb{Z}\omega_1+\mathbb{Z}\omega_2\}, \omega_1,\omega_2$ linear independent.

Theorem.(Uniformization Thm.) $Elliptic\ Curves$ **correspond uniquely to a complex toris** $\mathbb{C}/\Lambda$**.**

We must elaborate this a little bit more: Here the correspondence leads to a complex Lie group isomorphism. $z \in \mathbb{C}/\Lambda \mapsto (\wp(z), \wp'(z)) \in E$

Def. Weierstrass function.

$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda - \{(0,0)\}} (\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2})$, through analysis stuff we get $\wp(z)$ is a meromorphic function, and it converges absolutely and uniformly on $\mathbb{C} - \Lambda$

Def. Eisenstein series

$G_k(\Lambda) = \sum_{\omega \in \Lambda - \{(0,0)\}} \omega^{-k}$, $\Lambda = \mathbb{Z}(1, \tau)$, where τ is in the upper half plane, $k > 2$. $G_k = 0$ when k odd. Thus $G_k(\Lambda) = G_k(\mathbb{Z}(1,\tau))$ is a function on $\mathbb{H}$, and
$\begin{cases} G_k(\tau) = G_k(1+\tau) \\ G_k(-\tau^{-1}) = \tau^k G_k(\tau) \end{cases}$

$G_k(\tau)$ converges absolutely.

Proof. Take $\delta =$ the minimum distance between lattice points in Λ, take $Ann(r, d) = B_0(r+d) - B_0(r)$. Then $\#\Lambda \cap Ann(r, \delta/2) \leq 4\pi r/\delta$

And $Ann(n, 1) \leq Const. \cdot n$

Thus $\sum_{|\omega|<1} |\omega|^{-k} + \sum_{|\omega| \geq 1} |\omega|^{-k} \leq \sum_{|\omega|<1} |\omega|^{-k} + \sum_n \#Ann(n,1) \cap \Lambda \cdot n^{-k}$

The second term converges since it has the order n^{1-k}.

$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1) G_{2n+2}(\Lambda) z^{2n}$

Direct calculating:

Since $\frac{1}{(1-z)^2} = \sum_{n=0}^{\infty}(n+1)x^n$

Then $\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \omega^{-2}(\frac{1}{(1-(z/\omega))^2} - 1) = \sum_{n=1}^{\infty}(n+1)\frac{z^n}{\omega^{n+2}}$

$\wp'(z) = -2\sum_{\omega\in\Lambda}\frac{1}{(z-\omega^2)} = -2/z^3 + \sum_{n=1}^{\infty}(2n)(2n+1)G_{2n+2}(\Lambda)z^{2n-1}$

Thus

$\wp^3(z) = 1/z^6 + 9G_4/z^2 + 15G_6 + \cdots$
$\wp'^2(z) = 4/z^6 - 24G_4/z^2 - 80G_6 + \cdots$

Then $F(z) = \wp'^2 - 4\wp^3 + 60G_4\wp + 140G_6$ has no negative exponent terms. Thus F holomorphic and bounded (since periocity).

Thus $F = 0$ (Liouville Theorem)

$(\wp, \wp')\ satisfies\ y^2 = 4x^3 - g_2x - g_3$

Thus there $\exists\phi : \mathbb{C}/\Lambda \to E$, where $z \notin \Lambda \mapsto [\wp(z) : \wp'(z) : 1]; z \in \Lambda \mapsto O$

Conversely $H_1(E/\mathbb{C}, \mathbb{Z}) = \mathbb{Z}\oplus\mathbb{Z}, \omega_1 = \int dx/y, \omega_2 = \int dx/y$

j-Invariant

Given a non-singular elliptic curve $y^2 = x^3 + ax + b$. We define
$j(E) = 12^3 \cdot \frac{4a^3}{4a^3 + 27b^2} = 12^3\frac{g_2^3}{g_2^3 - 27g_3^2}$

Say $y^2 = (x-x_1)(x-x_2)(x-x_3)$, take x into $\dfrac{x-x_1}{x_3-x_1}$, We have the form $y^2 = x(x-1)(x-\alpha)$, then $j(E) = 2^8 \cdot \dfrac{(\alpha^2-\alpha+1)^2}{\alpha^2(\alpha-1)^2}$

Theorem. $(E \iff E') \iff \Lambda = \lambda\Lambda' \iff j(E) = j(E')$

i.e. j is invariant under $SL(2,\mathbb{Z})$ (act on lattice).

Since g_2^6/g_3^6 is invariant under $SL(2,\mathbb{Z})$, we immediately get the theorem.

If we quotient equivalent elliptic curve, then $\mathfrak{M}(E) = \mathbb{H}/SL(2,\mathbb{Z})$

Note that $PSL(2,\mathbb{Z}) = Sym^+(FG)$, $FG = Farey\ \ Graph$. Where FG has type (∞,∞,∞)

A precise construct: $FG_0 = \bar{\mathbb{Q}} = \{p/q\} \pm \{1/0 = \infty\}$,
$FG_1 = \{p/q \leftrightarrow r/s, |ps-qr| = 1\}$

$SL(2,\mathbb{Z})$ acts natually on $FG(\infty,\infty,\infty)$

Example $\Phi_{p/q} = \begin{pmatrix} 1-pq & p^2 \\ -q^2 & 1+pq \end{pmatrix}$ fixing p/q and act as rotating p/q:
$r/s \leftrightarrow p/q \iff \Phi_{p/q}(r/s) \leftrightarrow p/q$

This is the modular space of elliptic curves.

Some Remarks

Since $EC = a\ torus$, $\bar{\mathbb{Q}} = \{all\ simple\ closed\ curves\ on\ T\}$: viewed it as a rational slope line on the complex plane.

If $|ps-qr|=1, |C_{p/q} \cap C_{r/s}| = 1$.

Proof: Exists a action in $SL(2,\mathbb{Z})$ onto $T \to T : C_{p/q} \mapsto C_{0/1}, C_{r/s} \mapsto C_{0/1}$, then immediately get the result.

$Br_3 =< a,b > /(aba=bab), Z(Br_3) \to Br_3 \to PSL(2,\mathbb{Z})$

Consider $f=x^2-y^3, V(f)=\{x^2-y^3=0 | x,y \in \mathbb{C}, (x,y) \in S^3=\bar{\mathbb{R}^3}\}$, this is exactly the trefoil knot.

Proof of the fact: Since knot can be embedded onto a torus $T=S^1 \times S^1$, it satisfies $(e^{i\theta}, e^{i\phi}), 2\theta - 3\phi = 0$

On the other hand $|x|^2=|y|^3 \& |x|^2+|y|^2=1 \implies |x|, |y|$ can be fixed. Then $\begin{cases} x=m_x e^{i\pi\theta} \\ y=m_y e^{i\pi\phi} \end{cases}$, which leads to the result.

Remark. Given a knot $K_{p,q}=\mathbb{V}(x^p=y^q)$. $\pi_1(S^3-K_{p,q}) =< x,y > /(x^p=y^q)$

6. Geometry Mckay Correspondence

Recall. **ADE phenomenon**

1. Classification of regular 3D polyhedron
2. Spericalt triangle tiling
3. $$\begin{aligned} BinaryD(x^p=y^q=z^r=xyz=\delta, \delta^2=1) \to VonDyck(x^p=y^q=z^r=xyz= \\ \to Triangle(a^2=b^2=c^2=1, (ab)^p=(bc)^q=(ca)^r=1) \end{aligned}$$
4. Mckay Graph from Reps of BD.
5. Kleinian Singularities
6. Cluster
7. Quiver
8. Root System (Semi-simple Lie Algebra)

Finite Subgroup of $SL(2,\mathbb{C})$

Lemma. Any finite subgroup of $SL(n,\mathbb{Z})$ is conjugate to some $SU(n)$.

Proof: Recall weyl's unitary trick.

Table of ADE groups.

$A_n : C_{m=n+1} =< \phi > /\phi^m = 1, \phi_m = \begin{pmatrix} \omega_m & \\ & \omega_m^{-1} \end{pmatrix}$

$D_n : BD_{2m}(4m = n-2) =< \tilde{\phi}_{2m}, \tilde{\tau} > /(\phi^m = \tau^2 = -1), \tau = \begin{pmatrix} 0 & \mathbb{i} \\ \mathbb{i} & 0 \end{pmatrix}$

Lemma. $\mathbb{C}[u,v]^G = \{p | g(p) = p \forall g\}$ **is a (sub)ring.**

Calculate $\mathbb{C}[u,v]^G$ for $G = C_m$: type A_n.

$u \mapsto \omega_m u, v \mapsto \omega_m^{-1} v, u^i v^j \mapsto \omega_m^{i-j} uv$

Thus $\mathbb{C}[u,v]^G$ is generated by $u^i y^j, m | i-j$.

Calculate $\mathbb{C}[u,v]^G$ for $G = D_m$: type D_n.

$\phi(u) = \omega_{2m} u; \phi(v) = \omega_{2m}^{-1} v$
$\quad \tau(u) = iv; \tau(v) = iu$

Thus generated by $u^2 v^2, u^{2m} + (-1)^m v^{2m}, uv(u^{2m} - (-1)^m v^{2m})$

Thm. $G < SL(2,\mathbb{C})$**, denote** $\mathbb{C}^2/\mathbb{G} = \mathbb{C}[u,v]^G$**, then** $\exists P_1, P_2, P_3$**, s.t.** $\mathbb{C}^2/G =< P_i >$

The Raynold's operator: $R(P) = \frac{1}{|G|} \sum_{g \in G} g(P)$

$R : \mathbb{C}[u,v] \to \mathbb{C}[u,v]^G$ is a surjective operator, thus only need to calculate $R(u^i v^j)$.

For $A_n, R(u^iv^j)=\frac{1}{m}\sum_{k=1}^{m}\phi_m^k u^iv^j=\delta_{ij} \mod m u^iv^j$

Thus generator $P_1=u^m, P_2=v^m, P_3=uv$. Moreover $P_3^m=P_1P_2$

ForD_n,

$$R(u^iv^j)=\frac{1}{4m}\sum_{k=1}^{2m}\phi_{2m}^k(u^iv^j)+\phi_{2m}^k\tau(u^iv^j)=\frac{1}{4m}\sum_{k=1}^{2m}\omega_{2m}^{k(i-j)}u^iv^j$$

$$+\frac{1}{4m}\sum_{k=1}^{2m}\omega_{2m}^{k(j-i)}u^jv^i\mathbb{i}^{i+j}$$

$$=\begin{cases}0 & 2m\nmid i-j\\ \frac{1}{2}(u^iv^j+\mathbb{i}^{i+j}u^jv^i) & i\equiv j \mod 2m\end{cases}$$

Thus generator $P_1=u^{2m}+(-1)^mv^{2m}; P_2=uv(u^{2m}-(-1)^mv^{2m}); P_3=u^2v^2$

(The 2nd line of the result of $R(u^iv^j)$ can indeed be represented by this 3 generator, through computaion...)

For E_6, the generators are

$$P_1=(u^4+v^4)^3-36u^4v^4(u^4+v^4)$$
$$P_2=(u^4-v^4)^2+16u^4v^4$$
$$P_3=uv(u^4-v^4)$$

For E_7, the generators are

$$P_1=uv(u^8-v^8)[(u^4+v^4)^2-36u^4v^4]$$
$$P_2=(u^4+v^4)^2+12u^4v^4$$
$$P_3=u^2v^2(u^4-v^4)^2$$

For E_8, the generators are

Thm. $G<SL(2,\mathbb{C}), \mathbb{C}^2/G\cong\mathbb{C}[x,y,z]/f(x,y,z)$. x,y,z **corresponds to** P_1,P_2,P_3.

$Type$	f
A_n	$xy - z^{n+1}$ *or* $x^2 + y^2 - z^{n+1}$
D_n	$x^2 + y^2 z + z^{n-1}$
E_6	$x^2 + y^3 + z^4$
E_7	$x^2 + y^3 + yz^3$
E_8	$x^2 + y^3 + z^5$

Proof: Dimension Reasons (?)

Resolution of Singularities

For the polynomial corresponding to A_n, it corresponds to a cone when $n = 1$. i.e. $x^2 + y^2 = z^2$. Observing that $(0, 0, 0)$ is a singular point. We would expect to resolve it.

Now we are going to define rigrously about the resolution of singularities.

$\exists!$ Singularity at $O \iff (f = 0 = \dfrac{\partial f}{\partial x} = \cdots = \dfrac{\partial f}{\partial z}$ *has only one solution* $(0, 0, 0))$.

Definition(Resolution of a singular) The resolution of a singular algebraic variety is a smooth variety together with a regular map(morphism) $\pi : Y \to X$**. Since** X **has only one singular point** $X = X_{sm} \cap X_{sg}$**, we expect** $\pi^{-1}(X_{sm}) \cong X_{sm}$

Here isomorphism is define as usual in general constructions. $\phi \circ \psi = id; \psi \circ \phi = id$

Definition(Blow-up at $O \in \mathbb{C}^n$**) Let** $\mathbb{C}^n \times \mathbb{CP}^{n-1} = \{(x, y)\}$

Define $Bl_O(\mathbb{C}^n) = \mathbb{V}(x_i y_j = x_j y_i) \overset{\pi_1}{\to} \mathbb{C}^n$

i.e. $\pi^{-1}(x_1, \cdots, x_n) = ((x_1, \cdots, x_n), [x_1, \cdots, x_n])$

This blowing up actually add the tangent line information at the origin.

Consider the stropboid as a vivid example.

Definition.(Blow up of a variety) $X \subset \mathbb{C}^n, O \in X_{sg}, Bl_O(X) = \overline{\pi^{-1}(X/\{0\})} = \widetilde{X}$

Note that $\pi^{-1}(O) = (0, \mathbb{CP}^{n-1})$, it's necessary not to add all inverse images into the blow up since it will destroy the smooth property.

Remark. Blow-up is not necessarily a sing. resolution; Find Minimal Resolution?

Example. Take $X = \mathbb{V}(y^2 = x^2(x+1)) \subset \mathbb{C}^2$

Then $\widetilde{X} = Bl_O(X) \subset \mathbb{V}(xv - yu, f)$

Here we want to use $t = v/u, y = xt$ to represent the result.

Kleinian Singularities

$X = \mathbb{C}^2/G := \mathbb{V}(f) \subseteq \mathbb{C}^3$, here f refer to the generating relation. $\mathbb{C}[x,y,z]/(f)$

$Y \subset Bl_O(\mathbb{C}^3) = \{(x,y,z), [a,b,c]\}$

Thm. Let $\widetilde{X} \xrightarrow{\pi} X$ be a minimal resolution of X, then $E = \pi^{-1}(0) = \cup_{i \in \Delta_0} \mathbb{CP}^1_{(i)}$,
$\mathbb{CP}^1_{(i)} \cap \mathbb{CP}^1_{(j)} = \begin{cases} Point & \exists i \sim j \ in \ Dynkin \ Diagram \\ \varnothing & Otherwise \end{cases}$

Example. A_1.

$X = \mathbb{V}(xy - z^2); Y = \mathbb{V}(f, xb = ya, xc = za, yc = zb), E = \pi^{-1}(0) \subset Y$

Consider the coordinate region $U_a : a \neq 0$

Through computation we get $\{(x,y,z)[a,b,c]\} = \{(x, c^2/a^2 x, c/ax), [1 : c^2/a^2 : c/a]\}$

Let $x \to 0$, We get $E \cap U_a = \mathbb{C}_{(c/a)}$; Similarly $E \cap U_b = \mathbb{C}_{(c/b)}$

For U_c region. $E \cap U_c = \{(0,0,0)[a,b,c]\}, ab = c^2$.

Example A_n.

$f = xy - z^{n+1}$.

$E \cap U_a : (x, c^n/a^n \cdot x, c/a \cdot x)[1 : b/a : c/a] \sim \mathbb{C}_{c/a}$

$E \cap U_c : a/c \cdot b/c = z^{n-1}$

Hence we reduce the case to A_{n-2}.

7. Cluster Theory

Frieze

Definition A frieze pattern of height n consists of $(n+2)-$ row positive integer written as a net. s.t. Top row/Bottom row are all 1s.

Phenomenon 1. A lightingbolt (Path from Top to the Bottom) which are made up of 1 determine a frieze pattern uniquely.

(Converse does not holds: Using (2,2,1,3))

Phenomenon 2. All frieze is periodic under glide reflection, whose fundamental domain (the A, as shown below) is a regular triangle, thus with $n(n+3)/2$ non-top/bottom row elements. (A∀A∀A∀A∀)

Call the period of the 1st non trivial row a quddity sequence.

Thm. (Conway-Coxeter) $\forall$ quiddity seqqene of height n are precisely from

Quiver mutation

Recall the famailiar sequence $\{x_n\}$, $x_{n+1} = \dfrac{1+x_n}{x_{n-1}}, x_1 = a, x_2 = b$ has a period 5.

(Quiver) A directed graph without self-loop and 2-cycle(parallel opposite edge) is called a quiver.

Given a initial cluster $C = (Q, x), x = (x_i, i \in Q_0)$. i.e. putting a variable on all vertices of the initial cluster.

Mutation of C at $k \in Q_0$

Step1. $i \to k \to j \; then \; add \; i \to j$

Step2. $i \to k$, then reverse the arrow. Here the change is made in modification, instead of adding.

Step3. Kill all 2-cycle.

Step4. Change the point value $x_i' = x_i (i \neq k), x_k' = x_k^{-1}(\prod_{i->k} x_i + \prod_{j->k} x_j)$

Lemma. $\mu_k^2 = id$

Hence its easy to be shown that for a height-2 frieze, the zigzag line (middle 2 roows) are made exactly by conducting mutation on $x_1 < -x_2$. Hence easy to verify the periodic property.

Set up. Given a initial cluster $C = (Q, x)$, one can get all cluster from iteratedly mutation, (identify them if $\exists$ isomorphism $Q_1 \to Q_2, x_1 \mapsto x_2$)

A cluster variable is the variables(actually rational function resp. the initial variables) that appears in the cluster

FACTS: 1. Any cluster variable is a Laraunt Polynomial. i.e. $x = \frac{Polynomial}{\prod x_i^{d_i}}$; 2. Coefficient of the polynomial $P(x)$ is non-negative.

Def. Cluster Exchange Graph: $vertex -> cluster; Edge -> Mutation$

Thus the CEG of $x_1 -> x_2$ is exactly a pentagon.

Thm. (Fomin-Zelevinsky)

TFAE:

$|CEG(Q)| < +\infty$;

Q is mutation equivalent to a Dynkin graph, i.e. you can turn the graph into a dynkin one by some steps of mutations;

Any Q' mutated from Q has no double arrow.(Parallel Arrow)

Type A_n cluster $\iff$ Frieze(generalized)

At this time, the cluster variables are $n(n+3)/2$

A_2 example has been showned previously, now we compute the A_3 case.

Associahedron, Catalan Numbers, Triangulation of $(n+3)-$gon

Consider ways of adding (), each () only involve two parts. Say vertices to be the ways of adding n ()s on n+2 elements, connect a edge if the ways can be transformed by using associative law for 1 time, we get a graph. Call this graph a associahedron.

(The famous pentagon is the associahedron for $n = 2$, i.e. $abcd$)

This problem has another name: Effective parenthesis.

Binary Tree. A tree with $n+2$ leaves, any vertices has exactly 2 branches unless it reach the leaves.

Any tree corresponds to the way of multiplying the $n+2$ variables.

$$C_m = \frac{1}{m}\binom{2m}{m+1} = \frac{1}{2\pi}\int_0^4 x^m\sqrt{\frac{4-x}{x}}dx$$
$$= \frac{2}{\pi}4^m\int_{-1}^1 t^{2m}\sqrt{1-t^2}dt$$

Thus $\sum_{m=0}^{+\infty} C_m/2^{2m+1} = 1$

Proof: $C(x) = \sum C_m x^m, C(x) = 1 + xC(x)^2, C(x) = \frac{1-\sqrt{1-4x}}{2x}$

Expanding it using generalized bionomial theorem.

$$\frac{2}{\pi}\cdot 4^m \cdot \int_{-1}^1 t^{2m}\sqrt{1-t^2}dt = \frac{4^{m+1}}{\pi}\int_0^{\pi/2}\sin^{2m}\theta\cos^2\theta d\theta$$
$$= \frac{(2m-1)!!}{m!}$$

$$\sum_{m=0}^{+\infty} C_m/2^{2m+1} = \frac{1}{\pi}\int_{-1}^1 \frac{dx}{\sqrt{1-x^2}} = 1$$

Probability Explaination:

Consider a random walk from 0. Each step choose +1/-1 at probability 1/2. View -1 as a trapped state, then $1 = \sum C_m/2^{2m+1} = P(arriving\ at\ 1)$

Since 1-dimensional random walk is always recurrent, then the P should be 1.

$C_{n+1} = \#BT_{n+2}$

See Notes.

For any elements in BT_{n+2}, we view it as a series of $n+1$ pairs of parenthesis and $n+2$ variables $a_1, \cdots, a_{n+2}$, where each parenthesis contains 2 blocks. (For example $(a(bc))$ is a proper series)

We view left parenthesis "(" as "+", variables "a_i" as "-"($i \neq n+2$). Then we get a "+","-" sequence which satisfies #"+" in first k elements are no less than #"-".

Thus we get a map: $BT_{n+2} \to C_{n+1}$

For the inverse direction, given a sequence of "+" and "-", we first write the $a_1, \cdots, a_n$ and left parenthesis by view "+" as "(", "-" as "a_i", and add a_{n+2} at the end. Then we add right parenthesis so that each pair of parenthesis only contain 2 blocks. This can be completed uniquely since we can add right parenthesis from the right of the sequence. The adding method is also unique since each pair must contain 2 blocks.

These two operations are indeed inverse. Thus we get the result.

Definition. A triangulation of $\mathbb{S} = (n+3)-$gon is a collection of diagnols that divide $\mathbb{S}$ into triangles.

Similar to the associahedron, for triangulation we get a exchange graph where vertices are triangulation, edges are flip. We get a Graph $EG(\mathbb{S})$

Theorem. $|EG(\mathbb{S})| = C_{n+1}$

Proof: For the $n+3$-gon, fix an edge, and view the other $n+2$ edges as $n+2$ variables, the diagnols can be viewed as the ways of conducting multiplications. Thus it has a correspondonce with BT_{n+2}. Thus the theorem is trivial.

Taking midpoints of edges and diagnols, we immediately get an binary tree which is exactly the binary tree in the previous correspondonce!

Theorem. $\forall$ Quddity of frieze of height n, it arises from a triangular T, where a_i is the angle of T_i

Lemma. $(m+2)C_{m+1} = 2(2m+1)C_m$

Theorem. Exists a bijection: $\{cluster\ variables\} \leftrightarrow \{diagonols\}$**, such that exchange relation becomes Ptolemy relation.**

Moreover, variable on the diagonol $i \leftrightarrow j$ **has the form** $\mathbb{Z}^+[x_j, y_i]/\prod_{t<k<s} x_k$

Remark. For the meaning of y_i, Since the 1s in the frieze are actually edges of the polyton. Thus one can replace $1s$ with y_is temporarily.

Proof: Given $x_1, \cdots, x_n$ whereas the diagonals have a common point. We claim that $\exists!$ clusters forall diagonals such that Ptolemy relations are satisfied.

It suffices to discribe how quiver corresponds to the diagonals. However this is obvious since mutate at a point (or to say at a diagonal) is equivlant to conduct a fliping operation. The variable changes are exactly satisfying the Ptolemy relation. (Through a local check)

Thus all clusters mutated from A_n are exactly triangulation of the polygon.

Thus the rest is to say given a set of edge variable and the initial variables. This is an elementary result however. One can easily deduced it by induction.

Corollary. This bijection induces $EG(S) \cong CEG(S)$.

Corollary. $\forall$ general freize comes from cluster algebra of type A_n (in the sense that

01		12		23		34		45		56
	02		13		24		35		46	
		03		14		25		36		
			04		15		26			
				05		16				
					06					

, here ij denotes the diagonal numebr of $i \longleftrightarrow j$)

Corollary.(Conway-Coexter) $\exists$ bijection between $EG(S)$ and the integral frieze of height n.

Proof: Given a $T \in EG(S)$

$V_{st} = \#matchings\ of\ \{(V_k \in \triangle^k,\ for\ each\ s < k < t\}, such\ that\ \triangle^k \in T$

Lemma. $V_{st} = V_{ts}$. Checking that the complement mathcing satisfies the desired case.

Lemma. V_{st} satisfies the Ptolemy relation.

Lemma. $\forall$ quddity of an integral frieze, $\exists 1$.

Take the largest V_{st}, consider the edges $V_{s(t+1)}, V_{s(t-1)}$, then
$V_{(t+1)(t-1)} = (V_{s(t+1)} + V_{s(t-1)})/V_{st} \leq 2$. If the value equals 2. Then
$V_{s(t+1)} = V_{s(t-1)} = V_s t$, suppose no 1 exists, then all $V_{sx} = V_{st}$, contradiction.

Lemma.(Buliding) If $\exists 1$ on the quddity, i.e. $a_i = 1$, then exists a quddity by deleting a_i, then exists a quddity $a_1, \cdots, a_{i-1} - 1, a_{i+1} - 1, \cdots, a_n$. (The idea is deleting a corner of the polygon S)

Lemma.(Gluing) We can insert a 1 in the quddity, the idea is adding the corner on the polygon.

Lemma. If quiddity is $F(T)$ for some T, then the building is $F(\tilde{T})$

By lemmas above, the V_{st} we constructed indeed induces a frieze.

Now we prove the previous theorem. First we recall the description of Fomin-Zelevinsky theorem.

Thm. (Fomin-Zelevinsky)

TFAE:

$|CEG(Q)| < +\infty$;

Q is mutation equivalent to a Dynkin graph, i.e. you can turn the graph into a dynkin one by some steps of mutations;

Any Q' mutated from Q has no double arrow.(Parallel Arrow)

Proof: If a parallel arrow exists, through elementary check one can get it's impoosible to get the $\mu_1 \rightrightarrows \mu_2$ back again.

If a graph is not Dynkin, there must exists a Euclidean graph as subgraph. Through direct check one can get $\tilde{A}_n, \tilde{D}_n, \tilde{E}_n$ will induce a double arrow.

(One should also check D_n, E_n leads to a finite $CEG(Q)$.)

8. Lines in surfaces

A plane section of a conic is called a quadratic curve. It has a genereal form $Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0$, or $x^T Q x = 0$.

Quadratic Surfaces

For quadratic surfaces in $\mathbb{C}P^3$, it is always projectivly equivalent to $xy = zw$

It is doubly ruled: $\{x = \lambda z; y = \lambda^{-1} w\}$ or $\{x = \lambda w; y = \lambda^{-1} z\}$

For the converse, say $x = az + bw, y = cz + dw$, (x, y, z, w) lie on the quadratic surface if and only if $ac = bd = 0$, hence the result.

Cubic Surface

Fermat Cubic $x^3 + y^3 + z^3 + w^3 = 0$

For the lines, wlog $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} z \\ w \end{pmatrix}$

By solving this we get $x + \omega^j z = 0; y + \omega^k w = 0$, or cyclic the x, y, z, w.

By computing we get each line intersect with 10 lines, have no intersection with 16 lines.

We define $Conf(L)$: such that vertices are the lines, link a edge if they intersect.

Lem. $Sym(Conf(L)) = W(E_6)$**, where** W **is the Weyl Group.**

$W(Q) =< a_1, \cdots, a_n | a_i^2 = 1, a_i a_j a_i^{-1} a_j^{-1} = e(i \nleftrightarrow j); a_i a_j a_i = a_j a_i a_j (i \leftrightarrow j) >$

Clebsch Surface

A surface in $\mathbb{C}P^4, \sum x_i^3 = 0 \cap \sum x_i = 0$

Consider plane in the 3-manifold $\sum x_i^3$, and intersect it with the plane $\sum x_i = 0$

L be the planes in the 3-manifold, ζ be the 5th-unit root. in which 15 $\tilde{l} : x_i = x_j; x_k = x_l$, 12 $\tilde{l} : \sum x_{n_i} \zeta^i = 0, \sum x_{n_i} \zeta^{-i} = 0$.

Let $\mathfrak{m}$ be all smooth cubic in $\mathbb{C}P^{19}$

Then $\tilde{\mathfrak{m}} = \{(l, x) | a\ line\ in\ x \in \mathfrak{m}\}$ is a 2-cover of $\mathfrak{m}$.

Lemma. $\forall$ **Cubic Surface** $\cong$ **blow-up of** $\mathbb{C}P^2$ **at 6 points.**

$27 = 15(line\ passes\ through\ 6\ pt) + 6(blow\ up\ of\ 6\ pt) + 6(blow\ up\ of\ 6\ conics)$