Local-to-Global Principle in Symmetric Groups

by

Yitong Lu

David Zureick-Brown

Adviser

Department of Mathematics

David Zureick-Brown

Adviser

Shanshuang Yang

Committee Member

Eric Reinders

Committee Member

2019

Local-to-Global Principle in Symmetric Groups

by

Yitong Lu

David Zureick-Brown

Adviser

An abstract of

a thesis submitted to the Faculty of Emory College of Arts and Sciences

of Emory University in partial fulfillment

of the requirements of the degree of

Bachelor of Sciences with Honors

Department of Mathematics

2019

Abstract

Let G be a Symmetric Group S_n, B be S_{n-1} and H be a transitive subgroup of G. If for $\forall h \in H$, there exist $g \in G$ and $b \in B$ s.t. $ghg^{-1} = b$, then we can find a specific $g \in G$ s.t. $gHg^{-1} \subseteq B$

Local-to-Global Principle in Symmetric Groups

by

Yitong Lu

David Zureick-Brown

Adviser

A thesis submitted to the Faculty of Emory College of Arts and Sciences

of Emory University in partial fulfillment

of the requirements of the degree of

Bachelor of Sciences with Honors

Department of Mathematics

2019

Acknowledgment:

I would like to graciously thank my advisor, David Zureick-Brown, who guided me throughout my honor research. He gave me multitude of helpful suggestions of how should I approach this problem and immediately provided me counterexamples whenever I made a wrong conjecture. Without his support, this paper will never be completed.

Contents

1 Introduction

When I was studying Galois representation of elliptic curves, I encountered a very interesting Theorem. Consider the Galois group from $\mathbb{Q}$ to $\mathbb{Q}$ joint with n-torsion points on elliptic curve, then

$$Gal(\mathbb{Q}(E[n])/\mathbb{Q}) \subseteq GL_2(n)$$

Lets Denote $H(n) := Gal(\mathbb{Q}(E[n])/\mathbb{Q})$, B to be the matrix group $\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$

If for any $h \in H(n)$, $\exists g \in GL_2(n)$ $\exists b \in B$ $s.t. ghg^{-1} = b$, then there exists some $g \in GL_2(n)$ s.t. $gHg^{-1} \subseteq B$

I was wondering, forgetting about elliptic curves, does such group theoretical relation in general holds: Let H,B be two subgroups of G. Suppose every element of H is g-conjugate to an element of B, then is H itself g-conjugate to a subgroup of B?

In this paper, I will mainly focus on symmetric groups, i.e. the cases where G=S_n. I chose such concentration for the following two reasons:

Firstly, conjugation is easy to manipulate in symmetric groups, as I will show in next section. Secondly, I believe understanding this question over symmetric groups will contribute to the research in arithmetic dynamical systems.

2 Local-to-global relation in S_n

Here is our main question: Let G be a Symmetric Group S_n. Let H,B be two subgroups of G. Suppose every element of H is g-conjugate to an element of B, then is H itself g-conjugate to a subgroup of B?

To make the language easier, lets say it is **locally true** if and only if for every element $h \in H$, there exists some $g \in G$ and $b \in B$ s.t. $ghg^{-1} = b$. It is **globally true** if and only if there exist some $g \in G$ s.t. $gHg^{-1} \leq B$

Thus, our question can be rephrased as the following

Do locally true automatically implies globally true?

Even by intuition, it is easy to realize this local-to-global relation will in general fail. When it is locally true, different elements of H might conjugate to different elements of B through different elements of G. For example, it is possible that $g_1h_1g_1^{-1} = b_1$ and $g_2h_2g_2^{-1} = b_2$. But to let the global condition be true, we need to find a specific $g \in G$ s.t. $gHg^{-1} \leq B$. In other words, let $G_h = \{g \in G \mid \exists b \in B \; s.t. \; ghg^{-1} = b\}$. H and B are globally true only if $\bigcup_{h \in H} G_h \neq \emptyset$. Thus, the global is a much stronger condition than the local. In fact, the converse of our question is obviously always true. If $gHg^{-1} \leq B$, then $\forall h \in H, ghg^{-1} = b$ for some $b \in B$.

However, even the local-to-global relation fails in most cases, under some special condition it can be true.

Case 1: if G is abelian, then H is just a subgroup of B.

Case 2: if H=$<a>$, a subgroup generated by one element, if $gag^{-1} = b$ for some $b \in B$, then $gHg^{-1} = B$

Lemma 2.1 *If H=$<(a_1\,a_2), (a_3\,a_4), ..., (a_{2n-1}\,a_{2n})>$, a subgroup generated by n disjoint two cycles, and B=$<(b_1\,b_2), (b_3\,b_4), ..., (b_{2n-1}\,b_{2n})>$is also a subgroup generated by n disjoint two cycles. If $a_1, a_2, ..., a_{2n}, b_1, b_2, ..., b_{2n}$ are all distinct with each other, then locally true automatically implies globally true.*

Proof: Suppose exist $g_1, g_2, ..., g_n, f_1, f_2, ..., f_n$ from G such that

$g_1(a_1\,a_2)g_1^{-1} = (b_1\,b_2), g_2(a_3\,a_4)g_2^{-1} = (b_3\,b_4), ..., g_n(a_{2n-1}\,a_{2n})g_n^{-1} = (b_{2n}\,b_{2n-1})$. Because $a_1, a_2, ..., a_{2n}, b_1, b_2, ..., b_{2n}$ are all distinct with each other,

$g_1, g_2, ..., g_n, f_1, f_2, ..., f_n$ are disjoint with all the generators of H except the cycles they are directly conjugating. Thus, $g_1g_2...g_nHg_1^{-1}g_2^{-1}...g_n^{-1} = B$

On the other hands, it is easy to find finitely many counterexamples where such local-to-global principle fails.

For example, let G=S_{100}, H=S_3, B=$<(1\,2), (3\,4\,5)>$. Although every element of H is g-conjugate to an element of B, B is abelian and H is not abelian. Thus, it is always globally false.

Lemma 2.2 *For $\sigma, \tau \in S_n$, σ and τ are conjugated to each other, if and only if they have the same cycle type.*

Proof: suppose we have $\rho \in G$ s.t. $\rho = \sigma\tau\sigma^{-1}$. let $\rho(i) = (j)$. Then

$\rho(\tau(i)) = \sigma\tau\sigma^{-1}\tau(i) = \tau\sigma(i) = \tau(j)$. This means when we conjugate an element by τ, we just replace each entry a with $\tau(a)$. Thus, the cycle type remains the same after conjugation.

Conversely, suppose ρ and σ have the same cycle type. WLOG, suppose ρ and σ are both 4+2 cycles. Let $\sigma = (1\,2\,3\,4)(5\,6)$ and $\rho = (a\,b\,c\,d)(e\,f)$. Then if we let $\tau = (1\,a)(2\,b)(3\,c)(4\,d)(5\,e)(6\,f)$, then $\rho = \tau\sigma\tau^{-1}$.

Corollary 2.2.1 *Local is true if and only if B contains all the cycle types that H contains.*

This corollary is a direct result of Lemma 2.2 and gives us a useful way to check whether two subgroups are locally true or not – by just checking their cycle types.

Corollary 2.2.2 *If $G = S_n, B = A_n$, then locally true automatically implies globally true.*

Proof: A_n is by definition the group which contains all the even permutations of S_n. If H and B are locally true, then by Corollary 2.2.1, H can only contains even permutations. Thus, H is just a subgroup of B.

3 Cases when B = S_{n-1}

Let G be a Symmetric Group S_n, B be S_{n-1} and H be a subgroup of G. Suppose every element of H is g-conjugate to an element of B, then is H itself g-conjugate to a subgroup of B?

As we have showed in the previous section, the global is a much stronger condition than the local. However, if we make B just a little bit smaller than G, will local-to-global principle hold? For example, if we let $B = S_{n-1}$, and $G = S_n$, will locally true implies globally true?

Unfortunately, I soon found a plenty of counterexamples:

Let H=$\{(1\,2)(3\,4), (1\,2)(5\,6), (3\,4)(5\,6)\}$, $B = S_5$ and $G = S_6$. H and B are locally true because the only cycle type of H is 2+2 and S_5 obviously contains such cycle type. It is globally false, however, because in S_5, the point 6 is fixed, whereas in H we cannot find any fixed point. Notice that H is not a transitive subgroup of B. We have three orbits for $H \subseteq G$: $\{1,2\}$,$\{3,4\}$ and $\{5,6\}$. I believe that it is the intransitivity of H that makes the local-to-global principle fails here. By using the Cauchy's Theorem, we can prove the cases where n is a prime.

Lemma 3.1 *Let p to be a prime integer. Let G be a Symmetric Group S_p, B be S_{p-1} and H be a transitive subgroup of G. Then Local-to-Global Principle holds to be true.*

Proof: First notice that B is not a transitive subgroup of G. Any subgroup of B will not be transitive also. As H is transitive, the global will always fail. If we can show that the local also always fails, we can contrapositively prove that the local-to-global principle holds. H is transitive for the set $X = \{1, 2, 3, \ldots, p\}$. By Orbit-Stabilizer Theorem, $|Orbit\ x| = \dfrac{\mid H \mid}{\mid H_x \mid} = p$, where H_x is the stabilzer of x. ($H_x = \{h \in H \mid hx = x\}$) By Lagrange's Theorem, $p| \mid H \mid$. By Cauchy's Theorem, because p is a prime, H has an element of order p. As the only type of element in G with order p is p-cycle, H has a p-cycle. As we know that B cannot contain a p-cycle, the local fails.

Actually, local-to-global principle holds even when p is not a prime. But before we prove that, lets talk about alternating group A_n first.

Lemma 3.2 *Any A_n is transitive through $X = \{1, 2, 3, \ldots, n\}$*

Proof: $\forall i, j \in X$, we can have $(k\,i)(k\,j) = (j\,i\,k)$

Lemma 3.3 *For any $n \in \mathbb{Z}$, A_n contains at least one element that fix no point through $X = \{1, 2, 3, \ldots, n\}$*

Proof: if n is 0 mod 4, then we can have $(1\,2)(1\,2)\ldots((n-1)\,n) \in A_n$, and no point is fixed under this cycle.

if n is 1 or 3 mod 4, then we can have $(1\,2)(1\,3)\ldots(1\,n) = (n\,(n-1)\,\ldots\,2\,1)$, and no point is fixed under this cycle.

if n is 2 mod 4, we can have $(1\,2)\ldots((n/2-1)\,n/2)\ldots((n-1)\,n)$. In this way, we get 2 cycles with odd length, and we repeat the process when n is 1 or 3 mod 4.

Even this two lemma for alternating groups are proved by simple computations, they sort of told me that there should have some intrinsic relations between a subgroup's transitivity and the fact that such group always contains a fixed point free element. Why do we care whether a subgroup has a fixed point free element or not? It is because of the following lemma.

Lemma 3.4 *Local is false if and only if H contains a cycle that fixes no point among* $\{1, 2, 3, \ldots, n\}$.

Proof: This is simply a result from the fact that $B = S_{n-1}$ contains a fixed point.

Here comes my main theorem.

Theorem 3.5 *Let G be a Symmetric Group* S_n*, B be* S_{n-1} *and H be a transitive subgroup of G. Then Local-to-Global Principle holds to be true.*

Proof: Considering transitive group H, and set $X = \{1, 2, 3, \ldots, n\}$, by Burnside's lemma, the number of orbits in H is equal to the average number of points fixed by an element of H.

$$1 = \mid X/H \mid = \frac{\sum\limits_{h \in H} \mid X^h \mid}{\mid H \mid}$$

X^h denotes the set of element in X that are fixed by h. The left hand side of this equation is 1, because H in transitive in G. Since the identity $e \in h$ fixes every element of X, $\mid X^e \mid > 1$. Then, at least one of the term in the summation $\sum\limits_{h \in H} \mid X^h \mid$ must be 0. That means there exists at least one element $h \in H$ s.t. h fixes no point. However, any element from B has to fix at least one point. Thus, the local principle fails.

I also get a way to prove this Theorem without using Burnside's lemma. I personally like this prove because it talks about the relation between conjugation and stabilizers in symmetric groups. To start the prove, we need a small lemma first.

Lemma 3.6 *Let G be a finite group, H be any proper subgroup of G. Then the union of all the conjugation of H never equals G.*

Proof: let $\mid H \mid = k$, $\mid G : H \mid = h$. Then $\mid G \mid = nk$. As $(gH)(gH)^{-1} = gHg^{-1}$, the map from cosets to conjugates: $gH \rightarrow ghg^{-1}$ is well-defined and surjective. Thus, we have at most $\mid G : H \mid$ distinct conjugates. Notice that e is contained in every conjugate. Thus, the size of union is at most $1 + n(k-1) < n$ as long as $n > 1$

Second proof for Theorem 3.5:consider the set $X = \{1, 2, 3, \ldots, n\}$ and $\sigma \in H$. Suppose every element of H has a fixed point, then for $\forall h \in H$, we have $h(a) = a$ for some $a \in X$, i.e. $h \in H_a$. H is transitive, so for any $b \in x = \{1, 2, 3, \ldots, n\}$, we have $g \in H$ s.t. gb=a. Then

$$h(gb) = ha = a$$

$$(g^{-1}hg)b = g^{-1}a = b$$

Then, $g^{-1}hg \in H_b \Rightarrow g^{-1}H_a g = H_b$. Then $\bigcup_{g \in H} g^{-1}H_a g \supseteq H$. By Lemma 3.6, this is not possible, so we proved the theorem by contradiction.

Corollary 3.6.1 *Any transitive subgroup contains an element which fixes no point.*