from scratch series...........

Orbit-Stabilizer Theorem

If G is a finite group of permutations of the elements of a finite set S, then the order of G equals the order of the stabilizer of any element of S times the cardinality of the orbit of that element.

BACKGROUND:

This theorem expresses the intuitively reasonable fact that there is an inverse relationship between permutations that fix elements and the orbits of those elements. If many permutations in the group *G* fix a given element of *S*, then the other elements of *S* that can be reached by applying permutations in *G* to that fixed element are few. There aren't many places to visit if most trips never leave home. And vice versa. If most of the permutations in *G* do not fix the given element, but bump it around to something else, then orbits can be big while the set of permutations for which the given element is an invariant are few. Remarkably, the relationship is quantitatively exact.

The Orbit-Stabilizer Theorem is sometimes proved in passing as a lemma to support the proof of Burnside's Lemma, discovered in 1911. Burnside's Lemma is a powerful counting principle that is especially useful in situations where an enumeration is to be made in the presence of some kind of symmetry. See the separate article on Burnside's Lemma to see how this works.

Although Gallian doesn't say so, the more general setting for the Orbit-Stabilizer Theorem is the notion of a *group action*. If *G* is a group and *S* is a set, then a mapping $\gamma : G \times S \to S$ is called a *group action* if it satisfies two obviously desirable properties for all $s \in S$: (i) if e_G is the identity of *G*, then $e_G(s) = s$, and (ii) if $g, h \in G$, then $(gh)(s) = g(h(s))$. Other bells and whistles are possible, and there is a whole theory of these things. The most natural example of a group action is a set of objects shuffled by a group of permutations. Note that the two consistency properties for an action can be easily verified, and this is where our author picks up the thread. Here is an example of an action that is also fairly natural, but quite different than one based on permutations: suppose a physicist wants to keep track of *n* particles bouncing around inside a box. Each particle has three position and three momentum coordinates at any time *t*, so for *n* particles, the "configuration space" has 6*n* dimensions, and the state of the *n*-particle system at time *t* is represented by a 6*n*-tuple. Let the configuration space be the set *S* and the group of real numbers under addition be the group *G*. Then the group action is the mapping that takes the current state of the system and replaces it with some future state if $t > 0$ or some previous state if $t < 0$.

NOTATION:

(1) Algebraists like to use capital letters to stand for wild cards when they write various expressions. For example, if *A* and *B* are sets and it makes sense to operate from the left any element of *A* on any element of *B*, they will write *AB* to indicate the set $\{ab : a \in A, b \in B\}$. Typically, *A* and *B* are both subgroups of some given group. Also, computer scientists write things like *AB* to mean any word in the language *A* followed by (concatenated with) any word from the language *B*, so the usage transcends algebra proper. The idea is to simply let the set symbol stand for any of its elements whenever the context is appropriate.

(2) Even if a set is not a group, we will extend the "absolute value bars" notation for order of a group to mean simply the cardinality of a set. So |*S*| counts the elements of *S*, no matter what structure, if any, *S* has.

KEY DEFINITIONS:

1) A *permutation* is a bijective mapping from a set S to itself.

2) A *group homomorphism* is an operation preserving mapping between two groups, specifically if G and H are groups and $\phi : G \to H$, then ϕ is a homomorphism iff for all $x, y \in G$ it is true that $\phi(xy) = \phi(x)\phi(y)$. Another way to state the operation preserving property is to say that the group operations and the mapping commute.

3) A group *isomorphism* is a bijective group homomorphism. Group isomorphisms give all of the algebraic properties of the group on one side of the mapping to the group on the other side. Be careful to realize that properties like order and boundedness are not algebraic and do not need to be preserved by isomorphisms.

4) If G is a group, $g \in G$ an arbitrary element, and $H \leq G$ an arbitrary subgroup, the set $\{gh : h \in H\}$, abbreviated gH, is called the *left coset* (of H by g). The *right coset* Hg is defined analogously. The element g is called the *coset representative* of either gH.or Hg. Note the left or right designation agrees with the side on which the coset representative is applied.

5) If G is a finite group and $H \leq G$, the *index* of H in G is the number of distinct cosets of H in G. This index is written $[G : H]$.

6) If G is a group of permutations acting on the set S, then for a given $s \in S$, the *stabilizer* of s with respect to G is the subgroup (to be shown) of permutations that leave s fixed. We write this as $stab_G(s)$.

7) If G is a group of permutations acting on the set S, then for a given $s \in S$, the *orbit* of s with respect to G is the subset of elements of S that can be expressed as $\pi(s)$ for some $\pi \in G$. We write this as $orb_G(s)$.

KEY FACTS:

1) One-step subgroup test

2) Lagrange's Theorem

3) If $H \leq G$ and $x, y \in G$, then $x \in yH$ implies $xH = yH$

4) If $H \leq G$ and $x \in G$, then $xH = H$ implies $x \in H$

PROOF STRATEGY:

We fix an $s \in S$ and show that $stab_G(s) \leq G$. Then we compare the desired statement that $|G| = |stab_G(s)| \cdot |orb_G(s)|$ with the Lagrange formula $|G| = |stab_G(s)| \cdot [G : stab_G(s)]$ and realize that if we show $[G : stab_G(s)] \; = |orb_G(s)|$ we are done. To this end, we construct a bijection between $orb_G(s)$ and the family of left cosets of $stab_G(s)$ in G, whose population is measured exactly by $[G : stab_G(s)]$. The bijection establishes equal cardinality and we conclude the theorem is valid.

PROOF:

Fix $s \in S$. Define $stab_G(s) = \{\pi \in G : \pi(s) = s\}$. I claim this is not only a subset, but a subgroup of G. Given π_1 and π_2 in $stab_G(s)$, the claim is true if $\pi_1\pi_2^{-1} \in stab_G(s)$, by the one-step subgroup test. Certainly $\pi_2 \in stab_G(s)$ implies $\pi_2^{-1} \in stab_G(s)$, since permutations are invertible and unless $\pi_2^{-1}(s) = s$, the composition $\pi_2\pi_2^{-1}$ would not be the identity, as it must be. Now the composition $\pi_1\pi_2^{-1}$ must fix s, since each factor does. We conclude $stab_G(s) \leq G$.

Lagrange's Theorem then gives us $|G| = |stab_G(s)| \cdot [G : stab_G(s)]$. We seek a bijection between $orb_G(s)$ and the family of cosets of $stab_G(s)$ in G. What would a good guess be for this bijection?

Well, a member of $orb_G(s)$ looks like $\pi(s)$ for some $\pi \in G$. Maybe we should send that element to the coset of $stab_G(s)$ having that π as a coset representative. More specifically, let us try the mapping $\phi : orb_G(s) \rightarrow \{\pi stab_G(s) : \pi \in G\}$ given by $\phi(\pi(s)) = \pi stab_G(s)$. There are three tasks ahead of us: (i) verify ϕ is a valid mapping, or is well-defined, (ii) show ϕ is injective, and (iii) show ϕ is surjective.

Suppose we have two elements of $orb_G(s)$, say, $\pi_1(s)$ and $\pi_2(s)$. If $\pi_1(s) = \pi_2(s)$ we must also have their images under ϕ equal for ϕ to be well-defined. Since $\pi_1(s) = \pi_2(s)$, it must be true that $\pi_1^{-1}\pi_2(s) = s$, so apparently $\pi_1^{-1}\pi_2 \in stab_G(s)$. Postcomposing ("multiplying on the left") both sides with π_1 gives us $\pi_2 \in \pi_1 stab_G(s)$, and it follows that $\pi_2 stab_G(s) = \pi_1 stab_G(s)$ by Key Fact #3.

The string of logic in the preceding paragraph may be reversed to show that if $\pi_2 stab_G(s) = \pi_1 stab_G(s)$, then $\pi_1(s) = \pi_2(s)$. Specifically, $\pi_2 stab_G(s) = \pi_1 stab_G(s)$ implies $\pi_1^{-1}\pi_2 stab_G(s) = stab_G(s)$, from which it follows by Key Fact #4 that $\pi_1^{-1}\pi_2 \in stab_G(s)$, and hence $\pi_1^{-1}\pi_2(s) = s$. Obviously, this forces $\pi_1(s) = \pi_2(s)$.

Finally, we note the surjectivity of the mapping ϕ by observing that every coset $\pi stab_G(s)$ has a preimage under ϕ, namely $\pi(s)$. We have completed our tasks and conclude that ϕ is a bijection and therefore $[G : stab_G(s)] = |orb_G(s)|$, which establishes the lemma.