Lecture 5.4: Fixed points and Cauchy's theorem

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 4120, Modern Algebra

Fixed points of group actions

Recall the subtle difference between fixed points and stabilizers:

- The fixed points of an action $\phi \colon G \to \mathrm{Perm}(S)$ are the elements of S fixed by every $g \in G$.
- The stabilizer of an element $s \in S$ is the set of elements of G that fix s.

Lemma

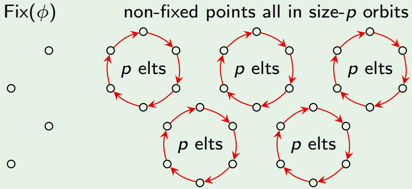
If a group G of prime order p acts on a set S via $\phi \colon G \to \mathrm{Perm}(S)$, then

$$|\,\mathrm{Fix}(\phi)| \equiv |S| \pmod{p}.$$

Proof (sketch)

By the Orbit-Stabilizer theorem, all orbits have size 1 or p.

I'll let you fill in the details.



Cauchy's Theorem

Cauchy's theorem

If p is a prime number dividing $|G|$, then G has an element g of order p.

Proof

Let P be the set of ordered p-tuples of elements from G whose product is e, i.e.,

$$(x_1, x_2, \dots, x_p) \in P \quad \text{iff} \quad x_1 x_2 \cdots x_p = e\,.$$

Observe that $|P| = |G|^{p-1}$. (We can choose $x_1, \dots, x_{p-1}$ freely; then x_p is forced.)

The group $\mathbb{Z}_p$ acts on P by cyclic shift:

$$\phi\colon \mathbb{Z}_p \longrightarrow \mathrm{Perm}(P), \qquad (x_1, x_2, \dots, x_p) \stackrel{\phi(1)}{\longmapsto} (x_2, x_3 \dots, x_p, x_1)\,.$$

(This is because if $x_1 x_2 \cdots x_p = e$, then $x_2 x_3 \cdots x_p x_1 = e$ as well.)

The elements of P are partitioned into orbits. By the orbit-stabilizer theorem, $|\operatorname{Orb}(s)| = [\mathbb{Z}_p : \operatorname{Stab}(s)]$, which divides $|\mathbb{Z}_p| = p$. Thus, $|\operatorname{Orb}(s)| = 1$ or p.

Observe that the only way that an orbit of $(x_1, x_2, \dots, x_p)$ could have size 1 is if $x_1 = x_2 = \cdots = x_p$.

Cauchy's Theorem

Proof (cont.)

Clearly, $(e, e, \dots, e) \in P$, and the orbit containing it has size 1.

Excluding $(e, \dots, e)$, there are $|G|^{p-1} - 1$ other elements in P, and these are partitioned into orbits of size 1 or p.

Since $p \nmid |G|^{p-1} - 1$, there must be some other orbit of size 1.

Thus, there is some $(x, x, \dots, x) \in P$, with $x \neq e$ such that $x^p = e$. $\square$

Corollary

If p is a prime number dividing $|G|$, then G has a subgroup of order p.

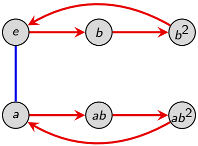
Note that just by using the theory of group actions, and the orbit-stabilzer theorem, we have already proven:

- Cayley's theorem: Every group G is isomorphic to a group of permutations.
- The size of a conjugacy class divides the size of G.
- Cauchy's theorem: If p divides $|G|$, then G has an element of order p.

Classification of groups of order 6

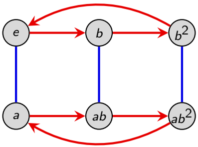
By Cauchy's theorem, every group of order 6 must have an element a of order 2, and an element b of order 3.

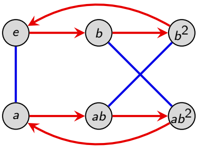
Clearly, $G = \langle a, b \rangle$ for two such elements. Thus, G must have a Cayley diagram that looks like the following:



It is now easy to see that up to isomorphism, there are only 2 groups of order 6:

$C_6 \cong C_2 \times C_3$





D_3