Math 350, Sections 01,03, Fall 2021

Optional Handout: Cauchy's Theorem

The point of this handout is to use the class equation (Theorem 10.9 in Saracino) to prove the following result:

Cauchy's Theorem: Let G be a finite group; write $n = |G|$. Let $p \geq 2$ be a prime number. If $p \mid n$, then G contains an element of order p.

Some notes:

1. The conclusion "G contains an element of order p" is the same as "G contains a subgroup of order p". (Given the element $a \in G$, the subgroup is $\langle a \rangle$. Conversely, by Theorem 10.5, any subgroup $H \subseteq G$ of order p must contain an element of order p.)

2. Section 15 of Saracino covers the Sylow Theorems, which say something **far** more general than Cauchy says: for starters, if p^r divides n, then G contains a subgroup of order p^r. (The Sylow Theorems go on to say, when the exponent r is as big as possible, that all such subgroups are conjugate to one another. They also put some restrictions on how many such subgroups there are.) But Cauchy's Theorem is definitely easier to prove. In addition, the usual proofs of the Sylow Theorems use Cauchy's Theorem.

To prove Cauchy's Theorem, we'll have to assume the following partial result:

Lemma. Cauchy's Theorem is true for finite **abelian** groups.

This Lemma is Theorem 11.7 in the book. Granted, we haven't gotten to that result yet, but we will soon enough; it requires the use of quotient groups in Section 11. So for the rest of this handout, you'll just have to take my word for it that the Lemma is true.

Proof of Cauchy. We'll do "strong" induction on n. That is, the statement for n is: "For any integer m with $1 \leq m \leq n$, if G is a group of order m and if $p|m$, then G has an element of order p."

For $n = 1$, the only m between 1 and n is 1 itself, and $p \nmid 1$. Therefore, the statement is vacuously true (i.e., there are no counterexamples because the hypothesis that $p|m$ is never satisfied).

Now given $n \geq 2$, assume that the statement is true for $n - 1$, and we'll prove it for n.

Given $1 \leq m \leq n$, note first that if $1 \leq m \leq n - 1$, the conclusion is true by the inductive hypothesis (that the statement is true for $n - 1$). Thus, we only need to consider the case $m = n$.

So, we may assume we are given a group G with $|G| = n$ and with $p|n$.

[We need to prove that G has an element of order p. Remember, we are allowed to assume the inductive hypothesis: that any group of strictly smaller order divisible by p has such an element.]

Let $a_1, \ldots, a_k \in G$ be representatives of all the distinct conjugacy classes of G **that have more than one element**.

For each such a_i, consider the centralizer subgroup $Z(a_i) \subseteq G$. We claim that $Z(a_i) \neq G$.

To see this, note that if $Z(a_i) = G$, then $a_i \in Z(G)$. (That is, a_i commutes with all elements of G). Thus, the conjugacy class of a_i consists only of a_i itself. However, we assumed a_i was in a conjugacy class with at least two elements. We have a contradiction, thus proving the claim.

Hence, $1 \leq |Z(a_i)| \leq n-1$ for all $i = 1, \ldots, k$. We consider two cases.

Case 1. Suppose that $|Z(a_i)|$ is divisible by p for some i. Then $Z(a_i)$ is a group of order both strictly smaller than n and divisible by p; by the inductive hypothesis, there must be an element $b \in Z(a_i)$ of order p. Since $Z(a_i) \subseteq G$, the same element $b \in G$ is our desired element of G of order p, and we are done.

Case 2. The only remaining case is that $|Z(a_i)|$ is not divisible by p, for all $i = 1, \ldots, k$. Thus, the index $[G : Z(a_i)] = n/|Z(a_i)|$ (where the equality is by Lagrange's Theorem) **is** divisible by p for all such i. By the class equation,

$$|Z(G)| = n - ([G : Z(a_1)] + \cdots + [G : Z(a_k)]) .$$

Since all the integers on the right are divisible by p, we must have $|Z(G)|$ divisible by p.

[It's tempting here to invoke the inductive hypothesis and say that $Z(G)$ is a subgroup and therefore has an element of order p; so G has the same element. However, that only works if $|Z(G)| \leq n-1$. In particular, it **doesn't** work in the oft-forgotten "stupid case" that $Z(G) = G$ is **not** a **proper** subgroup, i.e., that $|Z(G)| = n$. FYI: $Z(G) = G$ is the same as saying that G is abelian.]

Thus, $Z(G)$ is an **abelian** subgroup of G with order divisible by p. By the Lemma (i.e., by Theorem 11.7 in Saracino), then, $Z(G)$ contains an element of order p. The same element is of course also in G, and we are done. $\square$