II.H. Cauchy's Theorem

By Lagrange, the order of an element $g \in G$ divides $|G|$. The converse statement, that *for any positive integer n dividing G there exists $g \in G$ of order n*, is in general *false*. (Even for abelian groups: $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ contains no element of order 4.) But there is a pretty application of the theory of group actions we have developed to the case where n is prime. We'll give two proofs; for the first you'll have to accept something that we will prove later.

We begin with some preliminaries: recall the

II.H.1. DEFINITION. The **center** of a group is

$$C(G) := \{x \in G \mid gxg^{-1} = x \ \forall g \in G\},$$

the elements commuting with all the other elements of G.

Obviously we have:

(i) G is abelian $\iff G = C(G)$;
(ii) $C(G)$ is itself always abelian; and
(iii) $|\mathrm{ccl}_G(x)| = 1 \iff x \in C(G)$.

Recall also that if we take one representative x_i in each conjugacy class of G ($|G| < \infty$), then $G = \amalg_i \mathrm{ccl}_G(x_i)$ and so

$$|G| = \textstyle\sum_i |\mathrm{ccl}_G(x_i)|. \qquad \text{(II.H.2)}$$

Each element in $C(G)$ has its own conjugacy class, and the right-hand side of (II.H.2) becomes $|C(G)| + \sum_i |\mathrm{ccl}_G(x_i)|$, where the sum is *now* over representatives x_i of conjugacy classes with more than one element. Finally, by the Orbit-Stabilizer Theorem

$$|\mathrm{ccl}_G(x_i)| = \frac{|G|}{|C_G(x_i)|} = [G{:}C_G(x_i)],$$

and we get the

II.H.3. CLASS EQUATION. $|G| = |C(G)| + \sum_i [G{:}C_G(x_i)]$.

This will be used to prove

II.H.4. CAUCHY'S THEOREM. *If* $|G| < \infty$ *and* $p \in \mathbb{N}$ *is a prime dividing* $|G|$, *then* G *contains an element of order* p.

PROOF (A). by induction on $m \geq 1$, where $|G| = mp$.
base case ($m = 1$): We have $|G| = p$. Take any $g \in G \backslash \{1\}$. Its order is > 1 and divides p by Lagrange; hence $|\langle g \rangle| = p$.
inductive step: [Assume we know the result for groups of order kp, $k < m$.] Either (i) $p \big| |C_G(x)|$ for *some* $x \in G \backslash C(G)$, or (ii) $p \not\big| |C_G(x)|$ for *all* $x \in G \backslash C(G)$.

In case (i), $x \notin C(G) \implies |\mathrm{ccl}_G(x)| > 1$, and so

$$|C_G(x)| = \frac{|G|}{|\mathrm{ccl}_G(x)|} < |G|.$$

By Lagrange, $|C_G(x)| \big| |G|$; and so $|C_G(x)|$ is a proper factor of $|G| = mp$ divisible by p. That is, $|C_G(x)| = kp$ for some $k < m$ (with $k \mid m$); and we get an element in $C_G(x)$ of order p by the inductive assumption.

In case (ii), let $\{x_i\}$ be a set of representatives of the conjugacy classes outside the center; we have $p \not\big| |C_G(x_i)| \implies p \big| [G : C_G(x_i)]$ for each i. So p divides the left-hand side of II.H.3 and the sum on the right, hence also $|C(G)|$. Now we use the

Fact: *Any finite abelian group is a direct product of cyclic groups.*

to write $C(G) \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$. Clearly p must divide some m_j, which gives a direct factor of $C(G)$ of the form $\mathbb{Z}_{ap}$. The element $\bar{a}$ in this factor has order p in $C(G)$, thus also in G. □

PROOF (B). Inside $G^p = G \times \cdots \times G$ consider the set

$$X := \{(g_0, g_1, \ldots, g_{p-1}) \in G^p \mid g_0 g_1 \cdots g_{p-1} = 1\}.$$

Having chosen entries $g_1, \ldots, g_{p-1}$, we must take $g_0 = (g_1 \cdots g_{p-1})^{-1}$ to get an element of X, and so

$$|X| = |G|^{p-1}.$$

Introduce an action of $\mathbb{Z}_p$ on X by cyclic permutation:

$$\bar{a}.(g_0, g_1, \ldots, g_{p-1}) := (g_a, \ldots, g_{p-1}, g_0, g_1, \ldots, g_{a-1}).$$

This remains in X since $g_0 g_1 \cdots g_{p-1} = 1 \implies$

$$\begin{aligned} g_a \cdots g_{p-1} g_0 g_1 \cdots g_{a-1} &= (g_0 \cdots g_{a-1})^{-1} (g_0 g_1 \cdots g_{p-1})(g_0 \cdots g_{a-1}) \\ &= (g_0 \cdots g_{a-1})^{-1} (g_0 \cdots g_{a-1}) = 1 \end{aligned}$$

as required.

Now for given $x \in \mathrm{X}$, the Orbit-Stabilizer Theorem gives

$$|\mathbb{Z}_p(x)||(\mathbb{Z}_p)_x| = |\mathbb{Z}_p| = p$$

and so $|\mathbb{Z}_p(x)| = 1$ or p (depending on x). Clearly,

$$\begin{aligned} |\mathbb{Z}_p(x)| = 1 &\iff x \text{ invariant under cyclic permutations} \\ &\iff x = (g, \ldots, g) \text{ for some } g \in G \text{ with } g^p = 1 \end{aligned}$$

Let α resp. β denote the number of 1- resp. p-element orbits in X; since $(1, \ldots, 1) \in \mathrm{X}$ is fixed, $\alpha > 0$. If we can show that $\alpha > 1$, then there is some $g \neq 1$ with $g^p = 1$, and we are done!

Finally, as X is a disjoint union of $\mathbb{Z}_p$-orbits, we have

$$|G|^{p-1} = |\mathrm{X}| = \alpha + p\beta;$$

and since $p \big| |G|$, this yields $p \big| \alpha + p\beta \implies p \mid \alpha > 0$. So $\alpha \geq p$ and we are through. □

We can use Cauchy's Theorem to start classifying groups:

II.H.5. THEOREM. *Let p be an odd prime, $|G| = 2p$. Then $G \cong \mathbb{Z}_{2p}$ (cyclic) or D_p (dihedral).*[14]

PROOF. By Cauchy, there exist $a, b \in G$ with $|\langle a \rangle| = 2$ (hence $a = a^{-1}$) and $|\langle b \rangle| = p$. Now $a \notin \langle b \rangle$ since the order of a doesn't divide p, and so

$$ba \notin \langle b \rangle \tag{II.H.6}$$

[14]Note that $\mathbb{Z}_2 \times \mathbb{Z}_p \cong \mathbb{Z}_{2p}$ since $(2, p) = 1$.

since otherwise $ba = b^r \implies a = b^{r-1} \in \langle b \rangle$. Since $[G{:}\langle b \rangle] = 2$, there are 2 cosets:

$$\begin{aligned} G &= \langle b \rangle \amalg a\langle b \rangle \\ &= \{1, b, b^2, \ldots, b^{p-1}\} \amalg \{a, ab, ab^2, \ldots, ab^{p-1}\}. \end{aligned}$$

Thus

$$\begin{aligned} \text{(II.H.6)} &\implies ba = ab^r \quad (\text{for some } r \in [0, p-1] \cap \mathbb{Z}) \\ &\implies aba^{-1} = b^r \\ &\implies b = ab^r a^{-1} = (aba^{-1})^r = (b^r)^r = b^{r^2} \\ &\implies b^{r^2-1} = 1 \\ &\implies p \mid r^2{-}1 = (r+1)(r-1) \\ &\implies p \mid r{+}1 \text{ or } p \mid r{-}1 \\ &\implies 1 = b^{r+1} \text{ or } b^{r-1} \\ &\implies b^{-1} = b^r \text{ or } b = b^r \\ &\implies aba^{-1} = \underset{\text{(i)}}{b^{-1}} \text{ or } \underset{\text{(ii)}}{b}. \end{aligned}$$

In case (ii), a and b commute; use II.E.11 (on direct products) to deduce that $G \cong \mathbb{Z}_p \times \mathbb{Z}_2$. In case (i), we have just described the multiplication laws of D_p. □

II.H.7. DEFINITION. A group G with order $|G| = p^n$ $(p, n \in \mathbb{N}, p$ prime) is called a **p-group**. (When we use this terminology, it is understood that p is a prime.)

II.H.8. THEOREM. *Any p-group G has nontrivial*[15] *center* $C(G)$.

PROOF. We must show $|C(G)| \neq 1$. Recall the class equation

$$|G| = |C(G)| + \sum_i [G{:}C_G(x_i)],$$

[15] That is, $C(G) \neq \{1\}$.

where x_i are representatives of those conjugacy classes with more than one element. By the orbit-stabilizer theorem,

$$[G{:}C_G(x_i)] = |\mathrm{ccl}_G(x_i)| > 1 \;;$$

and by Lagrange's theorem, $[G{:}C_G(x_i)] \big| |G|$. Hence, $p \big| [G{:}C_G(x_i)]$ for every i, and so (by the class equation and $p \big| |G|$) it follows that $p \big| |C(G)|$. $\square$

For G a *non-p*-group, trivial center *is* possible: e.g., $C(\mathfrak{S}_n) = \{1\}$ for $n \geq 3$.

II.H.9. COROLLARY. *If $|G| = p^2$, p prime, then G is abelian (and $\cong \mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$).*

PROOF. By II.H.8, $|C(G)| > 1$. By Lagrange, there are two cases:
<u>Case (i): $|C(G)| = p$</u>. Taking $h \in G \backslash C(G)$,

$$1 < |\mathrm{ccl}_G(h)| \underset{\text{OST}}{=} [G{:}C_G(h)] \big| |G| = p^2.$$

Since $1 \notin \mathrm{ccl}_G(h)$, we have $|\mathrm{ccl}_G(h)| = p$ (rather than p^2) and thus $|C_G(h)| = p$; and since $C_G(h) \geq C(G) > \{1\}$, we must have $C_G(h) = C(G)$. But $h \in C_G(h)$ (commutes with itself) and $h \notin C(G)$, a contradiction. So the only possibility is . . .

<u>Case (ii): $|C(G)| = p^2$</u>. We have $|C(G)| = p^2 = |G| \implies C(G) = G \implies G$ abelian. By Cauchy's theorem, $G \ni h$ of order p; let $H := \langle h \rangle$. Take $g \in G \backslash H$; it has order > 1 dividing p^2. If this order is p^2 then $G \cong \langle g \rangle \cong \mathbb{Z}_{p^2}$.

Otherwise, $|\langle g \rangle| = p$; and setting $K := \langle g \rangle$, we have:

- $H \cap K < K$ with order dividing $|K| = p \implies H \cap K = \{1\}$;
- $hk = kh$ for every $h \in H$, $k \in K$ because G is abelian; and
- $|H||K| = p^2 = |G|$.

Thus by II.E.11 $G \cong H \times K \cong \mathbb{Z}_p \times \mathbb{Z}_p$. $\square$