Notes on Cauchy’s theorem

We first give McKay’s proof of Cauchy’s theorem. The following argument is a slight variant of §3.2 Exercise 9.

**Lemma.** Let $p$ be a prime number, and let $G$ be a $p$-group (a finite group of order $p^k$ for some $k \geq 1$) acting on a finite set $S$. Let $\text{Fix}$ be the set of fixed points of the action (i.e., $\text{Fix} = \{x \in S : g \cdot x = x, \forall g \in G\}$). Then

$$|\text{Fix}| \equiv |S| \pmod{p}.$$  

**Proof.** Let $x_1, \ldots, x_t$ represent the different orbits. Then

$$x_i \in \text{Fix} \iff \text{Orbit}(x_i) = \{x_i\}.$$  

Also, $|\text{Orbit}(x_i)| = [G : \text{Stab}(x_i)]$ divides $|G| = p^k$, so it is either 1 (if $x_i$ is a fixed point) or a power of $p$ (otherwise). Since the orbits partition $G$, we have

$$|S| = \sum_{i=1}^{t} [G : \text{Stab}(x_i)] \equiv |\text{Fix}| \pmod{p}.$$  

$$\square$$

**Theorem (Cauchy).** If $G$ is a finite group and $p$ is a prime dividing $|G|$, then $G$ has an element of order $p$ (and therefore a subgroup of order $p$).

**Proof.** Let

$$S = \{(x_1, x_2, \ldots, x_p) : x_i \in G, x_1x_2\ldots x_p = 1\}.$$  

Then $|S| = |G|^{p-1}$. The group $\mathbb{Z}/p\mathbb{Z}$ acts on $S$ by cyclically right-shifting the indices of the $x_i$’s. If $F$ denotes the number of fixed points of this action, then $F \equiv |G|^{p-1} \equiv 0 \pmod{p}$ by the Lemma. Since $(1,1,\ldots,1)$ is fixed, there must be at least $p-1$ other fixed points. All fixed points are of the form $(x,x,\ldots,x)$ with $x \in G$ and $x^p = 1$. Taking any $x \neq 1$ in $\text{Fix}$, we have $|x| = p$ and we’re done.  

$$\square$$
Here’s another proof of Cauchy’s theorem in the special case of abelian groups. It is interesting to give a separate proof in this case because (i) the proof is instructive, and (ii) the proof of the Sylow theorems requires only this special case.

**Lemma.** Let $G$ be a finite group, and let $x \in G$. Then $x^m = 1 \iff |x| \mid m$.

**Proof.** One implication is clear. For the other direction, suppose $x^m = 1$. Let $n = |x|$, and write $m = nq + r$ with $0 \leq r < n$. Then $x^r = x^m(x^{-q})^n = 1$ so $r = 0$ by the minimality of $n$. Thus $n \mid m$. \qed

Using this lemma, one deduces the following result.

**Lemma.** Let $G$ be a finite group, $x \in G$, and let $a$ be a positive integer. Finally, let $n = |x|$. Then

$$|x^a| = \frac{n}{(a, n)}.$$

In particular, if $(a, n) = 1$ then $|x^a| = |x|$, and if $a \mid n$ then $|x^a| = |x|/a$.

**Proof.** See §2.3 Prop. 5 on p.57 of the book. \qed

**Theorem (Cauchy’s theorem for abelian groups).** If $G$ is a finite abelian group and $p$ is a prime dividing $|G|$, then $G$ has an element of order $p$.

**Proof.** By induction on $|G|$. It’s clearly true for $|G| = 1$. Now suppose $|G| > 1$, and let $x$ be any non-identity element of $G$. If $p \mid |x|$, say $x = pk$, then $|x^k| = p$ by the above lemma, so we’re done. Suppose $p \nmid |x|$. Let $N = \langle x \rangle$. Since $G$ is abelian, $N$ is normal in $G$. Since $|G/N| = |G|/|N| < |G|$, and $p \nmid |N|$ implies $p \mid |G/N|$, we can apply induction to $G/N$ to conclude that there exists $\overline{y} \in G/N$ of order $p$. Let $y$ be a representative in $G$ for $\overline{y}$. Then $y \notin N$ but $y^p \in N$. Thus $\langle y^p \rangle$ is strictly smaller than $\langle y \rangle$. Thus $|y^p| < |y|$, and by the previous lemma we have $(p, |y|) > 1$, so that $p \mid |y|$. If $|y| = pk$ then $|y^k| = p$ as before and we’re done. \qed