2.8 Cauchy's Theorem

Let S be a set. Recall that the symmetric group on S is the set of all permutations of S:

$$A(S) = \{f : S \to S \ : \ f \text{ is a bijection}\}$$

This is a group under composition of functions.

Given $f \in A(S)$, we write f^n for the powers of f in the group $A(S)$. In particular, $f^0 = i_S$, the identity element of $A(S)$. As a function, this means that

$$f^0(x) = i_S(x) = x \quad \forall x \in S.$$

Then $f^1 = f$, and $f^2 = f \circ f$, so

$$f^2(x) = (f \circ f)(x) = f(f(x)), \quad x \in S.$$

so $f^2(x) = f(f(x)) \ \forall x$

By definition f^{-1} is the inverse map to f, which exists since f is a bijection. Then $f^{-2} = f^{-1} \circ f^{-1}$, so

$$f^{-2}(x) = (f^{-1} \circ f^{-1})(x) = f^{-1}(f^{-1}(x)), \quad x \in S.$$

Now let $f \in A(S)$ be fixed. Define a relation $\sim$ on S by

$$s \sim t \iff t = f^n(s) \text{ for some } n \in \mathbb{Z}.$$

Exercise: Show that $\sim$ is an equivalence relation on S.

As a consequence, the equivalence classes partition the set S. The equivalence class of an element $s \in S$ is

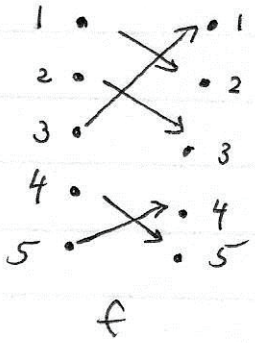
$$\begin{aligned}
[s] &= \{t \in S : s \sim t\} \\
&= \{f^n(s) : n \in \mathbb{Z}\} \\
&= \{\ldots, f^{-2}(s), f^{-1}(s), f^0(s), f^1(s), f^2(s), \ldots\} \\
&= \{\ldots, f^{-1}(f^{-1}(s)), f^{-1}(s), s, f(s), f(f(s)), \ldots\}
\end{aligned}$$

This is called the <u>orbit</u> of s under f. The orbit is the set of all points that s can map to by repeatedly applying f or f^{-1}.

Example

Let $S = \{1,2,3,4,5\}$, so $A(S) = S_5$.

Consider $f \in S_5$ defined by



f

picture notation

Other ways to describe f are to explicitly list what it does to each element:

explicit list $f(1) = 2,\ f(2) = 3,\ f(3) = 1,\ f(4) = 5,\ f(5) = 4$

or to use the shorthand notation

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$ two-line notation

or the cycle notation

$$f = (1\ 2\ 3)(4\ 5).$$ Cycle notation

However we choose to describe it, f is a bijection of $\{1,2,3,4,5\}$ onto itself (often called a permutation

[redacted]

The orbit of $x = 2$ is

$$[2] = \{1, 2, 3\} = [1] = [3]$$

while the orbit of $x = 5$ is

$$[5] = \{4, 5\} = [4]$$

Note that orbits need not have the same size, but they are either <u>equal</u> or <u>disjoint</u> (because they are equivalence classes!)

Exercise: What is f^{-1}? What is $o(f)$?

Example

Let $S = \mathbb{R}$, so $A(\mathbb{R})$ is the set of all bijections of $\mathbb{R}$ onto itself.

Consider $f \in A(\mathbb{R})$ defined by $f: \mathbb{R} \to \mathbb{R}$, $f(x) = 3x$.

To find the orbit of $x = 1$, we compute $f^n(1)$ for $n \in \mathbb{Z}$:

$f^0(1) = 1$ since f^0 is the identity map by definition

$f^1(1) = f(1) = 3$

$f^2(1) = f(f(1)) = f(3) = 3 \cdot 3 = 3^2$

$f^3(1) = f(f^2(1)) = 3 \cdot 3^2 = 3^3$

and so forth for the positive powers. Since $f^{-1}(x) = \frac{x}{3}$, the negative powers are

$f^{-1}(1) = \frac{1}{3}$

$f^{-2}(1) = f^{-1}(f^{-1}(1)) = f^{-1}\left(\frac{1}{3}\right) = \frac{1}{9} = \frac{1}{3^2} = 3^{-2}$

etc. We see that $f^n(1) = 3^n$ for $n \in \mathbb{Z}$. Thus

$[1]$ [redacted] $= \{f^n(1) : n \in \mathbb{Z}\} = \{3^n : n \in \mathbb{Z}\}$.

Example

Now consider a different $f \in A(S)$, say

$f: \mathbb{R} \to \mathbb{R}$, $f(x) = x^3$ Note that $f^{-1}: \mathbb{R} \to \mathbb{R}$ is defined by $f^{-1}(x) = x^{1/3}$

The values of $f^n(1)$ for some particular n are:

$f^0(1) = 1$, $f^1(1) = f(1) = 1$, $f^2(1) = f(f(1)) = 1$, ...

$f^{-1}(1) = 1$, $f^{-2}(1) = f^{-1}(f^{-1}(1)) = f^{-1}(1) = 1$, ...

Thus $f^n(1) = 1 \ \forall n \in \mathbb{Z}$, so the orbit of $x = 1$ is

$$[1] = \{ f^n(1) : n \in \mathbb{Z} \} = \{1\}$$ (only 1 element in the orbit)

On the other hand, for $x = 3$:

$f^0(3) = 3$

$f^1(3) = 3^3$

$f^2(3) = f(3^3) = (3^3)^3 = 3^{3 \cdot 3}$

$f^3(3) = f(3^{3 \cdot 3})^3 = 3^{3 \cdot 3 \cdot 3}$

etc. By induction, $f^n(3) = 3^{(3^n)}$, $n > 0$.

Also,

$$f^{-1}(3) = 3^{1/3} = 3^{(3^{-1})}$$

$$f^{-2}(3) = f^{-1}(3^{1/3}) = (3^{1/3})^{1/3} = 3^{\frac{1}{3}\cdot\frac{1}{3}} = 3^{(3^{-2})}$$

etc. By induction $f^n(3) = 3^{(3^n)}$ for $n < 0$. Thus

$$[3] = \{ 3^{(3^n)} : n \in \mathbb{Z} \}$$

Remark

If S is any set then $A(S)$ is a group. So we can talk about the order of an element $f \in A(S)$:

[redacted]

If there is a positive integer $n > 0$ such that $f^n = id_S$, then $o(f)$ is the smallest such n. If there is no $n > 0$ for which $f^n = id_S$, then $o(f) = \infty$.

Theorem
Let S be a set, & let p be prime.

Suppose $f \in A(S)$ & $o(f) = p$.

Then for any $s \in S$, the orbit $[s] = \{f^n(s) : n \in \mathbb{Z}\}$

contains either 1 or p elements.

Proof:
We are given that $f \in A(S)$ & $o(f) = p$. So $f: S \to S$

is a bijection, & p is the smallest positive integer

s.t. $f^p = i_S$.

Choose any particular $s \in S$. We want to show

that $[s]$ has either 1 or p elements.

Since f is a bijection, $f(s)$ is an element of S.

There are two possibilities: either $f(s) = s$ or $f(s) \neq s$.

Case 1: $f(s) = s$.

In this case $f^2(s) = f(f(s)) = f(s) = s$, etc., so

$f^n(s) = s \quad \forall n > 0$. Whatever f^{-1} is, it must precisely "undo" what f does. So since f maps s to s, f^{-1} must map s back to s. Hence $f^{-1}(s) = s$, & then $f^{-2}(s) = f^{-1}(f^{-1}(s)) = f^{-1}(s) = s$, etc. Thus $f^n(s) = s \quad \forall n \in \mathbb{Z}$. (Note that this does NOT say that f is the identity - we don't know what it does to the other elements of S!) Therefore

$$[s] = \{f^n(s) : n \in \mathbb{Z}\} = \{s\}$$

has only 1 element.

Case 2: $f(s) \neq s$.

Since $o(f) = p$, we have $f^p = i_S$, the identity map on S. Hence $f^p(s) = s$. We claim that $s, f(s), \ldots, f^{p-1}(s)$ are all distinct elements of S. If they weren't all distinct, then we would have

$f^m(s) = f^n(s)$ for some $m \neq n$ between 0 & $p-1$.

One of m, n must be larger, let's say $m < n$ (otherwise, switch their names). Then $k = n - m$ lies between 1 & $p-1$ (why?), and $f^k(s) = s$ (why?).

The GCD of k & p is $(k, p) = 1$. Hence, $\exists\, j, l \in \mathbb{Z}$ s.t. $jk + lp = 1$. Therefore,

$$s \neq f(s) = f^{jk+lp}(s)$$

See Theorem 1.5.3 in Herstein

$$= f^{lp}(f^{jk}(s))$$

$$= f^{lp}(s) \quad \text{because } f^k(s) = s$$

$$= s \quad \text{because } f^p(s) = s.$$

But this is a contradiction. Hence $s, f(s), \ldots, f^{p-1}(s)$ must indeed all be different.

Exercise: Now show that if n is any integer, then $f^n(s)$ equals one of $s, f(s), \ldots, f^{p-1}(s)$.

Hint: Write $n = jp + r$ with $0 \leq r \leq p-1$.

Finally, we conclude (why?) that

$$[s] = \{f^n(s) : n \in \mathbb{Z}\} = \{s, f(s), \ldots, f^{p-1}(s)\},$$

and hence $[s]$ contains exactly p elements. ▨

Cauchy's Theorem

If G is a group, p is prime, & $p \mid |G|$, then $\exists a \in G$ with $o(a) = p$.

Proof:

If $p = 2$ then $|G|$ is even. Homework #1 then shows that $\exists a \in G$ with $a \neq e$ s.t. $a^{-1} = a$. Hence $a^2 = e$, and $o(a) = 2$.

Now consider the case $p = 3$. Define

$$S = \{(a,b,c) : a,b,c \in G \ \& \ abc = e\}.$$

Note that if $(a,b,c) \in S$ then we are forced to have $c = (ab)^{-1} = b^{-1}a^{-1}$. Therefore, while a, b can be arbitrary elements of G, once we've chosen a and b, there is no choice left for c. Hence the size of S is

$$|S| = |G|^2.$$

S contains $|G|^2$ elements

Now define a function

$$f : S \longrightarrow S$$
$$f((a,b,c)) = (c,a,b)$$

Exercise: Show f is a bijection; hence $f \in A(S)$.

Since $3 \mid |G|$, we can find $a \neq b$ in G.

Setting $c = (ab)^{-1}$, we have $(a,b,c) \in S$.

Then $f((a,b,c)) = (c,a,b) \neq (a,b,c)$

since these components are not equal

Thus f is not the identity map on S;

$f \neq i$. On the other hand, $f^3 = i$.

Therefore the order of f as an element of the group $A(S)$ is >1 but divides 3, hence must be exactly $o(f) = 3$.

The preceding theorem therefore shows that the

orbit of under f will contain either 1 or 3 elements.

Since the distinct orbits partition S, we have

$$|S| = \#\text{1-element orbits} + 3 \times \#\text{3-element orbits}$$

Thus $|S| = m + 3n$ for some integers $m, n \geq 0$.

And we know that $m \geq 1$ because $(e,e,e) \in S$ has a 1-element orbit (why?). Further, $|S| = |G|^2$ so $3 \mid |S|$ since $3 \mid |G|$, and $3 \mid 3n$, so 3 must divide $m = |S| - 3n$. Hence $m \geq 3$, so there are at least 3 different 1-element orbits. One of these, as we said, is the orbit of (e,e,e). But there must be another one, there must be some $(a,b,c) \in S$ with $(a,b,c) \neq (e,e,e)$ that has a 1-element orbit. But the orbit of (a,b,c) includes

$$f^0((a,b,c)) = (a,b,c),$$

$$f^1((a,b,c)) = (c,a,b),$$

$$f^2((a,b,c)) = (b,c,a).$$

since all of these are in $[(a,b,c)]$ yet the set has only 1 element, they must be equal:

$$(a,b,c) = (c,a,b) = (b,c,a).$$

Consequently $a=b=c$. Thus $(a,a,a) = (a,b,c) \in S$, which implies that $a^3 = aaa = abc = e$.

Since $a \neq e$, this implies that $o(a) = 3$ (why?)

Hence we have shown that G contains an element of order 3.

Note: G does not have a unique element of order p.

For, $\langle a \rangle = \{e, a, a^2\} = \{e, a^2, a^4\} = \langle a^2 \rangle$.

The element a^2 also has order 3

What about larger primes? The proof is similar.

For an arbitrary prime p we take

$$S = \{(a_1, a_2, \ldots, a_p) : a_1, \ldots, a_p \in G \ \& \ a_1 \cdots a_p = e\}$$

Since we can choose $a_1, \ldots, a_{p-1}$ arbitrarily but are then forced to set $a_p = (a_1 \cdots a_{p-1})^{-1}$, we have $|S| = |G|^{p-1}$. We define

$$f : S \longrightarrow S$$
$$f(a_1, \ldots a_{p-1}, a_p) = (a_p, a_1, \ldots, a_{p-1})$$

and then consider elements of S that have 1-element & p-element orbits.

Exercise: Finish the proof. ∎

Cauchy's Theorem has many consequences, we will have time to consider only a few of them.

In particular, let us consider what Cauchy's Theorem implies about the structure of groups with certain orders. We already know that if $|G|=p$ is prime, then G is cyclic. What if $|G|=pq$ is the product of 2 primes?

Actually, we do NOT need q to be prime in this theorem!
We just need p prime and p > q.

Theorem
Suppose $|G|=pq$ where p, q are primes with $p>q$.
q can be any positive integer, but p is prime with p>q
Then G has a unique subgroup A with $|A|=p$, and A is normal in G.

Proof:
By Cauchy's Theorem, $\exists\, a \in G$ with $o(a)=p$.

Hence $A = \langle a \rangle$ is a subgroup of G with order p.

To show that A is unique, suppose that $B \neq A$ was another subgroup of order p. Consider the set

$$AB = \{xy : x \in A,\ y \in B\}.$$

We don't claim that AB is a subgroup, but we do claim that AB has exactly p^2 distinct elements. Note first that since $|A| = p$ & $|B| = p$, there can be at most p^2 elements in AB. There will be exactly p^2 elements if all the products xy with $x \in A$, $y \in B$ are distinct. So, suppose two such products were equal, say

$$xy = uv \quad \text{where } x, u \in A \ \& \ y, v \in B.$$

Then we have

$$\underbrace{u^{-1}x}_{\in A} = \underbrace{vy^{-1}}_{\in B}$$

Hence, this element belongs to both A & B, i.e., $u^{-1}x = vy^{-1} \in A \cap B$. But $A \cap B$ is a subgroup of both A & B (why?), so its order must divide $|A| = p = |B|$. If $|A \cap B| = p$ then

we would have $A = A \cap B = B$, a contradiction.

Hence $A \cap B = \{e\}$. Thus

$$u^{-1}x = vy^{-1} \in A \cap B = \{e\}$$

so $u^{-1}x = e = vy^{-1}$. But then $u = x$ & $v = y$.

Thus we do indeed have that $|AB| = p^2$.

But $AB \subseteq G$, so $|AB| \leq |G| = pq$.

Hence $p^2 \leq pq$, so $p \leq q$. This contradicts the fact that $p > q$. Hence there is no subgroup of G of order p other than A itself.

Thus A is the unique subgroup of order p, & now we show it is normal. Suppose $a \in G$. Then aAa^{-1} is a subgroup of G (why?) and $|aAa^{-1}| = |A|$ (why?). Hence aAa^{-1} is a subgroup of order p. But there's only one such

subgroup & it is A, so we must have $aAa^{-1} = A$. Therefore A is normal. ∎

Note

The final idea used in this proof is a useful fact: If a group G contains one & only one subgroup of a particular order, then that subgroup must be normal.

Corollary

Again, we do NOT need q to be prime in this corollary!
We just need p prime and p > q.

Suppose $|G| = pq$, where p, q are primes with $p > q$. Suppose

q is a positive integer and p is prime with p > q

$a \in G$ & $o(a) = p$. If $x \in G$, then $xax^{-1} = a^k$ for some $0 < k < p$ (k depends on x).

Proof:

By the Theorem, $A = \langle a \rangle$ is the unique subgroup of G of order p, & $A \triangleleft G$. Given $x \in G$, we therefore have $xax^{-1} \in A = \{e, a, \ldots, a^{p-1}\}$. Thus

$xax^{-1} = a^k$ for some $0 \leq k < p$. If $k=0$ then $xax^{-1} = e$, which implies $a = x^{-1}ex = e$, contradicting the fact that $o(a) = p$. Hence $0 < k < p$. ∎

We can now prove that many of the groups of order pq must be cyclic.

Theorem We DO need both p and q to be prime in this Theorem.

Suppose $|G| = pq$ where p, q are primes, $p > q$, & $q \nmid p-1$.

Then G is cyclic.

Proof

By Cauchy's Theorem, G has an element a of order p, and another element b of order q. By the preceding corollary, $bab^{-1} = a^k$ for some $0 < k < p$. Therefore

$$b^2ab^{-2} = b\,bab^{-1}b^{-1}$$

$$= ba^kb^{-1}$$

$$= (bab^{-1})(bab^{-1})\cdots(bab^{-1}) \quad (k \text{ times})$$

$$= a^k a^k \cdots a^k \quad (k \text{ times})$$

$$= (a^k)^k$$

$$= a^{k\cdot k} = a^{(k^2)}.$$

[redacted]

Exercise: Show that $b^j a b^{-j} = a^{(k^j)}$, all $j \geq 0$.

In particular, for $j = q$ we have

$$a = eae = b^q a b^{-q} = a^{(k^q)}.$$

Thus

$$a^{(k^q - 1)} = e.$$

Since $o(a) = p$, this implies $p \mid k^q - 1$, so

$$k^q \equiv 1 \mod p.$$

But recall that

$$\mathbb{Z}_p^\times = \{1, 2, \ldots, p-1\}$$

is a group under multiplication mod p (because p is prime), and $k \in \mathbb{Z}_p^\times$. The fact that $k^q \equiv 1 \mod p$ means that $o(k) \mid q$, so the order of k as an element of $\mathbb{Z}_p^\times$ must divide q. Since q is prime, this implies that $o(k)$ is either 1 or q. But $o(k)$ must also divide

the order of $\mathbb{Z}_p^\times$, so $o(k) \mid p-1$.

Since $q \nmid p-1$, $o(k)$ can't be q. Therefore $o(k) = 1$. Hence k is the identity element in $\mathbb{Z}_p^\times$, so $k = 1$. Therefore

$$bab^{-1} = a^k = a,$$

so $ba = ab$.

Let $A = \langle a \rangle$ & $B = \langle b \rangle$. Exercise: since $|A| = p$ & $|B| = q$ are relatively prime, $A \cap B = \{e\}$.

Now consider the element $c = ab$. Let $n = o(c)$. Since $|G| = pq$, we have $n \mid pq$. On the other hand, since a & b commute,

$$a^n b^n = (ab)^n = e.$$

Therefore $a^n = b^{-n}$, so

$$b^{-n} = a^n \in A \quad \& \quad a^n = b^{-n} \in B.$$

Thus $a^n = b^{-n} \in A \cap B = \{e\}$. Hence $a^n = e = b^n$. Since $p = o(a)$ & $q = o(b)$, we therefore have $p \mid n$ & $q \mid n$, and hence $pq \mid n$. But earlier we said $n \mid pq$, so $n = pq$. Therefore

$$o(c) = n = pq = |G|.$$

Hence $G = \langle c \rangle$, so G is cyclic. ∎

As a consequence of these results,
We can classify all groups of certain orders.

order = 1: $\cong$ to $\{e\}$

order 2, 3, 5, 7, ... p prime $\cong \mathbb{Z}_p$

Exercise
$|G| = 4 \Rightarrow G \cong \mathbb{Z}_4$ or $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

Exercise
$|G| = 6 \Rightarrow G \cong \mathbb{Z}_6$ or $G \cong S_3$.

The smallest nonabelian group is S_3.

For 8, 10, 12, 14, we can't yet classify all the groups of those orders. You can do it directly, working out the possible multiplication tables, but its not much fun. 12 is especially difficult!

But order 15 is easy: $15 = 5 \cdot 3$ & $3 \nmid 5-1$, so any group of order 15 is cyclic, hence isomorphic to $\mathbb{Z}_{15}$.

What other orders can you handle now?