MA294 Lecture

Timothy Kohl

Boston University

February 6, 2024

Other basic facts about groups:

Proposition

Let x, y, z, a, b *be elements of a group* $(G, *)$ *then*

$$x * y = x * z \to y = z \text{ (left cancellation)}$$
$$a * x = b * x \to a = b \text{ (right cancellation)}$$

Proof.

$$x * y = x * z$$
$$x^{-1} * x * y = x^{-1} * x * z \text{ (Note, we multiply both sides on the } \textit{left}.)$$
$$e * y = e * z$$
$$y = z$$

A similar argument works for the other statement. □

These 'cancellation' rules imply the following.

Proposition

The Cayley table for a group $(G,*)$ is a latin square.

Why? If we look at a row of the Cayley table:

$*$		y	$\dots$	z
x		$x*y$		$x*z$

we cannot have $x*y = x*z$ unless $y = z$ by left cancellation so there are no repeats in a given row.

And for columns:

$*$		x	$\dots$	
a		$a * x$		
b		$b * x$		

we find that $a * x = b * x$ only if $a = b$ so there are no repeated elements in a column.

The Order of a Group Element

Definition

In a group $(G, *)$ if $a \in G$ and $n \geq 1$ is an integer, then

$$a^n = \underbrace{a * a * \cdots * a}_{n\text{-times}}$$

That is $a^1 = a$, $a^2 = a * a$, $a^3 = a * a * a$, and similar to how one defines a^0 for a *number*, we define $a^0 = e$, the identity of G.

And the use of the notation 'a^{-1}' for the inverse, fits in with this definition, since

$$a^{-1} * a = a^{-1} * a^1 = a^{(-1)+1} = a^0 = e$$

and similarly, we may define a^{-n} to be $a^{-1} * a^{-1} * \cdots * a^{-1} = (a^{-1})^n$. That is, exponents in groups, work like they do for numbers.

Notation Alert: If $*=$'$+$' like in $\mathbb{Z}$ or $\mathbb{Z}_m$ then instead of writing

$$a^n = a * a * \cdots a$$

we write

$$na = a + a + \cdots + a$$

so that, for example, if $2 \in \mathbb{Z}_5$ we have $3 \cdot 2 = 2 + 2 + 2 = 6 = 1$.

An important, yet not so obvious point is that for any $a \in G$ and any n the power $a^n \in G$ by the closure property.

The simplest way to see this is by noting that

$$a^n = \underbrace{a * a * \cdots * a}_{(n-1)\text{-times}} * a$$

namely $a^{n-1} * a$.

So if we assume that $a^{n-1} \in G$ then $a^{n-1} * a \in G$ so $a^n \in G$.

And the same holds for negative powers.

Other examples:
In D_3, we have

$$r_{120}^{0} = r_0$$
$$r_{120}^{1} = r_{120}$$
$$r_{120}^{2} = r_{120} \circ r_{120} = r_{240}$$
$$r_{120}^{3} = r_{120}^{2} \circ r_{120} = r_{240} \circ r_{120} = r_0 \text{ [Why?]}$$
$$r_{120}^{4} = r_{120}^{3} \circ r_{120} = r_0 \circ r_{120} = r_{120} \text{ [Note: We're back at } r_{120}\text{]}$$
$$r_{120}^{-1} = r_{240}$$
$$r_{120}^{-2} = r_{120}$$
$$r_{120}^{-3} = r_0$$

For the flips like f_1, the powers are a bit simpler

$$\begin{aligned} f_1^0 &= r_0 \\ f_1^1 &= f_1 \\ f_1^2 &= r_0 \\ f_1^3 &= f_1 \\ f_1^{-1} &= f_1 \end{aligned}$$

And in $\mathbb{Z}_6$ we have

$$
\begin{aligned}
0 \cdot 2 &= 0 \\
1 \cdot 2 &= 2 \\
2 \cdot 2 &= 2 + 2 = 4 \\
3 \cdot 2 &= 2 + 2 + 2 = 0 \\
4 \cdot 2 &= 2 + 2 + 2 + 2 = 2 \\
(-1) \cdot 2 &= (-2) = 4 \\
(-2) \cdot 2 &= (-4) = 2 \\
&\text{etc...}
\end{aligned}
$$

The discussion of powers of elements leads naturally to the concept of 'order' of an element.

Definition

If $x \in G$ where G is finite, then the order of x is the least positive integer m such that $x^m = e$, in which case we write $|x| = m$.

If G is infinite, then it's possible that $x, x^2, x^3, \ldots$ are all distinct (non-identity) elements of G, in which case we say that x has infinite order and we write $|x| = \infty$.

Note, if G is infinite, (as a set) it's still possible that it has elements of finite order, there are many possibilities.

Examples:

For $2 \in \mathbb{Z}_6$ we have $1 \cdot 2 = 2$, $2 \cdot 2 = 4$ and $3 \cdot 2 = 0$ and so $|2| = 3$.

In D_3, $|r_{120}| = 3$ since $r_{120}^2 = r_{240}$ and $r_{120}^3 = r_{360} = r_0$

In contrast, $|f_1| = 2$ since $f_1^2 = r_0$.

For the element $1 \in \mathbb{Z}$ we have the multiples $1, 1+1 = 2, 1+1+1 = 3, \ldots$ none of which *ever* equals 0, so 1 has infinite order.

Note, for any group G, the identity element e has order 1, and it is the unique element of order 1.

If $x \in G$ has order m then $x^{2m} = (x^m)^2 = e^2 = e$, and similarly $x^{3m} = e$ etc.

Theorem

If $x \in G$ and $|x| = m$ then $x^t = e$ if and only if $m|t$.

Proof.

Suppose $x^t = e$, where t is *not* a multiple of m then by the division algorithm $t = qm + r$ where $r \in \{1, \ldots, m-1\}$ (i.e $r \neq 0$) which means $x^t = x^{qm+r} = x^{qm}x^r$.

But $x^{qm} = (x^m)^q = e$ so we have that $x^t = x^r$ but then since $x^t = e$ then $x^r = e$.

However, since $r < m$ this contradicts the fact that $|x| = m$, which is the *least* positive power of x which is the identity. □

What can happen is that for some groups G, there is an $x \in G$ such that $G = \{e, x, x^2, \ldots, x^{m-1}\}$ and one says that x *generates* G.

Also, we sometimes use the notation of '1' for the identity which is consistent with the usual view of raising a number to the zero-th power being 1, i.e. $x^0 = 1$, so that if G is generated by x, it consists of $\{1, x, x^2, \ldots, x^{m-1}\}$ if $|x| = m$.

If G is generated by x the we write $G = \langle x \rangle$, and we sometimes say G is a *cyclic* group since the powers of x 'cycle' through these distinct powers, i.e.

$$1, x, x^2, \ldots, x^{m-1}, x^m = 1, x^{m+1} = x, x^{m+2} = x^2, \ldots \text{ etc.}$$

If G is infinite, then it's possible that for some element x one has that $G = \langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$.

How does this work?

Well, it simply means that each non-zero power of x is not the identity of G, so that G consists of

$$\{\dots, x^{-3}, x^{-2}, x^{-1}, x^0 = 1, x^1 = x, x^2, x^3, \dots\}$$

in which case we say that G is an infinite cyclic group.
The prime example of this is $\mathbb{Z} = \langle 1 \rangle$ since every element of $\mathbb{Z}$ is a multiple of 1.

In fact, we can use this idea to actually *define* an infinite group consisting of powers of x.

For x a 'variable' (symbol, whatever), one can define 'the' infinite cyclic group

$$C_\infty = \{x^n \mid n \in \mathbb{Z}\}$$

with the group operation being based on the rules of exponents, namely:

$$x^i * x^j = x^{i+j}$$

which is very naturally closed, and associative since

$$x^i * (x^j * x^k) = x^i * x^{j+k} = x^{i+j+k}$$

which is the same as $(x^i * x^j) * x^k = x^{i+j} * x^k$.

Moreover, it contains an identity element $1 = x^0$ since clearly $x^0 * x^i = x^i$ and $x^i * x^0 = x^i$, and similarly every element x^i has inverse x^{-i}.

If you've observed that the operations in C_∞ mirror those of the integers, you are correct, but the interesting contrast is that C_∞ is 'multiplicative' while $\mathbb{Z}$ is an additive group.