Math 3200: Day 29

Recall the definition from last time:

Def: Define the operation $+_n$ on $\mathbb{Z}_n$ as follows: for any $[a],[b]\in\mathbb{Z}_n$, define

$$[a]+_n[b]=[a+b].$$

Likewise, define $\cdot_n$ on $\mathbb{Z}_n$ by

$$[a]\cdot_n[b]=[a\cdot b].$$

Now, there's something to worry about here. If $n=5$, then $[2]=[7]$ & $[3]=[8]$, so if I want to add $[2]+_5[3]$, should I take $[2+3]$ or $[7+3]$ or $[2+8]$ or $[7+8]$? Or something else?

In other words, if I'm defining addition of classes by adding representatives, you should be very worried that the answer you get may depend on the representatives you pick.

Worrying Example: Consider the equivalence relation R on $\mathbb{Q}$ given by aRb iff $\lfloor a\rfloor=\lfloor b\rfloor$ (why is this an equiv. relation?)

Then the set of equivalence classes looks like $\mathbb{Z}$ (as a set), but there's no way to define addition on this set.

If we tried to define $[a]+[b]=[a+b]$, then we'd have problems since

$$[1]=[1.9] \;\&\; [2]=[2.9], \text{ but}$$

$$[1+2]=[3] \;\&\; [1.9+2.9]=[4.8]=[4] \text{ and } [3]\neq[4].$$

However, in the case of $\mathbb{Z}_n$, nothing goes wrong, which we check by showing it doesn't matter which rep. you pick:

Prop: Addition is well-defined on $\mathbb{Z}_n$.

Proof: Suppose $[a],[b]\in\mathbb{Z}_n$ & suppose that $a'\in\mathbb{Z}$ so that $[a]=[a']$.

Then the question is whether $[a]+_n[b]=[a']+_n[b]$.

Clearly, if $[a]=[a']$, then $a\equiv a' \pmod n$, so $a'=xn+a$ for some $x\in\mathbb{Z}$.

But then $[a'] +_n [b] = [a'+b] = [xn+a+b] = [a+b] = [a] +_n [b]$.

Similarly for any $[b'] = [b]$, so we see that $+_n$ is a well-defined operation on $\mathbb{Z}_n$. ▨

Prop: For $n \geq 2$, if $[a] \in \mathbb{Z}_n$, then there exists $[b] \in \mathbb{Z}_n$ so that $[a] +_n [b] = [0]$.

Proof: Let $[b] = [-a]$. Then

$$[a] +_n [-a] = [a+(-a)] = [0].$$ ▨

One can also easily show that $+_n$ is associative (i.e., $([a] +_n [b]) +_n [c] = [a] +_n ([b] +_n [c])$ $\forall\, a, b, c \in \mathbb{Z}_n$).

This means that $\mathbb{Z}_n$ is a group.

Def: Suppose G is a set & that $*$ is a binary operation on G satisfying the following conditions:

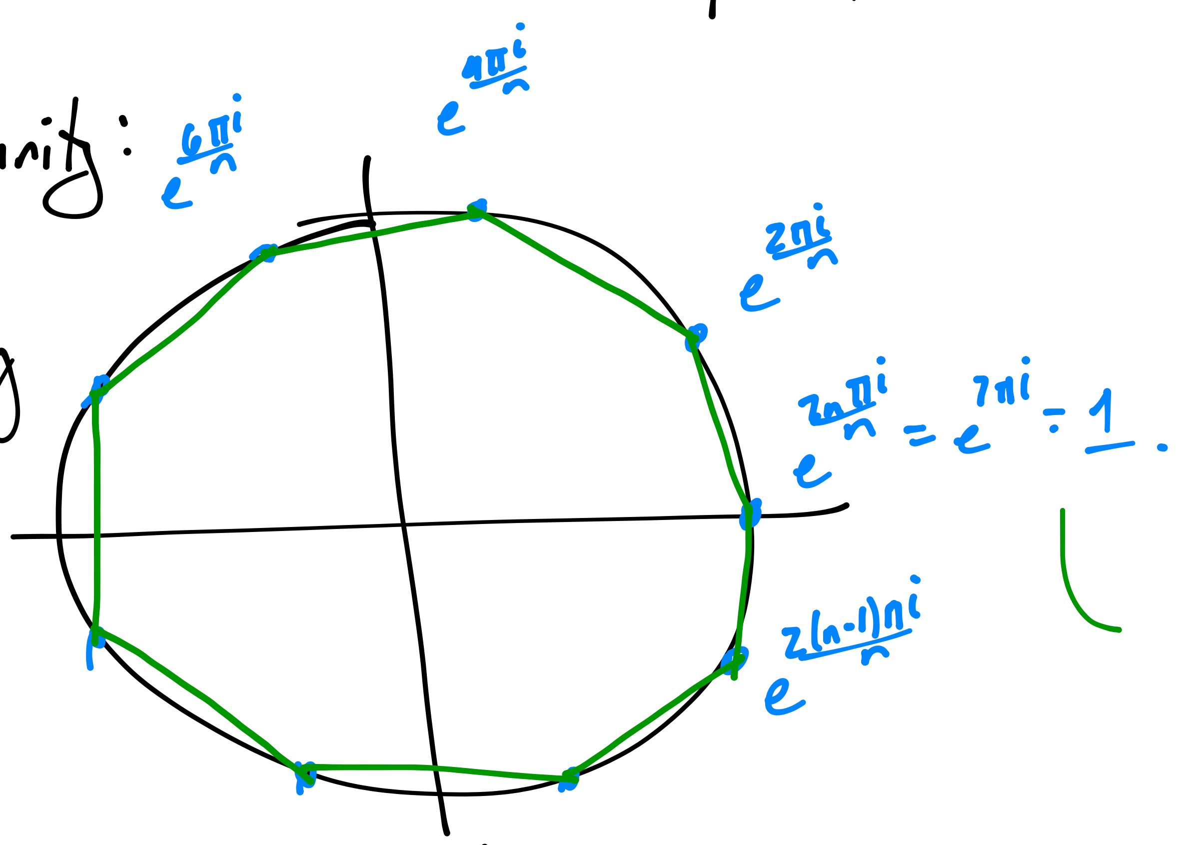
- $\exists\, e \in G$ (called the identity element) so that $e * g = g * e = g$ $\forall\, g \in G$.
- $\forall\, g \in G$ $\exists\, h \in G$ such that $g * h = h * g = e$. h is called the inverse of g & denoted g^{-1}.
- $*$ is associative; i.e., $\forall\, g, h, k \in G$, $(g*h)*k = g*(h*k)$

Visualizing $\mathbb{Z}_n$: Define the correspondence $[k] \longleftrightarrow e^{\frac{2\pi i k}{n}}$ for all $k \in \mathbb{Z}$.

Then $[k] +_n [l] = [k+l] \longleftrightarrow e^{\frac{2\pi i (k+l)}{n}} = e^{\frac{2\pi i k}{n} + \frac{2\pi i l}{n}} = e^{\frac{2\pi i k}{n}} e^{\frac{2\pi i l}{n}}$, as you'd want

(the point, as usual, is the exponential turns addition into multiplication).

So we can visualize $\mathbb{Z}_n$ as the n^{th} roots of unity:



So adding $[1]$ is the same as multiplying by $e^{\frac{2\pi i}{n}}$ which is the same as rotating the circle by an angle $\frac{2\pi i}{n}$.

So yet another way to think of $\mathbb{Z}_n$ is as the group of rotational symmetries of the regular n-gon!
This is where group theory really shines: in the study of symmetry.