Math 347 - Lecture 25

Topics: Some more visualization
- WpH - dependence and congruence (e.g.,

For an equivalence relation \( \sim \) on a set \( A \), it is often useful to visualize \( A/\sim \) as “gluing together” all points in each equivalence class.

Example Define \( \sim \) on \( \mathbb{R} \) by
\[
(x,y) \sim (u,v) \iff x-u \in \mathbb{Z} \text{ and } y-v.
\]

\[\mathbb{R}^2/\sim \text{ can be visualized as a cylinder.}\]

Example Define \( \sim \) on \( \mathbb{R}^2 \) by
\[
(x,y) \sim (u,v) \iff x-u \in \mathbb{Z} \text{ and } y-v \in \mathbb{Z}.
\]

\[\mathbb{R}^2/\sim \text{ can be visualized as a donut.}\]
Let \( n \in \mathbb{N} \) and let \( \equiv_n \) be the equivalence relation on \( \mathbb{Z} \) given by \( a \equiv_n b \iff a \equiv b \pmod{n} \).

**Notation:** \( \mathbb{Z}_n = \mathbb{Z}/\equiv_n \).

We saw last time that
\[
\mathbb{Z}_n = \mathbb{Z}/\equiv_n = \{ [0], [1], \ldots, [n-1] \}
\]
We also sometimes write \([0]_n, [1]_n\), etc. I'm not to make it clear that this is the equivalence class for \( n \).

**Def.** Define operations \( + \) and \( \cdot \) on \( \mathbb{Z}_n \) by
\[
[a] + [b] = [a+b] \\
[a] \cdot [b] = [ab]
\]

**Ex.** Say \( n = 7 \). Then
\[
\]

But wait: \( 12 = 5 \pmod{7} \), so \([5] = [12] \).

Then we would want
\[
\]
Will \([12] + [6] = [18] = [4] \), so this is ok.

But what happened here? The equivalence classes \([5] \) and \([12] \) are equal, but we have written them differently. The definition of \( + \) and \( \cdot \) looks like it depends on how we have written the equivalence class, because we have used this particular \( a \in [9] \) and \( b \in [6] \) to write \([a+b] \)

But it turns out that it doesn't matter!

**Def.** A concept is well-defined if it is independent of all choices made in its definition.
The $\mathbb{Z}/n\mathbb{Z}$ norm is well-defined.

Proof: For $n > 1$, we want to show that if $a, b, c, d \in \mathbb{Z}$ such that $[a] = [c]$ and $[b] = [d]$, then

$$[a+b] = [c+d].$$

If $[a] = [c]$, then $a = c + kn$ for some $k \in \mathbb{Z}$. If $[b] = [d]$, then $b = d + ln$ for some $l \in \mathbb{Z}$. Then

$$[a+b] = [c+kn+d+ln]$$

$$= [c+d+n(k+l)]$$

$$= [c+d]$$

since $c+d = c+d+n(k+l)(\text{mod} n)$

Thus $\mathbb{Z}/n\mathbb{Z}$ is well-defined.

NonExample: Say we tried to define a function $f: \mathbb{Z} \rightarrow \mathbb{Z}$ by $f([a]) = a^2 + 1$. This is not well-defined since for any $a \in \mathbb{Z}$, $[a] = [a+n]$, so we need $f([a]) = f([a+n])$.

But $a^2 + 1 \neq (a+n)^2 + 1$ since $n = 1$. So this doesn't make sense.

However, $F: \mathbb{Z} \rightarrow \mathbb{Z}$, given by $F([a]) = [a^2+1]$ is well-defined. Indeed

$$[a^2+1] = [a^2] + [1] = [a]^2 + [0] + [1]$$

Since both $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}$ are well-defined, $F$ is well-defined.