Part 5: Relations

More on Equivalence Relations

Martin Licht, Ph.D.

March 6, 2018

UC San Diego
Department of Mathematics

Math 109

Equivalence Relations

Suppose that X is a set with an equivalence relation $\sim_X$ and that Y is a set with an equivalence relation $\sim_Y$.

We are interested in functions that preserve equivalence relations.

We say that $f : X \to Y$ **preserves an equivalence relation** if for all $a, b \in X$ with $a \sim_X b$ we have $f(a) \sim_Y f(b)$. In other words,

$$\forall a, b \in X : \Big(a \sim_X b\Big) \to \Big(f(a) \sim_Y f(b)\Big).$$

This induces a function between the sets of equivalence classes:

$$f : X_{/\sim_X} \to Y_{|\sim_Y}, \quad [a]_{\sim_X} \to [f(a)]_{\sim_Y}.$$

Equivalence Relations

We sometimes want to do that for functions with several arguments too. Suppose that X is a set with an equivalence relation $\sim_X$ and that Y is a set with an equivalence relation $\sim_Y$.

We say that $f : X \times X \to Y$ **preserves an equivalence relation** if for all $a_0, a_1, b_0, b_1 \in X$ with $a_0 \sim_X b_0$ and $a_1 \sim_X b_1$ we have $f(a_0, a_1) \sim_Y f(b_0, b_1)$. In other words,

$$\forall a_0, a_1, b_0, b_1 \in X : \Big(a_0 \sim_X b_0 \wedge a_1 \sim_X b_1\Big) \to \Big((a_0, a_1) \sim_Y f(b_0, b_1)\Big).$$

This induces a function between the set of equivalence classes:

$$f : X_{/\sim_X} \times X_{/\sim_X} \to Y_{|\sim_Y}, \quad \Big([a]_{\sim_X}, [b]_{\sim_X}\Big) \to [f(a, b)]_{\sim_Y}.$$

Modulo Arithmetics

Let $p \in \mathbb{N}$. We say that $a, b \in \mathbb{Z}$ are equivalent modulo p if there exists $t \in \mathbb{Z}$ such that $a - b = tp$.

We also write

$$p\mathbb{Z} := \{tp \in \mathbb{Z} \mid t \in \mathbb{Z}\}$$

So $a, b \in \mathbb{Z}$ are equivalent modulo p precisely if $a - b \in p\mathbb{Z}$.

We also $a \sim_p b$ for equivalence modulo p and $[a]_p$ for the equivalence class of $a \in \mathbb{Z}$ modulo p. We write $\mathbb{Z}_p := \mathbb{Z}_{/\sim_p}$.

We conduct arithmetics with equivalence classes modulo p.

Modulo Arithmetics

Let $p \in \mathbb{N}$. We easily check the following:

- Let $a_0, a_1, b_0, b_1 \in \mathbb{Z}$.
  If $a_0 \sim_p a_1$ and $b_0 \sim_p b_1$, then $a_0 + b_0 \sim_p a_1 + b_1$.
- Let $a_0, a_1, b_0, b_1 \in \mathbb{Z}$.
  If $a_0 \sim_p a_1$ and $b_0 \sim_p b_1$, then $a_0 \cdot b_0 \sim_p a_1 \cdot b_1$.

This defines addition $[a]_p + [b]_p = [a + b]_p$ and multiplication $[a]_p \cdot [b]_p = [a \cdot b]_p$ of the equivalence classes modulo p.

- If p is not prime, then there exist $[a]_p, [b]_p \in \mathbb{Z}_p$ with $[a]_p \neq [0]_p \neq [b]_p$ and $[ab]_p = [0]_p$.
- If p is prime and $[a]_p, [b]_p \in \mathbb{Z}_p$ with $[a]_p \neq [0]_p \neq [b]_p$, then $[ab]_p \neq [0]_p$.
- If p is prime and $[a]_p \in \mathbb{Z}_p$ with $[a]_p \neq [0]_p$, then there exists a unique $[b]_p \in \mathbb{Z}_p$ such that $[ab]_p = [1]_p$.