Math 322

rctcwyvrn

August 2020

1 Lecture 1

Definition: Partition

Let X be a set, X_i subsets such that each $x \in X$ is in exactly one X_i (they make a **disjoint union of X**)

- The X_i are then a **partition** of X
- Note: The X_i maybe of differing sizes
- There may also be an infinite number of them

Definition: Equivalence relation

Elements of X are uniquely grouped by which X_i they're in, so we can use this to define an **equivalence relation ($\sim$)** ie: $\alpha \sim \beta$ if they live in the same X_i

Properties

- Reflexive: $x \sim x$ always
- Transitive: $a \sim b$ and $b \sim c$ means $a \sim c$
- Symmetric: $x \sim y$ implies $y \sim x$

Definition: Equivalence classes

Given a partition $\{X_i\}$ of X, you can form a new set whose elements are the sets $X_0, X_1, X_2 \ldots$. This is called $X/\sim$.

Elements of that set are **equivalence classes**

- If $\alpha \in X_i$ then α is called a **representative** of the equivalence class X_i
- Notation: $X_i = [\alpha] = \overline{\alpha}$
- We can also define a **projection** from X to $X/\sim$, which sends α to its equivalence class

$$\pi : X \to X/\sim \quad (1)$$
$$\alpha \mapsto [\alpha] \quad (2)$$

- Sends all the elements of a partition into the one equivalence class

Example: Odds and evens

Let X be the integers, with the partition X_1 evens, X_2 odds then $X/\sim$ is the two element set.

Note: Even though both the odds and the evens have infinite size, the quotient set has only two elements

Example: Integers mod N

Define $x \sim y$ if they have the same remainder mod N.

- N equivalence classes (one for each remainder, $0 \ldots N-1$)
- Notation: $\mathbb{Z}/N\mathbb{Z}$ (reason later (quotient groups)
- If $N = 2$ then it's just the evens and odds example from before
- If $N = 7$ then there's 7 elements,
  the equivalence classes for $0, 1, 2, 3, 4, 5, 6$

Division of integers (in $\mathbb{Z}$) (Some stuff very closely related to math 312, which we aren't going to prove)

- Let a, b integers , $a > 0$
- Then we have $b = qa + r$, $0 < r \leq a - 1$, q integer
- Note: the quotient and remainder are unique
- $a|b \iff r = 0$ divisible iff the remainder is zero
- We get that any integer n is unique defined by the primes that make it up

Lemma:

If a, b have no common factors, then $\exists m, n \in \mathbb{Z} : ma + mb = 1$

- Notation: (a, b): greatest common factor
- Notation: $[a, b]$: least common multiple

Example:

$7, 5$ share no common factors, $m = -2$, $n = 3$, $-14 + 15 = 1$

Remark: Division turns out to generate the basic structural properties of $\mathbb{Z}$

Lemma:

Suppose now that a, b share a gcd d, then $\exists m, n \in \mathbb{Z} : ma + mb = d$. So the earlier lemma is just a special case (when the gcd is 1)

- Note: because d divides both a and b, then it should be able to divide $ma + nb$ for any m, n