Abstract Structures 333

February 24, 2019

1 Equivalence Relations

Definition 1.1. Equivalence Relation
An equivalence relation, denoted by the symbol ˜, on a set S is a set R [1] of ordered pairs (a, b) ∈ S x S such that:

1. (a, a) ∈ R ∀ a ∈ S
2. (a, b) ∈ R implies (b, a) ∈ R ∀ a, b ∈ S
3. (a, b), (b, c) ∈ R implies (a, c) ∈ R ∀ a, b, c ∈ S

We are concerned with **what partition is R imposing on S**

Example 1. Define ℤ in the following way

Fix n ∈ ℤ+

We say a is congruent ≡ to b (mod n) or $a \equiv$ b (mod n) iff n | (a-b)
Show that the example above is an equivalence relation

Solution:

Proof. We must prove the following 3 properties

1. Reflexive [(i) in the def of ER]

   - Thought of as: An element a is always related (˜) to itself.

   We are trying to prove that $a \equiv$ a (mod n). We can start by rewriting this congruence as $n \mid (a - a)$ by def of congruence. This leaves us with $n \mid (0)$ which is true for all $n > 0$. Since n be def is fixed in ℤ+, this congruence will always hold.

2. Symmetric [(ii) in the def of ER]

[1] Need not be unique

- Thought of as: Given (a, b) is valid, we can show (b, c) is valid.

Since we are given (a, b) is valid, we can write $a \equiv \text{b (mod n)}$ or $n \mid (a - b)$. We must show that $b \equiv a(mod n)$ or $n \mid (b - a)$. We can rewrite $n \mid (b - a)$ as $-1 * n \mid (a - b)$. Since we know $n \mid (a - b)$ from out given, we know that this division holds true and therefore $n \mid (b - a)$ as well.

3. Transitive [(iii) in the def of ER]

   - Thought of as: Given $a\tilde{}b$ and $b\tilde{}c$ we must show $a\tilde{}c$.

   We can write the congruence as 2 linear equation.

   - $nk = a - b$
   - $nl = a - c$

   Rearranging we get: $n(k + l) = a - c$ which can be rewritten as $n \mid (a - c)$

□

Now that we have proved that a congruence is an ER on $S = \mathbb{Z}$ we would like to see what affect it has on $\mathbb{Z}$. ie : What is $a\tilde{}b$ / what partition does it impose.

Example 2. Take $n = 5$, given the following values for a which values in $\mathbb{Z}$ satisfy the congruence $a \equiv \text{b (mod n)}$ and is the resulting set equal to $\mathbb{Z}$?

- $a = 0$
- $a = 1$
- $a = 2$

Solution:

- $\{\pm 0, \pm 5, \pm 10 \ldots\}$
- $\{\pm 1, \pm 6, \pm 5k + 1 \ldots\}$
- $\{\pm 2, \pm 7, \pm 5k + 2 \ldots\}$

No sets equal $\mathbb{Z}$

We can see that it appears that a congruence will always split the set $\mathbb{Z}$ into n partitions.

Definition 1.2. Partition of a set
A partition of a set S is a collection of **non-empty, disjoint** subsets $\{s_0, s_1, \ldots\}$ such that (st) $\bigcup_{i=1}^{\infty} S_i = S$

Theorem 1. *The equivalence classes of a set S under ˜form a partition of S*

Proof. We need to show that given ˜, we are left with a collection of **disjoint** subsets who's union is S.
Let a ˜S. We know a is in its own set because a ˜a. So ∀ a ∈ S the set containing a is **non-empty**. If we do this for all a ∈ S then the union of those sets is S. So we need only show that these sets are **disjoint**. □

Example 3. Let S = $\mathbb{Z}x\mathbb{Z}$ [(a, b) a,b ∈ $\mathbb{Z}$] Define ˜ on S by (a, b) ˜ (c, d) iff ad = bc

1. Prove ˜ is an ER
2. What partition of $\mathbb{R}x\mathbb{R}$ does this impose

Solution:

Proof. If ER, 3 properties must hold:

1. Reflexive: (a, b) ˜ (a, b) $\Longrightarrow$ ab = ab which is true.
2. Symmetric: Given (a, b) ˜ (c, d) we can show (c, d) ˜ (a, b). (a, b) ˜ (c, d) $\Longrightarrow$ ad = bc, (c, d) ˜ (a, b) $\Longrightarrow$ cb = da. Since we are in the realm of $\mathbb{R}$ we can rearrange to bc = ad which is equal to ad = bc.
3. Transitive: We must show that if (a, b) ˜ (c, d) and (c, d) ˜ (e, f) then (a, b) ˜ (e, f). We can write it as follows ad = bc and cf = de the af = be. We can write

$$adcf = bcde$$
$$ace = bce$$
$$af = be$$

To find the partition we may start by plugging in random values.

$$(1,1)$$
$$1d = 1c$$
$$d = c$$
$$= \{(1,1),(2,2),\ldots,(n,n)\}$$

$$(1,2)$$
$$d = 2c$$
$$= \{(1,2),(2,4),\ldots,(n,2n)\}$$
$$\vdots$$
$$\infty$$

This partition forms all rational numbers. The first set represents $\frac{1}{1}$ or 1, the second represents $\frac{1}{2}$ ... ∞ $\square$

Example 4. Let S = $\mathbb{R} - \{0\}$
Define a $\tilde{} b \leftrightarrow ab > 0$
What partition does that make on $\mathbb{R}$

Solution:
By plugging in we see we get 2 sets.

1. {1, 2, ..., n} = All positive integers
2. {-n, -n-1, ..., -1} = All negative integers

Theorem 2. *Division Algorithm*
Let $D \in \mathbb{Z}+$, $a \in \mathbb{Z}$, $\exists! q$, r *s.t.* $a = dq + r$ *when* $0 < r \leq d$

Example 5. a = 100, d = 7

Solution:

$$\begin{aligned} 100 &= 7q + r = 7(14) + 2 \\ 7 &= 2q + r = 2(3) + 1 \\ 2 &= 1q + r = 1(2) + 0 \end{aligned}$$

So, 1 would be the GCD.

2 Chapter 1: Groups

Definition 2.1. Binary Operation We define a binary operation on set S is a function from SxS $\longrightarrow$ S
ie: Takes a pair of elements in S and sends them to another element in S

Example 6. Let S = $\mathbb{Z}$, with bin-op (+)
a + b = c
3 + 5 = 8
$3 \in \mathbb{Z}$, $5 \in \mathbb{Z}$, $8 \in \mathbb{Z}$.

Definition 2.2. Let S be a set w/ bin-op $*$[2]
If $\forall$ a, b $\in$ S, a + b $\in$ S we say S is closed (under $*$)

Example 7.
$(M_{22}, \cdot)$ is closed
$(\mathbb{R}, \div)$ is not closed

[2] $*$ denotes any bin-op

Definition 2.3. Let G be a set closed under bin-op * G is a group if the following hold:

1. Associative: $\forall$ a, b, c $\in$ G we have $(a*b)*c = a*(b*c)$
2. $\exists$ an Identity in G s.t. $\forall$ a $\in$ G we have $(e*a) = (a*e) = a$
3. ($\forall$ a $\in$ G)$\exists a^{-1}$ s.t. $a*a\prime = a^{-1}*a = e$

Example 8. $\mathbb{Z}_n$ = the group {0, 1, 2, ..., n-1} under addition mod n.
What is addition mod n?

For a, b $\in \mathbb{Z}_n$:
if $a+b<n$, $a+b=a+b$
if $a+b \geq n$, $a+b=a+b-n$

1. Associative: We are dealing with integers so associativity holds.
2. $\exists$ an Identity: The identity is 0 ($e=0$)
3. ($\forall$ a $\in$ G)$\exists a^{-1}$: The inverse is $n-a$

2.0.0.1 Common Groups

- ($\mathbb{Z}$, +)
- ($\mathbb{R}$, +)
- ($\mathbb{C}$, +)
- (GL_{2R}, *)

Proof. of (GL_{2R}, *)
We know from linear algebra that $det(AB) = det(A)det(B)$
We also know that the identity 2x2 matrix is

$$M_{2x2} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Additionally, we are able to inherit associativity from general matrices. This leaves inverse.
We prove inverse as follows:

$$A^{-1} = \frac{1}{det(A)} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

□

Definition 2.4. Order of a group
The order of a group, G, denoted $|G|$ is the number of elements in G as a set
If set G has a finite number of elements we say G is a finite group. If G has an infinite number of elements we say G is an infinite group.

Definition 2.5. Abelian Groups
If a group is commutative, we say it is Abelian. If not, we say its not-Abelian

Definition 2.6. Cayley Table
A cayley table is a way to describe the structure of a finite group.
Properties that may be derived from a cayley table are:

- If the table is reflect-able, the group is Abelian
- Every element appears in each row/column
- Easily find the identity (The row/column which entries is equal to the input)

Example 9. Write the Cayley Table for $\mathbb{Z}_3$

$\mathbb{Z}_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Example 10. Write the Cayley Table for $|G| = 3$

$\|G\| = 3$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Notice that this the second table above was forced. Meaning, no other configuration of e, a, b could have been entered into the table and the table maintain all group properties.

We see from this that there is only 1 group with order 3. Even though we may label that group with different elements, the underlying groups are all the same.

Claim 2.1. *$\exists!$ 2 groups of order 4 ($|G| = 4$)*

$\mathbb{Z}_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\mathbb{Z}_{2x2}$	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

Any other groups of order 4 will have a bijection to either $\mathbb{Z}_4$ or $\mathbb{Z}_{2x2}$
Here is an example of one of those:

Example 11. Let G = {1, -1, i, -i} under *

$\mathbb{G}_4$	1	-1	i	-i
1	1	-1	i	$-i$ l
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Claim 2.2. *If groups are structurally identical, then, you can find a bijection* $\phi(G_1) = G_2$

Definition 2.7. Order of an element
Let G be a group with g $\in G$. The order of g (referred to as the order of the element) is the smallest positive integer n s.t. $g^n = e$ where e is the identify element of G.

Definition 2.8. Cyclic Group
Let G be a group with order n. We say G is cyclic if $\exists g \in G$ s.t $|g| = n$

Theorem 3. *Let* $a \in \mathbb{Z}_n$, *then* $|a| = \frac{n}{(a,n)}$

Proof. $|a|$ is the smallest positive integer k s.t. $ka \equiv 0(n)$
i.e $ln - ka = 0$
Solve for k using linear diophantine equation

Claim 2.3. Z_n *is a cyclic group*

Proof. We know $\mathbb{Z}_n$ is cyclic if $\exists$ some a s.t. $|a| = n$ where $n = |G|$ by the proof above (Them. 3), $|a| = \frac{n}{(a,n)} \therefore (a, n) = 1$. To prove that $\mathbb{Z}_n$ is cyclic we must show that $\exists$ an a such that $(a, n) = 1$
We will choose $n - 1$ as our a giving us $(n - 1, n) = 1$ which is always true □

Definition 2.9. Group Generator
Let G be a cyclic group of order n.
If a has order n, we call a a generator of G and we write $< a >= G$. We say "the group generated by a"