MATH 335 Lecutre 9

Chris Camano: ccamano@sfsu.edu

September 20, 2022

Definition 1. : A group G is a non empty set with a binary operation $G \times G :\mapsto G \quad (a,b) \in G^2 \mapsto ab$ A bianry operation must satisfy the three following properties:

1. Associativity:

$$a(bc) = (ab)c \quad \forall a,b,c \in G$$

   The purpose of this property is to give access to statements such as abc without concern for ordering in operation composition

2. The existence of the identity element e in G
   Such that:

$$ae = ea = a \quad \forall a,e \in G$$

3. For all elements in G there exists an inverse uder the bianry oepration such that :

$$a(a^{-1}) = (a^{-1})a = e$$

Common Examples:
Let G=$\{\mathbb{Z},+\}$ This group has an identity element, inverse and Associativity over addition.
Let G=$\{\mathbb{R}/\{0\},\cdot\}$: Associativity over multiplication, idenity over 1, inverse would be the reciprocal of any element inG A new important Group
Let $n \in \mathbb{Z}^+$ Recall the equivilance realation on $\mathbb{Z}$ defined by:

$$a \sim b \to n|a-b$$

or rather:

$$a \equiv b \mod n$$

The set of equivilance classes of this equivilance relation is denoted as: $\mathbb{Z}_n$

$$\mathbb{Z}_n = \{[0],[1],[2],[3],...,[n-1]\}$$

$$|\mathbb{Z}_n| = n$$

We define the following binary operation on $\mathbb{Z}_n$: We cal this operation addition modulo n:

$$[a] \circ [b] := [(a+b) \mod n]$$

with addition we then say:

$$[a \mod n] \mathbf{+} [b \mod n] := [(a+b) \mod n]$$

Definition 2. Well defined: Does it depend on the names of the objects being related.

Proof of well definition of operation of equivilance class addition:
Suppose:

$$[a] = [a^*], [b] = [b^*]$$

We wish to show that :

$$[a] + [b] = [a^*] + [b^*]$$

$[a] = [a^*] arrow n | a - a^*, [b] = [b^*] \to n | b - b^*$

$$[a] + [b] = [a^*] + [b^*]$$

$$[a+b] = [a^* + b^*]$$

We need to show now that:

$$n | a + b - a^* + b^*$$

$$n | [a+b] - [a^* + b^*]$$
$$n | a - a^* + b - b^*$$
$$n | n(k) + n(l), k, l \in \mathbb{Z}$$
$$n | n(k+l)$$

We now prove this is a group

1. $$[a] + ([b] + [c]) = ([a] + [b]) + [c]$$
   $$[a] + ([b+c]) = ([a+b]) + [c]$$
   $$[a + (b+c)] = [(a+b) + c]$$
   $$[a+b+c] = [a+b+c]$$

2. Identity element [0]

3. Inverse : [n-a]$\sim [-a]$

   So we have proven that $\mathbb{Z}_n$ under addition is a group.

Definition 3. A group G is called abelian or ”commutative” if the binary operation on the group does not depend on the order of the operands. This is to say:

$$ab = ba \quad \forall a, b \in G$$