Abstract Algebra I

David Cardozo

Nombre del curso: Abstract Algebra I
Código del curso: MATE2101
Unidad académica: Departamento de Matemáticas
Periodo académico: 201510
Horario: Ma y Vi, 2:00 a 3:50

Nombre profesor(a) principal: Mehdi Garrousian
Horario y lugar de atención: Mo y 17:00 a 18:00, Office H-409

---

1 Organization of the course

- 5 Homework 15 /
- Quizzes 10 /
- Exam
- Parciales 35 %

We will cover Chapter 1-9 skiping 6, which will include

---

2 Introduction

We begin with section 0.3, let us consider the following quotient group, let n be a fixed integer $\frac{\mathbb{Z}}{n\mathbb{Z}}$ which is described better as:

- $a \iff n|(a-b)$ in better notation $a \equiv b \mod n$

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\bar{0} ... \bar{n-1}\}$$

Prove:

$$\bar{a} + \bar{b} = \bar{a+b} \quad \bar{a}\bar{b} = \bar{ab}$$

Check that this is well defined. The strategy is to use that if $\bar{a} = \bar{a}$ and $\bar{b} = \bar{b'}$ and it should imply that $\bar{ab} = \bar{a'b'}$

Example 1.

$$\bar{2}x = \bar{1} \mod 6$$
$$\bar{2}x = \bar{1} \mod 5$$

Observe that we can use a force-brute approach to solve each equation, and we see that the first one is not solvable, meanwhile the second is by $\bar{3}$. we now denote

$$\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^x = \{\text{ Elements with a multiplicative inverse}\}$$

for example

$$\bar{2} \in (\frac{\mathbb{Z}}{n\mathbb{Z}})^x \text{for n} = 5$$

Theorem 1. *The above group is given by* $\left\{\bar{a} \in (\frac{\mathbb{Z}}{n\mathbb{Z}})^x : (a,n) = 1\right\}$

Proof. Observe $(a,b) = \min\{ax + by > 0 : x, y \in \mathbb{Z}\}$ if we supoose $(a,n) = 1 \implies \exists x, y \in Z$ □

Example 2. *Compute the remainder of* 37^{1000} *in division by 29. Let us observe then* $|\frac{\mathbb{Z}}{n\mathbb{Z}}^x| = \phi(n)$*, and the properties of* ϕ *to calculate we use the prime decomposition. to solve the above problem we use Fermat little theorem.*

$$a^{p-1} \equiv 1 \mod p$$

.

3 Basic Axioms

Definition 1. *A binary* ***opertion*** $*$ *on a set* G *is a function:*

$$* : G \times G \to G$$

, $*(a,b) = a * b$ *which if it has the following properties:*

- $*$ *is associative, i.e*
- $*$ *is Abelian or commutative, i.e*

Example 3. *Observe that the following sets are group* $(R,+)$, $(R,\cdot)$. *The dot product fails since it is not an operation.*

Definition 2. *A group is an ordered pair* $(G,*)$ *set with a binary operation such that the following properties hold:*

- $*$ *is associative*
- $\exists e \in G \forall g \in G g * e = g = e * g$
- $\forall a \in G \exists b \in G$ *s.t* $a * b = b * a = e$

G is abelian if $*$ is abelian.

Example 4. $(\mathbb{R}, +), (\mathbb{C}^x, \cdot)$, $(M_{\mathbb{R}}(2,2), \cdot)$*is not associative,* $, GL_n(\mathbb{R}),$, $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +)$

So it is clear that it depends on the ground set and the operation.

Example 5. *If $(A, *)$ and $(B, \diamond)$ are groups thenn $A \times B$ has a natural group structure. Note: Prove that the operations hold the properties.*

Theorem 2. *If G is a group under $*$, then:*

- *the identity is unique*
- *a^{-1} is unique for every a*
- $(a^{-1})^{-1} = a$
- $(a * b)^{-1} = a^{-1} * b^{-1}$
- *for any $a_1, a_2, \ldots, a_n \in G$, $a_1 * \ldots a_n$ is well-defined*

Proof. Assume we have e and e' as identity, so that $e' * e = e'$ and because e' is an identity $e' = e' * e = e$. Note: Write number 2. Let b, b' be inverses of a, $b = be = b(ab')$, then by associativity $(ba)b' = eb' = b'$. Note: For five use induction □

Remark: Mathematics on a different planet

Proposition 1. *Let G be a group and $a, b \in G$. The equations $ax = b$ and $ya = b$ has unique solutions.*

Proof. Prove it! you will need left and right cancellation. □

Example 6. ***No cancelation*** $\bar{2}\bar{3} = \bar{0} \mod 6$, *observe that $\frac{Z}{6Z}$is not a group*

Definition 3. *The order of $x \in G$ is the least positive integer n such that $x^n = e$ and is denoted by (x). if there's no such n then $(x) = \infty$.*

Example 7. *Order of $\bar{2}$ is 5 in $(\frac{\mathbb{Z}}{5\mathbb{Z}}, +)$ where $e = 0$, Order of $\bar{2}$ in $((\frac{\mathbb{Z}}{5\mathbb{Z}})^x, \cdot)$.*