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 $a \equiv b \mod n$

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

Prove:

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

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 $a\bar{b} = a'\bar{b}'$

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 $a_1,a_2,\dots,a_n\in G$, $a_1*\dots a_n$ 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 $((\frac{\mathbb{Z}}{5\mathbb{Z}})^x,\cdot)$.*

---

4 Dihedral Group

Geometric Group.

$$D_{2n}=\{\text{the group of symmetries of the ngon}\}$$

$$|D_{2n}=2n|$$

elements: n rotations through $\theta=0,\frac{2\pi}{n},2\frac{2\pi}{n},...,(n-1)\frac{2\pi}{n}$ and n more which are reflections thorough vertices. and n reflections thoriugh edges. Rotations through $\frac{2\pi}{n}=r$, there are n, and let s, .. $|s|=n$. and $s\neq r^i$ for any i.

- $s \neq r^j$ for any j.
- $sr^i \neq s^j$ for all $0 \leq i \neq j \leq n-1$
- $rs = sr^{-1}$, more generally
- $r^i s = sr^{-i}$ for $0 \leq i \leq n$

Definition 4. *$S \subset G$, the subgroup generated by S, denoted $< S >=$ the smallest subgroup containing S.And formall $\bigcap_{S \subset H \ subgroup} H$ which is the collection all finite products and inverse of elements of S*

Example 8. *$< r >$ in D_{2n} is $\left\{r^i : i\right\}$ which is exactly $\frac{Z}{2Z}$, meanwhile $< s >= \frac{Z}{2Z}$ which $< r, s >= D_{2n}$*

Any equation that the generators satisfy is called a **relation**
Notation Presentation with generators and relations.

$$G =< S|R_1, \dots R_m$$

Example 9.

$$D_{2n} =< r, s|r^n = s^2 = 1, rs = sr^{-1} >$$

Example 10. *Symmetries of a regular tetrahedron $= 12$*

5 Symmetric Group

Let Ω be a set then S_Ω be the set of bijection from $\Omega \to \Omega$:

$$S_\Omega = \{\sigma : \sigma : \Omega \to \Omega\}$$

$$\begin{aligned} \Omega = [n] = \{1, 2, ...n\} \\ S_n := S_{[n]}\text{cycle} \quad (a_1 \to a_2 \dots ...a_m) \in S_n \\ \text{otherwise} \end{aligned}$$

We define elements $(ij)^{-1} = (ij)\ (ijk) = (jki)$. we observe $|S_n| = n!$

Example 11. *$|S_3| = 6$ and S_3 is not abelian. S_n $n \geq 3$ is nonabelian.*

Disjoint cycles commute, **rearranging the elements inside a cycle doesnt change it**

Matrix Group

Definition 5. *A **field** is the smallest math structure in which we can perform addition, and multiplication and division by nonzero element. To be more precise, a field F is a set with two operations $+$ and $\times$, such that:*

- $a \cdot (b + c) = a \cdot b + a \cdot c$
- $F^{\times} = F - \{0\}$ *all nonzero elements are invertible.*

Given any field F, we can construct $\mathrm{GL_n}(F)$ this is the group of all the invertible matrices over F. to do: How many elements do we have in $|GL_n|\,(F_p)$ for case 2 $(p^2 - 1)(p^2 - p)$

Recall that in the last class we saw that $G \circlearrowright A$ which takes $g \in G$ to σg a permutation for $a \in A$ $\sigma_g(a) = g \cdot a$. observe that we define:

Definition 6.

$$\begin{aligned} \mathrm{Kernel}(\phi) &= \left\{ g \in G | \sigma_g = \mathrm{id}_(A) \right\} \\ &= \{ g \in G | g \cdot a = a \textit{for all } a \in A \} \end{aligned}$$

is a subgroup.

Example 12. *Observe $G \circlearrowright G$ any groups acts on itself.*

Example 13. *V a vector space over F, $F - \{0\} = F^x \circlearrowright V$ by scalar multiplication*

Example 14. *$D_{2n} \circlearrowright [n] = \{1, \dots n\}$ so that $D_{2n} \to S_n$*

So observe that for $n = 3$ we have that $D_6 \to S_3$, we observe that this is an isomorphism (it just need to satisfy injectivity since it has the same elements).

6 Subgroups

Exercises to be done: 3,9,12,15,17

Definition 7. *Let G be a nonempty group. A subset H of G is a subgroup (denoted $H \leq G$), if H is closed under multiplications and inverses, more formally: $x, y \in H, x^{-1} \in H, \forall x, y \in H$*

Example 15. *$2\mathbb{Z} \leq \mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C} \leq \ldots$ with addition, and observe that $(\mathbb{Q}^x, \cdot) \not\leq (\mathbb{R}, +)$ since zero is not there*

Proposition 2. *$H \subseteq G$, then $H \leq G$ if and only if :*

1. *$H \neq \varnothing$*
2. *$\forall x, y \in H \quad xy^{-1} \in H$*

Proof. By condition 1, $x \in H$, so, by (2) $e = xx^{-1} \in H$. Use (2), let $x = e$, $\forall y (y \in H \implies y^{-1} \in H)$ $\square$

Exercise 6 G abelian torsion subgroup, $\mathrm{tor}(G) = \{g \in G | \, |g| < \infty\}$ Observe it is not empty, we find that $\mathrm{tor}(G)$ is not empty. and we prove that in general, $|g| = \left|g^{-1}\right|$.

$$\begin{aligned} g^n = e &\iff g^{-n} = e \\ &(g^{-1})^n = e \end{aligned}$$

Example $\mathrm{GL}_2(\mathbb{R})$, the $\mathrm{Tor}\,\mathrm{Gl}_2(\mathbb{R})$ is not a subgroup.

centralizers and normalizers

Definition 8. *Let $A \subseteq_{subset} G$. The centralizer of A in G is $C_G(A) = \left\{g \in G | gag^{-1} = a \quad \forall a \in A\right\}$*

$$gag^{-1} = a \iff ga = ag$$

this is the set of all elements that commute with all elements of A

Example 16. *$A = \{e\} \implies C_G(A) = G$, another **example** can be $r \notin C_D(\{s\}) but \quad s \in C_{D_{2n}}(\{s\})$.*

Show that $C_G(A)$ is a subgroup.

Proof.

$$g \in C_G(A) \xrightarrow{?} g^{-1} \in C_G(A)$$

ang we can observe that $gag^{-1} = a \implies a = g^{-1}ag$ □

Notation if $A = \{a\} \implies$ we write $C_g(a)$ **Examples** $C_{Q_8}(i) = \{\pm 1, \pm i\}$

Semidirect products

Setup $H, K < G$ with:

$$H \triangleleft$$