

## **MA672 - (Topics) Number Theory and Cryptography**

JIAHUA CHEN

Spring 2020

These are the course notes for Topics in Advanced Mathematics (**MA672**) at Hotchkiss taught by Dr. Weiss. These notes were last updated January 12, 2020. Any sections denoted with asterisks (\*\*\*) are currently incomplete, and I will update them when I get to those.

**Contents**

**1 Groups** **3**

1.1 Group Homomorphisms . . . . . 10

January 7, 2020

## Course Overview

- Abstract algebra: groups, rings, fields.
- Number Theory, arbitrary precision integer arithmetics.
- Cryptographic algorithms

## 1 Groups

We first define the group, which we will be using extensively.

**Definition 1.1. (Group).** A group is a set  $G$  with a binary operation “ $\circ$ ” such that

- $G$  is closed under  $\circ$ .
- $G$  is associative.
- There is an Identity Element:  $\exists e \in G \mid x \circ e = e \circ x = x \ \forall x \in G$ .
- Inverses:  $\forall x \in G \exists y \in G \mid x \circ y = y \circ x = e$ .

**Definition 1.2. (Abelian Group).** If  $\circ$  is commutative in group  $G$ , we call  $G$  Abelian. In that case,  $G$  is often written additively; i.e. we use “ $+$ ” for “ $\circ$ ”.

(If  $\circ$  is not commutative, we often write  $G$  multiplicatively.)

**Definition 1.3. (Subgroup).** Let  $G$  be a group, and  $\emptyset \neq H \subseteq G$ . Then  $H$  is called a subgroup of  $G$  if  $H$  is also a group.

A small proof to begin. . .

**Proposition 1.4.** Let  $G$  be a group and  $x \in G$ . Then  $x$  has a unique inverse  $y$ , so we can write  $y = x^{-1}$ .

*Proof.* Assume  $y$  and  $z$  are both inverses of  $x$ .

$$y = y \circ (x \circ z) = (y \circ x) \circ z = z$$

□

**Proposition 1.5.** A non-empty subset  $H \subseteq G$  is a subgroup of  $G$  iff  $xy^{-1} \in H \ \forall x, y \in H$ .

*Proof.* ( $\Rightarrow$ )

- Identity: Pick  $x \in H$ . Then  $xx^{-1} = e \in H$ .
- Inverse: If  $y \in H$ ,  $ey^{-1} = y^{-1} \in H$

- Closure: If  $x, y \in H$ ,  $y^{-1} \in H$ , so  $x(y^{-1})^{-1} = xy \in H$ .
- ( $\Leftarrow$ ) If  $H$  is a group, then  $y^{-1} \in H$  (existence of unverse) and  $xy^{-1} \in H$  (closure of  $\circ$ ).  $\square$

**Example:**

- Every vector space (without the scalars) is an Abelian group with identity  $\vec{0}$ .
- Modular arithmetic:

$$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$$

$\mathbb{Z}_n$  is an Abelian group under modular addition.

$$\mathbb{Z}_n^* = \{k \in \mathbb{Z}_n \mid \gcd(k, n) = 1\}$$

$\mathbb{Z}_n^*$  is an Abelian group under modular multiplication (this is sometimes also  $\mathbb{U}_n$ ).

Let's take  $\mathbb{Z}_4 - \{0\}$  and why it's not a group under multiplication. We can create a multiplication table:

$\circ$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

However there is no such problem with  $\mathbb{Z}_4^*$ :

$\circ$	1	3
1	1	3
3	3	1

**Definition 1.6. (Cyclic).** A group  $G$  is called cyclic if  $\exists g \in G$  (called generator) such that  $G = \{g^n \mid n \in \mathbb{Z}\}$ .

**Example:**  $\mathbb{Z}_n$  are cyclic groups with generator 1.

$\mathbb{Z}_4^*$  is cyclic with generator 3.

**Example:** The Klein 4-group is not cyclic:

$$K = \{(0, 0), (1, 0), (0, 1), (1, 1)\}$$

with componentwise addition mod 2.

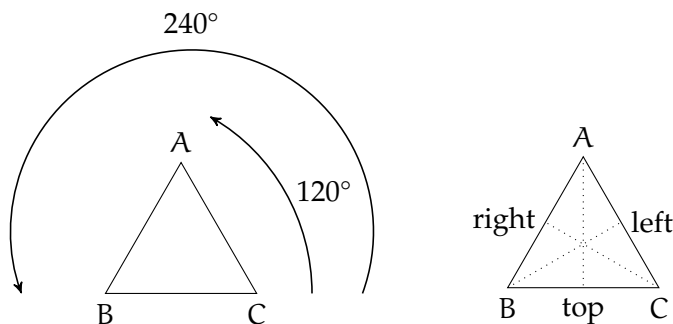
$$K = \mathbb{Z}_2 \oplus \mathbb{Z}_2 = \{(k, l) \mid k \in \mathbb{Z}_2, l \in \mathbb{Z}_2\}$$

**Proposition 1.7.** Every cyclic group is Abelian.

*Proof.* Let  $x, y \in G$ , a cyclic Abelian group. Let  $g$  be the generator in  $G$ . We write  $x = g^a$  and  $y = g^b$ . Then  $xy = g^a g^b = \underbrace{g \circ g \circ \dots \circ g}_{k+l \text{ times}} = g^b g^a = yx$ .  $\square$

**Example:** The symmetry transformation of an equilateral  $\triangle$  form a group under composition.

$$D_3 = \{\text{id}, 120^\circ, 240^\circ, \text{top}, \text{left}, \text{right}\}$$



$\circ$	id	$120^\circ$	$240^\circ$	top	left	right
id	id	$120^\circ$	$240^\circ$	top	left	right
$120^\circ$	$120^\circ$	$240^\circ$	id	left	right	top
$240^\circ$	$240^\circ$	id	$120^\circ$	right	top	left
top	top	right	left	id	$240^\circ$	$120^\circ$
left	left	top	right	$120^\circ$	id	$240^\circ$
right	right	left	top	$240^\circ$	$120^\circ$	id

**Definition 1.8. (Equivalence).** Let  $G$  be a group and  $H$  a subgroup. Define the relation  $x \sim y$  if  $xy^{-1} \in H$ .

**Proposition 1.9.**  $\sim$  is an equivalence relation on  $G$ .

If  $H = \{e\}$ , then  $\sim$  is  $=$ .

If  $H = G$ , then  $\sim$  is trivial.

*Proof.* We need to show that  $\sim$  is

- reflexive:  $x \sim x$  for all  $x \in G$

$$xx^{-1} = e \in H.$$

- symmetric:  $x \sim y \iff y \sim x$  for all  $x, y \in G$

Suppose  $x \sim y$ . Then  $xy^{-1} \in H$ . So  $(xy^{-1})^{-1} = yx^{-1} \in H \Rightarrow y \sim x$ .

- transitive: If  $x \sim y, y \sim z$  then  $x \sim z$  for all  $x, y, z \in G$ .

Suppose  $x \sim y, y \sim z$ . Then  $xy^{-1} \in H, yz^{-1} \in H$ . Then  $(xy^{-1})(yz^{-1}) = x(y^{-1}y)z^{-1} = xz^{-1} \in H \Rightarrow x \sim z$ .

□

If  $\sim$  is an equivalence relation on any set  $X$ , then  $\sim$  partitions  $X$  into equivalence classes: If  $y \in X$ ,  $[y] = \{x \in X \mid x \sim y\}$ .

Every element of  $X$  is in some equivalence class because  $\sim$  is reflexive and no two equivalence classes intersect. Consider  $[y_1], [y_2]$  and  $z \in [y_1] \cap [y_2]$ . Then  $z \sim y_1$  and  $z \sim y_2$  and  $y_1 \sim y_2$ . Hence,  $[y_1] = [y_2]$ .

**Theorem 1.10. (Lagrange's Theorem).** Let  $G$  be a finite group of order  $|G|$  and  $H$  a subgroup of  $G$ . Then  $|H|$  divides  $|G|$ .

*Proof.* We show that the above equivalence relation partitions  $G$  into equivalence classes of equal cardinality.

First, notice that  $H$  is an equivalence class by itself:  $H = [e]$ .

Let  $[x]$  be another equivalence class. Then  $[x] = Hx$ : Let  $y \in Hx$ . Then  $\exists a \in H$  such that  $y = ax$ . Then  $\exists a \in H$  such that  $y = ax$ . But then  $yx^{-1} = (ax)x^{-1} = a \in H$ , so  $y \sim x$ .

We need to find a bijection between  $H$  and  $Hx$  for  $x \in G$ . Let  $f : H \rightarrow Hx$ ,  $f(a) = ax$ . We need to show that  $f$  is one-to-one and onto:

$$\begin{aligned} \text{1-1: If } f(a_1) &= f(a_2) \\ a_1x &= a_2x \\ a_1xx^{-1} &= a_2xx^{-1} \\ a_1 &= a_2. \end{aligned}$$

Onto: Let  $y \in Hx$ . Then  $\exists a \mid y = ax \Rightarrow y = f(a)$ .

$\Rightarrow H \simeq Hx \Rightarrow$  they have the same cardinality.

□

**Definition 1.11. (Index).**  $[G : H]$  is the number of equivalence relations, which is called the index of  $H$  in  $G$ .

$$[G : H] = \frac{|G|}{|H|}.$$

January 9, 2020

## Quick Summary

We were talking about groups, which are

- associative,
- have an identity element,
- and have inverses.

There can be subgroups in groups, a subset of a group that is also a group.

An Abelian group is a commutative group.

A cyclic group is generated by an element  $g$ , they're always Abelian.

Lagrange's Theorem: the order of a subgroup divides the order of the group.

Index of  $H$  in  $G$ :  $[G : H] = \frac{|G|}{|H|}$ .

**Example:**

- $(\mathbb{R}^n, +), (\mathbb{C}^n, +)$ .
- $(\mathbb{Z}_n, +), (\mathbb{Z}_n^*, \cdot), (\mathbb{R}, +), (\mathbb{R}^*, \cdot), (\mathbb{C}, +), (\mathbb{C}^*, \cdot)$ .
- $GL_n(\mathbb{R})$ : Invertible  $n \times n$  matrices.
- $SL_n(\mathbb{R})$ : Subgroup of  $GL_n(\mathbb{R})$  with determinant 1.
- $GL_n(\mathbb{C})$ : Invertible  $n \times n$  complex matrices.
- $U(n)$ : Unitary group – determinant of absolute value 1.
- Symmetry groups of geometric shapes. (Dihedral groups)
- Frieze groups.
- Wallpaper groups.
- Crystallographic groups.
- Permutation groups of  $\{1, \dots, n\}$  under composition ( $S_n$ ), and its subgroups.

We will be focusing mainly on  $(\mathbb{Z}_n, +), (\mathbb{Z}_n^*, \cdot)$ .

**Definition 1.12. (Order of an element).** Let  $G$  be a group and  $g \in G$ . Then the order of  $o(g)$  is the smallest positive integer  $n$  such that  $g^n = e$ . (May be infinite)

**Proposition 1.13.** Every group of prime order is cyclic.

*Proof.* Let  $e \neq g \in G$ . Consider the subgroup  $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$  generated by  $g$ . Then  $|\langle g \rangle|$  divides  $|G|$ , which is prime. Hence  $\langle g \rangle = G$ .  $\square$

**Exercise 1.** Show that  $\{(1), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$  is a subgroup of  $S_4$ .

*Proof.* We can construct a Cayley table for the subgroup. (Top row is evaluated first).

$\circ$	(1)	(1, 2)(3, 4)	(1, 3)(2, 4)	(1, 4)(2, 3)
(1)	(1)	(1, 2)(3, 4)	(1, 3)(2, 4)	(1, 4)(2, 3)
(1, 2)(3, 4)	(1, 2)(3, 4)	(1)	(1, 4)(2, 3)	(1, 3)(2, 4)
(1, 3)(2, 4)	(1, 3)(2, 4)	(1, 4)(2, 3)	(1)	(1, 2)(3, 4)
(1, 4)(2, 3)	(1, 4)(2, 3)	(1, 3)(2, 4)	(1, 2)(3, 4)	(1)

Every element is its own inverse, and (1) is the identity element. It is evident from the table that we also have closure. Hence, the set is a valid subgroup under composition.  $\square$

**Exercise 2.** Let  $G$  be an Abelian group. Show that the set of all elements of  $G$  of finite order forms a subgroup of  $G$ .

*Proof.* Let  $H$  be the subset of  $G$  with elements of finite order. We want to show that  $\forall x, y \in H, xy^{-1} \in H$ . In other words,  $xy^{-1}$  also has finite order. Well,  $xy^{-1}$  has order at most  $k = \text{lcm}(o(x), o(y))$  such that

$$\begin{aligned}(xy^{-1})^k &= x^k(y^{-1})^k \\ &= x^k(y^k)^{-1} \\ &= e \cdot e^{-1} \\ &= e\end{aligned}$$

Thus,  $H$  is a subgroup of  $G$ .  $\square$

**Exercise 3.** Let  $G$  be a group. Define the set  $Z(G) = \{x \in G \mid xg = gx \text{ for all } g \in G\}$  of all elements that commute with every other element of  $G$  is called the center of  $G$ .

- (a) Show that  $Z(G)$  is a subgroup of  $G$ .
- (b) Show that  $Z(G) = \cap_{a \in G} C(a)$ .
- (c) Compute the center of  $S_3$ .

*Proof.* (a)  $e$  by definition commutes with every other element.  $\forall x, y \in Z(G), xy \in Z(G)$  as  $x, y$  commutes with every element.

$$(xy)a = x(ya) = x(ay) = (ax)y = a(xy)$$

Inverses also exist as

$$x^{-1}a = (a^{-1}x)^{-1} = (xa^{-1})^{-1} = ax^{-1}$$

- (b) If an element is in the intersection of all those sets, then it commutes with every element.
- (c) Realize this is simply  $D_3$ , where only the identity commutes with one another. *Answer:*

$$\boxed{\{e\}}$$

$\square$



January 10, 2020

**Exercise 4.** Show that a non-Abelian group must have at least five distinct elements.

*Proof.* 1 element is trivial. 2 and 3 are primes so all groups of order 2 or 3 are cyclic. So we turn to groups of order 4. Every element cannot have order 1, and shown previously the orders have to divide 4. Additionally, if an element has order 4, then it is a generator and the group is cyclic. So all non-trivial elements must have order 2. We can construct a Cayley table for this specific group.

$\circ$	$e$	$a$	$b$	$c$
$e$	$e$	$a$	$b$	$c$
$a$	$a$	$e$	$c$	$b$
$b$	$b$	$c$	$e$	$a$
$c$	$c$	$b$	$a$	$e$

Which gives us an Abelian group. □

**Exercise 5.** Let  $G$  be a group. Prove that  $(ab)^n = a^n b^n$  for all  $a, b \in G$  and all  $n \in \mathbb{Z}$  if and only if  $G$  is Abelian.

*Proof.* The left implication is trivial (rearrange). We focus on the right implication.

We let  $n = 2$ . Then

$$\begin{aligned}
 (ab)^2 &= a^2 b^2 \\
 abab &= aabb \\
 a^{-1}bab b^{-1} &= a^{-1}aabb b^{-1} \\
 ba &= ab
 \end{aligned}$$

For all  $a, b \in G$ . □

**Exercise 6.** Let  $G$  be a group. Prove that  $G$  is Abelian if and only if  $(ab)^{-1} = a^{-1}b^{-1}$  for all  $a, b \in G$ .

*Proof.*

$$\begin{aligned}
 (ab)^{-1} &= a^{-1}b^{-1} \\
 (b^{-1}a^{-1})^{-1} &= (a^{-1}b^{-1})^{-1} \\
 ab &= ba
 \end{aligned}$$

We can travel in both directions in this proof. □

**Exercise 7.** Let  $G$  be a group. Prove that if  $x^2 = e$  for all  $x \in G$ , then  $G$  is Abelian.

*Proof.* We use the fact that  $x^{-1} = e$  for all  $x \in G$ . Then we use the conclusion arrived at Exercise 6 to our advantage.

$$\begin{aligned} ab &= ab \\ (ab)^{-1} &= a^{-1}b^{-1} \end{aligned}$$

Which is as desired.  $\square$

**Exercise 8.** Show that if  $G$  is a finite group with an even number of elements, then there must exist an element  $a \in G$  with  $a \neq e$  such that  $a^2 = e$ .

*Proof.* Assume otherwise, that except for the identity, we can pair elements off such that their inverse isn't themselves. This gives us pairs and the identity, which means the group has an odd number of elements. So there has to be an element whose inverse is itself.  $\square$

**Exercise 9.** Let  $G$  be a group, and let  $a \in G$ . The set  $C(a) = \{x \in G \mid xa = ax\}$  of all elements of  $G$  is called the centralizer of  $a$ .

(a) Show that  $C(a)$  is a subgroup of  $G$ .

Let  $x, y \in C(a)$ . Consider

$$\begin{aligned} (xy)a &= x(ya) \\ &= x(ay) \\ &= (ax)y \\ &= a(xy) \end{aligned}$$

So  $C(a)$  is closed. We now show that inverses exist:

$$x^{-1}a = x^{-1}(ax)x^{-1} = x^{-1}(xa)x^{-1} = ax^{-1}$$

So  $xx^{-1} \in C(a)$  so  $C(a)$  is a group.

(b) Show that  $\langle a \rangle \subseteq C(a)$ .

$\langle a \rangle$  is cyclic and therefore Abelian, so all elements commute with  $a$ .

(c) Compute  $C(a)$  if  $G = S_3$  and  $a = (1, 2, 3)$ .

(d) Compute  $C(a)$  if  $G = S_3$  and  $a = (1, 2)$ .

*January 10, 2020*

## 1.1 Group Homomorphisms

**Definition 1.14. (Group Homomorphism).** Let  $G_1, G_2$  be groups. Then  $\varphi : G_1 \rightarrow G_2$  is called a group homomorphism if

$$\varphi(xy) = \varphi(x)\varphi(y) \tag{1.1}$$

for all  $x, y \in G_1$ .

**Definition 1.15. (Additional Terminology).** There are some additional classifications of homomorphisms:

$\varphi$  is called an isomorphism if  $\varphi$  is 1-1 and onto.

$\varphi$  is called automorphism if  $\varphi$  is an isomorphism and  $G_1 = G_2$

**Definition 1.16. (Kernel and Image).** Similar to linear algebra and linear transformations, we have kernel and image.

$$\ker \varphi \stackrel{\text{def}}{=} \{x \in G_1 \mid \varphi(x) = e_2\} \text{ where } e_2 \text{ is the identity in } G_2$$

$$\text{im} \varphi \stackrel{\text{def}}{=} \{\varphi(x) \mid x \in G_1\}$$

We call  $G_2$  the “codomain” of  $\varphi$ .

**Proposition 1.17.** Let  $\varphi : G_1 \rightarrow G_2$  be a homomorphism.  $e_1$  the identity of  $G_1$  and  $e_2$  the identity of  $G_2$ . Then

- (i)  $\varphi(e_1) = e_2$ ,
- (ii)  $\varphi(x^{-1}) = \varphi(x)^{-1}$  for all  $x \in G_1$ .

*Proof.* We use the homomorphism definition.

- (i)  $\varphi(e_1) \cdot \varphi(e_1) = \varphi(e_1^2) = \varphi(e_1) = \varphi(e_1) \cdot e_2 \Rightarrow \varphi(e_1) = e_2$
- (ii)  $\varphi(x^{-1}) \cdot \varphi(x) = \varphi(x^{-1} \cdot x) = \varphi(e_1) = e_2 \Rightarrow \varphi(x^{-1}) = \varphi(x)^{-1}$

□

**Proposition 1.18.**

- (i)  $\ker \varphi$  is a subgroup of  $G_1$ ,
- (ii)  $\text{im} \varphi$  is a subgroup of  $G_2$ .

*Proof.*

- (i) Let  $x, y \in \ker \varphi$ . Then  $\varphi(xy) = \varphi(x)\varphi(y) = e_2 \cdot e_2 = e_2 \Rightarrow xy \in \ker \varphi$ .
- (ii) Let  $u, w \in \text{im} \varphi$  such that  $\varphi(x) = u, \varphi(y) = w$ . This implies  $uw = \varphi(x)\varphi(y) = \varphi(xy) \Rightarrow uw \in \text{im} \varphi$ .

□

We also state the following without proof:

- The inverse of an isomorphism is an isomorphism.
- The composition of isomorphisms is an isomorphism.

- We say  $G_1 \cong G_2$  if there exists an isomorphism  $\varphi : G_1 \leftrightarrow G_2$ , and isomorphisms of groups in an equivalence relation.

**Exercise 10.** Let  $G$  be the following set of matrices over  $\mathbb{R}$ :

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

Show that  $G$  is isomorphic to  $\mathbb{Z}_2 \times \mathbb{Z}_2$ .

*Proof.* We can construct the map

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mapsto (0,0), \quad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \mapsto (0,1), \quad \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \mapsto (1,0), \quad \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \mapsto (1,1)$$

Constructing a Cayley table (or simple trial and error) shows that this is a valid isomorphism. Another things we could note is that the only groups with 4 elements are isomorphisms of  $\mathbb{Z}_4$  or  $\mathbb{Z}_2 \times \mathbb{Z}_2$ . Noting that the matrices aren't cyclic (there is no generator) also gives the compatible conclusion.  $\square$

**Exercise 11.** Let  $G$  be any group. and let  $a$  be a fixed element of  $G$ . Define a function  $\phi_a : G \rightarrow G$  by  $\phi_a(x) = axa^{-1}$ , for all  $x \in G$ . Show that  $\phi_a$  is an isomorphism.

*Proof.* We first show that  $\phi_a$  is a bijection by proving that it's 1-1 and onto:

$$\phi_a(x) = \phi_a(y)$$

$$axa^{-1} = aya^{-1}$$

$$x = y$$

Let  $w \in G$ . Then  $\phi_a(a^{-1}wa) = aa^{-1}waa^{-1} = w$ .

We now show that  $\phi_a$  is a homomorphism:

$$\phi_a(x)\phi_a(y) = axa^{-1}aya^{-1} = axya^{-1} = \phi_a(xy)$$

$\square$

**Proposition 1.19.** Let  $\varphi \in \text{Hom}(G_1, G_2)$ . Then  $\varphi$  is 1-1 iff  $\ker \varphi = \{e_1\}$

*Proof.* ( $\Rightarrow$ ) If  $\varphi$  is 1-1, and  $x \in \ker \varphi$ ,

$$\varphi(x) = \varphi(e_1) = e_2 \Rightarrow x = e_1$$

( $\Leftarrow$ ) If  $\ker \varphi = \{e_1\}$  and

$$\varphi(x) = \varphi(y)$$

$$\varphi(x)\varphi(y)^{-1} = e_2$$

$$\varphi(x)\varphi(y^{-1}) = e_2$$

$$\varphi(xy^{-1}) = e_2$$

$$xy^{-1} = e_1$$

$$x = y$$

□

**Exercise 12.** Show that the multiplicative group  $\mathbb{Z}_7^*$  is isomorphic to the additive group  $\mathbb{Z}_6$ .

*Proof.* By trial and error, we find that 3 is a generator in  $\mathbb{Z}_7^*$ .

$$3^1 = 3, \quad 3^2 = 2, \quad 3^3 = 6, \quad 3^4 = 4, \quad 3^5 = 5, \quad 3^6 = 1$$

. So we map powers of 3 to its powers which is an isomorphism.

□