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 8, 2020. Any sections denoted with asterisks (***) are currently incomplete, and I will update them when I get to those.

Contents

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:

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

  $\mathbb{Z}_n$ 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 $G = \{g^n \mid n \in Z\}$.

Example: Z_n are cyclic grous 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.

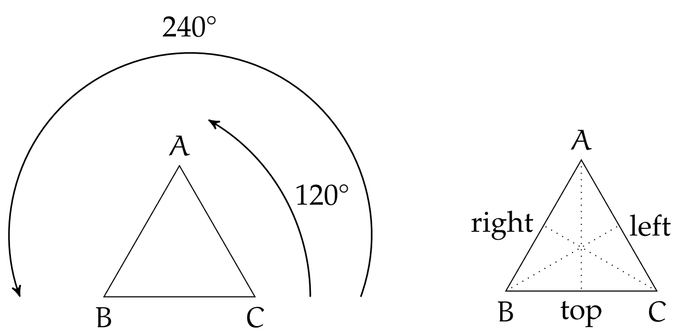
$$K = \mathbb{Z}_2 \oplus \mathbb{Z}_2 = \{(k, l) \mid k \in \mathbb{Z}_2, l \in \mathbb{Z}_2\}$$

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 $xy = g^a g^b = \underbrace{g \circ g \circ \cdots \circ g}_{k+l \text{ times}} = g^b g^a = yx$. □

Example: The symmetry transformation of an equilateral △ form a group under composition.

$$D_3 = \{\mathrm{id}, 120°, 240°, \mathrm{top}, \mathrm{left}, \mathrm{right}\}$$



∘	id	120°	240°	top	left	right
id	id	120°	240°	top	left	right
120°	120°	240°	id	left	right	top
240°	240°	id	120°	right	top	left
top	top	right	left	id	240°	120°
left	left	top	right	120°	id	240°
right	right	left	top	240°	120°	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 $f : H \to Hx$, $f(a) = ax$. We ened 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.

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