LECTURE 2. GROUPS AND SUBGROUPS

Please consider every proposition in this text as an exercise.

1. Groups

Definition 1.1. Consider a non-empty set G with a map mult : $G \times G \to G$. Such a map is called the binary operation. In this case, we will denote mult(a, b) by ab. The pair $(G, mult)$ is called a monoid if the following conditions hold:

(1) $a(bc) = (ab)c, \quad \forall a, b, c \in G$;
(2) $\exists e \in G$ such that $ae = ea = a, \quad \forall a \in G$ (e is called the identity element).

Exercise 1.2. Show that the identity element e in a monoid is unique.

Definition 1.3. A monoid G is called a group if $\forall a \in G\, \exists b \in G$ such that

$$ab = ba = e. \tag{1.1}$$

An element b is called an inverse element of a and is denoted by a^{-1}.

If the set G is finite, then the order of the group G is defined to be the number of its elements and is denoted by $|G|$.

Exercise 1.4. Show that for every group element, its inverse element is uniquely determined.

Exercise 1.5. Suppose that G is a group, $a, b \in G$ and $ab = e$. Is it always true that $ba = e$?

Exercise 1.6. Let G be a group. Show that

$$(a^{-1})^{-1} = a, \quad \forall a \in G. \tag{1.2}$$

Exercise 1.7. Let G be a group. Show that

$$(ab)^{-1} = b^{-1}a^{-1}, \quad \forall a, b \in G. \tag{1.3}$$

Proposition 1.8. *Let G be a group. Then for all $a, b \in G$ both equations*

$$ax = b \tag{1.4}$$

and

$$xa = b \tag{1.5}$$

have solutions and the solution of each equation is unique.

Definition 1.9. A group G such that

$$ab = ba\, \forall a, b \tag{1.6}$$

is called abelian. In an abelian group, the group operation is usually denoted by $+$, and the inverse element to an element a is denoted by $-a$.

Exercise 1.10. Does there exist a non-abelian group?

Date: February 18, 2026.

Proposition 1.11. *The set $\mathbb{Z}_n$ with respect to the addition operation is an abelian group.*

Proposition 1.12. *Let $n \in \mathbb{Z}_+$. For every integer k denote by $\bar{k}$ the equivalence class in $\mathbb{Z}_n$ containing k. Define*

$$\mathbb{Z}_n^* := \{\bar{k} \in \mathbb{Z}_n \mid \forall x \in \bar{k},\ \mathrm{GCD(x, n)} = 1\}. \tag{1.7}$$

Then the set $\mathbb{Z}_n^*$ with respect to the multiplication operation is an abelian group.

Exercise 1.13. Show that

$$\mathbb{Z}_n^* = \{\bar{k} \in \mathbb{Z}_n \mid \bar{k} \cdot \bar{m} \neq \bar{0},\ \forall \bar{m} \in \mathbb{Z}_n \setminus \{\bar{0}\}\}. \tag{1.8}$$

Proposition 1.14. *If p is a prime number, then*

$$\mathbb{Z}_p^* := \mathbb{Z}_p \setminus \{\bar{0}\}. \tag{1.9}$$

2. Subgroups

Definition 2.1. Let G be a group. A non-empty subset H of the set G is called a subgroup of G if $ab^{-1} \in H$ for all $a, b \in H$.

Proposition 2.2. *Let H be a subgroup of G. Then H is a group with respect to the operation of multiplication inherited from G.*

Exercise 2.3. Let

$$\{H_\alpha\}_{\alpha \in I} \tag{2.1}$$

be a family of subgroups of a group G. Show that

$$\bigcap_{\alpha \in I} H_\alpha \tag{2.2}$$

is also a subgroup of G.

Definition 2.4. Suppose that G is a group, $a \in G$ and $n \in \mathbb{Z}$. If $n \geq 0$, define the n-th power of the element a (denoted by a^n) inductively:

$$a^0 = e, \quad a^n := a^{n-1} \cdot a,\ \forall n \in \mathbb{Z}_+. \tag{2.3}$$

If $n < 0$, define

$$a^n := (a^{-n})^{-1}. \tag{2.4}$$

Exercise 2.5. Suppose that G is a group, $a \in G$ and $n, m \in \mathbb{Z}$. Then

$$a^{n+m} = a^n \cdot a^m, \quad (a^n)^m = a^{nm}. \tag{2.5}$$

Definition 2.6. Suppose that G is a group and $a \in G$. If the set

$$\{n \in \mathbb{Z}_+ \mid a^n = e\} \tag{2.6}$$

is nonempty, then the order of the element a (denoted by $\mathrm{ord(a)}$ or $|a|$) is defined by

$$\mathrm{ord(a)} := \min\{\mathrm{n} \in \mathbb{Z}_+ \mid \mathrm{a^n} = \mathrm{e}\}. \tag{2.7}$$

Otherwise, the order of the element a is said to be infinite.

Proposition 2.7. *Suppose that the order of an element $a \in G$ is finite order and $m \in \mathbb{Z} \setminus \{0\}$. Then*

$$\mathrm{ord(a^m)} = \frac{\mathrm{ord(a)}}{\mathrm{GCD(ord(a), m)}} = \frac{\mathrm{LCM(ord(a), m)}}{\mathrm{m}}. \tag{2.8}$$

Definition 2.8. A group G is called cyclic if $\exists a \in G$ such that $\forall g \in G\ \exists m \in \mathbb{Z}$ such that

$$g = a^m. \tag{2.9}$$

Such element a is called a generator of the group G.

Proposition 2.9. *Suppose that G is a group and $a \in G$. Among the subgroups of G containing a, there exists a minimal subgroup H_a and it is cyclic. H_a is finite iff the order of the element a is finite. In this case,*

$$|H_a| = \mathrm{ord(a)}. \tag{2.10}$$

Exercise 2.10. Is a subgroup of a cyclic group always cyclic?

3. Lagrange's Theorem

Proposition 3.1. *Let H be a subgroup of a group G. Define a binary relation on G by*

$$(x \sim_{lH} y) \iff (x^{-1}y \in H). \tag{3.1}$$

Then it is an equivalence relation. An equivalence class containing an element $g \in G$ is denoted by gH and is called a left coset. Then we get that

$$gH = \{gh \mid h \in H\}. \tag{3.2}$$

The set of all left cosets is denoted by G/H.

We may analogously define a right coset containing an element $g \in G$ by

$$Hg := \{hg \mid h \in H\}. \tag{3.3}$$

The set of all right cosets is denoted by $H\backslash G$.

Proposition 3.2. *Let H be a subgroup of a group G. For every element $g \in G$ the map $f_g : H \to gH$, defined by*

$$f_g(x) := gx, \tag{3.4}$$

is a bijection.

Proposition 3.3 (Lagrange's Theorem)**.** *Let H be a subgroup of a finite group G. Then $|H|$ divides $|G|$ and*

$$|G/H| = |H\backslash G| = \frac{|G|}{|H|}. \tag{3.5}$$

We define the index $[G : H]$ of a subgroup H in a group G by

$$[G : H] := |G/H|. \tag{3.6}$$

Proposition 3.4. *Suppose that G is a finite group and $a \in G$. Then the order of the element a divides the order of the group G. Therefore, we get that*

$$x^{|G|} = e, \quad \forall x \in G. \tag{3.7}$$

Proposition 3.5. *Every group of a prime order is cyclic.*

Proposition 3.6 (Fermat's little theorem)**.** *Let p be a prime, then for every integer m we have that*

$$m^p \equiv m \pmod{p} \tag{3.8}$$

Relevant textbook chapters:

- Pinter, Chapters 3-5, 13;
- Gallian, Chapters 2-4, 7;
- Fraleigh, Chapters 1, 2;
- Dummit, Foote, Sections 1.1, 2.1, 2.3, 3.1, 3.2;
- Allenby, Sections 5.3,5.4, 5.6-5.8.