Assignment 2

1 Symmetric Group

During the lecture, we have seen many abelian groups. Here, we will see a group that is not abelian. To introduce the group, we start by defining permutations.

Definition 1. A *permutation* of a set S is a bijective function $\sigma : S \to S$.

Example 1.

- Let $S = \{ 0, 1, 2 \}$. Define $\sigma : S \to S$ as follows:

$$0 \mapsto 1, \quad 1 \mapsto 2, \quad 2 \mapsto 0.$$

  Then σ is a permutation of S.

- Let $S = \{ \circ, \triangle, \square \}$. Define $\tau : S \to S$ as follows:

$$\circ \mapsto \triangle, \quad \triangle \mapsto \square, \quad \square \mapsto \circ.$$

  Then τ is a permutation of S.

We remark that what matters for a permutation is how many objects we have, not the objects' nature. We can label a set of n objects with $1, 2, \ldots, n$. In Example 1, we can label $\circ$ as 0, $\triangle$ as 1, and $\square$ as 2. Then σ and τ are the same permutation.

Now, we take a set S of n elements. Labeling the elements allows us to consider $S = \{ 1, \ldots, n \}$. Let S_n denote the set of all permutations of S. And let $\circ$ denote the composition of functions. Then it is easy to prove that

Lemma 1. $(S_n, \circ)$ is a group.

We note that the identity element in the group is the identity function $\sigma : S \to S$, $\sigma(s) = s \ \forall s \in S$. Any $\sigma \in S_n$ is bijective, the inverse of σ in S_n is then given by σ^{-1}.

Definition 2. $(S_n, \circ)$ is called the *symmetric group of degree n*.

Example 2. Let $n = 2$ and $S = \{ 1, 2 \}$. There are only two ways to permute two elements. So $S_2 = \{ \sigma_1, \sigma_2 \}$, where $\sigma_1 : S \to S$, $1 \mapsto 1, 2 \mapsto 2$ is the identity, and $\sigma_2 : S \to S$, $1 \mapsto 2, 2 \mapsto 1$.

Question 1 [A group that is not abelian] (2 marks) Let $n = 3$ and $S = \{ 1, 2, 3 \}$.

a) What is the cardinality of S_3?

b) Prove that S_3 is not an abelian group.

We can extend permutations in S_3 to permuting n elements by keeping the other $n - 3$ elements unchanged. Thus S_n is not abelian for any $n \geq 3$.

Definition 3. The *order* of a group $(G, \cdot)$ is the number of elements in G, or the cardinality of the set G, $|G|$. A group G is said to be *finite* if $|G| < \infty$ and *infinite* if $|G| = \infty$.

Example 3.

- We have seen a few infinite groups, for example, $(\mathbb{Z}, +)$ and $(\mathbb{R}^+, \times)$.

- We have also seen two finite groups, $|S_2| = 2$, $|S_3| = 6$.

Question 2.(1 mark) Compute the cardinality of S_n.

Definition 4. Let $(G, \cdot)$ be a group with identity element e, the *order* of an element $g \in G$, denoted $\mathrm{ord}\,(g)$, is the smallest positive integer k such that

$$\underbrace{g \cdot g \cdots g}_{k \text{ times}} = g^k = e.$$

When such a k does not exist, we define $\mathrm{ord}\,(g) = \infty$.

Example 4. In $(\mathbb{Z}, +)$, the identity element is 0, $\mathrm{ord}\,(1) = \infty$.

Question 3. (1 marks) Continue from Example 2, σ_1 is the identity. What is the order of σ_2? Why?

Definition 5. A group G is called *cyclic* if it is generated by one element, i.e.

$$G = \left\{ g^k \;\middle|\; k \in \mathbb{Z} \right\}.$$

Question 4. (1 mark) We have seen in Example 2, $S_2 = \{ \sigma_1, \sigma_2 \}$, where σ_1 is the identity element. In the previous question, we have computed the order of σ_2. Is S_2 cyclic? Why?

We now state a very useful theorem about the order of a group and the order of an element in the group. The proof follows from a famous theorem (Lagrange Theorem) named after Joseph-Louis Lagrange (1736-1813). Details of the theorem can be found in e.g. [Her96, page 59].

Theorem 1 (Lagrange Theorem)**.** Let $(G, \cdot)$ be a finite group with identity element e. For any $g \in G$, $\mathrm{ord}\,(g)$ divides $|G|$, in particular, $g^{|G|} = e$.

Question 5. (3 marks) Use Lagrange Theorem to prove Euler's Theorem

Theorem 2 (Euler's Theorem)**.** For any $a \in \mathbb{Z}$, $a^{\varphi(n)} \equiv 1 \bmod n$ if $\gcd(a, n) = 1$.

2 Substitution Cipher

Definition 6 (Substitution cipher)**.** Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$, and $\mathcal{K} = S_{26}$. For any key $\sigma \in S_{26}$, define

$$E_\sigma : \mathbb{Z}_{26} \to \mathbb{Z}_{26}, \quad p \mapsto \sigma(p); \qquad D_\sigma : \mathbb{Z}_{26} \to \mathbb{Z}_{26}, \quad c \mapsto \sigma^{-1}(c)$$

The cryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, where $\mathcal{E} = \{ E_\sigma : \sigma \in \mathcal{K} \}$, $\mathcal{D} = \{ D_\sigma : \sigma \in \mathcal{K} \}$, is called the *substitution cipher*.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
W	X	Y	Z	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
							U	V	W	X	Y	Z							
							V	A	B	C	D	E							

Table 1: Definition of σ, a key for substitution cipher.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
V	W	X	Y	Z	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	A	B	C	D

Table 2: Definition of σ^{-1}, where $\sigma \in S_{26}$ is a key for substitution cipher shown in Table 1.

Recall the symmetric group of degree n, denoted S_n, is the set of permutations of a set X with n elements (see Definition 2). We have discussed that a permutation is a bijective function and its inverse exists with respect to the composition of functions (see Lemma 1). In particular, any permutation $\sigma \in S_{26}$ has an inverse σ^{-1}.

We note that an affine cipher is also a substitution cipher.

Example 5. Define σ as in Table 1, then the corresponding table for decryption can be computed by flipping the two rows of the table (see Table 2). For example, to decrypt `UIFJNJUWUJPOHWNF`, using Table 2, we get `THE IMITATION GAME`.

Question 6. (1 mark) Decrypt the following message:

`JMPAFYSDQUPHSWQID`

Question 7. (1 mark)

a) Compute the size of key space for a substitution cipher.

b) Modern computers run at a speed of a few GHz, which is $\sim 10^9$ instructions per second. There are $\sim 10^5$ seconds per day, so one computer can run $\sim 10^{14}$ instructions per day, or $\sim 10^{16}$ instructions per year. If we would like to exhaust every key for substitution cipher, how many years will we need?

Compared to the age of the universe, which is 13.8 billion, i.e. 1.38×10^{10} years, exhaustive key search is impossible with current computation power.

What to submit.

- The submission should include detailed solution written in latex
- PDF to be submitted in AIS
- Add full name in both the file name and inside the file

When to submit: by Week 3 Thursday 8 am

References

[Her96] Israel N Herstein. *Abstract algebra*. Prentice Hall, 1996.