THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 2078 Honours Algebraic Structures 2023-24
Tutorial 1 Notes
15th January 2024

- If you have any questions, please contact Eddie Lam via echlam@math.cuhk.edu.hk or in person during office hours.

1. Order of an element in a group

Recall that for $g \in G$, $|g|$ or $\operatorname{ord}(g)$ is smallest positive integer n (if exists) so that $g^n = e$. If such integer does not exist, we write $|g| = \infty$ and say g has infinite order. Every element in a finite group has finite order by pigeonhole principle and cancellation law. In general, an element of an infinite group can have order either finite or infinite. For example, in the mulitplicative group of complex number $(\mathbb{C}^\times, \cdot)$, the number 2 has infinite order, since $2^n \neq 1$ for any $n > 0$; whereas the roots of unity, $e^{2\pi i/n}$ has order n which is finite. From this example, we can also see there exists infinite groups in which every element has finite order, for example $G = \{\zeta \in \mathbb{C}^\times | \, \zeta^k = 1 \text{ for some } k \in \mathbb{Z}\}$ is a subgroup of $\mathbb{C}^\times$, since if $\zeta, \eta \in G$, then there exists $n, m \in \mathbb{Z}$ so that $\zeta^n = 1$ and $\eta^m = 1$, then $(\zeta\eta)^{nm} = 1$ and so $\zeta\eta \in G$.

The order of an element and the order of the group are related by a corollary of Lagrange's theorem, which will be discussed in week 4 (c.f. section 4.3 in the lecture notes). The corollary says that $|g|$ divides $|G|$ for any $g \in G$. We will give a simple proof of this fact in the case when G is abelian, that does not rely on the techniques discussed in week 4.

Proposition. Let G be a finite abelian group, then any $g \in G$ has order dividing $|G|$.

Proof. We write $G = \{g_1, g_2, ..., g_n\}$ where $n = |G|$, and consider for each $g \in G$ the funciton $\phi : G \to G$ by $\phi(x) = gx$, where we multiply g on the left to any element in G. This function ϕ is bijective because $\phi(x) = \phi(y)$ gives $gx = gy$, whence cancellation law implies $x = y$. For sets with the same cardinality, injectivity implies bijectivity. Therefore, we have

$$\prod_{i=1}^{n} g_i = \prod_{i=1}^{n} (gg_i) = g^n \prod_{i=1}^{n} g_i.$$

Here the first equality holds because the product is taken over all elements in G, and is independent of the order in which the elements are multiplied as G is abelian. Therefore by cancellation law again we have $g^n = e$. Then by proposition 2.1.2, we have $|g|$ divides $n = |G|$. ■

It is instructive to figure out what are orders some of elements in specific groups. Recall the group $(\mathbb{Z}_n, +)$ where $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$ equipped with group operation given by addition mod n. We have the following result on the order of an element in $\mathbb{Z}_n$.

Proposition. Let $k \in \mathbb{Z}_n$, then $\operatorname{ord}(k) = \operatorname{lcm}(k, n)/k = n/\gcd(k, n)$.

Proof. By definition $\operatorname{ord}(k)$ is the smallest positive integer so that $\operatorname{ord}(k)k \equiv 0 \pmod{n}$, therefore $\operatorname{ord}(k)k$ is the smallest multiple of k that is also a multiple of n, so $\operatorname{ord}(k)k = \operatorname{lcm}(k, n)$. On the other hand, suppose that $mk \equiv 0 \pmod{n}$, in other words, n divides mk. This is equivalent to n dividing $\gcd(mk, mn) = m\gcd(k, n) \iff n/\gcd(k, n)$ divides m. In particular, putting $m = \operatorname{ord}(k)$ shows that $n/\gcd(k, n)$ divides $\operatorname{ord}(k)$. Meanwhile proposition 2.1.2 implies $\operatorname{ord}(k)$ divides $\gcd(k, n)$, so they are equal. ■

Remark. The identity $\gcd(k,n)\cdot \text{lcm}(k,n) = kn$ holds for arbitrary k, n, what we have done above is a fancy way to showing this equality. One can prove this in a more straightforward manner by writing k, n in terms of prime factorizations, $k = p_1^{i_1}\dots p_l^{i_l}$ and $n = p_1^{j_1}\dots p_l^{j_l}$. Then $\gcd(k,n) = p_1^{\min\{i_1,j_1\}}\dots p_l^{\min\{i_l,j_l\}}$ and $\text{lcm}(k,n) = p_1^{\max\{i_1,j_1\}}\dots p_l^{\max\{i_l,j_l\}}$. Then the equality follows from $\min\{a,b\}+\max\{a,b\} = a+b$.

In particular, as a corollary of the proposition above, whenever $\gcd(k,n) = 1$, we have $\text{ord}\,(k) = n$, therefore by proposition 2.1.3, we have $\langle k\rangle = \{0, k, 2k, ..., (n-1)k\}$ has cardinality n, so it must be the whole group $\mathbb{Z}_n$. This shows that $\mathbb{Z}_n$ is cyclic, and any k with $\gcd(k,n) = 1$ is a generator.

2. Cayley Table of a finite group

The multiplication table or the Cayley table of a finite group G is a table arranging all possible multiplications of two elements in G. For example, for a group $G = \{a, b, c, d\}$ consisting of 4 elements, the multiplication table would be constructed as below.

$\cdot$	a	b	c	d
a	aa	ab	ac	ad
b	ba	bb	bc	bd
c	ca	cb	cc	cd
d	da	db	dc	dd

The first observation is that the group is abelian, precisely when $gh = hg$ for all $g, h \in G$, therefore the Cayley table would appear to be symmetric along the diagonal. On the other hand, since in any group, there is a unique identity element e where $eg = ge = g$ for all $g \in G$, there will be a unique row and unique column which is the exact copy of the indexing row and column. For example, in the table below, the group is $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, note that the first row and the first column (labelled in red), corresponding to multiplication with the identity, are exactly the copy of the indexing row and columns.

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Recall that when we multiply an element g to any element in G on the left or on the right, we get a bijection from G to itself, i.e. it is a permutation of the elements in G. So each row and each column of the Cayley table is a unique permutation of G. Notice that in the above case, the group is cyclic, and the rows and columns are given by cyclic permutations.

Given an unfamiliar group, it is a manageable task to understand its structure by computing its Cayley table. It is possible to verify that two groups are isomorphic or not by comparing their Cayley tables.

For example, consider the following groups $G_1 = \mathbb{Z}_2\times\mathbb{Z}_2 = \{(0,0),(1,0),(0,1),(1,1)\}$, where the group operation is given by entry-wise addition modulo 2, i.e. $(a,b)+(c,d) = (a+c \mod 2, b+d \mod 2)$. And $G_2 = \mathbb{Z}_{12}^{\times}$, the multiplicative group of integers modulo 12. This group consists of those integers in $\{0, 1, 2, ..., 12\}$ which are invertible modulo 12, this is equivalent to picking those that are coprime to 12. So in our case $\mathbb{Z}_{12}^{\times} = \{1, 5, 7, 11\}$, one can

explicitly compute its multiplication: e.g. $5^2 = 25 \equiv 1 \mod 12$. The Cayley tables for G_1 and G_2 are given below.

$+$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

$\cdot$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

The two tables are the same under the identification $(0,0) \leftrightarrow 1$, $(1,0) \leftrightarrow 5$, $(0,1) \leftrightarrow 7$ and $(1,1) \leftrightarrow 11$. Therefore one can conclude that the two groups are isomorphic (having the same group structures).