11. General results about groups

Recall that in the last lecture we defined groups and introduced several (classes of) examples of groups. We start this lecture by establishing some general properties that hold in all groups (similarly to what we did with rings in Lecture 1).

Theorem 11.1. *Let $(G, *)$ be a group. The following hold:*

(a) *Identity element $e \in G$ is unique.*
(b) *For every $x \in G$, its inverse x^{-1} is unique.*
(c) *(cancellation laws) If $a * x = a * y$ for some $a, x, y \in G$, then $x = y$. Similarly if $x * a = y * a$ for some $a, x, y \in G$, then $x = y$.*
(d) *If $a * z = e$ for some $a, z \in G$, then $a = z^{-1}$ (and $z = a^{-1}$).*
(e) *$(x * y)^{-1} = y^{-1} * x^{-1}$ for all $x, y \in G$.*

Proof. (a) Suppose that e_1 and e_2 are both identity elements of G. By definition this means that for all $x \in G$ we have $x * e_1 = x$, $e_1 * x = x$ and also $x * e_2 = x$, $e_2 * x = x$. Setting $x = e_2$ in the second equation and $x = e_1$ in the third equation, we get $e_1 * e_2 = e_2$ and $e_1 * e_2 = e_1$, and combining those we conclude that $e_1 = e_2$. Thus identity element of G is unique.

(b) Let $x \in G$, and suppose that y and z are both inverses of x, so that $x * y = y * x = e$ and $x * z = z * x = e$. Then

$$y = y * e = y * (x * z) = (y * x) * z = e * z = z,$$

so inverse of x is unique.

(c) Suppose that $a * x = a * y$. Then $a^{-1} * (a * x) = a^{-1} * (a * y)$, whence $(a^{-1} * a) * x = (a^{-1} * a) * y$, so $e * x = e * y$ and therefore $x = y$. Similarly, $x * a = y * a$ implies $x = y$.

(d) If $a * z = e$, then $a * (z * a) = (a * z) * a = e * a = a = a * e$. Hence applying the first cancellation law with $x = z * a$ and $y = e$, we conclude that $z * a = e$. Once we know that $a * z = z * a = e$, we can say that by definition a is the inverse of z and z is the inverse of a.

(e) Let $a = x * y$ and $z = y^{-1} * x^{-1}$. By (d) we only need to check that $a * z = e$, which is done by direct computation:

$$\begin{aligned} a * z = (x * y) * (y^{-1} * x^{-1}) &= ((x * y) * y^{-1}) * x^{-1} \\ &= (x * (y * y^{-1})) * x^{-1} = (x * e) * x^{-1} = x * x^{-1} = e. \end{aligned}$$

□

Multiplicative notation in groups. From now on, given a group G and $x, y \in G$, we will usually write xy instead of $x * y$ (this is what we call multiplicative notation) and refer to group operation as *multiplication.*

We will NOT be using multiplicative notation when the multiplication symbol already has some meaning in G, and its meaning is different from group operation (so the use of multiplicative notation may be confusing). For instance, suppose that $G = (\mathbb{Z}, +)$, that is $G = \mathbb{Z}$ as a set, and the group operation is addition. In this case we do NOT write xy instead of $x + y$ to avoid confusion with the (usual) multiplication in $\mathbb{Z}$.

Once we start using multiplicative notation in groups, it is tempting to start applying the same rules that we routinely use when working with products of, say, real numbers. Some of the usual rules will still hold in arbitrary groups, while some will not. For instance,

(i) We do not have to write parentheses since $(xy)z = x(yz)$ by associativity (G1), so we can simply write xyz.

(ii) On the other hand, we cannot change the order of factors: $xy \neq yx$ in groups in general since we do not assume that group operation is commutative.

The multiplication table of a group. Let G be a group with operation $*$. The *multiplication table of G* is a table whose rows and columns are labeled by elements of G, and at the intersection of x-row and y-column we put element $x * y$. Let us consider two examples.

1. Let $G = (\mathbb{Z}_5, +)$. Since the group operation in this example is addition, the multiplication table of G is the same as the addition table of the ring $\mathbb{Z}_5$:

+	[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]

2. Let $G = (\mathbb{Z}_5 \setminus \{[0]\}, \cdot)$, the set of nonzero elements of $\mathbb{Z}_5$ with group operation given by multiplication in $\mathbb{Z}_5$. In this case the multiplication table for G is the same as the multiplication table for the ring $\mathbb{Z}_5$ with row and column labeled by 0 removed (since 0 is not an element of G).

$\cdot$	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[3]	[3]	[1]	[4]	[2]
[4]	[4]	[3]	[2]	[1]

Looking at multiplication tables in these two examples, we immediately observe two properties:

(i) The tables are symmetric with respect to the main diagonal. This holds precisely because both of those groups are commutative ($x*y = y*x$ for $x, y \in G$). Since commutativity is not required in groups, this property will not hold for group multiplication tables in general.

(ii) The "Sudoku property": every row and column contains every element of the group precisely once. This property WILL hold in arbitrary groups and follows easily from the cancellation laws (part (c) of Theorem 11.1). Formal verification of this property is left as a homework exercise.

11.1. **Multiplication tables for groups of order 3 and 4.** We finish the lecture by analyzing the possible multiplication tables for groups of order 3 and 4. Later in the course we will be able to obtain the same result more efficiently using, in particular, Lagrange Theorem, but it is useful to see how to do this by only exploiting the very basic tools.

Definition. The order of a group G, denoted by $|G|$, is the number of elements in G.

Groups of order 3. Let G be a group of order 3. One of the three elements of G must be the identity element e, and denote the other two elements of G by x and y. We can fill in the following part of the multiplication table of G just using the definition of e:

	e	x	y
e	e	x	y
x	x		
y	y		

and the rest is completed uniquely using the Sudoku property:

	e	x	y
e	e	x	y
x	x	y	e
y	y	e	x

Note that the multiplication tables forces the equality $y = x^2$. Replacing y by x^2 and also writing e as x^0 and x as x^1, we can now rewrite the multiplication table as follows:

	x^0	x^1	x^2
x^0	x^0	x^1	x^2
x^1	x^1	x^2	x^0
x^2	x^0	x^1	x^2

The pattern of exponents in the above table probably looks familiar. More precisely, note that if we erase all the x's in the above table (just leaving the exponents) and draw brackets around each exponent, we will get precisely the multiplication table for the group $(\mathbb{Z}_3, +)$. As we will see in Lecture 14, what this means formally is that every group of order 3 is isomorphic to $(\mathbb{Z}_3, +)$.

Before performing a similar analysis in groups of order 4, we prove a general result which is of independent interest.

Given a group G, let

$$A(G) = \{x \in G : x^{-1} \neq x\} \quad \text{and} \quad B(G) = \{x \in G : x^{-1} = x\}.$$

Thus, we always have $G = A(G) \cup B(G)$ and $A(G) \cap B(G) = \emptyset$; in particular, if G is finite, then $|G| = |A(G)| + |B(G)|$.

Lemma 11.2. *Let G be a finite group. The following hold:*

(a) *$|A(G)|$ is always even.*

(b) *If $|G|$ is even, then $|B(G)|$ is even and $|B(G)| \geq 2$.*

Proof. (a) is clear since elements of A can be divided into pairs (x, x^{-1}), where each element forms a pair with its inverse.

(b) Since $|G|$ is even by assumption and $|A(G)|$ is even by (a), $|B(G)| = |G| - |A(G)|$ must also be even. Also $|B(G)|$ cannot equal 0 since $B(G)$ always contains e, so we must have $|B(G)| \geq 2$. □

Groups of order 4. Let G be a group of order 4. By Lemma 11.2, $|B(G)|$ is equal to 4 or 2. We analyze those two cases separately.

Case 1: $|B(G)| = 4$. Denote the three non-identity elements of G by x, y and z. By assumption we have $x^{-1} = x$, $y^{-1} = y$ and $z^{-1} = z$, and therefore $x^2 = y^2 = z^2 = e$. Based on this, we can fill the following part of the multiplication table:

G	e	x	y	z
e	e	x	y	z
x	x	e		
y	y		e	
z	z			e

and the rest is completed using Sudoku property:

	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

Note that we did not have any choices with how to fill the multiplication table in Case 1. As we will see, this means that any two groups of order 4 with $|B(G)| = 4$ are isomorphic to each other. At this point we should actually ask if a group with the above multiplication table exists at all. The answer is yes, and an example of such a group is $G = \mathbb{Z}_8^\times = \{[1], [3], [5], [7]\}$ (check that all elements of this group are equal to their own inverses).

Case 1: $|B(G)| = 2$. In this case G has unique non-identity element equal to its own inverse. Call that element x and the other two non-identity elements of G by y and z. Thus, $G = \{e, x, y, z\}$, $x^2 = e$, $y^2 \neq e$ and $z^2 \neq e$. Based on this information, we can complete the multiplication table of G using just the Sudoku property in three stages, as shown below:

	e	x	y	z
e	e	x	y	z
x	x	e		
y	y		$\neq e$	
z	z			$\neq e$

	e	x	y	z
e	e	x	y	z
x	x	e		
y	y		$\neq e$	e
z	z		e	$\neq e$

	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	$\neq e$	e
z	z	y	e	$\neq e$

	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	x	e
z	z	y	e	x

Note that the above table implies that $y = x^2$ and $z = xy = y^3$. Thus, as for groups of order 3, we can express the entire table in terms of y. If we then swap the second and third rows and columns, we will see (similarly to the case of groups of order 3) that G must be isomorphic to $(\mathbb{Z}_4, +)$.

11.2. **Book references.** The general references for this lecture are [Pinter, Ch. 4] and [Gilbert, 3.2] (the multiplication tables in Pinter are defined in Chapter 3). The material in § 11.1 appears in the exercises at the end of Chapter 4 in Pinter (along with some other useful results).