MATH 323, Algebra I, Fall 2020

Course notes, Chapter 4, Lagrange's Theorem

Laurence Barker, Bilkent University. Version: 15 November 2020.

These notes, updated as the course progresses, are a record of the prepared text of the lectures, with a little more detail added, but they cannot cover much of the oral component of the lectures.

Summary of contents

We shall be discussing the notion of a group and some other basic notions relaing to that.

Fuller details on the material we shall be summarizing can be found in Judson, primarily Chapters 3, 4, 5, 6. These notes are independent of that text.

We shall be covering the notions of:

• a **group**,

• a **group isomorphism**,

• a **subgroup**,

• **left cosets** and **right cosets**,

• a **cyclic group**,

The notion of a group: This section is similar to the first and second sections of the previous chapter. The notion of a group is a generalization of the notation of an abelian group. One of the defining properties of abelian groups is the commutativity of the operation. We shall be abandoning that feature.

Thus, instead of introducing a new feature, we shall be removing a feature. But that will, in effect, yield a new concept that is much more widely applicable than the concept we were discussing before.

The following preliminary terminology is sometimes convenient. Given a set S, we define a **binary operation** on S to be a function $S \leftarrow S \times S$. Often, for a binary operation $*$ on S, we write $s * t$ instead of $*(s,t)$ for $s,t \in S$.

• We say that $*$ is **associative** provided $r*(s*t) = (r*s)*t$ for all $r,s,t \in S$. In that case, we can write $r*s*t$ unambiguously.

• We say that $*$ is **commutative** provided $s*t = t*s$ for all $s,t \in S$.

We define a **group** to be a pair $(G,*)$, where G is a set and $*$ is a binary operation on such that the following three conditions hold.

Associativity Axiom: The operation $*$ is associative.

Identity Axiom: There is an element $e \in G$ such that $e * g = g = g * e$ for all $g \in G$. We call e an **identity element** of G.

Inversion Axiom: For all $g \in G$, there exists $h \in G$ such that $g * h = e = h * g$. We call h an **inverse** of g.

We call the set G the **underlying set** of the group $(G, *)$. We call $*$ the **group operation** of $(G, *)$. As before, we often abuse notation, speaking of the group G, which we view as consisting of the underlying set G together with the binary operation $*$.

Let us point out that there is, in some sense, a redundency in the notation $(G, *)$, in that the underlying set G is part of the data in the specification of the binary operation $*$. Indeed, $*$ is a function whose codomain is the set G. So we can reinterpret the three axioms as defining conditions for the notion of a group operation. A group operation is a binary operation satisfying those three conditions. One can view group theory as the theory of group operations.

Let $(G, *)$ be a group. As before, we are justified in calling e *the* identity element because it is unique: given identity elements e and e' then $e = e * e' = e'$.

Usually, when discussing groups in abstract, we employ multiplicative notation, writing 1_G or just 1 instead of e, writing gh or $g.h$ instead of $g * h$.

Let G be a group, with the group operation written multiplicatively. For $g, h \in G$ such that h is an inverse of g, we call h *the* inverse of g, and we write $h = g^{-1}$. Again, the grammar and notation is justified because inverses are unique: given $g \in G$ with inverses $f, h \in G$, then $f = f.1 = fgh = 1.h = h$.

Of course, the group G is an abelian group if and only if the group operation is commutative.

The term *abelian group* is in honour of Niels Henrik Abel who, in the 1820s, made much use of symmetries in his study of polynomial equations. At that time, no clear notion of a group had been formulated. Rather, Abel's work formed part of the background behind the later emergence of the abstact concepts of group theory. I do not know why his name is attached specifically to abelian groups.

We have already seen, in the previous chapter, some examples of abelian groups. Let us now give an general example of a group which, in most cases, is non-abelian.

Important Example: Let Ω be a set. A bijection $\Omega \leftarrow \Omega$ is called a **permutation** of Ω. We write $\mathrm{Sym}(\Omega)$ to denote the set of permutations of Ω. Then $(\mathrm{Sym}(\Omega), \circ)$ is a group, where $\circ$ denotes composition of functions. We often use the same expression $\mathrm{Sym}(\Omega)$ to refer to that group. The group $\mathrm{Sym}(\Omega)$ is called the **symmetric group** on Ω.

The importance of that example will become apparent in the next chapter, when we discuss the theory of permutation groups. For now, let us just mention that, when groups arise in applications, they are very often appear within symmetric groups, and they very often express symmetries of mathematical objects.

A group G is said to be **infinite** when the underlying set G is infinite. Otherwise G is said to be **finite**. When G is finite, the size $|G|$ of the underlying set G is called

the **size** of G or, more often, the **order** of G. A group with order 1 is called a **trivial group**. Thus, G is trivial when $G = \{1_G\}$.

Again, let Ω be a set. Plainly, $\mathrm{Sym}(\Omega)$ is a finite group if and only if Ω is finite. In that case,

$$|\mathrm{Sym}(\Omega)| = |\Omega|! \ .$$

It is also clear that $\mathrm{Sym}(\Omega)$ is abelian if and only if Ω is finite and $|\Omega| \leq 2$.

Let us comment further on the finite case. If Ω is empty or singleton, then $\mathrm{Sym}(\Omega)$ is a trivial group. If $|\Omega| = 2$, then $\mathrm{Sym}(\Omega)$ is cyclic and of order 2. In the next section, we shall comment on the cases where $|\Omega| = 3$ or $|\Omega| = 4$.

The groups S_3 and S_4 and D_8: For a positive integer n, we define the **symmetric group** of degree n, denoted S_n, to be the symmetric group on the set $\{1, ..., n\}$ of positive integers less than or equal to n. Thus,

$$S_n = \mathrm{Sym}(\{1, ..., n\}) \ .$$

For $g \in S_n$ and $w \in \{1, 2, 3\}$, we write $gw = g(w)$. Since the group operation of S_n is composition, we have $f(gw) = (fg)w$. So we can write fgw unambiguously.

Let us examine the case $n = 3$. We define a to be the permutation of $\{1, 2, 3\}$ such that $a1 = 2$ and $a2 = 3$ and $a3 = 1$. We define b to be the permutation of $\{1, 2, 3\}$ such that $b1 = 2$ and $b2 = 1$ and $b3 = 3$.

We have $ab1 = a2 = 3$ and $ab2 = a1 = 2$ and $ab3 = a3 = 1$. Evidently, ab is the permutation of $\{1, 2, 3\}$ such that $1 \leftarrow\!\shortmid\ 3$ and $2 \leftarrow\!\shortmid\ 2$ and $3 \leftarrow\!\shortmid\ 1$. From the next table, we see that

$$S_3 = \{1, a, a^2, b, ab, a^2b\} \ .$$

Thus, all 6 elements of S_3 can be expressed in terms of a and b.

		w		
	gw	1	2	3
g	1	1	2	3
	a	2	3	1
	a^2	3	1	2
	b	2	1	3
	ab	3	2	1
	a^2b	1	3	2

It is straightforward to check that the Cayley table for S_3 is as follows.

		g					
	fg	1	a	a^2	b	ab	a^2b
f	1	1	a	a^2	b	ab	a^2b
	a	a	a^2	1	ab	a^2b	b
	a^2	a^2	1	a	a^2b	b	ab
	b	b	a^2b	ab	1	a^2	a
	ab	ab	b	a^2b	a	1	a^2
	a^2b	a^2b	ab	b	a^2	a	1

The Cayley table, in some sense, has got rid of the interpretation of S_3. We introduced S_3 as the group of permutations of the set $\{1, 2, 3\}$. But the Cayley table makes no mention of that set. In this way, we arrive at an abstract description of S_3 as a group with elements 1, a, a^2, b, ab, a^2b, where the rules for multiplication are:

$$a^3 = 1 \,, \qquad b^2 = 1 \,, \qquad ba = a^2b \,.$$

The last of those three equations is equivalent to $b^v a^u = a^{2u} b^v$.

Another way of viewing S_3 is in terms of Euclidian transformations. Consider the Euclidian plane $\mathbb{E}^2$. Recall $\mathbb{E}^2 = \mathbb{R}^2$ regarded as a metric space, without any vector space structure. Thus, $\mathbb{E}^2$ is just a set of points together with a distance function. A **Euclidian transformation** of $\mathbb{E}^2$ is a bijection $\mathbb{E}^2 \leftarrow \mathbb{E}^2$ that preserves distances. It can be shown that every Euclidian transformation of $\mathbb{E}^2$ can be expressed as a composite of rotations and reflections.

Fix an equilateral triangle T in $\mathbb{E}^2$. We can view S_3 as the group of Euclidian transformations of $\mathbb{E}^2$ that sends each vertex of T to a vertex of T. Indeed, we can enumerate the vertices of the triangle as 1, 2, 3, then let each element of S_3 move the triangle in the evident way. Thus, for instance, a sends the vertices labelled 1, 2, 3 to the vertices labelled 2, 3, 1, respectively.

[Cue diagram of six triangles. But this is already on page 32 of Judson.]

It is easy to see that, generally, $|S_n| = n!$ for any positive integer n. In particular, the group S_4 has order $|S_4| = 24$.

Writing down the Cayley table for S_4 would be a practical possibility. One could assign short names to all 24 elements so that, using pen and paper in an ordinary way, the table with $24^2 = 576$ entries could be fitted onto a page. However, the table would not be very useful.

Most of the particular finite groups that receive special attention form group theorists are very much bigger than S_4. For instance, of the 26 sporadic groups, the smallest is M_11, which has order $|M_11| = 7920$. The largest is the monster group M, which has order

$$|M| = 808\,017\,424\,794\,512\,875\,886\,459\,904\,961\,710\,757\,005\,754\,368\,000\,000\,000 \approx 8.10^{53} \,.$$

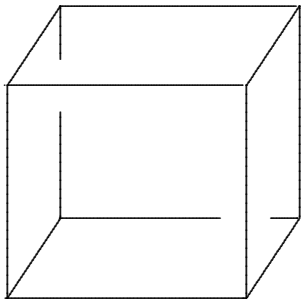
There would be scant point in trying to write down the Cayley table for any of the sporadic groups in humanly readable form.

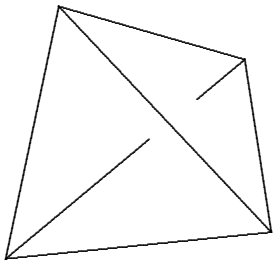
Instead of using Cayley tables, groups are often described as symmetries of other mathematical objects, rather as we did for S_3 above. The group M_11 is the symmetry group of a combinatorial object called a Steiner system. The group M was realized, by Robert Griess in 1982, as the symmetry group of a certain 196 884-dimensional non-associative algebra called the Griess algebra.

One way of viewing S_4 is as the group of rotational symmetries of a cube. Looking at the sketch of a cube below on the right, observe that, for any two vertices u and v of a cube, there are exactly 3 rotations sending u to v. Since a cube has exactly 8 vertices, the number of rotational symmetries of a cube is 24. To see that the group of rotations of a cube must be isomorphic to S_4, observe that every rotation permutes the

4 long diagonals of the cube, and the identity is the only rotation that fixes all 4 of those diagonals.

Alternatively, adapting the treatment we gave for S_3, we can realize S_4 as the Euclidian transformations of a regular tetrahedron in the 3-dimensional Euclidian space $\mathbb{E}^3$. By enumerating the vertices of the tetrahedron 1, 2, 3, 4, we can extend each element of S_4 to a Euclidian transformation that rearranges the vertices. See the diagram on the right, below.





But, to get back to Cayley tables for the time-being, let us now turn our attention to some but not all of the elements of S_4. Let $c \in S_4$ such that $c(1) = 2$ and $c(2) = 3$ and $c(3) = 4$, whence $c)4) = 1$. Let $d \in S_4$ such that $d(1) = 3$ and $d(2) = 4$ and $d^2 = 1$. We can form the group

$$D_8 = \{1, c, c^2, c^3, d, cd, c^2d, c^3d\}$$

whose multiplication operations are given by the conditions $c^4 = d^2 = 1$ and $dc = c^3d$. The Cayley table is as follows.

		g							
	fg	1	c	c^2	c^3	d	cd	c^2d	c^3d
f	1	1	c	c^2	c^3	d	cd	c^2d	c^3d
	c	c	c^2	c^3	1	cd	c^2d	c^3d	d
	c^2	c^2	c^3	1	c	c^2d	c^3d	d	cd
	c^3	c^3	1	c^2	c^3	c^3d	d	cd	c^2d
	d	d	c^3d	c^2d	cd	1	c^3	c^2	c
	cd	cd	d	c^3d	c^2	c	1	c^3	c^2
	c^2d	c^2d	cd	d	c^3d	c^2	c	1	c^3
	c^3d	c^3d	c^2d	cd	d	c^3	c^2	c	1

By labelling the vertices of a square as 1, 2, 3, 4 with 1 opposite to 3, thus with 3 opposite to 4, we can view D_8 as the group of Euclidian symmetries of a square.

Generally, for any integer $n \geq 2$, we define the **dihedral group** with order $2n$ to be the group

$$D_{2n} = \{1, c, c^2, ..., c^{n-1}, d, cd, c^2d, ..., c^{n-1}d\}$$

where $c^n = d^2 = 1$ and $dc = c^{n-1}d$. For $n \geq 3$, we can view D_{2n} as the group of Euclidian symmetries of a regular n-gon, that is, a relular polygon with n vertices and n edges.

Here, c is to be viewed as a rotation through $1/n$ of a full revolution, and d is to be viewed as a reflection.

The alert reader will notice that, in some sense, the group D_6 is the same as S_3. We have already indicated, in Chapter 2, how to capture such identificatrions. In that chapter, we were discussing isomorphisms only for abelian groups. In the next section, we generalize that material.

Group isomorphisms: The material in this section is a straightforward adaptation of the discussion of isomorphisms in the previous chapter. The only significant difference is that we shall be using multiplicative notation instead of additive notation.

Let F and G be groups. We define a **group isomorphism** $F \leftarrow G$ to be a bijection $\theta : F \leftarrow G$ such that $\theta(g_1 g_2) = \theta(g_1)\theta(g_2)$ for all $g_1, g_2 \in G$. There are many kinds of isomorphism in mathematics besides group isomorphisms. But, when the context makes the meaning clear, we may use the term *isomorphism* to mean *group isomorphism*.

When an isomorphism $F \leftarrow G$ exists, we say that F is isomorphic to G and we write $F \cong G$. Again, the inverse of a group isomorphism is a group isomorphism. The composite of two group isomorphisms is a group isomorphism. Hence, isomorphism has the reflexivity, symmetry and transitivity properties characteristic of equivalence relations: given groups E, F, G then:

- we have $G \cong G$,
- if $F \cong G$ then $G \cong F$,
- if $E \cong F$ and $F \cong G$, then $E \cong G$.

Let us give some examples. As we implicitly noted in the previous section,

$$D_6 \cong S_3 \ .$$

It is also easy to see that $D_4 \cong V_4$.

To see a slightly more subtle example, let Ω be any set with $|\Omega| = 3$. We claim that $\mathrm{Sym}(\Omega) \cong S_3$. Write $\Omega = \{w_1, w_2, w_3\}$. Let α be the unique permutation of Ω such that $w_3 \leftarrow\!\shortmid\, w_2 \leftarrow\!\shortmid\, w_1$. Let β be the unique permutation of Ω such that $1 \leftrightarrow 2$. Then the Cayley table for $\mathrm{Sym}(\Omega)$ is that same as the Cayley table for S_3, except with a and b replaced by α and β. So there is an isomorphism $\mathrm{Sym}(\Omega) \leftarrow S_3$ determined by the condition that $\alpha \leftarrow\!\shortmid\, a$ and $\beta \leftarrow\!\shortmid\, b$. Generally, $\alpha^u \beta^v \leftarrow\!\shortmid\, a^u b^v$.

Subgroups: The following remark is obvious.

Remark 4.1: *Let G be a group and $H \subseteq G$. Then the following three conditions are equivalent:*
(a) *The group operation $G \leftarrow G \times G$ restricts to a group operation $H \leftarrow H \times H$.*
(b) *For all $h, k \in H$, we have $hk \in H$ and $h^{-1} \in H$.*
(c) *For all $h, k \in H$, we have $hk^{-1} \in H$.*

When those three equivalent conditions hold, we regard H as a group by restriction of the operation, we write $H \leq G$ and we call H a **subgroup** of G.

When $H \leq G$ and $H \neq G$, we write $H < G$ and call H a **strict subgroup** of G. We often write the trivial subgroup $\{1_G\}$ just as 1. When $1 < H < G$, we call H a **proper subgroup** of G.

For example, the proper subgroups of S_3 are

$$\{1, b\}\ , \qquad \{1, ab\}\ , \qquad \{1, a^2b\}\ , \qquad \{1, a, a^2\}\ .$$

As another example, earlier in this chapter we constructed D_8 as a subgroup of S_4.

Left cosets, right cosets and Lagrange's Theorem: Let G be a group and $H \leq G$. For $g \in G$, the set

$$gH = \{gh : h \in H\}$$

is called a **left coset** of H in G. The set

$$Hg = \{hg : h \in H\}$$

is called a **right coset** of H in G. We have $1_G H = H = H 1_G$. So H is both a left coset and a right coset of H in G.

Lemma 4.2: *Let H be a subgroup of a group G. Then the left cosets of H in G are mutually disjoint. Also, the right cosets of H in G are mutually disjoint.*

Proof: For the first part, we are to show that, given $f, g \in G$, then $fH = gH$ or $fH \cap gH = \emptyset$. Suppose $fH \cap gH \neq \emptyset$. Let $e \in fH \cap gH$. Then $e = fh$ for some $h \in H$. It is now easy to see that $eH = fH$. Similarly, $eH = gH$. The first part of the required conclusion is now established. The second part holds similarly. □

The next result says that all the cosets, both left and right, have the same size.

Lemma 4.3: *Let G be a group, let H be a finite subgroup of G, and let $g \in G$. Then $|gH| = |H| = |Hg|$.*

Proof: The function $gH \ni gh \leftrightarrow h \in H$ is a bijection because the inverse is evidently $gH \ni f \mapsto g^{-1}f \in H$. So $|gH| = |H|$. The other required equality holds similarly. □

Obviously, any subgroup of a finite group is, itself, finite.

Theorem 4.4: (Lagrange's Theorem.) *Let G be a finite group and $H \leq G$. Then $|H|$ divides $|G|$.*

Proof: By the previous two lemmas, $|G|/|H|$ is equal to the number of left cosets of H in G. □

The proof also shows that $|G|/|H|$ is equal to the number of right cosets of H in G. A standard notation is

$$|G : H| = |G|/|H|\ .$$

We call $|G : H|$ the **index** of H in G.

For the sake of illustration, observe that the proper subgroups of S_3 are:

$$\langle b\rangle = \{1, b\}\ , \qquad \langle ab\rangle = \{1, ab\}\ , \qquad \langle a^2b\rangle = \{1, a^2b\}\ , \qquad \langle a\rangle = \{1, a, a^2\}\ .$$

We have isomorphisms $\langle b\rangle \cong \langle ab\rangle \cong \langle a^2b\rangle \cong C_2$ and $\langle a\rangle \cong C_3$. The orders of the elements 1, a, a^2, b, ab, a^2b are 1, 3, 3, 2, 2, 2, respectively.

Cyclic groups and cyclic subgroups, again: Cyclic groups are a particular kind of abelian group. We defined the notion in the previous chapter. Now that we are discussing groups in general, let us review the notion. A group G is said to be **cyclic** provided there exists an element $g \in G$ such that every element of G has the form g^m for some positive integer m. In that case, we say that the cyclic group G has **generator** g and, as an alternative phrasing, we say that G is **generated** by g.

Recall, every infinite cyclic group is isomorphic to the additive group $\mathbb{Z}$, we mean, the group $(\mathbb{Z}, +)$. Also, every finite cyclic group is isomorphic to the additive group $\mathbb{Z}/n$, where n is a positive integer. Now that we are working with arbitrary groups, with the group operation written as multiplication, a different notation is needed.

We write C_∞ for the infinite cyclic group, and C_n for the cyclic group with order n. Thus, C_∞ has a generator z such that each element of C_∞ can be written in the form z^m for a unique $m \in \mathbb{Z}$. There is a group isomorphism $C_\infty \leftarrow \mathbb{Z}$ given by $z^m \leftarrow\!\shortmid m$. In particular,

$$C_\infty \cong \mathbb{Z}\ .$$

Similarly, C_n has a generator z and every element can be expressed as z^m with $m \in \mathbb{Z}$, but now m is no longer unique. We have $z^m = z^{m'}$ if and only if $m \equiv_n m'$. Evidently, there is a well-defined group isomorphism $C_n \leftarrow \mathbb{Z}/n$ given by $z^m \leftarrow\!\shortmid [z]_n$. In particular,

$$C_n \cong \mathbb{Z}/n\ .$$

Let us restate Proposition 2.6 in this notation.

Proposition 4.5: *Every cyclic group is isomorphic to the infinite cyclic group C_∞ or the cyclic group C_n with order n, where n is a positive integer.*

Consder, again, an element g of a group G. Repeating a definition from Chapter 2, but now in a more general context, we define

$$\langle g\rangle = \{g^m : m \in \mathbb{Z}\}\ .$$

Plainly, $\langle g\rangle$ is a subgroup of G. In fact, $\langle g\rangle$ is a cyclic subgroup and $\langle g\rangle$ has generator g.

When the cyclic subgroup with generator g is infinite, g is said to be of **infinite order**. When $\langle g\rangle$ is finite, g is said to be of **finite order** and, in that case, the order $|\langle g\rangle|$ of the subgroup $\langle g\rangle$ is also called the **order** of the element g.

Now that we have generalized Lagrange's Theorem to the case of any finite group, we can also generalize Corollary 3.6.

Corollary 4.6: *Given an element g of a finite group G then g has finite order and the order $|\langle g\rangle|$ divides $|G|$.*

Proof: This is a special case of Lagrange's Theorem. □

Just to further familiarize ourselves with the notation for cyclic groups used in this chapter, let us restate Proposition 3.9.

Proposition 4.7: *Let n be a positive integer. Then there is a bijective correspondence between the divisors d of n and the subgroups H of C_n such that $m \leftrightarrow H$ provided $H \cong C_d$.*