6.S096: Number Theory January 24, 2024

Lecture 2— Group Theory

A. Anas Chentouf, M. Wacyl Meddour, M.A.O. *Scribe:*

In this lecture, we will introduce the basics of group theory. These are some lecture notes which we will follow during class, but the interested reader is invited to read Chapter 2 of Artin's *Algebra* [**?**]. In particular, we will introduce concepts for general groups, but almost all our applications will be ablien (commutative groups).

1 Basics of Group Theory Basics

1.1 Definitions and Examples

Recall that a binary operation $*$ on a set S is a map $* : S \times S \to S$ which sends the pair (a, b) to $a * b$. Note that a set is automatically *closed* under a binary operation that is defined on it.

Definition 1.1: Group

A group is a set G equipped with a binary operation $*$ such that the following properties hold:

1. **Associativity**: The binary operation is associative, and so for any $x, y, z \in G$, we have that $x * (y * z) = (x * y) * z$.[a]
2. **Identity**: There exists an identity element e_G such that $e_G * x = x = x * e_G$ for all $x \in G$.
3. **Inverses**: For all $x \in G$, there exists an inverse x such that $x * x^{-1} = e_G = x^{-1} * x$.

[a] As such, we henceforth write both as xyz.

If G is finite, we say that $|G|$ is the *order* of the group G. Otherwise, we say that G has infinite order.

We give the first example of a group: the integers.

Example.

Integers under Addition Consider $(\mathbb{Z}, +)$, the set of integers, under the addition binary operation: the sum of two integers is indeed an integer. We now verify the three group axioms.

1. **Associativity**: It is clear that $a+(b+c) = (a+b)+c$ for any three integers a, b, c.
2. **Identity:** The element 0 is an identity, since $0 + x = x = x + 0$ for all $x \in \mathbb{Z}$.
3. **Inverses**: For any $x \in \mathbb{Z}$, one can take $-x$ to be its inverse. Indeed, $x + (-x) = 0 = (-x) + x$.

Example.

Here is an example of other groups, which we will state but not prove.

1. $\mathbb{R}^{\times}$: nonzero real numbers under multiplication.
2. S_n (symmetric group): permutations on $\{1, \cdots, n\}$ under composition.
3. Klein-four group: the set

$$\{(0,0), (0,1), (1,0), (1,1)\}$$

under componentwise addition modulo 2.

As we have seen above the group is technically the ordered pair $(G, *)$, but when the operation has been made clear, we will often denote the group as G. Another observation is that the addition operation is commutative, and this special case warrants a definition of its own, named after Norwegian mathematician Niels Abel.

Definition 1.2: Abelian Group

We say that a group $(G, *)$ is *abelian* if the binary operation $*$ is abelian (commutative), that is,

$$x * y = y * x \text{ for all } x, y \in G.$$

The group $(\mathbb{Z}, +)$ defined above is clearly an abelian group. We now provide a (non-)example.

Example.

Let $\mathbb{R}^{n\times n}$ be the set of $n \times n$ real-valued matrices. Consider the set

$$\mathrm{GL}_n(\mathbb{R}) = \{A \in \mathbb{R}^{n\times n} : \det(A) \neq 0\}.$$

We claim that this set, considered under matrix multiplication, is a group. We first argue closure under matrix multiplication. Indeed, it follows from linear algebra that

$$\det(AB) = \det(A)\det(B),$$

and so the product of two matrices of nonzero determinant also has a nonzero determinant.

One can verify that matrix multiplication is associative. Note that I_n, the $n\times n$ identity matrix, acts as the identity for this group. Moreover, linear algebra tells us that if a matrix has nonzero determinant, then it has a two-sided inverse (say by applying row-echelon reduction).

1.2 Subgroups

An important concept in group theory is that of subgroups.

Definition 1.3: Subgroup

Let $(G, *)$ be a group. Then a subset $H \subset G$ is called a *subgroup* if it also forms a group under the binary operation $*$. We often denote this as $H \leq G$.

Here's a simple example, which you should verify for yourself.

Example.

Let a be an integer. Then the set $a\mathbb{Z} = \{na : n \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$.

In fact, this is a complete characterization of subgroups of $\mathbb{Z}$.

Proposition 1.4: Subgroups of the Integers

All subgroups of $\mathbb{Z}$ are of the form $a\mathbb{Z}$ for some integer a.

Proof. Consider a subgroup $H \leq \mathbb{Z}$. If $H = \{0\}$, then we are done (see the next proposition). Otherwise, consider there exists a minimal $a > 0$ in H (why?). We claim that $H = a\mathbb{Z}$.

For the first direction, note that H contains $a\mathbb{Z}$. This can be proven by induction.

For the other direction, consider an arbitrary $b \in H$. Using Euclidean division, we write $b = aq + r$ where $0 \leq r < a$. Since $b \in H$ and $a \in H$, then $r = b - aq \in H$. By minimality of a, we get that $r = 0$, as desired. □

1.2.1 Cyclic Groups

This idea can be generalized to an arbitrary group G. Let us write the group G under multiplcative notation, and consider an element $x \in G$. Consider $H = \{x^i : i \in \mathbb{Z}\}$. One can easily check that H is a subgroup of G, and in fact, it is the smallest subgroup of G containing H.

The following result, which appears as Proposition 2.4.2 in [**?**], allows us to characterize orders.

Proposition 1.5

Consider $x \in G$, and set S_x be the set of integers n such that $x^n = e_G$. Then S_x is a subgroup of $\mathbb{Z}$. Moreover, $x^r = x^s$ if and only if $r - s \in S_x$.

Definition 1.6: Order in a Group

Let x be an element of a group. Then $\text{ord}(x)$ is finite, is the smallest positive integer n such that $x^n = e_G$. Equivalently, it is the positive value of n such as $S_x = n\mathbb{Z}$.

Theorem 1.7: Groups of Prime Order

Let G be a finite group. If $|G|$ is prime, then G is cyclic.

Example.

Groups of Order 4

1.2.2 Properties

In general, we can prove some elementary yet very useful results about groups. We now state some elementary facts, which we leave as an exercise to the reader.

Proposition 1.8: Some elementary facts about groups

Let G and G' be groups with operations $*, *'$ respectively. Then the following results hold:

1. The inverse of an element in G is unique.
2. The identity element of G is unique.
3. If $xy = xz$ for elements $x, y, z \in G$, then $y = z$.
4. The relation $(xy)^{-1} = y^{-1}x^{-1}$ holds for all $x, y \in G$. [a]
5. G has at least two subgroups, $\{e_G\}$ and G itself.[b]
6. If $H \leq G$ and $x \in H$, then $\langle x \rangle \leq H$.
7. The product (G, G') under the operation $(*, *')$ is also a group.
8. The intersection of two subgroups of G is also a subgroup of G.
9. Let x be a group. The maps $\phi_g : G \to G$ sending $x \mapsto gx$ and $\phi^g : G \to G$ sending $x \mapsto xg$ are bijections.

[a] Does this remind you of something from linear algebra.

[b] Groups with only these two subgroups are called *simple*, and can be thought of as building blocks of groups. Does this remind you of anything?

1.3 Homomorphisms

Having defined a abstract object, one can ask how they can relate to each other: what are the "arrows" from a group the another. These are known as *homomorphisms*, named after Greek for *homo* (same) and *morphism* (of shape).

Definition 1.9: Homomorphisms

Let G_1, G_2 be two groups under the operations $*_1, *_2$ respectively. We say that a function $\phi : G_1 \to G_2$ is a *group homomorphism* if for all $g, g' \in G_1$,

$$\phi(gg') = \phi(g)\phi(g').$$

Example.

> We have shown that $\mathrm{GL}_n(\mathbb{R})$ is a group under matrix multiplication. The determinant function $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times$ is a group homomorphism from the group of invertible real matrices to the group of nonzero real numbers. This is because
>
> $$\det(AB) = \det(A)\det(B).$$

A homomorphism defines two special sets, which turn out to be very important. The first is the kernel, which encodes which elements are sent to the identity.

Definition 1.10: Kernel

The *kernel* of a group homomorphism $\phi : G_1 \to G_2$, denoted by $\ker(\phi)$ is given by

$$\ker(\phi) = \{g \in G_1 : \phi(g) = e_{G_2}\}.$$

Alternatively, it is the set of preimages of e_{G_2}.

The second is the image, which is simply the range of this map.

Definition 1.11: Image

The *image* of a group homomorphism $\phi : G_1 \to G_2$, denoted by $\mathrm{im}(\phi)$ is given by

$$\mathrm{im}(\phi) = \{x \in G_2 : x = \phi(g) \text{ for some } g \in G_1\}.$$

These subgroups control the properties of the group.

Proposition 1.12

A homomorphism is injective if and only if its kernel is trivial.

Example.

> In the above example, the kernel of the determinant map is the set of matrices whose determinant is exactly one. This is known as the *special linear group* $\mathrm{SL}_n(\mathbb{R})$.

Because of the added structure, the kernel "controls" a group homomorphism. To make this precise we state a few results on kernels, but before that, let us state someuseful facts about group homomorphisms.

Proposition 1.13: Elementary Facts about Group Homomorphisms

Let $\phi : G_1 \to G_2$ be a group homomoprhism. The following properties are true.

1. If $x_1, \cdots x_n$ are elements of G_1 then

$$\phi(x_1 \cdots x_n) = \phi(x_1) \cdots \phi(x_n).^a$$

2. The homomorphism sends the identity element to the identity element $\phi(e_{G_1}) = e_{G_2}$.

3. The homomorphism respects inversion:

$$\phi(x^{-1}) = \phi(x)^{-1}.$$

4. The kernel and the image are subgroups of G_1 and G_2, respectively.

5.

[a] Here, $x_1 \cdots x_n$ is the product under the G_1 group operation and $\phi(x_1) \cdots \phi(x_n)$ is the product under the G_2 group operation.

Definition 1.14: Group Isomorphism

A group homomorphism is called an *isomorphism* if it is both injective and surjective.

Example.

Exponential map $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \times)$

1.4 Cosets and Lagrange

Definition 1.15: Cosets

If $H \leq G$, then for any $a \in G$, we define the left coset

$$aH = \{ah : h \in H\}.$$

Lemma 1.16: Coset Properties

Let $H \leq G$ be subgroup.

1. The left cosets are all of equal size [a].
2. The left cosets of aH form an equivalence class on G under the relationship $a \sim b$ whenever $ab^{-1} \in H$. In particular, we can partition G into cosets.

[a] in bijection to each other

Definition 1.17: Index of a Subgroup

The number of cosets of H is called the *index* of H in G, and denoted as $[G : H]$.

Theorem 1.18: Lagrange's Theorem

If $H \leq G$, then

$$[G : H] = \frac{|G|}{|H|}.$$

In particular, we have that $|H|$ divides $|G|$ when G is a finite group. [a]

[a] This theorem makes sense even when H, G are infinite if we interpret the terms as cardinal numbers.

This has many applications, but we note one important one.

Corollary 1.19: Orders in a Finite Group

Let G be a finite group, and x and element of G. Then $\text{ord}(x)$ divides the order of the group. In particular, G has finite order.

Proof. Consider the subgroup $\langle x \rangle$ generated by x. This is a subgroup of G, and by Lagrange, its order divides the order of G. However, the order this subgroup is exactly the order of the element x. [1] □

1.5 Further Results

Theorem 1.20: Isomorphism Theorem

Let $\phi : G \to G'$ be a group isomorphism. Then

$$G/$$

Proposition 1.21: Kernel and Image

If $\phi : G \to G'$ is a group homomorphism then

$$|G| = |\ker G| \cdot |\operatorname{im} G|.$$

[1] Although we are using "order" to two different things, it should be clear from context which is which. Anyhow, the order of an element is the order of the subgroup it generates.

2 Re-expressing Previous Results

We devote this section to re-expressing previously proven results in the language of group theory.

2.1 Arithmetic

Theorem 2.1: GCD

Let a, b be nonzero integers. Then the subgroup $\langle a, b \rangle$ is exactly the subgroup generated by $\gcd(a, b)$.

Theorem 2.2: LCM

Let a, b be nonzero integers. Then the subgroup $\mathbb{Z}a \cap \mathbb{Z}b$ is exactly the subgroup generated by $\text{lcm}(a, b)$.

2.2 Fermat and Euler

Since Euler is a generalization of Fermat, we will only re-express Euler in the language of groups.

Recall Euler's theorem: that for any integer a such that a, n are coprime, then $a^{\varphi(n)} \equiv 1 \pmod{n}$, where φ is the Euler totient function.

Example.

> Let $n > 1$ be a positive integer. Consider the set of residues modulo n that are invertible (residues which are coprime to n). This forms a group which we denote as $(\mathbb{Z}/n\mathbb{Z})^\times$. One can check that it is a group, with closure and invertibility following from our results in the first week, with $\overline{1}$ (the residue corresponding to 1) being its identity. We will henceforth use 1 for simplicity.
>
> The group has order $\varphi(n)$, by definition. As such, it follows from Corollary [**?**] that the order of any element divides $\varphi(n)$. In particular, for any $x \in (\mathbb{Z}/n\mathbb{Z})^\times$, we have that $x^{\varphi(n)} = 1$. This is exactly the statement of Euler's theorem.

In fact, we can prove a very general statement.

Proposition 2.3: Order of the Group is an Order

Let G be a finite group. Then $x^{|G|} = 1$ for any $x \in G$.

2.3 Wilson

2.4 Chinese Remainder Theorem

The Chinese remainder theorem can be viewed as a group isomorphism.

Theorem 2.4: Chinese Remainder Theorem

Let m, n be coprime integers. Then the map

$$\phi : (\mathbb{Z}/mn\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$$

defined by the mapping

$$d \bmod mn \to (d \bmod m, d \bmod n)$$

is a group isomorphism.

2.5 Primitive Roots

Recall that a primitive root modulo n is an element whose order is exactly $\varphi(n)$. That is, in the language of group theory, it is an element $g \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $\text{ord}(g) = \varphi(n)$. We can say that

$$g \text{ is a primitive root} \Leftrightarrow \langle g \rangle = (\mathbb{Z}/n\mathbb{Z})^\times,$$

where the second condition means that g generates the group $(\mathbb{Z}/n\mathbb{Z})^\times$.

2.6 Quadratic Reciprocity

We can also express quadratic reciprocity in the language of group theory. This is in many ways a natural way to view things, and it is how one can prove the law of quadratic reciprocity using algebraic number theory.

Let p be an odd prime, and consider two groups: $(\mathbb{Z}/p\mathbb{Z})^\times$ and $\{\pm 1\}$. Recall that the Legendre symbol maps $(\mathbb{Z}/p\mathbb{Z})^\times$ to $\{\pm 1\}$, and since it satisfies

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right),$$

it is a group homomorphism. In fact, we can state more.

Proposition 2.5

There are only two group homomorphisms from $(\mathbb{Z}/p\mathbb{Z})^\times$ to $\{\pm 1\}$: the trivial homomorphism (sending all elements to 1) and the Legendre symbol.

Proof. Let ϕ be a homomorphism from $(\mathbb{Z}/p\mathbb{Z})^\times$ to $\{\pm 1\}$. By the existence of primitive roots, there exist g such that $(\mathbb{Z}/p\mathbb{Z})^\times = \langle g \rangle$. Note that $\phi(g)$ must be 1 or -1.

If $\phi(g) = 1$, then

$$\phi(g^i) = \phi(g)^i = 1^i = 1,$$

and so any element of $(\mathbb{Z}/p\mathbb{Z})^\times$ is sent to 1.

If $\phi(g) = -1$, then

$$\phi(g^i) = \phi(g)^i = (-1)^i.$$

This means that $\phi(g^i)$ is 1 if and only if g^i is a square, which is exactly the definition of the Legendre symbol. □

This proof also highlights a simple yet important principle: that any group homomorphism from G_1 to G_2 is uniquely determined by its values at the generators of G_1.

3 Elliptic Curves

3.1 One Last Ounce of Algebra

Definition 3.1: Field

Definition 3.2: Characteristic

3.2 Definition and Examples

Definition 3.3: Elliptic Curve

An elliptic curve over k is a set of solutions to an equation of the form $y^2 = x^3 + Ax + B$ where $x, y \in k$.

3.3 Group Operations

Definition 3.4: Elliptic Curve

An elliptic curve E/k is a set of solutions to an equation of the form

$$E : y^2 = x^3 + Ax + B$$

together with an extra point at infinity $\mathcal{O}$, where

$$4A^3 + 27B^2 \neq 0.$$

3.4 Elementary Properties

Theorem 3.5: Hasse Bound

Let E be an elliptic curve over $\mathbb{F}_p$. Then

$$\#E(\mathbb{F}_p) = p + 1 - t_p$$

where

$$|t_p| \leq 2\sqrt{p}.$$

Definition 3.6: Frobenius Trace

The quantity $t_p := p + 1 - \#E(\mathbb{F}_p)$ is called the *trace of Frobenius* of $E/\mathbb{F}_p$.