

---

# ALGEBRA 3 NOTES

NICHOLAS HAYEK

*Lectures by Prof. Henri Darmon*

---

## CONTENTS

<b>I Groups</b>	<b>1</b>
Axioms and First Properties	1

# I Groups

8/28/24

In Algebra 3, we will study abstract algebraic structures. Chiefly among them, we have *groups*, which are useful in representing symmetries, *rings & fields*, which help us think about number systems, and *vector spaces & modules*, which encode physical space.

## AXIOMS AND FIRST PROPERTIES

A *group* is a set  $G$  endowed with a binary composition  $G \times G \rightarrow G$  such that the following axioms hold:

1.  $\exists e \in G$ , an identity element, such that  $e * a = a * e = a \ \forall a \in G$ .
2.  $\forall a \in G, \exists a' \in G$  such that  $a * a' = a' * a = e$ .
3.  $a * (b * c) = (a * b) * c \ \forall a, b, c \in G$ .

If  $a * b = b * a \ \forall a, b \in G$ , we call  $G$  *commutative*.

Why do we care about groups? If  $X$  is an object, we call a *symmetry* of  $X$  a function  $X \rightarrow X$  which preserves the structure of the object.

e.g. a polygon, graphs, tilings, "crystal," "molecules," rings, vector spaces, metric spaces, manifolds

The collection of symmetries,  $\text{Aut}(X) = \{f : X \rightarrow X\}$ , we can structure as a group: let  $*$  be composition,  $e = \text{Id}$ , and  $f \in \text{Aut}(X)$  (note that, by axiom 2, these must be bijective).

A note on notation: for non-commutative groups, we write  $a * b = ab$ ,  $e = 1$  or  $\mathbb{1}$ ,  $a' = a^{-1}$ , and  $a^n = \underbrace{a \cdot \dots \cdot a}_{n \text{ times}}$ . This is called *multiplicative notation*. For commutative rings, we write  $a * b = a + b$ ,  $e = 0$  or  $\mathbb{0}$ ,  $a' = -a$ , and  $na = \underbrace{a + \dots + a}_{n \text{ times}}$ .

The following are some examples of groups generated by sets:

1. If  $X$  is a set with no operations,  $\text{Aut}(X)$  is the set of all bijections  $f : X \rightarrow X$ . One calls this the *permutation group*, or, if  $|X| = n < \infty$ , the *symmetric group*, and we write  $\text{Aut}(X) = S_n$ .
2. If  $V$  is a vector space over  $\mathbb{F}$ ,  $\text{Aut}(V) = \{T : V \rightarrow V\}$ , the set of vector space isomorphism. If  $\dim(V) = n$ , recall that we associate  $V$  with  $\mathbb{F}^n$ , whose set of isomorphism is given by  $GL_n(\mathbb{F})$ , the collection of  $n \times n$  invertible matrices. This is called the *linear group*.
3. If  $R$  is a ring, then  $(R, +, \mathbb{0})$  is a commutative group. Furthermore,  $(R^\times, \times, \mathbb{1})$  is a non-commutative group, where  $R^\times := R \setminus \{\text{non-invertible elements of } R\}$ .
4. If  $V$  is Euclidean space endowed with a dot product, where  $\mathbb{F} = \mathbb{R}$ , with  $\dim(V) < \infty$ ,  $\text{Aut}(V) = O(V)$  is called the *orthogonal group of  $V$* . In particular,  $O(V) = \{T : V \rightarrow V : T(u) \cdot T(v) = u \cdot v\}$ .

5. If  $X$  is a geometric figure (e.g. a polygon), we write  $\text{Aut}(X) = D_n$ , where  $|\text{Aut}(X)| = n$ , and call this the *dihedral group*.

A *homomorphism* from groups  $G_1 \rightarrow G_2$  is a function  $\varphi : G_1 \rightarrow G_2$  satisfying  $\varphi(ab) = \varphi(a)\varphi(b)$ , where  $a, b \in G_1$ .

$\varphi(1_{G_1}) = 1_{G_2}$  and  $\varphi(a^{-1}) = \varphi(a)^{-1} \forall a \in G_1$ .

8/30/23

PROP. 1.1

PROOF.

$$\begin{aligned} \varphi(1_{G_1}) &= \varphi(1_{G_1}^2) = \varphi(1_{G_1})^2 \implies \varphi(1_{G_1}) = \varphi(1_{G_1}^{-1})\varphi(1_{G_1}) = 1_{G_2}. \\ \varphi(a^{-1})\varphi(a) &= \varphi(a^{-1}a) = \varphi(1_{G_1}) = 1_{G_2} \implies \varphi(a^{-1}) = \varphi(a)^{-1}. \end{aligned}$$

□

A homomorphism which is bijective is called an *isomorphism*. If there exists an isomorphism between two groups  $G_1$  and  $G_2$ , we call them *isomorphic*, and write  $G_1 \cong G_2$ . One can thus call  $\text{Aut}(G)$  the set of isomorphisms from  $G \rightarrow G$ .

As an example, take  $G = \mathbb{Z}/n\mathbb{Z} = \{0, 1, \dots, n-1\}$ . Note that  $\varphi : G \rightarrow G$  is determined entirely by  $\varphi(1)$ , since  $\varphi(i) = \underbrace{\varphi(1 + \dots + 1)}_{i \text{ times}} = \underbrace{\varphi(1) + \dots + \varphi(1)}_{i \text{ times}}$ . How can we find

an element of  $\text{Aut}(G)$ ? Clearly, not all mappings  $\varphi(1)$  are bijective: take  $n$  to be even and  $\varphi(1) = 2$ . Then  $\varphi(2) = 4, \varphi(3) = 6, \dots, \varphi(n/2) = 0$ , so  $\varphi$  is not surjective. We know then that  $\varphi(G) = \varphi(1)\mathbb{Z} \pmod n$ , and would like  $\varphi(G) = G$ . If  $\varphi(1)$  and  $n$  are co-prime, then we can write  $k\varphi(1) + ln = k\varphi = 1$ , so every element can be reached.

We can construct a group isomorphism  $\eta : \text{Aut}(\mathbb{Z}/n\mathbb{Z}) \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times$  which sends  $\varphi \rightarrow \varphi(1)$ . Clearly  $\eta(\varphi_{t_1} \circ \varphi_{t_2}) = \varphi_{t_1} \circ \varphi_{t_2}(1) = \varphi_{t_1}(t_2) = t_1 t_2 = \eta(\varphi_{t_1})\eta(\varphi_{t_2})$ , so  $\eta$  is a homomorphism. It is also bijective: given  $\varphi(1)$ , we can deduce a mapping for each element.

For a group  $G$  and an object  $X$ , define an *action* to be a function from  $G \times X \rightarrow X$  such that

1.  $1 \times x = x$
2.  $(g_1 g_2)x = g_1(g_2 x)$

for  $x \in X, g_1, g_2 \in G$ . One can create from this the automorphism  $m_g : x \rightarrow gx$  of  $X$ : if  $gx_1 = gx_2$ , one can take the group inverse to conclude  $x_1 = x_2$ . Similarly, given  $x \in X$ , we know  $m_g(g^{-1}x) = x$ .

PROP. 1.2

Given an action of  $G$  on  $X$ , the assignment  $g \rightarrow m_g$  is a homomorphism between  $G \rightarrow \text{Aut}(X)$ .

PROOF.

$$m_{g_1 g_2}(x) = g_1 g_2 x = g_1(g_2 x) = g_1 m_{g_2}(x) = m_{g_1}(m_{g_2}(x)) = m_{g_1} \circ m_{g_2}(x)$$

□

9/4/24

In fact, given a homomorphism of this form, one can extract the group action.

A  $G$ -set is a set  $X$  endowed with a group action of  $G$ . If  $\forall x, y \in X, \exists g \in G : gx = y$ , we say that this  $G$ -set is *transitive*. Finally, a transitive  $G$ -set of a subset of  $X$  (“ $G$ -subset of  $X$ ”) is called an *orbit* of  $G$  on  $X$ .

Every  $G$ -set is a disjoint union of orbits.

PROP 1.3

We define a relation on  $X$  as follows:  $x \underset{G}{\sim} y$  if  $\exists g : gx = y$ . This is an equivalence relation:

PROOF.

1. Take  $g = 1$ . Then  $1x = x$ , so  $x \underset{G}{\sim} x$ .
2. If  $gx = y$ , then  $g^{-1}y = x$ , so  $x \underset{G}{\sim} y \implies y \underset{G}{\sim} x$ .
3. If  $gx = y$  and  $hy = z$ , then  $hgx = z$ , so  $x \underset{G}{\sim} y \wedge y \underset{G}{\sim} z \implies x \underset{G}{\sim} z$ .

From prior theory, we know that equivalence classes of an equivalence relation on  $X$  form a partition of  $X$ . However, by definition, the equivalence classes of the above relation are exactly the orbits of the  $G$ -set on  $X$ .  $\square$

We denote the set of equivalence classes defined in the proof above  $X/G$ .

### Examples:

1. Let  $X = \{\clubsuit\}$ ,  $G$  be a group, and  $g\clubsuit = \clubsuit$ . This is a group action. The homomorphism  $m : G \rightarrow \text{Aut}(X) = S_1$  sends  $g$  to the identity.
2. Let  $X = G$ ,  $G$  be a group, and  $gx = gx$  (group action on the LHS, left-multiplication on the RHS). We have the homomorphism  $m : G \rightarrow \text{Aut}(G)$  such that  $m(g)(x) = gx = gx$ . This is an injective function, since we can always take the group inverse, i.e.  $m(h)(x) = m(g)(x) \implies g = h$ . Thus,  $G \cong m(G) \subseteq \text{Aut}(G)$ .
3. Let  $X = G$  as before, but let  $gx = xg^{-1}$ . We can check that this is a group action: (1)  $1 * x = x1^{-1} = x1 = x$  and (2)  $g * (h * x) = (h * x)g^{-1} = xh^{-1}g^{-1}$ , where  $(gh) * x = x(gh)^{-1} = xh^{-1}g^{-1} \implies g * (h * x) = (gh) * x$ .
4. Letting  $X = G \times G$ , we can form a group action from both left- and right-multiplication:  $(g, h) * x = gxh^{-1}$ . One can check its validity.

### 1.1 Cayley

Every group  $G$  is isomorphic of a group of permutations (i.e. a subgroup of

a symmetric group). If  $G$  is finite, then  $G$  is isomorphic to  $S_n$ , where  $n = |G|$ .

If  $X_1$  and  $X_2$  are  $G$ -sets, then an *isomorphism* from  $X_1$  to  $X_2$  is a bijection  $\varphi : X_1 \rightarrow X_2$  such that  $\varphi(gx) = g\varphi(x) \forall x \in X_1, g \in G$ .

SOME STUFF