
ALGEBRA 3 NOTES

NICHOLAS HAYEK

Lectures by Prof. Henri Darmon

CONTENTS

I Groups	1
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*.

8/30/23

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 $a, b \in G_1$.

PROP. 1.1

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

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 φ 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 η 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 $\varphi(gx) = g\varphi(x) \forall x \in X_1, g \in G$.

Let $H < G$. Define G/H to be the set of orbits for right action on G , i.e. $\{aH : a \in G\}$, where $aH = \{ah : h \in H\}$. We call these *left cosets*. We also have *right cosets*, $\{Ha : a \in G\}$.

For example, take $G = S_3$ and $H = \{1, (12)\}$. Then $G/H = \{\{1, (12)\}, \{(13), (123)\}\} = \{H, (13)H\}$ and $H \setminus G = \{\{1, (12)\}, \{(13), (132)\}, \{(23), (123)\}\}$.

1.2 Size of Cosets

Let $H < G$. If H is finite, then $|H| = |aH| \forall a \in G$.

As proof of this fact, one may take the bijection $\varphi : H \rightarrow aH : \varphi(h) = ah$.

1.3 Lagrange

Let G be finite. The cardinality of any subgroup $H < G$ divides the cardinality of G . In particular, $|G| = |H| \cdot |G/H|$.

Define the *stabilizer* of an element of a G -set $x_0 \in X$ to be $\{g \in G : g \otimes x_0 = x_0\}$.

If X is a transitive G -set, then $\exists H < G$ such that $X \cong G/H$ as a G -set.

Choose $x_0 \in X$. Define $H = \text{stab}(x_0) := \{g \in G : g \otimes x_0 = x_0\}$. One may show that H is indeed a subgroup. We then define $\varphi : G/H \rightarrow X$ such that $gH \rightarrow gx_0$. Checking some properties:

1. φ is well defined. If $gH = g'H$, then $\exists h : gh = g'$. Then $\varphi(gH) = gx_0$ and $\varphi(g'H) = g'x_0 = ghx_0$. But $h \in \text{stab}(x_0)$, so this is just gx_0 .
2. φ is surjective. This follows from the fact that X is transitive: for $x, x_0 \in X, \exists g \in G$ with $gx_0 = x$. Then $\varphi(gH) = gx_0 = x$.
3. φ is injective. Take $g_1x_0 = g_2x_0$. Then $g_2^{-1}g_1x_0 = x_0$, so $g_2^{-1}g_1 \in H$, i.e. $g_2H = g_1H$.
4. φ is a G -set isomorphism. $\varphi(g \otimes aH) = \varphi(gaH) = gax_0 = g\varphi(aH)$. \square

1.4 Orbit-Stabilizer

If X is a transitive G -set, $x_0 \in X$, and $|G| < \infty$, then $X \cong G/\text{stab}_G(x_0)$. In particular, $|G| = |X| \cdot |\text{stab}_G(x_0)|$

9/6/24

PROP 1.4

PROOF.

Given $H < G$, we say $h_1, h_2 \in H$ are *conjugate* if $\exists g : g^{-1}h_1g = h_2$, or, equivalently, $gh_1g^{-1} = h_2$. Given $H_1, H_2 < G$, we say H_1 and H_2 are *conjugate equivalent* if every element in H_1 is conjugate to some element in H_2 .

Stabilizers of elements in a transitive G -set X are conjugate equivalent.

PROP 1.5

Let $x_1, x_2 \in X$ and consider $\text{stab}(x_1), \text{stab}(x_2)$. Since X is transitive, $\exists g : gx_1 = x_2$. Thus, if $h \in \text{stab}(x_2)$, i.e. $hx_2 = x_2$, then $hgx_1 = gx_1 \implies g^{-1}hgx_1 = x_1 \implies g^{-1}hg \in \text{stab}(x_1)$. Thus, there exists a conjugation of every element in $\text{stab}(x_2)$ which is an element in $\text{stab}(x_1)$. One shows the converse similarly to conclude that $\text{stab}(x_1)$ and $\text{stab}(x_2)$ are conjugate equivalent. \square

PROOF.

We can show a natural bijection between the “pointed G -sets” (X, x_0) with subgroups of G : send $(X, x_0) \rightarrow \text{stab}(x_0)$ and $H \rightarrow (G/H, H)$. This establishes the intuition that the number of transitive G -sets up to isomorphism is exactly the number of subgroups of G up to conjugation.

PROP 1.6

Consider an isomorphism class P of pointed G -sets, i.e. $\forall (X, x_0), (Y, y_0) \in P$, $X \cong Y$. Consider the mapping $\Phi : (X, x_0) \in P \rightarrow \text{stab}(x_0)$. The image of this mapping is a conjugation class: since $X \cong Y$, we know that there exists a unique mapping $\varphi(y_0) = x_k$. Since X is transitive, $\exists g : gx_k = x_0$. Then $h \in \text{stab}(x_0) \implies hx_0 = x_0 \implies hgx_k = gx_k \implies hg\varphi(y_0) = g\varphi(y_0) \implies \varphi(hgy_0) = \varphi(gy_0) \implies hgy_0 = gy_0 \implies g^{-1}hg \in \text{stab}(y_0)$.

PROOF.

Conversely, one can show that the image of the mapping $\Xi : H \rightarrow (G/H, H)$ over a conjugation class $I : \forall F, H \in I, \exists g \in G : g^{-1}Fg = H$ is an isomorphism class over G -sets.

Thus, the set of G -sets up to isomorphism is in bijection with the set of $H < G$ up to conjugation. \square

♠ Examples ♣

1. Let $H = G$. Then $G/H = \{H\}$. $X = \{*\} \cong G/H$. Similarly, if $H = 1$, then $G/H \cong G = X$.
2. Let $G = S_n$. Let $X = \{1, 2, \dots, n\}$. For $n \in X$, $X \cong G/\text{stab}(n) = G/S_{n-1}$.
3. Let X be a regular tetrahedron. Let $G = \text{Aut}(X)$ (the set of rigid motions). Notate $X = \{1, 2, 3, 4\}$ (for each vertex). Then G acts transitively on X . In particular, $\text{stab}(1) = \mathbb{Z}3 \implies |G| = 4 \cdot 3 = 12$.
4. Let $G = \text{Aut}(X)$ on a tetrahedron, this time *including* reflections. Then $G = S_4$, since one can always send $a \rightarrow b$ by reflecting through a plane intersecting c, d .

5. Let X be a cube, $G = \text{Aut}(X)$, the rigid motions on X . Note that there are 6 faces, 12 edges, and 8 vertices. If x_0 is a face, then $\text{stab}(x_0)$ are exactly the rotations about the axis intersecting the face, i.e. $|\text{stab}(x_0)| = 4$, so $|G| = 6 \cdot 4 = 24$. As $4! = 24$, it is tempting to consider that $G \cong S_4$. This turns out to be true: let G act on opposite

PROP 1.7

If $\varphi : G \rightarrow H$ is a homomorphism, then φ is injective $\iff \varphi(g) = 1 \implies g = 1 \forall g \in G$.

PROOF.

Let $\varphi(g) = 1$ and φ be injective. Then $\varphi(g^2) = \varphi(g) \implies g^2 = g \implies g = 1$.

Let $\varphi(g) = 1 \implies g = 1$. Then $\varphi(a) = \varphi(b) \implies \varphi(b^{-1}a) = 1 \implies b^{-1}a = 1 \implies a = b$, so φ is injective. \square

Define $\ker(\varphi) := \{g \in G : \varphi(g) = 1\}$. This is a subgroup.

Observe that, for $g \in G, h \in \ker(\varphi)$, we have $g^{-1}hg \in \ker(\varphi)$. Subgroups which obey this property are called *normal subgroups*.

PROP 1.8

If N is normal, then $G/N = N/G$, i.e. $gN = Ng \forall g$. One can view G/N as a group with $g_1N \cdot g_2N = g_1g_2N$, and $1_{G/N} = N$.

PROOF.

$gN = \{gn : n \in N\} = \{gg^{-1}ng : n \in N\} = \{ng : n \in N\} = Ng$. The group operations follow immediately. \square

1.5 Isomorphism Theorem for Groups

If $\varphi : G \rightarrow H$ is a homomorphism, $N = \ker(\varphi)$, then φ induces an injective homomorphism $\bar{\varphi} : G/N \hookrightarrow H : \bar{\varphi}(aN) = \varphi(a)$.

PROOF.

$\bar{\varphi}$ being a homomorphism follows from the fact that φ is a homomorphism. For injectivity, see that $\bar{\varphi}(aN) = 1 \implies \varphi(a) = 1 \implies a = 1$. \square