MATH456 - Algebra 3

Based on lectures from Fall 2024 by Prof. Henri Darmon.
Notes by Louis Meunier

Contents

1 Groups

1.1 Review

↪**Definition 1.1** (Group): A **group** is a set G endowed with a binary composition rule $G \times G \to G, (a, b) \mapsto a \star b$, satisfying

1. $\exists e \in G$ s.t. $a \star e = e \star a = a \forall a \in G$
2. $\forall a \in G, \exists a' \in G$ s.t. $a \star a' = a' \star a = e$
3. $\forall a, b, c \in G, (a \star b) \star c = a \star (b \star c)$.

If the operation on G also commutative for all elements in G, we say that G is *abelian* or *commutative*, in which case we typically adopt additive notation (i.e. $a + b$, $a^{-1} = -a$, etc).

⊛ **Example 1.1**: An easy way to "generate" groups is consider some "object" X (be it a set, a vector space, a geometric object, etc.) and consider the set of symmetries of X, denoted $\mathrm{Aut}(X)$, i.e. the set of bijections of X that preserve some desired quality of X.

1. If X just a set with no additional structure, $\mathrm{Aut}(X)$ is just the group of permutations of X. In particular, if X finite, then $\mathrm{Aut}(X) \cong S_{\#X}$.
2. If X a vector space over some field $\mathbb{F}$, $\mathrm{Aut}(X) = \{T : X \to X \mid \text{linear, invertible}\}$. If $\dim(X) = n < \infty$, $X \cong \mathbb{F}^n$ as a vector space, hence $\mathrm{Aut}(X) = \mathrm{GL}_n(\mathbb{F})$, the "general linear group" consisting of invertible $n \times n$ matrices with entires in $\mathbb{F}$.
3. If X a ring, we can always derive two groups from it; $(R, +, 0)$, which is always commutative, using the addition in the ring, and $(R^\times, \times, 1)$, the units under multiplication (need to consider the units such that inverses exist in the group).
4. If X a regular n-gon, $\mathrm{Aut}(X)$ can be considered the group of symmetries of the polygon that leave it globally invariant. We typically denote this group by D_{2n}.
5. If X a vector space over $\mathbb{R}$ endowed with an inner product $(\cdot, \cdot) : V \times V \to \mathbb{R}$, with $\dim V < \infty$, we have $\mathrm{Aut}(V) = O(V) = \{T : V \to V \mid T(v \cdot w) = v \cdot w \forall v, w \in V\}$, the "orthogonal group".

↪**Definition 1.2** (Group Homomorphism): Given two groups G_1, G_2, a *group homomorphism* $\varphi : G_1 \to G_2$ is a function satisfying $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G_1$.

If φ is bijective, we call it an *isomorphism* and say G_1, G_2 are *isomorphic*.

↳**Proposition 1.1**:

- $\varphi\left(1_{G_1}\right) = 1_{G_2}$
- $\varphi(a^{-1}) = \varphi(a)^{-1}$

⊛ **Example 1.2**: Let $G = \mathbb{Z}/n\mathbb{Z} = \{0, ..., n-1\}$ be the cyclic group of order n. Let $\varphi \in \operatorname{Aut}(G)$; it is completely determined by $\varphi(1)$, as $\varphi(k) = k \cdot \varphi(1)$ for any k. Moreover, it must be then that $\varphi(1)$ is a generate of G, hence $\varphi(1) \in (\mathbb{Z}/n\mathbb{Z})^\times$ (ie the units of the group considered as a ring), and thus

$$\operatorname{Aut}(G) \cong ((\mathbb{Z}/n\mathbb{Z})^\times, *).$$

1.2 Actions of Groups

↪**Definition 1.3** (Group Action): An *action* of G on an object X is a function $G \times X \to X, (g, x) \mapsto g \cdot$ such that

- $1 \cdot x = x$
- $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$
- $m_g : x \mapsto g \cdot x$ an *automorphism* of X.

↳**Proposition 1.2**: The map $m : G \to \operatorname{Aut}(X), g \mapsto m_g$ a group homomorphism.

Proof. One need show $m_{g_1 g_2} = m_{g_1} \circ m_{g_2}$. ■

↪**Definition 1.4** (G-set): A G*-set* is a set X endowed with an action of G.

↪**Definition 1.5** (Transitive): We say a G-set X is *transitive* if $\forall x, y \in X$, there is a $g \in G$ such that $g \cdot x = y$.

A transitive G-subset of X is called on *orbit* of G on X.

↳**Proposition 1.3**: Every G-set is a disjoint union of orbits.

Proof. Define a relation on X by $x \sim y$ if there exists a $g \in G$ such that $g \cdot x = y$. One can prove this is an equivalence relation on X. Equivalence relations partition sets into equivalence classes, which we denote in this case by X/G. The proof is done by remarking that an equivalence class is precisely an orbit. ■

Remark 1.2.1: As with most abstract objects, we are more interested in classifying them up to isomorphism. The same follows for G-sets.

↪**Definition 1.6**: An *isomorphism of G-sets* is a map between G-sets that respects the group actions. Specifically, if G a group and X_1, X_2 are G-sets, with the action G on X_1 denoted $\star$ and G on X_2 denoted $*$, then an isomorphism is a bijection

$$f : X_1 \to X_2,$$

such that

$$f(g \star x) = g * f(x)$$

for all $g \in G$, $x \in X_1$.

↪**Definition 1.7** (Cosets): Let $H \subseteq G$ be a subgroup of a group G. Then G carries a natural structure as an H set; namely we can define

$$H \times G \to g, \quad (h, g) \mapsto g \cdot h,$$

which can readily be seen to be a well-defined group action. We call, in this case, the set of orbits of the action of H on G *left cosets* of H in G, denoted

$$\begin{aligned} G/H &= \{\text{orbits of } H \text{ acting on } G\} \\ &= \{aH : a \in G\} = \{\{ah : h \in H\} : a \in G\} \subseteq 2^G. \end{aligned}$$

Symmetric definitions give rise to the set of *right cosets* of H in G, denoted $H \setminus G$, of orbits of H acting by left multiplication on G.

Remark 1.2.2: In general, $G/H \neq H \setminus G$. Further, note that at face value these are nothing more than sets; in general they will not have any natural group structure. They do, however, have a natural structure as G-sets, as a theorem to follow will elucidate.

↪**Theorem 1.1**: Let $H \subseteq G$ be a finite subgroup of a group G. Then every coset of H in G has the same cardinality.

Proof. Define the map $H \mapsto aH$ by $h \mapsto ah$. This is a bijection. ■

Remark 1.2.3: In general, if one considers the general action of G on some set X, then the orbits X/G need not all have the same size, though they do partition the set. It is in the special case where X a group and G a subgroup of X that we can guarantee equal-sized partitions.

↳**Theorem 1.2** (Lagrange's): Let G be a finite group and H a subgroup. Then

$$\#G = \#H \cdot \#(G/H).$$

In particular, $\#H \mid \#G$ for any subgroup H.

Proof. We know that G/H is a partition of G, so eg $G = H \sqcup H_1 \sqcup \cdots \sqcup H_n$. By the previous theorem, each of these partitions are the same size, hence

$$\begin{aligned}\#G &= \#(H \sqcup H_1 \sqcup \cdots \sqcup H_n) \\ &= \#H + \#H_1 + \cdots + \#H_{n-1} \quad \text{since } H_i\text{'s disjoint} \\ &= n \cdot \#H \quad \text{since each } H \text{ same cardinality} \\ &= \#(G/H) \cdot \#H.\end{aligned}$$

■

↳**Proposition 1.4**: G/H has a natural left-action of G given by

$$G \times G/H \to G/H, \quad (g, aH) \mapsto (ga)H.$$

Further, this action is always transitive.

↳**Proposition 1.5**: If X is a transitive G-set, there exists a subgroup $H \subseteq G$ such that $X \cong G/H$ as a G-set.

In short, then, it suffices to consider coset spaces G/H to characterize G-sets.

Proof. Fix $x_0 \in X$, and define the *stabilizer* of x_0 by

$$H := \mathrm{Stab}_G(x_0) := \{g \in G : gx_0 = x_0\}.$$

One can verify H indeed a subgroup of G. Define now a function

$$f : G/H \to X, \quad gH \mapsto g \cdot x_0,$$

which we aim to show is an isomorphism of G-sets.

First, note that this is well-defined, i.e. independent of choice of coset representative. Let $gH = g'H$, that is $\exists h \in H$ s.t. $g = g'h$. Then,

$$f(gH) = gx_0 = (g'h)x_0 = g'(hx_0) = g'x_0 = f(g'H),$$

since h is in the stabilizer of x_0.

For surjectivity, we have that for any $y \in X$, there exists some $g \in G$ such that $gx_0 = y$, by transitivity of the group action on X. Hence,

$$f(gH) = gx_0 = y$$

and so f surjective.

For injectivity, we have that

$$\begin{aligned} g_1 x_0 = g_2 x_0 &\Rightarrow g_2^{-1} g_1 x_0 = x_0 \\ &\Rightarrow g_2^{-1} g_1 \in H \\ &\Rightarrow g_2 h = g_1 \text{ for some } h \in H \\ &\Rightarrow g_2 H = g_1 H, \end{aligned}$$

as required.

Finally, we have that for any coset aH and $g \in G$, that

$$f(g(aH)) = f((ga)H) = (ga)x_0,$$

and on the other hand

$$gf(aH) = g(ax_0) = (ga)x_0.$$

Note that we were very casual with the notation in these final two lines; make sure it is clear what each "multiplication" refers to, be it group action on X or actual group multiplication. ∎

↳**Corollary 1.1**: If X is a transitive G set with G finite, then $\#X \mid \#G$. More precisely,

$$X \cong G/\mathrm{Stab}_G(x_0)$$

for any $x_0 \in X$. In particular, the *orbit-stabilizer formula* holds:

$$\#G = \#X \cdot \#\mathrm{Stab}_G(x_0).$$

The assignment $X \to H$ for subgroups H of G is not well-defined in general; given $x_1, x_2 \in X$, we ask how $\mathrm{Stab}_G(x_1)$, $\mathrm{Stab}_G(x_2)$ are related?

Since X transitive, then there must exist some $g \in G$ such that $x_2 = gx_1$. Let $h \in \mathrm{Stab}(x_2)$. Then,

$$hx_1 = x_2 \Rightarrow (hg)x_1 = gx_1 \Rightarrow g^{-1}hgx_1 = x_1,$$

hence $g^{-1}hg \in \mathrm{Stab}\ (x_1)$ for all $g \in G$, $h \in \mathrm{Stab}(x_2)$. So, putting $H_i = \mathrm{Stab}\ (x_i)$, we have that

$$H_2 = gH_1g^{-1}.$$

This induces natural bijections

$$\begin{aligned} \{\text{pointed transitive } G-\text{sets}\} &\leftrightarrow \{\text{subgroups of } G\} \\ (X, x_0) &\rightsquigarrow H = \mathrm{Stab}(x_0) \\ (G/H, H) &\leftarrow\!\!\!\!\!\sim H, \end{aligned}$$

and

$$\begin{aligned} \{\text{transitive } G-\text{sets}\} &\leftrightarrow \{\text{subgroups of } G\}/\text{ conjugation} \\ H_i &= gH_jg^{-1}, \text{some } g \in G. \end{aligned}$$

Given a G, then, we classify all transitive G-sets of a given size n, up to isomorphism, by classifying conjugacy classes of subgroups of "index n" $:= [G : H] = \frac{\#G}{n} = \#(G/H)$.

⊛ **Example 1.3**:

0. $G, \{e\}$ are always subgroups of any G, which give rise to the coset spaces $X = \{\star\}, G$ respectively. The first is "not faithful" (not injective into the group of permutations), and the second gives rise to an injection $G \hookrightarrow S_G$.
1. Let $G = S_n$. We can view $X = \{1, ..., n\}$ as a transitive S_n-set. We should be able to view X as G/H, where $\#(G/H) = \#X = n = \frac{\#G}{\#}(H) = \frac{n!}{\#H}$, i.e. we seek an $H \subset G$ such that $\#H = \frac{n!}{n} = (n-1)!$.

Moreover, we should have H as the stabilizer of some element $x_0 \in \{1, ..., n\}$; so, fixing for instance $1 \in \{1, ..., n\}$, we have $H = \mathrm{Stab}(1)$, i.e. the permutations of $\{1, ..., n\}$ that leave 1 fixed. But we can simply see this as the permutation group on $n-1$ elements, i.e. S_{n-1}, and thus $X \cong S_n / S_{n-1}$. Remark moreover that this works out with the required size of the subgroup, since $\#S_{n-1} = (n-1)!$.

2. Let $X =$ regular tetrahedron and consider

$$G = \mathrm{Aut}(X) := \{\text{rotations leaving } X \text{ globally invariant}\}.$$

We can easily compute the size of G without necessarily knowing G by utilizing the orbit-stabilizer theorem (and from there, somewhat easily deduce G). We can view the tetrahedron as the set $\{1, 2, 3, 4\}$, labeling the vertices, and so we must have

$$\#G = \#X \cdot \# \ \mathrm{Stab}(1),$$

where $\mathrm{Stab}(1) \cong \mathbb{Z}/3\mathbb{Z}$. Hence $\#G = 12$.

From here, there are several candidates for G; for instance, $\mathbb{Z}/12\mathbb{Z}$, D_{12}, A_4, ... Since X can be viewed as the set $\{1, 2, 3, 4\}$, we can view $X \rightsquigarrow G \hookrightarrow S_4$, where $\hookrightarrow$ an injective homomorphism, that is, embed G as a subgroup S_4. We can show both D_{12} and $\mathbb{Z}/12\mathbb{Z}$ cannot be realized as such (by considering the order of elements in each; there exists an element in D_{12} of order 6, which does not exist in S_4, and there exists an element in $\mathbb{Z}/12\mathbb{Z}$ of order 12 which also doesn't exist in S_4). We can embed $A_4 \subset S_4$, and moreover $G \cong A_4$. If we were to extend G to include planar reflections as well that preserve X, then our G is actually isomorphic to all of S_4.

4. Let X be the cube, $G = \{\text{rotations of } X\}$. There are several ways we can view X as a transitive G sets; for instance $F =$ faces, $E =$ edges, $V =$ vertices, where $\#F = 6, \#E = 12, \#V = 8$. Let's work with F, being the smallest. Letting $x_0 \in F$, we have that $\mathrm{Stab}\ (x_0) \cong \mathbb{Z}/4\mathbb{Z}$ so the orbit-stabilizer theorem gives $\#G = 24$.

This seems to perhaps imply that $G = S_4$, since $\#S_4 = 24$. But this further implies that if this is the case, we should be able to consider some group of size 4 "in the cube" on which G acts.

1.3 Homomorphisms, Isomorphisms, Kernels

↳**Proposition 1.6**: If $\varphi : G \to H$ a homomorphism, φ injective iff φ has a trivial kernel, that is, $\ker \varphi = \{a \in G : \varphi(a) = e_H\} = \{e\}$.

↪**Definition 1.8** (Normal subgroup): A subgroup $N \subset G$ is called *normal* if for all $g \in G, h \in N$, then $ghg^{-1} \in N$.

↪**Proposition 1.7**: The kernel of a group homomorphism $\varphi : G \to H$ is a normal subgroup of G.

↪**Proposition 1.8**: Let $N \subset G$ be a normal subgroup. Then $G/N = N \setminus G$ (that is, $gN = Ng$) and G/N a group under the rule $(g_1 N)(g_2 N) = (g_1 g_2)N$.

↪**Theorem 1.3** (Fundamental Isomorphism Theorem): If $\varphi : G \to H$ a homomorphism with $N := \ker \varphi$, then φ induces an injective homomorphism $\overline{\varphi} : G/N \hookrightarrow H$ with $\overline{\varphi}(aN) := \varphi(a)$.

↪**Corollary 1.2**: $\mathrm{im}(\varphi) \cong G/N$, by $\overline{\varphi}$ into $\mathrm{im}(\overline{\varphi})$.

⊛ **Example 1.4**: We return to the cube example. Let $\tilde{G} = \widetilde{\mathrm{Aut}}(X) =$ rotations and reflections that leave X globally invariant. Clearly, $G \subset \tilde{G}$, so it must be that $\# \tilde{G}$ a multiple of 24. Moreover, remark that relfections reverse orientation, while rotations preserve it; this implies that the index of G in $\tilde{G}$ is 2. Hence, the action of $\tilde{G}$ on a set $O = \{\text{orientations on} \mathbb{R}^3\}$ with $\# O = 2$ is transitive. We then have the induced map

$$\eta : \tilde{G} \to \mathrm{Aut}(O) \cong \mathbb{Z}/2$$

with kernel given by all of G; G fixes orientations after all.

Remark now the existence of a particular element in $\tilde{G}$ that "reflects through the origin", swapping each corner that is joined by a diagonal. This is not in G, but notice that it actually commutes with every other element in $\tilde{G}$ (one can view such an element by the matrix $\begin{pmatrix} -1 & & \\ & -1 & \\ & & -1 \end{pmatrix}$ acting on $\mathbb{R}^3$). Call this element τ. Then, since $\tau \notin G$, $\tau g \neq g$ for any $g \in G$. Hence, we can write $\tilde{G} = G \sqcup \tau G$; that is, $\tilde{G}$ is a disjoint union of two copies of S_4, and so

$$\tilde{G} \cong S_4 \times \mathbb{Z}/2\mathbb{Z}$$

$$f : S_4 \times \mathbb{Z}/2\mathbb{Z} \to \tilde{G}, \quad (g, j) \mapsto \tau^j g.$$

1.4 Conjugation and Conjugacy

↪**Definition 1.9**: Two elements $g_1, g_2 \in G$ are *conjugate* if $\exists h \in G$ such that $g_2 = h g_1 h^{-1}$.

Recall that we can naturally define G as a G-set in three ways; by left multiplication, by right multiplication (with an extra inverse), and by conjugation. The first two are always transitive, while the last is never (outside of trivial cases); note that if $g^n = 1$, then $\left(hgh^{-1}\right)^n = 1$, that is, conjugation preserves order, hence G will preserve the order of 1 of the identity element, and conjugation will thus always have an orbit of size 1, $\{e\}$.

An orbit, in this case, is called a *conjugacy class.*

↳**Proposition 1.9**: Conjugation on S_n preserves cycle shape.

Proof. Just to show an example, consider $(13)(245) \in S_5$ and let $g \in S_5$, and put $\sigma := g(13)(245)g^{-1}$. Then, we can consider what $\sigma g(k)$ is for each k;

$$\begin{aligned} \sigma(g(1)) &= g(3) \\ \sigma(g(3)) &= g(1) \\ \sigma(g(2)) &= g(4) \\ \sigma(g(4)) &= g(5) \\ \sigma(g(5)) &= g(2), \end{aligned}$$

hence, we simply have $\sigma = (g(1)g(3))(g(2)g(4)g(5))$, which has the same cycle shape as our original permutation. A similar logic holds for general cycles. ■

↪**Definition 1.10**: The cycle shape of $\sigma \in S_n$ is the partition of n by σ. For instance,

$$\begin{aligned} 1 &\leftrightarrow 1 + 1 + \ldots + 1 \\ \sigma = (12\ldots n) &\leftrightarrow n. \end{aligned}$$

⊛ **Example 1.5**: We compute all the "types" of elements in S_4 by consider different types of partitions of 4:

Partition	Size of Class
$1 + 1 + 1 + 1$	1
$2 + 1 + 1$	$\binom{4}{2} = 6$
$3 + 1$	$4 \cdot 2 = 8$ (4 points fixed, 2 possible orders)
4	$3! = 6$ (pick 1 first, then 3 choices, then 2)
$2 + 2$	3