The Chinese University of Hong Kong, Shenzhen
SSE · School of Science and Engineering

Yuanxin Guo · Fall Semester 2021/22

MAT 3004 – Abstract Algebra I

Tutorial 3

Symmetric groups and linear algebra Recall the way we defined symmetric groups: the **symmetric group** of n elements is the collection of all bijective functions $\sigma : X_n \to X_n$.

$$S_n := \{\sigma : X_n \to X_n \mid \sigma \text{ bijective}\},$$

where $X_n := \{1, 2, \cdots, n\}$. Now let's view symmetric groups from a linear algebraic point of view.[1]

Recall a theorem from linear algebra: let $\mathcal{B}_1 = (v_1, \cdots, v_n)$, $\mathcal{B}_2 = (w_1, \cdots, w_n)$ be two arbitrary ordered basis for an n-dimensional vector space V. Then there exists an invertible linear transformation $T : V \to V$ such that $T(v_i) = w_i$ for all $1 \leq i \leq n$. For simplicity, let's work in $V = \mathbb{R}^n$ and let $\mathcal{B} = (e_1, \cdots, e_n)$ to be the standard basis. For any $\sigma \in S_n$, we can define an ordered basis

$$\mathcal{B}_\sigma = (e_{\sigma(1)}, e_{\sigma(2)}, \cdots, e_{\sigma(n)}).$$

By the previous argument, we can find an element $T_\sigma \in \mathrm{GL}(n, \mathbb{R})$ such that $T_\sigma(e_i) = e_{\sigma(i)}$.[2]

Exercise E3.1 (Permutation Matrices):
A **permutation matrix** is a matrix that has exactly one nonzero entry, 1, in each row and each column.

a) Show that for any $\sigma \in S_n$, T_σ is a permutation matrix.
b) Show that any permutation matrix corresponds to a unique element in S_n. Conclude that permutation matrices correspond bijectively to elements in S_n.
c) Show that for $\sigma, \mu \in S_n$, we have
$$T_\sigma T_\mu = T_{\sigma\mu},$$
that is, the linear transformation corresponding to the composition of two permutations is the composition of the linear transformations corresponding to the two permutations. Argue that the set of permutation matrices P_n form a subgroup of $\mathrm{GL}(n, \mathbb{R})$.
d) Show that any permutation has determinant ± 1. In particular, for transposition τ, $\det T_\tau = -1$.
e) Let $\alpha \in A_n$, the alternating group of n elements. What can you say about $\det T_\alpha$? What can you say about $\det T_\beta$ for $\beta \in S_n \setminus A_n$?

[1] You can find this part of content in Artin 1.5.
[2] By slight abuse of notation, we identify a linear transformation with its matrix representation under the standard basis.

Homomorphisms, good functions Functions are one of the central themes in any field of mathematics. However, in different fields of mathematics, we often study special subclasses of functions that *preserve certain structures*. When we study set theory, we consider functions in full generality. When we study preorders, however, we are more interested in more specialized functions, namely monotone functions, as they *preserve* order. When we study topology, we study continuous functions, as they *preserve* openness of sets - but in a reversed manner.

For algebraic structures, we consider a function as a good function if it *preserves operations*. What are the three operations of groups? What are their arities? Do group homomorphisms preserve these operations?

In topology, thanks to continuity, several other topological property are preserved by continuous functions: the continuous image of a compact/connected/path-connected space is compact/connected/path-connected. What about in group theory? We have shown in class that the homomorphic image of a abelian/cyclic group is still cyclic. We thus have a rough idea on why we mainly study 'good' functions.

Mnemonically, consider additive groups $(G, +), (H, +)$. Then $f : G \to H$ is a homomorphism if for all $a, b \in G$,

$$f(a + b) = f(a) + f(b).$$

We can see this as some form of distributive law - function application *distributes over* binary operation.[3] We have to point out that this is only an mnemonic aid: it is imprecise since the groups G, H need not be equal, and hence the symbol '$+$' on both sides may refer to different operations. Yet when $G = H$, this provides plenty of examples of homomorphisms: let $G = \mathbb{Z}, \mathbb{Q}, \mathcal{M}_n(\mathbb{R})$ (the group of $n \times n$ matrices under addition), then for any $a \in G$, $f_a : G \to G$ given by $x \mapsto ax$ is a homomorphism.

We have actually, lowkey, seen examples of bijective, injective, and surjective homomorphisms in the previous exercise. In case you don't see them, let me spell them out:

$$S_n \longrightarrow P_n \hookrightarrow \mathrm{GL}(n, \mathbb{R}) \longrightarrow \mathbb{R}^\times$$

Why are all these arrows homomorphisms? Which is bijective, which is injective, and which is surjective?

Good functions are always preserved under function compositions - intuitively, the structures are preserved in each step, hence preserved as a whole. In particular, the composition of two homomorphisms is still a homomorphism. Denote the composition of arrows in the previous diagram by $\varphi : S_n \to (\{\pm 1\}, \times)$. Check by definition that the subset

$$\Lambda_n = \{\sigma \in S_n : \varphi(\sigma) = 1\} \subset S_n$$

forms a subgroup of S_n. Combine with part e) in Exercise 3.1, show that $A_n = \Lambda_n$.

Representation Representation theory is a way to better understand groups - we *represent* the group element as more concrete objects: matrices. The representations have to make sense - the matrix representing the product of two elements should be the product of the representing matrices of these two elements. Does this sound familiar?

Formally, a representation of a group G on a vector space V is a group homomorphism $\varphi : G \to \mathrm{GL}(V)$, i.e., $\varphi(g)\varphi(h) = \varphi(gh)$.

[3] One may be tempted to write the homomorphism condition with a commutative diagram. Here is a good reference: `https://math.stackexchange.com/questions/610866`

Exercise E3.2 (Three representations of S_3):
In this exercise, we will see three different representations of the group S_3.

a) Recall Exercise 3.1, what is a representation of S_3 on $\mathbb{R}^3$? Is it faithful?
b) What is the group $\mathrm{GL}(1,\mathbb{R})$? Is the map $\sigma \mapsto \det T_\sigma$ a representation of S_3 on $\mathbb{R}$?
c) Recall that $S_3 \cong D_3$, the dihedral group of order 6, which consists of rotations and reflections of equilateral triangles. Can you represent these rotations and reflections as 2×2 matrices? Can you obtain a representation of S_3 on $\mathbb{R}^2$?

Isomorphism, equality in disguise I believe we are all very confident when we talk about equality of numbers. For two real numbers a, b, what does $a = b$ mean? Figuratively, a and b take the same spot on the real line; using a more rigorous argument, we say both $a \leq b$ and $a \geq b$.

But what do we really mean when we say two groups are equal?[4] Consider the simplest nontrivial group, $\mathbb{Z}_2$. It has two elements, $[0], [1]$, where $[0]+[0] = [1]+[1] = [0]$, $[0]+[1] = [1]+[0] = [1]$. Also consider the subgroup of $(\mathbb{R}, \times)$ with two elements, $\{\pm 1\}$, where we have $1 \cdot 1 = (-1) \cdot (-1) = 1$, $1 \cdot (-1) = -1 \cdot 1 = -1$. The two groups have identical Cayley tables up to the naming of the elements - in fact, I could define an *abstract* group $(\{a, b\}, \star)$ by $a \star a = b \star b = a$, $a \star b = b \star a = b$, which can represent both groups.

The previous discussion shows that the names of the elements in a groups are immaterial - regarding S_3 and D_3 as distinct groups is unfair. This provides another perspective to understand isomorphisms - an isomorphism is an equality up to an appropriate renaming of the elements.

Group of functions of groups Sounds like a tongue twister, but let us return to the very beginning of our topic today: symmetric groups. A symmetric group is the set of bijective functions from a *set* to itself: bijectivity guarantees the closure of the group; does the set of isomorphisms from a group to itself form a group?

Exercise E3.3 (Automorphism group):
In this example, we explore the group-based analog of symmetric groups. Let G be a group, and define the set

$$\mathrm{Aut}(G) = \{\varphi : G \to G \mid \varphi \text{ group isomorphism}\}$$

In the homework exercise, you are supposed to show that $\mathrm{Aut}(G)$ has group structure, where the binary operation is function composition.

a) Show that $\mathrm{Aut}(\mathbb{R}^n) = \mathrm{GL}(n, \mathbb{R})$, where $\mathbb{R}^n$ is regarded as a group under vector addition.
b) Let $p \geq 3$ be a prime. Show that $\mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^*$.
c) Let V be the Klein 4-group. What is $\mathrm{Aut}(V)$? By writing the underlying set of V as $\{1, a, b, c\}$, can you make the connection between V and $\mathrm{Aut}(V)$?
d) Show that

$$\mathrm{conj}_h : G \to G \text{ defined by } g \mapsto hgh^{-1}$$

is an automorphism. Further show that

$$\mathrm{conj} : G \to \mathrm{Aut}(G) \text{ defined by } g \mapsto \mathrm{conj}_g$$

is a homomorphism from G to $\mathrm{Aut}(G)$.[5]

[4] This idea is borrowed from category theory, for a discussion on the 'right' notion of sameness, see pages 33-34 of Leinster's book *Basic Category Theory*: `https://arxiv.org/pdf/1612.09375.pdf`

[5] If G is a Lie group, the function mapping g to the derivative of conj_g at the origin is the *adjoint representation* of G.