MATH6130: Algebra I

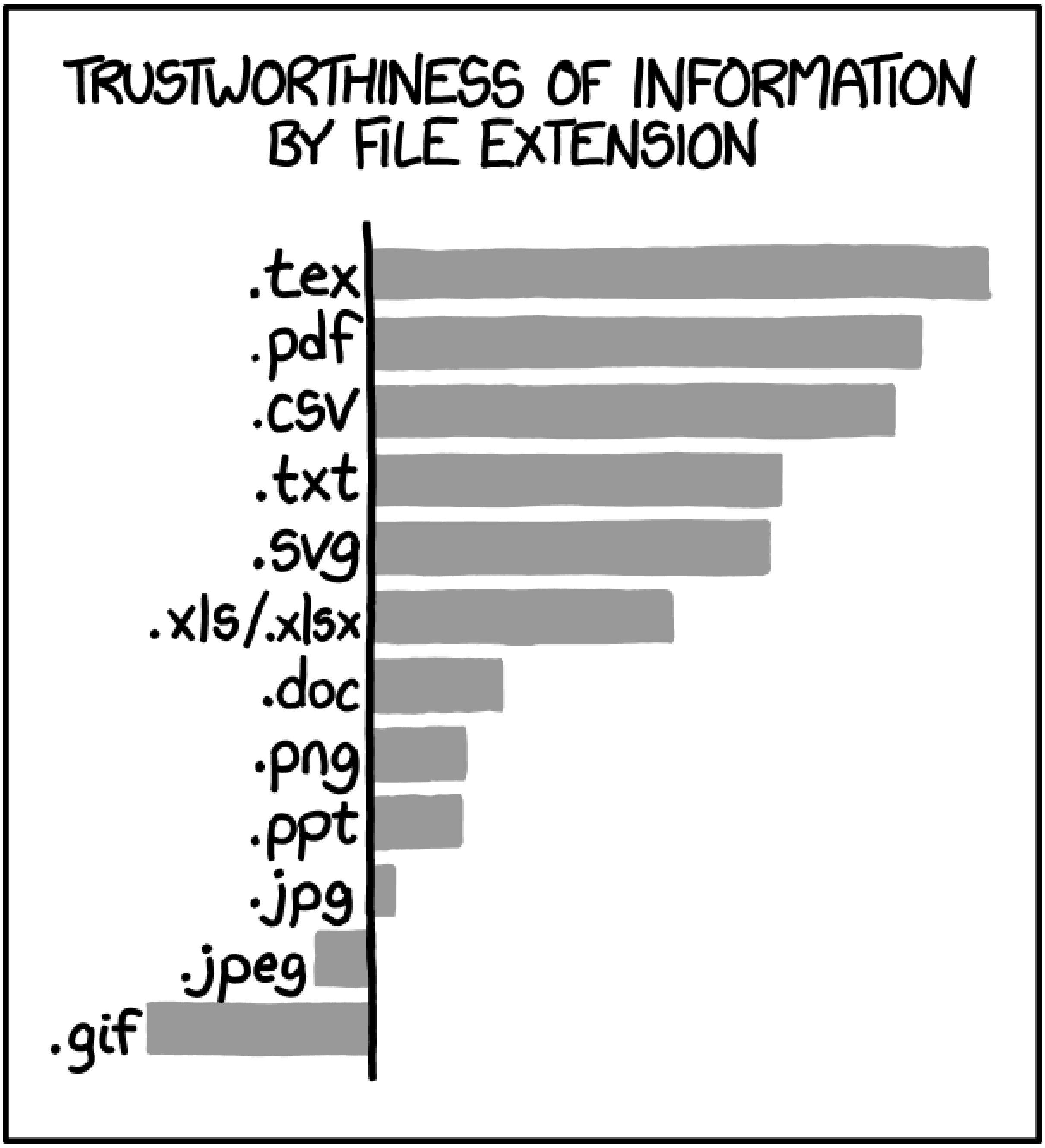
ADITHYA BHASKARA
PROFESSOR: NATHANIEL THIEM

TEXTBOOK: DUMMIT & FOOTE

UNIVERSITY OF COLORADO BOULDER

University of Colorado
Boulder

EDITION 1


TRUSTWORTHINESS OF INFORMATION
BY FILE EXTENSION
.tex
.pdf
.csv
.txt
.svg
.xls/.xlsx
.doc
.png
.ppt
.jpg
.jpeg
.gif

Contents

Preface

To the interested reader,

This document is a compilation of lecture notes taken during the Fall 2024 semester for MATH6130: Algebra I at the University of Colorado Boulder. The course used [DF21] as its primary text. The content in these course notes is from the above resources if not otherwise mentioned, and the author only takes responsibility for the synthesis of the content into these notes. Many theorems, definitions, and content may be quoted or derived from the aforementioned books. This course was taught by Nathaniel Thiem, Ph. D.

While much effort has been put in to remove typos and mathematical errors, it is very likely that some errors, both small and large, are present. Please keep in mind that the author wrote this resource during his undergraduate studies. If an error needs to be resolved, please contact Adithya Bhaskara at adithya@colorado.edu.

Best Regards,
Adithya Bhaskara

REVISED: September 11, 2024

1

Introduction to Groups

1.1 Lecture 1: August 26, 2024

1.1.1 Introduction

In this course, we seek to understand two fundamental "categories:" groups and rings. This course seeks to prepare Ph. D. students for the first half of the algebra preliminary exam. A category $(\mathcal{O}, \mathcal{M})$, informally, is a collection of objects $\mathcal{O}$ and a collection of morphisms $\mathcal{M}$ such that each morphism pairs two objects in such a way that reasonable things happen. For example, consider the table.

$\mathcal{O}$	$\mathcal{M}$
Sets	Functions
Vector Spaces	Linear Transformations
Groups	Group Homomorphisms
Rings	Ring Homomorphisms

We remark that vector spaces are $\mathbb{F}$-modules, functions are set homomorphisms, and linear transformations are $\mathbb{F}$-module homomorphisms. A benefit of this category-theoretic framework is that it highlights commonalities between families of algebraic structures. A drawback is that this framework may not be conducive to learning for the first time. Also, it is difficult to see the peculiarities of individual categories. In this course, we will indirectly use category theory to inform our constructions and definitions.

1.2 Lecture 2: August 28, 2024

1.2.1 Group Axioms and an Introduction to the Symmetric Group

We start with the following definition.

Definition 1.2.1: Functions

A function $f : A \to B$ from a set A to a set B is a subset $\{(a, f(a)) : a \in A\} \subseteq A \times B$ such that for each $a \in A$, there exists a unique $b = f(a) \in B$. By convention, if $f(a) = b$, we can write $a \mapsto b$.

We say that $f : A \to B$ is injective if $f(a) = f(b)$ implies $a = b$ and surjective if for every $b \in B$, there exists $a \in A$ with $f(a) = b$. Then, $f : A \to B$ is bijective if it is both injective and surjective.

Given functions $f : A \to B$ and $g : B \to C$, the composition $g \circ f : A \to C$ is the function given by

$$(g \circ f)(a) = g(f(a)), \quad a \in A.$$

Remark. *A function $f : A \to B$ is bijective if and only if there exists a function $f^{-1} : B \to A$ such that $(f \circ f^{-1})(b) = b$ for all $b \in B$, and $(f^{-1} \circ f)(a) = a$ for all $a \in A$.*

Let's talk about groups!

Definition 1.2.2: Groups

A group $(G, \circ)$ is a set G with a function $\circ : G \times G \to G, (g, h) \mapsto g \circ h$ such that

(G1) there exists $1 \in G$ such that $g \circ 1 = g = 1 \circ g$ for all $g \in G$,

(G2) for each $g \in G$ there exists $g^{-1} \in G$ such that $g \circ g^{-1} = 1 = g^{-1} \circ g$, and

(G3) for all $g, h, k \in G$, $g \circ (h \circ k) = (g \circ h) \circ k$.

Remark. *The element $1 \in G$ is called an identity. The element $g^{-1} \in G$ is an inverse of $g \in G$.*

Remark. *When the operation $\circ$ is clear from context, we will often refer to G as a group, when we really mean $(G, \circ)$. Similarly, we say that a group G under $\circ$ indicates that $\circ : G \times G \to G$ is the function that makes $(G, \circ)$ a group. Furthermore, we will often also write gh to mean $g \circ h$.*

Proposition 1.2.1: The Group Identity is Unique

If 1 and $1'$ are identities in group $(G, \circ)$, then, $1 = 1'$.

Proof. We have $1 = 1 \circ 1' = 1' \circ 1 = 1'$. □

Proposition 1.2.2: The Inverse of a Group Element is Unique

Let $(G, \circ)$ be a group. If $g \in G$, $f \circ g = g \circ f = 1$, and $h \circ g = g \circ h = 1$, then $f = h$.

Proof. We have that $g \circ f = g \circ h$. Multiplying both sides by f on the left gives $f \circ (g \circ f) = f \circ (g \circ h)$. and then using associativity gives us $(f \circ g) \circ f = (f \circ g) \circ h$. Since $f \circ g = 1$, we indeed have $f = h$, as desired. □

Proposition 1.2.3: The Inverse of a Product

Let $(G, \circ)$ be a group. If $g, h \in G$, then $(g \circ h)^{-1} = h^{-1} \circ g^{-1}$.

Proof. We have $(g \circ h) \circ (h^{-1} \circ g^{-1}) = g \circ (h \circ h^{-1}) \circ g^{-1} = g \circ g^{-1} = 1$ and $(h^{-1} \circ g^{-1}) \circ (g \circ h) = h^{-1} \circ (g^{-1} \circ g) \circ h = 1$. □

Proposition 1.2.4: The Inverse of Many Products

Let $(G, \circ)$ be a group. Then, $(g_1 \circ \cdots \circ g_n)^{-1} = g_n^{-1} \circ \cdots \circ g_1^{-1}$ for all $g_1, \ldots, g_n \in G$.

Proof. We proceed by induction on n. For $n = 1$, the proposition is trivial, with the left hand side being $(g_1)^{-1} = g_1^{-1}$, and the right hand side being g_1^{-1}. Suppose that for $n = k \geq 1$, it is the case that $(g_1 \circ \cdots \circ g_k)^{-1} = g_k^{-1} \circ \cdots \circ g_1^{-1}$. Then,

$$\begin{aligned}(g_1 \circ \cdots \circ g_k \circ g_{k+1})^{-1} &= g_{k+1}^{-1}(g_1 \circ \cdots \circ g_k)^{-1} \\ &= g_{k+1}^{-1} \circ g_k^{-1} \circ \cdots \circ g_1^{-1} \\ &= g_{k+1}^{-1} \circ \cdots \circ g_1^{-1},\end{aligned}$$

as desired. Note that we use Proposition 1.2.3 that $(g_i g_j)^{-1} = g_j^{-1} g_i^{-1}$ for all $i, j \in \{1, \ldots, n\}$. □

Intuitively, we can think of groups as a mathematical abstraction of a notion of symmetry.

Question. *What is a symmetry?*

Answer. *A symmetry on a set A is a bijective function $\sigma : A \to A$.*

Remark. *Usually, σ will respect additonal structure on A.*

A group is a "complete" set of symmetries on a set A that respect some set of structures on A.

Example 1. *Take $A = \{1, 2, 3, 4\}$. View each element as the corner of a square. The map $\{1, 2, 3, 4\} \mapsto \{2, 1, 3, 4\}$ does not preserve structure, whereas $\{1, 2, 3, 4\} \mapsto \{2, 3, 4, 1\}$ does.*

The axioms in Definition 1.2.2 encode this notion of symmetry as follows:

(G0) the composition of 2 symmetries is a symmetry,

(G1) doing nothing is a symmetry,

(G2) undoing a symmetry is a symmetry, and

(G3) function composition is associative.

We now consider the symmetric group.

Definition 1.2.3: The Symmetric Group

The symmetric group S_A on the set A is the group

$$S_A = \{w : A \to A : w \text{ is a bijection}\}$$

under function composition; S_A is the set of all symmetries of A with no additional structure. By convention, $S_n = S_{\{1,\dots,n\}}$.

By default, for $w \in S_n$, we write

$$w = \begin{bmatrix} 1 & \cdots & n \\ w(1) & \cdots & w(n) \end{bmatrix}.$$

Alternative notations exist. Braid notion refers to the canonical method of representing a function as a bipartite graph with nodes and edges. Cycle notation, as discussed in Definition 1.2.4, is also prevalent.

Definition 1.2.4: Cycles

An element $w \in S_n$ is a cycle if

$$w(b_1) = b_2, w(b_2) = b_3, \dots, w(b_{k-1}) = b_k, w(b_k) = b_1$$

for some set $B = \{b_1, \dots, b_k\} \subseteq \{1, \dots, n\}$ and $w(a) = (a)$ for all $a \notin B$.

The length of the cycle is k, and we refer to it as a k-cycle. We say that the cycles $(a_1 \ \cdots \ a_\ell)$ and $(b_1 \ \cdots \ b_k)$ are disjoint if $\{a_1, \dots, a_\ell\} \cap \{b_1, \dots, b_k\} = \emptyset$.

The cycle decomposition of an element $w \in S_n$ is the factorization $w = c_1 \circ \cdots \circ c_\ell$ where $\{c_1, \dots, c_\ell\}$ is a set of pairwise disjoint cycles of length greater than 1.

Remark. *Disjoint cycles commute.*

Theorem 1.2.1: 🛑 The Order of $\sigma \in S_n$

The order of an element in S_n equals the least common multiple of the lengths of the cycles in its cycle decomposition.

Proof. Let $\sigma \in S_n$ with $|\sigma| = k$. Suppose σ has cycle decomposition $\sigma = \tau_1 \cdots \tau_\ell$. Note that $\tau_1, \dots, \tau_\ell$ are disjoint by the definition of a cycle decomposition, so they commute. Then, $1 = \sigma^k = (\tau_1 \cdots \tau_\ell)^k = \tau_1^k \cdots \tau_\ell^k$. It is also the case that $\tau_1^k = \cdots = \tau_\ell^k = 1$ (if some $\tau_i^k \neq 1$, then it would be the case that $\sigma^k \neq 1$ since $\tau_1^k, \dots, \tau_\ell^k$ are disjoint). Since if $\tau_i^k = 1$, $|\tau_i| | k$, we have that k is a common multiple of the orders of each $\tau_1, \dots, \tau_\ell$. Since the order of a cycle is its length, k is indeed a common multiple of the lengths of the cycles $\tau_1, \dots, \tau_\ell$. Finally, since $|\sigma| = k$, k is the least number η such that $\sigma^\eta = 1$. So, k is the *least* common multiple of the cycle lengths, as desired. □

1.3 Lecture 3: Aug. 30, 2024

1.3.1 Subgroups and the Dihedral Group

Recall that S_A is the group of all possible symmetries of A with no additional structure. If we add structure to A, we should obtain a distinguished subset. For clarity, we provide another brief example.

Example 2. *Take $A = \{1, 2, 3, 4\}$, and impose that all maps must preserve the position of 1. This gives us the group $S_{\{2,3,4\}}$.*

We formalize the notion of a subgroup as follows.

Definition 1.3.1: Subgroups

A subset $H \subseteq G$ forms a subgroup of group $(G, \circ)$ if $1 \in H$, $h \in H$ implies $h^{-1} \in H$, and $h, k \in H$ implies $h \circ k \in H$. If $(H, \circ)$ is a subgroup of $(G, \circ)$, we write $H \leq G$.

Theorem 1.3.1: Subgroup Criterion

A nonempty subset $H \subseteq G$ forms a subgroup of $(G, \circ)$ if and only if $h \circ k^{-1} \in H$ for all $h, k \in H$.

Proof. The proof is in two parts.

($\Leftarrow$) If $H \leq G$, then it is clear, from Definition 1.3.1 that $h \circ k^{-1} \in H$ for all $h, k \in H$.

($\Rightarrow$) If $h \circ k^{-1} \in H$ for all $h, k \in H \neq \emptyset$, then $h \circ h^{-1} = 1 \in H$ implying that $h^{-1} = 1 \circ h^{-1} \in H$. Then since, we know that $k^{-1} \in H$. $h \circ k = h \circ (k^{-1})^{-1} \in H$.

We are done. □

Remark. *The above is probably the "wrong" definition; from a category-theoretic perspective, the condition should be that $H = \varphi(K)$, where K is a group and $\varphi : K \to G$ is a group homomorphism.*

Definition 1.3.2: Generated Subgroups

The subgroup $\langle A \rangle$ generated by a subset $A \subseteq G$ is the subgroup of $(G, \circ)$ containing A such that if $A \subseteq K \leq G$ is a subgroup, then $\langle A \rangle \subseteq K$.

Example 3. *If $g \in G$, then $\langle \{g\} \rangle = \{1, g, g^{-1}, g^2, g^{-2}, \dots\}$. We often use $\langle g \rangle$ as notational convenience instead of $\langle \{g\} \rangle$.*

Definition 1.3.3: Order of a Group Element

The order $|g|$ of an element $g \in G$ is the cardinality of the set $\langle g \rangle$; $|\langle g \rangle|$.

Definition 1.3.4: Cyclic Groups

A group $(G, \circ)$ is cyclic if there exists $g \in G$ with $G = \langle g \rangle$.

Example 4. *We have that $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \dots, \overline{n-1}\}$ is a group under addition modulo n. Then, $\mathbb{Z}/n\mathbb{Z} = \langle 1 \rangle$.*

Example 5. *Let $x = e^{\frac{2\pi i}{n}} \in \mathbb{C}$. Then, $\mathbb{C}_n = \{x^0, \dots, x^{n-1}\}$ is a group under multiplication in $\mathbb{C}$ and $\mathbb{C}_n = \langle x \rangle$. We can think of $\mathbb{C}_n$ as the set of rotations of a regular n-gon.*

Question. *Can we add the other symmetries of a regular n-gon to form a group?*

It turns out, that yes we can. This leads us to the notion of a dihedral group.

Definition 1.3.5: Order of a Group

The order $|G|$ of a group $(G, \circ)$ is the cardinality of the set G.

Definition 1.3.6: Dihedral Groups

Let $D_{2n} = \{w \in S_n : w(j) \equiv k \pmod{n} \implies w(j+1) \equiv k \pm 1 \pmod{n}\}$; $(D_{2n}, \circ)$ forms the dihedral group of order $2n$, and $D_{2n} \leq S_n$.

Remark. *The above definition captures the permutations that preserve the "neighborliness" of the vertices of the regular n-gon. Indeed, the full set of symmetries of the regular n-gon is captured by $(D_{2n}, \circ)$.*

Proposition 1.3.1: Order of the Dihedral Group

It is the case that $|D_{2n}| = 2n$.

Proof. Let $w \in D_{2n}$. Suppose $w(1) = k$.

- Case 1: If $w(2) = k + 1$, then, $w(3) \neq k$ so $w(3) = k + 2, w(4) = k + 3, \dots, w(n) = k - 1$.
- Case 2: If $w(2) = k - 1$, then, $w(3) \neq k$ so $w(3) = k - 2, w(4) = k - 3, \dots, w(n) = k + 1$.

Thus, $w \in D_{2n}$ is completely determined by $(w(1), w(2))$. There are n choices for the first coordinate, and 2 choices for the second coordinate. So, $|D_{2n}| = 2n$, as desired. □

Remark. *In Proposition 1.3.1, $+$ is addition modulo n.*

Let $r, s \in D_{2n}$ be given by

$$r(j) \equiv j + 1 \pmod{n}, \quad s(j) \equiv -j \pmod{n}.$$

We have that if $(w(1), w(2)) = (k, k+1)$, then $w = r^{k-1}$. If $(w(1), w(2)) = (k, k-1)$, then $w = r^{k+1}s$. So, $D_{2n} = \langle r, s \rangle$. In fact, $rs = sr^{-1}$. So, our presentation of D_{2n} will be

$$D_{2n} = \langle r, s : r^n = s^2 = (rs)^2 = 1 \rangle.$$

1.4 Lecture 4: Sep. 4, 2024

1.4.1 Homomorphisms & Isomorphisms

For motivation, we've seen groups that, intuitively at least, should behave the same way. For example, $\mathbb{C}_n$ and $\mathbb{Z}/n\mathbb{Z}$ are, at least at first glance, very similar. It also seems that S_A and $S_{|A|}$ should have some correspondence. Furthermore, it makes sense that if $A \subseteq B$, S_A should be related to S_B in some way. In this section, we make this notion precise.

Definition 1.4.1: Group Homomorphisms

A group homomorphism $\varphi : G \to H$ from a group $(G, \circ)$ to a group $(H, \star)$ is a function such that for all $g, h \in G$, $\varphi(x \circ y) = \varphi(x) \star \varphi(y)$.

The image of φ is the subgroup $\varphi(G) = \{\varphi(g) : g \in G\} \leq H$. The kernel of φ is the subgroup $\ker \varphi = \{g \in G : \varphi(g) = 1\} \leq G$.

We state some properties of group homomorphisms below.

Proposition 1.4.1: Properties of Group Homomorphisms

If $\varphi : G \to H$ is a group homomorphism, then

1. $\varphi(1) = 1$,
2. $\varphi(g)^{-1} = \varphi(g^{-1})$, and
3. $\varphi(G) \subseteq H$ and $\ker \varphi \subseteq G$ are subgroups.

Proof. We proceed as follows:

1. We have that $\varphi(1)\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)$. So, $\varphi(1) = \varphi(1)^{-1}\varphi(1)\varphi(1) = 1$.
2. Then, we have $\varphi(g^{-1})\varphi(g) = \varphi(g^{-1} \circ g) = \varphi(1) = 1$.
3. Suppose $\varphi(g), \varphi(h) \in \varphi(G)$. Then, $\varphi(g)\varphi(h)^{-1} = \varphi(g \circ h^{-1}) \in \varphi(G)$. Similarly, if $g, h \in \ker \varphi$. Then, $\varphi(g \circ h^{-1}) = \varphi(g)\varphi(h^{-1}) = \varphi(g)\varphi(h)^{-1} = 1$.

We are done. □

Definition 1.4.2: Group Isomorphism

A group isomorphism $\varphi : G \to H$ from a group $(G, \circ)$ to a group $(H, \star)$ is a bijective homomorphism. If an isomorphism $\varphi : G \to H$ exists, we write $G \cong H$ and say that G and H are isomorphic.

Theorem 1.4.1: 🛑 Isomorphisms of Cyclic Groups

Let $(G, \circ)$ be cyclic. Then,

$$G \cong \begin{cases} \mathbb{Z}/n\mathbb{Z} & |G| = n \\ \mathbb{Z} & |G| = \infty \end{cases}.$$

Proof. We start with the case that $|G| = n$. Let $G = \langle g \rangle$. Define $\varphi : G \to \mathbb{Z}/n\mathbb{Z}$ where $g^j \mapsto \overline{j}$. We first check that φ is well-defined as injective. We have that $g^i = g^j$ if and only if $g^{i-j} = 1$ if and only if $j - i \equiv 0 \pmod n$ if and only if $j \equiv i \pmod n$ if and only if $\overline{i} = \overline{j}$. Then, $\varphi(g^i g^j) = \varphi(g^{i+j}) = \overline{i+j} = \overline{i} + \overline{j} = \varphi(g^i) + \varphi(g^j)$, so φ is a homomorphism. If $\overline{j} \in \mathbb{Z}/n\mathbb{Z}$, then $\varphi(g^j) = \overline{j}$, so φ is surjective. Therefore, φ is an isomorphism and G and $\mathbb{Z}/n\mathbb{Z}$ are isomorphic. In the case where $|G| = \infty$, the argument is very similar, taking $\varphi : G \to \mathbb{Z}$ with $g^j \mapsto j$. □

Theorem 1.4.2: 🛑 Isomorphisms of Symmetric Groups

Let $A = \{a_1, \dots, a_n\}$. Then, $\varphi : S_n \to S_A$ with $w \mapsto \varphi(w) : A \to A$, $a_j \mapsto a_{w(j)}$ is an isomorphism.

Remark. *In Theorem 1.4.2, φ depends entirely on the choice of the total order n the elements in A. Consider $A = \{\spadesuit, \clubsuit, \heartsuit\} = \{\heartsuit, \spadesuit, \clubsuit\}$. If we take $(1\ 3) \in S_3$, $\varphi((1\ 3)) = (\spadesuit\ \heartsuit)$ under the first ordering, but $\varphi((1\ 3)) = (\heartsuit\ \clubsuit)$ under the second. Regardless, though, φ is an isomorphism.*

1.5 Lecture 5: Sep. 6, 2024

1.5.1 Group Actions

In this section, we explore how groups and sets can interact reasonably. Consider the following definitions.

Definition 1.5.1: Group Actions

A group $(G, \circ)$ acts on a set A if there exists a homomorphism $\varphi : G \to S_A$.

A left action of G on A is a function $G \times A \to A$, $(g, a) \mapsto g(a)$ such that

(A1) for all $a \in A$, $1(a) = a$, and

(A2) for all $a \in A$ and $g, h \in G$, $g(h(a)) = (g \circ h)(a)$.

Proposition 1.5.1: Left Action If and Only If Group Acts on the Set

A function $G \times A \to A$ is a left action if and only if

$$\varphi : G \to S_A, \quad g \mapsto \varphi(g) : A \to A, a \mapsto g(a).$$

is a homomorphism.

Definition 1.5.2: Triviality and Faithfulness

A group action $G \times A \to A$ is

- trivial if for all $a \in A$ and $g \in G$, $g(a) = a$, and
- faithful if $g(a) = a$ for all $a \in A$ implies $g = 1$.

Lemma 1.5.1: Injective Group Homomorphism If and Only if Kernel is Trivial

If $\varphi : G \to H$ is a group homomorphism, then φ is injective if and only if $\ker \varphi = \{1\}$.

Proof. The proof is in two parts.

($\Rightarrow$) Suppose that φ were injective but $\ker \varphi \neq \{1\}$. So, there would exist distinct $g, h \in G$ with $\varphi(g) = \varphi(h) = 1$ but $g \neq h$. This contradicts injectivity.

($\Leftarrow$) Suppose $\ker \varphi = \{1\}$. If $\varphi(g) = \varphi(h)$, then $1 = \varphi(g)\varphi(h^{-1}) = \varphi(g \circ h^{-1})$. So, $g \circ h^{-1} = 1$ and $g = h$, so φ is injective.

We are done. □

Theorem 1.5.1: Faithful Action If and Only If G Isomorphic to Subgroup of S_A

A group action $G \times A \to A$, with corresponding homomorphism $\varphi : G \to S_A$, is faithful if and only if G is isomorphic to a subgroup of S_A.

Proof. Let G act on A with corresponding homomorphism $\varphi : G \to S_A$. The action is faithful if and only if $g(a) = a$ for all $a \in A$ implies that $g = 1$. This means that $\ker \varphi$ must be trivial since otherwise $1 \neq x \in \ker \varphi$ has $\varphi(x) = 1 \neq x$. Then, φ is injective if and only if $\ker \varphi = \{1\}$, and it is surjective onto its range $H \leq S_A$. So, $\varphi : G \to H$ is the desired isomorphism. □

Corollary 1.5.1: Cayley's Theorem

If $|G| = n$, then G is isomorphic to a subgroup of S_n.

Proof. Note that $(G, \circ)$ acts on G by left multiplication:

$$g(h) = g \circ h, \quad g \in G, h \in G.$$

This action is faithful, so G is isomorphic to a subgroup of $S_G \cong S_{|G|} = S_n$ by Theorem 1.5.1. □

We now discuss group actions on sets with more structure. First, we define some algebraic structures.

Definition 1.5.3: Abelian Groups

A group $(G, \circ)$ is abelian $g \circ h = h \circ g$ for all $g, h \in G$.

Proposition 1.5.2: Isomorphic Groups are Either Both Abelian or Both Not Abelian

Let $\varphi : G \to H$ be a group isomorphism. Then, G is abelian if and only if H is abelian.

Proof. The proof is in two parts. Let $\varphi : G \to H$ be a isomorphism.

($\Rightarrow$) Suppose G is abelian. Take arbitrary $h_1, h_2 \in H$ and write $h_1 = \varphi(g_1)$ and $h_2 = \varphi(g_2)$ for $g_1, g_2 \in G$. Note that this is possible since φ is surjective. Then,

$$h_1 h_2 = \varphi(g_1)\varphi(g_2) = \varphi(g_1 g_2) = \varphi(g_2 g_1) = \varphi(g_2)\varphi(g_1) = h_2 h_1.$$

So, H is abelian.

($\Leftarrow$) Suppose H is abelian. Take arbitrary $g_1, g_2 \in G$ with $g_1 = \varphi^{-1}(h_1)$ and $g_2 = \varphi^{-1}(h_2)$ for $h_1, h_2 \in G$. Note that g_1 and g_2 are well-defined since φ is injective. Also, note that $\varphi^{-1} : H \to G$ is an isomorphism since $\varphi : G \to H$ is. So, we can write

$$g_1 g_2 = \varphi^{-1}(h_1)\varphi^{-1}(h_2) = \varphi^{-1}(h_1 h_2) == \varphi^{-1}(h_2 h_1) = \varphi^{-1}(h_2)\varphi^{-1}(h_1) = g_2 g_1.$$

So, G is abelian.

We are done. □

Remark. *If $(G, \circ)$ is abelian, we often, but not always, write $+$ for the group operation $\circ$. Here, $1 = 0$.*

Definition 1.5.4: Fields

A field $(\mathbb{F}, +, \cdot)$ is an abelian group under $+ : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ with a function $\cdot : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$, $(r, s) \mapsto rs$ such that

(F1) $\mathbb{F}^\times = \mathbb{F}\backslash\{0\}$ is an abelian group under $\cdot$, and

(F2) for $r, s, t \in \mathbb{F}$, $(r + s)t = rt + st$.

Definition 1.5.5: $\mathbb{F}$-Modules

An $\mathbb{F}$-module $(V, +, \cdot)$ is an abelian group under $+ : V \times V \to V$ with a function $\circ : \mathbb{F} \times V \to V$, $(r, v) \mapsto rv$ such that

(M1) $\mathbb{F}^\times \times V \to V$ is a left action on the set V, and

(M2) for all $a, b \in \mathbb{F}$ and $u, v \in V$, $(a + b)(u + v) = au + bu + av + bv$.

Remark. *In linear algebra, we call $\mathbb{F}$-modules vector spaces.*

Definition 1.5.6: Group Actions on $\mathbb{F}$-Modules

A group action of a group $(G, \circ)$ on an $\mathbb{F}$-module V is a left action $G \times V \to V$ on the set V such that for $g \in G$, $a, b \in \mathbb{F}$, $u, v \in V$, we have that

$$g(au + bv) = ag(u) + bg(v).$$

Example 6. *We have that S_n acts on $V = \mathbb{C}^n$ by*

$$w \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} v_{w(1)} \\ \vdots \\ v_{w(1)} \end{bmatrix}$$

Example 7. *We have that $\mathrm{GL}_n(\mathbb{C}) = \{A \in \mathbb{C}^{n \times n} : \det A \neq 0\}$ acts on $\mathbb{C}^n$ by usual matrix-vector multiplication.*

Remark. *For each action of G on an $\mathbb{F}$-module V, we get a homomorphism $\varphi : G \to \mathrm{GL}(V)$, where $\mathrm{GL}(V)$ is the group of invertible linear operators on V. Just as $S_A \cong S_{|A|}$, we have that for each choice of ordered basis B on V, we get $\mathrm{GL}(V) \cong \mathrm{GL}_{|B|}(\mathbb{F})$. We call φ a representation.*

Remark. *Group actions on $\mathbb{F}$-modules give us matrix groups.*

1.6 Lecture 6: Sep. 9, 2024

1.6.1 Subgroup Constructions

Recall Definition 1.3.2, where for a group $(G, \circ)$ and a set A, we have that $\langle A \rangle$ forms a subgroup of G. Define

$$W(A) = \{b_1, \ldots, b_\ell : \ell \in \mathbb{N}, b_1, \ldots, b_\ell \in A \cup A^{-1}\}$$

where $A^{-1} = \{a^{-1}, a \in A\}$. If $\ell = 0$, $b_1 \cdots b_\ell = 1$.

Proposition 1.6.1: Equivalent Characterizations of the Generated Subgroup

If $\emptyset \neq A \subseteq G$ for group $(G, \circ)$, then

$$W(A) = \langle A \rangle = \bigcap_{H \leq G, A \subseteq H} H.$$

Proof. Suppose $K \leq G$ is a subgroup with $A \subseteq K$. Then, by closure in a subgroup and $A^{-1} \subseteq K$, $W(A) \subseteq K$. Also, $\bigcap_{H \leq G, A \subseteq G} H \subseteq K$ since $K \leq G$. So,

$$W(A) = \langle A \rangle = \bigcap_{H \leq G, A \subseteq H} H,$$

as desired. □

Remark. *We use the uniqueness of $\langle A \rangle$ in the proof of Proposition 1.6.1.*

Example 8. *We have $D_{2n} \cong \langle (1 \ \cdots \ n), (1, n-1)(2, n-2), \ldots \rangle \leq S_n$.*

Example 9. *We have $\mathrm{GL}_n(\mathbb{F})$. Define $x_{i,j}(t) \in \mathbb{F}^{n \times n}$ to be the matrix with 1 on the main diagonal, t in the (i, j) position, and 0 elsewhere. Then,*

$$\langle x_{i,j}(t) : 1 \leq i < j \leq n, t \in \mathbb{F} \rangle = \langle x_{i,j+1}(t) : 1 \leq i < n, t \in \mathbb{F} \rangle$$

gives the upper triangular matrices. Then,

$$\mathrm{GL}_n(\mathbb{F}) = \langle x_{i,j}(t), w_k : 1 \leq i, j \leq n, t \in \mathbb{F}, k \leq k < n \rangle.$$

In this example, $x_{i,j}(\cdot)$ corresponds to the row operations of scaling and adding rows, while w_k encodes the operation of switching rows.

Consider the following definitions.

Definition 1.6.1: Maximal Subgroup

A subgroup $H \leq G$ is maximal if $H \neq G$ and $H \subseteq K \subseteq G$ a subgroup implies $K = H$ or $K = G$.

Definition 1.6.2: 🛑 Subgroup Lattice

The subgroup lattice of a group $(G, \circ)$ is the partial order $\subseteq$ on the set

$$\mathcal{S} = \{H \subseteq G : H \leq G\}.$$

Definition 1.6.3: 🛑 Hasse Diagrams

The Hasse diagram of the subgroup lattice is the directed graph with vertices $\mathcal{S}$ and an edge from H to K if H is a maximal subgroup of K.

Example 10. *For D_8, we have the following subgroup lattice, represented as a Hasse diagram.*

🛑🛑🛑🛑🛑🛑🛑🛑🛑🛑🛑🛑🛑🛑🛑

Definition 1.6.4: 🛑 Stabilizers

If a group $(G, \circ)$ acts on a set B and $A \subseteq B$, then the stabilizer $\operatorname{stab}_G(A)$ is the subgroup

$$\operatorname{stab}_G(A) = \{g \in G : g(a) = a, a \in A\} \leq G.$$

The weak stabilizer $\operatorname{wstab}_G(A)$ is the subgroup

$$\operatorname{wstab}_G(A) = \{g \in G : g(a), g^{-1}(a) \in A, a \in A\} \leq G.$$

Remark. *If $\varphi : G \to S_B$ is the corresponding homomorphism, then $\ker \varphi = \operatorname{stab}_G(B)$. Also, $\operatorname{stab}_G(A) \subseteq \operatorname{wstab}_G(A)$.*

Remark. *We can think of $\operatorname{wstab}_G(A)$ as capturing being able to permute the elements of A, while $\operatorname{stab}_G(A)$ fixes them.*

Example 11. *We have that $\operatorname{stab}_{S_n}(\{1, n\}) = \{w \in S_n : w(1) = 1, w(n) = n\} \cong S_{2,\ldots,n-1} \cong S_{n-2}$. Then, $\operatorname{wstab}_{S_n}(\{1, n\}) = \{ww' : w \in S_{\{1,n\}}, w' \in S_{\{2,\ldots,n-1\}} \cong S_{n-2} \times S_2\}$.*

Example 12. *We have that $\operatorname{stab}_{D_{2n}}(\{1, n\}) = \{1\}$ and $\operatorname{wstab}_{D_{2n}}(\{1, n\}) = \{1, rs\}$.*

Example 13. *Consider $\mathrm{GL}_n(\mathbb{F})$ acting on $\mathbb{F}^n$. Consider $V = \mathbb{F}\text{-span}\{v\}$, with $v \neq 0$. We have*

$$\operatorname{stab}_{\mathrm{GL}_n(\mathbb{F})}(V) = \{g \in \mathrm{GL}_n(\mathbb{F}) : v \textit{ is an eigenvector of } g \textit{ with eigenvalue } 1\}$$

and

$$\operatorname{wstab}_{\mathrm{GL}_n(\mathbb{F})}(V) = \{g \in \mathrm{GL}_n(\mathbb{F}) : v \textit{ is an eigenvector of } g\}.$$

Note $V \neq \mathbb{F} - \operatorname{span}\{v\}$, but $V \neq \mathbb{F}\text{-span}\{v\}$

1.7 Lecture 7: Sep. 11, 2024

1.7.1 Conjugacy and Orbits of a Group Action

Recall that the group $(G, \circ)$ acts on the set G by left multiplication, or

$$L : G \times G \to G, \quad (g, h) \mapsto gh.$$

If $A \subseteq G$, then $\operatorname{stab}_G(A) = \{1\}$. If $H \leq G$, then $\operatorname{wstab}_G(H) = H$.

Another action of $(G, \circ)$ on G is given by

$$G \times G \to G, \quad (g, h) \mapsto ghg^{-1}.$$

We call this action the conjugation action.

Remark. *Note that conjugation is trivial if G is abelian. In general, conjugation is not faithful, although it could be.*

We state some associated definitions below.

Definition 1.7.1: Centralizers

The centralizer $C_G(A)$ of a subset $A \subseteq G$ is the subgroup

$$C_G(A) = \operatorname{stab}_G(A)$$

where $(G, \circ)$ acts on G by conjugation.

Remark. *We have that $C_G(g)$ is the subgroup of all elements that commute with $g \in G$.*

Definition 1.7.2: Normalizers

The normalizer $N_G(A)$ of a subset $A \subseteq G$ is the subgroup

$$N_G(A) = \operatorname{wstab}_G(A)$$

where $(G, \circ)$ acts on G by conjugation.

Definition 1.7.3: Centers

The center $Z(G)$ of a group G is the subgroup $Z(G) = C_G(G)$.

Proposition 1.7.1: Conditions for Triviality and Faithfulness of Conjugation

We have that the conjugation action is

1. trivial if and only if $Z(G) = G$, and
2. faithful if and only if $Z(G) = \{1\}$.

Proof. The proof is in two parts.

1. We have $ghg^{-1} = h$ for all $g \in G$ if and only if $g \in Z(G)$.
2. We have $ghg^{-1} = h$ for all $h \in G$ if and only if $g \in Z(G)$.

We are done. □

Example 14. *We have*

$$Z(D_2 n) = \begin{cases} \{1\} & n \bmod 2 \neq 0 \\ \{1, r^{\frac{n}{2}}\} & n \bmod 2 = 0 \end{cases}.$$

Example 15. *We have* $N_G(G) = N_G(\{1\}) = G$.

Definition 1.7.4: Normal Subgroups

A subgroup $H \leq G$ is normal if

$$N_G(H) = G.$$

We write $H \trianglelefteq G$.

Example 16. *Since* $N_G(Z(G)) = G$, *we have* $Z(G) \trianglelefteq G$.

Remark. *The subgroup* $N_G(H)$ *is the largest subgroup of* G *is which* $H \trianglelefteq N_G(H)$.

Definition 1.7.5: Transitivity of Group Actions

A group action of $(G, \circ)$ on A is transitive if

$$A = \{g(a) : g \in G\}$$

for each $a \in A$.

Example 17. *We have that*

- S_n *acts transitively on* $\{1, \ldots, n\}$,
- D_{2n} *acts transitively on* $\{1, \ldots, n\}$,
- $\mathrm{GL}_n(\mathbb{F})$ *acts transitively on* $\mathbb{F}^n \backslash \{0\}$,
- S_n *acts transitively on* $\{\{i, j\} : 1 \leq i < j \leq n\}$, *and*
- D_{2n} *does not act transitively on* $\{\{i, j\} : 1 \leq i < j \leq n\}$.

Definition 1.7.6: 🛑 Orbits

Given $(G, \circ)$ acting on A and $a \in A$, the orbit $G(a)$ of a is the subset

$$G(a) = \{g(a) : g \in G\} \subseteq A.$$

Remark. *The orbits of an action are the equivalence classes of the equivalence relation*

$$a \sim b \iff b \in G(a).$$

Appendices

Bibliography

[DF21] David S. Dummit and Richard M. Foote. *Abstract Algebra*. John Wiley and Sons, Inc., third edition, 2021.