

Suns

Eric Liu

CONTENTS

CHAPTER 1

GROUPS

PAGE 2

| | | |
|-----|----------------------|---|
| 1.1 | Isomorphism theorems | 2 |
| 1.2 | Group action | 7 |

Chapter 1

Groups

1.1 Isomorphism theorems

Let M be a set equipped with a binary operation $M \times M \rightarrow M$. We say M is a **monoid** if the binary operation is associative and there exists a two-sided identity $e \in M$.

Example 1.1.1. Defining $(x, y) \mapsto y$, we see that the operation is associative and every element is a left identity, but no element is a right identity unless $|M| = 1$. This is an example why identity must be two-sided.

Because the identity of a monoid is defined to be two-sided, clearly it must be unique. Suppose every element of monoid M has a left inverse. Fix $x \in M$. Let $x^{-1} \in M$ be a left inverse of x . To see that x^{-1} is also a right inverse of x , let $(x^{-1})^{-1} \in M$ be a left inverse of x^{-1} and use

$$(x^{-1})^{-1} = (x^{-1})^{-1}e = (x^{-1})^{-1}(x^{-1}x) = ((x^{-1})^{-1}x^{-1})x = ex = x$$

to deduce

$$xx^{-1} = (x^{-1})^{-1}x^{-1} = e$$

In other words, if we require every element of a monoid M to have a left inverse, then immediately every left inverse upgrades to a right inverse. In such case, we call M a **group**. Notice that inverses of elements of a group are clearly unique.

Unlike the category of monoids, the category of groups behaves much better. Given two groups G, H and a function $\varphi : G \rightarrow H$, if φ respects the binary operation, then φ also respects the identity:

$$e_H = (\varphi(x)^{-1})\varphi(x) = (\varphi(x)^{-1})\varphi(xe_G) = (\varphi(x)^{-1}\varphi(x))\varphi(e_G) = \varphi(e_G)$$

which implies that φ must also respect inverse. In such case, we call φ a **group homomorphism**. Given a subset $H \subseteq G$ closed under the binary operation, if H forms a group itself, then since the set inclusion $H \hookrightarrow G$ forms a group homomorphism, we have $e_H = e_G$, and thus x^{-1} in H, G are the same element.

In this note, by a **subgroup** H of G , we mean an injective group homomorphism $H \hookrightarrow G$. Clearly, a subset of G forms a subgroup if and only if it is closed under both the binary operation and inverse. Note that one of the key basic property of subgroup $H \subseteq G$ is that if $g \notin H$, then $hg \notin H$, since otherwise $g = h^{-1}hg \in H$.

Let S be a subset of G . The group of **words** in S is clearly the smallest subgroup of G containing S . We say this subgroup is **generated** by S . If G is generated by a single element, we say G is **cyclic**. Let $x \in G$. The **order** of G is the cardinality of G , and the order of x is the cardinality of the cyclic subgroup $\langle x \rangle \subseteq G$, or equivalently the infimum of the set of natural numbers n that makes $x^n = e$. Clearly, finite cyclic groups of order n are all isomorphic to \mathbb{Z}_n .

Let G be a group and H a subgroup of G . The **right cosets** Hx are defined by $Hx \triangleq \{hx \in G : h \in H\}$. Clearly, when we define an equivalence relation in G by setting:

$$x \sim y \stackrel{\Delta}{\iff} xy^{-1} \in H$$

the equivalence class $[x]$ coincides with the right coset Hx . Note that if we partition G using **left cosets**, the equivalence relation being $x \sim y \iff x^{-1}y \in H$, then the two partitions need not to be identical.

Example 1.1.2. Let $H \triangleq \{e, (1, 2)\} \subseteq S_3$. The right cosets are

$$H(2, 3) = \{(2, 3), (1, 2, 3)\} \quad \text{and} \quad H(1, 3) = \{(1, 3), (1, 3, 2)\}$$

while the left cosets being

$$(2, 3)H = \{(2, 3), (1, 3, 2)\} \quad \text{and} \quad (1, 3)H = \{(1, 3), (1, 2, 3)\}$$

■

However, as one may verify, we have a well-defined bijection $xH \mapsto Hx^{-1}$ between the sets of left cosets and right cosets of H . Therefore, we may define the **index** $|G : H|$ of H in G to be the cardinality of the collection of left cosets of H , without falling into the discussion of left and right. Moreover, by axiom of choice, there exists a set $T \subseteq G$ such that $|T \cap xH| = 1$ for all $x \in G$. Such T clearly makes the set map $T \times H \rightarrow G$ defined by:

$$(t, h) \mapsto th$$

a bijection. This proves the **Lagrange's theorem**:

$$|G| = |G : H| \cdot |H|$$

Consider a group G of prime order. If $x \neq e \in G$, then clearly the cyclic subgroup $\langle x \rangle$ must be G by Lagrange's theorem.

Because the inverse of an injective group homomorphism forms a group homomorphism, we know the set $\text{Aut}(G)$ of automorphisms of G forms a group. We say $\phi \in \text{Aut}(G)$ is an **inner automorphism** if ϕ takes the form $x \mapsto gxg^{-1}$ for some fixed $g \in G$. We say two elements $x, y \in G$ are **conjugated** if there exists some inner automorphism that maps x to y . Clearly conjugacy forms an equivalence relation. We call its classes **conjugacy classes**.

Example 1.1.3. Consider $G \triangleq \text{GL}_2(\mathbb{R})$ and consider:

$$H \triangleq \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in \text{GL}_2(\mathbb{R}) : n \in \mathbb{Z} \right\} \quad \text{and} \quad g \triangleq \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \in \text{GL}_2(\mathbb{R})$$

Note that $gHg^{-1} \subset H$. In other words, inner automorphisms can map a subgroup H into a subgroup strictly contained by H if G is infinite.

Equivalent Definition 1.1.4. (Normal subgroups) Let G be a group and N a subgroup. We say N is a **normal subgroup** of G if any of the followings hold true:

- (i) $\phi(N) \subseteq N$ for all $\phi \in \text{Inn}(G)$
- (ii) $\phi(N) = N$ for all $\phi \in \text{Inn}(G)$
- (iii) $xN = Nx$ for all $x \in G$.
- (iv) The set of all left cosets of N equals the set of all right cosets of N .
- (v) N is a union of conjugacy classes.
- (vi) For all $n \in N$ and $x \in G$, their **commutator** $nxn^{-1}x^{-1} \in G$ lies in N .
- (vii) For all $x, y \in G$, we have $xy \in N \iff yx \in N$.

Proof. (i) \implies (ii): Let $\phi \in \text{Inn}(G)$. By premise, $\phi(N) \subseteq N$ and $\phi^{-1}(N) \subseteq N$. Applying ϕ to both side of $\phi^{-1}(N) \subseteq N$, we have $\phi(N) \subseteq N \subseteq \phi(N)$, as desired.

(ii) \implies (iii): Consider the automorphisms:

$$\phi_{L,x}(g) = xg \quad \text{and} \quad \phi_{L,x^{-1}}(g) = x^{-1}g \quad \text{and} \quad \phi_{R,x}(g) = gx$$

Because $\phi_{L,x^{-1}} \circ \phi_{R,x} \in \text{Inn}(G)$, by premise we have:

$$xN = \phi_{L,x}(N) = \phi_{L,x} \circ \phi_{L,x^{-1}} \circ \phi_{R,x}(N) = \phi_{R,x}(N) = Nx$$

(iii) \implies (iv) is clear. (iv) \implies (iii): Let $x \in G$. By premise, there exists some $y \in G$ that makes $xN = Ny$. Let $x = ny$. The proof then follows from noting

$$xN = Ny = N(n^{-1}x) = Nx$$

(iii) \implies (v): Let $n \in N$ and $x \in G$. We are required to show $xnx^{-1} \in N$. Because $xN = Nx$, we know $xn = \tilde{n}x$ for some $\tilde{n} \in N$. This implies

$$xnx^{-1} = \tilde{n}xx^{-1} = \tilde{n} \in N$$

(v) \implies (vi): Fix $n \in N$ and $x \in G$. By premise, $xn^{-1}x^{-1} \in N$. Therefore, $n(xn^{-1}x^{-1}) \in N$, as desired.

(vi) \implies (vii): Let $xy \in N$. To see yx also belong to N , observe:

$$(xy)^{-1}(yx) = (xy)^{-1}x^{-1}xyx = [xy, x] \in N$$

(viii) \implies (i): Let $n \in N$ and $x \in G$. Because $(nx)x^{-1} = n \in N$, by premise we have $x^{-1}nx \in N$, as desired. ■

From the point of view of inner automorphism, we see that it is well-defined whether an element $g \in G$ **normalize** a subset $S \subseteq G$, independent of left and right. Because of the independence, For each subset $S \subseteq G$, we see that the set of elements $g \in G$ that normalize S forms a group, called the **normalizer** of S . Note that if g normalize S , then $gS = Sg$.

As we shall show, normal subgroup are what we may perform quotient on in the category of groups. Let G be a group and $N \subseteq G$ a subgroup. We say a group homomorphism $G \rightarrow G/N$ that vanishes on N satisfies the **universal property of quotient group** G/N if

(i) it vanishes on N . (**Group condition**)

(ii) for all group homomorphism $f : G \rightarrow H$ that vanishes on N there exist a unique group homomorphism $\tilde{f} : G/N \rightarrow H$ that makes the diagram:

$$\begin{array}{ccc} G & \twoheadrightarrow & G/N \\ & \searrow f & \downarrow \tilde{f} \\ & & H \end{array}$$

commute. (**Universality**)

Theorem 1.1.5. (The first isomorphism theorem for groups) Let N be a subgroup of G and $j : G \rightarrow G/N$ satisfies the universal property. Then j is surjective with kernel N . ■

Proof.

Because the kernel of a group homomorphism is clearly normal, if N is not normal, then there can not be a pair $G \rightarrow G/N$ that satisfies the universal property. If any things, this is the "reason" why normal subgroups are what meant to be quotiented in the category of group.

Corollary 1.1.6. (The first isomorphism theorem)

Proof. ■

Example 1.1.7. $G \triangleq S_3$. $S \triangleq \langle (1,2) \rangle$ and $H \triangleq \langle (2,3) \rangle$. SH doesn't form a group. $(2,3)(1,2) \notin SH$.

Second isomorphism theorem.

Third isomorphism theorem.

Correspondence theorem.

Because $\varphi \circ \phi_g \circ \varphi^{-1} = \phi_{\varphi(g)}$, we know $\text{Inn}(G)$ forms a normal subgroup of $\text{Aut}(G)$.

1.2 Group action

Let G be a group and X a set. If we say G **acts** on X we are defining a function $G \times X \rightarrow X$ such that

- (i) $e \cdot x = x$ for all $x \in X$.
- (ii) $(gh) \cdot x = g \cdot (h \cdot x)$ for all $g, h \in G$.

Because groups admit inverses, a G -action is in fact a group homomorphism $G \rightarrow \text{Sym}(X)$. The trivial action then correspond to the trivial group homomorphism. An action is **faithful** if it is injective.

Show that $Z(G) \subseteq \text{Ker } \theta$ if and only if θ is faithful.

An action is **free** if $g \cdot x = x$ for a $x \in X$ implies $g = e$. Note that the isomorphism $\text{Sym}(X) \rightarrow \text{Sym}(X)$ is always injective but never free unless $|X| \leq 2$. The action is **transitive** if for any $x, y \in X$, there always exists some $g \in G$ such that $y = g \cdot x$. An action is **regular** if it is both free and tran