MATH 594 - Group

AResseges Stery

January 19, 2024

Contents

1 Group Preliminaries

Definition 1.1 (Group)**.** *A **group** is a set G together with a binary operation $G \times G \to G$, often written $(a, b) \mapsto a \cdot b$ or simply ab, s.t. the following properties are satisfied:*

1. Associativity: $(ab)c = a(bc)$ *for all* $a, b, c \in G$.
2. Existence of Identity*: There exists* $e = e_G \in G$ *s.t.* $\forall a \in G, ae = a = ea$.
3. Existence of Inverse*: For all* $a \in G$*. there exists* $b \in G$ *s.t.* $ab = e = ba$.

*Furthermore, if the operation is commutative, i.e. for all $a, b \in G$, $ab = ba$, then the group is **commutative**, or **abelian**.*

Remark 1.1. If the group G is abelian, then the operation is often represented in additive notations (with operation denoted as "$+$", and inverse of $a \in G$ being $-a$).

Remark 1.2. One implicitly presented condition is that the operation of groups need to be closed within the set predefined. This is indicated by the signature of the operation, which should land in G. This often needs to be checked when the group structure is defined in some larger structure.

Remark 1.3. From the definition of group there are some immediate facts/properties:

1) The identity in the group is unique. Suppose that there exist two identity elements e and e', then by rule 2, $e = ee' = e'$.

2) For a given element in the group, the inverse of it is unique. Let b and b' both be the inverse of some $a \in G$. Then

$$b = b(ab') = (ba)b' = b'$$

the uniqueness allows us to unambiguously denote the inverse of a as a^{-1}. This also implies $(a^{-1})^{-1} = a$, as clearly by the previous process a is the inverse of a^{-1}; and the inverse is unique.

3) $(ab)^{-1} = b^{-1}a^{-1}$. By the uniqueness of the inverse element, it suffices to check that the claimed inverse satisfies rule 2. This is indeed the case as

$$(ab)(b^{-1}a^{-1}) = (a(bb^{-1}))a^{-1} = (ae)a^{-1} = aa^{-1} = e$$

and for multiplication in the other sequence the checking is similar.

4) For $a, b, c \in G$, then $ab = ac \implies b = c$; and $ba = ca \implies b = c$. This results directly from the fact that a is invertible; and multiplying on the left/right, respectively, a, gives the desired result.

Remark 1.4. The associativity of operation in the groups gives the unambiguity of writing successive multiplications. Rigorously, when written $x_1 \dots x_n$ for $n \geq 2$, it is defined inductively on n via specifying the result to be $(x_1 \dots x_{n-1})x_n$. The convention is that for $n = 0$ this is simply the identity.

In particular one can unambiguously write out the power of an element:

$$a^n := \begin{cases} \underbrace{a \dots a}_{n} & n > 0 \\ e & n = 0 \\ \underbrace{a \dots a}_{-n} & n < 0 \end{cases}$$

This gives $a^m \cdot a^n = a^{m+n}$ for all $m, n \in \mathbb{Z}$. The cases where m and n are of the same sign are clear; and for those of opposite sign, applying the same elimination process as Remark 1.3 3) gives the desired result.

If G is abelian, in additive notation we often denote $n \cdot a := a^n$.

Definition 1.2. *If G and H are groups, a **group homomorphism** $f : G \to H$ is a map s.t. $f(a \cdot b) = f(a) \cdot f(b)$ for all $a, b \in G$.*

Proposition 1.1. *If $f : G \to H$ is a group homomorphism, then $f(e_G) = e_H$, and $f(a^{-1}) = (f(a))^{-1}$.*

Proof. By Remark 1.3 4) and the property of identity, we have

$$f(e_G) \cdot e_H = f(e_G) = f(e_G \cdot e_G) = f(e_G) \cdot f(e_G) \implies e_H = f(e_G)$$

For the second statement, use the above result:

$$e_H = f(e_G) = f(a \cdot a^{-1}) = f(a) \cdot f(a^{-1})$$

By the definition $(f(a))^{-1}$ is the inverse of $f(a)$. By the uniqueness of inverse this gives $f(a^{-1}) = f(a^{-1})$. □

Remark 1.5. Given $f : G \to H$, $g : H \to K$ which are both f and g are group homomorphisms, then $f \circ g$ is also a group homomorphism. This results from the fact that

$$f(g(a \cdot b)) = f(g(a) \cdot g(b)) = f(g(a)) \cdot f(g(b))$$

The fact that morphism is closed w.r.t. composition implies that the groups form a category Grps.

Definition 1.3. *If G and H are groups, then $f : G \to H$ is a **group isomorphism** if it is a bijective group homomorphism.*

Proposition 1.2. *$f : G \to H$ being a group homomorphism is a group isomorphism if and only if there exists a group homomorphism $g : H \to G$ s.t. $g \circ f = \mathrm{Id}_G$, and $f \circ g = \mathrm{Id}_H$.*

Proof. It suffices to show implication in two directions:

- $\Rightarrow$: Since f is bijective, there must admit a (pointwise) inverse of f s.t. $f^{-1} \circ f = \mathrm{Id}_G$, $f \circ f^{-1} = \mathrm{Id}_H$. Define $g = f^{-1}$. It suffices to check that g is a group homomorphism. To prove this we need to verify that for all $u, v \in H$, $g(u \cdot v) = g(u) \cdot g(v)$. Since f is bijective, f is in particular injective, i.e. $a = b$ if and only if $f(a) = f(b)$ for all $a, b \in G$. Therefore to verify the equality above it suffices to verify the equality after applying f, i.e. $f \circ g(u \cdot v) = f \circ g(u) \cdot f \circ g(v)$. Then the equality holds as $f \circ g = \mathrm{Id}_H$.
- $\Leftarrow$: Prove the contrapositive. If f is not injective, then g cannot be well-defined; and if f is not surjective, then the domain of the composition $f \circ g$ is not the whole H.

□

Remark 1.6. Recall that under the context of categories, isomorphisms are defined as in Proposition 1.2. The same proposition implies that group isomorphisms are isomorphisms in the categorical sense.

Remark 1.7. If there exists an isomorphism $f : G \to H$ between groups G and H, then G and H are considered as **isomorphic**, denoted $G \cong H$. This is an equivalence relation as compositions of isomorphisms are still isomorphisms.

Definition 1.4. *Let G be a group. Then a **subgroup** of G is a subset $H \subseteq G$, which is in it self a group; and the inclusion map $i : H \hookrightarrow G$ is a group homomorphism. H being the subgroup of G is denoted as $H \leq G$.*

Remark 1.8. The fact that the inclusion map is required to be a group homomorphism implies that the operation in H is simply the restriction of the operation in G.

Proposition 1.3. *Let G be a group, and $H \subseteq G$ a subset. Then the followings are equivalent:*

i) H is a subgroup of G.

ii) The following three conditions are satisfied:

1) For all $a, b \in H$, $a \cdot b \in H$.

2) $e_G \in H$.

3) (Under the same operation of G) $a^{-1} \in H$ for all $a \in H$.

iii) H is nonempty; and for all $x, y \in H$, $x \cdot y^{-1} \in H$.

The third condition is often used to test whether $H \subseteq G$ gives a subgroup.

Proof. Verify the following implications:

- i) $\implies$ ii). By the definition of subgroup, H together with the same operation is a group, which by the definition of group is closed w.r.t. the group; and every element should admit an inverse. By the fact that i is an inclusion, and by Proposition 1.1 $i(e_H) = e_G$ with $e_G = e_H$.
- ii) $\implies$ i). Check that H is a group: associativity is given by the fact that the operation is identical to that in G. and G is a group; existence of inverse and identity results directly from hypothesis 2) and 3); and the operation is defined as $H \times H \to H$ given by hypothesis 1).
- ii) $\implies$ iii). By 2) H is nonempty. For all $x, y \in H$, by 3) $y^{-1} \in H$; and by 1) $x \cdot y^{-1} \in H$ given that both x and y^{-1} are in H.
- iii) $\implies$ ii). Since H is nonempty, there exists $a \in H$. iii) implies that $a \cdot a^{-1} = e_G \in H$, giving 2). For all $a \in H$, let $x = e_G$ and $y = a$, which gives $a^{-1} \in H$, satisfying 3). For all $a, b \in H$, letting $x = a, y = b^{-1}$ gives $a \cdot b \in H$.

□

Proposition 1.4. *Let $f : G \to H$ be a group homomorphism, then if $G' \leq G$, then $f(G') \leq H$.*

Proof. Apply the result of Proposition 1.3. Since $G' \leq G$, $e_G \in G'$, and bby Proposition 1.1, $f(e_G) = e_H$, giving that $f(G')$ is nonempty. For all $x, y \in f(G')$, let $u, v \in G'$ s.t. $x = f(u), y = f(v)$. Since G' is a subgroup of G, $u \cdot v^{-1} \in G'$. By Proposition 1.1, this implies $f(u) \cdot f(v^{-1}) = f(u) \cdot f(v^{-1}) \in f(G')$, which gives that $f(G') \leq H$. □

Proposition 1.5. *Let $f : G \to H$ be a group homomorphism. If $H' \leq H$, then $f^{-1}(H') \leq G$. In particular, $f^{-1}(e_H) = \ker f := \{u \in G \mid f(u) = e_H\}$ is a subgroup of G.*

Proof. Apply the same argument as in the above proposition. $H' \leq H \implies e_H \in H' \implies e_G \in f^{-1}(H')$, i.e. $f^{-1}(H')$ is nonempty. For all $u, v \in f^{-1}(H')$, $f(u \cdot v^{-1}) = f(u)f(v)^{-1} \in H'$ since $H' \leq H$, which implies that $u \cdot v^{-1} \in f^{-1}(H')$, i.e. $f^{-1}(H')$ is a group. □

Proposition 1.6. *Let $f : G \to H$ be a group homomorphism. Then f is injective if and only if* $\ker f = \{e_G\}$.

Proof. Proceed by showing implication in both directions:

$\Rightarrow$: Let $u \in \ker f$. Then $f(a) = f(a) \cdot e = f(a) \cdot f(u) = f(a \cdot u)$. But f being injective implies that $a = a \cdot u$, i.e. $u = e$.

$\Leftarrow$: For $u, v \in G$ s.t. $f(u) = f(v)$, we have $e = f(u) \cdot (f(v))^{-1} = f(u) \cdot f(v^{-1}) = f(u \cdot v^{-1}) \implies thatu \cdot v^{-1} \in \ker f$. But since the only element in $\ker f$ is the identity, this gives $u \cdot v^{-1} = e \implies u = v$, i.e. f is injective.

□

2 Group of Permutations

Definition 2.1. *Given a set Ω, the **permutation group** is defined to be $S_\Omega := \{f : \Omega \to \Omega \mid f bijection\}$. Since compositions of bijective maps are still bijective, defining the operation to be composition gives this a group structure.*

Remark 2.1. Notice that the permutation group structure depends only on the cardinality of the group on which permutations are considered. Explicitly, for $\alpha : \Omega \to \Omega'$ a bijection, there exists an isomorphism between the corresponding groups of permutations: $\beta : S_\Omega \to S_{\Omega'} : f \mapsto \alpha \circ f \circ \alpha^{-1}$. This is indeed an isomorphism as this is first a group homomorphism since

$$\beta(f \circ g) = \alpha \circ f \circ g \circ \alpha^{-1} = \alpha \circ f \circ \alpha^{-1}\alpha \circ g \circ \alpha^{-1} = \beta(f) \circ \beta(g)$$

and this being an isomorphism follows from the fact that there exists an obvious inverse $\beta^{-1} : f \mapsto \alpha^{-1} \circ f \circ \alpha$. Therefore it suffices to denote such permutation group by the cardinality of Ω: for $\Omega = \{1, \ldots, n\}$ S_Ω is denoted as S_n.

Proposition 2.1 (Cayley)**.** *Every group can be embedded into some S_Ω. Explicitly, for group G the map $\alpha : G \to S_G$ s.t. $g \mapsto \alpha_g$ where $\alpha_g(h) = gh$ (α_g is the action of G on G defined by multiplication by g.) is an injective group homomorphism.*

Proof. It suffices to syntactically check that the following requirements are satisfied:

- $\alpha_g \in S_G$. It suffices to check that indeed multiplication by an element in the group gives a bijection. This is clear as the action has an inverse, namely multiplying the inverse of that element.
- *α gives a group homomorphism.* By definition $\alpha_{gh} = \alpha_g \cdot \alpha_h$.
- *α is injective.* It suffices to check that $\ker \alpha = e_G$. This is indeed the case, as for $g \in G$ s.t. $\alpha_g = \mathrm{Id}$, $\alpha_g(e_G) = g \cdot e_G = e_G \implies g = e_G$.

□

3 Groups Generated by a Subset

4 The Dihedral Groups