MATH 594 - Group

AResseges Stery

February 17, 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 1.2. 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 1.3. 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 1.4. 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 1.5. 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 1.4 3) gives the desired result.

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

Definition 1.6. 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 1.7. 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 1.4 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 1.8. 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 1.9. If G and H are groups, then $f : G \to H$ is a **group isomorphism** if it is a bijective group homomorphism.

Proposition 1.10. $f : G \to H$ 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 1.11. Recall that under the context of categories, isomorphisms are defined as in Proposition 1.10. The same proposition implies that group isomorphisms are isomorphisms in the categorical sense.

Remark 1.12. 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 1.13. 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 1.14. 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 1.15. 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 1.7 $i(e_H) = e_G$ 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 1.16. 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 1.15. Since $G' \leq G$, $e_G \in G'$, and bby Proposition 1.7, $f(e_G) = e_H$, 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 1.7, 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 1.17. 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 1.18. 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 $S_\Omega := \{f : \Omega \to \Omega \mid f \text{ bijection}\}$. Since compositions of bijective maps are still bijective, defining the operation to be composition gives this a group structure.

Remark 2.2. 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 2.3 (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

Remark 3.1. If $(H_i)_{i\in I}$ is a family of subgroups of G, then $\bigcap_{i\in I} H_i$ is also a subgroup of G. This can be verified by taking an element in the intersection, and check each rule of group in each of the H_is.

Definition 3.2. If $A \subseteq G$ is a subset of G, then the **subgroup generated by** A is defined as

$$\langle A\rangle := \bigcap_{A\subseteq H\leq G} H$$

Remark 3.3. By definition $\langle A\rangle$ is well-defined, as in particular $A \subseteq G \leq G$. By the previous remark, $\langle A\rangle$ is a subgroup of G. It is also the smallest subgroup that contains A.

Proposition 3.4. Let $A \subseteq G$ be a subset of G, then $\langle A\rangle = \{x_1 \dots x_n \mid n \in \mathbb{Z}_{>0}; \forall i, x_i \in G \text{ or } x_i^{-1} \in G\}$. For $n = 0$, $x_1 \dots x_n = e$.

Proof. Proceed by double inclusion:

$\subseteq$: Proceed to show that RHS satisfies the definition of the Hs above. For RHS consider $n = 1$, with $x_1 \in G$ which takes all elements in G. This gives $A \subseteq$ RHS. Further use Proposition 1.15, which for any $x_1 \dots x_m, y_1 \dots y_n \in$ RHS, each summand of $x_1 \dots x_m(y_1 \dots y_n)^{-1} = x_1 \dots x_m y_n^{-1} \dots y_1^{-1}$ is either in A or its inverse is in A implying that RHS is a group. Definition above gives the subset relation.

$\supseteq$: It suffices to verify that any element in the specified form is in $\langle A\rangle$. This is the case as for $x_1 \dots x_n$ where for all i, either $x_i \in A$ or $-x_i \in A$, $x_i \in \langle A\rangle$ by definition, and multiplication of two elements in the group is still in the group by closure of the operation.

□

Definition 3.5. The following defines some common terminology for characterization of a group:

- G is **finitely generated** if there exists a finite set $A \subseteq G$ s.t. $G = \langle A \rangle$.
- G is **finite** if it has finitely many elements.
- The **order** of G, denoted $|G|$, is the number of elements in G if it is finite; or ∞ if G is not finite (infinite).
- G is **cyclic** if it attains a generating set with a single element a. In this case G is denoted as $G = \langle A \rangle$.
- The **order** of $x \in G$, denoted $|a|$ is the order of $\langle a \rangle$.

Remark 3.6. Cyclic groups are abelian. By the alternative definition provided in Proposition 3.4, $\langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$.

Proposition 3.7. If a group G is cyclic, then $G \simeq \mathbb{Z}$ if G is infinite, or $G \simeq \mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{Z}_{>0}$.

Proof. Choose $a \in G$ s.t. $G = \langle a \rangle$. Proceed via showing implication in both directions:

$\Rightarrow$: Consider $f : \mathbb{Z} \to G$ s.t. $f(1) = a$. This is a group homomorphism, Then either

- *f is injective.* By definition of cyclic groups, for any $s \in G$ there exists $m \in G$ s.t. $s = a^m$. Then $f(m) = s$ according to the definition of f, giving that f is surjective. Then this falls into the first case, giving $G \simeq \mathbb{Z}$.
- *f is not injective.* Then there are nonzero elements in f. Since $\ker f \subseteq \mathbb{Z}$, there exists a smallest positive element. Define the map $f_n : \mathbb{Z}/n\mathbb{Z} \to G$ s.t. $[1] \mapsto a$. Check the followings:
  - *f_n is well-defined.* It suffices to check that if $[m_1] = [m_2]$, then $f([m_1]) = (f[m_2])$. This is indeed the case as

$$f([m_1]) = a^{m_1} \overset{!}{=} a^{m_1} \cdot a^{(m_2 - m_1)} = a^{m_2} \cdot a^{nk} = a^{m_2} \cdot (a^n)^k = a^{m_2} = f([m_2])$$

    for some $k \in \mathbb{Z}$, where $\overset{!}{=}$ holds since $[m_1] = [m_2]$ implies $n \mid (m_1 - m_2)$. This gives $a^{m_1 - m_2} = e$ since $a^n = e$.
  - *f_n is injective.* For $a \in \mathbb{Z}$ s.t. $f_n([a]) = 0$, $a = 0$ as otherwise this conflicts with the hypothesis that n is the smallest of such integers.
  - *f_n is surjective.* Follows from the same argument in the case where G is infinite.

$\Leftarrow$: Since $\mathbb{Z} = \langle 1 \rangle$ and $\mathbb{Z}/n\mathbb{Z} = \langle [1] \rangle$, both of which are cyclic.

□

4 The Dihedral Group

Definition 4.1. Let $n \geq 3$, and $P_n \subset \mathbb{R}^2 \simeq \mathbb{C}$ be the regular n-gon s.t. its vertices are at the n-th roots of 1. Then the **dihedral group** D_{2n} is the group of symmetry of P_n. Alternatively, one can write

$$D_{2n} = \{\varphi \in \mathrm{GL}_2(\mathbb{R}) \mid \varphi(P_n) = P_n\}$$

Remark 4.2. We have a injective map $\alpha : D_{2n} \to S_n$, where $\alpha(\varphi)$ is given by the restriction of φ to the vertices of P_n. This map is injective as $\{v_1, \ldots, v_n\}$ spans $\mathbb{R}^2$. Therefore, specifying how the vertices are transformed (permuted) fixes the whole linear transformation.

Remark 4.3. Notice the following relations: by definition of rotation $\sigma^n = e$; and $\sigma\tau\sigma = \tau$, which implies $\sigma^{n-1}\tau = \tau\sigma$. This enables changing the sequence of applying σs and τs.

Proposition 4.4. For a fixed n, let σ be the operation of counter-clockwise rotation by $\frac{2\pi}{n}$ on P_n; and τ_j be the operation of symmetry w.r.t. the symmetry axis passing through the vertex j (which is a direction; invariant w.r.t. transformations on P_n). Then for every $\alpha \in D_{2n}$, it must be in the form of σ^i or $\sigma^1 \cdot \tau_j$, for some $i, j \in \mathbb{Z}$.

Proof. How the operations permute the vertices is characterized by

$$\sigma : v_k \mapsto v_{k+1} \qquad \tau : v_{j+k} \mapsto v_{j-k}$$

Following the strategy of the previous remark, to fix the whole operation α it suffices to fix how vertices are transformed. Since elements of D_{2n} are linear transformations, they map line segments to line segments, and therefore adjacent vertices to adjacent vertices. Then for $v_1 \mapsto v_{i+1}$, either $v_2 \mapsto v_{i+2}$, then $\alpha = \sigma^i$; or $v_2 \mapsto v_i$, then $\alpha = \sigma^i\tau_j$. The indices are considered modulo n and then plus 1. □

Remark 4.5. Using Remark 4.3, we can check that indeed $\langle D_{2n} \rangle = D_{2n}$, by applying the remark to move all the rotations to the left of symmetries, and the reduce the expression by relations $\sigma^n = \tau^2 = e$.

5 Product of Groups

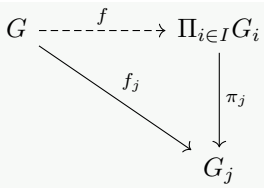
Definition 5.1. (Product of Groups) Suppose that we have a family of groups $(G_i)_{i\in I}$. The **product** of groups is defined as

$$\Pi_{i\in I} G_i := \{(x_i)_{i\in I} \mid x_i \in G_i \forall i \in I\}$$

with the operation defined component-wise i.e. $(x_i)_{i\in I} \cdot (y_i)_{i\in I} := (x_i y_i)_{i\in I}$.

Remark 5.2. By the definition of the operation, the identity in the product of groups $(G_i)_{i\in I}$ is $(e_i)_{i\in I}$ where e_i is the unique identity element in G_i; and the inverse of $(x_i)_{i\in I}$ is $(x_i^{-1})_{i\in I}$.

Proposition 5.3. (Universal Property of Product of Groups) Let group homomorphism $\pi_j : \Pi_{i\in I} G_i \to G_j, (x_i)_{i\in I} \mapsto x_j$ be the projections. Then given group homomorphisms $f_i : G \to G_i$ for all i, there exists a unique group homomorphism $f : G \to \Pi_{i\in I} G_i$ s.t. $\pi_i \circ f = f_i$ for all $i \in I$, i.e. the following diagram commute:



Proof. Since the diagram is required to commute, the homomorphism f can be only defined as $f(x) = (f_i(x))_{i\in I}$, which gives the uniqueness. Existence follows from the fact that f_is are group homomorphisms for all i, which implies that f is also a group homomorphism. □

Example 5.4. (Chinese Remainder Theorem) Let $m, n \in \mathbb{Z}_{\geq 0}$ which are relatively prime. Then there exists group isomorphism $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Proof. Consider group homomorphisms:

$$f : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, \quad [x + mn\mathbb{Z}] \mapsto [x + m\mathbb{Z}]$$

$$g : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad [x + mn\mathbb{Z}] \mapsto [x + n\mathbb{Z}]$$

Check that f and g are well-defined. For f, let $a = [x + mn\mathbb{Z}] = b = [y + mn\mathbb{Z}]$. This implies that $mn \mid (x - y)$. By definition, $f(a) = [x + m\mathbb{Z}], f(b) = [y + m\mathbb{Z}]$. But this implies that $[x + m\mathbb{Z}] = [y + m\mathbb{Z}]$ as $mn \mid (x - y) \implies m \mid (x - y)$. The well-definedness of g is similar.

Use the universal property above (Proposition 5.3), there exists a unique $h : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ s.t. $h_1 = f, h_2 = g$ where h_i indicates the projection to i-th field after applying h. Check that this is an isomorphism:

- h is injective. Consider the kernel of f: for all $[x + mn\mathbb{Z}] \in \ker f$, $[x + m\mathbb{Z}] = 0$ and $[x + n\mathbb{Z}] = 0$. But this implies that $m \mid x$ and $n \mid x$, i.e. $mn \mid x$, which gives $[x + mn\mathbb{Z}] = 0$. That is, elements in $\ker f$ are identically zero, which gives the injectivity.
- Notice that $\mathbb{Z}/mn\mathbb{Z}$ has mn elements, while $\mathbb{Z}/m \times \mathbb{Z}/n\mathbb{Z}$ has $m \cdot n = mn$ elements. Therefore h being injective implies h being bijective.

□

6 Normal Subgroup

Definition 6.1. (Left/Right Congruence) Let G be a group, with $H \leq G$. Then for $x, y \in G$,

- x and y are **left congruent** mod H, denoted $x \equiv_\ell y \pmod H$ if $x^{-1}y \in H$.
- x and y are **right congruent** mod H, denoted $x \equiv_r y \pmod H$ if $xy^{-1} \in H$.

Remark 6.2. $\equiv_\ell$ and $\equiv_r$ are equivalence relations. The equivalence classes are noted as xH and Hx for $x \in G$, respectively.

Notation. If G is abelian, the operation is written additively. The congruence classes will then be denoted as $x + H$ and $H + x$ for left and right congruence classes, respectively.2

Proof. The proof is similar for two equivalence relations, so we only check for left congruence:

- $\equiv_\ell$ *is Reflexive.* $x^{-1} \cdot x \equiv e \in H$.
- $\equiv_\ell$ *is symmetric.* If $x^{-1}y \in H$, given that H is a subgroup of G, $(x^{-1}y)^{-1} \in H$. This implies that $y^{-1}x \in H$, i.e. $y \equiv_\ell x \pmod H$.
- $\equiv_\ell$ *is transitive.* Suppose that $x \equiv_\ell y \pmod H, y \equiv_\ell z \pmod H$. By the fact that subgroups are closed, $(x^{-1}y)(y^{-1}z) = x^{-1}z \in H$.

□

Remark 6.3. G is the disjoint union of equivalence classes w.r.t. $\equiv_\ell$. For $x, y \in G$ s.t. $x \equiv_\ell y \pmod H$, there exists $h \in H$ s.t. $x = yh$.

Proposition 6.4. There is a bijection between xH and Hx for all $x \in G, H \leq G$.

Proof. Define the map $\varphi : \{xH \mid x \in G\} \to \{Hx \mid x \in G\}$, $gH \mapsto Hg^{-1}$. Check that this is well-defined: for $g_1, g_2 \in G$ s.t. $g_1H = g_2H$, there exists $h \in H$ s.t. $g_1 = g_2h$. Then $Hg_1 = H(g_2h)^{-1} = Hh^{-1}g_2^{-1} = Hg_2^{-1}$. It has inverse $Hg \mapsto g^{-1}H$, with well-definedness similarly proved, which implies that φ is a bijection. □

Remark 6.5. In the prove above, we cannot define $\varphi : gH \mapsto Hg$ as in this case this is not well-defined. Specifically, if g_1 does not commute with h for $g_1 = g_2h$, $\varphi(g_2H) = Hg_1h$ which is not necessarily equal to Hg_1.

Since the number of congruence classes w.r.t. $x \in G$ does not change with choice of left or right congruence classes and depends only on H, the following definition is well-defined:

Definition 6.6. (Index) Let G be a group, with $H \leq G$. Then the number of distinct xH for $x \in G$ is the **index** of H in G, denoted as $(G : H)$.

Remark 6.7. For all $g_1, g_2 \in H$, there exists bijections $g_1H \mapsto g_2H$ and $Hg_1 \mapsto g_2H$, given by multiplication on the left by $g_2g_1^{-1}$, and multiplication on the right by $g_1^{-1}g_2$, respectively.

Theorem 6.8. (Lagrange) Let G be a group. If $H \leq G$, and G is finite, then $|G| = |H| \cdot (G : H)$.

Proof. By Remark 6.3, G is the disjoint union of congruence classes. There are $(G : H)$ congruence classes, with each having $|H|$ elements. □

Corollary 6.9. In particular, for all $H \leq G$, $|H| \mid |G|$. If G is finite, for all $g \in G$, $|\langle g \rangle| \mid |G|$, i.e. $g^{|G|} = g^{|\langle g \rangle| \cdot (G:\langle g \rangle)} = e$.

Example 6.10. (Fermat's Little Theorem) Let $G = (\mathbb{Z}/p\mathbb{Z})^\times$ with p prime. Then $|G| = p-1$. For $a \in \mathbb{Z}$ s.t. $p \nmid a$, $|[a]| = p-1$, which implies that $a^{p-1} \equiv 1 \pmod{p}$.

We now seek to define a group structure on the congruence classes modulo a subgroup $H \leq G$. The issue is that the operation is not necessarily well-defined. The natural definition of the group operation is given via $(g_1H, g_2H) \mapsto (g_1g_2H)$. For $g_1 \equiv_\ell g_1' \pmod{H}, g_2 \equiv_\ell g_2' \pmod{H}$ we would like $g_1g_2 \equiv_\ell g_1'g_2'$. In terms of the elements, we have $g_1g_1'^{-1}g_2g_2'^{-1} \in H$ and we want $g_1g_2g_2'^{-1}g_1^{-1} \in H$. This requires extra requirements on H.

Claim 6.11. The following two conditions are equivalent:

- For all $g_1^{-1}g_1' \in H, g_2^{-1}g_2' \in H$, this implies $(g_1g_2)^{-1}(g_1g_2)' \in H$.
- For all $x \in G, h \in H, xhx^{-1} \in H$.

Proof. Consider the following constructions in two directions:

$\Rightarrow$ Notice $g_1^{-1}g_1 \in H$ by hypothesis. Choose $g_2^{-1} = x, g_2' = x^{-1}$.

$\Leftarrow$ Notice $(g_1g_2)^{-1}(g_1g_2)' = g_2^{-1}g_1^{-1}g_1'g_2' \in H$. Choose $g_2 = g_2' = x$, with $g_1^{-1}g_1' = h$. Such g_1 and g_1' exists by first arbitrarily choose $g_1 \in H$ then compute $g_1' = g_1h$.

□

Definition 6.12. (Normal Subgroup) A subgroup $H \leq G$ is **normal** if for all $x \in G, xHx^{-1} \in H$, where

$$xHx^{-1} := \{xhx^{-1} \mid h \in H\}$$

Normal subgroups are denoted by $H \lhd G$.