Math 2070 Week 1

Topics: Groups

Motivation

- How many ways are there to color a cube, such that each face is either red or green?

  Answer: 10. Why?

- How many ways are there to form a triangle with three sticks of equal lengths, colored red, green and blue, respectively?

- What are the symmetries of an equilateral triangle?

  Dihedral Group D_3

Cayley Table

$*$
a
b
c
a
a^2
ab
ac
b
ba
b^2
bc
c
ca
cb
c^2

Cayley Table for D_3

*
r_0
r_1
r_2
s_0
s_1
s_2

r_0
r_0
r_1
r_2
s_0
s_1
s_2

r_1
r_1
r_2
r_0
s_1
s_2
s_0

r_2
r_2
r_0
r_1
s_2
s_0
s_1

s_0
s_0
s_2
s_1
r_0
r_2
r_1

s_1
s_1
s_0
s_2
r_1
r_0
r_2

s_2
s_2
s_1
s_0
r_2
r_1
r_0

Groups

Definition 1.1. *A group G is a set equipped with a binary operation $* : G \times G \longrightarrow G$ (typically called* **group operation** *or "* **multiplication** *"), such that:*

- **Associativity**
$$(a * b) * c = a * (b * c),$$
for all $a, b, c \in G$. In other words, the group operation is **associative** *.*

- **Existence of an Identity Element**
There is an element $e \in G$, called an **identity element** *, such that:*
$$g * e = e * g = g,$$
for all $g \in G$.

- **Invertibility**
Each element $g \in G$ has an **inverse** *$g^{-1} \in G$, such that:*
$$g^{-1} * g = g * g^{-1} = e.$$

- Note that we do not require that $a * b = b * a$.

- We often write ab to denote $a * b$.

Definition 1.2. *If $ab = ba$ for all $a, b \in G$. We say that the group operation is* **commutative** *, and that G is an* **abelian group** *.*

Example 1.3. *The following sets are groups, with respect to the specified group operations:*

- *$G = \mathbb{Q}\backslash\{0\}$, where the group operation is the usual multiplication for rational numbers. The identity is $e = 1$, and the inverse of $a \in \mathbb{Q}\backslash\{0\}$ is $a^{-1} = \frac{1}{a}$. The group G is abelian.*

- *$G = \mathbb{Q}$, where the group operation is the usual addition $+$ for rational numbers. The identity is $e = 0$. The inverse of $a \in \mathbb{Q}$ with respect to $+$ is $-a$. Note that $\mathbb{Q}$ is* **NOT** *a group with respect to multiplication. For in that case, we have $e = 1$, but $0 \in \mathbb{Q}$ has no inverse $0^{-1} \in \mathbb{Q}$ such that $0 \cdot 0^{-1} = 1$.*

Exercise 1.4. *Verify that the following sets are groups under the specified binary operation:*

- $(\mathbb{Z}, +)$
- $(\mathbb{R}, +)$
- $(\mathbb{R}^\times, \cdot)$
- $(U_m, \cdot)$, *where* $m \in \mathbb{N}$,

$$U_m = \{1, \xi_m, \xi_m^2, \ldots, \xi_m^{m-1}\},$$

and $\xi_m = e^{2\pi i/m} = \cos(2\pi/m) + i\sin(2\pi/m) \in \mathbb{C}$.

- *The set of bijective functions* $f : \mathbb{R} \longrightarrow \mathbb{R}$, *where* $f * g := f \circ g$ *(i.e. composition of functions).*

Exercise 1.5. *1.* **WeBWork**

2. **WeBWork**

3. **WeBWork**

4. **WeBWork**

5. **WeBWork**

6. **WeBWork**

7. **WeBWork**

8. **WeBWork**

9. **WeBWork**

Example 1.6. *The set $G = \mathrm{GL}(2, \mathbb{R})$ of real 2×2 matrices with nonzero determinants is a group under matrix multiplication, with identity element:*

$$e = \begin{pmatrix} 1 & amp; 0 \\ 0 & amp; 1 \end{pmatrix}.$$

In the group G, we have:

$$\begin{pmatrix} a & amp; b \\ c & amp; d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & amp; -b \\ -c & amp; a \end{pmatrix}$$

Note that there are matrices $A, B \in \mathrm{GL}(2, \mathbb{R})$ such that $AB \neq BA$. Hence $\mathrm{GL}(2, \mathbb{R})$ is not abelian.

Exercise 1.7. *The set $\mathrm{SL}(2, \mathbb{R})$ (* **Special Linear Group** *) of real 2×2 matrices with determinant 1 is a group under matrix multiplication.*

Claim 1.8. *The identity element e of a group G is unique.*

Proof. Suppose there is an element $e' \in G$ such that $e'g = ge' = g$ for all $g \in G$. Then, in particular, we have:

$$e'e = e$$

But since e is an identity element, we also have $e'e = e'$. Hence, $e' = e$. □

Claim 1.9. *Let G be a group. For all $g \in G$, its inverse g^{-1} is unique.*

Proof. Suppose there exists $g' \in G$ such that $g'g = gg' = e$. By the associativity of the group operation, we have:

$$g' = g'e = g'(gg^{-1}) = (g'g)g^{-1} = eg^{-1} = g^{-1}.$$

Hence, g^{-1} is unique. □

Let G be a group with identity element e. For $g \in G$, $n \in \mathbb{N}$, let:

$$g^n amp; := \underbrace{g \cdot g \cdots g}_{n \text{ times}}.$$

$$g^{-n} amp; := \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{n \text{ times}}$$

$$g^0 amp; := e.$$

Claim 1.10. *Let G be a group.*

1. *For all $g \in G$, we have:*
$$(g^{-1})^{-1} = g.$$
2. *For all $a, b \in G$, we have:*
$$(ab)^{-1} = b^{-1}a^{-1}.$$
3. *For all $g \in G$, $n, m \in \mathbb{Z}$, we have:*
$$g^n \cdot g^m = g^{n+m}.$$

Proof. **Exercise.** □

Definition 1.11. *Let G be a group, with identity element e. The* **order** *of G is the number of elements in G. The* **order** $\operatorname{ord} g$ *of an $g \in G$ is the smallest $n \in \mathbb{N}$ such that $g^n = e$. If no such n exists, we say that g has* **infinite order** .

Theorem 1.12. *Let G be a group with identity element e. Let g be an element of G. If $g^n = e$ for some $n \in \mathbb{N}$, then $\operatorname{ord} g$ divides n.*

Proof. Shown in class. □

courseMath 2070 week2

Math 2070 Week 2

Topics: Groups

Definition 2.13. *Let G be a group, with identity element e.*

The **order** *of G is the number of elements in G.*

The **order** $\operatorname{ord} g$ *of an element $g \in G$ is the smallest $n \in \mathbb{N}$ such that $g^n = e$. If no such n exists, we say that g has* **infinite order** .

Theorem 2.14. *Let G be a group with identity element e. Let g be an element of G. If $g^n = e$ for some $n \in \mathbb{N}$, then $\operatorname{ord} g$ is finite, and moreover $\operatorname{ord} g$ divides n.*

Proof. Shown in class. □

Exercise 2.15. *If G has finite order, then every element of G has finite order.*

Definition 2.16. *A group G is* **cyclic** *if there exists $g \in G$ such that every element of G is equal to g^n for some integer n. In which case, we write: $G = \langle g \rangle$, and say that g is a* **generator** *of G.*

Note: The generator of of a cyclic group might not be unique.

Example 2.17. $(U_m, \cdot)$ *is cyclic.*

Exercise 2.18. *A finite cyclic group G has order (i.e. size) n if and only if each of its generators has order n.*

Exercise 2.19. $(\mathbb{Q}, +)$ *is not cyclic.*

Permutations

Definition 2.20. *Let X be a set. A* **permutation** *of X is a bijective map $\sigma : X \longrightarrow X$.*

Claim 2.21. *The set S_X of permutations of a set X is a group with respect to $\circ$, the composition of maps.*

Proof.

- Let σ, γ be permutations of X. By definition, they are bijective maps from X to itself. It is clear that $\sigma \circ \gamma$ is a bijective map from X to itself, hence $\sigma \circ \gamma$ is a permutation of X. So $\circ$ is a well-defined binary operation on S_X.
- For $\alpha, \beta, \gamma \in S_X$, it is clear that $\alpha \circ (\beta \circ \gamma) = (\alpha \circ \beta) \circ \gamma$.
- Define a map $e : X \longrightarrow X$ as follows:

$$e(x) = x, \quad \text{for all } x \in X.$$

  It is clear that $e \in S_X$, and that $e \circ \sigma = \sigma \circ e = \sigma$ for all $\sigma \in S_X$. Hence, e is an identity element in S_X.

- Let σ be any element of S_X. Since $\sigma : X \longrightarrow X$ is by assumption bijective, there exists a bijective map $\sigma^{-1} : X \longrightarrow X$ such that $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = e$. So σ^{-1} is an inverse of σ with respect to the operation $\circ$.

□

Terminology: We call S_X the **Symmetric Group** on X.
Notation: If $X = \{1, 2, \ldots, n\}$, where $n \in \mathbb{N}$, we denote S_X by S_n.
For $n \in \mathbb{N}$, the group S_n has $n!$ elements.
For $n \in \mathbb{N}$, by definition an element of S_n is a bijective map $\sigma : X \longrightarrow X$, where $X = \{1, 2, \ldots, n\}$. We often describe σ using the following notation:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$$

Example 2.22. *In S_3,*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

is the permutation on $\{1, 2, 3\}$ which sends 1 to 3, 2 to itself, and 3 to 1, i.e. $\sigma(1) = 3, \sigma(2) = 2, \sigma(3) = 1$.
For $\alpha, \beta \in S_3$ given by:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

we have:

$$\alpha\beta = \alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

(since, for example, $\alpha \circ \beta : 1 \overset{\beta}{\mapsto} 2 \overset{\alpha}{\mapsto} 3$*.).*

We also have:

$$\beta\alpha = \beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Since $\alpha\beta \neq \beta\alpha$*, the group* S_3 *is non-abelian.*

In general, for $n > 2$*, the group* S_n *is non-abelian (* **Exercise:** *Why?).*

For the same $\alpha \in S_3$ *defined above, we have:*

$$\alpha^2 = \alpha \circ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

and:

$$\alpha^3 = \alpha \cdot \alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$$

Hence, the order of α *is* 3*.*

Dihedral Group

Consider the subset $\mathcal{T}$ of transformations of $\mathbb{R}^2$, consisting of all rotations by fixed angles about the origin, and all reflections over lines through the origin.

Consider a regular polygon P with n sides in $\mathbb{R}^2$, centered at the origin. Identify the polygon with its n vertices, which form a subset $P = \{x_1, x_2, \ldots, x_n\}$ of $\mathbb{R}^2$. If $\tau(P) = P$ for some $\tau \in \mathcal{T}$, we say that P is **symmetric** with respect to τ.

Intuitively, it is clear that P is symmetric with respect to n rotations $\{r_0, r_1, \ldots, r_{n-1}\}$, and n reflections $\{s_1, s_2, \ldots, s_n\}$ in $\mathcal{T}$.

By Jim.belk - Own work, Public Domain, Link

Theorem 2.23. *The set* $D_n := \{r_0, r_1, \ldots, r_{n-1}, s_1, s_2, \ldots, s_n\}$ *is a group, with respect to the group operation defined by* $\tau * \gamma = \tau \circ \gamma$ *(composition of transformations).*

Terminology:
D_n is called a **dihedral group** .

More on S_n

Consider the following element in S_6:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 6 & 1 & 2 \end{pmatrix}$$

We may describe the action of $\sigma : \{1, 2, \ldots, 6\} \longrightarrow \{1, 2, \ldots, 6\}$ using the notation:

$$\sigma = (15)(246),$$

where $(n_1 n_2 \cdots n_k)$ represents the permutation:

$$n_1 \mapsto n_2 \ldots n_i \mapsto n_{i+1} \cdots \mapsto n_k \mapsto n_1$$

Viewing permutations as bijective maps, the "multiplication" $(15)(246)$ is by definition the composition $(15) \circ (246)$.

We call $(n_1 n_2 \cdots n_k)$ a k**-cycle** . Note that 3 is missing from $(15)(246)$. This corresponds to the fact that 3 is fixed by σ.

Claim 2.24. *Every non-identity permutation in S_n is either a cycle or a product of disjoint cycles.*

Proof. Discussed in class. □

Exercise 2.25. *Disjoint cycles commute with each other.*

A 2-cycle is often called a **transposition** , for it switches two elements with each other.

Claim 2.26. *Each element of S_n is a product of (not necessarily disjoint) transpositions.*

Sketch of proof:

Show that each permutation not equal to the identity is a product of cycles, and that each cycle is a product of transpositions:

$$(a_1 a_2 \ldots a_k) = (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_3)(a_1 a_2)$$

Example 2.27.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 6 & 1 & 2 \end{pmatrix} = steps1steps(15)(246)$$

$$steps1steps = (15)(26)(24)$$

$$steps1steps = (15)(46)(26)$$

Note that a given element σ of S_n may be expressed as a product of transpositions in different ways, but:

Claim 2.28. *In every factorization of σ as a product of transpositions, the number of factors is either always even or always odd.*

Proof. **Exercise.** One approach: Show that there is a unique $n \times n$ matrix, with either 0 or 1 as its coefficients, which sends each standard basis vector $\vec{e}_i$ in $\mathbb{R}^n$ to $\vec{e}_{\sigma(i)}$. Then, use the fact that the determinant of the matrix corresponding to a transposition is -1, and that the determinant function of matrices is multiplicative. □

Exercise 2.29. *1.* **WeBWork**

2. **WeBWork**

3. **WeBWork**

4. **WeBWork**

Math 2070 Week 3

Topics: Subgroups, Left Cosets, Index

Subgroups

Definition 3.30. *Let G be a group. A subset H of G is a* **subgroup** *of G if it satisfies the following properties:*

- **Closure** *If $a, b \in H$, then $ab \in H$.*
- **Identity** *The identity element of G lies in H.*
- **Inverses** *If $a \in H$, then $a^{-1} \in H$.*

In particular, a subgroup H is a group with respect to the group operation on G, and the identity element of H is the identity element of G.

Example 3.31.

- *For any $n \in \mathbb{Z}$, $n\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$.*
- *$\mathbb{Q}\backslash\{0\}$ is a subgroup of $(\mathbb{R}\backslash\{0\}, \cdot)$.*
- *$\mathrm{SL}(2, \mathbb{R})$ is a subgroup of $\mathrm{GL}(2, \mathbb{R})$.*
- *The set of all rotations (including the trivial rotation) in a dihedral group D_n is a subgroup of D_n.*
- *Let $n \in \mathbb{N}$, $n \geq 2$. We say that $\sigma \in S_n$ is an* **even permutation** *if it is equal to the product of an even number of transpositions. The subset A_n of S_n consisting of even permutations is a subgroup of S_n. A_n is called an* **alternating group** *.*

Claim 3.32. *A subset H of a group G is a subgroup of G if and only if H is nonempty and, for all $x, y \in H$, we have $xy^{-1} \in H$.*

Proof. Suppose $H \subseteq G$ is a subgroup. Then, H is nonempty since $e_G \in H$. For all $x, y \in H$, we have $y^{-1} \in H$; hence, $xy^{-1} \in H$.

Conversely, suppose H is a nonempty subset of G, and $xy^{-1} \in H$ for all $x, y \in H$.

- **Identity** Let e be the identity element of G. Since H is nonempty, it contains at least one element h. Since $e = h \cdot h^{-1}$, and by hypothesis $h \cdot h^{-1} \in H$, the set H contains e.
- **Inverses** Since $e \in H$, for all $a \in H$ we have $a^{-1} = e \cdot a^{-1} \in H$.
- **Closure** For all $a, b \in H$, we know that $b^{-1} \in H$. Hence, $ab = a \cdot (b^{-1})^{-1} \in H$.

Hence, H is a subgroup of G.

□

Claim 3.33. *The intersection of two subgroups of a group G is a subgroup of G.*

Proof. Exercise. □

Theorem 3.34. *Every subgroup of $(\mathbb{Z}, +)$ is cyclic.*

Proof. Let H be a subgroup of $G = (\mathbb{Z}, +)$. If $H = \{0\}$, then it is clearly cyclic.

Suppose $|H| > 1$. Consider the subset:

$$S = \{h \in H \,:\, h > 0\} \subseteq H$$

Since a subgroup is closed under inverse, and the inverse of any $z \in \mathbb{Z}$ with respect to $+$ is $-z$, the subgroup H must contain at least one positive element. Hence, S is a non-empty subset of $\mathbb{Z}$ bounded from below.

It then follows from the Least Integer Axiom that exists a minimum element h_0 in S. That is $h_0 \leq h$ for any $h \in S$.

Exercise. Show that $H = \langle h_0 \rangle$.

(**Hint** : The Division Theorem for Integers could be useful here.) □

Exercise 3.35. *Every subgroup of a cyclic group is cyclic.*

Lagrange's Theorem

Let G be a group, H a subgroup of G. We are interested in knowing how large H is relative to G.

We define a relation $\equiv$ on G as follows:

$$a \equiv b \text{ if } b = ah \text{ for some } h \in H,$$

or equivalently:

$$a \equiv b \text{ if } a^{-1}b \in H.$$

Exercise: $\equiv$ is an **equivalence relation** .

We may therefore partition G into disjoint equivalence classes with respect to $\equiv$. We call these equivalence classes the **left cosets** of H.

Each left coset of H has the form $aH = \{ah \,|\, h \in H\}$.

We could likewise define right cosets. These sets are of the form Hb, $b \in G$. In general, the number of left cosets and right cosets, if finite, are equal to each other

Example 3.36. *Let $G = (\mathbb{Z}, +)$. Let:*

$$H = 3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$$

The set H is a subgroup of G. The left cosets of H in G are as follows:

$$3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z},$$

where $i + 3\mathbb{Z} := \{i + 3k : k \in \mathbb{Z}\}$.

In general, for $n \in \mathbb{Z}$, the left cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ are:

$$i + n\mathbb{Z}, \quad i = 0, 1, 2, \ldots, n - 1.$$

Definition 3.37. *The number of left cosets of a subgroup H of G is called the* **index** *of H in G. It is denoted by:*

$$[G : H]$$

Example 3.38. *Let $n \in \mathbb{N}$, $G = (\mathbb{Z}, +)$, $H = (n\mathbb{Z}, +)$. Then,*

$$[G : H] = n.$$

Example 3.39. *Let $G = \mathrm{GL}(n, \mathbb{R})$. Let:*

$$H = \mathrm{GL}^+(n, \mathbb{R}) := \{h \in G : \det h > 0\}.$$

(**Exercise:** *H is a subgroup of G.)*

Let:

$$s = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \in G$$

Note that $\det s = \det s^{-1} = -1$.

For any $g \in G$, either $\det g > 0$ or $\det g < 0$. If $\det g > 0$, then $g \in H$. If $\det g < 0$, we write:

$$g = (ss^{-1})g = s(s^{-1}g).$$

Since $\det s^{-1}g = (\det s^{-1})(\det g) > 0$, we have $s^{-1}g \in H$. So, $G = H \sqcup sH$, and $[G : H] = 2$. Notice that both G and H are infinite groups, but the index of H in G is finite.

Example 3.40. *Let $G = \mathrm{GL}(n, \mathbb{R})$, $H = \mathrm{SL}(n, \mathbb{R})$. For each $x \in \mathbb{R}^\times$, let:*

$$s_x = \begin{pmatrix} x & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \in G$$

Note that $\det s_x = x$.

For each $g \in G$, we have:

$$g = s_{\det g}(s_{\det g}^{-1} g) \in s_{\det g} H$$

Moreover, for distinct $x, y \in \mathbb{R}^\times$, we have:

$$\det(s_x^{-1} s_y) = y/x \neq 1.$$

This implies that $s_x^{-1} s_y \notin H$, hence $s_y H$ and $s_x H$ are disjoint cosets. We have therefore:

$$G = \bigsqcup_{x \in \mathbb{R}^\times} s_x H.$$

The index $[G : H]$ in this case is infinite.

Theorem 3.41. *(* **Lagrange's Theorem** *) Let G be a finite group. Let H be subgroup of G, then $|H|$ divides $|G|$. More precisely, $|G| = [G : H] \cdot |H|$.*

We already know that the left cosets of H partition G. That is:

$$G = a_1H \sqcup a_2H \sqcup \ldots \sqcup a_{[G:H]}H,$$

where $a_iH \cap a_jH = \emptyset$ if $i \neq j$. Hence, $|G| = \sum_{i=1}^{[G:H]} |a_iH|$.

The theorem follows if we show that the size of each left coset of H is equal to $|H|$.

For each left coset S of H, pick an element $a \in S$, and define a map $\psi : H \longrightarrow S$ as follows:

$$\psi(h) = ah.$$

We want to show that ψ is bijective.

For any $s \in S$, by definition of a left coset (as an equivalence class) we have $s = ah$ for some $h \in H$. Hence, ψ is surjective. If $\psi(h') = ah' = ah = \psi(h)$ for some $h', h \in H$, then $h' = a^{-1}ah' = a^{-1}ah = h$. Hence, ψ is one-to-one.

So we have a bijection between two finite sets. Hence, $|S| = |H|$.

Corollary 3.42. *Let G be a finite group. The order of every element of G divides the order of G.*

Since G is finite, any element of $g \in G$ has finite order $\operatorname{ord} g$. Since the order of the subgroup:

$$H = \langle g \rangle = \{e, g, g^2, \ldots, g^{(\operatorname{ord} g)-1}\}$$

is equal to $\operatorname{ord} g$, it follows from Lagrange's Theorem that $\operatorname{ord} g = |H|$ divides $|G|$.

Corollary 3.43. *If the order of a group G is prime, then G is a cyclic group.*

courseMath 2070 week4 topicGroups

Math 2070 Week 4

Topics: Generators, Group Homomorphisms

Theorem 4.44 (Lagrange's Theorem)**.** *Let G be a finite group. Let H be subgroup of G, then $|H|$ divides $|G|$. More precisely, $|G| = [G : H] \cdot |H|$.*

Proof. We already know that the left cosets of H partition G. That is:

$$G = a_1H \sqcup a_2H \sqcup \ldots \sqcup a_{[G:H]}H,$$

where $a_iH \cap a_jH = \emptyset$ if $i \neq j$. Hence, $|G| = \sum_{i=1}^{[G:H]} |a_iH|$.

The theorem follows if we show that the size of each left coset of H is equal to $|H|$.

For each left coset S of H, pick an element $a \in S$, and define a map $\psi : H \longrightarrow S$ as follows:

$$\psi(h) = ah.$$

We want to show that ψ is bijective.

For any $s \in S$, by definition of a left coset (as an equivalence class) we have $s = ah$ for some $h \in H$. Hence, ψ is surjective.

If $\psi(h') = ah' = ah = \psi(h)$ for some $h', h \in H$, then $h' = a^{-1}ah' = a^{-1}ah = h$. Hence, ψ is one-to-one.

So we have a bijection between two finite sets. Hence, $|S| = |H|$.

□

Corollary 4.45. *Let G be a finite group. The order of every element of G divides the order of G.*

Since G is finite, any element of $g \in G$ has finite order $\operatorname{ord} g$. Since the order of the subgroup:

$$H = \langle g \rangle = \{e, g, g^2, \ldots, g^{(\operatorname{ord} g)-1}\}$$

is equal to $\operatorname{ord} g$, it follows from Lagrange's Theorem that $\operatorname{ord} g = |H|$ divides $|G|$.

Corollary 4.46. *If the order of a group G is prime, then G is a cyclic group.*

Corollary 4.47. *If a group G is finite, then for all $g \in G$ we have:*

$$g^{|G|} = e.$$

Corollary 4.48. *Let G be a finite group. Then a nonempty subset H of G is a subgroup of G if and only if it is closed under the group operation of G (i.e. $ab \in H$ for all $a, b \in H$).*

Proof. It is easy to see that if H is a subgroup, then it is closed under the group operation. The other direction is left as an **Exercise** . □

Example 4.49. *Let n be an integer greater than 1. The group A_n of even permutations on a set of n elements (see **??**) has order $\frac{n!}{2}$.*

Proof. View A_n as a subgroup of S_n, which has order $n!$.
Exercise : Show that $S_n = A_n \sqcup (12)A_n$.
Hence, we have $[S_n : A_n] = 2$.
It now follows from Lagrange's Theorem (**??**) that:

$$|A_n| = \frac{|S_n|}{[S_n : A_n]} = \frac{n!}{2}.$$

□

Generators

Let G be a group, X a nonempty subset of G. The subset of G consisting of elements of the form:

$$g_1^{m_1} g_2^{m_2} \cdots g_n^{m_n}, \quad \text{where} \quad n \in \mathbb{N}, g_i \in X, m_i \in \mathbb{Z},$$

is a subgroup of G. We say that it is the subgroup of G **generated** by X. If $X = \{x_1, x_2, \ldots, x_l\}$, $l \in \mathbb{N}$. We often write:

$$\langle x_1, x_2, \ldots, x_l \rangle$$

to denote the subgroup generated by X.

Example 4.50. *In D_n, $\{r_0, r_1, \ldots, r_{n-1}\} = \langle r_1 \rangle$.*

If there exists a finite number of elements $x_1, x_2, \ldots, x_l \in G$ such that $G = \langle x_1, x_2, \ldots, x_l \rangle$, we say that G is **finitely generated** .

For example, every cyclic group is finitely generated, for it is generated by one element.

Every finite group is finitely generated, since we may take the finite generating set X to be G itself.

Example 4.51. *Consider $G = D_3$, and its subgroup $H = \{r_0, r_1, r_2\}$ consisting of its rotations. (We use the convention that r_k is the anticlockwise rotation by an angle of $2\pi k/3$).*

By Lagrange's Theorem, the index of H in G is $[G : H] = |G| / |H| = 2$. This implies that $G = H \sqcup gH$ for some $g \in G$. Since $gH = H$ if $g \in H$, we may conclude that $g \notin H$. So, g is a reflection.

Conversely, for any reflection $s \in D_3$, the left coset sH is disjoint from H. We have therefore $G = H \sqcup s_1 H = H \sqcup s_2 H = H \sqcup s_3 H$, which implies that $s_1 H = s_2 H = s_3 H$.

In particular, for a fixed $s = s_i$, any element in G is either a rotation or equal to sr_i for some rotation r_i. Since H is a cyclic group, generated by the rotation r_1, we have $D_3 = \langle r_1, s \rangle$, where s is any reflection in D_3.

Exercise 4.52.

1. **WeBWork**
2. **WeBWork**
3. **WeBWork**
4. **WeBWork**
5. **WeBWork**
6. **WeBWork**
7. **WeBWork**
8. **WeBWork**
9. **WeBWork**
10. **WeBWork**
11. **WeBWork**
12. **WeBWork**

Group Homomorphisms

Definition 4.53. *Let $G = (G, *)$, $G' = (G', *')$ be groups. A* **group homomorphism** *ϕ from G to G' is a map $\phi : G \longrightarrow G'$ which satisfies:*

$$\phi(a * b) = \phi(a) *' \phi(b),$$

for all $a, b \in G$.

Claim 4.54. *If $\phi : G \longrightarrow G'$ is a group homomorphism, then:*

1. $\phi(e_G) = e_{G'}$.
2. $\phi(g^{-1}) = \phi(g)^{-1}$, *for all* $g \in G$.
3. $\phi(g^n) = \phi(g)^n$, *for all* $g \in G$, $n \in \mathbb{Z}$.

Proof. We prove the first claim, and leave the rest as an exercise. Since e_G is the identity element of G, we have $e_G * e_G = e_G$. On the other hand, since ϕ is a group homomorphism, we have:

$$\phi(e_G) = \phi(e_G * e_G) = \phi(e_G) *' \phi(e_G).$$

Since G' is a group, $\phi(e_G)^{-1}$ exists in G', hence:

$$\phi(e_G)^{-1} *' \phi(e_G) = \phi(e_G)^{-1} *' (\phi(e_G) *' \phi(e_G))$$

The left-hand side is equal to $e_{G'}$, while by the associativity of $*'$ the right-hand side is equal to $\phi(e_G)$.

□

Let $\phi : G \longrightarrow G'$ be a homomorphism of groups. The image of ϕ is defined as:

$$\operatorname{im} \phi := \phi(G) := \{\phi(g) : g \in G\} \subseteq G'$$

The kernel of ϕ is defined as:

$$\ker \phi = \{g \in G : \phi(g) = e_{G'}\} \subseteq G.$$

Claim 4.55. *The image of ϕ is a subgroup of G'. The kernel of ϕ is a subgroup of G.*

Claim 4.56. *A group homomorphism $\phi : G \longrightarrow G'$ is one-to-one if and only if* $\ker \phi = \{e_G\}$.

Example 4.57 (Examples of Group Homomorphisms)**.**

- $\phi : S_n \longrightarrow (\{\pm 1\}, \cdot)$,

$$\phi(\sigma) = \begin{cases} 1, & \sigma \text{ is an even permutation.} \\ -1, & \sigma \text{ is an odd permutation.} \end{cases}$$

  $\ker \phi = A_n$.

- $\det : \mathrm{GL}(n, \mathbb{R}) \longrightarrow (\mathbb{R}^\times, \cdot)$

  $\ker \det = \mathrm{SL}(n, \mathbb{R})$.

- *Let G be the (additive) group of all real-valued continuous functions on $[0, 1]$.*

$$\phi : G \longrightarrow (\mathbb{R}, +)$$
$$\phi(f) = \int_0^1 f(x)\, dx.$$

- $\phi : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^\times, \cdot)$.

$$\phi(x) = e^x.$$

Definition 4.58. *Let G, G' be groups. A map $\phi : G \longrightarrow G'$ is a group* **isomorphism** *if it is a bijective group homomorphism.*

Note that if a homomorphism ϕ is bijective, then $\phi^{-1} : G' \longrightarrow G$ is also a homomorphism, and consequently, ϕ^{-1} is an isomorphism. If there exists an isomorphism between two groups G and G', we say that the groups G and G' are **isomorphic** .

Definition 4.59. *Fix an integer $n > 0$.*

For any $k \in \mathbb{Z}$, let $\overline{k}$ denote the remainder of the division of k by n.

Let $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$. We define a binary operation $+_{\mathbb{Z}_n}$ on $\mathbb{Z}_n$ as follows:

$$k +_{\mathbb{Z}_n} l = \overline{k + l}.$$

Exercise 4.60. *$\mathbb{Z}_n = (\mathbb{Z}_n, +_{\mathbb{Z}_n})$ is a group, with identity element 0, and $j^{-1} = n - j$ for any $j \in \mathbb{Z}_n$.*

Example 4.61. *Let $n > 2$. Let $H = \{r_0, r_1, r_2, \ldots, r_{n-1}\}$ be the subgroup of D_n consisting of all rotations, where r_1 denotes the anticlockwise rotation by the angle $2\pi/n$, and $r_k = r_1^k$. Then, H is isomorphic to $\mathbb{Z}_n = (\mathbb{Z}_n, +_{\mathbb{Z}_n})$.*

Proof. Define $\phi : H \longrightarrow \mathbb{Z}_n$ as follows:

$$\phi(r_k) = k, \quad k \in \{0, 1, 2, \ldots, n-1\}.$$

For any $k \in \mathbb{Z}$, let $\overline{k} \in \{0, 1, 2, \ldots, n-1\}$ denote the remainder of the division of k by n. By the Division Theorem for Integers, we have:

$$k = nq + \overline{k}$$

for some integer $q \in \mathbb{Z}$.

It now follows from $\operatorname{ord} r_1 = n$ that, for all $r_i, r_j \in H$, we have:

$$\begin{aligned} r_i r_j &= r_1^i r_1^j = r_1^{i+j} \\ steps2steps&= r_1^{nq+\overline{i+j}} \\ steps2steps&= (r_1^n)^q \, r_1^{\overline{i+j}} \\ steps2steps&= r_{\overline{i+j}}. \end{aligned}$$

Hence,

$$\begin{aligned} \phi(r_i r_j) &= \phi(r_{\overline{i+j}}) \\ steps3steps&= \overline{i+j} \\ steps3steps&= i +_{\mathbb{Z}_n} j \\ steps3steps&= \phi(r_i) +_{\mathbb{Z}_n} \phi(r_j). \end{aligned}$$

This shows that ϕ is a homomorphism. It is clear that ϕ is surjective, which then implies that ϕ is one-to-one, for the two groups have the same size. Hence, ϕ is a bijective homomorphism, i.e. an isomorphism.

□

courseMath 2070 week5 topicGroup Homomorphisms topicRings

Math 2070 Week 5

Topics: Group Homomorphisms, Rings

Claim 5.62. *Any cyclic group of finite order n is isomorphic to $\mathbb{Z}_n$.*

Proof. Sketch of Proof:

By definition, a cyclic group G is equal to $\langle g \rangle$ for some $g \in G$. Moreover, $\operatorname{ord} g = \operatorname{ord} G$.

Define a map $\phi : G \longrightarrow \mathbb{Z}_n$ as follows:

$$\phi(g^k) = k, \quad k \in \{0, 1, 2, \ldots, n-1\}.$$

Show that ϕ is a group isomorphism.

(For reference, see the discussion of **??**.) □

Corollary 5.63. *If G and G' are two finite cyclic groups of the same order, then G is isomorphic to G'.*

Exercise 5.64. *An infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$.*

Exercise 5.65. *Let G be a cyclic group, then any group which is isomorphic to G is also cyclic.*

Product Group

Product Group

Let $(A, *_A), (B, *_B)$ be groups. The direct product:

$$A \times B := \{(a, b) \mid a \in A, b \in B\}$$

has a natural group structure where the group operation $*$ is defined as follows:

$$(a, b) * (a', b') = (a *_A a', b *_B b'), \quad (a, b), (a', b') \in A \times B.$$

The identity element of $A \times B$ is $e = (e_A, e_B)$, where e_A, e_B are the identity elements of A and B, respectively.

For any $(a, b) \in A \times B$, we have $(a, b)^{-1} = (a^{-1}, b^{-1})$, where a^{-1}, b^{-1} are the inverses of a, b in the groups A, B, respectively.

For any collection of groups $A_1, A_2, \ldots, A_n$, we may similarly define a group operation $*$ on:

$$A_1 \times A_2 \times \cdots \times A_n := \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i, i = 1, 2, \ldots n\}.$$

That is:

$$(a_1, a_2, \ldots, a_n) * (a_1', a_2', \ldots, a_n') = (a_1 *_{A_1} a_1', a_2 *_{A_2} a_2', \ldots, a_n *_{A_n} a_n')$$

The identity element of $A_1 \times A_2 \times \cdots \times A_n$ is:

$$e = (e_{A_1}, e_{A_2}, \ldots, e_{A_n}).$$

For any $(a_1, a_2, \ldots, a_n) \in A_1 \times A_2 \times \cdots \times A_n$, its inverse is:

$$(a_1, a_2, \ldots, a_n)^{-1} = (a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1}).$$

Exercise 5.66. *$\mathbb{Z}_6$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3$.*

Proof. **Hint:**
Show that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is a cyclic group generated by $(1, 1)$. □

Example 5.67. *The cyclic group $\mathbb{Z}_4$ is not isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.*

Proof. Each element of $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ is of order at most 2. Since $|G| = 4$, G cannot be generated by a single element. Hence, G is not cyclic, so it cannot be isomorphic to the cyclic group $\mathbb{Z}_4$.

□

Exercise 5.68. *Let G be an abelian group, then any group which is isomorphic to G is abelian.*

Example 5.69. *The group D_6 has 12 elements. We have seen that $D_6 = \langle r_1, s \rangle$, where r_1 is a rotation of order 6, and s is a reflection, which has order 2. So, it is reasonable to ask if D_6 is isomorphic to $\mathbb{Z}_6 \times \mathbb{Z}_2$. The answer is no. For $\mathbb{Z}_6 \times \mathbb{Z}_2$ is abelian, but D_6 is not.*

Claim 5.70. *The dihedral group D_3 is isomorphic to the symmetric group S_3.*

Proof. We have seen that $D_3 = \langle r, s\rangle$, where $r = r_1$ and s is any fixed reflection, with:

$$\operatorname{ord} r = 3, \quad \operatorname{ord} s = 2, \quad srs = r^{-1}.$$

In particular , any element in D_3 may be expressed as $r^i s^j$, with $i \in \{0, 1, 2\}$, $j \in \{0, 1\}$.

We have also seen that $S_3 = \langle a, b\rangle$, where:

$$a = (123), \quad b = (12), \quad \operatorname{ord} a = 3, \quad \operatorname{ord} b = 2, \quad bab = a^{-1}.$$

Hence, any element in S_3 may be expressed as $a^i b^j$, with $i \in \{0, 1, 2\}$, $j \in \{0, 1\}$.

Define map $\phi : D_3 \longrightarrow S_3$ as follows:

$$\phi(r^i s^j) = a^i b^j, \quad i, j \in \mathbb{Z}$$

We first show that ϕ is well-defined: That is, whenever $r^i s^j = r^{i'} s^{j'}$, we want to show that:

$$\phi(r^i s^j) = \phi(r^{i'} s^{j'}).$$

The condition $r^i s^j = r^{i'} s^{j'}$ implies that:

$$r^{i-i'} = s^{j'-j}$$

This holds only if $r^{i-i'} = s^{j'-j} = e$, since no rotation is a reflection.

Since $\operatorname{ord} r = 3$ and $\operatorname{ord} s = 2$, we have:

$$3|(i - i'), \quad 2|(j' - j),$$

by Theorem 2.14.

Hence,

$$\begin{aligned}
\phi(r^i s^j)\phi(r^{i'} s^{j'})^{-1} = (a^i b^j)(a^{i'} b^{j'})^{-1} & \\
steps4steps= a^i b^j b^{-j'} a^{-i'} & \\
steps4steps= a^i b^{j-j'} a^{-i'} & \\
steps4steps= a^{i-i'} & \qquad steps4steps \text{ since } \operatorname{ord} b = 2. \\
steps4steps= e & \qquad steps4steps \text{ since } \operatorname{ord} a = 3.
\end{aligned}$$

This implies that $\phi(r^i s^j) = \phi(r^{i'} s^{j'})$. We conclude that ϕ is well-defined.

We now show that ϕ is a group homomorphism:

Given $\mu, \mu' \in \{0, 1, 2\}$, $\nu, \nu' \in \{0, 1\}$, we have:

$$\phi(r^\mu s^\nu \cdot r^{\mu'} s^{\nu'}) = \begin{cases} \phi(r^{\mu+\mu'} s^{\nu'}), & \text{if } \nu = 0; \\ \phi(r^{\mu-\mu'} s^{\nu+\nu'}), & \text{if } \nu = 1. \end{cases}$$

$$= \begin{cases} a^{\mu+\mu'}b^{\nu'}, & \text{if } \nu = 0; \\ a^{\mu-\mu'}b^{\nu+\nu'} = a^{\mu}b^{\nu}a^{\mu'}b^{\nu'}, & \text{if } \nu = 1. \end{cases}$$

$$= \phi(r^{\mu}s^{\nu})\phi(r^{\mu'}s^{\nu'}).$$

This shows that ϕ is a group homomorphism.

To show that ϕ is a group isomorphism, it remains to show that it is surjective and one-to-one.

It is clear that ϕ is surjective. We leave it as an exercise to show that ϕ is one-to-one.

□

Example 5.71. *The group:*

$$G = \left\{ g \in \mathrm{GL}(2,\mathbb{R}) \;\middle|\; g = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \text{ for some } \theta \in \mathbb{R} \right\}$$

is isomorphic to

$$G' = \{z \in \mathbb{C} : |z| = 1\}.$$

Here, the group operation on G is matrix multiplication, and the group operation on G' is the multiplication of complex numbers.

Each element in G' is equal to $e^{i\theta}$ for some $\theta \in \mathbb{R}$. Define a map $\phi : G \longrightarrow G'$ as follows:

$$\phi\left(\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\right) = e^{i\theta}.$$

Exercise: *Show that ϕ is a well-defined map. Then, show that it is a bijective group homomorphism.*

Rings

Some Results in Elementary Number Theory

Theorem 5.72 (Division Theorem)**.** *Let $a, b \in \mathbb{Z}$, $a \neq 0$, then there exist unique q (called the quotient), and r (* **remainder** *) in $\mathbb{Z}$, satisfying $0 \leq r < |a|$, such that $b = aq + r$.*

Proof. We will prove the case $a > 0$, $b \geq 0$. The other cases are left as exercises.

Fix $a > 0$. First, we prove the existence of the quotient q and remainder r for any $b \geq 0$, using mathematical induction.

The base step corresponds to the case $0 \leq b < a$. In this case, if we let $q = 0$ and $r = b$, then indeed $b = qa + r$, where $0 \leq r = b < a$. Hence, q and r exist.

The inductive step of the proof of the existence of q and r is as follows: Suppose the existence of the quotient and remainder holds for all non-negative $b' < b$, we want to show that it must also hold for b.

First, we may assume that $b \geq a$, since the case $b < a$ has already been proved. Let $b' = b - a$. Then, $0 \leq b' < b$, so by the inductive hypothesis we have $b' = q'a + r'$ for some $q', r' \in \mathbb{Z}$ such that $0 \leq r' < a$.

This implies that $b = b' + a = (q' + 1)a + r'$.

So, if we let $q = q' + 1$ and $r = r'$, then $b = qa + r$, where $0 \leq r < a$. This establishes the existence of q, r for b. Hence, by mathematical induction, the existence of q, r holds for all $b \geq 0$.

Now we prove the uniqueness of q and r. Suppose $b = qa + r = q'a + r'$, where $q, q', r, r' \in \mathbb{Z}$, with $0 \leq r, r' < a$.

Then, $qa + r = q'a + r'$ implies that $r - r' = (q' - q)a$. Since $0 \leq r, r' < a$, we have:

$$a > |r - r'| = |q' - q|\, a.$$

Since $q' - q$ is an integer, the above inequality implies that $q' - q = 0$, i.e. $q' = q$, which then also implies that $r' = r$. We have therefore established the uniqueness of q and r.

The proof of the theorem, for the case $a > 0, b \geq 0$, is now complete.

□

Definition 5.73. *The* **Greatest Common Divisor** *$gcd(a, b)$ of $a, b \in \mathbb{Z}$ is the largest positive integer d which divides both a and b (Notation: $d|a$ and $d|b$).*

Note.

If $a \neq 0$, then $gcd(a, 0) = |a|$. $gcd(0, 0)$ is undefined.

Lemma 5.74. *If $b = aq + r$ $(a, b, q, r \in \mathbb{Z})$, then $gcd(b, a) = gcd(a, r)$.*

Proof. If $d|a$ and $d|b$, then $d|r = b - aq$. Conversely, if $d|a$ and $d|r$, then $d|a$ and $d|b = qa + r$. So, the set of common divisors of a, b is the same as the set of the common divisors of a, r. If two finite sets of integers are the same, then their largest elements are clearly the same. In other words:

$$gcd(b, a) = gcd(a, r).$$

□

The Euclidean Algorithm

Suppose $|b| \geq |a|$. Let $b_0 = b$, $a_0 = a$. Write $b_0 = a_0 q_0 + r_0$, where $0 \leq r_0 < |a_0|$.

For $n > 0$, let $b_n = a_{n-1}$ and $a_n = r_{n-1}$, where r_n is the remainder of the division of b_n by a_n. That is,

$$b_n = a_n q_n + r_n, \quad 0 \leq r_n < |a_n|.$$

If $r_0 = 0$, then that means that $a|b$, and $gcd(a, b) = |a|$. Now, suppose $r_0 > 0$. Since r_n is a non-negative integer and $0 \leq r_n < r_{n-1}$, eventually, $r_n = 0$ for some $n \in \mathbb{N}$.

Claim 5.75. $gcd(b, a) = |a_n|$.

Proof. By the previous lemma,

$$\begin{aligned} gcd(b, a) &= gcd(b_0, a_0) \\ &\quad steps5steps= gcd(a_0, r_0) = gcd(b_1, a_1) \\ &\quad steps5steps= gcd(a_1, r_1) = gcd(b_2, a_2) \\ &\quad steps5steps= \dots \\ &\quad steps5steps= gcd(a_n, r_n) = gcd(a_n, 0) = |a_n|. \end{aligned}$$

□

Example 5.76. *Find* $gcd(285, 255)$.

$$\underbrace{285}_{b_0} = \underbrace{255}_{a_0}\ \underbrace{1}_{q_0} + \underbrace{30}_{r_0}$$

$$steps6steps\underbrace{255}_{b_1=a_0} steps6steps= \underbrace{30}_{a_1=r_0}\ \underbrace{8}_{q_1} + \underbrace{15}_{r_1}$$

$$steps6steps\underbrace{30}_{b_2} steps6steps= \underbrace{15}_{a_2}\ \underbrace{2}_{q_2} + \underbrace{0}_{r_2}$$

So, $gcd(285, 255) = r_1 = 15$.