Math 235

Cole Killian

October 7, 2019

Contents

1 Cyclic Subgroups **3**

2 Chapter 5 09-27 **3**

3 Math 235 Tutorial — 09-27 **5**
3.1 Groups & Subgroups 5

4 Lecture 09-30 **9**
4.1 Review Complex Numbers 9

5 10-02 **10**
5.1 Cosets and Lagrange's Theorem 12

6 Tutorial 5: Cyclic Groups - 10-04 **15**

7 Lecture 10-07 **19**

§1 Cyclic Subgroups

Note 1.1 (Generator Group Notation)**.**
Let $g \in (G, \circ)$. Notation: $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$
Let $g \in (G, +)$. Notation: $\langle g \rangle = \{ng : n \in \mathbb{Z}\}$

Example 1.2 (Generator Groups)

$5 \in \mathbb{Z}$.	$\langle 5 \rangle = \{\ldots, -10, -5, 0, 5, \ldots\}$
$2 \in \mathbb{Z}$.	$\langle 2 \rangle = \{\text{Even integers.}\}$
$5 \in \mathbb{Z}_{10}$.	$\langle 5 \rangle = \{0, 5\}$
$6 \in \mathbb{Z}_{10}$.	$\langle 6 \rangle = \{6, 2, 8, 4, 0\}$

Note: $\mathbb{Z}_{10} = \langle 1 \rangle = \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle$

Theorem 1.3
Let G be a group. Let $x \in G$, then $\langle x \rangle$ is a subgroup of G. Also, $\langle x \rangle$ is the smallest subgroup containing x.

Definition 1.4. $\langle x \rangle$ is the cyclic subgroup generated by x. If $G = \langle x \rangle$, then G is a cyclic group and x is a generator of G.

Definition 1.5. Detecting wheter or not a subset is a subgroup.

1. The identity Element is in the subgroup.
2. Inverse of each element is inside.
3. If two elements are inside, their product is inside as well.

§2 Chapter 5 09-27

Definition 2.1. A permutation of set X is a bijection $f : X \to X$.

Example 2.2
$x = \{1, 2, 3, 4\} \to \{3, 1, 4, 3\}$

I'm not fast enough to write this

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 3 \end{bmatrix}$$

$$\text{General notation: } \begin{bmatrix} 1 & 2 \ldots\ldots\ldots\ldots n \\ f(1) & f(2) \ldots f(\ldots) \ldots f(n) \end{bmatrix}$$

Definition 2.3. The symmetric group of degree n (on n objects) is group S_N consisting of all permutations of $X = \{1, 2, \ldots n\}$

Theorem 2.4

S_n is a group whose binary operation is composition of functions.

Proof.

1. Composition of functions is associative.
2. Inverses exist because inverses of bijections are bijections. f^{-1} is inverse of f.

□

Example 2.5

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{bmatrix}$$

Note 2.6. S_n has $n!$ elements.

Example 2.7

Consider the following function.

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 4 & 5 & 2 & 6 \end{bmatrix}$$

Definition 2.8. A cycle is a permutation with property that there is a subset $\{a_1, a_2, \ldots, a_m\} \subset \{1, 2, \ldots, n\}$ such that $f(a_i) = a_{i+1}$ for $1 \leq i < m$, and $f(a_m) = a_1$, and $f(x) = x$ when $x \notin \{a_1, \ldots, a_m\}$.

Example 2.9

Consider the following function.

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 3 & 7 & 5 & 6 & 1 \end{bmatrix}$$

$1 \to 4 \to 7 \to 1$. $(1, 4, 7)$ are being cycled.
$(2, 3, 5, 6)$ are fixed.

Note 2.10. Use notation $(a_1, a_2, \ldots, a_m)$ for the cycle. All other elements are fixed.

Example 2.11

$(3\ 7\ 5\ 1) \in S_7$ contains the same information as:

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 7 & 4 & 1 & 6 & 5 \end{bmatrix}$$

But the former is easier to understand.

Note 2.12. $(a_1, a_2, \ldots, a_m)$ and $(b_1, b_2, \ldots, b_l)$ are disjoint if $a_i \neq b_j$ for i, j.

Example 2.13

(3 7 5 1) is disjoint from (64), but note that there are multiple ways of representing the same cycle.
For example. $(3\ 7\ 5\ 1) = (5\ 1\ 3\ 7) = (7\ 5\ 1\ 3)$

Theorem 2.14

Disjoint cycles commute.

$$(a_1\ \dots\ a_m)(b_1\ \dots\ b_l) = (b_1\ \dots\ b_l)(a_1\ \dots\ a_m)$$

if $c \notin \{a_1\ \dots\ a_m, b_1\ \dots\ b_l\}$

Theorem 2.15

Every permutation is a product of disjoint cycles.

Example 2.16

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 5 & 9 & 8 & 2 & 4 & 1 & 7 \end{bmatrix} = (3\ 5\ 8)(2\ 6)(7\ 4\ 9) \in S_9$$

More Practice:

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 8 & 2 & 1 & 5 & 3 & 6 & 10 & 9 & 4 \end{bmatrix} = (1\ 7\ 6\ 3\ 2\ 8\ 10\ 4)(5)(9) \in S_{10}$$

Practice in the other direction:

$$((1\ 3\ 5)(2\ 7\ 6\ 4))((1\ 2)(3\ 4)(5\ 6\ 7)) = (1\ 7)(2\ 3)(4\ 5)(6)$$

The (6) at the end is unnecessary because it is an identity element.

He just drew a pictorial circle on the board. I am just going to watch and absorb.

Theorem 2.17

Every permutation is a product of transpositions because:

> **Theorem 2.18**
> Every n-cycle is a product of $(n-1)$ transpositions.

Proof. $(a_1\ a_2\ \dots\ a_m) = (a_1\ a_m)(a_1\ a_{m-1})\dots(a_1\ a_3)(a_1\ a_2)$ □

§3 Math 235 Tutorial — 09-27

§3.1 Groups & Subgroups

Definition 3.1. A group $(G, \circ)$ is a set G together with an operation $\circ$ such that:

1. The elements are associative: $(a \circ b) \circ c = a \circ (b \circ c)$
2. There exists an identity element: $\exists e \in G$ such that $\forall g \in G$, $ge = eg = g$.
3. All elements contain an inverse within the group. $\forall g \in G \ \ \exists g^{-1}$ such that $g \circ g^{-1} = g^{-1}g = e$

Example 3.2

1. $(\mathbb{Z}, +)$. It is associative. Identity element is 0. $a^{-1} = -a$.
2. $(\mathbb{R} \setminus \{0\}, *)$. Is is associatve. Identity element is 1. All elements have an inverse (we removed 0 because 0 doesn't have an inverse).
3. $(\mathbb{Z}_n, +)$. It is associative. Identity element is 0. $a^{-1} = -a = n - a$.
4. $(\mathbb{Z}, *)$ is NOT a group because many integers do not have inverses that belong to the integers. $5^{-1} = \frac{1}{5} \notin \mathbb{Z}$
5. $(\mathbb{R}, *)$ is NOT a group because 0 does not have an inverse.

Note 3.3.

1. Multiplicative Notation: g^n means use the operation n times. $(G, \cdot)$
2. Additive Notation: ng means use the operation n times. $(G, +)$

Example 3.4

$$\begin{aligned} 11x + 2 &\equiv 16 \pmod{26} \\ 11x &\equiv 14 \pmod{26} \\ 11^{-1}11x &\equiv 11^{-1}14 \pmod{26} \\ x &\equiv 11^{-1}14 \pmod{26} \end{aligned}$$

If we were in $\mathbb{R}$, $(11)^{-1} = \frac{1}{11}$, but $\frac{1}{11} \notin \mathbb{Z}_{26}$ We need to find $(11)^{-1} \in \mathbb{Z}_{26}$. We know it exists because $\gcd(11, 26) = 1$

Euclidean Algorithm

$$\begin{aligned} 26 &= 2 * 11 + 4 \\ 11 &= 2 * 4 + 3 \\ 4 &= 1 * 3 + 1 \\ 3 &= 3 * 1 + 0 \end{aligned}$$

$$\begin{aligned} 1 &= 4 - 3 \\ &= 4 - (11 - 24) \\ &= 3 * 4 - 11 \\ &= 3(26 - 2 * 11) - 11 \\ &= 3 * 26 - 7 * 11 \end{aligned}$$

$\gcd(11, 26) = 1$ means there is a linear combination of 11 and 26 that equals 1. Taking the mod of both sides, mod of 26 is 0 and mod of 1 is 1 so it means that there is a multiple of 11 equal to 1 in mod 26. This means that it has an inverse. It's inverse is $-7 = 26 - 7 = 19$.

Back to equation:

$$\begin{aligned} 11x &= 14 \\ 19 \cdot 11x &= 19 \cdot 14 \\ x &= 266 \\ x &= 6 \end{aligned}$$

Solution: $\{x \in \mathbb{Z} : 26 \cdot n + 6 \quad n \in \mathbb{Z}\}$

Example 3.5

When presented with a Cayley table, how can we tell whether or not we are looking at a group.

$$\begin{bmatrix} a & b & c & d \\ b & b & c & d \\ c & d & a & b \\ d & a & b & c \end{bmatrix}$$

We must check identity element, inverses, and associativity,.

1. Identity element is a. ✓
2. b doesn't have an inverse so this is not a group.
3. Whether or not associativity fails, this is not a group. In order to see associativity in a cayley table, it must by symmetric along the line $y = -x$.

Advice: When checking if two groups are the same with cayley tables, look at the inverses and see if they match perfectly.

Exercise 3.6. Let G be a group such that $g^2 = e \quad \forall g \in G$. Show that G is abelian. In other words, $\forall a, b \in G \quad ab = ba$.

Solution. Let $a, b \in G$. We want to show that $ab = ba$. Note: $e = a^2 = b^2 = (ab)^2 = (ba)^2$

$$\begin{aligned} ab &= a \cdot e \cdot b \\ ab &= a \cdot (ab)(ab) \cdot b \\ ab &= (aa)(ba)(bb) \\ ab &= e \cdot ba \cdot e \\ ab &= ba \end{aligned}$$

□

Advice: when proving that a group is abelian, play around with the identity matrix.

Definition 3.7. H is a subgroup of G if $H \subset G$ and H is a group with the inherited operation from G.

Example 3.8

$(\mathbb{Z}, +)$. Even integers are a subgroup of $\mathbb{Z}$ with the $+$ operation.
$(\mathbb{Z}, +)$. Odd integers are NOT a subgroup of $\mathbb{Z}$ with the $+$ operation because they don't have closure. $1 + 3 = 4$ and 4 is not an element of the odd integers.

Exercise 3.9. H_1 and H_2 are subgroups of G. Prove or disprove the following:

1. $H_1 \cap H_2$ is a subgroup of G.

   This is TRUE because it has the identity element, it has the inverses, and there is closure. There is no need to prove associativity because it is inherited from the binary operation.

   a) (Identity) $e \in H_1$ and $e \in H_2$ because H_1 and H_2 are subgroups.

b) (Inverses) $a \in H_1 \cap H_2$. In particular, $a \in H_1 \Rightarrow a^{-1} \in H_1$ and $a \in H_2 \Rightarrow a^{-1} \in H_2$. So $a^{-1} \in H_1 \cap H_2$. Note: This works because inverses are unique.

c) (Closure) $a, b \in H_1 \cap H_2$. $a, b \in H_1 \Rightarrow ab \in H_1$. Same for H_2. Therefore $ab \in H_1 \cap H_2$.

2. $H_1 \cup H_2$ is a subgroup of G?

   This is FALSE. Counter example: Let $A = \{n \in \mathbb{Z} : \text{n is a multiple of 2}\}$. Let $B = \{n \in \mathbb{Z} : \text{n is a multiple of 5}\}$.

   a) Identity ✓

   b) Inverses ✓

   c) Closure ✗

§4 Lecture 09-30

§4.1 Review Complex Numbers

Recall $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$

Come equipped with:

1. Addition: $(a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2)i$
2. Multiplication:

Complex numbers are associative and commutative under these operations.

There exists a complex conjugate.

> **Example 4.1**
> Complex conjugate of $(a + bi) = (a - bi)$

Note 4.2. $(a + bi)(a - bi) = a^2 + b^2$

$\mathbb{C}^*$ is a multiplicative group of complex numbers. All imaginary numbers have an inverse.

Rectangular and Polar coordinates.

Rectangular: x axis is real component, y axis is imaginary component.

Polar: radius is $\sqrt{a^2 + b^2}$

$\sqrt{a^2 + b^2} \cos\theta + \sqrt{a^2 + b^2} \sin\theta i = \sqrt{a^2 + b^2} cis\theta = re^{i\theta}$

We have that $(r_1 cis\theta_1)(r_2 cis\theta_2) = r_1 r_2 cis(\theta_1 + \theta_2)$.

r is the "scale factor"

$cis\theta$ is the "rotation"

When $r = 1$, we get the subgroup of unit length com plex numbers.

$cis\theta = 1 =$ identity. $(cis\theta)^{-1} = cis(\theta)$ $cis\theta_1(cis\theta_2) = cis(\theta_1 + \theta_2)$

The nth roots of unity are the solutions to $x^n = 1$ in $\mathbb{C}^*$.

They form a cyclic subgroup of order n. Form verticies of a polygon with n verticies.

Recall. Given a geometric object X, its group of isometries or symmetries Isom(X) is a group with multiplication as composition of functions.

Recall. An isometry $f : X \to X$ is a distance preserving function.

dist $(p, q) =$ dist $(f(p), f(q) \forall p, q \in X$.

Definition 4.3. Dinedral group - D_n is the group of isometries of regular n-gon.

Example 4.4

$|D_n| = 2n$. It has n reflections and n rotations (counting the identity).

Consider $n = 3$. This gives a regular triangle. There are three reflections and three rotations. In this example, reflections fix 1 vertex and midpoing of opposite edge. Rotations fix the center. Group of isometries is not abelian because if you do the same thing in different orders you get different results.

Lemma. The set of rotations forms a subgroup.

Remark. Each reflection is its own inverse. Remark. Product of two reflections is a rotation.Generally it is by twice the angle between the axes of reflection.

When n is even, reflections occur in two ways.

1. Fix two vertices
2. Fix two midpopints of opposite edges.

Interpretation for $n = 1$ and $n = 2$.

1. $n = 2$ represented by isometry of "bigon" (looks like a lemon).
2. $n = 1$ represented by isometry of a water droplet. $reflection, identity$.

These two groups are the only abelian dinedral groups.

Let X be a rigid object. Its group of rigit motions consists of isometries that can be "physically realised". They are all rotations.

Example 4.5

Let X be a "brick". Dimensions: $2 \times 3 \times 5$

1. Isom X consists of 16 elements. We have 3 π rotations, the identity, and reflections.
2. Rigid motions of X consists of 8 elements.

§5 10-02

Theorem 5.1

Any n-cycle is the product of $(n-1)$ transpositions.

Proof.

$$(a_1\ a_2\ \dots\ a_n) = (a_1\ a_n)(a_1\ a_{n-1})\dots(a_1\ a_3)(a_1\ a_2)$$

An alternative proof:

$$(a_1\ a_2\ \dots\ a_n) = (a_1\ a_2)(a_2\ a_3)\dots(a_{n-1}\ a_n)$$

□

Definition 5.2. An element $\sigma \in S_n$ is:

1. Even if σ is the product of an even number of transpositions
2. Odd if σ is the product of an odd number of transpositions.

Theorem 5.3

No $\sigma \in S_n$ is both even and odd.

Note 5.4. This means that any odd σ can only be expressed as a product of an odd number of transpositions.

Proof. Matricies over $\mathbb{R}$ have det positive or negative. Positive determinent maintains orientation. Negative determinent inverses orientation. An even element can be likened to a matrix with a positive determinent, while an odd element can be likened to a matrix with a negative determinent. □

Example 5.5

(2 3 5 7 9) is even because it is the product of four transpositions $(n-1)$.
(1 8 6 2) is odd because it is the product of three transpositions $(n-1)$.

Theorem 5.6

The set of even permutations of S_n is a subgroup. $A_n \subset S_n$, alternating group.

Proof. Identity Element: $() = (1\ 2)(1\ 2)$
Inverse: $() \in A_n$. Need to prove that $\sigma \in A_n \Rightarrow \sigma^{-1} \in A_n$.Indeed:

$$\sigma = (a_1\ b_1)(a_2\ b_2)\dots(a_k\ b_k)$$

$$\sigma = (a_k\ b_k)\dots(a_2\ b_2)(a_1\ b_1)$$

Closure: $\sigma, \phi \in A_n \Rightarrow \sigma \cdot \phi \in A_n$. Even number of permutations times even number of permutations gives an even number of permuatations which is in A_n.

Note 5.7. $|A_n| = \frac{1}{2}|S_n|$.

□

Understanding $A_4 \subset S_4$.
Listing elements in S_4. $S_4 =$

$$\{()\}$$

$$\{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

$$\{(1\ 2\ 3), (1\ 3\ 2)$$
$$(1\ 2\ 4), (1\ 4\ 2)$$
$$(1\ 3\ 4), (1\ 4\ 3)$$
$$(2\ 3\ 4), (2\ 4\ 3)\}$$

Note 5.8. S_4 "is" an isometry group of tetrahedron.
A_4 "is" the subgroup of its rigit motions.

§5.1 Cosets and Lagrange's Theorem

Let $H \subset G$ be a subgroup.
Let $g \in G$.
The left coset of H represented by g is $gH = \{gh : h \in H\}$.
The right coset of H represented by g is $Hg = \{hg : h \in H\}$.
Usually $gH \neq Hg$. (If equal just call them cosets if you'd like).

Example 5.9

Misleading but simple example.
$G = \mathbb{Z}_{12}, H = \langle 4 \rangle = \{0, 4, 8\}$.

$$0 + H = 4 + H = 8 + H = \{0, 4, 8\}$$
$$1 + H = 5 + H = 9 + H = \{1, 5, 9\}$$
$$2 + H = 6 + H = 10 + H = \{2, 6, 10\}$$
$$3 + H = 7 + H = 11 + H = \{3, 7, 11\}$$

Note 5.10. Notation can be confusing. gh means binary operation between g and h so when binary operation is $+$ it means $g + h$.

Cosets formed a partition of the group.
Review: What is a partition? Disjoint subsets that unionize to form a set.

Example 5.11

$$H = \{1, -1, i, -i\} \subset \mathbb{Q}_8$$
$$1 \cdot H = \{1 * 1, 1 * -1, 1 * i, 1 * -i\}$$
$$jH = \{j * 1, j * -1, j * i, j * -i\} = \{j, -j, -k, k\} = Hj$$

Note 5.12. These form a partition of the quaternions.

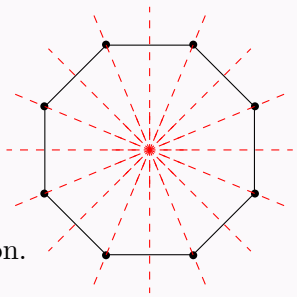
Example 5.13

$$K \subset \mathbb{Q}_8$$
$$K = \{1, -1\}$$

$$1K = \{1, -1\}$$
$$iK = \{i, -i\}$$
$$jK = \{j, -j\}$$
$$kK = \{k, -k\}$$

Note 5.14. For all of these, a left coset is a right coset.

Example 5.15



D_8. Symmetries of a regular octogon.

$$D_8 = \{r_i, \frac{i}{8}2\pi : 0 \leq i \leq 7\}$$

Subgroup (Same as the isometry of a rectangle living inside):

$$H = \{r_1, r_5, 0, \pi\}$$

Note 5.16. Product of rotation with rotation is a rotation. Product of a rotation with a reflection is a reflection. Product of a reflection with a reflection is a rotation.

$$0H = H$$
$$\frac{\pi}{8}H = \{r_2, r_6, \frac{\pi}{8}, \frac{5\pi}{8}\}$$
$$\frac{2\pi}{8}H = \{r_3, r_7, \frac{2\pi}{8}, \frac{6\pi}{8}\}$$
$$\frac{3\pi}{8}H = \{r_4, r_0, \frac{3\pi}{8}, \frac{7\pi}{8}\}$$
$$H\frac{\pi}{8} = \{r_0, r_4, \frac{\pi}{8}, \frac{5\pi}{8}\}$$

Note 5.17. Finding the product of a reflection and a rotation can be tricky. See how the composition affects a single point, and then identity a single rotation that affects the point in the same way.

Theorem 5.18

Lem 6.2. Let $g_1, g_2 \in G$ and $H \subset G$ be a group.
TFAE (similar for right cosets)

1. $g_1 H = g_2 H$
2. $Hg_1^{-1} = Hg_2^{-1}$. There is a bijection from a group to itself. Most obvious is identity bijection, but another one is every element to its inverse. In order to prove that statements 1 and 2 imply one another, use $\phi : G \to G, \phi(g) = g^{-1}.\phi$ is a bijection.$\phi(g_1 h) = h^{-1} g_1^{-1} \Rightarrow \phi(gH) \subset Hg^{-1}$.
3. $g_1 H \subset g_2 H$
4. $g_2 \in g_1 H$
5. $g_1^{-1} g \in H$. Reading this statement: "The difference between g_1 and g_2 lies in H.

Proof. $1 \Leftrightarrow 5$.
$\Rightarrow$. Suppose $g_1^{-1} g_2 \in H$, then $g_2^{-1} g_1 = (g_1^{-1} g_2)^{-1} \in H$.
Therefore $g_1 H \subset g_2 H$ because $g_1 h = (g_2 g_2^{-1}) g_1 h = g_2 (g_2^{-1} g_1) h \in g_2 H$. ($g_2 h'$ with $h' \in H$).
$\Leftarrow$. $(g_1 H = g_2 H) \Rightarrow (g_1 e \in g_2 H) \Leftrightarrow (g_1 \in g_2 H) \Rightarrow (g_1 = g_2 h$ for some $h \in H) \Rightarrow g_2^{-1} g_1 = h \in H$. □

Theorem 5.19

Lem 6.4. Let $H \subset G$ be a subgroup. The left (or right) cosets of H form a partition of G.

Proof. Look:

$$G = \bigcup_{g \in G} gH \text{ because } g = ge \in gH$$

If $g_1 H \cap g_2 H \neq \varnothing$, then $g_1 H = g_2 H$ because if $g_1 h_1 = g_2 h_2$, then $g_1^{-1} g_2 = h_1 h_2^{-1} \in H$, hence $g_1 H = g_2 H$. □

Definition 5.20. Let $[G : H]$ be the index of H in G denote the number of left cosets of H in G.

Example 5.21

$$[D_8 : \{r_1, r_5, 0, \pi\}] = 4$$
$$[\mathbb{Z}_{12} : \{0, 4, 8\}] = 4$$
$$[\mathbb{Q}_8 : \{-1, 1\}] = 4$$
$$[\mathbb{Q}_8 : \{-1, 1, i, -i\}] = 2$$
$$[\mathbb{Z} : n\mathbb{Z}] = n$$
$$[G : G] = 1$$
$$[G : \{e\}] = |G|$$

Theorem 5.22

6.4. Let $H \subset G$. The number of left cosets equals the number of right cosets.

Proof. The inversion map on G sends left cosets to right cosets and right cosets to left cosets.

Let L be the collection of left cosets and R be the collection of right cosets.

Define bijection $\phi : L \to R$ by $\phi(gH) = Hg^{-1}$. Now to check that this function is well defined

Definition 5.23. . Well defined: independent of choice of representative.

Check that if $gH = kH \Rightarrow \phi(gH) = \phi(kH)$.

$$gH = kH \Rightarrow Hg^{-1} = Hk^{-1} \Rightarrow \phi(gH) = \phi(kH).$$

Now check that ϕ is injective.

$$[\phi(gH) = \phi(kH)] \Rightarrow [Hg^{-1} = Hk^{-1}] \Rightarrow [gH = kH]$$

Now check that ϕ is surjective.

$Hx = H(x^{-1})^{-1} = \phi(x^{-1}H)$ □

§6 Tutorial 5: Cyclic Groups - 10-04

Theorem 6.1

Every cyclic group is abelian.

Theorem 6.2

Every subgroup of a cyclic group is cyclic.

Let G be a cyclic group and let $a \in G$ be of order n.

Theorem 6.3

$a^m = e \Leftrightarrow n|m$

Theorem 6.4

$b = a^k \in G$, then $|b| = \frac{n}{\gcd(n,k)}$

Corollary: In additive notation

- $\mathbb{Z}_n = \langle 1 \rangle$ with $|1| = n$.
- $k = k \cdot 1$, then $|k| = \frac{n}{\gcd(n,k)}$
- Generators of $\mathbb{Z}_n$ are the integers k such that $1 \leq k < n$ and $\gcd(k, n) = 1$.

Example 6.5

Subgroups of $(\mathbb{Z}_8, +)$. Observe that $1, 2, 4, 8$ divide 8. We have to find $k \in \mathbb{Z}_8$ such that:

- $\gcd(8, k) = 1$

  $\{1, 3, 5, 7\}$. These generate subgroups of order $\frac{8}{\gcd} = 8$. There is only one such subgroup of $\mathbb{Z}_8$ so they must all be the same.

- $\gcd(8, k) = 2$

  $\{2, 6\}$. These generate subgroups of order 4: $\{0, 2, 4, 6\}$

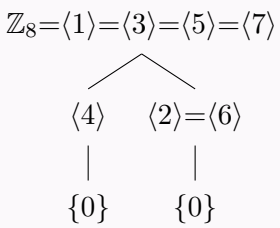
  A question arises: Do 2 and 6 generate the same subgroup? $\langle 2 \rangle = \{0, 2, 4, 6\}$. $6 \in \langle 2 \rangle$ so $\langle 2 \rangle = \langle 6 \rangle$.

- $\gcd(8, k) = 4$

  $\{4\}$. Generates a group of order 2: $\{0, 4\}$

- $\gcd(8, k) = 8$

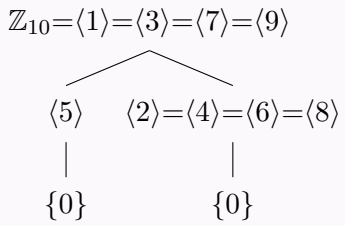
  $\{0\}$. Generates a sugroup of order 1: $\{0\}$



Example 6.6

List all the subgroups of $\mathbb{Z}_{10}$. Observe that 1, 2, 5, and 10 divide 10. Find $k \in \mathbb{Z}_{10}$ such that:

- $\gcd(k, 10) = 1$.
  $k = 1, 3, 7, 9$. $\mathbb{Z}_{10} = \langle 1 \rangle = \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle$
- $\gcd(k, 10) = 2$.
  $k = 2, 4, 6, 8$. These generate subgroups of order 5.
  $\langle 2 \rangle = \langle 4 \rangle = \langle 6 \rangle = \langle 8 \rangle = \{0, 2, 4, 6, 8\}$
- $\gcd(k, 10) = 5$.
  $k = 5$. $\langle 5 \rangle = \{0, 5\}$.
- $\gcd(k, 10) = 10$.
  $k = 0$. $\langle 0 \rangle = \{0\}$



Example 6.7

Let G be a group. Assume $a \in G$ such that $a^{24} = e$. What are the possible orders of a?

Recall that when $a^n = e$, the possible orders of a are those which divide n. Possible orders are therefore 1, 2, 3, 4, 6, 8, 12, 24.

$|a| = n \Rightarrow a^n = e$. NOT $\Leftarrow$

Example 6.8

Let $a, b \in G$. Prove the following statements:

(a) $|a| = |a^{-1}|$

Proof. $|a| = n$. $|a^{-1}| = m$

$$\begin{aligned} & a^n = e \\ \Rightarrow & (a^n)^{-1} \cdot a^n = (a^n)^{-1} \cdot e \\ \Rightarrow & e = (a^n)^{-1} \\ \Rightarrow & e = (a^{-1})^n \Rightarrow m|n \end{aligned}$$

You can show similarly that $n|m$. By proving that $m|n$ and that $n|m$, we have proven that $n = m$. □

(b) $\forall g \in G, |a| = |g^{-1}ag|$

Proof. Let $g \in G$, $|a| = n$, $|g^{-1}ag| = m$. Observe that:

$$\begin{aligned} & (g^{-1}ag)^m = e \\ \Rightarrow & (g^{-1}ag)(g^{-1}ag)\dots(g^{-1}ag) = e \\ \Rightarrow & g^{-1}a^m g = e \\ \Rightarrow & g \cdot g^{-1}a^m g \cdot g^{-1} = g \cdot e \cdot g^{-1} \\ \Rightarrow & a^m = e \end{aligned}$$

Therefore $n|m$ because $|a| = n$. Similarly $m|n$. Therefore $m = n$. □

(c) $|ab| = |ba|$

Proof. By (b), $|ab| = |a^{-1}(ab)a| = |a^{-1}aba| = |ba|$ □

Exercise 6.9. Show that if G has no proper non-trivial subgroups, then G is a cyclic group of prime orders.

Proof.

(a) Showing that G is cyclic. Let $g \in G : g \neq e$. $\langle g \rangle$ is a non-trivial subgroup of G because $g \in \langle g \rangle$ and $g \neq e$. By assumption that G has no proper non-trivial subgroups, $\langle g \rangle = G$.

(b) Showing that G must be of prime order.

a) Case where $|G| = \infty$. Let G

Observe that $\langle g^2 \rangle$ is a non-trivial subgroup of G. Observe that $\langle g^2 \rangle \neq G$ because $g \notin \langle g^2 \rangle$. "If the order of a group is infinity, we will always be able to generate non-trivial proper subgroups."

b) Case where $|G| = n < \infty$

Assume that $n = d \cdot m$ for some d, m. Since $d|n$, then G must have a subgroup H of order d. This would mean that H is non-trivial and $H \neq G$. This is a contradiction $\Rightarrow |G| = p$ for some prime number.

□

Exercise 6.10. An infinite cyclic group G has exactly 2 generators.
$G = \langle a \rangle = \langle b \rangle$. This would mean that $a = b^k$ for some k, and that $b = a^l$ for some l.

$$\begin{aligned} a = b^k = (a^l)^k = a^{lk} \\ \Rightarrow a^{-1} \cdot a = a^{-1}a^{lk} \\ \Rightarrow e = a^{lk-1} \end{aligned}$$

We know that $|a| = \infty$, therefore $lk - 1 = 0 \Rightarrow lk = 1$. This gives two possible cases: $l = k = 1$ or $l = k = -1$ because l and k must be integers. Therefore either $b = a$ or $b = a^{-1}$. This means that the only generators of G are a and a^{-1}.

§7 Lecture 10-07

Theorem 7.1

Proposition 6.9. Let $H \subset G$ and $g \in G$.
There is a bijection $\phi : H \to gH$ defined by $\phi(h) = gh$

Proof. This is injective because $(gh_1 = gh_2) \Rightarrow h_1 = h_2$
This is surjective because $gH = \{gh : h \in H\}$
$\{\phi(h) : h \in H\} = \phi(H)$ □

Theorem 7.2

Lagrange's Theorem
Let G be a finite group and $H \subset G$ a subgroup.
Then $\frac{|G|}{|H|} = [G : H]$

Proof. $G = g_1H \cup g_2H \dots g_hH$ by theorem 6.4
Each of $|g_iH| = |H|$ by proposition 6.9
$|G| = n|H| = [G : H]\,|H| \Rightarrow \frac{|G|}{|H|} = [G : H]$ □

Theorem 7.3

Corollary 6.11.
Let G be finite and $g \in G$. Then $|g|$ divides $|G|$.

Proof. $|g| = |\langle g \rangle|$ which represents a subgroup of G which divides $|G|$ by Lagrange's Theorem. □

Theorem 7.4

Corollary. If $g \in G$ is finite, then $g^{|G|} = e$. Intuitively this makes sense because the order of g divides the order of G.
$g^{|G|} = g^{|g| \cdot [G:\langle g \rangle]} = g^{|g|^{[G:\langle g \rangle]}} = e^{[G:\langle g \rangle]} = e$

Example 7.5

For $\sigma \in S_n, \sigma^{n!} = e$. But this is very inefficient.

Theorem 7.6

Corollary. If $|G| = p$ with p prime, then $G = \langle g \rangle$ for each $g \in G - \{e\}$.

Proof. $1 \neq |g|$ Nd $|g|$ divides $|G| = p (by 6.11)$. Therefore $|\langle g \rangle| = p$ so $\langle g \rangle = G$. □

Theorem 7.7

Corollary. If $K \subset H \subset G$ is a finite group, then $[G : K] = [G : H]\,[H : K]$

Proof. $[G : K] = \frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = [G : H]\,[H : K]$. □

Definition 7.8. Euler ϕ function. $\phi : \mathbb{N} \to \mathbb{N}$
$|U_n| = \phi(n)$

Example 7.9

$\phi(1) = 1$
$\phi(9) = |\{1, 2, 4, 7, 8\}| = 5$
$\phi(8) = |\{1, 3, 5, 7\}| = 4$

Theorem 7.10

6.18. Euler's Theorem
Let $a, n \in \mathbb{Z}$ with $n > 0$ and $\gcd(a, n) = 1$, then $a^{\phi(n)} = 1 \pmod{\text{n}}$

Proof. Regard $a \in U_n$.
$a^{\phi(n)} = a^{|U_n|} = 1 \pmod{\text{n}}$
i.e. $g^{|G|} = e$
At the time of righting this it makes perfect sense, but we will see how it goes when I revisit it haha. □

Theorem 7.11

6.19. Fermat Little Theorem.
Let p be prime and p does not divide a. (If p divided a, then a wouldn't be in the group of units U_p.)
Then $a^{p-1} = 1 \pmod{\text{p}}$

Proof. with $p = n$ prime, $a^{p-1} = a^{\phi(p)} \equiv_p 1$. This works because when p is prime, $\phi(n) = p - 1$.
moreover, for any a, $a^p \equiv_p a$. If $p|a$ this is $0 \equiv 0$. □

Definition 7.12. Conjugacy: Let $x, y \in G$. x is conjugate to y if there exists $g \in G$ such that $x = gyg^{-1}$. We use the notation $x \sim y$.
Lem: Conjugacy is an equivalence relation. Transitivity, Reflexivity, Symmetry.

Proof. Reflexivity: $x \sim x$ because $x = exe^{-1}$.
Symmetry: $(x \sim y) \Rightarrow (x = gyg^{-1}) \Rightarrow y = g^{-1}xg \Rightarrow y = gg^{-1}xg^{-1}g^{-1}$
Transitivity: □