PMATH 336 Course Notes - Spring 2019

Max Zhu

June 12, 2019

Contents

1 Groups

1.1 Definition and simple examples

Groups are used for describing symmetries of objects, and for finding solutions to equations. Before formally defining what a group is, we will start with some examples and note their properties.

Example 1.1: Integers with addition

$(\mathbb{Z}, +)$, the integers with usual addition, is a group. We notice the following properties.

- For all $a, b \in \mathbb{Z}$ we have $a + b \in \mathbb{Z}$. **(closure)**
- There is an identity $0 \in \mathbb{Z}$ such that for all $a \in \mathbb{Z}$, we have $a + 0 = 0 + a = a$. **(identity)**
- Every integer $a \in \mathbb{Z}$ has an inverse $a^{-1} \in \mathbb{Z}$ such that $a + a^{-1} = a^{-1} + a = 0$. Here, $a^{-1} = -a$. **(inverses)**
- Let $a, b, c \in \mathbb{Z}$. Then, $(a + b) + c = a + (b + c)$. **(associativity)**

Example 1.2: Rationals with addition

$(\mathbb{Q}, +)$, rational numbers with usual addition, is a group. Similarly to the integers,

- For all $a, b \in \mathbb{Q}$ we have $a + b \in \mathbb{Q}$. **(closure)**
- There is an identity $0 \in \mathbb{Q}$ such that for all $a \in \mathbb{Q}$, we have $a + 0 = 0 + a = a$. **(identity)**
- Every integer $a \in \mathbb{Q}$ has an inverse $a^{-1} \in \mathbb{Q}$ such that $a + a^{-1} = a^{-1} + a = 0$. Here, $b = -a$. **(inverses)**
- Let $a, b, c \in \mathbb{Q}$. Then, $(a + b) + c = a + (b + c)$. **(associativity)**

Example 1.3: Real and complex numbers with addition

$(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are also groups, and these properties can be verified.

Example 1.4

$(\{1, 1, i, -i\}, \cdot)$ is a group. We can create a table to show the result of the operation on any two elements of the set:

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

This kind of table is called a Cayley table.

- Note that each row and column contains each element exactly once.
- From the Cayley table, the set is closed under $\cdot$.
- The identity is 1.
- Each element has an inverse in the set:

$$\begin{aligned}(1)^{-1} &= 1 \\ (-1)^{-1} &= -1 \\ (i)^{-1} &= -i \\ (-i)^{-1} &= i\end{aligned}$$

Definition 1.5: Group

Let G be a set, and $\star : G \times G \to G$ be a binary operation on G. We say $(G, \star)$ is a group if it satisfies the following conditions:

(i) Associativity: Let $a, b \in G$. Then, $(a \star b) \star c) = a \star (b \star c)$.

(ii) Identity: There exists $e \in G$ such that for all $a \in G$, we have $a \star e = e \star a = a$.

(iii) Inverses: For all $a \in G$, there exists $a \in\in G$ such that $a \star a^{-1} = a^{-1} \star a = e$.

Remark 1.6

- When proving a set G with an operation $\star$ is a group, we must also show G is closed under $\star$.
- We often refer to a group $(G, \star)$ as simply G.
- We often write ab instead of $a \star b$ for some operation $\star$.
- We usually denote the identity element of a group with e.

Proposition 1.7: Nonzero rationals with multiplication is a group

$(\mathbb{Q}\backslash\{0\}, \cdot)$, nonzero rationals with usual multiplication, is a group.

Proof. We use the notation $\mathbb{Q}^* := \mathbb{Q}\backslash\{0\}$.
Let $a, b, c, d, e, f \in \mathbb{Z}$ so $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}^*$. Then,

(i) $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \in \mathbb{Q}^*$ **(closure)**

(ii) $\frac{a}{b} \cdot (\frac{c}{d} \cdot \frac{e}{f}) = (\frac{a}{b} \cdot \frac{c}{d}) \cdot \frac{e}{f}$ **(associativity)**

(iii) $\frac{1}{1} \cdot \frac{a}{b} = \frac{a}{b} \cdot \frac{1}{1} = \frac{a}{b}$ **(identity)**

(iv) $\frac{a}{b} \cdot \frac{b}{a} = \frac{b}{a} \cdot \frac{a}{b} = \frac{1}{1}$, and $\frac{b}{a} \in \mathbb{Q}^*$ **(inverses)**

So, $(\mathbb{Q}^*, \cdot)$ has all required properties of a group. □

Example 1.8: Integers modulo n with addition

$(\mathbb{Z}_n, +)$, integers modulo n with addition is a group.
Here, $\mathbb{Z}_n = \{[0], \ldots, [n-1]\}$ where $[a] = \{b \in \mathbb{Z} : b \text{ has remainder } a \text{ when dividing by n}\}$, and $[a] + [b] = [a+b]$. To save space, we may write a instead of $[a]$. Let us use $\mathbb{Z}_5$ as an example.

$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. Here is the Cayley table for $\mathbb{Z}_5$:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

We can quickly verify the 4 properties. Let $[a], [b], [c] \in \mathbb{Z}_5$. Then,

(i) Closure: obvious from the Cayley table.

(ii) Associativity: $[a] + ([b] + [c]) = [a] + [b+c] = [a+b+c] = [a+b] + c = ([a] + [b]) + c$

(iii) Identity: $[0] + [a] = [0+a] = [a] = [a+0] = [a] + [0]$

(iv) Inverses: $[a]^{-1} = [-a] = [n-a]$

Example 1.9: "Integers modulo n" with multiplication

$(\mathbb{Z}_n^*, \cdot)$, where $\mathbb{Z}_n^* := \{[a] \in \mathbb{Z}_n : \gcd(a,n) = 1\}$ and $[a] \cdot [b] = [ab]$, is a group. Let us use $\mathbb{Z}_6^*$ as an example.

$\mathbb{Z}_6^* = \{1, 5\}$. Note, $4 \notin \mathbb{Z}_6^*$ since $2|4$ and $2|6$, so $\gcd(4,6) = 2 \neq 1$. Here is the Cayley table for $\mathbb{Z}_6^*$:

$\cdot$	1	5
1	1	5
5	5	1

Here, the identity is 1 and the inverses are $(5)^{-1} = 5$ and $(1)^{-1} = 1$.

Example 1.10: General linear group in $\mathbb{R}$

We define the group $GL_n(\mathbb{R})$ to be the set $\{A \in M_n(\mathbb{R}) : \det(A) \neq 0\}$ with usual matrix multiplication. We can easily verify the properties. Let $A, B \in GL_n(\mathbb{R})$. Then,

(i) Closure: $\det(AB) = \det(A)\det(B) \neq 0$ so $AB \in GL_n(\mathbb{R})$.

(ii) Associativity: matrix multiplication is known to be associative.

(iii) Identity: $\det(I) = 1 \neq 0$ where $I = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$ is the identity matrix.

(iv) Inverses: usual matrix inverses, since $\det(A^{-1}) = \frac{1}{\det(A)} \neq 0$ so $A^{-1} \in GL_n(\mathbb{R})$.

Definition 1.11: Abelian groups

A group $(G, \star)$ is <u>abelian</u> if for all $a, b \in G$ we have $a \star b = b \star a$. Otherwise, the group is <u>non-abelian</u>.

Example 1.12: Some abelian groups

$(\mathbb{Z}, +), (\mathbb{Q}^*, \cdot), (\mathbb{Z}_n, +), (\mathbb{Z}_n^*)$ are all abelian.

Example 1.13: Dihedral groups

Dihedral groups $(D_n, \cdot)$ are a family of groups of symmetries of a regular n-gon. The operations can be thought of as operations that change places of the vertices but not the overall shape of the polygon. Let us use D_4 as an example.

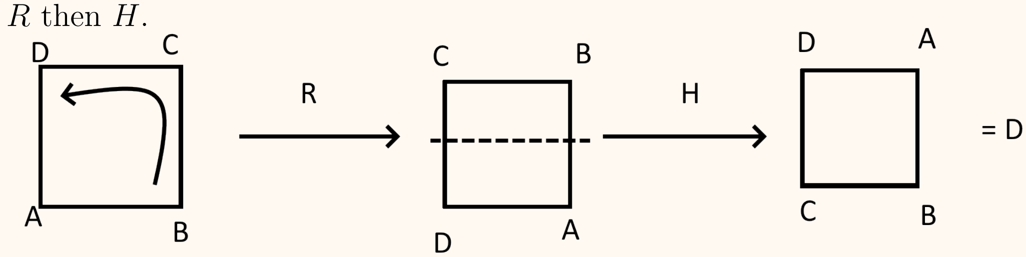
D_4 is the group of symmetries of a square. Elements of D_4 include:

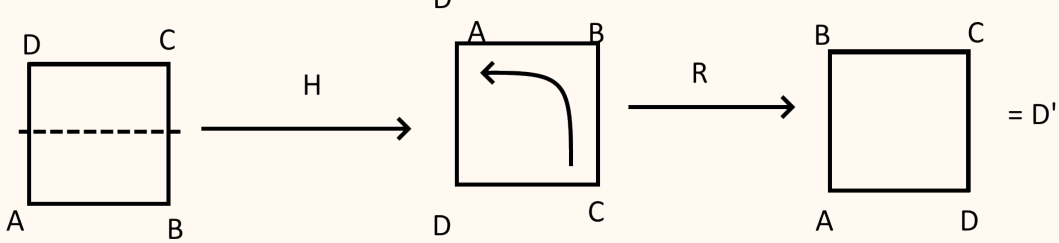
- e, rotation by 0°.
- R, rotation by 90°counter-clockwise.
- R^2, rotation by 180°counter-clockwise.
- R^3, rotation by 270°counter-clockwise.

We also have flips:

- H, flip through horizontal axis.
- V, flip through vertical axis.
- D, flip through top-left bottom-right diagonal axis.
- D', flip through top-right bottom-left diagonal axis.

The elements are functions from a set of vertices to itself which preserves distance and adjacent-ness. The operator is composition of functions. For example, HR is application of R then H.





From this MS Paint illustration of some operations in D_4, it is clear that D_4 is non-abelian.

Definition 1.14: Order of a group

Let $(G, \star)$ be a group. The order of G is the number of elements in G, which is denoted $|G|$. If G is infinite, we say $|G| = \infty$.

Example 1.15: Orders of some groups

$$\begin{aligned} |Z_n| &= n \\ |Z_n^*| &= \phi(n) \text{ (Euler's totient function)} \\ |(\mathbb{Z}, +)| &= \infty \\ |D_n| &= 2n \end{aligned}$$

1.2 Properties of groups

Proposition 1.16: Uniqueness of identity

In a group G, there is only one identity element.

Proof. Assume there are 2 identities $e, f \in G$. Since e is an identity,

$$ef = fe = f$$

And since f is an identity,

$$fe = ef = e$$

Therefore $e = f$. $\square$

Proposition 1.17: Cancellation

If G is a group, for all $a, b, c \in G$ we have:

$$ab = ac \implies b = c \text{ [Left cancellation]}$$
$$ba = ca \implies b = c \text{ [Right cancellation]}$$

Proof. Let $a, b, c \in G$ such that $ab = ac$. Then,

$$\begin{aligned} ab &= ac \\ a^{-1}(ab) &= a^{-1}(ac) \\ (a^{-1}a)b &= (a^{-1}a)c \text{ [associativity]} \\ eb &= ec \text{ [inverses]} \\ b &= c \text{ [identity]} \end{aligned}$$

As required. Right cancellation has similar proof. □

Remark 1.18

Cancellation should be on the same side. For example in D_4, $RH = D' = VR$ but $H \neq V$.

Proposition 1.19: Uniqueness of inverses

Let G be a group. If b, c are both inverses of a then $b = c$.

Proof. Suppose $e = ab = ac$. Then,

$$\begin{aligned} ab &= ac \\ b(ab) &= b(ac) \\ (ba)b &= (ba)c \text{ [associativity]} \\ eb &= ec \text{ [by hypothesis]} \\ b &= c \text{ [identity]} \end{aligned}$$

as required. □

Proposition 1.20: Socks-shoes

Let G be a group with $a, b \in G$. Then, $(ab)^{-1} = b^{-1}a^{-1}$.

Proof.

$$\begin{aligned}(ab)(b^{-1}a^{-1}) &= a(bb^{-1})a^{-1} \\ &= a(ea^{-1}) \\ &= aa^{-1} \\ &= e\end{aligned}$$

so $(ab)^{-1} = b^{-1}a^{-1}$ as required. □

Definition 1.21: Exponentiation

Let $(G, \star)$ be a group, with $a \in G$, $n \in \mathbb{Z}$. Then,

$$a^n := \begin{cases} a \star \cdots \star a \text{ (n times)}, & n > 0 \\ e, & n = 0 \\ a^{-1} \star \cdots \star a^{-1} \text{ (n times)}, & n < 0 \end{cases}$$

Note: some exponential properties work with the same base. For example,

$$\begin{aligned}a^n a^m &= a^{n+m} \\ (a^{-1})^n &= a^{-n}\end{aligned}$$

However, in general $(ab)^n \neq a^n b^n$ for $a.b \in G$ unless G is abelian.

Definition 1.22: Order of an element

Let G be a group with $a \in G$. The <u>order</u> of a is the smallest positive integer such that $a^k = e$. We denote this by $|a| = k$. If $a^k \neq e$ for all k, we say $|a| = \infty$.

Example 1.23: Some orders of group elements

- In all groups, $|e| = 1$
- In D_4, $|v| = 2$
- In $\mathbb{Z}_{15}^*$, $|z| = 4$
- In $\mathbb{Z}$, all nonzero elements have order ∞
- In $\mathbb{Q}^*$, $|1| = 1$ and $|-1| = 2$

Definition 1.24: Direct products

Let $(G, \star), (H, \cdot)$ be groups. Then, the set $G \times H = \{(g, h) : g \in G, h \in H\}$ with operation $(g_1, h_1)\Delta(g_2, h_2) := (g_1 \star g_2, h_1 \cdot h_2)$ is a group. $(G \times H, \Delta)$ is called the direct product of G and H.

2 Subgroups

Definition 2.1: Subgroup

Let $(G, \star)$ be a group, and $H \subseteq G$. Then H is a subgroup of G if $(H, \star)$ is a group.

If H is a subgroup of G, we say $H \leq G$ and if $H \subsetneq G$, we say $H < G$.

If $(H, \star)$ is not a group, we say $H \nleq G$.

Example 2.2: Some easy subgroups

For all groups $(G, \star)$, we know $\{e\} \leq G$ and $G \leq G$.

Example 2.3: Subgroups of $\mathbb{Z}$

Define $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ for $n \in \mathbb{Z}$. Then, $(n\mathbb{Z}, +)$ is a group, so $n\mathbb{Z} \leq \mathbb{Z}$.

Proposition 2.4: One-step test

Let G be a group, and $\emptyset \neq H \subseteq G$. If for all $a, b \in H$ we have $ab^{-1} \in H$, then $H \leq G$.

Proof. Let $a, b \in H$, since $H \neq \emptyset$.

(i) Associativity: follows from G being a group.

(ii) Identity: By hypothesis $aa^{-1} \in H$, so $e \in H$.

(iii) Inverses: We know $e \in H$, so by hypothesis $ea^{-1} \in H$ so $a^{-1} \in H$.

(iv) Closure: By inverses $b^{-1} \in H$, so by hypothesis $a(b^{-1})^{-1} \in H$ thus $ab \in H$.

So H satisfies all requirements of a group. □

Proposition 2.5: Two-step test

Let $(G, \star)$ be a group, and $\emptyset \neq H \subseteq G$. If $a, b \in H \implies ab \in H$ and $a \in H \implies a^{-1} \in H$, then $H \leq G$. In other words, $H \leq G$ iff H is closed under $\star$ and closed under inverses.

Proof. Let $a, b \in H$, since $H \neq \emptyset$.

(i) Associativity: follows from G being a group.

(ii) Identity: by hypothesis, $a^{-1} \in H$. Therefore, $aa^{-1} = e \in H$.

(iii) Inverses: by hypothesis.

(iv) Closure: by hypothesis.

So H satisfies all requirements of a group. □

Example 2.6: Center of a group

The center of a group G is defined

$$Z(G) := \{a \in G : ag = ga \text{ for all } g \in G\}$$

and is a subgroup of G.

Proof. Let $g \in G$ and $a, b \in Z(G)$. We know $eg = ge$ for all $g \in G$, so $Z(G) \neq \emptyset$. Now,

$$\begin{aligned}(ab)g &= a(bg)\\ &= a(gb)\\ &= (ag)b\\ &= (ga)b\\ &= g(ab)\end{aligned}$$

So $ab \in Z(G)$. Also, since $a \in Z(G)$,

$$\begin{aligned}ax &= xa\\ a^{-1}(ax) &= a^{-1}(xa)\\ (a^{-1}a)x &= a^{-1}(xa)\\ ex &= a^{-1}(xa)\\ x &= a^{-1}(xa)\\ xa^{-1} &= a^{-1}(xa)a^{-1}\\ xa^{-1} &= (a^{-1}x)(aa^{-1})\\ xa^{-1} &= (a^{-1}x)e\\ xa^{-1} &= a^{-1}x\end{aligned}$$

So $a^{-1} \in Z(G)$. By two-step test, $Z(G) \leq G$. □

Note: A group G is abelian iff $Z(G) = G$.

Definition 2.7: Generator of a group

Let G be a group, with $a \in G$. Then, $\langle a \rangle := \{a^n : n \in \mathbb{Z}\}$. This is the (sub)group generated by a and a is called the generator of this group.

Remark 2.8

Not all subgroups are generated by a single element. For example, if $H = \{(0,0), (0,2), (2,0), (2,2)\}$ then $H \leq \mathbb{Z}_4 \times \mathbb{Z}_4$ but H is not generated by any of its elements.

3 Lagrange's theorem

3.1 Cosets

Definition 3.1: Coset

Let G be a group and $H \leq G$.
For any $a \in G$,

$$aH := \{ah : h \in H\}$$

is the left coset of H containing a in G and

$$Ha := \{ha : h \in H\}$$

is the right coset of H containing a in G. We denote the number of left cosets of H in G by $|G : H|$, and call it the index of H in G.

Example 3.2: Cosets of $\mathbb{Z}_9$

Let $G = \mathbb{Z}_9$, $H = \{0, 3, 6\} = \langle 3 \rangle$. Then,

$$\begin{aligned} 0 + H &= \{0, 3, 6\} = 3 + H = 6 + H \\ 1 + H &= \{1, 4, 7\} = 4 + H = 7 + H \\ 2 + H &= \{2, 5, 8\} = 5 + H = 8 + H \end{aligned}$$

We can make several observations.

- aH may not be a group.
- aH may be equal to bH even if $a \neq b$.
- All cosets are the same size.
- No element is in two different cosets.

We will use some of these observations to prove Lagrange's theorem.

In all of these lemmas, G is a group and $H \leq G$.

Lemma 3.3

Element of G is in some left coset of H.

Proof. Let $a \in G$. Then, $a = ae$ and $e \in H$ so $a \in eH$. □

Lemma 3.4

Let $a, b \in G$. Then, $aH = bH$ or $aH \cap bH = \emptyset$.

Proof. Assume $aH \cap bH \neq \emptyset$. We will show that $aH = bH$.
By hypothesis there is $c \in aH \cap bH$, so $c = ah_1 = bh_2$ for $h_1, h_2 \in H$. Let $ah \in aH$ for some $h \in H$. Then,

$$\begin{aligned} ah &= aeh \\ &= a(h_1 h_1^{-1})h \\ &= (ah_1)(h_1^{-1}h) \\ &= bh_2 h_1^{-1} h \end{aligned}$$

So $ah \in bH$ since $h_2 h_1^{-1} h \in H$. Thus $aH \subseteq bH$ and similarly $bH \subseteq aH$. Therefore, $aH = bH$. □

Lemma 3.5

Any left coset of H has the same number of elements as H.

Proof. Let $a \in G$. We will show $|aH| = |H|$.
Let $f : H \to aH$ be defined $f(h) := aH$ for all $h \in H$. Then,

- f is injective: Let $h_1, h_2 \in H$. Then, $f(h_1) = f(h_2) \implies ah_1 = ah_2 \implies h_1 = h_2$ by cancellation.
- f is surjective: Let $ah \in aH$. Then, $f(h) = ah$.

So f is a bijection between H and aH, so $|aH| = |H|$. □

3.2 Lagrange's theorem and its corollaries

Theorem 3.6: Lagrange's theorem

Let G be a finite group, and $H \leq G$. Then, $|H|$ divides $|G|$.

Proof. By lemmas 3.3 and 3.4, there exist $a_1, \ldots, a_k \in G$ such that G is a disjoint union of cosets: $G = a_1 H \cup \cdots \cup a_k H$. By lemma 3.5,

$$\begin{aligned} |G| &= |a_1 H| + \cdots + |a_k H| \\ &= |H| + \cdots + |H| \\ &= kH \end{aligned}$$

Therefore $|H|$ divides $|G|$. □

Corollary 3.7

Let G be a finite group. Then,

(i) Let $H \leq G$. The index $|G : H| = \frac{|G|}{|H|}$.

(ii) Let $a \in G$. Then, $|a|$ divides $|G|$.

(iii) If $|G|$ is prime, then $G = \langle a \rangle$ for some $a \in G$.

(iv) Let $a \in G$. Then, $a^{|G|} = e$.

(v) **(Fermat's little theorem.)** Let $a \in \mathbb{Z}$, and p be prime. then, $a^p \equiv a \mod p$.

Proof.

(i) Follows immediately from proof of Lagrange's theorem.

(ii) We know $\langle a \rangle \leq G$. Since $|\langle a \rangle| = |a|$, the statement follows from Lagrange's theorem.

(iii) Let $a \in G$ with $a \neq e$. This is possible since $|G| \geq 2$. Then, $|a|$ divides $|G|$ by (ii). Since $a \neq e$ and $|G|$ is prime, $|a| = |G|$. So, since $|\langle a \rangle| = |G|$ and $\langle a \rangle \leq G$, we have $\langle a \rangle = G$.

(iv) exercise

(v) Let $a \in \mathbb{Z}$. Then, if $p|a$ then $p|a^p \implies a^p \equiv 0 \mod p$. If $p \nmid a$ then $\gcd(a, p) = 1$. So, $a \equiv n \mod p$ for some $n \in \mathbb{Z}_p^*$. Now, $|\mathbb{Z}_p^*| = p - 1$. By (iv) we have

$$\begin{aligned} n^{p-1} &\equiv 1 \mod p \\ n^p &\equiv n \mod p \\ a^p &\equiv a \mod p \end{aligned}$$

□

4 Cyclic groups

Definition 4.1: Cyclic group

Let G be a group. G is <u>cyclic</u> if there exists $a \in G$ such that $\langle a \rangle = G$. a is then a <u>generator</u> of G.

Example 4.2: Some cyclic groups

- $(\mathbb{Z}, +)$ is cyclic, since $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.
- $\mathbb{Z}_6$ is cyclic, since $\mathbb{Z}_6 = \langle 1 \rangle = \langle 5 \rangle$.
- $\mathbb{Z}_9^*$ is cyclic, since $\mathbb{Z}_9^* = \langle 2 \rangle$.

Proposition 4.3: Cyclic groups are abelian

Let $G = \langle a \rangle$ be a cyclic group. Then G is abelian.

Proof. Let $a^n, a^m \in G$ where $n, m \in \mathbb{Z}$. Then,

$$\begin{aligned} a^n a^m &= a^{n+m} \\ &= a^m a^n \end{aligned}$$

$\square$

Proposition 4.4: Subgroups of a cyclic group are cyclic

Let $G = \langle a \rangle$ be a cyclic group, and $H \leq G$. Then H is also cyclic.

Proof. If $G = \{e\}$, clearly $H = G$ so we're done. Thus assume $G \neq \{e\}$. So, $G = \langle a \rangle$ where $a \neq e$.

Let k be the smallest positive integer such that $a^k \in H$. Now, it is clear that $\langle a^k \rangle \subseteq H$ since H is a group. Let $a^n \in H$ for some integer n. By division algorithm, $n = qk + r$ for $q, r \in \mathbb{Z}$ and $0 \leq r < k$. So, $a^n = a^{kq+r} = (a^k)^q (a^r)$ which implies $(a^k)^{-q} a^n = a^r$. Since $a^k, a^n \in H$ we have $a^r \in H$. However, $r < k$ so $r = 0$, since k is the minimal positive integer such that $a^k \in H$. Therefore, $a^n = (a^k)^q$ so $H = \langle a^k \rangle$. $\square$

Theorem 4.5: Criterion for $a^i = a^j$

Let G be a group with $a \in G$.

- If $|a| = \infty$, then $a^i = a^j \iff i = j$.
- If $|a| = n \in \mathbb{N}$, then
  - (i) $\langle a \rangle = \{e, a, \ldots, a^{n-1}\}$
  - (ii) $a^i = a^j \iff n | i - j$.

Proof.

- Suppose $a \in G$ such that $a^i = a^j$ and $|a| = \infty$. Then, $a^{i-j} = e$. However since $|a| = \infty$, we know $a^k \neq e$ for all $k \in \mathbb{N}$. So, $i - j = 0$ and $i = j$. Trivially, $i = j \implies a^i = a^j$.
- Suppose $a \in G$ and $|a| = n \in \mathbb{N}$.
  - (i) We must prove that $\langle a \rangle \subseteq \{e, a, \ldots, a^{n-1}\}$ (*) and $\{e, a, \ldots, a^{n-1}\} \subseteq \langle a \rangle$ (**). (**) is trivial from definition of $\langle a \rangle$, so we will prove (*).

    Let $a^k \in \langle a \rangle$ for some $k \in \mathbb{N}$. If $k < n$ then clearly $a^k \in \{e, a, \ldots, a^{n-1}\}$. Otherwise, there exists $q, r \in \mathbb{Z}$ such that $k = qn + r$ with $0 \leq r < n$, by division algorithm. So, we have

$$\begin{aligned} a^k &= a^{nq+r} \\ &= a^{nq} a^r \\ &= (a^n)^q a^r \\ &= e^q a^r \\ &= a^r \end{aligned}$$

    So since $0 \leq r < n$, we have $a^k \in \{e, a, \ldots, a^{n-1}\}$ so (i) holds.
  - (ii) ($\Longrightarrow$) We know $a^i = a^j \implies a^{i-j} = e$. By division algorithm, $i - j = nq + r$ for $q, r \in \mathbb{Z}$ and $0 \leq r < n$. So,

$$\begin{aligned} i - j &= nq + r \\ a^{i-j} &= (a^n)^q a^r \\ e &= a^r \end{aligned}$$

    Since $|a| = n$, we know n is the smallest positive integer such that $a^n = e$, and we know $r < n$, therefore $r = 0$ and $i - j = nq$ for some $q \in \mathbb{Z}$.
    ($\Longleftarrow$) If $i - j = nq$ for some $q \in \mathbb{Z}$, then $a^{i-j} = (a^n)^q = e \implies a^i = a^j$.

□

Corollary 4.6

Suppose $|a| = n$. Then, $a^k = e$ iff $n|k$.

Proof. $a^k = e \iff a^k = a^n \iff n|k$ by theorem 4.5 $\square$

Remark 4.7

Note that $a^k = e$ does not imply $k = |a|$. It does, however, imply $|a|$ divides k.

Theorem 4.8

Suppose G is a cyclic group, with $G = \langle a \rangle$ and $|G| = |a| = n$. If $k \in \mathbb{Z}$, then

(i) $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$

(ii) $|\langle a^k \rangle| = \frac{n}{\gcd(n,k)}$

Proof.

(i) Let $d = \gcd(n,k)$. We want to prove $\langle a^k \rangle = \langle a^d \rangle$, and thus $\langle a^k \rangle \subseteq \langle a^d \rangle$ (*) and $\langle a^d \rangle \subseteq \langle a^k \rangle$ (**). By definition of gcd, we know $k = rd$ for some $r \in \mathbb{Z}$. Then,

$$\begin{aligned} a^k &= a^{rd} \\ &= (a^d)^r \in \langle a^d \rangle \end{aligned}$$

so (*) holds. To prove (**), it is enough to show $a^d \in \langle a^k \rangle$ since $d|k$. By Bézout's identity, there exist $s, t \in \mathbb{Z}$ such that $d = ns + kt$. So,

$$\begin{aligned} a^d &= a^{ns+kt} \\ &= a^{ns}a^{kt} \\ &= (a^n)^s(a^k)^t \\ &= (a^k)^t \end{aligned}$$

Thus (**) holds and $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$.

(ii) We want to prove $|a^d| = \frac{n}{d}$. Clearly $(a^d)^{\frac{n}{d}} = a^n = e$, so $|a^d| \leq \frac{n}{d}$. For contradiction suppose $|a^d| = \alpha < \frac{n}{d}$. Then,

$$\begin{aligned} (a^d)^\alpha &= e \\ a^{d\alpha} &= e \\ \alpha &< \frac{n}{d} \\ d\alpha &< n \end{aligned}$$

But this contradicts $|a| = n$ so (ii) holds.

$\square$

Example 4.9

Suppose $G = \langle a \rangle$ and $|a| = 30$. What is $\langle a^{26} \rangle$?

$$\begin{aligned}\langle a^{26} \rangle &= \langle a^{\gcd(26,30)} \rangle \\ &= \langle a^2 \rangle\end{aligned}$$

What about $\langle a^{23} \rangle$?

$$\begin{aligned}\langle a^{23} \rangle &= \langle a^{\gcd(23,30)} \rangle \\ &= \langle a \rangle\end{aligned}$$

Also, $|\langle a^{26} \rangle| = \frac{30}{2} = 15$.

Corollary 4.10

$\mathbb{Z}_n$ is a cyclic group of order n, and $i \in \mathbb{Z}_n$ generates $\mathbb{Z}_n \iff \gcd(i, n) = 1$.

Theorem 4.11: Fundamental theorem of cyclic groups

Let G be a finite cyclic group with $G = \langle a \rangle$ and $|G| = n$. Then,

1. Every subgroup of G is cyclic.
2. If $H \leq G$ then $|H|$ divides $|G|$.
3. If k is a divisor of n then there is a unique subgroup $H \leq G$ such that $|H| = k$ and $H = \langle a^{\frac{n}{k}} \rangle$.

Proof.

1. Proposition 4.4
2. Lagrange's theorem 3.6
3. Suppose k divides n. We need to prove there is a subgroup $H \leq G$ with $|H| = k$ (i) and that H is the unique such subgroup (ii).
   (i) Consider $H = \langle a^{\frac{n}{k}} \rangle$. From theorem 4.8, $|H| = |\langle a^{\frac{n}{k}} \rangle| = \frac{n}{\gcd(n, \frac{n}{k})}$. Since $\frac{n}{k} | n$, we have $\gcd(n, \frac{n}{k}) = \frac{n}{k}$. So, $|H| = \frac{n}{(n/k)} = k$.
   (ii) Suppose $P \leq G$ with $|P| = k$. From proposition 4.4, $P = \langle a^m \rangle$ for some $m \in \mathbb{N}$. By theorem 4.8, $P = \langle a^{\gcd(n,m)} \rangle$. Since $|P| = k$ we have $\frac{n}{k} = \gcd(n, m)$ so $P = \langle a^{\frac{n}{k}} \rangle = H$.

$\square$

Example 4.12: Subgroups of $\mathbb{Z}_12$

We know $\mathbb{Z}_{12} = \langle 1 \rangle$ and $|\mathbb{Z}_{12}| = 12$. Here are the subgroups of $\mathbb{Z}_{12}$.

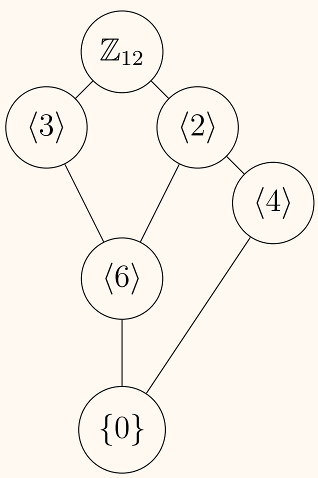
Order	Subgroup
1	$\langle 1^{12} \rangle = \{0\}$
2	$\langle 1^{6} \rangle = \{0, 6\}$
3	$\langle 1^{4} \rangle = \{0, 4, 8\}$
4	$\langle 1^{3} \rangle = \{0, 3, 6, 9\}$
6	$\langle 1^{2} \rangle = \{0, 2, 4, 6, 8, 10\}$
12	$\langle 1^{1} \rangle = \mathbb{Z}_{12}$

5 Subgroup lattices

Definition 5.1: Subgroup lattice

Let G be a group. A subgroup lattice is an illustration which describes all relationships between subgroups of G.

Example 5.2: Subgroup lattice of $\mathbb{Z}_{12}$



6 Permutation groups

Definition 6.1: Permutation group

Let $B = \{1, \ldots, n\}$. A permutation of B is a bijection from B to itself. That is to say, a function $\sigma : B \to B$ which is one-to-one and onto.
Let $n \in \mathbb{N}$. Then, the permutation group of order n is the set of all permutations on $\{1, \ldots, n\}$ with the operation being function composition.
Elements σ of S_n can be denoted $\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$.

Remark 6.2: Order of S_n

- What is $|S_n|$? Let $\sigma \in S_n$. There are n possibilities for $\sigma(1)$. Given $\sigma(1)$, there are $n-1$ possibilities for $\sigma(2)$, and so on. Thus, $|S_n| = n(n-1)(n-2)\ldots 1 = n!$.
- S_n is a non-abelian group. (Prove this!)

6.1 Cycle notation

Example 6.3: Cycle notation for elements of S_3

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Then, $\sigma = (12)(3)$ since $\sigma(1) = 2$ and $\sigma(2) = 1$ and $\sigma(3) = 3$.
Let $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$. Then, $\beta = (132) = (321) = (213)$.

Example 6.4: Cycle notation for an element of S_6

Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 2 & 5 & 1 \end{pmatrix}$. Then, $\sigma = (136)(24) = (24)(136)$.

Definition 6.5: Cycles and transpositions

An expression of the form $(a_1 \ldots a_m)$ is a cycle length m, and if $m = 2$, a transposition.

Theorem 6.6: Permutations are products of disjoint cycles

Let $\sigma \in S_n$. Then, σ can be written as a cycle or a product of disjoint cycles.

Proof. If σ is a cycle we're done, so suppose it's not. Then, let $a_1 \in \{1, \dots, n\}$ and $a_2 = \sigma(a_1), \dots, a_k = \sigma(a_{k-1}), a_1 = \sigma(a_k)$. This is always possible since $\{1, \dots, n\}$ is a finite set. Let $b_1 \in \{1, \dots, n\} \setminus \{a_1, \dots, a_k\}$ and $b_2 = \sigma(b_1), \dots, b_m = \sigma(b_{m-1}), b_1 = \sigma(b_m)$. We claim the cycles $(a_1 \dots a_k)$ and $(b_1 \dots b_m)$ are disjoint.
For contradiction suppose $a_i = b_j$ for some i, j. Then,

$$\begin{aligned} \sigma^{i-1}(a_1) &= \sigma^{j-1}(b_j) \\ b_1 &= \sigma^{j-1-i+1}(a_1) \in \{a_1, \dots, a_k\} \end{aligned}$$

which is impossible since $b_1 \notin \{a_1, \dots, a_k\}$.
Since $\{1, \dots, n\}$ is finite, this process stops eventually, and gives a representation of σ as a product of disjoint cycles. $\square$

Example 6.7

Let $\tau = (124)$, $\sigma = (1235)$. What are $\tau\sigma$ and $\sigma\tau$?

$$\begin{aligned} \tau\sigma &= (124)(1235) = (14)(235) \\ \sigma\tau &= (135)(24) \end{aligned}$$

Remark 6.8

$S_n \leq S_m$ for $m \geq n$.

Theorem 6.9: Disjoint cycles commute

Let $\sigma = (a_1 \dots a_k)$, $\tau = (b_1 \dots b_l)$ be disjoint cycles. Then $\sigma\tau = \tau\sigma$.

Proof. We know $\{1, \dots, n\} = \{a_1, \dots, a_k\} \cup \{b_1, \dots, b_l\} \cup \{c_1, \dots, c_m\}$
where $\{c_1, \dots, c_m\} = \{1, \dots, n\} \setminus (\{a_1, \dots, a_k\} \cup \{b_1, \dots, b_l\})$. So,

- For all $i \in \{1, \dots, k\}$, we have $\tau(\sigma(a_i)) = \tau(a_{i+1}) = a_{i+1} = \sigma(a_i) = \sigma(\tau(a_i))$ since $\tau(a_i) = a_i$.
- For all $i \in \{1, \dots, l\}$, we have $\sigma(\tau(b_i)) = \sigma(b_{i+1}) = b_{i+1} = \tau(b_i) = \tau(\sigma(b_i))$ since $\sigma(b_i) = b_i$.
- For all $i \in \{1, \dots, m\}$, we have $\sigma(\tau(c_i)) = \sigma(c_i) = c_i = \tau(c_i) = \tau(\sigma(c_i))$ since $\sigma(c_i)\tau(c_i) = c_i$.

Therefore in all cases, $\sigma\tau = \tau\sigma$. $\square$

Remark 6.10

Let σ be a k-cycle. Then $|\sigma| = k$.

Theorem 6.11: Order of a permutation

Let $\alpha \in S_n$. Then $|\alpha|$ is the least common multiple of the lengths of the disjoint cycles representing α.

Proof. Let $\sigma, \tau \in S_n$ be disjoint cycles, with σ being an m-cycle and τ being a k-cycle. Let $l = \operatorname{lcm}(k, m)$. We claim $n := |\sigma\tau| = l$.
Since $l = \operatorname{lcm}(k, m)$, we have $k|l$ and $m|l$. So,

$$\begin{aligned}(\tau\sigma)^l &= \tau^l\sigma^l \\ &= (\tau^k)^s(\sigma^m)^t\end{aligned}$$

for some $s, t \in \mathbb{Z}$. Now,

$$\begin{aligned}\tau^k = e &= \sigma^m \\ (\tau\sigma)^l &= e\end{aligned}$$

so $n|l$. $\square$