

# UNIVERSITY OF SOUTH CAROLINA

MATH 546 - Algebraic Structures I

Lecture Notes

## 1 Preliminaries

### 1.1 Notation

- $\ni$  is to be read as *such that*
- $\mathbb{N}$  - set of natural numbers  $\mathbb{N} = \{0, 1, 2, \dots\}$
- $\mathbb{Z}$  - set of integers  $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
- $\mathbb{Q}$  - set of rational numbers  $\mathbb{Q} = \{x/y \mid x \in \mathbb{Z} \wedge y \in \mathbb{N}\}$
- $\mathbb{R}$  - real numbers
- $\mathbb{C}$  - complex numbers
- $\mathbb{R}^* \equiv \mathbb{R} \setminus \{0\} = \{x : \exists x^{-1} \ni xx^{-1} = 1\}$  i.e. all reals with a multiplicative inverse
- $a \mid b$  is to be read as *a divides b*

### 1.2 Definitions

- For  $a, b \in \mathbb{Z}$  and  $a \neq 0$ : *a divides b* (or *b is divisible by a*)  $\iff \exists q \in \mathbb{Z} \ni aq = b$
- $p \in \mathbb{N} \setminus \{0, 1\}$  is *prime*  $\iff a \in \mathbb{N} \wedge a \mid p \Rightarrow a = p \wedge a = 1$
- greatest common divisor: For  $a, b \in \mathbb{Z}$  (both not 0):  $\gcd(a, b)$  is largest integer that divides both *a* and *b*
- $a, b \in \mathbb{Z}$  are *relatively prime*  $\iff \gcd(a, b) = 1$
- least common multiple:  $a, b \in \mathbb{Z}^* : \text{lcm}(a, b)$  is the smallest  $n \in \mathbb{N}$  such that  $(a \mid n) \wedge (b \mid n)$

### 1.3 Facts

Offered without proof:

**Theorem.** Fundamental Theorem of Arithmetic: every  $n \in \mathbb{N}^* \setminus \{1\}$  has a unique (up to order) prime factorization

**Lemma.** lcm and gcd are duals:

$$\text{lcm}(a, b) = \frac{ab}{\text{gcd}(a, b)}$$

**Lemma.** if  $p$  is prime and  $p \mid (ab)$  then  $(p \mid a) \vee (p \mid b)$

**Lemma.** if  $a$  and  $b$  are rel prime and  $a \mid bc$  then  $a \mid c$

**Lemma.** if  $d = \text{gcd}(a, b)$  then  $d = ja + kb$  for some  $j, k \in \mathbb{Z}$  (linear combo)

### 1.4 Euclid's Algorithm

#### 1.4.1 Finding gcd(a.b)

Assuming (wlog)  $a \leq b$  set  $r_0 = b$  and  $r_1 = a$  and iteratively compute  $r_{i+1} = (r_{i-1} \bmod r_i)$ . Then  $\text{gcd}(a, b) = r_i$  when  $r_{i+1} = 0$ .

#### 1.4.2 gcd(a.b) is a linear combo of a and b

The expression of  $\text{gcd}(a, b) = ja + kb$  is not unique. Values for  $j$  and  $k$  can be found by working the algorithm in 1.2.1 in reverse.

The algorithm can be expressed:

$$\begin{aligned} r_2 &= b - aq_1 = r_0 - r_1q_1 \\ r_3 &= a - r_2q_2 = r_1 - r_2q_2 \\ r_4 &= r_2 - r_3q_3 \\ &\dots \\ r_{i-1} &= r_{i-3} - r_{i-2}q_{i-2} \\ r_i &= r_{i-2} - r_{i-1}q_{i-1} \\ r_{i+1} &= r_{i-1} - r_iq_i = 0 \end{aligned}$$

Starting with the equation for  $r_i$  we substitute for the other  $r$ 's and repeat until only  $b = r_0$  and  $a = r_1$  and  $q$ 's are left. Combine terms and we have  $\gcd(a, b) = ja + kb$ .

## 2 Congruence Classes

### 2.1 Definitions

- For  $a, n \in \mathbb{Z}$  the congruence class  $[a]_n = \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\}$ .
- $b \equiv a \pmod{n} \iff n \mid (a - b)$  i.e.  $a$  and  $b$  have the same remainder when divided by  $n$
- $\mathbb{Z}_n = \{[a]_n\} = \{[0]_n, [1]_n, \dots, [n-1]_n\}$  a.k.a.  $\mathbb{Z}/n$
- and equivalence relation on a set  $S$  is a subset  $R \subseteq S \times S$  such that
  - $(a, b) \in R \implies (b, a) \in R$  (symmetric)
  - $(a, b) \in R \implies (a, a) \in R$  (reflexive)
  - $(a, b) \in R \wedge (b, c) \in R \implies (a, c) \in R$  (transitive)
- $|S|$  is the cardinality of set  $S$
- $[a]_n + [b]_n = [a + b]_n$  addition
- $[a]_n \cdot [b]_n = [a \cdot b]_n$  multiplication
- additive identity  $[0]_n$ , inverse  $[-a]_n$ 
  - $[0]_n + [a]_n = [a]_n$
  - $[a]_n + [-a]_n = [0]_n$
- multiplicative identity  $[1]_n$ , inverse  $([a]_n)^{-1}$  if it exists
  - $[1]_n \cdot [a]_n = [a]_n$
  - $[a]_n \cdot ([a]_n)^{-1} = [1]_n$
- $\mathbb{Z}_n^*$  is subset of  $\mathbb{Z}_n$  that have multiplicative inverses

## 2.2 Examples

- $[1]_2 = \{2k + 1 \mid k \in \mathbb{Z}\}$  i.e. odd integers
- $[0]_2 = \{2k \mid k \in \mathbb{Z}\}$  i.e. even integers
- $[3]_5 = \{\dots, -7, -2, 3, 8, \dots\} = \{5k + 3 \mid k \in \mathbb{Z}\}$
- $\mathbb{Z}_6^* = \{1, 5\}$
- $|\mathbb{Z}_n| = n$

## 2.3 Observations, Theorems and Lemmas

**Lemma.**  $[a]_n = [b]_n \iff b \in [a]_n$

**Lemma.**  $k \in \mathbb{Z}$  is in exactly one congruence class of  $\mathbb{Z}_n$

**Lemma.** the congruence classes of  $\mathbb{Z}_n$  partition  $\mathbb{Z}$  into  $n$  partitions

**Lemma.**  $([a]_n)^{-1}$  exists iff  $\gcd(a, n) = 1$

**Lemma.**  $([a]_n)^{-1} = [k]_n$  when  $ka + \ell n = 1$  (for  $k, \ell \in \mathbb{Z}$ )

## 3 Groups

### 3.1 Definition

A group  $(G; *)$  is a set  $G$  and a *binary* operation  $*$  with such that:

- Closure:  $\forall a, b \in G \Rightarrow (a * b) \in G$
- Identity:  $\exists e \in G$  such that  $\forall a \in G: e * a = a * e = a$
- Inverse:  $\forall a \in G \exists a^{-1}$  such that  $a * a^{-1} = a^{-1} * a = e$
- Associativity:  $\forall a, b, c \in G: a * (b * c) = (a * b) * c$

### 3.2 Notes and Observations

- Commutativity is *not* a requirement for a group
- a commutative group is called an *abelian* group.
- uniqueness of the identity and of inverses is *not* part of the definition
- there *are* non-commutative groups
- associativity can be assumed for multiplication, addition, composition of functions, matrix multiplication

### 3.3 Examples of Groups

- $(\mathbb{Z}; +)$
- $(\mathbb{Q}^*; \cdot)$
- $(\mathbb{R}; +)$
- $(\mathbb{Z}_2; +)$
- Invertable  $n \times n$  matrices under multiplication; this is a non-abelian group
- $(\mathbb{R} \setminus \{-1\}; *)$  where  $a * b = a + b + ab$ 
  - Show associativity by expanding each side of  $a * (b * c) \stackrel{?}{=} (a * b) * c$
  - Zero is clearly the identity.
  - Solve  $a + b + ab = 0$  for  $b$  to get  $b = a^{-1} = -a/(a + 1)$
  - Clearly  $(a + b + ab) \in \mathbb{R}$ : we need to show that  $(a + b + ab) \neq -1$  for all  $a$  and  $b$ : solve  $(a + b + ab) = -1$  for  $a$  and show  $a = -1$ .

### 3.4 Not Groups

- $(\mathbb{Z}; \cdot)$  – missing inverses
- $(\mathbb{Z} \setminus \{0\}; +)$  – no identity
- $(\mathbb{R}; -)$  – not associative

### 3.5 More ...

- $a, b \in (G; *)$ :  $(a * b)^{-1} = b^{-1} * a^{-1}$
- *Symmetric group*: for set  $S$  and  $(G; \circ)$  where  $G = \{f : S \mapsto S\}$  and  $f$  is a bijection (composition of functions)
- $e$  common notation for the identity
- $a^{-1}$  inverse of  $a$
- $(a^{-1})^{-1} = a$
- $a^n = a * a * a \cdots * a$  ( $n$ -times)
- $a^{-n} = (a^{-1})^n$
- $a^0 = e$
- $(a^n)^m = a^{nm}$
- $\forall a, b \in G \Rightarrow \exists! x \ni a * x = b \wedge \exists! y \ni y * a = b$

## 4 Multiplication (Cayley) Tables

### 4.1 For groups

We use row index times column index (order counts when non-ablian).

For  $(G; *)$  with  $G = \{e, a, b, \dots\}$

$*$	$e$	$a$	$b$	$c$	$\dots$
$e$	$e$	$a$	$b$	$c$	$\dots$
$a$	$a$				
$b$	$b$			$b * c$	
$c$	$c$				
$\vdots$	$\vdots$				

E.g.  $\mathbb{Z}_4$ :

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

## 4.2 Observations

Since  $\forall a, b \in G \exists! x \ni a * x = b$  we have

- Each row is unique, as is each column.
- An element  $x$  appears exactly once in each row or column
- An abelian (commutative) group is symmetric on the diagonal

## 4.3 Examples

### 4.3.1 2 element group

There is just one (up to isomorphism) and it's abelian:

*	$e$	$a$
$e$	$e$	$a$
$a$	$a$	$e$

Isomorphic to  $(\mathbb{Z}_2; +)$ ,  $(\{1, -1\}; \cdot)$

### 4.3.2 3 element group

Also unique and abelian:

*	$e$	$a$	$b$
$e$	$e$	$a$	$b$
$a$	$a$	$b$	$e$
$b$	$b$	$e$	$a$

There is only one way to fill in table with each element appearing exactly once in each row and column.

### 4.3.3 4 element groups

There are two up to relabeling (both abelian)

$*$	$e$	$a$	$b$	$c$	$*$	$e$	$a$	$b$	$c$
$e$	$e$	$a$	$b$	$c$	$e$	$e$	$a$	$b$	$c$
$a$	$a$	$b$	$c$	$e$	$a$	$a$	$e$	$c$	$b$
$b$	$b$	$c$	$e$	$a$	$b$	$b$	$c$	$e$	$a$
$c$	$c$	$e$	$a$	$b$	$c$	$c$	$b$	$a$	$e$

$\mathbb{Z}_4$  and Klein-4 group respectively.

### 4.3.4 5 element group

Just one:  $\mathbb{Z}_5$  also abelian.

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[0]$	$[1]$	$[2]$	$[3]$

## 5 Order of Groups and Elements

### 5.1 Definition and Notation

- The order of a group  $|G|$  is the number of elements in  $G$ .
- The order of  $a \in G$ :  $o(a)$  is the smallest positive integer  $n$  such that  $a^n = e$ .
- $o(a) = \infty$  if no such  $n$ .
- $\forall a \in G \setminus \{e\} : o(a) \geq 2$  i.e. only the identity has order 1
- The set generated by  $a \in G$  is  $\langle a \rangle = \{x \in G : x = a^n, n \in \mathbb{Z}\}$   
I.e.  $\langle a \rangle = \{a^0, a^1, \dots, a^n, a^{n+1}, \dots\}$
- $|\langle a \rangle| = o(a)$



## 5.2 Examples

- $G = \mathbb{Z}_{60}$  then  $|G| = 60$  and  $o([8]) = n$  where  $n \cdot 8 = 60k$  or  $2n = 15k$  so  $15 \mid 2n$  and  $\gcd(15, 2) = 1 \Rightarrow n = 15$
- $(\mathbb{R}^*, \cdot) : o(1) = 1, o(-1) = 2, o(x \notin \{1, -1\}) = \infty$

## 5.3 Theorems

For finite group  $G$ :

**Theorem.** Let  $N = |G| \in \mathbb{N}$  then  $x^N = e \iff o(x) \mid N$

*Proof.* Let  $n = o(x)$  then  $0 < n \leq N$

$$\Leftarrow n \mid N \Rightarrow \exists k \ni nk = N \Rightarrow x^N = x^{nk} = (x^n)^k = e^k = e$$

$\Rightarrow$  Suppose  $x^N = e$  and  $n$  does not divide  $N$ . Then

$\exists p, r \in \mathbb{N} \ni N = qn + r$  with  $0 < r < n$  and so

$$e = x^N = x^{qn+r} = x^{qn}x^r = x^r.$$

Therefore  $o(x) = r$ ; a contradiction.

□

**Lemma.** Let  $N = |G| \in \mathbb{N}$  and  $n = o(x)$  then  $x^k = x^\ell \iff n \mid (k - \ell)$ .

*Proof.*  $x^k = x^\ell \iff x^k x^{-\ell} = x^\ell x^{-\ell} \iff x^{k-\ell} = e$  and use previous theorem with  $N = k - \ell$  and  $o(x) = n$ . □

**Lemma.**  $o(a) = |\langle a \rangle|$

## 6 Subgroups

**Definition.** For group  $G$  and  $H \subseteq G$ .  $H$  is a *subgroup* of  $G \iff H$  satisfies the requirements of a group. We say  $H \leq G$ .

Exanples:

- $2\mathbb{Z} \leq \mathbb{Z}$
- $G \leq G$  trivially
- $\{e\} \leq G$  trivially
- $a \in G \Rightarrow \langle a \rangle \leq G$

**Definition.**  $\langle a \rangle$  for  $a \in G$  is the *cyclic subgroup* of  $G$  generated by  $a$ .

**Definition.** A group  $G$  is *cyclic*  $\iff \exists a \in G \ni \langle a \rangle = G$ .

To show that  $H$  is a subgroup  $G$  associativity is inherited. And so is the existence of the identity and inverses but their inclusion in  $H$  must be shown. Closure must be shown.

The one step verification:

**Theorem.** For  $(G; *)$  and  $H \subseteq G$ ,  $H$  is a subgroup of  $G$  ( $H \leq G$ ) iff  $a, b \in H \Rightarrow a * b^{-1} \in H$ .

*Proof.* Let  $a, b \in H$ .

$\Rightarrow$  Since  $H$  is a group:  $b \in H \Rightarrow b^{-1} \in H \Rightarrow a * b^{-1} \in H$

$\Leftarrow$  Associativity: inherited from  $G$

Identity:  $a * a^{-1} = e \Rightarrow e \in H$ .

Inverses:  $a \in H \Rightarrow e * a^{-1} = a^{-1} \in H$ .

Closure:  $e, a, b \in H \Rightarrow eb^{-1} = b^{-1} \in H \Rightarrow a * (b^{-1})^{-1} = a * b \in H$ .

□

## 6.1 Cyclic Subgroups

**Lemma.** For group  $G$  and  $a \in G$  then  $\langle a \rangle = \{a^0, a^1, a^2, \dots\}$  is a subgroup of  $G$ .

Example: For  $\mathbb{Z}_{10}$ :

$$\langle [0] \rangle = \{0\}$$

$$\langle [1] \rangle = \mathbb{Z}_{10} \text{ and}$$

$$\langle [2] \rangle = \{[0], [2], [4], [6], [8]\}$$

**Lemma.**  $\langle [a]_n \rangle = \mathbb{Z}_n \iff \gcd(a, n) = 1$

**Lemma.** Every cyclic subgroup is abelian.

Cyclic?:

$$(\mathbb{Z}_n; +): \text{ yes } \langle [1]_n \rangle$$

$$(\mathbb{Z}; +): \text{ yes } \langle 1 \rangle$$

$$\text{GL}_2(\mathbb{R}): \text{ no}$$

$$\mathbb{R}^*: \text{ no}$$

$$\mathbb{Z}_8^*: \text{ no: } \mathbb{Z}_8^* = \{[1], [3], [5], [7]\} \text{ and } \forall x \in \mathbb{Z}_8^* : x^2 = [1]$$

**Theorem.** Let  $G$  be a group with  $|G| = n$ .  $G$  is cyclic  $\iff \exists x \in G \ni o(x) = n$ .

## 6.2 Subgroups of $\mathbb{Z}$

**Theorem.** Every subgroup of the additive group  $(\mathbb{Z}; +)$  is cyclic.

*Proof.* Let  $H$  be a subgroup of  $\mathbb{Z}$ .

**Case 1:** If  $H = \{0\}$ , then  $H$  is cyclic, since  $H = \langle 0 \rangle$ .

**Case 2:** Suppose  $H \neq \{0\}$ . Then  $H$  contains some nonzero integer. Let  $n$  be the smallest positive integer in  $H$ .

**Step 1:**  $n\mathbb{Z} \subseteq H$ . Since  $n \in H$  and  $H$  is a subgroup, for all integers  $k$ ,  $kn \in H$ . Hence  $n\mathbb{Z} \subseteq H$ .

**Step 2:**  $H \subseteq n\mathbb{Z}$ . Take any  $h \in H$ . By the division algorithm, there exist integers  $q, r$  with

$$h = qn + r, \quad 0 \leq r < n.$$

Because  $qn \in n\mathbb{Z} \subseteq H$  and  $h \in H$ , their difference

$$r = h - qn$$

also lies in  $H$ . But  $r \in H$  and  $r < n$ . By the minimality of  $n$ , we must have  $r = 0$ . Thus  $h = qn \in n\mathbb{Z}$ .

**Step 3:** Combining the inclusions, we have

$$H = n\mathbb{Z} = \langle n \rangle.$$

Therefore,  $H$  is cyclic. □

**Lemma.** Every subgroup of a cyclic group is cyclic.

*Proof.* Same argument using exponents. □

**Definition.** The *join* of two subgroups  $H \leq G$  and  $K \leq G$  is

$$HK = \{hk : h \in H, k \in K\}$$

.

**Theorem.** If  $G$  is abelian with  $H \leq G$  and  $K \leq G$  then  $HK \leq G$ . I.e.  $HK$  is also a subgroup of  $G$ .

*Proof.* For  $h, h_1, h_2 \in H$  and  $k, k_1, k_2 \in K$

Associativity: inherited from  $G$ .

Identity:  $e \in H \wedge e \in K \Rightarrow ee = e \in HK$

Inverses:  $(hk)^{-1} = k^{-1}h^{-1} = h^{-1}k^{-1} \in HK$  since  $h^{-1} \in H \wedge k^{-1} \in K$

Closure:  $(h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2$   
 $= h_1(h_2k_1)k_2$   
 $= (h_1h_2)(k_1k_2)$   
 $\in HK$  since both  $H$  and  $K$  are closed

□

### 6.3 Subgroups of $\mathbb{Z}_n$

$\mathbb{Z}_n$  is cyclic, therefore so is  $H \leq \mathbb{Z}_n$

**Theorem.** If  $H \leq \mathbb{Z}_n$  then  $k = |H|$  divides  $n = |\mathbb{Z}_n|$

*Proof.*  $\mathbb{Z}_n = \langle [1] \rangle$  and  $H = \langle [h] \rangle$  for some  $0 \leq h < n$  but  $n[h] = [hn] = h[n] = h[0] = [0]$  so  $k = o([h])$  divides  $n$ . (See first lemma in 5.3). □

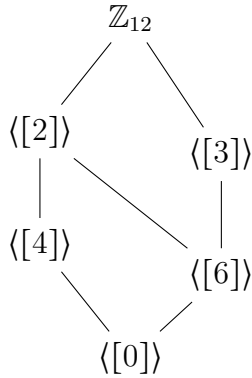
**Theorem.** If  $d \mid n$  then  $\exists H \leq \mathbb{Z}_n \ni |H| = d$ .

*Proof.* Consider  $H = \langle [k] \rangle$  where  $k \mid d \mid n$  and  $0 < k \leq n$ . Then  $H = \{[0], [k], 2[k], \dots, (d-1)[k]\}$  and  $|H| = d$  □

### 6.4 Subgroup Lattice Diagram

Also called Hasse diagram. This is a lattice with the group at the top and subgroups below with connections showing inclusion.

E.g. for  $\mathbb{Z}_{12}$ :



### 6.5 Joins

**Definition.** The *join* of subgroups  $H \leq G$  and  $K \leq G$  is the set  $HK = \{hk : h \in H \wedge k \in K\}$

Not all joins of subgroups are subgroups.

**Lemma.** If  $G$  is abelian then so is  $HK$  for  $H \leq G$  and  $K \leq G$ . And  $HK$  is a subgroup.

## 7 Direct Product of Groups

**Definition.** For groups  $G_1, G_2$  the *direct product* of  $(G_1; \bullet)$  and  $(G_2; *)$  is

$$G_1 \times G_2 = \{(g_1, g_2) : g_1 \in G_1 \wedge g_2 \in G_2\}$$

with

$$(a_1, a_2)(b_1, b_2) = (a_1 \bullet a_2, b_1 * b_2)$$

Think cartesian product.

**Lemma.**  $G_1 \times G_2$  is a group.

**Lemma.**  $o(G_1 \times G_2) = o(G_1)o(G_2)$

**Lemma.**  $G_1 \times G_2$  is abelian iff both  $G_1$  and  $G_2$  are abelian.

**Lemma.** If  $(g_1, g_2) \in G_1 \times G_2$  then  $o((g_1, g_2)) = \text{lcm}(o(g_1), o(g_2))$ .

**Theorem.** If  $G_1 \times G_2$  is cyclic then  $G_1, G_2$  are both cyclic.

*Proof.* Let  $(g_1, g_2)$  be a generator of  $G_1 \times G_2$  and consider  $a_1 \in G_1$  an arbitrary element of  $G_1$ . Then  $(a_1, e_2) \in G_1 \times G_2$  implies that  $(a_1, e_2) = (g_1, g_2)^n = (g_1^n, g_2^n)$  for some integer  $n$  and therefore  $a_1 = g_1^n$ . Since  $a_1$  is arbitrary,  $\langle g_1 \rangle = G_1$  and  $g_1$  is a generator of  $G_1$ . Similarly for  $g_2 \in G_2$ .  $\square$

But not conversely: consider  $\mathbb{Z}_2 \times \mathbb{Z}_4$ .

**Lemma.** If  $G_1, G_2$  are both cyclic and  $\gcd(|G_1|, |G_2|) = 1$  then  $G_1 \times G_2$  is cyclic.

**Lemma.** If  $H_1 \leq G_1$  and  $H_2 \leq G_2$  then  $H_1 \times H_2 \leq G_1 \times G_2$ .

All such products of subgroups do not necessarily produce all subgroups of the product. E.g.  $H = \langle (a, a) \rangle \leq \mathbb{Z} \times \mathbb{Z}$  is cannot be the product of subgroups of  $\mathbb{Z}$

## 8 Lagrange's Theorem

To be proved later: needs cosets.

**Theorem.** If  $H \leq G$  then  $|H| \mid |G|$ .

**Corollary.**  $g \in G \Rightarrow g^{|G|} = e$

*Proof.* Consider  $g \in G$  with  $n = |G|$  and  $k = |\langle g \rangle|$  then by Lagrange's theorem  $k \mid n$  and therefore  $n = km$  for some  $0 < m \leq n$ . And so  $g^n = g^{km} = (g^k)^m = e^m = e$ .  $\square$

**Lemma.** If  $|G| = p$  for a prime  $p$  and  $g \in G$ :  $o(g) = 1$  or  $o(g) = p$ .

**Definition.** Euler's Totient Function (a.k.a. Euler's Phi) for  $n \in \mathbb{Z}^+$  is  $\varphi(n) = |\{k \in \mathbb{Z} : 1 \leq k \leq n \wedge \gcd(k, n) = 1\}|$ .

In other words  $\varphi(n)$  is the number of positive integers less than  $n$  and coprime to  $n$ .

E.g.:

$$\varphi(4) = 2 = |\{1, 3\}|$$

$$\varphi(12) = 4 = |\{1, 5, 7, 11\}|$$

$$\varphi(23) = 22 = |\{1, 2, \dots, 21, 22\}|$$

**Lemma.** If  $p$  is prime  $\varphi(p) = p - 1$

**Corollary.** For positive integers  $a, n \ni \gcd(a, n) = 1$  then

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

.

*Proof.*  $\mathbb{Z}_n^* = \{[a]_n : \gcd(a, n) = 1\}$  and so  $\varphi(n) = |\mathbb{Z}_n^*|$  and therefore  $[a]^{\varphi(n)} = [1]$  or  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .  $\square$

## 9 Permutations

**Definition.** For  $N = \{1, 2, 3, \dots, n\}$ ,  $S_n = \{\sigma : N \mapsto N, \sigma \text{ is a bijection}\}$ . I.e.  $S_n$  is the set of all invertible functions from  $\{1, 2, 3, \dots, n\}$  onto itself. Each such function is a *permutation*. The elements of  $S_n$  form a group under composition with  $|S_n| = n!$ .

## 9.1 Two-Line Notation

The two-line notation describes a permutation with the top row being  $N$  and the bottom its image under the permutation. E.g. for  $S_3$  the function  $\sigma$  that maps 1 to 2, 2 to 3 and 3 to 1 is

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

E.g:

$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$$

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

The convention is that the top row is in order. Inverse of an element is found by switch top and bottom rows and reordering. The identity has top and bottom the same.

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} : 1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 3$$

Apply right to left (i.e. function composition):

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

## 9.2 Cycle Notation

This is a single line notation where each element maps to the neighbor on the right and that last maps to the first. By convention the lowest element is listed first. E.g:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = (1 \ 3 \ 4 \ 2)$$

Any element not in the cycle maps to itself. The identity maybe written as a single cycle (1) or the empty cycle ( ). The inverse of a cycle is the cycle reversed.



Disjoint cycles commute. Any permutation can be written as a composition of disjoint cycles. E.g.:

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

The order of a cycle is its length. The order of the composition of disjoint cycles is the lcm of the lengths.

E.g:

$S_2 = \{(1), (1, 2)\}$  i.e. the identity and swapping 1 and 2

$S_3 = \{(1), (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2)\}$

$S_4 = \{(1),$   
 $(1 \ 2), (1 \ 3), (1 \ 4), (2 \ 3), (2 \ 4), (3 \ 4),$   
 $(1 \ 2)(3 \ 4), (1 \ 3)(2 \ 4), (1 \ 4)(2 \ 3)$   
 $(1 \ 2 \ 3), (1 \ 3 \ 2), (1 \ 2 \ 4), (1 \ 4 \ 2),$   
 $(1 \ 3 \ 4), (1 \ 4 \ 3), (2 \ 3 \ 4), (2 \ 4 \ 3),$   
 $(1 \ 2 \ 3 \ 4), (1 \ 2 \ 4 \ 3), (1 \ 3 \ 2 \ 4), (1 \ 3 \ 4 \ 2), (1 \ 4 \ 2 \ 3), (1 \ 4 \ 3 \ 2)\}$

$S_4$  has one element of order 1. And 9 elements of order 2: 6 single cycle and 3 2-cycle elements. There are 8 single cycle elements of order 3 and 6 of order 4.

### 9.3 Transpositions

**Definition.** A transposition is a permutation cycle of length 2. It is the exchange of 2 elements.

Every cycle can be decomposed into a sequence of transpositions. One algorithm is to take the last element and pair it with each of the previous elements in reverse order. E.g.:  $(1 \ 3 \ 6 \ 5 \ 2) \rightarrow (2 \ 5)(2 \ 6)(2 \ 3)(2 \ 1)$ . So any permutation can be decomposed into a sequence of transpositions.

**Definition.** A permutation is even if a decomposition into transpositions has an even number of cycles. A permutation is odd if a decomposition into transpositions has an odd number of cycles.

Any decomposition of a particular permutation will always be even or odd. *Not proven here.* A cycle of length  $n$  decomposes into  $n - 1$  transpositions.

## 9.4 The Alternating Group $A_n$

**Definition.** The set of all even permutations in  $S_n$  is the *alternating (sub)group* designated  $A_n$ .

E.g:  $A_3 = \{(), (1\ 2\ 3), (1\ 3\ 2)\} = \langle (1\ 2\ 3) \rangle = \langle (2\ 3)(1\ 3) \rangle$ .

**Theorem.**  $A_n$  is a subgroup of  $S_n$ .

*Proof.* Associativity and identity are inherited. Let  $\sigma \in A_n$ , then  $\sigma = \tau_1\tau_2\cdots\tau_n$  for  $n$  transpositions  $\tau_i$  and  $\sigma^{-1} = \tau_n^{-1}\tau_{n-1}^{-1}\cdots\tau_1^{-1} = \tau_n\tau_{n-1}\cdots\tau_1$ . For closure, if  $\alpha, \beta \in A_n$  then each has decomposition into an even number of transpositions. Composing,  $\alpha\beta$  has a decomposition into  $\alpha$ 's transpositions followed by  $\beta$ 's which is still an even number of transpositions and  $\alpha\beta \in A_n$ .  $\square$

**Theorem.**  $|S_n| = 2 |A_n|$

*Proof.* Let  $O_n$  be the set of odd permutations in  $S_n$ . Let  $F : A_n \mapsto O_n$  where  $F(\sigma) = \sigma (1\ 2)$  and so  $F^{-1} : O_n \mapsto A_n$  is its inverse where  $F^{-1}(\alpha) = \alpha (1\ 2)$ .  $F^{-1}(F(\sigma)) = \sigma (1\ 2) (1\ 2) = \sigma$ . Likewise we have  $F(F^{-1}(\alpha)) = \alpha (1\ 2) (1\ 2) = \alpha$ . So  $F$  is a bijection and  $|A_n| = |O_n|$ . Since  $S_n = A_n \cup O_n$  and  $A_n \cap O_n = \emptyset$  then  $|S_n| = |A_n| + |O_n| = 2|A_n|$ .  $\square$

## 9.5 Decomposition Types and the Order of Permutations

A permutation can be characterized by its decomposition into disjoint cycles and the lengths of those cycles.

$S_4$  can have permutations with single cycles of length 2, 3, or 4. And double cycles of length 2 and 2. But not triple cycles. So  $A_4$  will contain the single cycles of lengths 1 or 3, these being the even permutations. As well as the double cycles of lengths 2, both odd so the permutation is even:

$$A_4 = \{(), (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 2), (1\ 3\ 4), (1\ 4\ 2), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

The classification of types on  $S_n$  comes down to the ways  $n$  can be composed of sums of positive integers.

For  $S_4$  we have sums: 4, 3+1, 2+2, 2+1+1, and 1+1+1+1. Ignoring the cycles of length 1 the types are (4), (3), (2,2), and (2). The type is the number of cycles and their individual lengths.

The order of a permutation is the lcm of the lengths of its disjoint cycles. The parity of a cycle is even if its length is odd and the parity is odd if its length is even (since the number of transpositions needed to compose a cycle is one less than its length).

The even permutations of  $S_4$  are the identity and those of type (3) or (2,2) with orders of 3 and 2 respectively. These make up the elements of  $A_4$ .

## 9.6 The Dihedral Group $D_n$

This is the group of symmetries of a regular  $n$ -gon (n-sided polygon with equal length sides).

These polygons can be inscribed in a circle with the  $n$  vertices equally spaced on the circle.

$D_n$  is a subgroup of  $S_n$ : think of it as a restricted set of permutations of the vertices on the  $n$ -gon.

### 9.6.1 More formally ...

**Definition.** A *metric* on a space  $M$  is a function  $d : M \times M \mapsto \mathbb{R}$  such that:

$\forall x, y, z \in M :$

$$\begin{aligned} d(x, x) &= 0 \\ d(x, y) &= d(y, x) \\ d(x, y) &> 0 \text{ for } x \neq y \\ d(x, z) &\leq d(x, y) + d(y, z) \end{aligned}$$

**Definition.** An *isometry* is a map from one space to another such that distances are preserved. I.e. for spaces  $M_1, M_2$  with metrics  $d_1, d_2$  we say  $\phi : M_1 \mapsto M_2$  is an isometry iff  $\forall a, b \in M_1 : d_1(a, b) = d_2(\phi(a), \phi(b))$ .

**Definition.** A *symmetry* is an isometry of an object onto itself.

In the case of  $D_n$ , symmetries of regular  $n$ -gons, we are sticking with subsets of  $\mathbb{R}^2$  with the usual Euclidean metric. The subset being the  $n$ -gon itself. The  $D_n$  group will have  $n$  rotations (including the identity of a zero rotation) and  $n$  reflections. There are  $2n$  elements in  $D_n$ .

Each rotation has order  $n$  and each reflection has order 2.

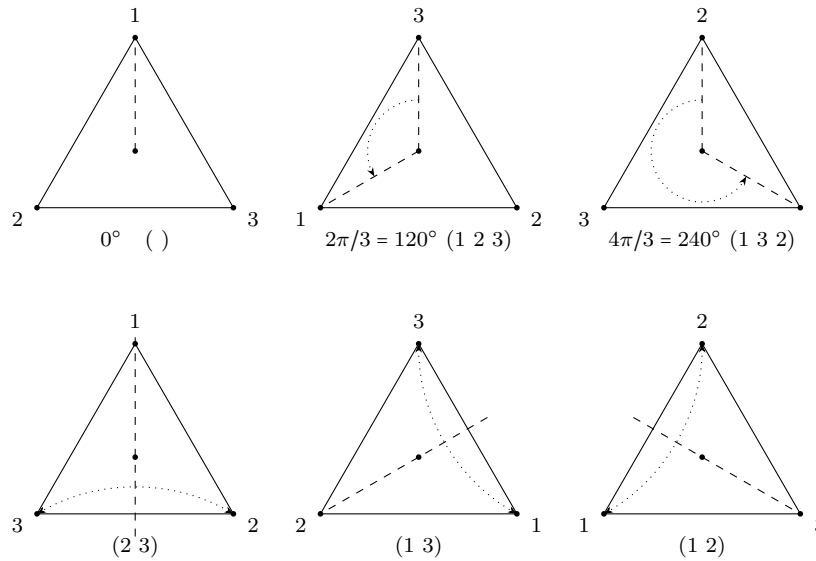
### 9.6.2 $D_1, D_2$ Trivial Symmetries of a Point and of a Line Segment

$D_1$  has but one element, the identity.  $D_2$  is the group of symmetries of a line segment. It has 2 elements: the identity and the interchange of the end points:  $D_2 = \{(), (1\ 2)\} = S_2$ .

### 9.6.3 $D_3$ Symmetries of the Triangle

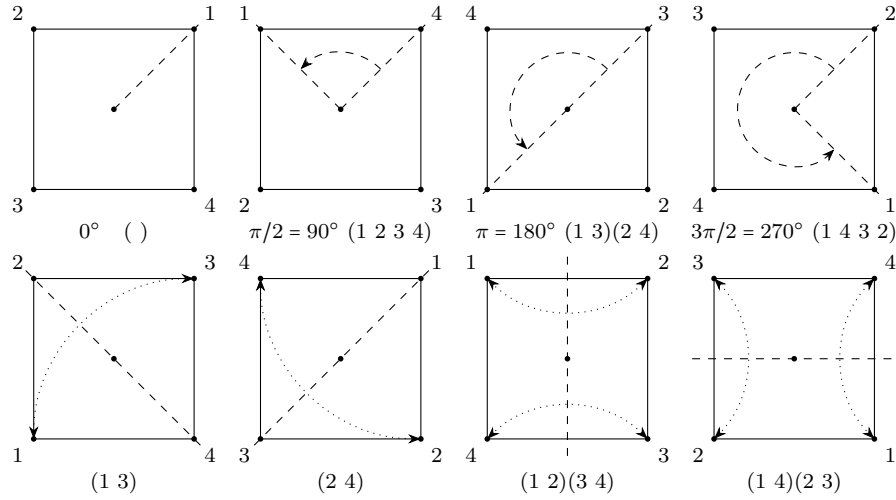
This is the simplest non-trivial dihedral group and it is the same as  $S_3$ . Rotations are through integral multiples of  $2\pi/3 = 120^\circ$  and reflections interchange a pair of vertices:

$$D_3 = \{(), (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2\ 3)\} = S_3$$



### 9.6.4 $D_4$ Symmetries of the Square

This is smallest  $D_n$  that is a proper subgroup of  $S_n$ . Rotations are through integral multiples of  $\pi/2 = 90^\circ$  and reflections interchange 2 pairs of vertices:  $D_4 = \{(), (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2), (1\ 3), (2\ 4), (1\ 2)(3\ 4), (1\ 4)(2\ 3)\}$



There are an even number of vertices and so the axes of reflection symmetry pass through opposite vertices and through the mid-points of opposite sides:

### 9.6.5 $D_5$ Symmetries of the Pentagon

The permutations in  $S_5$  that make up  $D_5$  are:

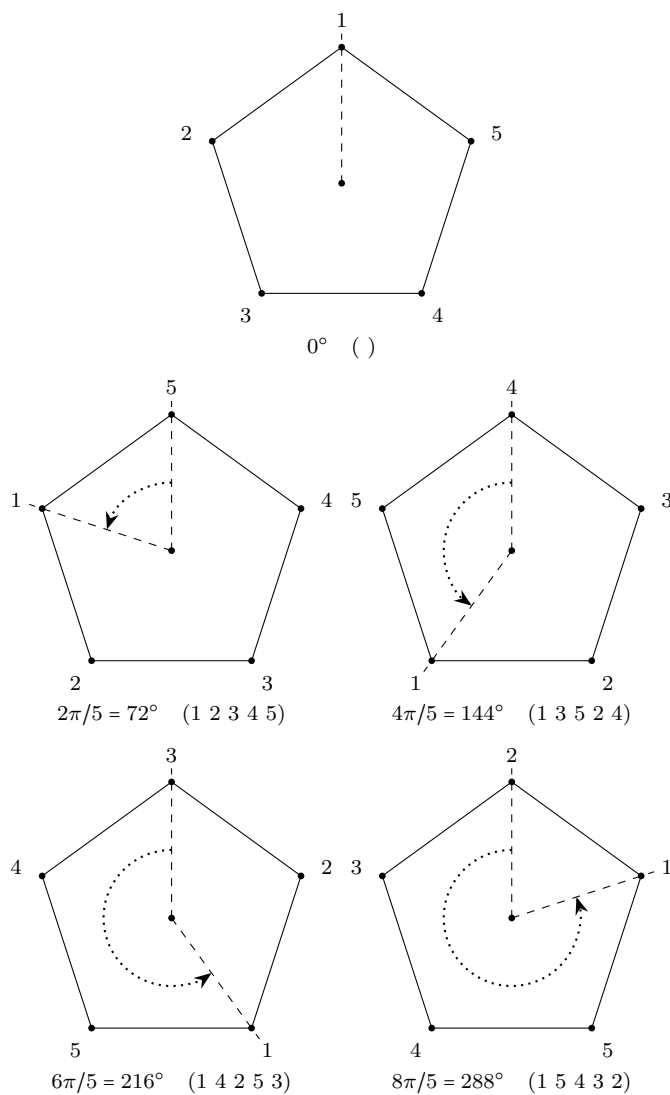
$$D_5 = \{(), (1\ 2\ 3\ 4\ 5), (1\ 3\ 5\ 2\ 4), (1\ 4\ 2\ 5\ 3), (1\ 5\ 4\ 3\ 2), (2\ 5)(3\ 4), (1\ 3)(4\ 5), (1\ 5)(2\ 4), (1\ 2)(3\ 5), (1\ 4)(2\ 3)\}$$

The five rotations move the vertices and integral multiple of  $2\pi/5$  around the circumcenter of the pentagon. Note that the order of the vertices is unchanged. These are in the top row above.

The reflections transpose the pentagon around a line of symmetry through a vertex and the mid-point opposite. This could also be considered a 3-D flip around the axis of symmetry. Reflections interchange 2 pairs of vertices.

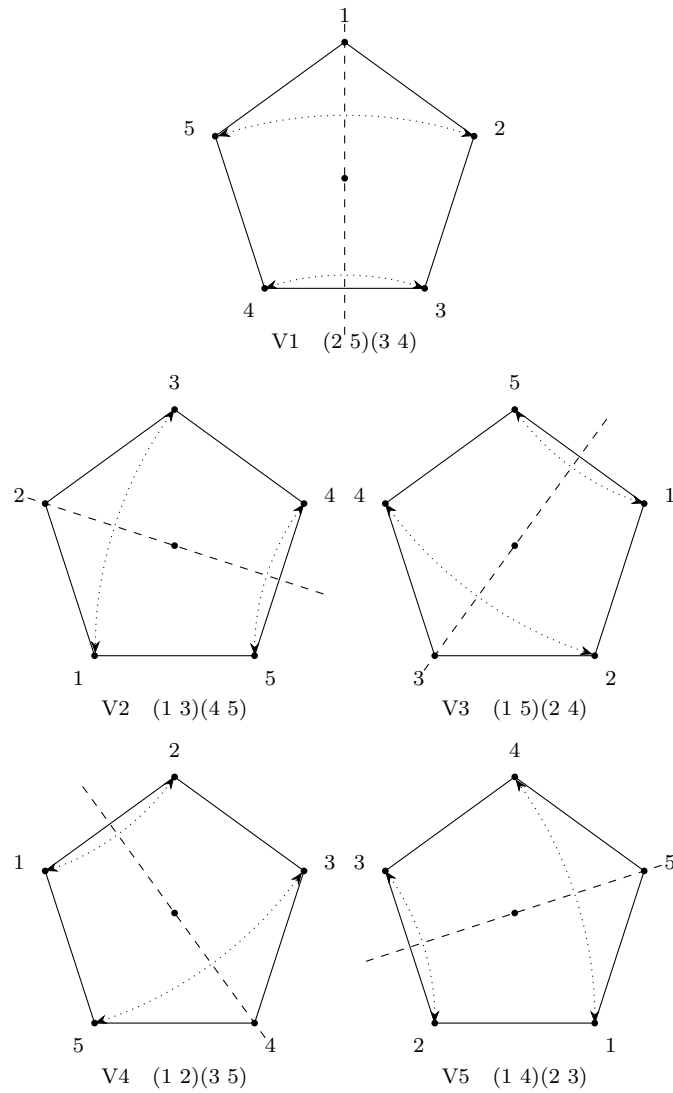
### Rotations:

Each rotation symmetry of a pentagon take it through an integral multiple of  $2\pi/5 = 72^\circ$ . Below are the 5 rotation symmetries.



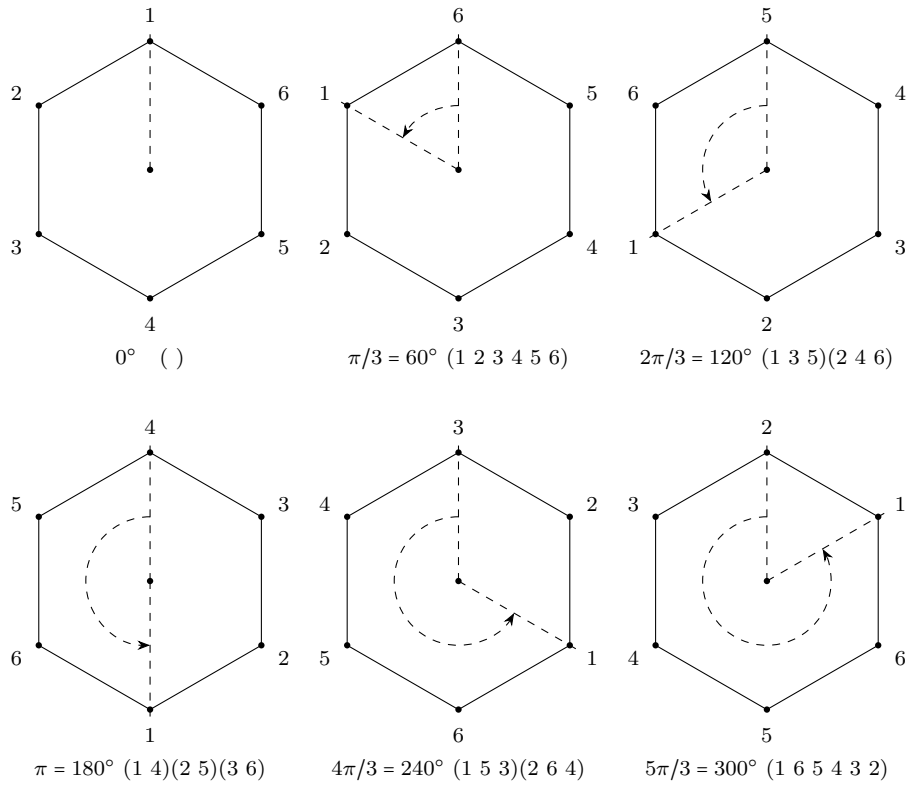
### Reflections:

The reflection symmetries of the pentagon are defined by a line of reflection through a vertex and the mid-point of the side opposite. In the figure below each is labeled with that vertex and the corresponding permutation element of  $S_5$ . The interchanged vertices are connected by the arc.



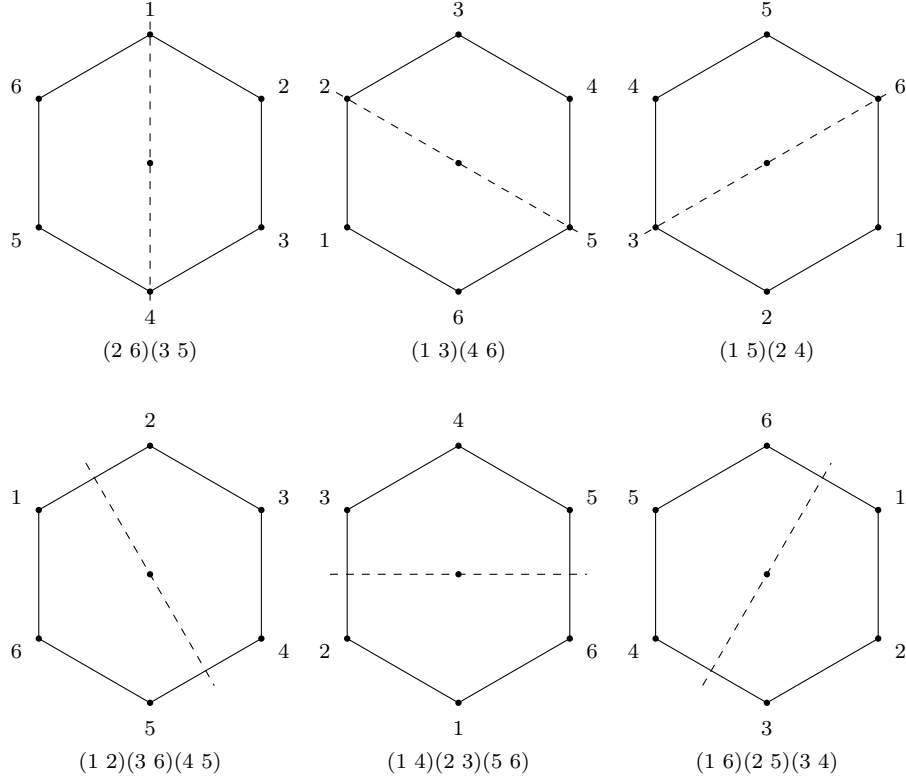
### 9.6.6 Symmetries of the Hexagon

Rotations:





## Reflections



## 9.7 Generators of $D_n$

Let  $r$  be the rotation of  $2\pi/n$  and  $s$  be the reflection about the axis of symmetry through vertex 1. Then

$$D_n = \{e, r, r^2, \dots, r^{n-1}, s, sr^2, \dots, sr^{n-1}\}$$

and

$$\begin{aligned} r^n &= e \\ s^2 &= e \\ sr &= r^{-1}s = r^{n-1}s \end{aligned}$$

and from these we can get the whole Cayley table.

## 9.8 Subgroups of $D_4$

There is one subgroup of order 1:  $\{e\}$ .

There are 5 subgroups of order 2:  $\{e, r^2\}, \{e, s\}, \{e, rs\}, \{e, r^2s\}, \{e, r^3s\}$

There are no subgroups of 3, 5, 6, or 7 since they do not divide 8.

There are 3 subgroups of order 3:  $\{e, r, r^2, r^3\}, \{e, r^2, s, r^2s\}, \{e, r^2, rs, r^3s\}$

There is one subgroup of order 8:  $D_4$

## 10 Isomorphisms

**Definition.** A *homomorphism* is a map  $f : (G; \cdot) \mapsto (H; *)$  such that  $\forall g_1, g_2 \in G : f(g_1 \cdot g_2) = f(g_1) * f(g_2)$ .

**Definition.** An *isomorphism* is a bijective homomorphism.

If there is an isomorphism between two groups  $G, H$  they are said to be *isomorphic*:  $G \cong H$ .

### 10.1 Examples

All groups of order 2 are isomorphic to  $\mathbb{Z}_2$ .

All groups of order 3 are isomorphic to  $\mathbb{Z}_3$ .

A group of order 4 is isomorphic to either  $\mathbb{Z}_4$  or to  $\mathbb{Z}_2 \times \mathbb{Z}_2$

All cyclic groups of order  $n$  are isomorphic to  $\mathbb{Z}_n$ .

A group,  $G$ , of order 5 is isomorphic to  $\mathbb{Z}_5$  since 5 is prime and there  $G$  is cyclic.

A group of order 6 is isomorphic to either  $\mathbb{Z}_6$  or  $S_3$ .

Every finite abelian group is isomorphic to some direct product of  $\mathbb{Z}_n$ 's.

Another one:

$$\mathbb{C}^* \cong G = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in GL_2 \right\}$$