

Criterion for Being Abelian^a

Lemma 109 *A group G is abelian if and only if for all $a, b \in G$, $(a \circ b)^{-1} = a^{-1} \circ b^{-1}$.*

- If (G, \circ) is abelian, then
$$(a \circ b)^{-1} = (b \circ a)^{-1} = a^{-1} \circ b^{-1}.$$
^b
- If $(a \circ b)^{-1} = a^{-1} \circ b^{-1}$, then $a \circ b = ((a \circ b)^{-1})^{-1} = (a^{-1} \circ b^{-1})^{-1} = (b^{-1})^{-1} \circ (a^{-1})^{-1} = b \circ a$.

^aContrast it with Lemma 100 (p. 766).

^bRecall p. 808.

Cyclic Groups

- A group G is called **cyclic** if there is an element $x \in G$ such that for each $a \in G$, $a = x^n$ for some $n \in \mathbb{Z}$.
- In other words,

$$G = \{ x^k : k \in \mathbb{Z} \}.$$

- G is said to be **generated** by x , denoted by

$$G = \langle x \rangle.$$

- This x is called a **generator**, **primitive root**, or **primitive element**.^a

^aPaolo Ruffini (1765–1822).

\mathbb{Z}_{14}^* Is a Cyclic Group

- First,

$$\mathbb{Z}_{14}^* = \{1, 3, 5, 9, 11, 13\}.$$

- Second, we knew (\mathbb{Z}_n^*, \times) is a group.^a
- Finally, 3 is a generator because

$$\{3^k \bmod 14 : k \in \mathbb{Z}\} = \mathbb{Z}_{14}^*.$$

^aRecall p. 803.

Cyclic Groups Are Abelian

Lemma 110 *Every cyclic group is abelian.*

- Let $x, y \in G = \langle g \rangle$, a cyclic group.
- Let $x = g^m$ and $y = g^n$ for some $m, n \in \mathbb{Z}$.
- Now,

$$x \circ y = g^m \circ g^n = g^{m+n} = g^{n+m} = g^n \circ g^m = y \circ x.$$

Orders^a of Groups and Group Elements

- For every group G , the number of elements in G is called the **order** of G , denoted by $|G|$.
- The **order** of $a \in G$, written $o(a)$, is the least *positive* integer n such that

$$a^n = e.$$

- If a finite n does not exist, a has infinite order.

^aRuffini (1799).

The Group $(\mathbb{Z}_n, +)$, $n > 1$

- Under ordinary $+$ modulo n , $(\mathbb{Z}_n, +)$ is an additive abelian group for any $n > 1$.^a
- Its order is n .
- Its generator is 1.
 - Every $i \in \mathbb{Z}_n$ can be expressed as

$$\overbrace{1 + 1 + \cdots + 1}^i.$$

^aRecall p. 802.

Orders of Group Elements

Lemma 111 *If x 's order is n and $x^k = e$, then $n \mid k$.*

- Assume otherwise and $k = qn + r$, where $0 < r < n$.
- So

$$e = x^k = x^{qn+r} = x^{qn} \circ x^r = x^r.$$

- So x 's order is at most $r < n$, a contradiction.

Finiteness of Orders of Groups and Group Elements^a

Lemma 112 *If G is a finite group, then the order of every element $a \in G$ must be finite.*

- Consider the chain $a^1, a^2, a^3, \dots \in G$.
- Because G is finite, the chain must eventually repeat itself.
- So there must be distinct $i < j$ such that $a^i = a^j$.
- Then $e = a^{j-i}$ by Lemma 106 (p. 811).
- As a result, a 's order is at most $j - i$, which is finite.

^aContributed by Mr. Bao (B90902039) on December 23, 2002.

Criterion for Being a Subgroup: The Finite Case

Corollary 113 *Let H be a nonempty subset of a finite group (G, \circ) . Then H is a subgroup of G if and only if for all $a, b \in H$, $a \circ b \in H$ (closure).*

- By Theorem 107 (p. 813), we only need to prove the closure property implies $a^{-1} \in H$ for all $a \in H$ (inverse).
- Let $a \in H$.
- Then $a^m = e$ for some $m \in \mathbb{Z}$ by Lemma 112 (p. 824).
- Hence $a^{-1} = a^{m-1} \in H$.
 - This is because $a \circ a^{m-1} = a^m = e$.

Remarks

- Corollary 113 may not hold for *infinite* groups.
- For example, $(\mathbb{Z}, +)$ is a group.^a
- Its subset $(\mathbb{N}, +)$ is closed under $+$.
- But $(\mathbb{N}, +)$ is *not* a subgroup of $(\mathbb{Z}, +)$!^b

^aRecall p. 801.

^bRecall p. 801 again.

Cyclic Subgroups

Lemma 114 *Let (G, \circ) be a group and $a \in G$. Then $H = (\{a^k : k \in \mathbb{Z}\}, \circ)$ is a subgroup of G and $H = \langle a \rangle$.*

- For $a^i, a^j \in H$, we have

$$a^i \circ a^{-j} = a^{i-j} \in H$$

by Lemma 106 (p. 811).

- Theorem 108 (p. 815) then implies the lemma.

Cyclic Subsets of *Finite* Groups

Lemma 115 Suppose (G, \circ) is a finite group and $a \in G$. (1) $\{a^k : k \in \mathbb{Z}\} = \{a^k : k \in \mathbb{Z}^+\}$. (2) $|\{a^k : k \in \mathbb{Z}\}| = o(a)$.

- The set $\{a^k : k \in \mathbb{Z}\}$ contains at least

$$a, a^2, a^3, \dots, a^{o(a)} = e.$$

- They are all distinct.
 - Otherwise, $a^i = a^j$ for $1 \leq i < j \leq o(a)$, and $e = a^{j-i}$, a contradiction because $j - i < o(a)$.
- It is easy to see that $a^m = a^{m \bmod o(a)}$ for all $m \geq 0$.
- Similarly, $a^{-m} = a^{(-m) \bmod o(a)}$ for all $m \geq 0$.
- Hence there are no other elements in $\{a^k : k \in \mathbb{Z}\}$.

Cyclic Subsets of *Finite* Groups (concluded)

Corollary 116 *Let (G, \circ) be a finite group and $a \in G$. Then $(\{ a^k : k \in \mathbb{Z}^+ \}, \circ)$ is a subgroup of G .*

- Lemma 114 (p. 827) says $\{ a^k : k \in \mathbb{Z} \}$ is a cyclic subgroup generated by a .
- Lemma 115(1) (p. 828) says $\{ a^k : k \in \mathbb{Z}^+ \}$ is, too.

Cyclic Structures Must Form a Group?^a

- Must a cyclic structure $(\{a^k : k \in \mathbb{Z}\}, \circ)$ be a group without restrictions on \circ and entity a ?
 - Note that Lemma 114 (p. 827) does impose some restrictions: (G, \circ) must be a group to start with.
- Consider algebraic structure $(\{2^k : k \in \mathbb{Z}\}, \times \text{ mod } 12)$.
- Note that 2 cannot have an inverse modulo 12 because $\gcd(2, 12) = 2 \neq 1$.
- Hence the cyclic structure is *not* a group.

^aContributed by Mr. Bao (B90902039) on December 23, 2002.

Cosets^a

- If H is a subgroup of G and $a \in G$, the set

$$aH = \{ a \circ h : h \in H \}$$

is called a **(left) coset** of H in G .^b

- An element of aH is called a **coset representative** of aH .

^aAugustin Louis Cauchy (1789–1857), who published more than 800 papers.

^bRecall p. 777.

Cosets (continued)

- $|aH| = |H|$ when H is finite.^a
 - $|aH| \leq |H|$ by definition.
 - If $|aH| < |H|$, then $a \circ h_i = a \circ h_j$ for some *distinct* $h_i, h_j \in H$.
 - But that implies $h_i = h_j$ by the left-cancellation property, a contradiction.

^aContributed by Mr. Kai-Yuan Hou (B99201038) on June 7, 2012. Of course, if G is finite, then H must be, too.

Cosets (concluded)

- Similarly, we can also define a **right coset** of H in G ,

$$Ha = \{ h \circ a : h \in H \}.$$

- Let

$$G/H$$

denote the family of all the (left) cosets of H .

Cosets as Partitions

- Let H be a subgroup of a group G .
- For $a, b \in G$, either $aH = bH$ or $aH \cap bH = \emptyset$.^a
 - Assume $aH \cap bH \neq \emptyset$.
 - Let $c = a \circ h_1 = b \circ h_2$ for some $h_1, h_2 \in H$.
 - If $x \in aH$, then $x = a \circ h$ for some $h \in H$ and

$$x = (b \circ h_2 \circ h_1^{-1}) \circ h = b \circ (h_2 \circ h_1^{-1} \circ h) \in bH.$$

- So $aH \subseteq bH$.
- Similarly, we can prove that $bH \subseteq aH$.

^aDo we need to require that G be finite for this result as the textbook does? Contributed by Mr. Kai-Yuan Hou (B99201038) on June 7, 2012.

Cosets as Partitions (continued)

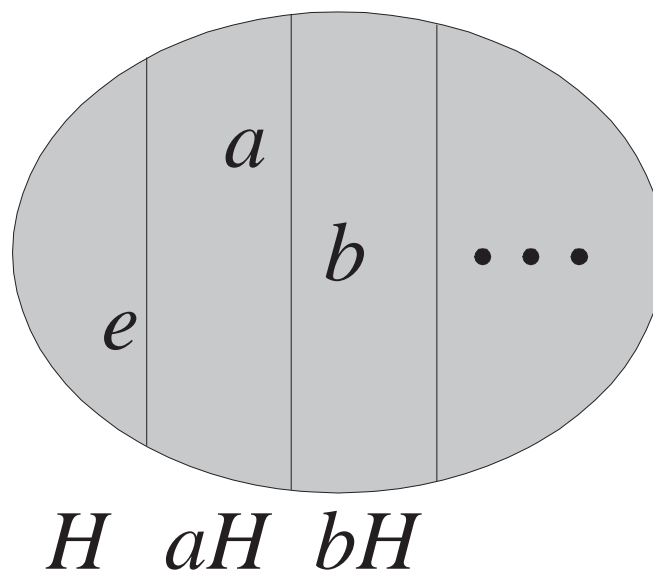
- Trivially,

$$a \in aH \quad \text{for any } a \in G$$

because $e \in H$.

- Hence $G = \bigcup_{a \in G} aH$.
- And G is partitioned by cosets.

Cosets as Partitions (concluded)



Constructing a Coset Partition of a Finite Group

Let G be a group and H a subgroup.

```
1: print  $H$ ;  
2:  $G := G - H$ ;  
3: while  $G \neq \emptyset$  do  
4:   Pick  $a \in G$ ;  
5:   print  $aH$ ;  $\{aH \text{ is disjoint from all earlier cosets.}\}$   
6:    $G := G - aH$ ;  
7: end while
```

Lagrange's^a Theorem

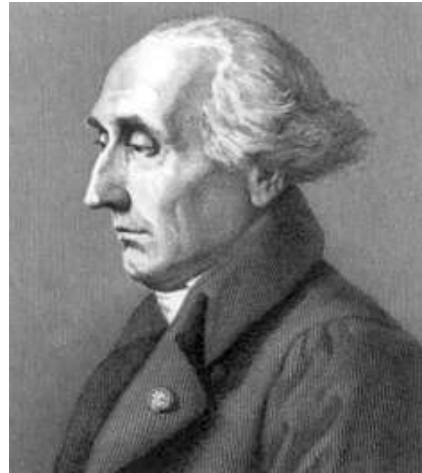
Theorem 117 *If G is a finite group with subgroup H , then $|H|$ divides $|G|$.*

- G can be partitioned by cosets of H
- Each coset of H has the same order, $|H|$.^b
- Hence $|H|$ divides $|G|$.

^aJoseph Louis Lagrange (1736–1813).

^bRecall p. 832.

Joseph Louis Lagrange (1736–1813)



Applications of Lagrange's Theorem

- Suppose $|G| = 16$, then the order of its subgroup must be 1, 2, 4, 8, or 16.
- Suppose $|G| = 18$, then the order of its subgroup must be 1, 2, 3, 6, 9, or 18.
- Suppose $|G| = 11$, a prime, then the order of its subgroup must be 1 or 11.

Index of a Subgroup

- Let H be a subgroup of G .
- The **index** of H in G , denoted by $[G : H]$, is the number of cosets of H in G .
- When G is finite, because every coset has the same size,^a

$$[G : H] = \frac{|G|}{|H|}. \quad (107)$$

^aRecall the proof of Lagrange's theorem (p. 838).

First Corollary of Lagrange's Theorem^a

Corollary 118 *If G is a finite group and $a \in G$, then $o(a)$ divides $|G|$.*

- The set generated by a , $\{a^k : k \in \mathbb{Z}\}$, has size $o(a)$ by Lemma 115(2) (p. 828).
- Set $\{a^k : k \in \mathbb{Z}\}$ is a subgroup of G by Lemma 114 (p. 827).
- Lagrange's theorem (p. 838) then implies it.

^aSee also Lemma 111 (p. 823).

The Fermat^a-Euler Theorem

Theorem 119 *If G is a finite group, then every $a \in G$ satisfies*

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

- By Corollary 118 (p. 842), $o(a)$ divides $|G|$.
- Let $|G| = o(a) \times k$, where $k \in \mathbb{Z}^+$.
- Now,

$$a^{|G|} = a^{o(a) \times k} = (a^{o(a)})^k = e^k = e.$$

^aPierre de Fermat (1601–1665).

Pierre de Fermat (1601–1665)



Euler's Theorem

Recall that \mathbb{Z}_n^* is the set of positive integers between 1 and $n - 1$ that are relatively prime to n .^a

Theorem 120 (Euler's theorem) *For all $a \in \mathbb{Z}_n^*$,*

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

- (\mathbb{Z}_n^*, \times) is a group.^b
- $|\mathbb{Z}_n^*| = \phi(n)$.^c
- Apply Theorem 119 (p. 843).

^aRecall p. 803.

^bRecall p. 803.

^cRecall p. 424.

Fermat's “Little” Theorem

Theorem 121 (Fermat’s “little” theorem) *Suppose p is a prime. Then*

$$a^{p-1} \equiv 1 \pmod{p}$$

for all $a \in \mathbb{Z}_p^$.*

- By Euler’s theorem (p. 845).

Three Easy Applications

- The inverse of a in (\mathbb{Z}_p^*, \times) is $a^{p-2} \bmod p$.
 - $a^{p-2}a = a^{p-1} \equiv 1 \bmod p$ by Fermat's “little” theorem.
- $3 \mid (n^2 - 1)$ when $3 \nmid n$.
 - The number 3 is a prime.
 - By Fermat's “little” theorem,

$$n^{3-1} = n^2 \equiv 1 \bmod 3.$$

Three Easy Applications (concluded)

- $a^{p^n - p^{n-1}} \equiv 1 \pmod{p^n}$ for odd prime p and $\gcd(a, p) = 1$.
 - By Euler's theorem (p. 845) and Theorem 59 (p. 425),

$$1 \equiv a^{\phi(p^n)} \equiv a^{p^n - p^{n-1}} \pmod{p^n}.$$

Application: The RSA Function^a

- Let $n = pq$, where p and q are distinct odd primes.
- Then

$$\phi(n) = (p - 1)(q - 1)$$

by Theorem 59 (p. 425).

- Let e be an odd integer relatively prime to $\phi(n)$.^b
- The RSA function is defined as

$$E(x) = x^e \bmod n,$$

where $\gcd(x, n) = 1$.

^aRivest, Shamir, & Adleman (1978).

^bThis e should not be confused with the identity of a group.

Adi Shamir, Ron Rivest, and Leonard Adleman



Encryption Using the RSA Function

- The RSA function is a good candidate for the **encryption** of message x .
- The number e is called the **encryption key**.
- The prime number theorem (p. 161) guarantees an abundance of primes.

Decryption and Trapdoor Information

- To be useful, an *efficient* algorithm must exist to recover x from $E(x)$.
- But this is an open problem (so far).
- The way out is the existence of the **trapdoor information** *not available* to others except the receiver.
- A candidate is the factorization of n .
 - Factorization is believed to be hard.^a

^aNumbers can be factorized efficiently by Shor's (1994) quantum algorithm.

Inversion of the RSA Function

- Let d be the inverse of e modulo $\phi(n)$, that is,

$$ed = 1 \bmod \phi(n).$$

- Because $\gcd(e, \phi(n)) = 1$, such d exists.
 - d can be found by the extended Euclidean algorithm (p. 784).

- By Euler's theorem (p. 845), the encrypted message $y \triangleq E(x)$ can be **decrypted** by

$$y^d = (x^e)^d = x^{ed} = x^{1+k\phi(n)} = xx^{k\phi(n)} = x \bmod n.$$

- So the decryption function is

$$D(y) = y^d \bmod n.$$

Sophie Germain Primes

- How many e 's are there such that $\gcd(e, \phi(n)) = 1$?
- The density of numbers between 1 and $\phi(n)$ that satisfy the above condition is^a

$$\frac{\phi(\phi(n))}{\phi(n)} = \frac{\phi((p-1)(q-1))}{(p-1)(q-1)}.$$

^aThe 5th edition of Grimaldi's *Discrete and Combinatorial Mathematics* errs with $\phi(n)/n$ on p. 760.

Sophie Germain Primes (concluded)

- Suppose $p = 2p' + 1$ and $q = 2q' + 1$, where p', q' are also primes.
 - Such primes are called **Sophie Germain primes**.
- The density becomes

$$\frac{\phi(4p'q')}{(p-1)(q-1)} = \frac{2(p'-1)(q'-1)}{4p'q'} \approx \frac{1}{2}.$$

Sophie Germain (1776–1831)

- A French mathematician.
- Gauss on Germain: “But when a person of the sex which, according to our customs and prejudices, must encounter infinitely more difficulties than men to familiarize herself with these thorny researches, succeeds nevertheless in surmounting these obstacles and penetrating the most obscure parts of them, then without doubt she must have the noblest courage, quite extraordinary talents and superior genius.”
- <http://www.pbs.org/wgbh/nova/proof/germain.html>.

Second Corollary of Lagrange's Theorem

Corollary 122 *Every group of prime order is cyclic.*

- Pick any element $a \neq e$ of the group G .^a
- Note that $o(a) > 1$.
- As $o(a)$ also divides $|G|$,^b a prime number, $o(a) = |G|$.
- This implies that every $b \in G$ must be of the form a^k for some $k \in \mathbb{Z}$.

^aBecause a group of prime order has at least 2 elements, such an a exists.

^bSee Corollary 118 (p. 842).

Criterion for Generators

- The computational problem of verifying if g is a generator is believed to be hard without the factorization of $|G|$.
- Exhaustive testing is too slow, taking $O(|G|)$ time.
- A better algorithm is based on the next corollary, assuming the factorization of $|G|$ is available.

Third Corollary of Lagrange's Theorem

Corollary 123 *Let G be a finite cyclic group with prime factorization of its order $m = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$. Then $g \in G$ is a generator of G if and only if*

$$g^{m/p_i} \neq e \quad (108)$$

for $i = 1, 2, \dots, n$.

- Define $m_i \triangleq m/p_i$.
- Hence

$$m_i = p_1^{a_1} p_2^{a_2} \cdots p_i^{a_i-1} \cdots p_n^{a_n}.$$

- Suppose g is a generator.

The Proof (continued)

- Because $o(g) = m$,

$$g^{m_i} = g^{m/p_i} \neq e$$

for all i .

- Conversely, assume inequality (108).
- We proceed to show that g must be a generator.
- Let $o(g) = j$ so $g^j = e$.
- By Lagrange's theorem (p. 838), j divides m .

The Proof (concluded)

- Let

$$j = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

where $0 \leq b_i \leq a_i$ for $i = 1, 2, \dots, n$.

- What if $j < m$?
- Then $b_i < a_i$ for some i .
- But then j divides m_i .
- This implies that $g^{m_i} = e$, contradicting inequality (108).
- We must conclude that $j = m$ and g is a generator.

Algorithm for Testing If g Is a Generator of G

- 1: $m := p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n};$
 - 2: **for** $i = 1, 2, \dots, n$ **do**
 - 3: **if** $g^{m/p_i} = e$ **then**
 - 4: **return** “ g is not a generator”;
 - 5: **end if**
 - 6: **end for**
 - 7: **return** “ g is a generator”;
- Note that $n = O(\log_2 m)$.
 - So the number of steps is polynomial in $\log_2 m$.
 - In contrast, the exhaustive method takes m steps.

Number of Generators in Finite Cyclic Groups

Lemma 124 *Let G be a finite cyclic group with order m and g be a generator of G . Then the generators are*

$$g^i,$$

where $1 \leq i < m$ and $\gcd(i, m) = 1$. Hence the number of generators is $\phi(m)$, Euler's phi function (p. 425).

- Suppose $1 \leq i < m$ is relatively prime to m .
- Let $j = o(g^i)$.
- So $g^{ij} = e$.
- As g is a generator, m divides ij by Lemma 111 (p. 823).

The Proof (concluded)

- As m cannot divide i because $\gcd(i, m) = 1$, m divides j .
- As $1 \leq j \leq m$, we must have $j = m$ and g^i is a generator.
- Next assume $1 \leq i < m$ but $\gcd(i, m) = d > 1$.
- Define $j = m/d$.
- Now, $0 < j < m$.
- By the Fermat-Euler theorem (p. 843),

$$(g^i)^j = g^{ij} = g^{im/d} = g^{m(i/d)} = (g^m)^{i/d} = e.$$

- So g^i is not a generator.

Number of Generators in (\mathbb{Z}_n^*, \times) , If Any

Theorem 125 *If (\mathbb{Z}_n^*, \times) has a generator, then it has $\phi(\phi(n))$ generators.^a*

- Recall Euler's phi function (p. 425).
- If (\mathbb{Z}_n^*, \times) has a generator, then it is a finite cyclic group with order $\phi(n)$.
- Lemma 124 (p. 863) then implies the theorem.

^aA common mistake is to answer $\phi(n)$. Is it easy to calculate $\phi(\phi(n))$ even if one knows the factorization of n ?

Powers of a Generator in (\mathbb{Z}_n^*, \times)

Corollary 126 *Suppose (\mathbb{Z}_n^*, \times) has a generator g . Then g^i is a generator if and only if $\gcd(i, \phi(n)) = 1$. Furthermore, there are no other generators.*

- (\mathbb{Z}_n^*, \times) is a finite cyclic group with order $\phi(n)$.
- Lemma 124 (p. 863) implies the claim.

$$F^*$$

- Let $(F, +, \cdot)$ be a finite field.
- $(F - \{0\}, \cdot)$ is an abelian group by the definition of ring.^a
- Define

$$F^* \triangleq (F - \{0\}, \cdot),$$

the multiplicative group of the *nonzero* elements of F .

^aRecall p. 750.

“Order Statistics”

Lemma 127 *If F is a finite field, then $\phi(d)$ elements of F^* have order^a d for every d that divides $|F^*|$.*

- Let $q \triangleq |F^*|$.
- Assume $q \geq 3$ without loss of generality.
- Let $o_i \geq 0$ denote the number of elements of F with order i .
- By Corollary 118 (p. 842), the order of an element must divide q .
- Hence $o_i = 0$ if i is not a divisor of q .

^aWith respect to “.”; same below.

The Proof (continued)

- As every element of F^* has a finite order by Lemma 112 (p. 824),

$$\sum_{d \mid q} o_d = q.$$

- But Theorem 60 (p. 432) says

$$\sum_{d \mid q} \phi(d) = q.$$

- As $o_d \geq 0$, it suffices to show

$$o_d \leq \phi(d)$$

for every d that divides q .

The Proof (concluded)

- Let d divide q .
- If $o_d > 0$, then $o_d = \phi(d)$.
 - Let $a \in F^*$ have order d .
 - Exactly $\phi(d)$ members of the cyclic group $\{a^i : 1 \leq i \leq d\}$ have order d by Lemma 124 (p. 863).
 - That group's d distinct members all satisfy $x^d = e$.^a
 - No other elements of F^* have order d because they would satisfy $x^d = e$, but its d roots have been found.
- Hence $o_d \leq \phi(d)$.

^aVerify it!

F^* Is Cyclic

Theorem 128 *If F is a finite field, then F^* is a cyclic group with $\phi(|F^*|)$ generators.*

- F^* has $\phi(|F^*|)$ generators of order $|F^*|$ by Lemma 127 (p. 868).
- But $\phi(|F^*|) \geq 1$.

Group Homomorphism and Isomorphism

- Let (G, \circ) and (H, \circ') be 2 groups.
- A function $f : G \rightarrow H$ is a **homomorphism** if

$$f(x \circ y) = f(x) \circ' f(y)$$

for all $x, y \in G$.

- It is called an **epimorphism** if f is onto.
- It is called an **isomorphism** if f is a bijection.
- An isomorphism is called an **automorphism** if $G = H$.

Group Homomorphism and Isomorphism (concluded)

- G and H are said to be **isomorphic** (written as $G \cong H$) if an isomorphism exists between them.
- Isomorphic groups have the same “multiplication table” (up to relabeling by f).
- When ambiguity may be an issue:
 - e_G for the identity of G .
 - e_H for the identity of H .

All Cyclic Groups Are Isomorphic

Lemma 129 *Cyclic groups of the same order are isomorphic.*

- Let $G = (\langle g \rangle, \circ_g)$ and $H = (\langle h \rangle, \circ_h)$ be 2 cyclic groups of the same order.
- Define $f : G \rightarrow H$ by $f(g^i) = h^i$.
- For all $x = g^i \in G$ and $y = g^j \in G$,

$$f(x \circ_g y) = f(g^{i+j}) = h^{i+j} = h^i \circ_h h^j = f(x) \circ_h f(y).$$

- f is a one-to-one correspondence between G and H because $f(g) = h$ generates H .

All Cyclic Groups Are Isomorphic (concluded)

Corollary 130 *Every cyclic group of order $n > 1$ is isomorphic to $(\mathbb{Z}_n, +)$.*

- $(\mathbb{Z}_n, +)$ is a cyclic group.^a
- Lemma 129 (p. 874) then implies this corollary.

^aRecall p. 822.

Permutations^a

- Let function $f : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ be one-to-one and onto.
- f must be a permutation of $\{1, 2, \dots, n\}$.
- Write f as

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix}$$

$$- I = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}, \text{ the identity permutation.}$$

^aLagrange (1770); Ruffini (1799); Cauchy (1815). Recall p. 436.

Permutations (concluded)

- So permutations are functions.
- We are mainly interested in permutations of a finite set.

Permutation Groups

- Let f and g be two permutations of $\{1, 2, \dots, n\}$.
- Then $f \circ g$ is defined as

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ g(f(1)) & g(f(2)) & \cdots & g(f(n)) \end{pmatrix}. \quad (109)$$

- Note that f is applied *first*.
 - The alternative of applying g first is more consistent with function composition on p. 318.
 - But our convention is more convenient in calculations.
 - Either convention works.

Permutation Groups (continued)

- For example,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

- In general, permutations can work on any finite set X of objects, not just $\{1, 2, \dots, n\}$.
 - In fact, X can even be a set of permutations.
- When a set of permutations forms a group under \circ , we have a **permutation group**.

Permutation Groups (continued)

- In general, \circ is not abelian.

- For example,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

- But

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}.$$














































Permutation Groups (concluded)

- A key result of Cayley says every group is isomorphic to a permutation group!^a
- But the permutation perspective has one unique advantage over groups: Permutations are functions!
- Under this perspective, $g(x)$ means group element $g \in G$ “acts on” $x \in X$.
- This idea is used to build interconnection networks for parallel computers.^b

^aSee p. 903.

^bAnnexstein, Baumslag, & Rosenberg (1990).

Group Action as a Table

						
g_1						
g_2						
g_3						
g_4						
g_5						
g_6						
	  					

The Symmetric Group

- There are $n!$ permutations of $\{1, 2, \dots, n\}$.
- These permutations form a group (verify it).
 - This group S_n is called the **symmetric group of degree n** .
- $|S_n| = n!$.
- Every permutation group is thus a subgroup of S_n .
- By Cayley's result^a again, every group is (isomorphic to) a subgroup of a symmetric group.
- In general, S_X denotes the set of all permutations of a set X .

^aSee p. 903.

Cycles

- Call a cycle $(i_1 \ i_2 \ \cdots \ i_m)$ an **m -cycle**, where i_1, i_2, \dots, i_m are distinct.
- It represents the permutation

$$\begin{pmatrix} i_1 & i_2 & i_3 & \cdots & i_{m-1} & i_m & \text{other fixed points} \\ i_2 & i_3 & i_4 & \cdots & i_m & i_1 & \text{other fixed points} \end{pmatrix}.$$

- The order of an m -cycle g is m because

$$g^m = I, \tag{110}$$

the identity permutation.

Cycles (concluded)

- A 1-cycle is a fixed point.
- The inverse of a cycle:

$$(i_1 \ i_2 \ \cdots \ i_m)^{-1} = (i_m \ i_{m-1} \ \cdots \ i_1).$$

– Because

$$(i_1 \ i_2 \ \cdots \ i_m)(i_m \ i_{m-1} \ \cdots \ i_1) = (i_1)(i_2) \cdots (i_m).^a$$

^aIn fact, $(i_m \ i_{m-1} \ \cdots \ i_1)(i_1 \ i_2 \ \cdots \ i_m) = (i_1)(i_2) \cdots (i_m)$, too (recall p. 800).

Cycle Decomposition of Permutations

- A permutation like $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}$ can be represented as

$$(1\ 3)(2\ 4)(5).$$

- There are 3 *disjoint* cycles above.
- 5 is a fixed point; it is **invariant** under the permutation.
- Obviously, a permutation is either a cycle or a product of disjoint cycles.

Cycle Decomposition of Permutations (concluded)

- A **cycle decomposition**^a of a permutation is a product of disjoint cycles that contains a 1-cycle for *every* invariant element.
- A cycle decomposition can be calculated efficiently.
- In practice, we often drop the fixed points.
- So

$$(1\ 3)(2\ 4)(5) = (1\ 3)(2\ 4).$$

^aAlso called a **complete factorization**.

Another Cycle Decomposition

- $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 4 & 6 \end{pmatrix} = (1\ 2\ 3)(4\ 5)(6).$
- There are 3 disjoint cycles above.
- Disjoint cycles can commute without affecting the result.
- Equivalent cycle decompositions:

$$(3\ 1\ 2)(5\ 4)(6),$$

$$(4\ 5)(1\ 2\ 3)(6),$$

$$\vdots$$

- The cycle decomposition is essentially unique.

Transpositions

- A 2-cycle is called a **transposition**.
- $(1\ 2\ 3) = (1\ 2)(1\ 3)$.^a
- In general,

$$(i_1\ i_2\ \cdots\ i_n) = (i_1\ i_2)(i_1\ i_3)\cdots(i_1\ i_n).$$

- So every permutation is a product of transpositions.
 - These transpositions are not necessarily disjoint.

^aFrom left to right always.

Order of a Permutation

Theorem 131 *Let $g \in S_n$. If $g = g_1 g_2 \cdots g_m$ is a product of disjoint cycles, then*

$$o(g) = \text{lcm}(r_1, r_2, \dots, r_m),$$

where g_i is an r_i -cycle.

- We knew $o(g_i) = r_i$.^a
- Suppose $o(g) = M$.
- Clearly,

$$g^M = (g_1 g_2 \cdots g_m)^M = g_1^M g_2^M \cdots g_m^M = I$$

because the g_i s are disjoint and hence commute.

^aRecall p. 884.

Order of a Permutation (concluded)

- But by Eq. (110) on p. 884, $g_i^M = I$ for $i = 1, 2, \dots, m$.
- Then $r_i \mid M$ by Lemma 111 (p. 823) for $i = 1, 2, \dots, m$.
- Hence $\text{lcm}(r_1, r_2, \dots, r_m) \mid M$ as well.
- But $g^{\text{lcm}(r_1, r_2, \dots, r_m)} = I$.
 - Trivially, r_i divides $\text{lcm}(r_1, r_2, \dots, r_m)$.
 - So

$$g^{\text{lcm}(r_1, \dots, r_m)} = \prod_{i=1}^m g_i^{\text{lcm}(r_1, \dots, r_m)} = I.$$

- Thus $M \mid \text{lcm}(r_1, r_2, \dots, r_m)$.
- We conclude that $\text{lcm}(r_1, r_2, \dots, r_m) = M$.

Conjugates

- Let f and g be permutations of $\{1, 2, \dots, n\}$.
- The permutation

$$g^{-1} \circ f \circ g$$

is called f 's **conjugate**.

- Conjugacy is an equivalence relation (prove it!).
- Take $f = (1\ 3)(2\ 4\ 7)(5)(6)$ and $g = (2\ 5\ 6)(1\ 3\ 4)(7)$.
- Then

$$\begin{aligned} & g^{-1} \circ f \circ g \\ &= (7)(4\ 3\ 1)(6\ 5\ 2)(1\ 3)(2\ 4\ 7)(5)(6)(2\ 5\ 6)(1\ 3\ 4)(7) \\ &= (1\ 7\ 5)(2)(3\ 4)(6). \end{aligned}$$

Conjugates (concluded)

- Interestingly,

$$\begin{aligned} & (g(1) \ g(3))(g(2) \ g(4) \ g(7))(g(5))(g(6)) \\ &= (3 \ 4)(5 \ 1 \ 7)(6)(2) \\ &= (1 \ 7 \ 5)(2)(3 \ 4)(6) \\ &= g^{-1} \circ f \circ g. \end{aligned}$$

- We simply replaced every element in a cycle of f by its image under the conjugating permutation g .
- The next theorem shows that this is not an accident.

Conjugate and Cycle Decomposition

Theorem 132 *Let f and g be permutations of $\{1, 2, \dots, n\}$. The conjugate $g^{-1} \circ f \circ g$ results by applying g to the symbols in the cycle decomposition of f .*

- If f fixes i , then $g^{-1} \circ f \circ g$ fixes $g(i)$ because

$$(g^{-1} \circ f \circ g)(g(i)) = g(f(g^{-1}(g(i)))) = g(f(i)) = g(i).$$

- So the 1-cycle (i) in the cycle decomposition of f becomes the 1-cycle

$$(g(i))$$

in that of $g^{-1} \circ f \circ g$.

The Proof (continued)

- Now suppose $f(i) = j$.
- The cycle decomposition of f contains a cycle

$$(i \ j \ \dots).$$

- Then $g^{-1} \circ f \circ g$ moves $g(i)$ to

$$(g^{-1} \circ f \circ g)(g(i)) = g(f(g^{-1}(g(i)))) = g(f(i)) = g(j).$$

- Hence the cycle decomposition of $g^{-1} \circ f \circ g$ contains the cycle

$$(g(i) \ g(j) \ \dots).$$

The Proof (concluded)

- So whenever $f(i) = j$, $g^{-1} \circ f \circ g$ moves $g(i)$ to $g(j)$ regardless of $i = j$ or not.
- As g is a bijection, there are no more numbers to consider.

Isomorphism between Symmetric Groups of the Same Degree

All symmetric groups of the same order are isomorphic.

Lemma 133 *If X and Y have the same cardinality, then $S_X \cong S_Y$.*

- Assume $X = \{x_1, x_2, \dots, x_n\}$ and $Y = \{y_1, y_2, \dots, y_n\}$.
- We shall demonstrate an isomorphism φ from S_X to S_Y .
- Let $\psi : X \rightarrow Y$ be an arbitrary bijective function.

The Proof (continued)

- Pick any arbitrary permutation from S_X :

$$f \triangleq \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ f(x_1) & f(x_2) & \cdots & f(x_n) \end{pmatrix}.$$

- We choose the mapping $\varphi : S_X \rightarrow S_Y$ that turns f into

$$f_\psi \triangleq \begin{pmatrix} \psi(x_1) & \psi(x_2) & \cdots & \psi(x_n) \\ \psi(f(x_1)) & \psi(f(x_2)) & \cdots & \psi(f(x_n)) \end{pmatrix}.$$

- So $\varphi(f) = f_\psi$.
- Note that $f_\psi \in S_Y$ because ψ and f are bijective.

The Proof (continued)

- Let

$$f_\psi(y_i) = y_j.$$

- It is one of the columns of f_ψ .
- So there is an $x_i \in X$ such that

$$\begin{aligned}y_i &= \psi(x_i), \\ y_j &= \psi(f(x_i)).\end{aligned}$$

- Hence

$$y_j = \psi \left(f \left(\psi^{-1}(y_i) \right) \right).$$

The Proof (continued)

- In summary,

$$f_\psi = \begin{pmatrix} y_1 & y_2 & \cdots & y_n \\ \psi(f(\psi^{-1}(y_1))) & \psi(f(\psi^{-1}(y_2))) & \cdots & \psi(f(\psi^{-1}(y_n))) \end{pmatrix}.$$

- So, with a slight abuse of notation,

$$\varphi(f) = \psi^{-1} \circ f \circ \psi.$$

The Proof (continued)

- Pick any $f_1, f_2 \in S_X$.
- Then

$$\begin{aligned}
 & \varphi(f_1 \circ f_2) \\
 = & \left(\begin{array}{ccc} y_1 & \cdots & y_n \\ \psi(f_2(f_1(\psi^{-1}(y_1)))) & \cdots & \psi(f_2(f_1(\psi^{-1}(y_n)))) \end{array} \right) \\
 = & \left(\begin{array}{ccc} y_1 & \cdots & y_n \\ \psi(f_2(\psi^{-1}(\psi(f_1(\psi^{-1}(y_1)))))) & \cdots & \psi(f_2(\psi^{-1}(\psi(f_1(\psi^{-1}(y_n)))))) \end{array} \right) \\
 = & \varphi(f_1) \circ \varphi(f_2).
 \end{aligned}$$

- Hence φ is a homomorphism.

The Proof (concluded)

- To show that φ is an isomorphism, it remains to show that φ is one-to-one.
- But this is obvious because all functions we used are bijective.

Cayley's Theorem

Theorem 134 *Every finite group is isomorphic to a group of permutations.*

- Let (G, \circ) be a finite group of order m ,

$$G = \{ g_1, g_2, \dots, g_m \}.$$

- Define m distinct permutations by

$$\pi_1(g) = g \circ g_1, \pi_2(g) = g \circ g_2, \dots, \pi_m(g) = g \circ g_m.$$

– They act on members of G .

- They are called (right) **translations**.^a

^aThe proof also works if we use *left* translations: $\pi_i(g) = g_i \circ g$.

The Proof (continued)

- Each π_i postmultiplies every $g \in G$ by g_i :

$$\pi_i = \begin{pmatrix} g_1 & g_2 & \cdots & g_m \\ g_1 \circ g_i & g_2 \circ g_i & \cdots & g_m \circ g_i \end{pmatrix}.$$

- It is easy to verify that π_i is a permutation.
- Consider the permutation set (G', \circ') , where

$$G' = \{ \pi_1, \pi_2, \dots, \pi_m \}$$

and \circ' denotes multiplication of permutations.^a

^aRecall p. 878.

The Proof (continued)

- (G', \circ') is a group (why?).
- We next show that $(G, \circ) \cong (G', \circ')$.
- Define $f : G \rightarrow G'$ by

$$f(g_i) = \pi_i, \quad i = 1, 2, \dots, m.$$

- Clearly, f is a one-to-one correspondence.
- Next we show that f is an isomorphism.

The Proof (concluded)

- Suppose $g_i \circ g_j = g_k$.
- For each $g \in G$,

$$\begin{aligned}\pi_k(g) &= g \circ g_k = g \circ (g_i \circ g_j) \\ &= (g \circ g_i) \circ g_j = \pi_i(g) \circ g_j \\ &= \pi_j(\pi_i(g)) = (\pi_i \circ' \pi_j)(g)\end{aligned}$$

by our convention on permutation composition.^a

- So $\pi_k = \pi_i \circ' \pi_j$.
- Finally,

$$f(g_i \circ g_j) = f(g_k) = \pi_k = \pi_i \circ' \pi_j = f(g_i) \circ' f(g_j).$$

^aRecall p. 878.