First Corollary of Lagrange’s Theorem

**Corollary 122** 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 119(2) (p. 850).
- Set $\{a^k : k \in \mathbb{Z}\}$ is a subgroup of $G$ by Lemma 118 (p. 849).
- Lagrange’s theorem (p. 860) then implies it.

---

See also Lemma 115 (p. 845).
The Fermat\textsuperscript{a}-Euler Theorem

**Theorem 123** If $G$ is a finite group, then every $a \in G$ satisfies
\[
a | G | = e.
\]

- By Corollary 122 (p. 864), $o(a)$ divides $| G |$.
- Let $| G | = o(a) \times k$, where $k \in \mathbb{Z}^+$.
- Now,
\[
a | G | = a^{o(a) \times k} = (a^{o(a)})^k = e^k = e.
\]

\textsuperscript{a}Pierre 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 $n$.

**Theorem 124 (Euler’s theorem)** For all $a \in \mathbb{Z}_n^*$,

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

- $(\mathbb{Z}_n^*, \times)$ is a group.
- $|\mathbb{Z}_n^*| = \phi(n)$.
- Apply Theorem 123 (p. 865).

---

\(^a\)Recall p. 825.
\(^b\)Recall p. 825.
\(^c\)Recall p. 424.
Fermat’s “Little” Theorem

Theorem 125 (Fermat’s “little” theorem) Suppose $p$ is a prime. Then

\[ a^{p-1} \equiv 1 \mod p \]

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

- By Euler’s theorem (p. 867).
Three Easy Applications

• The inverse of $a$ in $(\mathbb{Z}_p^*, \times)$ is $a^{p-2}$ mod $p$.
  
  - $a^{p-2}a = a^{p-1} \equiv 1 \pmod{p}$ 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,
    
    $$n^{3-1} = n^2 \equiv 1 \pmod{3}. $$
Three Easy Applications (concluded)

- \( a^{p^n} - p^{n-1} \equiv 1 \mod p^n \) for odd prime \( p \) and \( \gcd(a, p) = 1 \).
  
  - By Euler’s theorem (p. 867) and Theorem 59 (p. 425),
    
    \[ 1 \equiv a^{\phi(p^n)} \equiv a^{p^n - p^{n-1}} \mod p^n. \]
Application: The RSA Function

- 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 $\phi(n)$.
- The RSA function is defined as
  \[ E(x) = x^e \mod n, \]
  where $\gcd(x, n) = 1$.

---

\(^a\)Rivest, Shamir, & Adleman (1978).
\(^b\)This $e$ 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.\(^\text{a}\)

\(^\text{a}\)Numbers 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,
  \[
ed = 1 \mod \phi(n).
\]

• Because \( \gcd(e, \phi(n)) = 1 \), such \( d \) exists.
  
  – \( d \) can be found by the extended Euclidean algorithm (p. 806).

• By Euler’s theorem (p. 867), the encrypted message \( y \mathrel{\Delta} E(x) \) can be decrypted by
  \[
y^d = (x^e)^d = x^{ed} = x^{1+k\phi(n)} = xx^{k\phi(n)} = x \mod n.
\]

• So the decryption function is
  \[
  D(y) = y^d \mod n.
  \]
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\(^a\)

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

\(^a\)The 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.”

Second Corollary of Lagrange’s Theorem

Corollary 126  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 \( k \in \mathbb{Z} \).

\(^a\)Because a group of prime order has at least 2 elements, such an \( a \) exists.

\(^b\)See Corollary 122 (p. 864).
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 127**  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

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

(111)

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

- 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 (111).

- We proceed to show that \( g \) must be a generator.

- Let \( o(g) = j \) so \( g^j = e \).

- Because \( j \) divides \( m \) by Lagrange’s theorem (p. 860),
  \( m = dj \) for some \( d \geq 1 \).
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 \( i = 1, 2, \ldots, n \).

- 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 (111).

- 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 $i = 1, 2, \ldots, n$ do
3: \hspace{1em} if $g^{m/p_i} = e$ then
4: \hspace{2em} return “$g$ is not a generator”;
5: \hspace{1em} 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 128 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 115 (p. 845).
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. 865),
  \[(g^i)^j = g^{ij} = g^{im/d} = g^{m(i/d)} = (g^m)^{i/d} = e.\]
- So $g^i$ is not a generator.
Number of Generators in \((\mathbb{Z}_n^*, \times)\), If Any

**Theorem 129** If \((\mathbb{Z}_n^*, \times)\) has a generator, then it has \(\phi(\phi(n))\) generators.

- 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 128 (p. 885) then implies the theorem.

\(^{a}\text{A common mistake is to answer } \phi(n). \text{ Is it easy to calculate } \phi(\phi(n)) \text{ even if one knows the factorization of } n?\)
Powers of a Generator in \((\mathbb{Z}_n^*, \times)\)

**Corollary 130** 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 128 (p. 885) then 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 $F$.

\(^a\)Recall p. 772.
“Order Statistics”

**Lemma 131** If $F$ is a finite field and $d$ divides $|F^*|$, then $\phi(d)$ elements of $F^*$ have order $a$ $d$.

- 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 122 (p. 864), the order of an element must divide $q$.
- Hence $o_i = 0$ if $i$ is not a divisor of $q$.

---

With respect to “·”; same below.
The Proof (continued)

- As every element of $F^*$ has a finite order by Lemma 116 (p. 846),
  \[ \sum_{d \mid q} o_d = q. \]
- But Theorem 60 (p. 432) says
  \[ \sum_{d \mid q} \phi(d) = q. \]
- So 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 \( a \in F^\ast \) have order \( d \).
  – Exactly \( \phi(d) \) members of the cyclic group
    \( \{ a^i : 1 \leq i \leq d \} \) have order \( d \) by Lemma 128 (p. 885).
  – That group’s \( d \) distinct members all satisfy \( x^d = e \).\(^a\)
  – No other elements of \( F^\ast \) have order \( d \) because they
    would satisfy \( x^d = e \), but its \( d \) roots have been found.

• Hence \( o_d \leq \phi(d) \).

\(^a\)Verify it!
$F^*$ Is Cyclic

**Theorem 132** 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 131 (p. 890).
- 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:
  - Write $e_G$ for the identity of $G$.
  - Write $e_H$ for the identity of $H$. 
All Cyclic Groups Are Isomorphic

**Lemma 133** 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 $f : G \to H$ 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 $f(g) = h$ clearly generates $H$. 
Corollary 134  *Every cyclic group of order* $n > 1$ *is isomorphic to* $(\mathbb{Z}_n, +)$.

- $(\mathbb{Z}_n, +)$ is a cyclic abelian group.\(^a\)
- Lemma 133 (p. 896) then implies this corollary.

\(^a\)Recall p. 844.
Permutations\textsuperscript{a}

- Let function \( f : \{1, 2, \ldots, n\} \rightarrow \{1, 2, \ldots, n\} \) be one-to-one and onto.

- \( f \) must be a permutation of \( \{1, 2, \ldots, n\} \).

- Write \( f \) as

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

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

\textsuperscript{a}Lagrange (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 \( \{1, 2, \ldots, n\} \).

• 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 (112)

• 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, \ldots, 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, notations like \( g(x), x \in X \), make sense for a group element \( g \in G \) that “acts on” \( X \).

- This idea was used to construct interconnection networks for parallel computers.\(^b\)

---

\(^a\)See p. 925.

\(^b\)Annexstein, Baumslag, & Rosenberg (1990).
Permutation Group as a Multiplication Table

<table>
<thead>
<tr>
<th></th>
<th>$g_1$</th>
<th>$g_2$</th>
<th>$g_3$</th>
<th>$g_4$</th>
<th>$g_5$</th>
<th>$g_6$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$g_1$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$g_2$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$g_3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$g_4$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$g_5$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$g_6$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The Symmetric Group

- There are \( n! \) permutations of \( \{1, 2, \ldots, n\} \).

- 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 \( X \).

\(^a\)See p. 925.
Cycles

• Call a cycle \((i_1 \ i_2 \ \cdots \ i_m)\) an \(m\text{-cycle}\), where \(i_1, i_2, \ldots, i_m\) 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

\[g^m = I,\]

the identity permutation.
Cycles (concluded)

- A 1-cycle is a fixed point.
- The inverse of a cycle:
  \[(i_1 \ i_2 \ \cdots \ i_m)^{-1} = (i_m \ i_{n-1} \ \cdots \ i_1).\]
  - Because
    \[(i_1 \ i_2 \ \cdots \ i_m)(i_m \ i_{m-1} \ \cdots \ i_1) = (i_1)(i_2)\cdots(i_m).\]

\[a\]In 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. 822).
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)

- We often drop the fixed points.
- So

\[(1 \, 3)(2 \, 4)(5) = (1 \, 3)(2 \, 4).\]

- 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.

\(^a\)Also 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 (not necessarily disjoint) transpositions.

\(^a\)From left to right always.
Order of a Permutation

**Theorem 135** Let $g \in S_n$. If $g = g_1 g_2 \cdots g_m$ is a product of disjoint cycles, then

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

where $g_i$ is an $r_i$-cycle.

- We knew $o(g_i) = r_i$.
- 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.

\(^a\text{Recall p. 906.}\)
Order of a Permutation (concluded)

- The disjointness of the $g_i$s implies $g_i^M = I$ for each $i$.
- Then $r_i \mid M$ by Lemma 115 (p. 845) for $i = 1, 2, \ldots, m$.
- Hence $\text{lcm}(r_1, r_2, \ldots, r_m) \mid M$ as well.
- But $g^{\text{lcm}(r_1, r_2, \ldots, r_m)} = I$.
  - Trivially, $r_i$ divides $\text{lcm}(r_1, r_2, \ldots, r_m)$.
  - So
    \[
    g^{\text{lcm}(r_1, \ldots, r_m)} = \prod_{i=1}^{m} g_i^{\text{lcm}(r_1, \ldots, r_m)} = I.
    \]
- Thus $M \mid \text{lcm}(r_1, r_2, \ldots, r_m)$.
- We conclude that $\text{lcm}(r_1, r_2, \ldots, r_m) = M$. 
Conjugates

• Let \( f \) and \( g \) be permutations of \( \{1, 2, \ldots, n\} \).

• 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

\[
g^{-1} \circ f \circ g
= (7)(4 \ 3 \ 1)(6 \ 5 \ 2)(1 \ 3)(2 \ 4 \ 7)(5)(6)(2 \ 5 \ 6)(1 \ 3 \ 4)(7)
= (1 \ 7 \ 5)(2)(3 \ 4)(6).
\]
Conjugates (concluded)

- Interestingly,

\[(g(1) \ g(3))(g(2) \ g(4) \ g(7))(g(5))(g(6))\]

\[= (3 \ 4)(5 \ 1 \ 7)(6)(2)\]

\[= (1 \ 7 \ 5)(2)(3 \ 4)(6)\]

\[= g^{-1} \circ f \circ g.\]

- So we simply replaced every element in a cycle by its image under the conjugating permutation \(g\).

- The next theorem shows that this is not an accident.
Theorem 136 Let $f$ and $g$ be permutations of \{1, 2, \ldots, 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

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

- 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 \((i \ j \ \ldots)\).
- 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
  \((g(i) \ g(j) \ \ldots)\).
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 137** If $X$ and $Y$ have the same cardinality, then $S_X \cong S_Y$.

- Assume $X = \{x_1, x_2, \ldots, x_n\}$ and $Y = \{y_1, y_2, \ldots, y_n\}$.
- We shall demonstrate an isomorphism $\varphi$ from $S_X$ to $S_Y$.
- Let $\psi : X \to Y$ 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 $\varphi : S_X \to S_Y$ that turns $f$ into
  
  \[ f_\psi \triangleq \begin{pmatrix} \psi(x_1) & \psi(x_2) & \cdots & \psi(x_n) \\ \psi(f(x_1)) & \psi(f(x_2)) & \cdots & \psi(f(x_n)) \end{pmatrix}. \]

• Or, $\varphi(f) = f_\psi$.

• Note that $f_\psi \in S_Y$ because $\psi$ and $f$ are bijective.
The Proof (continued)

- Let
  \[ f_\psi(y_i) = y_j. \]
- It is one of the columns of \( f_\psi \).
- So there is an \( x_i \in X \) such that
  \[ y_i = \psi(x_i), \]
  \[ y_j = \psi(f(x_i)). \]
- Hence
  \[ y_j = \psi \left( f \left( \psi^{-1}(y_i) \right) \right). \quad (113) \]
The Proof (continued)

- After sorting, 
  \[
  f_\psi = \left( \begin{array}{cccc}
  y_1 & y_2 & \cdots & y_n \\
  \psi(f(\psi^{-1}(y_1))) & \psi(f(\psi^{-1}(y_2))) & \cdots & \psi(f(\psi^{-1}(y_n)))
  \end{array} \right).
  \]

- Alternatively and with a slight abuse of notation, 
  \[
  \varphi(f) = \psi^{-1} \circ f \circ \psi
  \]
  by Eq. (113).
The Proof (continued)

• Pick any \( f_1, f_2 \in S_X \).

• Then

\[
\varphi(f_1 \circ f_2) \\
= \begin{pmatrix}
  y_1 & \cdots & y_n \\
  \psi(f_2(f_1(\psi^{-1}(y_1)))) & \cdots & \psi(f_2(f_1(\psi^{-1}(y_n))))
\end{pmatrix}
\]

\[
= \begin{pmatrix}
  y_1 & \cdots & y_n \\
  \psi(f_2(\psi^{-1}(\psi(f_1(\psi^{-1}(y_1)))))) & \cdots & \psi(f_2(\psi^{-1}(\psi(f_1(\psi^{-1}(y_n))))))
\end{pmatrix}
\]

\[
= \varphi(f_1) \circ \varphi(f_2).
\]

• Hence \( \varphi \) is a homomorphism.
The Proof (concluded)

- To show that \( \varphi \) is an isomorphism, it remains to show that \( \varphi \) is one-to-one.

- But this is obvious because all functions we used are bijective.
Cayley’s Theorem

Theorem 138 *Every finite group is isomorphic to a group of permutations.*

- Let \((G, \circ)\) be a finite group of order \(m\),
  \[ G = \{ g_1, g_2, \ldots, g_m \}. \]
- Define \(m\) distinct permutations by
  \[ \pi_1(g) = g \circ g_1, \pi_2(g) = g \circ g_2, \ldots, \pi_m(g) = g \circ g_m. \]
  - They act on members of \(G\).
- They are called (right) translations.\(^a\)

\(^a\)The proof also works if we use left translations: \(\pi_i(g) = g_i \circ g\).
The Proof (continued)

• Each $\pi_i$ 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 $\pi_i$ is a permutation.

• Consider the permutation set $(G', \circ')$, where

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

and $\circ'$ denotes multiplication of permutations.\(^a\)

\(^a\)Recall p. 900.
The Proof (continued)

• \((G', \circ')\) is a group (why?).

• We next show that \((G, \circ)\) is isomorphic to \((G', \circ')\).

• Define \(f : G \to G'\) by

\[
f(g_i) = \pi_i, \quad i = 1, 2, \ldots, m.\]

• 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 $g \in G$,

\[
\begin{align*}
\pi_k(g) &= g \circ g_k = g \circ (g_i \circ g_j) \\
&= (g \circ g_i) \circ g_j = \pi_i(g) \circ g_j \\
&= \pi_j(\pi_i(g)) = (\pi_i \circ' \pi_j)(g).
\end{align*}
\]

- Recall our convention on permutation composition (p. 900).

• As $\pi_k = \pi_i \circ' \pi_j$, it means

\[
f(g_i \circ g_j) = f(g_k) = \pi_k = \pi_i \circ' \pi_j = f(g_i) \circ' f(g_j).
\]
Cyclic Permutation Group

Corollary 139 Let $g$ be a permutation of $\{1, 2, \ldots, n\}$. Then $\{g^0, g^1, g^2, \ldots\}$ is a finite cyclic group.

- First, it is a subset of the symmetric group $S_n$.
- Hence it is finite by Lemma 116 (p. 846).
- The set generated by $g$ is a cyclic group by Corollary 120 (p. 851).