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 $G = \langle x \rangle$.
- $x$ is called a generator, primitive root, or primitive element.$^a$

$^a$Paolo Ruffini (1765–1822).

Finiteness of Orders of Groups and Group Elements$^a$

**Lemma 57** If $G$ is a finite group, then the order of every element $a \in G$ must be finite.

- Consider the chain $a^1, a^2, a^3, \ldots$.
- Because $G$ is finite, the chain must eventually repeat itself.
- So there must be distinct $i < j$ such that $a^i = a^j$.
- By the cancellation property, $a^{j-i} = e$.

$^a$Contributed by Mr. Bao (990902039) on December 23, 2002.

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.
- If $n$ is $a$’s order and $a^k = e$, then $n | k$.
  - Otherwise, $e = a^k = a^{m+r} = a^r$, where $0 < r < n$.
  - This is a contradiction because $a$’s order is now at most $r < n$.

$^a$Paolo Ruffini.

Finite Cyclic Groups

**Lemma 58** Suppose $G$ is a finite group and $a \in G$. (1) $\langle a \rangle = \{a^k : k \in \mathbb{Z}^+\}$. (2) $|\langle a \rangle| = o(a)$.

- The set $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$ contains $a, a^2, a^3, \ldots, a^{o(a)} = e$.
- But no two of them are identical.
  - Otherwise, $a^i = a^j$ for $1 \leq i < j \leq o(a)$, and $a^{j-i} = e$, a contradiction because $j-i < o(a)$.
  - The set’s other $o(a)$ elements, $a^1, a^2, \ldots, a^{o(a)} = e$ are not new because $a^{-m} = a^{o(a)-m}$.
  - As $a^m = a^{m \text{ mod } o(a)}$, there are no other elements.
Cyclic Subgroups

**Lemma 59** Let \((G, \circ)\) be a group and \(a \in G\). Then \(\left\{a^k : k \in \mathbb{Z}\right\}, \circ\) is a subgroup of \(G\).

- For \(a^i, a^j \in G\), clearly \(a^i \circ a^j = a^{i+j}\) by Lemma 55 (p. 546).
- For \(a^i\), its inverse is \(a^{-i}\).
- Theorem 56 (p. 548) thus implies the lemma.

---

Cosets

- If \(H\) is a subgroup of \(G\), the set \(aH = \{ah : h \in H\}\) is called a (left) coset of \(H\) in \(G\).
- \(|aH| = |H|\) when \(G\) is finite.
  - \(|aH| \leq |H|\) by definition.
  - If \(|aH| < |H|\), then \(a \circ h_1 = a \circ h_2\) for some distinct \(h_1, h_2 \in H\), which implies \(h_1 = h_2\) by the left-cancellation property, a contradiction.
- Similarly, we can also define a right coset of \(H\) in \(G\), denoted by \(Ha\).

---

Cyclic Structures Must Form a Group?

- Must a cyclic structure \(\{a^k : k \in \mathbb{Z}\}, \circ\) be a group without restrictions on \(\circ\) and entity \(a\)?
  - Note that Lemma 59 does impose some restrictions.
- Consider algebraic structure \(\{2^k : k \in \mathbb{Z}\}, \times \mod 12\).
- Note that 2 cannot have an inverse modulo 12 because \(\gcd(2, 12) = 2 \neq 1\).
- Hence the cyclic structure is not a group.

---

Cosets as Partitions

- Let \(G\) be a finite group.
- For \(a, b \in G\), either \(aH = bH\) or \(aH \cap bH = \emptyset\).
  - 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 \(x = (b \circ h_2 \circ h_1^{-1}) \circ h = b \circ (h_2 \circ h_1^{-1} \circ h) \in bH\), which implies \(aH \subseteq bH\).
  - Similarly, we can prove that \(bH \subseteq aH\).
- As \(a \in aH\) for any \(a \in G\), \(G\) can be partitioned by cosets.

---

*Contributed by Mr. Bao (440902239) on December 23, 2002.*
Constructing a Coset Partition

1: print $H$;
2: $G := G - H$;
3: while $G \neq \emptyset$ do
4: Pick $a \in G$;
5: print $aH$;
6: $G := G - aH$;
7: end while

First Corollary of Lagrange's Theorem\(^a\)

**Corollary 61** 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 58 (p. 553).
- Set \{\(a^k : k \in \mathbb{Z}\)} is a subgroup of $G$ by Lemma 59 (p. 554).
- Lagrange's theorem thus implies our claim.

\(^a\)See also p. 551

Lagrange's\(^a\) Theorem

**Theorem 60** 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, $|H|$.
- Hence $|H|$ divides $|G|$.

\(^a\)Joseph Louis Lagrange (1736-1813).

Second Corollary of Lagrange's Theorem

**Corollary 62** Every group of prime order is cyclic.

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

Lemma 63 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. 131).

- Suppose $1 \leq i < m$ is relatively prime to $m$.
- Let $j = o(g^i)$.
- So $e = g^{ij} = g^{ij \mod m}$ by Corollary 61 (p. 560).
- As $g$ is a generator, $ij \mod m = 0$.

The Fermat-Euler Theorem

Theorem 64 If $G$ is a finite group, then every $a \in G$ satisfies

$$a^{[G]} = e,$$

- By Corollary 61 (p. 560), $o(a)$ 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.

\(\text{a} \text{Pierre de Fermat (1601-1665)}\)

The Proof (concluded)

- This implies that $m$ divides $ij$.
- As $m$ cannot divide $i$ by assumption, $m$ divides $j$.
- As $j > 0$, we must have $j = m$ and $g^i$ is a generator.
- Conversely, assume $1 \leq i < m$ but $\gcd(i, m) = d > 1$.
- Define $j = m/d$.
- But $g^i$ cannot be a generator.
- Indeed, $0 < j < m$ and

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

Permutations\(^a\)

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

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

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

\(\text{a} \text{Lagrange (1770)}\)
Permutation Groups

- Let \( f \) and \( g \) be two permutations on \( \{1, 2, \ldots, n\} \).
- Then \( f \circ g \) is defined as
  \[
  \begin{pmatrix}
  1 & 2 & \cdots & n \\
  g(f(1)) & g(f(2)) & \cdots & g(f(n))
  \end{pmatrix}
  \]
  \hspace{1em} (43)
  
  - Note that \( f \) is applied first (unlike other books).
- \( \begin{pmatrix}
  1 & 2 & 3 & 4 \\
  2 & 3 & 4 & 1
  \end{pmatrix} \circ \begin{pmatrix}
  1 & 2 & 3 & 4 \\
  3 & 4 & 1 & 2
  \end{pmatrix} = \begin{pmatrix}
  1 & 2 & 3 & 4 \\
  4 & 1 & 2 & 3
  \end{pmatrix} \).
- When a set of permutations forms a group under “\( \circ \),” we have a permutation group.

---

Cycle Decomposition of Permutations\(^a\)

- 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 cycles above.
- 5 is a fixed point; it is invariant under the permutation.
- The cycle decomposition can be calculated efficiently.

\(^a\)Augustin Louis Cauchy and Paolo Ruffini.

---

Permutation Group as a Multiplication Table

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 cycles above.
- Equivalent cycle decompositions:
  \( (3 \ 1 \ 2)(5 \ 4)(6) \),
  \( (4 \ 5)(1 \ 2 \ 3)(6) \),
  \( \cdots \).
Cycle Length

- Pick a permutation of \( \{1, 2, \ldots, n\} \) at random.
- We claim that the probability that the cycle containing 1 has length \( k \) is \( \frac{1}{n} \).
  - There are \( \binom{n}{k} \) ways to choose the elements of the cycle containing 1.
  - There are \( (k-1)! \) ways to order them.
  - There are \( (n-k)! \) ways to permute the rest.
  - Hence the desired probability equals
    \[
    \frac{\binom{n}{k}(k-1)!}{n!} = \frac{1}{n}.
    \]

Group Isomorphism

- Let \( (G, \circ) \) and \( (G', \circ') \) be 2 groups.
- They are isomorphic if there exists a one-to-one correspondence \( f \) between \( G \) and \( G' \) such that
  \[
  f(x \circ y) = f(x) \circ' f(y)
  \]
  for all \( x, y \in G \).
- Isomorphic groups have the same multiplication table (up to relabeling by \( f \)).

Properties of Isomorphic Groups

Lemma 65 If \( (G, \circ) \) and \( (G', \circ') \) are isomorphic, then their identities correspond under the isomorphism.

- Let \( f \) be an isomorphism.
- Let \( e \) be the identity of \( G \) and \( e' \) be the identity of \( G' \).
- Then
  \[
  e' \circ' f(x) = f(x) = f(e \circ x) = f(e) \circ' f(x).
  \]
  - By the right-cancellation property (p. 543), \( e' = f(e) \).
  - The lemma is proved by recalling that the identities are unique (p. 542).
Properties of Isomorphic Groups (concluded)

**Lemma 66** Let \((G, \circ)\) and \((G', \circ')\) be isomorphic under \(f\). Then if \(u\) and \(v\) are inverses in \(G\), then \(f(u)\) and \(f(v)\) are inverses in \(G'\).

- By Lemma 65 (p. 573),
  \[
  e' = f(e) = f(u \circ v) = f(u) \circ' f(v).
  \]

The Proof (continued)

- Consider permutation group \((G', \circ')\), where \(G' = \{ \pi_1, \pi_2, \ldots, \pi_m \}\) and \(\circ'\) denotes multiplication of permutations (p. 566).
- We next show that \((G, \circ)\) is isomorphic to \((G', \circ')\).
- Define a one-to-one correspondence \(f : G \rightarrow G'\) by
  \[
  f(g_i) = \pi_i, \quad i = 1, 2, \ldots, m.
  \]

Cayley's Theorem

**Theorem 67** Every finite group is isomorphic to a group of permutations.

- Let \((G, \circ)\) be a finite group of order \(m\), where \(G = \{ g_1, g_2, \ldots, g_m \}\).
- Define \(m\) distinct permutations by
  \[
  \pi_1(g) = g \circ g_1, \pi_2(g) = g \circ g_2, \pi_m(g) = g \circ g_m.
  \]
- Each \(\pi_i\) postmultiplies all the \(g \in G\) by \(g_i\):
  \[
  \pi_i = \begin{pmatrix}
  g_1 & g_2 & \cdots & g_m \\
  g_1 \circ g_i & g_2 \circ g_i & \cdots & g_m \circ g_i
  \end{pmatrix}.
  \]

The Proof (concluded)

- \(f\) is an isomorphism,
  - Suppose \(g \circ g_j = g_k\).
  - For each \(g \in G\),
    \[
    \pi_k(g) = g \circ g_k = g \circ (g_i \circ g_j)
    = (g \circ g_i) \circ g_j = \pi_i(g) \circ g_j
    = \pi_j(\pi_i(g)) = (\pi_i' \pi_j) g.
    \]
- As \(\pi_k = \pi_i' \pi_j\), function \(f\) preserves group multiplication.
Of Orbits, Stabilizers, and Characters

- Let $G$ be a permutation group on a finite set $X$.
- Let $x \in X$.
- $O_x = \{ g(x) : g \in G \}$ is called the orbit of $x$ with respect to $G$.
  - Note that $x \in O_x$.
- $G_x = \{ g \in G : g(x) = x \}$ is called the stabilizer of $x$ in $G$.
- $F(g) = \{ z \in X : g(z) = z \}$ is called the permutation character of $g$ in $X$.

Orbits as Partitions

**Lemma 68** If $G$ be a permutation group on set $X$, then $G$’s orbits partition $X$.

- $\bigcup_x O_x = G$ because $x \in O_x$ for all $x \in X$.
- If $O_x \cap O_y \neq \emptyset$, then $O_x \subseteq O_y$.
  - For any $a \in O_x$, $a = g''(x)$ for some $g'' \in G$.
  - Suppose $z \in O_x \cap O_y$.
  - Then $z = g(x) = g'(y)$ for some $g, g' \in G$.
  - Hence $a = g''(g^{-1}(z)) = g''(g^{-1}(g'(y))) \in O_y$.
- The other direction $O_y \subseteq O_x$ is symmetric.

Orbithood as an Equivalence Relation

**Lemma 69** Suppose $G$ be a permutation group on set $X$. Two $i, j \in X$ are in the same orbit if and only if there is a $g \in G$ such that $g(i) = j$.

- Suppose $i, j \in X$ are in the same orbit $O_x$.
  - $i = g_1(x)$ and $j = g_2(x)$ for some $g_1, g_2 \in G$.
  - Hence $j = g_2(x) = g_2(g_1^{-1}(i))$.
- Suppose there is a $g \in G$ such that $g(i) = j$.
- Then $j \in O_i$ and $i \in O_i$. 
Stabilizers Form a Group

Lemma 70 A stabilizer is a subgroup.
- Let $G$ be a permutation group on set $X$.
- Consider a stabilizer $G_x = \{ g \in G : g(x) = x \}$ for $x \in X$.
- For all $g_1, g_2 \in G_x$, $g_1 \circ g_2 \in G_x$ because $g_1 \circ g_2$ fixes $x$.
- For all $g \in G_x$, $g^{-1} \in G_x$ because $g^{-1}$ fixes $x$.
- The lemma follows by Theorem 56 (p. 548).

The Proof (continued)
- Each right coset of $G_x$ consists of those permutations in $G$ that map $x$ to a given element of $O_x$.
  - Elements of $O_x$ are mapped only to elements of $O_x$ by $G$ (Lemma 69 on p. 581).
  - Consider the right coset $G_x g$ for $g \in G$.
  - Every permutation in $G_x g$ maps $x$ to the same $g(x) \in O_x$ (see p. 558).
- Hence $G_x$ has $o_x$ right cosets.
- By the coset partition theorem (p. 557),
  $$|G_x| = \frac{|G|}{o_x}.$$  

Burnside's Lemma*

Theorem 71 $G$ is a permutation group on $\{1, 2, \ldots, n\}$. The average number of fixed points of permutations in $G$ equals the number of orbits.
- Let $O_1, O_2, \ldots, O_k$ be the distinct orbits with $|O_i| = o_i$.
- They partition $X = \{1, 2, \ldots, n\}$ by Lemma 68 (p. 580).
- Stabilizer $G_x$ is the set of permutations fixing $x$.
- $G_x$ is a subgroup of $G$ (Lemma 70 on p. 582).
- Consider $x \in X$ (note that $x \in O_x$).

*William Burnside (1852 1927) in 1911. The theorem is due to Cauchy and Ferdinand Frobenius (1849 1917) in 1896!

The Proof (concluded)
- Let $k(\pi)$ denote permutation $\pi$'s number of fixed points.
- Then the average number of fixed points is
  $$\frac{1}{|G|} \sum_{\pi \in G} k(\pi) = \frac{1}{|G|} \sum_{x \in \{1, 2, \ldots, n\}} |G_x|$$ (44)
  $$= \frac{1}{|G|} \sum_{i=1}^{k} \sum_{x \in O_i} |G_x|$$
  $$= \frac{1}{|G|} \sum_{i=1}^{k} o_i \frac{|G|}{o_i}$$
  $$= k.$$