Additional Properties

Corollary 107  For any ring \((R, +, \cdot)\), for all \(a, b \in R\),

1. \(-(-a) = a\).

2. \(a \cdot (-b) = (-a) \cdot b = -(a \cdot b)\).

3. \((-a) \cdot (-b) = a \cdot b\).

- By definition \(-(-a)\) is the additive inverse of \(-a\).
- As \((-a) + a = z\), \(a\) is also the additive inverse of \(-a\).
- By the uniqueness of the additive inverse,\(^a\) \(-(-a) = a\), establishing (1).

\(^a\)Recall p. 773.
The Proof (concluded)

• By definition \(-(a \cdot b)\) is the additive inverse of \(a \cdot b\).

• But by Corollary 105 (p. 782),

\[
a \cdot b + a \cdot (-b) = a \cdot [b + (-b)] = a \cdot z = z.
\]

• By the uniqueness of the additive inverse, \(^a\)

\[
a \cdot (-b) = -(a \cdot b),\text{ establishing part of (2).}
\]

• The other part of (2) can be proved similarly.

• From (2), \((-a) \cdot (-b) = -[a \cdot (-b)] = -[-(a \cdot b)].\]

• Part (3) then follows from (1).

\(^a\)Recall p. 773 again.
The Uniqueness of Unity\textsuperscript{a}

**Theorem 108** Let \((R, +, \cdot)\) be a ring with unity. (a) The unity is unique. (b) If \(x\) is a unit of \(R\), then the multiplicative inverse of \(x\) is unique.

- As a result, \(u\) (or 1) is the unity of a ring with unity.
- Furthermore, the multiplicative inverse of each unit \(x\) will be denoted by \(x^{-1}\).

\textsuperscript{a}Prove it!
Proper Divisor of Zero

• A ring may contain **proper divisors of zero**.

• *a* is a proper divisor of zero if *a* ≠ *z* and there exists a
  *b* ≠ *z* such that *a* · *b* = *z* or *b* · *a* = *z*.
  
  – The set of 2 × 2 integral matrices with matrix
    addition and multiplication is a ring.\(^a\)

  – But

\[
\begin{bmatrix}
1 & -1 \\
-1 & 1
\end{bmatrix}
\begin{bmatrix}
2 & 1 \\
2 & 1
\end{bmatrix}
= \begin{bmatrix}
0 & 0 \\
0 & 0
\end{bmatrix}.
\]

\(^a\)It is not commutative, however.
Units and Proper Divisors of Zero

Lemma 109  A unit in a ring $R$ cannot be a proper divisor of zero.

- Let $x \in R$ be a unit (p. 772).
- Hence there exists a $y \in R$ such that $x \cdot y = y \cdot x = 1$.
- Suppose $x \cdot w = z$ for some $w \in R$.
- By Corollary 105 (p. 782),
  
  \[ y \cdot (x \cdot w) = y \cdot z = z. \]

- On the other hand,
  
  \[ y \cdot (x \cdot w) = (y \cdot x) \cdot w = 1 \cdot w = w. \]

- As $w = z$, $x$ is not a proper divisor of zero.
Integral Domains and Fields

• Let \((R, +, \cdot)\) be a commutative ring with unity.
  - \(R\) is called an integral domain if \(R\) has no proper divisors of zero.
  - \(R\) is called a field if every nonzero element is a unit.

\(^a\)Due to Evariste Galois.
Evariste Galois (1811–1832)
Some Examples

• \((\mathbb{Z}, +, \cdot)\) is an integral domain but not a field.

• \((\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)\) are both integral domains and fields.
Fields Are Integral Domains

**Theorem 110** If \((F, +, \cdot)\) is a field, then it is an integral domain.

- Let \(a, b \in F\) with \(a \cdot b = z\).
- If \(a = z\), then we are done.
- Suppose \(a \neq z\).
- Then \(a\) has a multiplicative inverse \(a^{-1}\) as \(F\) is a field.
- Now, \(a \cdot b = z\) implies
  \[
  a^{-1} \cdot (a \cdot b) = a^{-1} \cdot z = z
  \]
  by Corollary 105 (p. 782).
The Proof (concluded)

• But

\[ a^{-1} \cdot (a \cdot b) = (a^{-1} \cdot a) \cdot b = u \cdot b = b. \]

• Hence \( b = z \) and \( F \) has no proper divisors of zero.
A Finite Integral Domain Must Be a Field

Theorem 111  A finite integral domain $(D, +, \cdot)$ is a field.

- Assume $D = \{d_1, d_2, \ldots, d_n\}$.
- For $d \in D$, where $d \neq z$, we have
  \[dD \triangleq \{d \cdot d_1, d \cdot d_2, \ldots, d \cdot d_n\} \subseteq D\]
  because $D$ is closed under $\cdot$.
- Suppose $|dD| < n$.
- Then
  \[d \cdot d_i = d \cdot d_j\]
  for some distinct $i, j$. 
The Proof (concluded)

• As $D$ is an integral domain and $d \neq z$, it follows that $d_i = d_j$ (why?), a contradiction.

• We conclude that $|dD| = n$ and thus $dD = D$.

• As a result, $d \cdot d_k = u$, the unity of $D$, for some $1 \leq k \leq n$.

• This implies $d$ is a unit of $D$.

• Because this is true for all $d \neq z$, $(D, +, \cdot)$ is a field.
The Integers Modulo $n$

- Let $n \in \mathbb{Z}^+$, $n > 1$.

- For $a, b \in \mathbb{Z}$, we say $a$ is congruent$^a$ to $b$ modulo $n$, written $a \equiv b \mod n$, if $n \mid (a - b)$.$^b$

- $n$ is the modulus.

- Congruence modulo $n$ is an equivalence relation on $\mathbb{Z}$.$^c$

- Let $\mathbb{Z}_n$ be the equivalence classes:

$$
\mathbb{Z}_n = \{ 0, 1, \ldots, n - 1 \}.
$$

- $\mathbb{Z}_n = \{ [0], [1], \ldots, [n - 1] \}$ is more precise.

---

$^a$Carl Friedrich Gauss.

$^b$Or $a$ and $b$ are congruent modulo $n$.

$^c$Recall p. 394.
Carl Friedrich Gauss (1777–1855)
\[ a \equiv b \mod n \text{ vs. } a = b \mod n \]

- \( a \equiv b \mod n \) is about a relation between \( a \) and \( b \).
- In contrast, \( a = b \mod n \) means \( a \) is the remainder of \( b \) when divided by \( n \).
- So \(-3 \equiv 9 \mod 6\).
- But \(-3 \neq 9 \mod 6\).
- Instead, \( 3 = 9 \mod 6 \).
Elementary Facts about Arithmetics in $\mathbb{Z}_n$

- In $\mathbb{Z}_n$, all arithmetics are modulo $n$.
  - $5 + 6 \equiv 2 \mod 3$, and $5 \times 7 \equiv 2 \mod 3$.

- If $f(x_1, x_2, \ldots, x_n)$ is a polynomial with integer coefficients and $a_j \equiv b_j \mod m$ for $1 \leq j \leq n$, then
  $$f(a_1, a_2, \ldots, a_n) \equiv f(b_1, b_2, \ldots, b_n) \mod m.$$ 

- $9^9 \mod 4 \equiv (9 \mod 4)^9 \equiv 1 \mod 4$. 
A Key Algorithm

- We are given two integers $m, n$.
- In many important applications, we need to find integers $m'$ and $n'$ such that
  $$mm' + nn' = \gcd(m, n).$$
- This is called the extended Euclidean algorithm.
Extended Euclidean Algorithm

1: \((u_1, u_2, u_3) := (1, 0, m)\);
2: \((v_1, v_2, v_3) := (0, 1, n)\);
3: while \(v_3 \neq 0\) do
4: \(q := \lfloor u_3 / v_3 \rfloor\);
5: \((t_1, t_2, t_3) := (u_1 - qv_1, u_2 - qv_2, u_3 - qv_3)\);
6: \((u_1, u_2, u_3) := (v_1, v_2, v_3)\);
7: \((v_1, v_2, v_3) := (t_1, t_2, t_3)\);
8: end while
9: \(m' := u_1\);
10: \(n' := u_2\);
11: \(\text{gcd} := u_3\);
12: return \((m', n', \text{gcd})\);
An Example: \( n = 100 \) and \( m = 17 \)

<table>
<thead>
<tr>
<th>( q )</th>
<th>( u_1 )</th>
<th>( u_2 )</th>
<th>( u_3 )</th>
<th>( v_1 )</th>
<th>( v_2 )</th>
<th>( v_3 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>1</td>
<td>0</td>
<td>100</td>
<td>0</td>
<td>1</td>
<td>17</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>1</td>
<td>17</td>
<td>1</td>
<td>-5</td>
<td>15</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>-5</td>
<td>15</td>
<td>-1</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>-1</td>
<td>6</td>
<td>2</td>
<td>8</td>
<td>-47</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
<td>-47</td>
<td>1</td>
<td>-17</td>
<td>100</td>
<td>0</td>
</tr>
</tbody>
</table>

We conclude that

\[
100 \times 8 + 17 \times (-47) = 1,
\]

which is true.
Inverses in \((\mathbb{Z}_n, \times)\)

- The \(x\) that solves \(ax \equiv 1 \mod m\) is \(a\)’s inverse.
- It is often denoted by \(a^{-1} \mod m\).
- \(\gcd(a, m) = 1\) is necessary to solve \(ax \equiv 1 \mod m\).
  - \(\gcd(a, m) > 1\) implies that \(\gcd(ax, m) > 1\).
  - That makes \(ax \equiv 1 \mod m\) unsolvable.\(^a\)

\(^a\)Prove it.
Inverses in \((\mathbb{Z}_n, \times)\) (continued)

- It is also sufficient to solve \(ax \equiv 1 \pmod{m}\).
  - The extended Euclidean algorithm yields two integers \(a'\) and \(m'\) such that
    \[aa' + mm' = 1.\]
  - This implies \(aa' \equiv 1 \pmod{m}\).
  - Thus \(x = a'\) is a solution.
Inverses in \((\mathbb{Z}_n, \times)\) (continued)

- The solution to \(ax \equiv 1 \mod m\) is unique modulo \(m\).\(^a\)
  - Suppose there are two solutions \(0 \leq x', x'' < m\).
  - Then
    \[
    \begin{align*}
    ax' &\equiv 1 \mod m, \\
    ax'' &\equiv 1 \mod m.
    \end{align*}
    \]
  - This implies that \(a(x' - x'') \equiv 0 \mod m\).
  - Hence \(m \mid a(x' - x'')\).
  - Because \(\gcd(a, m) = 1\), we have \(m \mid (x' - x'')\).
  - It must be that \(x' = x''\).

\(^a\)See also Theorem 108 (p. 786).
Inverses in \((\mathbb{Z}_n, \times)\) (concluded)

- The inverse \(a^{-1} \mod m\) is hence unique.
- \(a^{-1} \mod m\) has nothing to do with \(1/a \in \mathbb{Q}\).
  - Indeed, \(1/a\) is in general not an integer.
The Chinese Remainder Theorem

• Let $n = n_1 n_2 \cdots n_k$, where $n_i$ are pairwise relatively prime.

• Then for any integers $a_1, a_2, \ldots, a_k$, the set of simultaneous equations

$$
x \equiv a_1 \mod n_1,
$$

$$
x \equiv a_2 \mod n_2,
$$

$$
\vdots
$$

$$
x \equiv a_k \mod n_k,
$$

has a unique solution modulo $n$ for the unknown $x$. 
The Chinese Remainder Theorem (concluded)

• The solution can be expressed as a formula.

• Let \( m_i = n/n_i \) for \( i = 1, 2, \ldots, k \).\(^a\)

• The desired solution is

\[
x = a_1 c_1 + a_2 c_2 + \cdots + a_k c_k \mod n,
\]

(remainder after division by \( n \)) where

\[
c_i = m_i (m_i^{-1} \mod n_i)
\]

for \( i = 1, 2, \ldots, k \).

\(^a\)As \( m_i = n_1 \cdots n_{i-1}n_{i+1} \cdots n_k \), we have \( m_i \equiv 0 \mod n_j \) for \( i \neq j \).
An Example

• Let $n = 5 \times 13 = 65$.

• Hence $n_1 = 5, n_2 = 13, m_1 = 13, m_2 = 5$.

• Consider the equations

$$x \equiv 2 \mod 5,$$

$$x \equiv 3 \mod 13.$$

• Hence $a_1 = 2, a_2 = 3$. 
An Example (continued)

• Now verify that

\[ 13^{-1} \equiv 2 \mod 5, \]
\[ 5^{-1} \equiv 8 \mod 13. \]

– Indeed,

\[ 13 \cdot 2 \equiv 1 \mod 5, \]
\[ 5 \cdot 8 \equiv 1 \mod 13. \]
An Example (concluded)

• Hence the solution is

\[
2 \times [13 \times (13^{-1} \text{ mod } 5)] + 3 \times [5 \times (5^{-1} \text{ mod } 13)] \\
= 2 \times (13 \times 2) + 3 \times (5 \times 8) \\
= 2 \times 26 + 3 \times 40 \\
= 172 \\
\equiv 42 \text{ mod } 65.
\]

• It is easy to confirm that, indeed,

\[
42 \equiv 2 \text{ mod } 5, \\
42 \equiv 3 \text{ mod } 13.
\]
Groups, Coding Theory, and Polya’s Method of Enumeration
The pursuit of mathematics is a divine madness of the human spirit.
— Alfred North Whitehead (1861–1947),

*Science and the Modern World*
Group Theory\textsuperscript{a}

- Let $G \neq \emptyset$ be a set and $\circ$ be a binary operation on $G$.

- $(G, \circ)$ is called a group if it satisfies the following.
  1. For all $a, b \in G$, $a \circ b \in G$ (closure).
  2. For all $a, b, c \in G$, $a \circ (b \circ c) = (a \circ b) \circ c$ (associativity).
  3. There exists $e \in G$ with $a \circ e = e \circ a = a$ for all $a \in G$ (identity or unit element).
  4. For each $a \in G$, there is an element $b \in G$ such that $a \circ b = b \circ a = e$ (inverse).

- $G$ is commutative or abelian if $a \circ b = b \circ a$ for all $a, b \in G$.

\textsuperscript{a}Niels Henrik Abel (1802–1829) and Evariste Galois. This formal definition is by Cayley (1854).
Niels Henrik Abel (1802–1829)
Group as a Table
A Loose End in Item 4?\(^a\)

- Can a “right” inverse be different from a “left” inverse?

- Suppose \(a \circ b = e\) and \(b' \circ a = e\).
  - \(b\) is a right inverse of \(a\).
  - \(b'\) is a left inverse of \(a\).

- Then

\[
b' = b' \circ e = b' \circ (a \circ b) = (b' \circ a) \circ b = e \circ b = b.
\]

- Hence there is no point in distinguishing left and right inverses.

\(^a\)Contributed by Mr. Bao (B90902039) on December 23, 2002.
Examples of Groups

- Under ordinary $+$, $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ are groups.
  - The inverse of $a$ is simply $-a$, which exists.

- Under ordinary $+$, $(\mathbb{N}, +)$ is not a group.
  - The inverse of $a \in \mathbb{Z}^+$ does not exist.

- Under ordinary $\times$, none of $(\mathbb{Z}, \times), (\mathbb{Q}, \times), (\mathbb{R}, \times), (\mathbb{C}, \times)$ are groups.
  - The number 0 has no inverses.
Examples of Groups (concluded)

• Under ordinary $\times$, $(\mathbb{Q}^*, \times), (\mathbb{R}^*, \times), (\mathbb{C}^*, \times)$ are groups.
  – $A^*$ denotes the nonzero elements of $A$.

• Under ordinary $-$, $(\mathbb{Z}, -), (\mathbb{Q}, -), (\mathbb{R}, -)$ are not groups.
  – The associative axiom fails: $a - (b - c) \neq (a - b) - c$.

• $(\mathbb{Z}_n, +)$ is an abelian group for $n > 1$.

• For all $n \in \mathbb{Z}^+$, $| (\mathbb{Z}_n, +) | = n$.

• But $(\mathbb{Z}_n, \times)$ may not be a group for $n > 1$.

---

*aSee pp. 820–821.*
The Group \((\mathbb{Z}_n^*, \times)\)

- Let \(\mathbb{Z}_n^*\) stand for the set of positive integers between 1 and \(n - 1\) that are relatively prime to \(n\).

- \((\mathbb{Z}_n^*, \times)\) is a multiplicative abelian group.
  - Here, \(\times\) is done modulo \(n\).
  - See pp. 803ff for the inverses modulo \(n\).

- By definition (p. 421),
  \[
  \phi(n) \triangleq |(\mathbb{Z}_n^*, \times)|. 
  \]
  \(\text{(103)}\)

- \(\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}\).
- Hence \(\phi(12) = 4\).
The Group \((\mathbb{Z}_n^*, \times)\) (concluded)

- In particular, \((\mathbb{Z}_p^*, \times)\) is a multiplicative abelian group for prime \(p\).

- For all prime \(p\),

\[
| (\mathbb{Z}_p^*, \times) | = p - 1.
\]

- Note that \(p - 1\) is not a prime unless \(p = 3\).
Rings Redefined

• \((R, +, \cdot)\) is a ring if the following conditions hold.
  – \((R, +)\) is an abelian group.
  – \(a \cdot b \in R\) for all \(a, b \in R\) (closure).
  – \(a \cdot (b \cdot c) = (a \cdot b) \cdot c\) for all \(a, b, c \in R\) (associativity).
  – \(a \cdot (b + c) = a \cdot b + a \cdot c\) and \((b + c) \cdot a = b \cdot a + c \cdot a\) for all \(a, b, c \in R\) (distributive laws of \(\cdot\) over \(+\)).
Properties of Groups

- The identity of $G$ is unique.
  - If $e_1, e_2$ are both identities, then
    \[ e_1 = e_1 \circ e_2 = e_2 \]
    by the identity condition.

- The inverse of each element of $G$ is unique.
  - Suppose $b, c$ are both inverses of $a \in G$.
    - Then $b = b \circ e = b \circ (a \circ c) = (b \circ a) \circ c = e \circ c = c$.

\textsuperscript{a}Properties must be proved using only the four axioms or their logical corollaries.
The Cancellation Properties

The left-cancellation property: If \( a, b, c \in G \) and
\[
a \circ b = a \circ c,
\]
then \( b = c \).

- \[
b = (a^{-1} \circ a) \circ b = a^{-1} \circ (a \circ b) = a^{-1} \circ (a \circ c) = (a^{-1} \circ a) \circ c = c.
\]

The right-cancellation property: If \( a, b, c \in G \) and
\[
b \circ a = c \circ a,
\]
then \( b = c \).

\(^{\text{a}}\)Recall Theorem 104 (p. 780).
Inverses

• \((a^{-1})^{-1} = a\).
  
  – Both are inverses of \(a^{-1}\).
  
  – But inverse is unique.\(^a\)

• \((a \circ b)^{-1} = b^{-1} \circ a^{-1}\).
  
  \[ (b^{-1} \circ a^{-1}) \circ (a \circ b) = b^{-1} \circ (a^{-1} \circ a) \circ b = b^{-1} \circ b = e. \]

\(^a\)Recall p. 823.
Powers

- The associative property implies that $a_1 \circ a_2 \circ \cdots \circ a_n$ is well-defined.

- For $n > 0$, define

$$a^n = \underbrace{a \circ a \circ \cdots \circ a}_n.$$

- For $n < 0$, define

$$a^n = a^{-1} \circ a^{-1} \circ \cdots \circ a^{-1} = (a^{-1})^{-n}.$$  \hfill (104)

- Note that $(a^{-1})^n = a^{-n}$.

- Define $a^0 = e$. 
Powers (concluded)

• \((a^n)^{-1} = (a^{-1})^n\).

  - When \(n > 0\),
    
    \[
    a^n \circ (a^{-1})^n = a^{n-1} \circ a \circ a^{-1} \circ (a^{-1})^{n-1} \\
    = a^{n-1} \circ (a^{-1})^{n-1} \\
    = \cdots = e.
    \]

  - When \(n < 0\), by Eq. (104) on p. 826,
    
    \[
    a^n \circ (a^{-1})^n = (a^{-1})^{-n} \left( (a^{-1})^{-1} \right)^{-n},
    \]
    
    which equals \(e\) by the \(n > 0\) case.
Operations on Powers

Lemma 112 $a^n \circ a^m = a^{n+m}$ for $n, m \in \mathbb{Z}$.

- For $n, m \geq 0$,
  
  $a^n \circ a^m = \underbrace{a \circ \cdots \circ a}_n \circ \underbrace{a \circ \cdots \circ a}_m = \underbrace{a \circ \cdots \circ a}_{n+m} = a^{n+m}$.

- For $n \geq 0, m < 0$, and $-m \leq n$,
  
  $a^n \circ a^m = \underbrace{a \circ \cdots \circ a}_n \circ \underbrace{a^{-1} \circ \cdots \circ a^{-1}}_{-m} = \underbrace{a \circ \cdots \circ a}_{n-(-m)} = a^{n+m}$.

- The other cases are similar.
Subgroups

- Let \((G, \circ)\) be a group.
- Let \(\emptyset \neq H \subseteq G\).
- If \(H\) is a group under \(\circ\), we call it a subgroup of \(G\).
- For example, the set of even integers is a subgroup of \((\mathbb{Z}, +)\).
- \(H\) “inherits” \(\circ\) from \(G\) in that it produces the same result in both \(G\) and \(H\) wherever applicable.
- \(\{e\}\) and \(G\) are the two trivial subgroups of \(G\).
Criteria for Being a Subgroup

Only two axioms (out of four) need to be checked.

**Theorem 113** Let $H$ be a nonempty subset of a group $(G, \circ)$. Then $H$ is a subgroup of $G$ if and only if (1) for all $a, b \in H$, $a \circ b \in H$ (closure), and (2) for all $a \in H$, $a^{-1} \in H$ (inverse).

Proof ($\Rightarrow$):

- Assume that $H$ is a subgroup of $G$.
- Then $H$ is a group.
- So $H$ satisfies, among other things, the closure axiom (1) and the inverse axiom (2).
The Proof (concluded)

Proof ($\iff$):

• Let $H \neq \emptyset$ satisfy (1) and (2).

• We need to verify the associative axiom and the existence of identity.

  – **Associativity**: For all $a, b, c \in H$,
    \[(a \circ b) \circ c = a \circ (b \circ c) \in G, \text{ hence in } H \text{ by (1).}\]

  – **Identity**: For any arbitrary $a \in H$, $a^{-1} \circ a \in H$ by (2) and is an identity.
Simpler Criterion for Being a Subgroup

**Theorem 114** Let $H$ be a nonempty subset of a group $(G, \circ)$. Then $H$ is a subgroup of $G$ if and only if $a \circ b^{-1} \in H$ for all $a, b \in H$.

Proof $(\Rightarrow)$:

- Obvious by the axioms of group theory.

Proof $(\Leftarrow)$:

- First, $a \circ a^{-1} \in H$ for any $a \in H$.
- Hence

\[ e = a \circ a^{-1} \in H. \]
The Proof (concluded)

• By Theorem 113 (p. 830), we only need to prove the closure and inverse axioms hold when $a \circ b^{-1} \in H$ for all $a, b \in H$.

• **Inverse:** For any $b \in H$,

$$b^{-1} = e \circ b^{-1} \in H.$$ 

• **Closure:** For any arbitrary $a, b \in H$,

$$a \circ b = a \circ (b^{-1})^{-1} \in H.$$
Criterion for Being Abelian\textsuperscript{a}

Lemma 115 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 $(a \circ b)^{-1} = (b \circ a)^{-1} = a^{-1} \circ b^{-1}$ (p. 825).

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

\textsuperscript{a}Contrast it with Lemma 106 (p. 783).
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.\(^a\)

\(^a\)Paolo Ruffini (1765–1822).
Cyclic Groups Are Abelian

**Lemma 116** 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\textsuperscript{a} of Groups and Group Elements

• For every group $G$, the number of elements in $G$ is called the \textbf{order} of $G$, denoted by $|G|$.

• The \textbf{order} of $a \in G$, written $o(a)$, is the least \textit{positive} integer $n$ such that

$$a^n = e.$$ 

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

\textsuperscript{a}Ruffini (1799).
The Group \((\mathbb{Z}_n, +), n > 1\)

- Under ordinary \(+\) modulo \(n\), \((\mathbb{Z}_n, +)\) is an additive abelian group for \(n > 1\).\(^a\)
- Its order is \(n\).
- Its generator is 1.
  - Every \(i \in \mathbb{Z}_n\) can be expressed as
    \[
    i = \underbrace{1 + 1 + \cdots + 1}_{\text{\(i\) times}}.
    \]

\(^a\)Recall p. 819.
Orders of Group Elements

Lemma 117 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

Lemma 118 If $G$ is a finite group, then the order of every element $a \in G$ must be finite.

- Consider the chain $a^1, a^2, a^3, \ldots \in G$.
- 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 112 (p. 828).
- As a result, $a$’s order is at most $j - i$, which is finite.

Contributed by Mr. Bao (B90902039) on December 23, 2002.
Criterion for Being a Subgroup: The Finite Case

Corollary 119 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 113 (p. 830), we only need to prove that if the closure property holds, then $a^{-1} \in H$ for all $a \in H$ (inverse).

- Let $a \in H$.

- Then $a^m = e$ for some $m \in \mathbb{Z}$ by Lemma 118 (p. 840).

- Hence $a^{-1} = a^{m-1} \in H$.

  - This is because $a \circ a^{m-1} = a^m = e$. 

©2018 Prof. Yuh-Dauh Lyuu, National Taiwan University

Page 841
Remarks

- Corollary 119 may not hold for *infinite* groups.
- For example, $(\mathbb{Z}, +)$ is a group.\(^a\)
- Its subset $(\mathbb{N}, +)$ is closed under $+$.\(^b\)
- But $(\mathbb{N}, +)$ is *not* a subgroup of $(\mathbb{Z}, +)!\(^a\)

\(^a\)Recall p. 818.
\(^b\)Recall p. 818 again.
Cyclic Subgroups

Lemma 120 Let $(G, \circ)$ be a group and $a \in G$. Then $H = (\{ a^k : k \in \mathbb{Z} \}, \circ)$ is a subgroup of $G$. Hence $H = \langle a \rangle$.

- For $a^i, a^j \in H$, we have
  \[ a^i \circ a^{-j} = a^{i-j} \in H \]
  by Lemma 112 (p. 828).

- Theorem 114 (p. 832) then implies the lemma.
Cyclic Subsets of Finite Groups

Lemma 121  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 \(a, a^2, a^3, \ldots, a^{o(a)} = e\).

- 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 \(a^m = a^{m \mod o(a)}\) for all \(m \geq 0\).

- Similarly, \(a^{-m} = a^{(-m) \mod o(a)}\) for all \(m \geq 0\).

- Hence there are no other elements in \(\{ a^k : k \in \mathbb{Z} \}\).
Cyclic Subsets of \textit{Finite} Groups (concluded)

\textbf{Corollary 122} \textit{Let} \((G, \circ)\) \textit{be a finite group and} \(a \in G\). \textit{Then} \(\{a^k : k \in \mathbb{Z}^+ \}, \circ\) \textit{is a subgroup of} \(G\).

- Lemma 120 (p. 843) \textit{says} \(\{a^k : k \in \mathbb{Z} \}\) is a cyclic subgroup generated by \(a\).

- Lemma 121(1) (p. 844) \textit{says} \(\{a^k : k \in \mathbb{Z}^+ \}\) \textit{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 120 (p. 843) does impose some restrictions: \((G, \circ)\) must be a group to start with.

- 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.

\(^a\)Contributed 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 \( G \).

- An element of \( aH \) is called a \textbf{coset representative} of \( aH \).

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

\(^a\)Contributed 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 \( bH \subseteq aH \).

\(^a\)Do 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,
  \[ a \in aH \quad \text{for any} \quad a \in G \]
  because \( e \in H \).
- Hence \( G = \bigcup_{a \in G} aH \).
- And \( G \) can be partitioned by cosets.
Cosets as Partitions (concluded)

$H \ aH \ bH$

Diagram:
- $H$
- $aH$
- $bH$
- $e$
- $a$
- $b$
- $\cdots$
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 $aH$; \{ $aH$ is disjoint from all earlier cosets. \}`
6: $G := G - aH$;
7: `end while`
Lagrange’s\(^a\) Theorem

**Theorem 123** 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 \(|G|\).

\(^a\)Joseph Louis Lagrange (1736–1813).
\(^b\)Recall p. 848.
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,$^a$

\[
[G : H] = \frac{|G|}{|H|}.
\]  

$^a$Recall the proof of Lagrange’s theorem (p. 854).
First Corollary of Lagrange’s Theorem\textsuperscript{a}

\textbf{Corollary 124} \textit{If} $G$ \textit{is a finite group and} $a \in G$, \textit{then} $o(a)$ \textit{divides} $|G|$.  

- The set generated by $a$, \{ $a^k : k \in \mathbb{Z}$ \}, has size $o(a)$ by Lemma 121(2) (p. 844).

- Set \{ $a^k : k \in \mathbb{Z}$ \} is a subgroup of $G$ by Lemma 120 (p. 843).

- Lagrange’s theorem then implies our claim.

\textsuperscript{a}See also Lemma 117 (p. 839).
The Fermat$^a$-Euler Theorem

**Theorem 125**  *If $G$ is a finite group, then every $a \in G$ satisfies*

$$a \mid |G| = e.$$

- By Corollary 124 (p. 858), $o(a)$ divides $|G|$.
- Let $|G| = o(a) \times k$, where $k \in \mathbb{Z}^+$.
- Now,

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

\(^a\)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 $n$.\(^a\)

**Theorem 126 (Euler’s theorem)**  For all $a \in \mathbb{Z}_n^*$,

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

- $(\mathbb{Z}_n^*, \times)$ is a group.\(^b\)
- $|\mathbb{Z}_n^*| = \phi(n)$.\(^c\)
- Apply Theorem 125 (p. 859).

\(^{a}\text{Recall p. 820.}\)
\(^{b}\text{Recall p. 820.}\)
\(^{c}\text{Recall p. 421.}\)
Fermat’s “Little” Theorem

Theorem 127 (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. 861).