MATH 601
Abstract Algebra I

Richard Hammack

www.people.vcu.edu/∼rhammack/Math601/

Today: Chapter 0, Section 1.1

Goal: Establish notation; recall elemental ideas and the definition of a group; introduce groups of symmetries.

Chapter 0

The integers: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

Chapter 0

The integers: $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$

- **a divides b**, written $a \mid b$, means $b = ac$ for some $c \in \mathbb{Z}$.

Chapter 0

The integers: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

- **a divides b**, written $a \mid b$, means $b = ac$ for some $c \in \mathbb{Z}$.
  Example: $6|24$ because $24 = 6 \cdot 4$.

Chapter 0

The integers: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

- **a divides b**, written $a \mid b$, means $b = ac$ for some $c \in \mathbb{Z}$.
  Example: $6|24$ because $24 = 6 \cdot 4$.
  Example: $6 \nmid 25$ because $25 \neq 6 \cdot c$ for all $c \in \mathbb{Z}$.

Chapter 0

The integers: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

- **a divides b**, written $a \mid b$, means $b = ac$ for some $c \in \mathbb{Z}$.
  Example: $6|24$ because $24 = 6 \cdot 4$.
  Example: $6 \nmid 25$ because $25 \neq 6 \cdot c$ for all $c \in \mathbb{Z}$.
  Example: $6 \mid 0$ because $0 = 6 \cdot 0$.

Chapter 0

The integers: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

- **a divides b**, written $a \mid b$, means $b = ac$ for some $c \in \mathbb{Z}$.
  Example: $6|24$ because $24 = 6 \cdot 4$.
  Example: $6 \nmid 25$ because $25 \neq 6 \cdot c$ for all $c \in \mathbb{Z}$.
  Example: $6 \mid 0$ because $0 = 6 \cdot 0$.
- **Greatest common divisor** (largest positive divisor of 2 numbers)

Chapter 0

The integers: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

- **a divides b**, written $a \mid b$, means $b = ac$ for some $c \in \mathbb{Z}$.
  Example: $6|24$ because $24 = 6 \cdot 4$.
  Example: $6 \nmid 25$ because $25 \neq 6 \cdot c$ for all $c \in \mathbb{Z}$.
  Example: $6 \mid 0$ because $0 = 6 \cdot 0$.
- **Greatest common divisor** (largest positive divisor of 2 numbers)
  Example: $\gcd(12, 30) = 6$

Chapter 0

The integers: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

- **a divides b**, written $a \mid b$, means $b = ac$ for some $c \in \mathbb{Z}$.
  Example: $6|24$ because $24 = 6 \cdot 4$.
  Example: $6 \nmid 25$ because $25 \neq 6 \cdot c$ for all $c \in \mathbb{Z}$.
  Example: $6 \mid 0$ because $0 = 6 \cdot 0$.
- **Greatest common divisor** (largest positive divisor of 2 numbers)
  Example: $\gcd(12, 30) = 6$ or $(12, 30) = 6$

Chapter 0

The integers: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

- **a divides b**, written $a \mid b$, means $b = ac$ for some $c \in \mathbb{Z}$.
  Example: $6|24$ because $24 = 6 \cdot 4$.
  Example: $6 \nmid 25$ because $25 \neq 6 \cdot c$ for all $c \in \mathbb{Z}$.
  Example: $6 \mid 0$ because $0 = 6 \cdot 0$.
- **Greatest common divisor** (largest positive divisor of 2 numbers)
  Example: $\gcd(12, 30) = 6$ or $(12, 30) = 6$
  Example: $\gcd(12, 0) = 12$ or $(12, 0) = 12$

Chapter 0

The integers: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

- **a divides b**, written $a \mid b$, means $b = ac$ for some $c \in \mathbb{Z}$.
  Example: $6|24$ because $24 = 6 \cdot 4$.
  Example: $6 \nmid 25$ because $25 \neq 6 \cdot c$ for all $c \in \mathbb{Z}$.
  Example: $6 \mid 0$ because $0 = 6 \cdot 0$.
- **Greatest common divisor** (largest positive divisor of 2 numbers)
  Example: $\gcd(12, 30) = 6$ or $(12, 30) = 6$
  Example: $\gcd(12, 0) = 12$ or $(12, 0) = 12$
  Example: $\gcd(12, 35) = 1$ or $(12, 35) = 1$

Chapter 0

The integers: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

- **a divides b**, written $a \mid b$, means $b = ac$ for some $c \in \mathbb{Z}$.
  Example: $6|24$ because $24 = 6 \cdot 4$.
  Example: $6 \nmid 25$ because $25 \neq 6 \cdot c$ for all $c \in \mathbb{Z}$.
  Example: $6 \mid 0$ because $0 = 6 \cdot 0$.
- **Greatest common divisor** (largest positive divisor of 2 numbers)
  Example: $\gcd(12, 30) = 6$ or $(12, 30) = 6$
  Example: $\gcd(12, 0) = 12$ or $(12, 0) = 12$
  Example: $\gcd(12, 35) = 1$ or $(12, 35) = 1$
  If $\gcd(a, b) = 1$ we say a and b are *relatively prime*.

Chapter 0

The integers: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

- **a divides b**, written $a \mid b$, means $b = ac$ for some $c \in \mathbb{Z}$.
  Example: $6|24$ because $24 = 6 \cdot 4$.
  Example: $6 \nmid 25$ because $25 \neq 6 \cdot c$ for all $c \in \mathbb{Z}$.
  Example: $6 \mid 0$ because $0 = 6 \cdot 0$.
- **Greatest common divisor** (largest positive divisor of 2 numbers)
  Example: $\gcd(12, 30) = 6$ or $(12, 30) = 6$
  Example: $\gcd(12, 0) = 12$ or $(12, 0) = 12$
  Example: $\gcd(12, 35) = 1$ or $(12, 35) = 1$
  If $\gcd(a, b) = 1$ we say a and b are *relatively prime*.
- **Least common multiple** (least positive multiple of 2 numbers)

Chapter 0

The integers: $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$

- **a divides b**, written $a \mid b$, means $b = ac$ for some $c \in \mathbb{Z}$.
  Example: $6|24$ because $24 = 6 \cdot 4$.
  Example: $6 \nmid 25$ because $25 \neq 6 \cdot c$ for all $c \in \mathbb{Z}$.
  Example: $6 \mid 0$ because $0 = 6 \cdot 0$.
- **Greatest common divisor** (largest positive divisor of 2 numbers)
  Example: $\gcd(12, 30) = 6$ or $(12, 30) = 6$
  Example: $\gcd(12, 0) = 12$ or $(12, 0) = 12$
  Example: $\gcd(12, 35) = 1$ or $(12, 35) = 1$
  If $\gcd(a, b) = 1$ we say a and b are *relatively prime*.
- **Least common multiple** (least positive multiple of 2 numbers)
  $\operatorname{lcm}(12, 30) = 60$ $\operatorname{lcm}(12, 0)$ not defined

Chapter 0

The integers: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

- **a divides b**, written $a \mid b$, means $b = ac$ for some $c \in \mathbb{Z}$.
  Example: $6|24$ because $24 = 6 \cdot 4$.
  Example: $6 \nmid 25$ because $25 \neq 6 \cdot c$ for all $c \in \mathbb{Z}$.
  Example: $6 \mid 0$ because $0 = 6 \cdot 0$.
- **Greatest common divisor** (largest positive divisor of 2 numbers)
  Example: $\gcd(12, 30) = 6$ or $(12, 30) = 6$
  Example: $\gcd(12, 0) = 12$ or $(12, 0) = 12$
  Example: $\gcd(12, 35) = 1$ or $(12, 35) = 1$
  If $\gcd(a, b) = 1$ we say a and b are *relatively prime*.
- **Least common multiple** (least positive multiple of 2 numbers)
  $\text{lcm}(12, 30) = 60$ $\quad$ $\text{lcm}(12, 0)$ not defined
- **Division Algorithm** ($a \div b = q + r$, where $r =$ remainder)

Chapter 0

The integers: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

- **a divides b**, written $a \mid b$, means $b = ac$ for some $c \in \mathbb{Z}$.
  Example: $6|24$ because $24 = 6 \cdot 4$.
  Example: $6 \nmid 25$ because $25 \neq 6 \cdot c$ for all $c \in \mathbb{Z}$.
  Example: $6 \mid 0$ because $0 = 6 \cdot 0$.
- **Greatest common divisor** (largest positive divisor of 2 numbers)
  Example: $\gcd(12, 30) = 6$ or $(12, 30) = 6$
  Example: $\gcd(12, 0) = 12$ or $(12, 0) = 12$
  Example: $\gcd(12, 35) = 1$ or $(12, 35) = 1$
  If $\gcd(a, b) = 1$ we say a and b are *relatively prime*.
- **Least common multiple** (least positive multiple of 2 numbers)
  $\text{lcm}(12, 30) = 60$ $\text{lcm}(12, 0)$ not defined
- **Division Algorithm** ($a \div b = q + r$, where $r =$ remainder)
  If $a, b \in \mathbb{Z}$ and $b \neq 0$, then $\exists$ unique $q, r \in \mathbb{Z}$ with $a = qb + r$, where $0 \leq r < |b|$.

Chapter 0

The integers: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

- **a divides b**, written $a \mid b$, means $b = ac$ for some $c \in \mathbb{Z}$.
  Example: $6|24$ because $24 = 6 \cdot 4$.
  Example: $6 \nmid 25$ because $25 \neq 6 \cdot c$ for all $c \in \mathbb{Z}$.
  Example: $6 \mid 0$ because $0 = 6 \cdot 0$.

- **Greatest common divisor** (largest positive divisor of 2 numbers)
  Example: $\gcd(12, 30) = 6$ or $(12, 30) = 6$
  Example: $\gcd(12, 0) = 12$ or $(12, 0) = 12$
  Example: $\gcd(12, 35) = 1$ or $(12, 35) = 1$
  If $\gcd(a, b) = 1$ we say a and b are *relatively prime*.

- **Least common multiple** (least positive multiple of 2 numbers)
  $\operatorname{lcm}(12, 30) = 60$ $\operatorname{lcm}(12, 0)$ not defined

- **Division Algorithm** ($a \div b = q + r$, where $r =$ remainder)
  If $a, b \in \mathbb{Z}$ and $b \neq 0$, then $\exists$ unique $q, r \in \mathbb{Z}$ with $a = qb + r$, where $0 \leq r < |b|$.
  Example: $a = 11$, $b = 4$; $11 = 2 \cdot 4 + 3$

Chapter 0

The integers: $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$

- **a divides b**, written $a \mid b$, means $b = ac$ for some $c \in \mathbb{Z}$.
  Example: $6|24$ because $24 = 6 \cdot 4$.
  Example: $6 \nmid 25$ because $25 \neq 6 \cdot c$ for all $c \in \mathbb{Z}$.
  Example: $6 \mid 0$ because $0 = 6 \cdot 0$.
- **Greatest common divisor** (largest positive divisor of 2 numbers)
  Example: $\gcd(12, 30) = 6$ or $(12, 30) = 6$
  Example: $\gcd(12, 0) = 12$ or $(12, 0) = 12$
  Example: $\gcd(12, 35) = 1$ or $(12, 35) = 1$
  If $\gcd(a, b) = 1$ we say a and b are *relatively prime*.
- **Least common multiple** (least positive multiple of 2 numbers)
  $\operatorname{lcm}(12, 30) = 60$ $\operatorname{lcm}(12, 0)$ not defined
- **Division Algorithm** ($a \div b = q + r$, where $r =$ remainder)
  If $a, b \in \mathbb{Z}$ and $b \neq 0$, then $\exists$ unique $q, r \in \mathbb{Z}$ with $a = qb + r$, where $0 \leq r < |b|$.
  Example: $a = 11$, $b = 4$; $11 = 2 \cdot 4 + 3$
  Example: $a = -11$, $b = 4$; $-11 = -3 \cdot 4 + 1$

Math 601 Mantra

$$\boxed{\text{NEVER UNDERESTIMATE THE DIVISION ALGORITHM}}$$

Consequence of Division Algorithm

Theorem $\gcd(a, b) = 1 \iff \exists\, x, y \in \mathbb{Z}$ with $ax + by = 1$.

Consequence of Division Algorithm

Theorem $\gcd(a, b) = 1 \iff \exists\, x, y \in \mathbb{Z}$ with $ax + by = 1$.

Proof ($\Longrightarrow$) Suppose $\gcd(a, b) = 1$.

Consequence of Division Algorithm

Theorem $\gcd(a, b) = 1 \iff \exists\, x, y \in \mathbb{Z}$ with $ax + by = 1$.

Proof ($\Longrightarrow$) Suppose $\gcd(a, b) = 1$.

Choose $x, y \in \mathbb{Z}$ so that $k = ax + by$ has smallest possible positive value.

Consequence of Division Algorithm

Theorem $\gcd(a, b) = 1 \iff \exists\, x, y \in \mathbb{Z}$ with $ax + by = 1$.

Proof ($\Longrightarrow$) Suppose $\gcd(a, b) = 1$.

Choose $x, y \in \mathbb{Z}$ so that $k = ax + by$ has smallest possible positive value.
(Want to show $k = 1$.)

Consequence of Division Algorithm

Theorem $\gcd(a, b) = 1 \iff \exists\, x, y \in \mathbb{Z}$ with $ax + by = 1$.

Proof ($\Longrightarrow$) Suppose $\gcd(a, b) = 1$.

Choose $x, y \in \mathbb{Z}$ so that $k = ax + by$ has smallest possible positive value.
(Want to show $k = 1$.)
By Division Algorithm, $\boxed{a = qk + r}$ with $0 \leq r < k$.

Consequence of Division Algorithm

Theorem $\gcd(a, b) = 1 \iff \exists\, x, y \in \mathbb{Z}$ with $ax + by = 1$.

Proof ($\Longrightarrow$) Suppose $\gcd(a, b) = 1$.

Choose $x, y \in \mathbb{Z}$ so that $k = ax + by$ has smallest possible positive value.
(Want to show $k = 1$.)
By Division Algorithm, $\boxed{a = qk + r}$ with $0 \leq r < k$.
Then $r = a - qk$

Consequence of Division Algorithm

Theorem $\gcd(a, b) = 1 \iff \exists\, x, y \in \mathbb{Z}$ with $ax + by = 1$.

Proof ($\Longrightarrow$) Suppose $\gcd(a, b) = 1$.

Choose $x, y \in \mathbb{Z}$ so that $k = ax + by$ has smallest possible positive value.
(Want to show $k = 1$.)
By Division Algorithm, $\boxed{a = qk + r}$ with $0 \leq r < k$.
Then $r = a - qk = a - q(ax + by)$

Consequence of Division Algorithm

Theorem $\gcd(a, b) = 1 \iff \exists\, x, y \in \mathbb{Z}$ with $ax + by = 1$.

Proof ($\Longrightarrow$) Suppose $\gcd(a, b) = 1$.

Choose $x, y \in \mathbb{Z}$ so that $k = ax + by$ has smallest possible positive value.
(Want to show $k = 1$.)
By Division Algorithm, $\boxed{a = qk + r}$ with $0 \leq r < k$.
Then $r = a - qk = a - q(ax + by) = a(1 - qx) + b(-qy)$.

Consequence of Division Algorithm

Theorem $\gcd(a, b) = 1 \iff \exists\, x, y \in \mathbb{Z}$ with $ax + by = 1$.

Proof ($\Longrightarrow$) Suppose $\gcd(a, b) = 1$.

Choose $x, y \in \mathbb{Z}$ so that $k = ax + by$ has smallest possible positive value.
(Want to show $k = 1$.)
By Division Algorithm, $\boxed{a = qk + r}$ with $0 \leq r < k$.
Then $r = a - qk = a - q(ax + by) = a(1 - qx) + b(-qy)$.
Then $r = 0$ (by choice of k).

Consequence of Division Algorithm

Theorem $\gcd(a, b) = 1 \iff \exists\, x, y \in \mathbb{Z}$ with $ax + by = 1$.

Proof ($\Longrightarrow$) Suppose $\gcd(a, b) = 1$.

Choose $x, y \in \mathbb{Z}$ so that $k = ax + by$ has smallest possible positive value.
(Want to show $k = 1$.)
By Division Algorithm, $\boxed{a = qk + r}$ with $0 \leq r < k$.
Then $r = a - qk = a - q(ax + by) = a(1 - qx) + b(-qy)$.
Then $r = 0$ (by choice of k). The boxed equation gives $a = qk$, so $k|a$.

Consequence of Division Algorithm

Theorem $\gcd(a, b) = 1 \iff \exists\, x, y \in \mathbb{Z}$ with $ax + by = 1$.

Proof ($\Longrightarrow$) Suppose $\gcd(a, b) = 1$.

Choose $x, y \in \mathbb{Z}$ so that $k = ax + by$ has smallest possible positive value.
(Want to show $k = 1$.)
By Division Algorithm, $\boxed{a = qk + r}$ with $0 \leq r < k$.
Then $r = a - qk = a - q(ax + by) = a(1 - qx) + b(-qy)$.
Then $r = 0$ (by choice of k). The boxed equation gives $a = qk$, so $k | a$.
Reversing roles of a and b, we get $k | b$.

Consequence of Division Algorithm

Theorem $\gcd(a, b) = 1 \iff \exists\, x, y \in \mathbb{Z}$ with $ax + by = 1$.

Proof ($\Longrightarrow$) Suppose $\gcd(a, b) = 1$.

Choose $x, y \in \mathbb{Z}$ so that $k = ax + by$ has smallest possible positive value.
(Want to show $k = 1$.)
By Division Algorithm, $\boxed{a = qk + r}$ with $0 \leq r < k$.
Then $r = a - qk = a - q(ax + by) = a(1 - qx) + b(-qy)$.
Then $r = 0$ (by choice of k). The boxed equation gives $a = qk$, so $k|a$.
Reversing roles of a and b, we get $k|b$.
Thus k is a common positive divisor of both a and b.

Consequence of Division Algorithm

Theorem $\gcd(a,b) = 1 \iff \exists\, x, y \in \mathbb{Z}$ with $ax + by = 1$.

Proof ($\Longrightarrow$) Suppose $\gcd(a,b) = 1$.

Choose $x, y \in \mathbb{Z}$ so that $k = ax + by$ has smallest possible positive value.
(Want to show $k = 1$.)
By Division Algorithm, $\boxed{a = qk + r}$ with $0 \le r < k$.
Then $r = a - qk = a - q(ax + by) = a(1 - qx) + b(-qy)$.
Then $r = 0$ (by choice of k). The boxed equation gives $a = qk$, so $k|a$.
Reversing roles of a and b, we get $k|b$.
Thus k is a common positive divisor of both a and b.
Thus $1 \le k \le \gcd(a,b) = 1$, so $k = 1$.

Consequence of Division Algorithm

Theorem $\gcd(a, b) = 1 \iff \exists\, x, y \in \mathbb{Z}$ with $ax + by = 1$.

Proof ($\Longrightarrow$) Suppose $\gcd(a, b) = 1$.

Choose $x, y \in \mathbb{Z}$ so that $k = ax + by$ has smallest possible positive value.
(Want to show $k = 1$.)
By Division Algorithm, $\boxed{a = qk + r}$ with $0 \leq r < k$.
Then $r = a - qk = a - q(ax + by) = a(1 - qx) + b(-qy)$.
Then $r = 0$ (by choice of k). The boxed equation gives $a = qk$, so $k|a$.
Reversing roles of a and b, we get $k|b$.
Thus k is a common positive divisor of both a and b.
Thus $1 \leq k \leq \gcd(a, b) = 1$, so $k = 1$.

($\Longleftarrow$) (Contrapositive)
Suppose $\gcd(a, b) = k > 1$.

Consequence of Division Algorithm

Theorem $\gcd(a,b) = 1 \iff \exists\, x, y \in \mathbb{Z}$ with $ax + by = 1$.

Proof ($\Longrightarrow$) Suppose $\gcd(a,b) = 1$.

Choose $x, y \in \mathbb{Z}$ so that $k = ax + by$ has smallest possible positive value.
(Want to show $k = 1$.)
By Division Algorithm, $\boxed{a = qk + r}$ with $0 \leq r < k$.
Then $r = a - qk = a - q(ax + by) = a(1 - qx) + b(-qy)$.
Then $r = 0$ (by choice of k). The boxed equation gives $a = qk$, so $k|a$.
Reversing roles of a and b, we get $k|b$.
Thus k is a common positive divisor of both a and b.
Thus $1 \leq k \leq \gcd(a,b) = 1$, so $k = 1$.

($\Longleftarrow$) (Contrapositive)
Suppose $\gcd(a,b) = k > 1$.
Then $a = kc$ and $b = kc'$ for some $c, c' \in \mathbb{Z}$.

Consequence of Division Algorithm

Theorem $\gcd(a, b) = 1 \iff \exists\, x, y \in \mathbb{Z}$ with $ax + by = 1$.

Proof ($\Longrightarrow$) Suppose $\gcd(a, b) = 1$.

Choose $x, y \in \mathbb{Z}$ so that $k = ax + by$ has smallest possible positive value.
(Want to show $k = 1$.)
By Division Algorithm, $\boxed{a = qk + r}$ with $0 \leq r < k$.
Then $r = a - qk = a - q(ax + by) = a(1 - qx) + b(-qy)$.
Then $r = 0$ (by choice of k). The boxed equation gives $a = qk$, so $k|a$.
Reversing roles of a and b, we get $k|b$.
Thus k is a common positive divisor of both a and b.
Thus $1 \leq k \leq \gcd(a, b) = 1$, so $k = 1$.

($\Longleftarrow$) (Contrapositive)
Suppose $\gcd(a, b) = k > 1$.
Then $a = kc$ and $b = kc'$ for some $c, c' \in \mathbb{Z}$.
Thus for any integers x, y, we have
$ax + by = kcx + kc'y = k(cx + c'y) \neq 1$. ■

The Integers Modulo n

Given integer $n > 0$, define an equivalence relation on $\mathbb{Z}$ as:
$a \equiv b \pmod{n}$ provided $n|(a-b)$.

The Integers Modulo n

Given integer $n > 0$, define an equivalence relation on $\mathbb{Z}$ as:
$a \equiv b \pmod{n}$ provided $n | (a - b)$.

Example: $\mathbb{Z}/3\mathbb{Z}$

The Integers Modulo n

Given integer $n > 0$, define an equivalence relation on $\mathbb{Z}$ as:
$a \equiv b \pmod{n}$ provided $n|(a-b)$.

Example: $\mathbb{Z}/3\mathbb{Z}$

Equivalence classes:
$\overline{0} = \{x \in \mathbb{Z} \mid 3|(x-0)\} = \{3k+0 \mid k \in \mathbb{Z}\} = \{\ldots, -3, 0, 3, 6, \ldots\}$

The Integers Modulo n

Given integer $n > 0$, define an equivalence relation on $\mathbb{Z}$ as:
$a \equiv b \pmod{n}$ provided $n|(a-b)$.

Example: $\mathbb{Z}/3\mathbb{Z}$

Equivalence classes:
$\overline{0} = \{x \in \mathbb{Z} \mid 3|(x-0)\} = \{3k+0 \mid k \in \mathbb{Z}\} = \{\ldots, -3, 0, 3, 6, \ldots\}$
$\overline{1} = \{x \in \mathbb{Z} \mid 3|(x-1)\} = \{3k+1 \mid k \in \mathbb{Z}\} = \{\ldots, -2, 1, 4, 7, \ldots\}$

The Integers Modulo n

Given integer $n > 0$, define an equivalence relation on $\mathbb{Z}$ as:
$a \equiv b \pmod{n}$ provided $n|(a - b)$.

Example: $\mathbb{Z}/3\mathbb{Z}$

Equivalence classes:
$\overline{0} = \{x \in \mathbb{Z} \mid 3|(x - 0)\} = \{3k + 0 \mid k \in \mathbb{Z}\} = \{\dots, -3, 0, 3, 6, \dots\}$
$\overline{1} = \{x \in \mathbb{Z} \mid 3|(x - 1)\} = \{3k + 1 \mid k \in \mathbb{Z}\} = \{\dots, -2, 1, 4, 7, \dots\}$
$\overline{2} = \{x \in \mathbb{Z} \mid 3|(x - 2)\} = \{3k + 2 \mid k \in \mathbb{Z}\} = \{\dots, -1, 2, 5, 8, \dots\}$

The Integers Modulo n

Given integer $n > 0$, define an equivalence relation on $\mathbb{Z}$ as:
$a \equiv b \pmod{n}$ provided $n|(a-b)$.

Example: $\mathbb{Z}/3\mathbb{Z}$

Equivalence classes:
$\overline{0} = \{x \in \mathbb{Z} \mid 3|(x-0)\} = \{3k+0 \mid k \in \mathbb{Z}\} = \{\ldots, -3, 0, 3, 6, \ldots\}$
$\overline{1} = \{x \in \mathbb{Z} \mid 3|(x-1)\} = \{3k+1 \mid k \in \mathbb{Z}\} = \{\ldots, -2, 1, 4, 7, \ldots\}$
$\overline{2} = \{x \in \mathbb{Z} \mid 3|(x-2)\} = \{3k+2 \mid k \in \mathbb{Z}\} = \{\ldots, -1, 2, 5, 8, \ldots\}$

Addition on equivalence classes: $\overline{a} + \overline{b} = \overline{a+b}$

The Integers Modulo n

Given integer $n > 0$, define an equivalence relation on $\mathbb{Z}$ as:
$a \equiv b \pmod{n}$ provided $n|(a-b)$.

Example: $\mathbb{Z}/3\mathbb{Z}$

Equivalence classes:
$\overline{0} = \{x \in \mathbb{Z} \mid 3|(x-0)\} = \{3k+0 \mid k \in \mathbb{Z}\} = \{\dots, -3, 0, 3, 6, \dots\}$
$\overline{1} = \{x \in \mathbb{Z} \mid 3|(x-1)\} = \{3k+1 \mid k \in \mathbb{Z}\} = \{\dots, -2, 1, 4, 7, \dots\}$
$\overline{2} = \{x \in \mathbb{Z} \mid 3|(x-2)\} = \{3k+2 \mid k \in \mathbb{Z}\} = \{\dots, -1, 2, 5, 8, \dots\}$

Addition on equivalence classes: $\overline{a} + \overline{b} = \overline{a+b}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

The Integers Modulo n

Given integer $n > 0$, define an equivalence relation on $\mathbb{Z}$ as:
$a \equiv b \pmod{n}$ provided $n|(a-b)$.

Example: $\mathbb{Z}/3\mathbb{Z}$

Equivalence classes:
$\overline{0} = \{x \in \mathbb{Z} \mid 3|(x-0)\} = \{3k+0 \mid k \in \mathbb{Z}\} = \{\ldots, -3, 0, 3, 6, \ldots\}$
$\overline{1} = \{x \in \mathbb{Z} \mid 3|(x-1)\} = \{3k+1 \mid k \in \mathbb{Z}\} = \{\ldots, -2, 1, 4, 7, \ldots\}$
$\overline{2} = \{x \in \mathbb{Z} \mid 3|(x-2)\} = \{3k+2 \mid k \in \mathbb{Z}\} = \{\ldots, -1, 2, 5, 8, \ldots\}$

Addition on equivalence classes: $\overline{a} + \overline{b} = \overline{a+b}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

Multiplication on equivalence classes: $\overline{a}\overline{b} = \overline{ab}$

The Integers Modulo n

Given integer $n > 0$, define an equivalence relation on $\mathbb{Z}$ as:
$a \equiv b \pmod{n}$ provided $n|(a-b)$.

Example: $\mathbb{Z}/3\mathbb{Z}$

Equivalence classes:
$\overline{0} = \{x \in \mathbb{Z} \mid 3|(x-0)\} = \{3k+0 \mid k \in \mathbb{Z}\} = \{\ldots, -3, 0, 3, 6, \ldots\}$
$\overline{1} = \{x \in \mathbb{Z} \mid 3|(x-1)\} = \{3k+1 \mid k \in \mathbb{Z}\} = \{\ldots, -2, 1, 4, 7, \ldots\}$
$\overline{2} = \{x \in \mathbb{Z} \mid 3|(x-2)\} = \{3k+2 \mid k \in \mathbb{Z}\} = \{\ldots, -1, 2, 5, 8, \ldots\}$

Addition on equivalence classes: $\overline{a} + \overline{b} = \overline{a+b}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

Multiplication on equivalence classes: $\overline{a}\,\overline{b} = \overline{ab}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

The Integers Modulo n

Given integer $n > 0$, define an equivalence relation on $\mathbb{Z}$ as:
$a \equiv b \pmod{n}$ provided $n|(a-b)$.

Example: $\mathbb{Z}/3\mathbb{Z}$

Equivalence classes:
$\overline{0} = \{x \in \mathbb{Z} \mid 3|(x-0)\} = \{3k+0 \mid k \in \mathbb{Z}\} = \{\ldots, -3, 0, 3, 6, \ldots\}$
$\overline{1} = \{x \in \mathbb{Z} \mid 3|(x-1)\} = \{3k+1 \mid k \in \mathbb{Z}\} = \{\ldots, -2, 1, 4, 7, \ldots\}$
$\overline{2} = \{x \in \mathbb{Z} \mid 3|(x-2)\} = \{3k+2 \mid k \in \mathbb{Z}\} = \{\ldots, -1, 2, 5, 8, \ldots\}$

Addition on equivalence classes: $\overline{a} + \overline{b} = \overline{a+b}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

Multiplication on equivalence classes: $\overline{a}\,\overline{b} = \overline{ab}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

In general $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$

The Integers Modulo n

Given integer $n > 0$, define an equivalence relation on $\mathbb{Z}$ as:
$a \equiv b \pmod{n}$ provided $n|(a-b)$.

Example: $\mathbb{Z}/3\mathbb{Z}$

Equivalence classes:
$\overline{0} = \{x \in \mathbb{Z} \mid 3|(x-0)\} = \{3k+0 \mid k \in \mathbb{Z}\} = \{\ldots, -3, 0, 3, 6, \ldots\}$
$\overline{1} = \{x \in \mathbb{Z} \mid 3|(x-1)\} = \{3k+1 \mid k \in \mathbb{Z}\} = \{\ldots, -2, 1, 4, 7, \ldots\}$
$\overline{2} = \{x \in \mathbb{Z} \mid 3|(x-2)\} = \{3k+2 \mid k \in \mathbb{Z}\} = \{\ldots, -1, 2, 5, 8, \ldots\}$

Addition on equivalence classes: $\overline{a} + \overline{b} = \overline{a+b}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

Multiplication on equivalence classes: $\overline{a}\,\overline{b} = \overline{ab}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

In general $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$

Operations associative: $(\overline{a}\,\overline{b})\overline{c} = (\overline{ab})\overline{c} = \overline{(ab)c} = \overline{a(bc)} = \overline{a}(\overline{bc}) = \overline{a}(\overline{b}\,\overline{c})$

Section 1.1: Groups

Definition: A *group* is a set G with a binary operation $\star : G \times G \to G$.
Abbreviation: $\star(a, b) = a \star b$.
This is required to satisfy the following three axioms:

(i) $\star$ is associative: $\quad (a \star b) \star c = a \star (b \star c) \qquad \forall a, b, c \in G$.

(ii) $\exists$ element $e \in G$ for which $e \star a = a = a \star e \qquad \forall a \in G$.

(iii) If $a \in G$, then $\exists\ a^{-1} \in G$ for which $a \star a^{-1} = e = a^{-1} \star a$.

Section 1.1: Groups

Definition: A *group* is a set G with a binary operation $\star : G \times G \to G$.
Abbreviation: $\star(a, b) = a \star b$.
This is required to satisfy the following three axioms:

(i) $\star$ is associative: $(a \star b) \star c = a \star (b \star c) \qquad \forall a, b, c \in G$.

(ii) $\exists$ element $e \in G$ for which $e \star a = a = a \star e \qquad \forall a \in G$.

(iii) If $a \in G$, then $\exists\ a^{-1} \in G$ for which $a \star a^{-1} = e = a^{-1} \star a$.

G is called *abelian* or *commutative* if $a \star b = b \star a$ for all $a, b \in G$.

Section 1.1: Groups

Definition: A *group* is a set G with a binary operation $\star : G \times G \to G$.
Abbreviation: $\star(a, b) = a \star b$.
This is required to satisfy the following three axioms:

(i) $\star$ is associative: $(a \star b) \star c = a \star (b \star c) \qquad \forall a, b, c \in G$.

(ii) $\exists$ element $e \in G$ for which $e \star a = a = a \star e \qquad \forall a \in G$.

(iii) If $a \in G$, then $\exists\ a^{-1} \in G$ for which $a \star a^{-1} = e = a^{-1} \star a$.

G is called *abelian* or *commutative* if $a \star b = b \star a$ for all $a, b \in G$.

Notation

	$a \star b$	identity	inverse of a	powers	laws of exponents
Mult.	ab	1 or e	a^{-1}	$a^n = \underbrace{aaa\cdots a}_{n}$ $a^0 = e$	$a^m a^n = a^{m+n}$ $(a^m)^n = a^{mn}$ $a^{-n} = (a^{-1})^n$
Add.					

Section 1.1: Groups

Definition: A *group* is a set G with a binary operation $\star : G \times G \to G$.
Abbreviation: $\star(a, b) = a \star b$.
This is required to satisfy the following three axioms:

(i) $\star$ is associative: $(a \star b) \star c = a \star (b \star c) \quad \forall a, b, c \in G$.

(ii) $\exists$ element $e \in G$ for which $e \star a = a = a \star e \quad \forall a \in G$.

(iii) If $a \in G$, then $\exists\ a^{-1} \in G$ for which $a \star a^{-1} = e = a^{-1} \star a$.

G is called *abelian* or *commutative* if $a \star b = b \star a$ for all $a, b \in G$.

Notation

	$a \star b$	identity	inverse of a	powers	laws of exponents
Mult.	ab	1 or e	a^{-1}	$a^n = \underbrace{aaa \cdots a}_{n}$ $a^0 = e$	$a^m a^n = a^{m+n}$ $(a^m)^n = a^{mn}$ $a^{-n} = (a^{-1})^n$
Add.	$a + b$	0	$-a$	$na = \underbrace{a + a + \cdots + a}_{n}$ $0a = 0$	$ma + na = (m+n)a$ $m(na) = (mn)a$ $(-m)a = m(-a)$

Examples of Groups

Operation $+$: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$

Examples of Groups

Operation $+$: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$

Operation $\times$: $\mathbb{Q} - \{0\}$, $\mathbb{R} - \{0\}$, $\mathbb{C} - \{0 + 0i\}$ $\mathbb{Q}^+$, $\mathbb{R}^+$

Examples of Groups

Operation $+$: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$

Operation $\times$: $\mathbb{Q}-\{0\}$, $\mathbb{R}-\{0\}$, $\mathbb{C}-\{0+0i\}$ $\mathbb{Q}^+$, $\mathbb{R}^+$

Note: $\mathbb{Z}/n\mathbb{Z}$ is generally not a group under multiplication.
Example: $\overline{6} \in \mathbb{Z}/12\mathbb{Z}$ has no inverse; $\overline{6}\,\overline{a} = \overline{1}$ is impossible.

Examples of Groups

Operation $+$: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$

Operation $\times$: $\mathbb{Q} - \{0\}$, $\mathbb{R} - \{0\}$, $\mathbb{C} - \{0 + 0i\}$ $\mathbb{Q}^+$, $\mathbb{R}^+$

Note: $\mathbb{Z}/n\mathbb{Z}$ is generally not a group under multiplication.
Example: $\overline{6} \in \mathbb{Z}/12\mathbb{Z}$ has no inverse; $\overline{6}\,\overline{a} = \overline{1}$ is impossible.

Important class of multiplicative groups:
$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a, n) = 1\}$

Examples of Groups

Operation $+$: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$

Operation $\times$: $\mathbb{Q}-\{0\}$, $\mathbb{R}-\{0\}$, $\mathbb{C}-\{0+0i\}$ $\mathbb{Q}^+$, $\mathbb{R}^+$

Note: $\mathbb{Z}/n\mathbb{Z}$ is generally not a group under multiplication.
Example: $\overline{6}\in\mathbb{Z}/12\mathbb{Z}$ has no inverse; $\overline{6}\,\overline{a}=\overline{1}$ is impossible.

Important class of multiplicative groups:
$(\mathbb{Z}/n\mathbb{Z})^\times=\{\overline{a}\in\mathbb{Z}/n\mathbb{Z}\mid \gcd(a,n)=1\}$

Example: $(\mathbb{Z}/12\mathbb{Z})^\times=\{\overline{1},\overline{5},\overline{7},\overline{11}\}$

Examples of Groups

Operation $+$: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$

Operation $\times$: $\mathbb{Q}-\{0\}$, $\mathbb{R}-\{0\}$, $\mathbb{C}-\{0+0i\}$ $\mathbb{Q}^+$, $\mathbb{R}^+$

Note: $\mathbb{Z}/n\mathbb{Z}$ is generally not a group under multiplication.
Example: $\overline{6} \in \mathbb{Z}/12\mathbb{Z}$ has no inverse; $\overline{6}\,\overline{a} = \overline{1}$ is impossible.

Important class of multiplicative groups:
$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a, n) = 1\}$

Example: $(\mathbb{Z}/12\mathbb{Z})^\times = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$

$\cdot$	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$
$\overline{1}$	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$
$\overline{5}$	$\overline{5}$	$\overline{1}$	$\overline{11}$	$\overline{7}$
$\overline{7}$	$\overline{7}$	$\overline{11}$	$\overline{1}$	$\overline{5}$
$\overline{11}$	$\overline{11}$	$\overline{7}$	$\overline{5}$	$\overline{1}$

Examples of Groups

Operation $+$: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$

Operation $\times$: $\mathbb{Q}-\{0\}$, $\mathbb{R}-\{0\}$, $\mathbb{C}-\{0+0i\}$ $\mathbb{Q}^+$, $\mathbb{R}^+$

Note: $\mathbb{Z}/n\mathbb{Z}$ is generally not a group under multiplication.
Example: $\overline{6} \in \mathbb{Z}/12\mathbb{Z}$ has no inverse; $\overline{6}\,\overline{a} = \overline{1}$ is impossible.

Important class of multiplicative groups:
$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a,n)=1\}$

Example: $(\mathbb{Z}/12\mathbb{Z})^\times = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$

$\cdot$	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$
$\overline{1}$	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$
$\overline{5}$	$\overline{5}$	$\overline{1}$	$\overline{11}$	$\overline{7}$
$\overline{7}$	$\overline{7}$	$\overline{11}$	$\overline{1}$	$\overline{5}$
$\overline{11}$	$\overline{11}$	$\overline{7}$	$\overline{5}$	$\overline{1}$

If $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, its (multiplicative) inverse exists, as follows:

Examples of Groups

Operation $+$: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$

Operation $\times$: $\mathbb{Q}-\{0\}$, $\mathbb{R}-\{0\}$, $\mathbb{C}-\{0+0i\}$ $\mathbb{Q}^+$, $\mathbb{R}^+$

Note: $\mathbb{Z}/n\mathbb{Z}$ is generally not a group under multiplication.
Example: $\overline{6} \in \mathbb{Z}/12\mathbb{Z}$ has no inverse; $\overline{6}\,\overline{a} = \overline{1}$ is impossible.

Important class of multiplicative groups:
$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a,n)=1\}$

Example: $(\mathbb{Z}/12\mathbb{Z})^\times = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$

$\cdot$	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$
$\overline{1}$	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$
$\overline{5}$	$\overline{5}$	$\overline{1}$	$\overline{11}$	$\overline{7}$
$\overline{7}$	$\overline{7}$	$\overline{11}$	$\overline{1}$	$\overline{5}$
$\overline{11}$	$\overline{11}$	$\overline{7}$	$\overline{5}$	$\overline{1}$

If $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, its (multiplicative) inverse exists, as follows:
As $\gcd(a,n)=1$, we can obtain $ax+ny=1$, or $ax = 1-ny$.

Examples of Groups

Operation $+$: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$

Operation $\times$: $\mathbb{Q}-\{0\}$, $\mathbb{R}-\{0\}$, $\mathbb{C}-\{0+0i\}$ $\mathbb{Q}^+$, $\mathbb{R}^+$

Note: $\mathbb{Z}/n\mathbb{Z}$ is generally not a group under multiplication.
Example: $\overline{6} \in \mathbb{Z}/12\mathbb{Z}$ has no inverse; $\overline{6}\,\overline{a} = \overline{1}$ is impossible.

Important class of multiplicative groups:
$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a,n)=1\}$

Example: $(\mathbb{Z}/12\mathbb{Z})^\times = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$

$\cdot$	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$
$\overline{1}$	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$
$\overline{5}$	$\overline{5}$	$\overline{1}$	$\overline{11}$	$\overline{7}$
$\overline{7}$	$\overline{7}$	$\overline{11}$	$\overline{1}$	$\overline{5}$
$\overline{11}$	$\overline{11}$	$\overline{7}$	$\overline{5}$	$\overline{1}$

If $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$, its (multiplicative) inverse exists, as follows:
As $\gcd(a,n)=1$, we can obtain $ax+ny=1$, or $ax = 1-ny$.
Then $\overline{a}\,\overline{x} = \overline{ax} = \overline{1-ny} = \overline{1} - \overline{ny} = \overline{1} - \overline{0} = \overline{1}$.

The Direct Product

If G and H are groups, then
$G \times H = \{(g, h) | g \in G, h \in H\}$ is a group.

The Direct Product

If G and H are groups, then
$G \times H = \{(g, h) | g \in G, h \in H\}$ is a group.
Operation: $(g, h)(g', h') = (gg', hh')$

The Direct Product

If G and H are groups, then
$G \times H = \{(g, h) | g \in G, h \in H\}$ is a group.
Operation: $(g, h)(g', h') = (gg', hh')$

Example: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

The Direct Product

If G and H are groups, then
$G \times H = \{(g,h) | g \in G, h \in H\}$ is a group.
Operation: $(g,h)(g',h') = (gg',hh')$

Example: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$+$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

The Direct Product

If G and H are groups, then
$G \times H = \{(g, h) | g \in G, h \in H\}$ is a group.
Operation: $(g, h)(g', h') = (gg', hh')$

Example: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$+$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

Isomorphic to the **Klein 4-group:**

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

The Direct Product

If G and H are groups, then
$G \times H = \{(g, h) | g \in G, h \in H\}$ is a group.
Operation: $(g, h)(g', h') = (gg', hh')$

Example: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$+$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

Isomorphic to the **Klein 4-group:**

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

$\cdot$	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$
$\overline{1}$	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$
$\overline{5}$	$\overline{5}$	$\overline{1}$	$\overline{11}$	$\overline{7}$
$\overline{7}$	$\overline{7}$	$\overline{11}$	$\overline{1}$	$\overline{5}$
$\overline{11}$	$\overline{11}$	$\overline{7}$	$\overline{5}$	$\overline{1}$

Symmetries of Geometric Objects

(A significant source of groups)

Symmetries of Geometric Objects

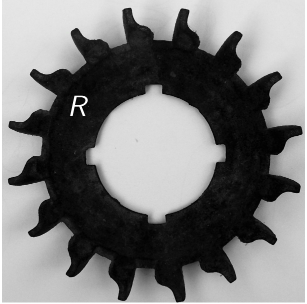
(A significant source of groups)

Given a geometric object R, a symmetry of R is a bijection $f : R \longrightarrow R$ that does not distort distances.

Symmetries of Geometric Objects

(A significant source of groups)

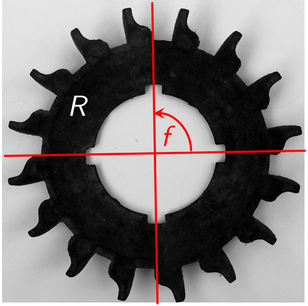
Given a geometric object R, a symmetry of R is a bijection $f : R \rightarrow R$ that does not distort distances.



Symmetries of Geometric Objects

(A significant source of groups)

Given a geometric object R, a symmetry of R is a bijection $f : R \to R$ that does not distort distances.



Example: $f : R \to R$ is rotation by 90°.

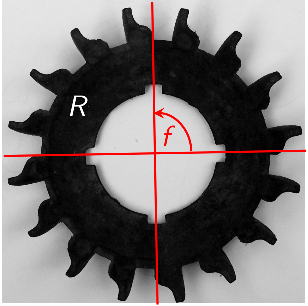
Symmetries of Geometric Objects

(A significant source of groups)

Given a geometric object R, a symmetry of R is a bijection $f : R \to R$ that does not distort distances.

Example: $f : R \to R$ is rotation by 90°.

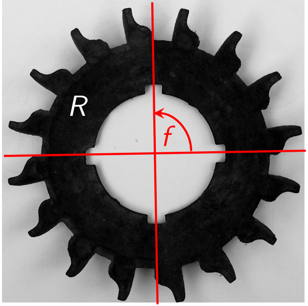
The composition of two symmetries is a symmetry. We write $f \circ g = fg$.
Thus $ff = f^2 =$ rotation by 180°.



Symmetries of Geometric Objects

(A significant source of groups)

Given a geometric object R, a symmetry of R is a bijection $f : R \to R$ that does not distort distances.



Example: $f : R \to R$ is rotation by $90°$.

The composition of two symmetries is a symmetry. We write $f \circ g = fg$.
Thus $ff = f^2 =$ rotation by $180°$.

The set of symmetries of R forms a group G:

(i) Function composition is associative.

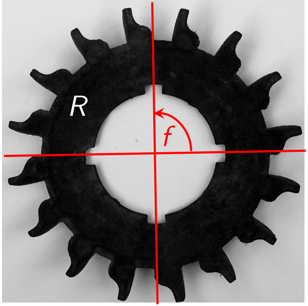
(ii) Identity is function $1 : R \to R$ defined as $1(x) = x$.

(iii) If f is a symmetry, then so is f^{-1}, and $f \circ f^{-1} = f^{-1} \circ f = 1$.

Symmetries of Geometric Objects

(A significant source of groups)

Given a geometric object R, a symmetry of R is a bijection $f : R \to R$ that does not distort distances.



Example: $f : R \to R$ is rotation by 90°.

The composition of two symmetries is a symmetry. We write $f \circ g = fg$.
Thus $ff = f^2 =$ rotation by 180°.

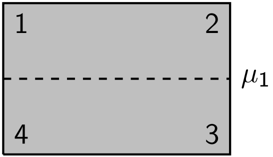
The set of symmetries of R forms a group G:

(i) Function composition is associative.
(ii) Identity is function $1 : R \to R$ defined as $1(x) = x$.
(iii) If f is a symmetry, then so is f^{-1}, and $f \circ f^{-1} = f^{-1} \circ f = 1$.

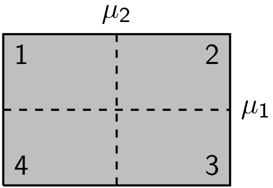
In above example $G = \{1, f, f^2, f^3\} = \{f^0, f^1, f^2, f^3\} \cong \mathbb{Z}/4\mathbb{Z}$.

Symmetry group of a rectangle

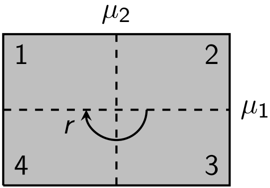
Symmetry group of a rectangle



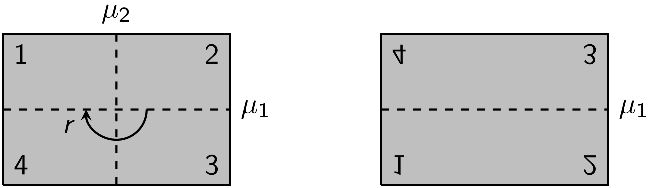
Symmetry group of a rectangle



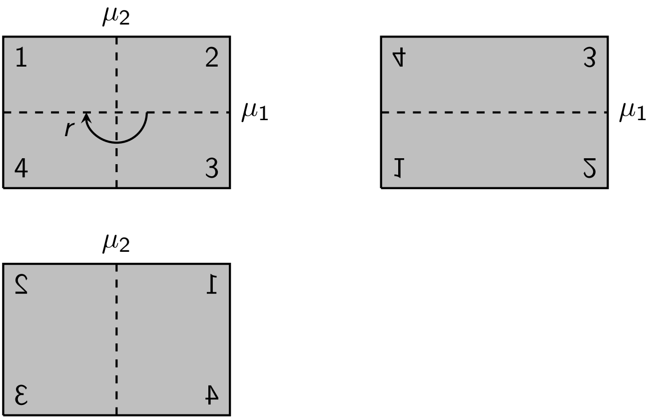
Symmetry group of a rectangle



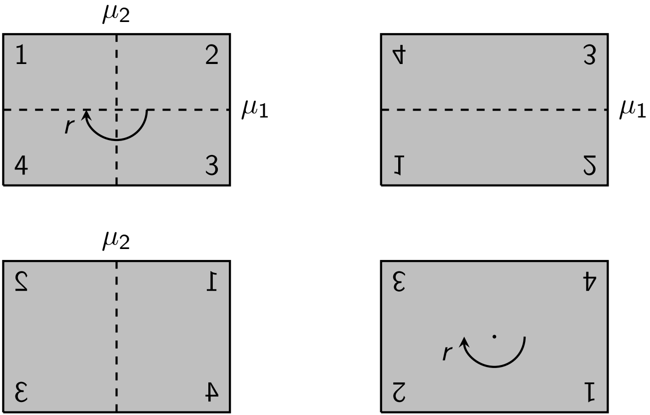
Symmetry group of a rectangle



Symmetry group of a rectangle

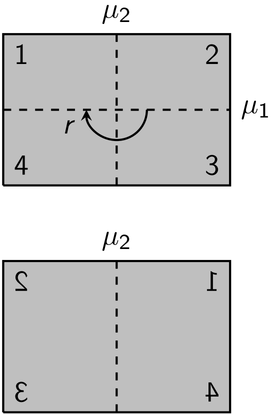


Symmetry group of a rectangle



Symmetry group of a rectangle

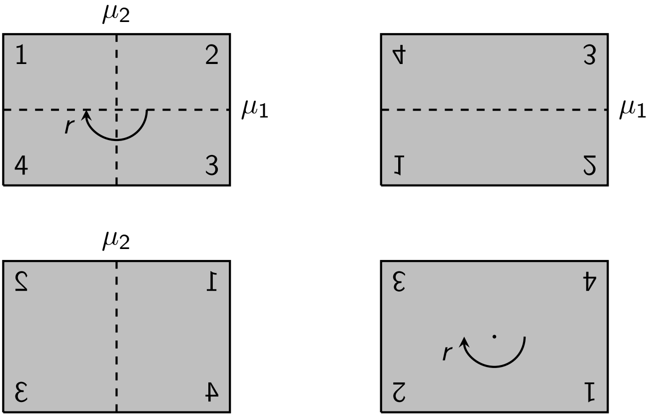
$$\mu_1^2 = 1$$



Symmetry group of a rectangle

$$\mu_1^2 = 1$$

$$\mu_2^2 = 1$$

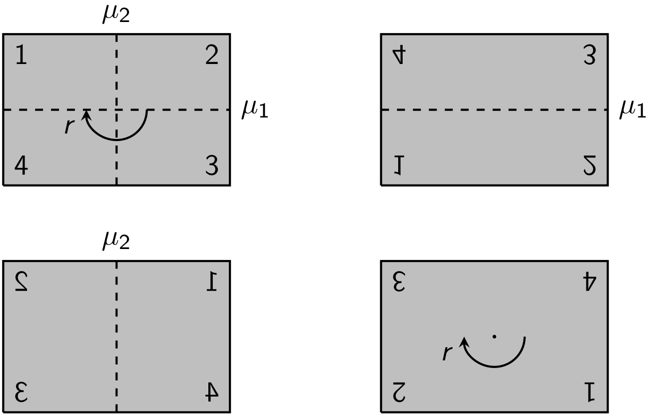


Symmetry group of a rectangle

$\mu_1^2 = 1$

$\mu_2^2 = 1$

$r^2 = 1$

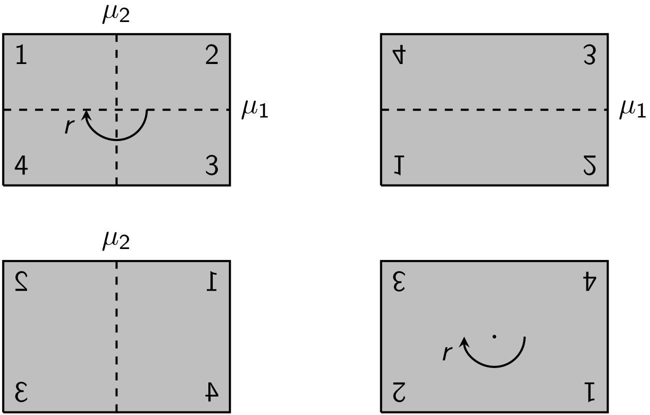


Symmetry group of a rectangle

$$\mu_1^2 = 1$$

$$\mu_2^2 = 1$$

$$r^2 = 1$$



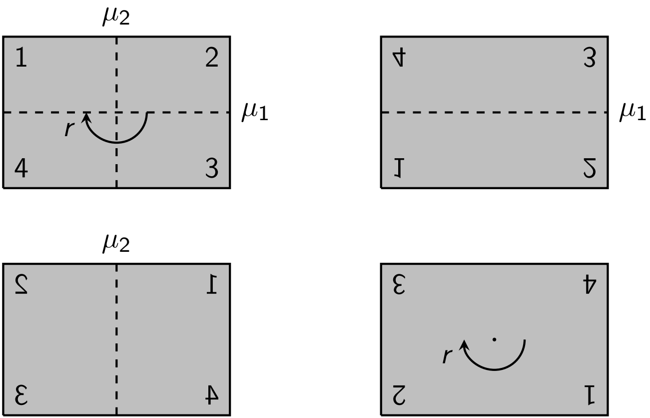
$\circ$	1	μ_1	μ_2	r
1				
μ_1				
μ_2				
r				

Symmetry group of a rectangle

$$\mu_1^2 = 1$$

$$\mu_2^2 = 1$$

$$r^2 = 1$$



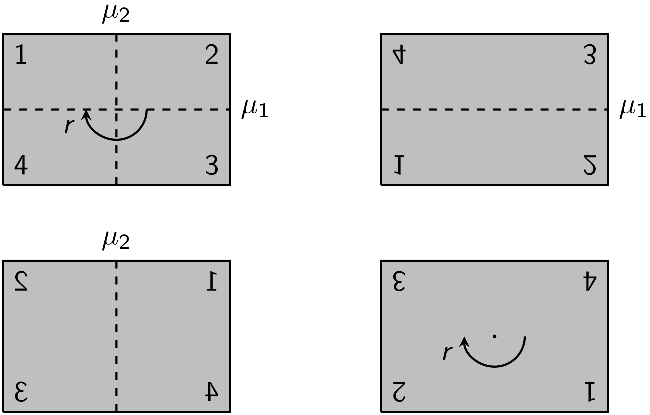
$\circ$	1	μ_1	μ_2	r
1	1	μ_1	μ_2	r
μ_1	μ_1			
μ_2	μ_2			
r	r			

Symmetry group of a rectangle

$$\mu_1^2 = 1$$

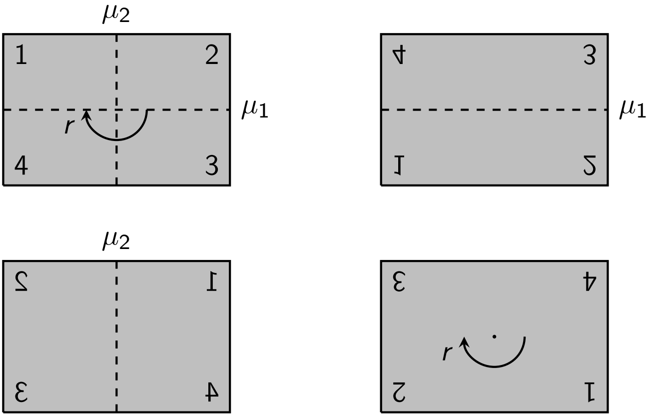
$$\mu_2^2 = 1$$

$$r^2 = 1$$



$\circ$	1	μ_1	μ_2	r
1	1	μ_1	μ_2	r
μ_1	μ_1	1		
μ_2	μ_2		1	
r	r			1

Symmetry group of a rectangle



$$\mu_1^2 = 1$$

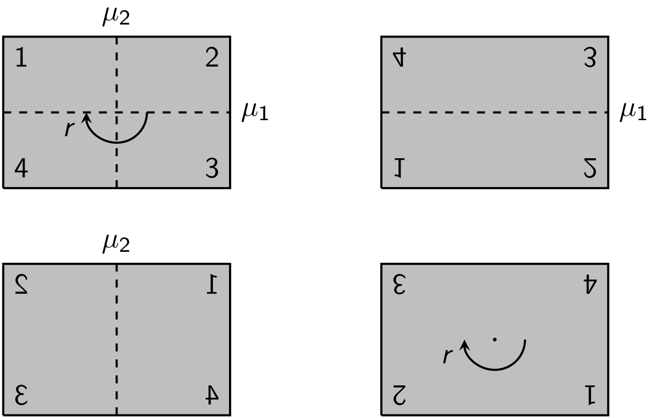
$$\mu_2^2 = 1$$

$$r^2 = 1$$

$$\mu_2\mu_1 = r$$

$\circ$	1	μ_1	μ_2	r
1	1	μ_1	μ_2	r
μ_1	μ_1	1		
μ_2	μ_2		1	
r	r			1

Symmetry group of a rectangle



$$\mu_1^2 = 1$$

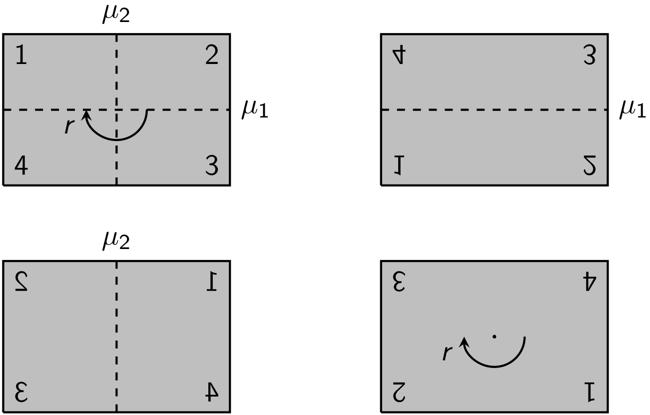
$$\mu_2^2 = 1$$

$$r^2 = 1$$

$$\mu_2 \mu_1 = r$$

$\circ$	1	μ_1	μ_2	r
1	1	μ_1	μ_2	r
μ_1	μ_1	1	r	
μ_2	μ_2	r	1	
r	r			1

Symmetry group of a rectangle



$$\mu_1^2 = 1$$

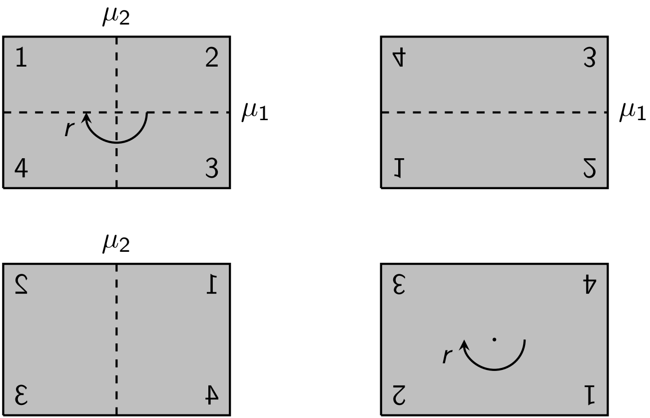
$$\mu_2^2 = 1$$

$$r^2 = 1$$

$$\mu_2 \mu_1 = r$$

$\circ$	1	μ_1	μ_2	r
1	1	μ_1	μ_2	r
μ_1	μ_1	1	r	μ_2
μ_2	μ_2	r	1	
r	r	μ_2		1

Symmetry group of a rectangle



$$\mu_1^2 = 1$$

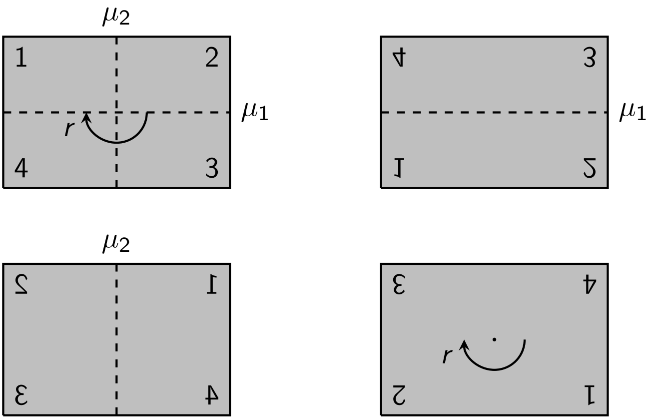
$$\mu_2^2 = 1$$

$$r^2 = 1$$

$$\mu_2\mu_1 = r$$

$\circ$	1	μ_1	μ_2	r
1	1	μ_1	μ_2	r
μ_1	μ_1	1	r	μ_2
μ_2	μ_2	r	1	μ_1
r	r	μ_2	μ_1	1

Symmetry group of a rectangle



$\mu_1^2 = 1$

$\mu_2^2 = 1$

$r^2 = 1$

$\mu_2\mu_1 = r$

$\circ$	1	μ_1	μ_2	r
1	1	μ_1	μ_2	r
μ_1	μ_1	1	r	μ_2
μ_2	μ_2	r	1	μ_1
r	r	μ_2	μ_1	1

Symmetry group of rectangle is Klein 4-group $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Symmetry group of a frieze pattern

Symmetry group of a frieze pattern

$t_n =$ move n units horizontally

Symmetry group of a frieze pattern

t_n = move n units horizontally

Group of symmetries:
$G = \{\ldots, t_{-3},\ t_{-2},\ t_{-1},\ t_0,\ t_1,\ t_2,\ t_3, \ldots\}$

Symmetry group of a frieze pattern

t_n = move n units horizontally

Group of symmetries:
$G = \{\ldots, t_{-3},\ t_{-2},\ t_{-1},\ t_0,\ t_1,\ t_2,\ t_3, \ldots\}$

Multiplication: $t_m t_n = t_{m+n}$

Symmetry group of a frieze pattern

t_n = move n units horizontally

Group of symmetries:

$G = \{\ldots, t_{-3},\ t_{-2},\ t_{-1},\ t_0,\ t_1,\ t_2,\ t_3, \ldots\}$

$G = \{\ldots, -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3, \ldots\}$

Multiplication: $t_m t_n = t_{m+n}$

Symmetry group of a frieze pattern

t_n = move n units horizontally

Group of symmetries:

$G = \{\ldots, t_{-3},\ t_{-2},\ t_{-1},\ t_0,\ t_1,\ t_2,\ t_3, \ldots\}$

$G = \{\ldots, -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3, \ldots\}$

Multiplication: $t_m t_n = t_{m+n}$

Multiplication: $m \star n = m + n$

Symmetry group of a frieze pattern

t_n = move n units horizontally

Group of symmetries:

$G = \{\ldots, t_{-3},\ t_{-2},\ t_{-1},\ t_0,\ t_1,\ t_2,\ t_3, \ldots\}$

$G = \{\ldots, -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3, \ldots\}$

Multiplication: $t_m t_n = t_{m+n}$

Multiplication: $m \star n = m + n$

$G \cong \mathbb{Z}$

Symmetry group of a frieze pattern

Symmetry group of a frieze pattern

t_n = move n units horizontally

Symmetry group of a frieze pattern

$t_n =$ move n units horizontally $\qquad t_m t_n = t_{m+n}$

Symmetry group of a frieze pattern

t_n = move n units horizontally $\qquad t_m t_n = t_{m+n}$

h = horizontal reflection

Symmetry group of a frieze pattern

t_n = move n units horizontally $\qquad t_m t_n = t_{m+n}$

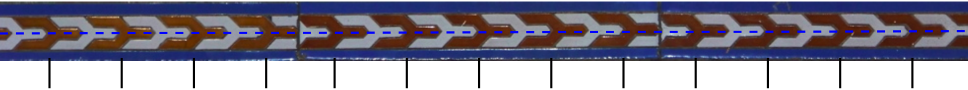
h = horizontal reflection

Symmetry group of a frieze pattern

$t_n =$ move n units horizontally $\qquad t_m t_n = t_{m+n}$

$h =$ horizontal reflection $\qquad h^2 = 1$

Symmetry group of a frieze pattern



$t_n =$ move n units horizontally $\qquad t_m t_n = t_{m+n}$

$h =$ horizontal reflection $\qquad h^2 = 1$ and $t_n h = h t_n$

Symmetry group of a frieze pattern

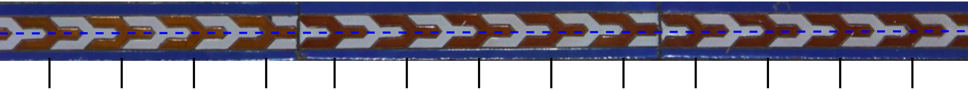
t_n = move n units horizontally $\qquad t_m t_n = t_{m+n}$

h = horizontal reflection $\qquad h^2 = 1$ and $t_n h = h t_n$

Group of symmetries:

$$G = \{\ldots, t_{-1}h^0,\ t_0h^0,\ t_1h^0,\ t_2h^0, \ldots\ \ \ldots, t_{-1}h^1,\ t_0h^1,\ t_1h^1,\ t_2h^1, \ldots\}$$

Symmetry group of a frieze pattern



$t_n =$ move n units horizontally $\qquad t_m t_n = t_{m+n}$

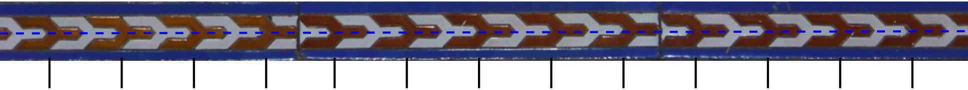
$h =$ horizontal reflection $\qquad h^2 = 1$ and $t_n h = h t_n$

Group of symmetries:

$$G = \{\ldots, t_{-1}h^0,\ t_0h^0,\ t_1h^0,\ t_2h^0, \ldots\ \ \ldots, t_{-1}h^1,\ t_0h^1,\ t_1h^1,\ t_2h^1, \ldots\}$$

$$\{\ldots, (-1,0),\ (0,0),\ (1,0),\ (2,0), \ldots\ \ \ldots,\ (-1,1),\ (0,1),\ (1,1),\ (2,1),\ \ldots\}$$

Symmetry group of a frieze pattern



$t_n =$ move n units horizontally $\qquad t_m t_n = t_{m+n}$

$h =$ horizontal reflection $\qquad h^2 = 1$ and $t_n h = h t_n$

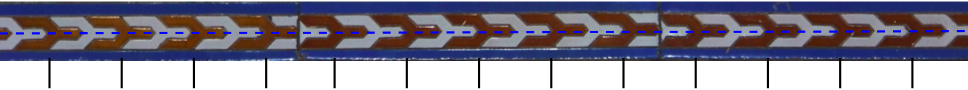
Group of symmetries:

$$G = \{\ldots, t_{-1}h^0,\ t_0h^0,\ t_1h^0,\ t_2h^0, \ldots\ \ \ldots, t_{-1}h^1,\ t_0h^1,\ t_1h^1,\ t_2h^1, \ldots\}$$

$$\{\ldots, (-1,0),\ (0,0),\ (1,0),\ (2,0), \ldots\ \ \ldots,\ (-1,1),\ (0,1),\ (1,1),\ (2,1),\ \ldots\}$$

Multiplication: $(t_m h^k)(t_n h^\ell) = t_m h^k t_n h^\ell = t_m t_n h^k h^\ell = t_{m+n} h^{k+\ell (\mathrm{mod}\ 2)}$

Symmetry group of a frieze pattern



$t_n =$ move n units horizontally $\qquad t_m t_n = t_{m+n}$

$h =$ horizontal reflection $\qquad h^2 = 1$ and $t_n h = h t_n$

Group of symmetries:

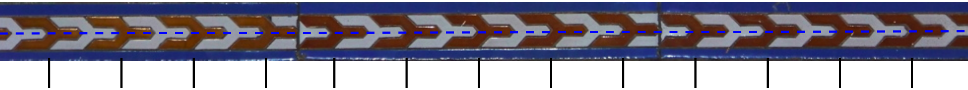
$$G = \{\ldots, t_{-1}h^0,\ t_0h^0,\ t_1h^0,\ t_2h^0, \ldots\ \ \ldots, t_{-1}h^1,\ t_0h^1,\ t_1h^1,\ t_2h^1, \ldots\}$$

$$\{\ldots, (-1,0),\ (0,0),\ (1,0),\ (2,0), \ldots\ \ \ldots,\ (-1,1),\ (0,1),\ (1,1),\ (2,1),\ \ldots\}$$

Multiplication: $(t_m h^k)(t_n h^\ell) = t_m h^k t_n h^\ell = t_m t_n h^k h^\ell = t_{m+n} h^{k+\ell (\text{mod } 2)}$

$$(m,k)+(n,\ell) = \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (m+n,\ k+\ell (\text{mod } 2))$$

Symmetry group of a frieze pattern



t_n = move n units horizontally $\qquad t_m t_n = t_{m+n}$

h = horizontal reflection $\qquad h^2 = 1$ and $t_n h = h t_n$

Group of symmetries:

$$G = \{\ldots, t_{-1}h^0,\ t_0h^0,\ t_1h^0,\ t_2h^0, \ldots\ \ \ldots, t_{-1}h^1,\ t_0h^1,\ t_1h^1,\ t_2h^1, \ldots\}$$

$$\{\ldots, (-1,0),\ (0,0),\ (1,0),\ (2,0), \ldots\ \ \ldots,\ (-1,1),\ (0,1),\ (1,1),\ (2,1),\ \ldots\}$$

Multiplication: $(t_m h^k)(t_n h^\ell) = t_m h^k t_n h^\ell = t_m t_n h^k h^\ell = t_{m+n} h^{k+\ell (\text{mod } 2)}$

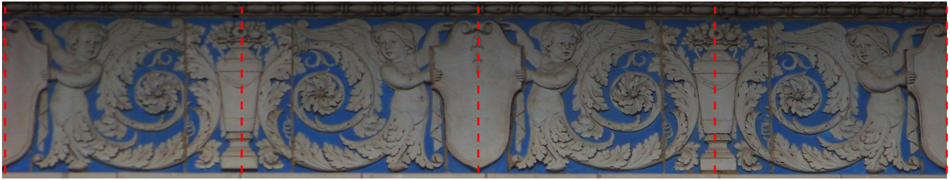
$$(m,k)+(n,\ell) = \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (m+n,\ k+\ell (\text{mod } 2))$$

$G \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

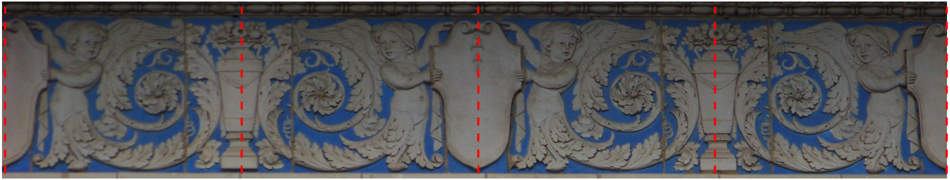
Further Examples

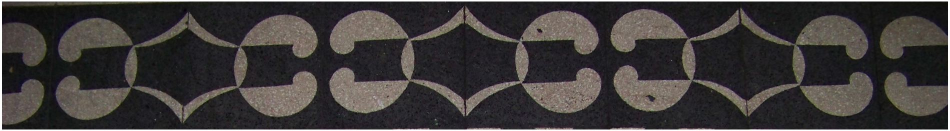
Further Examples

Further Examples

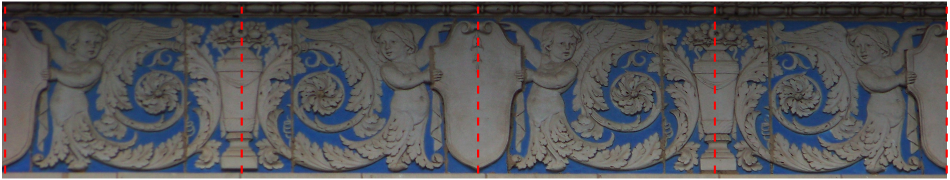


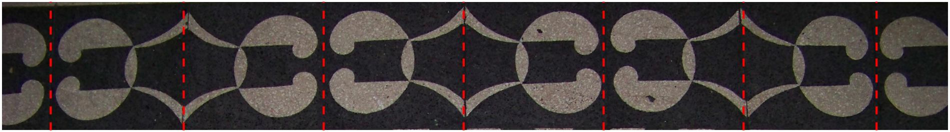
Further Examples



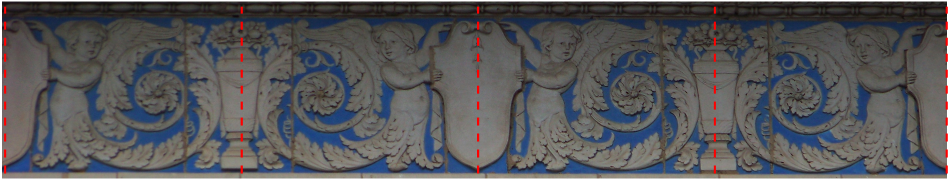


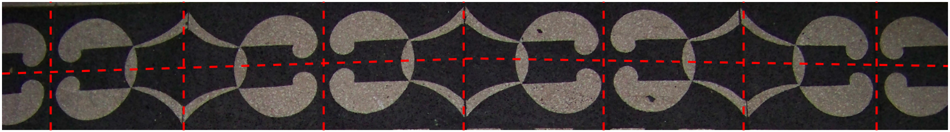
Further Examples



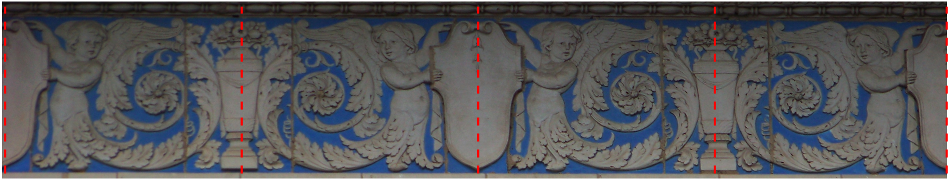


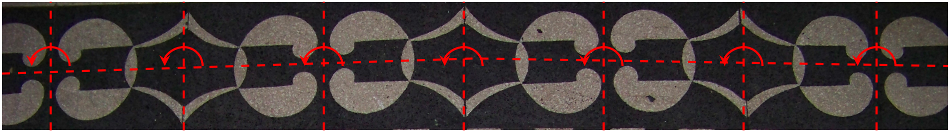
Further Examples



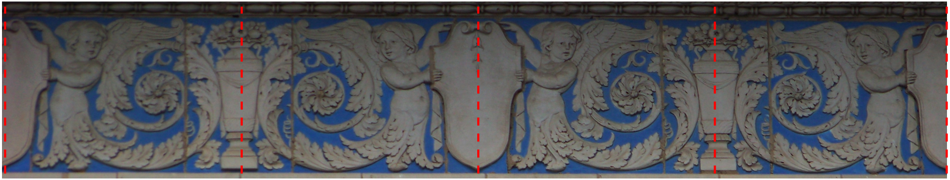


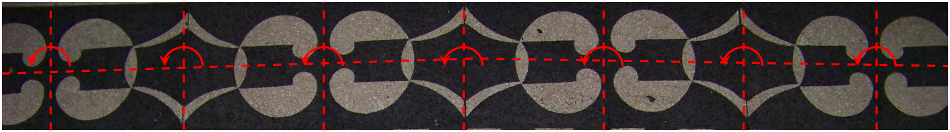
Further Examples





Further Examples





Describing groups of more complicated frieze patterns involves more sophisticated ideas in group theory (semi-direct products, etc.). This course will develop that theory, and more. Next time: **Dihedral groups**.