Brief Look at Groups, Rings, Fields, and Quotients

Dr. Chuck Rocca
roccac@wcsu.edu
http://sites.wcsu.edu/roccac

WESTERN CONNECTICUT STATE UNIVERSITY
MACRICOSTAS SCHOOL OF ARTS & SCIENCES

Table of Contents

Definition

Definition (Group)

A set G together with a binary operation $*$ is a group if it satisfies the following:

1. G is closed under $*$, $\forall a, b \in G : a * b \in G$
2. $*$ is associative, $\forall a, b, c \in G : a * (b * c) = (a * b) * c$
3. $\exists e \in G \; \forall a \in G : e * a = a * e = a$ (identity)
4. $\forall a \in G \; \exists a^{-1} \in G : a * a^{-1} = a^{-1} * a = e$ (inverses)

If in addition $\forall a, b \in G : a * b = b * a$, then we say G is commutative and call it an Abelian Group

Examples

Group Examples

- $(\mathbb{Z}, +)$

Examples

Group Examples

- $(\mathbb{Z}, +)$ ✓

Examples

Group Examples

- $(\mathbb{Z}, +)$ ✓
- $(\mathbb{Z}, \times)$

Examples

Group Examples

- $(\mathbb{Z}, +)$ ✓
- $(\mathbb{Z}, \times)$ ✗

Examples

Group Examples

- $(\mathbb{Z}, +)$ ✓
- $(\mathbb{Z}, \times)$ ✗
- $(\mathbb{Z}_n, +)$

Examples

Group Examples

- $(\mathbb{Z}, +)$ ✓
- $(\mathbb{Z}, \times)$ ✗
- $(\mathbb{Z}_n, +)$ ✓

Examples

Group Examples

- $(\mathbb{Z}, +)$ ✓
- $(\mathbb{Z}, \times)$ ✗
- $(\mathbb{Z}_n, +)$ ✓
- $(\mathbb{Z}_n, \times)$

Examples

Group Examples

- $(\mathbb{Z}, +)$ ✓
- $(\mathbb{Z}, \times)$ ✗
- $(\mathbb{Z}_n, +)$ ✓
- $(\mathbb{Z}_n, \times)$ ✗

Examples

Group Examples

- $(\mathbb{Z}, +)$ ✓
- $(\mathbb{Z}, \times)$ ✗
- $(\mathbb{Z}_n, +)$ ✓
- $(\mathbb{Z}_n, \times)$ ✗
- $(\mathbb{Z}_n^*, \times)$

Examples

Group Examples

- $(\mathbb{Z}, +)$ ✓
- $(\mathbb{Z}, \times)$ ✗
- $(\mathbb{Z}_n, +)$ ✓
- $(\mathbb{Z}_n, \times)$ ✗
- $(\mathbb{Z}_n^*, \times)$ ✓

Examples

Group Examples

- $(\mathbb{Z}, +)$ ✓
- $(\mathbb{Z}, \times)$ ✗
- $(\mathbb{Z}_n, +)$ ✓
- $(\mathbb{Z}_n, \times)$ ✗
- $(\mathbb{Z}_n^*, \times)$ ✓
- $(M_n(\mathbb{R}), +)$

Examples

Group Examples

- $(\mathbb{Z}, +)$ ✓
- $(\mathbb{Z}, \times)$ ✗
- $(\mathbb{Z}_n, +)$ ✓
- $(\mathbb{Z}_n, \times)$ ✗
- $(\mathbb{Z}_n^*, \times)$ ✓
- $(M_n(\mathbb{R}), +)$ ✓

Examples

Group Examples

- $(\mathbb{Z}, +)$ ✓
- $(\mathbb{Z}, \times)$ ✗
- $(\mathbb{Z}_n, +)$ ✓
- $(\mathbb{Z}_n, \times)$ ✗
- $(\mathbb{Z}_n^*, \times)$ ✓
- $(M_n(\mathbb{R}), +)$ ✓
- $(M_n(\mathbb{R}), \times)$

Examples

Group Examples

- $(\mathbb{Z}, +)$ ✓
- $(\mathbb{Z}, \times)$ ✗
- $(\mathbb{Z}_n, +)$ ✓
- $(\mathbb{Z}_n, \times)$ ✗
- $(\mathbb{Z}_n^*, \times)$ ✓
- $(M_n(\mathbb{R}), +)$ ✓
- $(M_n(\mathbb{R}), \times)$ ✗

Examples

Group Examples

- $(\mathbb{Z}, +)$ ✓
- $(\mathbb{Z}, \times)$ ✗
- $(\mathbb{Z}_n, +)$ ✓
- $(\mathbb{Z}_n, \times)$ ✗
- $(\mathbb{Z}_n^*, \times)$ ✓
- $(M_n(\mathbb{R}), +)$ ✓
- $(M_n(\mathbb{R}), \times)$ ✗
- $(GL_n(\mathbb{R}), \times)$

Examples

Group Examples

- $(\mathbb{Z}, +)$ ✓
- $(\mathbb{Z}, \times)$ ✗
- $(\mathbb{Z}_n, +)$ ✓
- $(\mathbb{Z}_n, \times)$ ✗
- $(\mathbb{Z}_n^*, \times)$ ✓
- $(M_n(\mathbb{R}), +)$ ✓
- $(M_n(\mathbb{R}), \times)$ ✗
- $(GL_n(\mathbb{R}), \times)$ ✓

Orders

Definition (Order of a Group)

If a group G is a finite group then its order is equal to the number of elements, otherwise the order is infinite. We may see this denoted as o(G) or $|G|$.

Orders

Definition (Order of a Group)

If a group G is a finite group then its order is equal to the number of elements, otherwise the order is infinite. We may see this denoted as o(G) or $|G|$.

Definition (Order of an Element)

Given $g \in G$, a group, if there exists d such that $g^d = e$ then we say the order of g is the least such power d, if no such power exists then we say g has infinite order. The order is sometimes denoted $o(g) = d$ or $|g| = d$.

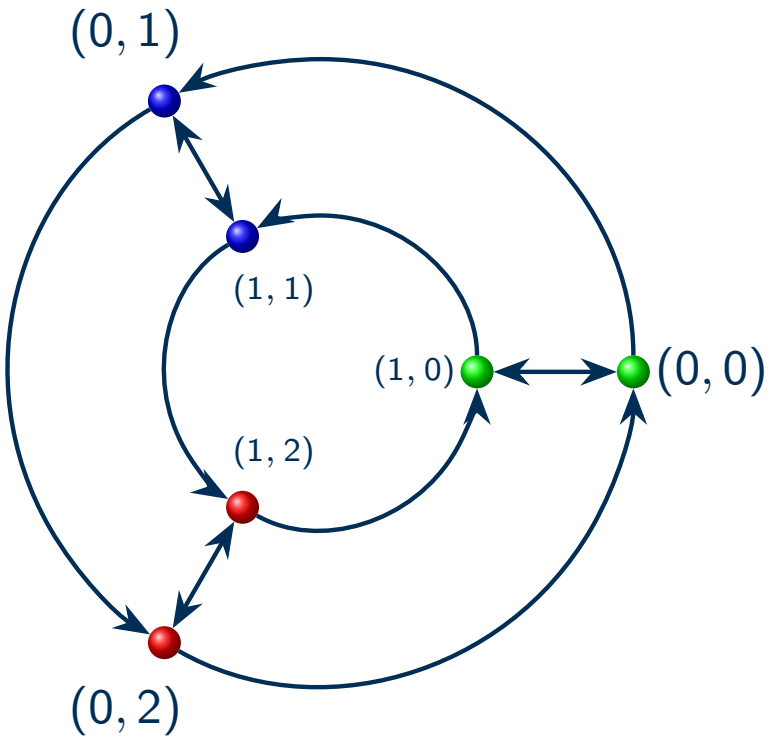
Lagrange's Theorem

Theorem (Lagrange's Theorem)

In a finite group G the order of every subgroup (and element) divides the order of G.

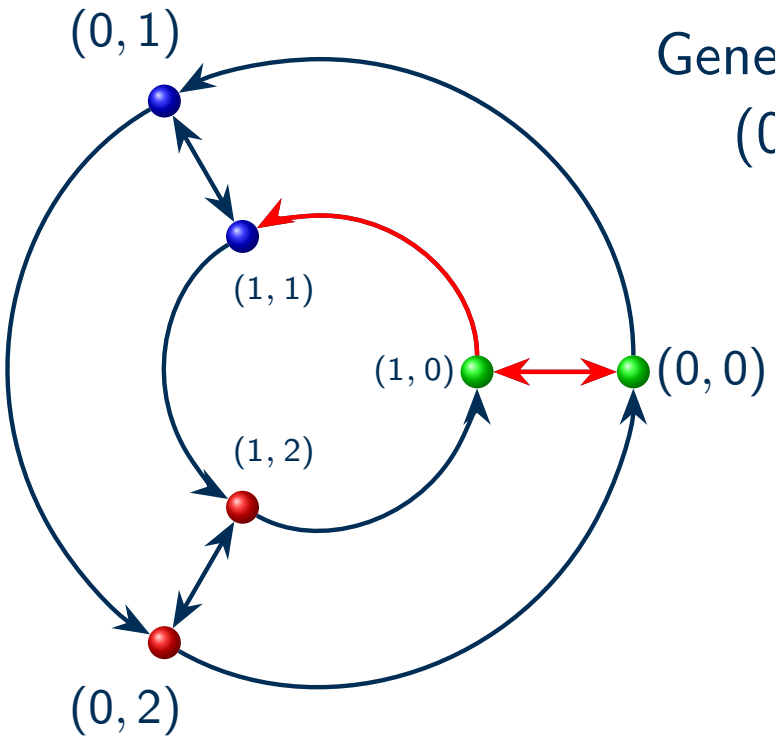
Lagrange's Theorem

$$G = \mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{(a, b) | a \in \mathbb{Z}_2,\ b \in \mathbb{Z}_3\} = \langle (1, 1) \rangle$$



Lagrange's Theorem

$$G = \mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{(a, b) | a \in \mathbb{Z}_2,\ b \in \mathbb{Z}_3\} = \langle (1, 1) \rangle$$

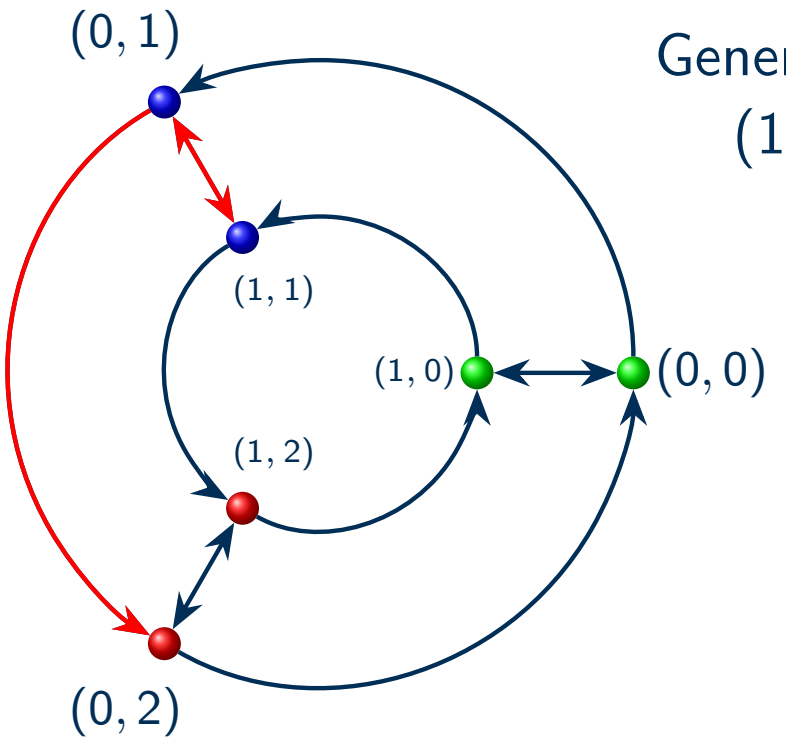


Generating with $(1, 1)$:

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

Lagrange's Theorem

$$G = \mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{(a, b) | a \in \mathbb{Z}_2,\ b \in \mathbb{Z}_3\} = \langle (1, 1) \rangle$$

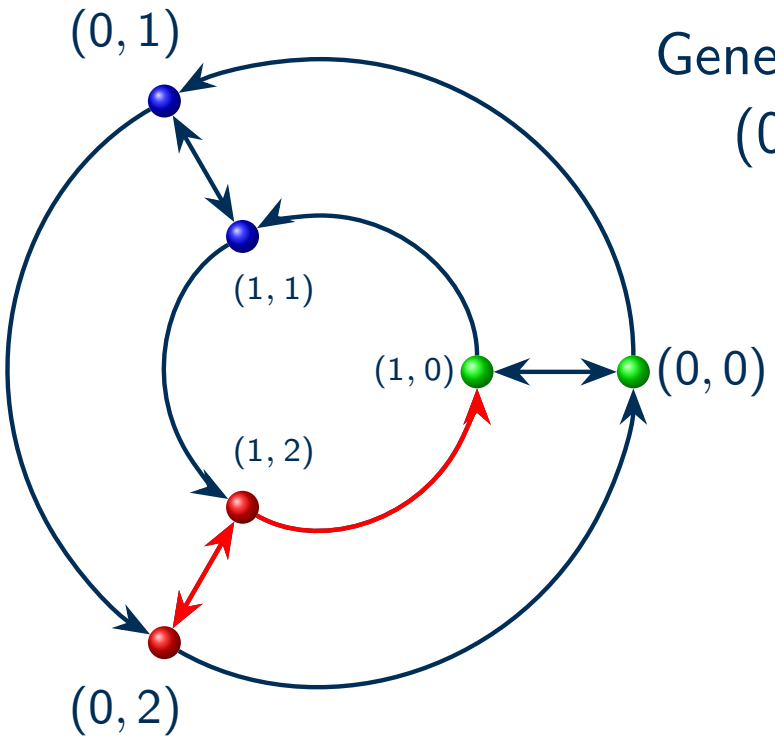


Generating with $(1, 1)$:

$$(1, 1) + (1, 1) = (0, 2)$$

Lagrange's Theorem

$$G = \mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{(a, b) | a \in \mathbb{Z}_2,\ b \in \mathbb{Z}_3\} = \langle (1, 1) \rangle$$

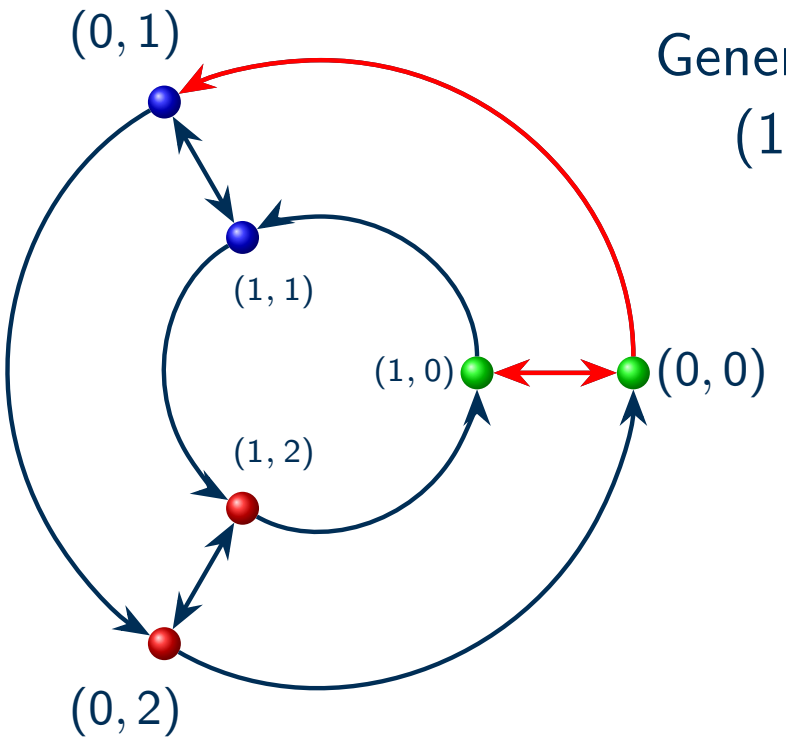


Generating with $(1, 1)$:

$$(0, 2) + (1, 1) = (1, 0)$$

Lagrange's Theorem

$$G = \mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{(a, b) | a \in \mathbb{Z}_2,\ b \in \mathbb{Z}_3\} = \langle (1, 1) \rangle$$

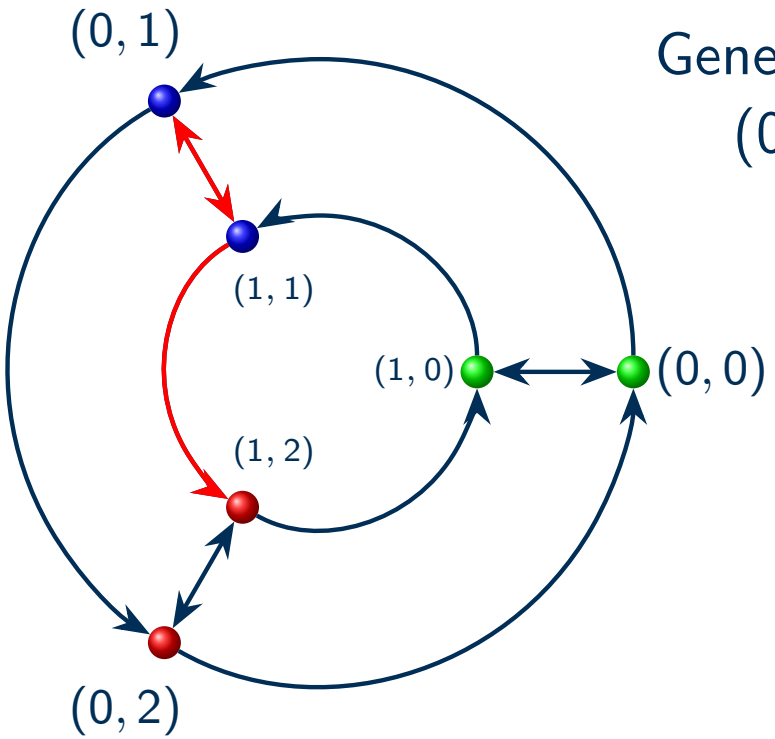


Generating with $(1, 1)$:

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

Lagrange's Theorem

$$G = \mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{(a, b) | a \in \mathbb{Z}_2,\ b \in \mathbb{Z}_3\} = \langle (1, 1) \rangle$$

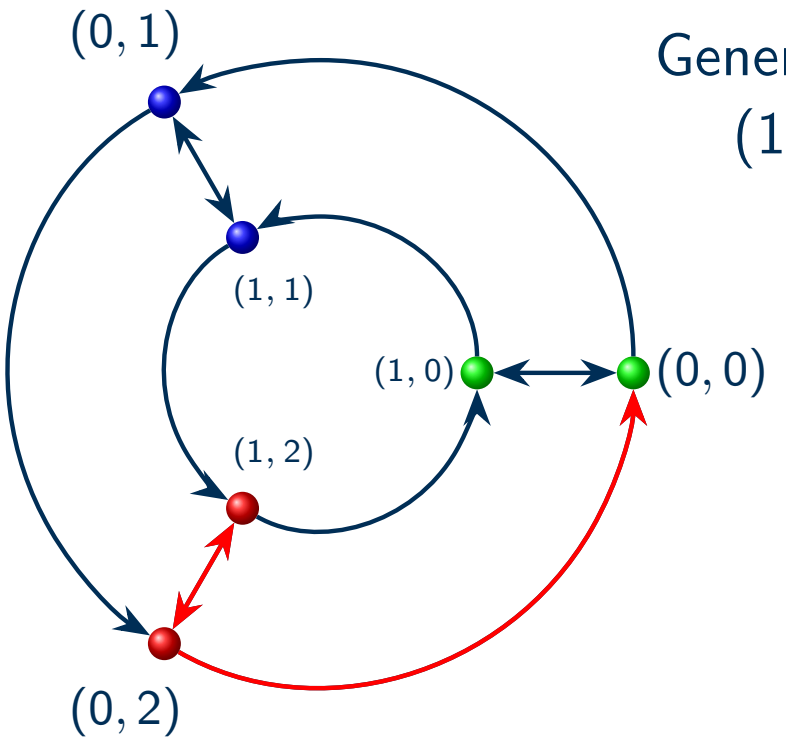


Generating with $(1, 1)$:

$$(0, 1) + (1, 1) = (1, 2)$$

Lagrange's Theorem

$$G = \mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{(a, b) | a \in \mathbb{Z}_2,\ b \in \mathbb{Z}_3\} = \langle (1, 1) \rangle$$

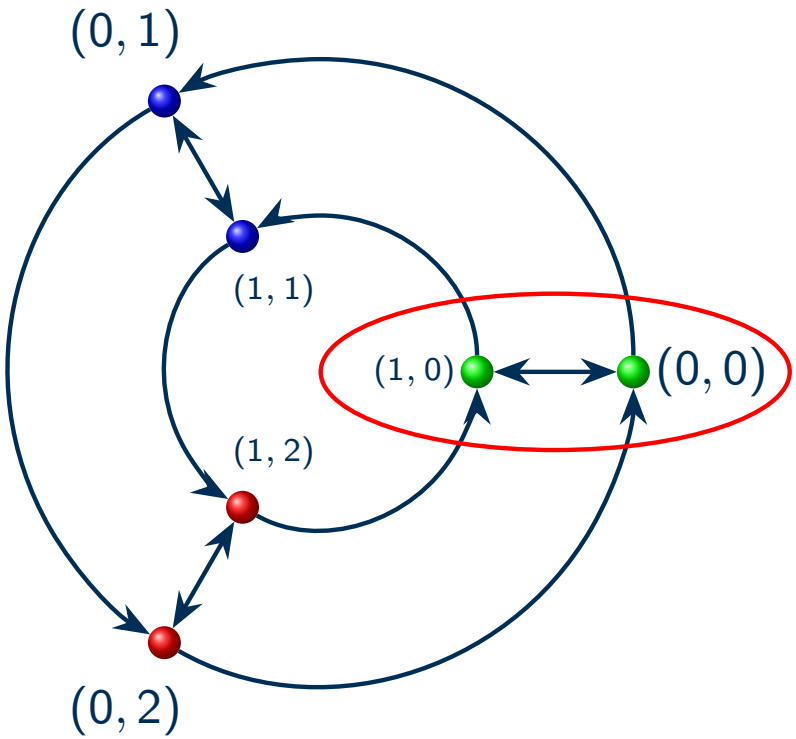


Generating with $(1, 1)$:

$$(1, 2) + (1, 1) = (0, 0)$$

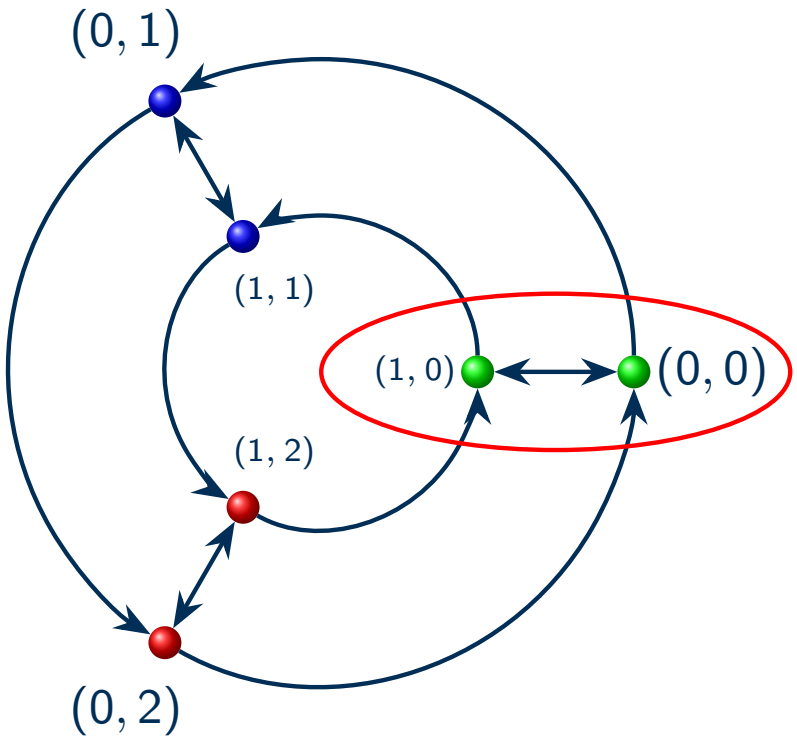
Lagrange's Theorem

$$G = \mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{(a, b) | a \in \mathbb{Z}_2,\ b \in \mathbb{Z}_3\} = \langle (1, 1) \rangle$$



Lagrange's Theorem

$$G = \mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{(a, b) | a \in \mathbb{Z}_2,\ b \in \mathbb{Z}_3\} = \langle (1, 1) \rangle$$

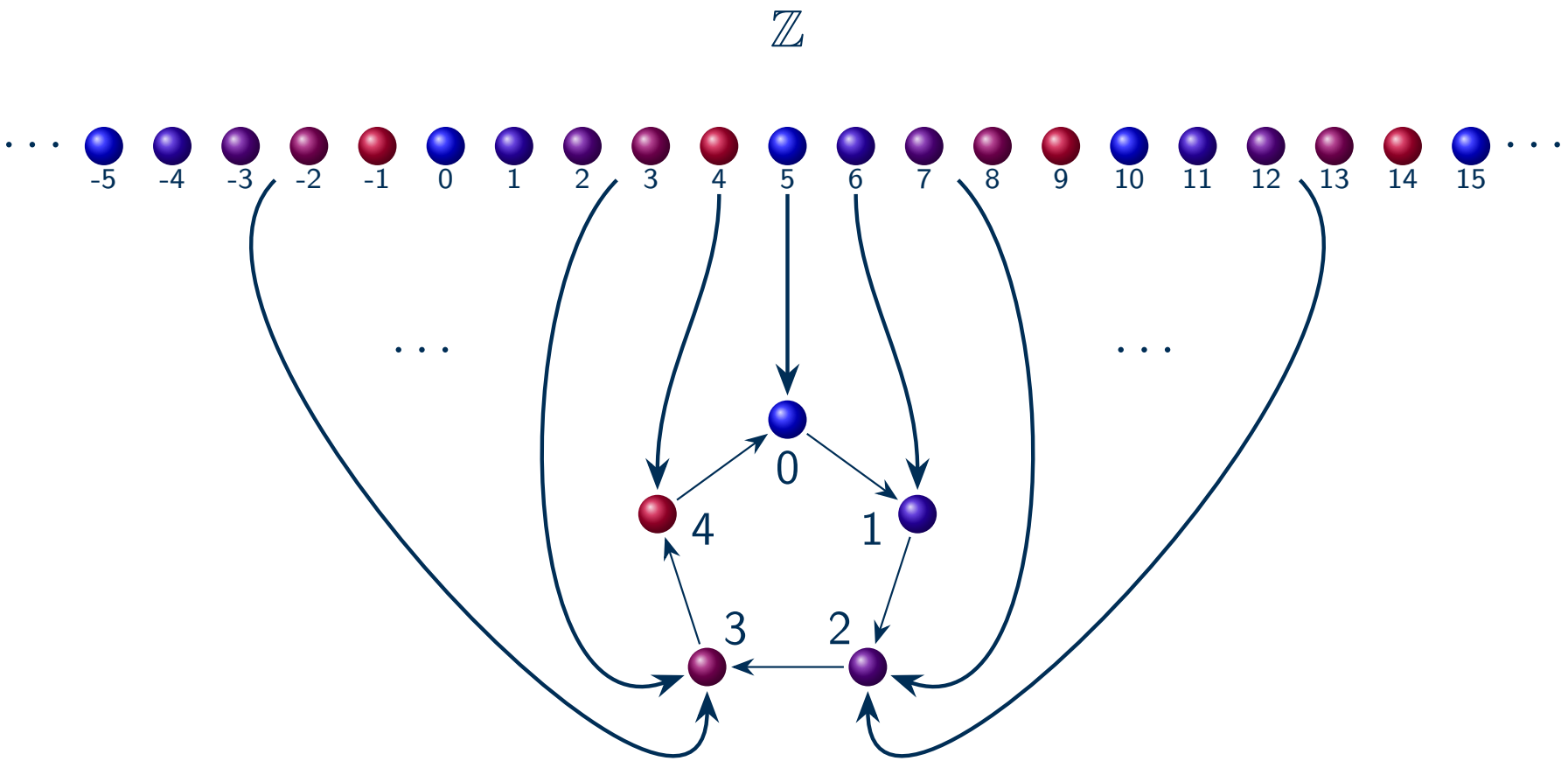


$$H = \{(0, 0), (1, 0)\}$$

$$(1, 1) + H = \{(1, 1), (0, 1)\}$$

$$(1, 2) + H = \{(1, 2), (0, 2)\}$$

Visualizing $\mathbb{Z}_n$



$$\mathbb{Z}_5 \cong \mathbb{Z}/5\mathbb{Z}$$

Table of Contents

Definition

Definition (Ring)

A ring is a set R together with two binary operations $+$ and $\times$ so that R is an abelian group with $+$ with identity is called 0, and

- $\forall a, b \in R : a \times b \in R$ (closure)
- $\forall a, b, c \in R : a \times (b \times c) = (a \times b) \times c$ (associative)
- $\forall a, b, c \in R : a \times (b + c) = (a \times b) + (a \times c)$ (distributive)
- $\forall a, b, c \in R : (b + c) \times a = (b \times a) + (c \times a)$ (distributive)
- $\exists 1 \forall a \in R : 1 \times a = a \times 1 = a$ (with unit)
- $\forall a, b \in R : a \times b = b \times a$ (commutative)

If in addition $R \setminus \{0\}$ is an abelian group we say that R is a field.

Example

Definition ($\mathbb{Z}_n$)

The integers modulo n is the set of equivalence classes of $\mathbb{Z}$ where $a, b \in \mathbb{Z}$ are equivalent if $n|(b-a)$. It can be shown that if $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$ then

$$a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$$

and

$$a_1 \times a_2 \equiv b_1 \times b_2 \pmod{n}$$

With this, $\mathbb{Z}_n$ is a ring.

Examples

$\mathbb{Z}_{10}$

- $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$
- $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$
- Zero divisors $\{2, 4, 5, 6, 8\}$
- $\mathbb{Z}_{10}$ is a ring but not a field.

Examples

$\mathbb{Z}_{10}$

- $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$
- $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$
- Zero divisors $\{2, 4, 5, 6, 8\}$
- $\mathbb{Z}_{10}$ is a ring but not a field.

$\mathbb{Z}_{11}$

- $\mathbb{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
- $\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
- Zero divisors $\{\}$
- $\mathbb{Z}_{11}$ is a ring and a field.
- $\mathbb{F}_{11} = \mathbb{Z}_{11}$

Table of Contents

Definition

Definition (Polynomials)

A polynomial of degree n over a field $\mathbb{F}$ is an expression of the form

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_nx^n$$

with $a_i \in \mathbb{F}$, $\forall i$. The set of all such expressions is denoted $\mathbb{F}[x]$ and forms a ring. Note that $f(x) = 0$ has no degree while other constants have degree 0.

Definition

Definition (Polynomials)

A polynomial of degree n over a field $\mathbb{F}$ is an expression of the form

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_nx^n$$

with $a_i \in \mathbb{F}$, $\forall i$. The set of all such expressions is denoted $\mathbb{F}[x]$ and forms a ring. Note that $f(x) = 0$ has no degree while other constants have degree 0.

Definition (Reducible/Irreducible)

A polynomial $f(x)$ of degree n is reducible if there exist polynomials $g(x)$ and $h(x)$ of degree greater than 0 such that $f(x) = g(x)h(x)$, otherwise we will call the polynomial irreducible.

Examples

- $f(x) = x^2 + 1$ is irreducible over $\mathbb{R}$
- $f(x) = x^2 + 1 = (x - i)(x + i)$ over $\mathbb{C}$, so reduces
- $f(x) = x^2 + 1 = x^2 - 1 = (x - 1)(x + 1)$ over $\mathbb{Z}_2$, so reduces
- $g(x) = x^4 - 2$ is irreducible over the ring $\mathbb{Z}$
- $g(x) = x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x^2 + \sqrt{2})$ over $\mathbb{R}$, so reduces
- $g(x) = x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2})$ over $\mathbb{C}$, so reduces

Polynomials vs. Integers

Integers:

- Prime

Polynomials:

Polynomials vs. Integers

Integers:

- Prime

Polynomials:

- Irreducible

Polynomials vs. Integers

Integers:

- Prime
- $a = qb + r$, $0 \leq r < |b|$

Polynomials:

- Irreducible

Polynomials vs. Integers

Integers:

- Prime
- $a = qb + r$, $0 \leq r < |b|$

Polynomials:

- Irreducible
- $a(x) = q(x)b(x) + r(x)$, $\deg(r) < \deg(b)$

Polynomials vs. Integers

Integers:

- Prime
- $a = qb + r$, $0 \leq r < |b|$
- Euclidean Algorithm

Polynomials:

- Irreducible
- $a(x) = q(x)b(x) + r(x)$, $\deg(r) < \deg(b)$

Polynomials vs. Integers

Integers:

- Prime
- $a = qb + r$, $0 \leq r < |b|$
- Euclidean Algorithm

Polynomials:

- Irreducible
- $a(x) = q(x)b(x) + r(x)$, $\deg(r) < \deg(b)$
- Euclidean Algorithm

Polynomials vs. Integers

Integers:

- Prime
- $a = qb + r$, $0 \leq r < |b|$
- Euclidean Algorithm
- $\mathbb{Z}/n\mathbb{Z}$ is a ring

Polynomials:

- Irreducible
- $a(x) = q(x)b(x) + r(x)$, $\deg(r) < \deg(b)$
- Euclidean Algorithm

Polynomials vs. Integers

Integers:

- Prime
- $a = qb + r$, $0 \leq r < |b|$
- Euclidean Algorithm
- $\mathbb{Z}/n\mathbb{Z}$ is a ring

Polynomials:

- Irreducible
- $a(x) = q(x)b(x) + r(x)$, $\deg(r) < \deg(b)$
- Euclidean Algorithm
- $\mathbb{F}[x]/\langle f(x) \rangle$ is a ring

Polynomials vs. Integers

Integers:

- Prime
- $a = qb + r$, $0 \leq r < |b|$
- Euclidean Algorithm
- $\mathbb{Z}/n\mathbb{Z}$ is a ring
- $\mathbb{Z}/p\mathbb{Z}$ is a field if p is prime

Polynomials:

- Irreducible
- $a(x) = q(x)b(x) + r(x)$, $\deg(r) < \deg(b)$
- Euclidean Algorithm
- $\mathbb{F}[x]/\langle f(x) \rangle$ is a ring

Polynomials vs. Integers

Integers:

- Prime
- $a = qb + r$, $0 \leq r < |b|$
- Euclidean Algorithm
- $\mathbb{Z}/n\mathbb{Z}$ is a ring
- $\mathbb{Z}/p\mathbb{Z}$ is a field if p is prime

Polynomials:

- Irreducible
- $a(x) = q(x)b(x) + r(x)$, $\deg(r) < \deg(b)$
- Euclidean Algorithm
- $\mathbb{F}[x]/\langle f(x)\rangle$ is a ring
- $\mathbb{F}[x]/\langle f(x)\rangle$ is a field if f is irreducible

Modular Arithmetic in $GF(2^3) \cong \mathbb{F}_2[x]/\langle x^3 + x + 1 \rangle$

- $f(x) = x^3 + x + 1$ is irreducible over $\mathbb{F}_2$
- $|\mathbb{F}_2[x]/\langle f(x) \rangle| = 8$ corresponding to possible values of $a_0 + a_1 x + a_2 x^2$
- With $h(x) = x + 1$ and $g(x) = x^2 + x + 1$

$$h(x) + g(x) = x^2 + 2x + 2 \equiv x^2 \pmod{f(x)}$$

- With $h(x) = x + 1$ and $g(x) = x^2 + x + 1$

$$h(x) \cdot g(x) = x^3 + 2x^2 + 2x + 1 \equiv x^3 + 1 \equiv x \pmod{f(x)}$$

- With $h(x) = x + 1$ and $\overline{h}(x) = x^2 + x$

$$h(x) \cdot \overline{h}(x) = x^3 + 2x^2 + x \equiv x^3 + x \equiv 1 \pmod{f(x)}$$

Modular Arithmetic in $GF(2^3) \cong \mathbb{F}_2[x]/\langle x^3 + x + 1 \rangle$

- $x^3 + x + 1 \equiv 0 \pmod{f(x)}$

Modular Arithmetic in $GF(2^3) \cong \mathbb{F}_2[x]/\langle x^3 + x + 1 \rangle$

- $x^3 + x + 1 \equiv 0 \pmod{f(x)}$
- $x^3 \equiv x + 1 \pmod{f(x)}$

Modular Arithmetic in $GF(2^3) \cong \mathbb{F}_2[x]/\langle x^3 + x + 1 \rangle$

- $x^3 + x + 1 \equiv 0 \pmod{f(x)}$
- $x^3 \equiv x + 1 \pmod{f(x)}$
- $x^4 \equiv x^2 + x \pmod{f(x)}$

Modular Arithmetic in $GF(2^3) \cong \mathbb{F}_2[x]/\langle x^3 + x + 1 \rangle$

- $x^3 + x + 1 \equiv 0 \pmod{f(x)}$
- $x^3 \equiv x + 1 \pmod{f(x)}$
- $x^4 \equiv x^2 + x \pmod{f(x)}$

$$(a_2x^2 + a_1x + a_0)(b_2x^2 + b_1x + b_0)$$

Modular Arithmetic in $GF(2^3) \cong \mathbb{F}_2[x]/\langle x^3 + x + 1 \rangle$

- $x^3 + x + 1 \equiv 0 \pmod{f(x)}$
- $x^3 \equiv x + 1 \pmod{f(x)}$
- $x^4 \equiv x^2 + x \pmod{f(x)}$

$$\begin{aligned}(a_2x^2 + a_1x + a_0)(b_2x^2 + b_1x + b_0) \\ = a_2b_2x^4 + (a_2b_1 + a_1b_2)x^3 \\ + (a_2b_0 + a_1b_1 + a_0b_2)x^2 + (a_1b_0 + a_0b_1)x + a_0b_0\end{aligned}$$

Modular Arithmetic in $GF(2^3) \cong \mathbb{F}_2[x]/\langle x^3 + x + 1 \rangle$

- $x^3 + x + 1 \equiv 0 \pmod{f(x)}$
- $x^3 \equiv x + 1 \pmod{f(x)}$
- $x^4 \equiv x^2 + x \pmod{f(x)}$

$$
\begin{aligned}
&(a_2x^2 + a_1x + a_0)(b_2x^2 + b_1x + b_0) \\
&\quad = a_2b_2x^4 + (a_2b_1 + a_1b_2)x^3 \\
&\qquad + (a_2b_0 + a_1b_1 + a_0b_2)x^2 + (a_1b_0 + a_0b_1)x + a_0b_0 \\
&\quad \equiv (a_2b_2 + a_2b_0 + a_1b_1 + a_0b_2)x^2 \\
&\qquad + (a_2b_2 + a_2b_1 + a_1b_2 + a_1b_0 + a_0b_1)x \\
&\qquad + (a_2b_1 + a_1b_2 + a_0b_0)
\end{aligned}
$$

Bit Operations

Definition (Crumb)

Let a sequence of three bits, 1's or 0's, be called a crumb, then we can define addition of crumbs by

$$(a_2\ a_1\ a_0) + (b_2\ b_1\ b_0) \equiv (a_2 + b_2\ a_1 + b_1\ a_0 + b_0) \pmod 2$$

and multiplication of crumbs, $(a_2\ a_1\ a_0) \times (b_2\ b_1\ b_0) = (c_2\ c_1\ c_0)$, by

$$\begin{aligned} c_2 &= (a_2b_2 + a_2b_0 + a_1b_1 + a_0b_2) && \pmod 2 \\ c_1 &= (a_2b_2 + a_2b_1 + a_1b_2 + a_1b_0 + a_0b_1) && \pmod 2 \\ c_3 &= (a_2b_1 + a_1b_2 + a_0b_0) && \pmod 2 \end{aligned}$$

We know that these operations are well defined and invertible because we can associate each crumb with an element of $GF(2^3) \cong \mathbb{F}_2[x]/\langle x^3 + x + 1\rangle$

Brief Look at Groups, Rings, Fields, and Quotients

Dr. Chuck Rocca
roccac@wcsu.edu
http://sites.wcsu.edu/roccac

WESTERN CONNECTICUT STATE UNIVERSITY
MACRICOSTAS SCHOOL OF ARTS & SCIENCES