CS250: Discrete Math for Computer Science

L15: Γ_Z and worlds $W \in \mathrm{World}[\Sigma_{\#thy}]$

$$\Sigma_{\#\mathrm{thy}} \stackrel{\mathrm{def}}{=} (\leq^2\ [\mathrm{infix}]; 0, 1, +^2[\mathrm{infix}], \cdot^2[\mathrm{infix}])$$

$$\mathbf{N},\ \mathbf{Z},\ \mathbf{Q},\ \mathbf{R} \in \mathrm{World}[\Sigma_{\#\mathrm{thy}}]$$

$$\text{“1 is id for }\cdot\text{”} \stackrel{\mathrm{def}}{=} \forall x\ x \cdot 1 = x$$

$$\mathbf{N},\ \mathbf{Z},\ \mathbf{Q},\ \mathbf{R} \models \text{“1 is id for }\cdot\text{”}$$

$$x < y \hookrightarrow x \leq y \land x \neq y$$

$$x|y \hookrightarrow \exists z\,(x \cdot z = y)$$

$$\mathrm{prime}(x) \hookrightarrow 1 < x \land \forall yz\,(1 < y \land x = y \cdot z \to y = x)$$

Prop. 13.1 $\Gamma_Z \vdash \forall xyz\,(x|y \land x|z \to x|(y+z))$

Prop. 13.2 $\Gamma_Z \vdash \forall xyz\,(x|y \to x|(y \cdot z))$

Prop. 13.3 $\Gamma_Z \vdash \forall xyz\,(x|y \land y|z \to x|z)$

Let's look at $\Gamma_Z \subseteq \mathrm{PredCalc}(\Sigma_{\#thy})$

$$R_1 \stackrel{\text{def}}{=} \forall x\, y\, z\, (x + (y + z) = (x + y) + z)$$ + is associative

Let's look at $\Gamma_Z \subseteq \mathrm{PredCalc}(\Sigma_{\#thy})$

$R_1 \stackrel{\text{def}}{=} \forall x\, y\, z\, (x + (y + z) = (x + y) + z)$ + is associative

$R_2 \stackrel{\text{def}}{=} \forall x\, y\, (x + y = y + x)$ + is commutative

Let's look at $\Gamma_Z \subseteq \mathrm{PredCalc}(\Sigma_{\#thy})$

$R_1 \stackrel{\text{def}}{=} \forall x\, y\, z\, (x + (y + z) = (x + y) + z)$ + is associative

$R_2 \stackrel{\text{def}}{=} \forall x\, y\, (x + y = y + x)$ + is commutative

$R_3 \stackrel{\text{def}}{=} 0 \neq 1 \wedge \forall x\; x + 0 = x$ 0 is id for $+$

Let's look at $\Gamma_Z \subseteq \mathrm{PredCalc}(\Sigma_{\#thy})$

R_1	$\stackrel{\mathrm{def}}{=}$	$\forall x\, y\, z\, (x + (y + z) \;=\; (x + y) + z)$	+ is associative
R_2	$\stackrel{\mathrm{def}}{=}$	$\forall x\, y\, (x + y \;=\; y + x)$	+ is commutative
R_3	$\stackrel{\mathrm{def}}{=}$	$0 \neq 1 \;\wedge\; \forall x\; x + 0 = x$	0 is id for $+$
R_4	$\stackrel{\mathrm{def}}{=}$	$\forall x\; \exists y\; x + y = 0$	Additive inverses

Let's look at $\Gamma_Z \subseteq \mathrm{PredCalc}(\Sigma_{\#thy})$

$R_1 \stackrel{\text{def}}{=} \forall x\, y\, z\, (x + (y + z) \;=\; (x + y) + z)$ + is associative

$R_2 \stackrel{\text{def}}{=} \forall x\, y\, (x + y \;=\; y + x)$ + is commutative

$R_3 \stackrel{\text{def}}{=} 0 \neq 1 \;\wedge\; \forall x\; x + 0 = x$ 0 is id for $+$

$R_4 \stackrel{\text{def}}{=} \forall x\; \exists y\; x + y = 0$ Additive inverses

$R_5 \stackrel{\text{def}}{=} \forall x\, y\, z\, (x \cdot (y \cdot z) \;=\; (x \cdot y) \cdot z)$ · is associative

Let's look at $\Gamma_Z \subseteq \mathrm{PredCalc}(\Sigma_{\#thy})$

R_1	$\stackrel{\text{def}}{=}$	$\forall x\, y\, z\, (x + (y + z) \;=\; (x + y) + z)$	+ is associative
R_2	$\stackrel{\text{def}}{=}$	$\forall x\, y\, (x + y \;=\; y + x)$	+ is commutative
R_3	$\stackrel{\text{def}}{=}$	$0 \neq 1 \;\wedge\; \forall x\; x + 0 = x$	0 is id for $+$
R_4	$\stackrel{\text{def}}{=}$	$\forall x\; \exists y\; x + y = 0$	Additive inverses
R_5	$\stackrel{\text{def}}{=}$	$\forall x\, y\, z\, (x \cdot (y \cdot z) \;=\; (x \cdot y) \cdot z)$	$\cdot$ is associative
R_6	$\stackrel{\text{def}}{=}$	$\forall x\; x \cdot 1 = x$	1 is id for $\cdot$

Let's look at $\Gamma_Z \subseteq \mathrm{PredCalc}(\Sigma_{\#thy})$

R_1	$\stackrel{\text{def}}{=}$	$\forall x\, y\, z\, (x + (y + z) \;=\; (x + y) + z)$	+ is associative
R_2	$\stackrel{\text{def}}{=}$	$\forall x\, y\, (x + y \;=\; y + x)$	+ is commutative
R_3	$\stackrel{\text{def}}{=}$	$0 \neq 1 \;\wedge\; \forall x\; x + 0 = x$	0 is id for $+$
R_4	$\stackrel{\text{def}}{=}$	$\forall x\, \exists y\; x + y = 0$	Additive inverses
R_5	$\stackrel{\text{def}}{=}$	$\forall x\, y\, z\, (x \cdot (y \cdot z) \;=\; (x \cdot y) \cdot z)$	$\cdot$ is associative
R_6	$\stackrel{\text{def}}{=}$	$\forall x\; x \cdot 1 = x$	1 is id for $\cdot$
R_7	$\stackrel{\text{def}}{=}$	$\forall x\, y\, z (x \cdot (y + z) = x \cdot y + x \cdot z) \wedge (y + z) \cdot x = y \cdot x + z \cdot x)$	+ distributes over $\cdot$

Let's look at $\Gamma_Z \subseteq \mathrm{PredCalc}(\Sigma_{\#thy})$

R_1	$\stackrel{\text{def}}{=}$	$\forall x\, y\, z\, (x + (y + z) \; = \; (x + y) + z)$	+ is associative
R_2	$\stackrel{\text{def}}{=}$	$\forall x\, y\, (x + y \; = \; y + x)$	+ is commutative
R_3	$\stackrel{\text{def}}{=}$	$0 \neq 1 \;\wedge\; \forall x\; x + 0 = x$	0 is id for $+$
R_4	$\stackrel{\text{def}}{=}$	$\forall x\, \exists y\; x + y = 0$	Additive inverses
R_5	$\stackrel{\text{def}}{=}$	$\forall x\, y\, z\, (x \cdot (y \cdot z) \; = \; (x \cdot y) \cdot z)$	$\cdot$ is associative
R_6	$\stackrel{\text{def}}{=}$	$\forall x\; x \cdot 1 = x$	1 is id for $\cdot$
R_7	$\stackrel{\text{def}}{=}$	$\forall x\, y\, z (x \cdot (y + z) = x \cdot y + x \cdot z) \wedge (y + z) \cdot x = y \cdot x + z \cdot x)$	+ distributes over $\cdot$
CR	$\stackrel{\text{def}}{=}$	$\forall x\, y\, (x \cdot y \; = \; y \cdot x)$	$\cdot$ is commutative

Let's look at $\Gamma_Z \subseteq \mathrm{PredCalc}(\Sigma_{\#thy})$

R_1	$\stackrel{\text{def}}{=}$	$\forall x\,y\,z\,(x + (y + z) \;=\; (x + y) + z)$	+ is associative
R_2	$\stackrel{\text{def}}{=}$	$\forall x\,y\,(x + y \;=\; y + x)$	+ is commutative
R_3	$\stackrel{\text{def}}{=}$	$0 \neq 1 \;\wedge\; \forall x\; x + 0 = x$	0 is id for $+$
R_4	$\stackrel{\text{def}}{=}$	$\forall x\; \exists y\; x + y = 0$	Additive inverses
R_5	$\stackrel{\text{def}}{=}$	$\forall x\,y\,z\,(x \cdot (y \cdot z) \;=\; (x \cdot y) \cdot z)$	$\cdot$ is associative
R_6	$\stackrel{\text{def}}{=}$	$\forall x\; x \cdot 1 = x$	1 is id for $\cdot$
R_7	$\stackrel{\text{def}}{=}$	$\forall x\,y\,z(x \cdot (y + z) = x \cdot y + x \cdot z) \wedge (y + z) \cdot x = y \cdot x + z \cdot x)$	+ distributes over $\cdot$
CR	$\stackrel{\text{def}}{=}$	$\forall x\,y\,(x \cdot y \;=\; y \cdot x)$	$\cdot$ is commutative

Def. A **ring** is a world $W \in \mathrm{World}[\Sigma_{\#thy}]$ s.t. $W \models R_1 \wedge \cdots \wedge R_7$

Let's look at $\Gamma_Z \subseteq \mathrm{PredCalc}(\Sigma_{\#\text{thy}})$

R_1	$\stackrel{\text{def}}{=}$	$\forall x\, y\, z\, (x + (y + z) \;=\; (x + y) + z)$	+ is associative
R_2	$\stackrel{\text{def}}{=}$	$\forall x\, y\, (x + y \;=\; y + x)$	+ is commutative
R_3	$\stackrel{\text{def}}{=}$	$0 \neq 1 \;\wedge\; \forall x\; x + 0 = x$	0 is id for $+$
R_4	$\stackrel{\text{def}}{=}$	$\forall x\, \exists y\; x + y = 0$	Additive inverses
R_5	$\stackrel{\text{def}}{=}$	$\forall x\, y\, z\, (x \cdot (y \cdot z) \;=\; (x \cdot y) \cdot z)$	$\cdot$ is associative
R_6	$\stackrel{\text{def}}{=}$	$\forall x\; x \cdot 1 = x$	1 is id for $\cdot$
R_7	$\stackrel{\text{def}}{=}$	$\forall x\, y\, z(x \cdot (y + z) = x \cdot y + x \cdot z) \wedge$ $(y + z) \cdot x = y \cdot x + z \cdot x)$	+ distributes over $\cdot$
CR	$\stackrel{\text{def}}{=}$	$\forall x\, y\, (x \cdot y \;=\; y \cdot x)$	$\cdot$ is commutative

Def. A **ring** is a world $W \in \mathrm{World}[\Sigma_{\#\text{thy}}]$ s.t. $W \models R_1 \wedge \cdots \wedge R_7$

Def. A **commutative ring** is a ring that satisfies CR

Let's look at $\Gamma_Z \subseteq \mathrm{PredCalc}(\Sigma_{\#thy})$

R_1	$\stackrel{\text{def}}{=}$	$\forall x\, y\, z\, (x + (y + z) \;=\; (x + y) + z)$	+ is associative
R_2	$\stackrel{\text{def}}{=}$	$\forall x\, y\, (x + y \;=\; y + x)$	+ is commutative
R_3	$\stackrel{\text{def}}{=}$	$0 \neq 1 \;\wedge\; \forall x\; x + 0 = x$	0 is id for $+$
R_4	$\stackrel{\text{def}}{=}$	$\forall x\, \exists y\; x + y = 0$	Additive inverses
R_5	$\stackrel{\text{def}}{=}$	$\forall x\, y\, z\, (x \cdot (y \cdot z) \;=\; (x \cdot y) \cdot z)$	$\cdot$ is associative
R_6	$\stackrel{\text{def}}{=}$	$\forall x\; x \cdot 1 = x$	1 is id for $\cdot$
R_7	$\stackrel{\text{def}}{=}$	$\forall x\, y\, z (x \cdot (y + z) = x \cdot y + x \cdot z) \wedge (y + z) \cdot x = y \cdot x + z \cdot x)$	+ distributes over $\cdot$
CR	$\stackrel{\text{def}}{=}$	$\forall x\, y\, (x \cdot y \;=\; y \cdot x)$	$\cdot$ is commutative

Def. A **ring** is a world $W \in \mathrm{World}[\Sigma_{\#thy}]$ s.t. $W \models R_1 \wedge \cdots \wedge R_7$

Def. A **commutative ring** is a ring that satisfies CR

Z, **Q**, **R** are commutative rings.

Let's look at $\Gamma_Z \subseteq \text{PredCalc}(\Sigma_{\#thy})$

R_1	$\stackrel{\text{def}}{=}$	$\forall x\, y\, z\, (x + (y + z) \;=\; (x + y) + z)$	+ is associative
R_2	$\stackrel{\text{def}}{=}$	$\forall x\, y\, (x + y \;=\; y + x)$	+ is commutative
R_3	$\stackrel{\text{def}}{=}$	$0 \neq 1 \;\wedge\; \forall x\; x + 0 = x$	0 is id for $+$
R_4	$\stackrel{\text{def}}{=}$	$\forall x\, \exists y\; x + y = 0$	Additive inverses
R_5	$\stackrel{\text{def}}{=}$	$\forall x\, y\, z\, (x \cdot (y \cdot z) \;=\; (x \cdot y) \cdot z)$	$\cdot$ is associative
R_6	$\stackrel{\text{def}}{=}$	$\forall x\; x \cdot 1 = x$	1 is id for $\cdot$
R_7	$\stackrel{\text{def}}{=}$	$\forall x\, y\, z(x \cdot (y + z) = x \cdot y + x \cdot z) \wedge$ $(y + z) \cdot x = y \cdot x + z \cdot x)$	+ distributes over $\cdot$
CR	$\stackrel{\text{def}}{=}$	$\forall x\, y\, (x \cdot y \;=\; y \cdot x)$	$\cdot$ is commutative

Def. A **ring** is a world $W \in \text{World}[\Sigma_{\#thy}]$ s.t. $W \models R_1 \wedge \cdots \wedge R_7$

Def. A **commutative ring** is a ring that satisfies CR

Z, **Q**, **R** are commutative rings.

iClicker 15.1 Is **N** a ring? **A: yes** **B: no**

Some other commutative rings: $\mathbf{Z}/m\mathbf{Z},\ m > 1$

$$|\mathbf{Z}/m\mathbf{Z}| = \{0, 1, \ldots, m{-}1\}, \quad a{+}b \stackrel{\text{def}}{=} (a{+}b)\% m, \quad a{\cdot}b \stackrel{\text{def}}{=} (a{\cdot}b)\% m$$

Some other commutative rings: $\mathbf{Z}/m\mathbf{Z},\ m > 1$

$$|\mathbf{Z}/m\mathbf{Z}| = \{0, 1, \ldots, m{-}1\}, \quad a{+}b \stackrel{\text{def}}{=} (a{+}b)\%m, \quad a{\cdot}b \stackrel{\text{def}}{=} (a{\cdot}b)\%m$$

Prop. for all $m > 1$, $\mathbf{Z}/m\mathbf{Z} \models R_1 \wedge \cdots \wedge R_7 \wedge CR$

Some other commutative rings: $\mathbf{Z}/m\mathbf{Z},\ m > 1$

$$|\mathbf{Z}/m\mathbf{Z}| = \{0, 1, \ldots, m{-}1\}, \quad a{+}b \stackrel{\text{def}}{=} (a{+}b)\%m, \quad a{\cdot}b \stackrel{\text{def}}{=} (a{\cdot}b)\%m$$

Prop. for all $m > 1$, $\mathbf{Z}/m\mathbf{Z} \models R_1 \wedge \cdots \wedge R_7 \wedge CR$

$|\mathbf{Z}/2\mathbf{Z}| = \{0, 1\}$

$+^{Z/2Z}$	0	1
0	0	1
1	1	0

$\cdot^{Z/2Z}$	0	1
0	0	0
1	0	1

Some other commutative rings: $\mathbf{Z}/m\mathbf{Z},\ m > 1$

$$|\mathbf{Z}/m\mathbf{Z}| = \{0, 1, \ldots, m-1\}, \quad a+b \stackrel{\text{def}}{=} (a+b)\%m, \quad a \cdot b \stackrel{\text{def}}{=} (a \cdot b)\%m$$

Prop. for all $m > 1$, $\mathbf{Z}/m\mathbf{Z} \models R_1 \wedge \cdots \wedge R_7 \wedge CR$

$$|\mathbf{Z}/2\mathbf{Z}| = \{0, 1\}$$

$+^{Z/2Z}$	0	1
0	0	1
1	1	0

$\cdot^{Z/2Z}$	0	1
0	0	0
1	0	1

$$F \stackrel{\text{def}}{=} \forall x\, (x \neq 0 \rightarrow \exists y\ x \cdot y = 1)$$

Some other commutative rings: $\mathbf{Z}/m\mathbf{Z},\ m > 1$

$$|\mathbf{Z}/m\mathbf{Z}| = \{0, 1, \ldots, m{-}1\}, \quad a{+}b \stackrel{\text{def}}{=} (a{+}b)\%m, \quad a{\cdot}b \stackrel{\text{def}}{=} (a{\cdot}b)\%m$$

Prop. for all $m > 1$, $\mathbf{Z}/m\mathbf{Z} \models R_1 \wedge \cdots \wedge R_7 \wedge CR$

$|\mathbf{Z}/2\mathbf{Z}| = \{0, 1\}$

$+^{Z/2Z}$	0	1
0	0	1
1	1	0

$\cdot^{Z/2Z}$	0	1
0	0	0
1	0	1

$$F \stackrel{\text{def}}{=} \forall x\, (x \neq 0 \rightarrow \exists y\ x \cdot y = 1)$$

Def. A **field** is a commutative ring that satisfies F

Some other commutative rings: $\mathbf{Z}/m\mathbf{Z},\ m > 1$

$$|\mathbf{Z}/m\mathbf{Z}| = \{0, 1, \ldots, m{-}1\}, \quad a{+}b \stackrel{\text{def}}{=} (a{+}b)\%m, \quad a{\cdot}b \stackrel{\text{def}}{=} (a{\cdot}b)\%m$$

Prop. for all $m > 1$, $\mathbf{Z}/m\mathbf{Z} \models R_1 \wedge \cdots \wedge R_7 \wedge CR$

$|\mathbf{Z}/2\mathbf{Z}| = \{0, 1\}$

$+^{Z/2Z}$	0	1
0	0	1
1	1	0

$\cdot^{Z/2Z}$	0	1
0	0	0
1	0	1

$$F \stackrel{\text{def}}{=} \forall x\, (x \neq 0 \rightarrow \exists y\ x \cdot y = 1)$$

Def. A **field** is a commutative ring that satisfies F

$\mathbf{Q}$, $\mathbf{R}$ are fields

Some other commutative rings: $\mathbf{Z}/m\mathbf{Z}$, $m > 1$

$$|\mathbf{Z}/m\mathbf{Z}| = \{0, 1, \ldots, m-1\}, \quad a+b \stackrel{\text{def}}{=} (a+b)\%m, \quad a \cdot b \stackrel{\text{def}}{=} (a \cdot b)\%m$$

Prop. for all $m > 1$, $\mathbf{Z}/m\mathbf{Z} \models R_1 \wedge \cdots \wedge R_7 \wedge CR$

$|\mathbf{Z}/2\mathbf{Z}| = \{0, 1\}$

$+^{Z/2Z}$	0	1
0	0	1
1	1	0

$\cdot^{Z/2Z}$	0	1
0	0	0
1	0	1

$$F \stackrel{\text{def}}{=} \forall x \, (x \neq 0 \rightarrow \exists y \; x \cdot y = 1)$$

Def. A **field** is a commutative ring that satisfies F

$\mathbf{Q}$, $\mathbf{R}$ are fields

iClicker 15.2 Is $\mathbf{Z}$ a field? **A: yes** **B: no**

Some other commutative rings: $\mathbf{Z}/m\mathbf{Z},\ m > 1$

$$|\mathbf{Z}/m\mathbf{Z}| = \{0, 1, \ldots, m{-}1\}, \quad a{+}b \stackrel{\text{def}}{=} (a{+}b)\%m, \quad a{\cdot}b \stackrel{\text{def}}{=} (a{\cdot}b)\%m$$

Prop. for all $m > 1$, $\mathbf{Z}/m\mathbf{Z} \models R_1 \wedge \cdots \wedge R_7 \wedge CR$

$|\mathbf{Z}/2\mathbf{Z}| = \{0, 1\}$

$+^{Z/2Z}$	0	1
0	0	1
1	1	0

$\cdot^{Z/2Z}$	0	1
0	0	0
1	0	1

$$F \stackrel{\text{def}}{=} \forall x\, (x \neq 0 \ \rightarrow\ \exists y\ x \cdot y = 1)$$

Def. A **field** is a commutative ring that satisfies F

$\mathbf{Q}$, $\mathbf{R}$ are fields

iClicker 15.2 Is $\mathbf{Z}$ a field? **A: yes** **B: no**

iClicker 15.3 Is $\mathbf{Z}/2\mathbf{Z}$ a field? **A: yes** **B: no**

$$|\mathbf{Z}/m\mathbf{Z}| = \{0, 1, \ldots, m-1\}, \quad a+b \stackrel{\text{def}}{=} (a+b)\%m, \quad a \cdot b \stackrel{\text{def}}{=} (a \cdot b)\%m$$

$$|\mathbf{Z}/m\mathbf{Z}| = \{0, 1, \ldots, m{-}1\}, \quad a{+}b \stackrel{\text{def}}{=} (a{+}b)\%m, \quad a{\cdot}b \stackrel{\text{def}}{=} (a{\cdot}b)\%m$$

$$|\mathbf{Z}/3\mathbf{Z}| = \{0, 1, 2\}$$

$+^{Z/3Z}$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot^{Z/3Z}$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$$|\mathbf{Z}/m\mathbf{Z}| = \{0, 1, \ldots, m-1\}, \quad a+b \stackrel{\text{def}}{=} (a+b)\%m, \quad a \cdot b \stackrel{\text{def}}{=} (a \cdot b)\%m$$

$$|\mathbf{Z}/3\mathbf{Z}| = \{0, 1, 2\}$$

$+^{Z/3Z}$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot^{Z/3Z}$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Is $\mathbf{Z}/3\mathbf{Z}$ a field?

$$|\mathbf{Z}/m\mathbf{Z}| = \{0, 1, \ldots, m-1\}, \quad a+b \stackrel{\text{def}}{=} (a+b)\%m, \quad a\cdot b \stackrel{\text{def}}{=} (a\cdot b)\%m$$

$$|\mathbf{Z}/m\mathbf{Z}| = \{0, 1, \ldots, m-1\}, \quad a+b \stackrel{\text{def}}{=} (a+b)\%m, \quad a\cdot b \stackrel{\text{def}}{=} (a\cdot b)\%m$$

$+^{Z/4Z}$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot^{Z/4Z}$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$$|\mathbf{Z}/m\mathbf{Z}| = \{0, 1, \ldots, m-1\}, \quad a+b \stackrel{\text{def}}{=} (a+b)\%m, \quad a\cdot b \stackrel{\text{def}}{=} (a\cdot b)\%m$$

$+^{Z/4Z}$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot^{Z/4Z}$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Is $\mathbf{Z}/4\mathbf{Z}$ a field?

$$|\mathbf{Z}/m\mathbf{Z}| = \{0, 1, \ldots, m-1\}, \quad a+b \stackrel{\text{def}}{=} (a+b)\%m, \quad a \cdot b \stackrel{\text{def}}{=} (a \cdot b)\%m$$

$+^{Z/4Z}$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot^{Z/4Z}$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Is $\mathbf{Z}/4\mathbf{Z}$ a field?

Which elements of $\mathbf{Z}/4\mathbf{Z}$ have multiplicative inverses?

$$|\mathbf{Z}/m\mathbf{Z}| = \{0, 1, \ldots, m{-}1\}, \quad a{+}b \stackrel{\text{def}}{=} (a{+}b)\%m, \quad a{\cdot}b \stackrel{\text{def}}{=} (a{\cdot}b)\%m$$

$+^{Z/4Z}$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot^{Z/4Z}$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Is $\mathbf{Z}/4\mathbf{Z}$ a field?

Which elements of $\mathbf{Z}/4\mathbf{Z}$ have multiplicative inverses?

1,3

$$|\mathbf{Z}/m\mathbf{Z}| = \{0, 1, \ldots, m-1\}, \quad a+b \stackrel{\text{def}}{=} (a+b)\%m, \quad a \cdot b \stackrel{\text{def}}{=} (a \cdot b)\%m$$

$$|\mathbf{Z}/m\mathbf{Z}| = \{0, 1, \ldots, m-1\}, \quad a+b \stackrel{\text{def}}{=} (a+b)\%m, \quad a \cdot b \stackrel{\text{def}}{=} (a \cdot b)\%m$$

$+^{Z/5Z}$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$.^{Z/5Z}$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$$|\mathbf{Z}/m\mathbf{Z}| = \{0, 1, \ldots, m-1\}, \quad a+b \stackrel{\text{def}}{=} (a+b)\%m, \quad a \cdot b \stackrel{\text{def}}{=} (a \cdot b)\%m$$

$+^{Z/5Z}$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot^{Z/5Z}$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Is $\mathbf{Z}/5\mathbf{Z}$ a field?

$$|\mathbf{Z}/m\mathbf{Z}| = \{0, 1, \ldots, m{-}1\}, \quad a{+}b \stackrel{\text{def}}{=} (a{+}b)\%m, \quad a{\cdot}b \stackrel{\text{def}}{=} (a{\cdot}b)\%m$$

$$|\mathbf{Z}/m\mathbf{Z}| = \{0, 1, \ldots, m-1\}, \quad a+b \stackrel{\text{def}}{=} (a+b)\%m, \quad a \cdot b \stackrel{\text{def}}{=} (a \cdot b)\%m$$

$+^{Z/6Z}$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot^{Z/6Z}$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$$|\mathbf{Z}/m\mathbf{Z}| = \{0, 1, \ldots, m{-}1\}, \quad a{+}b \stackrel{\text{def}}{=} (a{+}b)\%m, \quad a{\cdot}b \stackrel{\text{def}}{=} (a{\cdot}b)\%m$$

$+^{Z/6Z}$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot^{Z/6Z}$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Is $\mathbf{Z}/6\mathbf{Z}$ a field?

$$|\mathbf{Z}/m\mathbf{Z}| = \{0, 1, \ldots, m-1\}, \quad a+b \stackrel{\text{def}}{=} (a+b)\%m, \quad a \cdot b \stackrel{\text{def}}{=} (a \cdot b)\%m$$

$+^{Z/6Z}$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot^{Z/6Z}$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Is $\mathbf{Z}/6\mathbf{Z}$ a field?

Which elements of $\mathbf{Z}/6\mathbf{Z}$ have multiplicative inverses?

$$|\mathbf{Z}/m\mathbf{Z}| = \{0, 1, \ldots, m-1\}, \quad a+b \stackrel{\text{def}}{=} (a+b)\%m, \quad a\cdot b \stackrel{\text{def}}{=} (a\cdot b)\%m$$

$+^{Z/6Z}$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot^{Z/6Z}$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Is $\mathbf{Z}/6\mathbf{Z}$ a field?

Which elements of $\mathbf{Z}/6\mathbf{Z}$ have multiplicative inverses?

1,5

Prop. 1 $\Gamma_Z \vdash \forall xyz\,(x|y \wedge x|z \;\rightarrow\; x|(y+z))$

1	$x_0 \mid y_0 \wedge x_0 \mid z_0$	
2	$\exists uv\,(x_0 \cdot u = y_0 \;\wedge\; x_0 \cdot v = z_0)$	$\hookrightarrow$, 1
3	$x_0 \cdot u_0 = y_0 \;\wedge\; x_0 \cdot v_0 = z_0$	
4	$x_0 \cdot (u_0 + v_0) = y_0 + z_0$	Γ_Z, 3
5	$\exists w\,(x_0 \cdot w = y_0 + z_0)$	$\exists$-i, 4
6	$x_0 \mid (y_0 + z_0)$	$\hookrightarrow$, 5
7	$x_0 \mid (y_0 + z_0)$	$\exists$-e, 2, 3–6
8	$x_0 \mid y_0 \wedge x_0 \mid z_0 \;\rightarrow\; x_0 \mid (y_0 + z_0)$	$\rightarrow$-i, 1–7
9	$\forall xyz\,(x \mid y \wedge x \mid z \;\rightarrow\; x \mid (y+z))$	$\forall$-i, 8

Prop. 2 $\Gamma_Z \vdash \forall xyz\,(x|y \;\to\; x|(y \cdot z))$

1	$x_0 \mid y_0$	
2	$\exists u\; x_0 \cdot u = y_0$	$\hookrightarrow$, 1
3	$x_0 \cdot u_0 = y_0$	
4	$y_0 \cdot z_0 = y_0 \cdot z_0$	$=$-i
5	$(x_0 \cdot u_0) \cdot z_0 = y_0 \cdot z_0$	$=$-e, 3, 4
6	$x_0 \cdot (u_0 \cdot z_0) = y_0 \cdot z_0$	Γ_Z, 5
7	$\exists w\; (x_0 \cdot w = y_0 \cdot z_0)$	$\exists$-i, 6
8	$x_0 \mid (y_0 \cdot z_0)$	$\hookrightarrow$, 7
9	$x_0 \mid (y_0 \cdot z_0)$	$\exists$-e, 2, 3–8
10	$x_0 \mid y_0 \;\to\; x_0 \mid (y_0 \cdot z_0)$	$\to$-i, 1–9
11	$\forall xyz\,(x \mid y \;\to\; x \mid (y \cdot z))$	$\forall$-i, 10

Prop. 3 $\Gamma_Z \vdash \forall xyz\,(x|y \wedge y|z \rightarrow x|z)$

1	$x_0\|y_0 \wedge y_0\|z_0$	
2	$\exists uv\,(x_0 \cdot u = y_0 \wedge y_0 \cdot v = z_0)$	$\hookrightarrow$, 1
3	$x_0 \cdot u_0 = y_0 \wedge y_0 \cdot v_0 = z_0$	
4	$y_0 \cdot v_0 = y_0 \cdot v_0$	$=$-i
5	$(x_0 \cdot u_0) \cdot v_0 = y_0 \cdot v_0$	$=$-e, 3, 4
6	$x_0 \cdot (u_0 \cdot v_0) = y_0 \cdot v_0$	Γ_Z, 5
7	$x_0 \cdot (u_0 \cdot v_0) = z_0$	$=$-e, 3, 6
8	$\exists u\, x_0 \cdot u = z_0$	$\exists$-i, 7
9	$x_0\|z_0$	$\hookrightarrow$, 8
10	$x_0\|z_0$	$\exists$-e, 2, 3–9
11	$x_0\|y_0 \wedge y_0\|z_0 \rightarrow x_0\|z_0$	$\rightarrow$-i, 1–10
12	$\forall xyz\,(x\|y \wedge y\|z \rightarrow x\|z)$	$\forall$-i, 11