Definition: (field) A ring K is said to be a **field** if K is a commutative ring such that every $x \in K$ with x not equal to the additive identity is a unit.

Familiar Fields:

the rational numbers $\mathbb{Q}$ (inverse of $\frac{a}{b}$ is $\frac{b}{a}$ for $a \neq 0$), the real numbers $\mathbb{R}$ (inverse of x is $\frac{1}{x}$ for $x \neq 0$) and the complex numbers $\mathbb{C}$ (inverse of $z \in \mathbb{C}$ is $\frac{1}{z}$ - but this requires complex conjugation to see that $\frac{1}{z} \in \mathbb{C}$!)

Example 3: ($\mathbb{Z}_p$, p prime)

From your homework, if

$n \in \mathbb{N}$, $n \geq 2$, then if $m \in \mathbb{Z}$,

$[m] \in \mathbb{Z}_n$ is invertible if and only

if m and n are relatively prime.

If $n = p$ a prime number,

then m is rektively prime

to p if and only if p

does not divide m. Therefore,

every nonzero element in $\mathbb{Z}_p$

is invertible.

Since the multiplication is commutative, $\mathbb{Z}_p$ is a field for p prime.

Special case: $p=2$

Example 4: (field with four elements)

Start with symbols $0, 1, a, a^{-1}$.

Define binary operations that make $\{0, 1, a, a^{-1}\}$ into a field!

Note: $|\{0, 1, a, a^{-1}\}| = 4$ which is not prime. Since $|\mathbb{Z}_p| = p$, this field is different from the $\mathbb{Z}_p$ example.

Make tables!

"+"

	0	1	a	a^{-1}
0	0	1	a	a^{-1}
1	1	0	a^{-1}	a
a	a	a^{-1}	0	1
a^{-1}	a^{-1}	a	1	0

	0	1	a	a^{-1}
0	0	0	0	0
1	0	1	a	a^{-1}
a	0	a	a^{-1}	1
a^{-1}	0	a^{-1}	1	a

We'd need to check:

- associativity of "$+$" and "$\cdot$"
- distributivity of "$\cdot$" over "$+$"

This can be done tediously on a case-by-case basis!

Show distributivity

We want to show

$$x \cdot (y+z) = x \cdot y + x \cdot z$$

$$\forall \; x,y,z \in \{0, 1, a, a^{-1}\}$$

Trivial by definition if

$x = 0$ or $x = 1$

We only need to check

for $x = a$ and $x = a^{-1}$.

$x = a$

$y = 0$ or $z = 0$ is immediate

since one term of the sum

is zero.

$a(1 + 1) = a \cdot 0 = 0$ ✓

$a \cdot 1 + a \cdot 1 = a + a = 0$

$a \cdot (1 + a) = a \cdot a^{-1} = 1$

$a \cdot 1 + a \cdot a = a + a^{-1} = 1$ ✓

$$\begin{cases} a\cdot(1+a^{-1}) = a\cdot(a) = a^{-1} \\ a\cdot 1 + a\cdot a^{-1} = a+1 = a^{-1} \end{cases} \checkmark$$

$$\begin{cases} a\cdot(a+a^{-1}) = a\cdot(1) = a \\ a\cdot a + a\cdot a^{-1} = a^{-1}+1 = a \end{cases} \checkmark$$

$X = a^{-1}$

$$\begin{cases} a^{-1}(1+1) = a^{-1}\cdot 0 = 0 \\ a^{-1}\cdot 1 + a^{-1}\cdot 1 = a^{-1}+a^{-1} = 0 \end{cases} \checkmark$$

$$\begin{cases} a^{-1}\cdot(1+a) = a^{-1}\cdot a^{-1} = a \\ a^{-1}\cdot 1 + a^{-1}\cdot a = a^{-1}+1 = a \end{cases} \checkmark$$

$$\begin{cases} a^{-1}(1+a^{-1}) = a^{-1}\cdot a = 1 \\ a^{-1}\cdot 1 + a^{-1}\cdot a^{-1} = a^{-1} + a = 1 \end{cases}$$ ✓

$$\begin{cases} a^{-1}(a+a^{-1}) = a^{-1}\cdot(1) = a^{-1} \\ a^{-1}\cdot a + a^{-1}\cdot a^{-1} = 1 + a = a^{-1} \end{cases}$$ ✓

So distributivity holds!

Notation: If R is a unital ring, the notation $R^\times$ stands for all units of R.

$R^\times$ is a group (product of invertibles is invertible: $(xy)^{-1} = y^{-1}x^{-1}$)