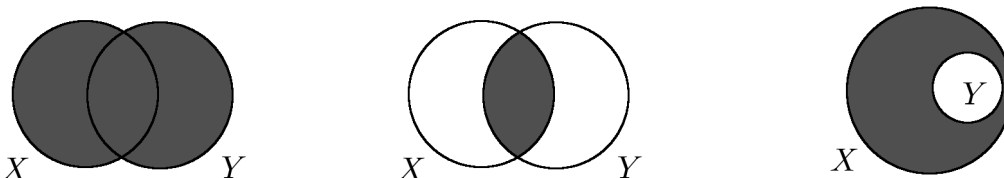


Sets & Notation

A *set* is a collection of things, called *elements* of the set. We usually use capital roman letters to refer to sets and lowercase roman or greek letters for elements of sets. The symbol \in stands for the phrase “is an element of” or “lives in”, so “ $x \in X$ ” means x is an element of the set X . Familiar sets include:

- \mathbb{N} The *natural numbers*, $\{0, 1, 2, 3, \dots\}$,
- \mathbb{Z} The *integers*, $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$,
- \mathbb{Q} The *rational numbers*, $\{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0, \gcd(a, b) = 1\}$,
- \mathbb{R} The *real numbers*, the set of all limits of infinite decimal expansions, and
- \mathbb{C} The *complex numbers*, $\{a + ib \mid a, b \in \mathbb{R}, i^2 = -1\}$.

Sets have operations such as union, intersection and difference:



$$X \cup Y = \{x \mid x \in X \text{ or } x \in Y\} \quad X \cap Y = \{x \mid x \in X \text{ and } x \in Y\} \quad X \setminus Y = \{x \mid x \in X \text{ and } x \notin Y\}$$

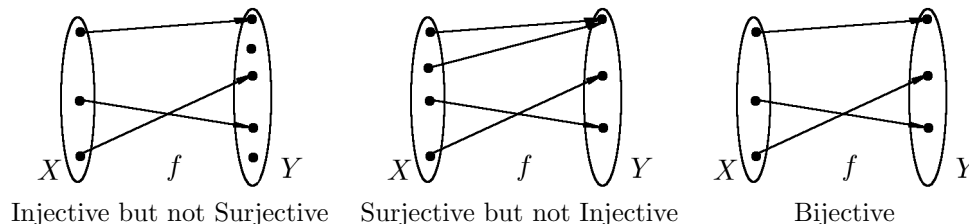
The *empty set* is the set with no elements: $\emptyset = \{\}$. Two sets are *disjoint* if their intersection is empty.

A set Y is a *subset* of X , denoted, $X \subset Y$ or $X \subseteq Y$, if every element of X is also an element of Y . Note that $X \subset X$ is always true. A subset $X \subset Y$ is *proper* if there is at least one element $y \in Y \setminus X$; we write $X \subsetneq Y$ in this case.

Let X and Y be sets. Recall that a *function* $f : X \rightarrow Y$ is a rule assigning an element $f(x) \in Y$ to each element $x \in X$. The set X of input values for f is called the *domain* of f and the set Y of potential output values is called the *codomain* of f . The set of output values actually hit by f , i.e. the subset

$$\text{Im}(f) = \{y \in Y \mid y = f(x) \text{ for some } x \in X\},$$

is called the *image* of f . A function is *one-to-one* or *injective* if no element of Y is reused by f , that is, if $f(x) = f(x')$ implies $x = x'$. A function is *onto* or *surjective* if every element of Y is hit by f at least once, i.e. if $\text{Im}(f) = Y$. Note that $\text{Im}(f)$ is always a subset of Y ; if the subset is proper, then f is not surjective. A function which is both injective and surjective is called *bijective*.



Fields

A *field* is a set \mathbb{F} with two operations, addition and multiplication, satisfying for all $\alpha, \beta, \gamma \in \mathbb{F}$

(i) Addition and multiplication are *associative*:

$$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma \quad \text{and} \quad \alpha(\beta\gamma) = (\alpha\beta)\gamma,$$

(ii) There is an *additive identity* $0 \in \mathbb{F}$ and a *multiplicative identity* $1 \in \mathbb{F}$ satisfying

$$\alpha + 0 = \alpha = 0 + \alpha \quad \text{and} \quad \alpha 1 = \alpha = 1\alpha,$$

(iii) Every element $\alpha \in \mathbb{F}$ has an *additive inverse* $-\alpha \in \mathbb{F}$ and every nonzero element $\beta \neq 0 \in \mathbb{F}$ has a *multiplicative inverse* $\beta^{-1} \in \mathbb{F}$ satisfying

$$\alpha + -\alpha = 0 = -\alpha + \alpha \quad \text{and} \quad \beta\beta^{-1} = 1 = \beta^{-1}\beta,$$

(iv) Addition and multiplication are *commutative*, i.e.

$$\alpha + \beta = \beta + \alpha \quad \text{and} \quad \alpha\beta = \beta\alpha,$$

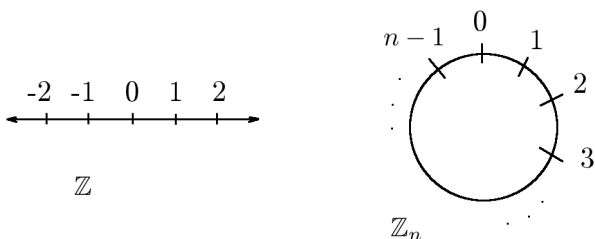
and

(v) Multiplication *distributes* over addition, i.e.,

$$\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma \quad \text{and} \quad (\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma.$$

Familiar examples of fields include \mathbb{Q}, \mathbb{R} and \mathbb{C} ; however, note that \mathbb{N} and \mathbb{Z} are not fields since \mathbb{Z} lacks multiplicative inverses for elements other than ± 1 and \mathbb{N} lacks additive inverses for elements other than 0.

A possibly less familiar example is $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$, the *integers modulo n*. Arithmetic in \mathbb{Z}_n involves an extra step of reducing mod n , meaning adding or subtracting multiples of n until you're back in the set $\{0, 1, 2, \dots, n-1\}$. Where \mathbb{Z} forms a number line, \mathbb{Z}_n forms a number circle, like an analog clock – in fact, we use mod 12 (and mod 60) arithmetic for telling time.



You can do reduction mod n at every step, or you can save it all up for the last step, and you'll get the same result. For example, in \mathbb{Z}_5 , $(2 + 4)3 - 4(3 + 3) = 2$:

$$\begin{array}{lcl} (2 + 4)3 - 4(3 + 3) & = & (6)3 - 4(9) \\ & = & 1(3) - 4(4) \\ & = & 3 - 16 & \text{or} & (2 + 4)3 - 4(3 + 3) = 18 - 36 \\ & = & 3 - 1 & & = -18 \\ & = & 2 & & = -3 \\ & & & & = 2 \end{array}$$

Note that \mathbb{Q}, \mathbb{R} and \mathbb{C} are fields, while \mathbb{N} and \mathbb{Z} are not – \mathbb{N} lacks additive and multiplicative inverses for elements greater than 1, and while \mathbb{Z} includes additive inverses for everything, the only elements in \mathbb{Z} with multiplicative inverses are 1 and -1 .

Example: \mathbb{Z}_5 is a field. To prove this, one needs to verify that all of the field axioms are satisfied. Most of these are straightforward: multiplication and addition are associative, commutative and distributive in \mathbb{Z}_5 because they are associative, commutative and distributive in \mathbb{Z} before reducing mod 5, and reducing equal quantities mod 5 yields equal quantities in \mathbb{Z}_5 . The interesting part is to check the additive and multiplicative inverses, which we can do by brute force since \mathbb{Z}_5 has only 5 elements.

α	$-\alpha$		α^{-1}	
0	0	$0 + 0 = 0$	–	
1	4	$1 + 4 = 5 = 0$	1	$1(1) = 1$
2	3	$2 + 3 = 5 = 0$	3	$2(3) = 6 = 1$
3	2	$3 + 2 = 5 = 0$	2	$3(2) = 6 = 1$
4	1	$4 + 1 = 5 = 0$	4	$4(4) = 16 = 1$

Note that \mathbb{Z}_n may or may not be a field depending on the value of n ; see the exercises for more.