Let me recall...

Group $(G, *)$

$* : G^2 \longrightarrow G$ (closure)

$\exists e\ \forall a$: $a * e = e * a = a$

$\forall a, b, c$: $(a * b) * c = a * (b * c)$

$\forall a\ \exists a'$: $a * a' = a' * a = e$

the e from the first property, which is unique.

If additionally, one has $a * b = b * a$ for all $a, b \in G$, then the group is called Abelian.

One can write Abelian groups additively, that mean the group operation is denoted by $+$, the neutral element by 0 and the inverse of a w.r.t. $+$ by $-a$.

A structure $(R, +, \cdot)$ with two operations $+ : R^2 \to R$ and $\cdot : R^2 \to R$ is called a ring if the following conditions hold:

$(R, +)$ is an Abelian group

$$\boxed{\begin{aligned} &a + 0 = 0 + a = a \\ &a + b = b + a \\ &(a + b) + c = a + (b + c) \\ &a + (-a) = 0 \end{aligned}}$$

- $\cdot$ is an associative operation, that is,

$\boxed{a \cdot (b \cdot c) = (a \cdot b) \cdot c}$ for all $a, b, c \in R$.

and, additionally, for $+$ and $\cdot$ the distributive laws are satisfied:

$$\boxed{\begin{aligned} &(a + b) \cdot c = a \cdot c + b \cdot c, \\ &c \cdot (a + b) = c \cdot a + c \cdot b \end{aligned}}$$

hold for all $a, b, c \in R$.

A ring $(R, +, \cdot)$ is called unitary if $\cdot$ has a neutral element, normally denoted as 1, that is
$$\exists 1 \, \forall a \; : \; a \cdot 1 = 1 \cdot a = a .$$
A unitary ring with $0 \neq 1$ is called non-trivial.

A commutative ring is a ring, in which the multiplication is commutative, which means
$$a \cdot b = b \cdot a$$
for all $a, b \in R$.

We will need non-trivial unitary commutative rings.

A non-trivial unitary commutative ring $(R, +, \cdot)$ is called <u>field</u> if all non-zero elements of R are invertible w.r.t. multiplication:
$$\forall a \in R \setminus \{0\} \; \exists \bar{a}^1 : \quad a \cdot \bar{a}^1 = 1 .$$

Let's have some examples....

Examples 4.1

- $(\mathbb{Z}, +, \cdot)$ nontrivial unitary commutative ring, but not a field because $\bar{a}^1$ exists in $\mathbb{Z}$ only for $a = 1$ and $a = -1$.

- $(\mathbb{R}^{n \times n}, +, \cdot)$ the set of $n \times n$ matrices over reals. It is a ring, but not commutative one (for $n \geq 2$). It is unitary

- $\{z \in \mathbb{Z} : z \text{ even}\}$ is a non-unitary commutative ring

- $(\mathbb{Q}, +, \cdot)$ field.
- $(\mathbb{R}, +, \cdot)$ field.
- $(\mathbb{R}[t], +, \cdot)$ the set of polynomials with the coefficients from $\mathbb{R}$ in the variable t. They form a unitary commutative ring but not a field.

4.2. Ideals and quotient rings

In what follows, by default, our rings are non-trivial unitary and commutative.

For subsets and elements of a ring we introduce the following notations:

$$A + B := \{a + b : a \in A, b \in B\},$$

$$A \cdot B := \{a \cdot b : a \in A, b \in B\},$$

$$f + A := \{f + a : a \in A\},$$

$$f \cdot B := \{f \cdot b : b \in B\},$$

where $A, B \subseteq R$ and $f \in R$ for a ring R.

Examples 4.2

- $2\mathbb{Z} = \{2 \cdot z : z \in \mathbb{Z}\}$ is the set of all even integers.
- $1 + 2\mathbb{Z} = \{1 + 2z : z \in \mathbb{Z}\}$ is the set of all odd integers.

- $1 + 5\mathbb{Z} = \{\ldots, -4, 1, 6, 11, 16, 21, \ldots\ldots\}$

- $(2\mathbb{Z}) \cap (3\mathbb{Z}) = 6\mathbb{Z}$

- $2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$, because $\underset{2\cdot(-1)+3\cdot 1.}{\underset{\shortparallel}{1}} \in 2\mathbb{Z} + 3\mathbb{Z}$

- $6\mathbb{Z} + 8\mathbb{Z} = 2\mathbb{Z}$.

$$\begin{aligned} 2\mathbb{Z} + 3\mathbb{Z} &= \{a + b : a \in 2\mathbb{Z}, b \in 3\mathbb{Z}\} \\ &= \{a + b : a = 2u, b = 3v \text{ where } u, v \in \mathbb{Z}\} \\ &= \{2u + 3v : u, v \in \mathbb{Z}\}. \end{aligned}$$

Def 4.3 A subset I of a ring $(R, +, \cdot)$ [remember, we are in the default setting] is called an ideal if the following hold:

(a) $0 \in I$

(b) $I + I \subseteq I$

(c) $R \cdot I \subseteq I$

Spelled out:

(a) $0 \in I$

(b) $a, b \in I \implies a + b \in I$

(c) $a \in R,\ b \in I \implies a \cdot b \in I$.

Example 4.4 Let's take $I = \{0\}$.

This is an ideal. The properties become:

(a) $0 = 0$

(b) $a = 0,\ b = 0 \implies a + b = 0$

(c) $a \in R,\ b = 0 \implies a \cdot b = 0$

Example 4.5 $f \in R$.

$fR = \{ f \cdot a : a \in R \}$ is always an ideal. For example

$$\left.\begin{matrix} 2\mathbb{Z} \\ 3\mathbb{Z} \\ 4\mathbb{Z} \\ 5\mathbb{Z} \\ 6\mathbb{Z} \end{matrix}\right\} \text{ are all ideals in } \mathbb{Z}.$$

Even more generally, when one has $f_1, \dots, f_m \in R$, the set

$f_1 R + f_2 R + \dots + f_m R$

$= \{ f_1 \cdot a_1 + f_2 \cdot a_2 + \dots + f_m a_m : a_1, \dots, a_m \in R \}$

is an ideal in R. This is called the ideal generated by $f_1, \dots, f_m$.

Definition 4.6. (Quotient ring)

Let I be an ideal in a ring R.

For $a, b \in R$ we write

$$a \equiv b \mod I$$ (a congruent to b modulo I)

if $a - b \in I$.

In particular, if $I = fR$ for some $f \in R$

we write $a \equiv b \mod f$.

The coset of $a \in R$ modulo I is the set

$$[a] := [a]_I := a + I.$$

The quotient ring R/I (the ring R modulo the ideal I) is the set

$$R/I := \{ [a]_I : a \in R \}$$

with $+$ and $\cdot$ defined as follows:

$$[a] + [b] = [a+b],$$

$$[a] \cdot [b] = [a \cdot b].$$

These two operations on R/I are well defined, that means, the choice of representatives in the cosets doesn't affect the result.

Example 4.7

$\mathbb{Z}/6\mathbb{Z}$

$R = \mathbb{Z}$

$I = 6\mathbb{Z}$

$\mathbb{Z}/6\mathbb{Z}$:

$0 + 6\mathbb{Z} = \{$ all integers divisible by 6 $\}$

$1 + 6\mathbb{Z} = \{$ all integers congruent to 1 modulo 6 $\}$, $-5, 1, 7, \dots$

$2 + 6\mathbb{Z}$ ⋮

$3 + 6\mathbb{Z}$.

$4 + 6\mathbb{Z}$ ⋮

$5 + 6\mathbb{Z}$ ⋮

$6 + 6\mathbb{Z}$ ⋮

$\mathbb{Z}/6\mathbb{Z} = \{[0], [1], [2], [3], [4], [5]\}$

$\mathbb{Z}/6\mathbb{Z}$ captures calculations modulo 6.
One does computations as if 6 and all of the elements of the idea $6\mathbb{Z}$ would be 0.

Some calculations:

$[2]\cdot[4] = [8] = [2]$

$[2]\cdot[3] = [6] = [0]$ so you may have: non-zero × non-zero = 0 in general rings.

$[3] + [5] = [3+5] = [8] = [2]$.

Example 4.8

int8 from the computer.

$2^8 = 256$

$\mathbb{Z}/256\mathbb{Z}$

Example 4.9

$\mathbb{Z}/2\mathbb{Z} = \{[0], [1]\}$

$[0]$: even numbers; $[1]$: odd numbers

$[0] + [0] = [0]$
$[0] + [1] = [1]$
$[1] + [1] = [0]$

$[0] \cdot [0] = [0]$
$[0] \cdot [1] = [0]$
$[1] \cdot [1] = [1]$

Compare to: $\{\text{false}, \text{true}\}$ with XOR and AND.

false XOR false = false
false XOR true = true
true XOR true = false

false AND false = false
false AND true = false
true AND true = true.

$0 \Longleftrightarrow$ false
$1 \Longleftrightarrow$ true
XOR $\Longleftrightarrow$ $+ \bmod 2$
AND $\Longleftrightarrow$ $\cdot \bmod 2$

$\mathbb{Z}/2\mathbb{Z}$ is actually a field.