Rings and Fields

A ring is a set with two binary operations
+ for addition
· for multiplication
must play well together!

Examples include $\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, ...

More complicated examples

(0) $\{0\}$ = zero ring

(1) $M_n(\mathbb{R})$ = set of $n \times n$ real matrices

(2) $\mathbb{R}[x]$ = set of polynomials with real coeffs.

Def: A ring R is a set with two binary operations addition + and multiplication · with the following properties

- $(R, +)$ is an Abelian group with identity 0_R
- multiplication · is associative
- distributive properties hold

$$\begin{cases} a\cdot(b+c) = (a\cdot b)+(a\cdot c) \\ (a+b)\cdot c = (a\cdot c)+(b\cdot c) \end{cases}$$ for all $a, b, c \in R$

- R has a multiplicative identity 1_R

WARNING: this is actually called a ring with identity by some authors

Def: A homomorphism $f: R \to S$ from a ring R to a ring S is a function satisfying

- $f(a+b) = f(a) + f(b)$
- $f(ab) = f(a)f(b)$
- $f(1_R) = 1_S$

R is called commutative if · is commutative.

WARNING: the condition is not included by some authors (including our book), but it is meaningful.

Def: The <u>product</u> of rings R and S is $R \times S$ with

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$$
$$(r_1, s_1) \cdot (r_2, s_2) = (r_1 r_2, s_1 s_2)$$
$$0_{R \times S} = (0_R, 0_S)$$
$$1_{R \times S} = (1_R, 1_S)$$

Ex: $f: \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$
$x \longmapsto (x, x)$ is a ring hom

$g: \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$
$x \longmapsto (x, 0)$ is not because $g(1) \neq (1,1)$

Some authors would consider it to be...

Ex: $\det: M_n(\mathbb{R}) \longrightarrow \mathbb{R}$ is NOT a ring hom.

Ex: $A \in M_n(\mathbb{R})$, $\det(A) \neq 0$

$f: M_n(\mathbb{R}) \rightarrow M_n(\mathbb{R})$, $f(B) = ABA^{-1}$ is a ring hom

Ex: Let R be a commutative ring and $a \in R$. The <u>evaluation homomorphism</u> is

$$\phi_a : R[x] \longrightarrow R$$
$$p(x) \longmapsto p(a)$$

Ex:
$$\phi_2 : \mathbb{Z}[x] \longrightarrow \mathbb{Z}$$
$$p(x) \longmapsto p(2)$$
$$\phi_2(3) = 3, \quad \phi_2(x^2+4) = 2^2 + 4 = 8$$

Def: An element $a \in R$ is called a <u>unit</u> if there exists $b \in R$ with $ab = ba = 1_R$.
A ring where every element but 0_R is a unit is called a <u>division ring</u> or <u>skew-field</u>.
A commutative division ring is called a <u>field</u>.

Ex: The units in $\mathbb{Z}$ are ± 1

Ex: The units in $\mathbb{Z}_n$ are $0 \leq k < n$ with $\gcd(n,k) = 1$
In particular, $\mathbb{Z}_p$ is a field.

Ex: The <u>quaternions</u> are

$$Q = \{ a + bi + cj + dk \mid a,b,c,d \in \mathbb{R} \}$$

where

	i	j	k
i	-1	k	$-j$
j	$-k$	-1	i
k	j	$-i$	-1

so that
$ij = k$
$jk = i$
$ki = j$

This is a skew-field!

$$(a+bi+cj+dk)(a-bi-cj-dk)$$

$$= \begin{bmatrix} a & b & c & d \end{bmatrix} \begin{bmatrix} 1 & i & j & k \\ i & -1 & k & -j \\ j & -k & -1 & i \\ k & j & -i & -1 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix}$$

$$= \begin{bmatrix} a & b & c & d \end{bmatrix} \begin{bmatrix} a + bi + cj + dk \\ ai - b + ck - dj \\ aj - bk - c + di \\ ak + bj - ci - d \end{bmatrix} = a^2 + b^2 + c^2 + d^2$$

Therefore $(a+bi+cj+dk)\dfrac{a-bi-cj-dk}{a^2+b^2+c^2+d^2} = 1.$

<u>Example</u>: The p-adic integers are

$$\mathbb{Z}_{p\text{-adic}} = \left\{ \sum_{k=0}^{\infty} a_k p^k \;\middle|\; 0 \le a_k < p \right\}$$

$$5 = 2 + 1\cdot 3 + 0\cdot 3^2 + 0\cdot 3^3 + 0\cdot 3^4 + \dots$$

$$\begin{aligned}
&2\cdot(2 + 1\cdot 3 + 1\cdot 3^2 + 1\cdot 3^3 + 1\cdot 3^4 + \dots) \\
&= (4 + 2\cdot 3 + 2\cdot 3^2 + 2\cdot 3^3 + 2\cdot 3^4 + \dots) \\
&= (1 + 3\cdot 3 + 2\cdot 3^2 + 2\cdot 3^3 + 2\cdot 3^4 + \dots) \\
&= (1 + 0\cdot 3 + 3\cdot 3^2 + 2\cdot 3^3 + 2\cdot 3^4 + \dots) \\
&= (1 + 0\cdot 3 + 0\cdot 3^2 + 3\cdot 3^3 + 2\cdot 3^4 + \dots) \\
&= (1 + 0\cdot 3 + 0\cdot 3^2 + 0\cdot 3^3 + 3\cdot 3^4 + \dots) \\
&= 1 \qquad \text{and therefore}
\end{aligned}$$

$$\frac{1}{2} = (2 + 1\cdot 3 + 1\cdot 3^2 + 1\cdot 3^3 + 1\cdot 3^4 + \dots) \quad \text{and } 2 \text{ is a unit!}$$