A *ring* is an algebraic object with two laws of composition: addition (for which this object is an Abelian group) and multiplication, and these two operations "interact" with each other in a certain sense. You are already familiar with quite a few rings such as the rational numbers, the real numbers, the complex numbers, the integers, but also for example the $n \times n$ matrices with coefficients taken in one of the previously mentioned rings. Here's the precise definition.

Definition A *ring* R is a set together with two laws of composition defined on this set

$x + y$	"addition"	$x, y \in R$
$x \cdot y$	"multiplication"	

(we will often write xy instead of $x \cdot y$) such that the following axioms are satisfied:

(R1) $\langle R, + \rangle$ is an additive Abelian group. 0_R denotes the additive identity; $-a$ is the additive inverse of a; $a - b$ denotes $a + (-b)$;

(R2) The multiplication is closed and *associative*: $\forall x, y, z \in R : x(yz) = (xy)z$;

(R3) There exists a *multiplicative identity* 1_R in R with the following property: $\forall x \in R : 1_R \cdot x = x \cdot 1_R = x$.

(R4) *Distributivity* holds: $\forall x, y, z \in R$ one has $x(y + z) = xy + xz$ and $(x + y)z = xz + yz$.

A few "expected" properties of a ring R can readily be verified, for example:

- $0_R \cdot x = x \cdot 0_R = 0_R$ for all $x \in R$. Indeed, by (R3), by distributivity (R4) and using the fact that 0_R is the additive identity, we have

$$0_R x + x = 0_R x + 1_R x = (0_R + 1_R)x = 1_R x = x = 0_R + x,$$

  and since we can cancel in the additive group R, we get $0_R x = 0_R$. Similarly, $x 0_R = 0_R$.
- $(-x)y = -xy$ (here, of course, $-x$ is the additive inverse of x, and $-xy = -(xy)$ is the additive inverse of xy). Indeed,

$$xy + (-x)y \overset{(R4)}{=} (x + (-x))y = 0_R y = 0_R,$$

  showing that $(-x)y$ is the additive inverse of xy: $(-x)y = -(xy)$.
- $x(-y) = -(xy)$ and $(-x)(-y) = xy$ (check!).

- The ring R is said to be *trivial* if $R = \{0_R\}$ (exercise sheet: R is trivial iff $0_R = 1_R$).
- The ring R is said to be *commutative* if $xy = yx$ for all $x, y \in R$.
- An element $x \in R$ is called a *unit* or *invertible* or is said to have a *multiplicative inverse* if there exists $y \in R$ such that $xy = yx = 1_R$.

We denote the subset of R consisting of all units by R^*:

$$R^* = \{x \in R \mid x \text{ is a unit}\}.$$

R^* together with multiplication as defined in R is a multiplicative group with identity 1_R (exercise sheet). It is called the *group of units of* R (or simply *unit group of* R).

- A non-trivial ring R such that $R^* = R \setminus \{0_R\}$ (i.e. a ring in which the unit group consists of all nonzero elements) is called a *division ring*.

- A commutative division ring is called a *field*.
- An element x in a commutative ring R is called a *zero divisor* if $x \neq 0_R$ and there exists $y \neq 0_R$ such that $xy = 0_R$.

  Example $R = \mathbb{Z}/6\mathbb{Z}$. $2.3 = 0$ so 2 and 3 are zero divisors.
- A commutative ring $R \neq \{0_R\}$ is said to be an *integral domain* if it does not contain any zero divisors, that is, $xy = 0_R \Rightarrow x = 0_R$ or $y = 0_R$.

Lemma 2.1.1 *In an integral domain D we have if $a \neq 0_D$ then*

$$ab = ac \Rightarrow b = c \quad \text{(left cancellation)}$$

$$ba = ca \Rightarrow b = c \quad \text{(right cancellation)}$$

Proof Exercise Sheet. □

Note: In Lemma 2.1.1 a need not be a unit.

Example If R is a field, then R is an integral domain (exercise sheet).

Example The rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$ are fields.

Example The integers $\mathbb{Z}$ form an integral domain. One has

$$\mathbb{Z}^* = \{1, -1\}$$

(check!). In particular, $\mathbb{Z}$ is not a field as $\mathbb{Z}^* \subsetneq \mathbb{Z} \setminus \{0\}$.

However we do have the following.

Theorem 2.1.2 *Every finite integral domain is a field.*

Proof Let $0_R, a_0 = 1_R, a_1, \ldots, a_n$ be the elements of some finite integral domain R. We need to show that for $a \in R$ where $a \neq 0_R$ there exists $b \in R$ such that $ab = 1_R$. Now consider

$$aa_0, aa_1, aa_2, \ldots, aa_n.$$

Now $aa_i = aa_j$ implies (by left cancellation) that $a_i = a_j$ and so these elements are distinct. Also none of these elements equal 0_R since R is an integral domain. It follows that $\{a_0 = 1_R, a_1, \ldots, a_n\} = \{aa_0 = a1_R, aa_1, \ldots, aa_n\}$. In particular $1_R \in \{aa_0, aa_1, \ldots, aa_n\}$ so $aa_k = 1_R$ for some k, as required. □

Example For $n \geq 2$ $\mathbb{Z}/n\mathbb{Z}$ with addition and multiplication mod n is a ring. We have $(\mathbb{Z}/n\mathbb{Z})^* = \{k : \gcd(k, n) = 1\}$ and $a \neq 0$ is a zero divisor in $\mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(a, n) > 1$. Therefore

$$\mathbb{Z}/n\mathbb{Z} \text{ is a field} \Leftrightarrow \mathbb{Z}/n\mathbb{Z} \text{ is an integral domain} \Leftrightarrow n \text{ is prime}$$

and we denote this field by $\mathbb{F}_p$.

Example $(\mathbb{Z}/10\mathbb{Z})^* = \{1, 3, 7, 9\}$. Zero divisors: $2, 4, 5, 6, 8$.

Example Let R and S be rings. Then $R \times S$ becomes a ring with the following operations:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$$
$$(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2).$$

This can be extended to $R_1 \times R_2 \times \ldots \times R_n$, direct product of rings.

Note $R \times S$ is never an integral domain.

Example $M_n(\mathbb{R})$ is a ring with the usual matrix addition and matrix multiplication. It is commutative if $n = 1$ (it can then be identified with $\mathbb{R}$), and noncommutative, so not an integral domain, if $n > 1$. For example,

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

whereas

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

The units in $M_n(\mathbb{R})$ are just the matrices that are invertible in the usual sense: $M_n(\mathbb{R})^* = GL_n(\mathbb{R})$.

Example Let S be a nonempty set and let A be a ring. We define

$$R = \mathrm{Map}(S, A) = \{\text{all maps } S \to A\}.$$

We define a product fg and a sum $f + g$ of two maps as follows:

$$\forall x \in S: \quad fg(x) := f(x)g(x), \quad (f+g)(x) := f(x) + g(x).$$

One now verifies readily that R together with this multiplication and this addition becomes a ring. The additive identity is given by the map

$$0_R \colon S \to A \colon x \to 0_A \quad (\forall x \in S)$$

and the multiplicative identity is given by

$$1_R \colon S \to A \colon x \to 1_A \quad (\forall x \in S).$$

We have

$$R^* = \{f \colon S \to A \mid f(x) \in A^* \text{ for all } x \in S\}.$$

Example $S = \{a, b\}$ $A = \mathbb{Z}/6\mathbb{Z}$ $R = \mathrm{Map}(S, A)$

$$R^* = \mathrm{Map}(S, A)^* = \{f : S \to A : f(x) \in A^* \text{ for all } x \in S\}$$
$$= \{f : S \to A : f(x) \in \{1, 5\} \text{ for all } x \in S\}.$$

This yields four maps

$$\begin{array}{ll} f_1(a) = 1 & f_1(b) = 1 \\ f_2(a) = 1 & f_2(b) = 5 \\ f_3(a) = 5 & f_3(b) = 1 \\ f_4(a) = 5 & f_4(b) = 5. \end{array} \qquad R^* = \{f_1, f_2, f_3, f_4\}$$

For example

$$(f_3 f_4)(a) = f_3(a) f_4(a) = 5.5 = 1$$
$$(f_3 f_4)(b) = f_3(b) f_4(b) = 1.5 = 5$$

shows $f_3 f_4 = f_2$.

Example Let R be a ring. If X is an indeterminate, then $R[X]$ is called the *polynomial ring in the indeterminate X with coefficients in R*:

$$R[X] = \{a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \mid n \in \mathbb{N} \cup \{0\},\ a_i \in R\}.$$

We add and multiply polynomials in the usual way:

$$(a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n) + (b_0 + b_1 X + \cdots + b_m X^m) =$$
$$(a_0 + b_0) + (a_1 + b_2) X + (a_2 + b_2) X^2 + \cdots$$

and $(a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n)(b_0 + b_1 X + \cdots + b_m X^m) =$

$$a_0 b_0 + (a_0 b_1 + a_1 b_0) X + (a_0 b_2 + a_1 b_1 + a_2 b_0) X^2$$
$$+ \cdots + a_n b_m X^{n+m}.$$

One can then verify that $R[X]$ together with this addition and this multiplication of polynomials becomes a ring. $0_{R[X]} = 0_R$ and $1_{R[X]} = 1_R$.

Note R is commutative if and only if $R[X]$ is commutative. $R[X]$ is not a division ring for any ring R, in particular, $R[X]$ is never a field.

Lemma 2.1.3 *If R is an integral domain then (i) $R[X]$ is an integral domain; and (ii) $R[X]^* = R^*$.*

Proof. (i) Exercise Sheet. (ii) Clearly every unit in R is a unit in $R[X]$ so $R^* \subseteq R[X]^*$. Let $P(X) \in R[X]^*$ so that $P(X)Q(X) = 1_R$ for some $Q(X) \in R[X]$. Put $P(X) = a_0 + a_1X + \ldots + a_mX^m$ ($m \geq 0$, $a_i \in R$, $a_m \neq 0_R$) and $Q(X) = b_0 + b_1X + \ldots + b_nX^n$ ($n \geq 0$, $b_j \in R$, $b_n \neq 0_R$). If $m = 0$ then $P(X) \in R^*$ and we are done so assume $m > 0$ and therefore $m + n \geq 1$. But $P(X)Q(X) = 1_R$ now forces $a_mb_nX^{m+n} = 0_R \Rightarrow a_mb_n = 0_R \Rightarrow a_m = 0_R$ or $b_n = 0_R$, a contradiction. $\square$

Example $\mathbb{Z}/8\mathbb{Z}[X]$ $(1+4X)(1+4X) = 1$ shows that $1+4X \in (\mathbb{Z}/8\mathbb{Z}[X])^*$. However $\mathbb{Z}/\mathbb{Z}8$ *not* an integral domain.

Definition Let R be a ring. A subset S of R is called a *subring of R* if the following axioms are satisfied:

(SR1) S is a subgroup of the additive group $\langle R, + \rangle$;

(SR2) S is closed under the multiplication in R:
$\forall a, b \in S$: $ab \in S$;

(SR3) $1_R \in S$.

Note To check (SR1) it is enough to confirm that S contains 0_R; that S is closed w.r.t. addition; that S is closed w.r.t. additive inverses.

Example $\mathbb{R}$ is a subring of $\mathbb{C}$, $\mathbb{Q}$ is a subring of $\mathbb{R}$ and of $\mathbb{C}$. $\mathbb{Z}$ is a subring of $\mathbb{Q}$, thus also of $\mathbb{R}$ and of $\mathbb{C}$.

Example

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$$

is a subring of $\mathbb{R}$ (see exercise sheet). But it is not a subring of $\mathbb{Q}$. Indeed, $\sqrt{2} = 0 + 1 \cdot \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, but $\sqrt{2} \notin \mathbb{Q}$.

Example If R is a ring, then R is a subring of the polynomial ring $R[X]$.

Example Let

$$D = \left\{ \left(\begin{array}{cccc} x_1 & 0 & \cdots & 0 \\ 0 & x_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & x_n \end{array} \right) \middle| \; x_i \in \mathbb{R},\ 1 \leq i \leq n \right\}$$

be the set of all diagonal matrices in $M_n(\mathbb{R})$. Then D is a commutative subring of $M_n(\mathbb{R})$ (which itself is noncommutative if $n \geq 2$). D^* consists of all diagonal matrices that only have nonzero elements on the diagonal.

Example Let

$$\mathrm{Sym}(\mathbb{R}) = \left\{ \begin{pmatrix} u & v \\ v & u \end{pmatrix} \;\middle|\; u, v \in \mathbb{R} \right\}.$$

Then $\mathrm{Sym}(\mathbb{R})$ is a commutative subring of $M_2(\mathbb{R})$. If we define $\mathrm{Sym}(\mathbb{Z})$ in an analogous way, but only allowing coefficients in $\mathbb{Z}$ (so the u, v above are integers), then $\mathrm{Sym}(\mathbb{Z})$ is a subring of $\mathrm{Sym}(\mathbb{R})$ (and hence of $M_2(\mathbb{R})$). We have

$$\mathrm{Sym}(\mathbb{R})^* = \left\{ \begin{pmatrix} u & v \\ v & u \end{pmatrix} \;\middle|\; u, v \in \mathbb{R},\ u \neq \pm v \right\}$$

and (exercise sheet)

$$\mathrm{Sym}(\mathbb{Z})^* = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \right\}$$

Definition The ring R is said to have *characteristic* $n > 0$ if n is the smallest positive integer such that $n.1_R = 0_R$; if no such n exists then R has characteristic 0. Where for $a \in R$

$$n.a := a + a + \cdots + a \quad (n \text{ times}).$$

Examples $\mathbb{Z}/n\mathbb{Z}$ has characteristic n.
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ have characteristic 0.
Lemma 2.1.4 *An integral domain has characteristic 0 or prime p.*
Proof Exercise Sheet. □
Example $\mathbb{F}_p[X]$ is an infinite ring of characteristic p.

Note: Ring will from now on always mean **commutative ring**.

Definition Let R be a ring. A nonempty subset I of R is called *ideal of* R (or *ideal in* R) if the following properties hold:

(I1) I is closed under addition: $a+b \in I$ for all $a, b \in I$

(I2) I is closed under multiplication by elements in R: $ra \in I$ for all $r \in R$ and for all $a \in I$.

Remark If I is an ideal then $\langle I, + \rangle \leq \langle R, + \rangle$ and so in particular $0_R \in I$ (check!). In fact if $a \in I$ then $(-1_R)a \in I$. But $(-1_R)a = -(1_R a) = -a$, the additive inverse of a.

Example All the different additive subgroups of $\mathbb{Z}$ are given exactly by all the $n\mathbb{Z}$ where $n \in \mathbb{N} \cup \{0\}$. One readily checks that all these sets satisfy (I2). Hence, these are also exactly all the different ideals of $\mathbb{Z}$ by the above remark. Note that $n\mathbb{Z}$ is *not* a subring for $n \neq 1$.

Lemma 2.2.1 (i) *If I, J are ideals of R then so is $I + J = \{x + y : x \in I, y \in J\}$.*

(ii) *If I is an ideal of R then $I = R$ if and only if $1_R \in I$ if and only if I is a subring of R.*

Proof. Exercise Sheet. □

Remark It follows from (i) that if I_j $(1 \leq j \leq k)$ are ideals then so is $I_1 + \ldots + I_k$.

Example Let R be a ring and $a \in R$. Consider the subset

$$Ra = \{ra \mid r \in R\}.$$

Ra is nonempty because it contains $0_R = 0_R.a$ (or $a = 1_R.a$). A quick check shows that Ra satisfies (I1) and (I2), so Ra is an ideal in R. One often uses the following notation:

$$(a) := Ra\ ,$$

and an ideal that can be written in such a way (i.e. as all the multiples of one particular element) will be called a *principal ideal*. We will study properties of such principal ideals more closely later on.

Note that $(0_R) = R.0_R = \{0_R\}$, and $(1_R) = R.1_R = R$.

Lemma 2.2.2 *Let R be a ring. Then R is a field if and only if the only ideals in R are $(0_R) = \{0_R\}$ and $(1_R) = R$.*

Proof. ($\Rightarrow$) Let R be a field and suppose that I is an ideal of R.

If $I \neq \{0_R\}$ then there is an $x \in I \backslash \{0_R\}$. Since R is a field x is a unit, that is there is a $y \in R$ such that $yx = 1_R$. But this means $1_R = yx \in I \Rightarrow I = R$ by Lemma 2.2.1(b).

($\Leftarrow$) Let $x \neq 0_R$ be in R. Then by assumption $(x) = \{rx : r \in R\}$, the ideal generated by x, is equal to R. In particular $1_R \in (x)$ and so there is an $r \in R$ such that $rx = 1_R$ which shows x is a unit and therefore R is a field. □

Example $\mathbb{Q}$ is a subring of $\mathbb{R}$ but *not* an ideal.

Now suppose I is an ideal of a ring R. Then I is in particular an additive subgroup of the additive group $(R,+)$ so that we can form the quotient group

$$R/I = \{a + I \,|\, a \in R\}.$$

(It is **important** that one writes $a+I$ and **not** aI.) Addition in this quotient group is as before given by
$(a+I)+(b+I) = (a+b)+I$.
Define a multiplication on R/I by

$$(a+I)(b+I) := ab + I.$$

We have to make sure that such a "multiplication" of cosets is well-defined, i.e. that the result does not depend on the choice of the coset representatives a and b.

So suppose $a + I = a' + I$ and $b + I = b' + I$. To get well-definition, we have to show that $ab + I = a'b' + I$ or, equivalently, that $ab \in a'b' + I$.
Now $a + I = a' + I$ is equivalent to $a \in a' + I$, which means that there exists $x \in I$ with $a = a' + x$. Similarly, $b + I = b' + I$ is equivalent to the existence of some $y \in I$ with $b = b' + y$. But then

$$ab = (a' + x)(b' + y) = a'b' + a'y + b'x + xy.$$

Since $x, y \in I$, we have $a'y,\ b'x,\ xy \in I$ by (I2), hence $z = a'y + b'x + xy \in I$ by (I1). Thus, $ab = a'b' + z \in a'b' + I$, and therefore this multiplication is well-defined.

It turns out that R/I with these "obvious" ways of addition and multiplication is again a ring. We omit the proof.

Theorem 2.2.3 *Let R be a ring and let I be an ideal in R. Then $R/I = \{a + I \mid a \in R\}$ together with*

$$\textit{addition} \quad (a + I) + (b + I) = a + b + I$$

and

$$\textit{multiplication} \quad (a + I)(b + I) = ab + I$$

is a ring with multiplicative identity $1_{R/I} = 1_R + I$ and additive identity $0_{R/I} = 0_R + I$.
This ring R/I is called the quotient (or factor) ring of R with respect to I.

Definition Let A and B be rings. A map $f: A \to B$ is called a *ring homomorphism* if it satisfies the following three properties:

(RH1) Additivity: $f(x + y) = f(x) + f(y)$ for all $x, y \in A$ (and so $f(0_A) = 0_B$; $f(-x) = -f(x)$);

(RH2) Multiplicativity: $f(xy) = f(x)f(y)$;

(RH3) $f(1_A) = 1_B$.

If the ring homomorphism $f: A \to B$ is bijective, then f is called a *ring isomorphism*.

Two rings A and B are called *isomorphic (as rings)*, denoted by $A \cong B$, if there exists a ring isomorphism $f: A \to B$.

For any ring homomorphism $f: A \to B$, we define the *kernel* $\mathrm{Ker}(f)$ and the *image* $\mathrm{Im}(f)$ as follows:

$$\mathrm{Ker}(f) = \{a \in A \mid f(a) = 0_B\} \quad \mathrm{Im}(f) = \{f(a) \mid a \in A\}.$$

Lemma 9.2.9. Let A and B be rings and let $f : A \to B$ be a ring homomorphism and let I be an ideal of A.

(a) $\ker(f)$ is an ideal of A.

(b) $\mathrm{im}(f)$ is a subring of B.

(c) $f(I)$ is an ideal of $\mathrm{im}(f)$.

(d) f is injective if and only if $\ker(f) = (0_A)$.

(e) If $f : A \to B$ is a ring homomorphism and if J is an ideal of A is this ideal must then f be also a ring homomorphism.

(f) If C is another ring and if $g : B \to C$ is a ring homomorphism, then the composition $g \circ f : A \to C$ is a ring homomorphism.

Proof.

(a) $f(0_A) = 0_B$ so $0_A \in \ker(f)$ which shows $\ker f \neq \emptyset$.

(b) If $x, y \in \ker f$ then $f(x+y) = f(x) + f(y) = 0_B + 0_B = 0_B$ so $x+y \in \ker f$ and $f(-x) = -f(x) = -0_B = 0_B$ so $-x \in \ker f$.

(c) If $x \in A$, $y \in \ker f$ then $f(xy) = f(x)f(y) = f(x)0_B$

shows that $by \in f(I)$ as required.

(d)–(f) Omitted. □

Example (See 2.2.4(c).) Let $f\colon \mathbb{Z} \to \mathbb{Q}$ be defined by $f(x) = x$. Then $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$ but $f(n\mathbb{Z}) = n\mathbb{Z}$ is *not* an ideal of $\mathbb{Q}$.

Example An important and often encountered case of a ring homomorphism is the following. Let R be a ring and I be an ideal in R. Consider the map

$$\pi\colon R \to R/I\colon a \mapsto a + I$$

from R onto the quotient ring R/I. This is clearly a ring homomorphism by the very way we defined addition and multiplication in R/I, and π is obviously surjective by the very construction of R/I. One also readily checks that $\mathrm{Ker}(\pi) = I$. This surjective ring homomorphism is sometimes called the *canonical surjection* of the ring R onto its quotient ring R/I.

Example Let A be a subring of a ring B, and let $b \in B$. Let $P(X) = a_0 + a_1X + \cdots + a_nX^n$ be a polynomial in the polynomial ring $A[X]$. Then we can evaluate this polynomial at b to get an element in B: $P(b) = a_0 + a_1b + \cdots + a_nb^n$. Thus, we get an *evaluation map* (evaluation in b):

$$ev_b \colon A[X] \to B \colon P(X) \mapsto P(b).$$

It's not difficult to verify that this map is indeed a ring homomorphism. Its kernel is

$$\mathrm{Ker}(ev_b) = \{P(X) \in A[X] \mid P(b) = 0_B\},$$

in other words, the kernel consists of all polynomials that have b as a root.

Example For

$$ev_i \colon \mathbb{C}[X] \to \mathbb{C}$$

(here, $i = \sqrt{-1}$) we get

$$\begin{aligned}\mathrm{Ker}(ev_i) &= \{P(X) \in \mathbb{C}[X] \mid P(i) = 0\} \\ &= \{(X - i)Q(X) \mid Q(X) \in \mathbb{C}[X]\} = (X - i)\end{aligned}$$

(principal ideal)

and for

$$ev_i \colon \mathbb{R}[X] \to \mathbb{C}$$

we get

$$\mathrm{Ker}(ev_i) = (X^2 + 1)$$

(exercise Sheet).

The next result is the ring-theoretic version of the "first isomorphism theorem for groups" (Theorem 1.5.1) and we omit the proof.

Theorem 2.2.5 (Main isomorphism theorem for rings) *Let A and B be rings and let $f: A \to B$ be a ring homomorphism. Let I be an ideal in A such that $I \subseteq \operatorname{Ker}(f)$. Then the map*

$$\overline{f}: A/I \to \operatorname{Im}(f): a + I \mapsto f(a)$$

is a well-defined surjective ring homomorphism.
$\overline{f}$ is injective if and only if $I = \operatorname{Ker}(f)$, in which case $\overline{f}$ is a ring isomorphism. In particular:

$$A/\operatorname{Ker}(f) \cong \operatorname{Im}(f).$$

Example Consider the ring homomorphism given by the evaluation map

$$ev_0: \mathbb{Q}[X] \to \mathbb{Q}: a_0 + a_1X + \cdots + a_nX^n \mapsto a_0.$$

This ring homomorphism is clearly surjective: For any $c \in \mathbb{Q}$, we obviously have that $ev_0(c) = c$. Also,

$$\begin{aligned}\operatorname{Ker}(ev_0) &= \{a_0 + a_1X + a_2X^2 + \cdots \in \mathbb{Q}[X] \mid a_0 = 0\} \\ &= X\mathbb{Q}[X] = (X).\end{aligned}$$

By the main isomorphism theorem for rings, we get

$$\mathbb{Q}[X]/(X) = \mathbb{Q}[X]/\operatorname{Ker}(ev_0) \cong \operatorname{Im}(ev_0) = \mathbb{Q}.$$

Similarly, if we consider $ev_1 : \mathbb{R}[X] \to \mathbb{R}$, we get again a surjective ring homomorphism since $ev_1(c) = c (\forall c \in \mathbb{R})$ with kernel

$$\begin{aligned} \mathrm{Ker}(ev_1) &= \{P(X) \in \mathbb{R}[X] \mid P(1) = 0\} \\ &= \{(X-1)Q(X) \mid Q(X) \in \mathbb{R}[X]\} = (X-1), \end{aligned}$$

which then yields

$$\mathbb{R}[X]/(X-1) \cong \mathbb{R}.$$

Example If we take the evaluation map $ev_i : \mathbb{R}[X] \to \mathbb{C}$ it can be shown (see exercise sheet) that

$$\mathbb{R}[X]/(X^2+1) \cong \mathbb{C}.$$

$ev_i : \mathbb{C}[X] \to \mathbb{C}$

وقالت طبقو المرهنة حلتة :

$\mathbb{C}[X] \setminus (X - i) \cong \mathbb{C}$

"ker{evi}

(x^2+1)

$f : A \to B$

domain codon

إما ترجمة - توفي (اختار التوفي المناسب) - مزاحات (مرهنة

إما اختيار ، الإجابة الصحيحة أو الخاطئة

choose the (or) right