MAU22102
Rings, Fields, and Modules
1 - Rings

Nicolas Mascot
mascotn@tcd.ie
Module web page

Hilary 2020–2021
Version: February 5, 2021

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Rings: Definitions, basic properties

Reminder: groups

Definition (Group)

A group is a set G equipped with a law (= operation)

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (x, y) & \longmapsto & x \cdot y \end{array}$$

such that:

- *(Associativity) For all $x, y, z \in G$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ $\rightsquigarrow$ $x \cdot y \cdot z \in G$ makes sense.*
- *(Identity) There exists an identity element $e \in G$ which satisfies: for all $x \in G$, $x \cdot e = e \cdot x = x$.*
- *(Inverses) Every $x \in G$ has an inverse $y \in G$ which satisfies: $x \cdot y = y \cdot x = e$.*

Reminder: groups

Remark

- Technically, we should write the group as $(G, \cdot)$ so as to specify the law.
- $G \neq \emptyset$, because $e \in G$. So the smallest (and most boring) possible group is $G = \{e\}$.
- The identity e is unique: If $e' \in G$ is another identity, then $e = e \cdot e' = e'$.
- Similarly, for each $x \in G$, the inverse of x is unique: If $y, y' \in G$ are inverses of x, then
$$y = y \cdot e = y \cdot x \cdot y' = e \cdot y' = y'.$$
$\rightsquigarrow$ we denote this unique inverse by x^{-1}.

Reminder: groups

Definition (Abelian group)

We say that a group G is Abelian if $x \cdot y = y \cdot x$ for all $x, y \in G$.

In an Abelian group, the operation is usually denoted by $+$ instead of $\cdot$, and inverses by $-x$ instead of x^{-1}.

Example

$(\mathbb{Z}, +)$ is an Abelian group.

Rings: definition

Definition (Ring)

A ring is a set R equipped with two laws:

$$\begin{array}{ccc} R \times R & \longrightarrow & R \\ (x,y) & \longmapsto & x+y \end{array} \quad \text{and} \quad \begin{array}{ccc} R \times R & \longrightarrow & R \\ (x,y) & \longmapsto & x \times y = xy \end{array}$$

such that:

- *(Addition) $(R,+)$ is an Abelian group.*
  The identity element for $+$ is written $0 \in R$. The inverse of $x \in R$ for $+$ is called the negative of x and written $-x$.
- *(Associativity) For all $x,y,z \in R$, $(xy)z = x(yz)$*
  $\rightsquigarrow xyz \in R$ makes sense.
- *(Identity) There exists an identity element $1 \in R$ which satisfies: for all $x \in R$, $x1 = 1x = x$.*
- *(Distributivity) For all $x,y,z \in R$, we have*
  $x(y+z) = (xy)+(xz)$ and $(x+y)z = (xz)+(yz)$.

Rings: examples

Example

- $(\mathbb{Z}, +, \times)$ is actually a ring.
- Let $n \in \mathbb{N}$. The set $\mathcal{M}_n(\mathbb{R})$ of $n \times n$ matrices with coefficients in $\mathbb{R}$ is a ring; its 0 is the matrix full of zeros, and its 1 is the identity matrix I_n.
- We could redefine the multiplication on $\mathcal{M}_n(\mathbb{R})$ by multiplying matrices coefficient-wise
  $\rightsquigarrow$ new ring structure on the same set $\mathcal{M}_n(\mathbb{R})$, with the same 0, but now the 1 is the matrix full of ones.

Rings: more examples

Example

- If R and S are rings, then their product
$$R \times S = \{(r, s) \mid r \in R, s \in S\}$$
endowed with the laws
$$(r, s) + (r', s') = (r + r', s + s'), \quad (r, s)(r', s') = (rr', ss'),$$
is a ring whose 0 is $(0_R, 0_S)$ and whose 1 is $(1_R, 1_S)$.

- If R is a ring, then we can define the ring
$$R[x] = \{r_n x^n + \cdots r_1 x + r_0 \mid r_0, r_1, \cdots, r_n \in R, n \in \mathbb{N}\}$$
of polynomials with coefficients in R.

Rings: basic properties

Remark

- $R \neq \emptyset$, because $0, 1 \in R$. We do not require $0 \neq 1$, more on this later.
- 0 is unique as the identity of $(R, +)$. Similarly, $1 \in R$ is unique (same proof, although $(R, \times)$ is not a group in general).
- Negatives are unique, as inverses for a group law.

Consequences of distributivity

Proposition

Let R be a ring. Then $x0 = 0x = 0$ for all $x \in R$, and $(-x)y = -(xy) = x(-y)$ for all $x, y \in R$.

Proof.

Let $x, y \in R$. Then

$$0x = 0x+x-x = 0x+1x-x = (0+1)x-x = 1x-x = x-x = 0;$$

similarly $x0 = x0 + x - x = x0 + x1 - x = x - x = 0.$

Therefore, $(-x)y + xy = (-x + x)y = 0y = 0$,
so $(-x)y = -(xy)$ since negatives are unique.
Similarly, $x(-y) = -xy$ because
$x(-y) + xy = x(y + -y) = x0 = 0.$ □

Consequences of distributivity

Proposition

Let R be a ring. Then $x0 = 0x = 0$ for all $x \in R$, and $(-x)y = -(xy) = x(-y)$ for all $x, y \in R$.

Corollary (Zero ring)

If $0 = 1$ in R, then $R = \{0\}$.

Proof.

If $0 = 1$, then for all $x \in R$, $x = x1 = x0 = 0$. □

Commutative rings

Definition (Commutative ring)

We say that a ring R is commutative if

$$xy = yx \text{ for all } x, y \in R.$$

Remark

By definition of a ring, $+$ is always commutative.

Example

The ring $\mathbb{Z}$ is commutative.

Counter-example

The ring $\mathcal{M}_n(\mathbb{R})$ is not commutative as soon as $n \geq 2$.

In this module, we will mostly focus on commutative rings.

The binomial formula

Theorem

In a commutative ring R, we have the binomial formula

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

for all $x, y \in R$ *and* $n \in \mathbb{N}$.

Proof.

When we expand $(x+y)^n = (x+y)(x+y)\cdots(x+y)$, we get a sum of terms such as $xxyxy\cdots$. As the ring is commutative, we may rearrange them in the form $x^k y^l$, where $k+l=n$, so $l=n-k$. Since $+$ is also commutative, we can gather the terms $x^k y^{n-k}$ which have the same k. The number of times we get $x^k y^{n-k}$ is by definition $\binom{n}{k}$. □

Domains & Fields

Invertible elements

Definition

An element $x \in R$ is invertible if there exists $y \in R$ such that $xy = 1 = yx$. This y is then unique, and denoted by x^{-1}. The set of invertibles of R is written $R^\times$.

Example

- $\mathbb{Z}^\times = \{1, -1\}$.
- $\mathcal{M}_n(\mathbb{R})^\times = \mathrm{GL}_n(\mathbb{R})$.

We always have $1 \in R^\times$. In fact, $R^\times$ is a group under $\times$, with identity 1, which is Abelian if R is commutative.

The 0 of R is never invertible, unless $R = \{0\}$: if 0 were invertible, then $1 = 00^{-1} = 0$.

Fields

Definition (Field)

A field is a commutative ring F such that $F^\times = F \setminus \{0\}$.

Example

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields.
If F is a field, then so is the rational fraction field $F(x) = \{\frac{P(x)}{Q(x)} \mid P(x), Q(x) \in F[x], Q(x) \neq 0\}$.

Counter-example

$\mathbb{Z}$ is not a field, since only 1 and -1 are invertible.
The zero ring $R = \{0\}$ is not a field, since $R \setminus \{0\} = \emptyset \neq R^\times = R$.

Fields

Definition (Field)

A field is a commutative ring F such that $F^\times = F \setminus \{0\}$.

Remark (Not examinable)

A "non-commutative field" is called a division algebra.
Example: the Hamilton quaternions.

Domains

Definition (Domain)

A domain (a.k.a integral domain) is a nonzero commutative ring D such that for all $x, y \in D$,

$$xy = 0 \text{ implies } x = 0 \text{ or } y = 0.$$

Counter-example

- If R and S are nonzero rings, then $R \times S$ is not a domain, since $x = (1_R, 0_S)$, $y = (0_R, 1_S) \in R \times S$ are such that $xy = (0_R, 0_S) = 0$ but $x, y \neq 0$.
- The set F of continuous functions $\mathbb{R} \longrightarrow \mathbb{R}$, equipped with point-wise operations $(f+g)(x) = f(x) + g(x)$, $(fg)(x) = f(x)g(x)$ for all $f, g \in F$ and $x \in \mathbb{R}$, is a commutative ring which is not a domain either: consider f which vanishes on $(-\infty, 1]$, and g which vanishes on $[-1, +\infty)$.

Domains

Definition (Domain)

A domain (a.k.a integral domain) is a nonzero commutative ring D such that for all $x, y \in D$,

$$xy = 0 \text{ implies } x = 0 \text{ or } y = 0.$$

Proposition

Every field is a domain.

Proof.

Let F be a field, and $x, y \in F$ be such that $xy = 0$. If $x \neq 0$, then x is invertible, whence $y = 1y = x^{-1}xy = x^{-1}0 = 0$. □

Counter-example

$\mathbb{Z}$ is a domain which is not a field.

Polynomials over a domain

Proposition

If D is a domain, then so is the polynomial ring $D[x]$, and we have the rule $\deg(PQ) = \deg P + \deg Q$ for all $P(x), Q(x) \in D[x]$.

Proof.

Let $P(x), Q(x) \in D[x]$, both non zero. We can write

$$P(x) = a_n x^n + \text{lower terms},$$

with $a_n \in D$, $a_n \neq 0$, so that $n = \deg P$; similarly

$$Q(x) = b_m x^m + \text{lower terms},$$

$b_m \neq 0$, $m = \deg Q$. Then

$$P(x)Q(x) = a_n b_m x^{n+m} + \text{lower terms},$$

and $a_n b_m \neq 0$ since D is a domain. Therefore $PQ \neq 0$, and has degree $n + m$. □

Classification of commutative rings

So far, we have

$$\text{Fields} \subsetneq \text{Domains} \subsetneq \text{Commutative rings}.$$

Commutative algebra is the branch of mathematics that refines this classification. A ring can be Noetherian, Artinian, a UFD, a PID, Euclidean, integrally closed, local, catenary, Cohen-Macaulay, Gorenstein, excellent, Japanese, ...

We will study some of this concepts in the next chapter.

From now on, in the rest of this module, we only consider commutative rings.

Subrings

Subrings

Definition (Subring)

Let R be a ring. A subring of R is a subset $S \subseteq R$ which contains 1_R and is closed under $+$, $-$, and $\times$.

Example

- $\mathbb{Z}$ is a subring of $\mathbb{Q}$.
- Let R be the ring of continuous functions $\mathbb{R} \longrightarrow \mathbb{R}$. Then smooth functions form a subring of R.

Counter-example

- $\mathbb{N}$ is not a subset of $\mathbb{Z}$, since it is not closed under $-$.
- Given two nonzero rings R and S, the subset $R \times \{0\} = \{(r, 0) \mid r \in R\}$ of $R \times S$ is closed under $+$, $-$, and $\times$, but it is not a subring since it does not contain $1 = (1_R, 1_S)$.

Operations on subrings

Proposition

An intersection of subrings is a subring.

Proof.

Let $S_1, S_2, \cdots, S_i, \cdots$ be subrings, and $S = \bigcap_i S_i$.
For all i, $1 \in S_i$ because S_i is a subring, so $1 \in S$.
Let $x, y \in S$. Then for all i, $x, y \in S_i$, so $x + y \in S_i$ because S_i is a subring; thus $x + y \in S$. Similarly for $-$ and $\times$. □

Operations on subrings

Definition

The subring generated by a subset $S \subset R$ is the smallest subring containing S.

This is the set of elements that we can obtain with $+, -, \times$ from S and 1; alternatively, it is

$$\bigcap_{\substack{T \text{ subring of } R \\ T \supseteq S}} T.$$

Example

The subring of $\mathbb{C}$ generated by i is

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\},$$

which is indeed a subring because

$(a + bi)(a' + b'i) = (aa' - bb') + (ab' + ba')i.$

Ideals

Ideals

Definition (Ideal)

An ideal of a ring R is a subset $I \subset R$ such that:

- $I \neq \emptyset$,
- *For all* $i, j \in I$, $i + j \in I$,
- *For all* $i \in I$ *and* $r \in R$, $ri \in I$.

Example

If F is the ring of continuous functions $\mathbb{R} \longrightarrow \mathbb{R}$ and if we fix $x_0 \in \mathbb{R}$, then the set of elements of F that vanish at $x = x_0$ is an ideal of F.

Remark

If I is an ideal, then $(I, +)$ is an Abelian group. Indeed, let $i \in I$; then $-i = (-1)i \in I$, so $0 = i + -i \in I$.
So the smallest ideal of R is $I = \{0\}$, and the largest is $I = R$.

Proper ideals

Lemma

Let $I \subseteq R$ be an ideal. Then

$$I = R \iff I \ni 1 \iff I \cap R^\times \neq \emptyset.$$

Proof.

If I contains an invertible $u \in R^\times$, then $1 = u^{-1}u \in I$.
If $I \ni 1$, then for all $r \in R$, $r = r1 \in I$, so $I \supseteq R$, so $I = R$.
If $I = R$, then $I \cap R^\times = R^\times \neq \emptyset$ since $R^\times \ni 1$. □

Corollary

The only subset of R which is both a subring and an ideal is R itself.

Corollary

If R is actually a field, then its only ideals are $\{0\}$ and R itself.

Operations on ideals

Proposition

An intersection of ideals is a ideal.

Proof.

Let $I_1, I_2, \cdots, I_k, \cdots$ be subrings, and $I = \bigcap_k I_k$.
For all k, $0 \in I_k$ because I_k is an ideal, so $0 \in I$.
Let $i, j \in I$. Then for all k, $i, j \in I_k$, so $i + j \in I_k$ because I_k is an ideal; thus $i + j \in I$.
Finally, let $i \in I$ and $r \in R$. Then for all k, $i \in I_k$, so $ri \in I_k$ because I_k is an ideal; thus $ri \in I$. □

Operations on ideals

Proposition

An intersection of ideals is a ideal.

Definition

The ideal generated by a subset $S \subseteq R$ is the smallest ideal containing S.

This is the set of elements that we can obtain from S and 0 with $+, -$, and multiplication by R; alternatively, it is

$$\bigcap_{\substack{I \text{ ideal of } R \\ I \supseteq S}} I.$$

Example

For $R = \mathbb{Z}$, the ideal generated by $\{4, 10\}$ is the ideal $2\mathbb{Z}$ of even numbers.

Operations on ideals

Proposition

If $I, J \subseteq R$ are ideals, then so is

$$I + J = \{i + j \mid i \in I, j \in J\}.$$

Proof.

Since I and J are ideals, they contain 0, so $0 = 0 + 0 \in I + J$.
Let $x, y \in I + J$, so $x = i + j$, $y = i' + j'$, where $i, i' \in I$, $j, j' \in J$. Then $x + y = (i + i') + (j + j') \in I + J$.
Let $x \in I + J$, so $x = i + j$ where $i \in I$, $j \in J$, and let $r \in R$.
Then $rx = ri + rj \in I + J$ since $ri \in I$, $rj \in J$. □

Operations on ideals

Proposition

If $I, J \subseteq R$ are ideals, then so is

$$IJ = \left\{ \sum_{k=1}^{n} i_k j_k \mid n \in \mathbb{N}, i_k \in I, j_k \in J \right\}.$$

Proof.

Since I and J are ideals, they contain 0, so $0 = 00 \in IJ$.
Let $x, y \in IJ$, so x and y are sums of products of the form $ij, i \in I, j \in J$. Then $x + y$ is a longer such sum, and thus lies in IJ.
Let $x \in IJ$, so $x = \sum_{k=1}^{n} i_k j_k$, where $n \in \mathbb{N}$ and $i_k \in I$, $j_k \in J$ for all k, and let $r \in R$. Then
$rx = r \sum_{k=1}^{n} i_k j_k = \sum_{k=1}^{n} (r i_k) j_k \in IJ$ since $r i_k \in I$ for all k. □

Operations on ideals

Proposition

An intersection of ideals is a ideal.

Proposition

If $I, J \subseteq R$ are ideals, then so is

$$I + J = \{i + j \mid i \in I, j \in J\}.$$

Proposition

If $I, J \subseteq R$ are ideals, then so is

$$IJ = \left\{ \sum_{k=1}^{n} i_k j_k \mid n \in \mathbb{N}, i_k \in I, j_k \in J \right\}.$$

Principal ideals

Let R be a ring. For $x \in R$, write

$$(x) = xR = \{xy \mid y \in R\}.$$

This is the ideal of R generated by $\{x\}$.

Definition (Principal)

An ideal is principal if it is of the form xR for some $x \in R$.
A ring is principal if all its ideals are principal.

Example

We will prove later that $\mathbb{Z}$ is principal,which means that every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

Principal ideals

Definition (Principal)

An ideal is principal if it is of the form xR for some $x \in R$.
A ring is principal if all its ideals are principal.

Example

We will prove later that $\mathbb{Z}$ is principal,which means that every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

Counter-example

Let $R = \mathbb{Z}[x]$, and $I = \{P(x) \in R \mid P(0) \text{ is even}\}$. Then I is an ideal of R, but it is not principal: suppose we $G(x) \in R$ such that $I = (G)$, then as $2 \in I$, $2 = GH$ for some $H(x) \in R$, so $\deg G = \deg H = 0$, so $G = \pm 2$. But then $P(x) = x \in I$ yet is not a multiple of G, absurd. So R is not principal.

Ring morphisms

Reminder: group morphisms

Definition (Group morphism)

A morphism from a group $(G, \cdot)$ to a group $(H, \times)$ is a function $f : G \longrightarrow H$ which satisfies $f(g \cdot g') = f(g) \times f(g')$ for all $g, g' \in G$.

This automatically implies that $f(e_G) = e_H$, and that $f(g^{-1}) = f(g)^{-1}$ for all $g \in G$.

Reminder: group morphisms

Definition (Group morphism)

A morphism from a group $(G, \cdot)$ *to a group* $(H, \times)$ *is a function* $f : G \longrightarrow H$ *which satisfies* $f(g \cdot g') = f(g) \times f(g')$ *for all* $g, g' \in G$*.*

Definition (Image)

The image of a group morphism $f : G \longrightarrow H$ *is*

$$\operatorname{Im} f = \{f(g) \mid g \in G\} \subseteq H.$$

$\operatorname{Im} f$ is a subgroup of H.

Definition (Kernel)

The kernel of a group morphism $f : G \longrightarrow H$ *is*

$$\operatorname{Ker} f = \{g \in G \mid f(g) = e_H\} \subseteq G.$$

$\operatorname{Ker} f$ is a normal subgroup of G.

Ring morphisms

Definition (Ring morphism)

Let R and S be rings. A morphism from R to S is a function $f : R \longrightarrow S$ which satisfies:

- *For all $x, y \in R$, $f(x+y) = f(x) + f(y)$,*
- *For all $x, y \in R$, $f(xy) = f(x)f(y)$,*
- *$f(1_R) = 1_S$.*

Remark

By the first point, f is in particular a group morphism from $(R, +)$ to $(S, +)$, so we automatically have that $f(0_R) = 0_S$, and that $f(-x) = -f(x)$ for all $x \in R$.

f also induces a group morphism from $(R^\times, \times)$ to $(S^\times, \times)$. Indeed, if $u \in R^\times$, then $f(u)f(u^{-1}) = f(uu^{-1}) = f(1_R) = 1_S$, which means that $f(u)$ is invertible with inverse $f(u)^{-1}$.

Ring morphisms

Definition (Ring morphism)

Let R and S be rings. A morphism from R to S is a function $f : R \longrightarrow S$ which satisfies:

- *For all $x, y \in R$, $f(x+y) = f(x) + f(y)$,*
- *For all $x, y \in R$, $f(xy) = f(x)f(y)$,*
- $f(1_R) = 1_S$.

Example

Let R be a ring, and fix $r \in R$. Then the evaluation map

$$\begin{array}{ccc} R[x] & \longrightarrow & R \\ P(x) & \longmapsto & P(r) \end{array}$$

is a ring morphism. Indeed, given $P(x), Q(x) \in R[x]$, we do have $(P+Q)(r) = P(r) + Q(r)$, $(PQ)(r) = P(r)Q(r)$, and $1_{R[x]}(r) = 1_R$.

Ring morphisms

Definition (Ring morphism)

Let R and S be rings. A morphism from R to S is a function $f : R \longrightarrow S$ which satisfies:

- *For all $x, y \in R$, $f(x+y) = f(x) + f(y)$,*
- *For all $x, y \in R$, $f(xy) = f(x)f(y)$,*
- *$f(1_R) = 1_S$.*

Remark

If $f : R \longrightarrow S$ and $g : S \longrightarrow T$ are ring morphisms, then so is $g \circ f : R \longrightarrow T$.

Image of a morphism

Definition (Image of a morphism)

The image of a ring morphism $f : R \longrightarrow S$ *is*

$$\operatorname{Im} f = \{f(r) \mid r \in R\} \subseteq S.$$

Example

Let $f : \begin{array}{ccc} \mathbb{Z}[x] & \longrightarrow & \mathbb{C} \\ P(x) & \longmapsto & P(i) \end{array}$.

If $P(x) \in \mathbb{Z}[x]$, then $P(x) = \sum_{k=0}^{n} a_k x^k$ with $a_k \in \mathbb{Z}$ for all k, so $P(i) = \sum_{k=0}^{n} a_k i^k$ is of the form $a + bi$ with $a, b \in \mathbb{Z}$ since $i^k = \pm 1$ or $\pm i$ for all k, so

$$\operatorname{Im} f \subseteq \{a + bi \mid a, b \in \mathbb{Z}\} = \mathbb{Z}[i].$$

Conversely, every $a + bi \in \mathbb{Z}[i]$ is reached by $P(x) = a + bx \in \mathbb{Z}[x]$, so

$$\operatorname{Im} f = \mathbb{Z}[i],$$

whence the notation $\mathbb{Z}[i]$.

Image of a morphism

Definition (Image of a morphism)

The image of a ring morphism $f : R \longrightarrow S$ is

$$\operatorname{Im} f = \{f(r) \mid r \in R\} \subseteq S.$$

Proposition

If $f : R \longrightarrow S$ is a ring morphism, then $\operatorname{Im} f$ is a subring of S.

Proof.

$1_S = f(1_R) \in \operatorname{Im} f$.
Besides, if $s, s' \in \operatorname{Im} f$, then $s = f(r)$, $s' = f(r')$ for some $r, r' \in R$, so
$s + s' = f(r) + f(r') = f(r + r') \in \operatorname{Im} f$,
$s - s' = f(r) - f(r') = f(r) + f(-r') = f(r - r') \in \operatorname{Im} f$,
and $ss' = f(r)f(r') = f(rr') \in \operatorname{Im} f$. □

Image of a morphism

Definition (Image of a morphism)

The image of a ring morphism $f : R \longrightarrow S$ is

$$\operatorname{Im} f = \{f(r) \mid r \in R\} \subseteq S.$$

Proposition

If $f : R \longrightarrow S$ is a ring morphism, then $\operatorname{Im} f$ is a subring of S.

Remark

f is surjective $\iff \operatorname{Im} f = S$.

Kernel of a morphism

Definition (Kernel of a morphism)

The kernel of a ring morphism $f : R \longrightarrow S$ is

$$\operatorname{Ker} f = \{r \in R \mid f(r) = 0_S\} \subseteq R.$$

Example

Let F be the ring of continuous functions $\mathbb{R} \longrightarrow \mathbb{R}$, and fix $x_0 \in \mathbb{R}$. Then

$$\begin{array}{ccc} F & \longrightarrow & \mathbb{R} \\ f & \longmapsto & f(x_0) \end{array}$$

is a ring morphism, whose kernel is the subset of F formed of the functions which vanish at x_0.

Kernel of a morphism

Definition (Kernel of a morphism)

The kernel of a ring morphism $f : R \longrightarrow S$ *is*

$$\operatorname{Ker} f = \{r \in R \mid f(r) = 0_S\} \subseteq R.$$

Proposition

If $f : R \longrightarrow S$ *is a ring morphism, then* $\operatorname{Ker} f$ *is a ideal of* R*.*

Proof.

$0_R \in \operatorname{Ker} f$ because $f(0_R) = 0_S$.
If $z, z' \in \operatorname{Ker} f$, then $f(z + z') = f(z) + f(z') = 0_S + 0_S = 0_S$, so $z + z' \in \operatorname{Ker} f$.
If $z \in \operatorname{Ker} f$ and $r \in R$, then $f(rz) = f(r)f(z) = f(r)0_S = 0_S$, so $rz \in \operatorname{Ker} f$. □

Kernel of a morphism

Definition (Kernel of a morphism)

The <u>*kernel*</u> *of a ring morphism* $f : R \longrightarrow S$ *is*

$$\operatorname{Ker} f = \{r \in R \mid f(r) = 0_S\} \subseteq R.$$

Proposition

If $f : R \longrightarrow S$ *is a ring morphism, then* $\operatorname{Ker} f$ *is a* <u>*ideal*</u> *of* R*.*

Remark

f is injective $\Longleftrightarrow \operatorname{Ker} f = \{0\}$.

Indeed, $\Rightarrow$ is clear; for $\Leftarrow$, simply observe that

$f(r) = f(r') \Leftrightarrow f(r) - f(r') = 0 \Leftrightarrow f(r - r') = 0 \Leftrightarrow r - r' \in \operatorname{Ker} f$.

Quotient rings

Binary relations

Definition (Relation)

Let X be a set. A relation R on X is a map

$$\begin{array}{ccc} X \times X & \longrightarrow & \{True, False\} \\ (x,y) & \longmapsto & xRy, \end{array}$$

Example

- $X = \mathbb{R}$, $R = <$.
- $X =$ any set, $R = \neq$.
- $X =$ subsets of some fixed set, $R = \subseteq$.

Binary relations

Definition (Relation)

Let X be a set. A relation R on X is a map

$$\begin{array}{ccc} X \times X & \longrightarrow & \{True, False\} \\ (x, y) & \longmapsto & xRy, \end{array}$$

Definition (Equivalence relation)

A relation R on a set X is an equivalence relation if:

- *(Reflexive) For all $x \in X$, xRx.*
- *(Symmetric) For all $x, y \in X$, $xRy \iff yRx$.*
- *(Transitive) For all $x, y, z \in X$, if xRy and yRz, then xRz.*

Example

If $X = \{$ People $\}$, then the relation "have the same given name" is an equivalence relation.

Quotient sets

Let X be a set, and let $\sim$ be an equivalence relation on X.

Definition (Equivalence class)

The class of $x \in X$ *is* $\overline{x} = \{y \in X \mid y \sim x\}$.

Definition (Quotient set)

The quotient of X *by* $\sim$ *is* $X/\sim\ = \{\overline{x} \mid x \in X\}$.

It comes with the projection $\begin{array}{ccc} X & \longrightarrow & X/\sim \\ x & \longmapsto & \overline{x}. \end{array}$

Example

If $X = \{\text{People}\}$ and $\sim\, =$ "have the same (given) name", then

$$\overline{x} = \{\text{ People } y \mid y \text{ has same name as } x\},$$

$$X/\sim = \Big\{\{\text{People named } n\} \mid n \text{ a name}\Big\}.$$

Induced maps

Let X be a set, $\sim$ an equivalence relation on X,
and $f : X \longrightarrow Y$ a map.

Definition

ONLY *if* $x \sim x' \implies f(x) = f(x')$, *then we can define*

$$\begin{array}{rcl} \overline{f} : X/\sim & \longrightarrow & Y \\ \overline{x} & \longmapsto & f(x). \end{array}$$

We then say that "f passes to the quotient".

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ \downarrow & \overset{?}{\nearrow} & \\ X/\sim & & \end{array}$$

Induced maps

Let X be a set, $\sim$ an equivalence relation on X, and $f : X \longrightarrow Y$ a map.

Definition

ONLY *if* $x \sim x' \implies f(x) = f(x')$, *then we can define*

$$\begin{array}{rcl} \overline{f} : X/\sim & \longrightarrow & Y \\ \overline{x} & \longmapsto & f(x). \end{array}$$

We then say that "f passes to the quotient".

Example

If $X = \{\text{People}\}$ and $\sim =$ "have the same full name", then

- If $f(x) =$ Initials of x, then f passes to the quotient.
- If $f(x) =$ age of x, then $\overline{f}$ is not defined.

Quotient structures: the example of groups

Let G be a group. For which $\sim$ on G do we still have a group structure on $G/\sim$? In other words, when do the definitions $\overline{g}\,\overline{h} = \overline{gh}$, $\overline{g}^{-1} = \overline{g^{-1}}$ make sense?

Then $N = \overline{e} = \{g \in G \mid g \sim e\}$ would determine $\sim$, since

$$g \sim h \Leftrightarrow \overline{g} = \overline{h} \Leftrightarrow \overline{g}\,\overline{h}^{-1} = \overline{e} \Leftrightarrow \overline{gh^{-1}} = \overline{e} \Leftrightarrow gh^{-1} \in N.$$

And we would need $\begin{cases} g, h \in N & \Rightarrow & gh \in N, \\ g \in N & \Rightarrow & g^{-1} \in N, \\ g \in N, h \in G & \Rightarrow & hgh^{-1} \in N, \end{cases}$

which means $N \lhd G$.

Conversely, we check that if $N \lhd G$, then $\sim$ defined by

$$g \sim h \iff gh^{-1} \in N \iff g = hn \text{ for some } n \in N$$

is an equivalence relation such that the group law passes to the quotient. This quotient group is denoted by G/N.

Quotient structures: the example of groups

And we would need $\begin{cases} g,h \in N & \Rightarrow & gh \in N, \\ g \in N & \Rightarrow & g^{-1} \in N, \\ g \in N, h \in G & \Rightarrow & hgh^{-1} \in N, \end{cases}$

which means $N \lhd G$.

Conversely, we check that if $N \lhd G$, then $\sim$ defined by

$$g \sim h \iff gh^{-1} \in N \iff g = hn \text{ for some } n \in N$$

is an equivalence relation such that the group law passes to the quotient. This quotient group is denoted by G/N.

For example, to check that $\overline{g}\,\overline{h} = \overline{gh}$ makes sense, we must prove that $g \sim g', h \sim h' \implies gh \sim g'h'$.
And indeed, if $g' = gn$, $h' = hm$ for some $n, m \in N$,
then $(g'h')(gh)^{-1} = gn \underbrace{hmh^{-1}}_{\in N} g^{-1} \in N$.

In particular, the projection $G \longrightarrow G/N$ is actually a morphism.

Quotient rings

Let R be a ring. For which $\sim$ on R do we still have a ring structure on $R/\sim$ by the definitions $\overline{x} + \overline{y} = \overline{x+y}$, $\overline{x}\,\overline{y} = \overline{xy}$?

Let $I = \overline{0} = \{x \in R \mid x \sim 0\}$. We have

$$x \sim y \Leftrightarrow \overline{x} = \overline{y} \Leftrightarrow \overline{x} - \overline{y} = \overline{0} \Leftrightarrow \overline{x-y} = \overline{0} \Leftrightarrow x - y \in I.$$

And we need $\begin{cases} i, j \in I & \Rightarrow & i + j \in I, \\ i \in I, x \in R & \Rightarrow & xi \in I, \end{cases}$

which means that I is an <u>ideal</u> of R.

Conversely, if I is any ideal of R, then $\sim$ defined by

$$x \sim y \iff x - y \in I \iff y = x + i \text{ for some } i \in I$$

is an equivalence relation such that $+$ and $\times$ pass to the quotient:

If $x \sim x', y \sim y'$, then $x' = x + i, y' = y + j$ for some $i, j \in I$,
so $x' + y' = x + y + (i + j) \sim x + y$,
and $x'y' = (x + i)(y + j) = xy + (iy + xj + ij) \sim xy$.

Quotient rings

Conversely, if I is any ideal of R, then $\sim$ defined by

$$x \sim y \iff x - y \in I \iff y = x + i \text{ for some } i \in I$$

is an equivalence relation such that $+$ and $\times$ pass to the quotient:
If $x \sim x', y \sim y'$, then $x' = x + i, y' = y + j$ for some $i, j \in I$,
so $x' + y' = x + y + (i + j) \sim x + y$,
and $x'y' = (x + i)(y + j) = xy + (iy + xj + ij) \sim xy$.

This quotient ring is denoted by R/I. Its 0 is $\overline{0}$, its 1 is $\overline{1}$.
Besides, we have $-\overline{x} = \overline{-x}$, and the projection $R \longrightarrow R/I$ is a ring morphism.

Quotient rings

This quotient ring is denoted by R/I. Its 0 is $\overline{0}$, its 1 is $\overline{1}$. Besides, we have $-\overline{x} = \overline{-x}$, and the projection $R \longrightarrow R/I$ is a ring morphism.

Remark

Every ideal $I \lhd R$ is a kernel, namely that of $R \to R/I$.

Every subring $S \subseteq R$ is an image, namely that of $S \hookrightarrow R$.

Example of quotient ring: $\mathbb{Z}/n\mathbb{Z}$

Let $n \in \mathbb{N}$. Then $n\mathbb{Z} = \{nx, x \in \mathbb{Z}\} \subseteq \mathbb{Z}$ is an ideal, so we have the quotient ring $\mathbb{Z}/n\mathbb{Z}$. This is the ring of integers modulo n.

By definition of the quotient, two integers are viewed as the same element of $\mathbb{Z}/n\mathbb{Z}$ iff. they differ by a multiple of n.

Example

In $\mathbb{Z}/5\mathbb{Z}$, we have $\overline{2} \times \overline{3} = \overline{6} = \overline{1}$.

So $\overline{2}$ has become invertible, $\overline{2}^{-1} = \overline{3}$.

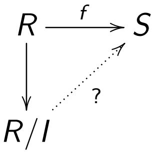
In fact, $\mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ is actually a field!

The isomorphism theorem

Induced ring morphisms

Proposition

Let R and S be rings, $f : R \longrightarrow S$ a morphism, and $I \lhd R$ an ideal. Then f passes to the quotient into $\overline{f} : R/I \longrightarrow S$ iff. $I \supseteq \operatorname{Ker} f$. In this case, $\overline{f}$ is also a ring morphism, and $\operatorname{Im} \overline{f} = \operatorname{Im} f \subseteq S$.



Induced ring morphisms

Proposition

Let R and S be rings, $f : R \longrightarrow S$ a morphism, and $I \lhd R$ an ideal. Then f passes to the quotient into $\overline{f} : R/I \longrightarrow S$ iff. $I \supseteq \operatorname{Ker} f$. In this case, $\overline{f}$ is also a ring morphism, and $\operatorname{Im} \overline{f} = \operatorname{Im} f \subseteq S$.

Proof.

f passes to the quotient iff. $f(r) = f(r')$ whenever $\overline{r} = \overline{r'}$, that is to say whenever $r - r' \in I$. But also $f(r) = f(r') \Leftrightarrow f(r) - f(r') = 0 \Leftrightarrow f(r - r') = 0 \Leftrightarrow r - r' \in \operatorname{Ker} f$, whence the condition.

If $\overline{f}$ exists, then it is automatically a morphism, since $\overline{f}(\overline{x}) + \overline{f}(\overline{y}) = f(x) + f(y) = f(x + y) = \overline{f}(\overline{x + y}) = \overline{f}(\overline{x} + \overline{y})$, and similarly $\overline{f}(\overline{x})\overline{f}(\overline{y}) = \overline{f}(\overline{xy})$ and $\overline{f}(\overline{1}) = f(1) = 1$. Finally $\operatorname{Im} \overline{f} = \operatorname{Im} f$ because $\overline{f}(\overline{x}) = f(x)$ by definition of $\overline{f}$. □

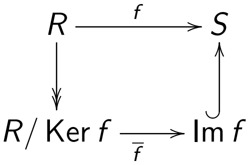
The isomorphism theorem

Theorem (First isomorphism theorem)

Let $f : R \longrightarrow S$ be a ring morphism. Then f induces a ring <u>*isomorphism*</u> $\overline{f} : R/\operatorname{Ker} f \xrightarrow{\sim} \operatorname{Im} f$.

Proof.

By the previous proposition, $\overline{f}$ exists, and is surjective onto $\operatorname{Im} \overline{f} = \operatorname{Im} f$. Besides, for all $\overline{x} \in \operatorname{Ker} \overline{f} \subseteq R/\operatorname{Ker} f$, we have $0 = \overline{f}(\overline{x}) = f(x)$, so $x \in \operatorname{Ker} f$, so $\overline{x} = \overline{0} \in R/\operatorname{Ker} f$; thus $\operatorname{Ker} \overline{f} = \{\overline{0}\}$ so $\overline{f}$ is also injective. □



The isomorphism theorem

Theorem (First isomorphism theorem)

Let $f : R \longrightarrow S$ be a ring morphism. Then f induces a ring <u>*isomorphism*</u> $\overline{f} : R/\operatorname{Ker} f \xrightarrow{\sim} \operatorname{Im} f$.

Proof.

By the previous proposition, $\overline{f}$ exists, and is surjective onto $\operatorname{Im} \overline{f} = \operatorname{Im} f$. Besides, for all $\overline{x} \in \operatorname{Ker} \overline{f} \subseteq R/\operatorname{Ker} f$, we have $0 = \overline{f}(\overline{x}) = f(x)$, so $x \in \operatorname{Ker} f$, so $\overline{x} = \overline{0} \in R/\operatorname{Ker} f$; thus $\operatorname{Ker} \overline{f} = \{\overline{0}\}$ so $\overline{f}$ is also injective. □

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ \downarrow & & \uparrow \\ X/\sim & \xrightarrow[\overline{f}]{} & \operatorname{Im} f \end{array}$$

where $x \sim x' \Leftrightarrow f(x) = f(x')$.

The isomorphism theorem

Theorem (First isomorphism theorem)

Let $f : R \longrightarrow S$ be a ring morphism. Then f induces a ring <u>*isomorphism*</u> $\overline{f} : R/\operatorname{Ker} f \overset{\sim}{\longrightarrow} \operatorname{Im} f$.

Proof.

By the previous proposition, $\overline{f}$ exists, and is surjective onto $\operatorname{Im} \overline{f} = \operatorname{Im} f$. Besides, for all $\overline{x} \in \operatorname{Ker} \overline{f} \subseteq R/\operatorname{Ker} f$, we have $0 = \overline{f}(\overline{x}) = f(x)$, so $x \in \operatorname{Ker} f$, so $\overline{x} = \overline{0} \in R/\operatorname{Ker} f$; thus $\operatorname{Ker} \overline{f} = \{\overline{0}\}$ so $\overline{f}$ is also injective. □

Application: In order to understand a quotient ring R/I, find a morphism $f : R \longrightarrow S$ such that $I = \operatorname{Ker} f$; then

$$R/I \simeq \operatorname{Im} f \subseteq S.$$

Example: the nature of $\mathbb{C}$

Let us apply the isomorphism theorem to the morphism

$$\begin{array}{rcl} f : \mathbb{R}[x] & \longrightarrow & \mathbb{C} \\ P(x) & \longmapsto & P(i). \end{array}$$

Every $a + bi \in \mathbb{C}$ is reached by $P(x) = a + bx$, so $\operatorname{Im} f = \mathbb{C}$. Thus $\mathbb{R}[x]/\operatorname{Ker} f \simeq \mathbb{C}$.

If $P(x) \in \operatorname{Ker} f$, then $P(i) = 0$ and $P(-i) = P(\bar{i}) = \overline{P(i)} = 0$, so $P(x)$ is divisible by $(x - i)(x + i) = x^2 + 1$. Thus

$$\operatorname{Ker} f = (x^2 + 1) = \{(x^2 + 1)Q(x),\ Q(x) \in \mathbb{R}[x]\}.$$

In conclusion, $\mathbb{C} \simeq \mathbb{R}[x]/(x^2 + 1)$ is "$\mathbb{R}$ adjoined some x such that $x^2 + 1 = 0$".