Saturated ideals and direct products

Marc Moreno Maza

CS 9652, January 20, 2020
Plan

Rings

Ideals

Maximal, Prime, Radical and Primary Ideals

Irreducible Ideals, Primary Decompositions

Saturated Ideals

Rings of Fractions

Relatively Prime Ideals

Products of Rings
Plan

Rings

Ideals

Maximal, Prime, Radical and Primary Ideals

Irreducible Ideals, Primary Decompositions

Saturated Ideals

Rings of Fractions

Relatively Prime Ideals

Products of Rings
**Operation (1/2)**

**Definition**

Given a non-empty set $M$, an *internal operation* (or simply *operation*) over $M$ is a function $f$ that maps any couple $(x, y)$ of elements from $M$ with an element $f(x, y)$ of $M$. The operation $f$

- is *associative* if the following holds
  $$(\forall x, y, z \in M) \quad f(x, f(y, z)) = f(f(x, y), z),$$

- is *commutative* if the following holds
  $$(\forall x, y \in M) \quad f(x, y) = f(y, x).$$

The set $M$ possesses an *identity element* if there exists $e \in M$ such that

$$(\forall x \in M) \quad f(e, x) = x = f(x, e)$$

Moreover, in this case, an element $x \in M$ possesses a *symmetric element* (or *reciprocal element*) if the following holds

$$(\exists x' \in M) \quad f(x, x') = f(x', x) = e$$
Proposition
Let $\mathbb{M}$ be a non-empty set with an operation $f$.

(i) If $\mathbb{M}$ possesses an identity element, then it is unique.

(ii) Moreover, in this case, if an element $x \in \mathbb{M}$ possesses a symmetric element $x' \in \mathbb{M}$, then it is unique.

Remark
For a non-empty set $\mathbb{M}$ with an associative operation $f$ it is natural to define $f(x_1, x_2, \ldots, x_n)$ for $x_1, x_2, \ldots, x_n \in \mathbb{M}$ with $n \geq 3$ by

$$f(x_1, x_2, \ldots, x_n) = f(x_1, f(x_2, \ldots, x_n))$$
A semi-group is a set \( M \) endowed with an operation such that this operation is associative.

- If for this operation, the set \( M \) admits an identity element, then it is said to be a monoid. Furthermore, if for this operation every element possesses a symmetric element, then the monoid is said to be a group.

- If this operation is commutative, then it is usually denoted additively (provided that this does lead to confusion with another operation) and the semi-group is said abelian or commutative. Otherwise this operation is usually denoted multiplicatively.

- If \( M \) is an abelian semi-group and a monoid, then its identity element is denoted 0 and \( M \) is said to be an abelian monoid.

- If \( M \) is a monoid which is not known to be commutative then its identity element is denoted 1.

- If \( M \) is an abelian monoid and a group, then the symmetric element of an element \( x \in M \) is denoted \(-x\) and called the opposite of \( x \). Moreover, in this case, \( M \) is said to be an abelian group.

- If \( M \) is a group which is not known to be commutative then the symmetric element of an element \( x \in M \) is denoted \( x^{-1} \) and called the multiplicative inverse of \( x \) (or simply the inverse of \( x \)).
A *semi-ring* is a set $A$ endowed with two operations one being denoted additively and the other being denoted multiplicatively, called respectively the *addition* of $A$ and the *multiplication* of $A$ such that

(i) $A$ is an abelian monoid for its addition,
(ii) $A^*$ is a semi-group for its multiplication,
(iii) the multiplication of $A$ is *distributive* w.r.t. its addition, which means that the following two conditions hold:

\[ (\forall x, y, z \in A) \; x(y + z) = xy + xz \; (\text{left-distributivity}), \]
\[ (\forall x, y, z \in A) \; (y + z)x = yx + zx \; (\text{right-distributivity}). \]

where $A^* = A \setminus \{0\}$. 
If $A$ is an abelian group for its addition, then $A$ is said to be a *ring*. From now on, we assume that $A$ is a ring.

- If $A^*$ is a monoid for its multiplication, then $A$ is said to be a *ring with identity element*.
- If $A^*$ is an abelian semi-group for its multiplication, then $A$ is said to be a *commutative ring*.
- If $A^*$ is an abelian monoid for its multiplication, then $A$ is said to be a *commutative ring with identity element*.
- If $A^*$ is a group for its multiplication, then $A$ is said to be a *division ring* (or a *skew field*).
- If $A^*$ is an abelian group for its multiplication, then $A$ is said to be a *field*. 
Some properties of rings (1/2)

Let $\mathbb{A}$ be a ring. For $x, y, z \in \mathbb{A}$ we have

$$x(y - z) + xz = x((y - z) + z) = xy \quad \text{and} \quad (y - z)x + zx = ((y - z) + z)x = yx$$

We deduce:

$$x(y - z) = xy - xz \quad \text{and} \quad (y - z)x = yx - zx. \quad (1)$$

By setting $y = z$ we obtain

$$x \times 0 = 0 = 0 \times x. \quad (2)$$

By setting $y = 0$ in Equation (1) we obtain

$$x \times (-z) = -(xz) \quad \text{and} \quad (-z)x = -(zx) \quad (3)$$

which implies

$$(-x)(-z) = xz. \quad (4)$$

Then, for every positive integer $n \in \mathbb{N}$ we deduce from Equation (4)

$$(-x)^n = (-1)^n x^n \quad (5)$$
Let $\mathbb{A}$ be a commutative ring with identity element. Let $x \in \mathbb{A}$. Because of the rule $x^{n+m} = x^n x^m$ with $n, m$ positive integers, it is natural to define

$$x^0 = 1$$  \hspace{1cm} (6)

Then, one obtains the \textit{Newton binomial formula} for every $x, y \in \mathbb{A}$

$$(x + y)^n = \sum_{k=0}^{n \choose k} x^k y^{n-k}$$  \hspace{1cm} (7)
Examples

We illustrate the above definitions.

- The set of the natural integer numbers $\mathbb{N}$ (endowed with its natural addition and multiplication) is a semi-ring but not a ring.

- The set of the integer numbers $\mathbb{Z}$ is a commutative ring with identity element, but not a field.

- For $p \in \mathbb{Z}$ with $p \geq 2$, the subset $p\mathbb{Z}$ of $\mathbb{Z}$ consisting of the multiples of $p$ is a commutative ring, but not a commutative ring with identity element.

- For $n \geq 2$, the set $\mathcal{M}_{n,n}(\mathbb{Z})$ of the square matrices of order $n$ with integer coefficients, is a ring with identity element, but not a commutative ring.
Complex numbers

- Let $\mathbb{F}$ be a field such that for every element $x \in \mathbb{F}$ we have $x^2 \neq -1$.
- Then, the subset $\text{Complex}(\mathbb{F})$ of $\mathcal{M}_{2,2}(\mathbb{F})$ (the ring of square matrices with order 2 and coefficients in $\mathbb{F}$) consisting of the matrices of the form

\[
C(a, b) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}
\]

is a field (for the addition and the multiplication of $\mathcal{M}_{2,2}(\mathbb{F})$), called the complex field of $\mathbb{F}$.
- It is also a vector subspace of $\mathcal{M}_{2,2}(\mathbb{F})$ with dimension 2.
Let $F$ be a field such that for all $x, y, z \in F$ we have $x^2 + y^2 + z^2 \neq -1$. Then, the subset $\text{Quaternion}(F)$ of $\mathcal{M}_{4,4}(F)$ (the ring of square matrices with order 4 and coefficients in $F$) consisting of the matrices of the form

$$H(a, b, c, d) = \begin{pmatrix} d & a & b & c \\ -a & d & -c & b \\ -b & c & d & -a \\ -c & -b & a & d \end{pmatrix}$$

is a division ring, which is not a field, called the quaternion ring of $F$. It is also a vector subspace of $\mathcal{M}_{4,4}(F)$ with dimension 4.
Plan

Rings

Ideals

Maximal, Prime, Radical and Primary Ideals

Irreducible Ideals, Primary Decompositions

Saturated Ideals

Rings of Fractions

Relatively Prime Ideals

Products of Rings
Definition
Let $A$ be a commutative ring with identity element. A non-empty subset $I$ of $A$ is an *ideal* of $A$ if and only if the following conditions hold

(i) $0 \in I$,

(ii) $1 \notin I$,

(iii) $(\forall a, b \in A)(\forall x, y \in I) \; ax - by \in I$. 
Definition
Let $A$ and $B$ be two commutative rings with identity element. A function that maps every element $x \in A$ with an element of $B$ is called a ring homomorphism from $A$ to $B$ if the following conditions hold for every $x, y \in A$

$(i)$ $f(x + y) = f(x) + f(y)$,
$(ii)$ $f(xy) = f(x)f(y)$,
$(iii)$ $f(1) = 1$.

The set of the homomorphisms from $A$ to $B$ is denoted by $\text{Hom}(A, B)$. Let $f \in \text{Hom}(A, B)$. As for vector space homomorphisms, we define the kernel of $f$ as

$$\text{Ker}(f) = \{x \in A \mid f(x) = 0\}$$

and the image of $f$ as

$$\text{Im}(f) = \{y \in B \mid (\exists x \in A) \ f(x) = y\}.$$

Finally, we say that $f$ is a ring isomorphism if $f$ is bijective. We denote by $\text{Isom}(A, B)$ the set of the isomorphisms from $A$ to $B$. 
Proposition

Let $f \in \text{Hom}(A, B)$. Then we have $f(0) = 0$ and for every $x \in A$ we have $f(-x) = -f(x)$.

Proposition

For every $f \in \text{Hom}(A, B)$, the set $\text{Ker}(f)$ is an ideal of $A$ and the set $\text{Im}(f)$ is a subring of $B$.

Proposition

Let $A$ be a commutative ring with identity element. Then, there is a unique ring homomorphism from $\mathbb{Z}$ to $A$. 
Theorem
Let \( \mathbb{A} \) be a commutative ring with identity element and let \( \mathcal{I} \) be an ideal of \( \mathbb{A} \). For every \( x, y \in \mathbb{A} \) we define

\[
x \equiv y \mod \mathcal{I} \iff x - y \in \mathcal{I}
\]

The binary relation \((x, y) \mapsto x \equiv y \mod \mathcal{I}\) is an equivalence relation. The set of its residue classes is denoted by \( \mathbb{A} / \mathcal{I} \) and called the residue class ring of \( \mathbb{A} \) by \( \mathcal{I} \). The residue class of an element \( x \in \mathbb{A} \) is also called its coset and is denoted \( \overline{x} \) or \( x + \mathcal{I} \).

Moreover, \( \mathbb{A} / \mathcal{I} \) is a commutative ring with identity element such that the application that maps any element \( x \in \mathbb{A} \) with its residue class is a ring homomorphism, called the canonical homomorphism from \( \mathbb{A} \) to \( \mathbb{A} / \mathcal{I} \). In particular, for every \( x, y \in \mathbb{A} \) we have

\[
\overline{x + y} = \overline{x} + \overline{y} \quad \text{and} \quad \overline{xy} = \overline{xy}.
\]
Definition
Let \( \mathcal{I}, \mathcal{J} \) be two ideals of \( \mathbb{A} \) and let \( X \) be a non-empty subset of \( \mathbb{A} \).

- The *sum* of \( \mathcal{I} \) and \( \mathcal{J} \) is denoted by \( \mathcal{I} + \mathcal{J} \) and defined by
  \[
  \mathcal{I} + \mathcal{J} = \{ a + b \mid (a, b) \in \mathcal{I} \times \mathcal{J} \}.
  \]

- The *product* \( \mathcal{I} \) and \( \mathcal{J} \) is denoted by \( \mathcal{IJ} \) and defined by
  \[
  \mathcal{IJ} = \{ ab \mid (a, b) \in \mathcal{I} \times \mathcal{J} \}.
  \]

- The *quotient* of \( \mathcal{I} \) by \( X \) is denoted by \( \mathcal{I} : X \) and defined by
  \[
  \mathcal{I} : X = \{ a \in \mathbb{A} \mid (\forall x \in X) \ ax \in \mathcal{I} \}.
  \]
Proposition

Let $\mathcal{I}, \mathcal{J}, \mathcal{K}$ be three ideals of $\mathbb{A}$ and let $X$ be a non-empty subset of $\mathbb{A}$. Then, the following properties hold.

(1) $\mathcal{I} \cap \mathcal{J}$ and $\mathcal{IJ}$ are ideals of $\mathbb{A}$.

(2) If $\mathcal{I} + \mathcal{J}$ is not $\mathbb{A}$, then it is an ideal of $\mathbb{A}$.

(3) If $\mathcal{I} : X$ is not $\mathbb{A}$, then it is an ideal of $\mathbb{A}$.

(4) We have $\mathcal{IJ} \subseteq \mathcal{I} \cap \mathcal{J}$.

(5) We have $\mathcal{J}(\mathcal{I} : \mathcal{J}) \subseteq \mathcal{I} \subseteq \mathcal{I} : \mathcal{J}$.

(6) We have $\mathcal{I} : (\mathcal{J} + \mathcal{K}) = \mathcal{I} : \mathcal{J} + \mathcal{I} : \mathcal{K}$.

(7) We have $(\mathcal{I} : \mathcal{J}) : \mathcal{K} = \mathcal{I} : (\mathcal{JK}) = (\mathcal{I} : \mathcal{K}) : \mathcal{J}$.

(8) We have $(\mathcal{I} \cap \mathcal{J}) : \mathcal{K} = (\mathcal{I} : \mathcal{K}) \cap (\mathcal{J} : \mathcal{K})$.
Example

Let $q, n, m \geq 2$ be three integers. As usual, we denote by $\langle n \rangle$ and $\langle m \rangle$ the ideals generated in $\mathbb{Z}$ by $n$ and $m$ respectively. Then one can easily check the following relations:

- $\langle n \rangle \langle m \rangle = \langle nm \rangle$,
- $\langle n \rangle + \langle m \rangle = \langle \gcd(n, m) \rangle$,
- $\langle n \rangle \cap \langle m \rangle = (\operatorname{lcm}(n, m) \mathbb{Z})$,
- $\langle n \rangle : \{q\} = \{p \in \langle n \rangle \mid pq \in \langle n \rangle\}$.

where $\gcd(n, m)$ and $\operatorname{lcm}(n, m)$ denote respectively the greatest common divisor and the least common multiple of $n$ and $m$. 
Plan

Rings

Ideals

Maximal, Prime, Radical and Primary Ideals

Irreducible Ideals, Primary Decompositions

Saturated Ideals

Rings of Fractions

Relatively Prime Ideals

Products of Rings
Maximal ideals

Throughout this section, we consider a commutative ring \( \mathbb{A} \) with identity element. We denote by \( \text{Ideal}(\mathbb{A}) \) the set of the ideals of \( \mathbb{A} \). The set inclusion \( \subseteq \) is a partial order for \( \text{Ideal}(\mathbb{A}) \).

**Definition**

An ideal \( \mathcal{I} \) of \( \mathbb{A} \) is *maximal* if it is a maximal element of the partially ordered set \( (\text{Ideal}(\mathbb{A}), \subseteq) \), that is if for every ideal \( \mathcal{J} \) of \( \mathbb{A} \) we have \( I \subseteq J \Rightarrow I = J \).

An *ascending chain of ideals* of \( \mathbb{A} \) is an ascending chain of the partially ordered set \( (\text{Ideal}(\mathbb{A}), \subseteq) \), that is an infinite sequence \( \mathcal{I}_1, \mathcal{I}_2, \ldots \) of ideals of \( \mathbb{A} \) such that for every \( i \in \mathbb{N} \) we have \( \mathcal{I}_i \subseteq \mathcal{I}_{i+1} \).

Such an ascending chain of ideals of \( \mathbb{A} \) is ultimately constant if there exists a positive integer \( N \) such that \( \mathcal{I}_i = \mathcal{I}_N \) for all \( i \geq N \).

**Theorem**

The ring \( \mathbb{A} \) admits at least one maximal ideal. Moreover, every ideal of \( \mathbb{A} \) is contained in a maximal ideal of \( \mathbb{A} \).
**Noetherian rings**

**Definition**
A commutative ring with identity element is Noetherian if every ideal of $\mathbb{A}$ is generated by finitely many elements of $\mathbb{A}$.

**Proposition**
The following conditions are equivalent:

(i) every ideal of $\mathbb{A}$ is generated by finitely many elements of $\mathbb{A}$,

(ii) every ascending chain of ideals of $\mathbb{A}$ is ultimately constant.

**Proposition**
Let $\mathbb{A}$ be a Noetherian ring and let $\mathcal{I}$ be an ideal of $\mathbb{A}$. Then the residue class ring $\mathbb{A}/\mathcal{I}$ is Noetherian too.
Prime ideals

**Definition**
An ideal $\mathcal{I}$ of $\mathbb{A}$ is *prime* if for every $a, b \in \mathbb{A}$ we have

$$ab \in \mathcal{I} \Rightarrow (a \in \mathcal{I} \text{ or } b \in \mathcal{I}).$$

(8)

**Proposition**
An ideal $\mathcal{I}$ of $\mathbb{A}$ is prime if and only if the residue class ring $\mathbb{A}/\mathcal{I}$ is an integral domain, that is, $\mathbb{A}/\mathcal{I}$ has no zero-divisors.

**Proposition**
An ideal $\mathcal{I}$ of $\mathbb{A}$ is maximal if and only if the residue class ring $\mathbb{A}/\mathcal{I}$ is a field.

**Lemma**
Let $\mathcal{I}_1, \ldots, \mathcal{I}_n, \mathcal{P}$ be ideals of $\mathbb{A}$ such that $\mathcal{P}$ is prime. If $\mathcal{P}$ contains the intersection of the ideals $\mathcal{I}_1, \ldots, \mathcal{I}_n$, then it contains one of them.
Example

Consider $\mathbb{A} = \mathbb{Z}/q\mathbb{Z}$ where $q$ is a power $p^n$ of a prime $p \in \mathbb{Z}$ with $n \geq 3$. The ideal generated by $p^i$ in $\mathbb{A}$ for each $i = 2, \ldots, n - 1$, is not a prime ideal. Indeed, $p$ remains a zero-divisor modulo each of $p^2, \ldots, p^{n-1}$. However, the ideal generated by $p$ in $\mathbb{A}$ is prime and maximal. Consider now $\mathbb{A} = \mathbb{Z}/q\mathbb{Z}$ where $q$ is a product of prime numbers $p_1, \ldots, p_n$ pairwise different with $n \geq 2$. The ideals generated in $\mathbb{A}$ by each of these prime numbers is a prime ideal if and only if $n = 2$. For instance, with $n = 3$, the element $p_2$ remains a zero-divisor modulo $p_1$, since $p_2p_3\cdots p_n = 0$ holds in $\mathbb{A}/p_1\mathbb{A}$. Exercise!

Example

Consider a field $k$ and the ring $\mathbb{A} = k[x, y]$ of bivariate polynomials over $k$. The ideal generated by $P = \{x\}$ in $\mathbb{A}$ is prime but not maximal (indeed, $\mathbb{A}/P = k[y]$ is not a field) whereas the ideal generated by $M = \{x, y\}$ in $\mathbb{A}$ is maximal (indeed, $\mathbb{A}/M = k$).
Proposition
Let $\mathcal{I}$ be an ideal of $\mathbb{A}$.
- The prime ideals of $\mathbb{A}/\mathcal{I}$ are the images modulo $\mathcal{I}$ of the prime ideals $\mathcal{P}$ of $\mathbb{A}$ such that $\mathcal{I} \subseteq \mathcal{P}$
- The maximal ideals of $\mathbb{A}/\mathcal{I}$ are the images modulo $\mathcal{I}$ of the maximal ideals $\mathcal{M}$ of $\mathbb{A}$ such that $\mathcal{I} \subseteq \mathcal{M}$

Proposition
An element $a \in \mathbb{A}$ is a unit of $\mathbb{A}$ if and only if it does not belong to any maximal ideal of $\mathbb{A}$. 
Radical ideals

Definition
The radical of an ideal $\mathcal{I}$ of $\mathbb{A}$ is denoted by $\sqrt{\mathcal{I}}$ and defined by

$$\sqrt{\mathcal{I}} = \{a \in \mathbb{A} \mid (\exists n \in \mathbb{N}) \ a^n \in \mathcal{I}\}$$

The ideal $\mathcal{I}$ of $\mathbb{A}$ is said radical if $\sqrt{\mathcal{I}} = \mathcal{I}$ holds.

Proposition
The radical of any ideal $\mathcal{I}$ of $\mathbb{A}$ is an ideal that contains $\mathcal{I}$.

Proposition
Let $\mathcal{I}$ and $\mathcal{J}$ be two ideals of $\mathbb{A}$. Then we have $\sqrt{\mathcal{I} \cap \mathcal{J}} = \sqrt{\mathcal{I}} \cap \sqrt{\mathcal{J}}$.

Proposition
The ideal $\mathcal{I}$ of $\mathbb{A}$ is radical if and only $\text{Nil}(\mathbb{A}/\mathcal{I})$ is the trivial ideal, that is, if only and if the only nilpotent element of the residue class ring $\mathbb{A}/\mathcal{I}$ is zero.
Primary ideals

**Definition**
An ideal \( \mathcal{I} \) of \( \mathbb{A} \) is *primary* if for every \( a, b \in \mathbb{A} \) we have

\[
ab \in \mathcal{I} \Rightarrow (a \in \mathcal{I} \text{ or } b \in \sqrt{\mathcal{I}}).
\]  

(9)

In particular, every prime ideal of \( \mathbb{A} \) is primary.

**Remark**
It is easy to check that the above definition can be reformulated as follows: An ideal \( \mathcal{I} \) of \( \mathbb{A} \) is primary if for every \( a, b \in \mathbb{A} \) we have

\[
(ab \in \mathcal{I} \text{ and } a, b \notin \mathcal{I}) \Rightarrow (a \in \sqrt{\mathcal{I}} \text{ and } b \in \sqrt{\mathcal{I}}).
\]  

(10)

**Proposition**
An ideal \( \mathcal{I} \) of \( \mathbb{A} \) is primary if and only if all the zero-divisors of the residue class ring \( \mathbb{A}/\mathcal{I} \) are nilpotent.

**Proposition**
Let \( \mathcal{I} \) be an ideal of \( \mathbb{A} \). If \( \mathcal{I} \) is primary then \( \sqrt{\mathcal{I}} \) is prime.
Example

In $\mathbb{A} = \mathbb{Z}[x]$, the ideal $\mathcal{I} = \langle x^2, 2x \rangle$ is not primary whereas the ideal $\mathcal{J} = \langle x^2, 2 \rangle$ is primary. Indeed, 2 is a non-nilpotent zero-divisor in $\mathbb{A}/\mathcal{I}$ whereas the zero-divisors of $\mathbb{A}/\mathcal{J}$ are all non-zero multiple of $x$, which is nilpotent.

Example

Let $\mathbb{K}$ be a field and consider the ring $\mathbb{A} = \mathbb{K}[x, y]$ of polynomials with coefficients in $\mathbb{K}$ and variables $x, y$. We consider the intersection $\mathcal{I}$ of the ideals $\mathcal{I}_1 = \langle x \rangle$ and $\mathcal{I}_2 = \langle x^2, y^2 \rangle$. Clearly, the ideal $\mathcal{I}_1$ is prime and, thus $\sqrt{\mathcal{I}_1} = \mathcal{I}_1$ holds. The ideal $\mathcal{I}_2$ is primary and $\sqrt{\mathcal{I}_2} = \langle x, y \rangle$ holds. Thus, we have $\sqrt{\mathcal{I}} = \langle x \rangle$ and thus $\sqrt{\mathcal{I}}$ is a prime ideal. However $\mathcal{I}$ is not a primary ideal. To see this we define $a = xy$ and $b = y$. Clearly $ab$ belongs $\mathcal{I}$. Moreover $a \notin \langle x^2, y^2 \rangle$ and thus $a \notin \mathcal{I}$. Finally $b \notin \sqrt{\mathcal{I}}$, which shows that $\mathcal{I}$ is not primary.
Plan

Rings

Ideals

Maximal, Prime, Radical and Primary Ideals

Irreducible Ideals, Primary Decompositions

Saturated Ideals

Rings of Fractions

Relatively Prime Ideals

Products of Rings
Irreducible ideals

Definition
An ideal \( \mathcal{I} \) of \( \mathbb{A} \) is called *irreducible* if for all ideals \( \mathcal{I}_1, \mathcal{I}_2 \) of \( \mathbb{A} \) we have

\[
\mathcal{I} = \mathcal{I}_1 \cap \mathcal{I}_2 \Rightarrow (\mathcal{I} = \mathcal{I}_1 \text{ or } \mathcal{I} = \mathcal{I}_2).
\]

Proposition
*Every prime ideal of \( \mathbb{A} \) is irreducible.*

Remark
The converse of the above proposition is false. Consider \( \mathbb{A} = \mathbb{K}[x] \) where \( \mathbb{K} \) is a field and its ideal \( \mathcal{I} = \langle x^2 \rangle \). This ideal is not a prime bit it is irreducible. Exercise!
Lemma
Let $\mathcal{A}$ be Noetherian. Every irreducible ideal of $\mathcal{A}$ is primary.

Remark
The converse is false. Indeed, consider $\mathcal{A} = \mathbb{K}[x, y]$ where $\mathbb{K}$ is a field and its ideals $\mathcal{I}_1 = \langle x^2, y \rangle$, $\mathcal{I}_2 = \langle x, y^2 \rangle$ and $\mathcal{I} = \mathcal{I}_1 \cap \mathcal{I}_2 = \langle x^2, xy, y^2 \rangle$. One can prove that these three ideals are primary, and that they have same radical, namely $\langle x, y \rangle$. Therefore, the ideal $\mathcal{I}$ is primary but not irreducible.

```plaintext
with(PolynomialIdeals):
> J := <x^2, y>; K := <y^2, x>;
                      2
J := <y, x >
                      2
K := <x, y >

> IsPrimary(J); IsPrimary(K);
                      true
                      true

> L := Intersect(J, K);
                      2  2
L := <x , y , x y>

> IsPrimary(L);
                      true
```
Primary decomposition

**Definition**

Let $Q_1, \ldots, Q_s$ be (finitely many) primary ideals of $A$ and let $I$ be another ideal of $A$. The set $\{Q_1, \ldots, Q_s\}$ is called a *primary decomposition* of $I$ if we have

$$I = Q_1 \cap \cdots \cap Q_s.$$ 

If this equality holds and if all the ideals $Q_1, \ldots, Q_s$ are prime, then the set $\{Q_1, \ldots, Q_s\}$ is called a *prime decomposition* of $I$.

**Theorem**

*Let $A$ be Noetherian. Every ideal of $A$ admits a primary decomposition.*
Remark
The question of unicity is much more complicated and will be discussed later. Without any additional constraint, an ideal in a Noetherian ring may admit several primary decompositions. Indeed, consider \( \mathbb{A} = \mathbb{K}[x, y] \) where \( \mathbb{K} \) is a field and its ideals \( \mathcal{P} = \langle x \rangle, \mathcal{Q}_2 = \langle x^2, xy, y^2 \rangle, \mathcal{Q}_3 = \langle x^2, y \rangle \) and \( \mathcal{I} = \langle x^2, xy \rangle \). One can easily prove that \( \mathcal{Q}_2 \) and \( \mathcal{Q}_3 \) are primary, both with the same radical, namely \( \mathcal{M} = \langle x, y \rangle \). One can show the equalities

\[
\mathcal{I} = \mathcal{P} \cap \mathcal{Q}_2 = \mathcal{P} \cap \mathcal{Q}_3.
\]

Since \( \mathcal{Q}_2 \neq \mathcal{Q}_3 \), it follows that the ideal \( \mathcal{I} \) has at least two different primary decompositions.

\[
\begin{align*}
\text{Q2} & := \langle x^2, x*y, y^2 \rangle; \quad \text{Q3} := \langle x^2, y \rangle; \quad \text{P} := \langle x+y \rangle; \\
& \quad 2 \quad 2 \\
\text{Q2} := \langle x, y, x y \rangle \\
& \quad 2 \\
\text{Q3} := \langle y, x \rangle \\
\text{P} := \langle y + x \rangle \\
\text{IsPrimary(Q1); IsPrimary(Q2); IsPrimary(P)}; & \quad \text{true} \\
& \quad \text{true} \\
& \quad \text{true} \\
\text{J2 := Intersect(Q2, P); J3 := Intersect(Q3, P)}; & \quad \text{true} \\
& \quad 2 \quad 2 \quad 2 \\
\text{J2} := \langle -x + y, x + x y \rangle \\
& \quad 2 \quad 2 \quad 2 \\
\text{J3} := \langle -x + y, x + x y \rangle \\
\text{IdealContainment(J2, J3, J2)}; & \quad \text{true}
\end{align*}
\]
Remark

> J := \langle x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1 \rangle;

    2  2  2
> J := \langle z + x + y - 1, y + x + z - 1, x + y + z - 1 \rangle

> dec := PrimaryDecomposition(J);

    2  2  2
dec := \langle y, x, z + x + y - 1, y + x + z - 1, x + y + z - 1 \rangle,

    2  2  2
\langle x, y - 1, z + x + y - 1, y + x + z - 1, x + y + z - 1 \rangle,

    2  2  2
\langle (x - 1), z + x + y - 1, y + x + z - 1, x + y + z - 1 \rangle,

    2  2  2
\langle x + 2 x - 1, z + x + y - 1, y + x + z - 1, x + y + z - 1 \rangle

> map(Groebner:-Basis, [dec], plex(x,y,z));

    2  2
[[-1 + z, y, x], [z, y - 1, x], [z, y - z, -1 + x + z], [z + 2 z - 1,
Remark

> raddec := PrimeDecomposition(J);

\[ \text{raddec} := \langle x - 1, z + x + y - 1, y + x + z - 1, x + y + z - 1 \rangle, \]

\[ \langle x + 2 x - 1, z + x + y - 1, y + x + z - 1, x + y + z - 1 \rangle, \]

\[ \langle x, y, z + x + y - 1, y + x + z - 1, x + y + z - 1 \rangle, \]

\[ \langle x, y - 1, z + x + y - 1, y + x + z - 1, x + y + z - 1 \rangle \]

> map(Groebner:-Basis, [raddec], plex(x,y,z));

\[ \text{[[[} z, y, x - 1 \text{]}, \text{[[} z + 2 z - 1, y - z, x - z \text{]}}, \text{[[-} 1 + z, y, x\text{]}, \text{[} z, y} \]
Plan

Rings

Ideals

Maximal, Prime, Radical and Primary Ideals

Irreducible Ideals, Primary Decompositions

Saturated Ideals

Rings of Fractions

Relatively Prime Ideals

Products of Rings
**Definition**
A subset $S$ of $A$ is *multiplicatively closed* if the following conditions hold: $1 \in S$, $0 \notin S$, and for every $s, s' \in S$ the product $ss'$ belongs to $S$.

**Definition**
Let $\mathcal{I}$ be an ideal of $A$ and let $S$ be a multiplicatively closed subset of $A$. The *saturated ideal* of $\mathcal{I}$ w.r.t. $S$ is denoted by $S^{-1}\mathcal{I}$ and defined by

$$ S^{-1}\mathcal{I} = \{a \in A \mid (\exists s \in S) \; sa \in \mathcal{I}\}. $$

Let $h \in A$ be a non-nilpotent element. The *saturated ideal* of $\mathcal{I}$ w.r.t. $h$ is denoted by $\mathcal{I} : h^{\infty}$ and defined by

$$ \mathcal{I} : h^{\infty} = \{a \in A \mid (\exists n \in \mathbb{N}) \; h^n a \in \mathcal{I}\}. $$

**Remark**
The notation $S^{-1}\mathcal{I}$ will make sense in the next section. Now, let us define $S_h = \{h^n \mid n \in \mathbb{N}\}$ for $h \notin \text{Nil}(A)$. It is easy to check that $S_h$ is multiplicatively closed set. Remember that $h^0 = 1$ holds.
Remark

> J := \langle x*y \rangle; Saturate(J, x);

\[ J := \langle x \quad y \rangle \]

> J := \langle x^2, x*y, y^2 \rangle; Saturate(J, x);

\[ J := \langle x^2, y^2, x*y \rangle \]

> J := \langle x^2, x*y, y^2 \rangle; Saturate(J, x-y);

\[ J := \langle x^2, y^2, x*y \rangle \]
Proposition

Let $\mathcal{I}, \mathcal{J}$ be two ideals of $A$ and let $S$ be a multiplicatively closed subset of $A$. Then the following properties hold:

1. The set $S^{-1}\mathcal{I}$ is an ideal of $A$ that contains $\mathcal{I}$, or the ring $A$,
2. $S^{-1}(\mathcal{I} \cap \mathcal{J}) = (S^{-1}\mathcal{I}) \cap (S^{-1}\mathcal{J})$,
3. $S \cap \sqrt{\mathcal{I}} \neq \emptyset \Rightarrow S^{-1}\mathcal{I} = A$,
4. $\mathcal{I} \subseteq \mathcal{J} \Rightarrow S^{-1}\mathcal{I} \subseteq S^{-1}\mathcal{J}$,
5. $S^{-1}\mathcal{I} + S^{-1}\mathcal{J} \subseteq S^{-1}(\mathcal{I} + \mathcal{J})$. 
Theorem
Let \( \mathcal{I}, Q_1, \ldots, Q_s, P_1, \ldots, P_s \) be ideals of \( A \), let \( S \) be a multiplicatively closed subset of \( A \) and let \( t \) be an integer such that the following conditions hold:

(i) for all \( 1 \leq i \leq s \) the ideal \( P_i \) is prime
(ii) for all \( 1 \leq i \leq s \) the ideal \( Q_i \) is primary and its radical is \( P_i \)
(iii) The \( \{ Q_1, \ldots, Q_s \} \) is a primary decomposition of \( \mathcal{I} \).
(iv) for all \( i \in \{ 1, \ldots, s \} \) we have \( P_i \cap S = \emptyset \iff i \leq t \).

Then the set \( \{ Q_1, \ldots, Q_t \} \) is a primary decomposition of \( S^{-1}\mathcal{I} \). In addition, we have
\[
\sqrt{S^{-1}\mathcal{I}} = S^{-1}\sqrt{\mathcal{I}}. \tag{11}
\]

Remark
With the notations and hypothesis of Theorem 24, if \( t < 1 \) the set \( \{ Q_1, \ldots, Q_t \} \) is empty which implies that \( S^{-1}\mathcal{I} \) is \( A \). The above theorem is very useful to understand what saturated ideals are. In broad words, it tells us that saturation by \( S \) removes the primary ideals \( Q \) such that \( \sqrt{Q} \cap S \neq \emptyset \).
Example

In the ring $\mathbb{A} = \mathbb{Q}[x, y, z]$ of polynomials with variables $x, y, z$, and coefficients in $\mathbb{Q}$ consider the primary ideals

$$Q_1 = \langle x^2, y, z \rangle, \quad Q_2 = \langle x + 1, y^2, z + 1 \rangle \quad \text{and} \quad Q_3 = \langle (x + 1)^2, y + 1, z \rangle$$

with respective radicals

$$P_1 = \langle x, y, z \rangle, \quad P_2 = \langle x + 1, y, z + 1 \rangle \quad \text{and} \quad P_3 = \langle x + 1, y + 1, z \rangle.$$

We define

$$I = Q_1 \cap Q_2 \cap Q_3 = \langle x^2 - 2x y + y z - y + z, x z + z, y^2 + y z + y, z^2 + z \rangle$$

Then we have

$$I : (x + 1)^\infty = Q_1, \quad I : z^\infty = Q_2 \quad \text{and} \quad I : y^\infty = Q_3.$$ 

All the computations of this example can be performed using well-known algorithms, available in Maple.
Proposition

Let \( \mathcal{I} \) be an ideal of \( A \) and let \( h, h_1, h_2 \in A \) be non-nilpotent elements. Then the following properties hold

1. \( \mathcal{I} : (h_1 h_2) = (\mathcal{I} : h_1) : h_2 \),
2. \( \mathcal{I} = \sqrt{\mathcal{I}} \Rightarrow \mathcal{I} : h = \mathcal{I} : h \),
3. \( \sqrt{\mathcal{I}} : h = \sqrt{\mathcal{I}} : h \),
4. \( \sqrt{\mathcal{I}} : h = \sqrt{\mathcal{I}} : h^N \).

Proposition

Let \( A \) be Noetherian. Let \( \mathcal{I} \) be an ideal of \( A \) and let \( h \) be non-nilpotent element. Then, there exists an integer \( N \) such that \( \mathcal{I} : h^\infty = \mathcal{I} : h^N \).
Plan

Rings

Ideals

Maximal, Prime, Radical and Primary Ideals

Irreducible Ideals, Primary Decompositions

Saturated Ideals

Rings of Fractions

Relatively Prime Ideals

Products of Rings
Definition
Let $S$ be a multiplicatively closed subset of $A$. In the set $A \times S$ we define the following equivalence relation. For every $(a, s), (b, t) \in A \times S$ we write

$$(a, s) \sim (b, t) \iff (\exists r \in S) \ r(at - bs) = 0$$

The residue class of any $(a, s) \in A \times S$ is denoted by $a/s$ or $\frac{a}{s}$ and called the fraction with numerator $a$ and denominator $s$.

The set of the residue classes of $A \times S$ w.r.t. $\sim$ is denoted by $S^{-1}A$ and called the ring of fractions of $A$ at $S$.

Remark
The definition of the relation $\sim$ in $A \times S$ may look surprising. However the other simpler relation

$$(a, s) \sim' (b, t) \iff at = bs$$

would not work. More precisely, this other relation is not transitive in general. This is easily seen when trying to prove that it is transitive. If $S$ does not contain any zero-divisors, then $\sim$ can be replaced by $\sim'$.
Proposition

Let \( S \) be a multiplicatively closed subset of \( \mathbb{A} \). The set \( S^{-1}\mathbb{A} \) endowed with the following addition

\[
\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'}
\]

and multiplication

\[
\frac{a}{s} \cdot \frac{a'}{s'} = \frac{a a'}{s s'}
\]

is a commutative ring with identity element. The map

\[
\text{loc}_S : \begin{cases} \mathbb{A} & \mapsto S^{-1}\mathbb{A} \\ a & \mapsto \frac{a}{1} \end{cases}
\]

is a ring homomorphism called the localization of \( \mathbb{A} \) at \( S \). Its kernel is given by

\[
\text{KER}(\text{loc}_S) = \{ a \in \mathbb{A} \mid (\exists r \in S) \ ar = 0 \} = \bigcup_{s \in S} \langle 0 \rangle : s.
\]

The ring homomorphism is injective if and only \( S \) does not contain any zero-divisors of \( \mathbb{A} \).
Example

Consider $\mathbb{A} = \mathbb{Z}/6\mathbb{Z}$ and denote its elements by 0, 1, 2, 3, 4, 5. The set $S = \{1, 2, 4\}$ is a multiplicatively closed subset of $\mathbb{A}$. We aim to describe $S^{-1}\mathbb{A}$. To do so, given $r \in S$, we need to solve in $\mathbb{A}$ the equation $rx = 0$ with unknown $x$. We have

$$
1x = 0 \quad \Rightarrow \quad x = 0 \\
2x = 0 \quad \Rightarrow \quad x \in \{0, 3\} \\
4x = 0 \quad \Rightarrow \quad x \in \{0, 3\}
$$

Hence

$$(a, s) \sim (b, t) \iff (at - bs) \in \{0, 3\}$$

Therefore, we obtain

$$
\begin{align*}
\frac{0}{1} &= \{(b, t) \mid b \in \{0, 3\}\} \\
\frac{1}{1} &= \{(b, t) \mid b \in \{t, 3 + t\}\} \\
\frac{1}{2} &= \{(b, t) \mid b \in \{2t, 3 + 2t\}\}
\end{align*}
$$

which leads to

$$
\begin{align*}
0 &= 0 = 0 = 3 = 3 = 3 = 3 \\
\frac{1}{2} &= \frac{1}{4} = \frac{1}{4} = \frac{1}{2} = \frac{1}{2} = \frac{1}{2} = \frac{1}{2} \\
\frac{1}{3} &= \frac{1}{4} = \frac{1}{2} = \frac{1}{2} = \frac{1}{2} = \frac{1}{2} = \frac{1}{2} \\
\frac{1}{1} &= \frac{2}{2} = \frac{2}{4} = \frac{2}{4} = \frac{2}{2} = \frac{2}{2} = \frac{2}{2}
\end{align*}
$$

From there, it is easy to see that $S^{-1}\mathbb{A}$ is isomorphic with $\mathbb{Z}/3\mathbb{Z}$. It follows that by allowing the zero-divisors 2 and 4 as denominators we have obtained a field!
Proposition

Let $S$ be a multiplicatively closed subset of $\mathbb{A}$. For every $(a, s) \in \mathbb{A} \times S$ the fraction $\frac{a}{s}$ is a unit of $S^{-1}\mathbb{A}$ if and only if the ideal $\langle a \rangle$ generated by $a$ in $\mathbb{A}$ meets $S$, that is, if $\langle a \rangle \cap S \neq \emptyset$.

Definition

The set $\text{Reg}(\mathbb{A})$ consisting of the regular elements of $\mathbb{A}$ is a multiplicatively closed subset of $\mathbb{A}$. The ring of fractions of $\mathbb{A}$ at $\text{Reg}(\mathbb{A})$ is called the total quotient ring of $\mathbb{A}$ and is denoted by $\text{Fr}(\mathbb{A})$.

Proposition

If $\mathbb{A}$ is an integral domain, then $\text{Fr}(\mathbb{A})$ is a field, called its field of fractions.
Let $S$ be a multiplicatively closed subset of $A$. Let $\phi$ be the localization of $A$ at $S$. For an ideal $I$ of $A$ we denoted by $I^\uparrow$ the extended ideal of $I$ by $\phi$. For an ideal $J$ of $S^{-1}A$, we denote by $J^\downarrow$ the contracted ideal of $J$ by $\phi$. Sometimes, the ideals $I^\uparrow$ and $J^\downarrow$ are also denoted by $IS^{-1}A$ and $J \cap A$ respectively.

**Theorem**

Let $I$ be an ideal of $A$, let $\{Q_1, \ldots, Q_s\}$ be a primary decomposition of $I$ and let $t$ be an integer such that for all $i \in \{1, \ldots, s\}$ we have $Q_i \cap S = \emptyset$ if and only if $i \leq t$. Then, the following properties hold:

1. If $t = 0$ then we have $I^\uparrow = S^{-1}A$ and $S^{-1}I = I^\uparrow = A$,
2. If $t > 0$ then we have $I^\uparrow = Q_1^\uparrow \cap \cdots \cap Q_t^\uparrow$ and $I^\downarrow = Q_1 \cap \cdots \cap Q_t$. 
Plan

Rings

Ideals

Maximal, Prime, Radical and Primary Ideals

Irreducible Ideals, Primary Decompositions

Saturated Ideals

Rings of Fractions

Relatively Prime Ideals

Products of Rings
Definition
Two ideals $\mathcal{I}$ and $\mathcal{J}$ are relatively prime if their sum $\mathcal{I} + \mathcal{J}$ is equal to the whole ring $\mathbb{A}$.

Proposition
Let $\mathcal{I}$ and $\mathcal{J}$ be two ideals of $\mathbb{A}$. The following conditions are equivalent

1. there exists $(a, b) \in \mathcal{I} \times \mathcal{J}$ such that $a + b = 1$,
2. there exists no maximal ideal containing $\mathcal{I} + \mathcal{J}$,
3. $\mathcal{I}$ and $\mathcal{J}$ are relatively prime.
Proposition

Let $\mathcal{I}_1, \ldots, \mathcal{I}_n$ be pairwise relatively prime ideals. Then, for every $i \in \{1, \ldots, n\}$ the ideals $\mathcal{I}_i$ and $\prod_{j \neq i} \mathcal{I}_j$ are relatively prime.

Proposition

Let $\mathcal{I}_1, \ldots, \mathcal{I}_n$ be pairwise relatively prime ideals. Then, their intersection is equal to their product, that is

$$\cap_{i=1}^{i=n} \mathcal{I}_i = \prod_{i=1}^{i=n} \mathcal{I}_i$$
Example

Let \( A = \mathbb{Q}[x] \) and let \( a_1, a_2 \in \mathbb{Q} \) be such that \( a_1 \neq a_2 \). The ideals \( \mathcal{I}_1 = \langle x - a_1 \rangle \) and \( \mathcal{I}_2 = \langle x - a_2 \rangle \) are relatively prime since we have

\[
\frac{1}{a_2 - a_1} (x - a_1) + \frac{-1}{a_2 - a_1} (x - a_2) = 1.
\]

Let us check that their product is equal to their intersection. By definition, the product ideal \( \mathcal{I}_1 \mathcal{I}_2 \) is generated by \( (x - a_1)(x - a_2) \). Now, let \( a \) be in the intersection \( \mathcal{I}_1 \cap \mathcal{I}_2 \). Then, there exists \( b, c \in A \) such that

\[
a = b(x - a_1) = c(x - a_2)
\]

Since \( A \) is a PID, its irreducible elements \( (x - a_1) \) and \( (x - a_2) \) are also prime elements. Hence, the prime \( (x - a_2) \) divides the product \( b(x - a_1) \) and thus \( b \) (since it does not divide \( (x - a_1) \)). Similarly, the prime \( (x - a_1) \) divides \( c \). Therefore, the element \( a \) is a multiple of \( (x - a_1)(x - a_2) \) and we have proved that \( \mathcal{I}_1 \cap \mathcal{I}_2 \subseteq \mathcal{I}_1 \mathcal{I}_2 \) holds.

Example

Let \( A = \mathbb{Q}[x] \) and consider the ideals

\[
\mathcal{I}_1 = \langle x^2 - 1 \rangle \quad \text{and} \quad \mathcal{I}_2 = \langle x^2 - 3x + 2 \rangle.
\]
Plan

Rings

Ideals

Maximal, Prime, Radical and Primary Ideals

Irreducible Ideals, Primary Decompositions

Saturated Ideals

Rings of Fractions

Relatively Prime Ideals

Products of Rings
Definition
Let $\mathbb{A}_1, \ldots, \mathbb{A}_n$ be commutative rings with identity element. The Cartesian product $\mathbb{A} = \mathbb{A}_1 \times \cdots \times \mathbb{A}_n$ endowed with the addition

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$$

and the multiplication

$$(a_1, \ldots, a_n)(b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n)$$

for every $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in \mathbb{A}$, is a commutative ring with identity element called the \textit{direct product} of the rings $\mathbb{A}_1, \ldots, \mathbb{A}_n$. Its elements 0 and 1 are respectively the $n$-uple $(0, \ldots, 0)$ and $(1, \ldots, 1)$. For an element $a = (a_1, \ldots, a_n) \in \mathbb{A}$ and for $i \in \{1, \ldots, n\}$ the element $a_i$ is called the $i$-th component of $a$ and is denoted by $\pi_i(a)$. 
Remark
Even if $A_1, \ldots, A_n, A$ are all fields, the direct product of the rings $A_1, \ldots, A_n$, with $n \geq 2$ is not an integral domain. More precisely, for $n = 2$, we have $(1, 0)(0, 1) = (0, 0)$ showing that $(1, 0)$ is a zero-divisor in $A_1 \times A_2$. 
Proposition

Let $\mathbb{A}_1, \ldots, \mathbb{A}_n, \mathbb{A}$ be commutative rings with identity element such that $\mathbb{A}$ is the direct product of the rings $\mathbb{A}_1, \ldots, \mathbb{A}_n$. Then the following properties hold.

1. The units of $\mathbb{A}$ are the elements of $\mathbb{A}$ of the form $(u_1, \ldots, u_n)$ where $u_i$ is a unit of $\mathbb{A}_i$ for every $i \in \{1, \ldots, n\}$.

2. The ideals of $\mathbb{A}$ are of the form $I_1 \times \cdots \times I_n$ where $I_i$ is an ideal of $\mathbb{A}_i$ or $\mathbb{A}_i$ itself, for every $i \in \{1, \ldots, n\}$ and where $I_i \neq \mathbb{A}_i$ holds for at least one $i$.

3. The prime ideals of $\mathbb{A}$ are of the form

$$\mathbb{A}_1 \times \cdots \times \mathbb{A}_{i-1} \times P_i \times \mathbb{A}_{i+1} \times \cdots \times \mathbb{A}_n$$

where $P_i$ is a prime ideal of $\mathbb{A}_i$ for some $i \in \{1, \ldots, n\}$.

4. The radical ideals of $\mathbb{A}$ are of the form $R_1 \times \cdots \times R_n$ where $R_i$ is a radical ideal of $\mathbb{A}_i$ or $\mathbb{A}_i$ itself, for every $i \in \{1, \ldots, n\}$ and where $R_i \neq \mathbb{A}_i$ holds for at least one $i$.

5. If $\mathbb{A}_1, \ldots, \mathbb{A}_n$ are all Noetherian, then $\mathbb{A}$ is Noetherian.
Proposition

Let $K_1, \ldots, K_n$ be fields and let $A$ be the direct product of $K_1, \ldots, K_n$. Then the following properties hold.

1. The zero-divisors of $A$ are the elements of $A$ which have at least one null and one non-null components.

2. The only nilpotent element of $A$ is zero.

3. Every non-zero element of $A$ is either a unit or a zero-divisor.

4. The total quotient ring of $A$ is $A$ itself.
Theorem
A Noetherian ring is isomorphic with a direct product of fields if and only if every non-zero element is either a unit or a non-nilpotent zero-divisor.

Theorem (Chinese Remaindering Theorem)
Let $A$ be a commutative ring with identity element. Let $I_1, \ldots, I_n$ be ideals of $A$ that are pairwise relatively prime. Then we have the following ring isomorphism

$$A/I_1\cdots I_n \cong \prod_{i=1}^{i=n} A/I_i.$$