Introduction to Commutative Algebra

by Atiyah and Macdonald

slideshow by
William M. Faucette

University of West Georgia

Outline

Definition

A **ring** is a set with two binary operations (addition and multiplication) such that

1. A is an abelian group with respect to addition (so that A has a zero element, denoted by 0, and every $x \in A$ has an (additive) inverse, $-x$).
2. Multiplication is associative and distributive over addition $((xy)z = x(yz))$ and distributive over addition $(x(y+z) = xy + xz$, $(y+z)x = yx + zx)$.

Definition

A ring A is **commutative** if

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

Definition

A ring A has an **identity element** if there exists an element, $1 \in A$, so that

$$1 \cdot x = x \cdot 1 = x \text{ for all } x \in A.$$

The identity element is then unique.

We shall consider only rings which are **commutative** and have an **identity element** (denoted by 1).

Definition

A **ring homomorphism** from a ring A to a ring B is a mapping $f : A \to B$ so that

1. $f(x+y) = f(x) + f(y)$ for all $x, y \in A$
2. $f(xy) = f(x)f(y)$ for all $x, y \in A$
3. $f(1) = 1$.

In other words, f respects addition, multiplication, and the identity element.

If f is a ring homomorphism, then f is a homomorphism of groups under addition, so it follows that $f(x-y) = f(x) - f(y)$, $f(-x) = -f(x)$, and $f(0) = 0$.

Definition

A subset S of a ring A is a **subring** of A if S is closed under addition and multiplication, is closed under taking additive inverses, and contains the identity element of A. The inclusion map $i : S \hookrightarrow A$ is then a ring homomorphism.

If $f : A \to B$ and $g : B \to C$ are ring homomorphisms, then $g \circ f : A \to C$ is a ring homomorphism.

Definition

An **ideal** $\mathfrak{a}$ of a ring A is a subset of A which is an additive subgroup and is such that $A\mathfrak{a} \subseteq \mathfrak{a}$ (i.e, $x \in A$ and $y \in \mathfrak{a}$ imply $xy \in \mathfrak{a}$).

Definition

Let $\mathfrak{a}$ be an ideal in a ring A. The set of cosets, $A/\mathfrak{a}$ has a natural ring structure inherited from that of A.

The resulting ring is called the **quotient ring** of A by $\mathfrak{a}$.

In this case, the natural map $\phi : A \to A/\mathfrak{a}$ defined by $\phi(x) = x + \mathfrak{a}$ is a surjective ring homomorphism.

We shall frequently use the following fact:

Proposition

There is a one-to-one order preserving correspondence between the ideals $\mathfrak{b}$ of A which contain $\mathfrak{a}$, and the ideals $\overline{\mathfrak{b}}$ of $A/\mathfrak{a}$, given by $\mathfrak{b} = \phi^{-1}(\overline{\mathfrak{b}})$.

Definition

If $f : A \to B$ is a ring homomorphism, the **kernel** of f, defined to be $f^{-1}(0)$, is an ideal $\mathfrak{a}$ of A, and the **image** of f, defined to be $f(A)$, is a subring C of B. The homomorphism f induces an isomorphism $A/\mathfrak{a} \cong C$.

We shall sometimes use the notation $x \equiv y \pmod{\mathfrak{a}}$. This means that $x - y \in \mathfrak{a}$.

Definition

A **zero-divisor** in a ring A is an element x for which there exists $y \neq 0$ in A such that $xy = 0$. A ring with no nonzero zero-divisors (and in which $0 \neq 1$) is called an **integral domain**.

For example, $\mathbb{Z}$ and $k[x_1, \ldots, x_n]$ (k a field, x_i indeterminates) are integral domains.

Definition

An element $x \in A$ is **nilpotent** if $x^n = 0$ for some $n > 0$.

A nilpotent element is a zero-divisor (unless $A = 0$), but not conversely (in general).

Definition

A **unit** in A is an element x such that $xy = 1$ for some $y \in A$.

The element y is then uniquely determined and is denoted x^{-1}.

The set of units in A form a (multiplicative) abelian group.

Definition

The multiples ax of an element $x \in A$ form a **principal** ideal, denoted by (x) or Ax.

The element x is a unit if and only if $(x) = A$.

The zero ideal (0) is usually denoted by 0.

Definition

A **field** is a ring A in which $1 \neq 0$ and every non-zero element is a unit.

Every field is an integral domain (but not conversely: $\mathbb{Z}$ is not a field).

Proposition

Let A be a ring $\neq 0$. Then the following are equivalent:

1. A is a field;
2. the only ideals in A are 0 and (1);
3. every homomorphism of A into a non-zero ring B is injective.

Definition

An ideal $\mathfrak{p}$ in A is **prime** if $\mathfrak{p} \neq (1)$ and if

$$xy \in \mathfrak{p} \implies x \in \mathfrak{p} \text{ or } y \in \mathfrak{p}.$$

Definition

An ideal $\mathfrak{m}$ is **maximal** if $\mathfrak{m} \neq (1)$ and if there is no ideal $\mathfrak{a}$ so that $\mathfrak{m} \subsetneq \mathfrak{a} \subsetneq (1)$.

Equivalently:

1. $\mathfrak{p}$ is prime $\Leftrightarrow A/\mathfrak{p}$ is an integral domain;
2. $\mathfrak{m}$ is maximal $\Leftrightarrow A/\mathfrak{m}$ is a a field.

Hence a maximal ideal is prime (but not conversely, in general). The zero ideal is prime $\Leftrightarrow A$ is an integral domain.

If $f : A \to B$ is a ring homomorphism and $\mathfrak{q}$ is a prime ideal in B, then $f^{-1}(\mathfrak{q})$ is a prime ideal in A, for $A/f^{-1}(\mathfrak{q})$ is isomorphic to a subring of $B/\mathfrak{q}$ and hence has no zero-divisor $\neq 0$.

But if $\mathfrak{n}$ is a maximal ideal of B it is not necessarily ture that $f^{-1}(\mathfrak{n})$ is maximal in A; all we can say for sure is that it is prime. (Example: $A = \mathbb{Z}$, $B = \mathbb{Q}$, $\mathfrak{n} = 0$.)

Prime ideals are fundamental to the whole of commutative algebra. The following theorem and its corollaries ensure that there is always a sufficient supply of them.

Theorem

Every ring $A \neq 0$ has at least one maximal ideal.

Proof.

Let Σ be the set of all proper ideals in A. Order Σ by inclusion. Σ is not empty, since $0 \in \Sigma$. Let $(\mathfrak{a}_\alpha)$ be a chain of ideals in Σ, so that for each pair of indices α, β we have either $\mathfrak{a}_\alpha \subset \mathfrak{a}_\beta$ or $\mathfrak{a}_\beta \subset \mathfrak{a}_\alpha$. Let $\mathfrak{a} = \bigcup_\alpha \mathfrak{a}_\alpha$. Then α is an ideal (verify this) and $1 \notin \mathfrak{a}$ since $1 \notin \mathfrak{a}_\alpha$ for all α. Hence $\alpha \in \Sigma$, and $\mathfrak{a}$ is an upper bound of the chain. Hence, by Zorn's lemma, Σ has a maximal element. $\square$

Theorem

Every ring $A \neq 0$ *has at least one maximal ideal.*

Corollary

If $\mathfrak{a} \neq (1)$ is an ideal of A, there exists a maximal ideal of A containing $\mathfrak{a}$.

Corollary

Every non-unit of A is contained in a maximal ideal.

Definition

A ring A with exactly one maximal ideal $\mathfrak{m}$ is called a **local ring**. In a local ring, the maximal ideal consists of all nonunits in A.

The field $k = A/\mathfrak{m}$ is called the **residue field** of A.

Proposition

1. Let A be a ring and $\mathfrak{m} \neq (1)$ an ideal of A such that every $x \in A - \mathfrak{m}$ is a unit in A. Then A is a local ring and $\mathfrak{m}$ its maximal ideal.
2. Let A be a ring and $\mathfrak{m}$ a maximal ideal of A, such that every element of $1 + \mathfrak{m}$ (i.e. every $1 + x$, where $x \in \mathfrak{m}$) is a unit in A. Then A is a local ring.

Examples

1. Let $A = k[x_1, \ldots, x_n]$, k a field. Let $f \in A$ be an irreducible polynomial. By unique factorization, the ideal (f) is prime.
2. Let $A = \mathbb{Z}$. Every ideal in $\mathbb{Z}$ is of the form (m) for some $m \geq 0$. The ideal (m) is prime $\Leftrightarrow m = 0$ or a prime number. All the ideals (p), where p is a prime number, are maximal: $\mathbb{Z}/(p)$ is the field of p elements.

   The same holds in Example (1) for $n = 1$, but not for $n > 1$.
3. A **principal ideal domain** is an integral domain in which every ideal is principal. In such a ring every non-zero prime ideal is maximal.

Proposition.

The set $\mathfrak{N}$ of all nilpotent elements in a ring A is an ideal, and $A/\mathfrak{N}$ has no nilpotent element $\neq 0$.

Proof.

If $x \in \mathfrak{N}$, clearly $ax \in \mathfrak{N}$ for all $a \in A$. Let x, $y \in \mathfrak{N}$: say $x^m = 0$, $y^n = 0$. By the binomial theorem (which is valid in any commutative ring), $(x+y)^{m+n-1}$ is the sum of integer multiples of products $x^r y^s$, where $r + s = m + n - 1$; we cannot have both $r < m$ and $s < n$, hence each of these products vanishes and therefore $(x+y)^{m+n-1} = 0$. Hence $x + y \in \mathfrak{N}$ and therefore $\mathfrak{N}$ is an ideal.

Let $\overline{x} \in A/\mathfrak{N}$ be represented by $x \in A$. Then $\overline{x}^n$ is represented by x^n, so that $\overline{x}^n = 0 \Rightarrow x^n \in \mathfrak{N} \Rightarrow (x^n)^k = 0$ for some $k > 0 \Rightarrow x \in \mathfrak{N} \Rightarrow \overline{x} = 0$. □

Definition

The set $\mathfrak{N}$ of all nilpotent elements in a ring A is called the **nilradical** of A.

The following proposition gives an alternative definition of $\mathfrak{N}$:

Proposition

The nilradical of A is the intersection of all the prime ideals of A.

Proof

Let $\mathfrak{N}'$ denote the intersection of all the prime ideals of A. If $f \in A$ is nilpotent and if $\mathfrak{p}$ is a prime ideal, then $f^n = 0 \in \mathfrak{p}$ for some $n > 0$, hence $f \in \mathfrak{p}$ (because $\mathfrak{p}$ is prime). Hence $f \in \mathfrak{N}'$.

Proof.

Conversely, suppose that f is not nilpotent. Let Σ be the set of ideals $\mathfrak{a}$ with the property

$$n > 0 \Rightarrow f^n \notin \mathfrak{a}.$$

Then Σ is not empty because $0 \in \Sigma$. Zorn's lemma can be applied to the set Σ, ordered by inclusion, and therefore Σ has a maximal element. Let $\mathfrak{p}$ be a maximal element of Σ. We shall show that $\mathfrak{p}$ is a prime ideal. Let x, $y \notin \mathfrak{p}$. Then the ideals $\mathfrak{p} + (x)$, $\mathfrak{p} + (y)$ strictly contain $\mathfrak{p}$ and therefore do not belong to Σ; hence

$$f^m \in \mathfrak{p} + (x), \quad f^n \in \mathfrak{p} + (y)$$

for some m, n. It follows that $f^{m+n} \in \mathfrak{p} + (xy)$, hence the ideal $\mathfrak{p} + (xy)$ is not in Σ and therefore $xy \notin \mathfrak{p}$. Hence we have a prime ideal $\mathfrak{p}$ such that $f \notin \mathfrak{p}$, so that $f \notin \mathfrak{N}'$. □

Definition

The **Jacobson radical** $\mathfrak{R}$ of A is defined to be the intersection of all the maximal ideals of A.

It can be characterized as follows:

Proposition

Let A be a ring and $\mathfrak{R}$ its Jacobson radical. An element $x \in A$ is in $\mathfrak{R}$ if and only if $1 - xy$ is a unit in A for all $y \in A$.

If $\mathfrak{a}$, $\mathfrak{b}$ are ideals in a ring A. Their **sum** $\mathfrak{a}+\mathfrak{b}$ is the set of all $x+y$ where $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$. It is the smallest ideal containing $\mathfrak{a}$ and $\mathfrak{b}$.

More generally, we may define the sum $\sum_{i \in I} \mathfrak{a}_i$ of any family (possibly infinite) of ideals $\mathfrak{a}_i$ of A; its elements are all sums $\sum x_i$ where $x_i \in \mathfrak{a}_i$ for all $i \in I$ and almost all of the x_i (i.e., all but a finite set) are zero. It is the smallest ideal of A which contains all the ideals $\mathfrak{a}_i$.

The **intersection** of any family $(\mathfrak{a}_i)$ of ideals is an ideal.

The **union** $\mathfrak{a} \cup \mathfrak{b}$ of ideals is not in general an ideal.

Definition

Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in a ring A. The **product** of $\mathfrak{a}$ and $\mathfrak{b}$ is the ideal $\mathfrak{ab}$ **generated** by all products xy, where $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$. It is the set of all finite sums $\sum x_i y_i$ where each $x_i \in \mathfrak{a}$ and each $y_i \in \mathfrak{b}$.

Similarly we define the product of any **finite** family of ideals. In particular the powers $\mathfrak{a}^n$ $(n > 0)$ of an ideal $\mathfrak{a}$ are defined; conventionally $\mathfrak{a}^0 = (1)$. Thus $\mathfrak{a}^n$ $(n > 0)$ is the ideal generated by all products $x_1 x_2 \cdots x_n$ in which each factor x_i belongs to $\mathfrak{a}$.

Examples

1) In the ring $\mathbb{Z}$, $\mathfrak{a} = (m)$, $\mathfrak{b} = (n)$, then $\mathfrak{a} + \mathfrak{b}$ is the ideal generated by the greatest common factor of m and n. The ideal $\mathfrak{a} \cap \mathfrak{b}$ is the ideal generated by their least common multiple. The ideal $\mathfrak{a}\mathfrak{b} = (mn)$. So (in this case) $\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b} \Leftrightarrow m$, n are coprime.

2) $A = k[x_1, \ldots, x_n]$, $\mathfrak{a} = (x_1, \ldots, x_n) =$ ideal generated by $x_1, \ldots, x_n$. Then $\mathfrak{a}^m$ is the set of all polynomials with no terms of degree $< m$.

The three operations so far defined (sum, intersection, product) are all commutative and associative. Also there is the **distributive law**

$$\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}.$$

In $\mathbb{Z}$, we have $(\mathfrak{a}+\mathfrak{b})(\mathfrak{a}\cap\mathfrak{b})=\mathfrak{a}\mathfrak{b}$; but in general we have only $(\mathfrak{a}+\mathfrak{b})(\mathfrak{a}\cap\mathfrak{b})\subseteq\mathfrak{a}\mathfrak{b}$ since

$$(\mathfrak{a}+\mathfrak{b})(\mathfrak{a}\cap\mathfrak{b})=\mathfrak{a}(\mathfrak{a}\cap\mathfrak{b})+\mathfrak{b}(\mathfrak{a}\cap\mathfrak{b})\subseteq\mathfrak{a}\mathfrak{b}.$$

Clearly, $\mathfrak{a}\mathfrak{b}\subseteq\mathfrak{a}\cap\mathfrak{b}$, hence

$$\mathfrak{a}\cap\mathfrak{b}=\mathfrak{a}\mathfrak{b} \text{ if } \mathfrak{a}+\mathfrak{b}=(1).$$

Definition

Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are **coprime** (or **comaximal**) if $\mathfrak{a} + \mathfrak{b} = (1)$.

By what we said above, for coprime ideals we have $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$.

Clearly two ideals $\mathfrak{a}$, $\mathfrak{b}$ are coprime if and only if there exist $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$ such that $x + y = 1$.

Definition

Let A_1, $\ldots A_n$ be rings. Their **direct product**

$$A = \prod_{i=1}^{n} A_i$$

is the set of all sequences $x = (x_1, \ldots, x_n)$ with $x_i \in A_i$ $(1 \leq i \leq n)$ with componentwise addition and multiplication.

A is a commutative ring with identity $(1, \ldots, 1)$.

We have projections $p_i : A \to A_i$ defined by $p_i(x) = x_i$; they are ring homomorphisms.

Proposition

Let A be a ring and let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideals of A. Define a homomorphism

$$\phi : A \to \prod_{i=1}^{n} (A/\mathfrak{a}_i)$$

by the rule $\phi(x) = (x + \mathfrak{a}_1, \ldots, x + \mathfrak{a}_n)$.

1. If $\mathfrak{a}_i$, $\mathfrak{a}_j$ are coprime whenever $i \neq j$, then $\prod \mathfrak{a}_i = \bigcap \mathfrak{a}_i$.
2. ϕ is surjective $\Leftrightarrow$ $\mathfrak{a}_i$, $\mathfrak{a}_j$ are coprime whenever $i \neq j$.
3. ϕ is injective $\Leftrightarrow$ $\bigcap \mathfrak{a}_i = (0)$.

Proof.

Put proof of 1 and 3 here. □

Proposition

1. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be prime ideals and let $\mathfrak{a}$ be an ideal contained in $\bigcup_{i=1}^n \mathfrak{p}_i$. Then $\mathfrak{a} \subseteq \mathfrak{p}_i$ for some i.
2. Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be ideals and let $\mathfrak{p}$ be a prime ideal containing $\bigcap_{i=1}^n \mathfrak{a}_i$. Then $\mathfrak{p} \supseteq \mathfrak{a}_i$ for some i. If $\mathfrak{p} = \bigcap \mathfrak{a}_i$, then $\mathfrak{p} = \mathfrak{a}_i$ for some i.

Proof.

Put proof here. $\square$

Definition

If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in a ring A, their **ideal quotient** is

$$(\mathfrak{a} : \mathfrak{b}) = \{x \in A : x\mathfrak{b} \subseteq \mathfrak{a}\},$$

which is an ideal.

In particular, $(0 : \mathfrak{b})$ is called the **annihilator** of $\mathfrak{b}$ and is also denoted $\operatorname{Ann}(\mathfrak{b})$. It is the set of all $x \in A$ such that $x\mathfrak{b} = 0$.

If $\mathfrak{a}$ is any ideal of A, the **radical** of $\mathfrak{a}$ is

$$\operatorname{rad}(\mathfrak{a}) = \{x \in A : x^n \in \mathfrak{a} \text{ for some } n > 0\}.$$

This is the same thing as the radical of the quotient ring $A/\mathfrak{a}$, so it is an ideal.

Let $f : A \to B$ be a ring homomorphism. The image of an ideal in A may not be an ideal in B. (e.g., let f be the embedding of $\mathbb{Z}$ in $\mathbb{Q}$, the field of rationals, and take $\mathfrak{a}$ be to be any non-zero ideal in $\mathbb{Z}$.).

However, we can define the **extension** of the image of $\mathfrak{a}$ in B.

Definition

Let $f : A \to B$ be a ring homomorphism. Let $\mathfrak{a}$ be an ideal in A. The **extension** $\mathfrak{a}^e$ of $\mathfrak{a}$ is the ideal $Bf(\mathfrak{a})$ generated by the image $f(\mathfrak{a})$ in B.

Explicitly, $\mathfrak{a}^e$ is the set of all sums $\sum y_i f(x_i)$ where $x_i \in \mathfrak{a}$ and $y_i \in \mathfrak{b}$.

If $\mathfrak{b}$ is an ideal of B, then $f^{-1}(\mathfrak{b})$ is always an ideal of A, called the **contraction** of $\mathfrak{b}$.

Definition

Let $\mathfrak{b}$ is an ideal of B. The **contraction** $\mathfrak{b}^c$ of $\mathfrak{b}$ in A is the ideal $f^{-1}(\mathfrak{b})$. If $\mathfrak{b}$ is prime, then $\mathfrak{b}^c$ is prime.