Commutative Algebra in Algebraic Geometry

Elementary Definitions

William M. Faucette

University of West Georgia

Outline

A **ring** is an abelian group R with multiplication operation $(a, b) \mapsto ab$ and an identity element 1, satisfying for all $a, b, c \in R$:

$$\begin{aligned} a(bc) &= (ab)c \\ a(b + c) &= ab + ac \\ (b + c)a &= ba + ca \\ 1a = a1 &= a \end{aligned}$$

We will only consider rings where multiplication is commutative

$$ab = ba.$$

A **unit** or **invertible element** in a ring R is an element u which has a multiplicative inverse. This inverse is unique and will be denoted u^{-1}.

A field is a ring in which ever nonzero element is invertible.

We write $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, respectively, for the ring of integers and the fields of rational, real, and complex numbers.

A **zerodivisor** in R is a nonzero element $r \in R$ such that there exists a nonzero element $s \in R$ with $rs = 0$.

An nonzero element that is not a zerodivisor is a **nonzerodivisor**.

An **ideal** in a commutative ring R is an additive subgroup I such that if $r \in R$ and $s \in I$, then $rs \in I$.

An ideal I is said to be generated by a subset $S \subset R$ if every element $t \in I$ can be written in the form

$$t = \sum_{i=1}^{n} r_i s_i \quad \text{with } r_i \in R \text{ and } s_i \in S.$$

An ideal is **principal** if it can be generated by one element.

By convention, the ideal generated by the empty set is 0.

An ideal I in a commutative ring R is **prime** if $I \neq R$ (we usually say I is a **proper ideal** in this case) and if $f, g \in R$ and $fg \in I$, then either $f \in I$ or $g \in I$.

Equivalently, I is prime if for any ideals J, K with $JK \subset I$ we have $J \subset I$ or $K \subset I$. By induction, this follows for any finite set of ideals.

A ring R is an **(integral) domain** if 0 is a prime ideal.

An ideal I in a commutative ring R is **maximal** if I is a proper ideal P not continued in any other proper ideal.

The ideal I is prime if and only if R/I is a domain. The ideal P is maximal if and only if R/P is a field.

Since every field is a domain, this implies that every maximal ideal is a prime ideal.

A ring R is a **local ring** if P is the unique maximal ideal.

We sometimes indicate this by saying that (R, P) is a local ring.

An element $h \in R$ is **prime** if it generates a prime ideal.

Equivalently, h is prime if h is not a unit and whenever h divides a product fg, then h divides f or h divides g.

A **ring homomorphism** or **ring map** from a ring R to a ring S is a homomorphism of abelian groups that preserves multiplication and takes the identity element of R to the identity element of S.

General we omit the adjective "ring" when it is clear from context.

A **subring** of S is a subset closed under, addition, subtraction, and multiplication, and containing the identity element of S.

If R and S are rings, then the direct product $R \times S$ is the set of ordered pairs (a, b) with $a \in R$ and $b \in S$ made into a ring by defining the operations componentwise:

$$(a, b) + (a', b') = (a + a', b + b')$$
$$(a, b)(a', b') = aa', bb')$$

The map $a \mapsto (a, 0)$ makes R a subset of $R \times S$ and similarly for S.

As subsets of $R \times S$, $RS = 0$.

In the ring $R \times S$, consider the elements $e_1 = (1, 0)$ and $e_2 = (0, 1)$.

The are **idempotent** in the sense that $e_i^2 = e_i$.

Furthermore, they are **orthogonal idempotents** in the sense that $e_1 e_2 = 0$.

They are even a **complete set of orthogonal idempotents** in the sense that $e_1 + e_2 = 1$.

Quite generally, if $e_1, \ldots, e_n$ is a complete set of orthogonal idempotents in a commutative ring R, then $R = Re_1 \times \cdots \times Re_n$.

If R is a commutative ring, then a **commutative algebra** over R (or **commutative** R**-algebra**) is a commutative ring S together with a homomorphirsm $\alpha : R \to S$ of rings. We usually suppress the homomorphism α from the notation, and write rs in place of $\alpha(r)s$ when $r \in R$ and $s \in S$.

Any ring is a $\mathbb{Z}$-algebra in a unique way.

A more interesting example of an R-algebra is the polynomial ring $S = R[x_1, \ldots, x_n]$ in finitely many variables.

A **subalgebra** of S is a subring S' that contains the image of R.

A **homomorphism of R-algebras** $\varphi : S \to T$ is a homomorphism of rings such that $\varphi(rs) = r\varphi(x)$ for $r \in R$, $s \in S$.

Given an ideal $I \subset S$ we shall often be interested in its preimage in R. We shall sometimes denote this preimage of $R \cap I$, even though R need not be a subset of S.

If k is a commutative ring, the a **polynomial ring** over k in r variables $x_1, \ldots, x_r$ is denoted by $k[x_1, \ldots, x_r]$.

The elements of k are generally referred to as **scalars**.

A **monomial** is a product of variables; its degree is the number of these factors (counting repeats) so that, for example, $x_1^2x_2^3 = x_1x_1x_2x_2x_2$ has degree 5.

By convention the element 1 is regarded as the empty product. It is the unique monomial of degree 0.

A **term** is a scalar times a monomial. Every polynomial can be written uniquely as a finite sum of nonzero terms.

If the monomials in the terms of a polynomial f all have the same degree (or if $f = 0$), then f is said to be **homogeneous**. We also use the word **form** to mean homogeneous polynomial.

If k is a field, and $I \subset k[X]$ is an ideal, and $f \in I$ is an element of lowest degree, then Euclid's algorithm for dividing polynomials shows that f divides every element of I.

Thus $k[x]$ is a **principal ideal domain**, a domain in which every ideal can be generated by one element.

In a ring R, an element $r \in R$ is **irreducible** if it is not a unit and if whenever $r = st$ with $s, t \in R$, then one of s and t is a unit.

A ring R is **factorial** (or a **unique factorization domain**, sometimes abbreviated **UFD**) if R is an integral domain and element of R can be factored uniquely into irreducible elements, the uniqueness being up to factors which are units.

Factoriality played an enormous role in the history of commutative algebra, and it will come up many times. Here is an elementary analysis of the condition:

If R is factorial, and if $a_1, a_2, \ldots$ is a sequence of elements such that a_i is divisible by a_{i+1}, then the prime factors of a_{i+1} (counted with multiplicity) are among the prime factors of a_i, so for large i the prime factorization is the same, and a_i, a_{i+1} different only by a unit. In the language of ideals, any increasing sequence of principal ideals

$$(a_1) \subset \cdots \subset (a_i) \subset \cdots$$

must terminate in the sense that for all large i we have $(a_i) = (a_{i+1})$. This condition is called the **ascending chain condition on principal ideals**.

Conversely, if R has the ascending chain condition on principal ideals, then any element of R can be factored in a product of irreducible elements.

If in addition, every irreducible element is prime, then the factorization into product of irreducible elements is unique, so R is factorial.

Using these ideas, it is easy to show that any principal ideal domain R is factorial. Put proof of this here.

The polynomial ring in any number of variables over a field, or, indeed, over any factorial ring, is again factorial.

This is proved in most elementary texts using a result called Gauss' lemma.

If R is a ring, then an R-**module** M is an abelian group with a product $R \times M \to M$ written $(r,m) \mapsto rm$, satisfying for all $r,s \in R$ and $m,n \in M$:

$$\begin{aligned} r(sm) &= (rs)m \\ r(m+n) &= rm + rn \\ (r+s)m &= rm + sm \\ 1m &= m \end{aligned}$$

The R-modules we will be most interested in are the ideals I and the corresponding factor rings R/I.

If M is an R-module, the **annihilator** of M is denoted and defined by

$$\operatorname{ann} M = \{r \in R \mid rM = 0\}.$$

For example, $\operatorname{ann} R/I = I$.

It is convenient to generalize this relation. if I and J are ideals of R, we write

$$(I : J) = \{f \in R \mid rJ \subset I\}$$

for the **ideal quotient**.

It is useful to extend this notation to submodules M, N of an R-module P, and write

$$(M : N) = \{f \in R \mid fN \subset M\}.$$

If $I \subset R$ is an ideal and $M \subset P$ is a submodule, then we occasionally write $(M : I)$ or $(M :_P I)$ for the submodule $\{p \in P \mid Ip \subset M\}$.

A homomorphism (or map) or R-modules is a homomorphism of abelian groups that preserves the action of R. We say that a homomorphism is a **monomorphism** (or an **epimorphism** or an **isomorphism**) if it is an injection (or surjection or bijection) of the underlying sets.

The inverse map of an isomorphism is automatically a homomorphism.

If M and N are R-modules, then the **direct sum** of M and N is the module $M \oplus N = \{(m, n) \mid m \in M, n \in N\}$ with the module structure $r(m, n) = (rm, rn)$. There are natural inclusion and projection maps $M \subset M \oplus N$ and $M \oplus N \to M$ given by $m \mapsto (m, 0)$ and $(m, n) \mapsto m$ (and similarly for N).

These maps are enough to identify a direct sum: That is, M is a **direct summand** or a module P if and only if there are homomorphisms $\alpha : M \to P$ and $\sigma : P \to M$ whose composition $\sigma\alpha$ is the identify map of M; then $P \cong M \oplus (\ker \sigma)$.

If $\{M_i\}_{i \in I}$ is any set of modules, the **direct product** $\prod_i M_i$ has elements of tuples $(m_i)_{i \in I}$ and the **direct sum** $\sum_i M_i \subset \prod_i M_i$ consisting of those tuples $(m_i)_{i \in I}$ such that all but finitely many m_i are 0.

A **free** R-**module** is a module isomorphic to a direct sum of copies of R. We usually write R^n for the direct sum of n copies of R.

If M is a finitely generated free module, that is $M \cong R^n$ for some n, then the number n is invariant of M. It is the **rank** of M.

If A, B, and C are R-modules and $\alpha : A \to B$, $\beta : B \to C$ are homomorphisms, the a pair of homomorphisms

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} C$$

is **exact** if the image of α is equal to $\ker \beta$, the kernel of β.

A **short exact sequence** is a sequence of maps

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

such that each pair of consecutive maps is exact. That is, α is injective, β is surjective, and the image of α is the kernel of β.

The short exact sequqence

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

is **split** if there is a homomorphism $\tau : C \to B$ such that $\beta\tau$ is the identity map of C.

Equivalently, the sequence is split if there exists a homomorphism $\sigma : B \to A$ such that $\sigma\alpha$ is the identity map on A.

If the short exact sequence is split, then $B = A \oplus C$.

As a first example, suppose M_1 and M_2 are submodules of M, and $M_1 + M_2 \subset M$ is the submodule they generate, then the two inclusion maps combine to give a map $M_1 \cap M_2 \to M_1 \oplus M_2$, and with the "difference" map $M_1 \oplus M_2 \to M_1 + M_2$ given by $(m_1, m_2) \mapsto m_1 - m_2$, this gives a short exact sequence

$$0 \to M_1 \cap M_2 \to M_1 \oplus M_2 \to M_1 + M_2 \to 0.$$

The case of vector spaces if probably already familiar, and this case is no different.

As a second example, if R is a ring, $I \subset R$ an ideal, and $a \in R$ an element, then R/I maps onto $R/(I+(a))$. The kernel is generated by the class of a module I. Since the kernel is generated by just one element, it has the form R/J for some ideal J; in fact, J is the annihilator of a modulo I, that is $J = (I : a)$. Putting this together, we see that there is an exact sequence

$$0 \to R/(I : a) \xrightarrow{a} R/I \to R/(I + (a)) \to 0,$$

where the element a over the left-hand map indicates that it is multiplication by a.

As a third example, let M be a R-module. An element $m \in M$ corresponds to a homomorphism from R to M sending 1 to m. Thus, given a set of elements $\{m_\alpha\}_{\alpha \in A} \in M$ corresponds to giving a homomorphism φ from the direct sum $G := R^A$ of copies of R, indexed by A, to M, sending the α^{th} basis element to m_α. If the m_α generate M, then φ is a surjection.

The relations on the m_α are the same as elements of the kernel of the map $G \to M$. A set of relations $\{n_\beta\}_{\beta \in B} \in G$ corresponds to a homomorphism ψ from the free module $F := R^B$ to the kernel of φ. The m_α generate M and the n_β generate the kernel.

That is, M may be described as the module with generators $\{m_\alpha\}_{\alpha \in A}$ and relations $\{n_\beta\}_{\beta \in B}$ if and only if the sequence

$$F \to G \to M \to 0.$$

is exact. This sequence is usually called a **free presentation** of M. In case A and B are finite sets, so that each of F and G is a finitely generated free module over R, it is called a **finite free presentation**. A module M is **finitely generated** if there exists a finite set of elements that generate M, and **finitely presented** if it has a finite free presentation.