1. Preliminaries

1.1 INTRODUCTION

The subject matter of commutative algebra is the common ground of geometry and arithmetic. As these subjects have grown more abstract, more and more common ground has been found, and commutative algebra has grown very large.

In chapters 1 to 5 we shall cover some general material; in chapter 6 there will be some results useful in geometry; and in chapters 7 and 8 some arithmetical results.

An undergraduate algebra course should be all you need to follow this course.

1.2 DEFINITIONS AND RECAPITULATIONS

By 'ring' we mean 'commutative ring with a one'; for example, the zero ring $\{0\}$:

$+$	0
0	0

$.$	0
0	0

By 'ring morphism' we mean a one-preserving homomorphism.

Let A and B be rings. We say that A is a subring of B iff $A \subseteq B$ and the inclusion map: $A \to B$ is a ring morphism. For example $\{0\}$ is not a subring of the integers $\mathbf{Z}$; but $\mathbf{Z}$ is

a subring of the rationals $\mathbf{Q}$.

We say that a ring A is integral iff

(i) A is non-zero

(ii) for $x, y \in A$, if $xy = 0$, then $x = 0$ or $y = 0$.

We say that a ring A is a field iff

(i) A is non-zero

(ii) for all $x \in A$ with $x \neq 0$ there exists $y \in A$ such that $xy = 1$.

(We write x^{-1} for this unique y.)

Let us write A^* for the set of all non-zero elements of a ring A. Then A is integral (resp. a field) iff A^* is a semigroup (resp. a group) under multiplication. Thus every field is integral.

For a non-zero ring A we define $\mathfrak{u}(A) = \{x \in A; xy = 1$ for some $y \in A\}$; $\mathfrak{u}(A)$ is a group under multiplication and is called the group of units of A. For a field $\mathfrak{u}(A) = A^*$.

Let $\mathfrak{a}$ be an ideal of A. The following statements are equivalent:

(i) $\mathfrak{a} \subset A$

(ii) $1 \notin \mathfrak{a}$

(iii) $\mathfrak{a} \cap \mathfrak{u}(A) = \emptyset$

and we call such an ideal proper. Note that for $x \in A$ we have:

$x \notin \mathfrak{u}(A)$ iff xA is proper.

A subset S is of a ring A is called multiplicative iff

(i) $1 \in S$

(ii) $x, y \in S$ implies $xy \in S$;

for example: $\{1\}$; $\mathfrak{u}(A)$; A itself.

Let $\mathfrak{p}$ be an ideal of A. The following conditions are equivalent:

(i) $A \setminus \mathfrak{p}$ is multiplicative
(ii) $A/\mathfrak{p}$ is integral.

We call such an ideal prime. Note that it must be proper. For example, A is integral iff $\{0\}$ is a prime ideal.

Let $\mathfrak{m}$ be an ideal of A. The following conditions are equivalent:

(i) $\mathfrak{m}$ is a maximal element of the set of all proper ideals ordered by inclusion
(ii) $A/\mathfrak{m}$ is a field.

We call such an ideal maximal. Every maximal ideal is prime.

1.2.1 (Proposition). Let A be a ring; $S \subseteq A$ be multiplicative; and $\mathfrak{a}$ be an ideal of A with $\mathfrak{a} \cap S = \emptyset$. Then there is an ideal $\mathfrak{p}$ of A, maximal among those ideals $\mathfrak{b}$ with $\mathfrak{b} \supseteq \mathfrak{a}$ and $\mathfrak{b} \cap S = \emptyset$; and any such $\mathfrak{p}$ is prime.

Proof. Let

$$X = \{\mathfrak{b} \text{ an A-ideal: } \mathfrak{b} \supseteq \mathfrak{a} \text{ and } \mathfrak{b} \cap S = \emptyset\}.$$

Then $\mathfrak{a} \in X \neq \emptyset$. Let $Y \subseteq X$ be non-empty and totally ordered by inclusion. Then $\cup(Y) \in X$ and by Zorn's lemma X has maximal elements. If $\mathfrak{p}$ is such an element, $1 \notin \mathfrak{p}$; and if $x, y \notin \mathfrak{p}$ and $xy \in \mathfrak{p}$, then $\mathfrak{p} + xA$, $\mathfrak{p} + yA \supset \mathfrak{p}$ so that $\mathfrak{p} + xA$, $\mathfrak{p} + yA \notin X$. Thus there exist $s, t \in S$; $p, q \in \mathfrak{p}$;

$a, b \in A$ such that $s = p + xa$ and $t = q + yb$. Then $st = pq + xaq + ybp + abxy \in \mathfrak{p} \cap S$, a contradiction. Thus $A \setminus \mathfrak{p}$ is multiplicative and $\mathfrak{p}$ is prime. □

1.2.1.1 (Corollary). A non-zero ring has a maximal ideal.

Proof. Take $S = \{1\}$ and $\mathfrak{a} = \{0\}$. □

1.2.1.2 (Corollary). Let A be a non-zero ring. Then $\mathfrak{u}(A) = A \setminus \bigcup_{\mathfrak{m}} \mathfrak{m}$ where the union is taken over all maximal ideals $\mathfrak{m}$ of A.

Proof. One way is immediate. Conversely let $x \in A \setminus \mathfrak{u}(A)$. Then $xA \subset A$ and there is a maximal ideal $\mathfrak{m}$ of A with $xA \subseteq \mathfrak{m}$: so that $x \in \mathfrak{m}$. □

We say that $x \in A$ is nilpotent iff $x^n = 0$ for some $n \in \omega$. We write $\mathfrak{n}(A)$ for the ideal of all nilpotent elements of A, and call $\mathfrak{n}(A)$ the nilradical of A.

1.2.1.3 (Corollary). Let A be a non-zero ring. Then

$$\mathfrak{n}(A) = \bigcap_{\mathfrak{p}} \mathfrak{p}$$

taken over all prime ideals $\mathfrak{p}$ of A.

Proof. If $x^n = 0$, then $x^n \in \mathfrak{p}$ so $x \in \mathfrak{p}$ for all prime ideals $\mathfrak{p}$. Conversely if $x^n \neq 0$ for all $n \in \omega$, then $S = \{x^n : n \in \omega\}$ is multiplicative and $S \cap \{0\} = \emptyset$; thus $S \cap \mathfrak{p} = \emptyset$ for some prime ideal $\mathfrak{p}$ of A, and in particular $x \notin \mathfrak{p}$. □

It may be that a non-zero ring A has only one maximal ideal $\mathfrak{m}(A)$. In this case we call A local; $\mathfrak{m}(A)$ is its greatest proper ideal; and $\mathfrak{u}(A) = A \setminus \mathfrak{m}(A)$. We call $A/\mathfrak{m}(A)$ the residual field $\kappa(A)$ of A. For example, a field is local and is its own residual field.

If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of a ring A we define the ideal $\mathfrak{a}\mathfrak{b}$ as follows:

$$\mathfrak{a}\mathfrak{b} = \{ \sum_{i=1}^{m} a_i b_i : a_i \in \mathfrak{a} \text{ and } b_i \in \mathfrak{b} \} .$$

If $\mathfrak{p}$ is prime and $\mathfrak{p} \supseteq \mathfrak{a}\mathfrak{b}$, then plainly $\mathfrak{p} \supseteq \mathfrak{a}$ or $\mathfrak{p} \supseteq \mathfrak{b}$. Thus $\supseteq$ is like 'divides'.

If $(\mathfrak{a}_\lambda)_{\lambda \in \Lambda}$ is a family of ideals of A, we define $\sum_{\lambda \in \Lambda} \mathfrak{a}_\lambda$ to be the ideal of all $\sum_{\lambda \in \Lambda} a_\lambda$ for families $(a_\lambda)_{\lambda \in \Lambda}$ in $\prod_{\lambda \in \Lambda} \mathfrak{a}_\lambda$ with $a_\lambda = 0$ for all but a finite number of $\lambda \in \Lambda$.

We call the set $\operatorname{spec}(A)$ of all prime ideals of a ring A the spectrum of A. It is non-empty iff A is non-zero. For ideals $\mathfrak{a}$ of A we define

$$V(\mathfrak{a}) = \{ \mathfrak{p} \in \operatorname{spec}(A) : \mathfrak{p} \supseteq \mathfrak{a} \} \text{ so that}$$

$$\operatorname{spec}(A) = V(\{0\})$$

$$\emptyset = V(A)$$

$$V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a}\mathfrak{b})$$

$$\bigcap_{\lambda \in \Lambda} V(\mathfrak{a}_\lambda) = V(\sum_{\lambda \in \Lambda} \mathfrak{a}_\lambda)$$

and the $V(\mathfrak{a})$ are thus the closed sets for a topology on spec(A), called the Zariski topology. It is rarely Hausdorff as we shall see.

Exercise. spec(A) is compact.

If $f:A \to B$ is a ring morphism we define $F:\text{spec}(B) \to \text{spec}(A)$ by $F(\mathfrak{q}) = f^{-1}[\mathfrak{q}]$. Then F is continuous because $F^{-1}[V(\mathfrak{a})] = V(Bf[\mathfrak{a}])$ for any ideal $\mathfrak{a}$ of A. Thus spec is a contravariant functor from the category of rings to the category of topological spaces (see Appendix 1). If f is onto, the homomorphism theorems for rings show that F is an embedding.

1.3 MODULES

Let A be a ring. An A-module M is an additive group $(M, +)$ together with a multiplication: $A \times M \to M$ such that

$$\lambda(m + m') = \lambda m + \lambda m'$$

$$(\lambda + \lambda')m = \lambda m + \lambda' m$$

$$(\lambda\lambda')m = \lambda(\lambda' m)$$

$$1m = m$$

for all $\lambda, \lambda' \in A$ and $m, m' \in M$. For example, if A is a field, an A-module is just a vector space over A.

Most definitions and some theorems for modules are just like those for vector spaces. For example, if $(M_\lambda)_{\lambda \in \Lambda}$ is a

family of A-modules, the direct sum $\bigoplus_{\lambda \in \Lambda} M_\lambda$ consists of all families $(m_\lambda)_{\lambda \in \Lambda} \in \prod_{\lambda \in \Lambda} M_\lambda$ of finite support (that is with $m_\lambda = 0$ for all but a finite number of $\lambda \in \Lambda$), and with componentwise addition and multiplication.

A ring is a module over itself; and its submodules are its ideals.

Let L and M be A-modules and N be an additive group (resp. an A-module). Let $g: L \times M \to N$. We say that g is bilinear iff

(i) $g(l + l', m) = g(l, m) + g(l', m)$

(ii) $g(l, m + m') = g(l, m) + g(l, m')$

(iii) $g(\lambda l, m) = g(l, \lambda m)$.

(resp. $g(\lambda l, m) = g(l, \lambda m) = \lambda g(l, m)$)

for $l, l' \in L$; $m, m' \in M$; and $\lambda \in A$.

On the set $\mathbf{Z}^{(L \times M)}$ of all functions $f: L \times M \to \mathbf{Z}$ with $f(l, m) = 0$ for all but a finite number of $(l, m) \in L \times M$, define addition thus:

$$(f + f')(l, m) = f(l, m) + f'(l, m)$$

Thus $\mathbf{Z}^{(L \times M)}$ becomes an additive group. Let W be the subgroup generated by

$$f_{(l + l', m)} - f_{(l, m)} - f_{(l', m)}$$

$$f_{(l, m + m')} - f_{(l, m)} - f_{(l, m')}$$

$$f_{(\lambda l, m)} - f_{(l, \lambda m)}$$

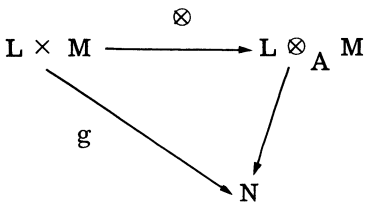
for all $l, l' \in L$; $m, m' \in M$; and $\lambda \in A$:
where f_α is the function such that

$$f_\alpha(\beta) = 1 \text{ if } \beta = \alpha$$

$$= 0 \text{ if } \beta \neq \alpha \ .$$

We call $\mathbf{Z}^{(L \times M)}/W$ the tensor product $L \otimes_A M$ of L and M, and write $l \otimes m$ for $f_{(l,m)} + W$. Thus if $x \in L \otimes_A M$ then $x = \sum_{i=1}^{r} l_i \otimes m_i$ for $l_i \in L$ and $m_i \in M$; and $\otimes : L \times M \to L \otimes_A M$ is bilinear.

$L \otimes_A M$ has the following universal property: if N is an additive group and $g: L \times M \to N$ is bilinear, then there is one and only one group morphism: $L \otimes_A M \to N$ such that the diagram



commutes: namely the function:

$$f + W \mapsto \sum_{\substack{l \in L \\ m \in M}} f(l, m)\, g(l, m) \ .$$

We use this universal property first of all to make $L \otimes_A M$ into an A-module: multiplication by $\lambda \in A$ is the unique group morphism: $L \otimes_A M \to L \otimes_A M$ such that $l \otimes m \mapsto (\lambda l) \otimes m$. With this structure, if N is an A-module and $g: L \times M \to N$ is bilinear, the unique group morphism:

$L \otimes_A M \to N$ such that $L \times M \to L \otimes_A M$ with $L \times M \to N$

commutes is also a module morphism (that is, a linear map).

Next if $g:L \to L'$ and $h:M \to M'$ are A-module morphisms, we define $g \otimes h$ to be the unique group morphism $L \otimes_A M \to L' \otimes_A M'$ such that $l \otimes m \mapsto g(l) \otimes h(m)$. Of course $g \otimes h$ is also an A-module morphism.

If $(M_\lambda)_{\lambda \in \Lambda}$ is a family of A-modules, there is a natural module isomorphism:

$$L \otimes_A \left(\bigoplus_{\lambda \in \Lambda} M_\lambda \right) \to \bigoplus_{\lambda \in \Lambda} (L \otimes_A M_\lambda) \quad \text{given by}$$

$l \otimes (m_\lambda)_{\lambda \in \Lambda} \mapsto (l \otimes m_\lambda)_{\lambda \in \Lambda}$ (its inverse comes from putting together the natural maps: $L \otimes_A M_\mu \to L \otimes_A \left(\bigoplus_{\lambda \in \Lambda} M_\lambda \right)$ for each $\mu \in \Lambda$).

Let M be an A-module and $(m_\lambda)_{\lambda \in \Lambda}$ be a family in M. We say that $(m_\lambda)_{\lambda \in \Lambda}$ generates (resp. bases) M iff for all $m \in M$ there is a family (resp. a unique family) $(\xi_\lambda)_{\lambda \in \Lambda}$ of finite support and such that $m = \sum_{\lambda \in \Lambda} \xi_\lambda m_\lambda$.

If M has a base we say that M is free: for example vector spaces are free.

If some finite family generates M, we say that M is of finite type.

If $f:A \to B$ is a ring morphism we make B into an A-module by defining $\lambda b = f(\lambda)b$ for $\lambda \in A$ and $b \in B$. If also M is an A-module we make $B \otimes_A M$ into a B-module by defining $\mu(b \otimes m) = (\mu b) \otimes m$ for $\mu, b \in B$ and $m \in M$. (We call $B \otimes_A M$ the B-ification of M.)

1.3.1 (Lemma). Let M be an A-module and $f:A \to B$ be a ring morphism. Suppose $(m_\lambda)_{\lambda \in \Lambda}$ generates (resp. bases) M. Then $(1 \otimes m_\lambda)_{\lambda \in \Lambda}$ generates (resp. bases) the B-module $B \otimes_A M$.

Proof. The generates part is immediate.

Suppose therefore that $(m_\lambda)_{\lambda \in \Lambda}$ bases M. For $\mu \in \Lambda$ define the A-module morphism $p_\mu:M \to A$ by

$$p_\mu(\sum_{\lambda \in \Lambda} \xi_\lambda m_\lambda) = \xi_\mu$$

and the B-module morphism $h_\mu:B \otimes_A M \to B$ by $h_\mu(b \otimes m) = bf(p_\mu(m))$. Then

$$h_\mu(\sum_{\lambda \in \Lambda} \eta_\lambda(1 \otimes m_\lambda)) = \sum_{\lambda \in \Lambda} \eta_\lambda f(p_\mu(m_\lambda))$$

$$= \eta_\mu$$

for any family $(\eta_\lambda)_{\lambda \in \Lambda}$ in B of finite support. Thus if $x \in B \otimes_A M$, there is a unique family $(h_\lambda(x))_{\lambda \in \Lambda}$ in B of finite support such that

$$x = \sum_{\lambda \in \Lambda} h_\lambda(x)\,(1 \otimes m_\lambda)\,. \square$$

1.3.1.1 (Corollary). Let A be a non-zero ring and M be a free A-module of finite type. Then there exists $n \in \omega$ such that if $(m_\lambda)_{\lambda \in \Lambda}$ bases M, then Λ has n elements.