Fall 2015 Notes – Atiyah and McDonald, Munkres, Lucier

Carlos Salinas

September 4, 2015

Contents

1 Commutative Algebra: Atiyah and McDonald

1.1 Rings and Ideals

Rings and ring homomorphisms

A *ring* A 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 ($(xy)z = x(yz)$) and distributive over addition ($(x(x+z) = xy+xz$, $(y+z)x = yx + zx$). We shall consider only rigs which are *commutative*:
(3) $xy = yx$ for all $x, y \in A$, and have an *identity element* (denoted by 1):
(4) $\exists 1 \in A$ such that $x1 = 1x = x$ for all $x \in A$. The identity element is then unique.

A *ring homomorphism* is a mapping f of a ring A into a ring B such that

(i) $f(x+y) = f(x) + f(y)$ (so that f is a homomorphism of abelian groups, and therefore also $f(x-y) = f(x) - f(y)$, $f(-x) = -f(x)$, $f(0) = 0$),
(ii) $f(xy) = f(x)f(y)$,
(iii) $f(1) = 1$.

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

A subset S of a ring A is a *subring* of A if S is closed under addition and multiplication and contains the identity element of A. The identity mapping of S into A is then a ring homomorphism.

If $f\colon A \to B$, $g\colon B \to C$ are ring homomorphisms so is their composition $g \circ f\colon A \to C$.

Ideals. Quotient rings

An *ideal* $\mathfrak{a}$ of a ring A is a subset of A which is an additive subgroup and is such that $A\mathfrak{a} \subset \mathfrak{a}$ (i.e., $x \in A$ and $y \in \mathfrak{a}$). The quotient group $A/\mathfrak{a}$ inherits a uniquely defined multiplication from A which makes it into a ring, called the *quotient ring* (or residue-class ring) $A/\mathfrak{a}$. The elements of $A/\mathfrak{a}$ are the cosets of $\mathfrak{a}$ in A, and the mapping $\varphi\colon A \to A/\mathfrak{a}$ which maps each $x \in A$ to its coset $x + \mathfrak{a}$ is a surjective ring homomorphism.

Proposition 1.1.1. *There is a 1-to-1 order-preserving correspondence between the ideals $\mathfrak{b}$ of A which contains $\mathfrak{a}$, and the ideals $\bar{\mathfrak{b}}$ of $A/\mathfrak{a}$, given by $\mathfrak{b} = \varphi^{-1}(\bar{\mathfrak{b}})$.*

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

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

Zero-divisors. Nilpotent elements. Units

A *zero-divisor* in a ring A is an element x which "divides 0", i.e., for which there exists $y \neq 0$ in A such that $xy = 0$. A ring with no zero-divisors $\neq 0$ (and in which $1 \neq 0$) is called an *integral domain.* For example, $\mathbf{Z}$ and $k[x_1, ..., x_n]$ (k a field, x_i indeterminates) are integral domains.

An element $x \in A$ is *nilpotent* if $x^n = 0$ for some $n > 0$. A nilpotent element is a zero-divisor (unless $A \neq 0$), but not conversely (in general).

A *unit* in A is an element x which "divides 1", i.e., an element x such that $xy = 1$ for some $y \in A$. The element y is then uniquely determined by x, and is written x^{-1}. The units in A form a (multiplicative) abelian group.

The multiples ax of an element $x \in A$ from a *principal* ideal, denoted by (x) or Ax. x is a unit $\iff (x) = A$. The *zero* ideal (0) is usually denoted by 0.

A *field* is a ring A in which $1 \neq 0$ and every nonzero element is a unit. Every field is an integral domain (but not conversely: $\mathbf{Z}$ is not a field).

Proposition 1.1.2. *Let A be a ring $\neq 0$. Then the following are equivalent:*

(i) A is a field;
(ii) the only ideals in A are 0 and (1);
(iii) every homomorphism of A into a nonzero ring B is injective.

Proof. (i) $\implies$ (ii). Let $\mathfrak{a} \neq 0$ be an ideal in A. Then $\mathfrak{a}$ contains a nonzero element x, x is a unit, hence $\mathfrak{a} \supset (x) = A$, hence $\mathfrak{a} = A$.

(ii) $\implies$ (iii). Let $\varphi\colon A \to B$ be a ring homomorphism. Then $\ker\varphi$ is an ideal $\neq (1)$ in A, hence $\ker\varphi = 0$, hence φ is injective.

(iii) $\implies$ (i). Let x be an element of A which is not a unit. Then $(x) \neq (1)$, hence $B = A/(x)$ is not the zero ring. Let $\varphi\colon A \to B$ be the natural homomorphism of A onto B, with kernel (x). By hypothesis, φ is injective, hence $x = 0$. ■

Prime ideals and maximal ideals

An ideal $\mathfrak{p}$ in A is *prime* if $\mathfrak{p} \neq (1)$ and if $xy \in \mathfrak{p} \implies x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

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

$$\mathfrak{p} \text{ is prime} \iff A/\mathfrak{p} \text{ is an integral domain;}$$

$$\mathfrak{m} \text{ is maximal} \iff A/\mathfrak{m} \text{ is a field.}$$

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

If $f\colon A \to B$ 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 a no zero-divisor $\neq 0$. But if $\mathfrak{n}$ is a maximal ideal of B is not necessarily true that $f^{-1}(\mathfrak{n})$ is maximal in A; all we can say for sure is that it is prime. (Example: $A = \mathbf{Z}$, $B = \mathbf{Q}$, $\mathfrak{n} = 0$.)

Theorem 1.1.3. *Every ring $A \neq 0$ has at least one maximal ideal.*

Proof. This is a standard application of Zorn's lemma. Let Σ be the set of all ideals $\neq (1)$ in A. Order Σ by inclusion. Σ is not empty, since $0 \in \Sigma$. To apply Zorn's lemma we must show that every chain in Σ has an upper bound in Σ; let then $(\mathfrak{a}_\alpha)$ 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 $\mathfrak{a}$ is an ideal and $1 \notin \mathfrak{a}$. Hence $\mathfrak{a} \in \Sigma$, and $\mathfrak{a}$ is an upper bound of the chain. Hence by Zorn's lemma Σ has a maximal element. ■

Corollary 1.1.4. *If $\mathfrak{a} \neq (1)$ is an ideal of A, there exists a maximal ideal of A containing $\mathfrak{a}$.*

Proof. Apply (1.3) to $A/\mathfrak{a}$ bearing in mind (1.1). Alternatively, modify the proof of (1.3). ■

Corollary 1.1.5. *Every nonunit of of A is contained in a maximal ideal.*

***Remarks**.* (1) If A is Noetherian we can avoid the use f Zorn's lemma: the set of all ideals $\neq (1)$ has a maximal element.

(2) There exists rings with exactly one maximal ideal, for example fields. A ring A with exactly one maximal ideal $\mathfrak{m}$ is called a *local ring*. The field $k = A/\mathfrak{m}$ is called the *residue field* of A.

Proposition 1.1.6. *(i) Let A be a ring and $\mathfrak{m} \neq (1)$ be 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.*

(ii) 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.

Proof. (i) Every ideal $\neq (1)$ consists of nonunits, hence is contained in $\mathfrak{m}$. Hence $\mathfrak{m}$ is the only maximal ideal of A.

(ii) Let $x \in A - \mathfrak{m}$. Since $\mathfrak{m}$ is maximal, then the ideal generated by x and $\mathfrak{m}$ is (1), hence there exists $y \in A$ and $\in \mathfrak{m}$ such that $xy + t = 1$; hence $xy = 1 - t$ belongs to $1 + \mathfrak{m}$ and therefore s a unit. Now use (i). ■

A ring with only a finite number of maximal ideals is called *semilocal*.

Examples 1.1.1. (1) $A = k[x_1, ..., x_n]$, k a field. Let $f \in A$ be an irreducible polynomial. By unique factorization, the ideal (f) is prime.

(2) $A = \mathbf{Z}$. Every ideal in $\mathbf{Z}$ is of the form (m) for some $m \geq 0$. The ideal (m) is prime $\iff$ $m = 0$ or a prime number. All ideals (p), where p is a prime number, are maximal: $\mathbf{Z}/(p)$ is the field of p elements.

(3) A *principal ideal domain* is an integral domain in which every ideal is principal. In such a ring every nonzero ideal is maximal. For if $(x) \neq 0$ is a prime ideal and $(y) \supset (x)$, we have $x \in (y)$, say $x = yz$, so that $yz \in (x)$ and $y \notin (x)$, hence $z \in (x)$, say $z = tx$. Then $x = yz = ytx$, so that $yt = 1$ and therefore $(y) = 1$.

Nilradical and Jacobson radical

Proposition 1.1.7. *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, $(x + y)^{m+n-1}$ is a 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 $\bar{x} \in \mathfrak{N}$ be represented by $x \in A$. Then $\bar{x}^n$ is prepresented by x^n, so that $\bar{x}^n = 0$ implies $x^n \in \mathfrak{N}$ implies $(x^n)^k = 0$ for some $k > 0$ implies $x \in \mathfrak{N}$ implies $\bar{x} = 0$. ■

The ideal $\mathfrak{N}$ is called the *nilradical* of A. The following proposition gives an alternative definition of $\mathfrak{N}$:

Proposition 1.1.8. *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 $f \in \mathfrak{N}'$.

Conversely, suppose that f is not nilpotent. Let Σ be the set of ideals $\mathfrak{a}$ with the property $n > 0 \implies f^n \notin \mathfrak{a}$. Then Σ is not empty because $0 \in \Sigma$. As in (1.3) 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

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

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 the prime ideal $\mathfrak{p}$ such that $f \notin \mathfrak{p}$, so that $f \notin \mathfrak{N}'$. ∎

The *Jacobson radical* $\mathfrak{R}$ of A is defined to be the intersection of all maximal ideals of A. It can be characterized as follows:

Proposition 1.1.9. *$x \in \mathfrak{R}$ if and only if $1 - xy$ is a unit for all $y \in A$.*

Proof. $\implies$: Suppose $1 - xy$ is not a unit. By (1.5) it belongs to some maximal ideal $\mathfrak{m}$; but $x \in \mathfrak{R} \subset \mathfrak{m}$, hence $xy \in \mathfrak{m}$ and therefore $1 \in \mathfrak{m}$ which is absurd.

$\impliedby$: Suppose $x \notin \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. Then $\mathfrak{m}$ and x generate the unit ideal (1), so that we have $u + xy = 1$ for some $u \in \mathfrak{m}$ and some $y \in A$. Hence $1 - xy \in \mathfrak{m}$ and is therefore not a unit. ∎

Operations on Ideals

Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are said to be *coprime* (or *comaximal*) if $\mathfrak{a} + \mathfrak{b} = (1)$. Thus for coprime ideals we have $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$.

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

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

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

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

$$\varphi \colon A \longrightarrow \prod_{i=1}^{n} \frac{A_i}{a_i}$$

by the rule $\varphi(x) = (x + \mathfrak{a}_1, ..., x + \mathfrak{a}_\mathfrak{n})$.

Proposition 1.1.10. *(i) If $\mathfrak{a}_i$, $\mathfrak{a}_j$ are coprime whenever $i \neq j$, then $\prod \mathfrak{a}_i = \bigcap \mathfrak{a}_i$.*
(ii) φ is injective $\iff$ $\mathfrak{a}_i$, $\mathfrak{a}_j$ are coprime whenever $i \neq j$.
(iii) φ is injective $\iff$ $\bigcap \mathfrak{a}_i = (0)$.

Proof. (i) By induction on n. The case $n = 2$ is dealt with above. Suppose $n > 2$ and the result true for $\mathfrak{a}_1, ..., \mathfrak{a}_{n-1}$, and let $\mathfrak{b} = \prod_{i=1}^{n-1} \mathfrak{a}_i = \bigcap_{i=1}^{n-1} \mathfrak{a}_i$. Since $\mathfrak{a}_i + a_j = (1)$ $(1 \leq i \leq n-1)$ we have equations $x_i + y_i = 1$ $(x_i \in \mathfrak{a}_i,\ y_i \in \mathfrak{a}_n)$ and therefore

$$\prod_{i=1}^{n-1} x_i = \prod_{i=1}^{n-1} (1 - y_i) \equiv 1 \pmod{\mathfrak{a}_n}.$$

Hence

$$\prod_{i=1}^{n} \mathfrak{a}_i = b\mathfrak{a}_n = \mathfrak{b} \cap \mathfrak{a}_n = \bigcap_{i=1}^{n} \mathfrak{a}_i.$$

(ii) $\Longrightarrow$: Let us show for example that $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are coprime. There exists $x \in A$ such that $\varphi(x) = (1, 0, ..., 0)$; hence $x \equiv 1 \pmod{\mathfrak{a}_1}$ and $x \equiv 0 \pmod{\mathfrak{a}_2}$, so that

$$1 = (1 - x) + x \in \mathfrak{a}_1 + \mathfrak{a}_2.$$

$\Longleftarrow$: It is enough to show, for example, that there is an element $x \in A$ such that $\varphi(x) = (1, 0, ..., 0)$. Since $\mathfrak{a}_1 + \mathfrak{a}_2 = (1)$ $(i > 1)$ we have equation $u_i + v_i = 1$ $(u_i \in \mathfrak{a}_1,\ v_i \in \mathfrak{a}_i)$. Take $x = \prod_{i=2}^{n} v_i$, then $x = \prod(1 - u_i) \equiv 1 \pmod{\mathfrak{a}_i}$, and $x \equiv 0 \pmod{\mathfrak{a}_i}$, $i > 1$. Hence $\varphi(x) = (1, 0, ..., 0)$ as required.

(iii) Clear, since $\bigcap \mathfrak{a}_i$ is the kernel of φ. ■

Proposition 1.1.11. *(i) Let $\mathfrak{p}_1, ..., \mathfrak{p}_n$ be prime ideals and let $\mathfrak{a}$ be an ideal contained in $\bigcup_{i=1}^{n} \mathfrak{p}_i$. Then $\mathfrak{a} \subset \mathfrak{p}_i$ for some i.*

(ii) Let $\mathfrak{a}_1, ..., \mathfrak{a}_n$ be ideals and let $\mathfrak{p}$ be a prime ideal containing $\bigcap_{i=1}^{n} \mathfrak{a}_i$. Then $\mathfrak{p} \supset \mathfrak{a}_i$ for some i.

Proof. (i) Is proved by induction on n in the form

$$\mathfrak{a} \subsetneq \mathfrak{p}_i \ (1 \leq i \leq n) \implies \mathfrak{a} \not\subset \bigcup_{i=1}^{n} \mathfrak{p}_i.$$

It is certainly true for $n = 1$. If $n > 1$ and the result is true for $n - 1$, then for each i there exists $x_i \in \mathfrak{a}$ such that $x_i \in \mathfrak{p}_i$ for all i. Consider the element

$$y = \sum_{i=1}^{n} x_1 \cdots x_{i-1} x_{i+1} \cdots x_n;$$

we have $y \in \mathfrak{a}$ and $y \notin \mathfrak{p}_i$ $(1 \leq i \leq n)$. Hence $\mathfrak{a} \not\subset \bigcup_{i=1}^{n} \mathfrak{p}_i$.

(ii) ■

2 Topology: Munkres