Notes on Commutative Algebra

David Easdown
School of Mathematics and Statistics
University of Sydney
NSW 2006, Australia
de@maths.usyd.edu.au

February 27, 2009

Contents

- **Part 2**
  - 2.1 Modules and Module Homomorphisms
  - 2.2 Submodules and Quotient Modules
  - 2.3 Operations on Modules
  - 2.4 Finitely Generated and Free Modules
  - 2.5 Nakayama's Lemma
  - 2.6 Exact Sequences
  - 2.7 Tensor Products of Modules
  - 2.8 Multilinear Mappings and Tensor Products
  - 2.9 Restriction and Extension of Scalars
  - 2.10 Exactness Properties of the Tensor Product
  - 2.11 Algebras

- **Part 3**
  - 3.1 Rings of Fractions
  - 3.2 Modules of Fractions
  - 3.3 Some Properties of Localization
  - 3.4 Extended and Contracted Ideals in Rings of Fractions
- **Part 4**
  - 4.1 Primary Decompositions
  - 4.2 Chain Conditions
  - 4.3 Composition Series
  - 4.4 Noetherian Rings
  - 4.5 Hilbert's Nullstellensatz (Zeros Theorem)
  - 4.6 Appendix: Gauss' Theorem

1.0 Overview

— study of commutative rings

— elaboration of selections from first 7 chapters of

"Introduction to Commutative Algebra"

by Atiyah and Macdonald

Part 1

A **ring** A is an "arithmetic" with $+, \bullet$.

If $\bullet$ is commutative, that is,

$$(\forall a, b \in A) \quad a \bullet b \; = \; b \bullet a$$

then we call A **commutative**.

Unless stated otherwise all rings will be assumed to be commutative.

Not all of the detail of a given ring A will be of interest.

Information is filtered from A by **factoring out by an ideal**.

Example: Say time in whole hours is modelled by $\mathbb{Z}$. If one is only interested in the time, but not the day itself, or even whether am or pm, then one works in the **quotient ring**

$$\mathbb{Z}/24\mathbb{Z} \qquad \text{or} \qquad \mathbb{Z}/12\mathbb{Z}\ .$$

The subsets $24\mathbb{Z}$ and $12\mathbb{Z}$ are **ideals** of $\mathbb{Z}$.

The quotient ring is the formal consequence of identifying elements of the ideal with zero . . .   . . . thinking of the ideal as "vanishing".

Rings can be arbitrarily complicated.

Sometimes they simplify or become tractable by factoring out by the **radical**

(the "nasty" part that we would like to "vanish").

We will meet the **nil** and **Jacobson** radical (which happen to coincide for example if the ring is finite).

Example: $\mathbb{Z}_9 = \{0, 1, \ldots, 8\}$, with mod 9 arithmetic, is not a **field**, but

$$\mathbb{Z}_3 \cong \mathbb{Z}_9 / 3\mathbb{Z}_9$$

is a field.

$3\mathbb{Z}_9$ is the radical of $\mathbb{Z}_9$.

Often we will factor out by **prime** or **maximal** ideals.

closely connected with **integral domains**

connected with **fields**

existence guaranteed by **Zorn's Lemma**

Rings with exactly one maximal ideal are called **local**.

— "close" to being fields, e.g. $\mathbb{Z}_9$ is close to $\mathbb{Z}_3$.

Part 2

Modules are like vector spaces, except that scalars may be ring (rather than field) elements.

Familiar example: Every abelian group M, written additively, becomes a module over $\mathbb{Z}$: for $x \in M$ and $n \in \mathbb{Z}$ define

$$n\,x \;=\; \begin{cases} \underbrace{x + ... + x}_{n \text{ times}} & \text{if } n > 0 \\ 0 & \text{if } n = 0 \\ -((-n)\,x) & \text{if } n < 0 \end{cases}$$

Modules "decompose" or "extend" . . .

We develop some theory of **exact sequences** . . .

Example (short exact sequences):

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}_2 & \longrightarrow & \mathbb{Z}_2 \oplus \mathbb{Z}_2 & \longrightarrow & \mathbb{Z}_2 & \longrightarrow & 0 \\ & & x & \mapsto & (x,0) & & & & \\ & & & & (x,y) & \mapsto & y & & \end{array}$$

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z}_2 & \longrightarrow & \mathbb{Z}_4 & \longrightarrow & \mathbb{Z}_2 & \longrightarrow & 0 \\
 & & 0 & \mapsto & 0 & & & & \\
 & & 1 & \mapsto & 2 & & & & \\
 & & & & 0,2 & \mapsto & 0 & & \\
 & & & & 1,3 & \mapsto & 1 & &
\end{array}
$$

$\mathbb{Z}_2 \oplus \mathbb{Z}_2$ and $\mathbb{Z}_4$ are **extensions** of $\mathbb{Z}_2$ by $\mathbb{Z}_2$.

We develop some theory of **tensor products** of modules.

Example (“extending” the ring of scalars)**:**

Now, $\mathbb{Z}_3$ is a module over $\mathbb{Z}$, $\mathbb{Z} \subseteq \mathbb{Q}$ and

$$\mathbb{Z} \subseteq A = \{ a/b \in \mathbb{Q} \mid b \text{ not divisible by } 3 \} .$$

Then $M = \underbrace{A \otimes_{\mathbb{Z}}}\ \mathbb{Z}_3$ is a module over $\mathbb{Z}$ and over A .

↑ provides a “buffer” for scalar multiplication by elements of A.

Identifying $x \in \mathbb{Z}_3$ with $1 \otimes x$ we get a scalar multiplication by elements of A:

$$\frac{a}{b}(1 \otimes x) \;=\; \frac{a}{b}(1 \otimes\; bb'x) \;=\; \frac{a}{b}b\,(1 \otimes\; b'x)$$

$$=\; a\,(1 \otimes\; b'x) \;=\; 1 \otimes\; ab'x$$

where b' is any integer such that $bb' \equiv 1 \mod 3$ (which exists because b is not divisible by 3).

Care is required: $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_3$ vanishes!!

$$\frac{a}{b} \otimes x \;=\; 3(\frac{a}{3b} \otimes x) \;=\; \frac{a}{3b} \otimes 3x \;=\; \frac{a}{3b} \otimes 0 \;\equiv\; 0\,.$$

Part 3

Rings of fractions: “formally inverting certain objects. . . and seeing what happens”

Familiar examples:

$$\mathbb{Z} \subseteq \mathbb{Q}$$

integral domain field of fractions

$$\mathbb{R}[x] \subseteq \mathbb{R}(x) = \{p(x)/q(x) \mid p(x), q(x) \in \mathbb{R}[x],\ q(x) \not\equiv 0\}$$

polynomial ring

A general construction exists for **multiplicatively closed** subsets of rings.

— important example: complement of a **prime** ideal;

— leads to "**localization** at a prime ideal".

Example:

$$A \;=\; \{m/n \mid m,n \in \mathbb{Z},\ n \text{ not divisible by } 3\}$$

is the result of localizing the ring $\mathbb{Z}$ at its prime ideal $3\mathbb{Z}$ (anything that is not a multiple of 3 can be inverted).

The ring A is **local**, "close" to being a field.

Modules of fractions:

—forcing some scalars to be "invertible" and seeing what happens;

—connection with **tensor products**, a module construction studied in the second part of the course.

$$S^{-1}M \quad \cong \quad S^{-1}A \otimes_A M$$

as $S^{-1}A$-modules
where M is an A-module and S is a multiplicatively closed subset of A

"enlarging" the scalar multiplication from A to $S^{-1}A$

Part 4:

Primary decomposition of (noetherian) rings:

—mimics factorization of integers into products of prime powers.

Chain conditions ("finiteness" conditions) on modules and rings

—**ascending chain condition (a.c.c.)**

$$R_1 \subseteq R_2 \subseteq \ldots \subseteq R_n \subseteq \ldots \qquad \text{"halts"}$$

—**descending chain condition (d.c.c.)**

$$R_1 \supseteq R_2 \supseteq \ldots \supseteq R_n \supseteq \ldots \qquad \text{"halts"}$$

Example: $\mathbb{Z}$ is a **principal ideal domain (PID)** (all ideals are **principal** of the form $n\mathbb{Z}$, $n \in \mathbb{Z}$.)

Observe that

$$2\mathbb{Z} \supset 4\mathbb{Z} \supset 8\mathbb{Z} \supset \dots \supset 2^n\mathbb{Z} \supset \dots$$

where $\supset$ means **proper** set containment, so

$\mathbb{Z}$ does not satisfy the d.c.c.

$\mathbb{Z}$ is not **artinian**

However

$\mathbb{Z}$ **does** satisfy the a.c.c.

$\mathbb{Z}$ is **noetherian**

Proof: Suppose

$$k_1\mathbb{Z} \subseteq k_2\mathbb{Z} \subseteq \dots \subseteq k_n\mathbb{Z} \subseteq \dots \qquad (*)$$

WLOG we may suppose $k_1 \neq 0$, so that each $k_n \neq 0$.

Now WLOG we may suppose each $k_n > 0$.

Hence

$$\ldots \quad | \quad k_n \quad | \quad k_{n-1} \quad | \quad \ldots \quad | \quad k_2 \quad | \quad k_1 \, .$$

↑

divides

In particular

$$k_1 \quad \geq \quad k_2 \quad \geq \quad \ldots \quad \geq \quad k_n \quad \geq \quad \ldots$$

which halts, because there is no infinite descending sequence of positive integers. Hence $(*)$ halts, and the claim is proved.

Final part of the main course, some classical results:

— **Jordan-Holder Theorem:** “no matter how you chop up a module you get the same simple pieces”.

— **Hilbert’s Basis Theorem:** “adjoining an indeterminate preserves being noetherian, so all ideals of a polynomial ring in several variables are finitely generated”.

— **Hilbert’s Nullstellensatz (Zeros Theorem):** “zero sets correspond to radical ideals”.

(For the last result we may need to review theory of **field extensions** and discuss Gauss’ Theorem concerning **unique factorization domains**.)