1

21/10/13

Ben Gurion University
Mathematics
Fall 2013/14

Commutative and Homological Algebra

Prof. Amnon Yekutieli

Introduction

Commutative algebra is the function theory of algebraic geometry, in the same sense that calculus is the function theory of differential geometry. The "functions" we will discuss here are polynomials, or fractions of polynomials (rational functions), or more generally elements of commutative rings with certain finiteness properties.

Homological algebra and commutative algebra are both generalizations of linear algebra. Recall that in linear algebra we considered vector spaces over a field K. Every vec. space V had a basis, so every linear transformation could be represented

(2) by a matrix. In our course we will replace the field K with a commutative ring A, and the vector space V with an A-module M. Usually M is not free (it does not have a basis). One of our goals in this course is to understand the various kinds of A-modules and the homomorphisms between them. Example: When $A = \mathbb{Z}$ the classification of finitely generated $\mathbb{Z}$-modules is already known to you: every f.g. $\mathbb{Z}$-module is a direct sum of a free module and a torsion module.

There is a tight interaction between the ideas in the previous paragraphs. For example we consider the concept of <u>projective module</u>, that comes from homological algebra. Another concept is that of <u>locally free module</u>, which comes from algebraic geometry. At the end of the course we will prove that (under suitable finiteness assumptions) an A-module P is projective iff it is locally free.

Modules

A quick review of rings.

A **ring** is a system $(A, 0, 1, +, \cdot)$ consisting of a set A; distinguished elements $0, 1 \in A$; and binary operations $+, \cdot$ on A.

The conditions are that $(A, 0, +)$ is an abelian group; the multiplication $\cdot$ is associative; the mult. $\cdot$ is distributive w.r.t the addition $+$; and the element 1 is neutral for multiplication.

A ring A is commutative if $a \cdot b = b \cdot a$ for every $a, b \in A$.

Convention In the first half of the course, all rings are commutative by default. (That's why we call it "commutative algebra".)

A ring A is trivial if $A = \{0\}$. It is easy to see that A is trivial iff $1 = 0$.

(4) A ring K is a *field* if it is not trivial, and any nonzero $a \in K$ has a multiplicative inverse, i.e. an element $b \in K$ s.t. $a \cdot b = 1$. The set $K^{\times}$ of nonzero elements of K is an abelian group.

In general, for any ring A we let
$$A^{\times} := \{ a \in A \mid a \text{ has a multip. inverse} \}.$$
This is the multiplicative group of A.
It can be very small:
$$\mathbb{Z}^{\times} = \{ \pm 1 \}.$$

An *ideal* in a ring A is a subset $I \subset A$ such that:
- $0 \in I$
- $a, b \in I \Rightarrow a + b \in I$ (additive subgroup of A)
- $a \in I,\ b \in A \Rightarrow a \cdot b \in I$.

I will sometimes use fractur letters like $\mathfrak{a}, \mathfrak{p}, \mathfrak{m}$ for ideals.

A *subring* of a ring A is a subset $B \subset A$ s.t. $0, 1 \in B$, and B is closed under the operations $+, \cdot$. So $(B, 0, 1, +, \cdot)$ is a ring.

(5) A *ring homomorphism* $f: A \to B$ is a function that respects the ring structures.

I.e. $f(0_A) = 0_B$, $f(1_A) = 1_B$,

$$f(a_1 + a_2) = f(a_1) + f(a_2),$$
$$f(a_1 \cdot a_2) = f(a_1) \cdot f(a_2).$$

The kernel of f is

$$Ker(f) := \{a \in A \mid f(a) = 0_B\}.$$

We know that $Ker(f)$ is an ideal of A, $Im(f)$ is a subring of B, and

$$A / Ker(f) \cong Im(f) \quad \text{as rings.}$$

(see exercise later re "$\cong$")

I remind you that given an ideal $\mathfrak{a} \subset A$, the quotient abelian group $A/\mathfrak{a}$ has on it a unique ring structure s.t. the canonical surjection $A \to A/\mathfrak{a}$ is a ring hom.

An ideal $\mathfrak{m} \subset A$ is *maximal* if $\mathfrak{m} \subsetneq A$, and there is no ideal $\mathfrak{n}$ s.t.

$$\mathfrak{m} \subsetneq \mathfrak{n} \subsetneq A.$$

We know that an ideal $\mathfrak{m} \subset A$ is maximal iff the ring $A/\mathfrak{m}$ is a field.

(If you don't know it - then prove it as an exercise.)

In algebra we use Zorn's Lemma freely. (Recall from "Set Theory" that this is equivalent to the Axiom of Choice.)

Proposition If A is a nontrivial ring, then it has a maximal ideal.

Proof. Consider the set

$$W := \left\{ \begin{array}{l} \text{ideals } \mathfrak{m} \subset A \text{ s.t.} \\ 1 \notin \mathfrak{m} \end{array} \right\}.$$

This is nonempty, since $\{0\} \in W$.
If $W' \subset W$ is a linearly ordered(*) nonempty subset of W, then it has a supremum in W: it is the ideal $\bigcup_{\mathfrak{m} \in W'} \mathfrak{m}$. Zorn's Lemma says that W has a maximal element, say $\mathfrak{m}$. (*) by inclusion
This is a maximal ideal of A. □

Theorem Let K be a field.

(1) Every K-module M has a basis.
(2) Suppose X and Y are bases of a K-module M. Then $|X| = |Y|$.

Here $|X|$ is the cardinality of the set X.

(2) Exercise Prove this thm. (Hint: we know it is true if M is fin. gen. Use Zorn and some set theory for a case.)
[not easy]

(7) **Exercise** (1) Let A be a ring. Show that there is a unique ring hom. $\mathbb{Z} \to A$.

(2) Let K, L be fields, and let $f: K \to L$ be a ring hom. Show that f is injective.

Exercise. What are the maximal ideals of these rings?

(2)
(a) $\mathbb{Z}$
(b) $\mathbb{C}[t]$, polynomials in variable t.
(c) $\mathbb{R}[t]$

Exercise Suppose $f: A \to B$ is a ring hom that is bijective. Let $g: B \to A$ be the inverse ~~function~~. Prove that g is also a ring hom. (Because of this we call f & g ring isomorphisms.)

(8) Free Modules

A reminder on modules. Let A be a ring. An A-module is a system $(M, 0, +, \cdot)$ where $(M, 0, +)$ is an abelian group, and

$$\cdot : A \times M \to M$$

is a function called multiplication. The conditions on $\cdot$ are:

- associativity $\quad a\cdot(b\cdot m) = (a\cdot b)\cdot m$
- distributivity $\quad (a+b)\cdot m = (a\cdot m) + (b\cdot m)$
  $\quad a\cdot(m+n) = (a\cdot m) + (a\cdot n)$
- neutrality of 1 $\quad 1\cdot m = m$.

Exercise Let M be an abelian group and let A be a ring. Consider the noncommutative (i.e. not necessarily comm.) ring

$$\mathrm{End}_{\mathbb{Z}}(M) := \left\{\begin{array}{c}\text{abelian group}\\ \text{endomorphisms of}\\ M \text{ (Operation is}\\ \text{composition)}\end{array}\right\}$$

Show that giving M a structure of A-module (i.e. defining $a\cdot m$) is the same as giving a ring hom $A \to \mathrm{End}_{\mathbb{Z}}(M)$.

to here 21/10