INTRODUCTION TO COMMUTATIVE ALGEBRA
MAT6608

ABRAHAM BROER

References

[1] Atiyah, M. F.; Macdonald, I. G. *Introduction to commutative algebra.* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1969

[2] Dummit, David S.; Foote, Richard M. *Abstract algebra. Third edition.* John Wiley & Sons, Inc., Hoboken, NJ, 2004.

[3] Eisenbud, David *Commutative algebra. With a view toward algebraic geometry.* Graduate Texts in Mathematics, **150**. Springer-Verlag, New York, 1995.

[4] Kunz, Ernst *Introduction to commutative algebra and algebraic geometry.* Birkhuser-Boston, Boston, MA, 1985.

[5] Matsumura, Hideyuki *Commutative algebra. Second edition.* Mathematics Lecture Note Series, **56**. Benjamin/Cummings Publishing Co., Inc., Reading, Mass., 1980.

[6] Matsumura, Hideyuki *Commutative ring theory.* Translated from the Japanese by M. Reid. Second edition. Cambridge Studies in Advanced Mathematics, **8**. Cambridge University Press, Cambridge, 1989.

[7] Reid, Miles *Undergraduate commutative algebra.* London Mathematical Society Student Texts, **29**. Cambridge University Press, Cambridge, 1995.

1. Preliminaries

This course MAT6608, Introduction à l'algèbre commutative, will give an introduction to the theory of commutative rings and their modules. I will provide some lecture notes (to be found on http://www.dms.umontreal.ca/ broera/), complemented by parts of the standard reference Dummit and Foote's volume on algebra, [2] (which was also used in the preliminary course MAT2611). We assume that the student has a good basis in linear algebra (MAT1600, in particular the material in sections 11.1 to 11.4 of [2]) and in general algebra (MAT2600 and MAT2611, in particular chapters 7 to 10, and 12 of [2]).

In this course a *ring* will be a commutative, associative unitary ring, and a *module* will be a unitary module (meaning that $\mathbf{1} \cdot m = m$, for all m in the module and $\mathbf{1}$ the unit element of the ring). If f is a homomorphism of rings, we shall assume that the unit of the first ring is mapped to the unit of the second ring. We assume that at least the notions of *subring, ideal, prime ideal, maximal ideal, domain, field, quotient ring, euclidean domain, principal ideal domain (PID), factorial domain, irreducible element, prime element, nilpotent element* are known and the various standard isomorphism theorems of rings. Also the existence and construction of the *fraction field* of a domain, the existence of maximal ideals and the chinese remainder theorem ([2, Sect. 7.6]); if R is a factorial domain, then $R[X]$ is also a factorial domain; in particular polynomial rings over a field are factorial domains. And the notions of *module, submodule, quotient module,*

Date: January 22, 2013.

finitely generated module, torsion module and torsion free module, free module, and the standard isomorphism theorems of modules.

The culmination of the theory developed in MAT2611 is the very useful structure theorem of the finitely generated modules over a principal ideal domain. The student is supposed to understand the statement of the theorem and some of its applications, but we shall rarely use in this course.

Theorem 1.1 ([2, Sect. 12.1])**.** *Let R be a principal ideal domain and M a non-zero finitely generated R-module. There exist unique integers r and d and unique ideals $0 \neq I_1 \subseteq I_1 \subseteq \ldots \subseteq I_d \neq R$ and an isomorphism*

$$M \simeq R^d \oplus R/I_1 \oplus R/I_2 \oplus \ldots \oplus R/I_d.$$

It has some important consequences in matrix theory (the existence of the *Jordan canonical form* of a complex $n \times n$-matrix) and in group theory (classification of finite abelian groups).

In particular, for a principal ideal domain every submodule of a finitely generated free module is free, and every torsion free module is free. Conversely, if R is a domain such that every submodule of a finitely generated free module is free then R is a principal ideal domain. Or if R is a ring such that every submodule of a finitely generated torsion free module is free then R is a principal ideal domain.

2. Introduction

The way we consider ("abstract") algebra and linear algebra nowadays originated in the early twentieth century, after the pioneering ideas of Hilbert in the 1890s and developed by Noether, Artin, Krull, van der Waerden and others. It brought about a revolution in the whole of mathematics, not just algebra. The preliminary work by Dedekind, Kronecker, Kummer, Weber, Weierstrass, Weber and others in the nineteenth century were great motivations. And of course the great mathematicians before that time used already many algebraic ideas in special cases, like Gauss in number theory and Cayley in matrix theory and in geometry.

The focus changed from studying specific rings one at the time (like the ring of Gaussian integers $\mathbb{Z}[i]$ or the subring of polynomials fixed under the action of a specific group) to studying whole classes of rings simultaneously (like all rings like $\mathbb{Z}[i]$ useful in number theory: the so-called Dedekind domains). The early results on finite group representation by matrices of Frobenius, Burnside, Wedderburn and Schur led Noether to realize that module theory was a useful tool for studying rings, and led eventually to the powerful homological algebra. She also realized that imposing her finite condition on rings, made it possible to prove many interesting general results (like primary decomposition of ideals and dimension theory).

The change of focus was initiated by the introduction of a new sort of methods and results in mathematics by the young Hilbert in the 1890's. For example, he proved that all ideals in a polynomial ring over a field with finitely many variables is finitely generated (without saying how to find the generators) and used it to give a proof of a famous finiteness theorem in invariant theory, which shocked the mathematical world at the time and made Hilbert famous. Before him most methods were constructive and concrete as opposed to the abstract methods of Hilbert.

Many interesting and motivating examples of rings arise in algebraic number theory and in algebraic geometry, but also in other fields, like complex analysis. Eventually Grothendieck realized

that commutative rings should be seen as the local building blocks of a more general algebraic geometry, glued together using a natural topology, the Zariski topology, on the collection of prime ideals. This revolutionized mathematics again, and not just algebraic geometry. Nowadays, his general algebraic geometry is being even further generalized, since it turned out to be not general enough, to enable people to prove enormously deep results, say in classical fields as number theory (e.g. Langlands correspondance).

But one of the basic tools necessary is still commutative algebra. In this course we shall discuss broadly some of its fundamental ideas.

3. Hilbert's Basis Theorem

We start our course by discussing some of Hilbert's algebraic results in the 1890's, and some of its more immediate generalizations. We shall use these results as motivations of more general results.

An early part of algebra consisted of abstraction of the properties of certain well-studied rings like polynomial rings (affine rings) or the rings of number theory (Dedekind domains). Some of those rings, such as $\mathbb{Z}, \mathbb{Z}[i]$ and $k[X]$ (where k is a field) are principal ideal domains (i.e., every ideal is generated by one element). A ring like $k[X, Y, Z]$ (k a field) is not a principal ideal domain, but Hilbert proved that all its ideals are at least finitely generated.

We say that a ring R is *Noetherian* if every ideal is finitely generated. The class of Noetherian rings is the most important class of rings in commutative algebra.

Theorem 3.1 (Hilbert's Basis Theorem, [2, Sec. 9.6])**.** *If R is a Noetherian ring, then the polynomial ring $R[X]$ of polynomials in one variable X and coefficients in R is also a Noetherian ring.*

Hilbert also noticed the following easy result.

Proposition 3.1. *Let $R \subset S$ be a subring and suppose there is a map $F : S \to R$ such that $F(rs) = rF(s)$ and $F(r) = r$ for all $r \in R$ and $s \in S$. If S is a Noetherian ring then R is also a Noetherian ring.*

Proof. Let $I \lhd R$ be an ideal. It generates the ideal IS in S which is finitely generated, since S is Noetherian. So there are finitely many elements $r_1, \ldots, r_n \in I$ that generate IS (why?). Let $r \in I$ be arbitrary. Then $r \in IS$, and so r can be written as $r = \sum_{i=1}^{n} r_i s_i$ for some $s_i \in S$. We apply F to this equation to get that $r = F(r) = \sum_{i=1}^{n} r_i F(s_i)$ is in the ideal of R generated by $r_1, \ldots, r_n$. We conclude that $I = (r_1, \ldots, r_n)$ is a finitely generated ideal in R. We have proved that R is a Noetherian ring. □

Exercise 3.1. Let $R \subset S$ and F are as in the proposition. Consider S in the natural way as an R-module. Then F is a surjective R-module and we get a direct sum decomposition $S = R \oplus K$, as R-modules with $K = \operatorname{Ker} F$. Conversely, if there is an R-submodule K of S such that $S = K \oplus R$ as R-modules, then there is an F as in the proposition.

In the early 1890's Hilbert combined the above two abstract results with a then classical invariant theory result by Cayley, to prove the finiteness theorem of classical invariant theory. A result and

method that made him famous overnight (in the mathematical micro-cosmos). We shall give a simple special case of this result, but will not go into this more deeply.

If $R \subset S$ is a subring and $s_1, \ldots, s_n$ are some elements of S, we denote the subring of S generated by R and $s_1, \ldots, s_n$ by $R[s_1, \ldots, s_n]$. Any element of $R[s_1, \ldots, s_n]$ can be written as a polynomial in $s_1, \ldots, s_n$ with coefficients in R (but not uniquely in general !). If $R[T_1, \ldots, T_n]$ is the polynomial ring with indeterminates $T_1, \ldots, T_n$, we get a natural surjective ring homomorphism $R[T_1, \ldots, T_n] \to R[s_1, \ldots, s_n]$ by replacing each T_i by s_i. The polynomials of the kernel I are called the *relations* among the $s_1, \ldots, s_n$.

A *graded algebra R over a field k*, is a ring R containing k together with a k-vector space decomposition $R = \sum_{i=0}^{\infty} R_i$, where $R_0 = k$, each R_i is finitely dimensional and ring multiplication induces a k-blinear map $R_i \times R_j \to R_{i+j} : r, s \mapsto rs$. Then $R_+ := \oplus_{i \geq 1} R_i$ is a maximal ideal. For example, let $R = k[X_1, \ldots, X_n]$ be the polynomial ring and R_i the collection of *homogeneous* polynomials of degree i, for the usual notion of degree and R_+ is the maximal ideal of polynomials with zero constant term. A module (or ideal) of R is called a *graded module*, if there is a k-vector space decomposition $M = \oplus_{i \in \mathbb{Z}} M_i$ such that multiplication induces a k-bilinear map $R_i \times M_j \to M_{i+j}$.

Example 3.1. Let $S := \mathbb{C}[X_1, \ldots, X_n]$ be a polynomial ring in n-variables with complex coefficients. By Hilbert's basis theorem S is a Noetherian ring. Let $\Gamma < S_n$ be a subgroup of order N of the group of all permutations of the n variables. Then Γ also acts on S by ring automorphisms. Write $R = S^{\Gamma}$ for the *invariant subring* of the polynomials fixed by all elements of Γ. *Hilbert's finiteness theorem* in this special case says that there are finitely many $f_1, \ldots, f_m \in S$ such that $R = \mathbb{C}[f_1, \ldots, f_m]$. The invariant ring is a graded algebra over $\mathbb{C}$, and the f_i can be chosen to be homogeneous polynomials.

To fix ideas, let $n = 3$ and $\Gamma :=< (123) >$. Then $b_1 = X_1 + X_2 + X_3, b_2 = X_1X_2 + X_2X_3 + X_3X_1, b_3 := X_1X_2X_3, b_4 = (X_1 - X_2)(X_2 - X_3)(X_3 - X_1)$ are invariant, and any invariant can be written as a polynomial in them. For example, $(X_1 - 2X_2)(X_2 - 2X_3)(X_3 - 2X_1) = b_1b_2 - 10b_3 + 3b_4$. We remark that b_1, b_2, b_3 and b_4 are not independent, there are relations among them, for example b_4^2 can be written as a polynomial in b_1, b_2, b_3 (can you find this polynomial?).

To prove this, consider the map $F : S \to R$ defined by $F(a) := \frac{1}{N} \sum_{\gamma \in \Gamma} \gamma(a)$. Then $F(ba) = bF(a)$ and $F(b) = b$ if $a \in S$ and $b \in R$. So by the proposition R is also Noetherian.

Let $R_+ \subset R$ be the ideal generated by all homogeneous elements of positive degree and let $b_1, \ldots, b_r$ be homogeneous generators of this (necessarily finitely generated) ideal. We want to show that any element of R can be written as a polynomial in $b_1, \ldots, b_r$ with coefficients in $\mathbb{C}$. i.e., an element of the subring $\mathbb{C}[b_1, \ldots, b_r]$. It suffices to prove $b \in \mathbb{C}[b_1, \ldots, b_r]$ for homogeneous elements $b \in B$. We shall use induction, starting with the trivial degree 0. Let $b \in R$ be homogeneous of degree d and suppose the result is true for smaller degrees. We can write $b = \sum_i r_i b_i$ where $r_i \in R$ is homogeneous of smaller degree than d. Hence, by induction, each $r_i \in R$ can be written as a polynomial in $b_1, \ldots, b_r$. Combining we see that b itself is in R.

Let R be a ring and M an R-module. If R is noetherian and M finitely generated, we get as a considerable bonus that all submodules of M are also finitely generated. A module M for any ring R is called *Noetherian* if every submodule is finitely generated.

Proposition 3.2. *Let R be a ring.*

(i) Let $N \subset M$ be a submodule. Then M is Noetherian if and only if both N and M/N are Noetherian.

(ii) If $M_1, \ldots, M_n$ are Noetherian modules, then also the direct sum $M_1 \oplus M_2 \oplus \ldots \oplus M_n$ is Noetherian.

(iii) R is Noetherian as a ring if and only if R is Noetherian as a module.

(iv) Let $I \lhd R$ be an ideal. If R is a Noetherian ring, then R/I is also a Noetherian ring.

(v) If R is Noetherian, then any finitely generated R-module is Noetherian.

Remark. The Noetherian property can be defined in a different way. We say that an R-module M satisfies the *ascending chain condition (ACC)* if every ascending chain of submodules

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \ldots \subseteq M_i \subseteq M_{i+1} \subseteq \ldots$$

becomes eventually stationary, i.e., there exists an n such that for all $i \geq 0$: $M_n = M_{n+i}$. We say that it satisfies the *maximality condition*, if every collection Ω of submodules of M has a maximal element (i.e., there exists an $N \in \omega$ that is not properly contained in any other element of Ω.

Proposition 3.3. *Let M be an R-module M. Then M is Noetherian if and only if it satisfies ACC if and only if it satisfies the maximality condition.*

We shall rarely use this proposition, but it points to the *dual* notion of an *Artinian module*, which is a module that satisfies the *descending chain condition (DCC)*: every descending chain of submodules

$$M_1 \supseteq M_2 \supseteq M_3 \supseteq \ldots \supseteq M_i \supseteq M_{i+1} \supseteq \ldots$$

becomes eventually stationary. Those modules need not be finitely generated, but nevertheless the condition is some sort of finiteness condition. They are important in duality theory, but probably will not play a role in this course.

A ring that satisfies DCC on ideals is called an *Artinian ring*. In contrast to the module case, the condition is a very strong finiteness condition: we shall show later that these rings are Noetherian and every prime ideal is necessarily a maximal ideal. We hope to discuss these rings later.

Département de mathématiques et de statistique, Université de Montréal, C.P. 6128, succursale Centre-ville, Montréal (Québec), Canada H3C 3J7

E-mail address: broera@DMS.UMontreal.CA