Orlando Marigliano Fall Term 2022

Commutative algebra and algebraic geometry – Supplementary material

Homomorphisms from a polynomial ring. Let A be a ring and $P = A[t_1, \dots, t_n]$ the polynomial ring in n variables over A. We have

- A ring homomorphism $u : A \to P$ (the obvious inclusion)
- A choice of n elements of P (the t_i)

with the following property:

> For all rings R, ring homomorphisms $v : A \to R$, and all choices of n elements $r_1, \dots, r_n$ of R, there exists a *unique* ring homomorphism $f : P \to R$ such that $f \circ u = v$ and $f(t_i) = r_i$ for all i.

This is called the 'universal property' of the polynomial ring in n variables over A, for the following reason. If any other ring P' with a ring homomorphism $u' : A \to P$ and a choice of n elements $t_i' \in P'$ satisfies the property above (with P', u' and t_i' instead of P, u, and t_i), then there exists a *unique* ring *isomorphism* $h : P \xrightarrow{\sim} P'$ such that $h \circ u = u'$ and $h(t_i) = t_i'$ for all i.

In other words, the above property characterizes the polynomial ring P up to unique isomorphism. The reason for this uniqueness is purely formal: given such a P', use the property of P to get a homomorphism $P \to P'$ and the property of P' to get a homomorphism $P' \to P$. From the *uniqueness* clause of the property of P, the composition $P \to P' \to P$ must be the identity. From the uniqueness clause of the property of P', the composition $P' \to P \to P'$ must be the identity. Thus the homomorphisms we found are mutually inverse, so isomorphisms.

As an example of how to use the universal property, let k be a field and suppose we want to define a ring homomorphism from $k[t_1, \dots, t_n]$ to some ring R. Then for this we just need to specify n elements of R and a ring homomorphism $k \to R$. In most cases, it will be clear what this homomorphism should be. For instance, if $R = k$ then take the identity, and if $R = A_x$ from the exercises, we could map $\lambda \in k$ to $\lambda/1$.

It is now time to prove the universal property for $P = A[t_1, \dots, t_n]$.

Proof. For an index tuple $I = (i_1, \dots, i_n)$ where $i_j \in \mathbb{Z}_{\geq 0}$, and a choice of n elements $r_1, \dots, r_n$ in an arbitrary ring R, we write r^I for the product $r_1^{i_1} \cdots r_n^{i_n}$. Thus every element of P can be written as a sum $\sum_I u(a_I) t^I$, where I ranges over all possible index tuples, $a_I \in A$, and all but a finite number of the $u(a_I)$ are zero. Now let $v : A \to R$ and $r_1, \dots, r_n$. If a ring homomorphism $f : P \to R$ is supposed to satisfy $f \circ u = v$ and $f(t_i) = r_i$, then setting for all $p = \sum_I u(a_I) t^I \in P$

$$f(p) = \sum_I f(u(a_I)) f(t^I) = \sum_I v(a_I) r^I$$

is our only choice. We see that by our definition, $f \circ u = v$ and $f(t_i) = r_i$. It remains to show that f is a homomorphism, but this I will leave to the reader. It follows from the fact that addition and multiplication of elements of R of the form $\sum_I b_I r^I$, where $b_I \in R$, mirrors precisely the addition and multiplication defined in the polynomial ring. □

On that last point, it may be good to recall the addition and multiplication in the polynomial ring: we have

$$\sum_I a_I t^I + \sum_I b_I t^I = \sum_I (a_I + b_I) t^I,$$
$$\Big(\sum_I a_I t^I\Big)\Big(\sum_I b_I t^I\Big) = \sum_I \Big(\sum_{J+K=I} a_J b_K\Big) t^I,$$

where the addition of index tuples is defined componentwise:

$$(j_1, \ldots, j_n) + (k_1, \ldots, k_n) = (j_1 + k_1, \ldots, j_n + k_n).$$

"Basic field theory." This section is to explain one step of the proof of Zariski's Lemma in Lecture 8. Field theory studies *field extensions*, which are inclusions of the form $K \subseteq L$, where K and L are fields. Such a field extension is often written L/K and L is said to be a field *over* K.

Given an extension L/K, an element $\alpha \in L$ is *algebraic* if there exists a polynomial $f \in K[t]$ such that $f(\alpha) = 0$.

If $\Sigma \subseteq L$ is any set of elements, then $K(\Sigma)$ denotes the smallest subfield of L that contains Σ. This is well-defined since the intersections of two subfields is again a field. In particular, if $\alpha_1, \ldots, \alpha_n \in L$ then $K(\alpha_1, \ldots, \alpha_n)$ is the smallest subfield containing all the α_i. Note already that $K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) = K(\alpha_1, \ldots, \alpha_n)$.

The field extension L/K is said to be

- *algebraic* if all elements $\alpha \in L$ are algebraic,
- *finitely-generated* if there exist $\alpha_1, \ldots, \alpha_n \in L$ such that $L = K(\alpha_1, \ldots, \alpha_n)$,
- *finite* if L is a finite-dimensional K-vector space.

Note that the extension L/K being finitely-generated is a very different condition from the field L being a finitely-generated K-algebra. The former says that every element of L can be written as a *rational expression* in the α_i with coefficient in K. The latter, that every element can be expressed as a *polynomial* in the α_i.

Being finite is a transitive condition: if $K \subseteq E \subseteq L$ are fields, E/K is finite, and L/E is finite, then L/K is finite. Indeed, if (x_i) is a K-basis of E and (y_j) is an E-basis of L, then $(x_i y_j)$ is a K-basis of L.

The first important fact about field extensions is the following: *Let L/K be a field extension. The following are equivalent:*

(1) L/K is finite.
(2) L/K is finitely-generated and algebraic.
(3) $L = K(\alpha_1, \ldots, \alpha_n)$ and the $\alpha_i \in L$ are algebraic.

Proof. (1) $\Rightarrow$ (2): Let L/K be finite. Then it is finitely generated. Now let $\alpha \in L$. Then there exists $n \in \mathbb{N}$ such that the $1, \alpha, \ldots, \alpha^n$ are linearly dependent over K. This gives a polynomial $f \in K[t]$ of degree n such that $f(\alpha) = 0$. Thus α is algebraic.

(2) $\Rightarrow$ (3): Clear.

(3) $\Rightarrow$ (1): Let $L = K(\alpha_1, \ldots, \alpha_n)$ with the $\alpha_i \in L$ algebraic. We proceed by induction on n. If $n = 1$ and $L = K(\alpha)$, let $\varphi := K[t] \to L$ be the ring homomorphism defined by

$t \mapsto \alpha$. Then $K[t]/\ker(\varphi) \simeq K[\alpha] \subseteq L$ is an integral domain, so $\ker(\varphi)$ is prime. Since α is algebraic, $\ker(\varphi)$ is nonzero. Since $K[t]$ is a principal ideal domain, $\ker(\varphi)$ is maximal. Thus $K[\alpha]$ is a field containing α, so $L = K[\alpha]$, and hence L is a finite-dimensional K-vector space, again since $\ker(\varphi) \neq 0$.

Now let $n > 1$ and $E \coloneqq K(\alpha_1, \ldots, \alpha_{n-1})$ Then $K \subseteq E \subseteq L$. By the induction assumption, E/K is finite and by the $n = 1$ case, L/E is finite. Thus L/K is finite. □

Now we can prove a statement that we need for Zariski's lemma: *If L/K is a finitely-generated field extension, then there exists a field $K \subseteq E \subseteq L$ such that E is isomorphic to the function field $K(t_1, \ldots, t_r)$ for some $r \geq 0$ and L/E is finite.*

Proof. Write $L = K(\alpha_1, \ldots, \alpha_n)$. We construct E step by step:
(1) Start with $E \coloneqq K$.
(2) For $i = 1, \ldots, n$: if α_i is not algebraic over E, then replace E by $E(\alpha_i)$.
(3) Rename the α_i so that $E = K(\alpha_1, \ldots, \alpha_r)$.

At the end of this algorithm, we have $L = E(\alpha_{r+1}, \ldots, \alpha_r)$ where $\alpha_{r+1}, \ldots, \alpha_n \notin E$, and by our construction the $\alpha_{r+1}, \ldots, \alpha_n$ are algebraic over E. Thus L is algebraic over E.

Moreover, $E \simeq K(t_1, \ldots, t_r)$, which we show by proving that $K[\alpha_1, \ldots, \alpha_r] \simeq K[t_1, \ldots, t_r]$. We have a surjective homomorphism $\varphi : K[t_1, \ldots, t_r] \to K[\alpha_1, \ldots, \alpha_r]$, and if f is a nonzero element of $\ker(\varphi)$, then f contains some variable t_i. Among these possible t_i, we can choose one such that α_i was added last in the algorithm, say for instance $i = r$. But then f shows that α_r is algebraic over $K(\alpha_1, \ldots, \alpha_{r-1})$, contradiction. □

Zariski's lemma's assumption is that L is even finitely generated as a K-algebra, so in particular L/K is a finitely generated as a field extension. Again, the former condition is much stronger: by Zariski's lemma itself, it implies for instance that we can take $E = K$ in the former statement.

Projective modules. This section is mostly relevant for the challenging exercises.

A sequence of A-modules and A-module homomorphisms of the form

$$\cdots \to M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \to \cdots$$

is *exact* if $\ker(f_{i+1}) = \operatorname{im}(f_i)$ for all i. A *short exact sequence* is an exact sequence

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0.$$

It says that f is injective, g surjective, and that $M'' \simeq M/M'$ via f and g.

Proposition: Let $0 \to N' \xrightarrow{u} N \xrightarrow{v} N''$ be an exact sequence of A-modules. Then for all A-modules M,

$$0 \to \operatorname{Hom}(M, N') \xrightarrow{u\circ -} \operatorname{Hom}(M, N) \xrightarrow{v\circ -} \operatorname{Hom}(M, N'')$$

is exact.

Proof: Since u is injective, so is $u \circ -$. Since $v \circ u = 0$, we have $v \circ (u \circ -) = 0$. Now let $\psi : M \to N$ with $v \circ \psi = 0$. Then $\mathrm{im}(\psi) \subseteq \ker(v) = \mathrm{im}(u)$, so $\psi = u \circ \psi'$ where ψ' is the composition $M \xrightarrow{\psi} \mathrm{im}(\psi) \subseteq \mathrm{im}(u) \xrightarrow{\sim} N'$. □

An A-module M is *projective* if for all exact sequences $0 \to N' \to N \to N'' \to 0$, the sequence

$$0 \to \mathrm{Hom}(M, N') \to \mathrm{Hom}(M, N) \to \mathrm{Hom}(M, N'') \to 0$$

is exact. This makes $\mathrm{Hom}(M, -)$ an *exact functor*.

Example: The A-module A is always projective. The $\mathbb{Z}$-module $\mathbb{Z}/(2)$ is not projective since the identity has no preimage under $\mathrm{Hom}(\mathbb{Z}/(2), \mathbb{Z}) \to \mathrm{Hom}(\mathbb{Z}/(2), \mathbb{Z}/(2))$.

Proposition: Let M be an A-module. The following are equivalent:
(1) M is projective;
(2) If $N \to N''$ is surjective then $\mathrm{Hom}(M, N) \to \mathrm{Hom}(M, N'')$ is surjective;
(3) There is an A-module P and a free A-module F such that $M \oplus P \simeq F$.

Proof: (1) ⇔ (2) by the previous proposition.

(2) ⇒ (3): Choose a free module F with a surjection $f : F \to M$. Let g be a preimage of id under $f \circ - : \mathrm{Hom}(M, F) \to \mathrm{Hom}(M, M)$, and let $P = \ker(f)$. Then $(f, \mathrm{id} - gf) : F \to M \oplus P$ is an isomorphism with inverse $(x, y) \mapsto g(x) + y$.

(3) ⇒ (2): Let $F = \bigoplus_{i \in I} Ae_i$ and $M \xrightarrow{i} F \xrightarrow{p} M$ the inclusion resp. projection maps. If $\varphi : N \to N''$ is surjective and $f : M \to N''$, construct $\tilde{g} : F \to N$ by mapping each e_i to any pre-image of $fp(e_i)$ under φ and define $g = \tilde{g}i$. Let $x \in M$ and write $i(x) = \sum_{i \in I} a_i e_i$ for some $a_i \in A$. Then

$$\varphi g(x) = \sum_{i \in I} a_i \varphi \tilde{g}(e_i) = \sum_{i \in I} a_i fp(e_i) = fpi(x) = f(x).$$

Example: Let $A = A_1 \times A_2$ be a product of nonzero rings. The ideals $\mathfrak{a}_1 = A_1 \times \{0\}$ and $\mathfrak{a}_2 = \{0\} \times A_2$ are A-modules with $\mathfrak{a}_1 \oplus \mathfrak{a}_2 = A$, so both are projective. But they are not free, for instance $\mathfrak{a}_1$ is annihilated by the nonzero element $(0, 1) \in A$, which does not happen in free modules.