Worksheet 16: Noether Normalization

Throughout, R, S, and T are commutative rings with unity, and k denotes a field. Recall the following definition, which was used when we investigated the notion of tensor products of algebras.

Definition. If S, T are R-algebras, then we call a map $\varphi : S \to T$ an *R-algebra homomorphism* if φ is a ring homomorphism that is also an R-module homomorphism. In other words, φ must preserve products and sums, and also satisfies $\varphi(rs) = r\varphi(s)$ for each $r \in R$ and $s \in S$ (note that multiplication often has different meanings on each side of this equation!)

1. **Warm-up: More on algebras**.
   (a) Suppose that S and T are R-algebras with structure maps $\alpha : R \to S$ and $\beta : R \to T$, respectively. Show that an R-algebra homomorphism $\varphi : S \to T$ is a ring homomorphism such that a certain diagram depending on α, β, and φ commutes.
   (b) Given a ring R, we may regard the polynomial ring $S = R[x_1, \ldots, x_n]$ as an R-algebra in the obvious way. Defining an R-algebra homomorphism from S to any other R-algebra T is equivalent to specifying n elements of T. Make this statement precise.[1]

   Hint: If $\varphi : S \to T$ is an R-algebra map, then where must $s \in S$ be sent? The variables?
   (c) Explain why the quotient of a finitely generated R-algebra S by an ideal I of S is again a finitely generated R-algebra. What is the structure homomorphism of S/I? What are the R-algebra generators of S/I in terms of the R-algebra generators of S?
   (d) Why is the structure map of a k-algebra injective? (Why is the structure map of an algebra not the zero map?) Conclude that a k-algebra is nothing more than a ring containing a copy of the field k. How does this simplify what it means to be a map of k-algebras? How do we define a k-algebra map from a polynomial ring over k?
   (e) Prove that S is a finitely-generated k-algebra if and only if for some integer $n \geq 0$ and some ideal I of the polynomial ring $\mathsf{k}[x_1, \ldots, x_n]$, there is a k-algebra isomorphism[2] $S \cong \mathsf{k}[x_1, \ldots, x_n]/I$.

   Hint: If S is algebra finite over k, fix n algebra generators and use them to construct a map from the polynomial ring to S.

Theorem (Noether Normalization)**.** *Let R be a finitely-generated k-algebra. Then there exists an integer $d \geq 0$ and elements $z_i \in R$, $1 \leq i \leq d$, that are algebraically independent over k, such that R is module finite over $A = \mathsf{k}[z_1, \ldots, z_d]$, the smallest subring of R containing k and the z_i.*

Definition. With the theorem's setup, the subring A is called a *Noether normalization* of R.

2. **Algebraic independence.** Let k be a field, and let R be a k-algebra. Informally, elements $z_1, \ldots, z_d$ of R are algebraically independent over k if they act as variables, as far as k is concerned. More precisely, $z_1, \ldots, z_d$ are algebraically independent over k if the only polynomial $f \in \mathsf{k}[x_1, \ldots, x_d]$ for which $f(z_1, \ldots, z_d) = 0$ is the zero polynomial.

[1] Compare this to the situation in linear algebra, where to define a linear transformation $T : V \to W$ from a finite dimensional vector space V, it suffices to describe what T does to a basis for V.

[2] You have just shown that any finitely-generated k-algebra must look like $\mathsf{k}[x_1, \ldots, x_n]/I$ for some ideal I. Though this might seem like a restrictive class of rings, it essentially encompasses every ring that appears in classical algebraic geometry (where it is even often assumed that $\mathsf{k} = \mathbb{C}$)! In fact, it is common to attend entire conferences/workshops/year-long seminars where every talk involves finitely generated algebras over a field, or modules over such rings, in an essential way.

For instance, if $\mathsf{k} = \mathbb{Q}$ and $R = \mathbb{R}$, then $\pi \in R$ is algebraically independent over k, but $\sqrt{2} \in R$ is not. Similarly, if $R = \mathsf{k}[x, y]$, then $x, x + y$ and $x + y, x - y$ are both algebraically independent over k, but $x + y, x^2 + y^2 + 2xy - x - y$ are not.

For elements $z_1, \ldots, z_d$ of a k-algebra R, show that the following are equivalent.

(a) $z_1, \ldots, z_d$ are algebraically independent over k.

(b) The k-algebra homomorphism $\mathsf{k}[x_1, \ldots, x_d] \to R$ given by $x_i \mapsto z_i$ is injective, and hence induces a k-algebra isomorphism from $\mathsf{k}[x_1, \ldots, x_d]$ to the subring $A = \mathsf{k}[z_1, \ldots, z_d] \subseteq R$.

(c) The collection of all monomials $z^{\mathbf{a}} = z_1^{a_1} \ldots z_d^{a_d} \in R$ with $\mathbf{a} = (a_1, \ldots, a_d) \in \mathbb{N}^d$ is *linearly* independent over the field k.

3. **Uniqueness properties of Noether normalizations.** As you will see in #5, a given finitely generated k-algebra R usually has more than one distinct Noether normalization; that is, there exist $z_1, \ldots, z_d \in R$ and $w_1, \ldots, w_e \in R$ satisfying the following conditions.

   - Each of $z_1, \ldots, z_d$ and $w_1, \ldots, w_e$ are algebraically independent over k.
   - The subrings $A = \mathsf{k}[z_1, \ldots, z_d]$ and $B = \mathsf{k}[w_1, \ldots, w_e]$ of R satisfy $A \neq B$.
   - Nevertheless, both extensions $A \subseteq R$ and $B \subseteq R$ are module finite.

   Explain why, in this context, we at least must have that $d = e$. Your arguments may use the formula (which we conjectured, but must still prove in the next worksheet) for the dimension of a polynomial ring over a field. *Hint*: Use Lying Over. Use dim corollary?

4. **Finding Noether normalizations.** Describe two Noether Normalizations $A \neq B$ of each finitely generated $\mathbb{Q}$-algebra R below. Justify that the extensions $A \subseteq R$ and $B \subseteq R$ are module finite by identifying generators.

   (a) $R = \mathbb{Q}[x, y, z]$. As one of A and B, find the simplest *proper* Noether normalization.

   (b) $R = \mathbb{Q}[x, y, z]/\langle z^2 - xy \rangle$.

   (c) $R = \mathbb{Q}[x, y]/\langle xy \rangle$. *Hint*: Apply a simple change of coordinates to $\mathbb{Q}[x, y]$.

   The following is called Zariski's lemma?

5. **Consequence: Algebra-finite field extensions are finite dimensional vector spaces.** Recall that we have shown that "module finite = algebra finite + integral" for ring extensions. You will now prove that "module finite = algebra finite" for field extensions: Suppose that $\mathsf{k} \hookrightarrow \mathbb{L}$ is an extension of fields, and that $\mathbb{L}$ is a finitely generated as a k-algebra (e.g., think of $\mathbb{R} \subseteq \mathbb{C}$). Prove that $[\mathbb{L} : \mathsf{k}]$ must be finite (i.e., $\mathbb{L}$ is a finite dimensional k-vector space).

   Hint: In a previous worksheet, we proved that the dimension of a polynomial ring over k in n variables is at least n. What does this tell us about how many "variables" can appear in a Noether Normalization for the field extension $\mathsf{k} \subseteq \mathbb{L}$?

6. **Consequence: The inverse image of a maximal ideal.** We know that the inverse image, under a ring map, of a prime ideal must also be prime. Here, we investigate the situation for maximal ideals. Consider a map of rings $\varphi : R \to S$, and fix a maximal ideal $\mathfrak{n}$ of S.

   (a) Illustrate, via example, that $\varphi^{-1}(\mathfrak{n})$ need not be a maximal ideal of R.

   (b) On the other hand, prove that if R, S are finitely-generated k-algebras, and $\varphi : R \to S$ is a k-algebra map, then $\varphi^{-1}(\mathfrak{n})$ is a maximal ideal of R.

Hint: Explain why there is a sequence of inclusions $\mathsf{k} \hookrightarrow R/\varphi^{-1}(\mathfrak{n}) \hookrightarrow S/\mathfrak{n}$. According to the warm-up, each of these rings is a finitely generated k-algebra. Problem #5 and the composition $\mathsf{k} \hookrightarrow S/\mathfrak{n}$ imply that $S/\mathfrak{n}$ is a finite dimensional vector space over k, and hence so is $R/\varphi^{-1}(\mathfrak{n})$. In other words, $\mathsf{k} \hookrightarrow R/\varphi^{-1}(\mathfrak{n})$ is a module finite extension. What does Lying Over tell us about the Krull dimension of $R/\varphi^{-1}(\mathfrak{n})$? But isn't $R/\varphi^{-1}(\mathfrak{n})$ a domain? Why do the answers to these questions force this ring to be a field?

Theorem (Hilbert's Nullstellensatz[3])**.** *If* k *is an algebraically closed field, then every maximal ideal* $\mathfrak{m}$ *of* $\mathsf{k}[x_1, \ldots, x_n]$ *has the form* $\mathfrak{m} = \langle x_1 - \alpha_1, \ldots, x_n - \alpha_n \rangle$ *for some* $\alpha_1, \ldots, \alpha_n \in \mathsf{k}$.

7. **Consequence: Hilbert's Nullstellensatz.**

(a) Prove that every ideal $\mathfrak{m}$ of the above form must be maximal, whether k is algebraically closed or not. Conclude that the Nullstellensatz provides a complete description of all the maximal ideals in $\mathsf{k}[x_1, \ldots, x_n]$ when k is algebraically closed.

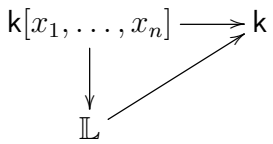
Hint: Consider the k-algebra map $\mathsf{k}[x_1, \ldots, x_n] \to \mathsf{k}$ defined by $x_i \mapsto \alpha_i$ for all i.

(b) Illustrate via example that the Nullstellensatz fails if we remove the hypothesis that $\mathsf{k} = \overline{\mathsf{k}}$.

(c) We now prove the Nullstellensatz: Suppose k is algebraically closed, and let $\mathfrak{m}$ be a maximal ideal of $R = \mathsf{k}[x_1, \ldots, x_n]$. The warm-up tells us that $\mathbb{L} := \mathsf{k}[x_1, \ldots, x_n]/\mathfrak{m}$ is a finitely-generated k-algebra, and maximality of $\mathfrak{m}$ implies that $\mathbb{L}$ is also a field.

i. Consider the sequence $\mathsf{k} \hookrightarrow R \to R/\mathfrak{m} = \mathbb{L}$, and explain why the composition $\mathsf{k} \hookrightarrow \mathbb{L}$ must be an isomorphism. *Hint*: Consider an earlier consequence, and use the fact that $\mathsf{k} = \overline{\mathsf{k}}$.

ii. Let $\alpha_i \in \mathsf{k}$ be the elements that correspond to $\overline{x_i} \in \mathbb{L}$ under this isomorphism, and let $\varphi : \mathsf{k}[x_1, \ldots, x_n] \to \mathsf{k}$ be the k-algebra map defined by $x_i \mapsto \alpha_i$. Verify that



commutes, where the horizontal map is φ, the vertical map is the quotient map, and the diagonal map is the inverse of the isomorphism $\mathsf{k} \hookrightarrow \mathbb{L}$.

iii. Use this diagram to explain why the ideals $\langle x_1 - \alpha_1, \ldots, x_n - \alpha_n \rangle$ and $\mathfrak{m}$ both lie in $\ker \varphi$. Conclude your proof by explaining why this forces these ideals to be equal.

iv. **Nullstellen-what?** From German, *Nullstellensatz* translates to *zero-locus-theorem*. Prove the following corollary, which explains the name: Suppose that I is an ideal of $\mathsf{k}[x_1, \ldots, x_n]$, where $\mathsf{k} = \overline{\mathsf{k}}$. Then I is proper if and only if the polynomials in I have a common zero, i.e., there exists $\mathbf{a} \in \mathsf{k}^n$ for which $f(\mathbf{a}) = 0$ for every $f \in I$.

Lemma. *Let* S *be a polynomial ring over* k *in some fixed variables, and fix a nonzero polynomial* $f \in S$. *Given a variable* x*, there exists a* change of variables*–i.e., an* k*-algebra automorphism of* S*–that fixes* x*, and transforms* f *into a nonzero* k*-multiple of a* monic *polynomial in* x *with coefficients in the polynomial ring over* k *generated by the other variables.*

Example. Consider $f = xy \in \mathsf{k}[x, y]$, which neither monic in x nor in y. However, after applying the change of variables given by $x \mapsto x$ and $y \mapsto x + y$, $f \mapsto x(x + y) = x^2 + xy$, which is

[3]This version of the theorem is sometimes called the "weak form" of Nullstellensatz; the full version gives a strong correspondence between algebra and geometry. You will get a taste of this in the last part of following problem.

monic in $S = T[x]$, with $T = \mathsf{k}[y]$. Similarly, if we instead send $x \mapsto x + y$ and $y \mapsto y$, then $f \mapsto (x+y)y = xy + y^2$, which is monic in y when we consider its coefficients to be in $\mathsf{k}[x]$.

8. **Proving the lemma.** Given a nonzero $f \in S = \mathsf{k}[x_0, x_1, \ldots, x_n]$, to prove the lemma, we seek to define an automorphism $S \to S$ of k-algebras such that $x_0 \mapsto x_0$ and

$$f \mapsto c(x_0^m + q_1 x_0^{m-1} + \cdots + q_{m-1}x_0 + q_m) \qquad (\clubsuit)$$

where $c \in \mathsf{k}$ is nonzero, m is a natural number, and each $q_i = q_i(x_1, \ldots, x_n) \in \mathsf{k}[x_1, \ldots, x_n]$.

   (a) Fix $g_1, \ldots, g_n \in \mathsf{k}[x_0]$, and consider the k-algebra map $\mathsf{k}[x_0, \ldots, x_n] \to \mathsf{k}[x_0, \ldots, x_n]$ given by $x_0 \mapsto x_0$ and $x_i \mapsto x_i + g_i$ for each $i \neq 0$. Explain why this is an k-algebra automorphism by briefly describing an inverse map that is also an k-algebra map.

   (b) Fix an integer $b > 0$, and consider the k-algebra automorphism ψ_b of S defined by

$$x_i \mapsto \begin{cases} x_0 & i = 0 \\ x_i + x_0^{b^i} & i \neq 0 \end{cases}$$

   With this change of variables, explain why ($\clubsuit$) holds when $f = cx_0^{a_0}x_1^{a_1}\cdots x_n^{a_n}$, where $c \in \mathsf{k}^*$.
   Hint: The m value in this case should be $m = a_0 + a_1 b + \cdots + a_n b^n$.

   (c) Now take an arbitrary nonzero $f \in S$, and fix an integer b larger than any exponent appearing in any supporting monomial of f. Explain why ψ_b satisfies ($\clubsuit$).
   Hint: Express f as the finite sum of terms of the form $c_{\mathbf{a}}x^{\mathbf{a}} := c_{\mathbf{a}}x_0^{a_0}\cdots x_n^{a_n}$, where $\mathbf{a} = (a_0, a_1, \ldots, a_n) \in \mathbb{N}^{n+1}$. Where does ψ_b send f? Finally, recall that every nonnegative integer has a unique base b expansion. Where does the choice of large b come into play?

9. **Proof of Noether Normalization.** Fix R be a finitely-generated k algebra. We will now prove[4] Noether Normalization by inducing on the number of generators of R over A.

   (a) Explain why the base case $n = 0$ is trivial.

   (b) Consider our inductive hypothesis: Suppose $g_0, \ldots, g_n$ are k-algebra generators for R, and that Noether Normalization holds for all k-algebras generated by fewer elements. Explain why the inductive step is trivial if $g_0, \ldots, g_n$ are algebraically independent over k.

   (c) Otherwise, there is some polynomial $F \in \mathsf{k}[x_0, \ldots, x_n]$ such that $F(g_0, \ldots, g_n) = 0$. Fix $b \in \mathbb{N}$ greater than any exponent appearing in F, and set $h_0 = g_0$ and $h_i = g_i + g_0^{b^i}$ for each $i \neq 0$. Explain why $A = \mathsf{k}[g_0, g_1, \ldots, g_n]$ and $B = \mathsf{k}[h_0, h_1, \ldots, h_n]$ both equal R.
   Hint: $A = R$ by our inductive hypothesis. To see that $A \subseteq B$, why does it suffice to show that $g_i \in B$ for all i?

   (d) Use the k-algebra automorphism ψ_b from #8 to explain why $F(g_0, \ldots, g_n) = 0$ in R can be expressed in terms of $h_0, \ldots, h_n$ as $c(h_0^m + a_1 h_0^{m-1} + \cdots + a_{m-1}h_0 + a_m) = 0$ where $c \in \mathsf{k}^*$ and each $a_i \in D = \mathsf{k}[h_1, \ldots, h_n]$.

   (e) Conclude that h_0 is integral over $D = \mathsf{k}[h_1, \ldots, h_n]$, and so $R = B$ is module finite over D. Finally, apply the inductive hypothesis to the finitely generated k-algebra D to conclude that there is a Noether normalization $N \subseteq D$ for D. But if $N \subseteq D$ is module finite and $D \subseteq A$ is module finite, then isn't the composition of module finite extensions module finite? Conclude that N is a Noether normalization of R!

[4] At this point, based on everything that follows from it, you should be left with the impression that Noether Normalization is important, and it is. Even better, its proof isn't too complicated!