SOME THOUGHTS ON FINITE EXTENSIONS OF RINGS

OTHERS AND MATTHIAS ZACH

Abstract. Dah.

We are considering complex analytic maps $f\colon (\mathbb{C}^n,0) \to (\mathbb{C}^p,0)$ which are *finite*. In particular, we may assume $n \geq p$. By definition, f is finite if and only if its pullback $\varphi\colon \mathcal{O}_p \to \mathcal{O}_n$ is a finite extension of rings, i.e. $\mathcal{O}_n = \mathbb{C}\{x_1,\dots,x_n\}$ is a finite $\mathcal{O}_p = \mathbb{C}\{y_1,\dots,y_p\}$-module via φ.

Definition 0.1. Let $\varphi\colon R \to S$ be a morphism of commutative rings with unit. An element $x \in S$ is called *integral* over R if there exists a *monic* polynomial

$$P = X^r + c_{r-1}\cdot X^{r-1} + \cdots + c_1 \cdot X + c_0 \in R[X]$$

such that $P(x) = 0$ in S.

Proposition 0.2. Let $\varphi\colon R \to S$ be a morphism of commutative, Noetherian rings with unit. The set of elements in S which are integral over R is a subalgebra of S. Moreover, S is finite over R if and only if S is generated as an R-algebra by finitely many integral elements.

For a proof see [1, Theorem 4.2 and Corollary 4.5].

For complex analytic mappings f as above, we are working with rings of convergent power series in several variables. In practice, however, we will mostly encounter maps which admit a *polynomial representative*

$$f\colon \mathbb{C}^n \to \mathbb{C}^p, \quad (x_1,\dots,x_n) \mapsto (y_1,\dots,y_p) = (f_1(x),\dots,f_p(x)), \quad f_j(x) \in \mathbb{C}[x_1,\dots,x_n].$$

It seems to be no significant restriction for practical applications to assume that also this polynomial representative is actually finite. For finite extensions of polynomial rings we do have algorithmic methods to compute with the structure of S as an R-module.

Proposition 0.3. Let $\varphi\colon \mathbb{C}[y] \to \mathbb{C}[x]$ be a mapping of polynomial rings given by $y_j \mapsto f_j(x_1,\dots,x_n)$. Let

$$J = \langle y_j - f_j(x) : j = 1,\dots,p\rangle \subset \mathbb{C}[y,x]$$

and LJ the *leading ideal* of J with respect to a monomial ordering which is an elimination ordering on the x-variables. Then φ is finite if and only if $\langle x_1,\dots,x_n\rangle^N \subset LJ$ for some $N \in \mathbb{N}$. In this case, the set of monomials $\{x^\alpha : \alpha \in \mathbb{N}^n,\, x^\alpha \notin LI\}$ are a generating set for $\mathbb{C}[x]$ as a $\mathbb{C}[y]$-module.

TODO: Find a reference for the proof.

Based on this result we can implement seamless transitions for elements $h \in S$ between their representation as polynomials $h \in \mathbb{C}[x]$ and module elements $v \in R\cdot e_1 + \cdots + R\cdot e_m$ with respect to a chosen system of generators over R.

Working with power series in computer algebra is an almost impossible undertaking beyond simple arithmetic. Recall that in general it must be deemed impossible to even decide equality of two given power series. Thus, the naive hope at this point would be that *localizing* at the origins of the domain and codomain of f, respectively, would bring us sufficiently close to working with power series by restricting ourselves to those which are in fact *rational functions*.

Proposition 0.4. Let $\varphi\colon R \to S$ be a finite extension of commutative Noetherian rings with unit. Let $P \subset R$ be a prime ideal and $Q \subset S$ prime with $\varphi^{-1}(Q) = P$ (i.e. Q is a *prime over* P). Then the naturally induced morphism on the localizations

$$\phi\colon R_P \to S_Q$$

is finite if and only if Q is the only prime in S with that property.

Proof. According to Proposition 0.2, we have finiteness of ϕ if and only if an arbitrary element $\frac{a}{b} \in S_Q$ is integral over R_P. Now by assumption both a and b are integral over R and hence over R_P and since $\frac{a}{b} = a\cdot\frac{1}{b}$ it suffices to consider elements of the form $\frac{1}{b}$ for $b \notin Q$.

Suppose we found a monic polynomial

$$F = X^r + c_{r-1}\cdot X^{r-1} + \cdots + c_1\cdot X^1 + c_0 \in R_P[X]$$

with $F\left(\frac{1}{b}\right) = 0$ in S_Q. Then we can clear denominators to obtain

$$F' = c'_r\cdot X^r + c'_{r-1}\cdot X^{r-1} + \cdots + c'_1\cdot X^1 + c'_0 \in R[X]$$

with $F'\left(\frac{1}{b}\right) = 0$ and $c'_r \notin P$. But then, by definition of localization at Q,

$$u \cdot \left(c'_r + c'_{r-1} \cdot b + \cdots + c'_1 \cdot b^{r-1} + c'_0 \cdot b^r\right) = 0$$

in S for some $u \notin Q$. This expression can be split as

$$-u \cdot c'_r = u \cdot b \cdot \left(c'_{r-1} + c'_{r-2} \cdot b + \cdots + c'_1 \cdot b^{r-2} + c'_0 \cdot b^{r-1}\right). \tag{1}$$

Now suppose $Q' \neq Q$ was another prime with $\varphi^{-1}(Q') = P = \varphi^{-1}(Q)$. Choosing $b \in Q' \setminus Q$ leads to a contradiction in (1): Clearly, the right hand side, containing b as a factor, is an element in Q'. Comparing with the left hand side, we find that $c'_r \notin P = \varphi^{-1}(Q) = \varphi^{-1}(Q')$ and, hence, $\varphi(c'_r) \in S$ is neither an element of Q, nor of Q'. This leaves us with $u \in Q'$.

To arrive at a contradiction, let

$$\operatorname{ord}_{Q'} \colon S \to \mathbb{N}_0, \quad a \mapsto \max\left\{k \in \mathbb{N}_0 : a \in Q'^{(k)}\right\}$$

where $Q'^{(k)}$ denotes the k-th *symbolic power*, i.e. the preimage of $\left(Q'_{Q'}\right)^k$ in S under the localization map $S \to S_{Q'}$. The map $\operatorname{ord}_{Q'}$ is a *valuation* and it is now easy to see that the valuation of the left hand side of (1) is strictly less than the valuation of the right hand side.

TODO: Find an argument to prove the converse.

□

Example 0.5. Consider the map

$$f \colon \mathbb{C} \to \mathbb{C}, \quad x \mapsto y = x - x^3.$$

Clearly, $\varphi \colon \mathbb{C}[y] \to \mathbb{C}[x]$ is finite and, in fact, $\mathbb{C}[x]$ is a free $\mathbb{C}[y]$-module with generating set $1, x, x^2$.

For the analytification of this map $f \colon (\mathbb{C}, 0) \to (\mathbb{C}, 0)$ the implicit function theorem yields that there exists a local inverse

$$y = x - x^3, \quad x = y + \sum_{k=2}^{\infty} c_k \cdot y^k \in \mathbb{C}\{y\}$$

as a convergent power series in y. Therefore $\varphi^h \colon \mathbb{C}\{y\} \to \mathbb{C}\{x\}$ is in fact an *isomorphism* and $\mathbb{C}\{x\}$ is generated as a $\mathbb{C}\{y\}$-module by the unit element $1 \in \mathbb{C}\{x\}$.

Thus we find a discrepancy of $3 - 1 = 2$ in the ranks of the two modules over the respective rings. One could hope that the localization

$$\phi \colon \mathbb{C}[y]_{\langle y \rangle} \to \mathbb{C}[x]_{\langle x \rangle}$$

provides us with a reasonable approximation to φ^h, but Proposition 0.4 tells us that the elements

$$M_p = \left\langle \left(\frac{1}{1-x}\right)^k : k \leq p \right\rangle_{\mathbb{C}[y]_{\langle y \rangle}}$$

form an infinite, ever increasing sequence of $\mathbb{C}[y]_{\langle y \rangle}$-submodules of $\mathbb{C}[x]_{\langle x \rangle}$ and that, hence, $\mathbb{C}[x]_{\langle x \rangle}$ does not have a finite $\mathbb{C}[y]_{\langle y \rangle}$-module structure.

References

[1] D. Eisenbud. Commutative Algebra with a View Toward Algebraic Geometry. Springer-Verlag New York, 1995.

Other authors...

Matthias Zach: RPTU Kaiserslautern-Landau, 67663 Kaiserslautern, Germany