Differentiation and Division

Rohan Hitchcock

8 September 2022

Let k be a commutative ring and R a k-algebra (soon we will assume k is a field of characteristic zero and R is a polynomial ring). Let $t = (t_1, \cdots, t_n)$ be a sequence of elements in R

Last talk we constructed a strong deformation retract involving the Koszul complex of t. This relied on the existence of certain k-linear maps $\partial_{t_1}, \dots, \partial_{t_n} : R \to R$, which together we referred to as a *system of t-derivatives*. In this talk we will show that such maps exist under certain assumptions on t, and that they can be computed algorithmically. Recall that a system of t-derivatives is defined as follows. Let $k[t]$ denote the k-algebra generated by $1, t_1, \dots, t_n$.

Definition 1. Given $t = (t_1, \dots, t_n)$, *system of t-derivatives* are k-linear maps $\partial_{t_i} : R \to R$, $i = 1, \dots, n$ which satisfy the following properties:

(1) Every $f \in R$ can be written uniquely in the form
$$f = \sum_{u \in \mathbb{N}^n} r_u t^u$$
where each $r_u \in \bigcap_i \ker(\partial_{t_i})$ and finitely many $r_u \neq 0$.

(2) $\partial_{t_i}(t^v) = v_i t^{v - e_i}$ for all $v \in \mathbb{N}^n$ (where we understand that $0 t_j^{-1} = 0$).

(3) For $f \in k[t]$ and $r \in \bigcap_i \ker(\partial_{t_i})$ we have $\partial_{t_i}(rf) = r\partial_{t_i}(f)$.

Now suppose that $R = k[x] = k[x_1, \dots, x_m]$. When $n = m$ and $t = x = (x_1, \dots, x_n)$ our construction will recover the usual partial derivative maps $\frac{\partial}{\partial x_1}, \dots, \frac{\partial}{\partial x_n}$. In other words our goal is the generalise the notion of taking partial derivatives with respect to the sequence $x = (x_1, \dots, x_n)$ to taking partial derivatives with respect to other sequences in $k[x]$.

This generalisation is motivated by the observation that taking derivatives of polynomials is related to polynomial division. Consider the one variable case $k[x] = k[x_1]$ and let $f \in k[x]$. For another formal variable y one can show that in the polynomial ring $k[x, y]$ we have
$$f(x) = \sum_{p=1}^{\infty} \frac{1}{p!} f^{(p)}(y)(x - y)^p$$
analogously to the analytic Taylor's Theorem, where $f^{(p)} = \frac{d^p}{dx^p}(f)$ is the p^{th} partial derivative of f. Notice that the right-hand-side is a polynomial since eventually $f^{(m)} = 0$. Rearranging this we have
$$f(x) - f(y) = f'(y)(x - y) + (x - y)^2 \sum_{p=2}^{\infty} \frac{1}{p!} f^{(p)}(y)(x - y)^{p-2}$$
or in other words, $f'(y)$ is the remainder of $f(x) - f(y)$ divided by $(x - y)^2$. A similar result can be shown in the multivariate case.

1 Iterated Euclidean division

Our first task is to prove a corollary of the division algorithm in $k[x]$. Let k be a field. We begin by recalling some concepts related to polynomial division in the multivariate polynomial ring $k[x]$ following the conventions of [CLO15, Chapter 2]. A *monomial* in $k[x]$ is any polynomial in the set $\{x^u\}_{u\in\mathbb{N}^n}$. A *monomial ordering* on $k[x]$ is a well-founded, total order relation $<$ on $\mathbb{N}^n$ with the property that $u < v \implies u+w < v+w$. A typical example of a monomial ordering is the lexicographic ordering on $\mathbb{N}^n$, and others are given in [CLO15, Section 2.2].

Let $f = \sum_{u\in\mathbb{N}^n} c_u x^u \in k[x]$ where $c_u \in k$ and finitely many $c_u \neq 0$. Any $c_u x^u$ for which $c_u \neq 0$ is called a *term* of f. Given a monomial ordering on $k[x]$, if $f \neq 0$ we define the *multi-degree* of f as

$$\operatorname{multideg}(f) = \max\{u \in \mathbb{N}^n \mid c_u \neq 0\}$$

where the maximum is taken with respect to the monomial ordering. Setting $u^* = \operatorname{multideg}(f)$ we define the *leading term* of f with respect to the given monomial ordering to be $\operatorname{LT}(f) = c_{u^*}x^{u^*}$. The coefficient c_{u^*} is called the *leading coefficient* and is denoted $\operatorname{LC}(f)$. Consider the division algorithm on $k[x]$ given in [CLO15, Theorem 2.3.3]. We recall its properties:

Theorem 2 (Division Algorithm)**.** *Let $f, g_1, \ldots, g_m \in k[x]$ and suppose we have a monomial ordering on $k[x]$ for which $\operatorname{LC}(g_1), \ldots, \operatorname{LC}(g_m)$ are invertible in k. Given such a monomial ordering the division algorithm produces $r, q_1, \ldots, q_m \in k[x]$ which satisfy*

(1)

$$f = r + \sum_{i=1}^{m} q_i g_i$$

(2) None of the terms of r are divisible by any of the $\operatorname{LT}(g_i)$, $i = 1, \ldots, m$.

(3) For all $i = 1, \ldots, m$ with $q_i \neq 0$ we have $\operatorname{multideg}(f) \geq \operatorname{multideg}(q_i g_i)$.

In [CLO15] the division algorithm theorem is stated under the assumption that k is a field, but by inspecting the algorithm and proof given in [CLO15] one can observe that this hypothesis is only needed so the $\operatorname{LC}(g_i)$ can be inverted.

We show that the division algorithm can be iterated to "completely divide" the coefficients of the divisors $g_1, \ldots, g_m$ of Theorem 2. The properties of this iterated division algorithm are stated and proved in Theorem 3 and the algorithm itself is given in Algorithm 1.0.4.

Theorem 3. *Let $f \in k[x]$ be a polynomial and $g_1, \ldots, g_m \in k[x]$ be non-constant polynomials. Suppose we have a monomial ordering on $k[x]$ such that $\operatorname{LC}(g_1), \ldots, \operatorname{LC}(g_m)$ are invertible in k. Given this monomial ordering,* ITERATEDDIVISION$(f, g_1, \ldots, g_m)$ *in Algorithm 1.0.4 computes an expression of the form*

$$f = \sum_{u\in\mathbb{N}^n} r_u g^u$$

where $g^u = g_1^{u_1} \cdots g_m^{u_m}$, all but finitely many of the $r_u = 0$ and for each $r_u \neq 0$, all terms of r_u are not divisible by any of the $\operatorname{LT}(g_i)$, $i = 1, \ldots, m$.

Proof. Let R_N and Q_N be the values of R and Q respectively in Algorithm 1.0.4 at the end of the N^{th} repetition of the loop on line 4, where we start counting from $N = 0$. Let $i(Q_N)$ and $i(R_N)$ be the indices arising in Q_N and R_N respectively, so $u \in i(Q_N)$ if and only if $(u, q) \in Q_N$ for some $q \in k[x]$ and likewise for $i(R_N)$.

We begin by showing that if the algorithm terminates then we obtain an expression of the stated form. First note that every index $u \in \mathbb{N}^n$ appears in Q_N and R_N at most once. That is, $|i(Q_N)| = |Q_N|$ and $|i(R_N)| = |R_N|$. Hence we can define

$$r_{u,N} = \begin{cases} 0 & u \notin i(R_N) \\ r & \text{where } (u, r) \in R_N \end{cases} \qquad \text{and} \qquad q_{u,N} = \begin{cases} 0 & u \notin i(Q_N) \\ q & \text{where } (u, q) \in Q_N \end{cases}$$

We aim to show that for all N we have

$$f = \sum_{u \in \mathbb{N}^m} r_{u,N} g^u + \sum_{u \in \mathbb{N}^m} q_{u,N} g^u$$

where $g^u = g_1^{u_1} \cdots g_m^{u_m}$. We proceed by induction on N. The base case is clear if we define R_{-1} and Q_{-1} to be the initial values of R and Q defined prior to line 4. Now consider the inductive case. For $u \in \mathbb{N}^m$ let $|u| = \sum_{i=1}^m u_i$. Note that if $r_{u,N-1} \neq 0$ then $|u| \leq N - 1$ and if $q_{u,N-1} \neq 0$ then $|u| \geq N$. We also have that if $r_{u,N-1} \neq 0$ then $r_{u,N} = r_{u,N-1}$ since we do not remove elements from R. Then we have

$$\begin{aligned} f &= \sum_{u:|u|<N} r_{u,N-1} g^u + \sum_{u:|u|\geq N} q_{u,N-1} g^u \\ &= \sum_{u:|u|<N} r_{u,N} g^u + \sum_{u:|u|\geq N} \left(r_{u,N} + \sum_{i=1}^m p_{u,i} g_i \right) g^u \\ &= \sum_u r_{u,N} g^u + \sum_u \sum_{i=1}^n p_{u,i} g^{u+e_i} \\ &= \sum_u r_{u,N} g^u + \sum_u q_{u,N} g^u \end{aligned}$$

where $p_{u,1}, \ldots, p_{u,m}$ are obtained by applying the division algorithm to $q_{u,N-1}$ as on line 7. Since the algorithm terminates when $Q = \emptyset$ and all $r_u \neq 0$ satisfy the required property this proves we have an expression of the desired form on termination.

It remains to prove that the algorithm terminates. We abuse notation and write $q \in Q_N$ to mean $(u, q) \in Q_N$ for some $u \in \mathbb{N}^m$. Now define

$$b_N = \max\{\text{multideg}(q) \mid q \in Q_N\}$$

where the maximum is taken with respect to the chosen monomial ordering. Consider $q \in Q_{N-1}$ and let $p_1, \ldots, p_m$ be the polynomials computed from q on line 7. By Theorem 2 we have that $\text{multideg}(q) \geq \text{multideg}(p_i g_i)$. By hypothesis g_i is not a constant polynomial so this implies $\text{multideg}(q) > \text{multideg}(p_i)$ and in particular $b_{N-1} > \text{multideg}(p_i)$. Now, the elements of Q_N consist of sums of the various $p_1, \ldots, p_m$ generated on line 7. Since for any $s + t \neq 0$ we have $\text{multideg}(s + t) \leq \max\{\text{multideg}(s), \text{multideg}(t)\}$ [CLO15, Lemma 2.2.8] it follows that for any $q' \in Q_N$ that $\text{multideg}(q') < b_{N-1}$. Therefore $b_N < b_{N-1}$ and since monomial orderings are well-founded the algorithm terminates. $\square$

Algorithm 1.0.4 Iterated Division Algorithm

Require: A polynomial $f \in k[x]$, non-constant polynomials $g_1, \ldots, g_m \in k[x]$, and a monomial ordering on $k[x]$ such that $\mathrm{LC}(g_1), \ldots, \mathrm{LC}(g_m)$ are invertible in k.

```
procedure iteratedDivision(f, g_1, ..., g_m)
    Q ← {(0⃗, f)}                                  ▷ 0⃗ = (0, ..., 0) ∈ ℕ^m
    R ← ∅
    while Q ≠ ∅ do
        Q_new ← ∅
        for all (u, q) ∈ Q do
            Apply the division algorithm to obtain r, p_1, ..., p_m ∈ k[x] satisfying
                q = r + Σ_{i=1}^{m} p_i g_i
            along with the other conditions in Theorem 2.
            Q_new ← Q_new ∪ {(u + e_i, p_i) | i = 1, ..., m where p_i ≠ 0}
            R ← {(u, r)} ∪ R
        Q ← collectTerms(Q_new)
    return R
function collectTerms(Q)
    Q_collected ← ∅
    for all u where (u, p) ∈ Q for some p do
        Let p_1, ..., p_s be all the polynomials such that (u, p_i) ∈ Q
        if Σ_{i=1}^{s} p_i ≠ 0 then
            Q_collected ← {(u, Σ_{i=1}^{s} p_i)} ∪ Q_collected
    return Q_collected
```

2 Differentiating with respect to a sequence of polynomials

Fix a monomial ordering $>_x$ on $k[x]$. We extend this to a monomial ordering on $k[x,y] = k[x_1,\dots,x_m,y_1,\dots,y_m]$ as follows. Let $(a,b),(a',b') \in \mathbb{N}^m \times \mathbb{N}^m$ where $a = (a_1,\dots,a_m) \in \mathbb{N}^m$ and likewise for b, a' and b'. We define

$$(a,b) >_{x,y} (a',b') \equiv a >_x a' \text{ or } (a = a' \text{ and } b >_x b')$$

That is $>_{x,y}$ is the lexicographic ordering on $\mathbb{N}^m \times \mathbb{N}^m$ given by considering $>_x$ on each factor. This is clearly a monomial ordering on $k[x,y]$ which agrees with the monomial order on $k[x]$ when restricted to monomials involving only x-variables, and for which $x_i > y_j$ for all $i,j = 1,\dots,m$. In particular $\mathrm{LT}_x(f(x)) = \mathrm{LT}_{x,y}(f(x)+f(y))$ for all $f \in k[x]$. From now on we dispense with distinguishing between $>_x$ and $>_{x,y}$ and simply use $>$ and LT to refer to both monomial orderings.

Consider a sequence $t = (t_1,\dots,t_n)$ in $k[x]$ and suppose it is both quasi-regular and a Gröbner basis for its ideal (see Section 3). We define $T_i = t_i(x) - t_i(y)$ and consider the sequence $T = (T_1,\dots,T_n)$ in $k[x,y]$. One can show that T is quasi-regular, and assume that T is also a Gróbner basis for its ideal (is this also automatic?).

The reason for these assumptions is that the sequences t and T have the following property.

Lemma 5. *Let $f \in k[x]$. Suppose we have an expression for f of the form*

$$f = \sum_{u \in \mathbb{N}^n} r_u t^u$$

where finitely many $r_u \neq 0$ and for all r_u, all terms of r_u are not divisible by any of the $\mathrm{LT}(t_i)$. Then all the coefficients r_u are uniquely determined by f. Likewise for $F \in k[x,y]$, in any expression for F of the form

$$F = \sum_{u \in \mathbb{N}^n} R_u T^u$$

where finitely many $R_u \neq 0$ and no term of R_u is divisible by any of the $\mathrm{LT}(T_i) = \mathrm{LT}(t_i)$, the coefficients R_u are uniquely determined by F.

Proof. See Section 3. □

Note that the expressions in the above lemma are exactly the expressions computed by the iterated division algorithm.

Given $f \in k[x]$ write

$$f(x) - f(y) = \sum_{u \in \mathbb{N}^n} r_u T^u$$

where the $r_u \in k[x,y]$ are the unique polynomials satisfying the conditions in Lemma 5. For each $u \in \mathbb{N}^n$ define a map $\rho_u : k[x] \to k[x,y]$ by setting $\rho_u(f) = r_u$. We now prove some facts about these maps. For $u,v \in \mathbb{N}^n$ define $u! = u_1!u_2!\cdots u_n!$ and

$$\binom{v}{u} = \begin{cases} 0 & \text{if any } v_i - u_i < 0 \\ \frac{v!}{u!(v-u)!} & \text{otherwise} \end{cases}$$

Lemma 6. *ρ_u is k-linear.*

Proof. Let $f, g \in k[x]$. Then we can write

$$(f+g)(x) - (f+g)(y) = \sum_{u \in \mathbb{N}^n} (\rho_u(f) + \rho_u(g)) T^u$$

Now, if $\rho_u(f) + \rho_u(g) \neq 0$ then no term of $\rho_u(f) + \rho_u(g)$ is divisible by any of the $\mathrm{LT}(T_i)$. Hence the right-hand-side satisfies the conditions in Lemma 5 and so by uniqueness $\rho_u(f + g) = \rho_u(f) + \rho_u(g)$. Likewise $\rho_u(cf) = c\rho_u(f)$ for $c \in k$. □

Lemma 7. *$\rho_u(t^v) = \binom{v}{u} t^{v-u}(y)$ for all $v \in \mathbb{N}^n$ and $u \neq 0$.*

Proof. It suffices to prove that

$$t^v(x) = \sum_u \binom{v}{u} t^{v-u}(y) T^u \tag{2.1}$$

Indeed, having shown (2.1) holds we have

$$t^v(x) - t^v(y) = \sum_{u \neq 0} \binom{v}{u} t^{v-u}(y) T^u$$

where we note that no term of $t^{v-u}(y)$ is divisible by any of the $\mathrm{LT}(T_i) = \mathrm{LT}(t_i(x))$.

We proceed by induction on $|v| = \sum_i v_i$. If $v = 0$ then both sides of (2.1) are equal to 1. Now suppose that $|v| \geq 1$. Let i be such that $v_i > 0$. Then, using the induction hypothesis, we have

$$\begin{aligned}
t^v(x) &= t_i(x) t^{v-e_i}(x) \\
&= t_i(x) \sum_u \binom{v-e_i}{u} t^{v-e_i-u}(y) T^u \\
&= (t_i(y) + T_i) \sum_u \binom{v-e_i}{u} t^{v-e_i-u}(y) T^u \\
&= \sum_u \binom{v-e_i}{u} t^{v-u}(y) T^u + \sum_u \binom{v-e_i}{u} t^{v-e_i-u}(y) T^{u+e_i} \\
&= \sum_u \binom{v-e_i}{u} t^{v-u}(y) T^u + \sum_{u \neq 0} \binom{v-e_i}{u} t^{v-u}(y) T^u \\
&= t^v(y) + \sum_{u \neq 0} \left(\binom{v-e_i}{u} + \binom{v-e_i}{u-e_i} \right) t^{v-u}(y) T^u \\
&= t^v(y) + \sum_{u \neq 0} \binom{v}{u} t^{v-u}(y) T^u \\
&= \sum_u \binom{v}{u} t^{v-u}(y) T^u
\end{aligned}$$

which proves the claim. □

Lemma 8. *Let $f \in k[t]$ and $r \in k[x]$ be such that no term of r is divisible by any of the $\mathrm{LT}(t_i)$. Then for $u \neq 0$ we have $\rho_u(rf) = r(x)\rho_u(f)$.*

Proof. It suffices to prove this for $f = t^v$ for $v \in \mathbb{N}^n$. Using Lemma 7 we have

$$\begin{aligned} r(x)t^v(x) - r(y)t^v(y) &= r(x)t^v(x) - r(x)t^v(y) + r(x)t^v(y) - r(y)t^v(y) \\ &= r(x)(t^v(x) - t^v(y)) + (r(x) - r(y))t^v(y) \\ &= r(x)\sum_{u\neq 0}\binom{v}{u}t^{v-u}(y)T^u + (r(x) - r(y))t^v(y) \\ &= (r(x) - r(y))t^v(y) + \sum_{u\neq 0}\binom{v}{u}r(x)t^{v-u}(y)T^u \end{aligned}$$

Notice that $\mathrm{LT}(t_j) = \mathrm{LT}(T_j)$ does not divide any term of $(r(x)-r(y))t^v(y)$ or $\binom{v}{u}r(x)t^{v-u}(y)$ for all $j = 1,\dots,n$ and $u \in \mathbb{N}^n$. Hence by Lemma 5 this proves the claim. □

Now let $e_i \in \mathbb{N}^n$ have a 1 in the i^{th} coordinate and 0 elsewhere and let $\varphi : k[x,y] \to k[x]$ be the k-algebra morphism identifying x and y. For each t_i we define a map $\partial_{t_i} : k[x] \to k[x]$ by setting $\partial_{t_i}(f) = \varphi\rho_{e_i}(f)$.

Proposition 9. *The maps $\partial_{t_i},\dots,\partial_{t_i} : k[x] \to k[x]$ form a system of t-derivatives as defined in Definition 1.*

Proof. We need to show that $\partial_{t_1},\dots,\partial_{t_n}$ are k-linear and satisfy

(1) Every $f \in k[x]$ can be written uniquely in the form

$$f = \sum_{u\in\mathbb{N}^n} r_u t^u$$

where $r_u \in \bigcap_i \ker(\partial_{t_i})$.

(2) $\partial_{t_i}(t^v) = v_i t^{v-e_i}$ for all $v \in \mathbb{N}^n$ (where we understand that $0t_j^{-1} = 0$).

(3) For $f \in k[t]$ and $r \in \bigcap_i \ker(\partial_{t_i})$ we have $\partial_{t_i}(rf) = r\partial_{t_i}(f)$.

That $\partial_{t_1},\dots,\partial_{t_n}$ are k-linear, and properties (2) and (3) follow directly from Lemma 6, Lemma 7 and Lemma 8 respectively. For (1) note that we can write any $f \in k[x]$ in the form

$$f(x) = \sum_u r_u(x)t^u(x)$$

where if $r_u \neq 0$ then no term of r_u is divisible by any of the $\mathrm{LT}(t_i)$. This expression exists by Theorem 3 and is unique by the assumption on t, and note that $\rho_{e_i}(r_u) = 0$ for all u by Lemma 5. □

Proposition 9 is the main result of this section, but before continuing we note some other properties of the maps $\partial_{t_1},\dots,\partial_{t_n}$ defined in Proposition 9. As noted previously, since $\partial_{t_1},\dots,\partial_{t_n}$ is a system of t-derivatives we have $\partial_{t_i}\partial_{t_j} = \partial_{t_j}\partial_{t_i}$ for all i,j. Hence for $a \in \mathbb{N}^n$ we define $\partial_t^a = \partial_{t_1}^{a_1}\cdots\partial_{t_n}^{a_n}$. The next result is analogous to Taylor's Theorem.

Proposition 10. *$\partial_t^a = a!\varphi\rho_a$ for all $a \neq 0$.*

Proof. Let $f \in k[x]$ and write

$$f(x) = \sum_u r_u(x)t^u(x)$$

where finitely many $r_u \neq 0$ and if $r_u \neq 0$ then no term of r_u is divisible by any of the $\mathrm{LT}(t_i)$. By Lemma 7 we have $\rho_a(t^u) = \binom{u}{a} t^{u-a}(y)$ and so

$$\begin{aligned}
\partial_t^a(f) &= \sum_u a! \binom{u}{a} r_u(x) t^{u-a}(x) \\
&= a! \sum_u r_u(x) \varphi \rho_a(t^u) \\
&= a! \sum_u \varphi \rho_a(r_u t^u) \\
&= a! \varphi \rho_a(f)
\end{aligned}$$

where we have that $r_u(x)\rho_a(t^u) = \rho_a(r_u t^u)$ by Lemma 8. □

Let $f \in k[x]$. Clearly one way to compute $\partial_{t_i}(f)$ is to use Algorithm 1.0.4 to compute an expression for f of the form

$$f(x) = \sum_u r_u(x) t^u(x)$$

where finitely many $r_u \neq 0$ and if $r_u \neq 0$ then no term of r_u is divisible by any of the $\mathrm{LT}(t_i)$. We then have

$$\partial_{t_i}(f) = \sum_u r_u(x) u_i t^{u-e_i}(x)$$

This approach needs many calls to the division algorithm as the whole expansion of $f(x)$ in terms of $t_1(x), \ldots, t_n(x)$ must be computed. A more efficient approach which only calls the division algorithm twice is given in Algorithm 2.0.11, in which $\partial_{t_j}(f) = \textsc{differentiate}(f, j, t_1, \ldots, t_n)$.

Algorithm 2.0.11 Computing ∂_{t_j}

1: **procedure** DIFFERENTIATE$(f, j, t_1, \ldots, t_n)$
2: Use the division algorithm in $k[x, y]$ to obtain $r(x, y), q_1(x, y), \ldots, q_n(x, y)$ satisfying

$$f(x) - f(y) = r(x, y) + \sum_{i=1}^{n} q_i(x, y)(t_i(x) - t_i(y))$$

along with the other conditions in Theorem 2.
3: Use the division algorithm in $k[x, y]$ to obtain $r'(x, y), p_1(x, y), \ldots, p_n(x, y)$ satisfying

$$q_j(x, y) = r'(x, y) + \sum_{i=1}^{n} p_i(x, y)(t_i(x) - t_i(y))$$

4: **return** $\varphi(r'(x, y))$

---

3 Appendix regarding the conditions on t

We first recall the concept of a Gröbner basis.

Definition 12. Fix a monomial ordering on $k[x]$ and let $I = (g_1, \ldots, g_n)$ be an ideal. Consider the set of leading terms of elements of I:

$$\mathrm{LT}(I) = \{\mathrm{LT}(f) \mid f \in I \setminus \{0\}\}$$

We say that $t_1, \ldots, t_n$ is a *Gröbner basis for* I if the ideal generated by $\mathrm{LT}(I)$ is equal to $(\mathrm{LT}(t_1), \ldots, \mathrm{LT}(t_n))$. Given a sequence $t = (t_1, \ldots, t_n)$ we say that t is a *Gröbner basis* to mean that t is a Gröbner basis for the ideal its elements generate.

Lemma 13 ([CLO15, Corollary 2.6.2])**.** *Let $f \in k[x]$. If t is a Gröbner basis then when we apply the division algorithm to divide f by t, the remainder term is zero if and only if $f \in I$.*

Note that the property of being a Gröbner basis is depends on the monomial ordering on $k[x]$. One can show that given a monomial ordering on $k[x]$ and an ideal I there always exists a Gröbner basis for that ideal [CLO15, Corollary 2.5.6], and moreover a Gröbner basis can be computed from a finite generating set for I via an algorithm called *Buchberger's Algorithm* [CLO15, Theorem 2.7.2]. For more on Gröbner basis see [CLO15, Chapter 2].

Next we discuss quasi-regular sequences. Let R be a commutative ring and $t = (t_1, \ldots, t_n)$ a sequence of elements in R. We denote by $I = (t_1, \cdots, t_n)$ the ideal generated by the elements of t. Consider the polynomial ring $(R/I)[x] = (R/I)[x_1, \cdots, x_n]$ with coefficients in R/I. We define a map

$$\alpha : (R/I)[x] \longrightarrow \bigoplus_{m \geq 0} I^m / I^{m+1} \tag{3.1}$$

by setting $\alpha(x_i) = t_i + I^2$, where we denote $I^0 = R$ by mild abuse of notation. This map is always surjective. Indeed, consider $t^u + I^{m+1} \in I^m / I^{m+1}$ where $u \in \mathbb{N}^n$ is such that $\sum_{i=1}^n u_i = m$. It is straightforward to show that $\alpha(x^u) = t^u + I^{m+1}$. Noting that any element of I^m / I^{m+1} can be written as a sum of elements of the form $at^u + I^{m+1}$ where $a \in R$ is not divisible by any of the t_i and applying linearity proves that α is surjective.

The definition of quasi-regular should be seen in the context of the other regularity conditions on sequences. Recall that part of the definition of a potential was that its sequence of partial derivatives is Koszul-regular.

Definition 14. We say the sequence t is:

(1) *regular* if each t_i is not a zero-divisor on $R/(t_1, \ldots, t_{i-1})$, and if the ring R/I is non-zero.

(2) *Koszul-regular* if the Koszul complex of t is exact except in degree zero.

(3) *quasi-regular* if the map α at (3.1) is an isomorphism.

The definition of Koszul-regular was first given in [Kab71, Definition 1] and the definition of quasi-regular was first given in [EGA, Volume IV Chapitre 0 15.1.7]. These regularity conditions and their relationships are also discussed in [Stacks, Sections 10.68, 10.69, 15.30]. In particular we have the following relationships, which are the main result of [Kab71].

Lemma 15. *For the sequence t we have:*

(1) If t is regular then t is Koszul-regular.

(2) If t is Koszul-regular then t is quasi-regular.

This is proved in [Kab71, Theorem 1.1] and also in [Stacks, Section 15.30]. Although it is not relevant for our purposes, it is worth pointing out that if R is a Noetherian local ring any quasi-regular sequence of non-units is necessarily a regular sequence [Stacks, Lemma 10.69.6] and so by Lemma 15 the regularity conditions of Definition 14 are equivalent for such sequences in Noetherian local rings. Examples presented in [Kab71] show that the implications in Lemma 15 cannot be reversed in general, or even under some generous assumptions on the ring R.

Now let k be a commutative ring and suppose R is a k-algebra. The next two results prove Lemma 5.

Lemma 16. *Suppose t is quasi-regular and suppose we have a k-linear map $\sigma : R/I \to R$ such that $\pi\sigma = 1$. Then if we have $\sum_{u\in\mathbb{N}^n} \sigma(r_u)t^u = 0$ for some $r_u \in R/I$, with finitely many $\sigma(r_u) = 0$. Then we necessarily have $\sigma(r_u) = 0$ for all $u \in \mathbb{N}^n$.*

Proof. Suppose for a contradiction that not all $r_u = 0$. Given $u \in \mathbb{N}^n$ let $|u| = \sum_{i=1}^n u_i$. We define

$$m = \min\{|u| \mid r_u \neq 0\}$$

Rearranging $\sum_{u\in\mathbb{N}^n} \sigma(r_u)t^u = 0$ we have

$$\sum_{|u|=m} \sigma(r_u)t^u = -\sum_{m<|u|} \sigma(r_u)t^u$$

which implies $\sum_{|u|=m} \sigma(r_u)t^u \in I^{m+1}$. Hence in I^m/I^{m+1} we have

$$\sum_{|u|=m} \sigma(r_u)t^u = 0$$

Since t is quasi-regular we have $\sigma(r_u) \in I$: if this were not the case then this would give us a non-zero element of $(R/I)[x]$ which is sent to zero by the map α of (3.1). Applying π gives $r_u = 0$ and hence $\sigma(r_u) = 0$, proving the claim. □

Similar results to the lemma above are also discussed in [Lip87, Chapter 3]. The next result provides a particularly useful section of the quotient map using a Gröbner basis.

Lemma 17. *Fix a monomial ordering on $k[x]$ and suppose t is a Gröbner basis with respect to this monomial order. Let*

$$V = \{r \in k[x] \mid \text{no term of } r \text{ is divisible by any of the } \mathrm{LT}(t_i)\}$$

Then the quotient map $\pi : k[x] \to k[x]/I$ restricts to an isomorphism $V \to k[x]/I$.

Proof. For injectivity suppose $r \in V$ is such that $\pi(r) = 0$. Applying the division algorithm to divide r by t yields the remainder term r, since none of the terms in r are divisible by any of the $\mathrm{LT}(t_i)$. Since $r \in I$, by Lemma 13 we have $r = 0$.

For surjectivity, consider $f \in k[x]$. Via the division algorithm we obtain an expression for f of the form

$$f = r + \sum_{i=1}^n q_i t_i$$

where $r \in V$. Then we have $\pi(f) = \pi(r)$, and noting that $\pi : k[x] \to k[x]/I$ proves the claim. □

References

[CLO15] David A. Cox, John Little and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. Cham: Springer International Publishing, 2015.

[EGA] Alexander Grothendieck and Jean Dieudonné. *Éléments de géométrie algébrique*. Institut des Hautes Études Scientifiques, 1961–1967.

[Kab71] Thomas Kabele. 'Regularity conditions in nonnoetherian rings'. In: *Transactions of the American Mathematical Society* 155.2 (1 Feb. 1971), pp. 363–374.

[Lip87] Joseph Lipman. *Residues and Traces of Differential Forms via Hochschild Homology*. Vol. 61. Contemporary Mathematics. Providence, R.I: American Mathematical Society, 1987. 95 pp.

[Stacks] The Stacks Project. URL: https://stacks.math.columbia.edu/ (visited on 06/12/2021).