Finiteness of Symmetric Ideals

Duong Hoang Dung

1 Introduction

It is well-known by Hilbert’s Basis Theorem that if $A$ is a Noetherian ring, then the ring $A[x]$ of polynomials in one variable $x$ and coefficients from $A$ is also Noetherian. We find by induction that the polynomial ring $R = A[x_1, x_2, \cdots, x_n]$ in finitely many variables is Noetherian. Moreover the notion of Grobner Basis allows us to do effective computations in $R/I$, where $I$ is an ideal in $S$.

The situation changes dramatically when one considers polynomial rings in infinitely variables. For instance, the ring $A[x_1, x_2, \cdots]$ is not Noetherian, since the ideal $(x_1, x_2, \cdots)$ does not have a finite set of generators.

However, if we have some special action of some special group on the ring $R$, we may occur finitely generation of invariant ideals. Indeed, if we let $X = \{x_1, x_2, \cdots\}$, and let $G = \text{Sym}(X)$ be the group of permutations of $X$. The group $G$ acts on $R$ in a natural way: if $\sigma \in G$ and $f \in R = A[x_1, x_2, \cdots, x_n]$, where $x_i \in X$, then

$$\sigma f(x_1, \cdots, x_n) = f(\sigma x_1, \cdots, \sigma x_n) \in R$$

and this in turn gives $R$ the structure of a left module over the left group ring $R[G] = \{\sum_{i=1}^{m} r_i \sigma_i : r_i \in R, \sigma_i \in G\}$ with multiplication given by $f \sigma g \tau = (f \sigma(g)) (\sigma \tau)$ for all $f, g \in R, \sigma, \tau \in G$. An ideal $I \subseteq R$ is called invariant under $G$ if

$$GI := \{\sigma f : \sigma \in G, f \in I\} \subseteq I$$

Notice that invariant ideals are simply the $R[G]$—submodules of $R$. We have the main theorem accordingly to Aschenbrenner and Hillar ([1]) as follows:


In this talk, we will try to understand the proof of the theorem by replacing a field $K$ for the Noetherian ring $A$ due to the talk of J.Draisma ([3]). We first start by introducing some basic notions of well-partial-ordering, in particular the shift-ordering on monomials in $K[X]$ in section 2. Next we going to prove in section 3 the main (reduced—) theorem. Finally, we close the talk in section
4 by showing some more results related to the main theorem, and some other questions as well.

2 Well-partial-odering

2.1 Preliminaries

A quasi-ordering on a set $S$ is a binary relation $\leq$ on $S$ which is reflexive and transitive. A quasi-ordered set is a pair $(S, \leq)$ consisting of a set $S$ and a quasi-ordering. If in addition, the relation $\leq$ is anti-symmetric then $\leq$ is called partial ordering on the set $S$. A trivial ordering on $S$ is given by $s \leq t \iff s = t$ for all $s, t \in S$. A quasi-ordering $\leq$ on $S$ induces a partial ordering on the set $S/\sim = \{s/\sim: s \in S\}$ of equivalence classes of the equivalence relation $s \sim t \iff s \leq t \land t \leq s$ on $S$.

An antichain of $S$ is a subset $A \subseteq S$ such that $s \not\leq t$ and $t \not\leq s$ for all $s \not\sim t$ in $A$. A final segment of a quasi-ordered set $(S, \leq)$ is a subset $F \subseteq S$ which is closed upwards : $s \leq t \land s \in F \Rightarrow t \in F$.

A quasi-ordered set $S$ is said to be well-founded if there is no infinite strictly decreasing sequence $s_1 > s_2 > \cdots$ in $S$, and well-quasi-ordered (well-partial-ordered if in addition every antichain of $S$ is finite. An infinite sequence $s_1, s_2, \cdots$ in $S$ is called good if $s_i \leq s_j$ for some indices $i < j$, and bad otherwise. We have the following characterization of well-partial-orderings as follows (see [4]).

Proposition 2.1 The following are equivalent, for a quasi-ordered set $S$:

1. $S$ is well-partial-ordered.
2. Every infinite sequence in $S$ is good.
3. Every infinite sequence in $S$ contains an infinite increasing subsequence.
4. Any final segment of $S$ is finitely generated.
5. $(F(S), \supseteq)$, where $F(S)$ is the set of final segments of $S$, is well-founded (i.e., the ascending chain condition holds for final segments of $S$).

Let $(S, \leq_S)$ and $(T, \leq_T)$ be quasi-ordered, the cartesian product $S \times T$ can be turned into a quasi-ordered set by using the cartesian product of $\leq_S$ and $\leq_T$:

$$(s, t) \leq (s', t') :\iff s \leq_S s' \land t \leq_T t', \quad \text{for } s, s', t, t' \in T$$

From the proposition 2.1 we easily obtain that the cartesian product of two well-partial-ordered sets is again well-partial-ordered.

Of course, the total ordering $\leq$ is well-partial-ordered if and only if it is well-founded, in this case $\leq$ is called well-ordering.
2.2 Setting up

In this talk, we simply consider the ring $R = \mathbb{C}[x_0, x_1, \ldots]$ of polynomials in infinitely indeterminates $x_0, x_1, \ldots$.

**Definition 2.2** For any map $\pi : \mathbb{N} \to \mathbb{N}$ and $r \in R$, we write $\pi r$ for the image of $r$ under the homomorphism $R \to R$ sending $x_i$ to $x_{\pi i}$.

**Definition 2.3** We define an order $\preceq$ on monomials in $x_0, x_1, \ldots$ as follows: it is the smallest relation on monomials satisfying $1 \preceq 1$ and $u \preceq v \implies u \preceq x_0^a \sigma v$ and $x_0^a \sigma u \preceq x_0^b \sigma v$ for all $u, v$ and $0 \leq a \leq b$. Here, as in the rest of this talk, $\sigma : \mathbb{N} \to \mathbb{N}, i \mapsto i + 1$.

**Definition 2.4** For $u$ a monomials we write $|u|$ for the largest $i$ such that $x_i$ appears in $u$. For $u = 1$ we write $|u| = -\infty$.

**Lemma 2.5** $u \preceq v$ if and only if there is an increasing map $\pi : \{0, \ldots, |u|\} \to \mathbb{N}$ such that $\pi u$ divides $v$.

*Proof.* $(\Rightarrow)$ Follows by induction: If $\pi$ does the trick for $u \preceq v$, i.e. we have $\pi u \preceq v$, then $\sigma \pi$ does the trick for $u \preceq v$ since $\pi u \preceq v$. Then the map $\varphi : \{0, \ldots, |u|\} \to \mathbb{N}$ defined as follows does the trick for $x_0^a u \preceq x_0^b v$, where $0 \leq a \leq b$.

$(\Leftarrow)$ From the increasing map $\pi$ as above. We easily construct a sequence of relations that deduce $u \preceq v$ from $1 \preceq 1$. For example, for $u = x_0^a_0 x_1^a_1 x_2^a_2$, $|u| = 2$, and $\pi$ is defined as

$$\pi(0) = 5, \pi(1) = 9, \pi(2) = 11$$

So $\pi u = x_0^{a_0} x_1^{a_1} x_2^{a_2}$. Since $\pi(2) = 11$, then $|u| \geq 11$, we may assume

$$v = x_0^{b_0} x_1^{b_1} \cdots x_{12}^{b_{12}}$$

where $a_0 \leq b_5, a_1 \leq b_9, a_2 \leq b_{11}$ because $\pi u \preceq v$. From $1 \preceq 1$, we have the following procedure to create the sequence as required:

1. $1 \preceq 1$
2. $1 \preceq x_0^{b_{12}}$
3. $x_0^{a_2} \preceq x_0^{b_{10}} x_1^{b_{12}} x_2^{b_{12}}$ (apply $x_0^a \sigma u \preceq x_0^b \sigma v$)
4. $x_0^{a_2} \preceq x_0^{b_{10}} x_1^{b_{12}} x_2^{b_{12}}$ (apply $u \preceq x_0^b \sigma v$)
5. $x_0^{a_2} x_1^{a_2} \preceq x_0^{b_9} x_1^{b_9} x_2^{b_{11}} x_3^{b_{12}}$ (apply $x_0^a \sigma u \preceq x_0^b \sigma v$)

Continuing this procedure, we obtain $u \preceq v$ as required. \blacksquare
Remark 2.6  This lemma implies that \( \lesssim \) is a partial order.

**Reflexive:** \( u \lesssim u \) by the identity map.

**Transitive:** Assume that \( u \lesssim v \) via \( \pi \) and \( v \lesssim w \) via \( \chi \pi \), since the composition of two increasing maps is an increasing map, and \( \pi u|v|, \chi v|w| \), so \( \chi \pi u|\chi v|w \).

**Anti-symmetric:** Assume that \( u \lesssim v \) via \( \pi \), and \( v \lesssim \) via \( \chi \). Then \( \pi \chi v|v \) and \( \chi \pi u|u \) which imply that \( \chi \pi \) and \( \pi \chi \) are identities, hence \( u \approx v \).

**Proposition 2.7**  The partial order \( \lesssim \) does not have infinite antichains.

**Proof.**  Suppose that there exists infinite antichains, then there exists an infinite never-increasing sequence (by proposition 2.1)

\[
u_1, u_2, \cdots, u_n, \cdots
\]

that is the sequence such that \( u_i \not\lesssim u_j \) for all \( i < j \). Moreover, we may take such a sequence with the additional property that \( |u_n| \) is minimal among all \( u_n \) such that \( u_1, \cdots, u_n \) can be extended to an infinite never-increasing sequence.

For all \( i \) let \( a_i \) be the exponent of \( x_0 \) in \( u_i \). Now there is an infinite sequence \( 1 \leq i_1 < i_2 < \cdots \) such that

\[
a_{i_1} \leq a_{i_2} \leq \cdots
\]

(take \( i_1 \) such that \( a_{i_1} \) is minimal, then take \( i_2 > i_1 \) such that \( a_{i_2} \) is minimal, etc.). But then consider the antichain

\[
u_1, \cdots, u_{i_1-1}, u_{i_1}, u_{i_2}, \cdots
\]

Let \( \alpha \) be the homomorphism that sends \( x_{i+1} \) to \( x_i \) for \( i \geq 0 \) and send 0 to 1. Consider the sequence

\[
u_1, \cdots, u_{i_1-1}, \alpha(u_{i_1}), \alpha(u_{i_2}), \cdots
\]

By the minimality of \( |u_{i_1}| \), this sequence is not never-increasing. Hence either there exist \( i < i_1 \) and \( j \geq 1 \) such that

\[
u_i \not\lesssim \alpha(u_j)
\]

or there exist \( 1 \leq j \leq k \) such that

\[
\alpha(u_j) \not\lesssim \alpha(u_k)
\]

But in the first case we have

\[
u_i \not\lesssim u_j
\]

by the first inductive property of \( \lesssim \), and in the second case we have

\[
u_{i_j} \geq u_{i_k}
\]

by the second inductive property of \( \lesssim \) and the fact that \( a_{i_j} \leq a_{i_k} \). We get a contradiction, hence the proposition is proved. ■
3 Proof of the main theorem

**Theorem 3.1** Let $G = \text{Sym}(\mathbb{N})$ act on the algebra $R = \mathbb{C}[x_0, x_1, \cdots]$ by permutations. Then any $G$–stable ideal $I$ of $R$ is finitely generated as $G$–stable ideal, that is, there exists finitely many $f_1, \cdots, f_k \in I$ such that $I$ is the smallest $G$–stable ideal containing $f_1, \cdots, f_k$.

**Proof.** Let $I$ be a $G$–stable ideal. To any $f \in R$ we associate its leading monomial $lm(f)$ in the lexicographic order, where $x_1 < x_2 < \cdots$. Now consider the set $M$ of all $\preceq$–minimal elements of the set $\{lm(f) : f \in I\}$. This is an antichain by definition, hence finite by the proposition 2.7. So there exist (monic) $f_1, \cdots, f_k \in I$ such that $M = \{lm(f_1), lm(f_2), \cdots, lm(f_k)\}$. We claim that $I$ equals the smallest $G$–stable ideal $J$ containing $f_1, \cdots, f_k$.

Suppose that $I$ contains a monic counterexample $f \notin J$. We may assume that $lm(f)$ lexicographically minimal among counterexamples (since the lexicographic order is a well-ordered). By construction, there exists an $i$ such that $lm(f_i) \preceq lm(f)$. Set $n = |lm(f_i)|$ and let $\pi : \{1, \cdots, n\} \to \mathbb{N}$ be increasing such that $\pi(lm(f_i)) | lm(f)$, say $lm(f) = u\pi lm(f_i)$. Then $\pi(f_i) \in J$ by $G$–stability, and

$$f' := f - u\pi(f_i) \notin J$$

We claim that the $lm(f')$ is lexicographically smaller than $lm(f)$, contradicting the minimality of the latter. But this is clear from $lm(\pi(f_i)) = \pi(lm(f_i))$, so that $lm(\pi(f_i)) = u\pi(lm(f_i)) = lm(f)$.

**Comment 3.2** In the main theorem due to Aschenbreiner and Hillar, we consider the case $R = A[X]$ where $A$ is the Noetherian ring, and the proof is a bit different, since we can not choose the monic polynomials $f_1, \cdots, f_k$ as above. But now then we use the Noetherianity of the ring $A$ to create the finite set of coefficients serving for our proof along with defining a new order on monomials by attaching the old-ordering with conditions on ideals of coefficients $J_u = \{a \in A : a = lc(g), g \in I, lm(g) = u\}$ ([1]).

4 Further

For $r \in \mathbb{N}$, let $[r] = \{1, 2, \cdots, r\}$, we consider the action of $\Pi$ on $K[X_{[r] \times \mathbb{N}}]$ by its action on the second index of the indeterminates $X_{[r] \times \mathbb{N}}$:

$$\pi x_{i,j} := x_{i,\pi(j)}, \quad \pi \in \Pi$$

We have the following result

**Theorem 4.1** The column-wise lexicographic term order $x_{i,j} \preceq x_{k,l}$ if $j < l$ or $(j = l \land i \leq k)$ is well-partial-order with respect to $\Pi$, and the ring $K[X_{[r] \times \mathbb{N}}]$
is \(\Pi\)-Noetherian.

So when \(r = 1\), we certainly have the case above. But when \(r = \infty\), which means we consider the ring \(K[N \times N]\) with the action of \(G = \text{Sym}(N)\) by permuting the indices simultaneously (i.e. \(\pi_{i,j} = x_{\pi(i),\pi(j)}\)), then \(R\) is not \(G\)-Noetherian. We may obtain the result by constructing the bad sequence of monomials as follows:

\[
\begin{align*}
s_3 & = x_{(1,2)}x_{(3,2)}x_{(3,4)} \\
s_4 & = x_{(1,2)}x_{(3,2)}x_{(4,3)}x_{(4,5)} \\
s_5 & = x_{(1,2)}x_{(3,2)}x_{(4,3)}x_{(5,4)}x_{(6,7)} \\
& \quad \vdots \\
s_n & = x_{(1,2)}x_{(3,2)}x_{(4,3)} \cdots x_{(n,n-1)}x_{(n,n+1)} \\
& \quad \vdots
\end{align*}
\]

For any \(n < m\) and any \(\sigma \in G\), the monomial \(\sigma s_n\) does not divide \(s_m\). Otherwise, notice that \(x_{(1,2)}x_{(3,2)}\) is the only pair of indeterminates which divides \(s_n\) or \(s_m\) and has form \(x_{(i,j)}x_{(i,j)}\). Therefore \(\sigma(2) = 2\), and either \(\sigma(1) = 1, \sigma(3) = 3\) or \(\sigma(3) = 1, \sigma(1) = 3\). But since 1 does not appear as the second component of a factor \(x_{(i,j)}\) of \(s_m\), we have \(\sigma(1) = 1, \sigma(3) = 3\). Since \(x_{(4,3)}\) is the only indeterminate dividing \(s_n\) or \(s_m\) of the form \(x_{(1,3)}\), we get \(\sigma(4) = 4\). Since \(x\) if the only indeterminate dividing \(s_n\) or \(s_m\) of the form \(x_{(1,4)}\), we get \(\sigma(5) = 5\), etc. So we get \(\sigma(i) = i\) for all \(i = 1, 2, \ldots, n\). But the only indeterminate dividing \(s_m\) of the form \(x_{(n,j)}\) is \(x_{(n,n-1)}\), hence the factor \(\sigma x_{(n,n+1)} = x_{n,\sigma(n+1)}\) of \(\sigma s_n\) does not divide \(s_m\). This shows that \(s_3, s_4, \cdots\) is a bad sequence, as required.

Remark 4.2 In fact, \(R = K[N \times N \times \cdots \times N]\), with \(k\) indices \(N\), is not \(G\)-Noetherian for all \(k \geq 2\). Indeed, if we denote \(R(k)\) the ring \(K[N \times N \times \cdots \times N]\) in \(k\) indices, then

\[x_{u_1, \ldots, u_k, u_{k+1}} \mapsto x_{u_1, \ldots, u_k}\]

defines the surjective \(K\)-algebra homomorphism \(\pi_k : R^{(k+1)} \to R^{(k)}\) with invariant kernel. Hence if \(R^{(k+1)}\) is \(G\)-Noetherian, then so is \(R^{(k)}\).

However, if we let \(R_{\leq d}\) denote the \(G\)-module of polynomials of degree at most \(d\), we do have the following result ([3])

Lemma 4.3 The \(G\)-module \(R_{\leq d}\) is Noetherian, i.e., every \(G\)-submodule of it is finitely generated.
References


