Groebner Bases and Symmetries

Daniel Felipe Ávila Girardot

July 19, 2014

Contents

Chapter 1

Introduction

1.1 Polynomial Ideals

The algebra of polynomials has always been a topic of interest. In particular, the understanding of ideals in polynomial rings has been fundamental to study objects such as affine varieties. For instance, suppose k is a field and let $R := k[x_1, ..., x_n]$. Given $f_1, ..., f_n \in R$ define the ideal $I = \langle f_1, ..., f_n \rangle$. It's easy to prove that the affine varieties $V(I)$ and $V(f_1, ..., f_n)$ are equal, so if we are able to describe I in an easier way the affine variety $V(I)$ will be easier to calculate. Therefore, some problems one may want to resolve are:

1. The Ideal Description Problem: Is every polynomial ideal finitely generated?

2. The Ideal Membership Problem: Given a polynomial ideal I and a polynomial f determine whether $f \in I$.

3. Given $f \in I = \langle f_1, ..., f_n \rangle$ determine polynomials $h_1, ..., h_n$ such that $f = h_1 f_1 + ... + h_n f_n$.

In 1888 David Hilbert prove that the answer for the first question is affirmative. Nowadays, in commutative algebra this fact is known as Hilbert basis theorem (HBT), which states: If A is a noetherian ring and X is a finite set of indeterminates then the polynomial ring $R = A[X]$ is noetherian. Recall that the noetherianity condition is equivalent to the fact that any ideal is finitely generated, so the ideal description problem is actually solved.

In the case we are given a polynomial ring $k[x]$ where k is a field any ideal is generated by a single element. Moreover, if $f_1, ..., f_n$ is a set of generators for an ideal I then using the division algorithm one can compute a polynomial $g = gcd(f_1, ..., f_n)$ (the greatest common divisor of $f_1, ..., f_n$ such that $I = \langle g \rangle$. Then, a polynomial $f \in k[x]$ lies in I if and only if when dividing f by g the remainder is 0. Therefore, in the one variable case there is a solution for the ideal membership problem. In the multivariate case (with finitely many variables) Groebner bases appear as an analogue of the greatest common divisor; that is: given an ideal I and a Groebner basis G for I then $I = \langle G \rangle$, and a polynomial f lies in I if and only if when dividing f by G the remainder is 0. Groebner bases were introduced by Bruno Buchberger in 1965, and in addition to their theoretical importance what makes them very useful is that there are algorithms to calculate them (see for instance [4]).

In the previous discussion the finiteness of the set X of variables was fundamental, for example in HBT: if X is an infinite set of indeterminates, the ideal $I = (x_1^2, x_2^2, ..., x_n^2, ...) \subset A[X]$ is not finitely generated, or the ascending chain $(x_1) \subset (x_1, x_2) \subset (x_1, x_2, x_3) \subset ....$ does not stabilize. On the other hand, the existence of Groebner bases depend on HBT. So an interesting question arises, under what conditions can we find analogues of finite generation of ideals, in polynomial rings where HBT does not apply?.
In a paper of 2007 by Matthias Aschenbrenner and Christopher Hillar this problem is treated and a generalization for the case of an infinite set X of indeterminates is given. In Chapter 2 we will discuss this result, and in Chapter 3 we will study in more detail a property that some groups have that allow the techniques of Aschenbrenner and Hillar to be applied. In a more recent paper [2], of 2013, Martin del Campo and Christopher Hillar develop some results concerning the relation of the previous results to invariant chain of ideals, we will briefly discuss this results in Chapter 4.

1.2 Invariant Ideals of Polynomial Rings

Let X be an infinite set of indeterminates, and let A be a noetherian commutative ring. Consider the polynomial ring $R = A[X]$ and let G be a permutation group of X. G acts on R in the following way: given $\sigma \in G$ and $f(x_1, ..., x_n) \in R$ we have

$$\sigma f(x_1, ..., x_n) = f(\sigma x_1, ..., \sigma x_n)$$

This action allows us to consider R as a left module over the skew group ring $R \star [G]$, which is defined as the set of linear combinations:

$$R \star [G] = \{\sum_{i=1}^{n} f_i \sigma_i : n \in \mathbb{N}, f_i \in R, \sigma_i \in G\}$$

Multiplication is given by $f_i\sigma_i \cdot f_j\sigma_j = f_i(\sigma_i f_j)(\sigma_i\sigma_j)$, and extended by linearity. An ideal $I \subset R$ is called invariant (under the action of G) if

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

The symmetric group of X will be denoted as S_X. An interesting subgroup of S_X that we will use in the next chapter is the finitary symmetric group denoted as $FSym(X)$, and defined as the subgroup of S_X consisting of all permutations that fix all but finitely many elements in X.

Example 1.2.1. *Let $X = \{x_1, x_2, ...\}$ be a set of indeterminates, and let A be a ring. Let I be the ideal generated by $\{x_i + x_j | 1 \leq i < j \text{ and } i, j \in \mathbb{N}\}$. Note that for any permutation σ, $\sigma(x_i + x_j) = x_{\sigma i} + x_{\sigma j} \in I$, and as a consequence $S_X I = I$. An example of an non-invariant ideal is the ideal generated by x_1.*

Remark 1.2.2. *Note that because of submodule definition, invariant ideals are just the $R \star [G]$-submodules of R.*

One of the results presented in [1], which is somehow an analogue of the HBT in the case of an infinite set X, states:

Theorem 1.2.3. *Every ideal of R invariant under the action of S_X is finitely generated as an $R \star [S_X]$-module.*

In other words R is Noetherian as an $R\star[S_X]$-module. In the next section we will discuss the proof presented in [1] of this fact. It's also important to note that the statement given in [1] of this theorem has a mistake. They claim R is Noetherian as an $R[S_X]$-module. However, R is not an $R[S_X]$-module: given $r, s \in R[S_X]$ and $f \in R$ it's not true that $(rs)f = r(sf)$. Nevertheless, the proof doesn't use this multiplicative structure so that the theorem is still true with the usage of the skew group ring. We found this skew group ring in a paper of 2012 by Christopher Hillar and S. Sullivant [3], which is related to the topic.

Chapter 2

Proof of Invariant Ideal's Theorem

The outline of the proof of Theorem 1.2.3 is as follows: the basic idea is to generalize the notion of Groebner bases, show that invariant ideals have finite Groebner bases (an analogue of Dickson's Lemma) and prove that this implies noetherianity. To achieve these results we will construct an ordering on monomials, the symmetric cancellation ordering, and show that it is a well-quasi-ordering on monomials. The symmetric cancellation ordering will allow us to create a notion of polynomial reduction and consider leading term ideals as final segments. Then, using the fact that final segments corresponding to well-quasi-orderings have finitely many minimal elements, we will obtain that invariant ideals have finite Groebner bases. We will start developing some required order theory, followed by the definition of the symmetric cancellation ordering and the proof that it is a well-quasi-ordering. After this, we will generalize Groebner bases theory and prove Theorem 1.2.3. In Chapter 3 we will discuss a property that some groups have, which is related to the symmetric cancellation ordering.

2.1 Preliminaries

Definition 1. *Let S be a set and $\leq$ a binary relation on S. A quasi-ordered set is a pair $(S, \leq)$ where the relation $\leq$ is reflexive and transitive. If in addition the relation is anti-symmetric we say the pair $(S, \leq)$ is an ordered set. A totally ordered set is an ordered set in which the relation $\leq$ satisfies comparability ($\forall a, b \in S$ either $a \leq b$ or $b \leq a$). In order to simplify the notation we will refer to S as a quasi-ordered set (respectively ordered or totally ordered set) when the relation is understood.*

Given a quasi-ordered set $(S, \leq)$ we can induce an ordering on the set $S/\sim$ of equivalence classes, where the equivalence relation is defined as $s \sim t \leftrightarrow s \leq t$ and $s \geq t$.

Definition 2. *Given a quasi-ordered set $(S, \leq)$, we say a subset $A \subseteq S$ is an antichain if A is a set of pairwise incomparable elements. We say $F \subset S$ is a final segment (or closed subset) if given $s \in S, t \in F$ such that $t \leq s$, then $s \in F$. A subset $I \subset S$ is an initial segment if I^c is a final segment.*

Definition 3. *Given a quasi-ordered set $(S, \leq)$ we say it is well-founded if there is no infinite strictly decreasing sequence $s_1 > s_2 > s_3 > \ldots$ in S; if in addition every antichain is finite we say that it is a well-quasi-ordered set. We say a pair $(S, \leq)$ is well-ordered if it is a total order and a well-quasi-order.*

In case we are given a well-quasi-ordered set, we have the following equivalences that will be helpful for our purposes. (See for instance [5])

Lemma 2.1.1. *For a quasi ordered set S, the following are equivalent:*

1. *S is well-quasi-ordered.*
2. *For every infinite sequence $s_1, s_2, \ldots$ in S there exist $i, j \in \mathbb{N}$, such that $i < j$ and $s_i \leq s_j$. (Such a sequence is called good)*
3. *Every infinite sequence $s_1, s_2, \ldots$ in S contains an infinite increasing subsequence.*
4. *Any final segment is generated by finitely many elements.*

The antichain definition given in [1] is quite different from the one we are presenting in this document. The definition given in [1] is: $A \subseteq S$ is an antichain if $\forall a, b \in A$ such that $a \nsim b$ then a, b are incomparable. However, this definition seems to be wrong, for instance: Let S be an infinite set and define the following quasi-ordering on S, $\forall s, t \in S$ $s \leq t$ and $t \leq s$. Note that every infinite sequence is good, so in view of Lemma 2.1.1 we have that S is a well-quasi-ordering. However, if we use the definition presented on [1] we would obtain that S is an infinite antichain contradicting the fact that S is a well-quasi-ordering. Using this definition and similar constructions is also possible to give counterexamples of Lemma 2.1.3. It's important to recall that this definition doesn't affect the development given in [1] since the symmetric cancellation ordering is anti-symmetric, so that both definitions agree.

Remark 2.1.2. *A totally ordered set is a well-quasi-ordering if and only if it is well-founded. To see this suppose for the sake of contradiction that there is an infinite antichain A. Let $a, b \in A$ such that $a \neq b$, then $a \nleq b$ and $a \ngeq b$ contradicting $\leq$ total order. So in fact an antichain cardinality is less or equal than 1.*

In view of this remark we can think of a well-ordered set just as a totally ordered set with no infinite strictly decreasing sequence.

Definition 4. *Let $(S, \leq_S)$ and $(T, \leq_T)$ be quasi ordered sets. We say a map $\phi : S \to T$ is decreasing if $s \leq_S t \implies \phi(s) \geq_T \phi(t)$. A map $\phi : S \to T$ is said to be increasing if $s \leq_S t \implies \phi(s) \leq_T \phi(t)$.*

The following lemma will be helpful to show that certain orders are well-quasi-orderings.

Lemma 2.1.3. *Let $(S, \leq_S)$ be a well-quasi-ordered set, and let $(T, \leq_T)$ be a quasi ordered set. If there exist an increasing surjection $\phi : S \to T$, then T is a well-quasi-ordered set.*

Proof. We need to prove the antichain and decreasing sequence condition. Let A be an antichain in T. If $|A| = 1$ we are done, so we can assume $|A| \geq 2$. For every $a \in A$ take an element $a' \in \phi(a)^{-1}$, call this set A'. Let $a', b' \in A'$ such that $\phi(a') = a$ and $\phi(b') = b$ for some different elements $a, b \in A$. Since

the map is increasing we have that $a' \leq_S b'$ implies $a \leq_T b$, contradicting the fact that a, b are different elements that belong to an antichain. A similar argument shows that $a' \ngeq_S b'$. This shows A' is an antichain in S, so that A can only have finitely many elements.
For a contradiction suppose there is an infinite strictly decreasing sequence $t_1 >_T t_2 >_T ...$ in T. For each $i \in \mathbb{N}^+$ pick an element t'_i of the inverse image of t_i. Since S is a well-quasi-orering then by Lemma 2.1.1, we have that $\{t'_i\}_{i=1}$ is good, that is for some $i < j$ we have $t'_i <_S t'_j$. Nevertheless, the map is increasing so $t'_i <_S t'_j$ implies $t_i <_T t_j$, contradicting the fact that the original sequence was strictly decreasing. □

Remark 2.1.4. *Suppose we are given $(S, \leq)$ a well-quasi ordered set, and $(S, \leq_S)$ a quasi-ordering such that $\leq_S$ extends $\leq$. Note that the inclusion $i : (S, \leq) \to (S, \leq_S)$ is an increasing surjection, that is: $s \leq t \implies i(s) \leq_S i(t)$. So using the above lemma we obtain that $(S, \leq_S)$ is also a well-quasi-ordering.*

Lemma 2.1.5. *Let $(S, \leq)$ be a well-quasi-ordered set and T a well-founded set. Given a decreasing map $\phi : S \to T$ the relation $\leq_\phi$ on S, defined as $s \leq_\phi t :\iff s \leq t$ and $\phi(s) = \phi(t)$, is a well-quasi-ordering.*

Proof. Let $\{s_i\}_{i\in\mathbb{N}}$ be a sequence in S. Because of Lemma 2.1.1 we know there is an infinite subsequence $\{s_{n_i}\}_{i\in\mathbb{N}}$ such that $s_{n_i} \leq s_{n_j}$ for all $i < j$. Since ϕ is decreasing we have that for all $i < j$, $\phi(s_{n_i}) \geq \phi(s_{n_j})$. Therefore, we obtain the following decreasing sequence $\phi(s_{n_0}) \geq \phi(s_{n_1}) \geq \phi(s_{n_2}) \geq ....$ Since T is well-founded there can not be infinite strictly decreasing sequences, so that $\phi(s_{n_i}) = \phi(s_{n_j})$ for infinitely many $i, j \in \mathbb{N}$. So that $\{s_i\}_{i\in\mathbb{N}}$ contains an infinite increasing subsequence with respect to $\leq_\phi$, and by Lemma 2.1.1 this implies that $(S, \leq_\phi)$ is a well-quasi-ordered set. □

In Section 2.2 we will be interested in the case we have a special ordering of X. Let X be a countable set. Note that we can well-order this set with the additional property that $|I| < |X|$ for all proper initial segments $I \subset X$. We will call such an ordering a cardinal well-ordering. In case X is an infinite countable set equipped with a cardinal well-ordering, we can identify X with the natural numbers and its usual order. In general, using the axiom of choice any set X can be equipped with such an ordering. However, since we are not interested in uncountable sets we will not discuss this fact.
Up to now we have discussed some order theory with respect to a set X.

However, in order to define the symmetric cancellation ordering we need a way to compare monomials. Given a set of indeterminates X we denote $X^\diamond$ as the set of commutative words in the alphabet X. If we allow $X^\diamond$ to have concatenation as an operation, we obtain a monoid.

Definition 5. *A term ordering of $X^\diamond$ is a well-ordering $\leq$ of $X^\diamond$ that satisfies:*

1. $1 \leq x$ *for all* $x \in X$.
2. $y \leq w \implies xy \leq xw$ *for all* $x \in X$.

We define the divisibility relation on $X^\diamond$ as: $v|w :\iff uv = w$ for some $u \in X^\diamond$. One interesting property that term orders satisfy is:

Lemma 2.1.6. *Let $\leq$ be a term ordering, and let $v, w \in X^\diamond$ and suppose $v|w$, then $v \leq w$.*

Proof. Suppose for the sake of contradiction that $v > w$. Since $v|w$ there exist $u \in X^\diamond$ such that $uv = w$. Now, by term order definition we have $v > w \implies w = uv \geq uw$. These terms are not equal so $w > uw$. Note that using again this property we obtain $w > uw \implies uw > uw^2$, so that we obtain a chain $w > uw > uw^2$. Note that doing the same process we could obtain an infinite strictly decreasing sequence $w > uw > uw^2 > ...$, contradicting that $\leq$ is a well-order. □

Remark 2.1.7. *We have that term orders are linear; that is: given monomials v, w, u we have $v \leq w \iff uv \leq uw$. In order to show this we only require $v \leq w \iff xv \leq xw$ where $x \in X$. One direction is just the definition, for the other suppose that $xv \leq xw$ but $v > w$. However, this implies $xv \geq xw$ so $xv = xw$ and as a consequence $v = w$.*

Example 2.1.8. *Let $X = \{x_1, x_2, ..., x_m\}$ be a set of indeterminates. The lexicographic ordering $\leq_{lex}$ on $X^\diamond$ is defined as: given $v = x_1^{a_1}...x_m^{a_m}$ and $w = x_1^{b_1}...x_m^{b_m}$ in $X^\diamond$, where the exponent vectors $\alpha := (a_1, ..., a_m), \beta := (b_1, ..., b_m) \in \mathbb{N^+}^m$; then $v \leq_{lex} w \iff$ in the vector difference $\beta - \alpha$ the right most nonzero entry is positive. This monomial ordering is a term ordering [6, Chapter 2].*

The lexicographic order allows us to compare monomials in the way a dictionary order works. Nevertheless, you sometimes want to increase the importance of the monomial degree, defined as the sum of the degrees of all the variables, in the comparison of two monomials. There are some modifications to the left lexicographic term order that allows us to do that:

- Graded Lex Order (Grlex): given $v = x_1^{a_1}...x_m^{a_m}$ and $w = x_1^{b_1}...x_m^{b_m}$ in $X^\diamond$, where $(a_1, ..., a_m), (b_1, ..., b_m) \in \mathbb{Z}^m$; then $v \leq_{grlex} w \iff a_1 + ... + a_m < b_1 + ... + b_m$, or $a_1 + ... + a_m = b_1 + ... + b_m$ and $v \leq_{lex} w$.
- Graded Reverse Lex Order(Grevlex): given $v = x_1^{a_1}...x_m^{a_m}$ and $w = x_1^{b_1}...x_m^{b_m}$ in $X^\diamond$, where $\alpha := (a_1, ..., a_m), \beta := (b_1, ..., b_m) \in \mathbb{Z}^m$; then $v \leq_{grevlex} w \iff a_1+...+a_m < b_1+...+b_m$, or $a_1+...+a_m = b_1+...+b_m$ and in the vector difference $\beta-\alpha$ the left most nonzero entry is negative.

Grlex and Grevlex are both term orderings [6, Chapter 2]. Note also that they order the variables in the same way that lexicographic order does, that is:

$$x_{n+1} \geq x_n \text{ for all } n \in [m]$$

Example 2.1.9. *We can actually define these orders for an arbitrary set of indeterminates X. By the Axiom of Choice we can well-order the set X. Now, given $v, w \in X^\diamond$ we can write $v = x_1^{a_1}...x_m^{a_m}$ and $w = x_1^{b_1}...x_m^{b_m}$, where $x_1, ..., x_m \in X$, $x_1 < x_2 < ... < x_m$ and the exponent vectors are $\alpha := (a_1, ..., a_m), \beta := (b_1, ..., b_m) \in \mathbb{N}^{+m}$; then $v \leq_{lex} w \iff$ in the vector difference $\beta - \alpha$ the right most nonzero entry is positive; that is if $\alpha \leq \beta$ lexicographically from the left.*

Lemma 2.1.10. *Let X be an arbitrary set of indeterminates, and let $\leq$ be a well-ordering on X. The lexicographic order defined above is a term ordering on $X^\diamond$.*

Proof. To compare monomials we only require the variables found in those monomials, which are finite. Then the reflexivity, transitivity, anti-symmetry, comparability, and properties 1, 2 of the definition of term order, follows directly from the fact that these properties hold in the finite case. So we only need to show that the ordering on $X^\diamond$ is well-founded. In [1] there is exposed a nice way of proving such fact. Below we will briefly discuss such method. □

One useful way to prove that a certain total ordering on monomials is a term ordering is to use Higman's lemma: Let X be a set and let $\leq$ be a quasi-ordering on X. We denote X^* as the set of non-commmutative words in the X alphabet. Define the Higman quasi-ordering (with respect to $\leq$) as follows:

$$x_1...x_m \leq_H y_1...y_n :\iff \begin{pmatrix} \text{There is a strictly increasing function} \\ \phi : [m] \to [n] \text{ such that} \\ x_i \leq y_{\phi(i)} \text{ for all } i \in [m]. \end{pmatrix}$$

We have the following lemma, due to Higman [5, Theorem 4.3].

Lemma 2.1.11. *If $\leq$ is a well-quasi-ordering on X, then $\leq_H$ is a well-quasi-ordering on X^*.*

Recall that $X^\diamond$ is the set of commutative words in the X alphabet. We have the following surjective homomorphism $\pi : X^* \to X^\diamond$ where $\pi(w)$ is just the commutative word. The Higman quasi order is not compatible with $X^\diamond$ in the sense that given non-commutative words v, v', w, w' such that $\pi(v) = \pi(v'), \pi(w) = \pi(w')$, it's not necessarily true that $v \leq_H w \implies v' \leq_H w'$. However, we can modify this ordering and construct a new quasi-ordering that satisfies this requirement:

$$x_1...x_m \leq^* y_1...y_n :\iff \begin{pmatrix} \text{There is an injective function} \\ \phi : [m] \to [n] \text{ such that} \\ x_i \leq y_{\phi(i)} \text{ for all } i \in [m]. \end{pmatrix}$$

Note that $\leq^*$ extends $\leq_H$, so in view of Remark 2.1.4 and Higman's lemma if $\leq$ is a well-quasi-ordering on X, then $\leq^*$ is also a well-quasi-ordering on X^*. This ordering satisfies $v \leq^* w \implies v' \leq^* w'$, for all non-commutative words v, v', w, w' such that $\pi(v) = \pi(v'), \pi(w) = \pi(w')$, then we can define the following quasi-ordering on $X^\diamond$, denoted as $\leq^\diamond$.

$$\pi(v) \leq^\diamond \pi(w) :\iff v \leq^* w.$$

Note that this relation makes π into an increasing map. Then π is an increasing surjection, so using Remark 2.1.4 we obtain the following corollary.

Corollary 2.1.12. *If $\leq$ is a well-quasi-ordering on a set X, then $\leq^\diamond$ is a well-quasi-ordering on $X^\diamond$.*

This corollary is useful to show that a certain total order on $X^\diamond$ is a term order: Let $\leq$ be a total order on a set X satisfying conditions 1) and 2) of the definition of term order, $\leq$ extends the ordering $\leq^\diamond$ obtained from the restriction of $\leq$ to X. So in view of Remark 2.1.4, to prove that $\leq$ is a well-order we only need to show that $\leq^\diamond$ is a well-quasi-ordering. However, by the corollary above it's enough to show that the restriction of $\leq$ to X is a well-quasi-ordering.

2.2 Symmetric cancellation ordering

We can now state the symmetric cancellation ordering. Let G be a permutation group acting on a set X. The action of G on X extends to an action of G on $X^\diamond$: for $\sigma \in G$ and $v = x_1...x_n \in X^\diamond$ we have $\sigma v = \sigma x_1 ... \sigma x_n$. Given $\leq$ a term ordering of $X^\diamond$ define:

Definition 6. *The symmetric cancellation ordering with respect to $\leq$ and G:*

$$v \preccurlyeq w :\Longleftrightarrow \begin{pmatrix} v \leq w \text{ and there exists } \sigma \in G \text{ such that} \\ \sigma v | w \text{ and } \sigma v' \leq \sigma v \text{ for all } v' \leq v \end{pmatrix}$$

In this case we say σ witnesses $v \preccurlyeq w$

Example 2.2.1. *Let $X = \{x_1, x_2, ...\}$ and $G = S_X$. Define $\leq$ as the lexicographic ordering on $X^\diamond$.*

- *We have that $x_1^3x_2^2 \preccurlyeq x_2^3x_4^2x_5$. Note that $x_1^3x_2^2 \leq x_2^3x_4^2x_5$, and $\sigma(x_1^3x_2^2)$ divides $x_2^3x_4^2x_5$, where $\sigma = (124)$. Let $v' \leq x_1^3x_2^2$. Since we are using lexicographic ordering we have $v' = x_1^{a_1}x_2^{a_2}$ where $a_2 = 2$ and $a_1 \leq 3$, or $a_2 < 2$. In both cases we obtain that $\sigma(v') = x_2^{a_1}x_4^{a_2}$ satisfies $\sigma(v') \leq \sigma(x_1^3x_2^2)$. So that $x_1^3x_2^2 \preccurlyeq x_2^3x_4^2x_5$.*
- *Note that $x_1^3x_2^2 \leq x_1^2x_4^3x_5$. The only way to obtain that $\sigma(x_1^3x_2^2)$ divides $x_1^2x_4^3x_5$ is with a permutation such that $\sigma(x_1) = x_4$ and $\sigma(x_2) = x_1$. However, if $x_1^4x_2 = v'$ then $v' \leq x_1^3x_2^2$, but $\sigma(v') = x_1x_4^4$ which is bigger than $\sigma(x_1^3x_2^2) = x_1^2x_4^3$. So that $x_1^3x_2^2 \not\preccurlyeq x_1^2x_4^3x_5$.*

Note that in this example the permutation that allowed monomials to be related was increasing in the indices appearing in $x_1^3x_2^2$. On the other hand, the 2 monomials that were not related didn't allow a permutation of this kind. In general we have the following lemma. This lemma doesn't appear in [1], but is a helpful observation.

Lemma 2.2.2. *Let X be a well ordered set, let $v, w \in X^\diamond$, and assume $\leq$ is the lexicographic ordering. Then, $v \preccurlyeq w \iff$ there exist $\sigma \in G$ such that $\sigma(v)|w$ and given $x_i < x_j$ variables such that x_j appears in v then $\sigma(x_i) < \sigma(x_j)$.*

Proof. " $\Rightarrow$ " Suppose that there exist variables $x_i < x_j$ such that x_j appears in v and $\sigma(x_i) > \sigma(x_j)$. Define v' as the monomial obtained when removing the x_j variable in v, and adding one x_i. For example if $v = x_1^2 x_2^3 x_4$ and $i = 1, j = 2$, then when removing the x_j variable we obtain $x_1^2 x_4$, and by adding one x_i we obtain $v' = x_1^3 x_4$. Note that since $x_i < x_j$ then $v' \leq v$. Now, all variables different from x_j appearing in v also appear in v', moreover $\sigma(v)$ and $\sigma(v')$ only differ in the $\sigma(x_i)$ and $\sigma(x_j)$ variable. However, $\sigma(x_i) > \sigma(x_j)$ and the variable x_i has higher degree in v' than in v, so that $\sigma(v) < \sigma(v')$ contradicting the definition of the ordering.
" $\Leftarrow$ " Let $v' \leq v$, and let x_n, x_m be the higher variables appearing in v', v respectively. Since we are using lexicographic ordering then $x_n \leq x_m$. In case $x_n < x_m$ then by hypothesis $\sigma(x_n) < \sigma(x_m)$, and since all variables x_i appearing in v' satisfy $x_i < x_n < x_m$ then $\sigma(x_i) < \sigma(x_m)$, so $\sigma(v') < \sigma(v)$. On the other hand, if $x_n = x_m$ then $a_n \leq b_m$ where a_n, b_m are the degrees of x_n and x_m respectively. If $a_n < b_m$ then $\sigma(x_n^{a_n}) < \sigma(x_m^{b_m})$, so $\sigma(v') \leq \sigma(v)$. Finally, if $a_n = b_m$ consider $h' = \frac{v'}{x_n^{a_n}}$ and $h = \frac{v}{x_m^{b_m}}$. We have that if $\sigma(h') \leq \sigma(h)$ then $\sigma(v') < \sigma(v)$. Note that $h' \leq h$ and for all indeterminates $x_i < x_j$ such that x_j appears in h we have $\sigma(x_i) < \sigma(x_j)$. Therefore, we can apply the process just described and by induction obtain $\sigma(h') \leq \sigma(h)$. □

One interesting fact about the symmetric cancellation ordering, is that if $v \preccurlyeq w$ then the witness permutation must satisfy $\sigma(v') \leq \sigma(v)$. This requirement is needed in order to have an useful cancellation of leading terms.

Lemma 2.2.3. *Let $f \in A[X]$, where A is a ring and X is a set of indeterminates. Let G be a permutation group of X, and let $v, w \in X^\diamond$. If $\sigma \in G$ witnesses $lm(f) \preccurlyeq w$ then $lm(u\sigma f) = u\sigma lm(f)$, where $u\sigma lm(f) = w$.*

Proof. Note that every monomial appearing in $u\sigma(f)$ has the form $u\sigma(v)$ for some $v \in X^\diamond$. By the ordering definition we know $v' \leq lm(f)$ satisfies $\sigma(v') \leq \sigma lm(f)$, so that $u\sigma(v') \leq u\sigma lm(f)$. Therefore, no monomial appearing in $u\sigma(f)$ is bigger than $u\sigma lm(f)$. □

As a consequence, if f, g are polynomials such that $lm(f) \preccurlyeq lm(g)$ and if σ witnesses this relation, then the polynomial $h = g - \frac{lt(g)}{\sigma(lt(f))}\sigma(f)$ has a lower leading monomial than g; that is: $lm(f) > lm(h)$. In the Groebner bases section we will discuss why this ordering definition is appropriate.

Lemma 2.2.4. *The symmetric cancellation ordering is an ordering on* $X^\diamond$

Proof.

- Reflexivity: Let $w \in X^\diamond$. By reflexivity of $\leq$ we have $w \leq w$. Let $\sigma \in G$ be the identity then $\sigma w | w$. Finally let $v \in X^\diamond$ such that $v \leq w$, since σ is the identity we have $\sigma v \leq \sigma w$.

- Transitivity: Suppose $z \preccurlyeq v \preccurlyeq w$. By transitivity of $\leq$, we obtain $z \leq w$. By definition there exist elements $\sigma, \tau \in G$ such that $\sigma z | v$ and $\tau v | w$. As a consequence there exist monomials $u_1, u_2 \in X^\diamond$ such that $u_1 \sigma z = v$ and $u_2 \tau v = w$. Replacing we obtain $w = u_2 \tau(u_1 \sigma z) = u_2(\tau u_1)(\tau\sigma z)$ so that $\tau\sigma z | w$. Finally if $v' \leq z$ then $\sigma v' \leq \sigma z$ which implies $u_1 \sigma v' \leq u_1 \sigma z = v$. The relation $u_1 \sigma v' \leq v$ implies $\tau u_1(\tau\sigma v') \leq \tau v = \tau u_1(\tau\sigma z)$. Now, since term orders are linear we have $\tau\sigma v' \leq \tau\sigma z$.

- Anti-symmetry: Suppose $v \preccurlyeq w$ and $w \preccurlyeq v$. By definition $v \leq w$ and $w \leq v$, so that $v = w$.

□

Recall that we want this symmetric cancellation ordering to be a well-quasi-ordering, since this definition depends on the choice of a group and a well-ordering on monomials we will use the following notation.

Definition 7. *Let $\leq$ be a term ordering on $X^\diamond$. We say $\leq$ is lovely for G if the symmetric cancellation order (with respect to $\leq$ and G) is a well-quasi-ordering.*

Remark 2.2.5. *Note that if $\leq$ is lovely for a subgroup G' of G, then $\leq$ is also lovely for G.*

We will close this section showing that the lexicographic ordering corresponding to a cardinal well-ordering of a countable set X is lovely for S_X, which will be fundamental to show Theorem 1.2.3. In order to achieve this, we will show that the lexicographic ordering is lovely for $FSym(X)$. Recall that a cardinal well-ordering of X allows us to identify X with $\mathbb{N}$ and its usual ordering, so we can enumerate the elements of X as $x_1 < x_2 < x_3 < \ldots$. However, the fundamental fact behind the usage of a cardinal well-ordering is Lemma 2.2.2. Note that because of this lemma, in order to prove $v \preccurlyeq w$ we only have to focus our attention on the initial segment $I_v := \{x_i \in X : x_i < x$ where x is the highest variable appearing in v $\}$ (we will continue using this notation to define such a set); that is: we only require an inyective function $f : I_v \to X$ that satisfies the hypothesis of the lemma, and prove that f can be extended to a permutation of X. Nevertheless, if X is just a well-order then I could have the same cardinality as X so that f could be a bijection. Cardinal well-orderings avoid this kind of situations, as the following lemma shows.

Lemma 2.2.6. *let X be a cardinal well-ordered set, and let I be a proper initial segment of X. If f is an injective function $f : I \to X$ then f can be extended to a permutation of X.*

Proof. In case X is finite the result is clear, so assume X is infinite. Recall from set theory that given A, B sets such that one of them is infinite then $|A \cup B| = max\{|A|, |B|\}$. We have that $X = I \cup \{X - I\}$. Now since X is infinite then one of theses sets must by infinite so $|X| = max\{|I|, |X - I|\}$. By hypothesis $|I| < |X|$, so that $|X| = |X - I|$. Since f is injective we have $|I| = |f(I)|$, so using a similar argument we obtain $|X| = |X - f(I)|$. Therefore, there exists a bijection $g : X - I \to X - f(I)$. Finally, defining $\sigma(x)$ as $f(x)$ when $x \in I$, and $g(x)$ when $x \in X - I$ we obtain a permutation of X. □

So in order to show $v \preccurlyeq w$, we only have to focus our attention on the set I_v. As a consequence of this lemma we also obtain the following corollary. In [1] this corollary only applies to a countable set X; here we present a generalization for an arbitrary set X.

Corollary 2.2.7. *Let X be a cardinal well-ordered set, and let $\preccurlyeq$ be the symmetric cancellation ordering with respect to S_X and the lexicographic ordering. If $\sigma \in S_X$ witnesses the relation $v \preccurlyeq w$, then we can select a σ with* *an additional property: $\sigma(x) = x$ for all $x > x_n$, where x_n is the highest indeterminate appearing in w.*

Proof. Since $v \preccurlyeq w$ then there exist $\tau \in S_X$ that witnesses the relation. Now, in view of Lemma 2.2.2 we know $\tau(x_j) < \tau(x_i) \leq x_n$ for all indeterminates $x_j < x_i$ such that x_i appears in v. Therefore, we have an inyective function $\tau' : I_v \to X_n$ where $X_n := \{x \in X : x \leq x_n\}$. In view of above lemma we know τ' can be extended to a permutation of X_n. Finally, define $\sigma : X \to X$ as $\sigma(x) = x$ for all $x > x_n$, and $\sigma(x) = \tau'(x)$ for $x \leq x_n$. □

In the case of a countable set X equipped with a cardinal well-ordering, every initial segment is finite so above corollary shows that if $v \preccurlyeq w$ with respect to S_X then $v \preccurlyeq w$ with respect to $FSym(X)$. Therefore, it makes sense to think that the lexicographic ordering is lovely for $FSym(X)$.

Theorem 2.2.8. *Let X be a countable set of indeterminates, and define a cardinal well-ordering $\leq$ on X. The lexicographic ordering of $X^\diamond$ is lovely for $FSym(X)$*

By using the ideas used in [1] to proof this fact, we were able to generalize this theorem, we will discuss such generalization in chapter 3. Therefore, Theorem 2.2.8 can be viewed as a corollary:

Proof. Because of previous lemma we can assume X is infinite, therefore we can apply Theorem 3.0.25 and obtain the result. □

In [1] there is a proof for the fact that if we are given any set X equipped with a cardinal well-ordering, then the lexicographic ordering is lovely for S_X. However, since we were not interested in the case of an uncountable set of indeterminates we decided not to discuss this proof. On the next chapter we will consider a countable set X equipped with a cardinal well-ordering and discuss other groups G, such that the lexicographic ordering is lovely for G.

2.3 Groebner bases

Our goal in this section is to prove Theorem 1.2.3. In order to achieve this result we will generalize the ideas of Groebner basis theory. Recall that in the case of a field k and a finite set of indeterminates X, in order to develop the theory of Groebner bases, over the polynomial ring $R = k[X]$, we needed a division algorithm (see for instance [5, Chapter 1]); that is given $f, g \in R$, if some term v of f is divisible by $lt(g)$ then $f \to_g h = f - \frac{v}{lt(g)}(g)$, so that in h the term v is missing and all new terms added have lower degree than v. By repeating this process we obtained a division algorithm (which was finite because all new terms had lower degree). In a more general case when we were given just a commutative notherian ring A, see for instance [5, Chapter 4], we defined a similar way to reduce polynomials: given $f, g \in R$, instead of dividing $lt(g)$ by some term of f, we just divided $lt(g)$ by $lt(f)$, so that $f \to_g h = f - \frac{lt(f)}{lt(g)}(g)$ and h satisfied $lm(h) < lm(f)$. As is pointed out in [5], in such context we only require to divide leading terms because the uniqueness of reduced Groebner bases is not guaranteed. Therefore, there is no need to ask for more conditions in our reduction. The following example appears as exercise 4.1.6 in [5].

Example 2.3.1. *Let $\langle 2x^2, 3y^2 + x\rangle, \langle 2x^2, 3y^2 + 3x^2\rangle$ be ideals of $\mathbb{Z}[x, y]$. Note that they are equal, and if we allow a reduced Groebner basis definition, both bases will satisfy such property.*

Finally, to divide f by a set B of polynomials, we had that $f \to_B h$ if $h = f - \sum_{i=1}^{n} a_i w_i b_i$ for some $b_i \in B$, $lm(f) = w_i lm(b_i)$ and $lc(f) = \sum_{1=1}^{n} a_i lc(b_i)$. In our context we would like to follow a similar process.
Let A be a commutative notherian ring, and let X be an infinite set of indeterminates and define $R := A[X]$. Fix a term ordering $\leq$ of $X^\diamond$, and let G be a permutation group over X. As we have seen R is a $R\star[X]$-module. Since we want to prove that every invariant ideal I satisfies $I = \langle f_1, ..., f_n\rangle_{R\star[G]}$ then we would like to show that if $f \in I$ then $f = \sum_{i=1}^{n} h_i \sigma_i(f_i)$. Therefore, given $B \subset R$ and $f \in R$ the first step of our polynomial reduction should be to write $lt(f) = \sum_{i=1}^{n} a_i w_i \sigma_i lt(f_i)$ where $f_i \in B$, $a_i \in A$, $w_i \in X^\diamond$,$\sigma_i \in G$, $lm(f) = w_i \sigma_i(lm(f_i))$ and $lc(f) = \sum_{i=1}^{n} a_i lc(f_i)$.

Example 2.3.2. *Let $f = 3x_3^2 x_4^2 + x_1, f_1 = 2x_1^2 x_2^2 + x_1^3, f_2 = x_1^2 x_2^2$ be polynomials in $\mathbb{Z}[X]$. We have that $lm(f_1) = lm(f_2) = x_1^2 x_2^2$. Then, if $\sigma = (14)(23)$*

we obtain $\sigma(lm(f_1)) = \sigma(lm(f_2)) = x_3^2x_4^2$.

$$lt(f) = 3x_3^2x_4^2 = 2x_1^2x_2^2 + x_1^2x_2^2 = \sigma(lt(f_1)) + \sigma(lt(f_2))$$

Then, we would like to consider a polynomial h such that the term $lt(f)$ is missing, and repeat the process just described for h. Note that the polynomial $h = f - \sum_{i=1}^{n} a_i w_i \sigma_i(f_i)$ satisfies such condition. However, if we want this reduction to be finite we want $lm(h) < lm(f)$.

Example 2.3.3. *In the previous example we had* $f = 3x_3^2x_4^2 + x_1, f_1 = 2x_1^2x_2^2 + x_1^3, f_2 = x_1^2x_2^2$, *and* $\sigma = (14)(23)$

$$lt(f) = 3x_3^2x_4^2 = 2x_3^2x_4^2 + x_3^2x_4^2 = \sigma(lt(f_1)) + \sigma(lt(f_2))$$

Therefore, the h polynomial is

$$h = f - (\sigma(f_1) + \sigma(f_2)) = 3x_3^2x_4^2 + x_1 - (\sigma(2x_1^2x_2^2 + x_1^3) + \sigma(x_1^2x_2^2))$$

$$h = x_1 - \sigma(x_1^3) = x_1 - x_4^3$$

whose leading monomial is bigger than lm(f).

Therefore, we need an additional requirement in the polynomial reduction so that $lm(h) < lm(f)$. Note that if $v \leq lm(f_i)$ implies $\sigma_i(v) \leq \sigma_i(lm(f_i))$ for all monomials v lower than $lm(f_i)$, then $lm(h) < lm(f)$; that is: the symmetric cancellation ordering. In view of these facts we see how the symmetric cancellation ordering is appropriate for our purposes. To sum up, we have the following definition of reduction of polynomials.

Definition 8. *Let f be a nonzero element in R and let B be a subset of R. Denote as $\preccurlyeq$ the symmetric cancellation ordering with respect to G and $\leq$. We say f is reducible by B, if there exist distinct elements $f_1, ...f_n \in B$, such that $lm(f_i) \preccurlyeq lm(f)$, and*

$$lt(f) = a_1 w_1 \sigma_1 lt(f_1) + ... + a_m w_m \sigma_m lt(f_n)$$

where $a_1, ..., a_n \in A$, σ_i witnesses $lm(f_i) \preccurlyeq lm(f)$ and $w_i\sigma_i(f_i) = lm(f)$.

Instead of saying f is reducible by B we will just say $f \to_B h$, where $h = f - (a_1 w_1 \sigma_1 f_1 + ... + a_m w_m \sigma_n f_n)$. In case some polynomial g is not reducible by B we say g is reduced with respect to B. We will say that the zero polynomial is reduced with respect to B.

Remark 2.3.4. *Note that in case A is a field, the fact that f is reducible by B just means that $lm(g) \preccurlyeq lm(f)$ for some $g \in B$. If X is finite and $G = \{id\}$ we obtain the usual reductions.*

In case we have $f \rightarrow_B h_1 \rightarrow_B h_2 ... \rightarrow_B h_n$ where $f, h_i \in R$ and h_i is reduced with respect to B, we will say $f \rightarrow_B^* h_n$. Note that in such a case $f - h_n \in \langle B \rangle_{R\star[G]}$.

Definition 9. *We call r a normal form of f with respect to B if $f \rightarrow_B^* r$ and r is reduced with respect to B.*

Lemma 2.3.5. *If $f \rightarrow_B h$ for some non-zero elements $f, h \in R$, then there exist a normal form r of f with respect to B. We also have that there exist $f_1, ..., f_n \in B$, $\sigma_1, ..., \sigma_n \in G$ and $g_1, ..., g_n \in R$ such that:*

$$f = r + \sum_{i=1}^{n} g_i \sigma_i f_i \text{ and } lm(f) \geq \max_{1 \leq i \leq n} lm(g_i \sigma_i f_i)$$

Proof. To see the first claim, note that $f \rightarrow_B h$ implies $lm(h) < lm(f)$. Therefore, every chain $f \rightarrow_B h \rightarrow_B h_1 \rightarrow_B h_2 ...$ where all h_i are different from 0 must end. So for some r, $f \rightarrow_B^* r$ and r is reduced with respect to B. For the second claim, in case h is reduced with respect to B the result is clear. Otherwise there exist $r \in X^\diamond$ such that $f \rightarrow_B h \rightarrow_B^* r$. Since $f \rightarrow_B h$, then there exist $\sigma_1, ..., \sigma_n \in G$, $f_1, ..., f_n \in B$ and $w_1, ..., w_n \in R$ such that

$$f = h + \sum_{i=1}^{n} a_i w_i \sigma_i f_i \text{ and}$$

For $1 \leq i \leq n$ define $g_i := a_i w_i$. Since $lt(f) = \sum_{i=1}^{n} a_i w_i \sigma lt(f_i)$, then $lm(f) = lm(g_i \sigma f_i)$ and $lm(h) < lm(f)$. As a consequence we can inductively find $\sigma_{1+n}, ..., \sigma_{n+m} \in G$, $f_{1+n}, ..., f_{n+m} \in B$ and $g_{1+n}, ..., g_{n+m} \in R$ such that

$$h = r + \sum_{i=n+1}^{n+m} g_i \sigma_i f_i \text{ and } lm(h) \geq \max_{1 \leq i \leq n} lm(g_i \sigma_i f_i)$$

We obtain as a consequence the desired result. □

Note that this lemma is somehow an analogue of the division algorithm. We "divide" f by B an obtain a symmetric linear combination of elements of B, whose leading monomials are lower with respect to our ordering, and a "residue" r not reducible by B.
With this ideas in mind, we can now define Groebner bases. Recall that in the usual case, given an ideal I and a subset $B \in I$ we defined the leading term ideals as $Lt(B) = \langle lt(b) : b \in B\rangle$ and B was a Groebner basis if $Lt(B) = Lt(I)$. This definition was made in order to be compatible with the polynomial reduction used. Therefore, in our context a definition for leading term ideals that is compatible with our polynomial reduction is: given $B \subset R$ then

$$lt(B) := \langle lc(g)w : g \in B \text{ and } lm(g) \preccurlyeq w\rangle_A$$

Note that when our permutation group G is the identity and X is a finite set of indeterminates, this definition coincides with the usual leading term ideal definition. As in the usual case we define Groebner bases as:

Definition 10. *A subset B of an invariant ideal I of R is said to be a Groebner basis for I if $lt(I) = lt(B)$.*

Remark 2.3.6. *Given an invariant ideal I of R we have $lt(I) = \langle lt(f) : f \in I\rangle_A$. Clearly, $\langle lt(f) : f \in I\rangle_A \subset lt(I)$. To see that $lt(I) \subset \langle lt(f) : f \in I\rangle_A$ let $\sum_{i=1}^n a_i lc(g_i)w_i \in lt(I)$, where $a_i \in A$ and $w_i = u_i\sigma_i(lm(g_i))$ for some monomial u_i and a permutation σ_i. Since I is invariant we know $u_i\sigma_i(g_i) \in I$, so $lc(g_i)lm(u_i\sigma_i(g_i)) \in \langle lt(f) : f \in I\rangle_A$. Recall that $u_i\sigma_i(lm(g_i)) = lm(u_i\sigma_i(g_i))$, so that $\sum_{i=1}^n a_i lc(g_i)w_i \in \langle lt(f) : f \in I\rangle_A$.*

The following lemma explains why the leading term ideal definition is appropriate.

Lemma 2.3.7. *Given a non-zero polynomial $f \in R$, then $lt(f) \in lt(B) \iff f$ is reducible by B.*

Proof. " $\Rightarrow$ " We have $lt(f) \in lt(B)$ so that $lt(f) = \sum_{i=1}^n a_i lc(g_i)w_i$, where $a_i \in A$, $g_i \in B$ and $lm(g_i) \preccurlyeq w_i$. Since $a_i lc(g_i) \in A$ then $w_i = lm(f)$, so f is reducible by B.

" $\Leftarrow$ " By definition of reduction and $lt(B)$, it's clear the result. □

These facts allow us to present the following characterization of Groebner bases.

Lemma 2.3.8. *Let I be an invariant ideal of R, and B a subset of non-zero elements of R. We have the following equivalences:*

1. *B is a Grobner basis for I.*
2. *Every non-zero $f \in I$ is reducible by B.*
3. *Every $f \in I$ has 0 as normal form. Moreover, $I = \langle B \rangle_{R\star[G]}$.*
4. *Every $f \in I$ has unique normal form 0.*

Proof. The implication "1) $\implies$ 2)" is just above lemma. For the implication "2) $\implies$ 3)", let $f \in I$ be a non-zero polynomial so by assumption f is reducible by B; that is: $f \to_B h_0$. Since I is an invariant ideal we have that $h_0 \in I$, in case $h_0 \neq 0$ we would have again that h_0 is reducible by B, so $h_0 \to_B h_1$. Therefore, if we keep doing this process and all h_i are different from 0, we would obtain a chain $h_0 \to_B h_1 \to_B h_2 \to_B ....$ Recall that if a, b are non-zero polynomials that satisfy $a \to_B b$, then $lm(a) > lm(b)$. As a consequence above chain would imply $lm(h_0) > lm(h_1) > lm(h_2) > ...$ contradicting the term order definition. Then, some $h_i = 0$ so that $f \to_B^* 0$. Since every $f \in I$ has 0 as normal form, then by Lemma 2.3.5 $I \subset \langle B \rangle_{R\star[G]}$. On the other hand, since I is an invariant ideal then $I = \langle B \rangle_{R\star[G]}$
To prove "3) $\implies$ 4)" suppose $f \to_B^* r$ for some $r \neq 0$. Therefore, by above lemma $lt(r) \notin lt(B)$. Because of Lemma 2.3.5 we know $f - r \in \langle B \rangle_{R\star[G]} = I$, so that $r \in I$. However, by hypothesis this implies that $r \to_B^* 0$ contradicting the fact that r was reduced.
Finally, for the "4) $\implies$ 1)" implication suppose $f \in I$ but $lt(f) \notin lt(B)$. By above lemma this implies that $lt(B)$ is reduced with respect to B. However, this would imply that $f, 0$ ar both normal forms for f. Therefore, $lt(B) = lt(I)$. □

In the following theorem we show that under certain hypothesis invariant ideals have finite Groebner basis. After proving this fact we will see how Theorem 2.2.8 help us to satisfy these hypothesis, and as a consequence to obtain the Theorem 1.2.3.

Theorem 2.3.9. *Suppose $\leq$ is lovely for G. Then every invariant ideal of R has a finite Groebner basis.*

Proof. The proof is as follows. Let I be an ideal of R. Given $w \in X^\diamond$ define the following set: $lc(I, w) := \{lc(f) : f \in I \text{ such that } lm(f) = w\} \cup \{0\}$. This definition makes $lc(I, w)$ into an ideal of A. Define $I(A)$ as the set of ideals of A, and order them by reverse inclusion. Since A is noetherian this definition makes $I(A)$ into a well-founded set. Consider the well-quasi-ordered set $(X^\diamond, \preccurlyeq)$ and define a map $\phi : X^\diamond \to I(A)$ as $\phi(w) = lc(I, w)$. By definition this map is decreasing, then applying Lemma 2.1.5 we obtain a well-quasi-ordering $\leq_\phi$ on $X^\diamond$, defined as: $s \leq_\phi t \iff s \preccurlyeq t$ and $lc(I, w) = lc(I, v)$. Note that $X^\diamond$ is a final segment of $(X^\diamond, \leq_\phi)$. Since $\leq_\phi$ is a well-quasi-ordering we know, because of Lemma 2.1.1, that every final segment has a only finitely many minimal elements. As a consequence there exist a finite subset $\{w_1, ..., w_n\}$ of $X^\diamond$ such that for all $w \in X^\diamond$, $w_i \preccurlyeq w$ and $lc(I, w_i) = lc(I, w)$ for some $i \in [n]$. Since A noetherian, we know each $lc(I, w_i)$ is finitely generated, that is: $lc(I, w_i) = \langle lc(f_{i1}), ..., lc(f_{in_i})\rangle_A$ for some $f_{i1}, ..., f_{in_i} \in I$. Define $B := \{f_{ij} : 1 \leq i \leq n \text{ and } 1 \leq j \leq n_i\}$. In case I is an invariant ideal of R we have that B is a Grobner basis for I. To see this note that given a non zero element f of I we have that for some $i \in [n]$, $w_i \preccurlyeq lm(f)$ and $lc(I, lm(f)) = lc(I, w_i)$. As a consequence, $lc(f) = a_1 lc(f_{i1}) + ... + a_{n_i} lc(f_{in_i})$ so that f is reducible by $\{f_{i1}, ... f_{in_i}\} \subset B$, and then by Lemma 2.3.8 we have that B is a Grobner basis for I. □

Remark 2.3.10. *Because of the previous theorem we know: $\leq$ lovely for G $\implies$ any invariant ideal I of R has a finite Groebner basis B. However, in view of Lemma 2.3.8 this also implies that $I = \langle B\rangle_{R\star[G]}$.*

Remark 2.3.11. *Note that for $G = \{1\}$ and a term order $\leq$ of $X^\diamond$, the symmetric cancellation ordering is just the relation $v \leq w$ and $v|w$. As a consequence $\leq$ is lovely for G if and only if X is finite. Then, in this case, previous remark is just Hilbert basis theorem.*

Proof of Theorem 1.2.3 Let X be an arbitrary set of indeterminates, A a noetherian commutative ring and define $R := A[X]$. Note that in case of a countable set X, Theorem 2.2.8 guarantees the existence of a lovely ordering with respect to S_X. As a consequence the Remark 2.3.10, of previous section, provide us the result in this case.

Now, in the general case suppose for contradiction that R is not noetherian as $R \star [S_X]$-module. Our goal is to find a countably generated $R \star [S_X]$-submodule of R, so that there exist a countable subset X' of X such that $R' := A[X']$ is not noetherian as $R' \star [S_{X'}]$-module. Contradicting the fact that the theorem is true for a countable set of indeterminates.

Then, to finish the proof we need to find a countably generated submodule of R. Since R is not noetherian as $R \star [S_X]$-module, there exist a submodule M of R not finitely generated. Given $g_1 \in M$ define $M_1 := \langle g_1 \rangle_{R\star[S_X]}$, pick $g_2 \in M - M_1$ and define $M_2 := \langle g_1, g_2 \rangle_{R\star[S_X]}$. Since M is not finitely generated we can keep doing this process and define $M' := \bigcup_{i=1}^{\infty} M_i$. M' is clearly a $R \star [S_X]$-submodule of R. We have that M' is generated by all the g_i's. Suppose M' were finitely generated, then there exist $m_1, ..., m_k \in M$ such that $M = \langle m_1, ..., m_k \rangle_{R\star[S_X]}$. However, by definition of M' we have $m_1, ...m_k \in M_i$ for some i, but g_{i+1} does not belong to M_i contradicting the fact that $m_1, ..., m_k$ were a generating set for M'. Then M' is a countably generated submodule of R.

Chapter 3

Lovely Permutation Groups

We already know that for a countable cardinal well-ordered set X the lexicographic ordering is lovely for $FSym(X)$, so an interesting question arises: What kind of subgroups of $FSym(X)$ are lovely?. On this section we give some examples that do not appear in [1], of groups that satisfy and don't satisfy this property. The first example we considered was the alternating group $AltSym(X)$, which happens to be lovely as the following corollary shows.

Corollary 3.0.12. *Let X be a countable set of indeterminates, and define a cardinal well-ordering $\leq$ on X. The lexicographic ordering of $X^\diamond$ is lovely for $AltSym(X)$, the subgroup of even permutations.*

Proof. Let's check that the symmetric cancellation order is a well-quasi-ordering with respect to $AltSym(X)$ and $\leq$. Note that if $a \prec b$ in $X^\diamond$ then $a < b$. Therefore, there are no infinite strictly decreasing sequences in $X^\diamond$ with respect to the symmetric cancellation order. So we only need to prove the antichain condition. In order to achieve that we will use the following observation. Observe that any odd permutation σ can be extended to an even permutation σ_1, such that $\sigma_1 = \sigma \cdot \tau$ where τ does not involve any number belonging to σ, just take $\tau = (ab)$ where $\sigma(a) = a$ and $\sigma(b) = b$ (this can be done since σ fixes all but finitely many numbers).

Now suppose there is an infinite antichain A with respect to $AltSym(X)$. We know the theorem holds for the finitary symmetric group $FSym(X)$, so that

A is not an antichain with respect to $FSym(X)$. Then, there exist $x, y \in A$ comparable elements so that there exist an odd permutation that witnesses $x \preceq y$. By the above observation we can extend this permutation to an even one, such that $x \preceq y$ with respect to $AltSym(X)$. This contradicts the fact that A was an antichain. □

Other subgroups we thought about are the finite ones. These are not lovely, as the following lemma shows.

Lemma 3.0.13. *Let X be an infinite countable set of indeterminates, and define a cardinal well-ordering $\leq$ on X. The lexicographic ordering of $X^\diamond$ is not lovely for G, where G is a finite subgroup of $FSym(X)$.*

Proof. Let $g_1, ..., g_n$ be the elements of G. Since G is a subgroup of $FSym(X)$ it means that $\forall i \in [n]$ there exist $n_i \in \mathbb{N}$ such that for all $b > n_i$ we have $g_i(b) = b$. As a consequence if we define N to be the maximum of the n_i we obtain that given any permutation $g_i \in G$ then for all $b > N$ $g_i(b) = b$. So by picking variables with higher indexes than N we can easily form an infinite antichain. □

In view of these examples, it seems that transitive groups are lovely. So what other subgroups of $FSym(X)$ are transitive?. Well, one interesting construction we found in [7] are the generalized wreath products, which are defined as follows.

Definition 11. *Let Δ be a totally ordered set, and for each $\lambda \in \Delta$ let H_λ be a transitive permutation group acting on a set X_λ. For all $\lambda \in \Delta$ pick an element $1_\lambda \in X_\lambda$, and define the following set*

$$X := \{x = (x_\lambda)_{\lambda \in \Delta} : x_\lambda \in X_\lambda \text{ and } x_\lambda = 1_\lambda \text{ for all but finitely many } \lambda\}$$

Let $\sigma \in X_\lambda$ and $x \in X$. A permutation σ_X of X is defined as follows:

1. *If $x_\mu = 1_\mu$ for all $\mu > \lambda$, define: $(\sigma_X(x))_\lambda = \sigma(x_\lambda)$, and $(\sigma_X(x))_\mu = x_\mu$ if $\mu \neq \lambda$.*
2. *Otherwise let $\sigma_X(x) = x$.*

As a consequence each permutation τ in H_λ produces a permutation τ_X acting on X. Define $J_\lambda := \langle \tau_X : \tau \in H_\lambda \rangle$, namely: the permutation group of X generated by all the permutations induced by H_λ. Finally, define the wreath product $W = Wr_{\lambda\in\Delta} H_\lambda$ of the groups H_λ $\lambda \in \Delta$ as:

$$W := \langle J_\lambda : \lambda \in \Delta \rangle$$

That is to say the permutation group of X generated by all J_λ.

The wreath product depends on the groups H_λ and on the way each H_λ acts on X_λ. However, it doesn't depend on the choice of the 1_λ's. To see this let $1 = (1_\lambda)_{\lambda\in\Delta}$ and $1' = (1'_\lambda)_{\lambda\in\Delta}$ be two different vectors. Let X and X' be the sets defined by these vectors, and denote W and W' as the wreath product induced by these choices, we want to show that W and W' are isomorphic as permutation groups. Since each H_λ is transitive, $\forall \lambda \in \Delta$ there exist $\tau_\lambda \in H_\lambda$ such that $\tau_\lambda(1_\lambda) = 1'_\lambda$. Therefore, we have a bijection $\tau : X \to X'$. Consider $\sigma \in H_\lambda$, note that if we define $\sigma' = \tau_\lambda^{-1} \sigma \tau_\lambda$ then $\sigma'_{X'} = \tau^{-1}\sigma_X \tau$. Obtaining as consequence an isomorphism between W and W'.
As we have said the wreath product is transitive. To see this let $1 = (1_\lambda)_{\lambda\in\Delta}$ be a vector, X the corresponding induced set and W the wreath product. Let $x, y \in X$, denote as $\lambda_1, ..., \lambda_n$ the elements of Δ such that $x_{\lambda_i} \neq 1_{\lambda_i}$, we can assume $\lambda_1 < ... < \lambda_n$. For each $i \in [n]$ pick an element $\sigma^i \in H_{\lambda_i}$ such that $\sigma^i(x_{\lambda_i}) = 1_{\lambda_i}$, and let σ^i_X be the corresponding induced permutation on the wreath product. Note that $\sigma^1_X \circ ... \circ \sigma^n_X(x) = 1$. Doing this process backwards we can obtain a permutation τ such that $\tau(1) = y$ so that $\tau \circ \sigma^1_X \circ ... \circ \sigma^n_X(x) = y$. We found the following example in [8].

Example 3.0.14. *Let C_2 be the cyclic group of 2 elements, and let $\{1, 0\}$ be the set into which C_2 is acting. Let $0 = (0)_{i\in\mathbb{N}}$ be a vector of $0's$ and define X as the set induced by this vector. The wreath product $W = Wr_{i\in\mathbb{N}} C_2$ is a subgroup of $S_{(\mathbb{N})}$. In order to prove this fact we want to show that there exist a bijection between X and $\mathbb{N}$. We have that X consists of sequences $(x_i)_{i\in\mathbb{N}}$ where each x_i is 0 or 1, and all but finitely many numbers are 0. Define $f : X \to \mathbb{N}$ as follows: $f(x) = x_0 \cdot 2^0 + x_1 \cdot 2^1 + ... + x_n \cdot 2^n + ...$, because of X definition we know this infinite sum is finite so that f is well-defined. By definition is inyective, to see it's surjective note that any $n \in \mathbb{N}$ can be written in binary notation. For example $53 = 1\cdot2^5 + 1\cdot2^4 + 0\cdot2^3 + 1\cdot2^2 + 0\cdot2^1 + 1\cdot2^0 = 110101_2$, so that $f^{-1}(53) = 101011000...$. In general to obtain $f^{-1}(n)$ we* *write n in binary notation, write this binary number backwards and add $0's$ to the right of this number.*

Lemma 3.0.15. *Let X be an infinite countable set of indeterminates and define a cardinal well-ordering $\leq$ in X. The lexicographic ordering is not lovely for W, where W is the wreath product defined in the last example.*

Proof. Consider the following set of monomials $A = \{x_0 x_i : i = 2^n - 1, n \in \mathbb{N}^+\}$. We claim this is an infinite antichain. Note that 0 is the infinite sequence of zeros 000..., and $2^n - 1$ is the infinite sequence 1...1000... where the most right 1 is in the $n-1$ position. Our goal is to show that given $i = 2^n - 1, j = 2^m - 1$ there is no $\sigma \in W$ such that $\sigma(0) = 0$ and $\sigma(i) = j$. It's enough to consider the case $i < j$, so we can assume $n < m$. We have that i, j are the infinite sequences 1...1000..., where the most right 1 in i is in the $n-1$ position, and the most right 1 in j is in the $m-1$ position.

Any generator $\sigma_k \in J_k$, where $k > n-1$, sends the k^{th} zero coordinate in the zeros sequence to 1, and the k^{th} zero coordinate in the i sequence to 1. Let $\sigma_h \in J_h$, if $h < k$ then $\sigma_h\sigma_k(i) = \sigma_k(i)$ and $\sigma_h\sigma_k(0) = \sigma_k(0) \neq 0$; if $h > k$ then $0 \neq \sigma_h\sigma_k(0)$. Therefore, by constructing permutations σ in such a way it's not possible to obtain $\sigma(0) = 0$ and $\sigma(i) = j$.

On the other hand, any generator $\sigma_k \in J_k$ where $k < n-1$, sends the k^{th} zero coordinate in the zeros sequence to 1, and is the identity in the i sequence. Let $\sigma_h \in J_h$, if $h < k$ then $\sigma_h\sigma_k(i) = i$ and $\sigma_h\sigma_k(0) = \sigma_k(0) \neq 0$; if $h > k$ then we also obtain $0 \neq \sigma_h\sigma_k(0)$. Therefore, by constructing permutations σ in such a way it's not possible to obtain $\sigma(0) = 0$ and $\sigma(i) = j$.

Finally, any generator $\sigma_k \in J_k$, where $k = n-1$, sends the k^{th} zero coordinate in the zeros sequence to 1, and the k^{th} 1 in the i sequence to 0. Let $\sigma_h \in J_h$, if $h < k$ then $\sigma_h\sigma_k(i) < i < j$ and $\sigma_h\sigma_k(0) = \sigma_k(0) \neq 0$; if $h > k$ then $0 \neq \sigma_h\sigma_k(0)$. Therefore, by constructing permutations σ in such a way it's not possible to obtain $\sigma(0) = 0$ and $\sigma(i) = j$.

An since any permutation is obtained by composition of generators, then it's not possible to obtain a permutation such that $\sigma(0) = 0$ and $\sigma(i) = j$.

$\square$

In general given any sequence $(a_n)_{n\in\mathbb{N}}$ and any $i \in \mathbb{N}^+$, we can form a family of groups $(C_{i^{a_n}})_{n\in\mathbb{N}}$ where each $C_{i^{a_n}}$ is the cyclic group acting on the set $[i^{a_n}]$. Let $W = Wr_{n\in\mathbb{N}}C_{i^{a_n}}$ be the induced wreath product. Note that we can write a natural number in base i, and then code it with respect to the $(a_n)_{n\in\mathbb{N}}$ sequence; that is:

Example 3.0.16. *Let $i = 2$ and $a_n = 2$ for all $n \in \mathbb{N}$. Consider $37 \in \mathbb{N}$, by writing it in base 2 we obtain $37_{10} = 100101_2$. Write this representation backwards and add infinite zeros to the right, so we obtain the infinite sequence 101001000.... Let $a_0 = 2$ be the first 2 bits of this sequence, so we obtain 10. Assume 10 is written in base 2, and write it in base 10, obtaining $10_2 = 1 * 2^1 + 0 * 2^0 = 2_{10}$. This number will be the first entry in our new sequence. For the second number, let $a_1 = 2$ be the next bits of the 101001000... sequence, which again is 10, and repeat above process. Therefore, the second number is again 2. By repeating this process we obtain the sequence 221000....*

Such map defines a bijection, so we can obtain that this wreath product is a subgroup of $FSym(\mathbb{N})$. In the previous lemma we just used the transitivity of C_2 so by an analogue proof we could obtain that the lexicographic ordering is not lovely for W.
Because of previous lemma we know that given an infinite countable set X, not all transitive subroups of $FSym(X)$ are lovely. Now, this wreath product is not lovely because it's not 2-transitive. In view of this observation one may think that 2-transitive subgroups are lovely. In [9, Theorem 7.2.4] we found that 2-transitive subgroups are primitive, and in [8, Theorem 2.1] we found that the only primitive subgroups of $FSym(\mathbb{N})$ are the whole group and $AltSym(\mathbb{N})$, the subgroup of even permutations. We have already shown that these groups are lovely, so that we obtain the following corollary.

Corollary 3.0.17. *Let X be an infinite set if indeterminates and let G be a 2-transitive subgroup of $FSym(X)$. If $\leq$ is a cardinal well-ordering of X, then the lexicographic ordering is lovely for G.*

Proof. □

In view of these facts a new question arises: Are lovely Groups 2-transitive?. We found that this is not the case. Let X be a countable set equipped with a cardinal well-ordering. If x_1 is the minimum element define $G = \{\sigma \in$

$FSym(X) : \sigma(x_1) = x_1\}$. Then, G is lovely for the lexicographic ordering. In order to prove this lemma we will use the following lemmas.

Lemma 3.0.18. *Let X be a cardinal well-ordered countable set, and let $v, w \in X^\diamond$ such that x_1 does not appear in v, w. If $v \preccurlyeq w$ with respect to $FSym(X)$ then $v \preccurlyeq w$ with respect to G.*

Proof. We know σ witnesses $v \preccurlyeq w$ for some $\sigma \in FSym(X)$. If $\sigma(x_1) = x_1$ then $\sigma \in G$, so that $v \preccurlyeq w$ with respect to G. Assume $\sigma(x_1) = x_a$ where $a \neq 1$. Define $f : I_v \to X$ as $f(x_1) = x_1$, otherwise $f(x) = \sigma(x)$; note that since x_1 does not appear in v and $\sigma(v)|w$, we also have $f(v)|w$. Now, in case $\sigma(x_b) = x_1$ for some $x_b \in I_v$ re define f as $f(x_b) = x_a$; note that since x_1 does not appear in w and $\sigma(x_b) = x_1$, we have that x_b doesn't appear in v so we also have $f(v)|w$. By construction f is inyective so in view of Lemma 2.2.6 we know f can be extended to a permutation f' of X. Finally, in order to prove $v \preccurlyeq w$ with respect to G we just have to check that the hypothesis of Lemma 2.2.2 are satisfied. Let $x_i < x_j$ be indeterminates such that x_j appears in v, in case i, j are both different from $1, b$ we know that $f(x_i) = \sigma(x_i) < \sigma(x_j) = f(x_j)$. In case $i = 1$ we clearly have $f(x_i) < f(x_j)$. Since x_b doesn't appear in v we have that $x_j \neq x_b$, so the only remaining case is $x_b < x_j$ for some x_j appearing in v. By definition of f we have $f(x_b) = x_a$ where $x_a = \sigma(x_1)$, we also have that $x_1 < x_j$ and by Lemma 2.2.2 this implies $x_a = \sigma(x_1) < \sigma(x_j)$, so that $f(x_b) < f(x_j)$. □

Lemma 3.0.19. *Let $v, w \in X^\diamond$ such that x_1 does not appear in v, w and let $a, b \in \mathbb{N}$ such that $a \leq b$. If $v \preccurlyeq w$ with respect to G then $x_1^a v \preccurlyeq x_1^b w$ with respect to G.*

Proof. Since $v \preccurlyeq w$, there exist $\sigma \in G$ that witnesses the relation. Since $\sigma(x_1) = x_1$ and $a \leq b$ we have $\sigma(x_1^a v)|x_1^b w$ so that $x_1^a v \preccurlyeq x_1^b w$ with respect to G. □

Lemma 3.0.20. *Let X be a countable set of indeterminates and define a cardinal well-ordering $\leq$ on X. The lexicographic ordering is lovely for G.*

Proof. Let A be an infinite antichain. Given $v, w \in A$ such that x_1 does not appear in v, w then because of Lemma 3.0.18 we know v, w doesn't compare with respect to $FSym(X)$. As a consequence A contains only a finite number of monomials without the x_1 indeterminate. Let A' be the infinite set obtained by pulling out all monomials without x_1 in A. Define the following sets:

$$A_i := \{w \in A' : x_1^i \text{ is the maximum power of } x_1 \text{ that appears in } w\}$$

We claim all A_i are finite. To see this suppose some A_i is infinite. Because of above lemma we know that if $x_1^i v, x_1^i w \in A_i$ then the monomials v, w do not compare, and in view of Lemma 3.0.18 we would have that v, w do not compare with respect to $FSym(X)$. As a consequence, we would have an infinite antichain with respect to $FSym(X)$.
Since A' is infinite we know there are infinitely many nonempty $A_i's$, to simplify notation we will assume all A_i are non-empty. Pick an element $x_1^i v_i \in A_i$ for all $i \in \mathbb{N}^+$, so that we can create an infinite sequence $(x_1^i v_i)_{i\in\mathbb{N}^+}$. Since the lexicographic ordering is a well-ordering, then by Lemma 2.1.1 we know $(x_1^i v_i)_{i\in\mathbb{N}^+}$ has an infinite increasing subsequence $(x_1^{n_i} v_{n_i})_{\imath\in\mathbb{N}}$. As a consequence we have that if $n_i < n_j$ then $x_1^{n_i} v_{n_i} < x_1^{n_j} v_{n_j}$, and $x_1^{n_i} v_{n_i}, x_1^{n_j} v_{n_j}$ do not compare with respect to the symmetric cancellation ordering. However, by above lemma this implies that $v_{n_i} \not\preceq v_{n_j}$ and since $x_1^{n_i} v_{n_i} < x_1^{n_j} v_{n_j}$ then $v_{n_j} \not\preceq v_{n_i}$. Finally, using Lemma 3.0.18 we have that v_{n_i}, v_{n_j} do not compare with respect to the symmetric cancellation ordering over $FSym(X)$. Now, since this applies for all indexes n_i we would obtain an infinite antichain with respect to $FSym(X)$. □

In general we have that given any finite set $A \subset X$ (X a countable set), and a group $G = \sigma \in FSym(X) : \sigma(a) = a$ for all $a \in A\}$ then the lexicographic ordering is lovely for G.

In view of these facts, one may conjecture that if a group G is lovely then G is 2-transitive on $X - A$ where A is a finite set. However, the lexicographic ordering is lovely for the group

$$G = FSym(O) \times FSym(E)$$

Where O is the set of odd numbers and E is the set of even numbers.

Lemma 3.0.21. *Let X be a countable set of indeterminates, and define a cardinal well-ordering $\leq$ on X. The lexicographic ordering of $X^\diamond$ is lovely for G.*

To show this fact, we followed the ideas used in [1] to prove Theorem 2.2.8. However, while proving it we realized that Theorem 2.2.8 can be generalized, below we present this fact as Theorem 3.0.25, so that lemma 3.0.21 is just a special case of Theorem 3.0.25. We discuss now the generalization of Theorem 2.2.8. Let $k \in \mathbb{N}^+$ and for each $i = 1, .., k$ define the following sets $A_i := \{i + rk : r \in \mathbb{N}\}$. Therefore, $\mathbb{N}^+ = \bigsqcup_{i=1}^k A_i$. Define the following groups

$$G := \prod_{i=1}^{k} H_i \qquad G^* := \prod_{i=1}^{k} FSym(A_i)$$

Where H_i is $FSym(A_i)$ or $AltSym(A_i)$, so G^* is a special case of G. We can induce an action of G on $\mathbb{N}^+$ in the following way, let $\sigma = (\sigma_i, ..., \sigma_k) \in G$ since the A_i are disjoint we can identify σ with the permutation $\sigma_i...\sigma_k$, so that σ acts in $\mathbb{N}^+$. The following lemmas will be helpful for our purposes.Let $\preccurlyeq$ be the symmetric cancellation ordering with respect to the lexicographic ordering and G.

Lemma 3.0.22. *Suppose we are given monomials $v := x_1^{a_1}...x_n^{a_n}$, $w := x_1^{b_1}...x_n^{b_n}$ such that $b_n > 0, x_n > x_k$ and $v \preccurlyeq w$. Then, for any $c_1, ..., c_k \in \mathbb{N}$ we have $v \preccurlyeq x_1^{c_1}...x_k^{c_k} x_{1+k}^{b_1}...x_{n+k}^{b_n}$.*

Proof. In case $v = 1$ the result is clear, assume $v \neq 1$. By definition of symmetric cancellation ordering we have $v \leq w$. Since $b_n > 0$ and $x_n > x_k$, then because of the definition of lexicographic ordering we have $v \leq x_1^{c_1}...x_k^{c_k} x_{1+k}^{b_1}...x_{n+k}^{b_n}$. Let $\sigma \in G$ witnesses $v \preccurlyeq w$, so that $u\sigma(v) = w$ for some $u \in X^{\diamond}$. Let $l_i \in A_i$ be the first element that is bigger than x_n, define $\tau_i = (i...(i + rk)...l_i) \in FSym(A_i)$; that is: the cycle that contains all elements of A_i that are less than l_i. Let σ_i be a transposition of numbers bigger than l_i, note that if $\tau_i \notin AltSym(A_i)$ then $\tau_i\sigma_i AltSym(A_i)$. Let $\tau \in G$ be $\tau_1...\tau_k$. Therefore, we have $\tau(w) = x_{1+k}^{b_1}...x_{n+k}^{b_n}$, and since $\tau(w) = \tau(u\sigma(v)) = \tau(u)\tau\sigma(v)$ then $\tau\sigma(v)|x_1^{c_1}...x_k^{c_k}\tau(w)$.
Suppose $v' \leq v$ for some $v' \in X^{\diamond}$. By $\preccurlyeq$ definition we have $\sigma(v') \leq \sigma(v)$. Since $\sigma(v)|w$ then any variable bigger than x_n doesn't appear in $\sigma(v)$. By construction τ is increasing in $[n]$, therefore if $x_i < x_j$ are indeterminates such that x_j appears in $\sigma(v)$ then $\tau(x_i) < \tau(x_j)$, and by Lemma 2.2.2 this implies that τ witnesses $\sigma(v) \preccurlyeq \tau\sigma(v)$. By symmetric cancellation ordering definition we have that if $a' \leq \sigma(v)$ then $\tau(a') \leq \tau\sigma(v)$, in particular $\sigma(v') \leq \sigma(v)$ so $\tau\sigma(v') \leq \tau\sigma(v)$.

□

Lemma 3.0.23. *Assume $\preccurlyeq$ is with respect to G^*. If $\sigma \in G^*$ witnesses the relation $v \preccurlyeq w$ then we can select σ with an additional property: $\sigma(x) = x$ for all $x > x_n$, where x_n is the highest indeterminate appearing in w.*

Proof. Since $v \preccurlyeq w$ then there exist $\tau \in G^*$ that witnesses the relation. Because of Lemma 2.2.2 we know that given indeterminates $x_j < x_i$ such that x_i appears in v then $\tau(x_j) < \tau(x_i) \leq x_n$. As a consequence, we have an injective function $\tau' : I_v \to X_n$ where $X_n := \{x \in X : x \leq x_n\}$. Moreover, we obtain a family of injective functions $\tau'|_{A_i} : I_v \cap A_i \to X_n \cap A_i$. In case all this functions are bijective we are done, just define $\sigma \in G^*$ as $\sigma(x) = x$ for all $x > x_n$, and $\sigma(x) = \tau'(x)$ for all $x < x_n$. Otherwise, for some A_i we have that $I_v \cap A_i$ is a proper initial segment of $X_n \cap A_i$. Consider all such sets and their respective $\tau'|_{A_i}$ function. In view of Lemma 2.2.6 we know each $\tau'|_{A_i}$ function can be extended to a permutation of $X_n \cap A_i, X_n \cap B_j$ respectively. Since $X_n = \bigcup_{i=1}^{k} A_i \cap X_n$, then we have a bijective function $\tau' : X_n \to X_n$ such that $\tau'(x) = \tau(x)$ for all $x \in I_v$. Finally, define $\sigma : X \to X$ as $\sigma(x) = x$ for all $x > x_n$, and $\sigma(x) = \tau'(x)$ for all $x \in X_n$. Since $\sigma(x) = \tau(x)$ for all $x \in I_v$ then by Lemma 2.2.2 we have that σ also witnesses $v \preccurlyeq w$. □

Lemma 3.0.24. *Suppose we are given monomials $v := x_1^{a_1}x_2^{a_2}...x_n^{a_n}$, $w := x_1^{b_1}x_2^{b_2}...x_n^{b_n}$ such that $b_n > 0, x_n > x_k$ and $v \preccurlyeq w$. Then, for any $(u_1, ..., u_k)$, $(v_1, ..., v_k) \in \mathbb{N}^k$ such that $(u_1, ..., u_k) \leq (v_1, ..., v_k)$ we have*

$$x_1^{u_1}...x_k^{u_k}x_{1+k}^{a_1}...x_{n+k}^{a_n} \preccurlyeq x_1^{v_1}...x_k^{v_k}x_{1+k}^{b_1}...x_{n+k}^{b_n}.$$

Proof. In case $v = 1$ the result is clear. Suppose $v \neq 1$, note that $(u_1, ..., u_k) \leq (v_1, ..., v_k)$ and $v \leq w$ imply $x_1^{u_1}...x_k^{u_k}x_{1+k}^{a_1}...x_{n+k}^{a_n} \leq x_1^{v_1}...x_k^{v_k}x_{1+k}^{b_1}...x_{n+k}^{b_n}$. Let $\sigma \in G$ be a permutation that witnesses $v \preccurlyeq w$. Let $\tau \in G$ be defined as in the previous proof. Therefore, $\tau^{-1}(x_1^{u_1}...x_k^{u_k}x_{1+k}^{a_1}...x_{n+k}^{a_n}) = v\tau^{-1}(x_1^{u_1}...x_k^{u_k}) = vh$ where $h = x_{l_1}^{u_1}...x_{l_k}^{u_k}$. Because of Lemma 3.0.23, σ can be chosen such that $\sigma(x_i) = x_i$ for all $x_i > x_n$. Note that by adding transpositions to σ, with numbers bigger than x_{n+k}, we can make a permutation σ^* that belongs to G and also witnesses $v \preccurlyeq w$. Therefore, $\sigma^*\tau^{-1}(x_1^{u_1}...x_k^{u_k}x_{1+k}^{a_1}...x_{n+k}^{a_n}) = \sigma^*(v)h$, and since $\sigma^*(v)|w$ and $(u_1, ..., u_k) \leq (v_1, ..., v_k)$, we have that $\sigma^*(v)h|wh'$ where $h' = x_{l_1}^{v_1}...x_{l_k}^{v_k}$. On the other hand, $\tau(wh') = x_1^{v_1}...x_k^{v_k}x_{1+k}^{b_1}...x_{n+k}^{b_n}$, so combining these facts we obtain $\tau\sigma^*\tau^{-1}(x_1^{u_1}...x_k^{u_k}x_{k+1}^{a_1}...x_{n+k}^{a_n}) = \tau(\sigma^*(v)h)|\tau(wh') =$

$x_1^{v_1}...x_k^{v_k}x_{1+k}^{b_1}...x_{n+k}^{b_n}$.
Suppose $v' := x_1^{h_1}...x_k^{h_k}x_{k+1}^{h_{k+1}}...x_{n+k}^{h_{n+k}} \leq x_1^{u_1}...x_k^{u_k}x_{1+k}^{a_1}...x_{n+k}^{a_n}$ for some $v' \in X^\diamond$. By lexicographic order definition this implies $x_{k+1}^{h_{k+1}}...x_{n+k}^{h_{n+k}} \leq x_{1+k}^{a_1}...x_{n+k}^{a_n}$. Is also clear that
$\tau^{-1}(x_{k+1}^{h_{k+1}}...x_{n+k}^{h_{n+k}}) = x_1^{h_{k+1}}...x_n^{h_{n+k}} \leq x_1^{a_1}...x_n^{a_n} = \tau^{-1}(x_{1+k}^{a_1}...x_{n+k}^{a_n}) = v$. Therefore, using $\preccurlyeq$ definition we obtain $\sigma\tau^{-1}(x_{k+1}^{h_{k+1}}...x_{n+k}^{h_{n+k}}) \leq \sigma v$. Now, since $\sigma(v)|w$ then the indeterminates $x_{n+1},...,x_{n+k}$ doesn't appear in $\sigma(v)$. We also have that τ is increasing in $[n]$ so by Lemma 2.2.2 we have that τ witnesses $\sigma(v) \preccurlyeq \tau\sigma(v)$. In particular this implies that $\tau\sigma\tau^{-1}(x_{k+1}^{h_{k+1}}...x_{n+k}^{h_{n+k}}) \leq \tau\sigma(v)$. Finally, since $\sigma(x_{n+1}...x_{n+k}) = x_{n+1}...x_{n+k}$ then $\tau\sigma\tau^{-1}(x_1...x_k) = x_1...x_k$. Combining these facts we obtain $\tau\sigma\tau^{-1}(v') \leq \tau\sigma\tau^{-1}(x_1^{u_1}...x_k^{u_k}x_{1+k}^{a_1}...x_{n+k}^{a_n})$. □

With this theorems in mind we can prove the generalization.

Lemma 3.0.25. *Let X be a countable set of indeterminates, and define a cardinal well-ordering $\leq$ on X. The lexicographic ordering of $X^\diamond$ is lovely for G^*.*

Proof. Given a monomial $w \in X^\diamond$ define $|w| = max\{x_i \in X : x_i|w\}$, here max refers to the maximum with respect to $\leq$. Suppose for sake of contradiction that the symmetric cancellation ordering is not a well-quasi-ordering, then using Lemma 2.1.1 there exist a sequence $w_1, w_2, ...$ in $X^\diamond$ which is not good. Define a function $j_X : X^\diamond \to \mathbb{N}$ as: $j(1) := 0$ and for $w \in X^\diamond$ different form 1, $j_X(w) := i$ where i is the index such that $|w| = x_i$. We can choose the sequence $w_0, w_1, ...$ such that it is minimal with respect to the j_X function; that is: define $F(X)$ as the set of all non-good sequences $b_0, b_1, ...$ Let w_0 be such that $j_X(w_0)$ is minimal among all the $j_X(b_0)$, where b_0 is the first element of a sequence appearing in $F(X)$, note that we can select a minimal element because of X well-order. Select w_1 such that $j_X(w_1)$ is minimal among all the $j_X(b_1)$, where b_1 belongs to a sequence $w_0, b_1, b_2, ...$ appearing in $F(X)$. Similarly, select w_i for all $i \in \mathbb{N}$. Note that since $1 \leq w\ \forall w \in X^\diamond$, we know $w_n \neq 1$ for all $n \in \mathbb{N}$.
Write $w_n = x_1^{1_n}v_n$, where x_1 does not appear in v_n. Consider the set $A := \{1_n : n \in \mathbb{N}\}$. Because of $\mathbb{N}$ well-order we can construct an increasing subsequence $0 \leq 1_{j_0} \leq 1_{j_1} \leq ...$. Consider the indexes j_n of this sequence. Since $\mathbb{N}$ is well-ordered we can select a sub-sequence $0 \leq 1_{n_0} \leq 1_{n_1} \leq ...$ such

that $1_{n_i} \leq 1_{n_j} \iff n_i \leq n_j \iff i \leq j$. By repeating this process we can construct a subsequence $\{w_{n_i}\}_{i\in\mathbb{N}}$ such that $w_{n_i} = x_1^{1_{n_i}}...x_k^{k_{n_i}}v'_{n_i}$ where v'_{n_i} does not contain any variable of the set $\{x_1, ..., x_k\}$, and for all $j = 1, .., k$ $j_{n_a} \leq j_{n_b} \iff a < b$. Define a monoid homomorphism $\phi : X^\diamond \to X^\diamond$ as $\phi(1) = 1$, $\phi(x_i) = x_{i-k}$ if $i \geq k+1$, and $\phi(x_i) = 1$ for all $i = 1, ...k$. Note that since the sequence of w_n is not good and since we are using lexicographic ordering, then for $i \geq 0$ the monomial v'_{n_i} appearing in w_{i_j} must be different from 1. Therefore, for $i \geq 0$ this homomorphism satisfies that $j_X(\phi(w_{n_i})) = j_X(w_{n_i}) - k$. Then, by minimality of the sequence $w_1, w_2, ...$ we have that the sequence $w_1, w_2, ..., w_{n_0-1}, \phi(w_{n_0}), \phi(w_{n_1}), ...$ is good. Then, there exist $a < n_0$ and $n_k \geq n_1$ such that $w_a \preccurlyeq \phi(w_{n_k})$, or there exist $n_l > n_k \geq n_1$ such that $\phi(w_{n_k}) \preccurlyeq \phi(w_{n_l})$. In the former case we have $w_a \preccurlyeq w_{n_k}$ because of Lemma 3.0.22. In the second case we have $w_{n_k} \preccurlyeq w_{n_l}$ because of Lemma 3.0.24. Both cases contradicting the choice of the sequence $\{w_n\}_{n\in\mathbb{N}^+}$. □

In general we think that if we partition $\mathbb{N}^+ = \bigsqcup A_1 \bigsqcup ... \bigsqcup A_k \bigsqcup B_1 \bigsqcup ... \bigsqcup B_l$ such that all A_i are infinite and all B_i are finite, and if we let $G = \prod_{i=1}^k H_i \times \prod_{j=i}^l G_j$ where H_i is $FSym(A_i)$ or $AltSym(A_i)$ and G_j is any subgroup of $FSym(B_j)$, then the lexicographic ordering is lovely for G. However, we were run out of time so that we did not study in detail such conjecture.

Chapter 4

Recent works

The finiteness theorem proved by Hillar and Aschenbrenner in [1], which is explained in Chapter 2, was motivated by some questions in chemistry [1, Section 5]. The problem of interest is the following:

Given a set S let $X_S := \{x_s : s \in S\}$ be a set of indeterminates indexed by S. Let $k \in \mathbb{N}^+$ and denote by $\langle S \rangle^k$ the set of all k-tuples $(u_1, ..., u_k) \in S^k$ such that the u_i are pairwise distinct. Given $n \geq k$ and $S = [n]$ we will write $\langle n \rangle^k$ for $\langle S \rangle^k$. Let K be a field and define

$$R_n := K[X_{\langle n \rangle^k}] \qquad\qquad R_{\mathbb{N}^+} := \bigcup_{n \geq k} R_n = K[X_{\langle \mathbb{N}^+ \rangle^k}]$$

The symmetric group S_n acts on the set $\langle n \rangle^k$ in the following way: Given $\sigma \in S_n$ and $(u_1, ..., u_k) \in \langle n \rangle^k$ then $\sigma(u_1, ..., u_k) = (\sigma(u_1), ..., \sigma(u_k))$. This action leads to an action of S_n on R_n, given $f(x_{v_1}, ..., x_{v_j}) \in R_n$ then $\sigma(f) = f(x_{\sigma(v_1)}, ..., x_{\sigma(v_j)})$. Note that the action of S_n on R_n gives an action of $FSym(\mathbb{N}^+)$ on $R_{\mathbb{N}^+}$. Given a family of ideals $\{I_n\}_{n \in \mathbb{N}^+}$ such that each I_n is an ideal of R_n and $I_n \subset I_{n+1}$ we say it's an invariant chain of ideals if in addition $S_m I_n \subset= I_m$ for all $m \geq n$.
Let $T_n := K[t_1, ..., t_n]$, and fix $f \in K[y_1, ..., y_k]$. Define the following K-algebra homomorphism:

$$\phi_n : R_n \to T_n : x_{(u_1,...,u_k)} \to f(t_{u_1}, ..., t_{u_k})$$

Example 4.0.26. *Let* $k = 3$ *and let* $f = y_2 y_3^2 \in K[y_1, y_2, y_3]$*. Then* $\phi_4(x_{(2,3,4)}) = y_3 y_4^2$.

Let Q_n be the kernel of the previous homomorphism. By construction these kernels produce a family of ideals $\{Q_n\}_{n\in\mathbb{N}^+}$ such that it's an invariant chain of ideals, and by a chemistry motivation [1] is interesting to see if the chain stabilizes modulo the action of the symmetric group; that is: $\langle S_m Q_N\rangle_{R_m} = Q_m$ for all $m \geq N$, such an N is called stabilization bound. Note that if we are able to found such bound then the ideal I_N describes all the chain for all $m \geq N$. Because of Theorem 1.2.3 we know that for $k = 1$ the chain stabilizes [1, Theorem 4.7]. However, in [1, Proposition 5.2] this approach fails for $k \geq 2$.

That document also shows that in a special case the chain stabilizes: If $f \in K[y_1, ..., y_k]$ is a free-square monomial then the chain of kernels described above stabilizes and a stabilization bound is $N = 4k$ [1, Theorem 5.7]. The authors finish the document giving a conjecture that generalizes this theorem: The sequence of kernels induced by a monomial f stabilizes [1, conjecture 5.10].

In a more recent paper by Aschenbrenner and Hillar [2], this invariant chain ideal problem is treated. Let $R_n, R_{\mathbb{N}^+}$ be defined as above. Let $[n]^k$ be the set of all k-tuples with entries in $[n]$, and define

$$\mathcal{R}_n := K[X_{[n]^k}] \qquad\qquad \mathcal{R}_{\mathbb{N}^+} := \bigcup_{n\geq k} R_n = K[X_{\langle\mathbb{N}^+\rangle^k}]$$

In that paper, they focus in invariant chain of localized ideals (Laurent ideals). Let $I_n \subset R_n$ (or $\mathcal{R}_n$), and denote $I_n^{\pm}$ as the localization of I_n with respect to the set of monomials of R_n (respectively $\mathcal{R}_n$). One of the results presented is

Theorem 4.0.27. *Every invariant chain $I_1^{\pm} \subset I_2^{\pm} \subset ...$ of Laurent Lattice ideals $I_n^{\pm} \subset R_n^{\pm}$ (respectively $I_n^{\pm} \subset \mathcal{R}_n$) stabilizes*

So that a Laurent version for the above conjecture is true. However, for applied objectives this proof is not very helpful since it's not constructive and doesn't give any information about stabilization bounds. The authors prove a more specific result [Theorem 4], which treats the problem of kernels induced by monomials, described above, when the kernels are localized.

Theorem 4.0.28. *Let $f \in K[y_1, ..., y_k]$ be a monomial of degree d in k variables. Given $n \geq k$ define the following map*

$$\phi_n : R_n \to T_n : x_{(u_1,...,u_k)} \to f(t_{u_1,...,t_{u_k}}).$$

Let $Q_n = ker(\phi_n)$*. The invariant chain* $Q_k^{\pm} \subset Q_{k+1}^{\pm} \subset \ldots$ *has* $N = 2d$ *as stabilization bound.*

Because of this theorem we know that the ideal $I_{2d}^{\pm}$ describes the chain for $m \geq 2d$. Therefore, a generating set for $I_{2d}^{\pm}$ will also be a generating set modulo symmetries for the chain $I_{2d}^{\pm} \subset I_{2d+1}^{\pm} \subset \ldots$. In the document is presented an algorithm [Theorem 7] to calculate these generators. It's also commented that the degree-complexity of an homogeneous ideal, defined as the maximal degree in a reduced Groebner basis, seems to be related to the stabilization. However, while examining such algorithm we found that it required an important amount of computational resources, so we decided not to study in more detail these ideas an rather explore the "lovely" property described in Chapter 2.

Bibliography

[1] Hillar, C.J., Aschenbrenner, M., Finite generation of symmetric ideals, Transactions of the American Mathematical Society, (2007).

[2] Hillar, C.J., Martin del Campo. A., Finiteness theorems and algorithms for permutation invariant chains of Laurent lattice ideals, Journal of Symbolic computation, (2013).

[3] Hillar, C.J., Sullivant, S., Finite Groebner bases in infinite dimensional polynomial rings and applications, Advances in Mathematics, (2012). (2006)

[4] Adams, W.W., Loustaunau, P., An introduction to Grbner Bases, American Mathematical Society.(1996). (2006)

[5] Higman, G., Ordering By Divisibility In Abstract Algebras. Proceedings London Mathematical Society. (1952).

[6] Cox, D., Little, J., O'Shea , D., Ideals, varieties and algorithms 3ed, Springer, (2006).

[7] Robinson, D. J. S., Finiteness Conditions and Generalized Soluble Groups, Springer-Verlag, (1972).

[8] Pinnock, C., Finitary Permutation Groups, Combinatorics Study Group.

[9] Derek, R., A Course in Theory Of Groups, 2ed, Springer (1995).