Abstract. Classical Buchberger theory is generalized to a new family of rings. The family includes all subalgebras of the polynomial algebra in one variable. Some subalgebras of polynomial algebras in several variables are included. The new rings are integral domains and have a number of other properties in common with polynomial rings. The rings sit in a field $F$ in appropriate position relative to a valuation ring in $F$. The valuation ring gives rise to a totally ordered monoid which plays the role of a term ordering in the classical Buchberger theory. The paper is reasonably self-contained and contains an infinite number of examples.

Introduction

The four cornerstones of classical Buchberger theory are: term orderings, the reduction algorithm, the test for when a set is a Gröbner basis and the algorithm for constructing Gröbner bases. The reduction algorithm, the test for when a set is a Gröbner basis and the algorithm for constructing Gröbner bases, all depend on term orderings and can be adapted to other rings which have suitable orderings. In this paper we shall present other rings with suitable orderings and show how the reduction algorithm and construction algorithm can be adapted to these rings. Along the way we shall see the intimate relationship between term orderings and valuation rings. This paper is intended to be fairly self-contained. Thus valuation rings and some of their elementary properties are outlined in Appendix 2. This includes some remarks about ordered abelian groups and monoids. Ideal theory in abelian monoids is presented in Appendix 1.

General Overview

[Rob85] classifies the possible term orders which can occur on the polynomial ring. Valuation theory is not explicitly mentioned but is there in spirit. For example, Robbiano uses the valuation theoretic term archimedean to describe certain orderings. In the present paper we show how term orderings give rise to valuation rings in the field of fractions of a polynomial ring. These valuation rings have small intersection with the original polynomial ring. The procedure is reversible, valuation rings, with small intersection with polynomial ring, give rise to term orderings on the polynomial ring. This is the starting point for orderings on a wider class of rings than polynomial rings. The idea is to start with a valuation ring $V$ and a ring $A$

This research was partially supported by the National Science Foundation and IBM.
which has *small* intersection with $V$. As with the polynomial ring, this leads to a quasi-ordering on $A$. This is the setting to which we extend Buchberger theory. The constructiveness of Buchberger theory is critical for computer applications. How constructive is the valuation theoretic extension? The matter of constructiveness comes down to whether we can constructively do arithmetic in the field in which $V$ and $A$ lie, whether we can constructively tell if an element of the field lies in $V$ and whether we can effectively work in the monoid $M$ as described below. A specific example of a ring $A$ to which we shall extend Buchberger theory is the subring of the polynomial ring $R[X]$ generated by $X^3, X^4,$ and $X^5$. We shall explicitly obtain a Gröbner basis for the ideal generated by $X^5 + X^3$ and $X^4$ in $A$. This example is presented in the end of the introduction. It should be noted that our extension of Buchberger theory to $A$ is not the same as writing $A$ as a quotient of the polynomial ring $R[Y, Z]$ and pulling back the ideal theory in $A$ to ideal theory in $R[Y, Z]$.

Term orderings on a polynomial ring give rise to filtrations of the polynomial ring. [Rob86] is about finding ideal bases in rings with filtrations. It nicely unifies the types of filtrations arising from term orderings with the types of filtrations arising from powers of an ideal. A key aspect of the theory is the associated graded ring to the filtration. In fact, Robbiano’s emphasis is on the associated graded ring rather than the filtration. With the filtrations arising from term ordering of a polynomial ring, the associated graded ring is isomorphic to the original polynomial ring. This is well known in classical Buchberger theory. It is utilized in arguments which prove that the Gröbner basis construction algorithm stops because the associated graded ring is Noetherian. It is also at the heart of the observation: “Gröbner bases reduce ideal theory in the polynomial ring to homogeneous ideal theory.” The filtrations which arise in classical Buchberger theory are filtrations over the group: $\mathbb{Z} \times \cdots \times \mathbb{Z}$ where $\mathbb{Z} \times \cdots \times \mathbb{Z}$ has a total order arising from the term ordering. Robbiano considers filtrations and gradings over arbitrarily totally ordered groups. The orderings arising from valuation rings, in this paper, give rise to filtrations which fall within the settings of [Rob86]. The filtrations are over the (totally ordered) value group of the valuation. In the associated graded ring, each homogeneous component is zero or one-dimensional over a ground field and only non-negative elements of the ordered group have non-zero homogeneous components. This is like classical Buchberger theory but is a special case of [Rob86]. As a result, some of the theory in [Rob86] is not relevant. This paper focuses on considerations having to do with the monoid of non-zero components.

As indicated in the previous paragraph, the focus in this article is on monoidal filtrations. In the course of writing this paper, it has become clear that the approach here applies to a larger family of rings than this which sit in fields and have small intersection with valuation rings. The proper context is algebras with monoidal filtration. This paper illustrates – in fact is a blueprint for – the features of the more general theory. It will appear subsequently.
The monoid $M$ of non-zero components is the subset of the ordered group consisting of elements $g$ where the $g^{th}$ graded component of the associated graded ring is non-zero. $M$ is an ordered monoid and plays an important role. In classical Buchberger theory, the monoid $M$ is $\mathbb{N}^n = \mathbb{N} \times \cdots \times \mathbb{N}$, with the ordering given by the term ordering. As we shall see, $\mathbb{N}^n$ is a very well behaved ordered monoid and many of the difficulties in extending Buchberger theory arise from areas where (general) $M$’s are not well behaved. Here is an example:

We shall define ideals in a monoid. $\mathbb{N}^n$ has the constructive principal intersection property, meaning that the intersection of principal ideals is again principal and the generator can be found constructively. The general monoid $M$ which arises does not have this property. However, when $M$ does have the constructive principal intersection property, the usual $S$-polynomial technique for constructing Gröbner bases applies.

The above example illustrates another aspect of this paper. Namely, it helps to pinpoint some of the basic ideas underlying classical Buchberger theory. Time will tell whether the extension of Buchberger theory presented here is worth pursuing on the basis of the wider class of rings for which one can find Gröbner bases. It is the author’s hope that even if the answer is “no”, the theory presented here will be considered useful in terms of the light it sheds on classical Buchberger theory.

**Specifics**

If $A$ is a polynomial ring with a term ordering, let $F$ be the field of fractions of $A$ and let $V$ be the subring of $F$ consisting of zero and the fractions $f/g$ where the leading monomial of $f$ is less than or equal to the leading monomial of $g$. Then $V$ is a valuation ring, meaning that for any nonzero element of $F$, either the element or its inverse lies in $V$. The term ordering is easily recovered from the valuation ring. The details appear in (1.3). Valuation rings can be used to construct ideal bases for ideals in rings $A$ other than polynomial rings. Here is the setup. Note that $A$ sits in a field $F$ as does a valuation ring $V$. Now, $A$ must have small intersection with $V$, meaning that $A \cap V$ must be a complement to the maximal ideal of $V$. (In (1.1) this is defined as $V$ being a complementary valuation ring to $A$ in $F$.) This gives a quasi order on $A$ where $a_1 \leq a_2$ if and only if $a_1/a_2 \in V$. With this quasi-ordering we imitate Buchberger theory to the extent possible. For a polynomial ring with a term ordering of the monomials, the quasi-order on the polynomial ring is given by $f \leq g$ if and only if the lead monomial of $f$ is less than or equal to the lead monomial of $g$.

The quasi-ordering on $A$ gives rise to an algebra filtration and an associated graded algebra. The valuation ring also gives rise to a valuation group, namely the nonzero elements of $V$. The images of nonzero elements of $A$ in this group form a monoid $M$. If $A$ is a polynomial ring and $V$ came from the term ordering on $A$, the monoid $M$ is just a finite product of copies of the natural numbers. The monoid has a total order
that comes from the valuation group being an ordered abelian group. Unlike groups, monoids have nontrivial ideals. ($S$ is an ideal in the abelian multiplicative monoid $M$ if and only if $MS \subset S$.) Roughly speaking the remark: “Gröbner bases reduce ideal theory in the polynomial ring to the homogeneous ideal theory” factors:

$$\begin{bmatrix}
\text{ideal theory in the polynomial ring}
\text{reduces to ideal theory in the monoid}
\end{bmatrix}
\begin{bmatrix}
\text{ideal theory in the monoid is equivalent to homogeneous ideal theory in the monoid algebra}
\end{bmatrix}
\begin{bmatrix}
\text{the monoid algebra is isomorphic to the polynomial ring}
\end{bmatrix}.$$

Rather than taking the product of all three factors, it seems more fundamental to stop at the point where ideal theory in the ring is reduced to ideal theory in the monoid. Although the valuation approach is discussed in this paper does indeed give rise to an associated graded algebra, we have no need of it and do not bother to introduce it.

Questions of finite generation of monoid ideals and Noetherian monoids arise. The Hilbert basis theorem for monoids exhibits the key points of the Hilbert basis theorem for rings. These are found in Appendix 1.

**Open Questions**

What are the rings $A$ that have complementary valuation rings? In the new theory there are usually more syzygies to resolve than in the classical Buchberger theory. This is discussed in more detail in the beginning of Section 3. See also (3.3), (3.7), and (3.14) for where the syzygies are defined and used. The number of syzygies stays as small as possible when the intersection of principal ideals in the monoid of $A$ is again a principal ideal. For example, $\mathbb{N} \times \cdots \times \mathbb{N}$ has this property. This raises the question of which monoids have the property that the intersection of principal ideals is again principal. Another monoid question concerns when the submonoid $\pi(A^0)$ of $\mathbb{N} \times \cdots \times \mathbb{N}$ is finitely generated. This question and a related question appear in (1.11). Another related question is to find an algorithm that explicitly gives (generators for) $\pi(B^0)$ when $A$ is a polynomial ring with a term ordering as in (2.4) and $B$ is a subalgebra of $A$.

**Acknowledgements**

IBM and the NSF provided support during the course of this research. Thanks to Barry Trager for many helpful conversations. Scratchpad II, IBM’s experimental computer language for algebraic computation, was used to compute examples that helped to contribute to my understanding.
ILLUSTRATIVE EXAMPLE

Let us end the introduction with an example that illustrates our approach. Assumed may be points in the example where you wonder “why do you do that?” The “why you do that” is told in the body of the paper. All rings discussed in this paper are assumed commutative. For a ring $B$ and a set $S$ in $B$:

- Notation: Denotes the set of elements of $B$
  - $B^I$: $B$ that are invertible
  - $B^U$: $B$ that are not invertible
  - $S^0$: $S$ other than 0

Here $B^I$ is a multiplicative group and $B^U$ is also closed under product. If $B$ is also a field, then $B^I$ and $B^U$ coincide.

Example 0.1. Let $R$ be a field and $A$ be $R[X^3, X^4, X^5]$, meaning the subalgebra of $R[X]$ generated by $X^3, X^4, X^5$. Concretely, this is the set of polynomials with no linear or quadratic term. The overfield $F$ is $R((X))$. The valuation ring $V$ is given by:

$$V = \{ f \in F \mid f = 0 \text{ or there are } a, b \in R[X] \text{ with } \deg a \leq \deg b \text{ and } f = a/b \}$$

$V \cap A = R$. There is a group homomorphism $\pi$ from the multiplicative group $F^I$ to the additive group $\mathbb{Z}$ given by $\pi(a/b) = \deg a - \deg b$. The monoid $M$ of importance is $\pi(A^I)$. More explicitly:

$$M = \{0, 3, 4, 5, 6, \ldots \}.$$ 

Like rings, monoids have ideals. See Section 2 and Appendix 1 for more about monoids. Let us find a Gröbner basis in $A$ for the ideal $J$ generated by $g_1 = X^4$ and $g_2 = X^5 + X^3$. In the classical Buchberger theory one would first find the $S$-polynomial of $g_1$ and $g_2$. In the new theory, there may be more than one $S$-polynomial. First take $\pi(g_1)$ and $\pi(g_2)$ and look at the intersection of the principal ideals they each generate in $M$. Now, $\pi(g_1) = 4$ and $\pi(g_2) = 5$. The following ideals are generated:

$$I_1 = \pi(g_1) + M = 4 + M \quad \{4, 6, 7, 8, 9, \ldots \}$$
$$I_2 = \pi(g_2) + M = 5 + M \quad \{5, 8, 9, 10, \ldots \}$$

Next take the intersection of the ideals $I_1$ and $I_2$.

$$I_1 \cap I_2 = \{8, 9, 10, \ldots \}$$

Then look for generators of the ideal $I_1 \cap I_2$. Because $M$ is a proper subset of $\mathbb{N}$, a minimal generating set for $I_1 \cap I_2$ is $\{8, 9, 10\}$. There is one $S$-polynomial for each generator of $I_1 \cap I_2$ and we shall find these shortly. Then we must see if they reduce to zero over $\{g_1, g_2\}$.

You have now seen the aspect of the new theory that is most different from Buchberger theory; namely, there is more than one $S$ polynomial for each $g_i, g_j$. There is one $S$ polynomial for each generator of the ideal which is the intersection of the two
principal ideals $I_1$ and $I_2$ in $M$. (A principal ideal in a monoid is an ideal generated by one element, (2.3).) As we shall see in example (2.4), for the full polynomial ring $R[X_1,\ldots,X_n]$, the monoid $M$ is $\mathbb{N} \times \cdots \times \mathbb{N}$; here the intersection of principal ideals is again principal. It will give rise to the usual $S$-polynomial.

For the generator 10 of the ideal $I_1 \cap I_2$,

\[ \pi(X^6g_1) = \pi X^6 + \pi g_1 = 6 + 4 = 5 + 5 = \pi X^5 + \pi g_2 = \pi(X^5 g_2) \]

Thus an $S$-polynomial for the generator 10 is given by:

\[ X^6g_1 - X^5 g_2 = -X^8 \]

In $M$: \( \pi(-X^8) = 8 = 4 + 4 = \pi X^4 + \pi g_1 = \pi(X^4 g_1) \). Thus \(-X^8 + X^4 g_1 = 0\) is a reduction of $-X^8$ to zero in $A$. For the generator 9 of the ideal $I_1 \cap I_2$:

\[ \pi(X^5 g_1) = \pi X^5 + \pi g_1 = 5 + 4 = 4 + 5 = \pi X^4 + \pi g_2 = \pi(X^4 g_2) \]

An $S$-polynomial for the generator 9 is given by:

\[ X^5 g_1 - X^4 g_2 = -X^7 \]

In $M$: \( \pi(-X^7) = 7 = 3 + 4 = \pi X^3 + \pi g_1 = \pi(X^3 g_1) \). Thus, $-X^7 + X^3 g_1 = 0$ is a reduction of $-X^7$ to zero in $A$.

Now the interesting generator 8. For the generator 8 of the ideal $I_1 \cap I_2$:

\[ \pi(X^4 g_1) = \pi X^4 + \pi g_1 = 4 + 4 = 3 + 5 = \pi X^3 + \pi g_2 = \pi(X^3 g_2) \]

An $S$-polynomial for the generator 8 is given by:

\[ X^4 g_1 - X^3 g_2 = -X^6 \]

\( \pi(-X^6) = 6 \) and there is no element $m \in M$ where $m + \pi g_1 = 6$ or $m + \pi g_2 = 6$. Thus $-X^6$ reduces no further in $A$. Throw $-X^6$ or its negative into the forming Gröbner basis. $g_3 = X^6$.

Next – as in classical Buchberger theory – we must consider $S$-polynomials for the pairs $g_1, g_3$ and $g_2, g_3$. We get sketchier now. The ideals generated by $\pi g_1$ and $\pi g_2$ in $M$ are described above. For $g_3$ the ideal is

\[ I_3 = \pi(g_3) + M = 6 + M = \{6, 9, 10, 11, \ldots\} \]

Thus

\[ I_1 \cap I_3 = I_2 \cap I_3 = \{9, 10, 11, \ldots\} \]

\( \{9, 10, 11\} \) is a minimal generating set for the ideal $\{9, 10, 11, \ldots\}$. For these generators, the $S$-polynomials are formed as above. For the $g_1, g_3$ pair all the $S$-polynomials are zero. For example, for the generator 9, the $S$-polynomial is $X^5 g_1 - X^3 g_3 = 0$. For the pair $g_2, g_3$, the $S$-polynomials are not zero, but they reduce to zero. For example, for the generator 9, the $S$-polynomial is $X^4 g_2 - X^3 g_3 = X^7$. This reduces to zero by $X^7 - X^3 g_1 = 0$.

Since the $S$-polynomials reduce to zero, no further elements are included in the forming Gröbner basis. Thus, \( \{g_1, g_2, g_3\} \) is a Gröbner basis for the ideal $J$ in $A$. 

Having a Gröbner basis, one can use reduction to determine whether an element of $A$ lies in $J$. One can also get canonical representatives for $A/J$ and imitate other applications of Gröbner bases.

1. **Complementary Valuation Rings and Reduction**

$\mathbb{Z}$ denotes the integers and $\mathbb{N}$ denotes $\{n \in \mathbb{Z} \mid 0 \leq n\}$. Valuation ring is defined at (A2.6). We use the notation used in the Illustrative Example in the introduction.

**Definition 1.1.** Let $F$ be a field with subring $A$ and valuation ring $V$. $V$ is a complementary valuation ring to $A$ in $F$ if $A \cap V$ is an abelian group complement in $V$ to $V^I$. I.e., $A \cap V^I = \{0\}$, and $V = (A \cap V) + V^I$.

The following properties concerning complementary valuation rings are immediate.

**Lemma 1.2.** Let $V$ be a complementary valuation ring to $A$ in the field $F$. Then

(a) $A \cap V$ is a field.

(b) $A \cap V$ contains all the invertible elements of $A$.

(c) If $B$ is a subring of $A$ where $B \supset A \cap V$, then $V$ is a complementary valuation ring to $B$ in $F$.

In the next statements $G$ is the value group of the valuation, (A2.8). $G$ is an ordered abelian group, (A2.7.f). $NN$ is the submonoid of nonnegative elements of $G$, (A2.4). A monoid is GUPI if generators are unique for principal ideals, (A1.17)–(A1.20). $\pi$ is the natural group homomorphism from $F^I$ to $G$, (A2.7.f).

(d) $\pi(A^n) \subset NN$, the nonnegative elements of $G$. $\pi(A^n)$ is a GUPI submonoid of $G$. $\pi(A^n)$ is totally ordered with the order inherited from $G$. If $m_1$ and $n$ are distinct elements of $\pi(A^n)$ and there is $m_2 \in \pi(A^n)$ with $m_1m_2 = n$, then $m_1 < n$.

(e) Say $0 \neq a, b \in A^n$. $\pi a < \pi b$ if and only if $a/b \in V^I$. $\pi a = \pi b$ if and only if $a/b \in V^I$. $\pi a \leq \pi b$ if and only if $a/b \in V$. If $a + b \neq 0$, then $\pi(a + b) \leq \max\{\pi a, \pi b\}$.

(f) Suppose $a, b \in A^n$, and $0 \neq \gamma, \lambda \in A \cap V$ where $\gamma a + \lambda b = 0$ or $\gamma a + \lambda b \neq 0$ and $\pi(\gamma a + \lambda b) < \max(\pi a + \pi b)$. Then $\pi a = \pi b$.

(g) For $0 \neq a, b \in A^n$ where $\pi a = \pi b$ there is $0 \neq \lambda A \cap V$ with $a = \lambda b$ or $a - \lambda b \neq 0$ and $\pi(a - \lambda b) < \pi a = \pi b$.

(h) Suppose $b \in A^n$ and for $i = 1, \ldots, N$, there exist $a_i \in A$ where $a_i = 0$ or $\pi a_i < \pi b$. Then $b + \sum_{i=1}^N a_i \neq 0$ and $\pi(b + \sum_{i=1}^N a + i) = \pi b$.

**Proof.** (a) By (A2.7,b), $V^I$ is a maximal ideal of $V$. Thus $V/V^I$ is a field. Since $A \cap V$ is an abelian group complement to $V^I$ in $V$, $A \cap V$ maps isomorphically to the field $V/V^I$ under the natural ring map $V \to V/V^I$.

(b) Say $a$ lies in $A - V$. By (A2.7,c), $a^{-1} \in V^I$. Since $A \cap V^I = \{0\}$, $a^{-1}$ cannot lie in $A$. 

(c) The hypotheses imply that \( B \cap V = A \cap V \) which is an abelian group complement in \( V \) to \( V^I \) since \( V \) is a complementary valuation ring to \( A \) in \( F \).

(d) Since \( A \cap V^I = \{0\} \), \( A^0 \subset F - V^I \). By (A2.7,f), it follows that \( \pi(A^0) \subset NN \). \( \pi(A^0) \) is a submonoid because \( \pi \) is the identity and \( A^0 \) is closed under product (and \( \pi \) is multiplicative.) \( \pi(A^0) \) is GUPI by (A1.20,a). Since \( G \) is totally ordered, so is \( \pi(A^0) \). With \( m_1, m_2 \) and \( n \) as described, we have: \( n/m_1 = m_2 \in \pi(A^0) \subset NN \). By (A2.4), this implies that \( m_1 \leq n \). Since \( m_1 \) is assumed to be distinct from \( n \), it follows that \( m_1 < n \).

(e) Say \( 0 \neq a, b \in A^0 \). See (A2.3) and (A2.4) for relevant details about ordered abelian groups. \( \pi a < \pi b \) if and only if \( \pi a/\pi b \) (= \( \pi(a/b) \)) is less than the identity of \( G \). Thus \( \pi a < \pi b \) if and only if \( \pi(a/b) \) does not lie in \( NN \), the set of non-negative elements. By (A2.7,f), \( \pi(a/b) \) does not lie in \( NN \) and only if \( a/b \in V^I \). This gives the first claim in e. \( \pi a = \pi b \) if and only if \( \pi a/\pi b \) is the identity of \( G \). Since the kernel of \( \pi \) is \( V^I \) the second assertion in e is proved. The third assertion about \( \pi a \leq \pi b \) follows from the first two assertions. Say \( a + b \neq 0 \). Since \( G \) is an ordered abelian group, it is totally ordered. Thus \( \pi a \leq \pi b \) or \( \pi b \leq \pi a \). Say \( \pi a \leq \pi b \). Then \( a/b \in V \) by what we have shown already of part e. Thus \( (a+b)/b = a/b + 1 \) lies in \( V \) and by what we have already shown it follows that \( \pi(a+b) \leq \pi b \). This finishes part e.

(f) Say \( \pi b = \text{max}(\pi a, \pi b) \). If \( \gamma a + \lambda b = 0 \), then \( \gamma a = b(-\lambda + 0) \). If \( \gamma a + \lambda b \neq 0 \) with \( \pi(\gamma a + \lambda b) < \text{max}(\pi a, \pi b) = \pi b \), by (A2.8), \( (\gamma a + \lambda b)/b \in V^I \), and so \( \gamma a = b(-\lambda + \gamma a + \lambda b)/b \). Either way, \( \gamma a = b(-\lambda + x') \) with \( x' \in V^I \). Since \( \lambda \neq 0 \), \( -\lambda + x' \in V^I \). By (A2.8), \( \pi x = \pi b \). Since \( \pi \gamma \) is the identity of \( G \) and \( \pi(\gamma a) = (\pi \gamma)(\pi a) \), \( f \) is proved.

(g) Say \( \pi a = \pi b \). By (A2.8), there is \( x \in V^I \) with \( a = xb \). Since \( A \cap V \) is a group theoretic complement to \( V^I \), \( x = \lambda + x' \) with \( \lambda \in A \cap V \) and \( x' \in V^I \). Since \( x \in V^I \), \( \lambda \neq 0 \). Now \( (a-\lambda b)/b = x' \in V^I \). Depending whether \( x' \) is zero or not: \( a-\lambda b = 0 \) or by (A2.8) \( \pi(a-\lambda b) < \pi b = \pi a \).

(h) Let \( a = \sum_{i=1}^N a_i \). We are trying to prove: \( a + b \neq 0 \) and \( \pi(a+b) = \pi b \). The result is clear if \( a = 0 \). Therefore we can assume that \( a \neq 0 \) and some of the \( a_i \)’s must not be zero. Let \( m' \) be the maximal value assumed by \( \pi a_i \) for non-zero \( a_i \). Note that \( m' < m \). By part e iterated: \( \pi a \leq m' \), which is less than \( m \). Thus by part e: \( a/b \in V^I \). \( V^I \) is closed under difference, (A2.7.b). Since \( 1 = (a/b+1) - a/b \) and \( a/b \in V^I \) it follows that \( (a/b+1) \notin V^I \) or else we would have the contradiction that \( 1 \in V^I \). Hence: \( (a/b+1) \in V^I \) and cannot be zero. \( (a/b+1) = (a+b)/b \). This shows that \( a+b \neq 0 \). By part e, the fact that \( (a+b)/b \in V^I \), implies that \( \pi(a+b) = \pi b \), as desired.

\( \pi(A^0) \) has two orderings. There is the ordering from (A1.20,c), which merely depends on \( \pi(A^0) \) being a GUPI monoid. There is the ordering inherited from the ordering on \( G \). For \( 0 \neq a, b \in A \), \( \pi a \leq \pi b \) in the GUPI ordering, (A1.20,c), if and only if \( \pi a/\pi b \) in \( \pi(A^0) \). This comes down to there being \( 0 \neq c \in A \) and \( x \in V^I \) with \( ca = bx \). In this case \( c^{-1} \in V^I \) and \( a/b = x/c \in V^I \). By (A2.8) this implies

\( \pi(A^0) \) has two orderings. There is the ordering from (A1.20,c), which merely depends on \( \pi(A^0) \) being a GUPI monoid. There is the ordering inherited from the ordering on \( G \). For \( 0 \neq a, b \in A \), \( \pi a \leq \pi b \) in the GUPI ordering, (A1.20,c), if and only if \( \pi a/\pi b \) in \( \pi(A^0) \). This comes down to there being \( 0 \neq c \in A \) and \( x \in V^I \) with \( ca = bx \). In this case \( c^{-1} \in V^I \) and \( a/b = x/c \in V^I \). By (A2.8) this implies
that \( \pi a < \pi b \) in the \( G \) ordering. The GUPI ordering is not a total ordering in general while the \( G \) ordering is a total ordering. When speaking about an ordering on \( \pi(A^0) \) we always mean the ordering inherited from \( G \), unless otherwise specified. In terms of classical Buchberger theory, the GUPI ordering corresponds to the partial ordering that arises from one monomial dividing another while the ordering from \( G \) corresponds to a refinement given by a term ordering. This is exhibited more clearly in the following example.

**Example 1.3.** Let \( A \) be a polynomial ring over a base field \( R \) and let \( F \) be the field of fractions of \( A \). Assume that \( A \) has a term ordering and let \( V \) be the subring of \( F \) consisting of zero and the fractions \( f/g \) where the leading monomial of \( f \) is less than or equal to the leading monomial of \( g \) for \( f, g \in A \). \( V \) is obviously a valuation ring. The noninvertible elements of \( V \) are zero and the elements of the form \( f/g \) where the leading monomial of \( f \) is strictly less than the leading monomial of \( g \) for \( f, g \in A \). \( A \cap V \) is just \( R \), which is a complement for the maximal ideal in \( V \). Thus \( V \) is a complementary valuation ring to \( A \) in \( F \). The invertible elements of \( V \) are the elements of the form \( f/g \) for \( 0 \neq f, g \in A \) where \( f, g \) have the same leading monomial. (A2.7,f) together with (A2.3) or (A2.4) gives an ordering on \( G = F^f/V^f \) and the natural multiplicative map \( \pi : A^0 \to G \). For \( 0 \neq f, g \in A \), \( \pi f = \pi g \) if and only if \( f \) and \( g \) have the same leading monomial and \( \pi f < \pi g \) if and only if the lead monomial of \( f \) is less than the lead monomial of \( g \) in the original term ordering. In other words, the order on \( G \) recaptures the original term ordering.

**Example 1.4.** Let \( A \) be a polynomial ring over a base field \( R \) and let \( F \) be the field of fractions of \( A \). Assume that \( A \) has a term ordering and let \( V \) be the subring of \( F \) consisting of zero and fractions \( f/g \) where the leading monomial of \( f \) is less than or equal to the leading monomial of \( g \) for \( f, g \in A \). As observed in the previous example, \( V \) is a complementary valuation ring to \( A \) and \( A \cap V = R \). Let \( B \) be any subring of \( A \) where \( B \) contains the constant polynomials \( R \). By (1.2,c), \( V \) is a complementary valuation ring to \( B \) in \( F \). As in the previous example, the \((\pi, G)\) ordering on \( B \) coincides with the ordering arising from looking at leading terms based on the term ordering.

**Definition 1.5.** Let \( V \) be a complementary valuation ring to \( A \) in \( F \) and \( a, b, c \in A^0 \). \( \pi b \) divides \( \pi a \) relative to \( V \), if there is \( d \in A \) with \( \pi a = (\pi b)(\pi d) \). \( c \) is an approximate quotient of \( a \) by \( b \), relative to \( V \), if \( a = bc \) or if \( a \neq bc \) and \( \pi(a - bc) < \pi a \).

In practice the “relative to \( V \)” will be omitted.

**Proposition 1.6.** Say \( a, b \in A^0 \). \( \pi b \) divide \( \pi a \) if and only if there is \( c \in A^0 \) which is an approximate quotient of \( a \) by \( b \). If \( c \) is an approximate quotient of \( a \) by \( b \) then \( \pi a = \pi(bc) = (\pi b)(\pi c) \).

**Proof.** If \( \pi b \) divides \( \pi a \) there is \( c \in A^0 \) with \( \pi a = (\pi b)(\pi c) \) and so \( \pi a = \pi(bc) \). By (1.2,g) – with \( bc \) for \( b \) – there is \( 0 \neq \lambda \in A \cap V \) with \( a - \lambda bc = 0 \) or \( a - \lambda bc \neq 0 \).
and $\pi(a - \lambda bc) < \pi a$. Since $\lambda$ is an invertible element of $V$, $\pi \lambda$ is the identity. Thus $\pi(\lambda c) = \pi c$ and $\lambda c$ is an approximate quotient of $a$ by $b$.

Now say $c$ is an approximate quotient of $a$ by $b$. By (1.2,f) – with $bc$ for $b$ – it follows that $\pi a = \pi(bc)$. Since $\pi(bc) = \pi(b)\pi(c)$ we are done. \hfill $\Box$

Here is the generalized form of Buchberger reduction.

**Reduction 1.7.** Let $V$ be a complementary valuation ring to $A$ in $F$, $G \subset A^\theta$ and $a \in A$. The following is called the reduction of $a$ over $G$ relative to $V$:

(a) $a$ has a first reductum over $G$ – i.e., (1.7) iterates at least one time – if and only if $a \neq 0$ and there is $g \in G$ where $\pi g$ divides $\pi a$.

Now assume that $a$ has an $n^{th}$ reductum $a_n$ over $G$ – i.e. (1.7) iterates at least $n$ times.

(b) $a = a_n + \sum_{i=0}^{n-1} g_i h_i$ where $\{g_i\} \subset G$, $\{h_i\} \subset A$.

(c) $\pi(g_{n-1} h_{n-1}) < \pi(g_{n-2} h_{n-2}) < \cdots < \pi(g_1 h_1) < \pi(g_0 h_0)$

(d) If $a_n \neq 0$, then $\pi a_n < \pi a_{n-1}$.

Now assume that $G$ lies in the ideal $I$.

(e) $a \in I$ if and only if $a_n \in I$.

**Proof.** Part a is immediate from the specification of (1.7).

Since $a_{i+1} = a_i - g_i h_i$, it follows that $a_n = a - \sum_{i=0}^{n-1} g_i h_i$. This give part b. Since $a_n$ is produced, none of $a_0, \ldots, a_{n-1}$ are zero. By definition of the approximate quotient of $a_i$ by $g_i$ if $a_i - g_i h_i$ is non-zero, then $\pi(a_i - g_i h_i) < \pi a_i$. Thus

$$\pi a_{n-1} < \pi a_{n-2} < \cdots < \pi a_0 = \pi a$$
and $\pi a_n < \pi a_{n-1}$ if $a_n \neq 0$. By (1.6), $\pi a_i = \pi (g_i h_i)$. This gives parts c and d of the proposition.

Part e follows from part b since $\sum_{i=0}^{n-1} g_i h_i \in I$. □

**Definition 1.9.** Let $V$ be a complementary valuation ring to $A$ in $F$, $I \subset A$ is a non-zero ideal and $G \subset I^\theta$. **G is a Gröbner basis for I relative to V** if it satisfies either of the following two conditions which are equivalent by (1.8,a):

(i) Every non-zero element of $I$ has a first reductum over $G$.
(ii) For every $a \in I^\theta \setminus I_0$ there is $g \in G$ where $\pi g$ divides $\pi a$.

In practice the “relative to $V$” will be omitted. Here is an instant algorithm for finding Gröbner bases of non-zero ideals: take the set theoretic complement to $\{0\}$ in the ideal. In other words, $I^\theta$ is always a Gröbner basis for a non-zero ideal $I$. It is not a useful Gröbner basis but it shows that every non-zero ideal has a Gröbner basis. Of course what we really need is a finite Gröbner basis.

Note that we do not require $G$ to generate $I$ as an ideal. However we have:

**Proposition 1.10.** Suppose $G$ is a Gröbner basis for $I$ and $a \in A$ where a reductum of $a$ over $G$ terminated with $b$ as the last reductum of $a$.

(a) $a \in I$ if and only if $b = 0$.
(b) If all the elements of $I$ have a terminating reduction over $G$, then $G$ generates the ideal $I$.

*Proof.* (a) If $b = 0$ then $a \in I$ by (1.8,e). Since the reduction of $a$ terminated at $b$, it follows that $b$ does not have a first reductum over $G$. Thus if $b \neq 0$, by (1.8,a) it follows that $\pi b$ is not divisible by $\pi g$ for any $g \in G$. By definition of Gröbner bases it follows that $b \notin I^\theta$ and hence $b \notin I$. By (1.8,e), this implies that $a \notin I$.

(b) Let $a$ be any element of $I$. By part a, the terminating reductum for $a$ must terminate in zero. Suppose zero is the $n^{th}$ reductum of $a$. By (1.6,b), it follows that:

$$a = \sum_{i=0}^{n-1} g_i h_i, \quad \text{where} \quad \{g_i\} \subset G, \{h_i\} \subset A.$$  

Thus $G$ generates $I$. □

**Chat 1.11.** To prove better results, it is necessary to know that elements of $A$ have a terminating reduction over $G$. This is studied in the next section. It involves closer study of the monoid $\pi (A^0)$, especially the ordering on the monoid. A set is **well-ordered** if it is totally ordered and every subset has a least element. For example, $\mathbb{N}$ is well-ordered. Well-orderedness is a strong assumption and extremely useful for insuring that iterative processes stop. As one example, it is easily verified that if a set is well-ordered, then decreasing sequences of elements from the set must become constant. It is also useful and easy to verify that a subset of a well-ordered set is well-ordered with the induced order. Thus $\pi (I^\theta)$ is well-ordered if $\pi (A^0)$ is well-ordered. (1.2,d) established the fact that $\pi (A^0)$ is totally ordered. Is it well-ordered? (2.8)
proves that $\pi(A^0)$ is well ordered if it is Noetherian. (A1.10) shows that $\pi(A^0)$ is Noetherian if it is finitely generated as a monoid, (A1.3). (A1.12) shows that $\pi(A^0)$ is finitely generated if it is a submonoid of $\mathbb{N}$. Example (2.5) shows that if $A$ is any subalgebra of the polynomial ring in one variable over a field, then a complementary valuation ring may be chosen so that $\pi(A^0) \subseteq \mathbb{N}$. Hence, our theory applies to all subalgebras of $R[X]$. Example (2.4) shows that in the classical situation with $A = R[X_1, \ldots, X_n]$ and $R$ a field, a complementary valuation ring arises from a term ordering on the monomials of $A$ whereby $\pi(A^0) = \mathbb{N} \times \cdots \times \mathbb{N}$ ($n$ times). If $B$ is a subring of $A$ and $B$ contains $R$, then the $V$ in (2.4) is a complementary valuation ring to $B$. $\pi(B^0) \subseteq \pi(A^0) = \mathbb{N} \times \cdots \times \mathbb{N}$. When is $\pi(B^0)$ a finitely generated monoid? The obvious more specific question is: is $\pi(B^0)$ finitely generated as a monoid if $B$ is a finitely generated algebra over $R$? (1.12) and (1.13) are what we can say if $\pi(I^0)$ is well-ordered:

**Lemma 1.12.** Let $V$ be a complementary valuation ring to $A$ in $F$, let $I$ be an ideal in $A$, $G \subset I^0$, and $a \in I$.

(a) If $\pi(I^0)$ is well ordered then reduction of $a$ over $G$ terminates after a finite number of steps.

(b) If $\pi(I^0)$ is well ordered then reduction of any element of $A$ over $G$ terminates after a finite number of steps.

**Proof.** (a) By (1.8,b), all the reductums of $a$ lie in $I$. By (1.8,c), if $a_n$ and $a_{n+1}$ are successive reductums of $a$ and $a_{n+1} \neq 0$, then $\pi a_n > \pi a_{n+1}$. If reduction does not terminate, the reductums are all non-zero and form a descending sequence in $\pi(I^0)$, which is impossible.

(b) Letting $I = A$, this follows from part a. □

**Proposition 1.13.** Let $V$ be a complementary valuation ring to $A$ in $F$ and let $I$ be an ideal in $A$. Suppose $G \subset I^0$ and assume that $\pi(I^0)$ is well-ordered.

(a) $G$ is a Gröbner basis for $I$ if and only if every element of $I$ reduces to zero over $G$.

(b) If $G$ is a Gröbner basis for $I$, then $G$ generates $I$ as an ideal.

(c) Suppose $G$ is a Gröbner basis for $I$ and $\pi(A^0)$ is well-ordered. If $a \in A$ then:

- $a \in I$ if and only if if $a$ reduces to zero over $G$.

**Proof.** (a) If every element of $I$ reduces to zero over $G$, then $G$ is a Gröbner basis for $I$ by (1.9,i). Conversely say $G$ is a Gröbner basis for $I$ and $a \in I$. If $a = 0$, there is nothing to show. Suppose $a \neq 0$. By (1.12,a), $a$ has a last reductum $a_n$ over $G$. Since a reduction of $a_n$ over $G$ is a further reduction of $a$, it follows that $a_n$ cannot be reduced over $G$. By (1.9,i), $a_n = 0$.

(b) (1.10,b) and (1.12,a).

(c) (1.10,a) and (1.12,b). □
2. The Monoid

Let $V$ be a complementary valuation ring to $A$ in the field $F$. In (1.12,d), we proved that $\pi(A^0)$ is a submonoid of $NN$. $\pi(A^0)$ being Noetherian, (A1.9), assures the termination of the main algorithm of our theory. In this section we develop properties of $\pi(A^0)$, which are needed for proving termination of algorithms. (1.10) was phrased in terms of whether elements have terminating reduction. In this section we prove that: $\pi(A^0)$ being Noetherian, assures termination, (2.9). Example (2.4) traces the classical theory in the present context. Example (2.5) develops a very simple example which is not covered by the classical theory. Both of these examples are carried further in the next section.

Lemma 2.1. Let $V$ be a complementary valuation ring to $A$ in the field $F$.

(a) If $I$ is an ideal of $A$, then $\pi(I^0)$ is an ideal in $\pi(A^0)$. (See (A1.1-A1.3) about ideals in monoids and the ideal generated by a set.)

(b) If $I$ is a non-zero principal ideal of $A$ generated by $a$, then $\pi(I^0)$ is the ideal in the monoid $\pi(A^0)$ generated by $\pi a$.

Proof. (a) If $a' \in \pi(I^0)$ and $x' \in \pi(A^0)$ let $a' = \pi a$ and $x' = \pi x$ for some $a \in I^0$ and $x \in A^0$. Then $x'a' = \pi(xa)$ and $xa \in I^0$ since $I$ is an ideal (and $A$ is an integral domain).

(b) $I^0$ consists of the elements of $A$ of the form $xa$ with $0 \neq x \in A$. Thus $\pi(I^0)$ consists of the elements of $\pi(A^0)$ of the form $(\pi x)(\pi a)$ with $0 \neq x \in A$. This gives the desired result.

Definition 2.2. Let $V$ be a complementary valuation ring to $A$ in the field $F$. $\pi(A^0) \subset NN$ is the monoid of $A$ with respect to $V$. If $I$ is a non-zero ideal in $A$, $\pi(I^0)$ is the ideal determined by $I$ in $\pi(A^0)$, with respect to $V$.

As usual the “with respect to $V$” is generally omitted. Say $V$ is a complementary valuation ring to $A$ in $F$, $I \subset A$ is a non-zero ideal and $G \subset I^0$. Rephrasing (1.9,ii) we have:

2.3. $G$ is a Gröbner basis for $I$ if and only if $\pi G$ generates the ideal $\pi(I^0)$ in the monoid $\pi(A^0)$.

Example 2.4. As in example (1.3), let $A$ be a polynomial ring $R[X_1, \ldots, X_n]$ over a base field $R$ and let $F$ be the field of fractions of $A$. Assume that $A$ has a term ordering and let $V$ be the subring of $F$ consisting of zero and fractions $f/g$ where the leading monomial of $f$ is less than or equal to the leading monomial of $g$ for $f, g \in A$. The monoid of $A$ is naturally isomorphic to $\mathbb{N} \times \cdots \times \mathbb{N}$ (n times). The isomorphism is given by: for $f \in A$ if the lead monomial of $f$ is $X_1^{e_1}X_2^{e_2}\cdots X_n^{e_n}$ then $\pi f = (e_1, \ldots, e_n)$.

Example 2.5. Suppose $R$ is a field and $AA$ is the polynomial ring $R[X]$, considered as an algebra over $R$. By subalgebra of $AA$, we mean subring containing $R$. Let
\( F = R(X) \) the field of rational functions in one variable. \( F \) is the field of fractions of \( AA \). Let \( V = \{ f \in F \mid \exists a, b \in AA \text{ with } \deg a \leq \deg b \text{ and } f = a/b \} \). \( AA \cap V = R \), so \( V \) is a complementary valuation ring to \( A \). A number of interesting rings arise as subalgebras of \( R[X] \). Let \( A \) be the subalgebra of \( R[X] \) generated by \( X^2 \) and \( X^3 \). (So \( A \) consists of polynomials with no term of degree one. Geometrically \( A \) represents the cusps.) \( \pi(A^0) \) is naturally isomorphic to the additive monoid \( \{0, 2, 3, 4, \ldots \} \) where \( \pi f = \deg f \) for \( f \in A \).

In (2.5) we have carried through an idea first mentioned in (1.4). Let us continue that example.

**Example 2.6.** Let \( A, F \) and \( V \) be as in example (1.3) and (2.4). Suppose that \( M \) is a submonoid of \( \mathbb{N} \times \cdots \times \mathbb{N} \) (\( n \) times). For each \( \mathbf{m} = (m_1, m_2, \ldots, m_n) \in M \), let \( x^\mathbf{m} \) denote the monomial \( x_1^{m_1}x_2^{m_2}\cdots x_n^{m_n} \in A \). (If \( 0 \) is the identity element of \( M \) or \( \mathbb{N} \times \cdots \times \mathbb{N} \) then \( x^0 = 1 \).) Submonoid monomials, \( \{x^\mathbf{m}\}_{\mathbf{m} \in M} \), are linearly independent over \( R \) and span a subalgebra \( B \) of \( A \). This is a special case of (1.4) and \( V \) is a complementary valuation ring to \( B \). Although different notation is sometimes used, \( B \) is the monoid algebra of \( M \). \( \pi(B^0) \) is naturally isomorphic to the additive monoid \( M \).

So far all the examples have been polynomial rings or monoid algebras. Here is one which is not.

**Example 2.7.** Let \( R, AA, F \) and \( V \) be as in example (2.5). Let \( A \) be the subalgebra of \( AA \) generated by \( X^3 - X \) and \( X^2 \). Does \( X \) lie in \( A \)? Thus may be determined using classical Gröbner bases as follows: form \( R[X, U, V] \) and use the pure lex term ordering with \( X > U > V \). The ideal \( J \) generated by \( X^3 - X - U \) and \( X^2 - V \) has the following Gröbner basis:

\[
X^2 - V, \ XU - V^2 + V, \ XV - X - U, \ U^2 - V^3 + 2V^2 - V
\]

If \( X \) were in \( A \), there would be some polynomial \( P(Y, Z) \) of two variables where \( X = P(X^3 - X, X^2) \). But then \( X - P(U, V) \in J \). However, \( X - P(U, V) \) cannot be reduced any further over the Gröbner basis for \( J \). Thus \( X \) does not lie in \( A \). The Gröbner basis also gives us the relation: \( U_2 - V^3 + 2V^2 - V \) between \( U = X^3 - X \) and \( V = X^2 \). This is not a relation arising from a relation in an underlying monoid. (Relations from an underlying monoid are of the form: monomial\(_1(U, V) - \)monomial\(_2(U, V) \).) Finally, it is easy to check that if \( \alpha, \beta, \gamma \in R \) and change to new generators of the form: new\(_1 = (X^3 - X) + \alpha X^2 + \beta \), new\(_2 = X^2 + \gamma \), then new\(_1\) and new\(_2\) do not satisfy a relation arising from an underlying monoid. What is \( \pi(A^0) \)? \( \pi(X^3 - X) = 3 \) and \( \pi(X^2) = 2 \). Since \( X \not\in A \), \( A \) does not contain any linear term. Thus \( \pi(A^0) = \{0, 2, 3, 4, \ldots \} \).

At (1.11) we discussed the property of well-orderedness and mentioned a condition which insures that \( \pi(A^0) \) is well-ordered. Here is the promised result:
Theorem 2.8. If $\pi(A^0)$ is Noetherian, then it is well-ordered.

Proof. Suppose $\pi(A^0)$ is not well-ordered. Let $S \subset \pi(A^0)$ be a subset with no least element. Choose a sequence of distinct elements of $S$, $s_1, s_2, s_3, \ldots$, where $s_1 > s_2 > s_3 > \cdots$. By (A1.16), there is a subsequence $(s_{e_1}, s_{e_2}, s_{e_3}, \ldots)$ consisting of distinct elements where $e_i < e_j$ and $s_{e_i} | s_{e_j}$ for $i < j$. By (1.12,d), $s_{e_i} | s_{e_j}$ implies that $s_{e_i} < s_{e_j}$ for $i < j$, which contradicts the fact that $s_1 > s_2 > s_3 > \cdots$. Hence $\pi(A^0)$ is well-ordered. □

A quick application:

Corollary 2.9. Let $V$ be a complementary valuation ring to $A$ in $F$ and $G \subset A^0$. If $\pi(A^0)$ is Noetherian then reduction of any element of $A$ over $G$ terminates after a finite number of steps.

Proof. (2.8) and (1.12,b). □

Another:

Corollary 2.10. Let $V$ be a complementary valuation ring to $A$ in $F$ and let $I$ be an ideal in $A$. Suppose $G \subset I^0$ and assume that $\pi(A^0)$ is Noetherian.

(a) $G$ is a Gröbner basis for $I$ if and only if every element of $I$ reduces to zero over $G$.

(b) If $G$ is a Gröbner basis for $I$ then $G$ generates $I$ as an ideal.

(c) If $G$ is a Gröbner basis for $I$ and $a \in A$, then $a \in I$ if and only if $a$ reduces to zero over $G$.

Proof. (2.8) and (1.13). □

It is natural to wonder whether the converse to (2.8) is true. The answer is NO as shown by:

Example 2.11. Let $A$, $F$, and $V$ be as in example (2.6) where the polynomial ring has two variables. Rather than write $X_1$ and $X_2$ we use $X$ and $Y$. Let $M$ be the submonoid of $\mathbb{N} \times \mathbb{N}$ generated by the set $\text{Gen} = \{(1,0), (1,1), (1,2), (1,3), \ldots\}$. As in (2.6) the subalgebra $B$ of $A$ corresponding to $M$ is generated as an algebra by \{X, XY, XY^2, XY^3, \ldots\}. $\mathbb{N} \times \mathbb{N}$ is well ordered by (2.8). Since $M \subset \mathbb{N} \times \mathbb{N}$ it is also well ordered. $M$ is not Noetherian. The ideal in $M$ generated by the set $\text{Gen}$ is not finitely generated.

3. Test and Construction

In section one we introduced reduction, (1.7). It was essentially the same as reduction in the classical Buchberger theory. Now we get to the syzygies. In classical Buchberger theory, for two polynomials there is a single $S$-polynomial. In the new theory there may be more than one $S$-polynomial. Two elements, $a$ and $b$ give rise to an $S$ family or syzygy family. There is one element in the family for each generator.
of a particular ideal in a monoid. The monoid $M$ is defined at (2.2). The ideal in $M$ is the intersection of principal ideals arising from $a$ and $b$. In the classical theory, $M = \mathbb{N} \times \cdots \times \mathbb{N}$, and the intersection of principal ideals is again principal. Hence, the syzygy family consists of one element. That is why starting with two polynomials yields one $S$ polynomial. Example (3.5) traces the classical theory in the present context. Example (3.6) develops a very simple example where a syzygy family has two elements. After syzygy families, our new theory again closely resembles classical Buchberger theory. For example, the syzygy family provides a test for when a set is a Gröbner basis, (3.7). The test is the usual test of whether every syzygy reduces to zero. This is also the key to constructing Gröbner bases. As in classical Buchberger theory, if a syzygy reduces to $r \neq 0$ then add $r$ to the forming Gröbner basis. If the process terminates, the test, just mentioned, shows that the result is a Gröbner basis. As in the classical theory, the question of whether or not the process stops, is not trivial. It comes down to whether ideals in the monoid $M$ are finitely generated.

**Notation 3.1.** Suppose $a \in A^g$, let $\langle \pi a \rangle$ denote the ideal in $\pi(A^g)$ generated by $\pi a$.

**Lemma 3.2.** Assume $a, b \in A^g$ and $m \in \langle \pi a \rangle \cap \langle \pi b \rangle$. There are $x, y \in A^g$ where $\pi(xa) = m = \pi(yb)$ and $xa = yb$ or $xa - yb \neq 0$ and $\pi(xa - yb) < m$.

**Proof.** Since $m \in \langle \pi a \rangle$ there is $x \in A^g$ where $m = (\pi x)(\pi a)$. Similarly there is $w \in A^g$ where $m = (\pi w)(\pi b)$. Thus $\pi(xa) = m = \pi(wb)$. By (1.2), there is $0 \neq \lambda \in A \cap V$ with $xa = \lambda wb$ or $xa - \lambda wb \neq 0$ and $\pi(xa - \lambda wb) < \pi a = m$. Since $\pi \lambda$ is the identity of $G$, $\pi(\lambda wb) = \pi w$. Hence letting $y = \lambda w$ finishes the lemma.

**Definition 3.3.** Let $V$ be a complementary valuation ring to $A$ in the field $F$ and let $a, b \in A$. $T \subset \pi(A^g)$ is a **monoid ideal generating set for a and b with respect to V** if $T$ is contained in and generates the ideal $\langle \pi a \rangle \cap \langle \pi b \rangle$ in $\pi(A^g)$. If $T$ is a monoid ideal generating set for $a$ and $b$, by (3.2) for each $t \in T$ there are $x_t, y_t \in A^g$ where $\pi(x_t a) = t = \pi(y_t b)$ and $x_t a = y_t b$ or $x_t a \neq y_t b$ and $\pi(x_t a - y_t b) < t$. This gives a map: $T \rightarrow A, t \mapsto x_t a - y_t b$. The image of this map: $\{ c \in A \mid c = x_t a - y_t b \text{ for } t \in T \}$, is a **syzygy family for a and b indexed by T**. $x_t a - y_t b$ is called the element of the family corresponding to $t$.

It is immediate from the definition that:

**3.4.** A syzygy family for $a$ and $b$ lies in the ideal in $A$ generated by $\{a, b\}$.

It is quite possible that for $t \neq u \in T$, the elements $x_t a - y_t b$ and $x_u a - y_u b$ are equal. Also there is not a unique syzygy family for $a$ and $b$ arising from $T$.

**Example 3.5** (continuing 2.4). In $\mathbb{N} \times \cdots \times \mathbb{N}$ generators are unique for principal ideals. This is easily verified directly or from (A1.5) and (A1.20,b). Also the intersection of principal ideals is again principal. The intersection of the principal ideals generated by $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$ has the (unique) generator $(z_1, z_2, \ldots, z_n)$, where $z_i = \max(x_i, y_i)$. Hence, for $a, b \in A^g$ there is a unique single
element monoid ideal generating set for $a$ and $b$. This set is $T = \{\pi m\}$ where $m$ is the monomial which is the least common multiple of the leading monomials of $a$ and $b$. Since $T$ has one element, a syzygy family indexed by $T$ is just a single $x^m a - y^m b \in A$ where $x^m a$ and $y^m b$ both have lead monomial $m$ and $x^m a = y^m b$ or $x^m a - y^m b \neq 0$ and $x^m a - y^m b$ has lead monomial which is less than $m$. This shows that for $A = R[X_1, \ldots, X_n]$, the classical notion of $S$ polynomial of two elements is – in terms of (3.3) – the singleton syzygy family indexed by the unique generator of the intersection of the two principal ideals.

**Example 3.6** (continuing 2.5). In the additive monoid $\{0, 2, 3, 4, \ldots \}$, the intersection of principal ideals is not principal. For example:

- $\langle \pi X^2 \rangle = 2 + \{0, 2, 3, 4, \ldots \} = \{2, 4, 5, 6, \ldots \}
- \langle \pi X^3 \rangle = 3 + \{0, 2, 3, 4, \ldots \} = \{3, 5, 6, 7, \ldots \}
- \langle \pi X^2 \rangle \cap \langle \pi X^3 \rangle = \{5, 6, 7, \ldots \}$

The ideal generated by 5 in the monoid is:

$$5 + \{0, 2, 3, 4, \ldots \} + \{5, 7, 8, \ldots \}$$

which misses the element 6. Thus, $\{5, 6\}$ is the smallest possible generating set for $\langle \pi X^2 \rangle \cap \langle \pi X^3 \rangle$. This shows that $T = \{5, 6\}$ is the smallest monoid ideal generating set for $X^2$ and $X^3$.

**Theorem 3.7** (Test Theorem). Assume $V$ is a complementary valuation ring to $A$ in the field $F$, $I$ is a non-zero ideal in $A$ where $\pi(I^0)$ is well-ordered and $G \subset I^0$ is a generating set for $I$. Suppose for each distinct set of elements $g, h \in G$: $T_{g,h}$ is a monoid ideal generating set for $g$ and $h$ and $S_{g,h}$ is a syzygy family for $g$ and $h$ indexed by $T_{g,h}$. Let $U = \cup_{g \neq h \in G} S_{g,h}$. $G$ is a Gröbner basis for $I$ if and only if every element of $U$ reduces to zero over $G$.

**COMMENTS:**

- See (1.11) for a discussion of when the “$\pi(I^0)$ is well-ordered” hypothesis holds.

  In various expositions of classical Buchberger theory, the Test Theorem seems to be the result whose proof has the most hand-waving. We go to the opposite extreme and present the proof in gruesome detail. It may be ugly and boring, but it is all here. Actually, the beginning of the proof presents an interesting representation of elements. About half way through the proof, (3.10), we put aside details and give an overview of the rest of the proof. Then we fill in the details.

  There is no assumption that $U$ is a finite set.

**Proof.** Suppose $G$ is a Gröbner basis for $I$. By (3.4): $U \subset I$. By (1.13,a), it follows that every element of $U$ reduces to zero over $G$.

  The hard part is the other direction. The proof proceeds by a double minimization argument. As a framework for the argument, we introduce a convenient terminology.
The terminology concerns the *representation* of sums, as opposed to the actual value of the sums. We shall sometimes put an expression in quotes to emphasize that we are concerned with the representation rather than the value. Say “\(\sum z_i\)” is a sum of elements of \(A\) and \(m \in \pi(A^0)\). Assume that not all of the \(z_i\)’s are zero and \(\pi z_i = m\) for the non-zero \(z_i\)’s. Then “\(\sum z_i\)” is called a **level sum**. \(m\) is called the **level of the sum**. The **length** of the sum is the number of non-zero \(z_i\)’s. If “\(\sum_1^N z_i\)” is a level \(m\) sum and \(a = \sum_1^N z_i\), then by (1.2,e), \(a = 0\) or \(\pi a \leq m\). All three cases: \(a = 0\), \(\pi a < m\), and \(\pi a = m\) can occur. Suppose \(z \in A\) and \(z\) is represented as a sum “\(\sum_1^N z_i\)” where not all the \(z_i\)’s are zero by “\(\sum_1^N z_i\)” is not necessarily a level sum. “\(\sum_1^N z_i\)” can be broken into a sum of level sums by renumbering terms in order to group non-zero \(z_i\)’s which map to the same value in \(\pi(A^0)\) under \(\pi\). (\(z_i\)’s which are zero may be distributed arbitrarily among the level sums or discarded.) Moreover, we can renumber so that the levels of the level sums are descending. Thus we can express \(z\) as:

\[
(3.8) \quad \pi z = \sum_{e_1}^{e_2} z_{i_1} + \sum_{e_2+1}^{e_3} z_{i_2} + \cdots + \sum_{e_{T+1}}^{e_{T+2}} z_{i_T}
\]

with \(1 = e_1 < e_2 < \cdots < e_T < e_{T+1} \leq N\) where each “\(\sum_{e_j+1}^{e_{j+1}} z_i\)” is a level \(m_j\) sum and \(m_1 > m_2 > \cdots > m_{T}\).

A sum of sums of the form (3.8) is a cascade. “\(\sum_{e_j+1}^{e_{j+1}} z_i\)” is the \(j^{th}\) sum of the cascade and \(m_1\) is the height of the cascade.

Suppose \(z \in I^0\). We shall find \(g_j \in G\) where \(\pi g_j\) divides \(\pi z\). By (1.9.ii), \(G\) is a Gröbner basis for \(I\).

Since \(G\) generates \(I\) as an ideal there are \(a_i\)’s in \(A\) and \(\{g_i\}_1^N \subset G\) with \(z = \sum_1^N a_i g_i\). Thinking of \(z_i\) in (3.8) as \(a_i g_i\), we can rearrange “\(\sum_1^N a_i g_i\)” to be a cascade. The height \(m\) of the cascade is an element of \(\pi(A^0)\). In fact, \(m \in \pi(I^0)\). Consider the elements of \(\pi(I^0)\) which arise as the height of a cascade which expresses \(z\). Since \(\pi(I^0)\) is well-ordered this set has a minimal element, \(m\). In other words there is a cascade which expresses \(z\) which has height \(m\) and no cascade which expresses \(z\) has smaller height. Among the cascades which express \(z\) and have height \(m\), there is one which has the shortest first sum. Say this doubly minimal cascade which expresses \(z\) is:

\[
(3.9) \quad \pi z = \sum_{e_1}^{e_2} a_{i_1} g_{i_1} + \sum_{e_2+1}^{e_3} a_{i_2} g_{i_2} + \cdots + \sum_{e_{T+1}}^{e_{T+2}} a_{i_T} g_{i_T}
\]

with \(1 = e_1 < e_2 < \cdots < e_T < e_{T+1} \leq N\) where each “\(\sum_{e_j+1}^{e_{j+1}} z_i\)” is a level \(m_j\) sum and \(m_1 > m_2 > \cdots > m_{T}\).

Suppose for the moment that the first level sum has length one. Then it has a single non-zero element \(a_i g_i\) where \(\pi (a_i g_i) = m_1 = m\), the level of the sum. Since \(a_i g_i\) is the only non-zero term of the first sum: \(z = a_i g_i + \sum\) the sum of terms in later sums. The later sums all have level less than \(\pi(a_j g_j)\). Thus we have \(z = a_j g_j + \cdots\)
the sum of terms, \( \pi \) of which is less than \( \pi(a_jg_j) \). By (1.2.h), we have \( z \neq 0 \) and \( \pi z = \pi(a_jg_j) = \pi(a_j)\pi(g_j) \). This shows that \( \pi(g_j) \) divides \( \pi z \), as desired, (1.9.ii).

3.10 (Outline of the rest of the proof).

We have reduced the problem to showing that the first sum has length one. If not, at least two of the first terms are non-zero. With renumbering, we can assume that \( a_1g_1 \neq 0 \) and \( a_2g_2 \neq 0 \). Before getting lost in details, here is an overview of the rest of the argument. We find \( u, x, y \in A \) where

\[
\begin{align*}
(a) & \quad (a_1 - ux_1)g_1 = 0 \text{ or } \pi((a_1 - ux_1)g_1) < m \\
(b) & \quad (a_2 + uy_1)g_1 = 0 \text{ or } \pi((a_2 + uy_1)g_1) \leq m \\
(c) & \quad u(x_1g_1 - y_1g_2) = 0 \text{ or } u(x_1g_1 - y_1g_2) = \sum uv_ig_i, \\
& \quad \text{where } \pi(uv_ig_i) < m \text{ for each } i
\end{align*}
\]

(3.11)

Then \( a_1g_1 + a_2g_2 \) equals:

\[
(a_1 - ux_1)g_1 + (a_2 + uy_1)g_2 + u(x_1g_1 - y_1g_2)
\]

(3.12)

Terms I + II + NEW replace the first two terms of the first level sum in (3.9). It is no longer a level sum and we must rearrange terms. Term I moves back to a lower level sum in the cascade, or introduces a new lower level sum to the cascade. Term NEW – if non-zero – is replaced by \( \sum uv_ig_i \), as in (3.11,c). Since \( \pi(uv_ig_i) < m \) for each \( i \), these “\( \pi(uv_ig_i) \)” terms move back to the lower level sums in the cascade or introduce new lower level terms. If Term II is zero, ignore it. If it is not zero and \( \pi((a_2 + uy_1)g_2) < m \), then Term II moves back to a lower level sum in the cascade, or introduces a new lower level sum to the cascade. If \( \pi((a_2 + uy_1)g_2) = m \), then Term II nonempty in the first sum. In any event, the first level sum has lost one or two non-zero terms. If there are other non-zero terms, it is still the first level sum, but has gotten one or two terms shorter. This contradicts the minimal length assumption for the first level sum. Thus the first level sum must have lost two non-zero terms these were the only non-zero terms in the sum. A lower level sum now becomes the new first sum. This contradicts the minimality of \( m \). Hence, the first sum must have had but one non-zero term.

Now to fill in the details. Since the first sum is a level \( m \) sum, \( (\pi a_1)(\pi g_1) = \pi(a_1g_1) = m = \pi(a_2g_2) = (\pi a_2)(\pi g_2) \). Thus \( m \in (\pi g_1) \cap (\pi g_2) \). \( T_{g_1,g_2} \) is a monoid ideal generating set for \( g_1 \) and \( g_2 \). Hence, there is a \( t \in T_{g_1,g_2} \) which divides \( m \). Let \( x_1g_1 - y_1g_2 \) be the element corresponding to \( t \) of the syzygy family \( S_{g_1,g_2} \) for \( g_1 \) and \( g_2 \) indexed by \( T_{g_1,g_2} \), (3.3). Then \( \pi(x_1g_1) = t \). Since \( t \) divides \( m \), by (1.6), there is \( u \in A^0 \) where \( u \) is an approximate quotient of \( a_1g_1 \) by \( x_1g_1 \). By the definition of approximate quotient, (1.5), \( a_1g_1 = ux_1g_1 \) or \( a_1g_1 \neq ux_1g_1 \) and \( \pi(a_1g_1 - ux_1g_1) < \pi(a_1g_1) = m \). Thus (3.11,a) is satisfied. By definition (3.3), \( \pi(y_1g_2) = t = \pi(x_1g_1) \) by (1.6),
\[ m = \pi(u)\pi(x_tg_1). \] Thus \( m = \pi(u)\pi(y_tg_2) = \pi(uy_tg_2). \] By (1.2,e), it follows that \( a_2g_2 + uy_tg_2 = 0 \) or \( \pi(a_2g_2 + uy_tg_2) \leq m. \) Hence, (3.11,b) is satisfied.

By (3.3), \( x_tg_1 = y_tg_2 \) or \( x_tg_1 - y_tg_2 \neq 0 \) and \( \pi(x_tg_1 - y_tg_2) < t. \) If \( x_tg_1 = y_tg_2 \) then (3.11,c) is satisfied. Suppose \( x_tg_1 - y_tg_2 \neq 0 \) and \( t' = \pi(x_tg_1 - y_tg_2) < t. \)

Since \( x_tg_1 - y_tg_2 \) is an element of the syzygy family \( S_{g_1,g_2}, \) it lies in \( U, \) the union of the syzygy families. By hypothesis, \( x_tg_1 - y_tg_2 \) reduces to zero over \( G. \) By (1.8,b) it follows that: \( x_tg_1 - y_tg_2 = \sum v_tg_i, \) where, by (1.8,c), \( \pi(v_tg_i) \leq t' < t. \) Then \( \pi(uv_tg_i) = \pi(u)\pi(v_tg_i) = \pi(u)t' < \pi(u)t = \pi(u)\pi(x_tg_1). \) Again by (1.6), \( \pi(u)\pi(x_tg_1) = m. \) Thus \( \pi(uv_tg_i) < m \) for each \( i \) and (3.11,c) is satisfied.

This fills in the outline presented at (3.10). \( \square \)

As in classical Buchberger theory, the test theorem us the key to proving that the construction algorithm gives a Gröbner basis. Proving termination is a separate matter. The remaining important result is the Gröbner basis construction technique. Here it is:

**Algorithm 3.13** (Gröbner Basis Construction Algorithm). Assume \( V \) is a complementary valuation ring to \( A \) in the field \( F, \) \( I \) is a nonzero ideal in \( A \) where \( \pi(I^0) \) is well-ordered and \( G \subset I^0 \) is a generating set for \( I. \)

(0) Let \( G_0 = G. \)

(1) For each pair of distinct elements \( g, h \in G: \) find \( T_{0,g,h}, \) a monoid ideal generating set for \( g \) and \( h, \) and find \( S_{0,g,h}, \) a syzygy family for \( g \) and \( h \) indexed by \( T_{0,g,h}. \) Let \( U_0 = \cup_{g \neq h \in G} S_{0,g,h}. \)

(2) We enter this step with \( G_i \subset I \) and \( U_i \subset I. \) Since \( \pi(I^0) \) is well-ordered, every element of \( U_i \) has a terminating reduction over \( G_i, \) (1.12,a). Let \( H_i \) be the set of nonzero final reductums that occur from reducing the elements of \( U_i \) over \( G_i. \) \( H_i \subset I, \) by (1.8,e).

(3) If \( H_i \) is empty, stop.

(4) Define \( G_{i+1} = G_i \cup H_i. \)

(5) For each pair of distinct elements \( g \in G_{i+1} \) and \( h \in H_i, \) find \( T_{i+1,g,h}, \) a monoid generating set for \( g \) and \( h, \) and find \( S_{i+1,g,h}, \) a syzygy family for \( g \) and \( h \) indexed by \( T_{i+1,g,h}. \) Let \( U_{i+1} = \cup_{g \neq h \in G} S_{i+1,g,h}. \) By (3.4), \( U_{i+1} \subset I. \)

(6) Go to step (2).

**Theorem 3.14** (Gröbner Basis Construction Theorem). Assume \( V \) is a complementary valuation ring to \( A \) in the field \( F, \) \( I \) is a nonzero ideal in \( A \) where \( \pi(I^0) \) is well-ordered and \( G \subset I^0 \) generates the ideal \( I. \) Use (3.13) to find successive \( G_i\)’s. Suppose the process iterates at least \( n \) times so that \( G_0, G_1, \ldots, G_n \) are produced. For \( m \) with \( 0 \leq m \leq n, \) let \( V_m = \cup_{i=0}^{m} U_i. \)

(a) \( G_0 \subset G_1 \subset \cdots \subset G_n. \)

(b) For distinct \( g, h \in G_m, \) \( V_m \) contains a syzygy family for \( g \) and \( h. \)

(c) For \( 0 \leq m < n, \) every element of \( V_m \) reduces to zero over \( G_{m+1}. \)
(d) If \( (3.13) \) terminates at \( G_n \) – meaning stops by step 3 with \( H_n \) empty – then \( G_n \) is a Gröbner basis for \( I \).

(e) Suppose \( (3.13) \) does not terminate. If \( G_\infty = \bigcup G_i \) then \( G_\infty \) is a Gröbner basis for \( I \).

(f) If \( \pi(I^0) \) is a finitely generated ideal in the monoid \( \pi(A^0) \), then \( (3.13) \) terminates after a finite number of steps.

(g) If \( G \) is finite and \( \pi(I^0) \) is Noetherian, meaning that ideals lying within \( \pi(I^0) \) are finitely generated, then \( (3.13) \) can be done so as to terminate with a finite Gröbner basis. (See the proof for how.)

**COMMENT:**

See (1.11) for a discussion of when the “\( \pi(I^0) \)” is well-ordered” hypothesis holds and when the “\( \pi(A^0) \)” is Noetherian” hypothesis holds. When \( \pi(A^0) \) is Noetherian, all ideals are finitely generated, so parts f and g apply.

**Proof.** (a) This follows immediately from step 4 of (3.13).

(b) If \( g, h \in G_m \) there is a minimal \( i \) with \( g, h \in G_i \). If \( i = 0 \) then \( g, h \in G \) and by step 1 of (3.13): \( S_{0,g,h} \subset U_0 \subset V_m \). If \( i > 0 \) then \( g \) or \( h \) or both are in \( H_{i-1} \) by the minimality of \( i \). Say \( h \in H_{i-1} \). By step 5 of (3.13): \( S_{i,g,h} \subset U_i \subset V_m \).

(c) \( V_0 = U_0 \). Let \( v \in V_0 \) and let \( w \) be the final reductum from reducing \( v \) over \( G_0 \). If \( w \neq 0 \) then \( w \in H_0 \) by definition of \( H_0 \), (3.13.2). By (3.13.4), \( w \in G_1 \). Hence, in one more step \( v \) reduces to zero over \( G_1 \). This shows that every element of \( V_0 \) reduces to zero over \( G_1 \). Now assume by induction that every element of \( V_{i-1} \) reduces to zero over \( G_i \). Let \( v \in V_i \) and let \( w \) be the final reductum from reducing \( v \) over \( G_{i+1} \) if \( v \in V_{i-1} \) then \( w = 0 \) by the induction assumption. If \( v \notin V_{i-1} \) then \( v \in U_i \) since \( V_i = V_{i-1} \cup U_i \). If \( w \neq 0 \), then \( w \in H_i \) by definition of \( H_i \), (3.13.2). By (3.13.4), \( w \in G_{i+1} \). Hence, in one more step \( v \) reduces to zero over \( G_{i+1} \). This completes the induction.

(d) \( G_n \) generates \( I \) since \( G = G_0 \subset G_n \) and \( G \) generates \( I \). By part b, \( V_n \) contains a syzygy family for distinct \( g, h \in G_n \). By part c, all elements of \( V_{n-1} \) reduce to zero over \( G_n \). If \( H_n \) is empty, then all elements of \( U_n \) reduce to zero over \( G_n \), (3.13.2). Since \( V_n = V_{n-1} \cup U_n \), all elements of \( V_n \) reduce to zero over \( G_n \). Thus by (3.7), \( G_n \) is a Gröbner basis for \( I \).

(e) Let \( V_\infty = \bigcup_{i=0}^\infty U_i \). For distinct \( g, h \in G_\infty \) there is some \( i \) where \( g, h \in G_i \). By part b, \( V_{i} \) contains a syzygy family for \( g \) and \( h \); hence, \( V_\infty \) contains a syzygy family for \( g \) and \( h \). \( V_\infty = \bigcup_{i=0}^\infty V_i \) and by part c, all elements of \( V_i \) reduce to zero over \( G_{i+1} \). Thus all elements of \( V_\infty \) reduce to zero over \( G_\infty \). Thus by (3.7), \( G_n \) is a Gröbner basis for \( I \).

(f) Suppose \( (3.13) \) does not terminate after a finite number of steps. By part e, \( G_\infty \) is a Gröbner basis for \( I \). By (1.19,ii), for every \( a \in I^0 \) there is \( g \in G_\infty \) where \( \pi g \) divides \( \pi a \). In other words \( \pi(G_\infty) \) generates the ideal \( \pi(I^0) \) in the monoid \( \pi(A^0) \). Since \( \pi(I^0) \) is finitely generated, a finite subset, \( fss \subset \pi(G_\infty) \), generates \( \pi(I^0) \). (If \( X \) is any finite generating set for \( \pi(I^0) \), for each \( x \in X \) there is an element \( g_x \in G_\infty \).
which divides $x$ since $G_\infty$ generates $\pi(I^0)$. Let $fss = \{g_x\}_x$. Thus there is a finite subset, FSS $\subset G_\infty$, where $\pi(FSS) = fss$. Since FSS is finite there is an $i$ where FSS $\subset G_i$. Since $\pi(FSS)$ generates the ideal $\pi(I^0)$ in the monoid $\pi(A^0)$, by (1.9,ii), $G_i$ is a Gröbner basis for $I$. Thus every element of $I$ reduces to zero over $G_i$, (1.13,a), and $H_i$ in step 2 of (3.13) is empty. Then by step 3 of (3.13), (3.13) terminates on the next step. This contradicts the assumption that (3.13) does not terminate after a finite number of steps. Hence, (3.13) terminates after a finite number of steps.

(g) If $\pi(I^0)$ is Noetherian, then $\pi(I^0)$ itself is finitely generated. Thus by part f, (3.13) terminates after a finite number of steps. In steps 1 and 5 of (3.13) a monoid ideal generating set for $g$ and $h$ is selected. $g, h \in I$ and the monoid ideal generating set is a generating set for the ideal $\langle \pi g \rangle \cap \langle \pi h \rangle$ which lies in $\pi(I^0)$. By the Noetherian hypothesis on $\pi(I^0)$, a finite monoid ideal generating set may be chosen. This insures that the syzygy family for $g$ and $h$ will be finite. As a result: if $G = G_0$ is finite then $U_0$ will be finite and if $G_i$ and $U_i$ are finite then $G_{i+1}$ and $U_{i+1}$ will be finite. □

APPENDIX 1: IDEAL THEORY IN COMMUTATIVE MONOIDS

By monoid we mean “group without inverses”. I.e. a set with an associative law of composition and a two sided identity element for this composition. In group theory normal subgroups more or less play the role of two sided ideals in ring theory. In a monoid $M$ we can define a left ideal $X$ to be a subset where $MX \subset X$. Unlike groups this does not force $X$ to equal $M$. The monoid ideal theory we outline is remarkably similar to ideal theory in rings. As with rings, matters of finite generation and Noetherian arise. In fact proof of the Hilbert basis theorem goes over to monoids. We shall only be concerned with commutative monoids and do not bother with the distinction between left, right and two-sided. Throughout this section $M$ is a commutative monoid. In fact all monoids which we discuss are commutative. Usually the law of composition in $M$ will be written multiplicatively and $e$ will stand for the identity element. There are many examples, starting with (A1.4).

DISCLAIMER: The lack of references for various results should NOT be interpreted as an indication that the results are first proved here. Rather it is a reflection of the author’s ignorance of the commutative monoid literature. One or two results are modeled after analogous results in commutative ring theory or elsewhere. In these cases the analogous results are mentioned.

Definition A1.1. A (possibly empty) subset $X$ of $M$ is an ideal if $MX \subset X$. An ideal is proper if it does not equal $M$. A subset $N$ of $M$ is a submonoid if $e \in N$ and $N \subset N$. An element $x \in M$ is called invertible if there is $y \in M$ where $xy = e$. $M^I$ denotes the set of invertible elements of $M$ and $M^I$ denotes the (possibly empty) set of all elements of $M$ which are not invertible.

Proposition A1.2. (a) The union and intersection of ideals is again an ideal.
(b) $M^0$ is an ideal in $M$. 

(c) The intersection of submonoids is again a submonoid.
(d) $M^I$ is a submonoid of $M$ and is the largest submonoid of $M$ which is a group.

Proof. Easy and left to the reader. □

The intersection of a finite number of non-empty ideals is non-empty because it contains an element which is the product of an element from each of the ideals being intersected. In example (A1.5), the intersection of all the non-empty ideals in the monoid is empty. In example (A1.6), the intersection of all the non-empty ideals in the monoid is non-empty.

**Chat A1.3.** Let $S$ be a subset of $M$. (A1.2,a) allows us to define the **ideal generated by S** as the intersection of all the ideals containing $S$. (A1.2,c) allows us to define the **submonoid generated by S** as the intersection of all submonoids containing $S$. This is the smallest ideal or submonoid containing $S$. If $S$ is empty, it is already an ideal. If $S$ is nonempty, the ideal generated by $S$ consists of all elements of $M$ which are the product of an element of $M$ by an element of $S$, i.e., $MS$. The submonoid generated by $S$ consists of all elements of $M$ which are monomials of elements of $S$. (A monomial of elements of $S$ is an element of the form $s_1s_2\cdots s_n$ for $n \in \mathbb{N}$ and $s_i \in S$. $e$ is considered to be a monomial of elements of $S$ where $n = 0$.) An ideal or submonoid is **principal** if there is a set consisting of one element which generates it. (So principal ideals are not empty.) This one element is called a **generator for the ideal or submonoid**. An ideal or submonoid is **finitely generated** if there is a finite set, possibly empty, which generates it. $m$ is a principal ideal of itself generated by $e$. $M$ may or may not be finitely generated as a submonoid of itself. When we speak about a monoid being principal or finitely generated and do not specify whether we mean as ideal or submonoid of itself, we mean as a submonoid of itself. This distinction comes out in the following examples.

**Example A1.4.** Commutative groups are commutative monoids. If $G$ is a commutative group, the only ideals in $G$ are the empty set and $G$ itself. (Groups are the fields of monoids.) Any element of $G$ generates the ideal $G$. Groups are not necessarily finitely generated.

**Example A1.5.** $\mathbb{N}$ under addition is a monoid. The non-empty ideals are subsets of the form $\{n, n + 1, n + 2, \ldots\}$. Hence, every non-empty ideal is principal and has a unique generator. The intersection of all the non-empty ideals is the empty ideal. $\mathbb{N}$ is principal (as a submonoid) with 1 the unique generator. (And principal as an ideal with 0 the unique generator.)

**Example A1.6.** $\mathbb{N} \cup \{\infty\}$ under addition is a monoid. The elements of $\mathbb{N}$ add as usual and for any $x \in \mathbb{N} \cup \{\infty\}$:

$$x + \infty = \infty = \infty + x$$

What are the non-empty ideals? $\{\infty\}$ is an ideal. The other non-empty ideals are subsets of the form $\{n, n + 1, n + 2, \ldots, \infty\}$. Hence, every non-empty ideal is principal.
and has a unique generator. The intersection of all the non-empty ideals is the non-empty ideal \( \{ \infty \} \). \( \mathbb{N} \cup \{ \infty \} \) is not principal (as a submonoid) but is generated by two elements \( \{ 1, \infty \} \).

**Example A1.7.** The additive group \( \mathbb{R} \) is a monoid. Let \( |\mathbb{R}| \) denote \( \{ r \in \mathbb{R} \mid r \geq 0 \} \). \( |\mathbb{R}| \) is a submonoid of \( \mathbb{R} \). What are the non-empty ideals in \( |\mathbb{R}| \)? If \( x \) lies in an ideal \( I \), then \( x + |\mathbb{R}| = [x, \infty) \subset I \). If \( c \) is the greatest lower bound of \( I \) then \( I = [c, \infty) \) or \( I = (c, \infty) \) depending on whether \( c \) lies in \( I \) or not. Thus, the non-empty ideals of \( |\mathbb{R}| \) come in two “flavors”: principal-with-a-unique-generator or not-finitely-generated. \( |\mathbb{R}| \) is not finitely generated (as a submonoid).

**Lemma A1.8.** The following conditions are equivalent:

(i) Every ascending sequence of ideals of \( M \) becomes constant. (By ascending sequence of ideals we mean ideals \( I_j \) with \( \cdots \subset I_{n-1} \subset I_n \subset I_{n+1} \subset \cdots \).

(ii) Every non-empty set of ideals of \( M \) has a maximal element.

(iii) For every set \( S \) in \( M \) there is a finite subset which generates the same ideal as \( S \).

(iv) Every ideal in \( M \) is finitely generated.

*Proof.* The easy (i) implies (ii) implies (iii) implies (iv) implies (i) proof is essentially the same as for modules over rings and is left to the reader. \( \square \)

**Definition A1.9.** \( M \) is called Noetherian if it satisfies the equivalent conditions of (A1.8).

**Theorem A1.10** (Hilbert Basis Theorem for Monoids). Suppose \( N \) is a Noetherian submonoid and \( S \) is a finite subset of a commutative monoid. The submonoid generated by \( N \cup S \) is a Noetherian submonoid. In particular a finitely generated monoid is Noetherian.

*COMMENT:* This is the “essence” of the proof on page 47 of [Kap70] of the Hilbert basis theorem for rings. It is too pretty too leave out.

*Proof.* By induction it suffices to consider the case where \( S \) consists of a single element \( s \). Let \( M \) denote the submonoid generated by \( N \cup S \). Clearly \( M \) is the union:

\[
N \cup Ns \cup Ns^2 \cup Ns^3 \cup \cdots
\]

Let \( X \) be a non-empty ideal in \( M \). Let \( N_0 \) denote \( N \cap X \). For \( 0 < n \in \mathbb{N} \) let \( N_n \) denote \( \{ a \in N \mid as^n \in X \} \). Each \( N_n \) is an ideal in \( N \) and \( N_0 \subset N_1 \subset N_2 \subset \cdots \). \( N \) being Noetherian implies this ascending sequence of ideals becomes constant, at say \( t \in \mathbb{N} \). We will show:

\[
X = N_0 \cup N_1 s \cup \cdots \cup N_t s^t \cup N_t s^{t+1} \cup N_t s^{t+2} \cup \cdots
\]

This will prove the theorem because if \( S_t \) is a finitely generating set of \( N_t \) as an ideal in \( N \) then \( S_0 \cup S_1 s \cup \cdots \cup S_t s^t \) is a finite generating set for \( X \) as an ideal in \( M \).
Say $x \in X$. By (1), $x \in N_i s^i$ for some $i$. If $i \leq t$, then $x \in N_i s^i$. If $i > t$ then $x = as^i$ and by definition $a \in N + i$. Since the ascending sequence of ideals became constant at $t$: $N_i = N_t$ so $x \in N_i s^i$. □

**Chat A1.11.** If $R$ is a commutative ring the monoid algebra of $M$ over $R$ is a free $R$-module with basis consisting of elements of $M$. Let $RM$ denote the monoid algebra.

For each $m \in M$ let $1 \cdot m$ denote the basis element of $RM$ corresponding to $m$. $RM$ has multiplication determined by: $(\lambda \cdot m_1)(\tau \cdot m_2) = \lambda \tau \cdot (m_1 m_2)$, where $\lambda, \tau \in R$ and $m_1, m_2 \in M$. $1 \cdot e$ is the unit of $RM$. Homogeneous ideals in $RM$ are the ideals which are spanned as an $R$-module by elements of the form $1 \cdot m$. Ideals in $M$ span homogeneous ideals in $RM$. (The empty ideal in $M$ spans the zero ideal in $RM$.) If two ideals of $M$ are distinct, the homogeneous ideals in $RM$ which they span are distinct. Thus if $RM$ is Noetherian so is $M$. On the other hand, even if $R$ is a field, $M$ may be Noetherian without $RM$ being Noetherian. For example, if $M$ is a group then the only ideals are $M$ itself and the empty ideal. Letting $M$ be an infinite direct product of copies of the integers gives an example where $M$ is Noetherian but $RM$ is not.

Just as (A1.10) is the monoid analog to the Hilbert basis theorem, the following result is the monoid analog to the fact that subalgebras of the polynomial ring in one variable over a field are finitely generated. This monoid result gives monoids to which (A1.10) applies.

**Proposition A1.12.** Submonoids of $\mathbb{N}$ are finitely generated.

**Proof.** Let $M$ be a submonoid of $\mathbb{N}$. If $M = \{0\}$, it is finitely generated. Say $M \neq \{0\}$. Let $m$ be the smallest non-zero element of $M$. There are $m$ equivalence classes in $\mathbb{Z}$ or $\mathbb{N}$ modulo $m$. For each of these equivalence classes, if there is an element of $M$ in the equivalence class, choose the smallest element of $M$ in the equivalence class. Let $SR$ be this set of Smallest Residues in $M$, modulo $m$. Suppose $x \in M$. By definition of $SR$, there is an element $g \in SR$ where: $x \mod m = g \mod m$ and $g \leq x$. Thus $x = g + m + \cdots + m$ for a suitable number of $m$’s. This shows that $M$ is finitely generated by $SR \cup \{m\}$. □

**Corollary A1.13** (to the proof of A1.12). If $M$ is a non-zero submonoid of $\mathbb{N}$ and $m$ is the smallest non-zero element of $M$, then $M$ is generated by $m$ or fewer elements.

**Proof.** The elements of $SR$ are distinct residues modulo $m$. Thus $SR$ has cardinality at most $m$. $0$ lies in $SR$ since it is the smallest residue in $M$ in the equivalence class of $0$. $M$ is generated by $(SR - \{0\}) \cup \{m\}$. □

**A1.14.** Submonoids of $\mathbb{N}$ are Noetherian.

**Proof.** (A1.10) and (A1.13). □

**Definition A1.15.** For $y, z \in M$, we say $y$ divides $z$, and write $y \mid z$, if there is $x \in M$ with $xy = z$ or equivalently $z$ lies in the principal ideal generated by $y$. 

Say $M$ is a Noetherian monoid and \((m_1, m_2, m_3, \ldots)\) is a sequence of elements of $M$ where $m_j|m_i$ for $i < j$. Then the principal ideals generated by the $m_i$’s form an ascending sequence of ideals. By the Noetherian property, this sequence of ideals must become constant. If the sequence of ideals becomes constant at $N$ it follows that for $i, j \geq N$: $m_i|m_j$ and $m_j|m_i$. With a little more work, we can get a remarkable result about divisibility of elements in any sequence of elements of $M$. It is the generalization of Dickson’s Lemma to Noetherian monoids:

**Theorem A1.16.** Let $M$ be a Noetherian commutative monoid.

(a) If $S$ is an infinite subset of $M$, there are distinct elements $s_1, s_2, s_3, \ldots \in S$ where $s_i|s_j$ for $i \leq j$.

(b) If $(m_1, m_2, m_3, \ldots)$ is a sequence of elements of $M$ where an infinite number of distinct elements occur, then there is a subsequence $(m_{e_1}, m_{e_2}, m_{e_3}, \ldots)$ consisting of distinct elements where $e_i \leq e_j$ and $m_{e_i}|m_{e_j}$ for $i \leq j$.

**COMMENT:** Although b implies a, the proof nicely breaks up into these parts. In several places we use ”−” for set-theoretic complement.

**Proof.** (a) Let $s_0 = e$ the identity of $M$ and $S_0 = S - \{e\}$. This begins an inductive procedure. Suppose we have constructed $s_0, s_1, \ldots, s_n \in S$ and subsets of $S$: $S_0, S_1, \ldots, S_n$ satisfying:

(i) $s_i \in S$ if $i \geq 1$

(ii) $S_i \supset S_j$ if $i \leq j$

(iii) $s_i \in S_{i-1} - S_i$ if $i \geq 1$

(iv) $s_i$ divides every element of $S_i$

(v) $S_i$ is an infinite set.

Let $I$ be the ideal generated by $S_n$. Since $M$ is Noetherian, $I$ is generated by a finite subset $F \subset S_n$. For each $f \in F$ let $S_f = \{s \in S_n \mid f \text{ divides } s\}$. $F$ generates $I$ implies that $S_n = \bigcup S_f$. Since there are a finite number of $S_f$’s, one of them must be infinite. Let $s_{n+1} = f$ where $S_f$ is infinite. Let $S_{n+1} = S_f - \{f\}$. This completes the induction.

The elements $s_1, s_2, s_3, \ldots$ lie in $S$ by part (i) and are distinct by part (iii). $s_i|s_j$ if $1 \leq i \leq j$ by parts (ii), (iii), and (iv). This proves part a.

(b) Let $S$ be the infinite set of distinct elements of $(m_1, m_2, m_3, \ldots)$. Let $s_1, s_2, s_3, \ldots \in S$ be as in part a and let $T_1 = \{s_{i+1}, s_{i+2}, \ldots\}$. Set $S_{d_1} = s_1$. $s_1$ equals some $m_{e_1}$ in the sequence $(m_1, m_2, m_3, \ldots)$. Although $s_2$ may occur before $m_{e_1}$, only a finite number $e_1 - 1$ of elements of $T_1$ can occur before $m_{e_1}$. Thus there is $s_{d_2} \in T_1$ which equals some $m_{e_2}$ in the sequence $(m_{e_1+1}, m_{e_1+2}, m_{e_1+3}, \ldots)$. Similarly, there is $s_{d_3} \in T_2$ which equals some $m_{e_3}$ in the sequence $(m_{e_2+1}, m_{e_2+2}, m_{e_2+3}, \ldots)$. This constructs a subsequence $(m_{e_1}, m_{e_2}, m_{e_3}, \ldots)$. By construction, $e_i < e_j$ for $i < j$. Also by the construction, $m_{e_i} = s_{d_i}$ and $d_i < d_j$ for $i < j$. This gives the required distinctness and divisibility.
Definition A1.17. \( M \) is a GUPI monoid – or simply GUPI – if whenever \( y \mid z \) and \( z \mid y \) it follows that \( y = z \).

(A1.20,c) shows that GUPI is the condition for “\( \mid \)” to give a partial order on \( M \). Since \( y \mid z \) if and only if \( z \) lies in the ideal generated by \( y \), being GUPI is equivalent to: principal ideals have unique generators. GUPI stands for: Generators are Unique for Principal Ideals. \( e \) divides all elements of \( M \) The invertible elements of \( M \) are those which divide \( e \). Thus:

\[ \text{A1.18. If } M \text{ is GUPI, } e \text{ is the only invertible element of } M. \text{ Hence, } M^0 \text{ is the set theoretical complement to } \{e\} \text{ in } M. \]

Examples (A1.5) and (A1.6) and (A1.7) are GUPI’s. Example (1.4) is not GUPI if the group consists of more than \( \{e\} \). The next example shows that: \( e \) being the only invertible element, does not imply that a monoid is GUPI.

\[ \text{A1.19 (A non GUPI example). Within } \mathbb{R} \times \mathbb{R} \text{ let } M \text{ be the multiplicative submonoid consisting of } (1,1) \text{ and elements of the form } (0,r) \text{ for } r \in \mathbb{R}. \text{ M is a monoid with identity } (1,1). \text{ M has no invertible elements other than the identity. } (0,r) \text{ and } (0,s) \text{ generate the same ideal in } M \text{ for non-zero } r,s \in \mathbb{R}. \]

The next result shows that submonoids and products of GUPI monoids are GUPI’s.

**Proposition A1.20.**

(a) A submonoid of a GUPI monoid is GUPI.

(b) The direct product of GUPI monoids is GUPI.

(c) For the monoid \( M \) set \( x \leq y \) when \( x \mid y \). This \( \leq \) makes \( M \) into a Partially Ordered Set (POSET) if and only if \( M \) is GUPI.

For the rest of the proposition suppose that \( M \) is Noetherian and GUPI. The “decreasing” in part d and the “\(<\)” in “\(m_i < m_j\)” in part e refer to the partial order in part c.

(d) If \((m_1,m_2,m_3,\ldots)\) is a decreasing sequence of elements of \( M \), then there is an integer \( N \) where \( m_i = m_j \) for \( i, j \geq N \).

(e) If \((m_1,m_2,m_3,\ldots)\) is a sequence of elements of \( M \) where an infinite number of distinct elements occur, then there is a subsequence \((m_{e_1},m_{e_2},m_{e_3},\ldots)\) consisting of distinct elements where \( e_i < e_j \) and \( m_{e_i} < m_{e_j} \) for \( i < j \).

**Proof.** Part a follows from the fact that if \( y \mid z \) in the submonoid then \( y \mid z \) in the over-

monoid. Part b follows from the fact that if \( y \mid z \) in the product monoid then each component of \( y \) divides the corresponding component of \( z \).

(c) Whether or not \( M \) is GUPI we have

\[ \text{(i) } z \leq z \quad \text{(ii) If } x \leq y \text{ and } y \leq z \text{ then } x \leq z. \]

Thus \( M \) is a POSET if and only if \( y \leq z \) and \( z \leq y \) imply that \( y = z \). This is just the GUPI property.

(d) Between (A1.15) and (A1.16) it is shown that there is an \( N \) where for \( i, j \geq N \): \( m_i \mid m_j \) and \( m_j \mid m_i \). Since \( M \) is GUPI: \( m_i = m_j \).
(e) This is just (A1,16,b) with “|” replaced by “<”.

Definition A1.21. $M$ is called cancelative if whenever $x, y, z \in M$ with $xz = yz$, it follow that $x = y$.

Proposition A1.22. $M$ is cancelative if and only if $M$ is a submonoid of a group.

Proof. (sketch) It is easy to verify that submonoids of groups are cancelative. If $M$ is cancelative, one constructs a group which contains $M$ in a fashion similar to constructing the field of fractions of an integral domain. The group $G$ consists of equivalence classes of pairs $(u, v)$ with $u, v \in M$. Two pairs $(u, v)$ and $(x, y)$ are equivalent when $uy = vx$. The product of equivalence classes is the equivalence class of the product of representatives and is independent of the representatives chosen. The product of the two pairs $(u, v)$ and $(x, y)$ is the pair $(ux, vy)$. The equivalence class of the pair $(e, e)$ is the identity of $G$. The inverse of the pair $(u, v)$ is the pair $(v, u)$. $M$ is considered a subset of $G$ by identifying each element $m \in M$ with the equivalence class of the pair $(m, 1)$. $M$ is a submonoid of $G$.

Theorem A1.23. If $M$ is GUPI, Noetherian and cancelative then $M$ is a finitely generated monoid. Any set which generates $M^I$ as an ideal also generates $M$ as a monoid.

Proof. $M^I$ is the set of elements of $M$ which are not invertible, (A1.1). Since $M$ is GUPI, $M = \{e\} \cup M^I$, (A1.18). By (A1.2,b), $M^I$ is an ideal in $M$ and since $M$ is Noetherian, $M^I$ is finitely generated. Thus it suffices to prove that any set which generates $M^I$ as an ideal also generates $M$ as a monoid. Say $F$ is a set which generates $M^I$ as an ideal. let $N$ be the submonoid of $M$ generated by $F$ and let $m \in M$. Set $m_0 = m$, $x_{-1} = m$ and do the following process:

If $m_t = e$, stop. Otherwise, $m_t \in M^I$ and since $F$ generates $M^I$, as an ideal, there is $x_i \in M$ and $f_i \in F$ with $m_t = x_i f_i$. Let $m_{t+1} = x_i$ and repeat the process.

If the process stops, it stops with $m_t = e$ for some $t$. If $t = 0$ then $m = m_0 = e \in N$. If $t > 0$ then $m = f_{t-1} f_{t-2} \cdots f_0$ which lies in $N$. So we must show that the process stops. Suppose not. Let $I_t$ be the ideal in $M$ generated by $m_t = x_i f_i$. Since $m_i = x_i f_i = m_{i+1} f_i$ it follows that $I_i \subset I_{i+1}$. Thus $I_0 \subset I_1 \subset \cdots$ is an ascending sequence of ideals in $M$ which must become constant by the Noetherian assumption. Say the ascending sequence of ideals becomes constant at $I_u = I_{u+1} = I_{u+2} = \cdots$. Since $I_j$ is the principal ideal generated by $m_j$ and $M$ is GUPI, it follows that $m_u = m_{u+1} = m_{u+2} = \cdots$. But then $m_u = m_{u+1} f_u$ becomes $m_u = m_u f_u$ and since $M$ is cancelative it follows that $f_u = e$. This is a contradiction because $f_u \in F \subset M^I$.

Appendix 2: Outline of Ordered Abelian Groups and Valuations

The idea of ordered abelian group is an abstraction of the real numbers. Once you have the so-called positive elements, you know the whole story.
Definition A2.1. An ordered abelian group is an abelian group $G$ together with a subset of elements $P$ called the positive elements of $G$. Assuming the product in $G$ is written multiplicatively and $e$ is the identity of $G$, $P$ must satisfy:

(i) $P$ is closed under product.

(ii) $e$ does not lie in $P$ and for any $g \in G$ with $g \neq e$, either $g$ or $g^{-1}$ lies in $P$.

Since $e$ does not lie in $P$ and $P$ is closed under product, only one of $g$ or $g^{-1}$ can lie in $P$. Thus:

A2.2. $G$ is the disjoint union: $G = P^{-1} \cup \{e\} \cup P$.

Definition A2.3. If $G$ is an ordered abelian group with positive elements $P$ then “$<$” is defined by: $g < h$ iff $g^{-1}h \in P$ for $g, h \in G$.

It is easy to check that “$<$” gives a total order on $G$.

Chat A2.4. Our notion of GUPI monoids in (A1.17) is closely related to ordered abelian groups. Let $NN$ be the submonoid of an ordered abelian group $G$ consisting of $\{e\} \cup P$. ($NN$ is the set of Non-negative elements of $G$.) $NN$ is GUPI because if $y|z$ and $z|y$ then there are $x, w \in NN$ with:

$$xy = z \text{ so } x = y^{-1}z \quad wz = y \text{ so } w = z^{-1}y$$

Thus $x = w^{-1}$ and both $w$ and $w^{-1}$ lie in $NN$. Since $P$ satisfies the positivity axiom (A2.1,ii), it follows that $w = e$ Hence $y = z$ and $NN$ is GUPI. $NN$ satisfies ii’: every element of $G$ or its inverse lies in $NN$. The notion of ordered abelian group can be posed in terms of an abelian group $G$ with a GUPI monoid $NN$ satisfying ii’. The set of positive elements consists of the elements of $NN$ other than $e$. The order on $G$ is given by: $g \leq h$ iff $g^{-1}h \in NN$. Notice that $NN$ has an order from (A1.20,c) and an order from being a subset of $G$. It is easy to check that these two orders coincide.

A2.5. Suppose $G$ is an ordered abelian group and $NN$ is the set of non-negative elements of $G$. By (A1.20,a), submonoids of $NN$ are GUPI.

Definition A2.6. A subring $V$ of a field $F$ is called a valuation ring of $F$ if every non-zero element of $F$ or its inverse lies in $V$. An integral domain is called a valuation ring if it is a valuation ring of its field of fractions.

A2.7 (Immediate Properties of Valuation Rings). Let $V$ be a valuation ring of the field $F$. (We use the notation introduced in the Illustrative Example in the introduction.

(a) $F$ is the field of fractions of $V$.

(b) $V^I$ is the unique maximal ideal of $V$.

(c) $f \notin V$ if and only if $f \neq 0$ and $f^{-1} \in V^I$.

(d) $F - V$, the set theoretic complement to $V$ in $F$, is closed under product.

(e) $(F - V)V^I \subset F - V$.

(f) Let $G$ be the multiplicative abelian group $F^I/V^I$ and $\pi : F^I \to G$ the natural map. Let $P$ denote $\pi(F - V)$. The pair $(G, P)$ is an ordered abelian group. $\pi(F - V^I) = NN$ the non-negative elements of $G$, (A2.4).
Proof. (a) Immediate from the definition of valuation ring of \( F \).

(b) The easy way to see this goes as follows: say \( x \) and \( y \) are non-zero, non-invertible elements of \( V \), i.e., \( x, y \in V^I \). By the definition of valuation ring either \( x/y \) or \( y/x \) lies in \( V \). Say \( x/y = v \in V \), so \( x = yv \). Then \( x + y = y(v + 1) \). This cannot be invertible without \( y \) being invertible. We have shown that the set of non-invertible elements of \( V \) is closed under “+”. It is easy to check that if the set of non-invertible elements of a commutative ring is closed under “+” then this set is the unique maximal ideal of the ring. (And conversely if a commutative ring has a unique maximal ideal, the set theoretic complement to the maximal ideal is the set of invertible elements in the ring.)

(c) If \( f^{-1} \in V^I \) then \((f^{-1})^{-1} \notin V \).

(d) If \( f, g \in F - V \) then \( f^{-1}, g^{-1} \in V^I \). Hence \( f^{-1}g^{-1} \in V^I \). Thus \( fg (f^{-1}g^{-1})^{-1} \in F - V \).

(e) This is proved similarly to part d.

(f) \( P \) is closed under product by part d. If \( \pi f \) is the identity of \( G \) then \( f \in V^I \). Thus \( P \) does not contain the identity of \( G \). Any element of \( G \) which is not the identity equals \( \pi f \) where \( f \notin V^I \). If \( f \notin V \) then \( \pi f \in P \). If \( f \in V \) then \( f \in V^I \); hence, \( f^{-1} \notin V \) and \( \pi f^{-1} \in P \). \( \square \)

A2.8. The ordered abelian group \( G \) is the valuation group of the valuation ring. \( \pi \) is the valuation. For \( 0 \neq f_1, f_2 \in F : \pi f_1 \leq \pi f_2 \) if and only if \( f_1/f_2 \in V \). A further breakdown is given by: \( \pi f_1 = \pi f_2 \) if and only if \( f_1/f_2 \in V^I \) and \( \pi f_1 < \pi f_2 \) if and only if \( f_1/f_2 \in V^I \).

Valuation rings need not be Noetherian. The standard result along this line is that a valuation ring, \( V \), is Noetherian if and only if the valuation group is isomorphic to \( \mathbb{Z} \). If so, \( V^I \) is generated by a single element, \( v \), and the only ideals in \( V \) are those which are generated by powers of \( v \). Such valuations are the so-called discrete valuation rings. An ordered abelian group is isomorphic to \( \mathbb{Z} \) if and only if its monoid of non-negative elements is isomorphic to \( \mathbb{N} \). (The isomorphism carries the monoid of non-negative elements to \( \mathbb{N} \) or \( -\mathbb{N} \). \( -\mathbb{N} \) is isomorphic to \( \mathbb{N} \).) Hence, if the valuation ring is Noetherian, the monoid of non-negative elements in the valuation group is \( \mathbb{N} \) which is a Noetherian monoid. There are many Noetherian monoids other than \( \mathbb{N} \) which occur as monoids of non-negative elements of valuation groups. (1.3) or (2.4) give an example where the valuation group is isomorphic to the \( n \)-fold product of copies of \( \mathbb{Z} \) and the monoid of non-negative elements is isomorphic to \( n \)-fold product of copies of \( \mathbb{N} \). By the above, when \( n > 1 \), the valuation ring is not a Noetherian ring, but the monoid of non-negative elements in the valuation group is a Noetherian monoid.
References

[Buc65] Bruno Buchberger. An algorithm for finding a basis for the residue class ring of a zero-
dimensional polynomial ideal, Dissertation. Universitaet Innsbruck, Institut fuer Mathe-
matik, 1965.

[Buc70] Bruno Buchberger. An algorithmic criterion for the solvability of algebraic systems of equa-

[Buc76] Bruno Buchberger. A theoretical basis for the reduction of polynomials to canonical forms.

[Buc84] Bruno Buchberger. A critical-pair/completion algorithm for finitely generated ideals in
rings, Decisive Problems and Complexity. (Proc. of the Symposium “Rekursive Kombi-
Springer Lecture Notes in Computer Science, 1984.

[Buc85] Bruno Buchberger. Groebner bases: an algorithmic method in polynomial ideal theory, Mul-


[Rob85] Lorenzo Robbiano. Term Orderings on the Polynomial Ring. Lecture Notes in Computer


[Swe] Moss Sweedler. Working Title: Ideal bases for algebras with monoidal filtration. in prepa-
ration.

Department of Mathematics, Cornell University, Ithaca, NY 14853