Strong Gröbner bases for polynomials over a principal ideal ring *

Graham H. Norton, Dept. Mathematics, Univ. of Queensland, Brisbane

Ana Sălăgean, Dept. Mathematics, Nottingham Trent Univ., Nottingham, U.K.

August 9, 2001

Abstract

Gröbner bases have been generalised to polynomials over a commutative ring A in several ways. Here we focus on strong Gröbner bases, also known as D-bases. Several authors have shown that strong Gröbner bases can be effectively constructed over a principal ideal domain. We show that this extends to any principal ideal ring: we characterise Gröbner bases and strong Gröbner bases when A is a principal ideal ring. We also give algorithms for computing Gröbner bases and strong Gröbner bases which generalise known algorithms to principal ideal rings. In particular, we give an algorithm for computing a strong Gröbner basis over a finite-chain ring, for example a Galois ring.

Subject Classification: 13F10, 13M10, 13P10.

1 Introduction

The notion of a Gröbner basis, introduced by Buchberger for ideals of polynomials when the coefficient ring A is a field, has been generalised to the case when A is a principal ideal domain (for an overview and references see [2, Chapter 10 and Appendix]) and to a Noetherian ring (see [1, Chapter 4]). We consider two possible generalisations, which we will call Gröbner bases and strong Gröbner bases as in [1]. As the names suggest, strong Gröbner bases are Gröbner bases but not conversely. In fact over certain rings, there are ideals which have a Gröbner basis but do not have a (finite) strong Gröbner basis (see [1, Example 4.5.7]). We show that strong Gröbner bases always exist for ideals of polynomial rings over any principal ideal ring and give algorithms to construct them. In view of previous work (see [1, 2] and the works cited there), we concentrate on rings with zero-divisors.

We begin by giving structure theorems for principal ideal rings and collecting typical examples. In Section 3 we recall the definitions of (strong) reduction and (strong) Gröbner bases over a commutative ring, following [1]. We show that when A is a finite-chain ring, i.e. a ring with finitely many ideals which are linearly ordered by inclusion, the notions of Gröbner basis and strong Gröbner basis coincide. Strong Gröbner bases consisting of a single polynomial are characterised in Subsection 3.3.

As a first step towards characterising strong Gröbner bases over a principal ideal ring, we see in Section 4 that the characterisation of Gröbner bases over Noetherian rings using syzygies (see [1,

*Research supported by the U.K. Engineering and Physical Sciences Research Council under Grant L07680, while the authors were with the Algebraic Coding Research Group, Centre for Communications Research, University of Bristol, U.K.

Theorem 4.2.3]) can be simplified for the particular case of a principal ideal ring: we give an explicit finite set of generators for the syzygy module in this case. The main problem encountered over a ring with zero-divisors is that multiplying a polynomial by a ring element may annihilate the leading term. We characterise Gröbner bases using classical S-polynomials and certain 'A-polynomials', see Theorem 4.10.

Theorem 5.10 characterises a strong Gröbner basis G as a Gröbner basis for which all G-polynomials (the latter being defined as in [2]) are 'strongly reducible' wrt. G. Based on these characterisations, Section 6 develops algorithms for computing strong Gröbner bases when A is a computable principal ideal ring, and includes proofs of correctness and termination. When A is a field or a principal ideal domain, our characterisations and algorithms reduce to the known ones. Finally, Section 7 recalls the notion of minimal strong Gröbner basis and gives several characterisations and properties of them over a principal ideal ring.

An outline and some applications of these results were presented at the Workshop on Coding and Cryptography, Paris, 2001, [9]. Allan Steel has implemented a strong Gröbner basis algorithm in Version 2.8 of Magma [3] using Corollary 5.13 below, generalising Faugère's algorithm [5] to Galois rings.

2 Principal Ideal Rings

We recall the structure of principal ideal rings and give some examples.

2.1 Commutative rings

Throughout, A will denote an arbitrary commutative ring with $1 \neq 0$. We denote by $\langle a_1, \ldots, a_k \rangle_A$ the ideal of A generated by $a_1, \ldots, a_k \in A$, and $\subset$ denotes strict inclusion. Let $A = \prod_{i=1}^{m} A_i$ be a product of commutative rings and denote by $\pi_i : A \to A_i$ the canonical projections. For any $a \in A$ we will write $a = (a_1, \ldots, a_m)$, where $a_i = \pi_i(a)$. Let $\mathbf{e}_i \in A$ be 1 in the i-th component and 0's elsewhere. An element $a \in A$ is a unit if and only if each $\pi_i(a)$ is a unit in A_i and a is a zero-divisor if and only if for some j, $\pi_j(a)$ is a zero-divisor in A_j. It is well-known that any ideal I of A has the form $I_1 \times \cdots \times I_m$ where I_i an ideal in A_i and that $\mathrm{Ann}(a) = \mathrm{Ann}(\pi_1(a)) \times \cdots \times \mathrm{Ann}(\pi_m(a))$ where each $\mathrm{Ann}(\pi_i(a))$ is computed in A_i.

2.2 The structure of principal ideal rings

Throughout the paper, we denote by R a (commutative) principal ideal ring. It is well-known and easy to see that a quotient of a principal ideal ring and a finite product of principal ideal rings are principal. Before recalling a general structure theorem for principal ideal rings, it is useful to recall that a *chain ring* is a ring whose ideals are linearly ordered by inclusion; see [6].

Definition 2.1 (Finite-chain ring) *A* finite-chain ring *is a chain ring with finitely many ideals.*

We will need the following properties of a finite-chain ring:

Proposition 2.2 *Let A be a finite-chain ring. Then:*

(i) A is a principal ideal ring

(ii) A is a local ring with maximal ideal M say

(iii) the elements of M are nilpotent and the elements of $A \setminus M$ are units.

Let γ be a fixed generator of M and ν the nilpotency index of γ i.e. the smallest positive integer for which $\gamma^\nu = 0$. Then

(iv) the distinct proper ideals of A are $\langle\gamma^i\rangle_A$, $i = 1, \ldots, \nu - 1$

(v) for any element $a \in A \setminus \{0\}$ there is a unique i and a unit $u \in A$ such that $a = u\gamma^i$ where $0 \leq i \leq \nu - 1$ and u is unique modulo $\gamma^{\nu-i}$

(vi) $\mathrm{Ann}(\gamma^i) = \langle\gamma^{\nu-i}\rangle_A$.

PROOF. (i) If I is a non-zero ideal of A, then $I = \cup_{a\in I}\langle a\rangle_A$. Since A is a finite-chain ring, this is a finite union of ascending ideals. Thus I is the largest ideal of the union and A is principal. For parts (ii)-(v) see [10, Vol.1, Ch. 4, Section 15]. □

Henceforth, γ and ν will always be used in the sense of the previous proposition. A finite-chain ring is a field if and only if $\nu = 1$. A principal ideal domain is not a finite-chain ring unless it is a field. In [10, Vol.1, Ch. 4, Section 15], a principal ideal ring is called special if it has a unique proper nilpotent prime ideal. It is also shown *loc.cit* that a ring is a special principal ideal ring if and only if it is a finite-chain ring (as defined above).

The following are examples of finite-chain rings: $\mathbb{Z}_{p^k}$, the integers modulo p^k with p a prime and $k \in \mathbb{Z}$, $k \geq 1$; Galois rings $GR(p^k, n) = \mathbb{Z}_{p^k}[x]/\langle f\rangle$ where $\langle f\rangle$ is the ideal generated by a monic irreducible polynomial $f \in \mathbb{Z}_{p^k}[x]$ of degree n whose image modulo p is irreducible in $GF(p^n)[x]$ (here γ and ν can be taken to be p and k, respectively); finite rings which are chain rings (these are completely characterised as certain homomorphic images of $GR(p^k, n)[x]$, see [7, Theorem XVII.5]; of course, not all finite-chain rings are finite); $K[x]/\langle f^k\rangle$ with K a field, f an irreducible polynomial and $k \in \mathbb{Z}$, $k \geq 1$ (here γ and ν can be taken to be f and k, respectively); $D/\langle a^k\rangle_D$ with D a principal ideal domain, a an irreducible element and $k \geq 1$.

Of course, $\mathbb{Z}_m$ is a finite-chain ring if and only if m is a power of a prime. The following theorem describes the structure of principal ideal rings.

Theorem 2.3 *([10, Vol.1, Ch. 4, Section 15, Theorem 33]) Any principal ideal ring is isomorphic to a finite product of principal ideal domains and finite-chain rings.*

Besides the usual examples of principal ideal rings, we note that $R[x]/\langle f\rangle$ is a principal ideal ring if R is a finite-chain ring and $f \bmod \gamma$ is square-free (for a proof see [4, Corollary to Theorem 6] or [8, Corollary 3.20, Remark 3.26]).

3 Strong Gröbner Bases

3.1 Polynomials and reduction

The monoid of terms in $x_1, \ldots, x_n$ is denoted by T. We fix an admissible order '$<$' on T. If $f = \sum_{t\in T} f_t t \in A[x_1, \ldots, x_n] \setminus \{0\}$ and $v = \max\{t \in T \ : \ f_t \neq 0\}$ then v is called the *leading term*, f_v the *leading coefficient* and $f_v v$ the *leading monomial* of f, denoted $\mathrm{lt}(f), \mathrm{lc}(f)$ and $\mathrm{lm}(f)$ respectively. If $S \subset A[x_1, \ldots, x_n] \setminus \{0\}$, we write $\mathrm{lm}(S)$ for $\{\mathrm{lm}(g) \ : \ g \in S\}$, and similarly for $\mathrm{lc}(S)$ and $\mathrm{lt}(S)$. Note that the terminology 'leading term', 'leading monomial' etc. differs from [1].

When A is a ring rather than a field, reduction of polynomials in $A[x_1, \ldots, x_n]$ can be generalised in several ways: reduction and strong reduction as defined in [1, Definition 4.1.1 and p. 252] are two such possibilities. We recall their definitions:

Definition 3.1 (Reduction, Strong reduction) *Let $f \in A[x_1, \ldots, x_n] \setminus \{0\}$ and let G be a finite, non-empty subset of $A[x_1, \ldots, x_n] \setminus \{0\}$.*

(i) We say that f reduces to *h* wrt. *G* in one step *(and that f is* reducible wrt. *G) if $h = f - \sum_{i=1}^{k} c_i t_i g_i$, where $c_i \in R$, $t_i \in T$, $g_i \in G$, $\mathrm{lm}(f) = \sum_{i=1}^{k} c_i t_i \mathrm{lm}(g_i)$ and $c_i \neq 0$ implies $c_i \mathrm{lc}(g_i) \neq 0$ and $\mathrm{lt}(f) = t_i \mathrm{lt}(g_i)$. We write this as $f \to_G h$.*

(ii) We say that f strongly reduces to h wrt. G in one step *(and that* f *is* strongly reducible wrt. G*) if* $h = f - mg$ *where* $g \in G$ *and* m *is a monomial such that* $\mathrm{lm}(f) = m\,\mathrm{lm}(g)$*. We write this as* $f \twoheadrightarrow_G h$*.*

(iii) The reflexive and transitive closures of the relations $\to_G$ *and* $\twoheadrightarrow_G$ *are denoted* $\to_G^*$ *and* $\twoheadrightarrow_G^*$ *respectively. When* $f \to_G^* h$ *we say that* f reduces to h wrt. G*. If, moreover,* h *is not reducible wrt.* G *then we say that* h *is a remainder of* f *wrt.* G *(by reduction) and we denote the set of all such remainders by* $\mathrm{Rem}(f, G)$*. Similarly for strong reduction. The set of remainders of* f *wrt.* G *(by strong reduction) is denoted by* $\mathrm{SRem}(f, G)$*. We adopt the convention that* $0 \to_G^* 0$*,* $0 \twoheadrightarrow_G^* 0$ *and that* $\mathrm{Rem}(0, G) = \mathrm{SRem}(0, G) = \{0\}$*.*

Note that if f reduces or strongly reduces to h then $\mathrm{lt}(f) > \mathrm{lt}(h)$. So for any polynomial f, $\mathrm{Rem}(f, G)$ and $\mathrm{SRem}(f, G)$ are non-empty. Note that we can have $f \twoheadrightarrow_G^* h_1$ and $f \twoheadrightarrow_G^* h_2$ for distinct h_1, h_2 even if $g \in G$ is fixed. For example, let $f = 4x^2 + 1, G = \{g\} = \{2x + y\}$ in $\mathbb{Z}_6[x, y]$. Then $f \twoheadrightarrow_G^* f - 2xg = 4xy + 1$ and $f \twoheadrightarrow_G^* f - 5xg = xy + 1$.

Clearly if $f \twoheadrightarrow_G^* h$, then $f \to_G^* h$. The converse is in general false: for example in $\mathbb{Z}[x, y]$ with $x > y$, $f = x + 2$ is reducible but not strongly reducible wrt. $G = \{2x + y, 3x + 1\}$. For finite-chain rings however we do have equivalence:

Proposition 3.2 *Let* R *be a finite-chain ring, let* $G \subset R[x_1, \ldots, x_n] \setminus \{0\}$ *be a finite set and* $f, h \in R[x_1, \ldots, x_n]$*. Then* f *is reducible wrt.* G *if and only if* f *is strongly reducible wrt.* G*.*

Proof. Let f be reducible wrt. G as in Definition 3.1. Proposition 2.2 implies that there is a j such that $\mathrm{lc}(g_j) \,|\, \mathrm{lc}(g_i)$ for $1 \le i \le k$. Then $\mathrm{lm}(g_j) \,|\, \mathrm{lm}(f)$ i.e. f is strongly reducible wrt. G. □

See also Corollary 5.9(iv) below.

Remark 3.3 *Strong reduction is called D-reduction in [2, Definition 10.1] when* A *is a principal ideal domain. Strong reduction is computationally more efficient than reduction. When* A *is Noetherian, strong reduction is in general not sufficient for computing Gröbner bases and reduction needs to be used. It will turn out that in the case when* A *is a principal ideal ring we can always avoid reduction and use only strong reduction to compute a 'strong Gröbner basis.'*

We denote the ideal generated by a set $F \subseteq A[x_1, \ldots, x_n]$ by $\langle F \rangle$ and write $\langle f_1, \ldots, f_k \rangle$ for $\langle \{f_1, \ldots, f_k\} \rangle$. Next we generalise the notions of standard representation and t-representation of [2, p.218-219] to polynomials over a ring.

Definition 3.4 (Standard representation) *Let* $t \in T$ *and* $0 \notin G \subset A[x_1, \ldots, x_n]$*. We define*

$$\mathrm{Rep}_{<t}(G) = \left\{ \sum_{i=1}^{k} c_i t_i g_i \;:\; g_i \in G, c_i \in A \setminus \{0\}, t_i \in T, \text{ and } t_i\,\mathrm{lt}(g_i) < t \text{ for } i = 1, \ldots, k \right\}$$

and similarly for $\mathrm{Rep}_{\le t}(G)$*. If* $f \in \mathrm{Rep}_{\le \mathrm{lt}(f)}(G)$ *we say that* f *has a* standard representation wrt. G*. We write* $\mathrm{Std}(G)$ *for the polynomials which have a standard representation w.r.t* G*.*

Note that in the preceding definition the $g_i \in G$ need not be distinct. One can easily check that if $f \to_G^* h$ or $f \twoheadrightarrow_G^* h$ then $f - h \in \mathrm{Std}(G)$. It is also clear that $\mathrm{Std}(G) \subseteq \langle G \rangle$. We easily have:

Lemma 3.5

(i) If $t_1 < t_2$ *then* $\mathrm{Rep}_{\le t_1}(G) \subseteq \mathrm{Rep}_{<t_2}(G)$*.*

(ii) If $f \in \mathrm{Rep}_{<t_1}(G)$ *then there is* $t_2 < t_1$ *such that* $f \in \mathrm{Rep}_{\le t_2}(G)$*.*

(iii) If $f \in \mathrm{Rep}_{\le t}(G)$ *then* $rt_1 f \in \mathrm{Rep}_{\le t_1 t}(G)$ *for any* $r \in A$ *and* $t_1 \in T$*.*

3.2 Definitions of Gröbner Bases and Strong Gröbner Bases

The following two theorems generalise some of the well-known equivalent definitions of Gröbner bases over fields.

Theorem 3.6 *([1, Theorem 4.1.12]) Let I be a non-zero ideal of $A[x_1, \ldots, x_n]$ and let G be a finite subset of $I \setminus \{0\}$. The following assertions are equivalent:*

(i) $\langle \mathrm{lm}(G) \rangle = \langle \mathrm{lm}(I \setminus \{0\}) \rangle$

(ii) $f \in I$ *if and only if* $f \to_G^* 0$

(iii) $I = \mathrm{Std}(G)$.

Theorem 3.7 *([1, Exercise 4.5.1]) Let I be a non-zero ideal of $A[x_1, \ldots, x_n]$ and let G be a finite subset of $I \setminus \{0\}$. The following assertions are equivalent:*

(i) any $f \in I$ is strongly reducible wrt. G

(ii) $f \in I$ *if and only if* $f \twoheadrightarrow_G^* 0$.

Note that when A is a field, Theorems 3.6 and 3.7 are equivalent, but in general the conditions of Theorem 3.7 are strictly stronger than those of Theorem 3.6.

Definition 3.8 (Gröbner basis, strong Gröbner basis) *([1, Definitions 4.1.13 and 4.5.6]) Let I be a non-zero ideal of $A[x_1, \ldots, x_n]$ and let G be a finite subset of $I \setminus \{0\}$. Then:*

(i) G is called a Gröbner basis for I if it satisfies any of the equivalent conditions of Theorem 3.6.

(ii) G is called a strong Gröbner basis for I if it satisfies any of the equivalent conditions of Theorem 3.7.

By Theorems 3.6 and 3.7, if G is a (strong) Gröbner basis for I then $I = \langle G \rangle$. We will often just say ' G is a (strong) Gröbner basis', meaning that G is a finite subset of $R[x_1, \ldots, x_n]$, $0 \notin G$ and G is a (strong) Gröbner basis for $\langle G \rangle$. (In [2, p. 462] strong Gröbner bases are called D-bases and remainders are called D-normal forms.)

Over a Noetherian ring, any non-zero ideal has a Gröbner basis, [1, Corollary 4.1.17]. It is clear that a strong Gröbner basis is a Gröbner basis, but the converse fails in general (see [1, Example 4.5.7]). We will show that when A is a principal ideal ring *any* non-zero ideal has a strong Gröbner basis. Proposition 3.2 yields:

Proposition 3.9 *Let R be a finite-chain ring. Then G is a Gröbner basis if and only if G is a strong Gröbner basis.*

3.3 Strong Gröbner bases of cardinality one

When $g \in A[x_1, \ldots, x_n]$ and A has zero-divisors, $\{g\}$ is not necessarily a Gröbner basis:

Example 3.10 *Let $g = px^2 + x + 1 \in \mathbb{Z}_{p^2}[x]$. Since $\mathrm{lt}(pg) < \mathrm{lt}(g)$, $\{g\}$ is not a Gröbner basis. Likewise $\{2x^2 + 3x + 1\} \subset \mathbb{Z}_6[x]$ is not a Gröbner basis.*

We characterise the polynomials g for which $\{g\}$ is a (strong) Gröbner basis.

Theorem 3.11 *Let $g \in A[x_1, \ldots, x_n] \setminus \{0\}$. The following assertions are equivalent:*

(i) $\{g\}$ is a strong Gröbner basis

(ii) $\{g\}$ is a Gröbner basis

(iii) $zg = 0$ *for all* $z \in \mathrm{Ann}(\mathrm{lc}(g))$.

PROOF. (ii) $\Rightarrow$ (iii) Assume $\{g\}$ is a Gröbner basis and let $z \in \mathrm{Ann}(\mathrm{lc}(g))$. If $zg \neq 0$ then $\mathrm{lt}(zg) < \mathrm{lt}(g)$. Since $\{g\}$ is a Gröbner basis, $\mathrm{lt}(g) | \mathrm{lt}(zg)$ and so $\mathrm{lt}(g) \leq \mathrm{lt}(zg)$, for a contradiction.

(iii) $\Rightarrow$ (i) Assume that $zg = 0$ for all $z \in \mathrm{Ann}(\mathrm{lc}(g))$. Let $f \in \langle g \rangle \setminus \{0\}$ and let $h \in A[x_1, \ldots, x_n]$ be such that $f = gh$ and $\mathrm{lt}(h)$ is minimal among all polynomials with this property. If $\mathrm{lc}(g)\,\mathrm{lc}(h) = 0$, then $\mathrm{lc}(h)g = 0$. Putting $h_1 = h - \mathrm{lm}(h)$, we have $0 \neq gh = g\,\mathrm{lm}(h) + gh_1 = gh_1$ and $\mathrm{lt}(h_1) < \mathrm{lt}(h)$ contradicting the minimality of $\mathrm{lt}(h)$. Hence $\mathrm{lc}(g)\,\mathrm{lc}(h) \neq 0$ so $\mathrm{lm}(gh) = \mathrm{lm}(g)\,\mathrm{lm}(h)$ i.e. $\mathrm{lm}(g) | \mathrm{lm}(f)$, as required. □

Thus if A is a domain, any $\{f\} \subset A[x_1, \ldots, x_n] \setminus \{0\}$ is a strong Gröbner basis. Also, if R is a finite-chain ring and $g \in R[x_1, \ldots, x_n]$ is monic, then for any $r \in R \setminus \{0\}$, $\{rg\}$ is a strong Gröbner basis. More generally, we have the following easy consequence of Theorem 3.11.

Corollary 3.12 *Let $a \in A \setminus \{0\}$ and $g \in A[x_1, \ldots, x_n] \setminus \{0\}$. If $\mathrm{lc}(g)$ is not a zero-divisor, then $\{ag\}$ is a strong Gröbner basis.*

See Proposition 4.2 for a converse to Corollary 3.12.

4 Characterisation of Gröbner bases over R

Buchberger's characterisation of a Gröbner basis over a field was generalised to the case of a Noetherian ring by generalising S-polynomials to certain polynomial combinations obtained from the generators of the syzygy modules of leading monomials (see [1, Theorem 4.2.3]). We simplify this characterisation for the case of R, a principal ideal ring, as a first step towards characterising strong Gröbner bases over R. We begin with some additional results on divisibility in R.

4.1 Divisibility in a principal ideal ring

If $a, b \in R$ are such that $b|a$, then $a = bc$ does not of course specify c uniquely, but the following proposition provides a 'natural choice' for c:

Proposition 4.1 *(i) Let $a, b \in R$ be such that $b|a$. There is an element $c \in R$, unique up to associates, such that $a = bc$ and $\langle c \rangle_R = (\langle a \rangle_R : \langle b \rangle_R)$. In particular, if $\langle a \rangle_R = \langle b \rangle_R$ then there is a unit $u \in R$ such that $a = ub$.*

(ii) Any element $r \in R$ can be written as $r = bc$ where b is not a zero-divisor and c such that $\mathrm{Ann}(\mathrm{Ann}(c)) = \langle c \rangle_R$. The elements b and c are unique up to associates.

PROOF. (i) The result is trivial if R is a domain. Assume that R is a finite-chain ring but not a field and let $a = u\gamma^i$, $b = v\gamma^j$ with u and v units. Since $b|a$, we have $j \leq i$. Put $c = uv^{-1}\gamma^{i-j}$. Obviously $(\langle a \rangle_R : \langle b \rangle_R) = \langle \gamma^{i-j} \rangle_R = \langle c \rangle_R$. For the general case, decompose R using Theorem 2.3. Then use the fact that the operations are component-wise and that the assertion holds in each component.

(ii) By Theorem 2.3, R is isomorphic to $\prod_{i=1}^{m} R_i$ with R_i either a domain or a finite-chain ring. For $r \in R$, define $b, c \in R$ by $\pi_i(b) = \pi_i(r)$ if $\pi_i(r)$ is not a zero-divisor and $\pi_i(b) = 1$ otherwise and $\pi_i(c) = \pi_i(r)$ if $\pi_i(r)$ is a zero-divisor and $\pi_i(c) = 1$ otherwise, where $i = 1, \ldots, m$. The rest of the proof is a simple exercise. □

An application of the foregoing is a converse to Corollary 3.12:

Proposition 4.2 *Let $g \in R[x_1, \ldots, x_n] \setminus \{0\}$ and let $\{g\}$ be a strong Gröbner basis. Then $g = cg'$ for some $c \in R$, $g' \in R[x_1, \ldots, x_n]$ for which $\mathrm{lc}(g')$ is not a zero-divisor.*

PROOF. Let $\{g\}$ be a strong Gröbner basis. By Proposition 4.1(ii), $\mathrm{lc}(g) = bc$ where $\mathrm{Ann}(\mathrm{Ann}(c)) = \langle c\rangle_R$, b is not a zero divisor and $\mathrm{Ann}(\mathrm{lc}(g)) = \mathrm{Ann}(c)$. It suffices to prove that for any $t \in T$, $g_t \neq 0$ implies $c|g_t$. Let z generate $\mathrm{Ann}(\mathrm{lc}(g))$. Then, by Theorem 3.11, $zg = 0$ i.e. $zg_t = 0$ for all $t \in T$ i.e. $g_t \in \mathrm{Ann}(z) = \mathrm{Ann}(\mathrm{Ann}(c)) = \langle c\rangle_R$. □

As usual, for $k \geq 1$ and $r_1, \ldots, r_k \in R \setminus \{0\}$, we say that $r \in R \setminus \{0\}$ is a *greatest common divisor* of $r_1, \ldots, r_k$ if $r|r_i$ for all $i = 1, \ldots, k$ and for any $r' \in R$ with the property that $r'|r_i$ for $i = 1, \ldots, k$, we have $r'|r$. A *least common multiple* of $r_1, \ldots, r_k$ is similarly defined. We denote by $\gcd(r_1, \ldots, r_k)$ and by $\mathrm{lcm}(r_1, \ldots, r_k)$ the set of greatest common divisors and the set of least common multiples of $r_1, \ldots, r_k$, respectively. If $S = \{r_1, \ldots, r_k\}$ we also write $\gcd(S)$ and $\mathrm{lcm}(S)$ for $\gcd(r_1, \ldots, r_k)$ and $\mathrm{lcm}(r_1, \ldots, r_k)$, respectively. The following result is straightforward:

Lemma 4.3 *Let $k \geq 2$ and $r, r_1, \ldots, r_k \in R$. Then*

(i) $r \in \gcd(r_1, \ldots, r_k)$ if and only if $\langle r\rangle_R = \langle r_1, \ldots, r_k\rangle_R$

(ii) $r \in \mathrm{lcm}(r_1, \ldots, r_k)$ if and only if $\langle r\rangle_R = \langle r_1\rangle_R \cap \ldots \cap \langle r_k\rangle_R$

(iii) Any two greatest common divisors of $r_1, \ldots, r_k$ are associate. Likewise for any two least common multiples of $r_1, \ldots, r_k$.

Note that we can have $0 \in \mathrm{lcm}(r_1, \ldots, r_k)$ for $r_1, \ldots, r_k \in R \setminus \{0\}$, in which case $\mathrm{lcm}(r_1, \ldots, r_k) = \{0\}$ and $r_1 \cdots r_k = 0$.

4.2 Syzygies over a principal ideal ring

Syzygies of elements of R will play an important role in computing strong Gröbner bases. We generalise some of the results presented in [1, Section 4.5] from principal ideal domains to principal ideal rings.

Definition 4.4 *Let $k \geq 1$ and let $(r_1, \ldots, r_k) \in R^k$. The set of syzygies of $(r_1, \ldots, r_k)$ is*

$$\mathrm{Syz}(r_1, \ldots, r_k) = \{(c_1, \ldots, c_k) \in R^k \mid \sum_{i=1}^{k} c_i r_i = 0\}.$$

It is trivial that $\mathrm{Syz}(r_1, \ldots, r_k)$ is a finitely generated submodule of R^k, but we are interested in finding explicit generators. We first need the following lemma:

Lemma 4.5 *(cf. [1, Lemma 4.5.2]) If $r, r_1, \ldots, r_k \in R$, $(\langle r_1, \ldots, r_k\rangle_R : r) = \sum_{j=1}^{k} (\langle r_j\rangle_R : r)$.*

PROOF. If R is a principal ideal domain, the assertion is proved in [1, Lemma 4.5.2]. If R is a finite-chain ring, write $r = u\gamma^l$ and $r_j = u_j\gamma^{i_j}$, where u, u_j are units and $l, i_j \in \{0, \ldots, \nu - 1\}$ and $j = 1, \ldots, k$. Then:

$$(\langle r_1, \ldots, r_k\rangle_R : r) = (\langle \gamma^{\min\{i_1, \ldots, i_k\}}\rangle_R : \gamma^l) = \langle \gamma^{\max\{0, \min\{i_1, \ldots, i_k\} - l\}}\rangle_R,$$

$$\sum_{j=1}^{k} (\langle r_j\rangle_R : r) = \sum_{j=1}^{k} \langle \gamma^{\max\{0, i_j - l\}}\rangle_R = \langle \gamma^{\min\{\max\{0, i_1 - l\}, \ldots, \max\{0, i_k - l\}\}}\rangle_R$$

and $\max\{0, \min\{i_1, \ldots, i_k\} - l\} = \min\{\max\{0, i_1 - l\}, \ldots, \max\{0, i_k - l\}\}$ is a simple exercise.

If $R = \prod_{i=1}^m R_i$ with each R_i a principal ideal domain or finite-chain ring, then using the fact that the theorem holds in each R_i, we have:

$$\begin{aligned}\sum_{j=1}^k (\langle r_j\rangle_R : r) &= \sum_{j=1}^k \prod_{i=1}^m (\langle \pi_i(r_j)\rangle_{R_i} : \pi_i(r)) = \prod_{i=1}^m \sum_{j=1}^k (\langle \pi_i(r_j)\rangle_{R_i} : \pi_i(r)) \\ &= \prod_{i=1}^m \left(\sum_{j=1}^k \langle \pi_i(r_j)\rangle_{R_i} : \pi_i(r) \right) = \left(\prod_{i=1}^m \sum_{j=1}^k \langle \pi_i(r_j)\rangle_{R_i} : \prod_{i=1}^m \langle \pi_i(r)\rangle_{R_i} \right) \\ &= \left(\sum_{j=1}^k \langle r_j\rangle_R : r \right) = (\langle r_1, \ldots, r_k\rangle_R : r).\end{aligned}$$

The result for an arbitrary principal ideal ring now follows easily from Theorem 2.3. □

Theorem 4.6 *(cf. [1, Proposition 4.5.3] Let $(r_1, \ldots, r_k) \in R^k$. For each i, $1 \le i \le k$, let $a_i \in R$ be such that $\langle a_i\rangle_R = \mathrm{Ann}(r_i)$. For any pair i, j with $1 \le i < j \le k$ let $r_{i,j} \in \mathrm{lcm}(r_i, r_j)$. If $r_{i,j} \neq 0$, let $b_{i,j}, b'_{i,j} \in R$ be such that $r_i b_{i,j} = r_j b'_{i,j} = r_{i,j}$. Then*

$$S = \{a_i \mathbf{e}_i \ : \ 1 \le i \le k\} \cup \{b_{i,j}\mathbf{e}_i - b'_{i,j}\mathbf{e}_j \ : \ 1 \le i < j \le k, \mathrm{lcm}(r_i, r_j) \neq \{0\}\}$$

generates $\mathrm{Syz}(r_1, \ldots, r_k)$.

Proof. It is easy to check that $S \subset \mathrm{Syz}(r_1, \ldots, r_k)$. Now let $c = (c_1, \ldots, c_k) \in \mathrm{Syz}(r_1, \ldots, r_k)$. We have to prove that c can be written as a linear combination of the elements of S. We induct on the number l of non-zero components of c.

For $l = 1$, $c = c_i \mathbf{e}_i$ for some i. We have $c_i r_i = 0$, so $c_i \in \mathrm{Ann}(r_i) = \langle a_i\rangle_R$. Hence there is an $r \in R$ such that $c_i = r a_i$ i.e. $c = r a_i \mathbf{e}_i$. For $l = 2$, $c = c_i\mathbf{e}_i + c_j\mathbf{e}_j$ for some $1 \le i < j \le k$. The syzygy $c_i r_i + c_j r_j = 0$ implies that $c_i r_i \in \langle r_i\rangle_R \cap \langle r_j\rangle_R = \langle r_{i,j}\rangle_R$. If $r_{i,j} = 0$ then $c_i r_i = c_j r_j = 0$ and we can apply case $l = 1$ to the syzygies $c_i\mathbf{e}_i$ and $c_j\mathbf{e}_j$. Otherwise, $c_i r_i = r r_{i,j} = r(r_i b_{i,j})$ for some $r \in R$. Also, $c_j r_j = -c_i r_i = -r r_{i,j} = -r(r_j b'_{i,j})$. We have $r_i(c_i - r b_{i,j}) = r_j(c_j + r b'_{i,j}) = 0$, so $c_i - r b_{i,j} \in \mathrm{Ann}(r_i) = \langle a_i\rangle_R$ and $c_j + r b'_{i,j} \in \mathrm{Ann}(r_j) = \langle a_j\rangle_R$. If $c_i = r b_{i,j} + s a_i$ and $c_j = -r b'_{i,j} + s' a_j$, then $c = r(b_{i,j}\mathbf{e}_i - b'_{i,j}\mathbf{e}_j) + s a_i \mathbf{e}_i + s' a_j \mathbf{e}_j$.

Now let $l > 2$. Without loss of generality assume that $c = \sum_{i=1}^l c_i \mathbf{e}_i$. The syzygy $\sum_{i=1}^l c_i r_i = 0$ implies that $c_l \in (\langle r_1, \ldots, r_{l-1}\rangle_R : r_l) = \sum_{i=1}^{l-1} (\langle r_i\rangle_R : r_l)$, by Lemma 4.5. We can then write $c_l = d_1 + \cdots + d_{l-1}$ with $d_i \in (\langle r_i\rangle_R : r_l)$ i.e. $d_i r_l = v_i r_i$ for some $v_i \in R$. This means that $d_i\mathbf{e}_l - v_i\mathbf{e}_i \in \mathrm{Syz}(r_1, \ldots, r_k)$ and we can write

$$c = \sum_{i=1}^{l-1} c_i\mathbf{e}_i + \sum_{i=1}^{l-1} d_i\mathbf{e}_l = \sum_{i=1}^{l-1} (c_i + v_i)\mathbf{e}_i + \sum_{i=1}^{l-1} (d_i\mathbf{e}_l - v_i\mathbf{e}_i).$$

Since c and each $d_i\mathbf{e}_l - v_i\mathbf{e}_i$ are in $\mathrm{Syz}(r_1, \ldots, r_k)$, so is $c' = \sum_{i=1}^{l-1}(c_i + v_i)\mathbf{e}_i$. By the inductive hypothesis, c' and all the $d_i\mathbf{e}_l - v_i\mathbf{e}_i$ are linear combinations of elements of S, as they have strictly less than l non-zero components. Hence c is a linear combination of elements in S. □

The reader may check for example that $\{(5,0,0), (0,0,2), (1,-8,0), (0,10,-1)\}$ is a basis for $\mathrm{Syz}(4,3,10) \subset \mathbb{Z}_{20}^3$.

4.3 S-polynomials and A-polynomials

We first adapt the definition of S-polynomials to polynomials over R.

Definition 4.7 (S-polynomial) *Let $g_1, g_2 \in R[x_1, \ldots, x_n] \setminus \{0\}$ be distinct polynomials. An S-polynomial of g_1 and g_2 is any polynomial $c_1 t_1 g_1 - c_2 t_2 g_2$ where*

$$c_1 \operatorname{lc}(g_1) = c_2 \operatorname{lc}(g_2) \in \operatorname{lcm}(\operatorname{lc}(g_1), \operatorname{lc}(g_2)) \neq \{0\},$$

$c_i \in R$ and $t_i = \operatorname{lcm}(\operatorname{lt}(g_1), \operatorname{lt}(g_2))/\operatorname{lt}(g_i)$. If $\operatorname{lcm}(\operatorname{lc}(g_1), \operatorname{lc}(g_2)) = \{0\}$, we define 0 to be the only S-polynomial of g_1, g_2. We write $\operatorname{Spol}(g_1, g_2)$ for the set of S-polynomials of g_1 and g_2.

Note that if $h \in \operatorname{Spol}(g_1, g_2)$ then $\operatorname{lt}(h) < \operatorname{lcm}(\operatorname{lt}(g_1), \operatorname{lt}(g_2))$. If R is a domain, two S-polynomials of g_1 and g_2 differ by multiplication with a unit of R, so we can safely speak of 'the' S-polynomial of g_1 and g_2. This is no longer the case when R has zero divisors.

Example 4.8 *Let $g_1 = 2x^2 + 3x + 1$ and $g_2 = 5xy + 2y + 1$ in $\mathbb{Z}_{20}[x, y]$. We have $10 \in \operatorname{lcm}(2, 5)$. Consider the S-polynomials $h_1 = 5yg_1 - 2xg_2 = 11xy + 18x + 5y$ and $h_2 = 5yg_1 - 10xg_2 = 15xy + 10x + 5y$. If there were a unit $u \in \mathbb{Z}_{20}$ such that $h_2 = uh_1$ then 15 would be a unit in $\mathbb{Z}_{20}$.*

We will see that our results do not depend on which S-polynomial is chosen. The main additional difficulty encountered when trying to construct Gröbner bases over rings with zero divisors is that we do not necessarily have $\operatorname{lt}(g) = \operatorname{lt}(cg)$ for all $c \in R$ and so $\{g\}$ is not necessarily a Gröbner basis, as we saw in Example 3.10. This motivates the following definition:

Definition 4.9 (A-polynomial) *Let $g \in R[x_1, \ldots, x_n] \setminus \{0\}$. An A-polynomial of g is any polynomial of the form ag where $a \in R$ is such that $\langle a \rangle_R = \operatorname{Ann}(\operatorname{lc}(g))$. We write $\operatorname{Apol}(g)$ for the set of A-polynomials of g.*

Note that if $h \in \operatorname{Apol}(g)$ then $\operatorname{lt}(h) < \operatorname{lt}(g)$ and that any two A-polynomials of g differ by multiplication by a unit of R. Of course if R is a principal ideal domain, then $\operatorname{Apol}(g) = \{0\}$ for all $g \in R[x_1, \ldots, x_n] \setminus \{0\}$.

4.4 Characterisation of Gröbner Bases over R

We characterise Gröbner bases over R using Theorem 4.6 to obtain generators for a syzygy module of leading coefficients.

Theorem 4.10 *Let $G \subset R[x_1, \ldots, x_n] \setminus \{0\}$, $|G| < \infty$. Then G is a Gröbner basis if and only if*

(A) for any $g_1, g_2 \in G$ with $g_1 \neq g_2$, there is an $h \in \operatorname{Spol}(g_1, g_2)$ such that $h \to_G^* 0$ and

(B) for any $g \in G$, there is an $h \in \operatorname{Apol}(g)$ such that $h \to_G^* 0$.

Proof. (Cf. [1, Theorem 3.2.5]) The necessity of conditions (A) and (B) is obvious. Let $G = \{g_1, \ldots, g_k\}$ and put $r_i = \operatorname{lc}(g_i)$ for $i = 1, \ldots, k$. First we give a basis for $\operatorname{Syz}(r_1, \ldots, r_k)$. For each i, let $h_i = a_i g_i \in \operatorname{Apol}(g_i) \cap \operatorname{Std}(G)$. For each $1 \leq i < j \leq k$ with $\operatorname{lcm}(r_i, r_j) \neq \{0\}$, let $h_{i,j} \in \operatorname{Spol}(g_i, g_j) \cap \operatorname{Std}(G)$ be given by

$$h_{i,j} = b_{i,j} g_i \operatorname{lcm}(\operatorname{lt}(g_i), \operatorname{lt}(g_j))/\operatorname{lt}(g_i) - b'_{i,j} g_j \operatorname{lcm}(\operatorname{lt}(g_i), \operatorname{lt}(g_j))/\operatorname{lt}(g_j).$$

Applying Theorem 4.6 and the definitions of S-polynomials and A-polynomials, we see that

$$S = \{a_i \mathbf{e}_i \ : \ 1 \leq i \leq k\} \cup \{b_{i,j}\mathbf{e}_i - b'_{i,j}\mathbf{e}_j \ : \ 1 \leq i < j \leq k, \operatorname{lcm}(r_i, r_j) \neq \{0\}\}$$

generates $\operatorname{Syz}(r_1, \ldots, r_k)$. Now let $f \in \langle G \rangle \setminus \{0\} = \bigcup_{t \in T} \operatorname{Rep}_{\leq t}(G)$. We need to prove that $f \in \operatorname{Std}(G)$ i.e $f \in \operatorname{Rep}_{\leq \operatorname{lt}(f)}(G)$. Let $f \in \operatorname{Rep}_{\leq t}(G)$ with t minimal, and assume that $t > \operatorname{lt}(f)$. Write $f = h + \sum_{j=1}^{l} c_{i_j} t_{i_j} g_{i_j}$ where $h \in \operatorname{Rep}_{<t}(G)$, $l \leq k$, $1 \leq i_1 < \cdots < i_l \leq k$, $c_{i_j} \in R$,

$t_{i_j} \in T$, $t_{i_j} \operatorname{lt}(g_{i_j}) = t$ and $c_{i_j} r_{i_j} \neq 0$ for $j = 1, \ldots, l$. Then $\sum_{j=1}^{l} c_{i_j} r_{i_j} = 0$ i.e. $\sum_{j=1}^{l} c_{i_j} \mathbf{e}_{i_j} \in \operatorname{Syz}(r_1, \ldots, r_k)$. We have $\operatorname{lt}(g_{i_j}) | t$, for $j = 1, \ldots, l$. So by Theorem 4.6, there are $u_{i_j}, v_{i_l, i_j} \in R$ such that

$$f - h = \sum_{j=1}^{l} c_{i_j} t_{i_j} g_{i_j} = \sum_{j=1}^{l} u_{i_j} t_{i_j} h_{i_j} + \sum_{1 \leq l < j \leq l} v_{i_l, i_j} t_{i_l, i_j} h_{i_l, i_j},$$

where $t_{i_l, i_j} = t / \operatorname{lcm}(\operatorname{lt}(g_{i_l}), \operatorname{lt}(g_{i_j}))$. Obviously, $t_{i_j} \operatorname{lt}(h_{i_j}) < t$ and $t_{i_l, i_j} \operatorname{lt}(h_{i_l, i_j}) < t$. Conditions (A), (B) and Lemma 3.5 imply that all the summands are in $\operatorname{Rep}_{<t}(G)$, so $f \in \operatorname{Rep}_{<t}(G)$. By Lemma 3.5 again, $f \in \operatorname{Rep}_{\leq t'}(G)$ for some $t' < t$, which contradicts the minimality of t. □

In particular, $\{g\} \subset R[x_1, \ldots, x_n] \setminus \{0\}$ is a strong Gröbner basis if and only if $\operatorname{Apol}(g) = \{0\}$, *cf.* Corollary 3.12 and Proposition 4.2.

5 Characterisation of Strong Gröbner Bases over R

We have seen that over a field, the notions of strong Gröbner basis and Gröbner basis coincide. Thus the classical effective characterisation of Gröbner bases in terms of S-polynomials holds for strong Gröbner bases as well. Over a principal ideal domain however, a strong Gröbner basis G can be characterised by: for any pair of polynomials in G (i) their S-polynomial reduces to 0 wrt. G and (ii) their 'G-polynomial' is strongly reducible to 0 wrt. G; see [2, Section 10.1] and the references therein. We generalise this to principal ideal rings in Corollary 5.12 below.

5.1 G-polynomials

Let us recall the definition of a G-polynomial (see [2, Definition 10.9]).

Definition 5.1 (G-polynomial) *Let $F = \{f_1, \ldots, f_k\} \subset R[x_1, \ldots, x_n] \setminus \{0\}$. A G-polynomial of F is any polynomial $\sum_{i=1}^{k} c_i t_i f_i$ where*

$$\sum_{i=1}^{k} c_i \operatorname{lc}(f_i) \in \gcd(\operatorname{lc}(F)),$$

$c_i \in R$ and $t_i = \operatorname{lcm}(\operatorname{lt}(F)) / \operatorname{lt}(f_i)$. We write $\operatorname{Gpol}(F)$ or $\operatorname{Gpol}(f_1, \ldots, f_k)$ for the set of G-polynomials of $\{f_1, \ldots, f_k\}$.

Note that $f \in \operatorname{Gpol}(f)$ and that if $h \in \operatorname{Gpol}(F)$ then $\operatorname{lt}(h) = \operatorname{lcm}(\operatorname{lt}(F))$ and $\operatorname{lc}(h) \in \gcd(\operatorname{lc}(F))$. Hence by Proposition 4.3, if $h_1, h_2 \in \operatorname{Gpol}(F)$ then $\operatorname{lm}(h_1) = u \operatorname{lm}(h_2)$ for some unit $u \in R$. If R is a domain, any two G-polynomials of f_1 and f_2 differ by multiplication with a unit, so we can safely speak of 'the' G-polynomial of f_1 and f_2. This is no longer the case when R has zero divisors, but we will see that our results do not depend on which G-polynomial is chosen.

Example 5.2 *For $f_1, f_2 \in \mathbb{Z}_{20}[x, y]$ as in Example 4.8, $h_1 = x f_2 - 2y f_1 = x^2 y - 4xy + x - 2y$ and $h_2 = 5x f_2 - 2y f_1 = x^2 y + 4xy + 5x - 2y$ are G-polynomials of f_1 and f_2. If there were a unit $u \in R$ such that $h_1 = u h_2$ then 5 would be a unit in $\mathbb{Z}_{20}$.*

5.2 A first construction of strong Gröbner bases over R

We begin by generalising the construction of strong Gröbner bases over principal ideal domains given in [1, Theorem 4.5.9] to principal ideal rings.

Definition 5.3 (Saturated subset) *(cf. [1, Definition 4.2.4]) Let S, S' be finite sets and $\emptyset \neq S' \subseteq S \subset T$. We say that S' is saturated wrt. S if*

$$S' = \{t \in S \ : \ t | \operatorname{lcm}(S')\}.$$

Theorem 5.4 *(cf. [1, Theorem 4.5.9]) Let I be a non-zero ideal of $R[x_1, \ldots, x_n]$ and let G be a Gröbner basis for I. For each $F \subseteq G$ choose an $h_F \in \operatorname{Gpol}(F)$. Then the set*

$$\{h_F \ : \ F \subseteq G \text{ and } \operatorname{lt}(F) \text{ is saturated wrt. } \operatorname{lt}(G)\}$$

is a strong Gröbner basis for I.

PROOF. The proof is similar to [1, Theorem 4.5.9]. □

For an alternative proof, see Remark 5.11(i) below.

5.3 Gpol-closure

If f is reducible wrt. G, it is easy to see that there is an $F \subseteq G$ and an $h \in \operatorname{Gpol}(F)$ such that f is strongly reducible wrt. $G \cup \{h\}$. This suggests the following definition.

Definition 5.5 (Gpol-closed, Gpol-closure) *Let G be a finite non-empty subset of $R[x_1, \ldots, x_n] \setminus \{0\}$. We say that*

(i) G is Gpol-closed *if for all $g_1, g_2 \in G$ with $g_1 \neq g_2$, there is an $h \in \operatorname{Gpol}(g_1, g_2)$ which is strongly reducible wrt. G.*

(ii) G is a Gpol-closure *of $G' \subseteq G$ if G is* Gpol-*closed and*

$$G \subseteq \bigcup_{\emptyset \neq F' \subseteq G'} \operatorname{Gpol}(F'). \tag{1}$$

Note that any strong Gröbner basis is Gpol-closed, if G is a Gpol-closure of G' then $\langle G \rangle = \langle G' \rangle$ and if G' is Gpol-closed then G' is a Gpol-closure of itself.

Proposition 5.6 *If R is a finite-chain ring, any non-empty subset of $R[x_1, \ldots, x_n] \setminus \{0\}$ is* Gpol-*closed.*

PROOF. Let $G \subseteq R[x_1, \ldots, x_n] \setminus \{0\}$ and let $g_1, g_2 \in G$ be distinct. If $h \in \operatorname{Gpol}(g_1, g_2)$, then h is reducible wrt. $\{g_1, g_2\}$, so by Proposition 3.2, h is strongly reducible wrt. G. □

The following properties of G-polynomials follow easily from the definition:

Lemma 5.7 *Let $F = \{f_1, \ldots, f_k\}$, $F' = \{f'_1, \ldots, f'_{k'}\}$ be subsets of $R[x_1, \ldots, x_n] \setminus \{0\}$ and let $h \in \operatorname{Gpol}(F)$, $h' \in \operatorname{Gpol}(F')$. Then:*

(i) $\operatorname{Gpol}(h, h') = \operatorname{Gpol}(F \cup F')$.

(ii) If $k = k'$ and $\operatorname{lm}(f_i) | \operatorname{lm}(f'_i)$ for $i = 1, \ldots, k$ then $\operatorname{lm}(h) | \operatorname{lm}(h')$.

Proposition 5.8 *Let $G, G' \subset R[x_1, \ldots, x_n] \setminus \{0\}$ be finite sets satisfying condition (1). The following assertions are equivalent:*

(i) G is a Gpol-*closure of G'*

(ii) for all non-empty $F' \subseteq G'$, there is an $h \in \operatorname{Gpol}(F')$ which is strongly reducible wrt. G

(iii) for all non-empty $F' \subseteq G'$ such that $\mathrm{lt}(F')$ is saturated wrt. $\mathrm{lt}(G')$, there is an $h \in \mathrm{Gpol}(F')$ which is strongly reducible wrt. G.

(iv) for all $f \in R[x_1, \ldots, x_n]$, f is reducible wrt. G' if and only if f is strongly reducible wrt. G.

PROOF. We will prove the equivalence of (ii) with the other assertions, starting with (ii) $\Leftrightarrow$ (i). For the forward implication we need only show that G is Gpol-closed, so let $h_1, h_2 \in G$. From condition (1), there are $F'', F' \subseteq G'$ such that $h_1 \in \mathrm{Gpol}(F')$ and $h_2 \in \mathrm{Gpol}(F'')$. By (ii), there is an $h \in \mathrm{Gpol}(F' \cup F'')$ which is strongly reducible wrt. G. By Lemma 5.7, $h \in \mathrm{Gpol}(h_1, h_2)$, so G is Gpol-closed.

We prove (i) $\Rightarrow$ (ii) by induction on the cardinality of $F' = \{f_1, \ldots, f_k\}$. For $k = 1, 2$ it obviously holds. Assume that $k \geq 3$ and that (i) $\Rightarrow$ (ii) for subsets of cardinality less than k. Then by the inductive hypothesis, there are $h_1 \in \mathrm{Gpol}(f_1, f_2)$ and $h_2 \in \mathrm{Gpol}(f_3, \ldots, f_k)$ which are strongly reducible wrt. G i.e. there are $g_i \in G$ such that $\mathrm{lm}(g_i) | \mathrm{lm}(h_i)$ for $i = 1, 2$. Since G is Gpol-closed, there is a $g \in \mathrm{Gpol}(g_1, g_2)$ which is strongly reducible wrt. G. Let $h \in \mathrm{Gpol}(h_1, h_2)$. By Lemma 5.7, $h \in \mathrm{Gpol}(F')$ and $\mathrm{lm}(g) | \mathrm{lm}(h)$, so h is strongly reducible wrt. G.

For (iii) $\Rightarrow$ (ii), let $F' \subseteq G'$ and $h \in \mathrm{Gpol}(F')$. Let $F'' = \{f \in G' \ : \ \mathrm{lt}(f) | \mathrm{lcm}(\mathrm{lt}(F'))\}$. Trivially $\mathrm{lt}(F'')$ is saturated wrt. $\mathrm{lt}(G')$, so there is a $g \in \mathrm{Gpol}(F'')$ which is strongly reducible wrt. G. Since $F' \subseteq F''$, $\mathrm{lc}(g) | \mathrm{lc}(h)$ and by construction $\mathrm{lt}(g) | \mathrm{lt}(h)$, so $\mathrm{lm}(g) | \mathrm{lm}(h)$ and h is also strongly reducible wrt. G.

We prove now (ii) $\Rightarrow$ (iv). Assume first that f is reducible wrt. G'. Then there is an $F' = \{f_1, \ldots, f_k\} \subset G'$ such that $\mathrm{lt}(f_i) | \mathrm{lt}(f)$ for $i = 1, \ldots, k$ and $\mathrm{lm}(f) = \sum_{i=1}^{k} c_i t_i \mathrm{lm}(f_i)$ for some $c_i \in R$ and $t_i \in T$. Hence $\mathrm{lcm}(\mathrm{lt}(F')) | \mathrm{lt}(f)$ and $\mathrm{lc}(f)$ is divisible by any element of $\gcd(\mathrm{lc}(F'))$ so $\mathrm{lm}(h) | \mathrm{lm}(f)$ for all $h \in \mathrm{Gpol}(F')$. By (ii), there is an $h \in \mathrm{Gpol}(F')$ which is strongly reducible wrt. G, so f is strongly reducible wrt. G.

Next assume that f is strongly reducible wrt. G. There is then an $h \in G$ such that $\mathrm{lm}(h) | \mathrm{lm}(f)$. We know from condition (1) that $h \in \mathrm{Gpol}(F')$ for some $F' \subseteq G'$. It can be easily checked that f is reducible wrt. F'.

For (iv) $\Rightarrow$ (ii), let $F' \subseteq G'$ and $h \in \mathrm{Gpol}(F')$. From the definition of a G-polynomial, we see that h is reducible wrt. G'. Hence, by (iv), h is strongly reducible wrt. G. $\square$

For the particular case $G' = G$, Proposition 5.8 yields:

Corollary 5.9 *Let $G \subset R[x_1, \ldots, x_n] \setminus \{0\}$ be a finite set. The following assertions are equivalent:*

(i) G is Gpol*-closed*

(ii) for all non-empty $F \subseteq G$, there is an $h \in \mathrm{Gpol}(F)$ which is strongly reducible wrt. G

(iii) for all non-empty $F \subseteq G$ such that $\mathrm{lt}(F)$ is saturated wrt. $\mathrm{lt}(G)$, there is an $h \in \mathrm{Gpol}(F)$ which is strongly reducible wrt. G

(iv) for all $f \in R[x_1, \ldots, x_n]$, f is reducible wrt. G if and only if f is strongly reducible wrt. G.

5.4 Characterisation of strong Gröbner bases over R

Our first characterisation does not use Theorem 4.10.

Proposition 5.10 *Let $G \subset R[x_1, \ldots, x_n] \setminus \{0\}$ be a finite set. The following assertions are equivalent:*

(i) G is a strong Gröbner basis

(ii) G is a Gröbner basis and G is Gpol*-closed*

(iii) G is a Gpol*-closure of some Gröbner basis $G' \subseteq G$.*

PROOF. For (iii) $\Rightarrow$ (i), let $f \in \langle G \rangle = \langle G' \rangle$. Since G' is a Gröbner basis, f is reducible wrt. G', so f is strongly reducible wrt. G by Proposition 5.8(iv). $\square$

Remark 5.11 *The implication (iii) $\Rightarrow$ (i) of Proposition 5.10 together with Proposition 5.8(iii) yields another proof of Theorem 5.4.*

Theorem 4.10, Proposition 5.10 and Proposition 5.6 easily yield:

Corollary 5.12 *Let $G \subset R[x_1, \ldots, x_n] \setminus \{0\}$ be a finite set. Then G is a strong Gröbner basis if and only if*

(A) for any $g_1, g_2 \in G$ with $g_1 \neq g_2$, there is an $h \in \mathrm{Spol}(g_1, g_2)$ such that $h \twoheadrightarrow_G^* 0$,

(B) for any $g \in G$, there is an $h \in \mathrm{Apol}(g)$ such that $h \twoheadrightarrow_G^* 0$ and

(C) for any $g_1, g_2 \in G$ with $g_1 \neq g_2$ there is an $h \in \mathrm{Gpol}(g_1, g_2)$ which is strongly reducible wrt. to G.

Corollary 5.13 *Let R be a finite-chain ring and $G \subset R[x_1, \ldots, x_n] \setminus \{0\}$ be a finite set. Then G is a strong Gröbner basis if and only if*

(A) for any $g_1, g_2 \in G$ with $g_1 \neq g_2$, there is an $h \in \mathrm{Spol}(g_1, g_2)$ such that $h \twoheadrightarrow_G^* 0$ and

(B) for any $g \in G$, there is an $h \in \mathrm{Apol}(g)$ such that $h \twoheadrightarrow_G^* 0$.

6 Strong Gröbner Basis Algorithms

6.1 The principal ideal ring case

We say that R is *computable* if there are algorithms which compute: sums; negation; products; an lcm; a generator of the annihilator ideal of an element; for any $r_1, r_2 \in R$ there is an algorithm which computes c_1, c_2 such that $c_1 r_1 + c_2 r_2 \in \gcd(r_1, r_2)$; for any $r_1, r_2 \in R$, there is an algorithm which decides whether $r_2 | r_1$ and in the affirmative case, produces an $r_3 \in R$ such that $r_1 = r_2 r_3$.

Examples of computable principal ideal rings are $\mathbb{Z}$ and $\mathbb{Z}_m$. If K is a computable field then $K[X]$ is a computable. Also, a quotient ring of a computable principal ideal ring and a finite product of computable principal ideal rings are computable. When R is a finite-chain ring in which γ and ν are given and there are algorithms which compute sums, negations and products, then R is computable (see Proposition 2.2). For example $GR(p^k, n)$ is computable . Throughout this section we will assume that R is computable.

Theorem 4.10 enables us to compute a Gröbner basis as follows:

Algorithm 6.1 (Gröbner basis)

$G \leftarrow$ **GB-PIR**(F)

Input: F a finite subset of $R[x_1, \ldots, x_n]$, where R is a computable principal ideal ring.
Output: G a Gröbner basis for $\langle F \rangle$.
Notes: B is the set of pairs of polynomials in G' whose S-polynomials still have to be computed.
C is the set of polynomials in G' whose A-polynomials still have to be computed.

begin
$G \leftarrow F$
$B \leftarrow \{\{f_1, f_2\} \ : \ f_1, f_2 \in G, f_1 \neq f_2\}$

$C \leftarrow F$
while $B \cup C \neq \emptyset$ **do**
  if $C \neq \emptyset$ **then**
    select f from C
    $C \leftarrow C \setminus \{f\}$
    compute $h \in \mathrm{Apol}(f)$
  else
    select $\{f_1, f_2\}$ from B
    $B \leftarrow B \setminus \{\{f_1, f_2\}\}$
    compute $h \in \mathrm{Spol}(f_1, f_2)$
  end if
  compute $g \in \mathrm{Rem}(h, G)$
  if $g \neq 0$ **then**
    $B \leftarrow B \cup \{\{g, f\} \ : \ f \in G\}$
    $C \leftarrow C \cup \{g\}$
    $G \leftarrow G \cup \{g\}$
  end if
end while
return(G)
end

Proposition 6.2 *Algorithm* **GB-PIR** *is correct and terminates.*

PROOF. We first show that the algorithm terminates. Any new polynomial g to be added to G is not reducible wrt. G i.e. $\mathrm{lm}(g) \notin \langle \mathrm{lm}(G) \rangle$. Thus $\langle \mathrm{lm}(G) \rangle$ increases strictly each time a new polynomial is added to G. Such a strictly ascending chain of ideals has to be finite because $R[x_1, \ldots, x_n]$ is Noetherian and so eventually no new polynomials are added to G, as required.

Let $I = \langle F \rangle$. We have $\langle G \rangle = I$ on initialising and all polynomials subsequently added to G are in I, so the property $I = \langle G \rangle$ is preserved. Any polynomial in $G \setminus C$ has an A-polynomial which reduces to 0 wrt. G and any pair of polynomials $g_1, g_2 \in G$ with $\{g_1, g_2\} \notin B$ has an S-polynomial which reduces to 0 wrt. G. Thus on termination, G satisfies conditions (A) and (B) of Theorem 4.10 and G is therefore a Gröbner basis. □

Each iteration of Algorithm **GB-PIR** computes either an A-polynomial or an S-polynomial. For the correctness of the algorithm, it does not matter which one is done first. We have preferred the former whenever possible since A-polynomials are easy to compute, have lower degree and can be used in subsequent reductions. Thus computing A-polynomials first is likely to be more efficient.

A first method for computing a *strong Gröbner basis* G for an ideal $\langle F \rangle$ could be based on Proposition 5.10(iii). Namely, we compute a Gröbner basis G' for $\langle F \rangle$ and then compute a Gpol-closure G of G' using the algorithm below.

Algorithm 6.3 (Gpol-closure)

$G \leftarrow$ **Gpol-closure**(G')

Input: G' a finite subset of $R[x_1, \ldots, x_n] \setminus \{0\}$.
Output: G a finite subset of $R[x_1, \ldots, x_n]$ which is a Gpol-closure of G'.

begin
$G \leftarrow G'$
for all $F' \subseteq G'$ **do**

```
    if lt(F') is saturated wrt. lt(G') then
      compute h ∈ Gpol(F')
      if h is not strongly reducible wrt. G then G ← G ∪ {h}
      end if
    end if
end for
return(G)
end
```

However, reduction is less efficient than strong reduction and in each reduction step we basically compute a G-polynomial and then discard it. Thus to compute a strong Gröbner basis as above we would have to recompute the discarded G-polynomials. The following algorithm, also based on Theorem 4.10 and Proposition 5.10, maintains a Gpol-closure G of the current basis G' and only uses strong reduction wrt. G rather than reduction wrt. G' (see Proposition 5.8(iv)).

Algorithm 6.4 (Strong Gröbner basis)

$G \leftarrow$ **SGB-PIR**(F)

Input: F a finite subset of $R[x_1, \ldots, x_n] \setminus \{0\}$, where R is a computable principal ideal ring.
Output: G a strong Gröbner basis for $\langle F \rangle$.
Notes: $G' \subseteq G$, so G is a Gpol-closure of G'; on termination, G' will be a Gröbner basis for $\langle F \rangle$.
B is the set of pairs of polynomials in G' whose S-polynomials still have to be computed.
C is the set of polynomials in G' whose A-polynomials still have to be computed.

```
begin
G' ← F
B ← {{g1, g2} : g1, g2 ∈ G', g1 ≠ g2}
C ← F
G ← Gpol-closure(G')
while B ∪ C ≠ ∅ do
      if C ≠ ∅ then
        select g from C
        C ← C \ {g}
        compute h ∈ Apol(g)
      else
        select {g1, g2} from B
        B ← B \ {{g1, g2}}
        compute h ∈ Spol(g1, g2)
      end if
      compute g ∈ SRem(h, G)
      if g ≠ 0 then
        B ← B ∪ {{g, f} | f ∈ G'}
        C ← C ∪ {g}
        G ← Gpol-closure-update(G', g, G)
        G' ← G' ∪ {g}
      end if
end while
return(G)
end
```

The auxiliary algorithm **Gpol-closure-update** is described below.

Algorithm 6.5 (Gpol-closure update)

$G \leftarrow$ **Gpol-closure-update**(G', g, G'')

Input: G' a finite subset of $R[x_1, \ldots, x_n] \setminus \{0\}$
$g \in R[x_1, \ldots, x_n] \setminus G'$, $g \neq 0$
G'' a Gpol-closure of G'.
Output: G a finite subset of $R[x_1, \ldots, x_n]$ which is a Gpol-closure of $G' \cup \{g\}$.

begin
$G \leftarrow G'' \cup \{g\}$
for all $g'' \in G''$ **do**
compute $h \in \mathrm{Gpol}(g, g'')$
if h is not strongly reducible wrt. G **then** $G \leftarrow G \cup \{h\}$
end if
end for
return(G)
end

Example 6.6 *Let* $g_1 = 2x^2 + 3x + 1 \in \mathbb{Z}_6[x]$ *and* $F = \{g_1\}$. *We will compute a strong Gröbner basis for* $\langle F \rangle$. *We have* $g_2 = 3x + 3 \in \mathrm{Apol}(g_1)$, $\mathrm{Spol}(g_1, g_2) = \{0\}$ *and* $h_1 = x^2 - 1 \in \mathrm{Gpol}(g_1, g_2)$. *Then* $G = \{g_1, g_2, h_1\}$ *is* Gpol*-closed and so* G *is a strong Gröbner basis for* $\langle F \rangle$.

Example 6.7 *(cf. [1, Example 4.2.12]) Let* $F = \{g_1, g_2\} \subset \mathbb{Z}_{20}[x, y]$, *where* $g_1 = 4xy + x$ *and* $g_2 = 3x^2 + y$. *We will compute a strong Gröbner basis for* $\langle F \rangle$ *wrt. the lexicographical order with* $x > y$. *Initially* $G' = F$. *The new polynomials introduced in* G' *will be denoted* g_3, g_4 *etc. A* Gpol*-closure of* F *will be* $G = \{g_1, g_2, h_1\}$ *where* $h_1 = x^2y + xy - y^2 \in \mathrm{Gpol}(g_1, g_2)$. *We have* $5x \in \mathrm{Apol}(g_1)$ *and* $5x$ *is not strongly reducible wrt.* G, *so we put* $g_3 = 5x$. *We update* G *by introducing* g_3 *and adding* $h_2 = xy - x \in \mathrm{Gpol}(g_1, g_3)$ *to* G. *We compute* $3x^2 - 4y^2 \in \mathrm{Spol}(g_1, g_2)$ *which strongly reduces to* $g_4 = 4y^2 + y$. *Updating* G *will result in adding* g_4 *to* G *only. We have* $g_5 = 5y \in \mathrm{Apol}(g_4)$. *The updated* G *will be* $G = \{4xy + x, 3x^2 + y, x^2y + xy - y^2, 5x, xy - x, 4y^2 + y, 5y, y^2 - y\}$, *the last polynomial being* $h_3 = y^2 - y \in \mathrm{Gpol}(g_4, g_5)$. *This is also a final strong Gröbner basis, as any further A-polynomials and S-polynomials strongly reduce to 0 wrt.* G.

We prove now the correctness and termination of the algorithms.

Theorem 6.8 *Algorithms* **Gpol-closure** *and* **Gpol-closure-update** *are correct and terminate.*

Proof. The termination of both algorithms is obvious. The correctness of Algorithm **Gpol-closure** follows from Proposition 5.8. To prove the correctness of Algorithm **Gpol-closure-update**, let $F' \subset G' \cup \{g\}$. We have to show that there is an $h \in \mathrm{Gpol}(F')$ which is strongly reducible wrt. G. If $F' \subseteq G'$, this follows from the fact that G'' is a Gpol-closure of G' and $G'' \subset G$. Otherwise, write $F' = F'' \cup \{g\}$ where $F'' \subset G'$. Since G'' is a Gpol-closure of G', there is an $h_1 \in \mathrm{Gpol}(F'')$ and a $g'' \in G''$ such that $\mathrm{lm}(g'') | \mathrm{lm}(h_1)$, and we have $\mathrm{Gpol}(g, h_1) = \mathrm{Gpol}(F')$ by Lemma 5.7(i). Algorithm **Gpol-closure-update** computes an $h_2 \in \mathrm{Gpol}(g, g'')$ and upon termination h_2 is strongly reducible wrt. G. Thus if $h \in \mathrm{Gpol}(g, h_1)$, then $h \in \mathrm{Gpol}(F')$ and $\mathrm{lm}(h_2) | \mathrm{lm}(h)$ by Lemma 5.7(ii), as required. □

The following lemma is an easy consequence of the definitions.

Lemma 6.9 *Let* G *be a Gpol-closure of* $G' \subset R[x_1, \ldots, x_n] \setminus \{0\}$ *and let* $f \in R[x_1, \ldots, x_n]$. *If* $f \twoheadrightarrow_G^* h$ *then* $f \rightarrow_{G'}^* h$.

Theorem 6.10 *Algorithm* **SGB-PIR** *is correct and terminates.*

PROOF. We first show that the algorithm terminates. The calls to **Gpol-closure** and **Gpol-closure-update** ensure that G is a Gpol-closure of G' throughout the algorithm. Now any new polynomial g to be added to G' is not strongly reducible wrt. G and so g is not reducible wrt. G' by Proposition 5.8(iv). In other words, if g is to be added to G', then $\mathrm{lm}(g) \notin \langle \mathrm{lm}(G') \rangle$. Thus $\langle \mathrm{lm}(G') \rangle$ increases strictly each time a new polynomial is added to G' and as above, eventually no new polynomials are added to G', as required.

Let $I = \langle F \rangle$. We have $\langle G' \rangle = I$ on initialising and all polynomials subsequently added to G' are in I, so the property $I = \langle G' \rangle$ is preserved.

For any polynomial $g \in G' \setminus C$, there is an $h \in \mathrm{Apol}(g)$ which strongly reduces to 0 wrt. G. Hence by Lemma 6.9, h reduces to 0 wrt G'. For any pair of polynomials $g_1, g_2 \in G'$, if $\{g_1, g_2\} \notin B$ then there is an $h \in \mathrm{Spol}(g_1, g_2)$ which strongly reduces to 0 wrt. G. Again, h reduces to 0 wrt. G' and on termination of the algorithm, G' satisfies properties (A) and (B) of Theorem 4.10 and is therefore a Gröbner basis. Finally, G will be a strong Gröbner basis by Proposition 5.10(iii). □

Remarks 6.11 *(i) The efficiency of Algorithm* **SGB-PIR** *can be improved by adapting the usual techniques used for computing Gröbner bases for polynomials over fields (e.g. avoiding unnecessary S-polynomials, strongly reducing the polynomials in the basis wrt. each other, processing the polynomials in a 'favourable' order) and possibly devising new techniques specifically for principal ideal rings. We will not investigate these issues here.*

(ii) When R is a field, our algorithm reduces to the classical Buchberger algorithm. Hence the complexity of Algorithm **SGB-PIR** *for principal ideal rings is at least as high as the complexity of the classical algorithm over fields.*

6.2 Two special cases

If R is a finite-chain ring, Algorithm **SGB-PIR** simplifies as Algorithms **Gpol-closure** and **Gpol-closure-update** are not needed in view of Corollary 5.13 i.e. in Algorithm **SGB-PIR** we can delete '$G \leftarrow$ **Gpol-closure**(G')', '$G \leftarrow$ **Gpol-closure-update**(G', g, G)' and replace G' by G. See [9, Algorithm 3.9] for complete details.

Example 6.12 *Let p be a prime and $g_1 = px + y \in \mathbb{Z}_{p^2}[x, y]$ with a term order such that $x > y$. We have $g_2 = py \in \mathrm{Apol}(g_1)$ and $y^2 \in \mathrm{Spol}(g_1, g_2)$. Any further A-polynomial and S-polynomial is reducible to 0, so a strong Gröbner basis for $\langle g_1 \rangle$ is $\{px + y, py, y^2\}$.*

Example 6.13 *As in Example 3.10, let $g_1 = px^2 + x + 1 \in \mathbb{Z}_{p^2}[x]$. We have $g_2 = px + p \in \mathrm{Apol}(g_1)$ and $(1 - p)x + 1 \in \mathrm{Spol}(g_1, g_2)$. As $1 - p$ is a unit, we put $g_3 = x + (1 + p)$. Since S-polynomials of g_1 and g_3 and of g_2 and g_3 strongly reduce to 0, a strong Gröbner basis for $\langle g_1 \rangle$ is $\{x + 1 + p, px + p, px^2 + x + 1\}$.*

If R is a principal ideal domain, Algorithm **SGB-PIR** simplifies since A-polynomials are not needed. So all instructions concerning C or Apol can be deleted. Algorithms **Gpol-closure** and **Gpol-closure-update** are unchanged. The algorithm thus obtained is similar to [2, Algorithm D-Gröbner, p. 461]. However, our algorithm is more efficient since it computes the S-polynomials of pairs of polynomials in G' rather than in G and in general $G' \subset G$.

7 Minimal strong Gröbner bases

7.1 Characterisation

We recall the definition of minimal strong Gröbner bases in $A[x_1, \ldots, x_n]$ and give a new characterisation.

Definition 7.1 (minimal strong Gröbner basis) *A strong Gröbner basis G is called* minimal *if no proper subset of G is a strong Gröbner basis for $\langle G \rangle$.*

The following equivalent definition of minimal strong Gröbner bases is well-known over a field and holds over A by the same argument.

Proposition 7.2 *Let G be a strong Gröbner basis in $A[x_1, \ldots, x_n]$. Then G is minimal if and only if for all distinct $g, g' \in G$, $\operatorname{lm}(g) \not| \operatorname{lm}(g')$.*

Given a strong Gröbner basis G we can obtain a minimal strong Gröbner basis by the usual algorithm, viz. as long as there are distinct $g, g' \in G$ such that $\operatorname{lm}(g) | \operatorname{lm}(g')$, remove g' from G.

Example 7.3 *For $\langle px^2 + x + 1 \rangle \subset \mathbb{Z}_{p^2}[x]$ of Example 6.13, a minimal strong Gröbner basis is $\{x+1+p\}$. For $\langle 2x^2+3x+1 \rangle \subset \mathbb{Z}_6[x]$ we obtain a minimal strong Gröbner basis $\{3(x+1), x^2+3x+2\}$ using the strong Gröbner basis computed in Example 6.6. A minimal strong Gröbner basis for $\langle 4xy + x, 3x^2 + y \rangle \subset \mathbb{Z}_{20}[x, y]$ is $\{xy - x, 3x^2 + y, y^2 - y, 5x, 5y\}$ using the strong Gröbner basis computed in Example 6.7.*

The following characterisation seems to be new:

Theorem 7.4 *Let R be a principal ideal ring which is not a field and let G be a strong Gröbner basis in $R[x_1, \ldots, x_n]$. Then G is minimal if and only if for all distinct $g, g' \in G$, $\operatorname{lt}(g) | \operatorname{lt}(g')$ implies $\operatorname{lt}(g) \neq \operatorname{lt}(g')$ and $\langle \operatorname{lc}(g) \rangle_R \subset \langle \operatorname{lc}(g') \rangle_R$.*

Proof. Assume that G is a minimal strong Gröbner basis, $g, g' \in G$ are distinct and $\operatorname{lt}(g) | \operatorname{lt}(g')$. If $\operatorname{lc}(g) | \operatorname{lc}(g')$ then $\operatorname{lm}(g) | \operatorname{lm}(g')$, which is impossible by Proposition 7.2. We now show that $\operatorname{lc}(g') | \operatorname{lc}(g)$. Let $h \in \operatorname{Gpol}(g, g')$. Then $\operatorname{lc}(h) | \operatorname{lc}(g)$, $\operatorname{lc}(h) | \operatorname{lc}(g')$ and $\operatorname{lt}(h) = \operatorname{lt}(g')$ i.e. $\operatorname{lm}(h) | \operatorname{lm}(g')$. Since $h \in I$, there is a $g'' \in G$ such that $\operatorname{lm}(g'') | \operatorname{lm}(h)$. Therefore $\operatorname{lm}(g'') | \operatorname{lm}(g')$, which can only happen if $g'' = g'$ by Proposition 7.2. Hence $\operatorname{lc}(g') | \operatorname{lc}(h) | \operatorname{lc}(g)$ and if $\operatorname{lt}(g') = \operatorname{lt}(g)$ then $\operatorname{lm}(g') | \operatorname{lm}(g)$ which again contradicts Proposition 7.2. Thus $\operatorname{lt}(g) \neq \operatorname{lt}(g')$ and $\langle \operatorname{lc}(g) \rangle_R \subset \langle \operatorname{lc}(g') \rangle_R$ as claimed.

The converse is an immediate consequence of Proposition 7.2. □

7.2 Leading monomials

Although minimal Gröbner bases are not unique, we can say something about their leading monomials:

Theorem 7.5 *Let $F = \{f_1, \ldots, f_k\}$ and $G = \{g_1, \ldots, g_l\}$ be minimal strong Gröbner bases for the same ideal of $A[x_1, \ldots, x_n]$. Then $k = l$ and after renumbering if necessary, $\operatorname{lt}(f_i) = \operatorname{lt}(g_i)$ and $\langle \operatorname{lc}(f_i) \rangle_A = \langle \operatorname{lc}(g_i) \rangle_A$ for $i = 1, \ldots, k$. If in addition A is a principal ideal ring, there are units $u_i \in A$ such that $\operatorname{lm}(f_i) = u_i \operatorname{lm}(g_i)$ for $i = 1, \ldots, k$.*

Proof. As in [1, Proposition 1.8.4], we obtain $k = l$ and after renumbering if necessary, $\operatorname{lm}(f_i)$ and $\operatorname{lm}(g_i)$ divide each other for $i = 1, \ldots, k$. This gives the first part. The second part now follows from Proposition 4.1(i). □

Corollary 7.6 *If $\{g\} \subseteq R[x_1, \ldots, x_n]$ is a strong Gröbner basis, then any minimal strong Gröbner basis of $\langle g \rangle$ is of the form $\{ug\}$ for some unit $u \in R$.*

PROOF. Let $\{f\}$ be another minimal strong Gröbner basis for $I = \langle g \rangle$. By Theorem 7.5, there is a unit $u \in R$ such that $\mathrm{lm}(f) = u\,\mathrm{lm}(g)$. Hence if $f - ug \neq 0$ then $\mathrm{lt}(f - ug) < \mathrm{lt}(g)$. This is impossible since $f - ug \in I$ and so $\mathrm{lm}(g) | \mathrm{lm}(f - ug)$. □

Acknowledgements. We thank Arthur Chatters for pointing out the results in [10] on the structure of principal ideal rings, and Aidan Schofield for a useful discussion. Financial support from the U.K. Engineering and Physical Sciences Research Council (EPSRC) under Grant L07680 is gratefully acknowledged.

E-mail addresses: ghn@maths.uq.edu.au ana.salagean@ntu.ac.uk

URL's: http://www.maths.uq.edu.au/∼ghn http://science.ntu.ac.uk/msor/ana/

References

[1] W. Adams and P. Loustaunau. *An Introduction to Gröbner bases*, Volume 3 of *Graduate Studies in Mathematics*. American Mathematical Society, 1994.

[2] T. Becker and V. Weispfenning. *Gröbner Bases*. Graduate Texts in Mathematics 141. Springer, 1993.

[3] W.Bosma, J. Cannon, and C.Playoust. The Magma algebra system I: The user language. *Journal of Symbolic Computation*, 24:235–265, 1997.

[4] A. R. Calderbank and N. J. A. Sloane. Modular and p-adic codes. *Designs, Codes and Cryptography*, 6:21–35, 1995.

[5] J.-C.Faugère. A new efficient algorithm for computing Gröbner bases (F_4). *Journal of Pure and Applied Algebra*, 139:61–88, 1999.

[6] R. Gilmer. *Multiplicative Ideal Theory*. Marcel Dekker, 1972.

[7] B. R. McDonald. *Finite Rings with Identity*. Marcel Dekker, New York, 1974.

[8] G. H. Norton and A. Sălăgean. On the structure of linear and cyclic codes over finite chain rings. *Applicable algebra in engineering, communication and computing*, 10:489–506, 2000.

[9] G. H. Norton and A. Sălăgean. Strong Gröbner bases and cyclic codes over a finite-chain ring. *Workshop on Coding and Cryptography, Paris 2001. Electronic Notes in Discrete Mathematics*, 6, April 2001. *http://www.elsevier.nl:80/inca/publications/store/5/0/5/6/0/9/*

[10] O. Zariski and P. Samuel. *Commutative Algebra*, Volume 1. Springer, 1979.