On Gröbner Bases in Monoid and Group Rings

Klaus Madlener
Birgit Reinert
Fachbereich Informatik, Universität Kaiserslautern
W–67653 Kaiserslautern, Germany
email: madlener@informatik.uni-kl.de, reinert@informatik.uni-kl.de

Abstract

Following Buchberger's approach to computing a Gröbner basis of a polynomial ideal in polynomial rings, a completion procedure for finitely generated right ideals in $\mathbf{Z}[\mathcal{H}]$ is given, where $\mathcal{H}$ is an ordered monoid presented by a finite, convergent semi–Thue system (Σ, T). Taking a finite set $F \subseteq \mathbf{Z}[\mathcal{H}]$ we get a (possibly infinite) basis of the right ideal generated by F, such that using this basis we have unique normal forms for all $p \in \mathbf{Z}[\mathcal{H}]$ (especially the normal form is 0 in case p is an element of the right ideal generated by F). As the ordering and multiplication on $\mathcal{H}$ need not be compatible, reduction has to be defined carefully in order to make it Noetherian. Further we no longer have $p \cdot x \rightarrow_p 0$ for $p \in \mathbf{Z}[\mathcal{H}], x \in \mathcal{H}$. Similar to Buchberger's s–polynomials, confluence criteria are developed and a completion procedure is given. In case $T = \emptyset$ or (Σ, T) is a convergent, 2–monadic presentation of a group providing inverses of length 1 for the generators or (Σ, T) is a convergent presentation of a commutative monoid , termination can be shown. So in this cases finitely generated right ideals admit finite Gröbner bases. The connection to the subgroup problem is discussed.

1 Introduction

The theory of Gröbner bases for polynomial ideals in commutative polynomial rings over fields $K[x_1, \ldots, x_n]$ was introduced by Buchberger in 1965 [Bu85]. It established a rewriting approach to the theory of polynomial ideals. A Gröbner basis G is a generating set of a polynomial ideal such that every polynomial has a unique normal form using the polynomials in G as rules (especially the polynomials in the ideal reduce to zero). Buchberger gave a terminating procedure to transform a generating set of polynomials into a Gröbner basis of the same ideal. In case we have a finite Gröbner basis many algebraic questions concerning polynomial ideals become solvable, e.g. the membership problem or the congruence problem. Authors as Buchberger, Kandri–Rody, Kapur, Lauer, Stifter and Weispfenning extended this theory to other coefficient rings as the integers, Euclidean rings or regular rings [Bu83, Bu85, KaKa84, KaKa88, La76, St85, We87]. Recently there have been some attempts to expand these ideas to non–commutative polynomial rings, which are in general non–Noetherian. Take for example $\mathbf{Z}[\mathcal{H}]$ where $\mathcal{H}$ is the free monoid presented by $\Sigma = \{a, b, c\}, T = \emptyset$. Then the corresponding (right–, left–) ideals generated by $\{ab^ic - b^i \mid i \in \mathbf{N}\}$ do not have a finite basis. Authors as Mora, Baader, Kandri–Rody and Weispfenning have investigated the situation for special non–commutative polynomial rings, e.g. the ring $R\langle x_1, \ldots, x_n\rangle$, where R denotes a field in [Mo85] or the integers in [Ba89], and algebras of solvable type as introduced in [KaWe90] or skew polynomial rings as introduced in [We92]. They have shown that in these cases finitely generated right ideals (or even ideals) admit finite Gröbner bases. These approaches have in common that their orderings are monotone with respect to multiplication on the respective structure: if $t_1 > t_2$ then $t_1 \cdot x > t_2 \cdot x$. The results of Baader and Mora can be described using the ring $R[\mathcal{H}]$, where $\mathcal{H}$ is the free monoid presented by $\Sigma = \{x_1, \ldots, x_n\}, T = \emptyset$. The main idea of this paper is to generalize these approaches to monoid rings $R[\mathcal{H}]$, where $\mathcal{H}$ is an ordered monoid presented by a finite, convergent semi–Thue system (Σ, T).
In the next section the basic definitions of monoid rings $R[\mathcal{H}]$ and some examples are given. Section 3 discusses how polynomials can be used as rules. Different definitions of reduction together with their properties and (dis–)advantages are given. Since ordering and multiplication on $\mathcal{H}$ need not be monotone, one main lack of our reduction is that $p \cdot x$, where $p \in \mathbf{Z}[\mathcal{H}], x \in \mathcal{H}$, need not be reducible to zero by p. In section 4 the concept of saturation is introduced, which gives a solution to this problem. Section 5 gives an algorithmic approach to this concept. We end up with (possibly infinite) sets of polynomials, which allow us to reduce $p \cdot x$ to zero. Saturating sets in general are no Gröbner bases, i.e. the reduction induced by them need not be confluent. In section 6 a confluence test is developed using a concept similar to Buchberger's s–polynomials. A procedure is provided, which takes a finite set $F \subseteq \mathbf{Z}[\mathcal{H}]$ and produces a (possibly infinite) Gröbner basis of the right ideal generated by F, such that using this basis we have unique normal forms for all $p \in \mathbf{Z}[\mathcal{H}]$, and the normal form is 0 in case p belongs to the right ideal generated by F. The procedure can be shown to terminate in case $T = \emptyset$ or (Σ, T) is a convergent, 2–monadic presentation of a group providing inverses of length 1, so in this case finitely generated right ideals admit finite Gröbner bases, even if the monoid ring is non–Noetherian. The class of groups presented by

convergent, 2–monadic presentations providing inverses of length 1 (which is indeed the same as the class of groups presented by convergent, 2–monadic presentations, as shown in [AvMaOt86]) is the class of plain groups, i.e. free products of free and finitely many finite groups [MaOt89]. Further we give a short outline how this approach can be successfully applied to other special presentations (Σ, T) of $\mathcal{H}$, where T contains a commutative system for all letters in Σ. In this case all finitely generated ideals admit finite Gröbner bases. Finally a brief application to the subgroup problem is given, i.e. given a subgroup S of a group $\mathcal{G}$ and an element $g \in \mathcal{G}$, decide whether $g \in S$.

2 Basic Definitions

Let R be a ring and let $\mathcal{H}$ be a monoid. Then $R[\mathcal{H}]$ denotes the set of all mappings $f : \mathcal{H} \to R$ where the set $\{m \in \mathcal{H} \mid f(m) \neq 0\}$ is finite. Abbreviating $f(m)$ by $a_m \in R$ we can express f by the "polynomial" $f = \sum_{m \in \mathcal{H}} a_m \cdot m$. Further we define *addition* and *multiplication* in $R[\mathcal{H}]$ as follows: Let $f = \sum_{m \in \mathcal{H}} a_m \cdot m$ and $g = \sum_{m \in \mathcal{H}} b_m \cdot m$ denote two elements of $R[\mathcal{H}]$. Then the sum of f and g is denoted by $f+g$, where $(f+g)(m) = f(m) + g(m)$ or expressed in terms of polynomials $f + g = \sum_{m \in \mathcal{H}} (a_m + b_m) \cdot m$. The product of f and g is denoted by $f \cdot g$, where $(f \cdot g)(m) = \sum_{x \cdot y = m \in \mathcal{H}} f(x) \cdot g(y)$ or expressed in terms of polynomials $f \cdot g = \sum_{m \in \mathcal{H}} c_m \cdot m$ with $c_m = \sum_{x \cdot y = m \in \mathcal{H}} a_x \cdot b_y$. It easily can be seen that $R[\mathcal{H}]$ indeed is a ring [1] and we call $R[\mathcal{H}]$ the *monoid ring* of $\mathcal{H}$ over R, or in case $\mathcal{H}$ is a group the *group ring* of $\mathcal{H}$ over R.

Example 1

(a) Let $\mathcal{G}$ be a group. Then $\mathbf{Z}[\mathcal{G}]$ denotes the group ring of $\mathcal{G}$ over the integers $\mathbf{Z}$.

(b) Let $\mathcal{H} = \langle x \rangle$ be the free monoid with one generator. Then $R[\mathcal{H}]$ is isomorphic to the well–known polynomial ring in one indeterminate $R[x]$.

We will restrict our considerations to right ideals mainly. For a subset $F \subseteq R[\mathcal{H}]$ we call $ideal_r(F) = \{\sum_{i=1}^{n} c_i \cdot p_i \cdot m_i \mid n \in \mathbf{N}, c_i \in R, p_i \in F, m_i \in \mathcal{H}\}$ the *right ideal* generated by F and $ideal(F) = \{\sum_{i=1}^{n} c_i \cdot m_i \cdot p_i \cdot m_i' \mid n \in \mathbf{N}, c_i \in R, p_i \in F, m_i, m_i' \in \mathcal{H}\}$ the *ideal* generated by F. Two elements $f, g \in R[\mathcal{H}]$ are said to be *congruent modulo the* $ideal(F)$[2], (we write $f \equiv_{ideal(F)} g$) if $f = g+h$, where $h \in ideal(F)$, i.e. $f-g \in ideal(F)$.

As we are interested in methods of Gröbner basis calculations for right ideals in $R[\mathcal{H}]$, we need a presentation of our monoid $\mathcal{H}$. Every monoid $\mathcal{H}$ can be presented by a pair (Σ, T), where Σ is an alphabet and T a semi–Thue system over Σ. One only has to choose $\Sigma = \mathcal{H}$ and T the multiplication table of the monoid. Since this presentation might be infinite or even non–recursive, we are only interested in monoids, which allow "nice" presentations. Therefore, we will restrict ourselves to presentations, where Σ is finite and T is finite, confluent and Noetherian, i.e. each word in Σ^* has a unique normal form with respect to T. We will call such a confluent and Noetherian presentation

[1] All operations mainly involve the coefficients in the ring R.

[2] Similar for $ideal_r(F)$.

convergent. Then each word in Σ^* has a unique normal form and the monoid $\mathcal{H}$ is isomorphic to the set $IRR(T)$. The empty word $\lambda \in \Sigma^*$ presents the identity of $\mathcal{H}$. If $\cdot$ denotes the binary operation on $\mathcal{H}$, given $x, y \in \mathcal{H}$ we define $x \cdot y = (xy)\downarrow_T$, where $w\downarrow_T$ denotes the normal form of w with respect to T.

Example 2

(a) Let $\Sigma = \{x_1, \ldots, x_n\}$ and $T_c = \{x_i x_j \to x_j x_i \mid j < i,\ i, j \in \{1, \ldots n\}\}$. Then $\mathcal{H}$ is the free commutative monoid generated by Σ and $R[\mathcal{H}]$ is isomorphic to $R[x_1, \ldots x_n]$, the polynomial ring in n indeterminates .

(b) Let $\Sigma = \{x_1, \ldots, x_n, x_1^{-1}, \ldots x_n^{-1}\}$ and $T = \{x_i^{\delta} x_j^{\delta'} \to x_j^{\delta'} x_i^{\delta} \mid j < i,\ i, j \in \{1, \ldots n\},\ \delta, \delta' \in \{1, -1\}\} \cup \{x_i x_i^{-1} \to \lambda, x_i^{-1} x_i \to \lambda \mid i \in \{1, \ldots n\}\}$. Then $\mathcal{G}$ is the free commutative group generated by Σ.

Remark 1
If $\mathcal{H}$ is not cancellative, $\mathbf{Z}[\mathcal{H}]$ may have zero divisors. Take $\Sigma = \{a, b, c\}$ and $T = \{ab \to c, ac \to b\}$. Then $a^2 - \lambda, c \neq 0$ but $(a^2 - \lambda) \cdot c = c - c = 0$.

3 Right Reduction in $R[\mathcal{H}]$

Throughout this section let $\mathcal{H}$ be a monoid with a finite convergent presentation (Σ, T). In order to define a reduction in $R[\mathcal{H}]$ we have to use polynomials as rules. Therefore, we introduce an ordering on monomials and, as we are interested in Noetherian reductions, we need a well–founded ordering on the elements of $R[\mathcal{H}]$. If not stated otherwise our well–founded ordering on $\mathcal{H}$ is the ordering induced by the admissible, i.e. compatible with concatenation, well–founded total ordering on Σ^* used for orienting T, for example the length–lexicographic ordering in case T is monadic and convergent, in particular $w \succ \lambda$ for all $w \in \Sigma^* - \{\lambda\}$. We will take R to be $\mathbf{Z}$, the ring of the integers.

Definition 1
Let $\succ$ denote a well–founded total ordering on $\mathcal{H}$ and $>_Z$ a well–founded ordering on $\mathbf{Z}$.

(a) Let $p \in \mathbf{Z}[\mathcal{H}]$.
Arranging the $w_i \in \mathcal{H}$ with $p(w_i) \neq 0$ according to $\succ$ we get $w_1 \succ \ldots \succ w_n$, where $w_i \neq w_j$ for $i \neq j$. Using this ordering we write $p = \sum_{i=1}^{n} a_i \cdot w_i$, where $a_i = p(w_i)$. We let $HM(p) = a_1 \cdot w_1$ denote the *head monomial*, $HT(p) = w_1$ the *head term* and $HC(p) = a_1$ the *head coefficient* of p. $RED(p) = p - HM(p)$ stands for the *reductum* of p. $T(p) = \{w_1, \ldots, w_n\}$ is the set of terms occurring in p.

(b) Let $p = \sum_{i=1}^{n} a_i \cdot w_i, q = \sum_{j=1}^{m} b_j \cdot v_j \in \mathbf{Z}[\mathcal{H}]$.
p is *greater* than q, i.e. $p > q$, if

(i) $HT(p) \succ HT(q)$ or

(ii) $HT(p) = HT(q)$ and $HC(p) >_Z HC(q)$ or

(iii) $HM(p) = HM(q)$ and $RED(p) > RED(q)$.

Now we are able to use a polynomial $p \in \mathbf{Z}[\mathcal{H}]$ as a rewriting rule by splitting it into $HM(p) \to -RED(p)$ and $HM(p) > -RED(p)$.
The following remark shows that in general a monotone ordering $\succ$ on $\mathcal{H}$ or $\mathcal{G}$ will not be well–founded.

Remark 2
Let $\mathcal{G} \neq \{1\}$ be a group [3] with a monotone ordering $\succ$.

1. $\mathcal{G}$ cannot contain an element of finite order $g \neq 1$.
   Suppose $g \in \mathcal{G} - \{1\}$ is of finite order, i.e. there is $n \in \mathbf{N}$ minimal such that $g^n = 1$. Without loss of generality let us assume $g \succ 1$. Then (as $\succ$ is monotone and transitive) we get $g^{n-1} \succ 1$ giving us $1 \succ g$, contradicting our assumption.

2. The ordering $\succ$ is not well–founded.
   Without loss of generality let us assume $g \succ 1$ for some $g \in \mathcal{G} - \{1\}$. Then (as $\succ$ is monotone) we have $1 \succ g^{-1}$ and (as $\succ$ is transitive) $g \succ 1 \succ g^{-1} \succ \ldots \succ g^{-n}$ for all $n \in \mathbf{N}$ [4].

Remark 3
We now will specify a total well–founded ordering on $\mathbf{Z}$ [5]:

$$a <_Z b \text{ iff } \begin{cases} a \geq 0 \text{ and } b < 0 \\ a \geq 0, b > 0 \text{ and } a < b \\ a < 0, b < 0 \text{ and } a > b \end{cases}$$

and $a \leq_Z b$ iff $a = b$ or $a <_Z b$.
Let $c \in \mathbf{N}$. We call the positive numbers $0, \ldots, c-1$ the remainders of c. Then for each $d \in \mathbf{Z}$ there are unique $a, b \in \mathbf{Z}$ such that $d = a \cdot c + b$ and b is a remainder of c. We get $b < c$ and in case $d > 0$ and $a \neq 0$ even $c \leq d$. Further c does not divide $b_1 - b_2$, if b_1, b_2 are different remainders of c.

In defining appropriate reductions in $\mathbf{Z}[\mathcal{H}]$ we have to be more cautious than in defining reductions in the polynomial ring $K[x_1, \ldots, x_n]$ (compare [Bu85]). We will give four possible definitions together with their advantages and disadvantages.

Definition 2 (Strong right reduction)
Let $p = \sum_{i=1}^{n} a_i \cdot w_i, g = \sum_{j=1}^{m} b_j \cdot v_j \in \mathbf{Z}[\mathcal{H}]$.
We say *g strongly right reduces p* to q at $a_k \cdot w_k$ in one step, i.e. $p \to_g^s q$, if

[3] The second remark is likewise true for any monoid $\mathcal{H}$ having elements of infinite order $h, h^{-1} \in \mathcal{H} - \{\lambda\}$ satisfying $h \cdot h^{-1} = 1$.

[4] As all $g \in \mathcal{G} - \{1\}$ have infinite order.

[5] If not stated otherwise $<$ is the usual ordering on $\mathbf{Z}$.

1. $HT(g \cdot x) = w_k$ for some $x \in \mathcal{H}$.
2. $HC(g \cdot x) > 0$ and $a_k = a \cdot HC(g \cdot x) + b$ for $a, b \in \mathbf{Z}$,$a \neq 0$, b a remainder of $HC(g \cdot x)$.
3. $q = p - a \cdot g \cdot x$.

We write $p \rightarrow_g^s$ if there is a polynomial q as defined above.
We can define $\stackrel{*}{\rightarrow}^s$, $\stackrel{+}{\rightarrow}^s$, $\stackrel{n}{\rightarrow}^s$ and strong right reduction by a set $F \subseteq \mathbf{Z}[\mathcal{H}]$ as usual.

Definition 3 (Right reduction)
Let $p = \sum_{i=1}^{n} a_i \cdot w_i, g = \sum_{j=1}^{m} b_j \cdot v_j \in \mathbf{Z}[\mathcal{H}]$.
We say g *right reduces* p to q at $a_k \cdot w_k$ in one step, i.e. $p \rightarrow_g^r q$, if

(a) $HT(g \cdot x) = v_1 \cdot x = w_k$ for some $x \in \mathcal{H}$.

(b) $HC(g \cdot x) > 0$ and $a_k = a \cdot HC(g \cdot x) + b$ for $a, b \in \mathbf{Z}$, $a \neq 0$, b a remainder of $HC(g \cdot x)$.

(c) $q = p - a \cdot g \cdot x$.

We write $p \rightarrow_g^r$ if there is a polynomial q as defined above.
We can define $\stackrel{*}{\rightarrow}^r$, $\stackrel{+}{\rightarrow}^r$, $\stackrel{n}{\rightarrow}^r$ and right reduction by a set $F \subseteq \mathbf{Z}[\mathcal{H}]$ as usual.

In order to decide, whether a polynomial g (strongly) right reduces a polynomial p at a monomial $a_k \cdot w_k$, the equation in (a) in the above definitions must be solvable in (Σ, T). Note that if this is possible, there can be no, one or even (infinitely) many solutions depending on $\mathcal{H}$. For example if $\mathcal{H}$ is a group there is always $x \in \mathcal{H}$ such that $u \cdot x = v$ for $u, v \in \mathcal{H}$, namely $x = u^{-1} \cdot v$. In case $\mathcal{H}$ is left–cancellative we have at most one solution. In case $\mathcal{H}$ is right–cancellative we know $HC(g \cdot x) = HC(g)$.

Example 3

1. Let $\Sigma = \{a, b, c\}$ with $a \succ b \succ c$ and $T = \{ab \rightarrow a, cb \rightarrow a\}$. Then $p = b^2$ is not right reducible by $g = a + b - c$, as $b^2 \neq a \cdot x$ for all $x \in \mathcal{H}$. On the other hand $p = a + c$ is right reducible by $g = 2a - c + \lambda$, as $g \cdot b = a + b$ and $HT(g \cdot b) = a \cdot b = a$.
2. The following phenomena can occur: $p \cdot x = q$ and $p \cdot y = k \cdot q$ for some $p, q \in \mathbf{Z}[\mathcal{H}], x, y \in \mathcal{H}, k \in \mathbf{Z}$. Let $\Sigma = \{a, b, c, d, e\}$ and $T = \{ad \rightarrow a, bd \rightarrow b^2, cd \rightarrow a, ae \rightarrow a, be \rightarrow b^2, ce \rightarrow b^2\}$. Take $p = -2a + b + c$, then $p \cdot d = -b^2 + a$ and $p \cdot e = 2b^2 - 2a$.

Note that we use $HM(g \cdot x) \rightarrow -RED(g \cdot x)$ as a rule only in case $HC(g \cdot x) > 0$ and additionly $HT(g \cdot x) = HT(g) \cdot x$ when talking of right reduction. We do not use $HM(g) \rightarrow -RED(g)$, since then $\rightarrow^r$ would no longer be Noetherian, i.e. infinite reduction sequences could arise. This is due to the unfortunate fact that our ordering $\succ$ on $\mathcal{H}$ is not necessarily monotone in the sense that $m_1 \succ m_2$ does not imply $m_1 \cdot x \succ m_2 \cdot x$.

Example 4
Let $\Sigma = \{x, x^{-1}\}$, $x^{-1} \succ x$ and $T = \{xx^{-1} \to \lambda, x^{-1}x \to \lambda\}$ be a presentation of the free group generated by $\{x\}$. If we use $HM(g) \to -RED(g)$ as a rule in definition 3 we can right reduce $x^2 + 1$ by $x^{-1} + x$ in the following manner:

$$x^2 + 1 \to^r_{x^{-1}+x} x^2 + 1 - (x^{-1} + x) \cdot x^3 = -x^4 + 1$$

and $-x^4+1$ likewise is right reducible by $x^{-1}+x$ causing an infinite reduction sequence.

Definition 4 (Prefix right reduction)
Let $p = \sum_{i=1}^n a_i \cdot w_i, g = \sum_{j=1}^m b_j \cdot v_j \in \mathbf{Z}[\mathcal{H}]$.
We say g *prefix right reduces* p to q at $a_k \cdot w_k$ in one step, i.e. $p \to^p_g q$, if

(a) $v_1 x = w_k$ for some $x \in \mathcal{H}$, i.e. v_1 is a prefix of w_k.

(b) $b_1 > 0$ and $a_k = a \cdot b_1 + b$ for $a, b \in \mathbf{Z}$, $a \neq 0$, b a remainder of b_1.

(c) $q = p - a \cdot g \cdot x$.

We write $p \to^p_g$ if there is a polynomial q as defined above.
We can define $\stackrel{*}{\to}^p$, $\stackrel{+}{\to}^p$, $\stackrel{n}{\to}^p$ and prefix right reduction by a set $F \subseteq \mathbf{Z}[\mathcal{H}]$ as usual.

Notice that in this case (a) has at most one solution and we always have $HC(g \cdot x) = HC(g)$.

If $T = T' \cup T_c$, where $T_c = \{ab \to ba \mid a \succ b, a, b \in \Sigma\}$, we can define commutative reduction by using $\circ$ as the multiplication in the free commutative semigroup generated by Σ, i.e. $u \circ v = (uv)\downarrow_{T_c}$. Note that commutative reduction is in fact the usual reduction in polynomial rings (see e.g. [Bu85]).

Definition 5 (Commutative reduction)
Let $p = \sum_{i=1}^n a_i \cdot w_i, g = \sum_{j=1}^m b_j \cdot v_j \in \mathbf{Z}[\mathcal{H}]$.
We say g *commutatively reduces* p to q at $a_k \cdot w_k$ in one step, i.e. $p \to^c_g q$, if

1. $v_1 \circ x = w_k$ for some $x \in \mathcal{H}$.
2. $b_1 > 0$ and $a_k = a \cdot b_1 + b$ for $a, b \in \mathbf{Z}$, $a \neq 0$, b a remainder of b_1.
3. $q = p - a \cdot g \cdot x$.

We write $p \to^c_g$ if there is a polynomial q as defined above.
We can define $\stackrel{*}{\to}^c$, $\stackrel{+}{\to}^c$, $\stackrel{n}{\to}^c$ and commutative reduction by a set $F \subseteq \mathbf{Z}[\mathcal{H}]$ as usual.

As the "multiplication" used for reduction in definition 4 and 5 is compatible with the ordering on $\mathcal{H}$ [6] we always have $HC(g \cdot x) = HC(g)$. We now can use $HM(g) \to$

[6] We get $HM(g \cdot x) = HC(g) \cdot HT(g)x > RED(g) \cdot x = RED(g \cdot x)$ respectively $HM(g \cdot x) = HC(g) \cdot HT(g) \circ x > RED(g) \cdot x = RED(g \cdot x)$.

$-RED(g)$ as a rule in case $b_1 > 0$ and $w_k = HT(g)x$ respectively $w_k = HT(g) \circ x$. Without this trick of using a restricted multiplication on $\mathcal{H}$ it is very hard to say how a polynomial will "behave".
Looking for properties of our reductions we immediately get $\rightarrow_g^p \subseteq \rightarrow_g^r \subseteq \rightarrow_g^s$ and $\rightarrow_g^c \subseteq \rightarrow_g^r \subseteq \rightarrow_g^s$.

Lemma 1
Let $F \subseteq \mathbf{Z}[\mathcal{H}]$. Then the following statements hold for all four definitions of reduction:

(1) For all $p, q \in \mathbf{Z}[\mathcal{H}]$, $p \rightarrow_F q$ implies $p > q$.

(2) $\rightarrow_F$ is Noetherian.

(3) $p \rightarrow_q 0$ and $q \rightarrow_w 0$ imply $p \rightarrow_{\{w,-w\}} 0$.

Proof :

1. This follows from the fact that using a polynomial f together with $a \in \mathbf{Z}, x \in \mathcal{H}$ for reduction we use $a \cdot HM(f \cdot x) \rightarrow -a \cdot RED(f \cdot x)$ as a rule and $HM(f \cdot x) > -RED(f \cdot x)$.

2. This follows from (1), as the ordering $>$ on $\mathbf{Z}[\mathcal{H}]$ is well–founded.

3. $p \rightarrow_q 0$ implies $p = a \cdot q \cdot x$ for some $a \in \mathbf{Z}, x \in \mathcal{H}$, $HC(q \cdot x) > 0$, and $q \rightarrow_w 0$ implies $q = b \cdot w \cdot y$ for some $b \in \mathbf{Z}, y \in \mathcal{H}$, $HC(w \cdot y) > 0$.
   In case we use strong right reduction we immediately get $p \rightarrow_{\{w,-w\}}^s 0$, as $p = a \cdot b \cdot w \cdot y \cdot x$ and $HT(w \cdot (y \cdot x)) = HT(p)$.
   In the other cases we have $HT(p) = HT(q) \cdot x$ (respectively $HT(p) = HT(q)x$ or $HT(p) = HT(q) \circ x$) as well as $HT(q) = HT(w) \cdot y$ (respectively $HT(q) = HT(w)y$ or $HT(q) = HT(w) \circ y$). Further $HT(w \cdot (y \cdot x)) = HT(w) \cdot (y \cdot x)$ (respectively $HT(w \cdot (y \cdot x)) = HT(w)yx$ or $HT(w \cdot (y \cdot x)) = HT(w) \circ yx$) gives us that p is right reducible to zero by w or $-w$ [7], respectively prefix right or commutative reducible to zero by w. q.e.d.

Unfortunately, reduction as defined above does lack some of the nice properties belonging to reduction in general, as e.g. $p \cdot x \rightarrow_p 0$ or transitivity in the sense that $p \rightarrow_q$ and $q \rightarrow_w q_1$ imply $p \rightarrow_w$ or $p \rightarrow_{q_1}$.

Remark 4

1. Looking at strong right reduction as defined in definition 2 we get

   (a) We do not have $p \cdot x \rightarrow_p^s 0$, but $p \cdot x \rightarrow_{\{p,-p\}}^s 0$ for $p \in \mathbf{Z}[\mathcal{H}], x \in \mathcal{H}$.

[7] In case $\mathcal{H}$ is right–cancellative, we can even restrict ourselves to reduction with w.

(b) Strong right reduction is not transitive.
Let $\Sigma = \{a, b, c\}$ with $a \succ b \succ c$ and $T = \{a^2 \to \lambda, b^2 \to \lambda, c^2 \to \lambda\}$ be the presentation of a group.
Looking at $p = ba+b, q = bc+\lambda$ and $w = ac+b$ we get $p \to^s_q p-q\cdot ca = -ca+b$ and $q \to^s_w q - w \cdot c = -a + \lambda =: q_1$.
Further p is neither strongly right reducible at ba by w or q_1, as $w\cdot a = aca + ba, w\cdot caba = ba+bcaba$ and $q_1\cdot aba = -ba+aba, q_1\cdot ba = -aba+ba$ all violate condition (a) of definition 2, nor at b, as $w \cdot cab = b + bcab, q_1 \cdot ab = -b + a$ and $q_1 \cdot b = -ab + b$.

2. Looking at right reduction as defined in definition 3 we get

(a) We no longer have $p \cdot x \xrightarrow{*}{}^r_p 0$ for $p \in \mathbf{Z}[\mathcal{H}], x \in \mathcal{H}$, not even $p \cdot x \to^r_{\{p,-p\}} 0$.
Taking $\mathcal{H}$ to be the free group generated by $\Sigma = \{x\}$ we find that $(x^{-1} + x) \cdot x = x^2 + 1$ is not right reducible by $x^{-1} + x$. (Compare example 4)

(b) Right reduction is not transitive.
Let $\Sigma = \{a, b, c\}$ with $a \succ b \succ c$ and $T = \{a^2 \to \lambda, b^2 \to \lambda, ab \to c, ac \to b, cb \to a\}$ be the presentation of a group.
Looking at $p = ba+b, q = a+\lambda$ and $w = c^2+b$ we get $p \to^r_q p-q\cdot ca = -ca+b$ and $q \to^r_w q - w \cdot bc = -c + \lambda =: q_1$.
Further p is neither right reducible at ba by w or q_1, as $w \cdot bc^2a = ba + c^2a$ and $q_1 \cdot bca = -ba + bca$ both violate condition (a) of definition 3, nor at b, as $w \cdot bc^2 = b + c^2$ and $q_1 \cdot bc = -b + bc$.

3. Looking at prefix right reduction as defined in definition 4 we get

(a) We no longer have $p \cdot x \xrightarrow{*}{}^p_p 0$ for $p \in \mathbf{Z}[\mathcal{H}], x \in \mathcal{H}$, not even $p \cdot x \to^p_{\{p,-p\}} 0$.
Taking $\mathcal{H}$ to be the free group generated by $\Sigma = \{x\}$ we find that $(x^{-2} + \lambda) \cdot x = x^{-1} + x$ is not prefix right reducible by $x^{-2} + \lambda$.

(b) Prefix right reduction is transitive.
Let $p \to^p_q$ and $q \to^p_w q_1$. In case $HM(q) = HM(q_1)$ we immediately get $p \to^p_{q_1}$.
Otherwise $HT(q) = HT(w)y$, for some $y \in \mathcal{H}$, and $0 < HC(w) \leq HC(q)$ together imply $p \to^p_w$.

4. Looking at commutative right reduction as defined in definition 5 we get

(a) We no longer have $p \cdot x \xrightarrow{*}{}^c_p 0$ for $p \in \mathbf{Z}[\mathcal{H}], x \in \mathcal{H}$, not even $p \cdot x \to^p_{\{p,-p\}} 0$.
Taking $\mathcal{H}$ to be generated by $\Sigma = \{a, b\}$, $T = \{ab \to ba, a^2 \to \lambda\}$ we find that $(ba + a) \cdot a = b + \lambda$ is not commutatively right reducible by $ba + a$.

(b) Commutative right reduction is transitive.
Let $p \to^c_q$ and $q \to^c_w q_1$. In case $HM(q) = HM(q_1)$ we immediately get $p \to^c_{q_1}$.
Otherwise $HT(q) = HT(w) \circ y$, for some $y \in \mathcal{H}$, and $0 < HC(w) \leq HC(q)$ together imply $p \to^c_w$.

The following lemmata are true for all four reductions.

Lemma 2
Let $F \subseteq \mathbf{Z}[\mathcal{H}], p, q, h \in \mathbf{Z}[\mathcal{H}]$. Then $p \overset{*}{\leftrightarrow}_F q$ implies $p + h \overset{*}{\leftrightarrow}_F q + h$.

Proof : Using induction on k we show that $p \overset{k}{\leftrightarrow}_F q$ implies $p + h \overset{*}{\leftrightarrow}_F q + h$.
In the base case $k = 0$ there is nothing to show.
Assuming $p \overset{k}{\leftrightarrow}_F p_k \leftrightarrow_F q$ and $p + h \overset{*}{\leftrightarrow}_F p_k + h$ we can distinguish two cases:

1. $p_k \rightarrow_f q$ for some $f \in F$ and $q = p_k - a \cdot f \cdot x$, where $a \in \mathbf{Z}, x \in \mathcal{H}$.
   In case $p_k + h \rightarrow_f p_k + h - a \cdot f \cdot x = q + h$ there is nothing to show.
   Suppose this is not true.
   Let $HT(f \cdot x) = t, HC(f \cdot x) = c > 0$ and a_i respectively b_i be the coefficients of t in p_k respectively h [8]. Further let $a_i = a \cdot c + b$, where b is a remainder of c. Then b is the coefficient of t in q. We know that $a_i + b_i \neq a \cdot c + d$ for all remainders d of c [9].
   Now we have to distinguish two cases:

   (a) $a_i + b_i$ is a remainder of c.
   Then looking at the coefficient of t in $q + h$ we get $b + b_i = a_i - a \cdot c + b_i$ and since $a_i + b_i$ is a remainder of c, we have $q + h \rightarrow_f q + h - (-a) \cdot f \cdot x = p_k + h$, hence $p + h \overset{*}{\leftrightarrow}_F q + h$.

   (b) $a_i + b_i = a' \cdot c + b'$, where b' is a remainder of c and $a \neq a'$.
   Since $a_i + b_i$ is the coefficient of t in $p_k + h$ we get $p_k + h \rightarrow_f p_k + h - a' \cdot f \cdot x$. Looking at the coefficient of t in $q + h$ we get $b + b_i = b + a' \cdot c + b' - a_i = b + a' \cdot c + b' - a \cdot c - b = (a' - a) \cdot c + b'$. Since $a \neq a'$ and b' is a remainder of c we have $q + h \rightarrow_f q + h - (a' - a) \cdot f \cdot x = p_k - a \cdot f \cdot x + h - a' \cdot f \cdot x + a \cdot f \cdot x = p_k + h - a' \cdot f \cdot x$, hence $p + h \overset{*}{\leftrightarrow}_F q + h$.

2. $q \rightarrow_f p_k$ can be treated analogously. q.e.d.

Lemma 3
Let $F \subseteq \mathbf{Z}[\mathcal{H}], p, q, h \in \mathbf{Z}[\mathcal{H}]$. Let $p - q \rightarrow_F h$, where the reduction takes place at the monomial $d \cdot t$ and let $t \notin T(h)$. Then there are $p', q' \in \mathbf{Z}[\mathcal{H}]$ such that $p \overset{*}{\rightarrow}_F p', q \overset{*}{\rightarrow}_F q'$ and $h = p' - q'$.

Proof : Let $p - q \rightarrow_F h = p - q - a \cdot f \cdot x$, where $a \in \mathbf{Z}, f \in F, x \in \mathcal{H}$ and $HT(f \cdot x) = t$. Let $HC(f \cdot x) = c > 0$ and d be the coefficient of t in $p - q$. As $t \notin T(h)$ we know $d = a \cdot c$. Let c_1 respectively c_2 be the coefficients of t in p respectively q and $c_1 = a_1 \cdot c + b_1, c_2 = a_2 \cdot c + b_2$, for some $a_1, a_2, b_1, b_2 \in \mathbf{Z}$, where b_1, b_2 are remainders of c.
Then $a \cdot c = c_1 - c_2 = (a_1 - a_2) \cdot c + b_1 - b_2$, and as $b_1 - b_2$ is no multiple of c we get $b_1 - b_2 = 0$ and $a_1 - a_2 = a$.
We have to distinguish two cases:

[8] Using the different reductions we even get additional information, as $HT(f) \cdot x = t$ or $HT(f)x = t$ or $HT(f) \circ x = t$, which is not needed, since the proof only uses reduction applying f together with x. This is likewise true for lemma 3, 4 and 5.

[9] Otherwise we immediately would get $p_k + h \rightarrow_f p_k + h - a \cdot f \cdot x = q + h$.

1. $a_1 \neq 0$ and $a_2 \neq 0$.
   Then $p \rightarrow_F p - a_1 \cdot f \cdot x =: p', q \rightarrow_F q - a_2 \cdot f \cdot x =: q'$ and $p' - q' = p - a_1 \cdot f \cdot x - q + a_2 \cdot f \cdot x = p - q - a \cdot f \cdot x = h$.

2. $a_1 = 0$ and $a_2 = -a$ (the case $a_1 = a$ and $a_2 = 0$ is similar).
   Then $p' := p, q \rightarrow_F q - a_2 \cdot f \cdot x = q + a \cdot f \cdot x =: q'$ and $p' - q' = p - q - a \cdot f \cdot x = h$.

q.e.d.

Lemma 4
Let $F \subseteq \mathbf{Z}[\mathcal{H}], 0 \neq p \in \mathbf{Z}[\mathcal{H}]$. Let 0 be the unique normal form (using the corresponding reduction) of p with respect to F, and $t = HT(p)$. Then there is a polynomial $f \in F$ such that $p \rightarrow_f p'$ and $t \notin T(p')$.

Proof : Since $p \xrightarrow{*}_F 0$, $HM(p) = c \cdot t$ is F–reducible. Let $f_{i_1}, \ldots, f_{i_k} \in F$ be all polynomials in F, which can be used to reduce $c \cdot t$. Let $a = min_{1 \leq j \leq k}\{HC(f_{i_j} \cdot x) \mid HT(f_{i_j} \cdot x) = t, x \in \mathcal{H}\}$ and $f \in \{f_{i_1}, \ldots, f_{i_k}\}$ a polynomial corresponding to a, i.e. there is $x \in \mathcal{H}$ such that $HT(f \cdot x) = t$ and $HC(f \cdot x) = a$.
Then $p \rightarrow_f p - d \cdot f \cdot x =: p'$, $d \in \mathbf{Z}$ and $p' \xrightarrow{*}_F 0$, as 0 is the unique normal form of p.
Suppose $HT(p') = t$. Then together with our definitions of reductions we have $0 < HC(p') < a$ and, therefore, $HM(p')$ is not F–reducible, contradicting $p' \xrightarrow{*}_F 0$. q.e.d.

Lemma 5
Let $F \subseteq \mathbf{Z}[\mathcal{H}], p, q \in \mathbf{Z}[\mathcal{H}]$. Let 0 be the unique normal form (using the corresponding reduction) of $p - q$ with respect to F. Then there exists a polynomial $g \in \mathbf{Z}[\mathcal{H}]$ such that $p \xrightarrow{*}_F g$ and $q \xrightarrow{*}_F g$.

Proof : Since 0 is the unique normal form of $p - q$ with respect to F, lemma 4 provides us with the existence of a reduction sequence $p - q \rightarrow_{f_{i_1}} h_1 = p - q - a_{i_1} \cdot f_{i_1} \cdot x_{i_1} \rightarrow_{f_{i_2}} h_2 \rightarrow_{f_{i_3}} \ldots \rightarrow_{f_{i_k}} 0$ such that $h_j = h_{j-1} - a_{i_j} \cdot f_{i_j} \cdot x_{i_j}$ and $HT(f_{i_j} \cdot x_{i_j}) \notin T(h_j)$.
We show our claim by induction on k, where $p - q \xrightarrow{k}_F 0$ is such a reduction sequence.
In the base case $k = 0$ there is nothing to show.
Let $p - q \rightarrow_F h \xrightarrow{k}_F 0$.
Then by lemma 3 there are $p', q' \in \mathbf{Z}[\mathcal{H}]$ such that $p \xrightarrow{*}_F p', q \xrightarrow{*}_F q'$ and $h = p' - q'$.
Now the induction hypothesis for $p' - q' \xrightarrow{k}_F 0$ yields the existence of $g \in \mathbf{Z}[\mathcal{H}]$ such that $p \xrightarrow{*}_F p' \xrightarrow{*}_F g$ and $q \xrightarrow{*}_F q' \xrightarrow{*}_F g$. q.e.d.

Unfortunately, the reflexive, symmetric and transitive closures of our reductions only capture the right ideal congruence relation in case we take strong right reduction and sets $F \subseteq \mathbf{Z}[\mathcal{H}]$ such that $f \in F$ implies $-f \in F$ [10].

[10] This condition is sufficient for the lemma, but not necessary, as we only need $-f$ in case there is some $x \in \mathcal{H}$ such that $HC(f \cdot x) < 0$. Then taking $-f$ into account corresponds to the process of saturating f, which will be introduced in the next section.

Lemma 6
Let $p, q \in \mathbf{Z}[\mathcal{H}]$ and $F \subseteq \mathbf{Z}[\mathcal{H}]$.

1. *$p \overset{*}{\leftrightarrow}^{s}_{F} q$ if and only if $p - q \in ideal_r(F)$ (assuming $f \in F$ implies $-f \in F$ [11]).*
2. *$p \overset{*}{\leftrightarrow}^{(r,p,c)}_{F} q$ implies $p - q \in ideal_r(F)$ but not vice versa.*

Proof :

1. (a) Using induction on k we show that $p \overset{k}{\leftrightarrow}^{s}_{F} q$ implies $p - q \in ideal_r(F)$.
   In the base case $k = 0$ there is nothing to show, since $p - p = 0 \in ideal_r(F)$.
   Let us assume that $p \overset{k}{\leftrightarrow}^{s}_{F} q$ implies $p - q \in ideal_r(F)$.
   Looking at $p \overset{k}{\leftrightarrow}^{s}_{F} p_k \leftrightarrow^{s}_{F} q$ we can distinguish two cases:
   i. $p_k \rightarrow^{s}_{f} q$ with $f \in F$.
   Then $q = p_k - a \cdot f \cdot x$, where $a \in \mathbf{Z}, x \in \mathcal{H}$ and since $p - q = p - p_k + a \cdot f \cdot x$ and $p - p_k \in ideal_r(F)$, we get $p - q \in ideal_r(F)$.
   ii. $q \rightarrow^{s}_{f} p_k$ with $f \in F$ can be treated similarly.

   (b) In case $p - q \in ideal_r(F)$ we get $p = q + \sum_{j=1}^{m} a_j \cdot f_j \cdot x_j$, where $a_j \in \mathbf{Z}, f_j \in F, x_j \in \mathcal{H}$.
   We can show $p \overset{*}{\leftrightarrow}^{s}_{F} q$ by induction on m.
   In the base case $m = 0$ there is nothing to show.
   Let $p = q + \sum_{j=1}^{m} a_j \cdot f_j \cdot x_j + a_{m+1} \cdot f_{m+1} \cdot x_{m+1}$ and by induction hypothesis $p \overset{*}{\leftrightarrow}^{s}_{F} q + a_{m+1} \cdot f_{m+1} \cdot x_{m+1}$.
   In case $q + a_{m+1} \cdot f_{m+1} \cdot x_{m+1} \rightarrow^{s}_{\{f_{m+1}, -f_{m+1}\}} q$ we are done.
   Now suppose this is not true.
   Let $HT(f_{m+1} \cdot x_{m+1}) = t$ and without loss of generality $HC(f_{m+1} \cdot x_{m+1}) = c > 0$. Let a be the coefficient of t in q. Then a is no remainder of c [12], i.e. $a = a' \cdot c + b'$,$a', b' \in \mathbf{Z}$, where b' is a remainder of c and $a' \neq 0$. We get $a + a_{m+1} \cdot c = (a' + a_{m+1}) \cdot c + b'$.
   In case $a' + a_{m+1} = 0$ we get $q \rightarrow^{s}_{f_{m+1}} q - a' \cdot f_{m+1} \cdot x_{m+1} = q + a_{m+1} \cdot f_{m+1} \cdot x_{m+1} \overset{*}{\leftrightarrow}^{s}_{F} p$ implying $p \overset{*}{\leftrightarrow}^{s}_{F} q$ [13].
   In case $a' + a_{m+1} \neq 0$ we get $p \overset{*}{\leftrightarrow}^{s}_{F} q + a_{m+1} \cdot f_{m+1} \cdot x_{m+1} \rightarrow^{s}_{f_{m+1}} q + a_{m+1} \cdot f_{m+1} \cdot x_{m+1} - (a' + a_{m+1}) \cdot f_{m+1} \cdot x_{m+1} = q - a' \cdot f_{m+1} \cdot x_{m+1} \overset{*}{\leftrightarrow}^{s}_{F} q$ since $q \rightarrow^{s}_{f_{m+1}} q - a' \cdot f_{m+1} \cdot x_{m+1}$, giving us $p \overset{*}{\leftrightarrow}^{s}_{F} q$.

2. The proof of the first claim is similar.
   To show that $p - q \in ideal_r(F)$ in general does not imply $p \overset{*}{\leftrightarrow}^{(r,p)}_{F} q$ let us look at the following example:

[11] Note that this additional information is necessary because of our handling of the coefficients in $\mathbf{Z}$ in our definition of strong right reduction. In case the coefficient domain is a field or the elements of $\mathbf{Z}$ are treated in another way, this is no longer necessary.

[12] Otherwise we would immediately get $q + a_{m+1} \cdot f_{m+1} \cdot x_{m+1} \rightarrow^{s}_{f_{m+1}} q$.

[13] Note that this cannot always be done in case we use the other reductions since we do not necessarily have $HT(f_{m+1} \cdot x_{m+1}) = HT(f_{m+1}) \cdot x_{m+1}$ respectively $HT(f_{m+1}) x_{m+1}$ or $HT(f_{m+1}) \circ x_{m+1}$.

Let $\Sigma = \{a, b, c\}$ with $a \succ b \succ c$ and $T = \{a^2 \to \lambda, b^2 \to \lambda, ab \to c, ac \to b, cb \to a\}$.
Taking $p = a + b + c, q = b - \lambda$ and $F = \{a + b + c\}$ we get $p - q = a + c + \lambda = (a + b + c) \cdot b \in ideal_r(F)$ but $a + b + c \not\overset{*}{\leftrightarrow}_F^{(r,p)} b - \lambda$.
Suppose $a + b + c \overset{*}{\leftrightarrow}_F^r b - \lambda$.
Since $a+b+c \to_F^r 0$, we get $b-\lambda \overset{*}{\leftrightarrow}_F^r 0$. Let $n \in \mathbf{N}$ be minimal such that $b-\lambda \overset{n}{\leftrightarrow}_F^r 0$. As $b - \lambda \not\to_F^r 0$ we know $n > 1$.
Let $b - \lambda =: p_0 \leftrightarrow_F^r p_1 \leftrightarrow_F^r \ldots \leftrightarrow_F^r p_{n-1} \leftrightarrow_F^r 0$, where for all $1 \leq i \leq n-1$, $p_i = p_{i-1} + c_i \cdot (a+b+c) \cdot x_i$, for $c_i \in \mathbf{Z}, x_i \in \mathcal{H}$ and $HT((a+b+c) \cdot x_i) = a \cdot x_i$. Further let $t = max\{HT(p_i) \mid 1 \leq i \leq n-1\}$, then $t > b$, as $HT((a + b + c) \cdot x) > b$ for all $x \in \mathcal{H}$.
Let p_l be the first polynomial, with $HT(p_l) = t$, i.e. $HT(p_j) < t$ for all $j < l$, and let p_{l+k} be the next polynomial, where the coefficient of t differs from $HC(p_l) = c_l$ [14].
Since $HT((a+b+c) \cdot x_{l+k}) = a \cdot x_{l+k} = t = a \cdot x_l = HT((a+b+c) \cdot x_l)$ and (Σ, T) presents a group, we get $x_{l+k} = x_l$. Substituting p_l by $p'_l = p_l + c_{l+k} \cdot (a+b+c) \cdot x_l$, p_{l+j} by $p'_{l+j} = p_{l+j} + c_{l+k} \cdot (a + b + c) \cdot x_l$ for $1 \leq j < k$ and deleting p_{l+k} we get a shorter sequence $b - \lambda \overset{n-1}{\leftrightarrow}_F^r 0$ contradicting our assumption. q.e.d.

The key idea behind weakening reduction is that if $\to^1 \subseteq \to^2$ and $\overset{*}{\leftrightarrow}^1 = \overset{*}{\leftrightarrow}^2$, the confluence of $\to^1$ implies the confluence of $\to^2$. Unfortunately the reflexive, symmetric and transitive closure of (prefix, commutative) right reduction via a set of polynomials, which are weaker than strong reduction, need not capture the congruence induced by the right ideal generated by these polynomials, i.e. do not describe the same congruence as the reflexive, symmetric and transitive closure of strong reduction. The solution to this problem will be given by enriching the set of polynomials used for reduction in order to achieve this property. This will be done in section 4
Next we define Gröbner bases.

Definition 6
A set $G \subseteq \mathbf{Z}[\mathcal{H}]$ is called a *Gröbner basis* of a (right, left) ideal generated by a set $F \subseteq \mathbf{Z}[\mathcal{H}]$ with respect to a reduction $\to$, if

(i) $\overset{*}{\leftrightarrow}_G = \equiv_{ideal_{(l,r)}(F)}$

(ii) $\overset{*}{\to}_G$ is confluent.

Note that if $\to^1 \subseteq \to^2$ and $\overset{*}{\leftrightarrow}_F^1 = \overset{*}{\leftrightarrow}_F^2 = \equiv_{ideal_{(l,r)}(F)}$, then a Gröbner basis G with respect to $\to^1$ is also a Gröbner basis with respect to $\to^2$.

[14] Note that the coefficient of t in p_{l+k} is $c_l + c_{l+k}$ and can be zero.

4 Saturation of a Polynomial $p \in \mathbf{Z}[\mathcal{H}]$

As stated in the previous section, reduction as defined in the definitions 2, 3, 4 and 5 does not have the property $p \cdot x \xrightarrow{*}_{p}^{(s,r,p,c)} 0$ and the reflexive, symmetric, transitive closure need not capture the right ideal congruence relation. In the previous section we saw that by taking the set $\{p, -p\}$ instead of p alone, we can repair these defects for strong right reduction. The main purpose of this section is to find sets of polynomials in $\mathbf{Z}[\mathcal{H}]$, which do the same for (prefix, commutative) right reduction, e.g. allow us to (prefix, commutatively) right reduce all $p \cdot x$ to zero, where $x \in \mathcal{H}$.

Definition 7
Let $p \in \mathbf{Z}[\mathcal{H}]$ and $F \subseteq \{canon(p \cdot x) \mid x \in \mathcal{H}\}$ [15]. F is called a *saturating set* for p, if for all $x \in \mathcal{H}$, $p \cdot x \rightarrow_F^r 0$ holds. F is called a *prefix saturating set* for p, if for all $x \in \mathcal{H}$, $p \cdot x \rightarrow_F^p 0$ holds. F is called a *commutatively saturating set* for p, if for all $x \in \mathcal{H}$, $p \cdot x \rightarrow_F^c 0$ holds. $\mathcal{SAT}(p)$, $SAT_p(p)$ respectively $\mathcal{SAT}_c(p)$ are the families of saturating, prefix saturating respectively commutatively saturating sets for p.

Remark 5

1. Note that in defining (prefix, commutatively) saturating sets we demand (prefix, commutative) right reducibility to 0 in *one* step.

2. To learn more about (prefix, commutatively) saturating sets for polynomials, we will take a more constructive look at them.
   Let $p = \sum_{i=1}^{k} c_i \cdot t_i$, where $c_i \in \mathbf{Z}, t_i \in \mathcal{H}$.
   Let $X_{t_i} = \{x \in \mathcal{H} \mid HT(p \cdot x) = t_i \cdot x\}$, i.e. the set of all elements, which put t_i in head position [16]. Let $Y_{t_i} = \{canon(p \cdot x) \mid x \in X_{t_i}\}$.

   (a) Choosing a set $B_{t_i} \subseteq Y_{t_i}$ such that for all $p_j \in Y_{t_i}$ we have $p_j \rightarrow_{B_{t_i}}^r 0$, we get $\bigcup_{i=1}^{k} B_{t_i} \in \mathcal{SAT}(p)$.

   (b) Choosing a set $B_{t_i} \subseteq Y_{t_i}$ such that for all $p_j \in Y_{t_i}$ we have $p_j \rightarrow_{B_{t_i}}^p 0$, we get $\bigcup_{i=1}^{k} B_{t_i} \in \mathcal{SAT}_p(p)$.

   (c) Choosing a set $B_{t_i} \subseteq Y_{t_i}$ such that for all $p_j \in Y_{t_i}$ we have $p_j \rightarrow_{B_{t_i}}^c 0$, we get $\bigcup_{i=1}^{k} B_{t_i} \in \mathcal{SAT}_c(p)$.

3. In 2 we do not specify how to choose the B_{t_i} and, therefore, (prefix, commutatively) saturating sets need not be unique. Choosing $B_{t_i} = Y_{t_i}$ we always get saturating sets, which are in general infinite.

4. Y_{t_1} must at least contain $canon(p)$, but all other Y_{t_i} can be empty. In case the multiplication on $\mathcal{H}$ is monotone, we get $Y_{t_1} = \{canon(p \cdot x) \mid x \in \mathcal{H}\}, Y_{t_i} = \emptyset$ for $i \neq 1$, and $B_{t_1} = \{canon(p)\}$ is a finite saturating set for p.

[15] $canon(p \cdot x) = p \cdot x$ if $HC(p \cdot x) > 0$ and $canon(p \cdot x) = -p \cdot x$ otherwise.
[16] Note that if $\mathcal{H}$ is not right–cancellative one x may belong to different sets.

5. The right ideal generated by p is the same as the right ideal generated by a (prefix, commutatively) saturating set of p.

6. $\mathcal{SAT}(p)$ and $\mathcal{SAT}_p(p)$ need not contain finite sets.
   Take $\Sigma = \{a, b, c, d, e, f\}$ with $a \succ b \succ c \succ d \succ e \succ f$ and $T = \{abc \to ba, bad \to e, fbc \to bf\}$. Then (Σ, T) is a convergent presentation of a cancellative monoid. Now look at $p = a + f$:
   Then $X_f = \{(bc)^i dw \mid i \in \mathbf{N}, w \in IRR(T)\}$, and $Y_f = \{b^{i+1}fdw + b^i ew \mid i \in \mathbf{N}, w \in IRR\}$ has no finite basis in either sense. Since if it had a finite basis B_f, we could choose $k \in \mathbf{N}$ such that $b^{k+1}fd + b^k e \notin B_f$. But then we get $b^{k+1}fd + b^k e \not\to_{B_f}^{(r,p)} 0$ as $b^{i+1}fdw \cdot x = b^{k+1}fd$ has no solution in $\mathcal{H}$ unless $w = \lambda$ and $i = k$ [17].

7. $\mathcal{SAT}_c(p)$ always contains finite sets due to Dickson's lemma (see later).

8. Finite saturating sets always exist in case $\mathcal{H}$ is a group. We can even say that for $p = \sum_{i=1}^{k} c_i \cdot t_i$ there exists a set $S \in \mathcal{SAT}(p)$ containing at most k elements.

9. If $q = p \cdot x$ then a (prefix, commutatively) saturating set for p is also a (prefix, commutatively) saturating set for q but not vice versa. Take for instance $\Sigma = \{a, b, c\}$ with $a \succ b \succ c$ and $T = \{ab \to ba, bc \to cb, ac \to ca, ab \to c\}$ and $p = a + 1, q = p \cdot b = b + c$.

Definition 8
Let $F \subseteq \mathbf{Z}[\mathcal{H}]$. We call F *(prefix, commutatively) saturated*, if for all $f \in F$, $x \in \mathcal{H}$ there is $g \in F$ such that $f \cdot x \to_g 0$ using the corresponding reduction.

Note that saturating sets for a polynomial p are saturated, prefix saturating sets are prefix saturated and commutatively saturating sets are commutatively saturated. Further prefix saturated sets as well as commutatively saturated sets are saturated sets and unions of (prefix, commutatively) saturated sets are again (prefix, commutatively) saturated.
However, (prefix, commutatively) saturated sets allow special representations of the elements belonging to their right ideal and, therefore, enable us to capture their right ideal congruence.

Lemma 7

1. *Let $F \subseteq \mathbf{Z}[\mathcal{H}]$ be a saturated set. Every $g \in ideal_r(F)$ has a representation $g = \sum_{i=1}^{k} c_i \cdot f_i \cdot x_i$, where $c_i \in \mathbf{Z}, f_i \in F, x_i \in \mathcal{H}$, and $HT(f_i \cdot x_i) = HT(f_i) \cdot x_i, HC(f_i \cdot x_i) > 0$.*

2. *Let $F \subseteq \mathbf{Z}[\mathcal{H}]$ be a prefix saturated set. Every $g \in ideal_r(F)$ has a representation $g = \sum_{i=1}^{k} c_i \cdot f_i \cdot x_i$, where $c_i \in \mathbf{Z}, f_i \in F, x_i \in \mathcal{H}$, and $HT(f_i \cdot x_i) = HT(f_i)x_i, HC(f_i) > 0$.*

[17] Every $S \in \mathcal{SAT}(p)$ or $S \in \mathcal{SAT}_p(p)$ must (prefix) right reduce the set X_f to zero in one step.

3. *Let* $F \subseteq \mathbf{Z}[\mathcal{H}]$ *be a commutatively saturated set. Every* $g \in ideal(F)$ *has a representation* $g = \sum_{i=1}^{k} c_i \cdot f_i \cdot x_i$, *where* $c_i \in \mathbf{Z}, f_i \in F, x_i \in \mathcal{H}$, *and* $HT(f_i \cdot x_i) = HT(f_i) \circ x_i, HC(f_i) > 0$.

Proof : This follows immediately from definition 8. q.e.d.

Further there is a strong relation between the different reductions and the concept of saturating polynomials as the following lemma shows.

Lemma 8
Let $f, g, p \in \mathbf{Z}[\mathcal{H}], S \in \mathcal{SAT}(p), S_p \in \mathcal{SAT}_p(p), S_c \in \mathcal{SAT}_c(p)$.

1. $f \rightarrow^s_{\{p,-p\}} g$ *if and only if* $f \rightarrow^r_S g$.
2. $f \rightarrow^r_S g$ *if and only if* $f \rightarrow^r_{S_p} g$.
3. $f \rightarrow^r_S g$ *if and only if* $f \rightarrow^p_{S_p} g$.
4. $f \rightarrow^r_S g$ *if and only if* $f \rightarrow^c_{S_c} g$.

Proof :

1. (a) Suppose $f \rightarrow^s_p g$, i.e. $g = f - c \cdot p \cdot x$ for some $c \in \mathbf{Z}, x \in \mathcal{H}, HC(p \cdot x) > 0$. Since $p \cdot x \rightarrow^r_S 0$ we have $p_1 \in S$ such that $p \cdot x = c_1 \cdot p_1 \cdot x_1$ for some $c_1 \in \mathbf{Z}, x_1 \in \mathcal{H}$, and hence $f \rightarrow^r_{p_1 \in S} g$.
   (b) Suppose $f \rightarrow^r_{p_1 \in S} g$, i.e. $g = f - c_1 \cdot p_1 \cdot x_1$ for some $c_1 \in \mathbf{Z}, x_1 \in \mathcal{H}$. Since $p_1 \in S$ we have $y \in \mathcal{H}$ such that $p_1 = canon(p \cdot y)$ and hence $f \rightarrow^s_{\{p,-p\}} g$.
2. (a) Suppose $f \rightarrow^r_{p_1 \in S} g$, i.e. $g = f - c_1 \cdot p_1 \cdot x_1$ for some $c_1 \in \mathbf{Z}, x_1 \in \mathcal{H}$. Since $p_1 \in S$, $HC(p_1 \cdot x_1) > 0$ and $p_1 \cdot x_1 \rightarrow^p_{p_2 \in S_p} 0$ we have $p_1 \cdot x_1 = c_2 \cdot p_2 \cdot x_2$ for some $c_2 \in \mathbf{Z}, x_2 \in \mathcal{H}$ and since $\rightarrow^p_{S_p} \subseteq \rightarrow^r_{S_p}$ we get $f \rightarrow^r_{p_2 \in S_p} g$.
   (b) Suppose $f \rightarrow^r_{p_1 \in S_p} g$, i.e. $g = f - c_1 \cdot p_1 \cdot x_1$ for some $c_1 \in \mathbf{Z}, x_1 \in \mathcal{H}$. Since $p_1 \in S_p$, $HC(p_1 \cdot x_1) > 0$ and $p_1 \cdot x_1 \rightarrow^r_S 0$ we have $p_1 \cdot x_1 = c_2 \cdot p_2 \cdot x_2$ for some $c_2 \in \mathbf{Z}, x_2 \in \mathcal{H}$, and hence $f \rightarrow^r_{p_2 \in S} g$.
3. (a) Suppose $f \rightarrow^r_{p_1 \in S} g$, i.e. $g = f - c_1 \cdot p_1 \cdot x_1$ for some $c_1 \in \mathbf{Z}, x_1 \in \mathcal{H}$. Since $p_1 \in S$, $HC(p_1 \cdot x_1) > 0$ and $p_1 \cdot x_1 \rightarrow^p_{p_2 \in S_p} 0$ we have $p_1 \cdot x_1 = c_2 \cdot p_2 \cdot x_2$ for some $c_2 \in \mathbf{Z}, x_2 \in \mathcal{H}$, and hence $f \rightarrow^p_{p_2 \in S_p} g$.
   (b) Suppose $f \rightarrow^p_{p_1 \in S_p} g$, i.e. $g = f - c_1 \cdot p_1 \cdot x_1$ for some $c_1 \in \mathbf{Z}, x_1 \in \mathcal{H}$. Since $p_1 \in S_p$, $HC(p_1 \cdot x_1) > 0$ and $p_1 \cdot x_1 \rightarrow^r_{p_2 \in S} 0$ we have $p_1 \cdot x_1 = c_2 \cdot p_2 \cdot x_2$ for some $c_2 \in \mathbf{Z}, x_2 \in \mathcal{H}$, and hence $f \rightarrow^r_{p_2 \in S} g$.
4. This can be shown analogously. q.e.d.

Lemma 9
Let $p \in \mathbf{Z}[\mathcal{H}]$ and $S_1, S_2 \in \mathcal{SAT}(p)$. Then $\overset{*}{\leftrightarrow}^r_{S_1} = \overset{*}{\leftrightarrow}^r_{S_2}$.

Proof : We show $\overset{*}{\leftrightarrow}^r_{S_1} \subseteq \overset{*}{\leftrightarrow}^r_{S_2}$ by induction on k for $\overset{k}{\leftrightarrow}^r_{S_1}$ [18].
In the base case $k = 0$ there is nothing to show.
Let us assume $\overset{k}{\leftrightarrow}^r_{S_1} \subseteq \overset{*}{\leftrightarrow}^r_{S_2}$.
Looking at $p_0 \overset{k}{\leftrightarrow}^r_{S_1} p_k \leftrightarrow^r_{S_1} p_{k+1}$ we distinguish two cases:

1. $p_k \rightarrow^r_q p_{k+1}$ with $q \in S_1$.
   Then $p_{k+1} = p_k - a \cdot q \cdot x$ for $a \in \mathbf{Z}, x \in \mathcal{H}$, and since S_2 is a saturating set of p we have $q_1 \in S_2$ with $q \cdot x \rightarrow^r_{q_1} 0$, i.e. $q \cdot x = c_1 \cdot q_1 \cdot y$, where $y \in \mathcal{H}$, $c_1 \in \mathbf{Z}$ and $p_{k+1} = p_k - a \cdot c_1 \cdot q_1 \cdot y$. Therefore we get $p_k \rightarrow^r_{q_1} p_{k+1}$, i.e. $p_k \rightarrow^r_{S_2} p_{k+1}$.
   Our induction hypothesis yields $p_0 \overset{*}{\leftrightarrow}^r_{S_2} p_k \leftrightarrow^r_{S_2} p_{k+1}$.

2. $p_{k+1} \rightarrow^r_q p_k$ gives us $p_0 \overset{*}{\leftrightarrow}^r_{S_2} p_{k+1}$ similarly. q.e.d.

Corollary 1
Let $p \in \mathbf{Z}[\mathcal{H}], S \in \mathcal{SAT}(p), S_p \in \mathcal{SAT}_p(p)$. Then $\overset{*}{\leftrightarrow}^r_S = \overset{*}{\leftrightarrow}^r_{S_p}$.

Corollary 2

1. *Let $F \subseteq \mathbf{Z}[\mathcal{H}], p \in \mathbf{Z}[\mathcal{H}]$ and F be a prefix saturated set. Then $p \rightarrow^r_F q$ if and only if $p \rightarrow^p_F q$.*

2. *Let $F \subseteq \mathbf{Z}[\mathcal{H}], p \in \mathbf{Z}[\mathcal{H}]$ and F be a commutatively saturated set. Then $p \rightarrow^r_F q$ if and only if $p \rightarrow^c_F q$.*

Right now we know that (prefix, commutatively) saturating sets for a polynomial p (prefix, commutative) right reduce the set $\{a \cdot p \cdot x \mid a \in \mathbf{Z}, x \in \mathcal{H}\}$ to zero in one step.

Theorem 1
Let $F \subseteq \mathbf{Z}[\mathcal{H}]$ be a saturated set, $F_p \subseteq \mathbf{Z}[\mathcal{H}]$ be a prefix saturated set, $F_c \subseteq \mathbf{Z}[\mathcal{H}]$ be a commutatively saturated set, and $p, q \in \mathbf{Z}[\mathcal{H}]$.

1. *Then $p \overset{*}{\leftrightarrow}^r_F q$ if and only if $p - q \in ideal_r(F)$.*

2. *Then $p \overset{*}{\leftrightarrow}^p_{F_p} q$ if and only if $p - q \in ideal_r(F_p)$.*

3. *Then $p \overset{*}{\leftrightarrow}^c_{F_c} q$ if and only if $p - q \in ideal_c(F_c)$.*

Proof : We only prove the first claim, since the other proofs are similar.

[18] The case $\overset{*}{\leftrightarrow}^r_{S_2} \subseteq \overset{*}{\leftrightarrow}^r_{S_1}$ is symmetric.

$\Rightarrow$ Using induction on k we show that $p \overset{k}{\leftrightarrow}^r_F q$ implies $p - q \in ideal_r(F)$.
In the base case $k = 0$ there is nothing to show since $p - p = 0 \in ideal_r(F)$.
Let us assume that $p \overset{k}{\leftrightarrow}^r_F q$ implies $p - q \in ideal_r(F)$.
Looking at $p \overset{k}{\leftrightarrow}^r_F p_k \leftrightarrow^r_F q$ we distinguish two cases:

(a) $p_k \rightarrow^r_f q$ with $f \in F$.
Then $q = p_k - a \cdot f \cdot x$ for $a \in \mathbf{Z}, x \in \mathcal{H}$ and since $p - q = p - p_k + a \cdot f \cdot x$ and $p - p_k \in ideal_r(F)$ we get $p - q \in ideal_r(F)$.

(b) $q \rightarrow^r_f p_k$ with $f \in F$ can be treated similarly.

$\Leftarrow$ $p - q \in ideal_r(F)$ implies $p = q + \sum_{j=1}^m a_j \cdot f_j \cdot x_j$, where $a_j \in \mathbf{Z}, f_j \in F, x_j \in \mathcal{H}$.
We show $p \overset{*}{\leftrightarrow}^r_F q$ by induction on m.
In the base case $m = 0$ there is nothing to show.
Let $p = q + \sum_{j=1}^m a_j \cdot f_j \cdot x_j + a_{m+1} \cdot f_{m+1} \cdot x_{m+1}$.
Our induction hypothesis yields $p \overset{*}{\leftrightarrow}^r_F q + a_{m+1} \cdot f_{m+1} \cdot x_{m+1}$.
Since F is a saturated set we know $a_{m+1} \cdot f_{m+1} \cdot x_{m+1} \rightarrow^r_F 0$, i.e. $a_{m+1} \cdot f_{m+1} \cdot x_{m+1} = k \cdot f' \cdot x'$, where $k \in \mathbf{Z}, f' \in F, x' \in \mathcal{H}$, and $HT(f' \cdot x') = HT(f') \cdot x'$.
In case $q + a_{m+1} \cdot f_{m+1} \cdot x_{m+1} \rightarrow^r_{f'} q$ we are done. Now suppose this is not true.
Let $HT(f' \cdot x') = t, HC(f' \cdot x') = c > 0$ and a be the coefficient of t in q. Then a is no remainder of c, i.e. $a = a' \cdot c + b'$, where b' is a remainder of c and $a' \neq 0$ [19]. We get $a + k \cdot c = (a' + k) \cdot c + b'$.
In case $a' + k = 0$ we get $q \rightarrow^r_{f'} q - a' \cdot f' \cdot x' = q + k \cdot f' \cdot x' \overset{*}{\leftrightarrow}^r_F p$ implying $p \overset{*}{\leftrightarrow}^r_F q$.
In case $a' + k \neq 0$ we get $p \overset{*}{\leftrightarrow}^r_F q + k \cdot f' \cdot x' \rightarrow^r_{f'} q + k \cdot f' \cdot x' - (a' + k) \cdot f' \cdot x' = q - a' \cdot f' \cdot x'$, giving us $p \overset{*}{\leftrightarrow}^r_F q$, since $q \rightarrow^r_{f'} q - a' \cdot f' \cdot x'$. q.e.d.

Corollary 3

1. *Let $p \in \mathbf{Z}[\mathcal{H}], S \in \mathcal{SAT}(p)$. Then we get*

$$\overset{*}{\leftrightarrow}^r_S = \equiv_{ideal_r(S)} = \equiv_{ideal_r(p)}$$

2. *Let $p_1, \ldots p_n \in \mathbf{Z}[\mathcal{H}]$ and $S_1 \in \mathcal{SAT}(p_1), \ldots, S_n \in \mathcal{SAT}(p_n)$. Then*

$$\overset{*}{\leftrightarrow}^r_{S_1 \cup \ldots \cup S_n} = \equiv_{ideal_r(S_1 \cup \ldots \cup S_n)} = \equiv_{ideal_r(p_1, \ldots, p_n)}$$

Notice that (prefix, commutatively) saturating sets for a polynomial p satisfy (i) of definition 6 but in general need not be right Gröbner bases of $\{p\}$, i.e. the Noetherian relation $\overset{*}{\rightarrow}^r$ induced by them need not be confluent, even restricted to $\{a \cdot p \cdot x \mid a \in \mathbf{Z}, x \in \mathcal{H}\}$ and so $ideal_r(p)$ does not necessarily right reduce to zero.

[19] Otherwise we have $q + a_{m+1} \cdot f_{m+1} \cdot x_{m+1} \rightarrow^r_{f'} q$.

Example 5

1. Let $\Sigma = \{a, b, c\}$ with $a \succ b \succ c$ and $T = \{a^2 \to \lambda, b^2 \to \lambda, ab \to c, ac \to b, cb \to a\}$ and $p = a + b + c$.
   Then $S = \{a + b + c, a + c + \lambda, bc + c^2 + b\} \in \mathcal{SAT}(p)$.
   Claim: $\to^r_S$ is not confluent on $\{p \cdot x \mid x \in \mathcal{H}\}$.
   We have $a + b + c \to^r_{a+c+\lambda} b - \lambda$ and $a + b + c \to^r_{a+b+c} 0$ but $b - \lambda \not\overset{*}{\to}^r_S 0$.

2. Let $\Sigma = \{a, b, c\}$ with $a \succ b \succ c$ and $T = \{a^2 \to \lambda, b^2 \to \lambda, ab \to c, ac \to b, cb \to a\}$ and $p = a + b + c$.
   Then $S_p = \{a+b+c, bc+c^2+b, a+c+\lambda, ba+ca+\lambda, ca+a+\lambda, c^2+b+c\} \in \mathcal{SAT}_p(p)$.
   Claim: $\to^r_{S_p}$ is not confluent on $\{p \cdot x \mid x \in \mathcal{H}\}$.
   We have $a + b + c \to^r_{a+c+\lambda} b - \lambda$ and $a + b + c \to^r_{a+b+c} 0$ but $b - \lambda \not\overset{*}{\to}^r_{S_p} 0$.

3. Let $\Sigma = \{a, b\}$ with $a \succ b$ and $T = \{a^2 \to \lambda, ab \to ba\}$ and $p = a + b + \lambda$.
   Then $S_c = \{a + b + \lambda, ba + a + \lambda\} \in \mathcal{SAT}_c(p)$.
   Claim: $\to^r_{S_c}$ is not confluent on $\{p \cdot x \mid x \in \mathcal{H}\}$.
   We have $ba+a+\lambda \to^r_{ba+a+\lambda} 0$ and $ba+a+\lambda \to^r_{a+b+\lambda} -b^2+a-b+\lambda \to^r_{a+b+\lambda} -b^2-2b$ but $-b^2 - 2b \not\overset{*}{\to}^r_{S_c} 0$.

Remark 6

1. Prefix Gröbner bases and commutative Gröbner bases are right Gröbner bases but not vice versa.
   Let $\Sigma = \{a, b\}$ with $a \succ b$ and $T = \{ab \to ba\}$. Then the set $F = \{a + \lambda\}$ is a right Gröbner basis, but not a prefix or commutative Gröbner basis.

2. Further right Gröbner bases are strong Gröbner bases but not vice versa.
   Let $\Sigma = \{a, b, c, d, e, f\}$ with $a \succ b \succ c \succ d \succ e \succ f$ and $T = \{abc \to ba, fbc \to bf, bad \to e\}$.
   Then the set $F = \{a + f\}$ is a strong Gröbner basis, but not a right Gröbner basis [20].

Note that even (prefix) saturated sets F do not guarantee that $p \overset{*}{\to}^r_F 0$ implies $p \cdot x \overset{*}{\to}^r_F 0$ for $p \in \mathbf{Z}[\mathcal{H}], x \in \mathcal{H}$.

Example 6
Let $\Sigma = \{a, b, c, d\}$ with $a \succ b \succ c \succ d$ and $T = \{abc \to ba, dbc \to bd\}$.
Then the set $F = \{a - c, cbc - ba, c + d\}$ is (prefix) saturated.
Looking at $p = a + d$ we get $p \overset{2}{\to}^r_F 0$. But $p \cdot bc = ba + bd$ is F–irreducible.

This example shows that removing elements from a set by interreduction can yield different normal forms. Just take $F' = F \cup \{a+d\}$. Then $ba+bd \overset{*}{\to}^r_{F'} 0$ but $ba+bd \not\overset{*}{\to}^r_F 0$.

[20] Remember that F allows no finite saturating sets.

5 Taking a Closer Look at Saturation

In this section we investigate saturation with respect to prefix right respectively commutative reduction. If finite prefix saturating sets exist, these are of course saturating sets and they contain additional structural information. We give a procedure to enumerate a prefix saturating set and there are several structures allowing finite prefix saturating sets, e.g. finite monoids, free monoids, and monoids having a monadic presentation. In commutative structures finite commutative saturating sets always exist.

5.1 Prefix Saturation in Finite Monoids

Let $\mathcal{H}$ be a finite monoid having a finite convergent presentation (Σ, T).

Procedure Prefix Saturation

input: $p = \sum_{i=1}^{k} c_i \cdot t_i \in \mathbf{Z}[\mathcal{H}]$ and (Σ, T) a presentation of $\mathcal{H}$.
output: $\mathrm{SAT}_p(p) \in \mathcal{SAT}_p(p)$.

$\mathrm{SAT}_p(p) := \{\mathrm{canon}(p)\}$;
for all $x \in \mathcal{H}$ do
  if $p \cdot x \not\to^{p}_{\mathrm{SAT}_p(p)} 0$
  then $\mathrm{SAT}_p(p) := \mathrm{SAT}_p(p) \cup \{\mathrm{canon}(p \cdot x)\}$
endfor

where *canon* canonizes a polynomial, i.e. multiplies it by -1 in case its head coefficient is not positive.

Theorem 2
The procedure terminates.

Proof : This is due to the fact that $\mathcal{H}$ is finite. q.e.d.

Theorem 3
The procedure is correct, i.e. for all $p \in \mathbf{Z}[\mathcal{H}]$, $x \in \mathcal{H}$ the polynomial $p \cdot x$ is prefix right reducible to zero by $\mathrm{SAT}_p(p)$.

Proof : This is due to the fact that all $p \cdot x, x \in \mathcal{H}$ are computed and their canonized form is added in case they do not prefix right reduce to zero by $\mathrm{SAT}_p(p)$. q.e.d.

5.2 Prefix Saturation for Monoids with Convergent Presentations

We will give a procedure, which enumerates a prefix saturating set for a polynomial in $\mathbf{Z}[\mathcal{H}]$.

Procedure Prefix Saturation

input: $p = \sum_{i=1}^{k} c_i \cdot t_i \in \mathbf{Z}[\mathcal{H}]$ and (Σ, T) a finite convergent presentation of $\mathcal{H}$.
output: $\textsc{Sat}_p(p) \in \mathcal{SAT}(p)$.

$\textsc{Sat}_p(p) := \{\text{canon}(p)\}$;
$H := \{\text{canon}(p)\}$;
while $H \neq \emptyset$ do
  $q := \text{remove}(H)$;
  $t := HT(q)$;
  for all $x \in C(t) = \{x \in \mathcal{H} \mid tx = t_1 t_2 x = t_1 l, t_2 \neq \lambda \text{ for some } (l, r) \in T\}$ do
    $q' := q \cdot x$
    if $q' \not\to^{p}_{\textsc{Sat}_p(p)} 0$
    then $\textsc{Sat}_p(p) := \textsc{Sat}_p(p) \cup \{\text{canon}(q')\}$;
      $H := H \cup \{\text{canon}(q')\}$
  endfor
endwhile

where *remove* removes a polynomial from a set and *canon* canonizes a polynomial, i.e. multiplies it by -1 in case its head coefficient is not positive.
The procedure is illustrated by the following example.

Example 7
Let $\Sigma = \{a, b, c\}$ with $a \succ b \succ c$ and $T = \{a^2 \to \lambda, b^2 \to \lambda, ab \to c, ac \to b, cb \to a\}$.
Saturating $p = a + b + c$ we get:
Initialization: $H := \{a + b + c\}, \textsc{Sat}_p(p) := \{a + b + c\}$.
1. Taking $a+b+c \in H$ and $x \in \{a, b, c\}$ we get $ba + ca + \lambda, a + c + \lambda, bc + c^2 + b$, which are all added to H and $\textsc{Sat}_p(p)$.
2. Taking $ba + ca + \lambda \in H$ and $x \in \{a, b, c\}$ we get $a + b + c, bc + c^2 + b, a + c + \lambda$, which prefix right reduce to zero by $\textsc{Sat}_p(p)$.
3. Taking $a + c + \lambda \in H$ and $x \in \{a, b, c\}$ we get $ca + a + \lambda, a + b + c, c^2 + b + c$ and $ca + a + \lambda, c^2 + b + c$ are added to H and $\textsc{Sat}_p(p)$.
4. Taking $bc + c^2 + b \in H$ and $x \in \{b\}$ we get $ba + ca + \lambda$, which prefix right reduces to zero by $\textsc{Sat}_p(p)$.
5. Taking $ca + a + \lambda \in H$ and $x \in \{a, b, c\}$ we get $a + c + \lambda, c^2 + b + c, a + b + c$, which prefix right reduce to zero by $\textsc{Sat}_p(p)$.
6. Taking $c^2 + b + c \in H$ and $x \in \{b\}$ we get $ca + a + \lambda$, which prefix right reduces to

zero by $\mathrm{SAT}_p(p)$.
7. As $H = \emptyset$ we get $\mathrm{SAT}_p(p) = \{a+b+c, bc+c^2+b, a+c+\lambda, ba+ca+\lambda, ca+a+\lambda, c^2+b+c\}$.

Now there are situations where finite saturating sets but no finite prefix saturating sets exist. Take for example $\Sigma = \{a, b, c\}$ with $a \succ b \succ c$ and $T = \{ac \to cb, bc \to ca\}$. Then $p = a + \lambda$ has a finite saturating set $\{p\}$ but no finite prefix saturating set.
Note that the procedure Prefix Saturation cannot be turned into a procedure to enumerate a (not necessarily prefix) saturating set of p by just replacing $q' \not\to^p_{\mathrm{SAT}_p(p)} 0$ with $q' \not\to^r_{\mathrm{SAT}(p)} 0$. Taking e.g. $\Sigma = \{a, a^{-1}\}, T = \{aa^{-1} \to \lambda, a^{-1}a \to \lambda\}$ and $p = a^3 + \lambda$ we would get $\mathrm{SAT}(p) = \{p\}$, but $p \cdot a^{-6} = a^{-6} + a^{-3} \not\to^r_{\mathrm{SAT}(p)} 0$.

Theorem 4
The procedure enumerates a prefix saturating set of a polynomial p, i.e. for all $p \in \mathbf{Z}[\mathcal{H}]$, $x \in \mathcal{H}$ the polynomial $p \cdot x$ is prefix right reducible to zero by $\mathrm{SAT}_p(p)$. Therefore the procedure is partially correct.

Proof : We show that for all $q \in \mathrm{SAT}_p(p), x \in \mathcal{H}$ we have $q \cdot x \to^p_{\mathrm{SAT}_p(p)} 0$. Suppose this is not true. We can choose a minimal counterexample $q \cdot x$, where $HT(q)x$ is minimal (according to the ordering $\succ$ on Σ^*) and $q \cdot x \not\to^p_{\mathrm{SAT}_p(p)} 0$. Then $HT(q)x$ is T–reducible, as otherwise $q \cdot x \to^p_{q \in \mathrm{SAT}_p(p)} 0$. Let $HT(q)x = t_1 t_2 x_1 x_2$ where $HT(q) = t_1 t_2, t_2 \neq \lambda, x = x_1 x_2$ and $l = t_2 x_1$ for some $(l, a) \in T$. Since $q \in \mathrm{SAT}_p(p)$ we have $x_1 \in C(HT(q))$.

1. If $canon(q \cdot x_1) \in \mathrm{SAT}_p(p)$ then $q \cdot x = (q \cdot x_1) \cdot x_2 \to^p_{\mathrm{SAT}_p(p)} 0$ since $HT(q)x = HT(q)x_1x_2 \succ HT(q \cdot x_1)x_2$, contradicting our assumption.

2. If $canon(q \cdot x_1) \notin \mathrm{SAT}_p(p)$ then $q \cdot x_1 \to^p_{q' \in \mathrm{SAT}_p(p)} 0$ and $HT(q)x_1 \succ HT(q \cdot x_1) = HT(q')z$ for some $z \in \mathcal{H}$. Further $q \cdot x_1 \in \{p \cdot y, -p \cdot y \mid y \in \mathcal{H}\}$, $q' \in \mathrm{SAT}_p(p) \subseteq \{canon(p \cdot y) \mid y \in \mathcal{H}\}$ and $HT(q \cdot x_1) = HT(q')z$ gives us $q \cdot x = (q \cdot x_1) \cdot x_2 = c \cdot (q' \cdot z) \cdot x_2$, $c \in \mathbf{Z}$ and $HT(q)x \succ HT(q')zx_2$. Therefore $q \cdot x = c \cdot (q' \cdot z) \cdot x_2 = c \cdot q' \cdot (zx_2) \to^p_{\mathrm{SAT}_p(p)} 0$ contradicting our assumption. q.e.d.

Theorem 5
The procedure terminates for left–cancellative monoids, having a finite convergent monadic presentation.

Proof : Let $\mathcal{H}$ be a monoid having a finite convergent presentation (Σ, T), where T is monadic including no rules as $a \to b$ or $a \to \lambda$, $a, b \in \Sigma$. Further we use the length–lexicographical ordering as our ordering on $\mathcal{H}$.

1. We start our proof with the following technical remark:
   Let $q \in \mathbf{Z}[\mathcal{H}]$. We call a chain $x_1, x_2, \ldots$,where $x_i \in \mathcal{H}$, an irreducible reduction sequence of q, if for all i:

(a) $q_i = q \cdot x_1 \dots x_i$

(b) $HT(q_i)x_{i+1} = tl$, where t is a prefix of $HT(q_i)$ and $(l, a) \in T$

(c) $x_1 \dots x_i x_{i+1}$ is T-irreducible.

Now we can state our first subclaim: A possible irreducible reduction sequence of a polynomial $q = \sum_{i=1}^{k} c_i \cdot t_i$ has at most length $k \cdot |HT(q)| \cdot |\Sigma|$. We get this bound by examining the set of possible head terms for the q_i: $HT(q_i) = t'_j b x'$, $j \in \{1, \dots, k\}$ where t'_j is a prefix of t_j, $b \in \Sigma \cup \{\lambda\}$ and x' is a suffix of $x_1 \dots x_i$ [21]. This can occur at most $|t_j| \cdot |\Sigma|$ times since T is monadic describing a left–cancellative monoid and irreducible reductions always affect $t'_j b$. Since q has k different terms and $|t_j| \leq |t_1|$ the irreducible sequences of q have at most length $k \cdot |HT(q)| \cdot |\Sigma|$.
An easy conclusion of this [22] is the fact that for each $x \in \mathcal{H}$ looking at $p \cdot x$ we can split x into $x = x_1 \dots x_n y$ where:

(a) $x_1, \dots, x_n$ describes an irreducible reduction sequence of p

(b) $HT(p \cdot x) = HT(p \cdot x_1 \dots x_n)y$, i.e. $(p \cdot x) \rightarrow^{p}_{(p \cdot x_1 \dots x_n)} 0$

(c) $|x_1 \dots x_n| \leq k \cdot |HT(q)| \cdot |\Sigma| \cdot (max\{|l| \mid (l, a) \in T\} - 1)$

2. If we organize the set H as a first in first out set, we can simulate the proceeding of the procedure by constructing a tree in the following way:

   (a) The root is the polynomial p.

   (b) If q is a polynomial at a node then its sons are the $q \cdot y$ [23] , where $y \in C(HT(q))$, which cannot be prefix right reduced to 0 by any of the polynomials at already constructed nodes.

3. We will show the following useful second subclaim: If a polynomial q appears as a node at depth j then for any $x \in \mathcal{H}$, $q \cdot x$ is prefix right reducible to 0 by a polynomial appearing as a node at most at depth $j + |x|$.
   Let us suppose this is not true.
   Then we can choose $x \in \mathcal{H}$ with $|x|$ minimal such that there is a polynomial q at a node at depth j and $q \cdot x$ is not prefix right reducible by any polynomial at a node at depth less or equal to $j + |x|$. Now by the above conclusion x can be written as $x = x_1 \dots x_n y$ where $x_1, \dots, x_n$ describe an irreducible reduction sequence of q and as x is minimal $y = \lambda$ [24]. Since such a reduction sequence could describe a path from q ending with $q \cdot x$, where $q \cdot x$ would be at depth less or equal to $j + |x|$ [25], this

[21] This is due to the fact that T is monadic and $x_1 \dots x_i$ is T–irreducible.

[22] Note that this is no longer true if we drop the condition left–cancellative. Take for example $\Sigma = \{a, b\}, T = \{ab \rightarrow a\}$. Then we get $ab^n \xrightarrow{*} a$ for all $n \in \mathbf{N}$ and $b^n \in IRR(T)$.

[23] Without loss of generality we will assume the polynomials $q \cdot y$ at the nodes to be canonized.

[24] Otherwise $(p \cdot x) \rightarrow^{p}_{(p \cdot x_1 \dots x_n)} 0$ immediately gives us a contradiction since $|x_1 \dots x_n| < |x_1 \dots x_n y|$ in case $y \neq \lambda$.

[25] As each x_i must at least have length 1.

sequence must have been cut off before reaching $q \cdot x$. Let $q \cdot x_1 \ldots x_m, (m < n-1)$ [26] be the ancestor of $q \cdot x$ where the path stops, i.e. $q \cdot x_1 \ldots x_{m+1}$ prefix right reduces to 0 by a polynomial q', which must occur as a node at depth less or equal to $j+m+1 \leq j+|x_1 \ldots x_{m+1}|$. Now $HT(q \cdot x_1 \ldots x_{m+1}) = HT(q')w$ for some $w \in \mathcal{H}$ and we know $HT(q')w \in IRR(T), x_{m+2} \ldots x_n \in IRR(T)$ but $HT(q')wx_{m+2} \ldots x_n$ is T-reducible as otherwise $q \cdot x \rightarrow^p_{q'} 0$ contradicting our assumption. Let $w'bx'$ be the (not necessarily different) T-normal form of $wx_{m+2} \ldots x_n$ [27], where w' is a prefix of $w, b \in \Sigma \cup \{\lambda\}$ and x' is a suffix of $x_{m+2} \ldots x_n$. In case $HT(q')w'bx'$ is T–irreducible we get $q \cdot x \rightarrow^p_{q'} 0$, contradicting our assumption. Now let us assume $HT(q')w'bx' = t_1t_2w'bx'_1x'_2 = t_1lx'_2$, where $t_1t_2 = HT(q'), x'_1x'_2 = x', (l,a) \in T$ and $|x'_2| < |x_{m+2} \ldots x_n|$. Since $q' \in S$ and $w'bx'_1 \in C(HT(q'))$ this situation is investigated by our procedure. We have to distinguish two cases:

(a) $q' \cdot w'bx'_1$ is a node at most at depth $j+m+2$ and added to S. Since $|x'_2| < |x_{m+2} \ldots x_n| < |x|$ we get a polynomial q'' at a node at most at depth

$$\begin{aligned} j+m+2+|x'_2| &\leq j+|x_1 \ldots x_m|+2+|x'_2| \\ &< j+|x_1 \ldots x_{m+1}|+1+|x_{m+2} \ldots x_n| \\ &< j+|x|+1 \end{aligned}$$

with $q \cdot x = q' \cdot w'bx'_1x'_2 \rightarrow^p_{q''} 0$ contradicting our assumption.

(b) If $q' \cdot w'bx'_1$ is no node we have $q' \cdot w'bx'_1 \rightarrow^p_{q''} 0$ for some polynomial q'', which is at a node at most at depth $j+m+2$. Again we get $HT(q' \cdot w'bx'_1) = HT(q'')w''$ and $|x'_2| < |x_{m+2} \ldots x_n|$. Now this is exactly the same situation we had before with q', w' and x' except that $|x'_2| < |x'|$. In case $x'_2 = \lambda$ we get $q \cdot x \rightarrow^p_{q''} 0$ contradicting our assumption. Otherwise we can proceed as above.

4. Now it remains to show that our procedure terminates, i.e. there are no infinite branches in our tree. Suppose that there is an infinite branch.
Then we may assume that we have a sequence $z_1, z_2, \ldots$, where $z_i \in \mathcal{H}$ and $p \cdot z_i$ is an ancestor of $p \cdot z_j$ on our infinite branch for $i < j$. Now let N be chosen such that $p \cdot z_N$ is at depth $N > k \cdot |HT(q)| \cdot |\Sigma| \cdot (max\{|l| \mid (l,a) \in T\} - 1)$. Then by the conclusion of our first subclaim we can decompose $z_N = x_1 \ldots x_{N_1}y$ such that $x_1, \ldots x_{N_1}$ is an irreducible sequence of p, $|x_1 \ldots x_{N_1}| \leq k \cdot |HT(q)| \cdot |\Sigma| \cdot (max\{|l| \mid (l,a) \in T\} - 1)$ and $p \cdot x \rightarrow^p_{p \cdot x_1 \ldots x_{N_1}} 0$. The second subclaim gives us that there exists a node q' at most at depth $m \leq |x_1 \ldots x_{N_1}| \leq k \cdot |HT(q)| \cdot |\Sigma| \cdot (max\{|l| \mid (l,a) \in T\} - 1)$ with $p \cdot x_1 \ldots x_{N_1} \rightarrow^p_{q'} 0$. But then $p \cdot z_N \rightarrow^p_{q'} 0$, contradicting the fact that $p \cdot z_{N+1}$ is a node. q.e.d.

[26] $m = n-1$ would imply $q \cdot x \rightarrow^p_{q'} 0$ with a polynomial q', which must occur at a node at depth less or equal to $j + |x|$ contradicting our assumption.

[27] This is due to the fact that T is monadic.

5.3 Commutative Saturation in Commutative Monoids

Let $\mathcal{H}$ be a commutative monoid having a finite convergent presentation (Σ, T), where T includes the commutative rules for all letters in Σ. Further let $\mathcal{F}_c(\Sigma)$ denote the free commutative monoid generated by Σ with multiplication $\circ$. We will use the ordering induced by the ordering of T as our ordering on $\mathcal{H}$. The existence of finite commutatively saturating sets is guaranteed by Dickson's Lemma.

Lemma 10 (Dickson)
For every infinite sequence of elements $m_s \in \mathcal{F}_c(\Sigma)$,$s \in \mathbf{N}$, there exists an index $k \in \mathbf{N}$ such that for all $i > k$ we have $j \leq k, x \in \mathcal{F}_c(\Sigma)$ such that $m_i = m_j \circ x$.

Now we can state:

Lemma 11
Let $p = \sum_{i=1}^{n} c_i \cdot t_i \in \mathbf{Z}[\mathcal{H}], c_i \in \mathbf{Z}, t_i \in \mathcal{H}$ and $Y_{t_i} = \{canon(p \cdot x) \mid x \in X_{t_i}\}$ as specified in remark 5. Then each Y_{t_i} has a finite basis via commutative reduction.

Proof : Let $Z_{t_i} = \{HT(q) \mid q \in Y_{t_i}\}$. Then Z_{t_i} is a (possibly infinite) subset of $\mathcal{F}_c(\Sigma)$ in the sense of Dickson's Lemma and we can choose a finite basis of Z_{t_i}. Since commutative reduction just requires $\circ$ as multiplication we are done. q.e.d.

It remains to give a procedure, which actually computes a commutatively saturating set of a polynomial p.

Procedure Commutative Saturation

input: $p = \sum_{i=1}^{k} c_i \cdot t_i \in \mathbf{Z}[\mathcal{H}]$ and (Σ, T) a presentation of $\mathcal{H}$.
output: $\textsc{Sat}_c(p) \in \mathcal{SAT}_c(p)$.

$\textsc{Sat}_c(p) := \{\text{canon}(p)\}$;
$H := \{\text{canon}(p)\}$;
while $H \neq \emptyset$ do
  $q := \text{remove}(H)$;
  $t := HT(q)$;
  for all $(l, r) \in T$ do
    if $t \circ x_1 = l \circ x_2$ is the least common multiply of t and l in $\mathcal{F}_c(\Sigma)$
    then $q' := (q \cdot x_1)$
      if $q' \not\xrightarrow{c}_{\textsc{Sat}_c(p)} 0$
      then $\textsc{Sat}_c(p) := \textsc{Sat}_c(p) \cup \{\text{canon}(q')\}$,
        $H := H \cup \{\text{canon}(q')\}$
  endfor
endwhile

where *remove* removes a polynomial from a set and *canon* canonizes a polynomial, i.e. multiplies it by -1 in case its head coefficient is not positive.

Theorem 6
The procedure is correct, i.e. for all $p \in \mathbf{Z}[\mathcal{H}]$, $x \in \mathcal{H}$ the polynomial $p \cdot x$ is commutatively reducible to zero by $\text{SAT}_c(p)$.

Proof : We show that for all $q \in S$,$x \in \mathcal{H}$ we have $q \cdot x \rightarrow_S^c 0$. Suppose this is not true. We can choose a minimal counterexample $q \cdot x$ where $HT(q) \circ x$ is minimal (according to the ordering on $\mathcal{H}$) and $q \cdot x \not\rightarrow_S^c 0$. Then $HT(q) \circ x$ is T–reducible, as otherwise $q \cdot x \rightarrow_q^c 0$ and $q \in S$. Let $x = x_1 \circ x_2$ such that x_1 is minimal causing $HT(q \cdot x_1) \neq HT(q) \circ x_1$. Then we have $HT(q) \circ x_1 = l \circ z$ for some $(l, a) \in T$ and $z \in \mathcal{H}$. Therefore $q \cdot x_1$ is considered during the computation of S.

1. If $q \cdot x_1 \in S$ then $q \cdot x = (q \cdot x_1) \cdot x_2 \rightarrow_S^c 0$ since $HT(q) \circ x \succ HT(q \cdot x_1) \circ x_2$ contradicting our assumption.

2. If $q \cdot x_1 \notin S$ then $q \cdot x_1 \rightarrow_{q' \in S}^c 0$ and $HT(q \cdot x_1) = HT(q') \circ z$ for some $z \in \mathcal{H}$. Further $q \cdot x = (q \cdot x_1) \cdot x_2 = c \cdot (q' \cdot z) \cdot x_2$, $c \in \mathbf{Z}$ and $HT(q) \circ x_1 x_2 \succ HT(q') \circ z x_2$. Therefore $q \cdot x = c \cdot (q' \cdot z) \cdot x_2 = c \cdot q' \cdot (z x_2) \rightarrow_S^c 0$ contradicting our assumption.

q.e.d.

Theorem 7
The procedure terminates.

Proof : Suppose our procedure does not terminate. Then infinitely many polynomials q' are added to one set Y_{t_i}. Due to lemma 11 this can only happen a finite number of times until there are enough polynomials in the already computed set S to ensure $q' \rightarrow_S^c 0$ for all $q' \in Y_{t_i}$. q.e.d.

Note that for $F \subseteq \mathbf{Z}[\mathcal{H}]$ we have $ideal(F) = ideal_l(F) = ideal_r(F)$.

6 Completion in $\mathbf{Z}[\mathcal{H}]$

As we are interested in Gröbner bases of right ideals we are looking for a finite test for checking, whether the reduction relation induced by a finite set of polynomials is confluent, using the concepts of superpositions, critical pairs and s–polynomials, as introduced by Buchberger.

6.1 Completion Using Strong Right Reduction

First we define critical pairs of polynomials via $\rightarrow^s$ and show a criterion that implies confluence for $\rightarrow^s$.

Definition 9 (Strong s–polynomials)
Given two polynomials $p_1, p_2 \in \mathbf{Z}[\mathcal{H}]$. If there are $x_1, x_2 \in \mathcal{H}$ with $HT(p_1 \cdot x_1) = HT(p_2 \cdot x_2)$, $HC(p_2 \cdot x_2) \geq HC(p_1 \cdot x_1) > 0$ and $HC(p_2 \cdot x_2) = a \cdot HC(p_1 \cdot x_1) + b$, where $a, b \in \mathbf{Z}$, b a remainder of $HC(p_1 \cdot x_1)$, we get the following superposition causing a critical pair:

$$\begin{array}{ccc} & HM(p_2 \cdot x_2) = a \cdot HM(p_1 \cdot x_1) + b \cdot HT(p_1 \cdot x_1) & \\ \swarrow & & \searrow \\ -RED(p_2 \cdot x_2) & & -a \cdot RED(p_1 \cdot x_1) + b \cdot HT(p_1 \cdot x_1) \end{array}$$

This gives us the strong s–polynomial

$$spol_s(p_1, p_2, x_1, x_2) = a \cdot p_1 \cdot x_1 - p_2 \cdot x_2.$$

Let $U_{p_1,p_2} \subseteq \mathcal{H}^2$ be the set containing all pairs $x_1, x_2 \in \mathcal{H}$ as above.

Remark 7
Sometimes two polynomials p_1, p_2 can cause infinitely many critical situations, which cannot be avoided by taking a suitable "basis" of the set U_{p_1,p_2}.
Let $\Sigma = \{a, b, c, d, e, f\}, T = \{abc \to ba, fbc \to bf, bad \to e\}$ and $p_1 = a + f, p_2 = bf + a$. Then we get the following critical situations $f \cdot (bc)^i dw = bf \cdot (bc)^{i-1} dw$, where $i \in \mathbf{N}^+, w \in IRR(T)$, giving us the strong s–polynomials $(a + f) \cdot (bc)^i dw - (bf + a) \cdot (bc)^{i-1} dw$.

Note that this phenomena corresponds to the example in remark 5 given to show that saturation in general does not terminate. This shows how closely related saturation of a weaker reduction and critical situations of strong reduction are.

Theorem 8
Let $F \subseteq \mathbf{Z}[\mathcal{H}]$ and let $f \in F$ imply $-f \in F$. Equivalent are:

1. *F is a Gröbner basis via $\to^s$.*
2. *$ideal_r(F) \xrightarrow{*}{}^s_F 0$.*
3. *For all not necessarily different $f_k, f_l \in F, (x_k, x_l) \in U_{f_k,f_l}$ we have:*

$$spol_s(f_k, f_l, x_k, x_l) \xrightarrow{*}{}^s_F 0.$$

Proof :

$1 \Rightarrow 2$ By lemma 6 $f \in ideal_r(F)$ implies $f \overset{*}{\leftrightarrow}{}^s_F 0$ and as F is confluent $f \xrightarrow{*}{}^s_F 0$.

$2 \Rightarrow 1$ Since $\to^s_F$ is Noetherian, we only have to prove local confluence.
Suppose $f \to^s_F f_1, f \to^s_F f_2$ and $f_1 \neq f_2$. Then $f_1 - f_2 \in ideal_r(F)$ and, therefore, $f_1 - f_2 \xrightarrow{*}{}^s_F 0$. By lemma 5 there exists $g \in \mathbf{Z}[\mathcal{H}]$ such that $f_1 \xrightarrow{*}{}^s_F g, f_2 \xrightarrow{*}{}^s_F g$.

$2 \Rightarrow 3$ Let $(x_k, x_l) \in U_{f_k,f_l}$ give us a strong s–polynomial of f_k, f_l. Then by definition 9 we get

$$spol_s(f_k, f_l, x_k, x_l) = a \cdot f_k \cdot x_k - f_l \cdot x_l \ \in ideal_r(F).$$

and hence we get $spol_s(f_k, f_l, x_k, x_l) \xrightarrow{*}_F^s 0$.

$3 \Rightarrow 2$ We have to show that every $g \in ideal_r(F) - \{0\}$ is $\rightarrow_F^s$–reducible to zero. As $\rightarrow_F^s$ is Noetherian and $h \in ideal_r(F)$, $h \rightarrow_F^s h'$ implies $h' \in ideal_r(F)$, it suffices to show that every $g \in ideal_r(F) - \{0\}$ is $\rightarrow_F^s$–reducible.
Let $g = \sum_{i=1}^m c_i \cdot f_i \cdot x_i$, where $c_i \in \mathbf{Z}, f_i \in F, x_i \in \mathcal{H}$.
Depending on this representation of g we define $t = max\{HT(f_i \cdot x_i) \mid i \in \{1, \ldots m\}\}, M = \{\{HC(f_i \cdot x_i) \mid HT(f_i \cdot x_i) = t\}\}$. (Note that M is a multiset with elements in $\mathbf{Z}$).
We call another representation of g with $\tilde{t}, \tilde{M}$ *smaller*, if $\tilde{t} < t$ or $\tilde{t} = t$ and $\tilde{M} \ll M$.
Without loss of generality we can assume $HC(f_i \cdot x_i) > 0$, as otherwise we can substitute f_i by $-f_i$ and $HT(f_i \cdot x_i) = HT(-f_i \cdot x_i)$ together with $HC(f_i \cdot x_i) >_Z HC(-f_i \cdot x_i)$ gives us a smaller representation of g. Important is that now M is a multiset with elements in $\mathbf{N}$.
Our intention is to show that if t, M belong to a minimal representation of g [28], then $|M| = 1$, e.g. $M = \{\{HC(f_k \cdot x_k)\}\}$. This gives us $HT(g) = t = HT(f_k \cdot x_k)$ and as $HC(f_k \cdot x_k) > 0$, g is $\rightarrow_F^s$–reducible by f_k.
Let us assume there is a polynomial $g \in ideal_r(F) - \{0\}$ with a minimal representation $g = \sum_{i=1}^m c_i \cdot f_i \cdot x_i$ together with t, M and $|M| > 1$.
Let $HC(f_k \cdot x_k), HC(f_l \cdot x_l) \in M$,$k \neq l$ [29] and $a \cdot HC(f_k \cdot x_k) + b = HC(f_l \cdot x_l)$ for $a, b \in \mathbf{Z}$, b a remainder of $HC(f_k \cdot x_k)$.
Since $HT(f_k \cdot x_k) = HT(f_l \cdot x_l)$ by definition 9 we have a strong s–polynomial $spol_s(f_k, f_l, x_k, x_l) = a \cdot f_k \cdot x_k - f_l \cdot x_l$. Let us assume $spol_s(f_k, f_l, x_k, x_l) \neq 0$ [30].
Now $spol_s(f_k, f_l, x_k, x_l) \xrightarrow{*}_F^s 0$ implies $a \cdot f_k \cdot x_k - f_l \cdot x_l = \sum_{i=1}^n d_i \cdot h_i \cdot w_i, d_i \in \mathbf{Z}, h_i \in F, w_i \in \mathcal{H}$, where the h_i are due to the reduction of the s–polynomial, i.e. $HC(h_i \cdot w_i) > 0$, and all terms occurring in the sum are bounded by $HT(spol_s(f_k, f_l, x_k, x_l)) \leq t$.
Now we get:

$$\begin{aligned} g &= c_k \cdot f_k \cdot x_k + c_l \cdot f_l \cdot x_l + \sum_{\substack{i=1 \\ k \neq i \neq l}}^{m} c_i \cdot f_i \cdot x_i \\ &= c_k \cdot f_k \cdot x_k + \underbrace{c_l \cdot a \cdot f_k \cdot x_k - c_l \cdot a \cdot f_k \cdot x_k}_{=0} + c_l \cdot f_l \cdot x_l + \sum_{\substack{i=1 \\ k \neq i \neq l}}^{m} c_i \cdot f_i \cdot x_i \end{aligned}$$

[28] Such minimal representations of polynomials exist as our ordering on representations as defined above is well–founded.

[29] Not necessarily $f_l \neq f_k$.

[30] In case $spol_s(f_k, f_l, x_k, x_l) = 0$ the proof is similar. Substituting 0 for $\sum_{i=1}^n d_i \cdot h_i \cdot w_i$ in the equations below immediately gives us a smaller representation of g, contradicting our assumption.

$$= (c_k + c_l \cdot a) \cdot f_k \cdot x_k - c_l \cdot \underbrace{(a \cdot f_k \cdot x_k - f_l \cdot x_l)}_{= spol_s(f_k, f_l, x_k, x_l)} + \sum_{\substack{i=1 \\ k \neq i \neq l}}^{m} c_i \cdot f_i \cdot x_i$$

$$= (c_k + c_l \cdot a) \cdot f_k \cdot x_k - c_l \cdot (\sum_{i=1}^{n} d_i \cdot h_i \cdot w_i) + \sum_{\substack{i=1 \\ k \neq i \neq l}}^{m} c_i \cdot f_i \cdot x_i$$

and depending on this new representation of g we define $\tilde{t} = max\{HT(h_i \cdot w_i), HT(f_i \cdot x_i) \mid h_i, f_i$ appearing in the sum $\}, \tilde{M} = \{\{HC(h_i \cdot w_i), HC(f_i \cdot x_i) \mid HT(h_i \cdot w_i) = \tilde{t} = HT(f_i \cdot x_i)\}\}$ and we either get $\tilde{t} < t$ or $\tilde{t} = t$ and we have to distinguish two cases:

(a) $c_k + c_l \cdot a = 0$.
Then $\tilde{M} = (M - \{HC(f_k \cdot x_k), HC(f_l \cdot x_l)\}) \cup \{\{HC(h_i \cdot w_i) \mid HT(h_i \cdot w_i) = t\}\}$.

(b) $c_k + c_l \cdot a \neq 0$.
Then $\tilde{M} = (M - \{HC(f_l \cdot x_l)\}) \cup \{\{HC(h_i \cdot w_i) \mid HT(h_i \cdot w_i) = t\}\}$.

As the polynomials h_i with $HT(h_i \cdot w_i) = t$ are used to strongly right reduce $b \cdot t$ in $spol_s(f_k, f_l, x_k, x_l)$ we know $HC(h_i \cdot w_i) \leq b < HC(f_k \cdot x_k) \leq HC(f_l \cdot x_l)$ and hence $\tilde{M} \ll M$.
However we get a smaller representation of g contradicting our assumption. q.e.d.

6.2 Completion Using Right Reduction

Now we define critical pairs of polynomials via $\rightarrow^r$ and show a criterion that implies confluence for $\rightarrow^r$.

Definition 10
Given two polynomials $p_1, p_2 \in \mathbf{Z}[\mathcal{H}]$ with $HT(p_i) = t_i$, $i = 1, 2$. If there are $x_1, x_2 \in \mathcal{H}$ with $t_1 \cdot x_1 = t_2 \cdot x_2 = t$, let c_1, c_2 be the coefficients of t in $p_1 \cdot x_1$ respectively $p_2 \cdot x_2$. If $c_2 \geq c_1 > 0$ and $c_2 = a \cdot c_1 + b$, where $a, b \in \mathbf{Z}$, b a remainder of c_1, we get the following s–polynomial

$$spol(p_1, p_2, x_1, x_2) = a \cdot p_1 \cdot x_1 - p_2 \cdot x_2.$$

Let $U_{HM(p_1),HM(p_2)} \subseteq \mathcal{H}^2$ be the set containing all pairs $x_1, x_2 \in \mathcal{H}$ as above.

Notice that $p_1 = p_2$ is possible. The set $U_{HM(p_1),HM(p_2)}$ can be empty, finite or even infinite depending on $\mathcal{H}$, i.e. given a finite set $F \subseteq \mathbf{Z}[\mathcal{H}]$ the set of critical situations belonging to the polynomials in F can be infinite.

Theorem 9
Let $F \subseteq \mathbf{Z}[\mathcal{H}]$, F saturated. Equivalent are:

1. *F is a Gröbner basis via $\rightarrow^r$.*
2. *$ideal_r(F) \stackrel{*}{\rightarrow}^r_F 0$.*

3. *For all not necessarily different* $f_k, f_l \in F, (x_k, x_l) \in U_{HM(f_k),HM(f_l)}$ *we have:*

$$spol(f_k, f_l, x_k, x_l) \xrightarrow{*}{}^{r}_{F} 0.$$

Proof :

$1 \Rightarrow 2$ By theorem 1 $f \in ideal_r(F)$ implies $f \overset{*}{\leftrightarrow}{}^{r}_{F} 0$ and as G is confluent $f \xrightarrow{*}{}^{r}_{F} 0$.

$2 \Rightarrow 1$ Since $\rightarrow^r_F$ is Noetherian, we only have to prove local confluence.
Suppose $f \rightarrow^r_F f_1, f \rightarrow^r_F f_2$ and $f_1 \neq f_2$. Then $f_1 - f_2 \in ideal_r(F)$ and, therefore, $f_1 - f_2 \xrightarrow{*}{}^{r}_{F} 0$. By lemma 5 there exists $g \in \mathbf{Z}[\mathcal{H}]$ such that $f_1 \xrightarrow{*}{}^{r}_{F} g, f_2 \xrightarrow{*}{}^{r}_{F} g$, i.e. $\rightarrow^r_F$ is confluent.

$2 \Rightarrow 3$ Let $(x_k, x_l) \in U_{HM(f_k),HM(f_l)}$ give us a s–polynomial of f_k, f_l. Then by definition 10 we get

$$spol(f_k, f_l, x_k, x_l) = a \cdot f_k \cdot x_k - f_l \cdot x_l \in ideal_r(F).$$

and hence $spol(f_k, f_l, x_k, x_l) \xrightarrow{*}{}^{r}_{F} 0$.

$3 \Rightarrow 2$ We have to show that every element $g \in ideal_r(F) - \{0\}$ is $\rightarrow^r_F$–reducible to zero. As $\rightarrow^r_F$ is Noetherian and $h \in ideal_r(F)$, $h \rightarrow^r_F h'$ implies $h' \in ideal_r(F)$, it suffices to show that every element $g \in ideal_r(F) - \{0\}$ is $\rightarrow^r_F$–reducible.
Let $g = \sum_{i=1}^{m} c_i \cdot f_i \cdot x_i$, where $c_i \in \mathbf{Z}, f_i \in F, x_i \in \mathcal{H}$.
Depending on this representation of g we define $t = max\{HT(f_i \cdot x_i) \mid i \in \{1, \ldots m\}\}, M = \{\{HC(f_i \cdot x_i) \mid HT(f_i \cdot x_i) = t\}\}$. (Note that M is a multiset with elements in $\mathbf{Z}$).
We call another representation of g with $\tilde{t}, \tilde{M}$ *smaller* if $\tilde{t} < t$ or $\tilde{t} = t$ and $\tilde{M} \ll M$.
By lemma 7 we can assume $HT(f_i \cdot x_i) = HT(f_i) \cdot x_i$ and $HC(f_i \cdot x_i) > 0$, as if $HT(f_i \cdot x_i) \neq HT(f_i) \cdot x_i$ for some f_i in our representation of g, we know $f_i \cdot x_i \rightarrow^r_F 0$, i.e. $f_i \cdot x_i = d_i \cdot f_i' \cdot x_i'$ for some $d_i \in \mathbf{Z}, f_i' \in F, x_i' \in \mathcal{H}$ and $HT(f_i \cdot x_i) = HT(f_i' \cdot x_i') = HT(f_i') \cdot x_i' = t$ together with $HC(f_i' \cdot x_i') \leq_Z HC(f_i \cdot x_i)$ gives us that the representation is not increased by substituting $d_i \cdot f_i' \cdot x_i'$ for $f_i \cdot x_i$.
Note that now M is a multiset with elements in $\mathbf{N}$, since $HC(f_i' \cdot x_i') \in \mathbf{N}$.
Our intention is to show that if t, M belong to a minimal representation of g [31], then $|M| = 1$, e.g. $M = \{\{HC(f_k \cdot x_k)\}\}$. This gives us $HT(g) = t = HT(f_k) \cdot x_k$ and as $HC(f_k \cdot x_k) > 0$, g is $\rightarrow^r_F$–reducible by f_k.
Let us assume there is a polynomial $g \in ideal_r(F) - \{0\}$ with a minimal representation $g = \sum_{i=1}^{m} c_i \cdot f_i \cdot x_i$ together with t, M and $|M| > 1$.
Let $HC(f_k \cdot x_k), HC(f_l \cdot x_l) \in M$,$k \neq l$ [32] and $a \cdot HC(f_k \cdot x_k) + b = HC(f_l \cdot x_l)$ for $a, b \in \mathbf{Z}$,b a remainder of $HC(f_k \cdot x_k)$. Since $HT(f_k) \cdot x_k = HT(f_l) \cdot x_l$ by definition 10 we have an s–polynomial $spol(f_k, f_l, x_k, x_l) = a \cdot f_k \cdot x_k - f_l \cdot x_l$, and let us assume $spol(f_k, f_l, x_k, x_l) \neq 0$ [33].

[31] Such minimal representations of polynomials exist as our ordering on representations as defined above is well–founded.

[32] Not necessarily $f_l \neq f_k$.

[33] In case $spol(f_k, f_l, x_k, x_l) = 0$ the proof is similar. Substituting 0 for $\sum_{i=1}^{n} d_i \cdot h_i \cdot w_i$ in the equations below immediately gives us a smaller representation of g, contradicting our assumption.

Now $spol(f_k, f_l, x_k, x_l) \xrightarrow{*}_F 0$ implies $a \cdot f_k \cdot x_k - f_l \cdot x_l = \sum_{i=1}^{n} d_i \cdot h_i \cdot w_i, d_i \in \mathbf{Z}, h_i \in F, w_i \in \mathcal{H}$, where the h_i are due to the reduction of the s–polynomial to zero, i.e. all terms occurring in the sum are bounded by $HT(spol(f_k, f_l, x_k, x_l)) \leq t$ and $HC(h_i \cdot w_i) > 0$.
Now we get:

$$\begin{aligned}
g &= c_k \cdot f_k \cdot x_k + c_l \cdot f_l \cdot x_l + \sum_{\substack{i=1 \\ k \neq i \neq l}}^{m} c_i \cdot f_i \cdot x_i \\
&= c_k \cdot f_k \cdot x_k + \underbrace{c_l \cdot a \cdot f_k \cdot x_k - c_l \cdot a \cdot f_k \cdot x_k}_{=0} + c_l \cdot f_l \cdot x_l + \sum_{\substack{i=1 \\ k \neq i \neq l}}^{m} c_i \cdot f_i \cdot x_i \\
&= (c_k + c_l \cdot a) \cdot f_k \cdot x_k - c_l \cdot \underbrace{(a \cdot f_k \cdot x_k - f_l \cdot x_l)}_{= spol(f_k, f_l, x_k, x_l)} + \sum_{\substack{i=1 \\ k \neq i \neq l}}^{m} c_i \cdot f_i \cdot x_i \\
&= (c_k + c_l \cdot a) \cdot f_k \cdot x_k - c_l \cdot (\sum_{i=1}^{n} d_i \cdot h_i \cdot w_i) + \sum_{\substack{i=1 \\ k \neq i \neq l}}^{m} c_i \cdot f_i \cdot x_i
\end{aligned}$$

and depending on this new representation of g we define $\tilde{t} = max\{HT(h_i \cdot w_i), HT(f_i \cdot x_i) \mid h_i, f_i$ appearing in the sum $\}$, $\tilde{M} = \{\{HC(h_i \cdot w_i), HC(f_i \cdot x_i) \mid HT(h_i \cdot w_i) = \tilde{t}, HT(f_i \cdot x_i) = \tilde{t}\}\}$ and we either get $\tilde{t} < t$ or $\tilde{t} = t$ and we have to distinguish two cases:

(a) $c_k + c_l \cdot a = 0$.
Then $\tilde{M} = (M - \{HC(f_k \cdot x_k), HC(f_l \cdot x_l)\}) \cup \{\{HC(h_i \cdot w_i) \mid HT(h_i \cdot w_i) = t\}\}$.

(b) $c_k + c_l \cdot a \neq 0$.
Then $\tilde{M} = (M - \{HC(f_l \cdot x_l)\}) \cup \{\{HC(h_i \cdot w_i) \mid HT(h_i \cdot w_i) = t\}\}$.

As the polynomials h_i with $HT(h_i) \cdot w_i = t$ are used to right reduce $b \cdot t$ in $spol(f_k, f_l, x_k, x_l)$ we know $0 < HC(h_i \cdot w_i) \leq b < HC(f_k \cdot x_k) \leq HC(f_l \cdot x_l)$ and hence $\tilde{M} \ll M$.
However we get a smaller representation of g contradicting our assumption. q.e.d.

Unfortunately theorem 9 is only of theoretical interest as in general it only provides an infinite test verifying that a set is a Gröbner basis. Trying to localize this test severe problems arise, as our reduction relation is not transitive (compare remark 4).
In ordinary polynomial rings as $\mathbf{Z}[x_1, \ldots x_n]$ one can select a "smallest" critical pair by taking the least common multiply of t_1 and t_2 and it is sufficient to examine this case [KaKa84, KaKa88]. In $\mathbf{Z}[\mathcal{H}]$ the situation is more complicated. Reviewing definition 10 we see that it is important to solve the equation $t_1 \cdot x = t_2 \cdot y$.
Therefore, we are looking for a suitable "basis" of a set

$$U_{t_1,t_2} = \{(x_1, x_2) \in \mathcal{H}^2 \mid t_1 \cdot x_1 = t_2 \cdot x_2\}.$$

One idea might be to look at a basis $B_{t_1,t_2} \subseteq U_{t_1,t_2}$ such that for all $(x_1, x_2) \in U_{t_1,t_2}$ we have $(b_1, b_2) \in B_{t_1,t_2}, m \in \mathcal{H}$ fulfilling $x_1 = b_1 \cdot m, x_2 = b_2 \cdot m$. But this is not sufficient as the following example shows:

Example 8
Let $\Sigma = \{a, b, c, d, e, f\}$ with $d \succ a \succ b \succ c \succ e \succ f$ and $T = \{abc \to d^2, b^2ce \to d^2f\}$.
Take $F = \{a + b, b^2c + d^2, d^2e + d^2f, d + \lambda\}$.
Looking at $a + b$ and $d + \lambda$ we get a critical situation in d^2 which leads to $b^2c - d$ and $b^2c - d \xrightarrow{*}_F 0$. But d^2e gives us $d^2f - de$, which does not right reduce to zero by F. The clue is that d^2 is no "real" critical situation, in the sense that $a + b$ cannot be applied to right reduce d^2, but d^2e can be right reduced by both, $a + b$ and $d + \lambda$.

Example 8 is due to the fact that we have an s–polynomial $spol(p_1, p_2, x_1, x_2)$, where $RED(p_1) \cdot x_1 > HD(p_1) \cdot x_1$ or $RED(p_2) \cdot x_2 > HD(p_2) \cdot x_2$, which can be reduced to zero by saturating sets for p_1 and p_2, while $spol(p_1, p_2, x_1, x_2) \cdot z$ with $z \in \mathcal{H}$ is not trivial according to those sets. Even taking a saturated set of polynomials into account does not guarantee the Gröbner basis property, as the set F in our example is a (prefix) saturated set.
Another approach might be to look for a suitable basis of a set

$$U_{p_1,p_2} = \{(x_1, x_2) \in \mathcal{H}^2 \mid HT(p_1 \cdot x_1) = t_1 \cdot x_1 = t_2 \cdot x_2 = HT(p_2 \cdot x_2),$$
$$HC(p_1 \cdot x_1), HC(p_2 \cdot x_2) > 0\}.$$

U_{p_1,p_2} describes real critical situations in the sense that $t_1 \cdot x_1 = t_2 \cdot x_2$ is an overlap, where both p_1 and p_2 can be applied for reduction. But even a "basis" for such a set is not sufficient.

Example 9
Let $\Sigma = \{a, b, c, d, e, f, g\}$ with $a \succ b \succ c \succ d \succ e \succ f \succ g$ and $T = \{ac \to d, bc \to e, dg \to b, eg \to f\}$.
Take $F = \{a + b, d + e, b + f, fc + e, d + \lambda, b + g, gc + e, e + g, g^2 + f, g + \lambda\}$.
Looking at $a + b$ and $d + \lambda$ we get a real critical situation in d, which leads to $e - \lambda \to^r_{e+g} -g - \lambda \to^r_{g+\lambda} 0$, but $(e - \lambda) \cdot g = f - g$ is F–irreducible.

As seen in example 9 even (prefix) saturated sets do not guarantee that $p \xrightarrow{*}_F 0$ implies $p \cdot x \xrightarrow{*}_F 0$ for $p \in \mathbf{Z}[\mathcal{H}], x \in \mathcal{H}$. Now prefix right reduction is transitive and gives enough information to cope with this defect. It will enable us to formulate another characterization of Gröbner bases.

6.3 Completion Using Prefix Right Reduction

Prefix saturation enriches a polynomial p by adding a set $S \in \mathcal{SAT}_p(p)$ such that we can substitute $q \to_p^{(s,r)} q'$ by $q \to^p_{p' \in S} q'$. Therefore, we have more information on the reduction step than using (strong) right reduction, enabling a finite confluence criterion.

Lemma 12
Let $F \subseteq \mathbf{Z}[\mathcal{H}]$ and $p, q \in \mathbf{Z}[\mathcal{H}]$. Let $p \to^p_q 0$ and $q \xrightarrow{*}_F 0$. From these reduction sequences we get the representations $p = d \cdot q \cdot x$ and $q = \sum_{i=1}^k d_i \cdot g_i \cdot x_i$, for $d, d_i \in \mathbf{Z}, g_i \in F, x, x_i \in \mathcal{H}$, where the following statements hold:

1. $HM(p) \geq d_i \cdot g_i \cdot x_i \cdot x$ *for all* $i \in \{1, \ldots k\}$.

2. *If* $HT(p) = HT(g_i \cdot x_i \cdot x)$ *then* $HT(g_i \cdot x_i \cdot x) = HT(g_i \cdot x_i)x$ *and* $HC(g_i \cdot x_i \cdot x) \leq |HC(p)|$.

Proof : Since $p \rightarrow_q^p 0$ and $p = d \cdot q \cdot x$ we know $HT(p) = HT(q)x$, $HC(q) > 0$ and $HC(p) = d \cdot HC(q)$.
In case $HT(g_i \cdot x_i) = HT(q)$ we get $HC(q) \geq d_i \cdot HC(g_i \cdot x_i)$, as g_i then is used to reduce $HM(q)$. Further $HT(q) \geq HT(g_i \cdot x_i) > RED(g_i \cdot x_i)$ gives us $HT(p) = HT(q)x \geq t$, for all $t \in T(g_i \cdot x_i \cdot x)$, $i \in \{1, \ldots k\}$. Together this gives us $HM(p) = d \cdot HM(q) \cdot x \geq d_i \cdot g_i \cdot x_i \cdot x$ for all $i \in \{1, \ldots k\}$.
Now let us assume $HT(p) = HT(g_i \cdot x_i \cdot x) \neq HT(g_i \cdot x_i)x$ for some $i \in \{1, \ldots k\}$. Let $HT(g_i \cdot x_i) = t_i$ and $HT(g_i \cdot x_i \cdot x) = t_j \cdot x$. Then $HT(q) \geq t_i > t_j$ [34], but $HT(q) > t_j$ implies $HT(q)x > t_j \cdot x$ contradicting our assumption that $HT(q)x = t_j \cdot x$.
Therefore, $HT(p) = HT(g_i \cdot x_i \cdot x)$ implies $HT(g_i \cdot x_i) = HT(q)$ and $HT(g_i \cdot x_i \cdot x) = HT(g_i \cdot x_i)x$. As g_i is used to right reduce $HT(q)$ we have $HC(g_i \cdot x_i \cdot x) = HC(g_i \cdot x_i) \leq HC(q) \leq |d| \cdot HC(q) \leq |HC(p)|$ [35]. q.e.d.

We can even restrict ourselves to special s–polynomials to localize our confluence test.

Definition 11 (Prefix s–polynomials)
Given two polynomials $p_1, p_2 \in \mathbf{Z}[\mathcal{H}]$ with $HC(p_i) = c_i > 0, HT(p_i) = t_i, RED(p_i) = r_i$ for $i = 1, 2$. If there is $x \in \mathcal{H}$ with $t_1 = t_2 x$ we have to distinguish:

1. If $c_1 \geq c_2$, $c_1 = a \cdot c_2 + b$, where $a, b \in \mathbf{Z}$, b a remainder of c_2, we get the following superposition causing a critical pair:

$$\begin{array}{ccc} & a \cdot c_2 \cdot t_2 x + b \cdot t_2 x = c_1 \cdot t_1 & \\ \swarrow & & \searrow \\ -a \cdot r_2 \cdot x + b \cdot t_2 x & & -r_1 \end{array}$$

   This gives us the prefix s–polynomial

$$spol_p(p_1, p_2) = a \cdot r_2 \cdot x - b \cdot t_2 x - r_1 = a \cdot p_2 \cdot x - p_1.$$

2. If $c_2 > c_1$, $c_2 = a \cdot c_1 + b$, where $a, b \in \mathbf{Z}$, b a remainder of c_1, we get the following superposition causing a critical pair:

$$\begin{array}{ccc} & c_2 \cdot t_2 x = a \cdot c_1 \cdot t_1 + b \cdot t_1 & \\ \swarrow & & \searrow \\ -r_2 \cdot x & & -a \cdot r_1 + b \cdot t_1 \end{array}$$

   This gives us the prefix s–polynomial

$$spol_p(p_1, p_2) = a \cdot r_1 - r_2 \cdot x - b \cdot t_1 = a \cdot p_1 - p_2 \cdot x.$$

[34] As $t_i = HT(g_i \cdot x_i)$ and $t_j \in T(RED(g_i \cdot x_i))$.
[35] Remember that in this case $HC(q) = HC(q \cdot x)$.

Notice that as two polynomials at most give us one prefix s–polynomial, a finite set $F \subseteq \mathbf{Z}[\mathcal{H}]$ only gives us finitely many prefix s–polynomials.

Theorem 10
Let $F \subseteq \mathbf{Z}[\mathcal{H}]$, F prefix saturated. Equivalent are:

1. *F is a Gröbner basis via $\rightarrow^r$.*
2. *$ideal_r(F) \stackrel{*}{\rightarrow}_F^r 0$*
3. *For all $f_k, f_l \in F$ we have $spol_p(f_k, f_l) \stackrel{*}{\rightarrow}_F^r 0$.*

Proof :

$1 \Leftrightarrow 2$ Follows from theorem 9.

$2 \Rightarrow 3$ Let $HT(f_k) = HT(f_l)x$ for $x \in \mathcal{H}$, $HC(f_k) \geq HC(f_l) > 0$ and $HC(f_k) = a \cdot HC(f_l) + b$, where $a, b \in \mathbf{Z}$ and b is a remainder of $HC(f_l)$ (the other case is similar). Then by definition 11 we get

$$spol_p(f_k, f_l) = a \cdot f_l \cdot x - f_k \ \in ideal_r(F),$$

and hence $spol_p(f_k, f_l) \stackrel{*}{\rightarrow}_F^r 0$.

$3 \Rightarrow 2$ We have to show that every element $g \in ideal_r(F)$ is $\rightarrow_F^r$-reducible to zero. As $\rightarrow_F^r$ is Noetherian and $h \in ideal_r(F)$, $h \rightarrow_F^r h'$ implies $h' \in ideal_r(F)$, it suffices to show that every element $g \in ideal_r(F) - \{0\}$ is $\rightarrow_F^r$-reducible.
Let $g = \sum_{i=1}^m c_i \cdot f_i \cdot x_i$, where $c_i \in \mathbf{Z}, f_i \in F, x_i \in \mathcal{H}$.
Depending on this representation of g we define $t = max\{HT(f_i \cdot x_i) \mid i \in \{1, \ldots m\}\}, M = \{\{HC(f_i) \mid HT(f_i \cdot x_i) = t\}\}$. (Note that M is a multiset with elements in $\mathbf{Z}$).
We call another representation of g with $\tilde{t}, \tilde{M}$ *smaller* if $\tilde{t} < t$ or $\tilde{t} = t$ and $\tilde{M} \ll M$.
By lemma 7 we can assume $HT(f_i \cdot x_i) = HT(f_i)x_i$ and $HC(f_i) > 0$, as if $HT(f_i \cdot x_i) \neq HT(f_i)x_i$ for some f_i in our representation of g, we know $f_i \cdot x_i \rightarrow_F^p 0$, i.e. $f_i \cdot x_i = d_i \cdot f_i' \cdot x_i'$ for some $d_i \in \mathbf{Z}, f_i' \in F, x_i' \in \mathcal{H}$ and $HT(f_i \cdot x_i) = HT(f_i' \cdot x_i') = HT(f_i')x_i' = t$ together with $HC(f_i') \leq_Z HC(f_i)$ gives us that the representation is not increased by substituting $d_i \cdot f_i' \cdot x_i'$ for $f_i \cdot x_i$. Important is that now M is a multiset with elements in $\mathbf{N}$, since $HC(f_i) > 0$.
Our intention is to show that if t, M belong to a minimal representation of g [36], then $|M| = 1$, e.g. $M = \{\{HC(f_k)\}\}$. This gives us $HT(g) = t = HT(f_k)x_k$ and as $HC(f_k) > 0$, g is $\rightarrow_F^r$-reducible by f_k.
Let us assume there is a polynomial $g \in ideal_r(F) - \{0\}$ with a minimal representation $g = \sum_{i=1}^m c_i \cdot f_i \cdot x_i$ together with t,M and $|M| > 1$.

[36] Such minimal representations of polynomials exist as our ordering on representations as defined above is well-founded.

Let $HC(f_k), HC(f_l) \in M, k \neq l$ [37] and $a \cdot HC(f_k) + b = HC(f_l)$ for $a, b \in \mathbf{Z}$, b a remainder of $HC(f_k)$.
Since $HT(f_k)x_k = HT(f_l)x_l$ we have either $HT(f_k)z = HT(f_l)$ or $HT(f_k) = HT(f_l)z$ for some $z \in \mathcal{H}$. Without loss of generality let us assume $HT(f_k)z = HT(f_l)$ and hence $x_k = zx_l$. Then by definition 11 we have a prefix s-polynomial such that

$$a \cdot f_k \cdot x_k - f_l \cdot x_l = a \cdot f_k \cdot zx_l - f_l \cdot x_l = spol_p(f_k, f_l) \cdot x_l.$$

In case $spol_p(f_k, f_l) \neq 0$ [38] this implies $HT(spol_p(f_k, f_l) \cdot x_l) \leq t$, as $HT(spol_p(f_k, f_l)) \leq HT(f_l)$ and $t = HT(f_l)x_l$.
In case $b = 0$ we have $HT(spol_p(f_k, f_l) \cdot x_l) < t$ and $spol_p(f_k, f_l) \xrightarrow{*}{}^{r}_{F} 0$ implies $spol_p(f_k, f_l) = \sum_{i=1}^{n} d_i \cdot h_i \cdot w_i, d_i \in \mathbf{Z}, h_i \in F, w_i \in \mathcal{H}$, where the h_i are due to the reduction of $spol_p(f_k, f_l)$ and all terms occurring in the sum $spol_p(f_k, f_l) \cdot x_l = \sum_{i=1}^{n} d_i \cdot h_i \cdot w_i \cdot x_l$ are bounded by $HT(spol_p(f_k, f_l) \cdot x_l) < t$.
In case $b \neq 0$ we get $HT(spol_p(f_k, f_l) \cdot x_l) = HT(spol_p(f_k, f_l))x_l = HT(f_l)x_l = t$ and $spol_p(f_k, f_l) \cdot x_l \rightarrow^{p}_{spol_p(f_k,f_l)} 0$. Then lemma 12 implies $spol_p(f_k, f_l) = \sum_{i=1}^{n} d_i \cdot h_i \cdot w_i, d_i \in \mathbf{Z}, h_i \in F, w_i \in \mathcal{H}$, where the h_i are due to the reduction of $spol_p(f_k, f_l)$ and all terms occurring in the sum $spol_p(f_k, f_l) \cdot x_l = \sum_{i=1}^{n} d_i \cdot h_i \cdot w_i \cdot x_l$ are bounded by t.
In both cases we can substitute $h_i \cdot w_i \cdot x_l$ by $h'_i \cdot w'_i$ (without increasing the representation) such that $HT(h'_i \cdot w'_i) = HT(h'_i)w'_i$ and $HC(h'_i) > 0$ by lemma 7 since F is prefix saturated.
Now we get:

$$\begin{aligned}
g &= c_k \cdot f_k \cdot x_k + c_l \cdot f_l \cdot x_l + \sum_{\substack{i=1 \\ k \neq i \neq l}}^{m} c_i \cdot f_i \cdot x_i \\
&= c_k \cdot f_k \cdot x_k + \underbrace{c_l \cdot a \cdot f_k \cdot x_k - c_l \cdot a \cdot f_k \cdot x_k}_{=0} + c_l \cdot f_l \cdot x_l + \sum_{\substack{i=1 \\ k \neq i \neq l}}^{m} c_i \cdot f_i \cdot x_i \\
&= (c_k + c_l \cdot a) \cdot f_k \cdot x_k - c_l \cdot \underbrace{(a \cdot f_k \cdot x_k - f_l \cdot x_l)}_{= spol_p(f_k, f_l) \cdot x_l} + \sum_{\substack{i=1 \\ k \neq i \neq l}}^{m} c_i \cdot f_i \cdot x_i \\
&= (c_k + c_l \cdot a) \cdot f_k \cdot x_k - c_l \cdot (\sum_{i=1}^{n} d_i \cdot h'_i \cdot w'_i) + \sum_{\substack{i=1 \\ k \neq i \neq l}}^{m} c_i \cdot f_i \cdot x_i \qquad (1)
\end{aligned}$$

and depending on this new representation of g we define $\tilde{t} = max\{HT(h'_i \cdot w'_i), HT(f_i \cdot x_i) \mid h'_i, f_i$ appearing in (1) $\}, \tilde{M} = \{\{HC(h'_i), HC(f_i) \mid HT(h'_i \cdot w'_i) = \tilde{t}, HT(f_i \cdot x_i) = \tilde{t}\}\}$

and we either get $\tilde{t} < t$ or $\tilde{t} = t$ and we have to distinguish two cases:

[37] Not necessarily $f_l \neq f_k$.

[38] In case $spol_p(f_k, f_l) = 0$ the proof is similar. Substituting 0 for $\sum_{i=1}^{n} d_i \cdot h_i \cdot w_i$ in the equations below immediately gives us a smaller representation of g, contradicting our assumption.

(a) $c_k + c_l \cdot a = 0$.
Then $\tilde{M} = (M - \{HC(f_k), HC(f_l)\}) \cup \{\{HC(h_i') \mid HT(h_i') \cdot w_i' = t\}\}$.

(b) $c_k + c_l \cdot a \neq 0$.
Then $\tilde{M} = (M - \{HC(f_l)\}) \cup \{\{HC(h_i') \mid HT(h_i') \cdot w_i' = t\}\}$.

By lemma 12 we know that if there are polynomials h_i' with $HT(h_i') \cdot w_i' = t$, the corresponding polynomials h_i from above are used to right reduce $HM(spol_p(f_k, f_l))$ and, therefore, $HC(h_i') \leq HC(spol_p(f_k, f_l)) = b < HC(f_k) \leq HC(f_l)$, hence $\tilde{M} \ll M$.
However we get a smaller representation of g contradicting our assumption. q.e.d.

In fact we have shown the existence of Gröbner basis with respect to a weaker reduction, namely prefix right reduction.

Corollary 4
Let $F \subseteq \mathbf{Z}[\mathcal{H}]$, F prefix saturated. Equivalent are:

1. *F is a Gröbner basis via $\rightarrow^p$.*
2. *$ideal_r(F) \xrightarrow{*}{}_F^p 0$*
3. *For all $f_k, f_l \in F$ we have $S_p \xrightarrow{*}{}_F^r 0$, where $S_p \in \mathcal{SAT}_p(spol_p(f_k, f_l))$.*

Proof : Let $g \in ideal_r(F) - \{0\}$. Then for a minimal representation t, M of g as described in the proof of theorem 10, we have $M = \{\{HC(f_k \cdot x_k)\}\}$ and $t = HT(g) = HT(f_k)x_k$ and $HC(f_k) > 0$, i.e. g is $\rightarrow_F^p$–reducible by f_k. q.e.d.

Using the localisation given in theorem 10 we can state the following procedure.

Procedure Completion with respect to Prefix Saturation

input: $F \subseteq \mathbf{Z}[\mathcal{H}]$, $F = \{f_1, \ldots f_n\}$
output: $\textsc{Gb}(F)$, a Gröbner basis of $ideal_r(F)$ with respect to $\rightarrow^r$ (even $\rightarrow^p$).

$G := \bigcup_{i=1}^n \textsc{Sat}_p(f_i)$;
$B := \{(q_1, q_2) \mid q_1, q_2 \in G, q_1 \neq q_2\}$;
while $B \neq \emptyset$ do
    $(q_1, q_2) :=$ remove(B);
    if $h := spol_p(q_1, q_2)$ exists then;
        $h' := hnf(h, G)$;
        if $h' \neq 0$ then
            $B := B \cup \{(f, \tilde{h}) \mid f \in G, \tilde{h} \in \textsc{Sat}_p(h')\}$;
            $G := G \cup \textsc{Sat}_p(h')$;
endwhile
$\textsc{Gb}(F) := G$

where SAT_p denotes the output of our prefix saturation procedure, *remove* removes an element from a set and $hnf(g, G)$ computes a "canonized normal form" of g with respect to G, where only right reduction at the head monomial is allowed.
There are two critical points, why this procedure might not terminate: prefix saturation of a polynomial need not terminate and the set B need not become empty.

Theorem 11
In case the procedure terminates the output is a Gröbner basis even with respect to prefix right reduction.

Proof : This follows immediately from theorem 10 and its corollary. q.e.d.

Note that in general monoid rings are not (right–, left–) Noetherian, i.e. not every ideal can be finitely generated. Our intention is to show that in special cases finitely generated right ideals allow finite Gröbner bases, even when the corresponding monoid ring is not right–Noetherian.

Theorem 12
Let $F \subseteq \mathbf{Z}[\mathcal{H}]$ be finite. The procedure terminates when $\mathcal{H}$ is a finite monoid.

Proof :
The procedure stops as soon as all s–polynomials reduce to zero.
Now suppose that our procedure does not terminate.
Then since $\mathcal{H}$ is finite there is a term $t \in \mathcal{H}$, which occurs infinitely many times among the head terms of the polynomials h' as computed in the above procedure and added to G, i.e. we get an infinite set $\{a_i \cdot t \mid a_i \in \mathbf{N}\}$ of head terms, where the polynomial with head coefficient a_{i+1} is added later than the polynomial with head coefficient a_i. Since the h' are in normal form we get a descending sequence $a_k > a_{k-1} > \ldots > a_i > \ldots > 0$ in $\mathbf{N}$ contradicting the fact that $(\mathbf{N}, <)$ is well–founded. q.e.d.

Theorem 13
Let $F \subseteq \mathbf{Z}[\mathcal{H}]$ be finite. The procedure terminates when $\mathcal{H}$ is a free monoid presented by finite Σ and $T = \emptyset$.

Proof :
Since we have $\text{SAT}_p(p) = \{\text{canon}(p)\}$ in this case as $T = \emptyset$, we have to take a closer look at the s–polynomials. Looking at the critical overlaps we see that all polynomials q added have $|HT(q)| \leq max\{|HT(f)| \mid f \in F\}$. Further the head of any added polynomial is in canonized normal form with respect to the already computed set G. Hence if $HT(q)$ occurs among the head terms of the polynomials in G, it has a smaller head coefficient as it is not further reducible by G. That is if $a_i \in \mathbf{N}$ is the head coefficient of the first occurrence of a head term s_i then this term can at most occur $a_i - 1$ times as a head term and since there are only finitely many candidates for head terms our procedure terminates. q.e.d.

In the following we will take a closer look at monadic presentations of monoids and groups. We state the following useful lemma.

Lemma 13
Let (Σ, T) be a finite convergent interreduced monadic presentation of a cancellative monoid $\mathcal{H}$. Then no rules of the form $xa \to a$ or $ax \to a$ appear in T for $a \in \Sigma$.

Proof : Suppose we have $xa \to a \in T$. Since $\mathcal{H}$ is cancellative $xa \overset{*}{\leftrightarrow}_T a$ implies $x \overset{*}{\leftrightarrow}_T \lambda$. As T is finite convergent we have $x \overset{*}{\to}_T \lambda$ contradicting that T is interreduced. q.e.d.

This lemma allows us to conclude that $axb \to c \in T$, $a, b, c \in \Sigma, x \in \Sigma^*$, implies $a \neq c$ and $b \neq c$.

Theorem 14
Let $F \subseteq \mathbf{Z}[\mathcal{H}]$ be finite. The procedure terminates when $\mathcal{H}$ is a group presented by a finite convergent interreduced 2–monadic system including inverses of length 1 for the generators.

Proof :

1. We say a polynomial q has property $\mathcal{P}_F$ if and only if

   (α) $|HT(q)| \leq K$, where $K = max\{|HT(f)| \mid f \in F\} + 1$.

   (β) If $|HT(q)| = K$ then there is $a \in \Sigma$ such that

   (i) all terms of length K in q have a as a common suffix.

   (ii) for all $s \in T(q)$ with $|s| = K - 1$ we either have $s = s_1 a$ or in case $s = s_1 d$, $d \in \Sigma - \{a\}$ there is a rule $ea \to d \in T, e \in \Sigma$.

   We will show that all polynomials q computed by our procedure for input F have $\mathcal{P}_F$.
   By the choice of K all input polynomials have $\mathcal{P}_F$.
   Let G be an already computed prefix saturated set of polynomials having $\mathcal{P}_F$, let q be the next polynomial computed by our procedure.
   Showing that q has $\mathcal{P}_F$ we have to distinguish three cases:

   (a) In case q is due to saturating a polynomial q' with a rule $ab \to c \in T, c \in \Sigma \cup \{\lambda\}$ we can show that $\mathcal{P}_F$ is preserved. Note that only the case $|HT(q)| = K$ is critical.

      i. In case $|HT(q')| < K$ and $|HT(q)| = K$ we know $HT(q) = tb$ and for all $s \in T(q')$ with $|s \cdot b| = K - 1$ either $s \cdot b = sb \in IRR(T)$ or $s = s_1 e$ and $s \cdot b = s_1 e \cdot b = s_1 d$, where $eb \to d \in T$. Note that these are the only possibilities to gain a term of length $K - 1$ from a term of length less or equal to $K - 1$ by multiplication with a letter b.

      ii. Let $|HT(q')| = K$ with $HT(q') = ta$. We can only lose $\mathcal{P}_F$ in case we have $t_1, t_2 \in T(q')$ such that $|t_1| = K, |t_2| = K - 1, t_1 = t_1' a$ and $t_1 \cdot b = t_1' c, t_2 \cdot b = t_2 b$ with $c \neq \lambda$. Therefore, we examine all $s \in T(q')$ with $|s| = K - 1$.

If there are none q must have $\mathcal{P}_F$, since then a term $s \in T(q')$ can only reach length $K-1$ by multiplication with b in case $|s| = K-2$ and $sb \in IRR(T)$. Since $ab \to c \in T$ and $\mathcal{G}$ is a group including inverses of length 1 for the generators a has an inverse a^{-1} and $b \overset{*}{\leftrightarrow}_T a^{-1}ab \overset{*}{\leftrightarrow}_T a^{-1}c$ gives us the existence of a rule $a^{-1}c \to b \in T$ as T is confluent [39].
Now let $s \in T(q')$ have length $K-1$.
In case $s = s_1 a$ there is nothing to show [40].
In case $s = s_1 d, d \neq a$ we know that there is a rule $ea \to d \in T$ as q' has $\mathcal{P}_F$. Then we have $db \leftarrow eab \to ec$ and since $ea \to d \in T$ gives us $e \neq d$ there are rules $db \to g, ec \to g \in T, g \in \Sigma$.

(b) q is due to s–polynomial computation. As we use polynomials having $\mathcal{P}_F$ and prefix overlaps of their head terms to get q, in case $|HT(q)| = K$, q inherits $\mathcal{P}_F$ from the involved polynomials q_1, q_2, where $HT(q_1) = HT(q_2)z$ for some $z \in \mathcal{H}$.
In case $z = \lambda$ there is nothing to show.
Let $|HT(q_2)z| = K$ and $z \neq \lambda$, i.e. $z = z'a$ for some $a \in \Sigma$. Looking at $s \in T(q_2 \cdot z)$ we get that

i. $|s| < K-1$ is not critical.

ii. $|s| = K$ gives us $s = s_1 \cdot z$, where $s_1 \in T(q_2), |s_1| < K$, and as $s_1, z \in IRR(T)$ and T is monadic, we get $s = s_1' b z'' a$, where s_1' is a prefix of s_1, $b \in \Sigma \cup \{\lambda\}$, and z'' is a suffix of z'.

iii. $|s| = K-1$ gives us $s = s_1 \cdot z$, where $s_1 \in T(q_2), |s_1| < K$, and as $s_1, z \in IRR(T)$ and T is monadic either $s = s_1' b z'' a$ as above or $s = s_1' b$ and $|s_1| = K-1, s_1 = s_1' e$ and $ez'a \overset{*}{\to}_T fa \to b$, as T is 2–monadic, i.e. we have $fa \to b \in T$.

Since $T(q) \subseteq T(q_1) \cup T(q_2 \cdot z)$ we are done.

(c) q is the result of computing the canonized normal form of an s–polynomial using right reduction with respect to G at head monomials only.
The case $|HT(q)| < K$ is not critical.
Therefore, suppose $|HT(q)| = K$. We show that using right reduction on the head monomial of a polynomial q' having $\mathcal{P}_F$, with $|HT(q')| = K, HT(q') = ta, q' \to^r_{g \in G} q''$, gives us that q'' has $\mathcal{P}_F$.
Let $HT(g) = t'$ and $ta = t' \cdot x$ and $q'' = q' - k \cdot g \cdot x, k \in \mathbf{Z}, x \in \mathcal{H}$. Since G is prefix saturated we know $g \cdot x \to^p_{g' \in G} 0$, i.e. $HT(g) \cdot x = HT(g')z$ for some $z \in \mathcal{H}$, and g' has $\mathcal{P}_F$ [41]. Further $g' \cdot z$ has $\mathcal{P}_F$ [42] and as $q'' = q' - k \cdot g \cdot x = q' - k \cdot g' \cdot z$ we know $T(q'') \subseteq T(q') \cup T(g' \cdot z)$, and hence q'' likewise has $\mathcal{P}_F$.

2. The procedure stops as soon as all s–polynomials reduce to zero. Let us assume our procedure does not terminate. Then there are infinitely many s–polynomials $q_i, i \in \mathbf{N}$, with heads in canonized normal form added.

[39] This is no longer true in case a has an inverse u_a of length $|u_a| > 1$ or no inverse at all.
[40] Then $s \cdot b = s_1 a \cdot b = s_1 \cdot c$ and either $|s \cdot b| < K-1$ or $s \cdot b = s_1 c$.
[41] In case $|HT(g')| = K$ we have $z = \lambda$ and $g \cdot x = g'$.
[42] Compare the argumentation in (b).

As $|HT(q_i)| \leq K$ there is a term t, which occurs infinitely often as a head term among these polynomials, giving us a subsequence $q_k \in \mathbf{N}$ with $HT(q_k) = t$. Since the heads of all q_k are in canonized normal form with respect to the already computed set G including the q_k with lower index, the corresponding head coefficients $a_k \in \mathbf{N}$ have to decrease, i.e. $a_{k+1} < a_k$, contradicting the fact that $(\mathbf{N}, <)$ is well–founded. q.e.d.

Theorem 15
The existence of finite Gröbner bases for finitely generated right ideals in $\mathbf{Z}[\mathcal{H}]$ *has been shown in case*

1. $\mathcal{H}$ *is finite*
2. $\mathcal{H}$ *is a free finitely generated monoid*
3. $\mathcal{H}$ *is a plain group.*

Using the appropriate presentation the procedure "Completion with respect to Prefix Saturation" computes such bases.

As shown by Avenhaus, Madlener and Otto in [AvMaOt86] given a finite convergent, 2–monadic presentation of a group it is possible to get a finite convergent, 2–monadic presentation including inverses of length one for the generators of the same group. The same is possible for a finite convergent, monadic presentation including inverses of length one for the generators. All these presentations give us that our group is a free product of a finitely generated free group with finitely many finite groups.

6.4 Completion Using Commutative Reduction

In case we have a commutative monoid with a presentation $(\Sigma, T = T' \cup T_c)$, commutative saturation, as prefix saturation, enriches a polynomial and provides enough information to give a finite confluence test.

Definition 12 (Commutative s–polynomials)
Given two polynomials $p_1, p_2 \in \mathbf{Z}[\mathcal{H}]$ with $HC(p_2) = c_2 \geq HC(p_1) = c_1 > 0$, $HT(p_i) = t_i$, $RED(p_i) = r_i$ for $i = 1, 2$. If there are $x_1, x_2 \in \mathcal{H}$ such that $t_1 \circ x_1 = t_2 \circ x_2 \in IRR(T)$ is the least common multiple of t_1, t_2 in $\mathcal{F}_c(\Sigma)$ and $a, b \in \mathbf{Z}$, b a remainder of c_1 with $c_2 = a \cdot c_1 + b$, we get the following superposition causing a critical pair:

$$\begin{array}{ccc} & c_2 \cdot t_2 \circ x_2 = a \cdot c_1 \cdot t_1 \circ x_1 + b \cdot t_1 \circ x_1 & \\ \swarrow & & \searrow \\ -r_2 \cdot x_2 & & -a \cdot r_1 \cdot x_1 + b \cdot t_1 \circ x_1 \end{array}$$

This gives us the commutative s–polynomial

$$spol_c(p_1, p_2, x_1, x_2) = a \cdot r_1 \cdot x_1 - r_2 \cdot x_2 - b \cdot t_1 \cdot x_1 = a \cdot p_1 \cdot x_1 - p_2 \cdot x_2.$$

Lemma 14
Let $F \subseteq \mathbf{Z}[\mathcal{H}]$ and $p, q \in \mathbf{Z}[\mathcal{H}]$. Let $p \rightarrow_q^c 0$ and $q \stackrel{*}{\rightarrow}_F^r 0$. From these reduction sequences we get the representations $p = d \cdot q \cdot x$ and $q = \sum_{i=1}^{k} d_i \cdot g_i \cdot x_i$, for $d, d_i \in \mathbf{Z}, g_i \in F, x, x_i \in \mathcal{H}$, where the following statements hold:

1. *$HM(p) \geq d_i \cdot g_i \cdot x_i \cdot x$ for all $i \in \{1, \ldots k\}$.*
2. *If $HT(p) = HT(g_i \cdot x_i \cdot x)$ then $HT(g_i \cdot x_i \cdot x) = HT(g_i \cdot x_i) \circ x$ and $HC(g_i \cdot x_i \cdot x) \leq |HC(p)|$.*

Proof : Since $p \rightarrow_q^p 0$ and $p = d \cdot q \cdot x$ we know $HT(p) = HT(q) \circ x$, $HC(q) > 0$ and $HC(p) = d \cdot HC(q)$.
In case $HT(g_i \cdot x_i) = HT(q)$ we get $HC(q) \geq d_i \cdot HC(g_i \cdot x_i)$, as g_i then is used to reduce $HM(q)$. Further $HT(q) \geq HT(g_i \cdot x_i) > RED(g_i \cdot x_i)$ gives us $HT(p) = HT(q) \circ x \geq t$, for all $t \in T(g_i \cdot x_i \cdot x)$, $i \in \{1, \ldots k\}$. Together this gives us $HM(p) = d \cdot HM(q) \cdot x \geq d_i \cdot g_i \cdot x_i \cdot x$ for all $i \in \{1, \ldots k\}$.
Now let us assume $HT(p) = HT(g_i \cdot x_i \cdot x) \neq HT(g_i \cdot x_i) \circ x$ for some $i \in \{1, \ldots k\}$. Let $HT(g_i \cdot x_i) = t_i$ and $HT(g_i \cdot x_i \cdot x) = t_j \cdot x$. Then $HT(q) \geq t_i > t_j$ [43], but $HT(q) > t_j$ implies $HT(q) \circ x > t_j \cdot x$ contradicting our assumption that $HT(p) = HT(q) \circ x = HT(g_i \cdot x_i \cdot x) = t_j \cdot x$. Therefore, $HT(p) = HT(g_i \cdot x_i \cdot x)$ implies $HT(g_i \cdot x_i) = HT(q)$ and $HT(g_i \cdot x_i \cdot x) = HT(g_i \cdot x_i) \circ x$. As g_i is used to right reduce $HT(q)$ we get $HC(g_i \cdot x_i \cdot x) \leq HC(g_i \cdot x_i) \leq HC(q) \leq |d| \cdot HC(q) \leq |HC(p)|$. q.e.d.

Theorem 16
Let $F \subseteq \mathbf{Z}[\mathcal{H}]$, F commutatively saturated. Equivalent are:

1. *F is a Gröbner basis via $\rightarrow^r$.*
2. *$ideal_r(F) \stackrel{*}{\rightarrow}_F^r 0$.*
3. *For all $f_k, f_l \in F$ we have $spol_c(f_k, f_l) \stackrel{*}{\rightarrow}_F^r 0$.*

Proof :

$1 \Leftrightarrow 2$ Follows from theorem 9.

$2 \Rightarrow 3$ Let $HT(f_k) \circ x_k = HT(f_l) \circ x_l$ for $x_k, x_l \in \mathcal{H}$ be the least common multiple of $HT(f_k), HT(f_l)$, $HC(f_k) \geq HC(f_l) > 0$ and $HC(f_l) = a \cdot HC(f_k) + b$, where $a, b \in \mathbf{Z}$ and b is a remainder of $HC(f_k)$. Then by definition 12 we get

$$spol_c(f_k, f_l, x_k, x_l) = a \cdot f_k \cdot x_k - f_l \cdot x_l \in ideal_r(F),$$

and hence $spol_c(f_k, f_l, x_k, x_l) \stackrel{*}{\rightarrow}_F^r 0$.

[43] As $t_i = HT(g_i \cdot x_i)$ and $t_j \in T(RED(g_i \cdot x_i))$.

$3 \Rightarrow 2$ We have to show that every element $g \in ideal_r(F)$ is $\rightarrow_F^r$-reducible to zero. As $\rightarrow_F^r$ is Noetherian and $h \in ideal_r(F)$, $h \rightarrow_F^r h'$ implies $h' \in ideal_r(F)$, it suffices to show that every element $g \in ideal_r(F) - \{0\}$ is $\rightarrow_F^r$-reducible.
Let $g = \sum_{i=1}^m c_i \cdot f_i \cdot x_i$, where $c_i \in \mathbf{Z}, f_i \in F, x_i \in \mathcal{H}$.
Depending on this representation of g we define $t = max\{HT(f_i \cdot x_i) \mid i \in \{1, \ldots m\}\}, M = \{\{HC(f_i) \mid HT(f_i \cdot x_i) = t\}\}$. (Note that M is a multiset with elements in $\mathbf{Z}$).
We call another representation of g with $\tilde{t}, \tilde{M}$ *smaller* if $\tilde{t} < t$ or $\tilde{t} = t$ and $\tilde{M} \ll M$.
By lemma 7 we can assume $HT(f_i \cdot x_i) = HT(f_i) \circ x_i$ and $HC(f_i) > 0$, as if $HT(f_i \cdot x_i) \neq HT(f_i) \circ x_i$ for some f_i in our representation of g, we know $f_i \cdot x_i \rightarrow_F^c 0$, i.e. $f_i \cdot x_i = d_i \cdot f_i' \cdot x_i'$ for some $d_i \in \mathbf{Z}, f_i' \in F, x_i' \in \mathcal{H}$ and $HT(f_i \cdot x_i) = HT(f_i' \cdot x_i') = HT(f_i') \circ x_i' = t$ together with $HC(f_i') \leq_Z HC(f_i)$ gives us that the representation is not increased by substituting $d_i \cdot f_i' \cdot x_i'$ for $f_i \cdot x_i$.
Important is that now M is a multiset with elements in $\mathbf{N}$, since $HC(f_i) > 0$.
Our intention is to show that if t, M belong to a minimal representation of g [44], then $|M| = 1$, e.g. $M = \{\{HC(f_k \cdot x_k)\}\}$. This gives us $HT(g) = t = HT(f_k) \circ x_k$ and as $HC(f_k) > 0$, g is $\rightarrow_F^r$-reducible by f_k.
Let $HC(f_k), HC(f_l) \in M, k \neq l$ [45] and $a \cdot HC(f_k) + b = HC(f_l)$ for $a, b \in \mathbf{Z}$, b a remainder of $HC(f_k)$.
Since $HT(f_k) \circ x_k = HT(f_l) \circ x_l$ we have a commutative s-polynomial such that

$$a \cdot f_k \cdot x_k - f_l \cdot x_l = a \cdot f_k \cdot z_k \cdot m - f_l \cdot z_l \cdot m = spol_c(f_k, f_l, z_k, z_l) \cdot m.$$

In case $spol_c(f_k, f_l, z_k, z_l) \neq 0$ [46] this implies $HT(spol_c(f_k, f_l, z_k, z_l) \cdot m) \leq t$ as $HT(spol_c(f_k, f_l, z_k, z_l)) < HT(f_l) \cdot z_l$ and $t = HT(f_l) \circ z_l \circ m$.
In case $b = 0$ we know $HT(spol_c(f_k, f_l, z_k, z_l) \cdot m) < t$ and $spol_c(f_k, f_l, z_k, z_l) \rightarrow_q^{*r} 0$ implies $spol_c(f_k, f_l, z_k, z_l) = \sum_{i=1}^n d_i \cdot h_i \cdot w_i, d_i \in \mathbf{Z}, h_i \in F, w_i \in \mathcal{H}$, where the h_i are due to the reduction of $spol_c(f_k, f_l, z_k, z_l)$ and all terms occurring in the sum $spol_c(f_k, f_l, z_k, z_l) \cdot m = \sum_{i=1}^n d_i \cdot h_i \cdot w_i \cdot m$ are bounded by $HT(spol_c(f_k, f_l, z_k, z_l) \cdot m) < t$.
In case $b \neq 0$ we get $HT(spol_c(f_k, f_l, z_k, z_l) \cdot m) = t$ and $spol_c(f_k, f_l, z_k, z_l) \cdot m \rightarrow_{spol_c(f_k, f_l, z_k, z_l)}^c 0$. Then lemma 14 implies $spol_c(f_k, f_l, z_k, z_l) = \sum_{i=1}^n d_i \cdot h_i \cdot w_i, d_i \in \mathbf{Z}, h_i \in F, w_i \in \mathcal{H}$, where the h_i are due to the reduction of $spol_c(f_k, f_l, z_k, z_l)$ and all terms occurring in the sum $spol_c(f_k, f_l, z_k, z_l) \cdot m = \sum_{i=1}^n d_i \cdot h_i \cdot w_i \cdot m$ are bounded by $HT(spol_c(f_k, f_l, z_k, z_l) \cdot m) \leq t$.
In both cases we can substitute $h_i \cdot w_i \cdot y$ by $h_i' \cdot w_i'$ (without increasing the representation) such that $HT(h_i' \cdot w_i') = HT(h_i') \circ w_i'$ and $HC(h_i') > 0$ by lemma 7 since F is commutatively saturated .

[44] Such minimal representations of polynomials exist as our ordering on representations as defined above is well-founded.

[45] Not necessarily $f_l \neq f_k$.

[46] In case $spol_c(f_k, f_l, x_k, x_l) = 0$ the proof is similar. Substituting 0 for $\sum_{i=1}^n d_i \cdot h_i \cdot w_i$ in the equations below immediately gives us a smaller representation of g, contradicting our assumption.

Now we get:

$$\begin{aligned} g &= c_k \cdot f_k \cdot x_k + c_l \cdot f_l \cdot x_l + \sum_{\substack{i=1 \\ k \neq i \neq l}}^{m} c_i \cdot f_i \cdot x_i \\ &= c_k \cdot f_k \cdot x_k + \underbrace{c_l \cdot a \cdot f_k \cdot x_k - c_l \cdot a \cdot f_k \cdot x_k}_{=0} + c_l \cdot f_l \cdot x_l + \sum_{\substack{i=1 \\ k \neq i \neq l}}^{m} c_i \cdot f_i \cdot x_i \\ &= (c_k + c_l \cdot a) \cdot f_k \cdot x_k - c_l \cdot \underbrace{(a \cdot f_k \cdot x_k - f_l \cdot x_l)}_{= spol_c(f_k, f_l, z_k, z_l) \cdot m} + \sum_{\substack{i=1 \\ k \neq i \neq l}}^{m} c_i \cdot f_i \cdot x_i \\ &= (c_k + c_l \cdot a) \cdot f_k \cdot x_k - c_l \cdot (\sum_{i=1}^{n} d_i \cdot h'_i \cdot w'_i) + \sum_{\substack{i=1 \\ k \neq i \neq l}}^{m} c_i \cdot f_i \cdot x_i \qquad (2) \end{aligned}$$

and depending on this new representation of g we define $\tilde{t} = max\{HT(h'_i \cdot w'_i), HT(f_i \cdot x_i) \mid h'_i, f_i$ appearing in (2) $\}, \tilde{M} = \{\{HC(h'_i), HC(f_i) \mid HT(h'_i \cdot w'_i) = \tilde{t}, HT(f_i \cdot x_i) = \tilde{t}\}\}$. We either get $\tilde{t} < t$ or $\tilde{t} = t$ and we have to distinguish two cases:

(a) $c_k + c_l \cdot a = 0$.
Then $\tilde{M} = (M - \{HC(f_k), HC(f_l)\}) \cup \{\{HC(h'_i) \mid HT(h'_i) \cdot w'_i = t\}\}$.

(b) $c_k + c_l \cdot a \neq 0$.
Then $\tilde{M} = (M - \{HC(f_l)\}) \cup \{\{HC(h'_i) \mid HT(h'_i) \cdot w'_i = t\}\}$.

By lemma 14 we know that if there are polynomials h'_i with $HT(h'_i) \cdot w'_i = t$ the corresponding polynomials h_i from above are used to right reduce $HT(spol_c(f_k, f_l, z_k, z_l))$, and, therefore, we know $HC(h'_i) \leq HC(spol_c(f_k, f_l, z_k, z_l)) \leq b < HC(f_k) \leq HC(f_l)$, hence $\tilde{M} \ll M$.
However we get a smaller representation of g contradicting our assumption. q.e.d.

However we even have a Gröbner basis via $\rightarrow^c$.

Corollary 5
Let $F \subseteq \mathbf{Z}[\mathcal{H}]$, F commutatively saturated. Equivalent are:

1. *F is a Gröbner basis via $\rightarrow^c$.*
2. *$ideal(F) \xrightarrow{*}{}^c_F 0$.*
3. *For all $f_k, f_l \in F$ we have $S_c \xrightarrow{*}{}^r_F 0$, where $S_c \in \mathcal{SAT}_c(spol_c(f_k, f_l))$.*

Proof : Let $g \in ideal_r(F) - \{0\}$. Then for a minimal representation t, M of g as described in the proof of theorem 10, we have $M = \{\{HC(f_k \cdot x_k)\}\}$ and $t = HT(g) = HT(f_k) \circ x_k$ and $HC(f_k) > 0$, i.e. g is $\rightarrow^c_F$–reducible by f_k. Further $ideal_r(F) = ideal(F)$. q.e.d.

Procedure Completion via Commutative Saturation

input: $F \subseteq \mathbf{Z}[\mathcal{H}]$, $F = \{f_1, \ldots f_n\}$
output: $\mathrm{GB}_c(F)$, a commutatively saturated Gröbner basis of F.

$G := \mathrm{SAT}_c(F)$;
$B := \{(q_1, q_2) \mid q_1, q_2 \in G, q_1 \neq q_2\}$;
while $B \neq \emptyset$ do
    $(q_1, q_2) := remove(B)$;
    $h := spol_c(q_1, q_2, x_1, x_2)$;
    $h' := cnf(h, G)$;
    if $h' \neq 0$ then
        $B := B \cup \{(f, \tilde{h}) \mid f \in G, \tilde{h} \in \mathrm{SAT}_c(h')\}$;
        $G := G \cup \{\mathrm{SAT}_c(h')\}$;
endwhile

where SAT_c denotes the output of our commutative saturation procedure, *remove* removes an element from a set and $cnf(g, G)$ computes a normal form of g via G and canonizes it.

Lemma 15
The procedure is correct.

Proof : Follows immediately from theorem 16. q.e.d.

Lemma 16
The procedure terminates.

Proof : The procedure stops as soon as all s–polynomials reduce to zero. Now suppose that our procedure does not terminate. Then there is a term t among the terms of our input polynomials, which occurs infinitely many times among the head terms of the polynomials h' as computed in the above procedure giving us an infinite set $\{a_i \cdot t \cdot y_i \mid a_i \in \mathbf{N}, y_i \in \mathcal{H}\}$ of head terms. Since the h' are in normal form, no $a_j \cdot t \cdot y_j$ is reducible by any previously added polynomial. But by Dickson's lemma there is a N such that for all $k > N$ there is a $j < N$ such that $t \cdot y_k = (t \cdot y_j) \circ z$ for some $z \in \mathcal{H}$ and as $\circ$ is monotone we must have $a_k < a_j$ as otherwise we get a contradiction to h' being in normal form. But this leads to the existence of an infinite set $\{b_i \cdot (t \cdot y_j) \circ z_i \mid i \in \mathbf{N}, b_i \in \mathbf{N}\}$ with $b_{i+1} < b_i$ contradicting the fact that $(\mathbf{N}, <)$ is well–founded. q.e.d.

Theorem 17
The existence of finite Gröbner bases for ideals in $\mathbf{Z}[\mathcal{H}]$ has been shown for commutative monoids. Using the appropriate presentation of $\mathcal{H}$ the procedure "Completion with respect to Commutative Saturation" computes such bases.

6.5 Finitely Generated Two Sided Ideals in a Free Monoid Ring

In the previous section we saw that ideals in commutative monoid rings have finite Gröbner bases. Looking at finitely generated two sided ideals in arbitrary monoid rings the situation is much harder. In particular we show that for a fixed reduction the existence of finite Gröbner bases for finitely generated ideals in the free monoid ring $\mathbf{Q}[\Sigma^*]$ is undecidable, where $\Sigma = \{d_1, \ldots, d_n\}$ is a finite alphabet with $d_1 \succ \ldots \succ d_n$ inducing a length–lexicographical ordering on Σ^*.

Definition 13
Let $p = \sum_{i=1}^{n} a_i \cdot w_i, g = \sum_{j=1}^{m} b_j \cdot v_j \in \mathbf{Q}[\Sigma^*]$ and $b_1 > 0$.
We say *g reduces p to q at $a_k \cdot w_k$* in one step, i.e. $p \rightarrow_g q$, if

(a) $xv_1y = w_k$ for some $x, y \in \Sigma^*$.

(b) $q = p - (a_k \cdot b_1^{-1}) \cdot x \cdot g \cdot y$.

We write $p \rightarrow_g$ if there is a polynomial q as defined above.
We can define $\stackrel{*}{\rightarrow}$, $\stackrel{+}{\rightarrow}$, $\stackrel{n}{\rightarrow}$ and reduction by a set $F \subseteq \mathbf{Q}[\Sigma^*]$ as usual and $\stackrel{*}{\leftrightarrow}_F = \equiv_F$.

Theorem 18 *It is undecidable, whether a finitely generated ideal has a finite Gröbner basis in* $\mathbf{Q}[\Sigma^*]$.

Proof : Let $\Gamma = \{a_i | i \in \mathbf{N}\}$ be an alphabet with $\succ$ a length–lexicographical ordering on Γ^*. According to the results in [OD83] for finite Thue systems (Σ, T), $\Sigma \subset \Gamma$, we can state:
If $\mathcal{P}$ is a property of finite Thue systems fulfilling

1. If $(\Sigma, T_1), (\Sigma, T_2)$ are two equivalent Thue systems, then $\mathcal{P}(T_1)$ implies $\mathcal{P}(T_2)$.
2. Every trivial Thue system has $\mathcal{P}$.
3. For each finite Thue system having $\mathcal{P}$ the word problem is decidable.

then the following problem is undecidable:
Input: A finite Thue system (Σ, T).
Question: Does (Σ, T) have $\mathcal{P}$?
Setting $\mathcal{P}(T)$ iff there is an equivalent, finite system T', which is convergent with respect to $\succ$ we get that the following question is undecidable:
Given a finite Thue system (Σ, T), is there an equivalent, finite system (Σ, T') which is convergent with respect to $\succ$?
Our claim is:
(Σ, T) has an equivalent, finite presentation (Σ, T') convergent with respect to $\succ$ iff the set $P_T = \{l - r \mid (l, r) \in T\}$ has a finite Gröbner basis in the free monoid ring

$\mathbf{Q}[\Sigma^*]$ generated by Σ according to the ordering $\succ$.
If there is an equivalent, finite presentation (Σ, T') convergent with respect to $\succ$, then the set $P_{T'} = \{l - r \mid (l,r) \in T'\}$ is a finite Gröbner basis of P_T in $\mathbf{Q}[\Sigma^*]$, since possible s–polynomials of $P_{T'}$ correspond to critical pairs of T' and reduction in T' can be simulated in $\mathbf{Q}[\Sigma^*]$ (compare definition 13).
It remains to show that in case P_T has a finite Gröbner basis in $\mathbf{Q}[\Sigma^*]$ there exists a finite Gröbner basis G such that for all $g \in G$ we have $g = u - v$, where $u, v \in \Sigma^*$, and $u \overset{*}{\leftrightarrow}_T v$. Then (Σ, T) has an equivalent, convergent, finite presentation (Σ, T'), where $T' = \{(u,v) \mid u - v \in G\}$ as the reduction $\rightarrow$ in $\mathbf{Q}[\Sigma^*]$ as defined above can be compared to the usual reduction in a Thue system.
First we show that in case a finite set F has a finite Gröbner basis in $\mathbf{Q}[\Sigma^*]$ the following procedure also computes a finite Gröbner basis of F (compare [Mo85]).

Procedure Completion in $\mathbf{Q}[\Sigma^*]$

input: $F \subseteq \mathbf{Q}[\Sigma^*]$ finite
output: $\text{GB}(F)$, a Gröbner basis of F.

$G := F$;
$B := \{(q_1, q_2) \mid q_1, q_2 \in G\}$;
while $B \neq \emptyset$ do
    $(q_1, q_2) :=$ remove(B);
    for all $h \in spols(q_1, q_2)$ do
        $h' :=$ cnf(h, G);
        if $h' \neq 0$ then
            $G := G \cup \{h'\}$;
            $B := B \cup \{(f, h'), \mid f \in G\}$;
    endfor
endwhile
$\text{GB}(F) := G$

where $remove$ removes an element from a set, $cnf(h, G)$ computes a "canonized normal form" of h with respect to G, and $spols(q_1, q_2) = \{canonize(HC(q_1)^{-1} \cdot x \cdot q_1 \cdot y - HC(q_2)^{-1} \cdot q_2 \mid xHT(q_1)y = HT(q_2)\} \cup \{canonize(HC(q_1)^{-1} \cdot q_1 \cdot y - HC(q_2)^{-1} \cdot x \cdot q_2 \mid HT(q_1)y = xHT(q_2)\}$.
Now let $\tilde{G}$ be a finite Gröbner basis of P_T with $HT(\tilde{G}) = \{HT(g) \mid g \in \tilde{G}\} = \{t_1, \ldots, t_k\}$. Let $H_{t_i} = \{xt_iy \mid x, y \in \Sigma^*\}$, then $HT(ideal(P_T)) = \bigcup_{i=1}^{k} H_{t_i}$, since all polynomials in $ideal(P_T)$ reduce to zero by $\tilde{G}$. Further our procedure is correct and, therefore, for each t_i there has to be at least one g_i added to G or already in G such that $t_i = xHT(g_i)y$ for some $x, y \in \Sigma^*$, i.e. $HT(g_i)$ divides t_i. Note that as soon as all such g_i are added to G, we have $HT(ideal(G)) = \bigcup_{i=1}^{k} H_{t_i} = HT(ideal(P_T))$ and as for all h' added to G we know $h' \in ideal(P_T)$ and, as h' is in normal form with respect to the already computed polynomials, no further polynomials will be added.
It remains to show that in case P_T has a finite Gröbner basis the finite output $\text{GB}(P_T)$ of our procedure has the desired structure that for all $g \in \text{GB}(P_T)$, $g = u - v$ where $u, v \in \Sigma^*$, and $u \overset{*}{\leftrightarrow}_T v$.

Let us look at the polynomials added to G and in G: In case $g \in P_T$ there is nothing to show. Now let us assume all polynomials in G have the desired structure and a new polynomial g is added. In case g is due to s–polynomial computation of two polynomials $u_1 - v_1$,$u_2 - v_2$ we do not lose our structure. The same is true for computing the canonized head normal form of a polynomial $u - v$ via a set of polynomials having the same structure. Further $u \overset{*}{\leftrightarrow}_T v$ is inherited within these operations. q.e.d.

7 Relations to Gröbner Bases in Special Monoid Rings

In our approach to generalize the concept of Gröbner bases to monoid rings, we find that in order to give a criteria for a set to be a Gröbner basis (in our case of a right ideal), there are two main problems to solve. They arise from the fact that in general the ordering and multiplication on our monoid are not compatible, i.e. $m_1 \succ m_2$ need not imply $m_1 \cdot x \succ m_2 \cdot x$. Let $\rightarrow$ be a computable reduction on our monoid ring $R[\mathcal{H}]$ (e.g. as described in definition 3). Trying to characterize a set $F \subseteq R[\mathcal{H}]$ as a Gröbner basis of a (right, left) ideal by means of s–polynomials and their reducibility as in Buchberger's work, we have to solve the following problems:

1. We have to check our reduction and eventually correct some "defects".
2. We have to localize our critical situations.
3. We have to guarantee that $p \rightarrow_q 0$ and $q \overset{*}{\rightarrow}_F 0$ implies the existence of a representation of p as $p = \sum_{i=1}^{k} d_i \cdot g_i \cdot x_i$, $d_i \in \mathbf{Z}, g_i \in F, x_i \in \mathcal{H}$ such that $HM(p) \geq d_i \cdot g_i \cdot x_i$ for all $i \in \{1, \ldots k\}$. Note that this is weaker than demanding $p \overset{*}{\rightarrow}_F 0$.

In case these problems are solved we immediately get: $F \subseteq R[\mathcal{H}]$ is a Gröbner basis for the (right, left) ideal generated by F if and only if for all $f, g \in F$ the "appropriate" s–polynomials reduce to zero by $\overset{*}{\rightarrow}_F$.
In the previous sections we have solved these problems by introducing prefix right reduction, prefix saturation and prefix s–polynomials. Unfortunately prefix saturation need not be finite in general. For example take $T = \{ba \rightarrow ab\}$ and $p = b + \lambda$. Then a prefix saturating set of p must prefix right reduce the set $\{a^n b + a^n | n \in \mathbf{N}\}$ to zero. It is obvious that no such finite prefix saturating sets of p exist.
In case T contains the commutator set of Σ, $T_c = \{a_j a_i \rightarrow a_i a_j |$ for all $a_i, a_j \in \Sigma, a_i \prec a_j\}$ the two problems can be solved in a similar way by introducing commutative right reduction, commutative saturation and commutative s–polynomials. Due to Dickson's lemma we always get finite Gröbner bases (in this case even of ideals).
Now we want to sketch, how the results of Buchberger [Bu85], Kandri–Rody, Kapur [KaKa84, KaKa88], Mora [Mo85], Baader [Ba89] and Weispfenning [We92] can be seen in this context. Note that the approach can easily be modified for $K[\mathcal{H}]$, where K is a field.

1. Gröbner bases for $R[x_1, \ldots x_n]$, where R is a field or $\mathbf{Z}$, as described in [Bu85, KaKa84, KaKa88]:
   We can view $R[x_1, \ldots x_n]$ as the monoid ring over the free commutative monoid $\mathcal{H}$ generated by $\{x_1, \ldots, x_n\}$ and for instance the lexicographic–degree ordering is monotone on $\mathcal{H}$. Therefore, p itself is (commutatively) saturated and we can take the usual definition of s–polynomials as a basis for our set of s–polynomials. Such s–polynomials are for example in case $R = \mathbf{Z}$ defined as follows: Given two polynomials p_1, p_2 with $HC(p_2) = c_2 \geq HC(p_1) = c_1 > 0$, $HT(p_i) = t_i, RED(p_i) = r_i$ for $i = 1, 2$. Let x_1, x_2 such that $t_1 \cdot x_1 = t_2 \cdot x_2$ is the least common multiple of t_1, t_2 and $a, b \in \mathbf{Z}$, b a remainder of c_1 with $c_2 = a \cdot c_1 + b$. We get the following $spol(p_1, p_2) = a \cdot p_1 \cdot x_1 - p_2 \cdot x_2$.
   Equivalent are:

   (a) $ideal_r(F) \xrightarrow{*}_F 0$

   (b) For all $f_k, f_l \in F$ we have: $spol(f_k, f_l) \xrightarrow{*}_F 0$.

2. Gröbner bases for $R\langle x_1, \ldots x_n\rangle$, where R is a field or $\mathbf{Z}$, as described in [Mo85, Ba89]:
   We can view $R\langle x_1, \ldots x_n\rangle$ as the monoid ring over the free monoid $\mathcal{H}$ generated by $\{x_1, \ldots, x_n\}$. We know that p itself is (prefix) saturated since $T = \emptyset$ and we can take prefix s–polynomials as described in definition 11.
   Equivalent are:

   (a) $ideal_r(F) \xrightarrow{*}_F 0$

   (b) For all $f_k, f_l \in F$ we have: $spol_p(f_k, f_l) \xrightarrow{*}_F 0$.

3. Gröbner bases for skew polynomials rings $K\langle X, Y\rangle$ as described in [We92]:
   We can view the skew polynomial ring $K\langle X, Y\rangle$ as a monoid ring over a monoid $\mathcal{H}$ presented by $\Sigma = \{X, Y\}, T = \{YX \to X^e Y\}$, where $e \in \mathbf{N}^+$. Since the ordering used by Weispfenning is monotone, p itself is saturated and taking his s–polynomials as a basis for our set of s–polynomials we are done. Weispfenning's s–polynomials are defined as follows: Given two polynomials p_1, p_2 with $HC(p_i) = c_i$, $HT(p_i) = t_i, RED(p_i) = r_i$ for $i = 1, 2$. Let x_1, x_2 such that $t_1 \cdot x_1 = t_2 \cdot x_2$ is the "least common multiple" of t_1, t_2 according to the "modified" multiplication. We get the following $spol(p_1, p_2) = c_2 \cdot p_1 \cdot x_1 - c_1 \cdot p_2 \cdot x_2$.
   Equivalent are:

   (a) $ideal_r(F) \xrightarrow{*}_F 0$

   (b) For all $f_k, f_l \in F$ we have: $spol(f_k, f_l) \xrightarrow{*}_F 0$.

8 Applications

Definition 14
Let $\mathcal{G}$ be a group, $S \subseteq \mathcal{G}$ and $\langle S \rangle$ denote the subgroup generated by S. The *generalized word problem or subgroup problem* for $\mathcal{G}$ is to determine, given $w \in \mathcal{G}$, whether $w \in \langle S \rangle$.

In [KuMa89] prefix rewriting is used to solve the generalized word problem for a group $\mathcal{G}$. A special basis of a subgroup is computed which allows to decide the generalized word problem for an element in $\mathcal{G}$ by prefix reducing it with respect to this basis. A similar approach can be given using completion with respect to prefix saturation showing the connection to the ideas used in [KuMa89]. Let (Σ, T) be a finite convergent presentation of a group $\mathcal{G}$. Further let $S = \{u_1, \ldots, u_n\}$ be a subset of $\mathcal{G}$ (we will identify $\mathcal{G}$ and $IRR(T)$ throughout this section) and $P_S = \{u_i - 1 \mid u_i \in S\}$. Before we show how completion in $\mathbf{Z}[\mathcal{G}]$ can be used to study the subgroup problem in $\mathcal{G}$ we give a useful lemma on the structure of the right Gröbner basis $\textsc{Gb}(P_S)$ computed by one of our procedures.

Lemma 17
For all $f \in \textsc{Gb}(P_S)$ the following hold:

(α) *$f = x - y$, where $x, y \in \mathcal{G}$.*

(β) *For $f = x - y$ either $x, y \in \langle S \rangle$ or $x, y \notin \langle S \rangle$.*

(γ) *For $f = x - y$ we have $x \cdot y^{-1}, y \cdot x^{-1} \in \langle S \rangle$.*

Proof : Our input is $P_S = \{u_i - 1 \mid u_i \in S\}, S \subseteq \mathcal{G}$ finite.

1. Let $f \in \textsc{Gb}(P_S)$ be due to the saturation of a polynomial $x - y$, fulfilling (α),(β),(γ), i.e. $f = (x - y) \cdot z = x' - y'$ for some $z \in \mathcal{G}$ and (α) is true. Without loss of generality let us assume $x' = x \cdot z$ and $y' = y \cdot z$.

   (a) $x, y \in \langle S \rangle$

      i. $z \in \langle S \rangle$
      Then $x \cdot z, y \cdot z \in \langle S \rangle$ and f fulfills (β). Further $x' \cdot y'^{-1} = x \cdot z \cdot z^{-1} \cdot y^{-1} = x \cdot y^{-1}$ and $y' \cdot x'^{-1} = y \cdot z \cdot z^{-1} \cdot x^{-1}$ both are in $\langle S \rangle$, i.e. f fulfills (γ).

      ii. $z \notin \langle S \rangle$
      Now let us assume $x' \in \langle S \rangle$. Since $x \in \langle S \rangle$ we get $x^{-1} \in \langle S \rangle$ and therefore $z = x^{-1} \cdot (x \cdot z) = x^{-1} \cdot x' \in \langle S \rangle$ contradicting our assumption. Similarly we can show $y' \notin \langle S \rangle$ and together with $x' \cdot y'^{-1}, y' \cdot x'^{-1} \in \langle S \rangle$ we find that f fulfills (β) and (γ).

   (b) $x, y \notin \langle S \rangle$

      i. $z \in \langle S \rangle$
      Let us assume $x' \in \langle S \rangle$. Since $z \in \langle S \rangle$ gives us $z^{-1} \in \langle S \rangle$ we get $x = (x \cdot z) \cdot z^{-1} \in \langle S \rangle$ contradicting our assumption. Similarly we can

show $y' \notin \langle S\rangle$ and together with $x' \cdot y'^{-1}, y' \cdot x'^{-1} \in \{x \cdot y^{-1}, y \cdot x^{-1}\}$ we find that f fulfills (β) and (γ).

ii. $z \notin \langle S\rangle$
Let us assume $x' \in \langle S\rangle$ and $y' \notin \langle S\rangle$. Since $y \cdot x^{-1} \in \langle S\rangle$ we get $y' = y \cdot z = (y \cdot x^{-1}) \cdot (x \cdot z) \in \langle S\rangle$ contradicting our assumption. This together with $x' \cdot y'^{-1}, y' \cdot x'^{-1} \in \{x \cdot y^{-1}, y \cdot x^{-1}\}$ gives us that f fulfills (β) and (γ).

2. Let $f \in \text{GB}(P_S)$ be due to s–polynomial computation of $x_1 - y_1, x_2 - y_2$ both fulfilling (α),(β),(γ). Without loss of generality let us assume $x_1 \cdot z_1 = x_2 \cdot z_2$ for some $z_1, z_2 \in \mathcal{H}$ according to the appropriate definition. This gives us the s–polynomial $y_1 \cdot z_1 - y_2 \cdot z_2$ which clearly fulfills (α). It remains to show that it also fulfills (β) and (γ). We know $x_1^{-1} \cdot x_2 = z_1 \cdot z_2^{-1}$ and $x_2^{-1} \cdot x_1 = z_2 \cdot z_1^{-1}$.

(a) $x_1, x_2, y_1, y_2 \in \langle S\rangle$
Then either $x_1 \cdot z_1, x_2 \cdot z_2, y_1 \cdot z_1, y_2 \cdot z_2 \in \langle S\rangle$ or $x_1 \cdot z_1, x_2 \cdot z_2, y_1 \cdot z_1, y_2 \cdot z_2 \notin \langle S\rangle$ giving us (β). Further we get $y_1 \cdot z_1 \cdot (y_2 \cdot z_2)^{-1} = y_1 \cdot z_1 \cdot z_2^{-1} \cdot y_2^{-1} = y_1 \cdot x_1^{-1} \cdot x_2 \cdot y_2^{-1} \in \langle S\rangle$ and $y_2 \cdot z_2 \cdot (y_1 \cdot z_1)^{-1} = y_2 \cdot z_2 \cdot z_1^{-1} \cdot y_1^{-1} = y_2 \cdot x_2^{-1} \cdot x_1 \cdot y_1^{-1} \in \langle S\rangle$ giving us (γ).

(b) $x_1, x_2, y_1, y_2 \notin \langle S\rangle$
This case goes analogously.

(c) $x_1, y_1 \in \langle S\rangle$ and $x_2, y_2 \notin \langle S\rangle$

i. $z_1 \in \langle S\rangle$, i.e. $x_1 \cdot z_1, y_1 \cdot z_1 \in \langle S\rangle$
As $x_1 \cdot z_1 = x_2 \cdot z_2$ we know $z_2 \notin \langle S\rangle$ as otherwise $x_1 \cdot z_1, z_2^{-1} \in \langle S\rangle$ would imply $x_2 \in \langle S\rangle$. Further $x_2 \cdot z_2 \in \langle S\rangle$ implies $y_2 \cdot z_2 \in \langle S\rangle$ [47] , i.e. (β) is fulfilled, and, therefore, $y_1 \cdot z_1 \cdot (y_2 \cdot z_2)^{-1}, y_2 \cdot z_2 \cdot (y_1 \cdot z_1)^{-1} \in \langle S\rangle$, i.e. (γ) is fulfilled.

ii. $z_1 \notin \langle S\rangle$, i.e. $x_1 \cdot z_1, y_1 \cdot z_1 \notin \langle S\rangle$
As $x_1 \cdot z_1 = x_2 \cdot z_2$ we know $x_2 \cdot z_2, y_2 \cdot z_2 \notin \langle S\rangle$, i.e. (β) is fulfilled, and $y_1 \cdot z_1 \cdot (y_2 \cdot z_2)^{-1}, y_2 \cdot z_2 \cdot (y_1 \cdot z_1)^{-1} \in \langle S\rangle$, i.e. (γ) is fulfilled.

3. Let $f \in \text{GB}(P_S)$ be the canonized normal form of a polynomial $x - y$, which fulfills (α), (β) and (γ). We show that reducing a polynomial $x_1 - y_1$ by a polynomial $x_2 - y_2$, both fulfilling $(\alpha), (\beta)$ and (γ), the canonized version of the result again fulfills $(\alpha), (\beta)$ and (γ). Without loss of generality let us assume $x_1 = x_2 \cdot z$, i.e. $z = x_2^{-1} \cdot x_1, z^{-1} = x_1^{-1} \cdot x_2$. Then $x_1 - y_1 \to^r_{x_2 - y_2} x_1 - y_1 - (x_2 - y_2) \cdot z$.

(a) $x_1, x_2 \in \langle S\rangle$
Then $x_1 = x_2 \cdot z \in \langle S\rangle$ implies $y_2 \cdot z \in \langle S\rangle$ as in 1. Further $y_1 \cdot (y_2 \cdot z)^{-1} = y_1 \cdot z^{-1} \cdot y_2^{-1} = y_1 \cdot x_1^{-1} \cdot x_2 \cdot y_2^{-1} \in \langle S\rangle$ and $y_2 \cdot z \cdot y_1^{-1} = y_2 \cdot x_2^{-1} \cdot x_1 \cdot y_1^{-1} \in \langle S\rangle$, i.e. the canonized version of the result again fulfills $(\alpha), (\beta)$ and (γ).

[47] To get these results we can apply the same argumentation as in part 2 of this proof.

(b) $x_1, x_2 \notin \langle S \rangle$
Then $x_1 = x_2 \cdot z \notin \langle S \rangle$ implies $y_2 \cdot z \notin \langle S \rangle$ as in 1. Again $y_1 \cdot (y_2 \cdot z)^{-1}, y_2 \cdot z \cdot y_1^{-1} \in \langle S \rangle$ gives us that the canonized version of the result again fulfills $(\alpha), (\beta)$ and (γ). q.e.d.

Lemma 18
Let $S \subseteq \mathcal{G}$. Then the following statements are equivalent:

1. $w \in \langle S \rangle$
2. $w - 1 \in ideal_r(P_S)$
3. $w - 1 \xrightarrow{*_r}_{\mathrm{GB}(P_S)} 0$

Proof :

$1 \Rightarrow 2$ Let $w = u_{i_1} \cdot \ldots \cdot u_{i_k}$.
We show $w - 1 \in ideal_r(P_S)$ by induction on k.
In the base case $k = 1$ there is nothing to show.
Suppose $w = u_{i_1} \cdot \ldots \cdot u_{i_{k+1}}$ and $u_{i_1} \cdot \ldots \cdot u_{i_k} - 1 \in ideal_r(P_S)$. Then $(u_{i_1} \cdot \ldots \cdot u_{i_k} - 1) \cdot u_{i_{k+1}} \in ideal_r(P_S)$ and since $u_{i_{k+1}} - 1 \in ideal_r(P_S)$ we get $(u_{i_1} \cdot \ldots \cdot u_{i_k} - 1) \cdot u_{i_{k+1}} + (u_{i_{k+1}} - 1) = w - 1 \in ideal_r(P_S)$.

$2 \Rightarrow 3$ This follows immediately from the fact that $\mathrm{GB}(P_S)$ is a Gröbner basis via $\rightarrow^r$.

$3 \Rightarrow 1$ Suppose $w - 1 \xrightarrow{k_r}_{\mathrm{GB}(P_S)} 0$. We show $w \in \langle S \rangle$ by induction on k.
In the base case $k = 1$ we have $w - 1 = (x - y) \cdot z$ for some $x - y \in \mathrm{GB}(P_S), z \in \mathcal{G}$ and $w = x \cdot z, 1 = y \cdot z$. Then $w = x \cdot y^{-1} \in \langle S \rangle$ by lemma 17.
Suppose $w - 1 \rightarrow_{\mathrm{GB}(P_S)}^r w - 1 - (x - y) \cdot z = y \cdot z - 1 \xrightarrow{k_r}_{\mathrm{GB}(P_S)} 0$. Then our induction hypothesis yields $y \cdot z \in \langle S \rangle$. By lemma 17 we have to distinguish the following cases:

(a) $x, y \in \langle S \rangle$
Then $y \cdot z \in \langle S \rangle$ and $y^{-1} \in \langle S \rangle$ give us $z \in \langle S \rangle$ and therefore $w = x \cdot z \in \langle S \rangle$.

(b) $x, y \notin \langle S \rangle$ Then $y \cdot z \in \langle S \rangle$ together with $x \cdot y^{-1} \in \langle S \rangle$ (compare lemma 17) gives us $w = x \cdot z = (x \cdot y^{-1}) \cdot (y \cdot z) \in \langle S \rangle$. q.e.d.

Example 10
Let $\Sigma = \{a, b, c\}, T = \{a^4 \rightarrow \lambda, b^2 \rightarrow \lambda, ab \rightarrow c, a^3c \rightarrow b, cb \rightarrow a\}$ denote a group $\mathcal{G}$ and $S = \{ca, a^2ca^3, b\}$ a subset of $\mathcal{G}$. Then $\{b - 1, ca - 1, c^2 - b, a^2c - a, a^3 - c\}$ is a right Gröbner basis of P_S via $\rightarrow^r$.

A word of caution: This cannot be generalized to the submonoid problem as the following example shows:

Example 11
Let $\Sigma = \{a, b\}, T = \{ab \rightarrow \lambda\}$ denote a monoid $\mathcal{H}$. Let $U = \{a^n \mid n \in \mathbf{N}\}$ be the submonoid of $\mathcal{H}$ generated by $S = \{a\}$. Then we have $b - 1 \in ideal_r(P_S)$ since $b - 1 = -1(a - 1) \cdot b$ but $b \notin U$.

In case $\mathcal{H}$ is a free monoid or a free commutative monoid the results of this section can be applied.

Acknowledgements
We would like to thank Andrea Sattler-Klein and Thomas Deiß for many valuable discussions on this paper.

References

[AvMaOt86] J. Avenhaus, K. Madlener, F. Otto. *Groups Presented by Finite Two–Monadic Church–Rosser Thue Systems.* Transactions of the American Mathematical Society, Volume 297(1986). pp 427–443.

[Ba89] F. Baader. *Unification in Commutative Theories, Hilbert's Basis Theorem and Gröbner Bases.* Proc. 3rd UNIF'89.

[Bu83] B. Buchberger. *A Critical–Pair Completion Algorithm for Finitely Generated Ideals in Rings.* Proc. Logic and Machines: Decision Problems and Complexity. Springer LNCS 171. pp 137–161.

[Bu85] B. Buchberger. *Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory.* N. K. Bose (ed). Multidimensional Systems Theory. Chapter 6. 1985. Dordrecht: Reidel. pp 184–232.

[KaKa84] A. Kandri–Rody and D. Kapur. *An Algorithm for Computing the Gröbner Basis of a Polynomial Ideal over an Euclidean Ring.* Technical Information Series General Electric Company Corporate Research and Development Schenectady. NY 12345. Dec. 1984.

[KaKa88] A. Kandri–Rody and D. Kapur. *Computing a Gröbner Basis of a Polynomial Ideal over an Euclidean domain.* Journal of Symbolic Computation 6(1988). pp 37–57.

[KaWe90] A. Kandri–Rody and V. Weispfenning. *Non–Commutative Gröbner Bases in Algebras of Solvable Type.* Journal of Symbolic Computation 9(1990). pp 1–26.

[KuMa89] N. Kuhn, K. Madlener. *A Method for Enumerating Cosets of a Group Presented by a Canonical System.* Proc. ISSAC'89. pp 338–350.

[La76] M. Lauer. *Kanonische Repräsentanten für die Restklassen nach einem Polynomideal.* Diplomarbeit. Universität Kaiserslautern. 1976.

[MaOt89] K.Madlener, F. Otto. *About the Descriptive Power of Certain Classes of Finite String–Rewriting Systems.* Theoretical Computer Science 67(1989). pp 143–172.

[Mo85] F. Mora. *Gröbner Bases for Non–Commutative Polynomial Rings.* Proc. AAECC–3(1985). Springer LNCS 229. pp 353–362

[NaOD89] P. Narendran and C. Ó'Dúnlaing. *Cancellativity in Finitely Presented Semigroups.* Journal of Symbolic Computation 7(1989). pp 457–472.

[OD83] C. Ó'Dúnlaing. *Undecidable Questions Related to Church–Rosser Thue Systems.* Theoretical Computer Science 23(1983). pp 339–345.

[St85] S. Stifter. *Computation of Gröbner Bases over the Integers and in General Reduction Rings.* Diplomarbeit. Johannes Kepler Universität Linz. 1985.

[We87] V. Weispfenning. *Gröbner Basis for Polynomial Ideals over Commutative Regular Rings.* Proc. EUROCAL'87. Springer LNCS 378. pp 336–347.

[We92] V. Weispfenning. *Finite Gröbner Bases in Non-Noetherian Skew Polynomial Rings.* Proc. ISSAC'92. pp 329–334.