Seeing farther

Clay lecture II

Hendrik Lenstra

Mathematisch Instituut
Universiteit Leiden

based on work with Daan van Gent and Alexander Spieksma

The fourteen integers problem

Problem. *Design a polynomial-time algorithm that, given fourteen positive integers a, b, c, d, e, f, g, h, i, j, k, l, m, n, decides whether or not one has*

$$a^b c^d e^f g^h = i^j k^l m^n.$$

The fourteen integers problem

Problem. *Design a polynomial-time algorithm that, given fourteen positive integers* a, b, c, d, e, f, g, h, i, j, k, l, m, n, *decides whether or not one has*

$$a^b c^d e^f g^h = i^j k^l m^n.$$

Non-method 1*:* multiply out.

The fourteen integers problem

Problem. *Design a polynomial-time algorithm that, given fourteen positive integers* a, b, c, d, e, f, g, h, i, j, k, l, m, n, *decides whether or not one has*

$$a^b c^d e^f g^h = i^j k^l m^n.$$

Non-method 1*:* multiply out.

Non-method 2*:* compare the prime factorizations left and right.

The fourteen integers problem

Problem. *Design a polynomial-time algorithm that, given fourteen positive integers* a, b, c, d, e, f, g, h, i, j, k, l, m, n, *decides whether or not one has*

$$a^b c^d e^f g^h = i^j k^l m^n.$$

Non-method 1*:* multiply out.

Non-method 2*:* compare the prime factorizations left and right.

Solution: factor a, c, e, g, i, k, m over a *coprime base*, and compare the factorizations left and right.

Creating the coprime base

Start from a, c, e, g, i, k, m.

If two of these, say r and s, satisfy $t = \gcd(r, s) > 1$, replace r and s by $r' = r/t$, t, $s' = s/t$.

Creating the coprime base

Start from a, c, e, g, i, k, m.

If two of these, say r and s, satisfy $t = \gcd(r, s) > 1$, replace r and s by $r' = r/t$, t, $s' = s/t$.

The gcd is computed by Euclid's algorithm, and one has $r'ts' = rs/t$ (and $\gcd(r', s') = 1$).

After a polynomial number of such steps, one arrives at the coprime base.

Algebraic number fields

An *algebraic number field* is a field K that contains $\mathbf{Q}$ such that the vector space dimension d of K over $\mathbf{Q}$ is *finite*.

Additively, K is isomorphic to $\mathbf{Q}^{\oplus d}$.

Algebraic number fields

An *algebraic number field* is a field K that contains $\mathbf{Q}$ such that the vector space dimension d of K over $\mathbf{Q}$ is *finite*.

Additively, K is isomorphic to $\mathbf{Q}^{\oplus d}$.

Examples: $K = \mathbf{Q}(\sqrt{2})$ (with $d = 2$), $K = \mathbf{Q}(\exp(2\pi\mathrm{i}/n))$ (with $d = \varphi(n)$).

One specifies K by giving d and d^3 rational numbers $(a_{ijk})_{0 \le i,j,k < d}$ such that some $\mathbf{Q}$-basis $(e_i)_i$ of K satisfies $e_i \cdot e_j = \sum_k a_{ijk} e_k$.

Algebraic number theory

$$\begin{array}{ccccc} \mathbf{p} & \subset & \mathcal{O}_K & \subset & K \\ \cup & & \cup & & \cup \\ p\mathbf{Z} & \subset & \mathbf{Z} & \subset & \mathbf{Q} \end{array}$$

Algebraic number theory

$$\begin{array}{ccccc} \mathbf{p} & \subset & \mathcal{O}_K & \subset & K \\ \cup & & \cup & & \cup \\ p\mathbf{Z} & \subset & \mathbf{Z} & \subset & \mathbf{Q} \end{array}$$

An *order* is a ring with additive group $\cong \mathbf{Z}^n$,
and $\mathcal{O}_K$ is the unique maximal order inside K.

Algebraic number theory

$$\begin{array}{ccccc} \mathbf{p} & \subset & \mathcal{O}_K & \subset & K \\ \cup & & \cup & & \cup \\ p\mathbf{Z} & \subset & \mathbf{Z} & \subset & \mathbf{Q} \end{array}$$

An *order* is a ring with additive group $\cong \mathbf{Z}^n$,
and $\mathcal{O}_K$ is the unique maximal order inside K.

Example:

$$\begin{array}{ccccc} (2-\mathrm{i})\mathbf{Z}[\mathrm{i}] & \subset & \mathbf{Z}[\mathrm{i}] & \subset & \mathbf{Q}(\mathrm{i}) \\ \cup & & \cup & & \cup \\ 5\mathbf{Z} & \subset & \mathbf{Z} & \subset & \mathbf{Q} \end{array}$$

Polynomial-time algorithms

Finding a polynomial-time algorithm that, given K, computes $\mathcal{O}_K$, would be a major breakthrough, even for quadratic fields ($d = 2$).

Likewise, polynomial-time algorithms have difficulties working with prime ideals.

Polynomial-time algorithms

Finding a polynomial-time algorithm that, given K, computes $\mathcal{O}_K$, would be a major breakthrough, even for quadratic fields ($d = 2$).

Likewise, polynomial-time algorithms have difficulties working with prime ideals.

However, we *can* solve the analogue of the fourteen integers problem in polynomial time.

Multiplicative relations

Theorem (Guoqiang Ge, 1993)**.** *There is a polynomial-time algorithm that, given K and a finite set S of non-zero elements of K, computes a $\mathbf{Z}$-basis for the kernel of the group homomorphism*

$$\mathbf{Z}^S \to K^*,\ (n_s)_{s\in S} \mapsto \prod_s s^{n_s}.$$

Greatest common divisors

Key step over $\mathbf{Z}$:

> "if r and s satisfy $t = \gcd(r, s) > 1$,
> replace r and s by $r' = r/t$, t, $s' = s/t$."

Likewise, Ge's algorithm uses a "gcd that one can divide by".

Greatest common divisors

Key step over $\mathbf{Z}$:

> "if r and s satisfy $t = \gcd(r, s) > 1$,
> replace r and s by $r' = r/t$, t, $s' = s/t$."

Likewise, Ge's algorithm uses a "gcd that one can divide by".

Note: $\mathbf{Z} \cdot r + \mathbf{Z} \cdot s = \mathbf{Z} \cdot \gcd(r, s)$.

Greatest common divisors

Key step over $\mathbf{Z}$:

> "if r and s satisfy $t = \gcd(r, s) > 1$,
> replace r and s by $r' = r/t$, t, $s' = s/t$."

Likewise, Ge's algorithm uses a "gcd that one can divide by".

Note: $\mathbf{Z} \cdot r + \mathbf{Z} \cdot s = \mathbf{Z} \cdot \gcd(r, s)$.

Over an order $R \subset K$, the gcd of r, $s \in K$ is defined to be $R \cdot r + R \cdot s$.

How to divide by it? And which R to use?

Invertible ideals

For additive subgroups I, $J \subset K$, write

$$I \cdot J = \{\textstyle\sum_i x_i y_i : x_i \in I,\, y_i \in J\},$$
$$I : J = \{x \in K : xJ \subset I\}.$$

Invertible ideals

For additive subgroups I, $J \subset K$, write

$$I \cdot J = \{\textstyle\sum_i x_i y_i : x_i \in I,\, y_i \in J\},$$
$$I : J = \{x \in K : xJ \subset I\}.$$

For a subring $R \subset K$, an *invertible R-ideal in K* is an additive subgroup $I \subset K$ such that $R \cdot I = I$ and $\exists J : I \cdot J = R$.

Those I's form a *multiplicative group*, so if $R \cdot r + R \cdot s$ is invertible, we can divide by it.

Producing invertible gcd's

Ge's main lemma. *There is a polynomial-time algorithm that, given K and a finite non-empty subset $T \subset K^*$, finds an order $R \subset K$ for which $\sum_{t \in T} Rt$ is an invertible R-ideal in K.*

Producing invertible gcd's

Ge's main lemma. *There is a polynomial-time algorithm that, given K and a finite non-empty subset $T \subset K^*$, finds an order $R \subset K$ for which $\sum_{t \in T} Rt$ is an invertible R-ideal in K.*

To pass from relations between fractional ideals to relations between elements, one has to deal with the group of units of R. Since R is an order, one can control this group through field embeddings $K \to \mathbf{C}$.

Producing invertible gcd's

Ge's main lemma. *There is a polynomial-time algorithm that, given K and a finite non-empty subset $T \subset K^*$, finds an order $R \subset K$ for which $\sum_{t \in T} Rt$ is an invertible R-ideal in K.*

Surprising discovery: among all such R, there is a *unique smallest* one.

Producing invertible gcd's

Ge's main lemma. *There is a polynomial-time algorithm that, given K and a finite non-empty subset $T \subset K^*$, finds an order $R \subset K$ for which $\sum_{t \in T} Rt$ is an invertible R-ideal in K.*

Surprising discovery: among all such R, there is a *unique smallest* one.

To state this, I replace T by the additive group I that it generates, so that $\sum_{t \in T} Rt = R \cdot I$.

Producing invertible gcd's

Ge's main lemma. *There is a polynomial-time algorithm that, given K and a finite non-empty subset $T \subset K^*$, finds an order $R \subset K$ for which $\sum_{t \in T} Rt$ is an invertible R-ideal in K.*

Surprising discovery: among all such R, there is a *unique smallest* one.

To state this, I replace T by the additive group I that it generates, so that $\sum_{t \in T} Rt = R \cdot I$.

I also replace K by any commutative $\mathbf{Q}$-algebra of finite vector space dimension d.

The smallest ring

Theorem. *Let K be a commutative $\mathbf{Q}$-algebra of finite vector space dimension d over $\mathbf{Q}$, and let $I \subset K$ be a finitely generated additive subgroup of K for which $K \cdot I = K$.*

The smallest ring

Theorem. *Let K be a commutative $\mathbf{Q}$-algebra of finite vector space dimension d over $\mathbf{Q}$, and let $I \subset K$ be a finitely generated additive subgroup of K for which $K \cdot I = K$. Then there is an order $B \subset K$ such that for every subring $R \subset K$ one has:*

$$R \cdot I \text{ is an invertible } R\text{-ideal in } K \iff B \subset R.$$

The smallest ring

Theorem. *Let K be a commutative $\mathbf{Q}$-algebra of finite vector space dimension d over $\mathbf{Q}$, and let $I \subset K$ be a finitely generated additive subgroup of K for which $K \cdot I = K$. Then there is an order $B \subset K$ such that for every subring $R \subset K$ one has:*

$$R \cdot I \text{ is an invertible } R\text{-ideal in } K \iff B \subset R.$$

References:
Everett Dade, Olga Taussky, Hans Zassenhaus (1961);
Daan van Gent; Alexander Spieksma.

Examples

If I is infinite cyclic, then $B = \mathbf{Z}$.

Examples

If I is infinite cyclic, then $B = \mathbf{Z}$.

If $I = \mathbf{Z} + \mathbf{Z}\alpha$, where α has minimal polynomial $a_n X^n + \ldots + a_1 X + a_0$ over $\mathbf{Q}$, with $\sum_i \mathbf{Z} a_i = \mathbf{Z}$, $n > 1$, then B has $\mathbf{Z}$-basis

$$1, \quad a_n\alpha, \quad a_n\alpha^2 + a_{n-1}\alpha, \ \ldots, \quad a_n\alpha^{n-1} + \ldots + a_2\alpha.$$

If also $a_n = \pm 1$, then $B = \mathbf{Z}[\alpha]$.

Examples

If I is infinite cyclic, then $B = \mathbf{Z}$.

If $I = \mathbf{Z} + \mathbf{Z}\alpha$, where α has minimal polynomial $a_n X^n + \ldots + a_1 X + a_0$ over $\mathbf{Q}$, with $\sum_i \mathbf{Z} a_i = \mathbf{Z}$, $n > 1$, then B has $\mathbf{Z}$-basis

$$1, \quad a_n\alpha, \quad a_n\alpha^2 + a_{n-1}\alpha, \ \ldots, \quad a_n\alpha^{n-1} + \ldots + a_2\alpha.$$

If also $a_n = \pm 1$, then $B = \mathbf{Z}[\alpha]$.

In general one has

$$\mathbf{Q} \cdot B = \mathbf{Q}[x/y : x \in I, y \in I \cap K^*].$$

Computing B

Theorem. *There is a polynomial-time algorithm that, given K and I as in the previous theorem, computes B.*

Computing B

Theorem. *There is a polynomial-time algorithm that, given K and I as in the previous theorem, computes B.*

Here is the algorithm:

- put $n = \max\{d-1, 1\}$, where $d = \dim_{\mathbf{Q}} K$;
- compute $I^n = I \cdot I \cdot \ldots \cdot I$;
- then $B = I^n : I^n$.

Computing B

Theorem. *There is a polynomial-time algorithm that, given K and I as in the previous theorem, computes B.*

Here is the algorithm:

- put $n = \max\{d-1, 1\}$, where $d = \dim_{\mathbf{Q}} K$;
- compute $I^n = I \cdot I \cdot \ldots \cdot I$;
- then $B = I^n : I^n$.

What can we use it for?

Subrings of finite type

A ring is *of finite type* if, as a ring, it is generated by a finite subset S.

Subrings of finite type

A ring is *of finite type* if, as a ring, it is generated by a finite subset S.

Example: $\mathbf{Z}[1/2] = \{a/2^n : a, n \in \mathbf{Z}, n \geq 0\} \subset \mathbf{Q}$.

Non-examples: $\mathbf{Q}$, $\{a/(2n+1) : a, n \in \mathbf{Z}\} \subset \mathbf{Q}$.

Subrings of finite type

A ring is *of finite type* if, as a ring, it is generated by a finite subset S.

Example: $\mathbf{Z}[1/2] = \{a/2^n : a,\, n \in \mathbf{Z},\, n \geq 0\} \subset \mathbf{Q}$.

Non-examples: $\mathbf{Q}$, $\{a/(2n+1) : a,\, n \in \mathbf{Z}\} \subset \mathbf{Q}$.

For a commutative $\mathbf{Q}$-algebra K of finite vector space dimension, we will consider subrings $\mathbf{Z}[S] \subset K$ of finite type. Just as orders in number fields, they may be viewed as analogous to curves over finite fields.

Algorithms for subrings of finite type

We specify our rings $\mathbf{Z}[S]$ by specifying K as well as a finite subset $S \subset K$.

Theorem (Alexander Spieksma)**.** *There is a polynomial-time algorithm that, given K as before, as well as $\alpha \in K$ and two finite subsets S, $S' \subset K$, decides whether one has $\alpha \in \mathbf{Z}[S]$, whether $\mathbf{Z}[S'] \subset \mathbf{Z}[S]$, and whether $\mathbf{Z}[S'] = \mathbf{Z}[S]$.*

Algorithms for subrings of finite type

We specify our rings $\mathbf{Z}[S]$ by specifying K as well as a finite subset $S \subset K$.

Theorem (Alexander Spieksma)**.** *There is a polynomial-time algorithm that, given K as before, as well as $\alpha \in K$ and two finite subsets S, $S' \subset K$, decides whether one has $\alpha \in \mathbf{Z}[S]$, whether $\mathbf{Z}[S'] \subset \mathbf{Z}[S]$, and whether $\mathbf{Z}[S'] = \mathbf{Z}[S]$.*

It is not even obvious that these are decidable at all!

Additive structure

The additive group of $\mathbf{Z}[S]$ is usually very complicated.

Additive structure

The additive group of $\mathbf{Z}[S]$ is usually very complicated.

Algorithm. *Given K and S, this algorithm constructs an* order $B \subset K$ *and an* invertible B*-ideal J in K with $J \subset B$ such that $\mathbf{Z}[S] = B[J^{-1}] = \bigcup_{n \geq 0} J^{-n}$.*

Additive structure

The additive group of $\mathbf{Z}[S]$ is usually very complicated.

Algorithm. *Given K and S, this algorithm constructs an* order $B \subset K$ *and an* invertible B*-ideal J in K with $J \subset B$ such that $\mathbf{Z}[S] = B[J^{-1}] = \bigcup_{n \geq 0} J^{-n}$.*

- *$I =$ additive group generated by $S \cup \{1\}$;*
- *the previous algorithm gives B, and $J = (B \cdot I)^{-1}$.*

Namely, $\mathbf{Z}[S] = \mathbf{Z}[S] \cdot I$ is an invertible $\mathbf{Z}[S]$-ideal in K, so $B \subset \mathbf{Z}[S]$, and therefore $\mathbf{Z}[S] = B[B \cdot I]$.

This algorithm runs in polynomial time.

Membership testing

Let $B \subset K$ be an order and let $J \subset B$ be an invertible B-ideal in K. Let $\alpha \in K$.

Membership testing

Let $B \subset K$ be an order and let $J \subset B$ be an invertible B-ideal in K. Let $\alpha \in K$.

The *denominator ideal* $\operatorname{den}(\alpha) = \{x \in B : x\alpha \in B\}$ has finite index in B.

One has $\alpha \in B[J^{-1}]$ if and only if the image of J in the finite ring $B/\operatorname{den}(\alpha)$ is nilpotent.

Membership testing

Let $B \subset K$ be an order and let $J \subset B$ be an invertible B-ideal in K. Let $\alpha \in K$.

The *denominator ideal* $\operatorname{den}(\alpha) = \{x \in B : x\alpha \in B\}$ has finite index in B.

One has $\alpha \in B[J^{-1}]$ if and only if the image of J in the finite ring $B/\operatorname{den}(\alpha)$ is nilpotent.

This is easy to test in polynomial time.

If $\alpha \in B[J^{-1}] = \mathbf{Z}[S]$, one can also obtain an expression for α in terms of the elements of S.

Finding polynomial relations

$K =$ a commutative $\mathbf{Q}$-algebra with $\dim_{\mathbf{Q}}(K) < \infty$, $S \subset K$ a finite subset, $\psi\colon \mathbf{Z}[X_s : s \in S] \to K$ the ring homomorphism with $X_s \mapsto s$ $(s \in S)$.

Finding polynomial relations

$K =$ a commutative $\mathbf{Q}$-algebra with $\dim_{\mathbf{Q}}(K) < \infty$, $S \subset K$ a finite subset, $\psi\colon \mathbf{Z}[X_s : s \in S] \to K$ the ring homomorphism with $X_s \mapsto s$ $(s \in S)$.

Tentative theorem (Alexander Spieksma)**.** *There is a polynomial-time algorithm that, given K and S, finds a set $T \subset \mathbf{Z}[X_s : s \in S]$ of generators of* $\ker \psi$.

Finding polynomial relations

$K =$ a commutative $\mathbf{Q}$-algebra with $\dim_{\mathbf{Q}}(K) < \infty$, $S \subset K$ a finite subset, $\psi\colon \mathbf{Z}[X_s : s \in S] \to K$ the ring homomorphism with $X_s \mapsto s$ $(s \in S)$.

Tentative theorem (Alexander Spieksma)**.** *There is a polynomial-time algorithm that, given K and S, finds a set $T \subset \mathbf{Z}[X_s : s \in S]$ of generators of* $\ker \psi$.

Most likely, T is the *reduced Gröbner basis* of $\ker \psi$ with respect to a suitable *term order* of $\mathbf{Z}[X_s : s \in S]$ that refines the ordering by total degree.

Gröbner bases

k is a field, n, $m \in \mathbf{Z}_{\geq 0}$, $C = k[X_1, \ldots, X_n]$,
$f_1, \ldots, f_m \in C$, $\mathbf{a} = (f_1, \ldots, f_m) \subset C$,

$$0 \to \mathbf{a} \to C \to C/\mathbf{a} \to 0.$$

Gröbner bases

k is a field, n, $m \in \mathbf{Z}_{\geq 0}$, $C = k[X_1, \ldots, X_n]$,
$f_1, \ldots, f_m \in C$, $\mathbf{a} = (f_1, \ldots, f_m) \subset C$,

$$0 \to \mathbf{a} \to C \to C/\mathbf{a} \to 0.$$

For a given term order on C, one can define and "compute" the *reduced Gröbner basis* for $\mathbf{a}$. It is a set of ideal generators of $\mathbf{a}$ that makes *equality tests* in $C/\mathbf{a}$ possible, and it gives rise to a *vector space basis* of $C/\mathbf{a}$ over k.

Gröbner bases

k is a field, n, $m \in \mathbf{Z}_{\geq 0}$, $C = k[X_1, \ldots, X_n]$,
$f_1, \ldots, f_m \in C$, $\mathbf{a} = (f_1, \ldots, f_m) \subset C$,

$$0 \to \mathbf{a} \to C \to C/\mathbf{a} \to 0.$$

For a given term order on C, one can define and "compute" the *reduced Gröbner basis* for $\mathbf{a}$. It is a set of ideal generators of $\mathbf{a}$ that makes *equality tests* in $C/\mathbf{a}$ possible, and it gives rise to a *vector space basis* of $C/\mathbf{a}$ over k.

It can be extended to cover the case $k = \mathbf{Z}$.

Efficiency

The Gröbner basis algorithm generalizes both the *Euclidean algorithm* ($n = 1$) and *Gaussian elimination* (all $\deg f_j = 1$). In almost all other cases, the running time estimates are very far from polynomial, and are typically gigantic as a function of n.

Efficiency

The Gröbner basis algorithm generalizes both the *Euclidean algorithm* ($n = 1$) and *Gaussian elimination* (all $\deg f_j = 1$). In almost all other cases, the running time estimates are very far from polynomial, and are typically gigantic as a function of n.

It is of great interest to find more situations in which Gröbner bases can be computed efficiently.

The main results so far

K finite over $\mathbf{Q}$, $S \subset K$ a finite subset,
$I \subset K$ a f.g. additive subgroup with $K \cdot I = K$.

The main results so far

K finite over $\mathbf{Q}$, $S \subset K$ a finite subset,
$I \subset K$ a f.g. additive subgroup with $K \cdot I = K$.

(1) There is a unique minimal subring $B \subset K$ for which $B \cdot I$ is B-invertible, and B is an order.

(2) Given K and I, we can quickly find B.

(3) Given K and S, we can probably quickly find a "reduced Gröbner basis for $\mathbf{Z}[S]$".

The main results so far

K finite over $\mathbf{Q}$, $S \subset K$ a finite subset,
$I \subset K$ a f.g. additive subgroup with $K \cdot I = K$.

(1) There is a unique minimal subring $B \subset K$ for which $B \cdot I$ is B-invertible, and B is an order.

(2) Given K and I, we can quickly find B.

(3) Given K and S, we can probably quickly find a "reduced Gröbner basis for $\mathbf{Z}[S]$".

How to transplant this to algebraic geometry?

Projective schemes

Let $R = \bigoplus_{n \geq 0} R_n$ be a *graded commutative ring*, of finite type over R_0, with R_0 *noetherian*.

In this situation, one defines the *scheme* $\operatorname{Proj} R$, which is a scheme over $\operatorname{Spec} R_0$.

Projective schemes

Let $R = \bigoplus_{n \geq 0} R_n$ be a *graded commutative ring*, of finite type over R_0, with R_0 *noetherian*.

In this situation, one defines the *scheme* $\operatorname{Proj} R$, which is a scheme over $\operatorname{Spec} R_0$.

Theorem. $(\exists B : \operatorname{Proj} R = \operatorname{Spec} B) \Longleftrightarrow \operatorname{Proj} R$ *is finite over* $\operatorname{Spec} R_0$.

Projective schemes

Let $R = \bigoplus_{n \geq 0} R_n$ be a *graded commutative ring*, of finite type over R_0, with R_0 *noetherian*.

In this situation, one defines the *scheme* $\operatorname{Proj} R$, which is a scheme over $\operatorname{Spec} R_0$.

Theorem. $(\exists B : \operatorname{Proj} R = \operatorname{Spec} B) \Longleftrightarrow \operatorname{Proj} R$ *is finite over* $\operatorname{Spec} R_0$.

Theorem (Elie Studnia)**.** *If* B *exists, it is the injective limit for* $m \to \infty$ *of the ring of degree preserving* R*-linear endomorphisms of* $\bigoplus_{n \geq m} R_n$.

Algorithms

In the number theory situation, the graded ring equals $\bigoplus_{n \geq 0} I^n$, with $I \subset K$ as before, and $I^0 = R_0 = \overline{\mathbf{Z}}$.

Algorithms

In the number theory situation, the graded ring equals $\bigoplus_{n \geq 0} I^n$, with $I \subset K$ as before, and $I^0 = R_0 = \bar{\mathbf{Z}}$.

The algorithm for finding B may extend to the case R_0 has Krull dimension at most 1, and maybe more generally.

Finding Gröbner bases

Using the B-algorithm, we could find a Gröbner basis for $\mathbf{Z}[S]$. The ring $\mathbf{Z}[S]$ is *quasifinite* over $\mathbf{Z}$.

Which rings are quasifinite over a subring so that we can find a Gröbner basis in a similar manner?

Finding Gröbner bases

Using the B-algorithm, we could find a Gröbner basis for $\mathbf{Z}[S]$. The ring $\mathbf{Z}[S]$ is *quasifinite* over $\mathbf{Z}$.

Which rings are quasifinite over a subring so that we can find a Gröbner basis in a similar manner?

Note: $\mathbf{Z}[S]$ was not given by generators and relations, but as a subring of K. One may wish to impose a similar condition on $R_0[S]$.

Finding Gröbner bases

Using the B-algorithm, we could find a Gröbner basis for $\mathbf{Z}[S]$. The ring $\mathbf{Z}[S]$ is *quasifinite* over $\mathbf{Z}$.

Which rings are quasifinite over a subring so that we can find a Gröbner basis in a similar manner?

Note: $\mathbf{Z}[S]$ was not given by generators and relations, but as a subring of K. One may wish to impose a similar condition on $R_0[S]$.

Ignorance is the beginning of progress!

I thank you for your attention.