Some finiteness results on monogenic orders in arbitrary characteristic

Khoa D. Nguyen

Department of Mathematics
University of British Columbia
and Pacific Institute for the Mathematical Sciences

March 2016

Overview

$\mathbb{N} = \{1, 2, \ldots\}$ and $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

R : integrally closed finitely generated domain, $K = \mathrm{Frac}(R)$.
Most important example: number field K and ring of S-integers $R = \mathcal{O}_{K,S}$.

Other examples: polynomial rings $\mathcal{O}_{K,S}[x_1, \ldots, x_n]$, $\mathbb{F}_q[x_1, \ldots, x_n]$, and (certain of) their quotients.

We consider the following 2 problems:

(A) Fix s integral over R and separable over K, describe all t such that $R[s] = R[t]$.

(B) Fix s and t integral over R and separable over K, describe all $(m, n) \in \mathbb{N} \times \mathbb{N}$ such that $R[s^m] = R[t^n]$.

Overview

$\mathbb{N} = \{1, 2, \ldots\}$ and $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

R : integrally closed finitely generated domain, $K = \mathrm{Frac}(R)$.
Most important example: number field K and ring of S-integers $R = \mathcal{O}_{K,S}$.

Other examples: polynomial rings $\mathcal{O}_{K,S}[x_1, \ldots, x_n]$, $\mathbb{F}_q[x_1, \ldots, x_n]$, and (certain of) their quotients.

We consider the following 2 problems:

(A) Fix s integral over R and separable over K, describe all t such that $R[s] = R[t]$.

(B) Fix s and t integral over R and separable over K, describe all $(m, n) \in \mathbb{N} \times \mathbb{N}$ such that $R[s^m] = R[t^n]$.

Overview

$\mathbb{N} = \{1, 2, \ldots\}$ and $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

R : integrally closed finitely generated domain, $K = \mathrm{Frac}(R)$.
Most important example: number field K and ring of S-integers $R = \mathcal{O}_{K,S}$.

Other examples: polynomial rings $\mathcal{O}_{K,S}[x_1, \ldots, x_n]$, $\mathbb{F}_q[x_1, \ldots, x_n]$, and (certain of) their quotients.

We consider the following 2 problems:

(A) Fix s integral over R and separable over K, describe all t such that $R[s] = R[t]$.

(B) Fix s and t integral over R and separable over K, describe all $(m, n) \in \mathbb{N} \times \mathbb{N}$ such that $R[s^m] = R[t^n]$.

Overview

$\mathbb{N} = \{1, 2, \ldots\}$ and $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

R : integrally closed finitely generated domain, $K = \mathrm{Frac}(R)$.
Most important example: number field K and ring of S-integers $R = \mathcal{O}_{K,S}$.

Other examples: polynomial rings $\mathcal{O}_{K,S}[x_1, \ldots, x_n]$, $\mathbb{F}_q[x_1, \ldots, x_n]$, and (certain of) their quotients.

We consider the following 2 problems:

(A) Fix s integral over R and separable over K, describe all t such that $R[s] = R[t]$.

(B) Fix s and t integral over R and separable over K, describe all $(m, n) \in \mathbb{N} \times \mathbb{N}$ such that $R[s^m] = R[t^n]$.

Overview

$\mathbb{N} = \{1, 2, \ldots\}$ and $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

R : integrally closed finitely generated domain, $K = \mathrm{Frac}(R)$.
Most important example: number field K and ring of S-integers $R = \mathcal{O}_{K,S}$.

Other examples: polynomial rings $\mathcal{O}_{K,S}[x_1, \ldots, x_n]$, $\mathbb{F}_q[x_1, \ldots, x_n]$, and (certain of) their quotients.

We consider the following 2 problems:

(A) Fix s integral over R and separable over K, describe all t such that $R[s] = R[t]$.

(B) Fix s and t integral over R and separable over K, describe all $(m, n) \in \mathbb{N} \times \mathbb{N}$ such that $R[s^m] = R[t^n]$.

Overview

What are known?

Bell and Hare: some partial results for (A) and (B) in characteristic 0, and applications to Pisot numbers.

Evertse and Győry: solve (A) in characteristic 0.

N.: solve (B) in characteristic 0.

Bell and N.: solve (A) and (B) in characteristic $p > 0$.

Overview

What are known?

Bell and Hare: some partial results for (A) and (B) in characteristic 0, and applications to Pisot numbers.

Evertse and Győry: solve (A) in characteristic 0.

N.: solve (B) in characteristic 0.

Bell and N.: solve (A) and (B) in characteristic $p > 0$.

Overview

What are known?

Bell and Hare: some partial results for (A) and (B) in characteristic 0, and applications to Pisot numbers.

Evertse and Győry: solve (A) in characteristic 0.

N.: solve (B) in characteristic 0.

Bell and N.: solve (A) and (B) in characteristic $p > 0$.

Overview

What are known?

Bell and Hare: some partial results for (A) and (B) in characteristic 0, and applications to Pisot numbers.

Evertse and Győry: solve (A) in characteristic 0.

N.: solve (B) in characteristic 0.

Bell and N.: solve (A) and (B) in characteristic $p > 0$.

Overview

What are known?

Bell and Hare: some partial results for (A) and (B) in characteristic 0, and applications to Pisot numbers.

Evertse and Győry: solve (A) in characteristic 0.

N.: solve (B) in characteristic 0.

Bell and N.: solve (A) and (B) in characteristic $p > 0$.

References

- J.-H. Evertse and K. Győry, *On unit equations and decomposable form equations*, Crelle **358**, 1985
- J. P. Bell and K. Hare, *On $\mathbb{Z}$-modules of algebraic integers,* Canad. J. Math. **61**, 2009
- K. N. *On modules of integral elements over finitely generated domains*, to appear Trans. Amer. Math. Soc.
- K. N. and J. P. Bell, *Some finiteness results on monogenic orders in positive characteristic*, arXiv:1508.07624

Part I: Results in Characteristic 0

Problem (A)

Let s be integral over R. Observation: if $R[t] = R[s]$ then $R[at + b] = R[s]$ for $a \in R^*$ and $b \in R$.

Evertse and Győry prove that up to the transformations $t \mapsto at + b$, there are only finitely many t's satisfying $R[t] = R[s]$.

Problem (A)

Let s be integral over R. Observation: if $R[t] = R[s]$ then $R[at + b] = R[s]$ for $a \in R^*$ and $b \in R$.

Evertse and Győry prove that up to the transformations $t \mapsto at + b$, there are only finitely many t's satisfying $R[t] = R[s]$.

Problem (A)

Theorem (Evertse-Győry)

There are $t_1, \dots, t_N$ such that $R[t_i] = R[s]$ for every $i \in \{1, \dots, N\}$, and for any t satisfying $R[t] = R[s]$, we have $t = at_i + b$ for some $i \in \{1, \dots, N\}$, $a \in R^*$, and $b \in R$.

The number of elements N can be bounded by an explicit constant c_1 with a mild dependence on R and s.

Example: for $R = \mathcal{O}_{K,S}$, c_1 only depends on $\#S$ and $[K(s) : \mathbb{Q}]$.

When $R = \mathcal{O}_{K,S}$, the list $t_1, \dots, t_N$ can be determined effectively.

Problem (A)

Theorem (Evertse-Győry)

There are $t_1, \dots, t_N$ such that $R[t_i] = R[s]$ for every $i \in \{1, \dots, N\}$, and for any t satisfying $R[t] = R[s]$, we have $t = at_i + b$ for some $i \in \{1, \dots, N\}$, $a \in R^*$, and $b \in R$.

The number of elements N can be bounded by an explicit constant c_1 with a mild dependence on R and s.

Example: for $R = \mathcal{O}_{K,S}$, c_1 only depends on $\#S$ and $[K(s) : \mathbb{Q}]$.

When $R = \mathcal{O}_{K,S}$, the list $t_1, \dots, t_N$ can be determined effectively.

Problem (A)

Theorem (Evertse-Győry)

There are $t_1, \dots, t_N$ such that $R[t_i] = R[s]$ for every $i \in \{1, \dots, N\}$, and for any t satisfying $R[t] = R[s]$, we have $t = at_i + b$ for some $i \in \{1, \dots, N\}$, $a \in R^*$, and $b \in R$.

The number of elements N can be bounded by an explicit constant c_1 with a mild dependence on R and s.

Example: for $R = \mathcal{O}_{K,S}$, c_1 only depends on $\#S$ and $[K(s) : \mathbb{Q}]$.

When $R = \mathcal{O}_{K,S}$, the list $t_1, \dots, t_N$ can be determined effectively.

Problem (A)

Theorem (Evertse-Győry)

There are $t_1, \dots, t_N$ such that $R[t_i] = R[s]$ for every $i \in \{1, \dots, N\}$, and for any t satisfying $R[t] = R[s]$, we have $t = at_i + b$ for some $i \in \{1, \dots, N\}$, $a \in R^*$, and $b \in R$.

The number of elements N can be bounded by an explicit constant c_1 with a mild dependence on R and s.

Example: for $R = \mathcal{O}_{K,S}$, c_1 only depends on $\#S$ and $[K(s) : \mathbb{Q}]$.

When $R = \mathcal{O}_{K,S}$, the list $t_1, \dots, t_N$ can be determined effectively.

Problem (A)

Let E be a field and α be separable over E.

Let $\alpha_1 = \alpha, \ldots, \alpha_D$ be the conjugates of α over E. Define:

$$\mathrm{disc}_E(\alpha) = \prod_{1 \le i < j \le D} (\alpha_i - \alpha_j)^2 \in E$$

Solving for t satisfying $R[t] = R[s]$ is equivalent to solving the "discriminant form equation":

$$\mathrm{disc}_K(t) = u \, \mathrm{disc}_K(s) \text{ for } t \in R[s], \text{ and } u \in R^*.$$

Problem (A)

Let E be a field and α be separable over E.

Let $\alpha_1 = \alpha, \ldots, \alpha_D$ be the conjugates of α over E. Define:

$$\mathrm{disc}_E(\alpha) = \prod_{1 \le i < j \le D} (\alpha_i - \alpha_j)^2 \in E$$

Solving for t satisfying $R[t] = R[s]$ is equivalent to solving the "discriminant form equation":

$$\mathrm{disc}_K(t) = u \,\mathrm{disc}_K(s) \text{ for } t \in R[s], \text{ and } u \in R^*.$$

Problem (A)

Let E be a field and α be separable over E.

Let $\alpha_1 = \alpha, \ldots, \alpha_D$ be the conjugates of α over E. Define:

$$\mathrm{disc}_E(\alpha) = \prod_{1 \le i < j \le D} (\alpha_i - \alpha_j)^2 \in E$$

Solving for t satisfying $R[t] = R[s]$ is equivalent to solving the "discriminant form equation":

$$\mathrm{disc}_K(t) = u\,\mathrm{disc}_K(s) \text{ for } t \in R[s], \text{ and } u \in R^*.$$

Problem (B)

Fix s and t that are integral over R. Solve for (m, n) satisfying $R[s^m] = R[t^n]$.

Also assume $s^n \notin R$ and $t^n \notin R$ for every $n \in \mathbb{N}$. Actually, the problem becomes much easier otherwise.

"Experience" tells us that there should be finitely many such pairs (m, n) unless there is a "special" relation between s and t.

Consider the following 3 subsets of $\mathbb{N}^2$.

Problem (B)

Fix s and t that are integral over R. Solve for (m, n) satisfying $R[s^m] = R[t^n]$.

Also assume $s^n \notin R$ and $t^n \notin R$ for every $n \in \mathbb{N}$. Actually, the problem becomes much easier otherwise.

"Experience" tells us that there should be finitely many such pairs (m, n) unless there is a "special" relation between s and t.

Consider the following 3 subsets of $\mathbb{N}^2$.

Problem (B)

Fix s and t that are integral over R. Solve for (m, n) satisfying $R[s^m] = R[t^n]$.

Also assume $s^n \notin R$ and $t^n \notin R$ for every $n \in \mathbb{N}$. Actually, the problem becomes much easier otherwise.

"Experience" tells us that there should be finitely many such pairs (m, n) unless there is a "special" relation between s and t.

Consider the following 3 subsets of $\mathbb{N}^2$.

Problem (B)

Fix s and t that are integral over R. Solve for (m, n) satisfying $R[s^m] = R[t^n]$.

Also assume $s^n \notin R$ and $t^n \notin R$ for every $n \in \mathbb{N}$. Actually, the problem becomes much easier otherwise.

"Experience" tells us that there should be finitely many such pairs (m, n) unless there is a "special" relation between s and t.

Consider the following 3 subsets of $\mathbb{N}^2$.

Problem (B): 3 special subsets

$\mathcal{A}(R,s,t) := \{(m,n) \in \mathbb{N}^2 : \ \dfrac{s^m}{t^n} \in R^*\}$

Obviously, $R[s^m] = R[t^n]$ for $(m,n) \in A(R,s,t)$.

$\mathcal{B}(R,s,t) := \{(m,n) \in \mathbb{N}^2 : \ [K(t^n) : K] = 2$ and $\dfrac{s^m}{\sigma(t^n)} \in R^*\}$,

σ is the non-trivial automorphism of the quadratic extension $K(t^n)/K$.

If $(m,n) \in B(R,s,t)$ then $R[t^n] = R[\sigma(t^n)]$ (since $t^n + \sigma(t^n) \in R$), and $R[\sigma(t^n)] = R[s^m]$.

$\mathcal{C}(R,s,t) := \{(m,n) \in \mathbb{N}^2 : \ s^m t^n \in R^*\}$

If $(m,n) \in \mathcal{C}(R,s,t)$, we also have $R[s^m] = R[t^n]$ as follows.

Problem (B): 3 special subsets

$$\mathcal{A}(R,s,t) := \{(m,n) \in \mathbb{N}^2 : \ \frac{s^m}{t^n} \in R^*\}$$

Obviously, $R[s^m] = R[t^n]$ for $(m,n) \in A(R,s,t)$.

$$\mathcal{B}(R,s,t) := \{(m,n) \in \mathbb{N}^2 : \ [K(t^n) : K] = 2 \text{ and } \frac{s^m}{\sigma(t^n)} \in R^*\},$$

σ is the non-trivial automorphism of the quadratic extension $K(t^n)/K$.

If $(m,n) \in B(R,s,t)$ then $R[t^n] = R[\sigma(t^n)]$ (since $t^n + \sigma(t^n) \in R$), and $R[\sigma(t^n)] = R[s^m]$.

$$\mathcal{C}(R,s,t) := \{(m,n) \in \mathbb{N}^2 : \ s^m t^n \in R^*\}$$

If $(m,n) \in \mathcal{C}(R,s,t)$, we also have $R[s^m] = R[t^n]$ as follows.

Problem (B): 3 special subsets

$\mathcal{A}(R, s, t) := \{(m, n) \in \mathbb{N}^2 : \ \frac{s^m}{t^n} \in R^*\}$
Obviously, $R[s^m] = R[t^n]$ for $(m, n) \in A(R, s, t)$.

$\mathcal{B}(R, s, t) := \{(m, n) \in \mathbb{N}^2 : \ [K(t^n) : K] = 2 \text{ and } \frac{s^m}{\sigma(t^n)} \in R^*\}$,
σ is the non-trivial automorphism of the quadratic extension $K(t^n)/K$.

If $(m, n) \in B(R, s, t)$ then $R[t^n] = R[\sigma(t^n)]$ (since $t^n + \sigma(t^n) \in R$), and $R[\sigma(t^n)] = R[s^m]$.

$\mathcal{C}(R, s, t) := \{(m, n) \in \mathbb{N}^2 : \ s^m t^n \in R^*\}$
If $(m, n) \in \mathcal{C}(R, s, t)$, we also have $R[s^m] = R[t^n]$ as follows.

Problem (B): 3 special subsets

$\mathcal{A}(R, s, t) := \{(m, n) \in \mathbb{N}^2 : \ \frac{s^m}{t^n} \in R^*\}$
Obviously, $R[s^m] = R[t^n]$ for $(m, n) \in A(R, s, t)$.

$\mathcal{B}(R, s, t) := \{(m, n) \in \mathbb{N}^2 : \ [K(t^n) : K] = 2 \text{ and } \frac{s^m}{\sigma(t^n)} \in R^*\}$,
σ is the non-trivial automorphism of the quadratic extension $K(t^n)/K$.

If $(m, n) \in B(R, s, t)$ then $R[t^n] = R[\sigma(t^n)]$ (since $t^n + \sigma(t^n) \in R$), and $R[\sigma(t^n)] = R[s^m]$.

$\mathcal{C}(R, s, t) := \{(m, n) \in \mathbb{N}^2 : \ s^m t^n \in R^*\}$
If $(m, n) \in \mathcal{C}(R, s, t)$, we also have $R[s^m] = R[t^n]$ as follows.

Problem (B): 3 special subsets

α integral over R. Say α is a unit over R if one of the following equivalent conditions holds:

(i) α is a unit of $R[\alpha]$.

(ii) The constant coefficient of its minimal polynomial over K is in R^*.

For $(m, n) \in \mathcal{C}(R, s, t)$, we have $s^m t^n \in R^*$ so both s^m and t^n are units over R.

So $R[s^m] = R[1/t^n] \subseteq R[t^n]$, likewise $R[t^n] \subseteq R[s^m]$. Hence $R[s^m] = R[t^n]$.

Problem (B): 3 special subsets

α integral over R. Say α is a unit over R if one of the following equivalent conditions holds:

(i) α is a unit of $R[\alpha]$.

(ii) The constant coefficient of its minimal polynomial over K is in R^*.

For $(m, n) \in \mathcal{C}(R, s, t)$, we have $s^m t^n \in R^*$ so both s^m and t^n are units over R.

So $R[s^m] = R[1/t^n] \subseteq R[t^n]$, likewise $R[t^n] \subseteq R[s^m]$. Hence $R[s^m] = R[t^n]$.

Problem (B): 3 special subsets

α integral over R. Say α is a unit over R if one of the following equivalent conditions holds:

(i) α is a unit of $R[\alpha]$.

(ii) The constant coefficient of its minimal polynomial over K is in R^*.

For $(m, n) \in \mathcal{C}(R, s, t)$, we have $s^m t^n \in R^*$ so both s^m and t^n are units over R.

So $R[s^m] = R[1/t^n] \subseteq R[t^n]$, likewise $R[t^n] \subseteq R[s^m]$. Hence $R[s^m] = R[t^n]$.

Problem (B)

For a "random" pair (s, t), the sets $\mathcal{A}(R, s, t)$, $\mathcal{B}(r, s, t)$, and $\mathcal{C}(R, s, t)$ are empty. If non-empty, they have the form

$$\{(km_0, kn_0) : \ k \in \mathbb{N}\}.$$

We prove that outside $\mathcal{A}(R, s, t) \cup \mathcal{B}(R, s, t) \cup \mathcal{C}(R, s, t)$, there are only finitely many (m, n) satisfying $R[s^m] = R[t^n]$.

Problem (B)

For a "random" pair (s, t), the sets $\mathcal{A}(R, s, t)$, $\mathcal{B}(r, s, t)$, and $\mathcal{C}(R, s, t)$ are empty. If non-empty, they have the form

$$\{(km_0, kn_0) : \ k \in \mathbb{N}\}.$$

We prove that outside $\mathcal{A}(R, s, t) \cup \mathcal{B}(R, s, t) \cup \mathcal{C}(R, s, t)$, there are only finitely many (m, n) satisfying $R[s^m] = R[t^n]$.

Problem (B)

Theorem (K. N.)

Let s and t be integral over R such that $s^n \notin R$ and $t^n \notin R$ for every $n \in \mathbb{N}$. Outside $\mathcal{A}(R, s, t) \cup \mathcal{B}(R, s, t) \cup \mathcal{C}(R, s, t)$, there are only finitely many (m, n) satisfying $R[s^m] = R[t^n]$.

There is an explicit bound with a mild dependence on R, s, and t for the number of such pairs (m, n).

The proof is not effective.

Problem (B)

Theorem (K. N.)

Let s and t be integral over R such that $s^n \notin R$ and $t^n \notin R$ for every $n \in \mathbb{N}$. Outside $\mathcal{A}(R, s, t) \cup \mathcal{B}(R, s, t) \cup \mathcal{C}(R, s, t)$, there are only finitely many (m, n) satisfying $R[s^m] = R[t^n]$.

There is an explicit bound with a mild dependence on R, s, and t for the number of such pairs (m, n).

The proof is not effective.

Problem (B)

Theorem (K. N.)

Let s and t be integral over R such that $s^n \notin R$ and $t^n \notin R$ for every $n \in \mathbb{N}$. Outside $\mathcal{A}(R, s, t) \cup \mathcal{B}(R, s, t) \cup \mathcal{C}(R, s, t)$, there are only finitely many (m, n) satisfying $R[s^m] = R[t^n]$.

There is an explicit bound with a mild dependence on R, s, and t for the number of such pairs (m, n).

The proof is not effective.

Unit equation

Proofs use the celebrated theorem of Evertse, Schlickewei, and Schmidt on unit equations.

Key fact: the group R^* is finitely generated (Roquette, 1958).

Let E be a field, $n \geq 2$, $a_1, \ldots, a_n \in E^*$. Consider the equation:

$$a_1 X_1 + \ldots + a_n X_n = 1.$$

A solution $(x_1, \ldots, x_n)$ is said to be non-degenerate if no subsum vanishes: there does not exist non-empty proper $J \subset \{1, \ldots, n\}$ such that $\sum_{j \in J} a_j x_j = 0$.

Unit equation

Proofs use the celebrated theorem of Evertse, Schlickewei, and Schmidt on unit equations.

Key fact: the group R^* is finitely generated (Roquette, 1958).

Let E be a field, $n \geq 2$, $a_1, \ldots, a_n \in E^*$. Consider the equation:

$$a_1 X_1 + \ldots + a_n X_n = 1.$$

A solution $(x_1, \ldots, x_n)$ is said to be non-degenerate if no subsum vanishes: there does not exist non-empty proper $J \subset \{1, \ldots, n\}$ such that $\sum_{j \in J} a_j x_j = 0$.

Unit equation

Proofs use the celebrated theorem of Evertse, Schlickewei, and Schmidt on unit equations.

Key fact: the group R^* is finitely generated (Roquette, 1958).

Let E be a field, $n \geq 2$, $a_1, \ldots, a_n \in E^*$. Consider the equation:

$$a_1 X_1 + \ldots + a_n X_n = 1.$$

A solution $(x_1, \ldots, x_n)$ is said to be non-degenerate if no subsum vanishes: there does not exist non-empty proper $J \subset \{1, \ldots, n\}$ such that $\sum_{j \in J} a_j x_j = 0$.

Unit equation

Proofs use the celebrated theorem of Evertse, Schlickewei, and Schmidt on unit equations.

Key fact: the group R^* is finitely generated (Roquette, 1958).

Let E be a field, $n \geq 2$, $a_1, \ldots, a_n \in E^*$. Consider the equation:

$$a_1 X_1 + \ldots + a_n X_n = 1.$$

A solution $(x_1, \ldots, x_n)$ is said to be non-degenerate if no subsum vanishes: there does not exist non-empty proper $J \subset \{1, \ldots, n\}$ such that $\sum_{j \in J} a_j x_j = 0$.

Theorem of Evertse, Schlickewei, and Schmidt

Let E be a field of characteristic 0, let $n \geq 2$, and let Γ be a subgroup of $(E^*)^n$ having finite rank r.

This means $\mathbb{Q} \otimes_{\mathbb{Z}} \Gamma$ is a finite dimensional $\mathbb{Q}$-vector space and r is the dimension.

Theorem (Evertse, Schlickewei, Schmidt)

Assume $\mathrm{char}(E) = 0$. *Let* $a_1, \ldots, a_n \in E^*$, *then the equation* $a_1 X_1 + \ldots + a_n X_n = 1$ *has at most* $\exp((6n)^{3n}(r+1))$ *non-degenerate solutions* $(x_1, \ldots, x_n) \in \Gamma$.

Theorem of Evertse, Schlickewei, and Schmidt

Let E be a field of characteristic 0, let $n \geq 2$, and let Γ be a subgroup of $(E^*)^n$ having finite rank r.

This means $\mathbb{Q} \otimes_{\mathbb{Z}} \Gamma$ is a finite dimensional $\mathbb{Q}$-vector space and r is the dimension.

Theorem (Evertse, Schlickewei, Schmidt)

Assume $\mathrm{char}(E) = 0$. *Let* $a_1, \ldots, a_n \in E^*$, *then the equation* $a_1 X_1 + \ldots + a_n X_n = 1$ *has at most* $\exp((6n)^{3n}(r+1))$ *non-degenerate solutions* $(x_1, \ldots, x_n) \in \Gamma$.

Theorem of Evertse, Schlickewei, and Schmidt

Let E be a field of characteristic 0, let $n \geq 2$, and let Γ be a subgroup of $(E^*)^n$ having finite rank r.

This means $\mathbb{Q} \otimes_{\mathbb{Z}} \Gamma$ is a finite dimensional $\mathbb{Q}$-vector space and r is the dimension.

Theorem (Evertse, Schlickewei, Schmidt)

Assume $\mathrm{char}(E) = 0$. *Let* $a_1, \ldots, a_n \in E^*$, *then the equation* $a_1 X_1 + \ldots + a_n X_n = 1$ *has at most* $\exp((6n)^{3n}(r+1))$ *non-degenerate solutions* $(x_1, \ldots, x_n) \in \Gamma$.

Unit equations: remarks

Note the rather amazing uniform upper bound.

The proof uses the (quantitative) Subspace Theorem, hence not effective except when $n = 2$ and $E \subseteq \bar{\mathbb{Q}}$ where other methods (eg Baker's method) can be applied.

Using this theorem: reduce our problem to such a unit equation.

Non-degenerate solutions $\longrightarrow$ finiteness.

Degenerate solutions $\longrightarrow$ vanishing proper subsums. Further (algebraic, combinatorial, Galois,...) arguments give the desired special relation.

Unit equations: remarks

Note the rather amazing uniform upper bound.

The proof uses the (quantitative) Subspace Theorem, hence not effective except when $n = 2$ and $E \subseteq \bar{\mathbb{Q}}$ where other methods (eg Baker's method) can be applied.

Using this theorem: reduce our problem to such a unit equation.

Non-degenerate solutions $\longrightarrow$ finiteness.

Degenerate solutions $\longrightarrow$ vanishing proper subsums. Further (algebraic, combinatorial, Galois,...) arguments give the desired special relation.

Unit equations: remarks

Note the rather amazing uniform upper bound.

The proof uses the (quantitative) Subspace Theorem, hence not effective except when $n = 2$ and $E \subseteq \bar{\mathbb{Q}}$ where other methods (eg Baker's method) can be applied.

Using this theorem: reduce our problem to such a unit equation.

Non-degenerate solutions $\longrightarrow$ finiteness.

Degenerate solutions $\longrightarrow$ vanishing proper subsums. Further (algebraic, combinatorial, Galois,...) arguments give the desired special relation.

Unit equations: remarks

Note the rather amazing uniform upper bound.

The proof uses the (quantitative) Subspace Theorem, hence not effective except when $n = 2$ and $E \subseteq \bar{\mathbb{Q}}$ where other methods (eg Baker's method) can be applied.

Using this theorem: reduce our problem to such a unit equation.

Non-degenerate solutions $\longrightarrow$ finiteness.

Degenerate solutions $\longrightarrow$ vanishing proper subsums. Further (algebraic, combinatorial, Galois,...) arguments give the desired special relation.

From Problem (A) to unit equations

Fix s integral over R, let's assume $[K(s) : K] \geq 3$. Let L be the Galois closure of $K(s)/K$, and let $\mathcal{O}$ be the integral closure of R in L.

If $R[t] = R[s]$ then

$$\sigma(t) - \tau(t) = u_{\sigma,\tau}(\sigma(s) - \tau(s))$$

for some $u_{\sigma,\tau} \in \mathcal{O}^*$ for distinct K-embeddings σ and τ of $K(s)$ into L.

Hence $\sigma(t) - \tau(t)$ belongs to a fixed finitely generated subgroup of L^*.

From Problem (A) to unit equations

Fix s integral over R, let's assume $[K(s) : K] \geq 3$. Let L be the Galois closure of $K(s)/K$, and let $\mathcal{O}$ be the integral closure of R in L.

If $R[t] = R[s]$ then

$$\sigma(t) - \tau(t) = u_{\sigma,\tau}(\sigma(s) - \tau(s))$$

for some $u_{\sigma,\tau} \in \mathcal{O}^*$ for distinct K-embeddings σ and τ of $K(s)$ into L.

Hence $\sigma(t) - \tau(t)$ belongs to a fixed finitely generated subgroup of L^*.

From Problem (A) to unit equations

Fix s integral over R, let's assume $[K(s) : K] \geq 3$. Let L be the Galois closure of $K(s)/K$, and let $\mathcal{O}$ be the integral closure of R in L.

If $R[t] = R[s]$ then

$$\sigma(t) - \tau(t) = u_{\sigma,\tau}(\sigma(s) - \tau(s))$$

for some $u_{\sigma,\tau} \in \mathcal{O}^*$ for distinct K-embeddings σ and τ of $K(s)$ into L.

Hence $\sigma(t) - \tau(t)$ belongs to a fixed finitely generated subgroup of L^*.

From Problem (A) to unit equations

For any 3 distinct embeddings σ, τ, η, from Siegel's identity:

$$\frac{\sigma(t)-\tau(t)}{\sigma(t)-\eta(t)}+\frac{\tau(t)-\eta(t)}{\sigma(t)-\eta(t)}=1$$

we get a solution of the unit equation

$$X_1+X_2=1.$$

From Problem (B) to unit equations

Fix s, t integral over R. Let L be the Galois closure of $K(s,t)/K$, and let $\mathcal{O}$ be the integral closure of R in L.

If $R[t^n] = R[s^m]$, get

$$\sigma(t)^n - \tau(t)^n = u_{m,n,\sigma,\tau}(\sigma(s)^m - \tau(s)^m)$$

for some $u_{m,n,\sigma,\tau} \in \mathcal{O}^*$. For simplicity, write u for $u_{m,n,\sigma,\tau}$. Then

$$\sigma(t)^n - \tau(t)^n + u\tau(s)^m = u\sigma(s)^m$$

$$\frac{\sigma(t)^n}{u\sigma(s)^m} - \frac{\tau(t)^n}{u\sigma(s)^m} + \frac{\tau(s)^m}{\sigma(s)^m} = 1$$

From Problem (B) to unit equations

Fix s, t integral over R. Let L be the Galois closure of $K(s,t)/K$, and let $\mathcal{O}$ be the integral closure of R in L.

If $R[t^n] = R[s^m]$, get

$$\sigma(t)^n - \tau(t)^n = u_{m,n,\sigma,\tau}(\sigma(s)^m - \tau(s)^m)$$

for some $u_{m,n,\sigma,\tau} \in \mathcal{O}^*$. For simplicity, write u for $u_{m,n,\sigma,\tau}$. Then

$$\sigma(t)^n - \tau(t)^n + u\tau(s)^m = u\sigma(s)^m$$

$$\frac{\sigma(t)^n}{u\sigma(s)^m} - \frac{\tau(t)^n}{u\sigma(s)^m} + \frac{\tau(s)^m}{\sigma(s)^m} = 1$$

From Problem (B) to unit equations

Fix s, t integral over R. Let L be the Galois closure of $K(s,t)/K$, and let $\mathcal{O}$ be the integral closure of R in L.

If $R[t^n] = R[s^m]$, get

$$\sigma(t)^n - \tau(t)^n = u_{m,n,\sigma,\tau}(\sigma(s)^m - \tau(s)^m)$$

for some $u_{m,n,\sigma,\tau} \in \mathcal{O}^*$. For simplicity, write u for $u_{m,n,\sigma,\tau}$. Then

$$\sigma(t)^n - \tau(t)^n + u\tau(s)^m = u\sigma(s)^m$$
$$\frac{\sigma(t)^n}{u\sigma(s)^m} - \frac{\tau(t)^n}{u\sigma(s)^m} + \frac{\tau(s)^m}{\sigma(s)^m} = 1$$

From Problem (B) to unit equations

We get a solution of the unit equation:

$$X_1 - X_2 + X_3 = 1.$$

By Evertse-Schlickewei-Schmidt, finitely many non-degenerate solutions.

To study degenerate solutions: use further Galois and combinatorial arguments to get the relations described in the sets $\mathcal{A}(R, s, t)$, $\mathcal{B}(R, s, t)$, and $\mathcal{C}(R, s, t)$.

From Problem (B) to unit equations

We get a solution of the unit equation:

$$X_1 - X_2 + X_3 = 1.$$

By Evertse-Schlickewei-Schmidt, finitely many non-degenerate solutions.

To study degenerate solutions: use further Galois and combinatorial arguments to get the relations described in the sets $\mathcal{A}(R, s, t)$, $\mathcal{B}(R, s, t)$, and $\mathcal{C}(R, s, t)$.

From Problem (B) to unit equations

We get a solution of the unit equation:

$$X_1 - X_2 + X_3 = 1.$$

By Evertse-Schlickewei-Schmidt, finitely many non-degenerate solutions.

To study degenerate solutions: use further Galois and combinatorial arguments to get the relations described in the sets $\mathcal{A}(R, s, t)$, $\mathcal{B}(R, s, t)$, and $\mathcal{C}(R, s, t)$.

Part II: Results in Positive Characteristic

Unit equations in positive characteristic

Consider similar problems when $\mathrm{char}(K) = p > 0$ with the extra condition that s and t are separable over K.

Previous tricks to obtain unit equations still work. However...

... due to the Frobenius automorphism $x \mapsto x^p$, results for unit equations in characteristic p are not as "clean" as the Evertse-Schlickewei-Schmidt theorem.

For example, if (x, y) is a solution of $X + Y = 1$ then (x^{p^k}, y^{p^k}) is a solution for every $k \in \mathbb{N}$. Similarly, if $R[s^m] = R[t^n]$ then $R[s^{mp^k}] = R[t^{np^k}]$.

Unit equations in positive characteristic

Consider similar problems when $\mathrm{char}(K) = p > 0$ with the extra condition that s and t are separable over K.

Previous tricks to obtain unit equations still work. However...

... due to the Frobenius automorphism $x \mapsto x^p$, results for unit equations in characteristic p are not as "clean" as the Evertse-Schlickewei-Schmidt theorem.

For example, if (x, y) is a solution of $X + Y = 1$ then (x^{p^k}, y^{p^k}) is a solution for every $k \in \mathbb{N}$. Similarly, if $R[s^m] = R[t^n]$ then $R[s^{mp^k}] = R[t^{np^k}]$.

Unit equations in positive characteristic

Consider similar problems when $\mathrm{char}(K) = p > 0$ with the extra condition that s and t are separable over K.

Previous tricks to obtain unit equations still work. However...

... due to the Frobenius automorphism $x \mapsto x^p$, results for unit equations in characteristic p are not as "clean" as the Evertse-Schlickewei-Schmidt theorem.

For example, if (x, y) is a solution of $X + Y = 1$ then (x^{p^k}, y^{p^k}) is a solution for every $k \in \mathbb{N}$. Similarly, if $R[s^m] = R[t^n]$ then $R[s^{mp^k}] = R[t^{np^k}]$.

Unit equations in positive characteristic

Consider similar problems when $\mathrm{char}(K) = p > 0$ with the extra condition that s and t are separable over K.

Previous tricks to obtain unit equations still work. However...

... due to the Frobenius automorphism $x \mapsto x^p$, results for unit equations in characteristic p are not as "clean" as the Evertse-Schlickewei-Schmidt theorem.

For example, if (x, y) is a solution of $X + Y = 1$ then (x^{p^k}, y^{p^k}) is a solution for every $k \in \mathbb{N}$. Similarly, if $R[s^m] = R[t^n]$ then $R[s^{mp^k}] = R[t^{np^k}]$.

Equation in 2 variables

For simplicity, let E be a finitely generated field over $\mathbb{F}_p$, and let G be a finitely generated subgroup of E^*.

Theorem (2-variable equations)

There exist a finite subset $\mathscr{X}$ of $\bar{L}^*$ such that every solution $(x, y) \in G^2$ of the equation $X + Y = 1$ has the form $x = x_0^{p^k}$ and $y = y_0^{p^k}$ for some $x_0, y_0 \in \mathscr{X}$ and $k \in \mathbb{N}_0$.

Equation in 2 variables

For simplicity, let E be a finitely generated field over $\mathbb{F}_p$, and let G be a finitely generated subgroup of E^*.

Theorem (2-variable equations)

There exist a finite subset $\mathscr{X}$ of $\bar{L}^*$ such that every solution $(x, y) \in G^2$ of the equation $X + Y = 1$ has the form $x = x_0^{p^k}$ and $y = y_0^{p^k}$ for some $x_0, y_0 \in \mathscr{X}$ and $k \in \mathbb{N}_0$.

Equation in 3 variables

Theorem (3-variable equations)

There exist a constant $C \in \mathbb{N}_0$ and a finite subset $\mathscr{X}$ of $\bar{L}^*$ such that every solution $(x, y, z) \in G^3$ of $X + Y + Z = 1$ satisfies:

$$x^{p^C} = x_1^{p^k} x_2^{p^\ell};\ y^{p^C} = y_1^{p^k} y_2^{p^\ell};\ z^{p^C} = z_1^{p^k} z_2^{p^\ell}$$

for some $x_1, \ldots, z_2 \in \mathscr{X}$ and $k, \ell \in \mathbb{N}_0$.

Similar result for a general equation in n variables. This time, we need $n - 1$ "Frobenius orbits": $x_1^{p^{k_1}} \ldots x_{n-1}^{p^{k_{n-1}}}$.

Expect $C = 0$ (as in the case of 2 variables), but we are unable to prove it. Anyway, above results are good enough for our purpose.

Equation in 3 variables

Theorem (3-variable equations)

There exist a constant $C \in \mathbb{N}_0$ and a finite subset $\mathscr{X}$ of $\bar{L}^*$ such that every solution $(x, y, z) \in G^3$ of $X + Y + Z = 1$ satisfies:

$$x^{p^C} = x_1^{p^k} x_2^{p^\ell};\ y^{p^C} = y_1^{p^k} y_2^{p^\ell};\ z^{p^C} = z_1^{p^k} z_2^{p^\ell}$$

for some $x_1, \ldots, z_2 \in \mathscr{X}$ and $k, \ell \in \mathbb{N}_0$.

Similar result for a general equation in n variables. This time, we need $n - 1$ "Frobenius orbits": $x_1^{p^{k_1}} \ldots x_{n-1}^{p^{k_{n-1}}}$.

Expect $C = 0$ (as in the case of 2 variables), but we are unable to prove it. Anyway, above results are good enough for our purpose.

Equation in 3 variables

Theorem (3-variable equations)

There exist a constant $C \in \mathbb{N}_0$ and a finite subset $\mathscr{X}$ of $\bar{L}^*$ such that every solution $(x, y, z) \in G^3$ of $X + Y + Z = 1$ satisfies:

$$x^{p^C} = x_1^{p^k} x_2^{p^\ell};\ y^{p^C} = y_1^{p^k} y_2^{p^\ell};\ z^{p^C} = z_1^{p^k} z_2^{p^\ell}$$

for some $x_1, \ldots, z_2 \in \mathscr{X}$ and $k, \ell \in \mathbb{N}_0$.

Similar result for a general equation in n variables. This time, we need $n - 1$ "Frobenius orbits": $x_1^{p^{k_1}} \ldots x_{n-1}^{p^{k_{n-1}}}$.

Expect $C = 0$ (as in the case of 2 variables), but we are unable to prove it. Anyway, above results are good enough for our purpose.

Problem (A) in characteristic p

R, K, p as before. Fix s that is integral over R and separable over K.

Theorem

Write $d = [K(s) : K]$ and $D = \mathrm{disc}_K(s)$. There are finitely many elements $t_1, \ldots, t_N$ satisfying:

(a) $R[t_i] = R[s]$ *for* $1 \leq i \leq N$.

(b) *If* $R[t] = R[s]$ *then* $t = at_i^q + b$ *for some* $1 \leq i \leq N$, $q \geq 1$ *is a power of* p, $a, b \in K$ *such that* $\dfrac{a^{d(d-1)}}{D^{1-q}} \in R^*$.

Problem (A) in characteristic p

R, K, p as before. Fix s that is integral over R and separable over K.

Theorem

Write $d = [K(s) : K]$ and $D = \mathrm{disc}_K(s)$. There are finitely many elements $t_1, \ldots, t_N$ satisfying:

(a) $R[t_i] = R[s]$ *for* $1 \leq i \leq N$.

(b) *If* $R[t] = R[s]$ *then* $t = at_i^q + b$ *for some* $1 \leq i \leq N$, $q \geq 1$ *is a power of* p, $a, b \in K$ *such that* $\dfrac{a^{d(d-1)}}{D^{1-q}} \in R^*$.

Problem (A): further remarks

We also provide an explicit bound on N.

The conclusion above cannot be improved in the following sense:

(i) Raising to the q-th power is needed when, say, $R[s] = R[s^p]$. Indeed $R[t^{p^n}] = R[s]$ whenever $R[t] = R[s]$.

(ii) The condition on a is needed so that $\operatorname{disc}_K(t)/\operatorname{disc}_K(s) \in R^*$.

(iii) There is an example that we cannot improve the conclusion from $b \in K$ to $b \in R$.

Reduce to unit equations as before. However, the resulting combinatorial problem is much more complicated this time.

Problem (A): further remarks

We also provide an explicit bound on N.

The conclusion above cannot be improved in the following sense:

(i) Raising to the q-th power is needed when, say, $R[s] = R[s^p]$. Indeed $R[t^{p^n}] = R[s]$ whenever $R[t] = R[s]$.

(ii) The condition on a is needed so that $\operatorname{disc}_K(t)/\operatorname{disc}_K(s) \in R^*$.

(iii) There is an example that we cannot improve the conclusion from $b \in K$ to $b \in R$.

Reduce to unit equations as before. However, the resulting combinatorial problem is much more complicated this time.

Problem (A): further remarks

We also provide an explicit bound on N.

The conclusion above cannot be improved in the following sense:

(i) Raising to the q-th power is needed when, say, $R[s] = R[s^p]$. Indeed $R[t^{p^n}] = R[s]$ whenever $R[t] = R[s]$.

(ii) The condition on a is needed so that $\operatorname{disc}_K(t)/\operatorname{disc}_K(s) \in R^*$.

(iii) There is an example that we cannot improve the conclusion from $b \in K$ to $b \in R$.

Reduce to unit equations as before. However, the resulting combinatorial problem is much more complicated this time.

Problem (A): further remarks

We also provide an explicit bound on N.

The conclusion above cannot be improved in the following sense:

(i) Raising to the q-th power is needed when, say, $R[s] = R[s^p]$. Indeed $R[t^{p^n}] = R[s]$ whenever $R[t] = R[s]$.

(ii) The condition on a is needed so that $\operatorname{disc}_K(t)/\operatorname{disc}_K(s) \in R^*$.

(iii) There is an example that we cannot improve the conclusion from $b \in K$ to $b \in R$.

Reduce to unit equations as before. However, the resulting combinatorial problem is much more complicated this time.

Problem (A): further remarks

We also provide an explicit bound on N.

The conclusion above cannot be improved in the following sense:

(i) Raising to the q-th power is needed when, say, $R[s] = R[s^p]$. Indeed $R[t^{p^n}] = R[s]$ whenever $R[t] = R[s]$.

(ii) The condition on a is needed so that $\operatorname{disc}_K(t)/\operatorname{disc}_K(s) \in R^*$.

(iii) There is an example that we cannot improve the conclusion from $b \in K$ to $b \in R$.

Reduce to unit equations as before. However, the resulting combinatorial problem is much more complicated this time.

Problem (B) in characteristic p

Fix s and t that are integral over R and separable over K. As before, assume $s^n \notin R$ and $t^n \notin R$ for every $n \in \mathbb{N}$ (the problem is easier otherwise).

Define the sets $\mathcal{A} = \mathcal{A}(R, s, t)$, $\mathcal{B} = \mathcal{B}(R, s, t)$, $\mathcal{C} = \mathcal{C}(R, s, t)$ as in characteristic 0.

Theorem

The set of pairs (m, n) satisfying $R[s^m] = R[t^n]$ is contained in the union of $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, and finitely many sets of the form

$$\{(c_1 q^k + c_2 q^\ell, c_3 q^k + c_4 q^\ell) : \ k, \ell \in \mathbb{N}_0\}$$

for some power $q > 1$ of p and some $c_1, \ldots, c_4 \in \mathbb{Q}$.

Problem (B) in characteristic p

Fix s and t that are integral over R and separable over K. As before, assume $s^n \notin R$ and $t^n \notin R$ for every $n \in \mathbb{N}$ (the problem is easier otherwise).

Define the sets $\mathcal{A} = \mathcal{A}(R, s, t)$, $\mathcal{B} = \mathcal{B}(R, s, t)$, $\mathcal{C} = \mathcal{C}(R, s, t)$ as in characteristic 0.

Theorem

The set of pairs (m, n) satisfying $R[s^m] = R[t^n]$ is contained in the union of $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, and finitely many sets of the form

$$\{(c_1 q^k + c_2 q^\ell, c_3 q^k + c_4 q^\ell) : \ k, \ell \in \mathbb{N}_0\}$$

for some power $q > 1$ of p and some $c_1, \ldots, c_4 \in \mathbb{Q}$.

Problem (B) in characteristic p

Fix s and t that are integral over R and separable over K. As before, assume $s^n \notin R$ and $t^n \notin R$ for every $n \in \mathbb{N}$ (the problem is easier otherwise).

Define the sets $\mathcal{A} = \mathcal{A}(R, s, t)$, $\mathcal{B} = \mathcal{B}(R, s, t)$, $\mathcal{C} = \mathcal{C}(R, s, t)$ as in characteristic 0.

Theorem

The set of pairs (m, n) satisfying $R[s^m] = R[t^n]$ is contained in the union of $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, and finitely many sets of the form

$$\{(c_1 q^k + c_2 q^\ell, c_3 q^k + c_4 q^\ell) : \ k, \ell \in \mathbb{N}_0\}$$

for some power $q > 1$ of p and some $c_1, \ldots, c_4 \in \mathbb{Q}$.

Problem (B): further remarks

The point is that outside $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, there could be finitely many sets depending on 2 "free" variables k and ℓ as described.

This aspect cannot be improved. At first, we tried to use only "single" Frobenius orbits (i.e. $\{(c_1 q^k, c_2 q^k)\}_k$). Then we realize an example that really needs both k and ℓ as in the statement of the theorem.

Problem (B): further remarks

The point is that outside $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, there could be finitely many sets depending on 2 "free" variables k and ℓ as described.

This aspect cannot be improved. At first, we tried to use only "single" Frobenius orbits (i.e. $\{(c_1 q^k, c_2 q^k)\}_k$). Then we realize an example that really needs both k and ℓ as in the statement of the theorem.

THANK YOU!