COMPUTATION OF TRIANGULAR INTEGRAL BASES

Jens Bauch & Ha Tran

Simon Fraser University & University of Calgary

ANTS XIII
University of Wisconsin

July 16, 2018

Example

Let $K = \mathbb{Q}(\theta)$ be a number field of degree n.

The **ring of integers** $\mathbb{Z}_K$ of K is the **integral closure** of $\mathbb{Z}$ in K.

A basis $(b_0, \ldots, b_{n-1})$ is called a **triangular basis** of $\mathbb{Z}_K$ if

$$b_i = \frac{\theta^i + \sum_{j<i} \lambda_{i,j}\theta^j}{h_i}, \quad \lambda_{i,j}, h_i \in \mathbb{Z}.$$

Example

Let $K = \mathbb{Q}(\theta)$ be a number field of degree n.

The **ring of integers** $\mathbb{Z}_K$ of K is the **integral closure** of $\mathbb{Z}$ in K.

A basis $(b_0, \ldots, b_{n-1})$ is called a **triangular basis** of $\mathbb{Z}_K$ if

$$b_i = \frac{\theta^i + \sum_{j<i} \lambda_{i,j}\theta^j}{h_i}, \quad \lambda_{i,j}, h_i \in \mathbb{Z}.$$

For $K = \mathbb{Q}(\sqrt{5})$ we have

$$Z_K = \left\langle 1, \frac{\sqrt{5}+1}{2} \right\rangle_{\mathbb{Z}}.$$

Approaches

$K = \mathbb{Q}(\theta)$, f monic minimal polynomial of θ.

$\mathrm{Disc}(f) = I \cdot \mathcal{S}^2$ with $I, \mathcal{S} \in \mathbb{Z}$ and I $\square$-free and p prime dividing $\mathcal{S}$.

1. Linear algebra over $\mathbb{Z}$
   - Round 2 Algorithm (Pohst-Zassenhaus)
2. p-adic approach
   - Round 4 Algorithm (Zassenhaus, Ford, ...)
   - OM-Representation (Nart, Guardia, Stainsby, B.)
   - Puiseux expansion (v. Hoeij, Decker, ...)

Approaches

$K = \mathbb{Q}(\theta)$, f monic minimal polynomial of θ.

$\mathrm{Disc}(f) = I \cdot \mathcal{S}^2$ with $I, \mathcal{S} \in \mathbb{Z}$ and I $\square$-free and p prime dividing $\mathcal{S}$.

1. Linear algebra over $\mathbb{Z}$
   - Round 2 Algorithm (Pohst-Zassenhaus)
2. p-adic approach
   - Round 4 Algorithm (Zassenhaus, Ford, ...)
   - OM-Representation (Nart, Guardia, Stainsby, B.)
   - Puiseux expansion (v. Hoeij, Decker, ...)

Our algorithm: $\mathfrak{p}$-adic initialization step and then linear algebra.

Notations

- A Dedekind domain, K the fraction field of A.
- Fix a non-zero prime ideal $\mathfrak{p}$ of A with prime element π.
- $A_{\mathfrak{p}}$ localization of A at $\mathfrak{p}$.
- θ is a root of a monic irreducible separable polynomial $f \in A[x]$ of degree n.
- $L = K(\theta)$ finite separable extension of K generated by θ.
- $\mathcal{O}$ is the integral closure of A in L and $\mathcal{O}_{\mathfrak{p}}$ is the integral closure of $A_{\mathfrak{p}}$ in L.
- A $\mathfrak{p}$-integral basis is an $A_{\mathfrak{p}}$-basis of $\mathcal{O}_{\mathfrak{p}}$.

Notations

- A Dedekind domain, K the fraction field of A.
- Fix a non-zero prime ideal $\mathfrak{p}$ of A with prime element π.
- $A_{\mathfrak{p}}$ localization of A at $\mathfrak{p}$.
- θ is a root of a monic irreducible separable polynomial $f \in A[x]$ of degree n.
- $L = K(\theta)$ finite separable extension of K generated by θ.
- $\mathcal{O}$ is the integral closure of A in L and $\mathcal{O}_{\mathfrak{p}}$ is the integral closure of $A_{\mathfrak{p}}$ in L.
- A $\mathfrak{p}$-integral basis is an $A_{\mathfrak{p}}$-basis of $\mathcal{O}_{\mathfrak{p}}$.

This talk: Construct a triangular $\mathfrak{p}$-integral basis.

Notations

- A Dedekind domain, K the fraction field of A.
- Fix a non-zero prime ideal $\mathfrak{p}$ of A with prime element π.
- $A_{\mathfrak{p}}$ localization of A at $\mathfrak{p}$.
- θ is a root of a monic irreducible separable polynomial $f \in A[x]$ of degree n.
- $L = K(\theta)$ finite separable extension of K generated by θ.
- $\mathcal{O}$ is the integral closure of A in L and $\mathcal{O}_{\mathfrak{p}}$ is the integral closure of $A_{\mathfrak{p}}$ in L.
- A $\mathfrak{p}$-integral basis is an $A_{\mathfrak{p}}$-basis of $\mathcal{O}_{\mathfrak{p}}$.

This talk: Construct a triangular $\mathfrak{p}$-integral basis.

Example: $A = \mathbb{Z}$, $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{5})$, $f(x) = x^2 - 5$.

Notations

- A Dedekind domain, K the fraction field of A.
- Fix a non-zero prime ideal $\mathfrak{p}$ of A with prime element π.
- $A_{\mathfrak{p}}$ localization of A at $\mathfrak{p}$.
- θ is a root of a monic irreducible separable polynomial $f \in A[x]$ of degree n.
- $L = K(\theta)$ finite separable extension of K generated by θ.
- $\mathcal{O}$ is the integral closure of A in L and $\mathcal{O}_{\mathfrak{p}}$ is the integral closure of $A_{\mathfrak{p}}$ in L.
- A $\mathfrak{p}$-integral basis is an $A_{\mathfrak{p}}$-basis of $\mathcal{O}_{\mathfrak{p}}$.

This talk: Construct a triangular $\mathfrak{p}$-integral basis.

Example: $A = \mathbb{Z}$, $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{5})$, $f(x) = x^2 - 5$.
$\mathrm{Disc}(f) = 2^2 \cdot 5$, $\mathfrak{p} = 2 \cdot \mathbb{Z}$, $\pi = 2$.

$(1, \frac{1+\sqrt{5}}{2})$ is a triangular 2-integral basis.

Construction of triangular bases

Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_s$ be all prime ideals of $\mathcal{O}$ lying over $\mathfrak{p}$. Denote by e_i the ramification index of $\mathfrak{P}_i$ over $\mathfrak{p}$.

$$\omega : L \to \mathbb{Z} \cup \{\infty\}, \quad \omega(z) = \left\lfloor \min_{1 \le i \le s} \left\{ \frac{v_{\mathfrak{P}_i}(z)}{e_i} \right\} \right\rfloor.$$

For $0 \le i \le n-1$, we call a monic degree i polynomial $g_i(x)$ in $A[x]$ *i-maximal* if

$$\omega(g_i(\theta)) \ge \omega(g(\theta))$$

for all monic $g \in A[x]$ of degree i.

Construction of triangular bases

Theorem (H. D. Stainsby, 2018.)

Let $b_0, \ldots, b_{n-1} \in L$ with

$$b_i = \frac{g_i(\theta)}{\pi^{\omega(g_i(\theta))}}, \quad g_i(x) \in A[x] \text{ } i\text{-maximal},$$

then $(b_0, \ldots, b_{n-1})$ is a triangular $\mathfrak{p}$-integral basis.

Construction of triangular bases

Theorem (H. D. Stainsby, 2018.)

Let $b_0, \ldots, b_{n-1} \in L$ with

$$b_i = \frac{g_i(\theta)}{\pi^{\omega(g_i(\theta))}}, \quad g_i(x) \in A[x] \text{ } i\text{-maximal},$$

then $(b_0, \ldots, b_{n-1})$ is a triangular $\mathfrak{p}$-integral basis.

Idea of the algorithm: Construct $g_i(x) \in A[x]$ being i-maximal.

Augmentation-Step

Denote by $\mathcal{R} \subset A$ a fixed system of representatives of $k_\mathfrak{p} = A/\mathfrak{p}$. Let $c_0, \ldots, c_m$ be in L ordered by non-decreasing ω-value and

$$c_m^* = c_m + \sum_{j=0}^{m-1} \lambda_j \pi^{\omega(c_m)-\omega(c_j)} c_j \text{ with } \lambda_0, \ldots \lambda_{m-1} \in \mathcal{R}.$$

If $\omega\left(c_m^*\right) > \omega(c_m)$, then we call c_m^* an **augmentation-step**.

Augmentation-Step

Denote by $\mathcal{R} \subset A$ a fixed system of representatives of $k_{\mathfrak{p}} = A/\mathfrak{p}$.
Let $c_0, \ldots, c_m$ be in L ordered by non-decreasing ω-value and

$$c_m^* = c_m + \sum_{j=0}^{m-1} \lambda_j \pi^{\omega(c_m)-\omega(c_j)} c_j \text{ with } \lambda_0, \ldots \lambda_{m-1} \in \mathcal{R}.$$

If $\omega\left(c_m^*\right) > \omega(c_m)$, then we call c_m^* an **augmentation-step**.

The algorithm: Set $b_0 = 1$.

Augmentation-Step

Denote by $\mathcal{R} \subset A$ a fixed system of representatives of $k_{\mathfrak{p}} = A/\mathfrak{p}$. Let $c_0, \ldots, c_m$ be in L ordered by non-decreasing ω-value and

$$c_m^* = c_m + \sum_{j=0}^{m-1} \lambda_j \pi^{\omega(c_m)-\omega(c_j)} c_j \text{ with } \lambda_0, \ldots \lambda_{m-1} \in \mathcal{R}.$$

If $\omega\left(c_m^*\right) > \omega(c_m)$, then we call c_m^* an **augmentation-step**.

The algorithm: Set $b_0 = 1$.

Find $\lambda_{0,0} \in \mathcal{R}$ s.t. $b_1^* = \theta + \lambda_{0,0} b_0$ is 1-maximal. Set $b_1 = b_1^* / \pi^{\omega(b_1^*)}$.

Augmentation-Step

Denote by $\mathcal{R} \subset A$ a fixed system of representatives of $k_{\mathfrak{p}} = A/\mathfrak{p}$. Let $c_0, \ldots, c_m$ be in L ordered by non-decreasing ω-value and

$$c_m^* = c_m + \sum_{j=0}^{m-1} \lambda_j \pi^{\omega(c_m)-\omega(c_j)} c_j \text{ with } \lambda_0, \ldots \lambda_{m-1} \in \mathcal{R}.$$

If $\omega\left(c_m^*\right) > \omega(c_m)$, then we call c_m^* an **augmentation-step**.

The algorithm: Set $b_0 = 1$.

Find $\lambda_{0,0} \in \mathcal{R}$ s.t. $b_1^* = \theta + \lambda_{0,0} b_0$ is 1-maximal. Set $b_1 = b_1^*/\pi^{\omega(b_1^*)}$.

Find $\lambda_{1,0}, \lambda_{1,1} \in \mathcal{R}$ s.t. $b_2^* = \theta^2 + \lambda_{1,1} b_1 + \lambda_{1,0} b_0$ is 2-maximal. Set $b_2 = b_2^*/\pi^{\omega(b_2^*)}$.

$\vdots$

Augmentation-Step

Denote by $\mathcal{R} \subset A$ a fixed system of representatives of $k_{\mathfrak{p}} = A/\mathfrak{p}$. Let $c_0, \ldots, c_m$ be in L ordered by non-decreasing ω-value and

$$c_m^* = c_m + \sum_{j=0}^{m-1} \lambda_j \pi^{\omega(c_m)-\omega(c_j)} c_j \text{ with } \lambda_0, \ldots \lambda_{m-1} \in \mathcal{R}.$$

If $\omega\left(c_m^*\right) > \omega(c_m)$, then we call c_m^* an **augmentation-step**.

The algorithm: Set $b_0 = 1$.

Find $\lambda_{0,0} \in \mathcal{R}$ s.t. $b_1^* = \theta + \lambda_{0,0} b_0$ is 1-maximal. Set $b_1 = b_1^* / \pi^{\omega(b_1^*)}$.

Find $\lambda_{1,0}, \lambda_{1,1} \in \mathcal{R}$ s.t. $b_2^* = \theta^2 + \lambda_{1,1} b_1 + \lambda_{1,0} b_0$ is 2-maximal. Set $b_2 = b_2^* / \pi^{\omega(b_2^*)}$.

$\vdots$

$\Rightarrow$ $b_0, \ldots, b_{n-1}$ triangular with b_i is i maximal.

Realization of Augmentation

- Let $K_{\mathfrak{p}}$ be the completion of K at $\mathfrak{p}$, extend $v_{\mathfrak{p}}$ to $K_{\mathfrak{p}}$.
- Denote by $\hat{A}_{\mathfrak{p}}$ the valuation ring of $v_{\mathfrak{p}}$ in $K_{\mathfrak{p}}$.
- For $1 \leq i \leq s$, we denote by $L_{\mathfrak{P}_i}$ the completion of L at $\mathfrak{P}_i$.
- $f = f_1 \cdots f_s \in \hat{A}_{\mathfrak{p}}[x]$ and θ_i is a root of f_i.
- We write $L_{\mathfrak{P}_i} = K_{\mathfrak{p}}(\theta_i)$ and define

$$\iota_i : L \to L_{\mathfrak{P}_i}, \quad \theta \mapsto \theta_i.$$

- $\mathcal{O}_{\mathfrak{P}_i}$ integral closure of $\hat{A}_{\mathfrak{p}}$ in $L_{\mathfrak{P}_i}$ with integral basis $\mathcal{B}_i$.
- For $z \in L_{\mathfrak{P}_i}$, we denote by $\mathcal{C}_{\mathcal{B}_i}(z) = (z_1, \ldots, z_{n_i}) \in K_{\mathfrak{p}}^{n_i}$ the coefficients of z w.r.t $\mathcal{B}_i$, where $n_i = e_i \cdot f(\mathfrak{P}_i/\mathfrak{p})$.

We define $\iota : L \to \prod_i K_{\mathfrak{p}}^{n_i} = K_{\mathfrak{p}}^n, \qquad \iota(z) = (\mathcal{C}_{\mathcal{B}_i}(\iota_i(z)))_{1 \leq i \leq s}$.

Realization of Augmentation

For $z \in L$ we write $\iota(z) = (z_1, \ldots, z_n) \in K_{\mathfrak{p}}^n$.

Lemma

$\omega(z) = \min_{1 \le i \le n}\{v_{\mathfrak{p}}(z_i)\}$.

Realization of Augmentation

For $z \in L$ we write $\iota(z) = (z_1, \dots, z_n) \in K_{\mathfrak{p}}^n$.

Lemma

$\omega(z) = \min_{1 \le i \le n} \{v_{\mathfrak{p}}(z_i)\}$.

For $\lambda \in K_{\mathfrak{p}}$ with $v_{\mathfrak{p}}(\lambda) = m$, we write $\lambda = \sum_{j=m}^{\infty} \lambda_j \pi^j$ with $\lambda_j \in \mathcal{R}$. For an integer $r \ge m$, we define

$$\mathrm{lt}_{\mathrm{r}}(\lambda) = \begin{cases} \lambda_m & \text{if } r = m \\ 0 & \text{else.} \end{cases}$$

Realization of Augmentation

For $z \in L$ we write $\iota(z) = (z_1, \ldots, z_n) \in K_{\mathfrak{p}}^n$.

Lemma

$\omega(z) = \min_{1 \leq i \leq n}\{v_{\mathfrak{p}}(z_i)\}$.

For $\lambda \in K_{\mathfrak{p}}$ with $v_{\mathfrak{p}}(\lambda) = m$, we write $\lambda = \sum_{j=m}^{\infty} \lambda_j \pi^j$ with $\lambda_j \in \mathcal{R}$.
For an integer $r \geq m$, we define

$$\mathrm{lt_r}(\lambda) = \begin{cases} \lambda_m & \text{if } r = m \\ 0 & \text{else.} \end{cases}$$

For $z \in L$ and $r \geq \omega(z)$, we set

$$\mathrm{LT}_r(z) = (\mathrm{lt_r}(\mathrm{z_i}))_{1 \leq i \leq n} \in k_{\mathfrak{p}}^n.$$

Lemma

Let $c_0, \dots, c_m \in L$ ordered by non-decreasing ω-value and $\alpha_0, \dots, \alpha_m \in \mathcal{R}$ with $\alpha_m \neq 0$ such that

$$\sum_{0 \leq i \leq m} \alpha_i \mathrm{LT}_{\omega(c_i)}(\iota(c_i)) = 0. \quad (1)$$

Then, $c_m^* = c_m + \sum_{j=0}^{m-1} \frac{\alpha_j}{\alpha_m} \pi^{\omega(c_m)-\omega(c_j)} c_j$ realizes an augmentation-step.

Realization of Augmentation

Lemma

Let $c_0, \ldots, c_m \in L$ ordered by non-decreasing ω-value and $\alpha_0, \ldots, \alpha_m \in \mathcal{R}$ with $\alpha_m \neq 0$ such that

$$\sum_{0 \leq i \leq m} \alpha_i \mathrm{LT}_{\omega(c_i)}(\iota(c_i)) = 0. \tag{1}$$

Then, $c_m^* = c_m + \sum_{j=0}^{m-1} \frac{\alpha_j}{\alpha_m} \pi^{\omega(c_m)-\omega(c_j)} c_j$ realizes an augmentation-step.

Moreover, if the $\mathrm{LT}_{\omega(c_i)}(\iota(c_i))$ are $k_{\mathfrak{p}}$-linearly independent, then no augmentation-step is applicable.

Example

Let $A = \mathbb{F}_{13}[t]$ and L be the function field defined by
$f = x^4 + 4x^3 + (4t^2 + 4)x^2 + 8t^2x + 2t^8 + 4t^4 + 8t^2 \in A[x]$.

Example

Let $A = \mathbb{F}_{13}[t]$ and L be the function field defined by
$f = x^4 + 4x^3 + (4t^2 + 4)x^2 + 8t^2x + 2t^8 + 4t^4 + 8t^2 \in A[x]$.

$\mathrm{Disc}(f) = I \cdot \mathcal{S}^2$ with $\mathcal{S} = t^2(t^3 + 3)(t^3 + 10)$.

We consider $\mathfrak{p} = t \cdot A$ with $\pi = t$, and $\mathfrak{p}\mathcal{O} = \mathfrak{P}_1 \cdot \mathfrak{P}_2$.

Example

Let $A = \mathbb{F}_{13}[t]$ and L be the function field defined by
$f = x^4 + 4x^3 + (4t^2+4)x^2 + 8t^2x + 2t^8 + 4t^4 + 8t^2 \in A[x]$.

$\mathrm{Disc}(f) = I \cdot \mathcal{S}^2$ with $\mathcal{S} = t^2(t^3+3)(t^3+10)$.

We consider $\mathfrak{p} = t \cdot A$ with $\pi = t$, and $\mathfrak{p}\mathcal{O} = \mathfrak{P}_1 \cdot \mathfrak{P}_2$.

$f = f_1 \cdot f_2$ over $\hat{A}_{\mathfrak{p}}[x] = \mathbb{F}_{13}[[t]][x]$

$f_1 \approx \Phi_1 = x^2 + 2t^2, \qquad f_2 \approx \Phi_2 = x^2 + 4x + 2t^2 + 4.$

Example

Let $A = \mathbb{F}_{13}[t]$ and L be the function field defined by $f = x^4 + 4x^3 + (4t^2 + 4)x^2 + 8t^2x + 2t^8 + 4t^4 + 8t^2 \in A[x]$.

$\mathrm{Disc}(f) = I \cdot \mathcal{S}^2$ with $\mathcal{S} = t^2(t^3 + 3)(t^3 + 10)$.

We consider $\mathfrak{p} = t \cdot A$ with $\pi = t$, and $\mathfrak{p}\mathcal{O} = \mathfrak{P}_1 \cdot \mathfrak{P}_2$.

$f = f_1 \cdot f_2$ over $\hat{A}_{\mathfrak{p}}[x] = \mathbb{F}_{13}[[t]][x]$

$f_1 \approx \Phi_1 = x^2 + 2t^2, \qquad f_2 \approx \Phi_2 = x^2 + 4x + 2t^2 + 4.$

$L_{\mathfrak{P}_i} = \mathbb{F}_{13}((t))[x]/(f_i) \approx \mathbb{F}_{13}((t))[x]/(\Phi_i)$.

$\mathcal{B}_1 = (1, \theta_1/t)$, $\mathcal{B}_2 = (1, (\theta_2 + 2)/t)$ with $\Phi_i(\theta_i) = 0$, for $i = 1, 2$.

Example

Let $A = \mathbb{F}_{13}[t]$ and L be the function field defined by $f = x^4 + 4x^3 + (4t^2+4)x^2 + 8t^2x + 2t^8 + 4t^4 + 8t^2 \in A[x]$.

$\mathrm{Disc}(f) = I \cdot \mathcal{S}^2$ with $\mathcal{S} = t^2(t^3+3)(t^3+10)$.

We consider $\mathfrak{p} = t \cdot A$ with $\pi = t$, and $\mathfrak{p}\mathcal{O} = \mathfrak{P}_1 \cdot \mathfrak{P}_2$.

$f = f_1 \cdot f_2$ over $\hat{A}_{\mathfrak{p}}[x] = \mathbb{F}_{13}[[t]][x]$

$f_1 \approx \Phi_1 = x^2 + 2t^2, \qquad f_2 \approx \Phi_2 = x^2 + 4x + 2t^2 + 4.$

$L_{\mathfrak{P}_i} = \mathbb{F}_{13}((t))[x]/(f_i) \approx \mathbb{F}_{13}((t))[x]/(\Phi_i)$.

$\mathcal{B}_1 = (1, \theta_1/t)$, $\mathcal{B}_2 = (1, (\theta_2+2)/t)$ with $\Phi_i(\theta_i) = 0$, for $i = 1, 2$.

	ι_1	ι_2
1	1	1
θ	θ_1	θ_2
θ^2	$11t^2$	$9\theta_2 + 11t^2 + 9$
θ^3	$11t^2\theta_1$	$(11t^2+12)\theta_2 + 8t^2 + 3$

Example

	$\mathcal{B}_1$		$\mathcal{B}_2$		ω
$\iota(1)$	1	0	1	0	0
$\iota(\theta)$	0	t	11	t	0
$\iota(\theta^2)$	$11t^2$	0	$11t^2 + 4$	$9t$	0
$\iota(\theta^3)$	0	$11t^3$	$12t^2 + 5$	$11t^3 + 12t$	0

Example

	$\mathcal{B}_1$		$\mathcal{B}_2$		ω
$\iota(1)$	1	0	1	0	0
$\iota(\theta)$	0	t	11	t	0
$\iota(\theta^2)$	$11t^2$	0	$11t^2+4$	$9t$	0
$\iota(\theta^3)$	0	$11t^3$	$12t^2+5$	$11t^3+12t$	0

$$M = \begin{bmatrix} \mathrm{LT}_0(1) \\ \vdots \\ \mathrm{LT}_0(\theta^3) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 11 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 5 & 0 \end{bmatrix} \in \mathbb{F}_{13}^{4\times 4}, \quad \mathrm{rank}(M) = 2 < 4$$

Example

	$\mathcal{B}_1$		$\mathcal{B}_2$		ω
$\iota(1)$	1	0	1	0	0
$\iota(\theta)$	0	t	11	t	0
$\iota(\theta^2)$	$11t^2$	0	$11t^2 + 4$	$9t$	0
$\iota(\theta^3)$	0	$11t^3$	$12t^2 + 5$	$11t^3 + 12t$	0

$$M = \begin{bmatrix} \mathrm{LT}_0(1) \\ \vdots \\ \mathrm{LT}_0(\theta^3) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 11 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 5 & 0 \end{bmatrix} \in \mathbb{F}_{13}^{4\times 4}, \quad \mathrm{rank}(M) = 2 < 4$$

$$\implies \theta^2 - \frac{4}{11}\theta = \theta^2 + 2\theta, \quad \theta^3 - \frac{5}{11}\theta = \theta^3 + 9\theta.$$

Example

	$\mathcal{B}_1$		$\mathcal{B}_2$		ω
$\iota(1)$	1	0	1	0	0
$\iota(\theta)$	0	t	11	t	0
$\iota(\theta^2)$	$11t^2$	0	$11t^2+4$	$9t$	0
$\iota(\theta^3)$	0	$11t^3$	$12t^2+5$	$11t^3+12t$	0

$$M = \begin{bmatrix} \mathrm{LT}_0(1) \\ \vdots \\ \mathrm{LT}_0(\theta^3) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 11 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 5 & 0 \end{bmatrix} \in \mathbb{F}_{13}^{4\times 4}, \quad \mathrm{rank}(M) = 2 < 4$$

$$\Longrightarrow \theta^2 - \frac{4}{11}\theta = \theta^2 + 2\theta, \quad \theta^3 - \frac{5}{11}\theta = \theta^3 + 9\theta.$$

Updated basis: $1, \theta, \theta^2 + 2\theta, \theta^3 + 9\theta$.

Example

	$\mathcal{B}_1$		$\mathcal{B}_2$		ω
$\iota(1)$	1	0	1	0	0
$\iota(\theta)$	0	t	11	t	0
$\iota(\theta^2+2)$	$11t^2$	$2t$	$11t^2$	$11t$	1
$\iota(\theta^3+9\theta)$	0	$11t^3+9t$	$12t^2$	$11t^3+8t$	1

Example

	$\mathcal{B}_1$		$\mathcal{B}_2$		ω
$\iota(1)$	1	0	1	0	0
$\iota(\theta)$	0	t	11	t	0
$\iota(\theta^2+2)$	$11t^2$	$2t$	$11t^2$	$11t$	1
$\iota(\theta^3+9\theta)$	0	$11t^3+9t$	$12t^2$	$11t^3+8t$	1

$$M = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 11 & 0 \\ 0 & 2 & 0 & 11 \\ 0 & 9 & 0 & 8 \end{bmatrix}, \quad \mathrm{rank}(M) = 4$$

$\Longrightarrow (1, \theta, \frac{\theta^2+2\theta}{t}, \frac{\theta^3+9\theta}{t})$ is a triangular $\mathfrak{p}$-integral basis.

Thank you! . . . Questions?

Complexity

Theorem

The algorithm needs at most

$$O\left(n^3\delta + n^2\delta^2 + n^{1+\epsilon}\delta\log q + n^{1+\epsilon}\delta^{2+\epsilon}\right)$$

$\mathfrak{p}$*-small operations. In particular, the runtime after the initialization is equal to* $O(n^2\delta^2)$ $\mathfrak{p}$*-small operations.*

Here $\delta := v_{\mathfrak{p}}(\mathrm{Disc}\, f)$ *and* $q = \#A/\mathfrak{p}$*.)*