On an index of finitely generated $\mathbb{Z}[X]$-modules

Pavel Francírek

Department of Mathematics and Statistics,
Faculty of Science, Masaryk University,
Brno

4 September 2018

Introduction

Introduction

Let $\mathcal{L}$ be a finite lattice.

Introduction

Let $\mathcal{L}$ be a finite lattice. The least element of $\mathcal{L}$ will be denoted by 0.

Introduction

Let $\mathcal{L}$ be a finite lattice. The least element of $\mathcal{L}$ will be denoted by 0. For each $i \in \mathcal{L}$ let $D(i)$ be the lower set generated by i,

Introduction

Let $\mathcal{L}$ be a finite lattice. The least element of $\mathcal{L}$ will be denoted by 0. For each $i \in \mathcal{L}$ let $D(i)$ be the lower set generated by i, i.e.

$$D(i) = \{j \in \mathcal{L}; j \leq i\}.$$

Introduction

Let $\mathcal{L}$ be a finite lattice. The least element of $\mathcal{L}$ will be denoted by 0. For each $i \in \mathcal{L}$ let $D(i)$ be the lower set generated by i, i.e.

$$D(i) = \{j \in \mathcal{L}; j \leq i\}.$$

Suppose that M is a finitely generated $\mathbb{Z}[X]$-module whose generators will be denoted by $\xi_i, i \in \mathcal{L}$.

Introduction

Let $\mathcal{L}$ be a finite lattice. The least element of $\mathcal{L}$ will be denoted by 0. For each $i \in \mathcal{L}$ let $D(i)$ be the lower set generated by i, i.e.

$$D(i) = \{j \in \mathcal{L}; j \leq i\}.$$

Suppose that M is a finitely generated $\mathbb{Z}[X]$-module whose generators will be denoted by $\xi_i, i \in \mathcal{L}$. For each $i \in \mathcal{L}$ let $\varkappa_i$ be an element of M given by

$$\varkappa_i = H_i \cdot \xi_i$$

for some $H_i \in \mathbb{Z}[X]$.

Introduction

Let $\mathcal{L}$ be a finite lattice. The least element of $\mathcal{L}$ will be denoted by 0. For each $i \in \mathcal{L}$ let $D(i)$ be the lower set generated by i, i.e.

$$D(i) = \{j \in \mathcal{L}; j \leq i\}.$$

Suppose that M is a finitely generated $\mathbb{Z}[X]$-module whose generators will be denoted by $\xi_i, i \in \mathcal{L}$. For each $i \in \mathcal{L}$ let $\varkappa_i$ be an element of M given by

$$\varkappa_i = H_i \cdot \xi_i$$

for some $H_i \in \mathbb{Z}[X]$. By N we shall denote the submodule of M generated by all the elements $\varkappa_i$.

For each lower set $D \subseteq \mathcal{L}$ we define the following submodules:

For each lower set $D \subseteq \mathcal{L}$ we define the following submodules:
Let M_D be the submodule of M generated by ξ_i for all $i \in D$.

For each lower set $D \subseteq \mathcal{L}$ we define the following submodules:
Let M_D be the submodule of M generated by ξ_i for all $i \in D$. Let N_D be the submodule of N generated by $\varkappa_i$ for all $i \in D$.

For each lower set $D \subseteq \mathcal{L}$ we define the following submodules:
Let M_D be the submodule of M generated by ξ_i for all $i \in D$. Let N_D be the submodule of N generated by $\varkappa_i$ for all $i \in D$. We further assume that the elements ξ_i and $\varkappa_i$ satisfy the following relations:

For each lower set $D \subseteq \mathcal{L}$ we define the following submodules:
Let M_D be the submodule of M generated by ξ_i for all $i \in D$. Let N_D be the submodule of N generated by $\varkappa_i$ for all $i \in D$. We further assume that the elements ξ_i and $\varkappa_i$ satisfy the following relations:
For each $i \in \mathcal{L}$ there is a polynomial $F_i \in \mathbb{Z}[X]$ such that

$$F_i \cdot \varkappa_i \in N_{D(i)\setminus\{i\}} \qquad \text{and} \qquad F_i \cdot \xi_i \in M_{D(i)\setminus\{i\}}.$$

For each lower set $D \subseteq \mathcal{L}$ we define the following submodules:
Let M_D be the submodule of M generated by ξ_i for all $i \in D$. Let N_D be the submodule of N generated by $\varkappa_i$ for all $i \in D$. We further assume that the elements ξ_i and $\varkappa_i$ satisfy the following relations:
For each $i \in \mathcal{L}$ there is a polynomial $F_i \in \mathbb{Z}[X]$ such that

$$F_i \cdot \varkappa_i \in N_{D(i)\setminus\{i\}} \qquad \text{and} \qquad F_i \cdot \xi_i \in M_{D(i)\setminus\{i\}}.$$

Theorem

Suppose that all the polynomials F_i are monic. We shall further assume that for each $i \in \mathcal{L}$ we have

$$\operatorname{rank}_{\mathbb{Z}} M_{D(i)} = \operatorname{rank}_{\mathbb{Z}} M_{D(i)\setminus\{i\}} + \deg F_i,$$
$$\operatorname{rank}_{\mathbb{Z}} N_{D(i)} = \operatorname{rank}_{\mathbb{Z}} N_{D(i)\setminus\{i\}} + \deg F_i.$$

It follows that $\operatorname{rank}_{\mathbb{Z}} M = \operatorname{rank}_{\mathbb{Z}} N$ and

$$[M\colon N] = \prod_{i\in\mathcal{L}} \left|\mathbb{Z}[X]/\left(F_i, H_i\right)\right| = \prod_{i\in\mathcal{L}} \left|\operatorname{Res}\left(F_i, H_i\right)\right|.$$

Auxilliary result

Proposition

Let $F, G \in \mathbb{Z}[X]$ be polynomials which have no common root in $\mathbb{C}$ and suppose that F is monic. Then we have

$$\left|\mathbb{Z}[X]/(F,G)\right| = \left|\mathrm{Res}\,(F,G)\right|.$$

Auxilliary result

Proposition

Let $F, G \in \mathbb{Z}[X]$ be polynomials which have no common root in $\mathbb{C}$ and suppose that F is monic. Then we have

$$\left|\mathbb{Z}[X]/(F,G)\right| = \left|\mathrm{Res}\,(F,G)\right|.$$

Proof:

Auxilliary result

Proposition

Let $F, G \in \mathbb{Z}[X]$ be polynomials which have no common root in $\mathbb{C}$ and suppose that F is monic. Then we have

$$\left|\mathbb{Z}[X]/(F,G)\right| = \left|\mathrm{Res}\,(F,G)\right|.$$

Proof: At first, let us suppose that G is also monic, so we can write

$$F(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + a_n$$

and

$$G(X) = X^m + b_1 X^{m-1} + \cdots + b_{m-1}X + b_m,$$

where a_i and b_i are integers.

Auxilliary result

Proposition

Let $F, G \in \mathbb{Z}[X]$ be polynomials which have no common root in $\mathbb{C}$ and suppose that F is monic. Then we have

$$\left|\mathbb{Z}[X]/(F,G)\right| = \left|\mathrm{Res}\,(F,G)\right|.$$

Proof: At first, let us suppose that G is also monic, so we can write

$$F(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + a_n$$

and

$$G(X) = X^m + b_1 X^{m-1} + \cdots + b_{m-1}X + b_m,$$

where a_i and b_i are integers. Then we have

$$\mathbb{Z}[X]/(F,G) \cong \mathbb{Z}[X]/(F\cdot G) \Big/ (F,G)/(F\cdot G).$$

Auxilliary result

Proposition

Let $F, G \in \mathbb{Z}[X]$ be polynomials which have no common root in $\mathbb{C}$ and suppose that F is monic. Then we have

$$\left|\mathbb{Z}[X]/(F,G)\right| = \left|\mathrm{Res}\,(F,G)\right|.$$

Proof: At first, let us suppose that G is also monic, so we can write

$$F(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + a_n$$

and

$$G(X) = X^m + b_1 X^{m-1} + \cdots + b_{m-1}X + b_m,$$

where a_i and b_i are integers. Then we have

$$\mathbb{Z}[X]/(F,G) \cong \mathbb{Z}[X]/(F\cdot G)\Big/(F,G)/(F\cdot G).$$

Let $\overline{X}$ be the class of $\mathbb{Z}[X]/(F\cdot G)$ containing X.

Auxilliary result

Proposition

Let $F, G \in \mathbb{Z}[X]$ be polynomials which have no common root in $\mathbb{C}$ and suppose that F is monic. Then we have

$$\left|\mathbb{Z}[X]/(F,G)\right| = \left|\mathrm{Res}\,(F,G)\right|.$$

Proof: At first, let us suppose that G is also monic, so we can write

$$F(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + a_n$$

and

$$G(X) = X^m + b_1 X^{m-1} + \cdots + b_{m-1}X + b_m,$$

where a_i and b_i are integers. Then we have

$$\mathbb{Z}[X]/(F,G) \cong \mathbb{Z}[X]/(F\cdot G)\Big/(F,G)/(F\cdot G).$$

Let $\overline{X}$ be the class of $\mathbb{Z}[X]/(F\cdot G)$ containing X. Clearly $\mathbb{Z}[X]/(F\cdot G)$ is a free $\mathbb{Z}$-module with a basis $1, \overline{X}, \ldots, \overline{X}^{n+m-1}$.

Every element of the ideal (F, G) can be uniquely expressed in the form

$$u \cdot F + v \cdot G + w \cdot F \cdot G$$

with $u, v, w \in \mathbb{Z}[X]$ satisfying $\deg u < \deg G$ and $\deg v < \deg F$.

Every element of the ideal (F, G) can be uniquely expressed in the form

$$u \cdot F + v \cdot G + w \cdot F \cdot G$$

with $u, v, w \in \mathbb{Z}[X]$ satisfying $\deg u < \deg G$ and $\deg v < \deg F$. Hence

$$F(\overline{X}), \overline{X}F(\overline{X}), \ldots, \overline{X}^{n-1}F(\overline{X}), G(\overline{X}), \overline{X}G(\overline{X}), \ldots, \overline{X}^{m-1}G(\overline{X})$$

is a $\mathbb{Z}$-basis for $(F, G)/(F \cdot G)$.

Every element of the ideal (F, G) can be uniquely expressed in the form

$$u \cdot F + v \cdot G + w \cdot F \cdot G$$

with $u, v, w \in \mathbb{Z}[X]$ satisfying $\deg u < \deg G$ and $\deg v < \deg F$. Hence

$$F(\overline{X}), \overline{X}F(\overline{X}), \ldots, \overline{X}^{n-1}F(\overline{X}), G(\overline{X}), \overline{X}G(\overline{X}), \ldots, \overline{X}^{m-1}G(\overline{X})$$

is a $\mathbb{Z}$-basis for $(F, G)/(F \cdot G)$. Thus the index $[\mathbb{Z}[X]/(F \cdot G) : (F, G)/(F \cdot G)]$ is finite and it is equal to the absolute value of the following determinant

Every element of the ideal (F, G) can be uniquely expressed in the form

$$u \cdot F + v \cdot G + w \cdot F \cdot G$$

with $u, v, w \in \mathbb{Z}[X]$ satisfying $\deg u < \deg G$ and $\deg v < \deg F$. Hence

$$F(\overline{X}), \overline{X}F(\overline{X}), \ldots, \overline{X}^{n-1}F(\overline{X}), G(\overline{X}), \overline{X}G(\overline{X}), \ldots, \overline{X}^{m-1}G(\overline{X})$$

is a $\mathbb{Z}$-basis for $(F, G)/(F \cdot G)$. Thus the index $[\mathbb{Z}[X]/(F \cdot G) : (F, G)/(F \cdot G)]$ is finite and it is equal to the absolute value of the following determinant

$$\begin{vmatrix}
1 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\
a_1 & 1 & \cdots & 0 & b_1 & 1 & \cdots & 0 \\
a_2 & a_1 & \ddots & 0 & b_2 & b_1 & \ddots & 0 \\
\vdots & \vdots & \ddots & 1 & \vdots & \vdots & \ddots & 1 \\
a_n & a_{n-1} & \cdots & \vdots & b_m & b_{m-1} & \cdots & \vdots \\
0 & a_n & \ddots & \vdots & 0 & b_m & \ddots & \vdots \\
\vdots & \vdots & \ddots & a_{n-1} & \vdots & \vdots & \ddots & b_{m-1} \\
0 & 0 & \cdots & a_n & 0 & 0 & \cdots & b_m
\end{vmatrix}$$

Every element of the ideal (F, G) can be uniquely expressed in the form

$$u \cdot F + v \cdot G + w \cdot F \cdot G$$

with $u, v, w \in \mathbb{Z}[X]$ satisfying $\deg u < \deg G$ and $\deg v < \deg F$. Hence

$$F(\overline{X}), \overline{X}F(\overline{X}), \ldots, \overline{X}^{n-1}F(\overline{X}), G(\overline{X}), \overline{X}G(\overline{X}), \ldots, \overline{X}^{m-1}G(\overline{X})$$

is a $\mathbb{Z}$-basis for $(F, G)/(F \cdot G)$. Thus the index $[\mathbb{Z}[X]/(F \cdot G) : (F, G)/(F \cdot G)]$ is finite and it is equal to the absolute value of the following determinant

$$\begin{vmatrix}
1 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\
a_1 & 1 & \cdots & 0 & b_1 & 1 & \cdots & 0 \\
a_2 & a_1 & \ddots & 0 & b_2 & b_1 & \ddots & 0 \\
\vdots & \vdots & \ddots & 1 & \vdots & \vdots & \ddots & 1 \\
a_n & a_{n-1} & \cdots & \vdots & b_m & b_{m-1} & \cdots & \vdots \\
0 & a_n & \ddots & \vdots & 0 & b_m & \ddots & \vdots \\
\vdots & \vdots & \ddots & a_{n-1} & \vdots & \vdots & \ddots & b_{m-1} \\
0 & 0 & \cdots & a_n & 0 & 0 & \cdots & b_m
\end{vmatrix} = \operatorname{Res}(F, G).$$

We shall suppose now that G is not monic.

We shall suppose now that G is not monic. We take the following polynomial

$$H = X^{\deg G+1} \cdot F + G \in \mathbb{Z}[X].$$

Clearly H is monic and we have $(F, G) = (F, H)$.

We shall suppose now that G is not monic. We take the following polynomial

$$H = X^{\deg G+1} \cdot F + G \in \mathbb{Z}[X].$$

Clearly H is monic and we have $(F, G) = (F, H)$. Therefore it only remains to show the equality of resultants $\mathrm{Res}\,(F, G) = \mathrm{Res}\,(F, H)$.

We shall suppose now that G is not monic. We take the following polynomial

$$H = X^{\deg G+1} \cdot F + G \in \mathbb{Z}[X].$$

Clearly H is monic and we have $(F, G) = (F, H)$. Therefore it only remains to show the equality of resultants $\mathrm{Res}\,(F, G) = \mathrm{Res}\,(F, H)$. Let $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ be all the roots of F.

We shall suppose now that G is not monic. We take the following polynomial

$$H = X^{\deg G+1} \cdot F + G \in \mathbb{Z}[X].$$

Clearly H is monic and we have $(F, G) = (F, H)$. Therefore it only remains to show the equality of resultants $\mathrm{Res}\,(F, G) = \mathrm{Res}\,(F, H)$. Let $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ be all the roots of F. Then we have

$$\mathrm{Res}\,(F, H) = \prod_{i=1}^{n} H(\alpha_i) = \prod_{i=1}^{n} \big(\underbrace{\alpha_i^{m+1} F(\alpha_i)}_{0} + G(\alpha_i)\big) = \mathrm{Res}\,(F, G)$$

and the proposition follows.

We shall suppose now that G is not monic. We take the following polynomial

$$H = X^{\deg G+1} \cdot F + G \in \mathbb{Z}[X].$$

Clearly H is monic and we have $(F, G) = (F, H)$. Therefore it only remains to show the equality of resultants $\mathrm{Res}\,(F, G) = \mathrm{Res}\,(F, H)$. Let $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ be all the roots of F. Then we have

$$\mathrm{Res}\,(F, H) = \prod_{i=1}^{n} H(\alpha_i) = \prod_{i=1}^{n} \big(\underbrace{\alpha_i^{m+1} F(\alpha_i)}_{0} + G(\alpha_i)\big) = \mathrm{Res}\,(F, G)$$

and the proposition follows.

Proposition

Let $m, n, m < n$ be positive integers. Then we have

$$|\mathrm{Res}\,(\Phi_n, \Phi_m)| = \begin{cases} p^{\varphi(m)} & \text{if } \frac{n}{m} = p^k \text{ for some prime } p, \\ 1 & \text{otherwise.} \end{cases}$$

Proof of the main theorem

We shall prove using induction with respect to the size of D that $\operatorname{rank}_{\mathbb{Z}} M_D = \operatorname{rank}_{\mathbb{Z}} N_D$ and that

$$[M_D : N_D] = \prod_{i \in D} \left| \mathbb{Z}[X] / \left(F_i, H_i \right) \right|.$$

Proof of the main theorem

We shall prove using induction with respect to the size of D that $\operatorname{rank}_{\mathbb{Z}} M_D = \operatorname{rank}_{\mathbb{Z}} N_D$ and that

$$[M_D : N_D] = \prod_{i \in D} \left| \mathbb{Z}[X] / \left(F_i, H_i \right) \right|.$$

Suppose $D = \{0\}$.

Proof of the main theorem

We shall prove using induction with respect to the size of D that $\operatorname{rank}_{\mathbb{Z}} M_D = \operatorname{rank}_{\mathbb{Z}} N_D$ and that

$$[M_D : N_D] = \prod_{i \in D} \left| \mathbb{Z}[X] / \left(F_i, H_i \right) \right|.$$

Suppose $D = \{0\}$. Obviously $\operatorname{rank}_{\mathbb{Z}} M_D = \operatorname{rank}_{\mathbb{Z}} N_D = \deg F_0$.

Proof of the main theorem

We shall prove using induction with respect to the size of D that $\operatorname{rank}_{\mathbb{Z}} M_D = \operatorname{rank}_{\mathbb{Z}} N_D$ and that

$$[M_D : N_D] = \prod_{i \in D} \left| \mathbb{Z}[X]/(F_i, H_i) \right|.$$

Suppose $D = \{0\}$. Obviously $\operatorname{rank}_{\mathbb{Z}} M_D = \operatorname{rank}_{\mathbb{Z}} N_D = \deg F_0$. The map $\mathbb{Z}[X]/(F_0) \to M_D$ given by

$$[f] \mapsto f \cdot \xi_0$$

is a surjective homomorphism of $\mathbb{Z}[X]$-modules.

Proof of the main theorem

We shall prove using induction with respect to the size of D that $\operatorname{rank}_{\mathbb{Z}} M_D = \operatorname{rank}_{\mathbb{Z}} N_D$ and that

$$[M_D : N_D] = \prod_{i \in D} \left| \mathbb{Z}[X]/(F_i, H_i) \right|.$$

Suppose $D = \{0\}$. Obviously $\operatorname{rank}_{\mathbb{Z}} M_D = \operatorname{rank}_{\mathbb{Z}} N_D = \deg F_0$. The map $\mathbb{Z}[X]/(F_0) \to M_D$ given by

$$[f] \mapsto f \cdot \xi_0$$

is a surjective homomorphism of $\mathbb{Z}[X]$-modules. Since they have the same $\mathbb{Z}$-rank and $\mathbb{Z}[X]/(F_0)$ is a free $\mathbb{Z}$-module, it is an isomorphism.

Proof of the main theorem

We shall prove using induction with respect to the size of D that $\operatorname{rank}_{\mathbb{Z}} M_D = \operatorname{rank}_{\mathbb{Z}} N_D$ and that

$$[M_D : N_D] = \prod_{i \in D} \left| \mathbb{Z}[X]/(F_i, H_i) \right|.$$

Suppose $D = \{0\}$. Obviously $\operatorname{rank}_{\mathbb{Z}} M_D = \operatorname{rank}_{\mathbb{Z}} N_D = \deg F_0$. The map $\mathbb{Z}[X]/(F_0) \to M_D$ given by

$$[f] \mapsto f \cdot \xi_0$$

is a surjective homomorphism of $\mathbb{Z}[X]$-modules. Since they have the same $\mathbb{Z}$-rank and $\mathbb{Z}[X]/(F_0)$ is a free $\mathbb{Z}$-module, it is an isomorphism. The preimage of N_D in this isomorphism is the ideal $([H_0])$.

Proof of the main theorem

We shall prove using induction with respect to the size of D that $\operatorname{rank}_{\mathbb{Z}} M_D = \operatorname{rank}_{\mathbb{Z}} N_D$ and that

$$[M_D : N_D] = \prod_{i \in D} \left| \mathbb{Z}[X]/(F_i, H_i) \right|.$$

Suppose $D = \{0\}$. Obviously $\operatorname{rank}_{\mathbb{Z}} M_D = \operatorname{rank}_{\mathbb{Z}} N_D = \deg F_0$. The map $\mathbb{Z}[X]/(F_0) \to M_D$ given by

$$[f] \mapsto f \cdot \xi_0$$

is a surjective homomorphism of $\mathbb{Z}[X]$-modules. Since they have the same $\mathbb{Z}$-rank and $\mathbb{Z}[X]/(F_0)$ is a free $\mathbb{Z}$-module, it is an isomorphism. The preimage of N_D in this isomorphism is the ideal $([H_0])$. Therefore the quotient M_D/N_D is isomorphic to

$$\mathbb{Z}[X]/(F_0) \Big/ ([H_0]),$$

which is isomorphic to

$$\mathbb{Z}[X]/(F_0, H_0).$$

Now suppose $|D| \geq 2$.

Now suppose $|D| \geq 2$. Let m be a maximal element of D.

Now suppose $|D| \geq 2$. Let m be a maximal element of D. The lower set $D \setminus \{m\}$ will be denoted by D'.

Now suppose $|D| \geq 2$. Let m be a maximal element of D. The lower set $D \setminus \{m\}$ will be denoted by D'. Let T_D be the $\mathbb{Z}[X]$-module generated by $M_{D'}$ and $\varkappa_m$.

Now suppose $|D| \geq 2$. Let m be a maximal element of D. The lower set $D \setminus \{m\}$ will be denoted by D'. Let T_D be the $\mathbb{Z}[X]$-module generated by $M_{D'}$ and $\varkappa_m$. We have

$$[M_D : N_D] = [M_D : T_D] \cdot [T_D : N_D].$$

Now suppose $|D| \geq 2$. Let m be a maximal element of D. The lower set $D \setminus \{m\}$ will be denoted by D'. Let T_D be the $\mathbb{Z}[X]$-module generated by $M_{D'}$ and $\varkappa_m$. We have

$$[M_D : N_D] = [M_D : T_D] \cdot [T_D : N_D].$$

From the induction hypothesis we derive that the modules M_D, N_D and T_D have the same $\mathbb{Z}$-rank.

Now suppose $|D| \geq 2$. Let m be a maximal element of D. The lower set $D \setminus \{m\}$ will be denoted by D'. Let T_D be the $\mathbb{Z}[X]$-module generated by $M_{D'}$ and $\varkappa_m$. We have

$$[M_D : N_D] = [M_D : T_D] \cdot [T_D : N_D].$$

From the induction hypothesis we derive that the modules M_D, N_D and T_D have the same $\mathbb{Z}$-rank. Moreover, the $\mathbb{Z}$-bases of T_D and of N_D can be obtained by adding $\{X^i \cdot \varkappa_m; 0 \leq i < \deg F_m\}$ to $\mathbb{Z}$-bases of $M_{D'}$ and of $N_{D'}$, respectively.

Now suppose $|D| \geq 2$. Let m be a maximal element of D. The lower set $D \setminus \{m\}$ will be denoted by D'. Let T_D be the $\mathbb{Z}[X]$-module generated by $M_{D'}$ and $\varkappa_m$. We have

$$[M_D : N_D] = [M_D : T_D] \cdot [T_D : N_D].$$

From the induction hypothesis we derive that the modules M_D, N_D and T_D have the same $\mathbb{Z}$-rank. Moreover, the $\mathbb{Z}$-bases of T_D and of N_D can be obtained by adding $\{X^i \cdot \varkappa_m; 0 \leq i < \deg F_m\}$ to $\mathbb{Z}$-bases of $M_{D'}$ and of $N_{D'}$, respectively. Hence, using the determinants of transition matrices we get

$$[T_D : N_D] = [M_{D'} : N_{D'}].$$

The map $\mathbb{Z}[X]/(F_m) \to M_D/M_{D'}$ given by

$$[f] \mapsto f \cdot [\xi_m]$$

is a surjective homomorphism of $\mathbb{Z}[X]$-modules.

The map $\mathbb{Z}[X]/(F_m) \to M_D/M_{D'}$ given by

$$[f] \mapsto f \cdot [\xi_m]$$

is a surjective homomorphism of $\mathbb{Z}[X]$-modules. Since they have the same $\mathbb{Z}$-rank and $\mathbb{Z}[X]/(F_m)$ is a free $\mathbb{Z}$-module, it is an isomorphism.

The map $\mathbb{Z}[X]/(F_m) \to M_D/M_{D'}$ given by

$$[f] \mapsto f \cdot [\xi_m]$$

is a surjective homomorphism of $\mathbb{Z}[X]$-modules. Since they have the same $\mathbb{Z}$-rank and $\mathbb{Z}[X]/(F_m)$ is a free $\mathbb{Z}$-module, it is an isomorphism. The preimage of $T_D/M_{D'}$ in this isomorphism is the ideal $([H_m])$.

The map $\mathbb{Z}[X]/(F_m) \to M_D/M_{D'}$ given by

$$[f] \mapsto f \cdot [\xi_m]$$

is a surjective homomorphism of $\mathbb{Z}[X]$-modules. Since they have the same $\mathbb{Z}$-rank and $\mathbb{Z}[X]/(F_m)$ is a free $\mathbb{Z}$-module, it is an isomorphism. The preimage of $T_D/M_{D'}$ in this isomorphism is the ideal $([H_m])$. Therefore we have

$$M_D/T_D \cong M_D/M_{D'} \Big/ T_D/M_{D'} \cong \mathbb{Z}[X]/(F_m) \Big/ ([H_m]),$$

The map $\mathbb{Z}[X]/(F_m) \to M_D/M_{D'}$ given by

$$[f] \mapsto f \cdot [\xi_m]$$

is a surjective homomorphism of $\mathbb{Z}[X]$-modules. Since they have the same $\mathbb{Z}$-rank and $\mathbb{Z}[X]/(F_m)$ is a free $\mathbb{Z}$-module, it is an isomorphism. The preimage of $T_D/M_{D'}$ in this isomorphism is the ideal $([H_m])$. Therefore we have

$$M_D/T_D \cong M_D/M_{D'} \Big/ T_D/M_{D'} \cong \mathbb{Z}[X]/(F_m) \Big/ ([H_m]),$$

which is isomorphic to

$$\mathbb{Z}[X]/(F_m, H_m).$$

The map $\mathbb{Z}[X]/(F_m) \to M_D/M_{D'}$ given by

$$[f] \mapsto f \cdot [\xi_m]$$

is a surjective homomorphism of $\mathbb{Z}[X]$-modules. Since they have the same $\mathbb{Z}$-rank and $\mathbb{Z}[X]/(F_m)$ is a free $\mathbb{Z}$-module, it is an isomorphism. The preimage of $T_D/M_{D'}$ in this isomorphism is the ideal $([H_m])$. Therefore we have

$$M_D/T_D \cong M_D/M_{D'} \Big/ T_D/M_{D'} \cong \mathbb{Z}[X]/(F_m) \Big/ ([H_m]),$$

which is isomorphic to

$$\mathbb{Z}[X]/(F_m, H_m).$$

The induction hypothesis gives

$$\begin{aligned}[M_D : N_D] &= [M_D : T_D] \cdot [T_D : N_D] = \\ &= |\mathbb{Z}[X]/(F_m, H_m)| \cdot [M_{D'} : N_{D'}] = \\ &= |\mathbb{Z}[X]/(F_m, H_m)| \cdot \prod_{i \in D'} |\mathbb{Z}[X]/(F_i, H_i)|.\end{aligned}$$

It remains to show that the polynomials F_i and H_i have no common root for each $i \in D$.

It remains to show that the polynomials F_i and H_i have no common root for each $i \in D$. Suppose that for some $i \in D$ the polynomials F_i and H_i have a common root in $\mathbb{C}$.

It remains to show that the polynomials F_i and H_i have no common root for each $i \in D$. Suppose that for some $i \in D$ the polynomials F_i and H_i have a common root in $\mathbb{C}$. Let us denote $P \in \mathbb{Z}[X]$ their greatest common divisor, so we can write

$$F_i = PF_i' \qquad \text{and} \qquad H_i = PH_i'$$

for suitable polynomials $F_i', H_i' \in \mathbb{Z}[X]$.

It remains to show that the polynomials F_i and H_i have no common root for each $i \in D$. Suppose that for some $i \in D$ the polynomials F_i and H_i have a common root in $\mathbb{C}$. Let us denote $P \in \mathbb{Z}[X]$ their greatest common divisor, so we can write

$$F_i = PF_i' \qquad \text{and} \qquad H_i = PH_i'$$

for suitable polynomials $F_i', H_i' \in \mathbb{Z}[X]$. It follows that the polynomials P and F_i' are monic.

It remains to show that the polynomials F_i and H_i have no common root for each $i \in D$. Suppose that for some $i \in D$ the polynomials F_i and H_i have a common root in $\mathbb{C}$. Let us denote $P \in \mathbb{Z}[X]$ their greatest common divisor, so we can write

$$F_i = PF_i' \qquad \text{and} \qquad H_i = PH_i'$$

for suitable polynomials $F_i', H_i' \in \mathbb{Z}[X]$. It follows that the polynomials P and F_i' are monic. The lower set $D(i) \setminus \{i\}$ will be denoted by D'. As before, we shall denote the $\mathbb{Z}[X]$-module generated by $M_{D'}$ and $\varkappa_i$ by $T_{D(i)}$.

It remains to show that the polynomials F_i and H_i have no common root for each $i \in D$. Suppose that for some $i \in D$ the polynomials F_i and H_i have a common root in $\mathbb{C}$. Let us denote $P \in \mathbb{Z}[X]$ their greatest common divisor, so we can write

$$F_i = PF_i' \qquad \text{and} \qquad H_i = PH_i'$$

for suitable polynomials $F_i', H_i' \in \mathbb{Z}[X]$. It follows that the polynomials P and F_i' are monic. The lower set $D(i) \setminus \{i\}$ will be denoted by D'. As before, we shall denote the $\mathbb{Z}[X]$-module generated by $M_{D'}$ and $\varkappa_i$ by $T_{D(i)}$. Now we have

$$F_i' \cdot \varkappa_i = F_i' \cdot (H_i \cdot \xi_i) = PF_i'H_i' \cdot \xi_i = H_i'F_i \cdot \xi_i \in M_{D'}.$$

It remains to show that the polynomials F_i and H_i have no common root for each $i \in D$. Suppose that for some $i \in D$ the polynomials F_i and H_i have a common root in $\mathbb{C}$. Let us denote $P \in \mathbb{Z}[X]$ their greatest common divisor, so we can write

$$F_i = PF_i' \qquad \text{and} \qquad H_i = PH_i'$$

for suitable polynomials $F_i', H_i' \in \mathbb{Z}[X]$. It follows that the polynomials P and F_i' are monic. The lower set $D(i) \setminus \{i\}$ will be denoted by D'. As before, we shall denote the $\mathbb{Z}[X]$-module generated by $M_{D'}$ and $\varkappa_i$ by $T_{D(i)}$. Now we have

$$F_i' \cdot \varkappa_i = F_i' \cdot (H_i \cdot \xi_i) = PF_i'H_i' \cdot \xi_i = H_i'F_i \cdot \xi_i \in M_{D'}.$$

Hence

$$\begin{aligned} \operatorname{rank}_{\mathbb{Z}} T_{D(i)} &\leq \operatorname{rank}_{\mathbb{Z}} M_{D'} + \deg F_i' < \\ &< \operatorname{rank}_{\mathbb{Z}} M_{D'} + \deg F_i = \operatorname{rank}_{\mathbb{Z}} M_{D(i)}, \end{aligned}$$

which is not possible.

Application

Application

Notation:

Application

Notation:

$\ell =$ an odd prime number,

Application

Notation:

$\ell =$ an odd prime number,

$K =$ a real cyclic field of ℓ-power degree $[K : \mathbb{Q}] = \ell^k$,

Application

Notation:

$\ell =$ an odd prime number,
$K =$ a real cyclic field of ℓ-power degree $[K : \mathbb{Q}] = \ell^k$,
$F =$ a quadratic imaginary field,

Application

Notation:

$\ell =$ an odd prime number,
$K =$ a real cyclic field of ℓ-power degree $[K : \mathbb{Q}] = \ell^k$,
$F =$ a quadratic imaginary field,
$L = KF$ and $\mathrm{Gal}\,(L/\mathbb{Q}) = \langle \gamma \rangle$,

Application

Notation:

$\ell =$ an odd prime number,
$K =$ a real cyclic field of ℓ-power degree $[K : \mathbb{Q}] = \ell^k$,
$F =$ a quadratic imaginary field,
$L = KF$ and $\mathrm{Gal}\,(L/\mathbb{Q}) = \langle \gamma \rangle$,
$L^{(i)} =$ the unique subfield of L of degree $[L^{(i)} : \mathbb{Q}] = 2\ell^i$,

Application

Notation:

$\ell =$ an odd prime number,
$K =$ a real cyclic field of ℓ-power degree $[K : \mathbb{Q}] = \ell^k$,
$F =$ a quadratic imaginary field,
$L = KF$ and $\mathrm{Gal}\,(L/\mathbb{Q}) = \langle \gamma \rangle$,
$L^{(i)} =$ the unique subfield of L of degree $[L^{(i)} : \mathbb{Q}] = 2\ell^i$,
$n_i =$ the conductor of $L^{(i)}$,

Application

Notation:

$\ell =$ an odd prime number,
$K =$ a real cyclic field of ℓ-power degree $[K : \mathbb{Q}] = \ell^k$,
$F =$ a quadratic imaginary field,
$L = KF$ and $\mathrm{Gal}\,(L/\mathbb{Q}) = \langle \gamma \rangle$,
$L^{(i)} =$ the unique subfield of L of degree $[L^{(i)} : \mathbb{Q}] = 2\ell^i$,
$n_i =$ the conductor of $L^{(i)}$,
$s_i =$ the number of primes ramified in $L^{(i)}$ that split completely in F.

Application

Notation:

$\ell =$ an odd prime number,
$K =$ a real cyclic field of ℓ-power degree $[K : \mathbb{Q}] = \ell^k$,
$F =$ a quadratic imaginary field,
$L = KF$ and $\mathrm{Gal}\,(L/\mathbb{Q}) = \langle\gamma\rangle$,
$L^{(i)} =$ the unique subfield of L of degree $[L^{(i)} : \mathbb{Q}] = 2\ell^i$,
$n_i =$ the conductor of $L^{(i)}$,
$s_i =$ the number of primes ramified in $L^{(i)}$ that split completely in F.
The ideal class group $\mathcal{C}\ell(L)$ forms a $\mathbb{Z}[\langle\gamma\rangle]$-module.

Application

Notation:

$\ell =$ an odd prime number,
$K =$ a real cyclic field of ℓ-power degree $[K : \mathbb{Q}] = \ell^k$,
$F =$ a quadratic imaginary field,
$L = KF$ and $\mathrm{Gal}\,(L/\mathbb{Q}) = \langle\gamma\rangle$,
$L^{(i)} =$ the unique subfield of L of degree $[L^{(i)} : \mathbb{Q}] = 2\ell^i$,
$n_i =$ the conductor of $L^{(i)}$,
$s_i =$ the number of primes ramified in $L^{(i)}$ that split completely in F.
The ideal class group $\mathcal{C}\ell(L)$ forms a $\mathbb{Z}[\langle\gamma\rangle]$-module. We want to study annihilators of its ℓ-Sylow subgroup $\mathcal{C}\ell(L)_\ell$.

Application

Notation:

$\ell =$ an odd prime number,
$K =$ a real cyclic field of ℓ-power degree $[K : \mathbb{Q}] = \ell^k$,
$F =$ a quadratic imaginary field,
$L = KF$ and $\mathrm{Gal}\,(L/\mathbb{Q}) = \langle\gamma\rangle$,
$L^{(i)} =$ the unique subfield of L of degree $[L^{(i)} : \mathbb{Q}] = 2\ell^i$,
$n_i =$ the conductor of $L^{(i)}$,
$s_i =$ the number of primes ramified in $L^{(i)}$ that split completely in F.
The ideal class group $\mathcal{C}\ell(L)$ forms a $\mathbb{Z}[\langle\gamma\rangle]$-module. We want to study annihilators of its ℓ-Sylow subgroup $\mathcal{C}\ell(L)_\ell$.
For each $i = 0, 1, \ldots, k$ we define

$$\varkappa_i = \mathrm{cor}_{L/L^{(i)}} \mathrm{res}_{\mathbb{Q}(\zeta_{n_i})/L} n_i(1-\tau)\theta_{n_i} \in \mathbb{Z}[\langle\gamma\rangle],$$

Application

Notation:

$\ell =$ an odd prime number,
$K =$ a real cyclic field of ℓ-power degree $[K : \mathbb{Q}] = \ell^k$,
$F =$ a quadratic imaginary field,
$L = KF$ and $\mathrm{Gal}\,(L/\mathbb{Q}) = \langle\gamma\rangle$,
$L^{(i)} =$ the unique subfield of L of degree $[L^{(i)} : \mathbb{Q}] = 2\ell^i$,
$n_i =$ the conductor of $L^{(i)}$,
$s_i =$ the number of primes ramified in $L^{(i)}$ that split completely in F.
The ideal class group $\mathcal{C}\ell(L)$ forms a $\mathbb{Z}[\langle\gamma\rangle]$-module. We want to study annihilators of its ℓ-Sylow subgroup $\mathcal{C}\ell(L)_\ell$.
For each $i = 0, 1, \ldots, k$ we define

$$\varkappa_i = \mathrm{cor}_{L/L^{(i)}} \mathrm{res}_{\mathbb{Q}(\zeta_{n_i})/L} n_i(1-\tau)\theta_{n_i} \in \mathbb{Z}[\langle\gamma\rangle],$$

where τ denotes the complex conjugation and θ_m is the Stickelberger element for the field $\mathbb{Q}(\zeta_m)$.

Application

Notation:

$\ell =$ an odd prime number,
$K =$ a real cyclic field of ℓ-power degree $[K : \mathbb{Q}] = \ell^k$,
$F =$ a quadratic imaginary field,
$L = KF$ and $\mathrm{Gal}\,(L/\mathbb{Q}) = \langle\gamma\rangle$,
$L^{(i)} =$ the unique subfield of L of degree $[L^{(i)} : \mathbb{Q}] = 2\ell^i$,
$n_i =$ the conductor of $L^{(i)}$,
$s_i =$ the number of primes ramified in $L^{(i)}$ that split completely in F.
The ideal class group $\mathcal{C}\ell(L)$ forms a $\mathbb{Z}[\langle\gamma\rangle]$-module. We want to study annihilators of its ℓ-Sylow subgroup $\mathcal{C}\ell(L)_\ell$.
For each $i = 0, 1, \ldots, k$ we define

$$\varkappa_i = \mathrm{cor}_{L/L^{(i)}} \mathrm{res}_{\mathbb{Q}(\zeta_{n_i})/L} n_i(1-\tau)\theta_{n_i} \in \mathbb{Z}[\langle\gamma\rangle],$$

where τ denotes the complex conjugation and θ_m is the Stickelberger element for the field $\mathbb{Q}(\zeta_m)$. Let N be the ideal of $\mathbb{Z}[\langle\gamma\rangle]$ generated by all the $\varkappa_i$.

For each $i = 0, 1, \ldots, k$ we can explicitly construct $\xi_i \in \mathbb{Z}[\langle\gamma\rangle]$ such that

$$\varkappa_i = H_i(\gamma)\xi_i,$$

For each $i = 0, 1, \ldots, k$ we can explicitly construct $\xi_i \in \mathbb{Z}[\langle\gamma\rangle]$ such that

$$\varkappa_i = H_i(\gamma)\xi_i,$$

where

$$H_i(X) = \begin{cases} (X+1)^{s_i-1} = \Phi_2(X)^{s_i-1}, & \text{if } s_i > 0, \\ 1, & \text{otherwise.} \end{cases}$$

For each $i = 0, 1, \ldots, k$ we can explicitly construct $\xi_i \in \mathbb{Z}[\langle\gamma\rangle]$ such that

$$\varkappa_i = H_i(\gamma)\xi_i,$$

where

$$H_i(X) = \begin{cases} (X+1)^{s_i-1} = \Phi_2(X)^{s_i-1}, & \text{if } s_i > 0, \\ 1, & \text{otherwise.} \end{cases}$$

Let M be the ideal of $\mathbb{Z}[\langle\gamma\rangle]$ generated by all the ξ_i.

For each $i = 0, 1, \ldots, k$ we can explicitly construct $\xi_i \in \mathbb{Z}[\langle\gamma\rangle]$ such that

$$\varkappa_i = H_i(\gamma)\xi_i,$$

where

$$H_i(X) = \begin{cases} (X+1)^{s_i-1} = \Phi_2(X)^{s_i-1}, & \text{if } s_i > 0, \\ 1, & \text{otherwise.} \end{cases}$$

Let M be the ideal of $\mathbb{Z}[\langle\gamma\rangle]$ generated by all the ξ_i. The elements $\varkappa_i$ and ξ_i satisfy the relations with

$$F_i(X) = \Phi_{2\ell^i}(X).$$

For each $i = 0, 1, \ldots, k$ we can explicitly construct $\xi_i \in \mathbb{Z}[\langle\gamma\rangle]$ such that

$$\varkappa_i = H_i(\gamma)\xi_i,$$

where

$$H_i(X) = \begin{cases} (X+1)^{s_i-1} = \Phi_2(X)^{s_i-1}, & \text{if } s_i > 0, \\ 1, & \text{otherwise.} \end{cases}$$

Let M be the ideal of $\mathbb{Z}[\langle\gamma\rangle]$ generated by all the ξ_i. The elements $\varkappa_i$ and ξ_i satisfy the relations with

$$F_i(X) = \Phi_{2\ell^i}(X).$$

Moreover, it can be shown that polynomials F_i satisfy the assumptions of the main theorem, so we can compute the index $[M : N]$

For each $i = 0, 1, \ldots, k$ we can explicitly construct $\xi_i \in \mathbb{Z}[\langle\gamma\rangle]$ such that

$$\varkappa_i = H_i(\gamma)\xi_i,$$

where

$$H_i(X) = \begin{cases} (X+1)^{s_i-1} = \Phi_2(X)^{s_i-1}, & \text{if } s_i > 0, \\ 1, & \text{otherwise.} \end{cases}$$

Let M be the ideal of $\mathbb{Z}[\langle\gamma\rangle]$ generated by all the ξ_i. The elements $\varkappa_i$ and ξ_i satisfy the relations with

$$F_i(X) = \Phi_{2\ell^i}(X).$$

Moreover, it can be shown that polynomials F_i satisfy the assumptions of the main theorem, so we can compute the index $[M\colon N]$

$$[M\colon N] = \prod_{i=0}^{k} |\mathrm{Res}\,(F_i, H_i)| = \prod_{i=1}^{k} |\mathrm{Res}\,(\Phi_{2\ell^i}, \Phi_2^{t_i})| = \prod_{i=1}^{k} \ell^{t_i},$$

For each $i = 0, 1, \ldots, k$ we can explicitly construct $\xi_i \in \mathbb{Z}[\langle\gamma\rangle]$ such that

$$\varkappa_i = H_i(\gamma)\xi_i,$$

where

$$H_i(X) = \begin{cases} (X+1)^{s_i-1} = \Phi_2(X)^{s_i-1}, & \text{if } s_i > 0, \\ 1, & \text{otherwise.} \end{cases}$$

Let M be the ideal of $\mathbb{Z}[\langle\gamma\rangle]$ generated by all the ξ_i. The elements $\varkappa_i$ and ξ_i satisfy the relations with

$$F_i(X) = \Phi_{2\ell^i}(X).$$

Moreover, it can be shown that polynomials F_i satisfy the assumptions of the main theorem, so we can compute the index $[M\colon N]$

$$[M\colon N] = \prod_{i=0}^{k} |\mathrm{Res}\,(F_i, H_i)| = \prod_{i=1}^{k} |\mathrm{Res}\,(\Phi_{2\ell^i}, \Phi_2^{t_i})| = \prod_{i=1}^{k} \ell^{t_i},$$

where $t_i = \max\{s_i - 1, 0\}$.

Thank you for your attention!