Conjugacy of Integral Matrices over Algebraic Extensions

Rebecca Afandi

Conjugacy over R

- For a ring R, we say that $A, B \in R^{n \times n}$ are R-**conjugate** if there is a $C \in R^{n \times n}$ with $\det(C) \in R^{\times}$ such that $C^{-1}AC = B$.

Conjugacy over R

- For a ring R, we say that $A, B \in R^{n\times n}$ are R-**conjugate** if there is a $C \in R^{n\times n}$ with $\det(C) \in R^{\times}$ such that $C^{-1}AC = B$.
- Write $A \sim_R B$.

Conjugacy over R

- For a ring R, we say that $A, B \in R^{n\times n}$ are R-**conjugate** if there is a $C \in R^{n\times n}$ with $\det(C) \in R^{\times}$ such that $C^{-1}AC = B$.
- Write $A \sim_R B$.
- $\mathbb{Z}, \mathbb{Z}_{(p)}, \mathcal{O}_K$ for a number field K

Conjugacy over R

- For a ring R, we say that $A, B \in R^{n\times n}$ are R-**conjugate** if there is a $C \in R^{n\times n}$ with $\det(C) \in R^{\times}$ such that $C^{-1}AC = B$.
- Write $A \sim_R B$.
- $\mathbb{Z}, \mathbb{Z}_{(p)}, \mathcal{O}_K$ for a number field K

The localization of $\mathbb{Z}$ at p is

$$\mathbb{Z}_{(p)} = \{\frac{a}{b} : a, b \in \mathbb{Z}, p \nmid b\}$$

Conjugacy over R

- For a ring R, we say that $A, B \in R^{n\times n}$ are R-**conjugate** if there is a $C \in R^{n\times n}$ with $\det(C) \in R^{\times}$ such that $C^{-1}AC = B$.
- Write $A \sim_R B$.
- $\mathbb{Z}, \mathbb{Z}_{(p)}, \mathcal{O}_K$ for a number field K

Conjugacy over R

- For a ring R, we say that $A, B \in R^{n\times n}$ are R-**conjugate** if there is a $C \in R^{n\times n}$ with $\det(C) \in R^\times$ such that $C^{-1}AC = B$.
- Write $A \sim_R B$.
- $\mathbb{Z}, \mathbb{Z}_{(p)}, \mathcal{O}_K$ for a number field K

$\mathcal{O}_K$ is the set of algebraic integral elements (elements with monic integral minimal polynomial)

Conjugacy over R

- For a ring R, we say that $A, B \in R^{n\times n}$ are R-**conjugate** if there is a $C \in R^{n\times n}$ with $\det(C) \in R^{\times}$ such that $C^{-1}AC = B$.
- Write $A \sim_R B$.
- $\mathbb{Z}, \mathbb{Z}_{(p)}, \mathcal{O}_K$ for a number field K

Conjugacy over R	R is a field
• For a ring R, we say that $A, B \in R^{n \times n}$ are R-**conjugate** if there is a $C \in R^{n \times n}$ with $\det(C) \in R^{\times}$ such that $C^{-1}AC = B$. • Write $A \sim_R B$. • $\mathbb{Z}, \mathbb{Z}_{(p)}, \mathcal{O}_K$ for a number field K	

Conjugacy over R

- For a ring R, we say that $A, B \in R^{n\times n}$ are R-**conjugate** if there is a $C \in R^{n\times n}$ with $\det(C) \in R^{\times}$ such that $C^{-1}AC = B$.
- Write $A \sim_R B$.
- $\mathbb{Z}, \mathbb{Z}_{(p)}, \mathcal{O}_K$ for a number field K

R is a field

- All matrices with the same square-free characteristic polynomial are conjugate over a field.

Conjugacy over R

- For a ring R, we say that $A, B \in R^{n\times n}$ are R-**conjugate** if there is a $C \in R^{n\times n}$ with $\det(C) \in R^{\times}$ such that $C^{-1}AC = B$.
- Write $A \sim_R B$.
- $\mathbb{Z}, \mathbb{Z}_{(p)}, \mathcal{O}_K$ for a number field K

R is a field

- All matrices with the same square-free characteristic polynomial are conjugate over a field.
- Let $f \in \mathbb{Z}[x]$ be monic and square-free of degree n.

Conjugacy over R

- For a ring R, we say that $A, B \in R^{n\times n}$ are R-**conjugate** if there is a $C \in R^{n\times n}$ with $\det(C) \in R^\times$ such that $C^{-1}AC = B$.
- Write $A \sim_R B$.
- $\mathbb{Z}, \mathbb{Z}_{(p)}, \mathcal{O}_K$ for a number field K

R is a field

- All matrices with the same square-free characteristic polynomial are conjugate over a field.
- Let $f \in \mathbb{Z}[x]$ be monic and square-free of degree n.
- $\mathcal{M}_f = \{A \in \mathbb{Z}^{n\times n} : \det(xI - A) = f\}$

Conjugacy over R	R is a field
• For a ring R, we say that $A, B \in R^{n \times n}$ are R-**conjugate** if there is a $C \in R^{n \times n}$ with $\det(C) \in R^{\times}$ such that $C^{-1}AC = B$. • Write $A \sim_R B$. • $\mathbb{Z}, \mathbb{Z}_{(p)}, \mathcal{O}_K$ for a number field K	• All matrices with the same square-free characteristic polynomial are conjugate over a field. • Let $f \in \mathbb{Z}[x]$ be monic and square-free of degree n. • $\mathcal{M}_f = \{A \in \mathbb{Z}^{n \times n} : \det(xI - A) = f\}$

Latimer and MacDuffee Correspondence (1933)

Conjugacy over R	R is a field
• For a ring R, we say that $A, B \in R^{n\times n}$ are R-**conjugate** if there is a $C \in R^{n\times n}$ with $\det(C) \in R^{\times}$ such that $C^{-1}AC = B$. • Write $A \sim_R B$. • $\mathbb{Z}, \mathbb{Z}_{(p)}, \mathcal{O}_K$ for a number field K	• All matrices with the same square-free characteristic polynomial are conjugate over a field. • Let $f \in \mathbb{Z}[x]$ be monic and square-free of degree n. • $\mathcal{M}_f = \{A \in \mathbb{Z}^{n\times n} : \det(xI - A) = f\}$

Latimer and MacDuffee Correspondence (1933)

Taussky (1949)

Conjugacy over R	R is a field
• For a ring R, we say that $A, B \in R^{n\times n}$ are R-**conjugate** if there is a $C \in R^{n\times n}$ with $\det(C) \in R^{\times}$ such that $C^{-1}AC = B$. • Write $A \sim_R B$. • $\mathbb{Z}, \mathbb{Z}_{(p)}, \mathcal{O}_K$ for a number field K	• All matrices with the same square-free characteristic polynomial are conjugate over a field. • Let $f \in \mathbb{Z}[x]$ be monic and square-free of degree n. • $\mathcal{M}_f = \{A \in \mathbb{Z}^{n\times n} : \det(xI - A) = f\}$

Latimer and MacDuffee Correspondence (1933)

Taussky (1949)

- $f(x)$ irreducible with root α

Conjugacy over R	R is a field
• For a ring R, we say that $A, B \in R^{n\times n}$ are R-**conjugate** if there is a $C \in R^{n\times n}$ with $\det(C) \in R^{\times}$ such that $C^{-1}AC = B$. • Write $A \sim_R B$. • $\mathbb{Z}, \mathbb{Z}_{(p)}, \mathcal{O}_K$ for a number field K	• All matrices with the same square-free characteristic polynomial are conjugate over a field. • Let $f \in \mathbb{Z}[x]$ be monic and square-free of degree n. • $\mathcal{M}_f = \{A \in \mathbb{Z}^{n\times n} : \det(xI - A) = f\}$

Latimer and MacDuffee Correspondence (1933)

Taussky (1949)

- $f(x)$ irreducible with root α
- Let $K = \mathbb{Q}(\alpha)$

Conjugacy over R	R is a field
• For a ring R, we say that $A, B \in R^{n\times n}$ are R-**conjugate** if there is a $C \in R^{n\times n}$ with $\det(C) \in R^{\times}$ such that $C^{-1}AC = B$. • Write $A \sim_R B$. • $\mathbb{Z}, \mathbb{Z}_{(p)}, \mathcal{O}_K$ for a number field K	• All matrices with the same square-free characteristic polynomial are conjugate over a field. • Let $f \in \mathbb{Z}[x]$ be monic and square-free of degree n. • $\mathcal{M}_f = \{A \in \mathbb{Z}^{n\times n} : \det(xI - A) = f\}$

Latimer and MacDuffee Correspondence (1933)

Taussky (1949)

- $f(x)$ irreducible with root α
- Let $K = \mathbb{Q}(\alpha)$
- $\mathcal{M}_f/_{\sim_{\mathbb{Z}}} \leftrightarrow$ fractional $\mathbb{Z}[\alpha]$-ideal classes in K

$\mathbb{Z}$-conjugacy within $\mathscr{M}_f$ for $f = x^2 + 5$

$\mathbb{Z}$-conjugacy within $\mathscr{M}_f$ for $f = x^2 + 5$

- Let $f = x^2 + 5$ and K be the number field $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$. Note: $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Some $\mathbb{Z}[\alpha]$-fractional ideals in K are:

$\mathbb{Z}$-conjugacy within $\mathscr{M}_f$ for $f = x^2 + 5$

- Let $f = x^2 + 5$ and K be the number field $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$. Note: $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Some $\mathbb{Z}[\alpha]$-fractional ideals in K are:
    - $\mathbb{Z}[\alpha] = 1\mathbb{Z} \oplus \alpha\mathbb{Z}$

$\mathbb{Z}$-conjugacy within $\mathcal{M}_f$ for $f = x^2 + 5$

- Let $f = x^2 + 5$ and K be the number field $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$. Note: $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Some $\mathbb{Z}[\alpha]$-fractional ideals in K are:
  - $\mathbb{Z}[\alpha] = 1\mathbb{Z} \oplus \alpha\mathbb{Z}$
  - $I = 2\mathbb{Z} \oplus (1 + \alpha)\mathbb{Z}$ (non-principal)

$\mathbb{Z}$-conjugacy within $\mathcal{M}_f$ for $f = x^2 + 5$

- Let $f = x^2 + 5$ and K be the number field $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$. Note: $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Some $\mathbb{Z}[\alpha]$-fractional ideals in K are:
  - $\mathbb{Z}[\alpha] = 1\mathbb{Z} \oplus \alpha\mathbb{Z}$
  - $I = 2\mathbb{Z} \oplus (1 + \alpha)\mathbb{Z}$ (non-principal)
- These are representatives of the fractional ideal classes (fractional ideals I and J are equivalent if there is $k \in \mathbb{Q}(\alpha)$ such that $kI = J$).

$\mathbb{Z}$-conjugacy within $\mathcal{M}_f$ for $f = x^2 + 5$

- Let $f = x^2 + 5$ and K be the number field $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$. Note: $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Some $\mathbb{Z}[\alpha]$-fractional ideals in K are:
  - $\mathbb{Z}[\alpha] = 1\mathbb{Z} \oplus \alpha\mathbb{Z}$
  - $I = 2\mathbb{Z} \oplus (1 + \alpha)\mathbb{Z}$ (non-principal)
- These are representatives of the fractional ideal classes (fractional ideals I and J are equivalent if there is $k \in \mathbb{Q}(\alpha)$ such that $kI = J$).
- The fractional ideal classes form the ideal class group, denoted by Pic($\mathbb{Z}[\alpha]$). The class number is the order of the class group. ($h_K = 2$ for $K = \mathbb{Q}(\alpha)$.)

$\mathbb{Z}$-conjugacy within $\mathcal{M}_f$ for $f = x^2 + 5$

- Let $f = x^2 + 5$ and K be the number field $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$. Note: $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Some $\mathbb{Z}[\alpha]$-fractional ideals in K are:
  - $\mathbb{Z}[\alpha] = 1\mathbb{Z} \oplus \alpha\mathbb{Z}$
  - $I = 2\mathbb{Z} \oplus (1+\alpha)\mathbb{Z}$ (non-principal)

$$\begin{aligned} \alpha \cdot 1 &= 0 \cdot 1 + 1 \cdot \alpha \\ \alpha \cdot \alpha &= -5 \cdot 1 + 0 \cdot \alpha \end{aligned}$$

so $\mathbb{Z}[\alpha]$ corresponds to $C_f = \begin{pmatrix} 0 & 1 \\ -5 & 0 \end{pmatrix}$.

$$\begin{aligned} \alpha \cdot 2 &= -1 \cdot 2 + 2 \cdot (1+\alpha) \\ \alpha \cdot (1+\alpha) &= -3 \cdot 2 + 1 \cdot (1+\alpha) \end{aligned}$$

so I corresponds to $\begin{pmatrix} -1 & 2 \\ -3 & 1 \end{pmatrix}$.

$\mathbb{Z}$-conjugacy within $\mathscr{M}_f$ for $f = x^2 + 5$

$$\mathbb{Z}[\alpha] \ncong_{\mathbb{Z}[\alpha]} I \implies \begin{pmatrix} 0 & 1 \\ -5 & 0 \end{pmatrix} \nsim_{\mathbb{Z}} \begin{pmatrix} -1 & 2 \\ -3 & 1 \end{pmatrix}$$

$) \cong \mathbb{Q}[x]/(f)$.

ls in K are:

- $\mathbb{Z}[\alpha] = 1\mathbb{Z} \oplus \alpha\mathbb{Z}$
- $I = 2\mathbb{Z} \oplus (1 + \alpha)\mathbb{Z}$ (non-principal)

$$\alpha \cdot 1 = 0 \cdot 1 + 1 \cdot \alpha$$
$$\alpha \cdot \alpha = -5 \cdot 1 + 0 \cdot \alpha$$

so $\mathbb{Z}[\alpha]$ corresponds to $C_f = \begin{pmatrix} 0 & 1 \\ -5 & 0 \end{pmatrix}$.

$$\alpha \cdot 2 = -1 \cdot 2 + 2 \cdot (1 + \alpha)$$
$$\alpha \cdot (1 + \alpha) = -3 \cdot 2 + 1 \cdot (1 + \alpha)$$

so I corresponds to $\begin{pmatrix} -1 & 2 \\ -3 & 1 \end{pmatrix}$.

Conjugacy over R	R is a field
• For a ring R, we say that $A, B \in R^{n\times n}$ are R-**conjugate** if there is a $C \in R^{n\times n}$ with $\det(C) \in R^{\times}$ such that $C^{-1}AC = B$. • Write $A \sim_R B$. • $\mathbb{Z}, \mathbb{Z}_{(p)}, \mathcal{O}_K$ for a number field K	• All matrices with the same square-free characteristic polynomial are conjugate over a field. • Let $f \in \mathbb{Z}[x]$ be monic and square-free of degree n. • $\mathcal{M}_f = \{A \in \mathbb{Z}^{n\times n} : \det(xI - A) = f\}$

Latimer and MacDuffee Correspondence (1933)

Taussky (1949)

- $f(x)$ irreducible with root α
- Let $K = \mathbb{Q}(\alpha)$
- $\mathcal{M}_f/_{\sim_{\mathbb{Z}}} \leftrightarrow$ fractional $\mathbb{Z}[\alpha]$-ideal classes in K

Conjugacy over R	R is a field
• For a ring R, we say that $A, B \in R^{n\times n}$ are R-**conjugate** if there is a $C \in R^{n\times n}$ with $\det(C) \in R^{\times}$ such that $C^{-1}AC = B$. • Write $A \sim_R B$. • $\mathbb{Z}, \mathbb{Z}_{(p)}, \mathcal{O}_K$ for a number field K	• All matrices with the same square-free characteristic polynomial are conjugate over a field. • Let $f \in \mathbb{Z}[x]$ be monic and square-free of degree n. • $\mathcal{M}_f = \{A \in \mathbb{Z}^{n\times n} : \det(xI - A) = f\}$

Latimer and MacDuffee Correspondence (1933)

Taussky (1949)

- $f(x)$ irreducible with root α
- Let $K = \mathbb{Q}(\alpha)$
- $\mathcal{M}_f/_{\sim_{\mathbb{Z}}} \leftrightarrow$ fractional $\mathbb{Z}[\alpha]$-ideal classes in K

Marseglia (2019)

Conjugacy over R	R is a field
• For a ring R, we say that $A, B \in R^{n \times n}$ are R-**conjugate** if there is a $C \in R^{n \times n}$ with $\det(C) \in R^{\times}$ such that $C^{-1}AC = B$. • Write $A \sim_R B$. • $\mathbb{Z}, \mathbb{Z}_{(p)}, \mathcal{O}_K$ for a number field K	• All matrices with the same square-free characteristic polynomial are conjugate over a field. • Let $f \in \mathbb{Z}[x]$ be monic and square-free of degree n. • $\mathcal{M}_f = \{A \in \mathbb{Z}^{n \times n} : \det(xI - A) = f\}$

Latimer and MacDuffee Correspondence (1933)

Taussky (1949)

- $f(x)$ irreducible with root α
- Let $K = \mathbb{Q}(\alpha)$
- $\mathcal{M}_f/_{\sim_{\mathbb{Z}}} \leftrightarrow$ fractional $\mathbb{Z}[\alpha]$-ideal classes in K

Marseglia (2019)

- $f(x) = \prod_{i=1}^{m} f_i$ square-free with $\alpha = (\alpha_1, \ldots, \alpha_m)$

Conjugacy over R	R is a field
• For a ring R, we say that $A, B \in R^{n\times n}$ are R-**conjugate** if there is a $C \in R^{n\times n}$ with $\det(C) \in R^\times$ such that $C^{-1}AC = B$. • Write $A \sim_R B$. • $\mathbb{Z}, \mathbb{Z}_{(p)}, \mathcal{O}_K$ for a number field K	• All matrices with the same square-free characteristic polynomial are conjugate over a field. • Let $f \in \mathbb{Z}[x]$ be monic and square-free of degree n. • $\mathcal{M}_f = \{A \in \mathbb{Z}^{n\times n} : \det(xI - A) = f\}$

Latimer and MacDuffee Correspondence (1933)

Taussky (1949)

- $f(x)$ irreducible with root α
- Let $K = \mathbb{Q}(\alpha)$
- $\mathcal{M}_f/_{\sim_\mathbb{Z}} \leftrightarrow$ fractional $\mathbb{Z}[\alpha]$-ideal classes in K

Marseglia (2019)

- $f(x) = \prod_{i=1}^{m} f_i$ square-free with $\alpha = (\alpha_1, \ldots, \alpha_m)$
- Let $K = \prod_{i=1}^{m} \mathbb{Q}(\alpha_i)$

Conjugacy over R	R is a field
• For a ring R, we say that $A, B \in R^{n\times n}$ are R-**conjugate** if there is a $C \in R^{n\times n}$ with $\det(C) \in R^{\times}$ such that $C^{-1}AC = B$. • Write $A \sim_R B$. • $\mathbb{Z}, \mathbb{Z}_{(p)}, \mathcal{O}_K$ for a number field K	• All matrices with the same square-free characteristic polynomial are conjugate over a field. • Let $f \in \mathbb{Z}[x]$ be monic and square-free of degree n. • $\mathcal{M}_f = \{A \in \mathbb{Z}^{n\times n} : \det(xI - A) = f\}$

Latimer and MacDuffee Correspondence (1933)

Taussky (1949)

- $f(x)$ irreducible with root α
- Let $K = \mathbb{Q}(\alpha)$
- $\mathcal{M}_f/_{\sim_\mathbb{Z}} \leftrightarrow$ fractional $\mathbb{Z}[\alpha]$-ideal classes in K

Marseglia (2019)

- $f(x) = \prod_{i=1}^{m} f_i$ square-free with $\alpha = (\alpha_1, \ldots, \alpha_m)$
- Let $K = \prod_{i=1}^{m} \mathbb{Q}(\alpha_i)$
- $\mathcal{M}_f/_{\sim_\mathbb{Z}} \leftrightarrow$ full $\mathbb{Z}[(\alpha_1, \ldots, \alpha_m)]$-module classes in K

$\mathbb{Z}$-conjugacy within $\mathcal{M}_f$ for $f = f_1 f_2$ with $f_1 = x^2 + 4x + 7, f_2 = x^3 - 9x^2 - 3x - 1$

$\mathbb{Z}$-conjugacy within $\mathscr{M}_f$ for $f = f_1 f_2$ with $f_1 = x^2 + 4x + 7, f_2 = x^3 - 9x^2 - 3x - 1$

- Letting $K_i = \mathbb{Q}(\alpha_i) \cong \mathbb{Q}[x]/(f_i)$ we consider classes of $\mathbb{Z}[(\alpha_1, \alpha_2)]$-modules within $K := K_1 \times K_2$.

$\mathbb{Z}$-conjugacy within $\mathscr{M}_f$ for $f = f_1 f_2$ with $f_1 = x^2 + 4x + 7, f_2 = x^3 - 9x^2 - 3x - 1$

- Letting $K_i = \mathbb{Q}(\alpha_i) \cong \mathbb{Q}[x]/(f_i)$ we consider classes of $\mathbb{Z}[(\alpha_1, \alpha_2)]$-modules within $K := K_1 \times K_2$.

- $\mathcal{O}_K = \mathcal{O}_{K_1} \times \mathcal{O}_{K_2}$ but in general, fractional ideals are not products of fractional ideals in the $\mathcal{I}_{\mathbb{Z}[\alpha_i]}$.

$\mathbb{Z}$-conjugacy within $\mathscr{M}_f$ for $f = f_1 f_2$ with $f_1 = x^2 + 4x + 7, f_2 = x^3 - 9x^2 - 3x - 1$

- Letting $K_i = \mathbb{Q}(\alpha_i) \cong \mathbb{Q}[x]/(f_i)$ we consider classes of $\mathbb{Z}[(\alpha_1, \alpha_2)]$-modules within $K := K_1 \times K_2$.

- $\mathcal{O}_K = \mathcal{O}_{K_1} \times \mathcal{O}_{K_2}$ but in general, fractional ideals are not products of fractional ideals in the $\mathscr{I}_{\mathbb{Z}[\alpha_i]}$.

- $\mathscr{M}_{f_1}$ has 2 $\mathbb{Z}$-conjugacy classes and $\mathscr{M}_{f_2}$ has 6 $\mathbb{Z}$-conjugacy classes, but $\mathscr{M}_f$ has 852 $\mathbb{Z}$-classes.

Marseglia’s bijection

Marseglia's bijection

$$\varphi_{\mathbb{Z}} : \mathscr{I}_{\mathbb{Z}[\alpha]}/_{\cong \mathbb{Z}[\alpha]} \to \mathscr{M}_f/_{\sim \mathbb{Z}}$$
$$[I] \mapsto [A]$$

Marseglia's bijection

$$\varphi_{\mathbb{Z}} : \mathscr{I}_{\mathbb{Z}[\alpha]} /_{\cong \mathbb{Z}[\alpha]} \to \mathscr{M}_f /_{\sim \mathbb{Z}}$$
$$[I] \mapsto [A]$$

$\mathscr{I}_{\mathbb{Z}[\alpha]}$ denotes the set of fractional $\mathbb{Z}[\alpha]$-ideals.

Marseglia's bijection

$$\varphi_{\mathbb{Z}} : \mathscr{I}_{\mathbb{Z}[\alpha]}/_{\cong \mathbb{Z}[\alpha]} \to \mathscr{M}_f/_{\sim \mathbb{Z}}$$

$$[I] \mapsto [A]$$

I can be written as

$$I = \bigoplus_{i=1}^{n} v_i \mathbb{Z}.$$

Marseglia's bijection

$$\varphi_{\mathbb{Z}} : \mathcal{I}_{\mathbb{Z}[\alpha]}/_{\cong \mathbb{Z}[\alpha]} \to \mathcal{M}_f/_{\sim \mathbb{Z}}$$
$$[I] \mapsto [A]$$

I can be written as
$$I = \bigoplus_{i=1}^{n} v_i \mathbb{Z}.$$

A is the multiplication-by-α matrix with respect to the $\mathbb{Z}$-basis $\{v_1, \ldots, v_n\}$

Marseglia's bijection

$$\varphi_{\mathbb{Z}} : \text{ICM}(\mathbb{Z}[\alpha]) \to \mathcal{M}_f/_{\sim\mathbb{Z}}$$

$$[I] \mapsto [A]$$

I can be written as

$$I = \bigoplus_{i=1}^{n} v_i\mathbb{Z}.$$

A is the multiplication-by-α matrix with respect to the $\mathbb{Z}$-basis $\{v_1, \ldots, v_n\}$

Marseglia's bijection

$$\varphi_{\mathbb{Z}} : \text{ICM}(\mathbb{Z}[\alpha]) \to \mathscr{M}_f/_{\sim\mathbb{Z}}$$
$$[I] \mapsto [A]$$

Marseglia's bijection

$$\varphi_{\mathbb{Z}} : \text{ICM}(\mathbb{Z}[\alpha]) \to \mathcal{M}_f/_{\sim\mathbb{Z}}$$
$$[I] \mapsto [A]$$

- How to find $\psi_{\mathbb{Z}} := \varphi_{\mathbb{Z}}^{-1}$

Marseglia's bijection

$$\varphi_{\mathbb{Z}} : \text{ICM}(\mathbb{Z}[\alpha]) \to \mathscr{M}_f/_{\sim\mathbb{Z}}$$
$$[I] \mapsto [A]$$

- How to find $\psi_{\mathbb{Z}} := \varphi_{\mathbb{Z}}^{-1}$

- For f irreducible, find $\overline{v} = (v_1, \dots, v_n)^t$ so that $A\overline{v} = \alpha\overline{v}$. Let $I = \bigoplus v_i\mathbb{Z}$ and let $\psi_{\mathbb{Z}}([A]) = [I]$.

Marseglia's bijection

$$\varphi_{\mathbb{Z}} : \text{ICM}(\mathbb{Z}[\alpha]) \to \mathcal{M}_f/_{\sim\mathbb{Z}}$$
$$[I] \mapsto [A]$$

- How to find $\psi_{\mathbb{Z}} := \varphi_{\mathbb{Z}}^{-1}$

- For f irreducible, find $\overline{v} = (v_1, \dots, v_n)^t$ so that $A\overline{v} = \alpha\overline{v}$. Let $I = \bigoplus v_i\mathbb{Z}$ and let $\psi_{\mathbb{Z}}([A]) = [I]$.

- For f with $m > 1$ irreducible factors, let $A\overline{v}_i = \alpha_i\overline{v}_i$ and $\overline{v}_i = (v_{i1}, \dots, v_{in})^t$, then $\psi_{\mathbb{Z}}([A])$ has representative $I = (v_{11}, \dots v_{m1})\mathbb{Z} \oplus \dots \oplus (v_{1n}, \dots, v_{mn})\mathbb{Z}$.

Example: $\mathbb{Z}$-conjugacy within $\mathscr{M}_f$ for $f = x^2 + 23$

Example: $\mathbb{Z}$-conjugacy within $\mathcal{M}_f$ for $f = x^2 + 23$

- Letting $K := \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f)$, we have
  $\mathbb{Z}[\alpha] = 1\mathbb{Z} \oplus \alpha\mathbb{Z} \subsetneq \mathcal{O}_K = 1\mathbb{Z} \oplus \left(\frac{1+\alpha}{2}\right)\mathbb{Z}$

Example: $\mathbb{Z}$-conjugacy within $\mathcal{M}_f$ for $f = x^2 + 23$

- Letting $K := \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f)$, we have
$\mathbb{Z}[\alpha] = 1\mathbb{Z} \oplus \alpha\mathbb{Z} \subsetneq \mathcal{O}_K = 1\mathbb{Z} \oplus \left(\frac{1+\alpha}{2}\right)\mathbb{Z}$

- For a $\mathbb{Z}[\alpha]$-ideal I, the **multiplicator ring** of I is $(I : I)$.

Example: $\mathbb{Z}$-conjugacy within $\mathscr{M}_f$ for $f = x^2 + 23$

- Letting $K := \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f)$, we have
  $\mathbb{Z}[\alpha] = 1\mathbb{Z} \oplus \alpha\mathbb{Z} \subsetneq \mathcal{O}_K = 1\mathbb{Z} \oplus \left(\frac{1+\alpha}{2}\right)\mathbb{Z}$

- For a $\mathbb{Z}[\alpha]$-ideal I, the **multiplicator ring** of I is $(I : I)$.

$$(I : J) = \{x \in \mathbb{Q}(\alpha) : xJ \subseteq I\}$$

Example: $\mathbb{Z}$-conjugacy within $\mathscr{M}_f$ for $f = x^2 + 23$

- Letting $K := \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f)$, we have
$$\mathbb{Z}[\alpha] = 1\mathbb{Z} \oplus \alpha\mathbb{Z} \subsetneq \mathcal{O}_K = 1\mathbb{Z} \oplus \left(\frac{1+\alpha}{2}\right)\mathbb{Z}$$

- For a $\mathbb{Z}[\alpha]$-ideal I, the **multiplicator ring** of I is $(I : I)$.

- If $I = kJ$ for $k \in \mathbb{Q}(\alpha)$, then $(I : I) = (J : J)$.

Example: $\mathbb{Z}$-conjugacy within $\mathcal{M}_f$ for $f = x^2 + 23$

- Letting $K := \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f)$, we have $\mathbb{Z}[\alpha] = 1\mathbb{Z} \oplus \alpha\mathbb{Z} \subsetneq \mathcal{O}_K = 1\mathbb{Z} \oplus \left(\frac{1+\alpha}{2}\right)\mathbb{Z}$

- For a $\mathbb{Z}[\alpha]$-ideal I, the **multiplicator ring** of I is $(I : I)$.

- If $I = kJ$ for $k \in \mathbb{Q}(\alpha)$, then $(I : I) = (J : J)$.

- $\mathbb{Z}[\alpha] \leftrightarrow C_f = \begin{pmatrix} 0 & 1 \\ -23 & 0 \end{pmatrix}$ and $\mathcal{O}_K \leftrightarrow A = \begin{pmatrix} -1 & 2 \\ -12 & 1 \end{pmatrix}$. These matrices are not $\mathbb{Z}$-conjugate.

Example: $\mathbb{Z}$-conjugacy within $\mathscr{M}_f$ for $f = x^2 + 23$

- Letting $K := \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f)$, we have
  $\mathbb{Z}[\alpha] = 1\mathbb{Z} \oplus \alpha\mathbb{Z} \subsetneq \mathcal{O}_K = 1\mathbb{Z} \oplus \left(\frac{1+\alpha}{2}\right)\mathbb{Z}$

- For a $\mathbb{Z}[\alpha]$-ideal I, the **multiplicator ring** of I is $(I : I)$.

- If $I = kJ$ for $k \in \mathbb{Q}(\alpha)$, then $(I : I) = (J : J)$.

- $\mathbb{Z}[\alpha] \leftrightarrow C_f = \begin{pmatrix} 0 & 1 \\ -23 & 0 \end{pmatrix}$ and $\mathcal{O}_K \leftrightarrow A = \begin{pmatrix} -1 & 2 \\ -12 & 1 \end{pmatrix}$. These matrices are not $\mathbb{Z}$-conjugate.

- ICM($\mathbb{Z}[\alpha]$) = Pic($\mathbb{Z}[\alpha]$) $\sqcup$ Pic($\mathcal{O}_K$). Each Picard group has order 3, so there are 6 $\mathbb{Z}$-conjugacy classes within $\mathscr{M}_f$.

Example: $\mathbb{Z}$-conjugacy within $\mathscr{M}_f$ for $f = x^2 + 23$

- Letting $K := \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f)$, we have
  $\mathbb{Z}[\alpha] = 1\mathbb{Z} \oplus \alpha\mathbb{Z} \subsetneq \mathcal{O}_K = 1\mathbb{Z} \oplus \left(\frac{1+\alpha}{2}\right)\mathbb{Z}$
- For a $\mathbb{Z}[\alpha]$-ideal I, the **multiplicator ring** of I is $(I : I)$.
- If $I = kJ$ for $k \in \mathbb{Q}(\alpha)$, then $(I : I) = (J : J)$.
- $\mathbb{Z}[\alpha] \leftrightarrow C_f = \begin{pmatrix} 0 & 1 \\ -23 & 0 \end{pmatrix}$ and $\mathcal{O}_K \leftrightarrow A = \begin{pmatrix} -1 & 2 \\ -12 & 1 \end{pmatrix}$. These matrices are not $\mathbb{Z}$-conjugate.

$\mathrm{ICM}(\mathbb{Z}[\alpha]) = \sqcup_{\mathcal{O}} \mathrm{ICM}_{\mathcal{O}}(\mathbb{Z}[\alpha]) \supseteq \sqcup_{\mathcal{O}} \mathrm{Pic}(\mathcal{O})$

- $\mathrm{ICM}(\mathbb{Z}[\alpha]) = \mathrm{Pic}(\mathbb{Z}[\alpha]) \sqcup \mathrm{Pic}(\mathcal{O}_K)$. Each Picard group has order 3, so there are 6 $\mathbb{Z}$-conjugacy classes within $\mathscr{M}_f$.

$\mathbb{Z}_{(p)}$-conjugacy

$\mathbb{Z}_{(p)}$-conjugacy

- For f square-free, integral matrices in $\mathcal{M}_f$ are $\mathbb{Z}_{(p)}$-conjugate for $p \nmid \text{disc}(f)$.

$\mathbb{Z}_{(p)}$-conjugacy

- For f square-free, integral matrices in $\mathscr{M}_f$ are $\mathbb{Z}_{(p)}$-conjugate for $p \nmid \mathrm{disc}(f)$.

- A local-global principal does not hold for matrix conjugacy: $A \sim_{\mathbb{Z}_{(p)}} B \ \forall\ p \not\Rightarrow A \sim_{\mathbb{Z}} B$

$\mathbb{Z}_{(p)}$-conjugacy

- For f square-free, integral matrices in $\mathcal{M}_f$ are $\mathbb{Z}_{(p)}$-conjugate for $p \nmid \mathrm{disc}(f)$.
- A local-global principal does not hold for matrix conjugacy: $A \sim_{\mathbb{Z}_{(p)}} B \;\forall\, p \not\Rightarrow A \sim_{\mathbb{Z}} B$
- I refer to matrices which satisfy $A \sim_{\mathbb{Z}_{(p)}} B$ for all primes p as **locally conjugate**.

Failure of local-global principal

Failure of local-global principal

$A = \begin{pmatrix} 0 & -6 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 2 \\ -3 & 0 \end{pmatrix}$ have characteristic polynomial $c(x) = x^2 + 6$, with disc$(c) = -24$.

Failure of local-global principal

$A = \begin{pmatrix} 0 & -6 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 2 \\ -3 & 0 \end{pmatrix}$ have characteristic polynomial $c(x) = x^2 + 6$, with disc$(c) = -24$.

- A and B are conjugate over $\mathbb{Z}_{(p)}$ for $p \neq 2,3$.

Failure of local-global principal

$A = \begin{pmatrix} 0 & -6 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 2 \\ -3 & 0 \end{pmatrix}$ have characteristic polynomial $c(x) = x^2 + 6$, with disc$(c) = -24$.

- A and B are conjugate over $\mathbb{Z}_{(p)}$ for $p \neq 2,3$.
- $C_1 = \begin{pmatrix} -3 & 0 \\ 0 & 1 \end{pmatrix}$ yields a conjugating matrix over $\mathbb{Z}_{(2)}$.

Failure of local-global principal

$A = \begin{pmatrix} 0 & -6 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 2 \\ -3 & 0 \end{pmatrix}$ have characteristic polynomial $c(x) = x^2 + 6$, with disc$(c) = -24$.

- A and B are conjugate over $\mathbb{Z}_{(p)}$ for $p \neq 2,3$.
- $C_1 = \begin{pmatrix} -3 & 0 \\ 0 & 1 \end{pmatrix}$ yields a conjugating matrix over $\mathbb{Z}_{(2)}$.
- $C_2 = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$ yields a conjugating matrix over $\mathbb{Z}_{(3)}$.

Failure of local-global principal

$A = \begin{pmatrix} 0 & -6 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 2 \\ -3 & 0 \end{pmatrix}$ have characteristic polynomial $c(x) = x^2 + 6$, with disc$(c) = -24$.

- A and B are conjugate over $\mathbb{Z}_{(p)}$ for $p \neq 2,3$.
- $C_1 = \begin{pmatrix} -3 & 0 \\ 0 & 1 \end{pmatrix}$ yields a conjugating matrix over $\mathbb{Z}_{(2)}$.
- $C_2 = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$ yields a conjugating matrix over $\mathbb{Z}_{(3)}$.
- A and B are not conjugate over $\mathbb{Z}$.

Failure of local-global principal

$A = \begin{pmatrix} 0 & -6 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 2 \\ -3 & 0 \end{pmatrix}$ have characteristic polynomial $c(x) = x^2 + 6$, with disc$(c) = -24$.

- A and B are conjugate over $\mathbb{Z}_{(p)}$ for $p \neq 2,3$.
- $C_1 = \begin{pmatrix} -3 & 0 \\ 0 & 1 \end{pmatrix}$ yields a conjugating matrix over $\mathbb{Z}_{(2)}$.
- $C_2 = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$ yields a conjugating matrix over $\mathbb{Z}_{(3)}$.
- A and B are not conjugate over $\mathbb{Z}$.

Theorem of Guralnick (1980): $A \sim_{\mathbb{Z}_{(p)}} B$ over for all prime ideals $p \iff A \sim B$ over some finite integral extension E of $\mathbb{Z}$.

Failure of local-global principal

$A = \begin{pmatrix} 0 & -6 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 2 \\ -3 & 0 \end{pmatrix}$ have characteristic polynomial $c(x) = x^2 + 6$, with $\text{disc}(c) = -24$.

- A and B are conjugate over $\mathbb{Z}_{(p)}$ for $p \neq 2,3$.
- $C_1 = \begin{pmatrix} -3 & 0 \\ 0 & 1 \end{pmatrix}$ yields a conjugating matrix over $\mathbb{Z}_{(2)}$.
- $C_2 = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$ yields a conjugating matrix over $\mathbb{Z}_{(3)}$.
- A and B are not conjugate over $\mathbb{Z}$.

Theorem of Guralnick (1980): $A \sim_{\mathbb{Z}_{(p)}} B$ over for all prime ideals $p \iff A \sim B$ over some finite integral extension E of $\mathbb{Z}$.

Example:

Failure of local-global principal

$A = \begin{pmatrix} 0 & -6 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 2 \\ -3 & 0 \end{pmatrix}$ have characteristic polynomial $c(x) = x^2 + 6$, with $\text{disc}(c) = -24$.

- A and B are conjugate over $\mathbb{Z}_{(p)}$ for $p \neq 2,3$.
- $C_1 = \begin{pmatrix} -3 & 0 \\ 0 & 1 \end{pmatrix}$ yields a conjugating matrix over $\mathbb{Z}_{(2)}$.
- $C_2 = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$ yields a conjugating matrix over $\mathbb{Z}_{(3)}$.
- A and B are not conjugate over $\mathbb{Z}$.

Theorem of Guralnick (1980): $A \sim_{\mathbb{Z}_{(p)}} B$ over for all prime ideals $p \iff A \sim B$ over some finite integral extension E of $\mathbb{Z}$.

Example:

- $f(x, y) = \det(xC_1 + yC_2) = -3x^2 - 2y^2$ realizes a unit over some extension.

Failure of local-global principal

$A = \begin{pmatrix} 0 & -6 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 2 \\ -3 & 0 \end{pmatrix}$ have characteristic polynomial $c(x) = x^2 + 6$, with disc$(c) = -24$.

- A and B are conjugate over $\mathbb{Z}_{(p)}$ for $p \neq 2,3$.
- $C_1 = \begin{pmatrix} -3 & 0 \\ 0 & 1 \end{pmatrix}$ yields a conjugating matrix over $\mathbb{Z}_{(2)}$.
- $C_2 = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$ yields a conjugating matrix over $\mathbb{Z}_{(3)}$.
- A and B are not conjugate over $\mathbb{Z}$.

Theorem of Guralnick (1980): $A \sim_{\mathbb{Z}_{(p)}} B$ over for all prime ideals $p \iff A \sim B$ over some finite integral extension E of $\mathbb{Z}$.

Example:

- $f(x, y) = \det(xC_1 + yC_2) = -3x^2 - 2y^2$ realizes a unit over some extension.
- $f(i,1) = 1$ so $iC_1 + C_2 = \begin{pmatrix} -3i & 2 \\ 1 & i \end{pmatrix}$ conjugates A to B.

Failure of local-global principal

$A = \begin{pmatrix} 0 & -6 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 2 \\ -3 & 0 \end{pmatrix}$ have characteristic polynomial $c(x) = x^2 + 6$, with disc$(c) = -24$.

- A and B are conjugate over $\mathbb{Z}_{(p)}$ for $p \neq 2,3$.
- $C_1 = \begin{pmatrix} -3 & 0 \\ 0 & 1 \end{pmatrix}$ yields a conjugating matrix over $\mathbb{Z}_{(2)}$.
- $C_2 = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$ yields a conjugating matrix over $\mathbb{Z}_{(3)}$.
- A and B are not conjugate over $\mathbb{Z}$.

Theorem of Guralnick (1980): $A \sim_{\mathbb{Z}_{(p)}} B$ over for all prime ideals $p \iff A \sim B$ over some finite integral extension E of $\mathbb{Z}$.

I refer to the problem of determining the algebraic extension over which locally conjugate matrices are conjugate as the **conjugacy extension problem.**

Failure of local-global principal

$A = \begin{pmatrix} 0 & -6 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 2 \\ -3 & 0 \end{pmatrix}$ have characteristic polynomial $c(x) = x^2 + 6$, with disc$(c) = -24$.

- A and B are conjugate over $\mathbb{Z}_{(p)}$ for $p \neq 2,3$.
- $C_1 = \begin{pmatrix} -3 & 0 \\ 0 & 1 \end{pmatrix}$ yields a conjugating matrix over $\mathbb{Z}_{(2)}$.
- $C_2 = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$ yields a conjugating matrix over $\mathbb{Z}_{(3)}$.
- A and B are not conjugate over $\mathbb{Z}$.

Theorem of Guralnick (1980): $A \sim_{\mathbb{Z}_{(p)}} B$ over for all prime ideals $p \iff A \sim B$ over some finite integral extension E of $\mathbb{Z}$.

Example:

- $f(x, y) = \det(xC_1 + yC_2) = -3x^2 - 2y^2$ realizes a unit over some extension.
- $f(i,1) = 1$ so $iC_1 + C_2 = \begin{pmatrix} -3i & 2 \\ 1 & i \end{pmatrix}$ conjugates A to B.

Correspondence for an integral domain R

Correspondence for an integral domain R

- The Latimer and MacDuffee correspondence can be generalized to hold over any integral domain R.

Correspondence for an integral domain R

- The Latimer and MacDuffee correspondence can be generalized to hold over any integral domain R.

For $f = \prod_{i=1}^{m} f_i$, a **fractional** $R[\alpha]$**-ideal** is an $R[\alpha]$-module within $\prod_{i=1}^{m} \mathrm{Frac}(R)(\alpha_i)$ which is also a free R-module of rank $\deg(f)$.

Correspondence for an integral domain R

- The Latimer and MacDuffee correspondence can be generalized to hold over any integral domain R.
- Let $\mathscr{I}_{R[\alpha]}$ denote the set of fractional $R[\alpha]$-ideals.

Correspondence for an integral domain R

- The Latimer and MacDuffee correspondence can be generalized to hold over any integral domain R.
- Let $\mathscr{I}_{R[\alpha]}$ denote the set of fractional $R[\alpha]$-ideals.
- There is a bijection

$$\psi_R : \mathscr{M}_f / {\sim_R} \to \mathscr{I}_{R[\alpha]} / {\cong_{R[\alpha]}}$$

$$[A]_R \mapsto [I]_{R[\alpha]}$$

Correspondence for an integral domain R

- The Latimer and MacDuffee correspondence can be generalized to hold over any integral domain R.
- Let $\mathcal{I}_{R[\alpha]}$ denote the set of fractional $R[\alpha]$-ideals.
- There is a bijection
$$\psi_R : \mathcal{M}_f/_{\sim R} \to \mathcal{I}_{R[\alpha]}/_{\cong_{R[\alpha]}}$$
$$[A]_R \mapsto [I]_{R[\alpha]}$$
- For $A \in \mathbb{Z}^{n\times n}$ and $\mathbb{Z} \subseteq R$, we have that $\psi_R([A]) = R \otimes_{\mathbb{Z}} \psi_{\mathbb{Z}}([A])$.

Correspondence for an integral domain R

- The Latimer and MacDuffee correspondence can be generalized to hold over any integral domain R.
- Let $\mathcal{I}_{R[\alpha]}$ denote the set of fractional $R[\alpha]$-ideals.
- There is a bijection

$$\psi_R : \mathcal{M}_f/_{\sim R} \to \mathcal{I}_{R[\alpha]}/_{\cong_{R[\alpha]}}$$
$$[A]_R \mapsto [I]_{R[\alpha]}$$

If $[A]_{\sim\mathbb{Z}} \leftrightarrow [I] = [\bigoplus p_i(\alpha)\mathbb{Z}]$,
then
$[A]_{\sim R} \leftrightarrow [R \otimes I] = [\bigoplus p_i(\tilde{\alpha})R]$ where the form of $\tilde{\alpha}$ depends on the factorization of f in $R[x]$

Example: f factors further

Example: f factors further

Let $f = x^4 - 2$ and α be a root. Let $R = \mathbb{Z}[\sqrt[4]{2}]$. Over $R[x]$, we have that f factors as $f = (x^2 + \sqrt{2})(x - \sqrt[4]{2})(x + \sqrt[4]{2})$.

Example: f factors further

Let $f = x^4 - 2$ and α be a root. Let $R = \mathbb{Z}[\sqrt[4]{2}]$. Over $R[x]$, we have that f factors as $f = (x^2 + \sqrt{2})(x - \sqrt[4]{2})(x + \sqrt[4]{2})$.

Let α_1 denote a root of $x^2 + \sqrt{2}$.

Example: f factors further

Let $f = x^4 - 2$ and α be a root. Let $R = \mathbb{Z}[\sqrt[4]{2}]$. Over $R[x]$, we have that f factors as $f = (x^2 + \sqrt{2})(x - \sqrt[4]{2})(x + \sqrt[4]{2})$.

Let α_1 denote a root of $x^2 + \sqrt{2}$.

$[C_f]_{\mathbb{Z}} \leftrightarrow [\mathbb{Z}[\alpha]]_{\mathbb{Z}[\alpha]} = [1\mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \alpha^2\mathbb{Z} \oplus \alpha^3\mathbb{Z}]_{\mathbb{Z}[\alpha]}$ while

$[C_f]_R \leftrightarrow [R \otimes_{\mathbb{Z}} \mathbb{Z}[\alpha]]_{R[\alpha]}$

Example: f factors further

Let $f = x^4 - 2$ and α be a root. Let $R = \mathbb{Z}[\sqrt[4]{2}]$. Over $R[x]$, we have that f factors as $f = (x^2 + \sqrt{2})(x - \sqrt[4]{2})(x + \sqrt[4]{2})$.

Let α_1 denote a root of $x^2 + \sqrt{2}$.

$[C_f]_{\mathbb{Z}} \leftrightarrow [\mathbb{Z}[\alpha]]_{\mathbb{Z}[\alpha]} = [1\mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \alpha^2\mathbb{Z} \oplus \alpha^3\mathbb{Z}]_{\mathbb{Z}[\alpha]}$ while
$[C_f]_R \leftrightarrow [R \otimes_{\mathbb{Z}} \mathbb{Z}[\alpha]]_{R[\alpha]}$

Example: f factors further

Let $f = x^4 - 2$ and α be a root. Let $R = \mathbb{Z}[\sqrt[4]{2}]$. Over $R[x]$, we have that f factors as $f = (x^2 + \sqrt{2})(x - \sqrt[4]{2})(x + \sqrt[4]{2})$.

Let α_1 denote a root of $x^2 + \sqrt{2}$.

$[C_f]_{\mathbb{Z}} \leftrightarrow [\mathbb{Z}[\alpha]]_{\mathbb{Z}[\alpha]} = [1\mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \alpha^2\mathbb{Z} \oplus \alpha^3\mathbb{Z}]_{\mathbb{Z}[\alpha]}$ while

$$[C_f]_R \leftrightarrow [R \otimes_{\mathbb{Z}} \mathbb{Z}[\alpha]]_{R[\alpha]}$$
$$= [(1,1,1)R \oplus (\alpha_1, \sqrt[4]{2}, -\sqrt[4]{2})R \oplus \ldots \oplus (\alpha_1^3, \sqrt[4]{2}^3, -\sqrt[4]{2}^3)R]_{R[\alpha]}$$

Algorithm if $R \supseteq \mathbb{Z}$

Input: Integral matrices A and B and a ring R.

Tests if $A \sim_R B$ and if yes, returns $C \in \mathrm{GL}_n(R)$ with $C^{-1}AC = B$.

Algorithm if $R \supseteq \mathbb{Z}$

Input: Integral matrices A and B and a ring R.

Tests if $A \sim_R B$ and if yes, returns $C \in \mathrm{GL}_n(R)$ with $C^{-1}AC = B$.

- Step 1: From A and B, find $R \otimes I$ and $R \otimes J$.

Algorithm if $R \supseteq \mathbb{Z}$

Let $f = x^2 + 23$, $K := \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f)$,
$L := \mathbb{Q}[x]/(x^3 + 6x^2 + 9x - 23)$ and $R = \mathcal{O}_L$.

- Step 1: From A and B, find $R \otimes I$ and $R \otimes J$.

Algorithm if $R \supseteq \mathbb{Z}$

Let $f = x^2 + 23$, $K := \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f)$,
$L := \mathbb{Q}[x]/(x^3 + 6x^2 + 9x - 23)$ and $R = \mathcal{O}_L$.

- Step 1: From A and B, find $R \otimes I$ and $R \otimes J$.

$$A := \begin{pmatrix} -1 & 2 \\ -12 & 1 \end{pmatrix} \leftrightarrow R \otimes I := 2R \oplus (1+\alpha)R$$

and

$$B := \begin{pmatrix} 1 & 4 \\ -6 & -1 \end{pmatrix} \leftrightarrow R \otimes J := 4R \oplus (-1+\alpha)R$$

Algorithm if $\mathbb{Z} \subseteq R$

Let $f = x^2 + 23$, $K := \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f)$,
$L := \mathbb{Q}[x]/(x^3 + 6x^2 + 9x - 23)$ and $R = \mathcal{O}_L$.

- Step 1: From A and B, find $R \otimes I$ and $R \otimes J$.
- Step 2: Find multiplicator ring of $R \otimes I$ and $R \otimes J$. If not the same, $A \nsim_R B$.

Algorithm if $\mathbb{Z} \subseteq R$

Let $f = x^2 + 23$, $K := \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f)$,
$L := \mathbb{Q}[x]/(x^3 + 6x^2 + 9x - 23)$ and $R = \mathcal{O}_L$.

- Step 1: From A and B, find $R \otimes I$ and $R \otimes J$.
- Step 2: Find multiplicator ring of $R \otimes I$ and $R \otimes J$. If not the same, $A \nsim_R B$.

$$\mathcal{O}_K = (I : I) = (J : J)$$

$$\mathcal{O} := (R \otimes I : R \otimes I) = R \otimes (I : I)$$

$$= 1R \oplus \left(\frac{1+\alpha}{2}\right) R$$

Algorithm if $\mathbb{Z} \subseteq R$

Let $f = x^2 + 23$, $K := \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f)$,
$L := \mathbb{Q}[x]/(x^3 + 6x^2 + 9x - 23)$ and $R = \mathcal{O}_L$.

- Step 1: From A and B, find $R \otimes I$ and $R \otimes J$.
- Step 2: Find multiplicator ring of $R \otimes I$ and $R \otimes J$. If not the same, $A \nsim_R B$.

$$\mathcal{O}_K = (I : I) = (J : J)$$

$$\mathcal{O} := (R \otimes I : R \otimes I) = R \otimes (I : I)$$

$$= 1R \oplus \left(\frac{1+\alpha}{2}\right) R$$

Note: A and B are locally conjugate iff $\mathbb{Z}_{(p)} \otimes I \cong_{\mathbb{Z}_{(p)}[\alpha]} \mathbb{Z}_{(p)} \otimes J$ iff $(I : I) = (J : J)$.

Algorithm if $\mathbb{Z} \subseteq R$

Let $f = x^2 + 23$, $K := \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f)$,
$L := \mathbb{Q}[x]/(x^3 + 6x^2 + 9x - 23)$ and $R = \mathcal{O}_L$.

- Step 1: From A and B, find $R \otimes I$ and $R \otimes J$.
- Step 2: Find multiplicator ring of $R \otimes I$ and $R \otimes J$. If not the same, $A \nsim_R B$.
- Step 3: Test if $R \otimes (I : J)$ principal. If not, $A \nsim_R B$. Otherwise, compute change of basis.

Algorithm if $\mathbb{Z} \subseteq R$

Let $f = x^2 + 23$, $K := \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f)$,
$L := \mathbb{Q}[x]/(x^3 + 6x^2 + 9x - 23)$ and $R = \mathcal{O}_L$.

- Step 1: From A and B, find $R \otimes I$ and $R \otimes J$.
- Step 2: Find multiplicator ring of $R \otimes I$ and $R \otimes J$. If not the same, $A \nsim_R B$.
- Step 3: Test if $R \otimes (I : J)$ principal. If not, $A \nsim_R B$. Otherwise, compute change of basis.

In $\mathcal{O}$, $R \otimes (I : J) = (\gamma)$.

Algorithm if $\mathbb{Z} \subseteq R$

Let $f = x^2 + 23$, $K := \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f)$,
$L := \mathbb{Q}[x]/(x^3 + 6x^2 + 9x - 23)$ and $R = \mathcal{O}_L$.

- Step 1: From A and B, find $R \otimes I$ and $R \otimes J$.
- Step 2: Find multiplicator ring of $R \otimes I$ and $R \otimes J$. If not the same, $A \nsim_R B$.
- Step 3: Test if $R \otimes (I : J)$ principal. If not, $A \nsim_R B$. Otherwise, compute change of basis.

In $\mathcal{O}$, $R \otimes (I : J) = (\gamma)$.

Then $R \otimes I = \gamma(R \otimes J)$. So $R \otimes I$ has R-bases

$\{2, 1 + \alpha\}$ and $\{4\gamma, \gamma(-1 + \alpha)\}$.

Algorithm if $\mathbb{Z} \subseteq R$

Let $f = x^2 + 23$, $K := \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f)$,
$L := \mathbb{Q}[x]/(x^3 + 6x^2 + 9x - 23)$ and $R = \mathcal{O}_L$.

- Step 1: From A and B, find $R \otimes I$ and $R \otimes J$.
- Step 2: Find multiplicator ring of $R \otimes I$ and $R \otimes J$. If not the same, $A \nsim_R B$.
- Step 3: Test if $R \otimes (I : J)$ principal. If not, $A \nsim_R B$. Otherwise, compute change of basis.

For a particular $\mathbb{Z}$-basis $\{\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3\}$of R, we find that

$$C = \begin{pmatrix} -\mathcal{B}_1 + \mathcal{B}_3 & -\mathcal{B}_1 - \mathcal{B}_2 \\ 2\mathcal{B}_1 + 3\mathcal{B}_2 + \mathcal{B}_3 & -2\mathcal{B}_1 + 2\mathcal{B}_3 \end{pmatrix}$$

has determinant in $R^\times$ and conjugates A to B.

Implementation of Algorithm

Implementation of Algorithm

- Implemented algorithm for $R = \mathcal{O}_L$ and for matrices in $\mathscr{M}_f$ with f irreducible using subroutine IsPrincipal in Magma.

Implementation of Algorithm

- Implemented algorithm for $R = \mathcal{O}_L$ and for matrices in $\mathcal{M}_f$ with f irreducible using subroutine IsPrincipal in Magma.

- IsPrincipal is not valid for objects within a Frac(R)-algebra of the form $\prod_{i=1}^{m}$ Frac$(R)(\alpha_i)$ unless $R = \mathbb{Z}$ (or $m = 1$).

Hilbert Class Fields

Hilbert Class Fields

- The **Hilbert class field** of a number field K, denoted HCF(K), is the maximal unramified abelian extension of K.

Hilbert Class Fields

- The **Hilbert class field** of a number field K, denoted HCF(K), is the maximal unramified abelian extension of K.

- **Principal ideal theorem:** Let L denote the Hilbert class field of K. Every fractional $\mathcal{O}_K$-ideal is principal in $\mathcal{O}_L$.

Hilbert Class Fields

- The **Hilbert class field** of a number field K, denoted HCF(K), is the maximal unramified abelian extension of K.

- **Principal ideal theorem:** Let L denote the Hilbert class field of K. Every fractional $\mathcal{O}_K$-ideal is principal in $\mathcal{O}_L$.

- $\mathscr{M}_f \Rightarrow K := \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f) \Rightarrow L = \text{HCF}(K)$

Hilbert Class Fields

- The **Hilbert class field** of a number field K, denoted HCF(K), is the maximal unramified abelian extension of K.

- **Principal ideal theorem:** Let L denote the Hilbert class field of K. Every fractional $\mathcal{O}_K$-ideal is principal in $\mathcal{O}_L$.

- $\mathscr{M}_f \Rightarrow K := \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f) \Rightarrow L =$ HCF(K)

- However, since $\alpha \in \mathcal{O}_L$, f factors further over $\mathcal{O}_L[x]$.

Hilbert class field does not always solve the conjugacy extension problem

Let $f = x^2 + 5$ and $K = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$.

$$A = \begin{pmatrix} -1 & 2 \\ -3 & 1 \end{pmatrix} \leftrightarrow I = 2\mathbb{Z} \oplus (\alpha + 1)\mathbb{Z} \text{ (not principal)}$$

Hilbert class field does not always solve the conjugacy extension problem

Let $f = x^2 + 5$ and $K = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$.

$$A = \begin{pmatrix} -1 & 2 \\ -3 & 1 \end{pmatrix} \leftrightarrow I = 2\mathbb{Z} \oplus (\alpha + 1)\mathbb{Z} \text{ (not principal)}$$

- Let L denote the Hilbert class field of K and $R = \mathcal{O}_L$. The R-conjugacy class of A corresponds to $R \otimes I = (2,2)R \oplus (\alpha + 1, -\alpha + 1)R$.

Hilbert class field does not always solve the conjugacy extension problem

Let $f = x^2 + 5$ and $K = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$.

$$A = \begin{pmatrix} -1 & 2 \\ -3 & 1 \end{pmatrix} \leftrightarrow I = 2\mathbb{Z} \oplus (\alpha + 1)\mathbb{Z} \text{ (not principal)}$$

- Let L denote the Hilbert class field of K and $R = \mathcal{O}_L$. The R-conjugacy class of A corresponds to $R \otimes I = (2{,}2)R \oplus (\alpha + 1, -\alpha + 1)R$.
- Letting $\{\mathcal{B}_1, \ldots, \mathcal{B}_4\}$ denote a $\mathbb{Z}$-basis for R, we have $2R \oplus (\alpha + 1)R = 2R \oplus (-\alpha + 1)R = (g)$ where $g = \mathcal{B}_1 - 2\mathcal{B}_1 - \mathcal{B}_4$.

Hilbert class field does not always solve the conjugacy extension problem

Hilbert class field does not always solve the conjugacy extension problem

If $R \otimes I = (\gamma_1, \gamma_2)R[(\alpha, -\alpha)]$ for a generator $(\gamma_1, \gamma_2) \in L(\alpha) \times L(-\alpha) = L \times L$, there are $(r_i, r_i) \in R$ with

Hilbert class field does not always solve the conjugacy extension problem

If $R \otimes I = (\gamma_1, \gamma_2)R[(\alpha, -\alpha)]$ for a generator $(\gamma_1, \gamma_2) \in L(\alpha) \times L(-\alpha) = L \times L$, there are $(r_i, r_i) \in R$ with

$$(2,2)(r_1, r_1) + (\alpha + 1, -\alpha + 1)(r_2, r_2) = (\gamma_1, \gamma_2)$$
$$(2,2)(r_3, r_3) + (\alpha + 1, -\alpha + 1)(r_4, r_4) = (\gamma_1 \alpha, -\gamma_2 \alpha)$$

Hilbert class field does not always solve the conjugacy extension problem

If $R \otimes I = (\gamma_1, \gamma_2)R[(\alpha, -\alpha)]$ for a generator $(\gamma_1, \gamma_2) \in L(\alpha) \times L(-\alpha) = L \times L$, there are $(r_i, r_i) \in R$ with

$$(2,2)(r_1, r_1) + (\alpha + 1, -\alpha + 1)(r_2, r_2) = (\gamma_1, \gamma_2)$$

$$(2,2)(r_3, r_3) + (\alpha + 1, -\alpha + 1)(r_4, r_4) = (\gamma_1 \alpha, -\gamma_2 \alpha)$$

Hilbert class field does not always solve the conjugacy extension problem

If $R \otimes I = (\gamma_1, \gamma_2)R[(\alpha, -\alpha)]$ for a generator $(\gamma_1, \gamma_2) \in L(\alpha) \times L(-\alpha) = L \times L$, there are $(r_i, r_i) \in R$ with

$$(2,2)(r_1, r_1) + (\alpha + 1, -\alpha + 1)(r_2, r_2) = (\gamma_1, \gamma_2)$$
$$(2,2)(r_3, r_3) + (\alpha + 1, -\alpha + 1)(r_4, r_4) = (\gamma_1 \alpha, -\gamma_2 \alpha)$$

Hilbert class field does not always solve the conjugacy extension problem

If $R \otimes I = (\gamma_1, \gamma_2)R[(\alpha, -\alpha)]$ for a generator $(\gamma_1, \gamma_2) \in L(\alpha) \times L(-\alpha) = L \times L$, there are $(r_i, r_i) \in R$ with

$$(2,2)(r_1, r_1) + (\alpha + 1, -\alpha + 1)(r_2, r_2) = (\gamma_1, \gamma_2)$$
$$(2,2)(r_3, r_3) + (\alpha + 1, -\alpha + 1)(r_4, r_4) = (\gamma_1\alpha, -\gamma_2\alpha)$$

(change of basis also must have unit determinant)

Hilbert class field does not always solve the conjugacy extension problem

If $R \otimes I = (\gamma_1, \gamma_2)R[(\alpha, -\alpha)]$ for a generator $(\gamma_1, \gamma_2) \in L(\alpha) \times L(-\alpha) = L \times L$, there are $(r_i, r_i) \in R$ with

$$(2,2)(r_1, r_1) + (\alpha + 1, -\alpha + 1)(r_2, r_2) = (\gamma_1, \gamma_2)$$

$$(2,2)(r_3, r_3) + (\alpha + 1, -\alpha + 1)(r_4, r_4) = (\gamma_1 \alpha, -\gamma_2 \alpha)$$

Hilbert class field does not always solve the conjugacy extension problem

If $R \otimes I = (\gamma_1, \gamma_2)R[(\alpha, -\alpha)]$ for a generator $(\gamma_1, \gamma_2) \in L(\alpha) \times L(-\alpha) = L \times L$, there are $(r_i, r_i) \in R$ with

$$(2,2)(r_1, r_1) + (\alpha + 1, -\alpha + 1)(r_2, r_2) = (\gamma_1, \gamma_2)$$

$$(2,2)(r_3, r_3) + (\alpha + 1, -\alpha + 1)(r_4, r_4) = (\gamma_1 \alpha, -\gamma_2 \alpha)$$

Hilbert class field does not always solve the conjugacy extension problem

$2R \oplus (\alpha + 1)R = 2R \oplus (-\alpha + 1)R = (g)$ where
$g = \mathscr{B}_1 - 2\mathscr{B}_1 - \mathscr{B}_4$.

We may assume $\gamma_1 = g$ and $\gamma_2 = gu$ for some $u \in R^\times$.

Hilbert class field does not always solve the conjugacy extension problem

$2R \oplus (\alpha + 1)R = 2R \oplus (-\alpha + 1)R = (g)$ where

$g = \mathscr{B}_1 - 2\mathscr{B}_1 - \mathscr{B}_4$.

We may assume $\gamma_1 = g$ and $\gamma_2 = gu$ for some $u \in R^\times$.

There is no unit u so that there is a solution over R to

Hilbert class field does not always solve the conjugacy extension problem

$2R \oplus (\alpha+1)R = 2R \oplus (-\alpha+1)R = (g)$ where

$g = \mathscr{B}_1 - 2\mathscr{B}_1 - \mathscr{B}_4$.

We may assume $\gamma_1 = g$ and $\gamma_2 = gu$ for some $u \in R^\times$.

There is no unit u so that there is a solution over R to

$$(2,2)(r_1, r_1) + (\alpha+1, -\alpha+1)(r_2, r_2) = (g, gu)$$
$$(2,2)(r_3, r_3) + (\alpha+1, -\alpha+1)(r_4, r_4) = (g\alpha, -gu\alpha)^{.}$$

Hilbert class field does not always solve the conjugacy extension problem

$2R \oplus (\alpha+1)R = 2R \oplus (-\alpha+1)R = (g)$ where
$g = \mathscr{B}_1 - 2\mathscr{B}_1 - \mathscr{B}_4$.

We may assume $\gamma_1 = g$ and $\gamma_2 = gu$ for some $u \in R^\times$.
There is no unit u so that there is a solution over R to

$$(2,2)(r_1, r_1) + (\alpha+1, -\alpha+1)(r_2, r_2) = (g, gu)$$
$$(2,2)(r_3, r_3) + (\alpha+1, -\alpha+1)(r_4, r_4) = (g\alpha, -gu\alpha).$$

Then $(2,2)R \oplus (\alpha+1, -\alpha+1)R$ is not principal and so $A \nsim_R C_f$ for R the ring of integers of the Hilbert class field of K.

Subfields of the Hilbert class field

Subfields of the Hilbert class field

To avoid the difficulty that arises when f factors further, we instead test whether there is R, the ring of integers of a subfield of the Hilbert class field, such that:

Subfields of the Hilbert class field

To avoid the difficulty that arises when f factors further, we instead test whether there is R, the ring of integers of a subfield of the Hilbert class field, such that:

- f is irreducible in $R[x]$

Subfields of the Hilbert class field

To avoid the difficulty that arises when f factors further, we instead test whether there is R, the ring of integers of a subfield of the Hilbert class field, such that:

- f is irreducible in $R[x]$
- $(I : J)$ is principal in R

Subfields of the Hilbert class field

f	$\text{disc}(f)$	h_K	A	$A \sim C_f$ over subfield of HCF?
$x^2 - x + 4$	$-3 \cdot 5$	2	$\begin{pmatrix} -1 & 2 \\ -3 & 2 \end{pmatrix}$	$x^2 + 2x + 4$
$x^2 + 5$	$-2^2 \cdot 5$	2	$\begin{pmatrix} -1 & 2 \\ -3 & 1 \end{pmatrix}$	No
$x^2 + 10$	$-2^3 \cdot 5$	2	$\begin{pmatrix} 0 & 2 \\ -5 & 0 \end{pmatrix}$	$x^2 + 2$
$x^2 - x + 13$	$-3 \cdot 17$	2	$\begin{pmatrix} -1 & 3 \\ -5 & 2 \end{pmatrix}$	$x^2 + 8x + 19$
$x^2 + 13$	$-2^2 \cdot 13$	2	$\begin{pmatrix} -1 & 2 \\ -7 & 1 \end{pmatrix}$	No
$x^2 - x + 6$	-23	3	$\begin{pmatrix} 0 & 2 \\ -3 & 1 \end{pmatrix}$	$x^3 + 6x^2 + 9x - 23$
$x^2 - x + 8$	-31	3	$\begin{pmatrix} -1 & 2 \\ -5 & 2 \end{pmatrix}$	No
$x^2 + 17$	$-2^2 \cdot 17$	4	$\begin{pmatrix} -2 & 3 \\ -7 & 2 \end{pmatrix}$	No
$x^2 + 21$	$-2^2 \cdot 3 \cdot 7$	4	$\begin{pmatrix} -2 & 5 \\ -5 & 2 \end{pmatrix}$	Yes

Subfields of the Hilbert class field

f	$\text{disc}(f)$	h_K	A	$A \sim C_f$ over subfield of HCF?
$x^2 - x + 4$	$-3 \cdot 5$	2	$\begin{pmatrix} -1 & 2 \\ -3 & 2 \end{pmatrix}$	$x^2 + 2x + 4$
$x^2 + 5$	$-2^2 \cdot 5$	2	$\begin{pmatrix} -1 & 2 \\ -3 & 1 \end{pmatrix}$	No
$x^2 + 10$	$-2^3 \cdot 5$	2	$\begin{pmatrix} 0 & 2 \\ -5 & 0 \end{pmatrix}$	$^2 + 2$
$x^2 - x + 13$	$-3 \cdot 17$	2	$\begin{pmatrix} -1 & 3 \\ -5 & 2 \end{pmatrix}$	$x^2 + 8x + 19$
$x^2 + 13$	$-2^2 \cdot 13$	2	$\begin{pmatrix} -1 & 2 \\ -7 & 1 \end{pmatrix}$	No
$x^2 - x + 6$	-23	3	$\begin{pmatrix} 0 & 2 \\ -3 & 1 \end{pmatrix}$	$x^3 + 6x^2 + 9x - 23$
$x^2 - x + 8$	-31	3	$\begin{pmatrix} -1 & 2 \\ -5 & 2 \end{pmatrix}$	No
$x^2 + 17$	$-2^2 \cdot 17$	4	$\begin{pmatrix} -2 & 3 \\ -7 & 2 \end{pmatrix}$	No
$x^2 + 21$	$-2^2 \cdot 3 \cdot 7$	4	$\begin{pmatrix} -2 & 5 \\ -5 & 2 \end{pmatrix}$	Yes

A is chosen to correspond to a non-principal $\mathbb{Z}[\alpha]$-ideal

Subfields of the Hilbert class field

f	$\mathrm{disc}(f)$	h_K	A	$A \sim \mathcal{C}_f$ over subfield of HCF?
$x^2 - x + 4$	$-3 \cdot 5$	2	$\begin{pmatrix} -1 & 2 \\ -3 & 2 \end{pmatrix}$	$x^2 + 2x + 4$
$x^2 + 5$	$-2^2 \cdot 5$	2	$\begin{pmatrix} -1 & 2 \\ -3 & 1 \end{pmatrix}$	No
$x^2 + 10$	$-2^3 \cdot 5$	2	$\begin{pmatrix} 0 & 2 \\ -5 & 0 \end{pmatrix}$	$x^2 + 2$
$x^2 - x + 13$	$-3 \cdot 17$	2	$\begin{pmatrix} -1 & 3 \\ -5 & 2 \end{pmatrix}$	$x^2 + 8x + 19$
$x^2 + 13$	$-2^2 \cdot 13$	2	$\begin{pmatrix} -1 & 2 \\ -7 & 1 \end{pmatrix}$	No
$x^2 - x + 6$	-23	3	$\begin{pmatrix} 0 & 2 \\ -3 & 1 \end{pmatrix}$	$x^3 + 6x^2 + 9x - 23$
$x^2 - x + 8$	-31	3	$\begin{pmatrix} -1 & 2 \\ -5 & 2 \end{pmatrix}$	No
$x^2 + 17$	$-2^2 \cdot 17$	4	$\begin{pmatrix} -2 & 3 \\ -7 & 2 \end{pmatrix}$	No
$x^2 + 21$	$-2^2 \cdot 3 \cdot 7$	4	$\begin{pmatrix} -2 & 5 \\ -5 & 2 \end{pmatrix}$	Yes

Subfields of the Hilbert class field

f	$\mathrm{disc}(f)$	h_K	A	$A \sim \mathcal{C}_f$ over subfield of HCF?
$x^2 - x + 4$	$-3 \cdot 5$	2	$\begin{pmatrix} -1 & 2 \\ -3 & 2 \end{pmatrix}$	$x^2 + 2x + 4$
$x^2 + 5$	$-2^2 \cdot 5$	2	[illegible]	No
$x^2 + 10$	$-2^3 \cdot 5$	2	[illegible]	[illegible] $^2 + 2$
$x^2 - x + 13$	$-3 \cdot 17$	2	[illegible]	[illegible] $8x + 19$
$x^2 + 13$	$-2^2 \cdot 13$	2	$\begin{pmatrix} -1 & 2 \\ -7 & 1 \end{pmatrix}$	No
$x^2 - x + 6$	-23	3	$\begin{pmatrix} 0 & 2 \\ -3 & 1 \end{pmatrix}$	$x^3 + 6x^2 + 9x - 23$
$x^2 - x + 8$	-31	3	$\begin{pmatrix} -1 & 2 \\ -5 & 2 \end{pmatrix}$	No
$x^2 + 17$	$-2^2 \cdot 17$	4	$\begin{pmatrix} -2 & 3 \\ -7 & 2 \end{pmatrix}$	No
$x^2 + 21$	$-2^2 \cdot 3 \cdot 7$	4	$\begin{pmatrix} -2 & 5 \\ -5 & 2 \end{pmatrix}$	Yes

$A \sim_R C_f$ for R the ring of integers of $L = \mathbb{Q}[x]/(x^2 + 2x + 4)$

Subfields of the Hilbert class field

f	$\mathrm{disc}(f)$	h_K	A	$A \sim C_f$ over subfield of HCF?
$x^2 - x + 4$	$-3 \cdot 5$	2	$\begin{pmatrix} -1 & 2 \\ -3 & 2 \end{pmatrix}$	$x^2 + 2x + 4$
$x^2 + 5$	$-2^2 \cdot 5$	2	$\begin{pmatrix} -1 & 2 \\ -3 & 1 \end{pmatrix}$	No
$x^2 + 10$	$-2^3 \cdot 5$	2	$\begin{pmatrix} 0 & 2 \\ -5 & 0 \end{pmatrix}$	$x^2 + 2$
$x^2 - x + 13$	$-3 \cdot 17$	2	$\begin{pmatrix} -1 & 3 \\ -5 & 2 \end{pmatrix}$	$x^2 + 8x + 19$
$x^2 + 13$	$-2^2 \cdot 13$	2	$\begin{pmatrix} -1 & 2 \\ -7 & 1 \end{pmatrix}$	No
$x^2 - x + 6$	-23	3	$\begin{pmatrix} 0 & 2 \\ -3 & 1 \end{pmatrix}$	$x^3 + 6x^2 + 9x - 23$
$x^2 - x + 8$	-31	3	$\begin{pmatrix} -1 & 2 \\ -5 & 2 \end{pmatrix}$	No
$x^2 + 17$	$-2^2 \cdot 17$	4	$\begin{pmatrix} -2 & 3 \\ -7 & 2 \end{pmatrix}$	No
$x^2 + 21$	$-2^2 \cdot 3 \cdot 7$	4	$\begin{pmatrix} -2 & 5 \\ -5 & 2 \end{pmatrix}$	Yes

Example: Generalized method

Let $f = x^2 + 5$ and $K = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$.

$$A = \begin{pmatrix} -1 & 2 \\ -3 & 1 \end{pmatrix} \leftrightarrow I = 2\mathbb{Z} \oplus (\alpha + 1)\mathbb{Z} \text{ (not principal)}$$

Example: Generalized method

Let $f = x^2 + 5$ and $K = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$.

$$A = \begin{pmatrix} -1 & 2 \\ -3 & 1 \end{pmatrix} \leftrightarrow I = 2\mathbb{Z} \oplus (\alpha + 1)\mathbb{Z} \text{ (not principal)}$$

- We want $(I : \mathbb{Z}[\alpha]) = I$ to be principal.

Example: Generalized method

Let $f = x^2 + 5$ and $K = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$.

$$A = \begin{pmatrix} -1 & 2 \\ -3 & 1 \end{pmatrix} \leftrightarrow I = 2\mathbb{Z} \oplus (\alpha + 1)\mathbb{Z} \text{ (not principal)}$$

- We want $(I : \mathbb{Z}[\alpha]) = I$ to be principal.
- The ray class field L (ramifies at 3, which is relatively prime to I) has degree 8 over $\mathbb{Q}$.

Example: Generalized method

Let $f = x^2 + 5$ and $K = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$.

$$A = \begin{pmatrix} -1 & 2 \\ -3 & 1 \end{pmatrix} \leftrightarrow I = 2\mathbb{Z} \oplus (\alpha + 1)\mathbb{Z} \text{ (not principal)}$$

- We want $(I : \mathbb{Z}[\alpha]) = I$ to be principal.
- The ray class field L (ramifies at 3, which is relatively prime to I) has degree 8 over $\mathbb{Q}$.
- The subfield $F := \mathbb{Q}[x]/(x^4 - 12x^3 + 158x^2 + 228x + 3721)$ of L satisfies the desired properties.

Example: Generalized method

Let $f = x^2 + 5$ and $K = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$.

$$A = \begin{pmatrix} -1 & 2 \\ -3 & 1 \end{pmatrix} \leftrightarrow I = 2\mathbb{Z} \oplus (\alpha + 1)\mathbb{Z} \text{ (not principal)}$$

- We want $(I : \mathbb{Z}[\alpha]) = I$ to be principal.
- The ray class field L (ramifies at 3, which is relatively prime to I) has degree 8 over $\mathbb{Q}$.
- The subfield $F := \mathbb{Q}[x]/(x^4 - 12x^3 + 158x^2 + 228x + 3721)$ of L satisfies the desired properties.
- $C = \begin{pmatrix} -\mathscr{B}_2 & -1 - \mathscr{B}_4 \\ 3 + \mathscr{B}_2 + 3\mathscr{B}_4 & -1 - 2\mathscr{B}_2 - 2\mathscr{B}_3 - \mathscr{B}_4 \end{pmatrix}$ is a matrix in $\mathrm{GL}_2(\mathscr{O}_F)$ which conjugates $\mathscr{C}_f$ to A.

Open problems

Open problems

- Is there a way to implement the algorithm to test for $\mathrm{GL}_n(R)$-conjugacy in the non-irreducible case? Need an algorithm that determines whether an ideal in $\prod_{i=1}^{m} \mathrm{Frac}(R)(\alpha_i)$ (as a $\mathrm{Frac}(R)$-algebra) is principal.

Open problems

- Is there a way to implement the algorithm to test for $\mathrm{GL}_n(R)$-conjugacy in the non-irreducible case? Need an algorithm that determines whether an ideal in $\prod_{i=1}^{m} \mathrm{Frac}(R)(\alpha_i)$ (as a $\mathrm{Frac}(R)$-algebra) is principal.

- How often does the method of searching through class fields succeed? Is there a nice classification for the cases in which the method works?

Open problems

- Is there a way to implement the algorithm to test for $\mathrm{GL}_n(R)$-conjugacy in the non-irreducible case? Need an algorithm that determines whether an ideal in $\prod_{i=1}^{m} \mathrm{Frac}(R)(\alpha_i)$ (as a $\mathrm{Frac}(R)$-algebra) is principal.

- How often does the method of searching through class fields succeed? Is there a nice classification for the cases in which the method works?

- Should we consider ray class fields which ramify at primes related to the discriminant of f?