Constructing Monogenic Fields of Cryptographic Size

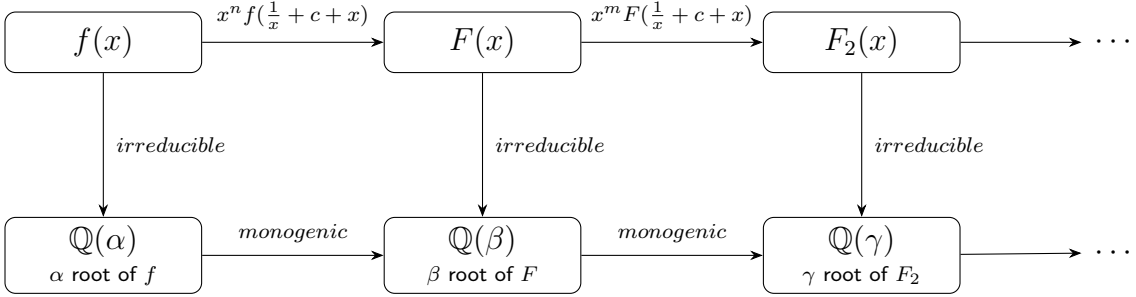
Part 3

Swechchha Adhikari

Department of Mathematics
Brigham Young University

July 6, 2026

The Big Picture



Ring of Integers

Take $f = x^2 - 2$, so $\mathbb{Q}[x]/(f) = \mathbb{Q}(\sqrt{2})$

$$\mathcal{O}_{\mathbb{Q}(\sqrt{2})} = \mathbb{Z}[\sqrt{2}]$$
$$\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$$

$\mathcal{O}_K =$ the set of all roots of monic polynomials over $\mathbb{Z}$

Monogenic Number Fields

$$\mathcal{O}_{\mathbb{Q}(\sqrt{2})} = \mathbb{Z}[\sqrt{2}]$$

$$\mathcal{O}_{\mathbb{Q}(\sqrt{5},\sqrt{13})} = \mathbb{Z}\left[\tfrac{1+\sqrt{5}}{2}, \tfrac{1+\sqrt{13}}{2}\right]$$

Which *number field* is monogenic?

- $\mathcal{O}_K$ generated by a single element

Checking Monogenicity

Option 1:

- Compute the ring of integers
- Check if it's generated by a single element

Checking Monogenicity

Option 1:

- Compute the ring of integers
- Check if it's generated by a single element

Generally very difficult to check

Checking Monogenicity

Option 2:

- Compute $\frac{\operatorname{disc} f}{\operatorname{disc} K} = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2$
- If this ratio equals 1, $\mathbb{Z}[\alpha] = \mathcal{O}_K$

Discriminant of the Transformed Polynomial

Let $f = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0$ be monic, then

$$\operatorname{disc}(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2$$

Discriminant of the Transformed Polynomial

Let $f = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0$ be monic, then

$$\operatorname{disc}(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2$$

Roots of F?

Discriminant of the Transformed Polynomial

Lemma (Adhikari, McKean, Plott, Torgersen '26)

Let α be a root of $f(x)$. Then the corresponding roots of $F(x)$ are

$$\frac{(\alpha - c) \pm \sqrt{(\alpha - c)^2 - 4}}{2}$$

- Write $f(x) = \prod_i (x - \alpha_i)$
- Apply the transformation to each root

Discriminant of the Transformed Polynomial

Roots of $F(x)$:

$$\frac{(\alpha - c) \pm \sqrt{(\alpha - c)^2 - 4}}{2}.$$

Discriminant of the Transformed Polynomial

Roots of $F(x)$:

$$\frac{(\alpha - c) \pm \sqrt{(\alpha - c)^2 - 4}}{2}.$$

- Plug the roots of $F(x)$ into the discriminant formula

Discriminant of the Transformed Polynomial

Roots of $F(x)$:

$$\frac{(\alpha - c) \pm \sqrt{(\alpha - c)^2 - 4}}{2}.$$

- Plug the roots of $F(x)$ into the discriminant formula
- Treat $+$ and $-$ roots separately

Discriminant of the Transformed Polynomial

Roots of $F(x)$:

$$\frac{(\alpha - c) \pm \sqrt{(\alpha - c)^2 - 4}}{2}.$$

- Plug the roots of $F(x)$ into the discriminant formula
- Treat $+$ and $-$ roots separately
- Collect all terms

Discriminant of the Transformed Polynomial

Roots of $F(x)$:

$$\frac{(\alpha - c) \pm \sqrt{(\alpha - c)^2 - 4}}{2}.$$

Discriminant of $F(x)$:

Proposition (Adhikari, McKean, Plott, Torgersen '26)

$$\operatorname{disc}(F) \;=\; \operatorname{disc}(f)^2 \cdot \prod_{i=1}^{n} \big((\alpha_i - c)^2 - 4\big),$$

where $\alpha_1, \ldots, \alpha_n$ are the roots of $f(x)$.

Discriminant Simplification

$$\begin{aligned}\operatorname{disc}(F) &= \operatorname{disc}(f)^2 \cdot \prod_{i=1}^{n} \left((\alpha_i - c)^2 - 4\right) \\ &= \operatorname{disc}(f)^2 \cdot \prod_{i=1}^{n} (\alpha_i - c - 2)(\alpha_i - c + 2) \\ &= \operatorname{disc}(f)^2 \, f(c+2) \, f(c-2)\end{aligned}$$

Discriminant of K

Recall:

$$\frac{\operatorname{disc} f}{\operatorname{disc} K} = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2$$

Discriminant of K

Recall:

$$\frac{\operatorname{disc} f}{\operatorname{disc} K} = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2$$

Discriminant of the number field K?

Discriminant of K

Recall:

$$\frac{\operatorname{disc} f}{\operatorname{disc} K} = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2$$

Discriminant of the number field K?

Generally very difficult to compute!

Conductor-Discriminant Formula

Theorem (Conductor-Discriminant Formula)

For any two number fields $A \subset B$, we have $\mathrm{disc}(A)^{[B:A]} | \mathrm{disc}(B)$.

Conductor-Discriminant Formula

Proposition (Adhikari, McKean, Plott, Torgersen '26)

If β is a root of F then $\alpha = \beta + \beta^{-1} + c$ is a root of f. This gives us $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\beta)$.

Conductor-Discriminant Formula

Fact: $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\beta)$

Conductor-Discriminant Formula

Fact: $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\beta)$

Theorem (Conductor-Discriminant Formula)

For any two number fields $A \subset B$, we have $\mathrm{disc}(A)^{[B:A]} | \mathrm{disc}(B)$.

$[\mathbb{Q}(\beta) : \mathbb{Q}(\alpha)] = 2$, so

$$\mathrm{disc}(\mathbb{Q}(\alpha))^2 \mid \mathrm{disc}(\mathbb{Q}(\beta))$$

Conductor-Discriminant Formula

Fact: $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\beta)$

Theorem (Conductor-Discriminant Formula)

For any two number fields $A \subset B$, we have $\mathrm{disc}(A)^{[B:A]} | \mathrm{disc}(B)$.

$[\mathbb{Q}(\beta) : \mathbb{Q}(\alpha)] = 2$, so

$$\mathrm{disc}(\mathbb{Q}(\alpha))^2 \mid \mathrm{disc}(\mathbb{Q}(\beta))$$

Assuming f is monogenic, $\mathrm{disc}(f) = \mathrm{disc}(\mathbb{Q}(\alpha))$, hence

$$\mathrm{disc}(f)^2 \mid \mathrm{disc}(\mathbb{Q}(\beta))$$

Discriminant Ratio

$$\frac{\operatorname{disc}(F)}{\operatorname{disc}(\mathbb{Q}(\beta))} = \frac{\operatorname{disc}(f)^2 f(c+2)f(c-2)}{\operatorname{disc}(f)^2 k}$$

$$= \frac{f(c+2)f(c-2)}{k}$$

$$= [\mathcal{O}_{\mathbb{Q}(\beta)} : \mathbb{Z}[\beta]]^2$$

$$\Rightarrow \quad f(c+2)f(c-2) = k \cdot [\mathcal{O}_{\mathbb{Q}(\beta)} : \mathbb{Z}[\beta]]^2$$

Square-Free Consequence

$$f(c+2)f(c-2) = k \cdot [\mathcal{O}_{\mathbb{Q}(\beta)} : \mathbb{Z}[\beta]]^2$$

$$f(c+2)f(c-2) \text{ square-free } \Rightarrow \text{ only square divisor } = 1$$

Square-Free Consequence

$$f(c+2)f(c-2) = k \cdot [\mathcal{O}_{\mathbb{Q}(\beta)} : \mathbb{Z}[\beta]]^2$$

$$f(c+2)f(c-2) \text{ square-free } \Rightarrow \text{ only square divisor } = 1$$

$$[\mathcal{O}_{\mathbb{Q}(\beta)} : \mathbb{Z}[\beta]] = 1$$

$$\mathcal{O}_{\mathbb{Q}(\beta)} = \mathbb{Z}[\beta]$$

Sufficient Condition

Theorem (Adhikari, McKean, Plott, Torgersen '26)

Assume that F is transformed from some monogenic f. Then, $\mathbb{Q}[x]/F$ is a monogenic number field if

$$f(c+2)f(c-2) \text{ is square-free.}$$

Checking Square-Free

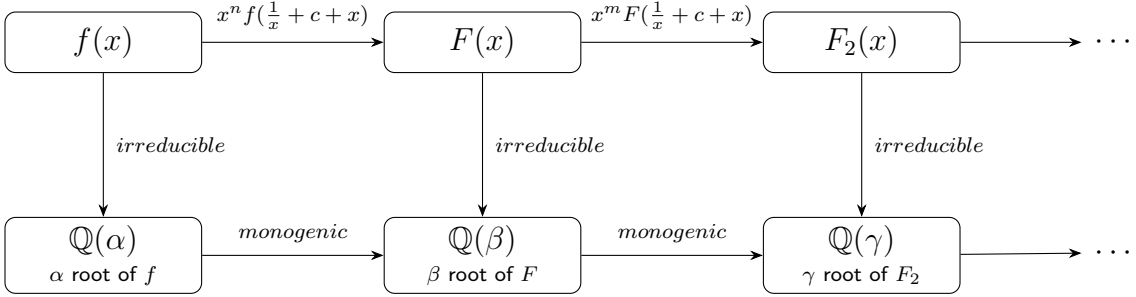
- $f(c+2)$ and $f(c-2)$ individually squarefree and relatively prime
- Generally very hard

Checking Square-Free

- $f(c+2)$ and $f(c-2)$ individually squarefree and relatively prime
- Generally very hard

Work in progress! Stay tuned! SRC 2027!!!

The Big Picture



The End

Thank you!