Vive Galois! Part 1: Optimal SIMD Packing and Packed Bootstrapping for FHE

Chris Peikert Zachary Pepin

University of Michigan

Dec 2nd, 2025

Lattice-Based Cryptography over Rings

- Lattices: the foundation for the only plausible fully homomorphic encryption (FHE) schemes [Gen'09, . . .]

Lattice-Based Cryptography over Rings

- Lattices: the foundation for the only plausible fully homomorphic encryption (FHE) schemes [Gen'09, ...]

- Use rings (in number fields) for efficiency [HPS'96,Mic'02,PR'06,LM'06,LPR'10,...]

Lattice-Based Cryptography over Rings

- Lattices: the foundation for the only plausible fully homomorphic encryption (FHE) schemes [Gen'09, ...]
- Use rings (in number fields) for efficiency [HPS'96,Mic'02,PR'06,LM'06,LPR'10,...]
- Important FHE technique: "SIMD packing" [SV'11]

Lattice-Based Cryptography over Rings

- Lattices: the foundation for the only plausible fully homomorphic encryption (FHE) schemes [Gen'09, ...]
- Use rings (in number fields) for efficiency [HPS'96,Mic'02,PR'06,LM'06,LPR'10,...]
- Important FHE technique: "SIMD packing" [SV'11]
  - ⋆ plaintext $\mu \in \mathbb{F}_q$

Lattice-Based Cryptography over Rings

- Lattices: the foundation for the only plausible fully homomorphic encryption (FHE) schemes [Gen'09, ...]
- Use rings (in number fields) for efficiency [HPS'96,Mic'02,PR'06,LM'06,LPR'10,...]
- Important FHE technique: "SIMD packing" [SV'11]
  - ⋆ plaintext $\mu \in \mathbb{F}_q$ $\vec{\mu} \in \mathbb{F}_q^n$

Lattice-Based Cryptography over Rings

- Lattices: the foundation for the only plausible fully homomorphic encryption (FHE) schemes [Gen'09, ...]

- Use rings (in number fields) for efficiency [HPS'96,Mic'02,PR'06,LM'06,LPR'10,...]

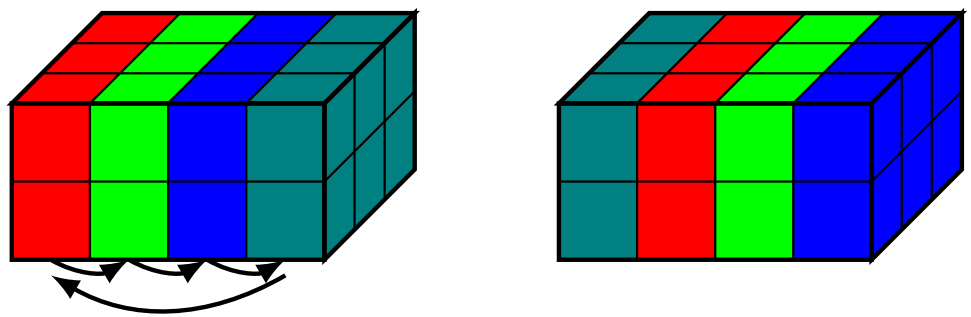
- Important FHE technique: "SIMD packing" [SV'11]
  - ★ plaintext ~~$\mu \in \mathbb{F}_q$~~ $\vec{\mu} \in \mathbb{F}_q^n$
  - ★ fast homomorphic coordinate-wise field operations

Lattice-Based Cryptography over Rings

- Lattices: the foundation for the only plausible fully homomorphic encryption (FHE) schemes [Gen'09, ...]

- Use rings (in number fields) for efficiency [HPS'96,Mic'02,PR'06,LM'06,LPR'10,...]

- Important FHE technique: "SIMD packing" [SV'11]
  - ★ plaintext ~~$\mu \in \mathbb{F}_q$~~ $\vec{\mu} \in \mathbb{F}_q^n$
  - ★ fast homomorphic coordinate-wise field operations
  - ★ certain vector permutations, for linear algebra and "packed bootstrapping" [BGV'12,GHS'12ab,HS'14]



Cyclotomics and Their Limitations

- Prior work has focused almost entirely on cyclotomic fields/rings.

Cyclotomics and Their Limitations

- Prior work has focused almost entirely on cyclotomic fields/rings.

✔ original setting for hardness of Ring-SIS/LWE (now all rings [PRS'17])

Cyclotomics and Their Limitations

- Prior work has focused almost entirely on cyclotomic fields/rings.

✔ original setting for hardness of Ring-SIS/LWE (now all rings [PRS'17])

✔ computationally fast

Cyclotomics and Their Limitations

- Prior work has focused almost entirely on cyclotomic fields/rings.

✔ original setting for hardness of Ring-SIS/LWE (now all rings [PRS'17])

✔ computationally fast

✔ geometrically nice (for error growth & decoding)

Cyclotomics and Their Limitations

- Prior work has focused almost entirely on cyclotomic fields/rings.

✔ original setting for hardness of Ring-SIS/LWE (now all rings [PRS'17])

✔ computationally fast

✔ geometrically nice (for error growth & decoding)

✗ difficult to get the desired SIMD "slot type"

Cyclotomics and Their Limitations

- Prior work has focused almost entirely on cyclotomic fields/rings.

✔ original setting for hardness of Ring-SIS/LWE (now all rings [PRS'17])

✔ computationally fast

✔ geometrically nice (for error growth & decoding)

✗ difficult to get the desired SIMD "slot type"

- ⋆ for homomorphic AES evaluation, [GHS'12c] was induced to use $\mathbb{F}_{2^{24}}$-slots, a $3\times$ loss in 'capacity' vs the most natural $\mathbb{F}_{2^8}$

Cyclotomics and Their Limitations

- Prior work has focused almost entirely on cyclotomic fields/rings.

✔ original setting for hardness of Ring-SIS/LWE (now all rings [PRS'17])

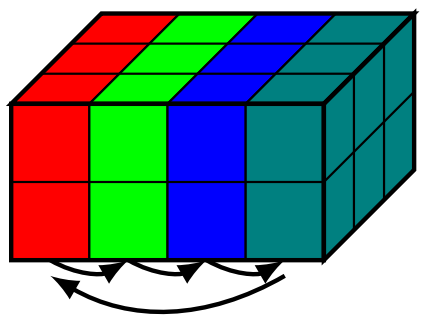
✔ computationally fast

✔ geometrically nice (for error growth & decoding)

✗ difficult to get the desired SIMD "slot type"

- ⋆ for homomorphic AES evaluation, [GHS'12c] was induced to use $\mathbb{F}_{2^{24}}$-slots, a $3\times$ loss in 'capacity' vs the most natural $\mathbb{F}_{2^8}$

✗ difficult to get desired slot-tensor "shape" and data movement.



Beyond Cyclotomics

- [AritaHanda'17]: use decomposition subfields of cyclotomics:

Beyond Cyclotomics

- [AritaHanda'17]: use decomposition subfields of cyclotomics:
  - ✔ Get *exactly* the desired slot "type"—no wasted capacity!

Beyond Cyclotomics

- [AritaHanda'17]: use decomposition subfields of cyclotomics:
  - ✔ Get *exactly* the desired slot "type"—no wasted capacity!
  - ✗ Limited to subfields of prime cyclotomics

Beyond Cyclotomics

- [AritaHanda'17]: use decomposition subfields of cyclotomics:
  - ✔ Get *exactly* the desired slot "type"—no wasted capacity!
  - ✗ Limited to subfields of prime cyclotomics
  - ✗ Lacked specialized fast algorithms for field/ring arithmetic

Beyond Cyclotomics

- [AritaHanda'17]: use decomposition subfields of cyclotomics:
  - ✔ Get *exactly* the desired slot "type"—no wasted capacity!
  - ✗ Limited to subfields of prime cyclotomics
  - ✗ Lacked specialized fast algorithms for field/ring arithmetic
  - ✗ No treatment of packed bootstrapping

Beyond Cyclotomics

- [AritaHanda'17]: use decomposition subfields of cyclotomics:
  - ✔ Get *exactly* the desired slot "type"—no wasted capacity!
  - ✗ Limited to subfields of prime cyclotomics
  - ✗ Lacked specialized fast algorithms for field/ring arithmetic
  - ✗ No treatment of packed bootstrapping

- Our work: use abelian (Galois) number fields (e.g., $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\zeta_8)$)

Beyond Cyclotomics

- [AritaHanda'17]: use decomposition subfields of cyclotomics:
  - ✔ Get *exactly* the desired slot "type"—no wasted capacity!
  - ✗ Limited to subfields of prime cyclotomics
  - ✗ Lacked specialized fast algorithms for field/ring arithmetic
  - ✗ No treatment of packed bootstrapping

- Our work: use abelian (Galois) number fields (e.g., $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\zeta_8)$)
  - ⋆ i.e., the subfields of arbitrary cyclotomics [Kronecker–Weber]

Beyond Cyclotomics

- [AritaHanda'17]: use decomposition subfields of cyclotomics:
  - ✔ Get *exactly* the desired slot "type"—no wasted capacity!
  - ✗ Limited to subfields of prime cyclotomics
  - ✗ Lacked specialized fast algorithms for field/ring arithmetic
  - ✗ No treatment of packed bootstrapping

- Our work: use abelian (Galois) number fields (e.g., $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\zeta_8)$)
  - ⋆ i.e., the subfields of arbitrary cyclotomics [Kronecker–Weber]

Our Take-Home Message

We instantiate FHE over abelian number fields and show, vs. cyclotomics:

Beyond Cyclotomics

- [AritaHanda'17]: use decomposition subfields of cyclotomics:
  - ✔ Get *exactly* the desired slot "type"—no wasted capacity!
  - ✗ Limited to subfields of prime cyclotomics
  - ✗ Lacked specialized fast algorithms for field/ring arithmetic
  - ✗ No treatment of packed bootstrapping

- Our work: use abelian (Galois) number fields (e.g., $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\zeta_8)$)
  - ⋆ i.e., the subfields of arbitrary cyclotomics [Kronecker–Weber]

Our Take-Home Message

We instantiate FHE over abelian number fields and show, vs. cyclotomics:

- ✔ comparable algorithmic efficiency & geometry

Beyond Cyclotomics

- [AritaHanda'17]: use decomposition subfields of cyclotomics:
  - ✔ Get *exactly* the desired slot "type"—no wasted capacity!
  - ✗ Limited to subfields of prime cyclotomics
  - ✗ Lacked specialized fast algorithms for field/ring arithmetic
  - ✗ No treatment of packed bootstrapping

- Our work: use abelian (Galois) number fields (e.g., $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\zeta_8)$)
  - ⋆ i.e., the subfields of arbitrary cyclotomics [Kronecker–Weber]

Our Take-Home Message

We instantiate FHE over abelian number fields and show, vs. cyclotomics:

- ✔ comparable algorithmic efficiency & geometry
- ✔ easy to get desired slot 'type', and fine-grained 'shape' & movement

Beyond Cyclotomics

- [AritaHanda'17]: use decomposition subfields of cyclotomics:
  - ✔ Get *exactly* the desired slot "type"—no wasted capacity!
  - ✗ Limited to subfields of prime cyclotomics
  - ✗ Lacked specialized fast algorithms for field/ring arithmetic
  - ✗ No treatment of packed bootstrapping

- Our work: use abelian (Galois) number fields (e.g., $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\zeta_8)$)
  - ⋆ i.e., the subfields of arbitrary cyclotomics [Kronecker–Weber]

Our Take-Home Message

We instantiate FHE over abelian number fields and show, vs. cyclotomics:

- ✔ comparable algorithmic efficiency & geometry
- ✔ easy to get desired slot 'type', and fine-grained 'shape' & movement
- ✔ $\implies$ packed bootstrapping with comparable (or better) efficiency

Our Technical Contributions

- A toolkit for ring-based crypto & FHE over abelian number fields, achieving *optimal SIMD packing* and *packed bootstrapping*

Our Technical Contributions

- A toolkit for ring-based crypto & FHE over abelian number fields, achieving *optimal SIMD packing* and *packed bootstrapping*

1. short, 'structured' $\mathbb{Z}$-bases for wide class of abelian number rings, to:
   - ⋆ represent ring elements
   - ⋆ sample/decode error in encryption/decryption & bootstrapping

Our Technical Contributions

- A toolkit for ring-based crypto & FHE over abelian number fields, achieving *optimal SIMD packing* and *packed bootstrapping*

1. short, 'structured' $\mathbb{Z}$-bases for wide class of abelian number rings, to:
   - ⋆ represent ring elements
   - ⋆ sample/decode error in encryption/decryption & bootstrapping
2. Chinese Remainder Theorem bases in arbitrary abelian number rings:
   - ⋆ yield fast ring arithmetic and SIMD plaintext slots
   - ⋆ have tensor structure & data movement mirroring Galois group

Our Technical Contributions

- A toolkit for ring-based crypto & FHE over abelian number fields, achieving *optimal SIMD packing* and *packed bootstrapping*

1. short, 'structured' $\mathbb{Z}$-bases for wide class of abelian number rings, to:
   - ⋆ represent ring elements
   - ⋆ sample/decode error in encryption/decryption & bootstrapping
2. Chinese Remainder Theorem bases in arbitrary abelian number rings:
   - ⋆ yield fast ring arithmetic and SIMD plaintext slots
   - ⋆ have tensor structure & data movement mirroring Galois group
3. Fast 'CRT transforms' between these bases:

Our Technical Contributions

- A toolkit for ring-based crypto & FHE over abelian number fields, achieving *optimal SIMD packing* and *packed bootstrapping*

1. short, 'structured' $\mathbb{Z}$-bases for wide class of abelian number rings, to:
   - ⋆ represent ring elements
   - ⋆ sample/decode error in encryption/decryption & bootstrapping
2. Chinese Remainder Theorem bases in arbitrary abelian number rings:
   - ⋆ yield fast ring arithmetic and SIMD plaintext slots
   - ⋆ have tensor structure & data movement mirroring Galois group
3. Fast 'CRT transforms' between these bases:
   - ⋆ "in the clear" (directly on coordinate vectors)

Our Technical Contributions

- A toolkit for ring-based crypto & FHE over abelian number fields, achieving *optimal SIMD packing* and *packed bootstrapping*

1. short, 'structured' $\mathbb{Z}$-bases for wide class of abelian number rings, to:
   - ⋆ represent ring elements
   - ⋆ sample/decode error in encryption/decryption & bootstrapping
2. Chinese Remainder Theorem bases in arbitrary abelian number rings:
   - ⋆ yield fast ring arithmetic and SIMD plaintext slots
   - ⋆ have tensor structure & data movement mirroring Galois group
3. Fast 'CRT transforms' between these bases:
   - ⋆ "in the clear" (directly on coordinate vectors)
   - ⋆ homomorphically (via automorphisms)

Our Technical Contributions

- A toolkit for ring-based crypto & FHE over abelian number fields, achieving *optimal SIMD packing* and *packed bootstrapping*

1. short, 'structured' $\mathbb{Z}$-bases for wide class of abelian number rings, to:
   - ⋆ represent ring elements
   - ⋆ sample/decode error in encryption/decryption & bootstrapping
2. Chinese Remainder Theorem bases in arbitrary abelian number rings:
   - ⋆ yield fast ring arithmetic and SIMD plaintext slots
   - ⋆ have tensor structure & data movement mirroring Galois group
3. Fast 'CRT transforms' between these bases:
   - ⋆ "in the clear" (directly on coordinate vectors)
   - ⋆ homomorphically (via automorphisms)
4. Tools for constructing abelian number rings with:
   - ⋆ exactly the desired "slot type"
   - ⋆ a wide variety of slot-tensor shapes and data movements

Our Technical Contributions

- A toolkit for ring-based crypto & FHE over abelian number fields, achieving *optimal SIMD packing* and *packed bootstrapping*

1. short, 'structured' $\mathbb{Z}$-bases for wide class of abelian number rings, to:
   - ⋆ represent ring elements
   - ⋆ sample/decode error in encryption/decryption & bootstrapping
2. Chinese Remainder Theorem bases in arbitrary abelian number rings:
   - ⋆ yield fast ring arithmetic and SIMD plaintext slots
   - ⋆ have tensor structure & data movement mirroring Galois group
3. Fast 'CRT transforms' between these bases:
   - ⋆ "in the clear" (directly on coordinate vectors)
   - ⋆ homomorphically (via automorphisms)
4. Tools for constructing abelian number rings with:
   - ⋆ exactly the desired "slot type"
   - ⋆ a wide variety of slot-tensor shapes and data movements

CRT and SIMD Slots

Reminder: Chinese Remainder Theorem

Let $\mathfrak{q}$ be an R-ideal that splits as $\mathfrak{q} = \mathfrak{q}_1 \cdots \mathfrak{q}_\ell$ for pairwise coprime $\mathfrak{q}_i$.
Then the natural map is a ring isomorphism:

$$R/\mathfrak{q} \cong (R/\mathfrak{q}_1) \times \cdots \times (R/\mathfrak{q}_\ell).$$

CRT and SIMD Slots

Reminder: Chinese Remainder Theorem

Let $\mathfrak{q}$ be an R-ideal that splits as $\mathfrak{q} = \mathfrak{q}_1 \cdots \mathfrak{q}_\ell$ for pairwise coprime $\mathfrak{q}_i$.
Then the natural map is a ring isomorphism:

$$R/\mathfrak{q} \cong (R/\mathfrak{q}_1) \times \cdots \times (R/\mathfrak{q}_\ell).$$

Ring addition/multiplication $\leftrightarrow$ component-wise addition/multiplication

CRT and SIMD Slots

Reminder: Chinese Remainder Theorem

Let $\mathfrak{q}$ be an R-ideal that splits as $\mathfrak{q} = \mathfrak{q}_1 \cdots \mathfrak{q}_\ell$ for pairwise coprime $\mathfrak{q}_i$.
Then the natural map is a ring isomorphism:

$$R/\mathfrak{q} \cong (R/\mathfrak{q}_1) \times \cdots \times (R/\mathfrak{q}_\ell).$$

Ring addition/multiplication $\leftrightarrow$ component-wise addition/multiplication

Implications

- Fast arithmetic on ciphertexts (mod $\mathfrak{q}$)
- SIMD arithmetic on plaintext 'slots' (mod $\mathfrak{p}$)

CRT and SIMD Slots

Reminder: Chinese Remainder Theorem

Let $\mathfrak{q}$ be an R-ideal that splits as $\mathfrak{q} = \mathfrak{q}_1 \cdots \mathfrak{q}_\ell$ for pairwise coprime $\mathfrak{q}_i$.
Then the natural map is a ring isomorphism:

$$R/\mathfrak{q} \cong (R/\mathfrak{q}_1) \times \cdots \times (R/\mathfrak{q}_\ell).$$

Ring addition/multiplication $\leftrightarrow$ component-wise addition/multiplication

Implications

- Fast arithmetic on ciphertexts (mod $\mathfrak{q}$)
- SIMD arithmetic on plaintext 'slots' (mod $\mathfrak{p}$)

Key Question: How to Construct 'Well Splitting' $R, \mathfrak{q}$?

CRT and SIMD Slots

Reminder: Chinese Remainder Theorem

Let $\mathfrak{q}$ be an R-ideal that splits as $\mathfrak{q} = \mathfrak{q}_1 \cdots \mathfrak{q}_\ell$ for pairwise coprime $\mathfrak{q}_i$.
Then the natural map is a ring isomorphism:

$$R/\mathfrak{q} \cong (R/\mathfrak{q}_1) \times \cdots \times (R/\mathfrak{q}_\ell).$$

Ring addition/multiplication $\leftrightarrow$ component-wise addition/multiplication

Implications

- Fast arithmetic on ciphertexts (mod $\mathfrak{q}$)
- SIMD arithmetic on plaintext 'slots' (mod $\mathfrak{p}$)

Key Question: How to Construct 'Well Splitting' $R, \mathfrak{q}$?

1. Desired ring structure of $R/\mathfrak{q}_i$

CRT and SIMD Slots

Reminder: Chinese Remainder Theorem

Let $\mathfrak{q}$ be an R-ideal that splits as $\mathfrak{q} = \mathfrak{q}_1 \cdots \mathfrak{q}_\ell$ for pairwise coprime $\mathfrak{q}_i$.
Then the natural map is a ring isomorphism:

$$R/\mathfrak{q} \cong (R/\mathfrak{q}_1) \times \cdots \times (R/\mathfrak{q}_\ell).$$

Ring addition/multiplication $\leftrightarrow$ component-wise addition/multiplication

Implications

- Fast arithmetic on ciphertexts (mod $\mathfrak{q}$)
- SIMD arithmetic on plaintext 'slots' (mod $\mathfrak{p}$)

Key Question: How to Construct 'Well Splitting' $R, \mathfrak{q}$?

1. Desired ring structure of $R/\mathfrak{q}_i$
2. Many factors $\mathfrak{q}_i$

CRT and SIMD Slots

Reminder: Chinese Remainder Theorem

Let $\mathfrak{q}$ be an R-ideal that splits as $\mathfrak{q} = \mathfrak{q}_1 \cdots \mathfrak{q}_\ell$ for pairwise coprime $\mathfrak{q}_i$.
Then the natural map is a ring isomorphism:

$$R/\mathfrak{q} \cong (R/\mathfrak{q}_1) \times \cdots \times (R/\mathfrak{q}_\ell).$$

Ring addition/multiplication $\leftrightarrow$ component-wise addition/multiplication

Implications

- Fast arithmetic on ciphertexts (mod $\mathfrak{q}$)
- SIMD arithmetic on plaintext 'slots' (mod $\mathfrak{p}$)

Key Question: How to Construct 'Well Splitting' $R, \mathfrak{q}$?

1. Desired ring structure of $R/\mathfrak{q}_i$
2. Many factors $\mathfrak{q}_i$
3. Fine-grained data movement among the slots

Galois Theory: Splitting and Inertness

- Let M/K be an abelian extension of number fields, (e.g., $\mathbb{Q}(\zeta_m)/\mathbb{Q}$) and $\mathfrak{q}_K$ be a prime ideal in K's ring of integers $\mathcal{O}_K$.

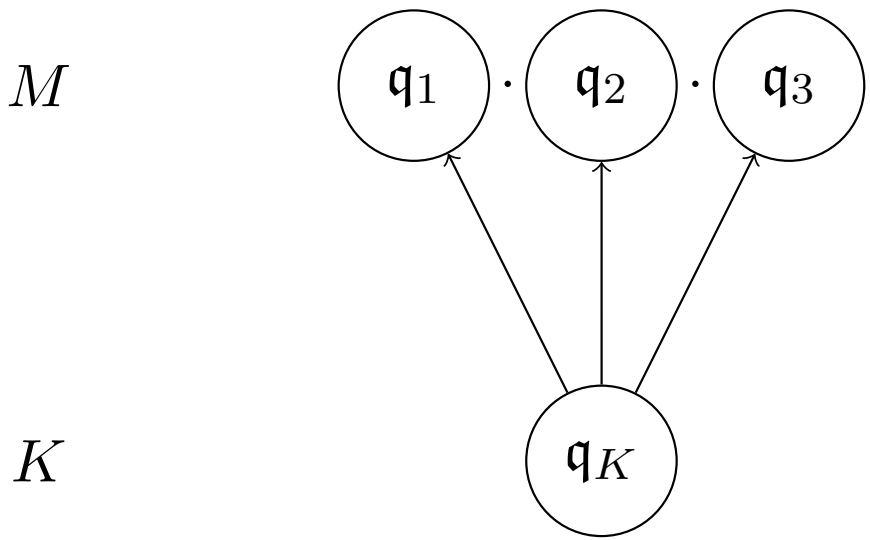
M

K

Galois Theory: Splitting and Inertness

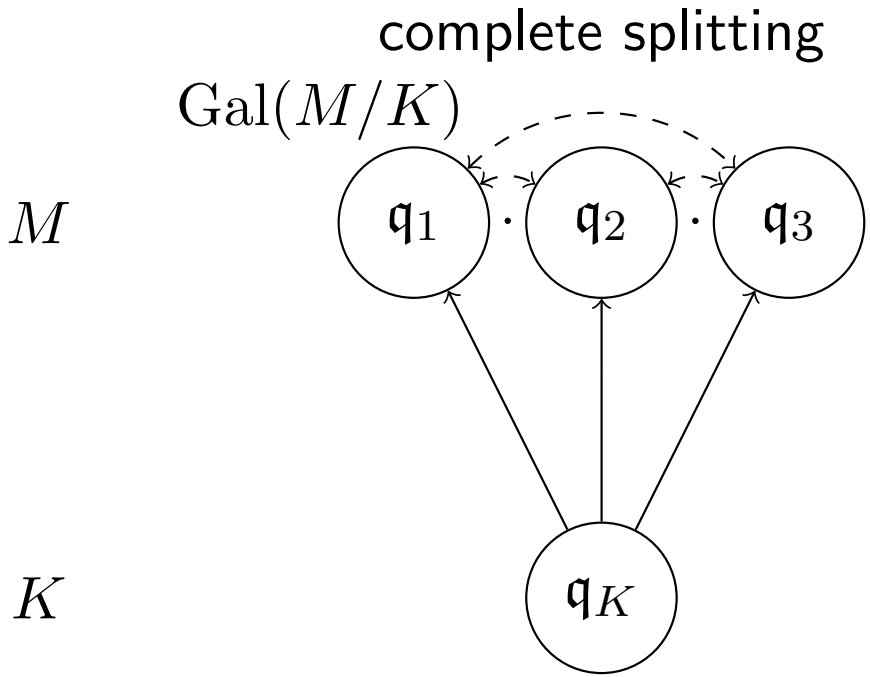
- Let M/K be an abelian extension of number fields, (e.g., $\mathbb{Q}(\zeta_m)/\mathbb{Q}$) and $\mathfrak{q}_K$ be a prime ideal in K's ring of integers $\mathcal{O}_K$.

complete splitting



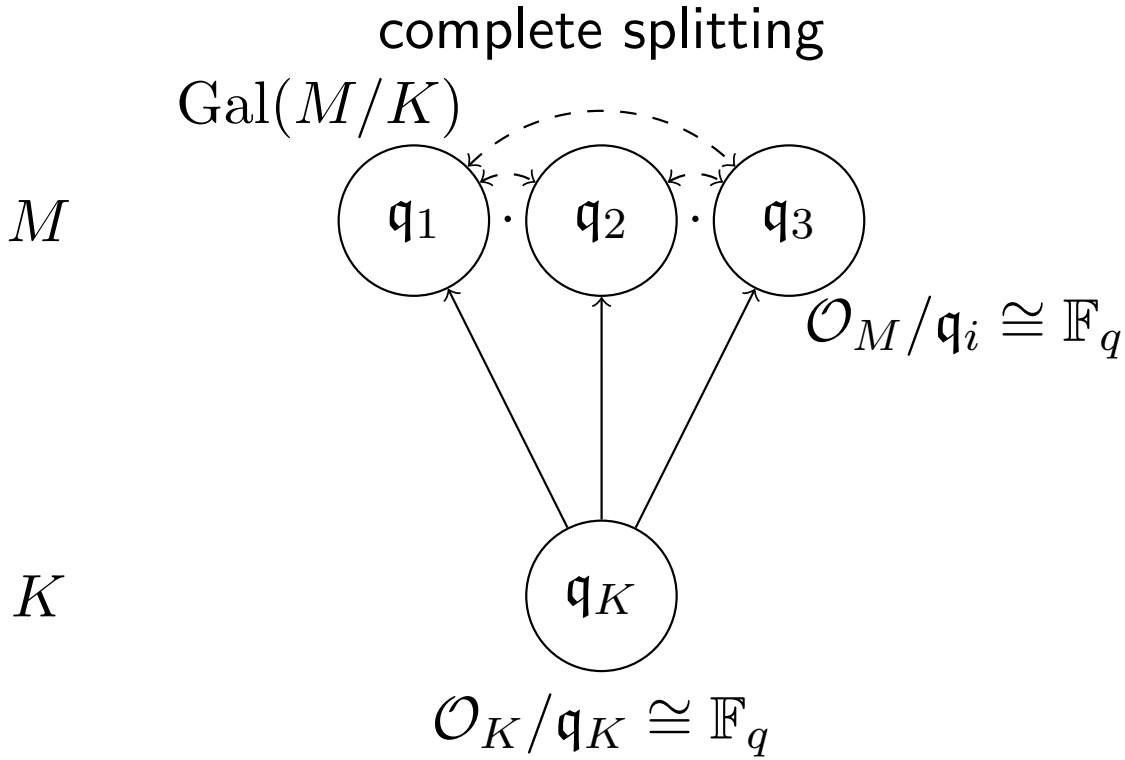
Galois Theory: Splitting and Inertness

- Let M/K be an abelian extension of number fields, (e.g., $\mathbb{Q}(\zeta_m)/\mathbb{Q}$) and $\mathfrak{q}_K$ be a prime ideal in K's ring of integers $\mathcal{O}_K$.



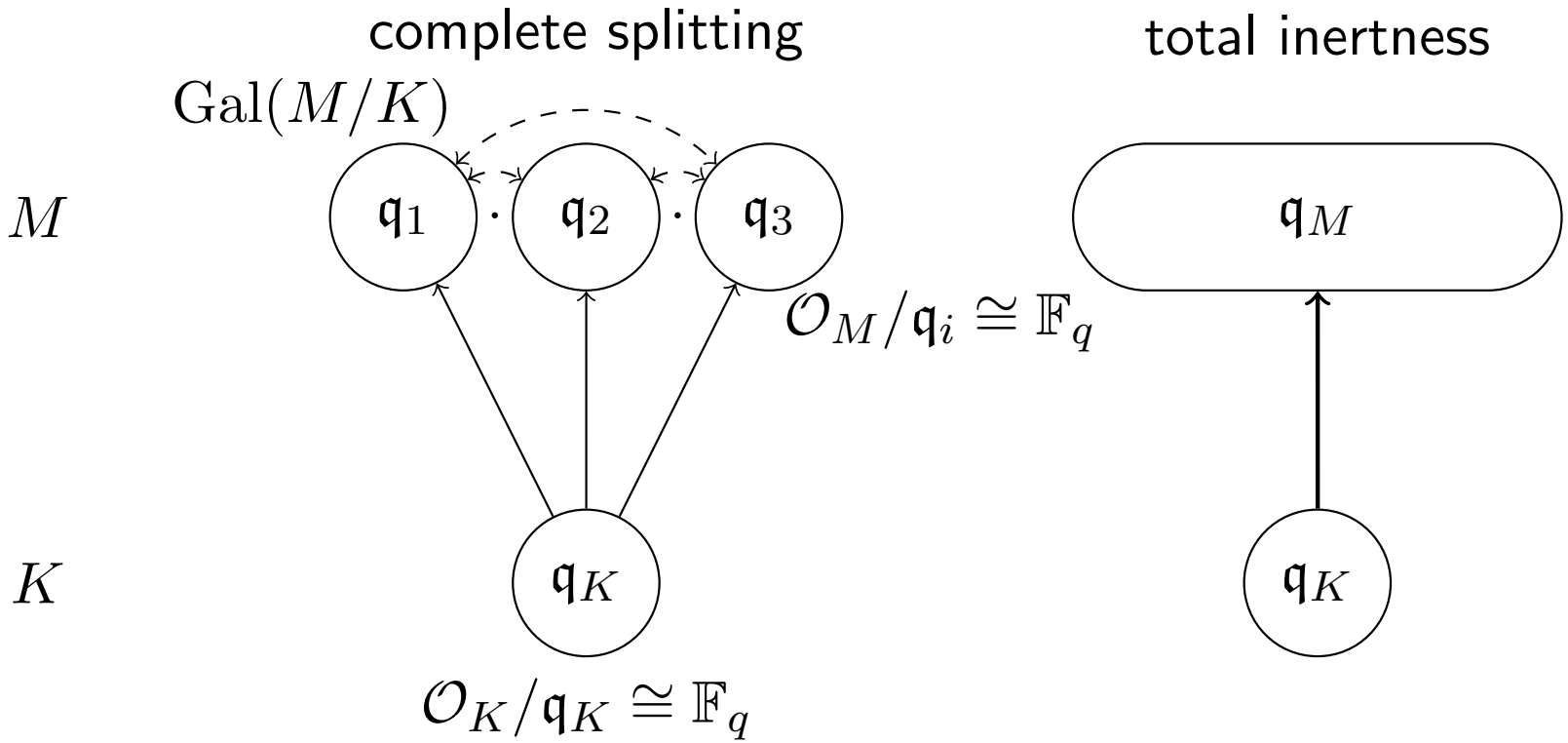
Galois Theory: Splitting and Inertness

- Let M/K be an abelian extension of number fields, (e.g., $\mathbb{Q}(\zeta_m)/\mathbb{Q}$) and $\mathfrak{q}_K$ be a prime ideal in K's ring of integers $\mathcal{O}_K$.



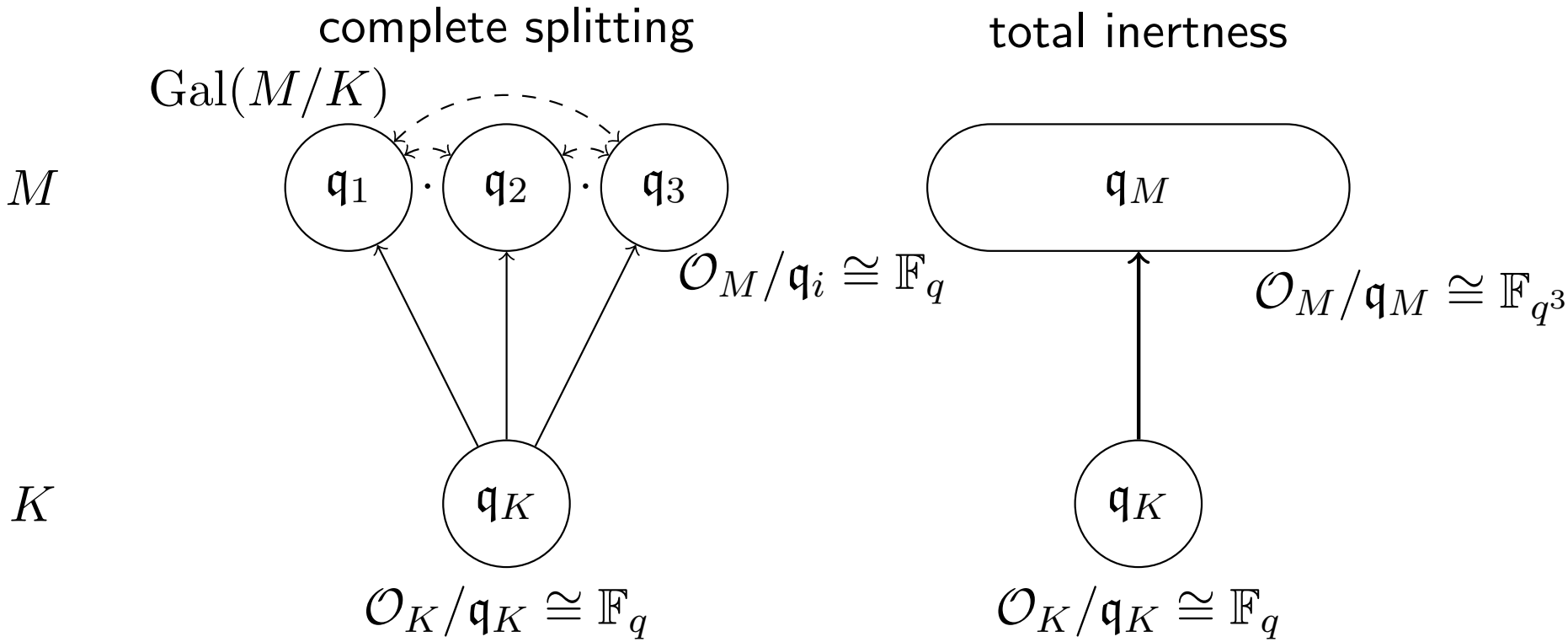
Galois Theory: Splitting and Inertness

- Let M/K be an abelian extension of number fields, (e.g., $\mathbb{Q}(\zeta_m)/\mathbb{Q}$) and $\mathfrak{q}_K$ be a prime ideal in K's ring of integers $\mathcal{O}_K$.



Galois Theory: Splitting and Inertness

- Let M/K be an abelian extension of number fields, (e.g., $\mathbb{Q}(\zeta_m)/\mathbb{Q}$) and $\mathfrak{q}_K$ be a prime ideal in K's ring of integers $\mathcal{O}_K$.

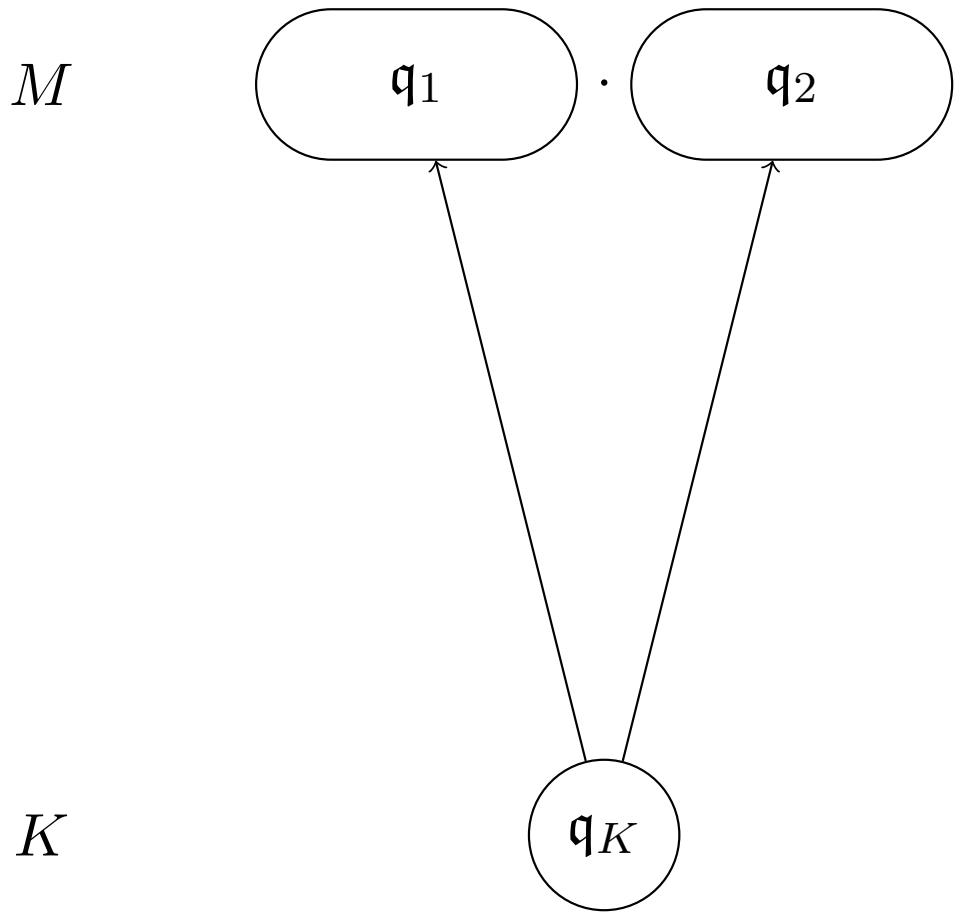


Splitting and Inertness

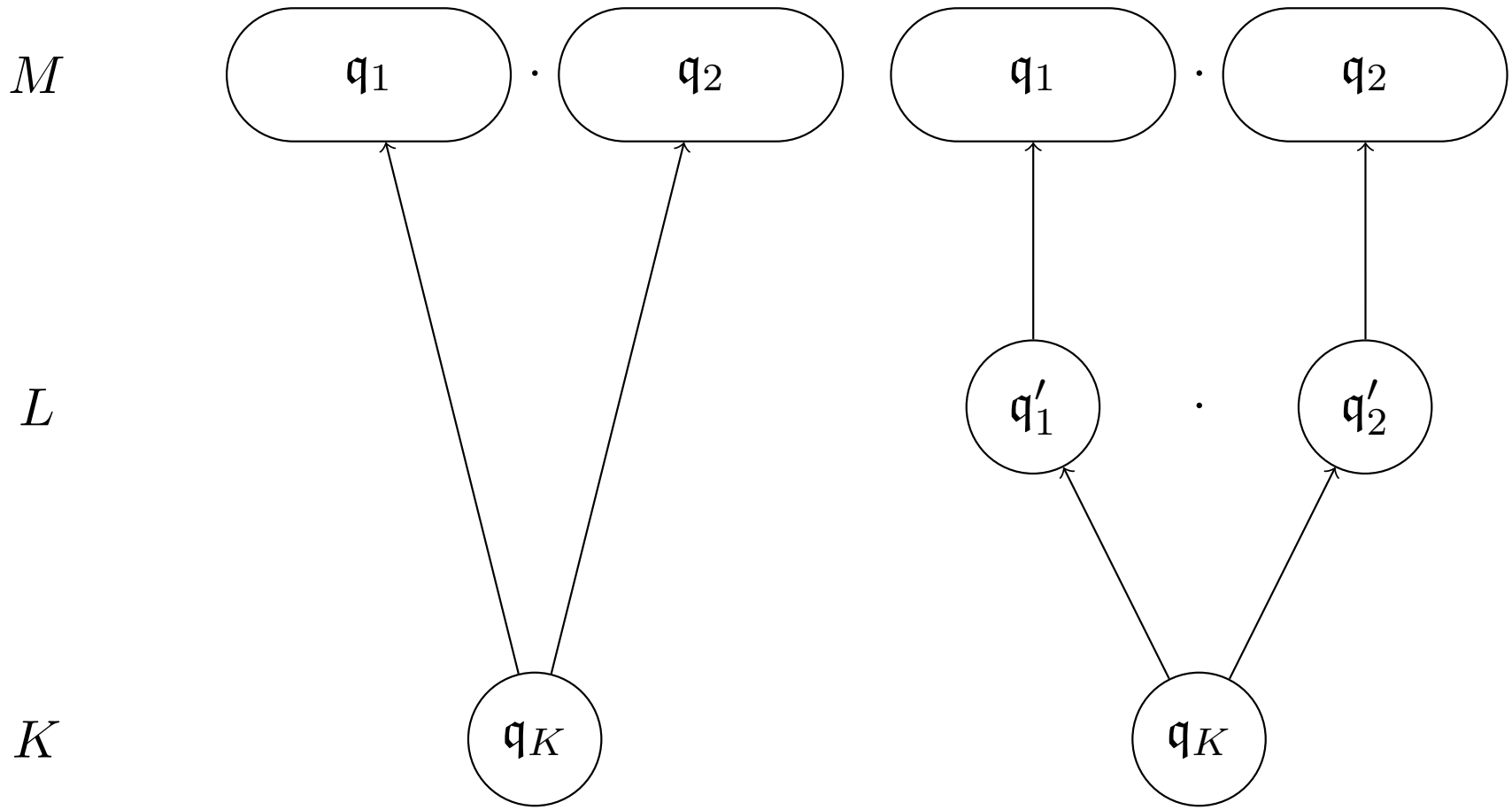
M

K

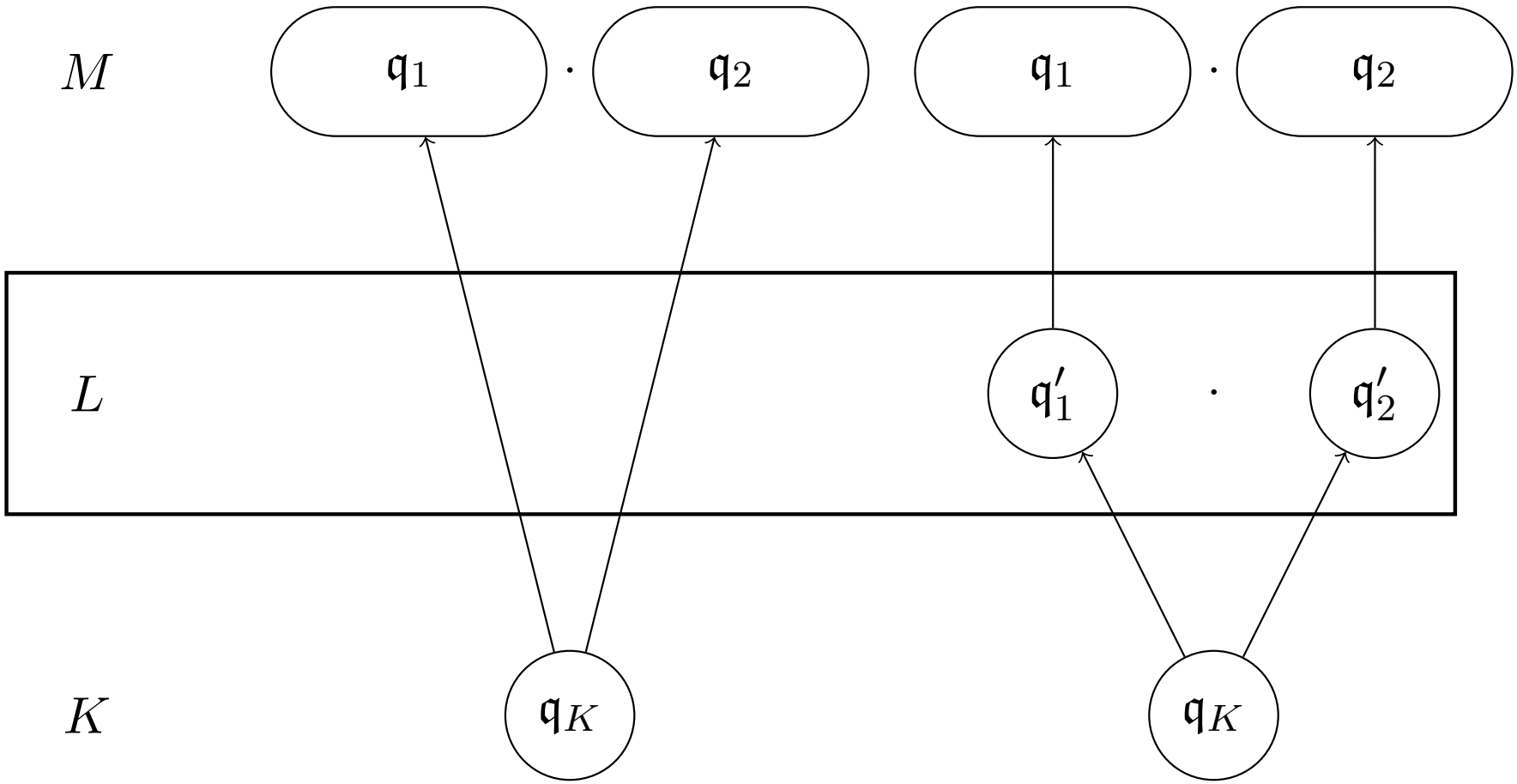
Splitting and Inertness



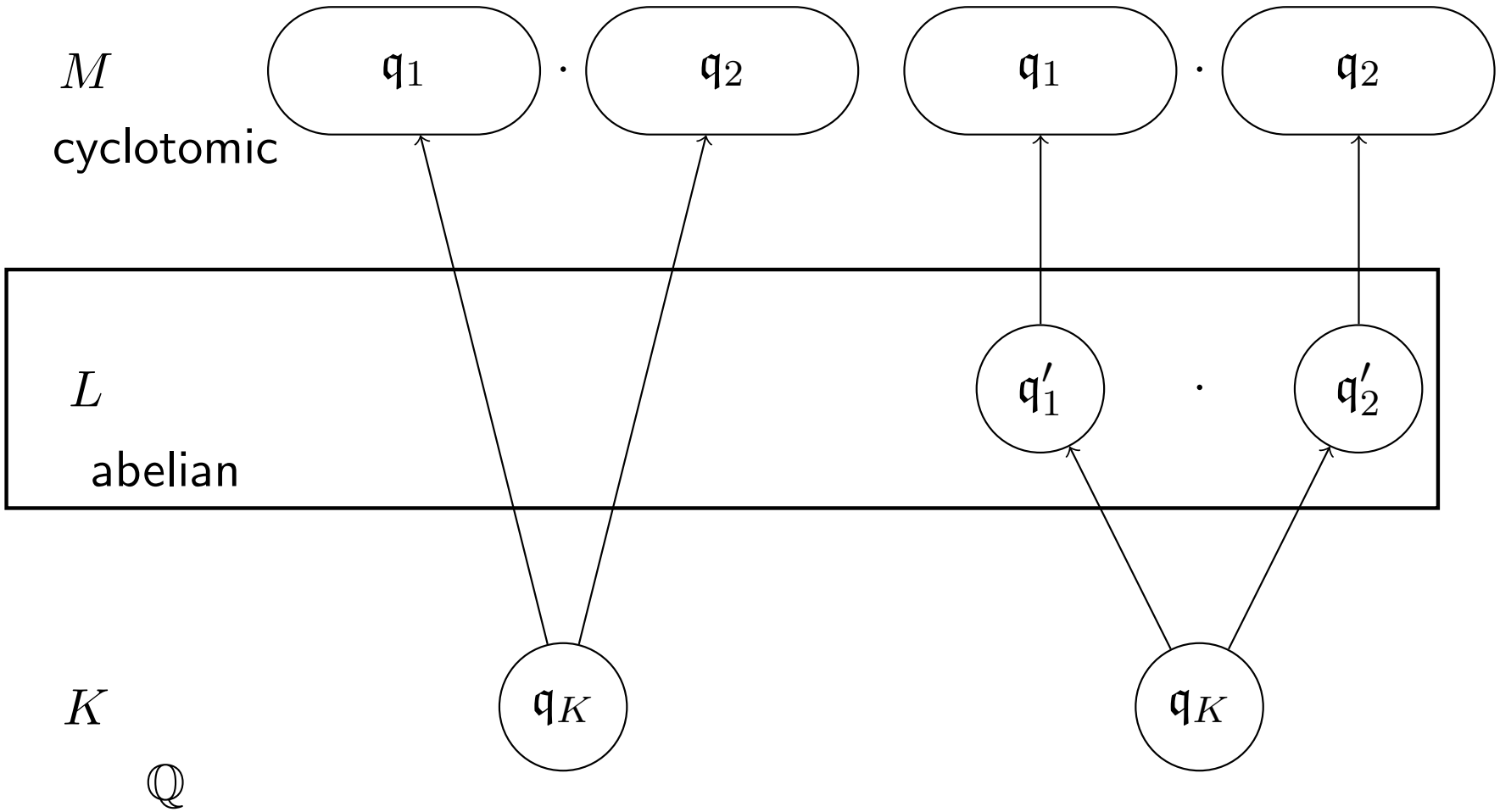
Splitting and Inertness



Splitting and Inertness



Splitting and Inertness



Slot-Tensor Shape and Data Movement

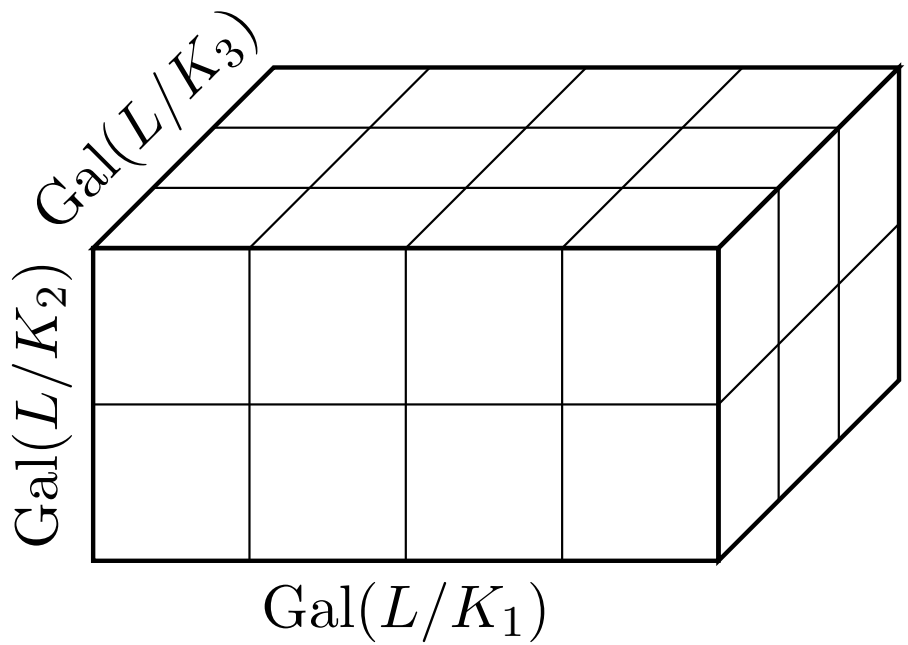
$$\mathrm{Gal}(L/K) = H_1 \cdot H_2 \cdot H_3$$

Slot-Tensor Shape and Data Movement

$$\mathrm{Gal}(L/K) = \mathrm{Gal}(L/K_1) \cdot \mathrm{Gal}(L/K_2) \cdot \mathrm{Gal}(L/K_3)$$

Slot-Tensor Shape and Data Movement

$$\mathrm{Gal}(L/K) = \mathrm{Gal}(L/K_1) \cdot \mathrm{Gal}(L/K_2) \cdot \mathrm{Gal}(L/K_3)$$



Conclusions

Main Contribution

- A toolkit for efficient and flexible FHE over abelian number fields

Conclusions

Main Contribution

- A toolkit for efficient and flexible FHE over abelian number fields

1. Short, "structured" $\mathbb{Z}$-bases for a wide class of abelian number fields

Conclusions

Main Contribution

- A toolkit for efficient and flexible FHE over abelian number fields

1. Short, "structured" $\mathbb{Z}$-bases for a wide class of abelian number fields
2. CRT bases of abelian number fields

Conclusions

Main Contribution

- A toolkit for efficient and flexible FHE over abelian number fields

1. Short, "structured" $\mathbb{Z}$-bases for a wide class of abelian number fields
2. CRT bases of abelian number fields
3. Fast CRT transforms between these bases, both:
   - ⋆ "in the clear" (directly on coefficient vectors)
   - ⋆ homomorphically (via automorphisms)

Conclusions

Main Contribution

- A toolkit for efficient and flexible FHE over abelian number fields

1. Short, "structured" $\mathbb{Z}$-bases for a wide class of abelian number fields
2. CRT bases of abelian number fields
3. Fast CRT transforms between these bases, both:
   - ⋆ "in the clear" (directly on coefficient vectors)
   - ⋆ homomorphically (via automorphisms)
4. Tools for constructing abelian number fields with desired properties

Conclusions

Main Contribution

- A toolkit for efficient and flexible FHE over abelian number fields

1. Short, "structured" $\mathbb{Z}$-bases for a wide class of abelian number fields
2. CRT bases of abelian number fields
3. Fast CRT transforms between these bases, both:
   - ⋆ "in the clear" (directly on coefficient vectors)
   - ⋆ homomorphically (via automorphisms)
4. Tools for constructing abelian number fields with desired properties

Future Work

- Implementation
- Other applications (e.g., proof systems)