Chebotarev's theorem for groups of order pq and an uncertainty principle

Maria Loukaki

University of Crete

Central China Normal University,
Wuhan

September 9, 2025

Introduction- The problem

Theorem (Chebotarev, 1926)

If $I, J \subseteq \{0, 1, 2, \cdots p-1\}$ with p a prime and $|I| = |J|$ then the matrix $(\zeta_p^{ij})_{i \in I, j \in J}$ has non-zero determinant.

- Discrete Fourier Transform: $\mathcal{F}_n = (\zeta_n^{ij})$ with $i, j \in \{0, 1, \cdots, n-1\}$
- Chebotarev $\rightsquigarrow$ any (square) submatrix of $\mathcal{F}_p$ is nonsingular

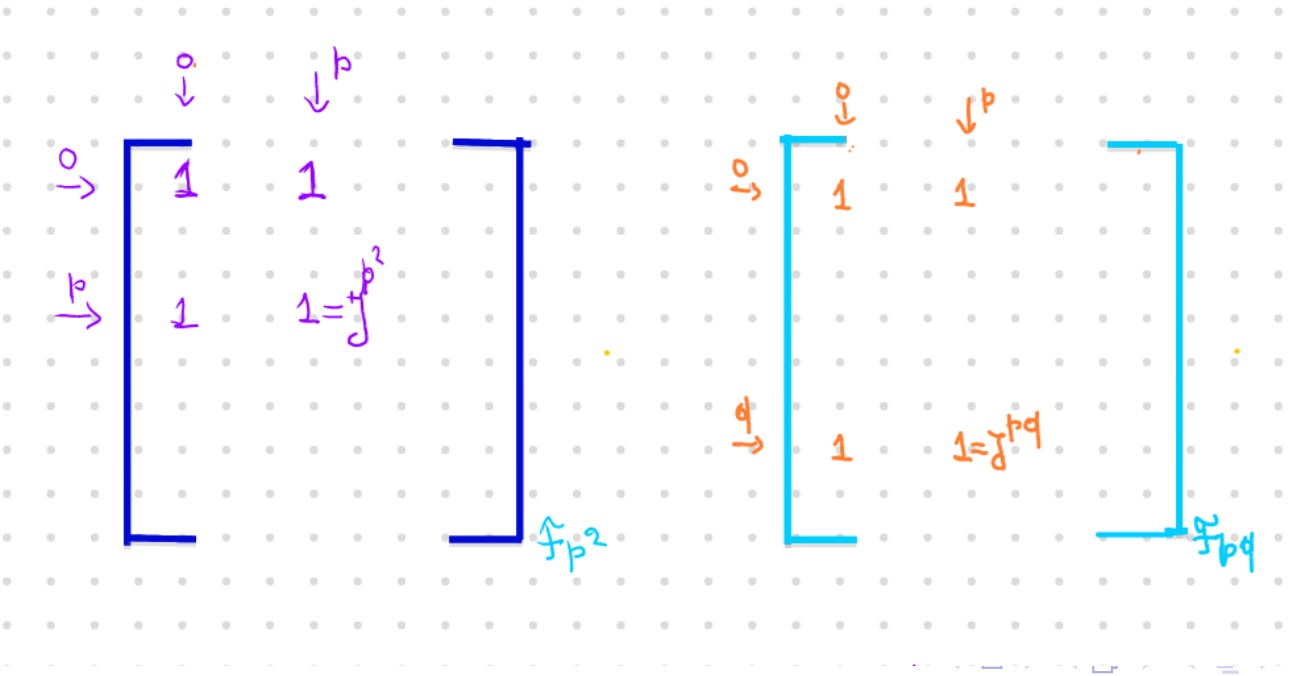
Introduction- The problem

Theorem (Chebotarev, 1926)

If $I, J \subseteq \{0, 1, 2, \cdots p-1\}$ with p a prime and $|I| = |J|$ then the matrix $(\zeta_p^{ij})_{i \in I, j \in J}$ has non-zero determinant.

- Discrete Fourier Transform: $\mathcal{F}_n = (\zeta_n^{ij})$ with $i, j \in \{0, 1, \cdots, n-1\}$
- Chebotarev $\rightsquigarrow$ any (square) submatrix of $\mathcal{F}_p$ is nonsingular

What about $\mathcal{F}_n$, for general n?



Introduction- The problem

For Finite fields:

Theorem (Zhang, 2019)

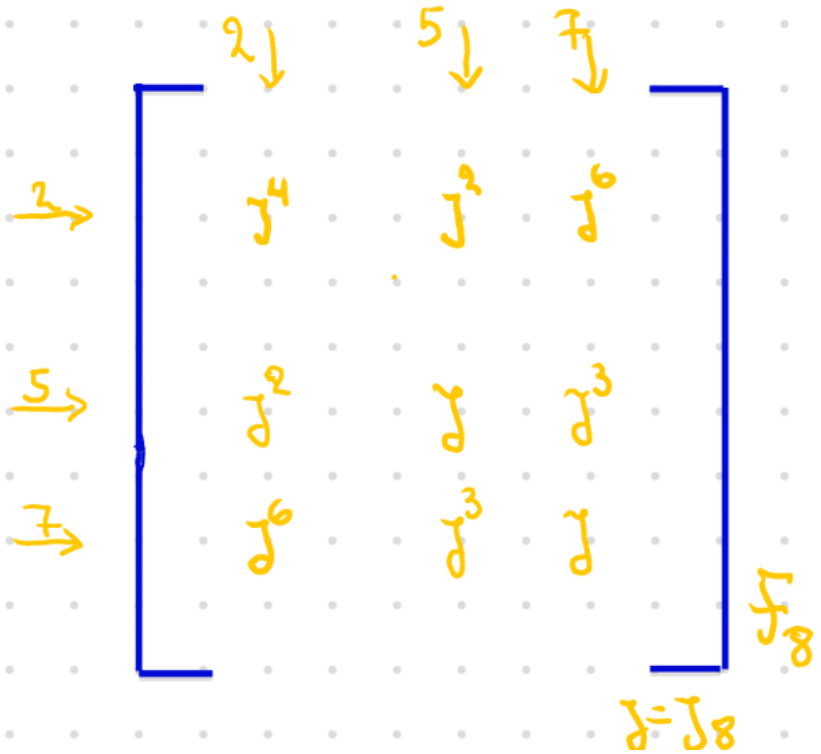
Let p, r be distinct odd primes, with p primitive in $\mathbb{F}_r$ and $p > \Gamma_r$. Suppose that ω is an r-th primitive root of unity in $\mathbb{F}_{p^{r-1}}$. Then all submatrices of $(\omega^{ij})_{i,j=0}^{r-1}$ have non-zero determinant in $\mathbb{F}_{p^{r-1}}$.

Introduction- The problem

Conjecture (Cabrelli, Molter, Negreira (2024) and Caragea, Lee, Malikiosis, Pfander (2024))

If n is square-free then all principal submatrices of $\mathcal{F}_n = (\zeta_n^{ij})$ have nonzero determinant.

Principal submatrix of $\mathcal{F}_n$: $(\zeta_n^{ij})_{i,j\in I}$ for some $I \subseteq \{0, 1, \cdots, n-1\}$



Introduction- The problem

Both groups arrived independently to the same conjecture, via
a) conditions needed to make bases in f.d. Hilbert spaces woven
b) the construction of exponential Riesz bases.

Question (Caragea, Lee, Malikiosis, Pfander, 2024)

For which $N \in \mathbf{N}$ does there exist a permutation matrix P such that all principal submatrices of the column permuted Fourier matrix $\mathcal{F}_N P$ are non-singular?

Introduction- Some first cases

- Any 2×2 principal submatrix of $\mathcal{F}_n$ is non-singular iff n is square free n (Cabreli, Molter, Negreira and Caragea, Lee (2024))
- For $n > 4$, any 3×3 principal submatrix is non-singular iff n is square free (Caragea, Lee (2024))
- Any $k \times k$ submatrix of $\mathcal{F}_n$ is invertible if and only if any $(n-k) \times (n-k)$ is invertible (Works for unitary matrices)
- If n is divisible by the square of a prime, then $\mathcal{F}_n$ has principal submatrices of size $r \times r$ with determinant zero for all r between 2 and $n-2$(Caragea, Lee (2024)).

Results

Theorem (L, 2024)

Conjecture holds when a) $n = 2p$ with p an odd prime, and b) $n = rp$ with r, p distinct odd primes, p primitive in $\mathbb{Z}_r$ and big enough ($p > \Gamma_r$).

A bit more is shown: submatrices of a specific type (principals included) are non-singular.

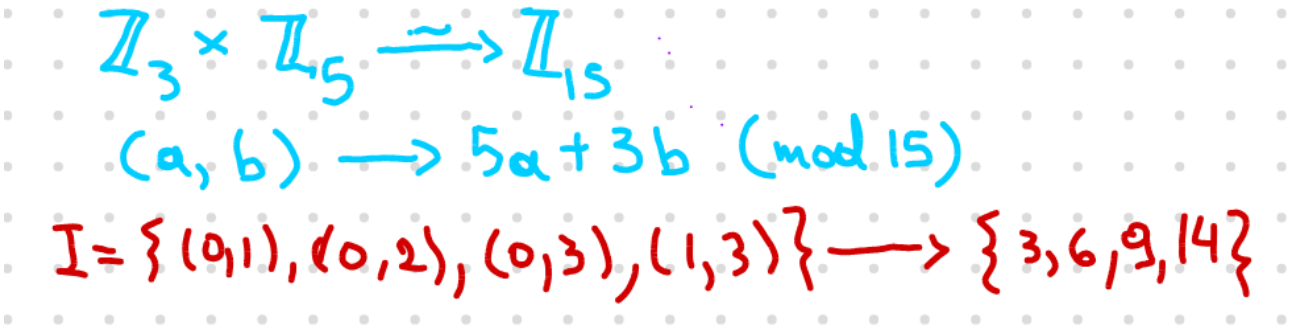
Some notation

$$n = pr,\ \mathcal{F}_n = (\zeta_n^{ij})$$

The map

$$\mathbb{Z}_p \times \mathbb{Z}_r \ni (i_p,\ i_r) \longrightarrow i \in \mathbb{Z}_n$$

with $i \equiv i_p \cdot r + i_r \cdot p \pmod{pr}$ is an isomorphism. For example:



$$\zeta_n^i = (\zeta_n^r)^{i_p} \cdot (\zeta_n^p)^{i_r} = \zeta_p^{i_p} \cdot \zeta_r^{i_r}$$

and

$$\zeta_n^{ij} = \zeta_p^{ri_pj_p} \cdot \zeta_r^{pi_rj_r}$$

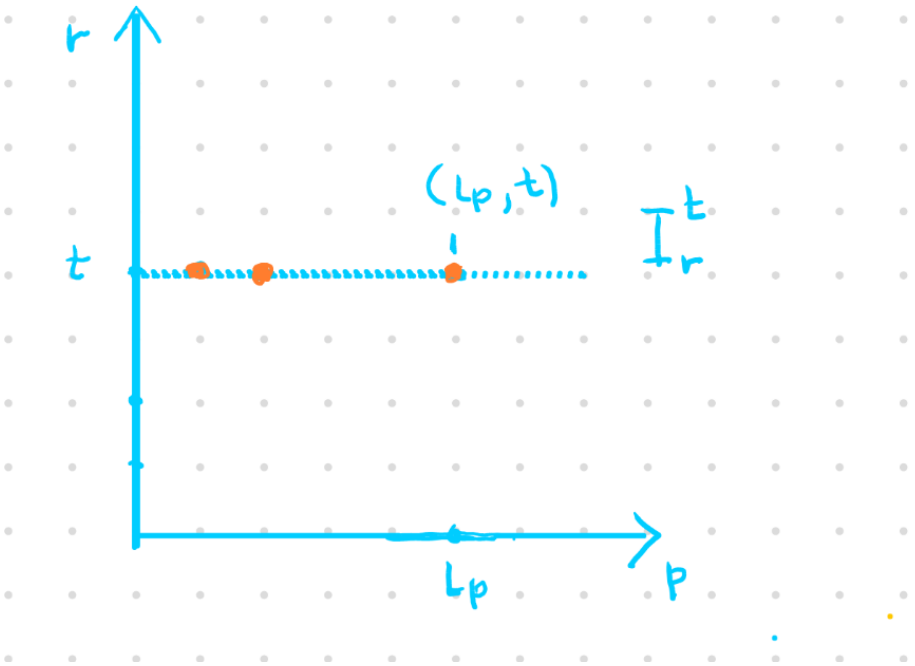
Some notation

If $I \subseteq \mathbb{Z}_p \times \mathbb{Z}_r \cong \mathbb{Z}_n$ define

$$I_r^t = \{i \in I \mid i_r = t\}$$

for $t = 0, 1, \ldots, r-1$. Observe

$$I = \dot{\bigcup}_t I_r^t$$

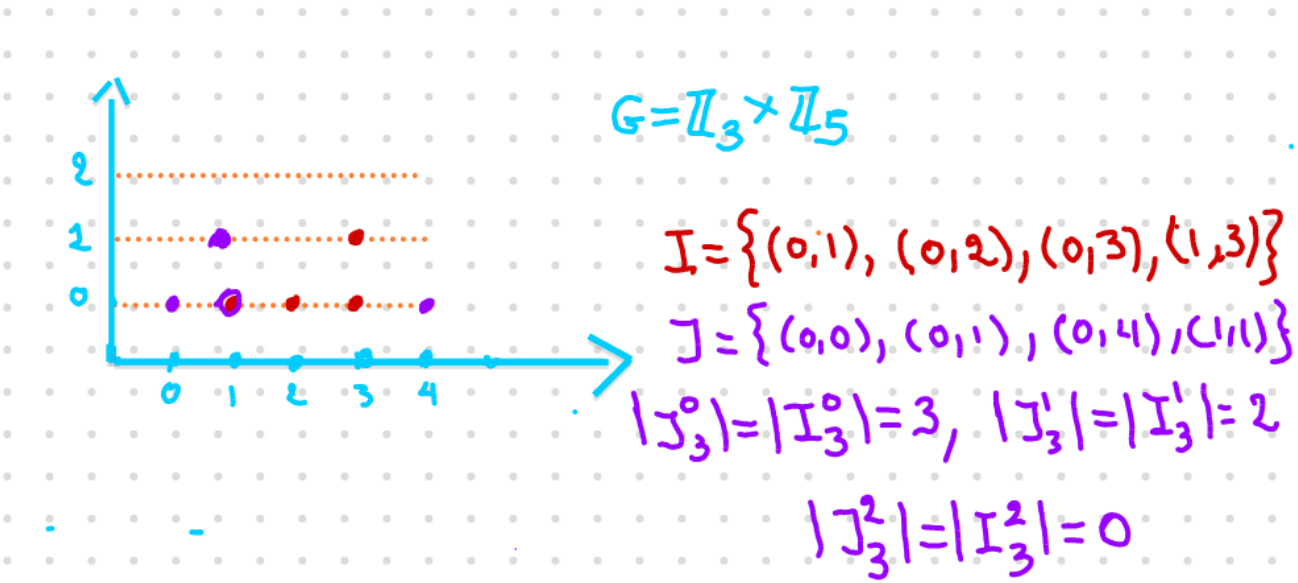


A more general result

Our main result states:

Theorem (L, 2024)

Let $n = pr$, where p and r are distinct odd primes such that p is primitive in $\mathbb{Z}_r$ and $p > \Gamma_r$. If $I, J \leq \mathbb{Z}_n$ with $|I_r^k| = |J_r^k|$, for all $k = 0, 1, \cdots, r-1$, then the matrix $(\zeta_n^{ij})_{i \in I, j \in J}$ has nonzero determinant.



Sketch of the proof

- We follow Frenkel's approach to Chebotarev's theorem.
- Fix $n = pr$, I, J as in the Theorem. Get

$$B = (\zeta_n^{ij})_{i \in I, j \in J}$$

  Need to show B is non-singular
- B is non-singular **iff** whenever $z_j \in \mathbb{Q}(\zeta_n)$ satisfy

$$\sum_{j \in J} z_j \zeta_n^{ij} = 0, \ \forall i \in I$$

  then $z_j = 0$ for every $j \in J$.
- without loss may assume $z_j \in \mathbb{Z}[\zeta_n]$ (multiply by denominators)

Sketch of the proof

- We follow Frenkel's approach to Chebotarev's theorem.
- Fix $n = pr$, I, J as in the Theorem. Get

$$B = (\zeta_n^{ij})_{i \in I, j \in J}$$

  Need to show B is non-singular
- B is non-singular **iff** whenever $z_j \in \mathbb{Q}(\zeta_n)$ satisfy

$$\sum_{j \in J} z_j \zeta_n^{ij} = 0, \ \forall i \in I$$

  then $z_j = 0$ for every $j \in J$.
- without loss may assume $z_j \in \mathbb{Z}[\zeta_n]$ (multiply by denominators)
- The problem is translated to: Let

$$r(x) := \sum_{j \in J} z_j x^j \in \mathbb{Z}[\zeta_n][x]$$

- If $r(x)$ vanishes at ζ_n^i for all $i \in I$ (with I, J, n as in the theorem),
- then $r(x)$ is the zero polynomial.

Sketch of the proof

- It suffices to show that all z_j are divisible by $1-\zeta_p$ in $\mathbb{Z}[\zeta_n]$. Why?

Sketch of the proof

- It suffices to show that all z_j are divisible by $1-\zeta_p$ in $\mathbb{Z}[\zeta_n]$. Why?
- Because: We divide with $1-\zeta_p$ and iterate the argument leading to *descent infinie*.
- $\mathbb{Z}[\zeta_n]$ is a Dedekind domain so there is a max power of the prime ideal $\langle 1-\zeta_p \rangle$ that divides every ideal $\langle z_j \rangle$.

Sketch of the proof

- Define

$$g(x,y) := \sum_{j\in J} z_j x^{j_p} y^{j_r} \in \mathbb{Z}[\zeta_n][x,y].$$

So

- $$g(\zeta_p^{ri_p}, \zeta_r^{pi_r}) = \sum_{j\in J} z_j \zeta_p^{ri_p j_p} \zeta_r^{pi_r j_r} = \sum_{j\in J} z_j \zeta_n^{ij} = 0$$

for all $i \in I$.

Sketch of the proof

- $$J_r^k := \{j \in J \mid j_r = k\} \neq \emptyset$$

  and $|J_r^k| = |I_r^k|$
- Put them in order $0 < |I_r^{k_1}| \leq |I_r^{k_2}| \leq \cdots \leq |I_r^{k_{|L|}}|$
- For $t \in L = \{k_1, \cdots, k_{|L|}\}$ define

$$T_t(x) := g(x, \zeta_r^{pt}) = \sum_{k \in L} \zeta_r^{ptk} \sum_{j \in J_r^k} z_j x^{j_p} \in \mathbb{Z}[\zeta_n][x]$$

- $T_t(\zeta_p^{ri_p}) = 0$ for all $i \in I_r^t$.
- Note $I_r^t \ni i = (i_p, t)$ and so $\zeta_p^{ri_p}$ are all distinct, as i_p are all distinct

Sketch of the proof

- Rewrite $T_t(x) = \sum_{k \in L} \zeta_r^{ptk} S_k(x)$ with $S_k(x) = \sum_{j \in J_r^k} z_j x^{j_p}$
- End up with the system

$$\begin{pmatrix} T_1(x) \\ \vdots \\ T_{|L|}(x) \end{pmatrix} = R \cdot \begin{pmatrix} S_1(x) \\ \vdots \\ S_{|L|}(x) \end{pmatrix}$$

- The matrix $R = (R_{t,k}) = (\zeta_r^{ptk})_{t,k \in L} = (\omega_r^{tk})_{t,k \in L}$, and $\omega_r = \zeta_r^p$ a primitive r-th root.
- Note all the coefficients are in $\mathbb{Z}[\zeta_n]$
- Now we mod out everything with the ideal $\langle 1 - \zeta_p \rangle$ i.e. work in the quotient $\mathbb{Z}[\zeta_n]/\langle 1 - \zeta_p \rangle$.

Sketch of the proof

Lemma(L, 2024)

Assume p, r are distinct odd primes such that p is primitive in $\mathbb{Z}_r$. Then

$$\mathbb{Z}[\zeta_{pr}]/\langle 1-\zeta_p\rangle = \mathbb{F}_{p^{r-1}}$$

and the image $\bar{\zeta}_r$ of $\zeta_r \in \mathbb{Z}[\zeta_{pr}]$ in $\mathbb{Z}[\zeta_{pr}]/\langle 1-\zeta_p\rangle$ is also a primitive r-th root of unity in $\mathbb{F}_{p^{r-1}}$.

$$\text{We get } \begin{pmatrix} \bar{T}_1(x) \\ \vdots \\ \bar{T}_{|L|}(x) \end{pmatrix} = \bar{R} \cdot \begin{pmatrix} \bar{S}_1(x) \\ \vdots \\ \bar{S}_{|L|}(x) \end{pmatrix}$$

$\bar{R}$ is invertible by Zhang's Theorem!!

Sketch of the proof

- Solve for $\bar{S}_i$ to get

$$\bar{S}_{k_1}(x) = \sum_{t \in L} \bar{a}_t \bar{T}_t(x)$$

  with $\bar{a}_t \in \mathbb{Z}[\zeta_n]/\langle 1 - \zeta_p \rangle$
- But $\bar{T}_t(x)$ is divisible by $(x - \bar{1})^{|I_r^t|}$
- So $\bar{S}_{k_1}$ is divisible by $(x - \bar{1})^{|I_r^{k_1}|}$
- $\bar{1}$ is a root of $\bar{S}_{k_1}$ of multiplicity at least $|I_r^{k_1}|$
- By hypothesis $|J_r^{k_1}| = |I_r^{k_1}|$

Sketch of the proof

- By definition

$$S_{k_1}(x) = \sum_{j \in J_r^{k_1}} z_j x^{j_p}$$

- Thus, the number of non-zero coefficients of $\bar{S}_{k_1}(x)$ is at most $|J_r^{k_1}|$

Lemma (Frenkel, 2004)

Let $\mathbb{F}$ be a finite field of characteristic p and $0 \neq g(x) \in \mathbb{F}[x]$ be a polynomial of degree $< p$. If $0 \neq a \in \mathbb{F}$ is a root of $g(x)$ then its multiplicity is strictly less that the number of non-zero coefficients of $g(x)$.

- Hence $\bar{S}_{k_1} = 0$, by Frenkel's lemma, i.e.

$$(1 - \zeta_p) \mid z_j, \quad \text{for all } j \in J_r^{k_1}$$

Sketch of the proof

- Repeat the argument for the system

$$\begin{pmatrix} \bar{T}_{k_2}(x) \\ \vdots \\ \bar{T}_{k_{|L|}}(x) \end{pmatrix} = \bar{D} \cdot \begin{pmatrix} \bar{S}_{k_2}(x) \\ \vdots \\ \bar{S}_{k_{|L|}}(x) \end{pmatrix}$$

  with $\bar{D} = (\bar{D}_{k_t,k_l}) = (\bar{\omega}_r^{k_t k_l})_{k_t,k_l \neq k_1}$.
- Get $\bar{S}_{k_2} = \bar{0}$.
- Repeat. End up with $\bar{S}_{k_i} = \bar{0}$ for $i = 1, \cdots, |L|$.
- But $S_k(x) = \sum_{j \in J_r^k} z_j x^{j_p}$. So $1 - \zeta_p$ divides z_j for all $j \in J_r^k$
- Also $\bigcup_{i=1}^{|L|} J_r^{k_i} = J$

Sketch of the proof

Hence the initial polynomial

$$r(x) = \sum_{j \in J} z_j x^j$$

has coefficients all divisible by $1 - \zeta_p$!!!!

Uncertainty Principle

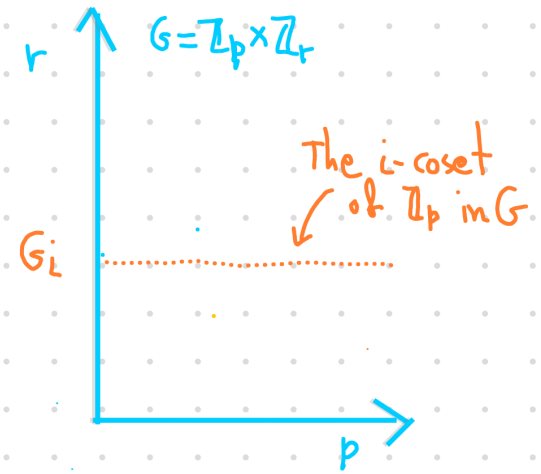
As a corollary we get an "Uncertainty Principle"

Corollary (L, 2024)

Let p and r be distinct odd primes, with p being primitive in $\mathbb{Z}_r$ and $p > \Gamma_r$. If $f : G := \mathbb{Z}_p \times \mathbb{Z}_r \to \mathbb{C}$ is a non-zero function, then for at least one $i \in \{0, 1, \ldots, r-1\}$, we have

$$|\mathrm{supp}\,(f) \cap G_i| + |\mathrm{supp}\,(\widehat{f}) \cap \widehat{G}_i| \geq p + 1.$$

where $G_i = \mathbb{Z}_p \times \{i\} = \{(k, i) \mid k \in \mathbb{Z}_p\}$.



Uncertainty Principle-Sketch of the proof

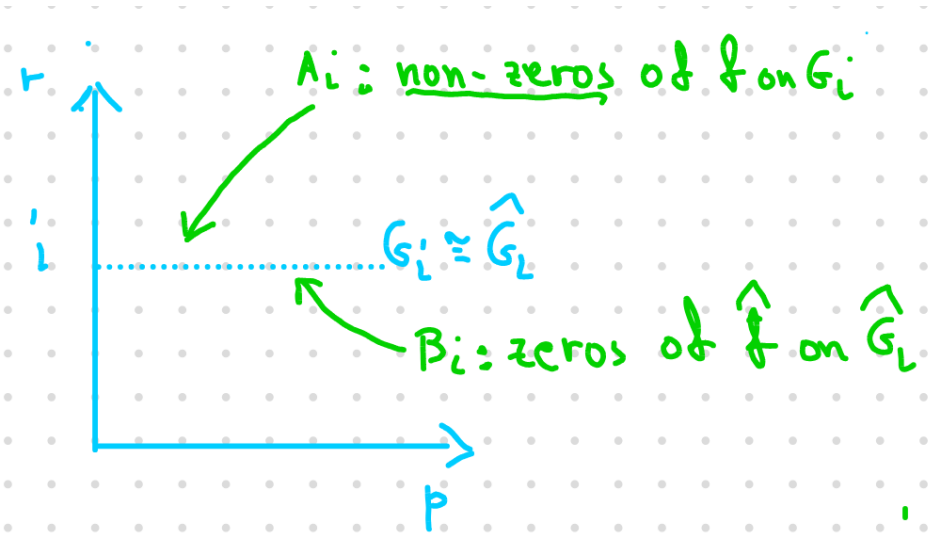
- Assume not, then for all $i = 0, 1, \cdots, r-1$,

$$|\mathrm{supp}\,(f) \cap G_i| + |\mathrm{supp}\,(\widehat{f}) \cap \widehat{G}_i| \leq p$$

so

$$|\mathrm{supp}\,(f) \cap G_i| \leq p - |\mathrm{supp}\,(\widehat{f}) \cap \widehat{G}_i|$$

- Let $A_i := \mathrm{supp}\,(f) \cap G_i$.
- Then there exists $B_i \subseteq \widehat{G}_i$ with $|A_i| = |B_i|$ and $\widehat{f}(b) = 0$ for every $b \in B_i$.



Uncertainty Principle-Sketch of the proof

- If

$$A := \bigcup_{i=0}^{r-1} A_i \text{ and } \quad B = \bigcup_{i=0}^{r-1} B_i$$

- Then $A = \operatorname{supp} f$ and $\widehat{f}|_B = 0$.

Uncertainty Principle-Sketch of the proof

- If
$$A := \bigcup_{i=0}^{r-1} A_i \text{ and } \quad B = \bigcup_{i=0}^{r-1} B_i$$
- Then $A = \operatorname{supp} f$ and $\widehat{f}|_B = 0$.
- The matrix $(\zeta_{rm}^{ji})_{i\in A, j\in B}$ defines a linear map $T : l^2(A) \to l^2(B)$.
- $T(f) = \widehat{f}|_B = 0$ for the non-zero function f.
- Hence the matrix $(\zeta_{rm}^{ji})_{i\in A, j\in B}$ is singular.
- Contradiction to the theorem (as A, B satisfy the hypothesis: same cardinality at every i-level)

A bit of algebraic number theory

We want to prove

Lemma(L, 2024)

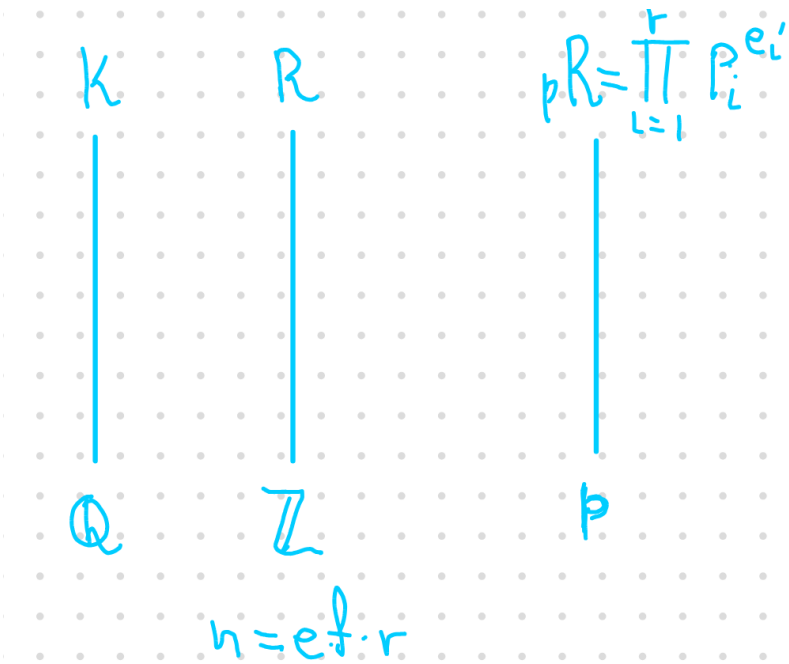
Assume p, r are distinct odd primes such that p is primitive in $\mathbb{Z}_r$. Then

$$\mathbb{Z}[\zeta_{pr}]/\langle 1-\zeta_p\rangle = \mathbb{F}_{p^{r-1}}$$

and the image $\bar{\zeta}_r$ of $\zeta_r \in \mathbb{Z}[\zeta_{pr}]$ in $\mathbb{Z}[\zeta_{pr}]/\langle 1-\zeta_p\rangle$ is also a primitive r-th root of unity in $\mathbb{F}_{p^{r-1}}$.

- $K/\mathbb{Q}$ Galois, $[K:\mathbb{Q}] = n$, R alg. integ. of K,
- $e = e(P_i/p)$ ramification index, $f = f(P_i/p)$ residual degree,
- $f = [R/P : \mathbb{Z}_p]$

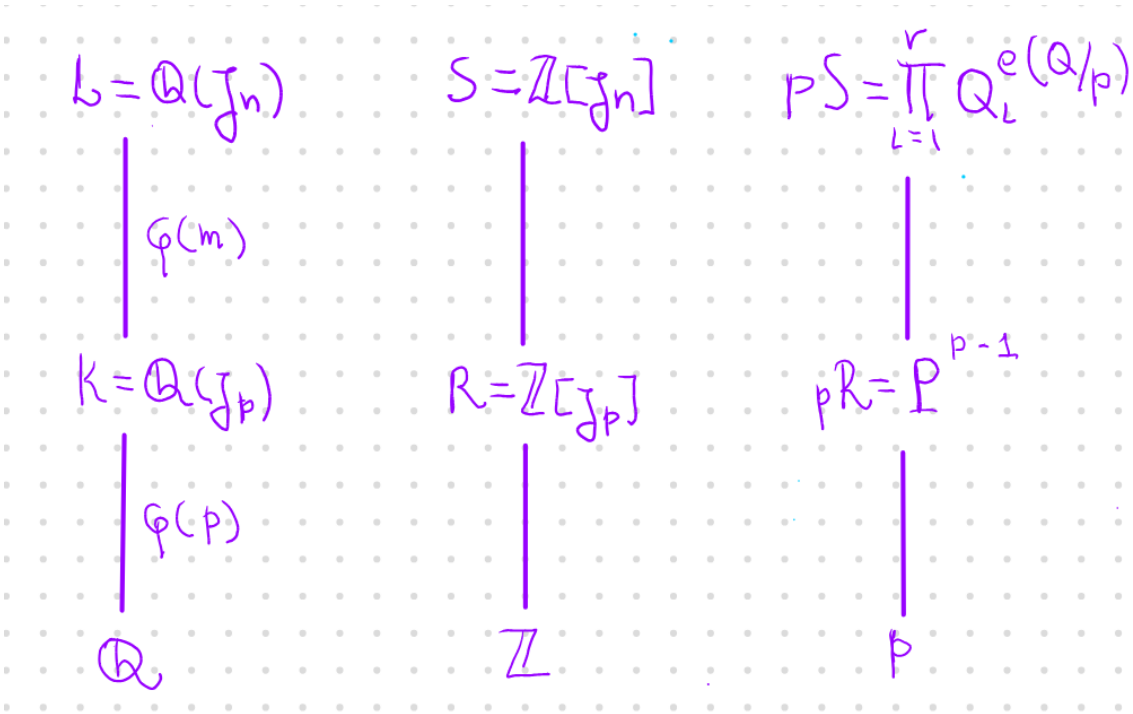
A bit of algebraic number theory



- If $K = \mathbb{Q}(\zeta_n)$ then $R = \mathbb{Z}[\zeta_n]$
- Assume $n = pm$ and $(p, m) = 1$
  Then
- $e = p - 1,\ r = \frac{\phi(m)}{h}$ with h the order of p in $\mathbb{Z}_m^*$

Sketch of the proof of Lemma

Want: $\mathbb{Z}[\zeta_n]/\langle 1-\zeta_p\rangle = S/PS$ to be a finite field



$P = (1-\zeta_p)R$ unique above $p\mathbb{Z}$

- Have $pR = P^{p-1}$ so $e(P/p) = p-1$ and $f(P/p) = 1$
- L/Q Galois so

$$pS = \prod_{i=1}^{r} Q_i^{e(Q/p)}$$

with $e(Q_i/p) = p-1$ and $r = \frac{\phi(m)}{h}$ where h is the order of p in the multiplicative group $\mathbb{Z}_m^*$

Sketch of the proof of Lemma

- L/K Galois so

$$PS = \prod_{i=1}^{r} Q_i^{e(Q/P)}.$$

- $PS = \langle 1-\zeta_p \rangle S$ prime **iff** $r = 1$ **iff** $\phi(m) = h$
- Transitivity of ramification

$$p-1 = e(Q/p) = e(Q/P)\cdot e(P/p) = e(Q/P)\cdot(p-1) \iff e(Q/P) = 1$$

- So for $r = 1$ get $PS = Q$ and
- $\phi(m) = h = f(Q/p) = [S/Q : \mathbb{Z}/p\mathbb{Z}] = [\mathbb{Z}[\zeta_n]/\langle 1-\zeta_p \rangle : \mathbb{Z}_p]$
- Hence $\mathbb{Z}[\zeta_n]/\langle 1-\zeta_p \rangle$ is a finite field of order $p^h = p^{\phi(m)}$
- $\mathbb{Z}_m^*$ is cyclic iff $m = 2, 4, q^k$ or $2q^k$ (done by Gauss)

Current status of the conjecture

Theorem (Caragea-Lee-Malikiosis-Pfander, 2025)

Assume $N = p_1 \cdots p_k$ for primes with $p_1 < p_2 < \cdots < p_k$ and $p_{j+1} > \Gamma_j$ where Γ_j depends on $p_1 p_2 \cdots p_j$. Then all principal submatrices of $\mathcal{F}_N$ are non-singular.

Their result uses

- Tao's approach of Chebotarev's theorem, and
- An improvement of Zhang's theorem where the condition of primitivity is removed, but the bounds are kept the same.

Simultaneously and independently:

Theorem (Emmrich and Kunis, 2025)

Let $p, r \in \mathbf{N}$ be two distinct primes, $\omega_r \in \mathbb{F}_{p^{r-1}}$ be a r-th root of unity, and p sufficiently large, then all submatrices of the matrix (ω_r^{ij}) have non-zero determinant in $\mathbb{F}_{p^{r-1}}$.

Their bounds are considerably improved.

Current status of the conjecture

As far as the question of C-L-M-P regarding the permutation matrix, they found a counterexample:

Theorem (Caragea-Lee-Malikiosis-Pfander, 2025)

If $N = 16$ no permutation P exists so that the matrix $\mathcal{F}_{16}P$ has all its pincipal submatrices non-singular.

The refined new question is:

Question (Caragea-Lee-Malikiosis-Pfander, 2025)

Does there exist a permutation matrix P , so that all principal minors of $\mathcal{F}_N P$ are non-zero, exactly if N is not divisible by a fourth power of a prime?

谢谢

Thank you!