Problem Set Week 9 Solutions

Math Olympiad Club Zurich

Spring 2025

Problem: X-ENS 11 Orals

Let $(G, \cdot, e_G)$ be a finite non-commutative group. Show that the probability that two elements $x, y \in G$ chosen uniformly at random commute is less than or equal to $\frac{5}{8}$, and show that this bound is tight, i.e., provide an example where the bound is attained.

Solution:

Take the probability space:

$$(\Omega, \mathcal{F}, \mathbb{P}) := \left(G \times G, \mathscr{P}(G \times G), \frac{|\cdot|}{|G|^2}\right).$$

Define the event $C = \{(x, y) \in \Omega \mid x \cdot y = y \cdot x\} \in \mathcal{F}$. We need to show $\mathbb{P}(C) \leq \frac{5}{8}$. To study the commutativity of an element, one (left) group action is particularly useful—namely, the conjugation action:

$$\phi : G \longrightarrow \mathrm{Aut}_{\mathrm{Ens}}(G),$$

where $\phi(a) : G \longrightarrow G$ is defined by $\phi(a)(g) = a \cdot g \cdot a^{-1}$.

Under this group action ϕ, we can rewrite:

$$\begin{aligned} C &= \left\{(x, y) \in \Omega \mid x \cdot y \cdot x^{-1} = y\right\} \\ &= \{(x, y) \in \Omega \mid \phi(x)(y) = y\} \\ &= \{(x, y) \in \Omega \mid y \in \mathrm{Stab}_\phi(x)\}. \end{aligned}$$

Therefore:

$$C = \bigsqcup_{x \in G} \{x\} \times \mathrm{Stab}_\phi(x).$$

To compute $\mathbb{P}(C)$, we need to compute $|C|$, which is equal to the sum of the cardinalities of the stabilisers under the conjugation action ϕ. But we can do better:

Fix $\tilde{x} \in G$. Then either $\tilde{x}$ commutes with all elements—i.e., $\tilde{x} \in Z(G) \Leftrightarrow \mathrm{Stab}_\phi(\tilde{x}) = G$—or it does not—i.e., $\tilde{x} \in G \setminus Z(G) \Leftrightarrow \mathrm{Stab}_\phi(\tilde{x}) \subsetneq G$. Thus, we can further decompose C as:

$$\begin{aligned} C &= \left(\bigsqcup_{x \in Z(G)} \{x\} \times G\right) \sqcup \left(\bigsqcup_{x \in G \setminus Z(G)} \{x\} \times \mathrm{Stab}_\phi(x)\right) \\ &= (Z(G) \times G) \sqcup \left(\bigsqcup_{x \in G \setminus Z(G)} \{x\} \times \mathrm{Stab}_\phi(x)\right). \end{aligned}$$

Let us compute $|C|$:

$$|C| = |Z(G) \times G| + \sum_{x \in G \setminus Z(G)} |\{x\} \times \mathrm{Stab}_\phi(x)| = |Z(G)| \cdot |G| + \sum_{x \in G \setminus Z(G)} |\mathrm{Stab}_\phi(x)|. \quad (*)$$

This equation is valid for any finite group G. Now, since for every group action the stabiliser is a subgroup of the group, by Lagrange's theorem $|\mathrm{Stab}_\phi(x)| \mid |G|$. Moreover, the orbit–stabiliser theorem gives:

$$|G| = |\mathrm{Orb}_\phi(x)| \cdot |\mathrm{Stab}_\phi(x)| \Rightarrow |\mathrm{Stab}_\phi(x)| = \frac{|G|}{|\mathrm{Orb}_\phi(x)|}.$$

For $x \notin Z(G)$, we have (by the finiteness of G) that $|\mathrm{Stab}_\phi(x)| < |G|$, so:

$$|\mathrm{Stab}_\phi(x)| = \frac{|G|}{|\mathrm{Orb}_\phi(x)|} \leq \frac{|G|}{2}. \quad (1)$$

This equation is valid for any finite non-commutative group.

Therefore:

$$|C| \leq |Z(G)| \cdot |G| + \sum_{x \in G \setminus Z(G)} \frac{|G|}{2} = |G| \cdot \left(|Z(G)| + \frac{|G| - |Z(G)|}{2} \right) = |G| \cdot \frac{|G| + |Z(G)|}{2}.$$

Since G is non-commutative, $Z(G) \subsetneq G$. Take $\hat{x} \in G \setminus Z(G)$. Then since $\hat{x} \in \mathrm{Stab}_\phi(\hat{x})$ and $\hat{x} \notin Z(G)$, we must have:

$$Z(G) \subsetneq \mathrm{Stab}_\phi(\hat{x}) \subsetneq G.$$

Because everything is finite, we have by Lagrange's theorem (all of them are strict subgroups):

$$|Z(G)| \leq \frac{|\mathrm{Stab}_\phi(\hat{x})|}{2} \leq \frac{\frac{|G|}{2}}{2} = \frac{|G|}{4}. \quad (2)$$

This equation is also valid for any finite non-commutative group.

We conclude:

$$|C| \leq |G| \cdot \frac{|G| + \frac{|G|}{4}}{2} = |G|^2 \cdot \frac{5}{8} \Rightarrow \mathbb{P}(C) \leq \frac{5}{8},$$

as desired.

To show that the bound is tight, consider the non-commutative quaternion group Q_8[1] of 8 elements:

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}, \quad i^2 = j^2 = k^2 = ijk = -1.$$

[1] We can realise Q_8 concretely as a subgroup of $GL_4(\mathbb{Q})$, where

$$1 = I_4, \quad i := \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}, \quad j := \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad k := \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix},$$

or abstractly as the quotient group

$$\left\langle x, y \mid x^4 = 1 = y^4,\, x^2 = y^2,\, y^{-1}xy = x^{-1} \right\rangle := F(\{x, y\}) \,/\, \left\langle\!\left\langle x^4,\, y^4,\, x^2y^{-2},\, y^{-1}xyx \right\rangle\!\right\rangle,$$

where $F(\{x, y\})$ is the free group on two generators and $\left\langle\!\left\langle x^4,\, y^4,\, x^2y^{-2},\, y^{-1}xyx \right\rangle\!\right\rangle$ is the normal subgroup generated by the relations $x^4 = y^4 = 1$, $x^2 = y^2$, and $y^{-1}xy = x^{-1}$. The generators x and y correspond to any two distinct elements of Q_8, interpreted as i and j (in any order), while the element k can be defined as ij^{-1} in the chosen interpretation for i, j.

As seen in (2), the size of $Z(Q_8)$ is bounded above by $\frac{8}{4} = 2$. Since ± 1 commutes with every element, the centre must be $Z(Q_8) = \{\pm 1\}$. For any element not in the centre, $s \in \{\pm i, \pm j, \pm k\}$, we have seen in (1) that its stabiliser must satisfy

$$2 = |Z(Q_8)| < |\mathrm{Stab}_\phi(s)| < |Q_8| = 8,$$

so the only possibility is that its size is 4 (from this, we can directly deduce that $\mathrm{Stab}_\phi(s) = \{\pm 1, \pm s\}$, which is unnecessary, since we only require the cardinalities). Combining all of this in equation (*), we obtain:

$$\begin{aligned} |C| &= |Z(Q_8)| \cdot |Q_8| + \sum_{s \in Q_8 \setminus Z(Q_8)} |\mathrm{Stab}_\phi(s)| \\ &= |\{\pm 1\}| \cdot |Q_8| + \sum_{s \in \{\pm i, \pm j, \pm k\}} |\mathrm{Stab}_\phi(s)| \\ &= 2 \cdot 8 + 6 \cdot 4 = 16 + 24 = 40. \end{aligned}$$

Thus, among the 64 possible ordered pairs in $Q_8 \times Q_8$, exactly 40 commute, giving:

$$\mathbb{P}(C) = \frac{40}{64} = \frac{5}{8}.$$

Hence, the bound is attained.

Problem: from the book Selected Problems in Real Analysis

Let S be a set and $f : S \to S$ a bijection. Show that f can be written as the composition of two involutions, where an involution h is a function that is its own inverse.

Solution:

For an arbitrary point $s \in S$, its orbit is the set of elements

$$s, \quad f(s), \quad f^{-1}(s), \quad f^2(s), \quad f^{-2}(s), \quad \dots$$

Denote it temporarily by $A_s := \{f^n(s) \mid n \in \mathbb{Z}\} \subset S$.

If there exist two involutions $h, k : S \to S$ such that $h \circ k = f$, then for every $n \in \mathbb{Z}$,

$$f^{n+1}(s) = f \circ f^n(s) = (h \circ k)(f^n(s)) \Rightarrow h\left(f^{n+1}(s)\right) = k(f^n(s)).$$

Moreover, we require that $(h \circ h)(f^n(s)) = f^n(s)$ and $(k \circ k)(f^n(s)) = f^n(s)$, so we may consider two auxiliary involutions of $\mathbb{Z}$, $k', h' : \mathbb{Z} \to \mathbb{Z}$, satisfying

$$h'(n+1) = k'(n). \tag{1}$$

Such h', k' will help us define involutions on A_s; we want to define the following relations (trivially over A_s):

$$\hat{h} := \left\{\left(f^n(s), f^{h'(n)}(s)\right) \mid n \in \mathbb{Z}\right\}, \quad \hat{k} := \left\{\left(f^n(s), f^{k'(n)}(s)\right) \mid n \in \mathbb{Z}\right\},$$

such that they are functional. That is, for $m, m' \in \mathbb{Z}$, if $f^m(s) = f^{m'}(s)$, then

$$f^{h'(m)}(s) = f^{h'(m')}(s) \quad \text{and} \quad f^{k'(m)}(s) = f^{k'(m')}(s).$$

A simple condition to impose on h' and k' so that $\hat{h}, \hat{k}$ are functional is that for every $m, m' \in \mathbb{Z}$, we have

$$|h'(m) - h'(m')| = |m - m'| = |k'(m) - k'(m')|. \tag{2}$$

Because then, whenever $f^m(s) = f^{m'}(s)$, we get $f^{|m-m'|}(s) = s$, so that:

$$f^{|h'(m)-h'(m')|}(s) = s = f^{|k'(m)-k'(m')|}(s),$$

and thus $f^{h'(m)}(s) = f^{h'(m')}(s)$ and $f^{k'(m)}(s) = f^{k'(m')}(s)$.

Once $\hat{h}, \hat{k} : A_s \to A_s$ are functional, we will get for $n \in \mathbb{Z}$:

$$\left(\hat{h} \circ \hat{k}\right)(f^n(s)) = f^{h' \circ k'(n)}(s) = f^{n+1}(s) = f(f^n(s)),$$

and

$$\left(\hat{h} \circ \hat{h}\right)(f^n(s)) = f^{h' \circ h'(n)}(s) = f^n(s) = f^{k' \circ k'(n)}(s) = \left(\hat{k} \circ \hat{k}\right)(f^n(s)).$$

Therefore, by the arbitrariness of $n \in \mathbb{Z}$, $\hat{h}, \hat{k}$ will be two involutions of A_s such that $\hat{h} \circ \hat{k} = f|_{A_s}$, and it would suffice to "repeat" the process for another $s' \in S \setminus A_s$.

So we must find involutions k', h' of $\mathbb{Z}$ that satisfy the properties (1) and (2). For example, we may choose the simplest involution $k' := -\mathrm{id}_{\mathbb{Z}}$, which is clearly an involution. The corresponding involution $h' : \mathbb{Z} \to \mathbb{Z}$ satisfying (1)

$$h'(n) := k'(n-1) = -(n-1) = -n + 1$$

is also an involution, since

$$h'\left(h'\left(n\right)\right) = -h'\left(n\right) + 1 = -\left(-n+1\right) + 1 = n - 1 + 1 = n = \mathrm{id}_{\mathbb{Z}}\left(n\right).$$

By construction, h', k' satisfy (1) and are involutions. Moreover, k', h' trivially satisfy (2). So $\hat{h}, \hat{k}$ are functional relations and, by the above, they are involutions of A_s with $\hat{h} \circ \hat{k} = f|_{A_s}$.

Now, let us formalise our argument. Consider the subgroup $f^{\mathbb{Z}} := \langle\{f\}\rangle \leq \mathrm{Aut}_{\mathrm{Ens}}(S)$. It acts on the left of S via the group action

$$\mathrm{eval} : f^{\mathbb{Z}} \longrightarrow \mathrm{Aut}_{\mathrm{Ens}}(S),$$

where, for each $g \in f^{\mathbb{Z}}$, we define $\mathrm{eval}(g) : S \to S$ by $\mathrm{eval}(g)(s) := g(s)$.

For an arbitrary point $s \in S$, its orbit is given by $\mathrm{Orb}_{\mathrm{eval}}(s)$, and it cannot be empty. Consider the set of all such orbits. Then, by the axiom of choice[2], there exists a function

$$\chi : \{\mathrm{Orb}_{\mathrm{eval}}(s) \mid s \in S\} \longrightarrow \bigcup_{s \in S} \mathrm{Orb}_{\mathrm{eval}}(s)$$

such that, for every $s \in S$, we have $\chi\left(\mathrm{Orb}_{\mathrm{eval}}(s)\right) \in \mathrm{Orb}_{\mathrm{eval}}(s)$. Since the set of orbits of a group action on a set S partitions S, this yields the disjoint decomposition:

$$S = \bigsqcup_{t \in \mathrm{ran}(\chi)} \mathrm{Orb}_{\mathrm{eval}}(t).$$

Inspired by our previous construction, we now need to define the involutions on each disjoint orbit; $\forall t \in \mathrm{ran}(\chi)$, $\mathrm{Orb}_{\mathrm{eval}}(t)$. This is captured, by defining the following relations:

$$\hat{h} := \left\{ \left(s, f^{-m+1}\left(\chi\left(\mathrm{Orb}_{\mathrm{eval}}\left(s\right)\right)\right)\right) \,\middle|\, \exists s \in S\, \exists m \in \mathbb{Z} \text{ such that } f^m\left(\chi\left(\mathrm{Orb}_{\mathrm{eval}}\left(s\right)\right)\right) = s \right\},$$

$$\hat{k} := \left\{ \left(s, f^{-m}\left(\chi\left(\mathrm{Orb}_{\mathrm{eval}}\left(s\right)\right)\right)\right) \,\middle|\, \exists s \in S\, \exists m \in \mathbb{Z} \text{ such that } f^m\left(\chi\left(\mathrm{Orb}_{\mathrm{eval}}\left(s\right)\right)\right) = s \right\}.$$

Then $\hat{h}, \hat{k}$ are relations on S, since for any $s \in S$, the condition

$$\exists m \in \mathbb{Z} \text{ such that } f^m\left(\chi\left(\mathrm{Orb}_{\mathrm{eval}}(s)\right)\right) = s$$

is always met, because we always have

$$s \in \mathrm{Orb}_{\mathrm{eval}}(s) = \mathrm{Orb}_{\mathrm{eval}}\left(\chi\left(\mathrm{Orb}_{\mathrm{eval}}(s)\right)\right),$$

in other words, there exists $m \in \mathbb{Z}$ such that $s = f^m\left(\chi\left(\mathrm{Orb}_{\mathrm{eval}}(s)\right)\right)$.

Moreover, $\hat{h}, \hat{k}$ are functional relations: for any $s \in S$ and $m, m' \in \mathbb{Z}$ such that

$$f^m\left(\chi\left(\mathrm{Orb}_{\mathrm{eval}}(s)\right)\right) = f^{m'}\left(\chi\left(\mathrm{Orb}_{\mathrm{eval}}(s)\right)\right),$$

we obtain

$$f^{m-m'}\left(\chi\left(\mathrm{Orb}_{\mathrm{eval}}(s)\right)\right) = \chi\left(\mathrm{Orb}_{\mathrm{eval}}(s)\right),$$

which implies by composing with f^{-m} that:

$$f^{-m}\left(\chi\left(\mathrm{Orb}_{\mathrm{eval}}(s)\right)\right) = f^{-m'}\left(\chi\left(\mathrm{Orb}_{\mathrm{eval}}(s)\right)\right),$$

[2] If we are in the finite case, we may construct a choice function by induction.

and by composing with f once:

$$f^{-m+1}\left(\chi\left(\mathrm{Orb}_{\mathrm{eval}}(s)\right)\right) = f^{-m'+1}\left(\chi\left(\mathrm{Orb}_{\mathrm{eval}}(s)\right)\right).$$

Hence $\hat{h}$ and $\hat{k}$ are indeed well-defined functions. Furthermore, they are involutions and satisfy $\hat{h} \circ \hat{k} = f$: for any $s \in S$, there exists $m \in \mathbb{Z}$ with $f^m\left(\mathrm{Orb}_{\mathrm{eval}}(s)\right) = s$, so that, by the well-definedness of $\hat{h}$ and $\hat{k}$, we get

$$\begin{aligned}
\hat{h} \circ \hat{h}(s) &= \hat{h}\left(f^{-m+1}\left(\mathrm{Orb}_{\mathrm{eval}}(s)\right)\right) = f^{-(-m+1)+1}\left(\mathrm{Orb}_{\mathrm{eval}}(s)\right) = f^m\left(\mathrm{Orb}_{\mathrm{eval}}(s)\right) = s, \\
\hat{k} \circ \hat{k}(s) &= \hat{k}\left(f^{-m}\left(\mathrm{Orb}_{\mathrm{eval}}(s)\right)\right) = f^{-(-m)}\left(\mathrm{Orb}_{\mathrm{eval}}(s)\right) = f^m\left(\mathrm{Orb}_{\mathrm{eval}}(s)\right) = s, \\
\hat{h} \circ \hat{k}(s) &= \hat{h}\left(f^{-m}\left(\mathrm{Orb}_{\mathrm{eval}}(s)\right)\right) = f^{-(-m)+1}\left(\mathrm{Orb}_{\mathrm{eval}}(s)\right) \\
&= f^{m+1}\left(\mathrm{Orb}_{\mathrm{eval}}(s)\right) = f\left(f^{-m}\left(\mathrm{Orb}_{\mathrm{eval}}(s)\right)\right) = f(s).
\end{aligned}$$

Since $s \in S$ was arbitrary, we conclude.

Problems: from Sudakov & Milojevic

0.1

Let C_1, C_2, C_3 be disjoint circles in the plane of different radii, and let T_{ij} be the intersection point of the common tangent to C_i and C_j for all $1 \leq i < j \leq 3$. Show that the points T_{12}, T_{23}, and T_{13} lie on a common line.

Solution:

This solution needs to be written more formally

Sketch: Embed the given planar configuration in $\mathbb{R}^3$ so that all three circles C_1, C_2, C_3 lie in some plane π. For each $i = 1, 2, 3$, construct a right circular cone K_i in $\mathbb{R}^3$ whose base is the circle C_i in the plane π and whose apex is placed at a height equal to r_i, the radius of C_i.

Denote by α the plane determined by the three apexes X_1, X_2, X_3 of these cones. Observe that each line T_{ij} (the line determined by the common tangent point in the plane) lifts to a line lying on the lateral surface of these cones. By similar triangles and symmetry, one shows that each T_{ij} lies on the intersection of π (the original plane) with α (the plane of the apexes). Hence T_{12}, T_{23}, T_{13} all lie on the common line $\pi \cap \alpha$. It follows that they are collinear.

0.2

Several spherical planets, each of radius R, are placed in a greenhouse. On each planet, Mark colors in black the regions that are not visible from any other planet by a single straight-line segment. Prove that the total area of the colored regions, summed over all planets, is exactly $4\pi R^2$.

Solution:

This solution needs to be written more formally

The key insight is that for each planet of radius R, the "invisible" zones (where no direct line of sight from another planet can reach) collectively contribute an area equal to the surface area of *one entire sphere* of radius R. Intuitively, imagine taking each planet in turn and considering all lines of sight originating from other planets. The geometry of occlusion ensures each planet has a portion that is fully "shadowed." Summing over all planets leads to the remarkable simplification that the total "shadowed" area is $4\pi R^2$.

In more technical terms, one can show that for every point on a planet's surface that is claimed to be invisible, there is a matching visible point on some other planet's surface, and these pairings add up in such a way that the net invisible area across all planets matches the surface area of one full sphere of radius R. Hence the total blackened area is

$$4\pi R^2.$$

0.3

There is a pile of silver coins on a table. John holds two pieces of paper and performs the following process: at each step, he can add one gold coin to the table and write the current number of silver coins on one piece of paper, or remove one silver coin from the table and write down the current number of gold coins on the other piece of paper. This process runs until no more silver coins remain on the table. Show that at the end of the process, the sums of the numbers on both pieces of paper are equal.

Solution:

This solution needs to be written more formally

See e.g. the solution proposed by Sean Lo at this Post

Problem: Romanian IMO Team Selection Tests 1998

Show that the polynomial with integer coefficient $(X^2+X)^{(2^n)}+1 \in \mathbb{Z}[X]$ is irreducible over $\mathbb{Q}[X]$.

Solutions:

Solution 1.

Fix $n \in \mathbb{N}$ and define the integer polynomial $P(X) := (X^2+X)^{(2^n)}+1 \in \mathbb{Z}[X]$. Since $P(X)$ is monic, it is primitive. The irreducibility of $P(X)$ over $\mathbb{Q}[X] = \mathrm{Frac}(\mathbb{Z})[X]$ is therefore equivalent, by Gauss's Lemma III, to its irreducibility over $\mathbb{Z}[X]$.

Suppose, for the sake of contradiction, that $P(X)$ is reducible over $\mathbb{Z}[X]$. Then there exist $Q(X), T(X) \in \mathbb{Z}[X] \setminus (\mathbb{Z}[X]^\times \cup \{0\})$ such that:

$$P(X) = Q(X)T(X).$$

Since $P(X)$ is monic, we have $Q(X), T(X) \notin \mathbb{Z}$, and we may (by multiplying both polynomials by -1) assume that $Q(X)$ and $T(X)$ are monic as well.

Now, consider the ring reduction morphism $\pi_2 : \mathbb{Z} \twoheadrightarrow \mathbb{F}_2 \hookrightarrow \mathbb{F}_2[X]$. It induces, by the universal property of polynomial rings, a surjective ring reduction morphism $\overline{\pi_2} := \mathrm{ev}_{\pi_2, X} : \mathbb{Z}[X] \twoheadrightarrow \mathbb{F}_2[X]$ with kernel:

$$\ker(\overline{\pi_2}) = 2\mathbb{Z}[X]. \tag{1}$$

Thus, we have the decomposition:

$$\overline{\pi_2}(Q(X))\,\overline{\pi_2}(T(X)) = \overline{\pi_2}(Q(X)T(X)) = \overline{\pi_2}(P(X)) = \left(X^2+X\right)^{(2^n)} + [1]_2.$$

By the freshman's dream (since $\mathrm{char}(\mathbb{F}_2[X]) = 2$), we obtain:

$$\overline{\pi_2}(Q(X))\,\overline{\pi_2}(T(X)) = \left(X^2+X\right)^{(2^n)} + 1_{\mathbb{F}_2} = \left(X^2+X+1_{\mathbb{F}_2}\right)^{(2^n)}.$$

Since $\mathbb{F}_2$ is a field, $X^2+X+1_{\mathbb{F}_2} \in \mathbb{F}_2[X]$ is a polynomial of degree 2 with no roots in $\mathbb{F}_2$ (such as $0^2+0+1=1$ and $1^2+1+1=1$), we conclude that it is irreducible in $\mathbb{F}_2[X]$.

As $\mathbb{F}_2$ is a field, $\mathbb{F}_2[X]$ is a unique factorisation domain (UFD), since deg is a Euclidean function, hence $\mathbb{F}_2[X]$ is Euclidean, thus principal, hence a UFD (or simply $\mathbb{F}_2$ is a UFD hence by the UFD Extension Theorem so is $\mathbb{F}_2[X]$).

Therefore, by unique factorisation, and the fact that $\overline{\pi_2}(Q(X)), \overline{\pi_2}(T(X))$ are each of degree at least 1 (since $Q(X), T(X)$ are monic), there exists $0 < k < 2^n$ such that:

$$\overline{\pi_2}(Q(X)) = \left(X^2+X+1_{\mathbb{F}_2}\right)^k, \quad \overline{\pi_2}(T(X)) = \left(X^2+X+1_{\mathbb{F}_2}\right)^{(2^n)-k}.$$

The form (1) of the kernel $\overline{\pi_2}$, tell us then that there exist $Q'(X), T'(X) \in \mathbb{Z}[X]$ such that:

$$Q(X) = \left(X^2+X+1\right)^k + 2Q'(X), \quad T(X) = \left(X^2+X+1\right)^{(2^n)-k} + 2T'(X).$$

Hence:

$$P(X) = \left(\left(X^2+X+1\right)^k + 2Q'(X)\right)\left(\left(X^2+X+1\right)^{(2^n)-k} + 2T'(X)\right).$$

Let $\epsilon \in \mathbb{C}$ be a root of X^2+X+1, i.e. $\epsilon \in \left\{\frac{-1}{2} \pm \frac{\sqrt{3}}{2}i\right\}$, then from $\epsilon^2+\epsilon=-1$ we obtain $P(\epsilon)=(-1)^{2^n}+1=2$, so:

$$2=\left(\left(\epsilon^2+\epsilon+1\right)^k+2Q'(\epsilon)\right)\cdot\left(\left(\epsilon^2+\epsilon+1\right)^{(2^n)-k}+2T'(\epsilon)\right)\overset{1\leq k\leq 2^n-1}{=}4Q'(\epsilon)T'(\epsilon)$$

This is impossible. Indeed, apply the Euclidean division of $Q'(X)$ and $T'(X)$ by X^2+X+1 in $\mathbb{Z}[X]$ (this is possible since $\mathbb{Z}$ is commutative and X^2+X+1 has an invertible leading coefficient) to obtain unique remainders $r_1(X)=aX+b$, $r_2(X)=cX+d\in\mathbb{Z}[X]$, with $a,b,c,d\in\mathbb{Z}$, and unique $Q''(X),T''(X)\in\mathbb{Z}[X]$ such that:

$$Q'(X)=Q''(X)\left(X^2+X+1\right)+r_1(X),\quad T'(X)=T''(X)\left(X^2+X+1\right)+r_2(X).$$

Then:

$$2=4r_1(\epsilon)r_2(\epsilon)=4(a\epsilon+b)(c\epsilon+d)=4ac\epsilon^2+4(ad+bc)\epsilon+4bd.$$

i.e., after some algebra (using the fact that $\epsilon^2=-\epsilon-1$),

$$\frac{1}{2}=(bd-ac)+(ad+bc-ac)\,\epsilon.$$

From:

$$(bd-ac)+(ad+bc-ac)\,\bar{\epsilon}=\overline{(bd-ac)+(ad+bc-ac)\,\epsilon}=\overline{\frac{1}{2}}$$

$$=\frac{1}{2}=(bd-ac)+(ad+bc-ac)\,\epsilon.$$

We get:

$$(ad+bc-ac)\,(\bar{\epsilon}-\epsilon)=0,$$

and because $\bar{\epsilon}\neq\epsilon$, we must have $(ad+bc-ac)=0$, so that: $\frac{1}{2}=(bd-ac)\in\mathbb{Z}$. This is a clear contradiction. Therefore $P(X)=\left(X^2+X\right)^{(2^n)}+1$ must be irreducible.

Solution 2.

Lemma. *Capelli's Lemma: Let K be a field, and let $P(X),g(X)\in K[X]$. Let $\iota:K\hookrightarrow K^{alg}$ be an algebraic closure of K, and let $\alpha\in K^{alg}$ be a root of $P(X)$. Assume without loss of generality that $K\subset K^{alg}$ (the ring morphism is injective).*

Then the polynomial $P\left(g(X)\right)$ (obtained via the canonical universal evaluation morphism at $g(X)$) is irreducible over $K[X]$ if and only if the following two conditions hold simultaneously:

1. *$P(X)$ is irreducible over $K[X]$, and*
2. *$g(X)-\alpha$ is irreducible over $K(\alpha)[X]$, where $K(\alpha)$ is the smallest subfield of K^{alg} containing $K\cup\{\alpha\}$.*

The proof can be found in Appendix [A.1].

Apply this result to the field $\iota:\mathbb{Q}\hookrightarrow\mathbb{Q}^{\text{alg}}$, and the polynomials $P(X)=X^{(2^n)}+1$ and $g(X)=X^2+X$ in $\mathbb{Q}[X]$. Assume without loss of generality that $\mathbb{Q}\subset\mathbb{Q}^{\text{alg}}\subset\mathbb{C}$ (all ring morphism involved in making the identification are injective and the algebraic closure is unique up to a ring isomorphism). The polynomial $P\left(g(X)\right)=\left(X^2+X\right)^{(2^n)}+1$ is then irreducible over $\mathbb{Q}[X]$ if and only if $P(X)$ is irreducible over $\mathbb{Q}[X]$, and if we fix one of its root $\zeta\in\mathbb{Q}^{\text{alg}}$,

we have that $g(X) - \zeta \in \mathbb{Q}(\zeta)[X]$ is irreducible.

Clearly, $X^{(2^n)} + 1$ is irreducible over $\mathbb{Q}[X]$, since it is the 2^{n+1}-th cyclotomic polynomial:

$$\Phi_{2^{n+1}}(X) = \Phi_2\left(X^{2^{(n+1)-1}}\right) = \Phi_2\left(X^{(2^n)}\right) = X^{(2^n)} + 1.$$

Let $\zeta := \exp\left(\frac{\pi i}{2^n}\right) \in \mathbb{Q}^{\text{alg}}$ be our choice of root in the algebraic closure of $P(X)$ (a primitive 2^{n+1}-th root of unity). To conclude that $P\left(g(X)\right)$ is irreducible it only remains to show that $g(X) - \zeta \in \mathbb{Q}(\zeta)[X]$ is irreducible over $\mathbb{Q}(\zeta)[X]$. Since $g(X) - \zeta$ is of degree 2 and $\mathbb{Q}(\zeta)$ is a field, this is equivalent to show that it has no root in $\mathbb{Q}(\zeta)$. The roots of $g(X) - \zeta$ lie in $\mathbb{Q}^{\text{alg}}$ (since $g(X) - \zeta \in \mathbb{Q}^{\text{alg}}[X]$ and $\mathbb{Q}^{\text{alg}}$ is algebraically closed), moreover they are given by the quadratic formula; for any element $\xi \in \mathbb{Q}^{\text{alg}}$ such that $\xi^2 = 1 + 4\zeta$[3]:

$$\frac{-1 \pm \xi}{2} \text{ is a root of } g(X) - \zeta,$$

i.e.

$$g(X) - \zeta = X^2 + X - \zeta = \left(X + \left(\frac{1-\xi}{2}\right)\right)\left(X + \left(\frac{1+\xi}{2}\right)\right),$$

so it suffices to show that $\frac{-1\pm\xi}{2} \notin \mathbb{Q}(\zeta)$, or equivalently that $\xi \notin \mathbb{Q}(\zeta)$. So without further ado, we suppose for the sake of contradiction that $\xi \in \mathbb{Q}(\zeta)$.

Since $P(X)$ is irreducible and $P(\zeta) = 0$, we have:

$$\mathbb{Q}[X]/\left(P(X)\right) \cong \mathbb{Q}\left(\zeta\right),$$

hence $\mathbb{Q} \hookrightarrow \mathbb{Q}\left(\zeta\right)$ is a finite extension of $\mathbb{Q}$, and therefore algebraic. As $\text{char}\left(\mathbb{Q}\right) = 0$, this extension is separable. Since $P(X)$ splits over $\mathbb{Q}\left(\zeta\right)[X]$ (because $\left\{\zeta^{2k+1} \mid 0 \leq k \leq 2^n - 1\right\}$ are pairwise distinct roots of $P(X)$ and $\deg(P(X)) = 2^n$), and clearly $\mathbb{Q}\left(\zeta\right)$ is minimal in terms of degree $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg(P(X)) = 2^n$ with the property of splitting $P(X)$ (because any subfield of $\mathbb{Q}^{\text{alg}}$ splitting $P(X)$ must contain $\mathbb{Q} \cup \{\zeta\}$), we conclude that $\mathbb{Q}\left(\zeta\right)$ is a splitting field of $P(X)$. Thus, $\mathbb{Q} \hookrightarrow \mathbb{Q}\left(\zeta\right)$ is a finite field extension generated by the separable element ζ and is a splitting field of $P(X) \in \mathbb{Q}[X]$. Hence it is Galois. In particular (since we are in the finite case),

$$\left|\text{Gal}\left(\mathbb{Q}(\zeta)/\mathbb{Q}\right)\right| = [\mathbb{Q}(\zeta) : \mathbb{Q}] = 2^n.$$

Let the field norm of the extension $N_{\mathbb{Q}(\zeta)/\mathbb{Q}} : \mathbb{Q}(\zeta) \to \mathbb{Q}$ (the general theory of field norm is developed in Appendix A.2). Applying it to $\xi \in \mathbb{Q}(\zeta)$, we must have:

$$N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\xi)^2 = N_{\mathbb{Q}(\zeta)/\mathbb{Q}}\left(\xi^2\right) = N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1 + 4\zeta),$$

where we used, for the first equality, the fact that the field norm is compatible with multiplication (and $\xi \in \mathbb{Q}(\zeta)$). Now, since $\mathbb{Q} \hookrightarrow \mathbb{Q}(\zeta) = \mathbb{Q}(1 + 4\zeta)$ is a finite Galois extension, generated by the element $1 + 4\zeta$ (clear), we can use the closed form (**) of the field norm at this element $1 + 4\zeta$ to obtain the first equality:

$$N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1 + 4\zeta) = \prod_{\sigma \in \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})} \sigma(1 + 4\zeta) = \prod_{\sigma \in \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})} (1 + 4\sigma(\zeta)) = \prod_{i < 2^n} \left(1 + 4\zeta^{2i+1}\right).$$

where we used for the last equality, the fact that

$$\{\sigma(\zeta) \mid \sigma \in \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})\} = \text{Root}_{P_{\min,\zeta}(X)}\left(\mathbb{Q}(\zeta)\right) = \text{Root}_{P(X)}\left(\mathbb{Q}(\zeta)\right) = \left\{\zeta^{2i+1} \mid i < 2^n\right\},$$

[3]Another way of seeing that such an element ξ exists is that ξ would be a root of $\left(\frac{1}{4}(X^2 - 1)\right)^{(2^n)} + 1 \in \mathbb{Q}[X]$.

together with $[\mathbb{Q}(\zeta):\mathbb{Q}] = |\mathrm{Gal}\,(\mathbb{Q}(\zeta)/\mathbb{Q})| = 2^n$. However, since

$$X^{(2^n)} + 1 = P(X) = \prod_{i<2^n} \left(X - \zeta^{2i+1}\right),$$

we obtain, magically,

$$\prod_{i<2^n} \left(1 + 4\zeta^{2i+1}\right) = \prod_{i<2^n} \left(-4\left(-\frac{1}{4} - \zeta^{2i+1}\right)\right) = 2^{\left(2^{n+1}\right)}(-1)^{2^n} \prod_{i<2^n} \left(-\frac{1}{4} - \zeta^{2i+1}\right)$$

$$= 2^{\left(2^{n+1}\right)} P\left(-\frac{1}{4}\right) = 2^{\left(2^{n+1}\right)} \left(\left(-\frac{1}{4}\right)^{(2^n)} + 1\right) = 2^{\left(2^{n+1}\right)} \left(\frac{1}{2^{\left(2^{n+1}\right)}} + 1\right) = 1 + 2^{\left(2^{n+1}\right)}.$$

In total:

$$N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\xi)^2 = 1 + 2^{\left(2^{n+1}\right)}.$$

Since $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\xi) \in \mathbb{Q}$, write $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\xi) = \frac{a}{b}$ for $a, b \in \mathbb{Z}$, $b \neq 0$, with $\gcd(a,b) = 1$. Then

$$a^2 = b^2 + b^2 2^{\left(2^{n+1}\right)}.$$

If there is a prime $p \in \mathbb{P}$ such that $p \mid b$, then $p \mid b^2 + b^2 2^{\left(2^{n+1}\right)} = a^2$, so $p \mid a$, a contradiction to $\gcd(a,b) = 1$. Thus, $b \in \mathbb{Z}^\times$, i.e. $b^2 = 1$, but then $a^2 = 1 + 2^{2^{n+1}}$, i.e.

$$\left(a - 2^{(2^n)}\right)\left(a + 2^{(2^n)}\right) = 1,$$

which implies $a - 2^{(2^n)}$, $a + 2^{(2^n)} \in \mathbb{Z}^\times = \{\pm 1\}$ and $a - 2^{(2^n)} = a + 2^{(2^n)}$. In particular $-2^{(2^n)} = 2^{(2^n)}$ i.e. $2^{(2^n+1)} = 0$, a contradiction.

Therefore it is a contradiction to assume that $\xi \in \mathbb{Q}(\zeta)$, so that $g(X) - \zeta \in \mathbb{Q}(\zeta)[X]$ is irreducible.

Thus $P(g(X)) = \left(X^2 + X\right)^{(2^n)} + 1$ is irreducible.

Problem: B6 Putnam 1985

Let $n \geq 1$ and $G \leq \mathrm{GL}_n(\mathbb{R})$ be a finite group consisting of real $n \times n$ matrices under matrix multiplication. Suppose the sum of the traces of all elements in G is zero:

$$\sum_{M \in G} \mathrm{tr}(M) = 0.$$

Prove that the sum of the elements of G is the zero matrix:

$$\sum_{M \in G} M = \mathbf{0}_{n \times n}.$$

Solution:

Define the matrix $A := \sum_{M \in G} M \in \mathbb{R}^{n \times n}$. Let $N \in G \subset \mathrm{GL}_n(\mathbb{R})$; then left multiplication by N clearly defines a bijection $N \cdot \_ : G \to G$. In particular, $\mathrm{ran}(N \cdot \_) = G$. Since $+$ is commutative, we have:

$$N \cdot A = \sum_{M \in G} N \cdot M = \sum_{T \in \mathrm{ran}(N \cdot \_)} T = \sum_{T \in G} T = A.$$

Since $N \in G$ was arbitrary, we have in particular

$$A^2 = \left(\sum_{M \in G} M \right) \cdot A = \sum_{M \in G} (M \cdot A) = \sum_{M \in G} A = |G| A.$$

In particular, $A^2 - |G| A = \mathbf{0}_{n \times n}$, which implies that the minimal polynomial of A, denoted $P_{\min,A}(X) \in \mathbb{R}[X]$, divides $X(X - |G|)$. In particular, since the roots of the minimal polynomial of a matrix over a field are precisely the roots of its characteristic polynomial (i.e., the eigenvalues of the matrix), it follows that all eigenvalues of A are either 0 or $|G| \geq 1$.

Denote by $m_0(A) := \dim_{\mathbb{R}}(\ker(A))$ and $m_{|G|}(A) := \dim_{\mathbb{R}}(\ker(A - |G| I))$ the respective geometric multiplicities. Since the trace of a matrix equals the sum of its eigenvalues (by Vieta's formula), and the trace map tr is $\mathbb{R}$-linear, the condition

$$0 = \sum_{M \in G} \mathrm{tr}(M) = \mathrm{tr}(A) = m_0(A) \cdot 0 + m_{|G|}(A) \cdot |G| = m_{|G|}(A) \cdot |G|,$$

implies that there are no eigenvalues of A equal to $|G|$; $m_{|G|}(A) = 0$. Hence all eigenvalues of A are 0. Thus $P_{\min,A}(X) = X$, which means $\mathbf{0}_{n \times n} = P_{\min,A}(A) = A = \sum_{M \in G} M$, and this concludes.

A

A.1

Lemma. *Capelli's Lemma: Let K be a field, and let $P(X), g(X) \in K[X]$. Let $\iota : K \hookrightarrow K^{alg}$ be an algebraic closure of K, and let $\alpha \in K^{alg}$ be a root of $P(X)$. Assume without loss of generality that $K \subset K^{alg}$ (the ring morphism is injective).*

Then the polynomial $P(g(X))$ (obtained via the canonical universal evaluation morphism at $g(X)$) is irreducible over $K[X]$ if and only if the following two conditions hold simultaneously:

1. *$P(X)$ is irreducible over $K[X]$, and*
2. *$g(X) - \alpha$ is irreducible over $k(\alpha)[X]$, where $K(\alpha)$ is the smallest subfield of K^{alg} containing $K \cup \{\alpha\}$.*

Proof. Let K be a field, and let $P(X), g(X) \in K[X]$. Let $K \hookrightarrow K^{\text{alg}}$ be an algebraic closure of K, and let $\alpha \in K^{\text{alg}}$ be a root of $P(X)$. Now, let $\theta \in K^{\text{alg}}$ be a root of $g(X) - \alpha \in K^{\text{alg}}[X]$. From $g(\theta) = \alpha$, we obtain $P(g(\theta)) = 0$. Notice then that $\alpha = g(\theta) \in K(\theta)$, so that $K(\alpha) \subset K(\theta)$. Now it is a matter of field extensions:

$$K \longhookrightarrow K(\alpha) \longhookrightarrow K(\theta) \longhookrightarrow K^{\text{alg}}$$

Let $P_{\min,K,\alpha}(X) \in K[X]$, $P_{\min,K,\theta}(X) \in K[X]$, and $P_{\min,K(\alpha),\theta}(X) \in K(\alpha)[X]$ be the minimal polynomial of $\alpha \in K^{\text{alg}}$ over K, and the minimal polynomials of $\theta \in K^{\text{alg}}$ over K and $K(\alpha)$ respectively. Then $P_{\min,K,\alpha}(X) \mid_{K[X]} P(X)$, $P_{\min,K,\theta}(X) \mid_{K[X]} P(g(X))$, and $P_{\min,K(\alpha),\theta}(X) \mid_{K(\alpha)[X]} g(X) - \alpha$. Hence,

$$[K(\alpha) : K] = \deg\left(P_{\min,K,\alpha}(X)\right) \leq \deg\left(P(X)\right), \tag{1}$$

$$[K(\theta) : K] = \deg\left(P_{\min,K,\theta}(X)\right) \leq \deg\left(P\left(g(X)\right)\right) = \deg\left(P(X)\right) \cdot \deg\left(g(X)\right), \tag{2}$$

$$[K(\theta) : K(\alpha)] = \deg\left(P_{\min,K(\alpha),\theta}(X)\right) \leq \deg\left(g(X) - \alpha\right) = \deg\left(g(X)\right). \tag{3}$$

It is clear that each inequality becomes an equality if and only if the corresponding polynomial is irreducible (because then they are, up to units, the corresponding minimal polynomial). Recall the general dimension formula,

$$[K(\theta) : K] = [K(\theta) : K(\alpha)] \cdot [K(\alpha) : K]. \tag{4}$$

If $P(g(X))$ is irreducible over $K[X]$ then (2) is an equality:

$$[K(\theta) : K] = \deg\left(P(X)\right) \cdot \deg\left(g(X)\right),$$

but then by (in order) (3), (4), and (1):

$$\begin{aligned}\deg\left(g(X)\right) \cdot [K(\alpha) : K] &\geq [K(\theta) : K(\alpha)] \cdot [K(\alpha) : K] \\ &= \deg\left(P(X)\right) \cdot \deg\left(g(X)\right) \\ &\geq [K(\alpha) : K] \cdot \deg\left(g(X)\right).\end{aligned}$$

This implies (since everything is finite and positive) that $\deg\left(P(X)\right) = [K(\alpha) : K]$, i.e., $P(X)$ is irreducible over $K[X]$. Therefore, from (4), we have:

$$[K(\theta) : K(\alpha)] \cdot [K(\alpha) : K] = [K(\theta) : K] = \deg\left(P(X)\right) \cdot \deg\left(g(X)\right) = [K(\alpha) : K] \cdot \deg\left(g(X)\right).$$

Since everything is finite and positive, it follows that $\deg(g(X) - \alpha) = \deg(g(X)) = [K(\theta) : K(\alpha)]$, i.e., $g(X) - \alpha$ is irreducible over $K(\alpha)[X]$.

Conversely, if $P(X)$ is irreducible over $K[X]$ and $g(X) - \alpha$ is irreducible over $K(\alpha)[X]$, then (1) and (3) are equalities, and so, by (in order) (4) and (2), we have:

$$\begin{aligned}\deg(P(g(X))) &= \deg(P(X)) \cdot \deg(g(X)) \\ &= [K(\alpha) : K] \cdot [K(\theta) : K(\alpha)] \\ &= [K(\theta) : K] \\ &\leq \deg(P(g(X)))\,,\end{aligned}$$

hence $\deg(P(g(X))) = [K(\theta) : K]$, i.e., $P(g(X))$ is irreducible.

This concludes the lemma.

A.2

For a field extension $K \hookrightarrow L$, for each $\alpha \in L$, we can consider the K-linear endomorphism of mutliplication by α:

$$[\times\alpha] : L \to L.$$

If the extension is K-finite-dimensional (then it is algebraic), we can compute its characteristic polynomial $P_{\text{char},[\times\alpha]}(X) \in K[X]$. In particular, we can compute its determinant (the constant term of $P_{\text{char},[\times\alpha]}(X)$), which defines the *field norm*:

$$N_{L/K} : L \to K, \quad N_{L/K}(\alpha) := \det_K([\times\alpha]).$$

Since $\forall\beta \in L,\ [\times\alpha\beta] = [\times\alpha] \circ [\times\beta]$, we have

$$N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta).$$

In the case where L/K is Galois (which is equivalent to $K \hookrightarrow L$ being a normal and separable field extension), we must have that the roots in L of the minimal polynomial of α in $K[X]$ satisfy

$$\{\sigma(\alpha) \mid \sigma \in \text{Gal}(L/K)\} = \text{Root}_{P_{\min,\alpha}(X)}(L) = \text{Root}_{P_{\min,\alpha}(X)}\left(K^{\text{alg}}\right),$$

where the first equality follows from standard Galois theory, and the second from the fact that the extension is normal. Now, because $P_{\min,\alpha}(X) = P_{\min,[\times\alpha]}(X)$ (a mental exercise), we have:

$$\text{Root}_{P_{\text{char},[\times\alpha]}(X)}\left(K^{\text{alg}}\right) = \text{Root}_{P_{\min,[\times\alpha]}(X)}\left(K^{\text{alg}}\right) = \text{Root}_{P_{\min,\alpha}(X)}\left(K^{\text{alg}}\right),$$

where the first equality follows since the roots (in K^{alg}) of the minimal polynomial of an endomorphism (on a finite-dimensional vector space) are precisely its eigenvalues. Combining:

$$\text{Root}_{P_{\text{char},[\times\alpha]}(X)}\left(K^{\text{alg}}\right) = \{\sigma(\alpha) \mid \sigma \in \text{Gal}(L/K)\}. \tag{1}$$

If α generates the extension, i.e. $L = K(\alpha)$, or equivalently $\deg\left(P_{\min,\alpha}(X)\right) = [L : K]$, then, since the extension is finite and Galois, we have $|\text{Gal}(L/K)| = [L : K]$. From this, as $P_{\min,\alpha}(X)$ is separable, it follows that for each $\sigma, \sigma' \in \text{Gal}(L/K)$, $\sigma \neq \sigma'$ implies $\sigma(\alpha) \neq \sigma'(\alpha)$. Thus:

$$|\{\sigma(\alpha) \mid \sigma \in \text{Gal}(L/K)\}| = [L : K] = \deg\left(P_{\text{char},[\times\alpha]}(X)\right). \tag{2}$$

From (1) and (2), we obtain:

$$P_{\text{char},[\times\alpha]}(X) = \prod_{\sigma\in\text{Gal}(L/K)} (X - \sigma(\alpha))\,[4],$$

and so, by Vieta's formula:

$$N_{L/K}(\alpha) = \prod_{\sigma\in\text{Gal}(L/K)} \sigma(\alpha). \tag{**}$$

□

[4] In fact, this holds even if α does not generate the extension (but still L/K is finite and Galois), as one can show that the multiplicities of each root of the characteristic polynomial $\theta \in \text{Root}_{P_{\text{char},[\times\alpha]}(X)}\left(K^{\text{alg}}\right)$ coincide with the number of automorphisms of L fixing K and sending α to θ, that is, $|\{\sigma \in \text{Gal}(L/K) \mid \sigma(\alpha) = \theta\}|$.