- We "correct" this by moving to the splitting field K' of $x_2^3 - x_2 - x_1^2$ over $k(x_1)$. So,

$$K' \supset K \supset k(x_1) \supset k = \mathbb{F}_q,$$

& $K' \supset k$ is Galois!

- If we let C' be the curve corresponding to K', then we have the following covering:

$$C' \to C \to \mathbb{P}^1$$

where, C' is called the Galois covering of C.

Proposition: Let C be a smooth proj. curve over k & let C' be its Galois covering. Let G be the group of K-automorphisms of $K' := k(C')$.

Then, $|G| = [K' : K]$.

Proof sketch: • The idea is that $\exists f \in K[x]$ s.t. $K' \cong K[x]/\langle f \rangle$ is a splitting field of f.

• Thus, each $\sigma \in G$ sends a root of f to a conjugate, implying, $|G| = \deg_x f = [K' : K]$. $\square$

- Apart from these field automorphisms, we also have the interesting Frobenius morphism: $\underline{F} : K' \to K'$
$f \mapsto f^q$.

▷ F is a k-monomorphism in K'.

- This naturally makes F a morphism of C', as well as, C.
Explicitly, F sends a point (α, β) to $(\alpha^{q^{-1}}, \beta^{q^{-1}})$. Or, a max. ideal $\langle x_1 - \alpha, x_2 - \beta \rangle$ to $\langle x_1 - \alpha^{q^{-1}}, x_2 - \beta^{q^{-1}} \rangle \supset \langle x_1^q - \alpha, x_2^q - \beta \rangle$.

▷ The k-points in C are exactly the fixed points of F, i.e. $\{P \in C \mid F(P) = P\}$.

- We now relate the k-points of C, with those of C':

- Defn: For $\sigma \in G$, $\underline{N_1(C', \sigma)} := \{P \in C' \mid F(P) = \sigma(P)\}$, & $\underline{N_1(C)} := N_1(C, 1)$.

- Proposition: With the above setting,
$$\sum_{\sigma \in G} N_1(C', \sigma) = |G| \cdot N_1(C) + O(1)$$

where, the latter constant is independent of q.

Proof: • Let ϕ be the Galois covering $\phi: C' \to C$.

• For a $P \in C$, let the distinct points in C', above P, be $\phi^{-1}(P) = \{Q_1, \ldots, Q_r\}$.

• Clearly, $F(Q_i) \in \phi^{-1}(P)$, $\forall i$.

• If $f(x)$ is the defining polynomial for K' over K, then clearly $r \leq \deg_x f = |G|$.

• When are they unequal?

• That happens only when P has repeated conjugates (P is ramified). Such P are at most the total-degree of f, thus, $O(1)$.

• For an unramified k-point $P \in C$,
$$\#\{Q \in \phi^{-1}(P) \mid F(Q) = \sigma(Q), \sigma \in G\} = r = |G|.$$

• Also, any $Q \in C$ with $F(Q) = \sigma(Q)$, satisfies:
$$\phi \circ F(Q) = \phi \circ \sigma(Q) \Rightarrow F(\phi(Q)) = P \Rightarrow F(P) = P.$$