- Hence, a $Q \in C$ contributing to $\sum_{\sigma \in G} N_1(C', \sigma)$ <u>either</u> has $\varphi(Q)$ ramified, <u>or</u> has $\varphi(Q)$ an unramified k-point in C.

$$\Rightarrow \sum_{\sigma \in G} N_1(C', \sigma) = |G| \cdot N_1(C) + O(1). \quad \square$$

— With this quantitative relation between the curves C' & C where $C' \to C$ is Galois, we prove a strong estimate which would later imply RH.

- <u>Theorem</u> (Weil 1930s, Bombieri–Stepanov 1960s): Let $C \to \mathbb{P}_1$ be a Galois covering defined over $\mathbb{F}_q$. Assume $q = p^\alpha$ with even α & $q > (g+1)^4$, were g is the genus of C/k. Then $\forall \sigma \in \mathrm{Aut}(C/\mathbb{P}^1)$, $N_1(C, \sigma) \leq (q+1) + (2g+1)\sqrt{q}$.

<u>Rmk</u>: Genus g is at most d^2, where d is the degree of the polynomial defining the curve C. So, $q > (g+1)^4$ is achievable!

- Before giving the long proof, let us see why this proves the RH.

- Let C_0 be a curve over $k = \mathbb{F}_q$ with fn. field K_0. Let $K = K_0 \cdot \bar{k}$ be the fn. field over the algebraic closure of $\mathbb{F}_q$.
- To avoid confusion, let C be the curve corr. to K.
- Let $K' \supseteq K$ be the <u>smallest</u> field extn. that provides a Galois covering $C' \to C$.
- $C' \to \mathbb{P}^1$ is also a Galois covering!
- Let $H := Gal(K'/K)$. Then, by the proposition

$$N_1(C) = |H|^{-1} \cdot \sum_{h \in H} N_1(C', h) + O(1).$$

- Also, for $G := Gal(K'/\bar{k})$, the proposition gives

$$(q+1) = N_1(\mathbb{P}^1) = |G|^{-1} \cdot \sum_{\sigma \in G} N_1(C', \sigma) + O(1).$$

- Together with the Thm. $\Rightarrow N_1(C', \sigma) = q + 1 + O(\sqrt{q})$. which plugged in the previous equality gives:

$N_1(C_0) = N_1(C) = q + 1 + O(\sqrt{q})$; $\Rightarrow$ RH for C_0 !

Let us now prove the Thm:

Proof: • We will prove the bound by designing a "low degree" function G whose zeros cover all the points counted in $N_1(C,\sigma)$. We will use the L-vector-spaces to design G. Finally, the parameters are optimized to get the estimate.

we find G with a unique pole.

• In the proof we work with $k = \overline{\mathbb{F}_q}$ & the corr. fn. field K.

• If $N_1(C,\sigma) = 0$, then we are done. So assume that $\exists P \in C$, $F(P) = \sigma(P)$. Fix this P. ($\because k$ is alg. closed, $d(P) = 1$.)

• Let $a \in \mathbb{N}$ be large enough, and define $L_a := L(aP)$. Let $l_a := \ell(aP)$.

$$\text{Riemann-Roch} \Rightarrow l_a = a + 1 - g.$$

(Note: It is true when $a > 2g-2$.)

• Define $\varphi := \sigma^{-1} \circ F$ & $L_a^{\varphi} := \{ f \circ \varphi \mid f \in L_a \}$.

• Observe that for a $Q \in C$ and $f \in L_a$, the new fn. has $\mathrm{ord}_{\varphi(Q)}(f \circ \varphi) = q \cdot \mathrm{ord}_Q f$. (Why?)

$\Rightarrow$ we have a sequence of maps:

$$L_a \xrightarrow[\sim]{\varphi} L_a^{\varphi} \longrightarrow L_{aq}.$$

- We will also need the Frobenius map that raises by the p-th power:

$$F_{abs} : K \to K \ ; \ f \mapsto f^p .$$

- Similar to L_a^{Φ}, define for a $\mu \in \mathbb{N}$ and a large enough $b \in \mathbb{N}$,

$$L_b^{p,\mu} := \{ f \circ (F_{abs})^{\mu} \mid f \in L_b \} .$$

- Again, we have a sequence of maps

$$L_b \xrightarrow{\sim} L_b^{p,\mu} \longrightarrow L_{bp^{\mu}} .$$

- We first need to compose L_a^{Φ} with $L_b^{p,\mu}$:

<u>Claim 1</u>: : If $bp^{\mu} < q$, then the multiplication map

$$L_b^{p,\mu} \otimes_k L_a^{\Phi} \xrightarrow{\sim} L_b^{p,\mu} \cdot L_a^{\Phi} \hookrightarrow L_{bp^{\mu}+aq}$$

giving, eventually, an injection.

<u>Proof</u>: • Notice that, by defn., L_a has a tower of subspaces: $k = L_0 \subseteq L_1 \subseteq L_2 \subseteq \dots \subseteq L_a$.

$$\Rightarrow L_a \cong \bigoplus_{i=0}^{a} L_i / L_{i-1} .$$