Notação : $G(K|\mathbf{Q}) =: G$ o grupo de Galois de $K|\mathbf{Q}$ (galoisiana), $\mathfrak{O}$ é o anel de inteiros de K. X é o conjunto dos primos $\mathfrak{p}$ em $\mathfrak{O}$ tais que $\mathfrak{p} \cap \mathbf{Z}$ não ramifica em $K|\mathbf{Q}$ (isto é, o conjunto dos ideais primos que não dividem o diferente). Dado um ideal primo de $\mathfrak{p} \in X$, $(\mathfrak{p}, K|\mathbf{Q})$ denota o elemento de Frobenius associado a $\mathfrak{p}|p$. O elemento de Frobenius é um automorfismo de K que fixa $\mathfrak{p}$ e reduzindo induz o Frobenius em $\mathbf{F}_p, p = \mathbf{Z} \cap \mathfrak{p}$, explicitamente

$$(\mathfrak{p}, K|\mathbf{Q})z \equiv z^p \mod \mathfrak{p},\ z \in \mathfrak{O}.$$

O truque é usar o Teorema de densidade de Frobenius, que diz:

Teorema 1. *Dado um $\sigma \in G$, o conjunto de primos $S_\sigma := \{\mathfrak{p} \in X; \sigma = (\mathfrak{p}, K|\mathbf{Q})\}$ tem densidade (no sentido de Dirichlet, isto é, o limite*

$$\lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in S_\sigma} \frac{1}{N\mathfrak{p}^s}}{\log(s-1)}$$

existe e é positivo). Em particular é infinito.

A título de informação , se eu não me engano, a densidade é $\frac{1}{|G|}$ (com certeza é no caso abeliano).

Agora seja $f = (X - x_1) \cdots (X - x_m) \in \mathbf{Z}[X]$ mônico (pra facilitar) e seja K o corpo de raízes. Assumindo que para todo primo p, a redução módulo p de f possui uma raíz é o mesmo que: Para todo primo $\mathfrak{p} \in X$, existe x_i tal que $(\mathfrak{p}, K|\mathbf{Q})x_i - x_i \in \mathfrak{p}$, ou $\bigcup T_i = X$, onde $T_i = \{\mathfrak{p} \in X; (\mathfrak{p}, K|\mathbf{Q})x_i \equiv x_i \mod \mathfrak{p}\}$.

Defina $S_\sigma = \{\mathfrak{p} \in X; \sigma = (\mathfrak{p}, K|\mathbf{Q})\}$. Portanto $S_\sigma \cap T_i \subset \{\mathfrak{p} \in X; \sigma x_i - x_i \in \mathfrak{p}\}$ e tomando união $S_\sigma \subset \bigcup_i \{\mathfrak{p} \in X; \sigma x_i - x_i \in \mathfrak{p}\}$. Assim, basta verificar que $\bigcup_i \{\mathfrak{p} \in X; \sigma x_i - x_i \in \mathfrak{p}\}$ é finito, para algum σ, ou seja, existe um $\sigma \in G$ que não fixa elemento algum de $\{x_1 \ldots, x_m\}$. Mas eu acho que isso é feito contando elementos, isto é, $\bigcup_i G(K|\mathbf{Q}(x_i)) \neq G$.

Bacana que ainda prova um resultado famoso (do Kronecker) que diz que se um número algébrico reduz a um racional no corpo residual, então está em $\mathbf{Q}$.