IV.4 The Kronecker-Weber's theorem

48
Prop: If the K-W thm holds for every cyclic subextension of prime power degree $\Rightarrow$ it holds for all abelian extensions.

Proof:
Let $K|\mathbb{Q}$ be an abelian extension, $G := \mathrm{Gal}(K|\mathbb{Q})$. Since every abelian group decomposes as a direct product of p-groups $\Rightarrow$ $G = \prod_{i=1}^{r} G_i$, G_i cyclic of order $p_i^{k_i}$, p_i prime. Let $K_i := K^{H_i}$, $H_i := \prod_{j \neq i} G_j \cong G/G_i$

$$\begin{tikzcd} K \arrow[d, dash, "G"'] \arrow[dr, dash, "H_i"] & \\ \mathbb{Q} & K_i \arrow[l, dash, "G_i"] \end{tikzcd}$$

$\Rightarrow$ Since $K|K_i$ Galois $\Rightarrow K_i|\mathbb{Q}$ Galois and $[K_i:\mathbb{Q}] = |G_i| = p_i^{k_i}$

$\Rightarrow K_i \subseteq \mathbb{Q}(\zeta_i)$ ζ_i n_i-th root of unity $\Rightarrow K \subseteq K_1 \cdot \ldots \cdot K_r \subseteq \mathbb{Q}(\zeta_{n_1}) \ldots \mathbb{Q}(\zeta_{n_r}) \subseteq \mathbb{Q}(\zeta_N)$. #

Now, every finite extension of $\mathbb{Q}$ ramifies at some prime (those dividing the discriminant). Indeed, from Minkowski's bound seen in ANT: $|\Delta| \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{n/2} > 1$.

We will prove:

49
Prop: If the K-W thm holds for all p-abelian extensions whose set of ramifying primes consists only of the prime dividing the degree $\Rightarrow$ it holds for all p-abelian extension.

Proof: Let $K|\mathbb{Q}$ be a p-abelian extension, $[K:\mathbb{Q}] = p^n$. Suppose $\ell \neq p$ is a ramifying prime, let $\mathfrak{L} \in \mathrm{Spec}(\mathcal{O}_K)$ be a prime ideal over ℓ
$\Rightarrow$ Since the residual char. of $\mathcal{O}_K/\mathfrak{L}$ is $\ell \Rightarrow K|\mathbb{Q}$ is tamely ramified at ℓ.

indeed: $[K:\mathbb{Q}] = p$-power $= e(\mathfrak{L}|\ell)\cdot f(\mathfrak{L}|\ell)\cdot g_\ell \Rightarrow e(\mathfrak{L}|\ell)$ p-power, coprime to $\ell \Rightarrow |G_0(\mathfrak{L}|\ell)| = e(\mathfrak{L}|\ell) = p^m \mid \ell-1$. Indeed:

$|G_0/G_1| = |G_0| \mid \ell^f-1 \mid \ell-1$.

$\Rightarrow \ell \equiv 1 \bmod p^m$. But $\mathbb{Q}(\zeta_\ell)$ is cyclic, unramified outside ℓ and totally ramified ~~outside~~ at $\ell \Rightarrow$

$$\begin{array}{c} \mathbb{Q}(\zeta_\ell) \\ \ell-1 \Big(\quad | \quad \rangle L \\ \mathbb{Q} \end{array}$$

L (unique) $\nearrow$ check (use Galois correspondence)

$\nwarrow$ cyclic, tot. ramified at ~~ℓ~~ ℓ (and unramified everywhere else)

$[L:\mathbb{Q}] = p^m$.

Consider KL, of degree p^{n+t}, $t \leq m$, $p^n = [K:\mathbb{Q}]$.

Let $\mathfrak{L}' \in \mathrm{Spec}(\mathcal{O}_{KL}) \mid \mathfrak{L}$, $I' = G_0(\mathfrak{L}'|\ell)$, $H := \mathrm{Gal}(L|\mathbb{Q}) \cong \mathbb{Z}/p^m\mathbb{Z}$

The morphism $\mathrm{Gal}(KL|\mathbb{Q}) \to \mathrm{Gal}(K|\mathbb{Q}) \to 1$ sends I' to $G_0(\mathfrak{L}|\ell)$ $\swarrow$ check

$\Rightarrow I' \subseteq G_0(\mathfrak{L}|\ell) \times H$ via $\mathrm{Gal}(KL|\mathbb{Q}) \leq \mathrm{Gal}(K|\mathbb{Q}) \times \mathrm{Gal}(L|\mathbb{Q})$.

$\Rightarrow |I'|$ is multiple of p^m, since $e(\mathfrak{L}'|\ell)$ is divisible by $e(\mathfrak{L}|\ell) = p^m$. $e(\mathfrak{L}'|\ell) = e(\mathfrak{L}'|\mathfrak{L})\cdot e(\mathfrak{L}|\ell)$ Also $G_i(\mathfrak{L}'|\ell) = \{1\}$ for $i \geq 1$ since the extension has p-power degree $\Rightarrow I'$ is cyclic.

The order of the elements of $G_0(\mathfrak{L}|\ell) \times H$ divides p^m since both groups are cyclic of order p^m. Since $|I'| \geq p^m \Rightarrow |I'| = p^m$.

$K' := KL^{I'} \Rightarrow K'|\mathbb{Q}$ is not ramified at $\ell \Rightarrow$ since $L|\mathbb{Q}$ is totally ramified at $\ell \Rightarrow K' \cap L = \mathbb{Q}$ ⊛ $\Rightarrow K'L \subseteq KL$ has degree

$[K'L:\mathbb{Q}] = [K':\mathbb{Q}][L:\mathbb{Q}] = [KL:\mathbb{Q}] \Rightarrow K'L = KL$.

$\uparrow$ $[K':\mathbb{Q}] = \dfrac{[KL:\mathbb{Q}]}{[L:\mathbb{Q}]}$ $\hookleftarrow e(\mathfrak{L}'|\ell)$.

⊛
$$\begin{array}{ccc} K' & & L \\ & P & \\ & \mathbb{Q} & \end{array}$$
$e^{\ell-1}$, $e = \ell-1$, $e \geq 1 \to$

Hence, if we prove that K' is cyclotomic, since L is so $\Rightarrow$ $\underset{\| K'L}{KL}$ will be so

$\Rightarrow$ K will be so.

K' does not ramify at ℓ and its ramifying primes form a subset of the ramifying primes of $K|\mathbb{Q}$.

Since this set is finite, we can repeat this argument by induction and suppose that $K'|\mathbb{Q}$ is unramified outside p $\Rightarrow$ it's cyclotomic.

Moreover:

(50) **Cor**: Let $K|\mathbb{Q}$ be abelian, $[K:\mathbb{Q}]=p^m$ ramifying at $\ell \neq p$. Then $\ell \equiv 1 \mod p^m$, K is totally ramified at ℓ and K is the only subfield of $\mathbb{Q}(\zeta_\ell)$ of degree p^m. In particular, $K|\mathbb{Q}$ is cyclic.

(51) **Cor**: Let $K|\mathbb{Q}$ be p-abelian and tamely ramified at each prime $\Rightarrow K$ is cyclotomic.

Proof: Can suppose $K|\mathbb{Q}$ cyclic, ramifying at most only at p. Assume $e(\mathfrak{Q}|\mathfrak{p}) = p^m \underset{\substack{\uparrow \\ \text{coprime to } p}}{=} 1 \Rightarrow G_0(\mathfrak{Q}|\mathfrak{p}) = \{1\}$, $L=\mathbb{Q}$, $H=\{1\} \Rightarrow I'=\{1\}$

$\Rightarrow K'=K$ not ramified at $p \Rightarrow K'=K=\mathbb{Q}$. #

Rem: For $p>2$, $K|\mathbb{Q}$ only ramifying at p, $[K:\mathbb{Q}]=p \Rightarrow G_2=\{1\}$

(52) **Thm**: Let $K|\mathbb{Q}$, Galois abelian extension of $\deg = [K:\mathbb{Q}] = 2^m$ which only ramifies at 2. Suppose $K \subseteq \mathbb{R} \Rightarrow K=\mathbb{Q}(\zeta+\zeta^{-1})$, ζ is a 2^{m+2}-root of 1 (left as exercise).

53

Prop: $K|\mathbb{Q}$, $[K:\mathbb{Q}]=2^m$ (abelian) unramified outside 2.

$\Rightarrow K = \mathbb{Q}(\zeta^2), \mathbb{Q}(\zeta+\zeta^{-1}), \mathbb{Q}(\zeta-\zeta^{-1})$, ζ 2^{m+2}-root of 1. (These are the only subfields of degree 2^m over $\mathbb{Q}$). (exercise).

Def: Let $K|\mathbb{Q}$ be an abelian extension. The smallest $n \geq 1$ s.t. $K \subseteq \mathbb{Q}(\zeta_n)$ is called the conductor of the extension.

Notice: If n odd $\Rightarrow$ $\mathbb{Q}(\zeta_{2n}) = \mathbb{Q}(\zeta_n)$ $\Rightarrow$ the conductor $\not\equiv 2 \bmod 4$.