Corps cyclotomiques

Gozard, p. 70
Artiz, p. 152

Lemme : Soit $\alpha \in U_p^*$, $\beta \in U_q^*$ tel que $p \wedge q = 1$. Notons $\mathbb{Q}(\alpha)\mathbb{Q}(\beta)$ le sous-corps de $\mathbb{C}$ engendré par $\mathbb{Q}(\alpha)$ et $\mathbb{Q}(\beta)$.
Alors $\mathbb{Q}(\alpha)\mathbb{Q}(\beta) = \mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha\beta)$.

$\mathbb{Q}(\alpha)\mathbb{Q}(\beta) = \mathbb{Q}(\alpha,\beta)$: Puisque $\alpha, \beta \in \mathbb{Q}(\alpha)\mathbb{Q}(\beta)$, $\mathbb{Q}(\alpha,\beta) \subset \mathbb{Q}(\alpha)\mathbb{Q}(\beta)$ (car $\mathbb{Q}(\alpha,\beta)$ est le plus petit ss-corps de $\mathbb{C}$ contenant α et β). Puisque $\mathbb{Q}(\alpha), \mathbb{Q}(\beta) \subset \mathbb{Q}(\alpha,\beta)$ (car $\alpha, \beta \in \mathbb{Q}(\alpha,\beta)$), $\mathbb{Q}(\alpha)\mathbb{Q}(\beta) \subset \mathbb{Q}(\alpha,\beta)$ (car $\mathbb{Q}(\alpha)\mathbb{Q}(\beta)$ est le plus petit ss-corps de $\mathbb{C}$ contenant $\mathbb{Q}(\alpha)$ et $\mathbb{Q}(\beta)$).

$\mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha\beta)$: D'une part, $\alpha\beta \in \mathbb{Q}(\alpha,\beta)$ donc $\mathbb{Q}(\alpha\beta) \subset \mathbb{Q}(\alpha,\beta)$. D'autre part, puisque $p \wedge q = 1$, α^q est d'ordre p donc $\mathbb{Q}(\alpha^q) = \mathbb{Q}(\alpha)$. De même, $\mathbb{Q}(\beta^p) = \mathbb{Q}(\beta)$. Or, $(\alpha\beta)^p = \beta^p$ donc $\beta^p \in \mathbb{Q}(\alpha\beta)$ d'où $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\alpha\beta)$. De même, $\mathbb{Q}(\beta) \subset \mathbb{Q}(\alpha\beta)$. Donc $\mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha)\mathbb{Q}(\beta) \subset \mathbb{Q}(\alpha\beta)$. (Comme $p \wedge q = 1$ et $\alpha\beta = \beta\alpha$, $\alpha\beta \in U_{pq}^*$)

Proposition : Soit $m, n \in \mathbb{N}^*$ et $N = m \vee n$. On note $\zeta_i \in U_i^*$, $\forall i \in \mathbb{N}^*$.
Alors $\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_N)$.

On décompose en produit de facteurs premiers : $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $n = p_1^{\beta_1} \cdots p_k^{\beta_k}$ et $N = p_1^{\gamma_1} \cdots p_k^{\gamma_k}$ avec $\gamma_i = \max(\alpha_i, \beta_i)$.
Par récurrence dans le lemme : $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{p_1^{\alpha_1}}, \dots, \zeta_{p_k^{\alpha_k}})$ et $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{p_1^{\beta_1}}, \dots, \zeta_{p_k^{\beta_k}})$ (si $p_k \wedge p_i = 1$, $\forall i \in [\![1, k-1]\!]$ alors $p_k \wedge p_1 \cdots p_{k-1} = 1$).

Or, $\forall a, b \in \mathbb{N}^*$, $\mathbb{Q}(\zeta_a) \subset \mathbb{Q}(\zeta_{ab})$ car $\zeta^{ab} - 1 = (\underbrace{\zeta^a}_{=1})^b - 1 = 0$. D'où $\mathbb{Q}(\zeta_{p_i^{\alpha_i}}, \zeta_{p_i^{\beta_i}}) = \mathbb{Q}(\zeta_{p_i^{\gamma_i}})$.

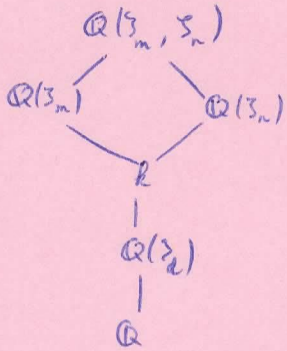
Par itération, on a donc : $\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{p_1^{\alpha_1}}, \dots, \zeta_{p_k^{\alpha_k}}, \zeta_{p_1^{\beta_1}}, \dots, \zeta_{p_k^{\beta_k}}) = \mathbb{Q}(\zeta_{p_1^{\gamma_1}}, \dots, \zeta_{p_k^{\gamma_k}}) \overset{\text{par le lemme}}{=} \mathbb{Q}(\zeta_{p_1^{\gamma_1} \cdots p_k^{\gamma_k}}) = \mathbb{Q}(\zeta_N)$.

Lemme : Soit $k \subset K$, $F \subset L$ tels que $[L:k] < +\infty$ et $H = {}^{KF}$ le ss-corps de L engendré par K et F.
Alors $(H:F) \leq [K:k]$.

Rq : On a $H = \{\sum f_i k_i \,;\, f_i \in F, k_i \in K\}$. En effet, H est une ss-k-algèbre de L intègre de dimension finie.
Donc $\forall x \in H$, l'application $\begin{matrix} H \to H \\ y \mapsto xy \end{matrix}$ est injectif (car intègre) et donc bijectif (car dim finie). D'où $\exists y \in H$ tq $xy = 1$.
H est donc un corps et $H = KF$.

Soit $n = [K:k]$ et $(x_1, \dots, x_n)$ une k-base de K. Puisque $k \subset F$ et par définition de H, $(x_1, \dots, x_n)$ est une F-famille génératrice de H. D'où $(H:F) \leq n$.

Proposition : On a $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_d)$ où $d = m \wedge n$.



Posons $k = \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)$. Puisque $d \mid m$ et $d \mid n$, $\mathbb{Q}(\zeta_d) \subset k$.
Par multiplicativité des degrés, on a :

$$\varphi(m) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = [\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_d)] \underbrace{[\mathbb{Q}(\zeta_d) : \mathbb{Q}]}_{=\varphi(d)} \Rightarrow [\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_d)] = \frac{\varphi(m)}{\varphi(d)}.$$

D'après la proposition précédente, $[\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}] = \varphi(N)$ donc

$$[\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}(\zeta_m)] = \frac{\varphi(N)}{\varphi(m)} \text{ et } [\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}(\zeta_n)] = \frac{\varphi(N)}{\varphi(n)}$$

On applique le lemme à $H = \mathbb{Q}(\zeta_m, \zeta_n)$: $\frac{\varphi(N)}{\varphi(n)} = [\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}(\zeta_n)] \leq [\mathbb{Q}(\zeta_m) : k] \leq [\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_d)] = \frac{\varphi(m)}{\varphi(d)}$.
Or, puisque $mn = Nd$, par multiplicativité de φ, $\varphi(m)\varphi(n) = \varphi(N)\varphi(d)$, d'où $\frac{\varphi(N)}{\varphi(n)} = \frac{\varphi(m)}{\varphi(d)}$. (raisonner facteur premier par facteur premier)
Ainsi, $[\mathbb{Q}(\zeta_m) : k] = [\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_d)]$ et comme $\mathbb{Q}(\zeta_d) \subset k \subset \mathbb{Q}(\zeta_m)$, $\mathbb{Q}(\zeta_d) = k$.

$(k : \mathbb{Q}(\zeta_d)) = 1 \Rightarrow k = \mathrm{Vect}_{\mathbb{Q}(\zeta_d)}(x)$ où $x \in k$
et $\exists y \in \mathbb{Q}(\zeta_d)$ tq $1 = xy$ donc $x \in \mathbb{Q}(\zeta_d)$
$\Rightarrow k \subset \mathbb{Q}(\zeta_d)$