Le Théorème de Kronecker-Weber.

1) étude des corps de nombre $K_n = \mathbb{Q}(e^{2i\pi/n})$

On commence par un lemme général

Lemme 1 : Soit K un corps de nombre t.q $K = \mathbb{Q}(x)$ où $x \in \mathcal{O}_K$.
On note π_x le polynôme de x sur $\mathbb{Q}$ et $d = \mathrm{disc}(\pi_x)$
On sait que $\pi_x \in \mathbb{Z}[X]$ donc $d \in \mathbb{Z}$
Alors On a : * $\mathcal{O}_K\left[\frac{1}{d}\right] = \mathbb{Z}\left[\frac{1}{d}\right][x]$ (1)

* $\mathbb{Z}\left[\frac{1}{d}\right][x] = \mathbb{Z}\left[\frac{1}{d}\right][X]/(\pi_x)$ (2)

* si $p \nmid d$ alors p non ramifié dans K (3)

Démo (1) On a $\mathbb{Z}[x] \subset \mathcal{O}_K$ donc $\mathbb{Z}\left[\frac{1}{d}\right][x] \subset \mathcal{O}_K\left[\frac{1}{d}\right]$
On va m.q $\mathcal{O}_K \subset \mathbb{Z}\left[\frac{1}{d}\right][x]$

Soit $z \in \mathcal{O}_K$ & Soit $\lambda_0, \dots, \lambda_{n-1} \in \mathbb{Q}$ t.q

$$z = \sum_{i=0}^{n-1} \lambda_i x^i$$

On regarde $\begin{pmatrix} \mathrm{tr}(z\,x^0) \\ \vdots \\ \mathrm{tr}(z\,x^{n-1}) \end{pmatrix} = \begin{pmatrix} \sum \lambda_i \mathrm{tr}(x^{i+0}) \\ \vdots \\ \sum \lambda_i \mathrm{tr}(x^{i+n-1}) \end{pmatrix}$

$$= \left(\mathrm{tr}(x^{i+j})\right)_{i,j \le n-1} \begin{pmatrix} \lambda_0 \\ \vdots \\ \lambda_{n-1} \end{pmatrix}$$

or $z x^i \in \mathcal{O}_K$ donc $\mathrm{tr}(z x^i) \in \mathbb{Z}$

et $\det\left(\mathrm{tr}(x^{i+j})\right) = d$ donc $\left(\mathrm{tr}(x^{i+j})\right)^{-1} \in M_n\left(\mathbb{Z}\left[\frac{1}{d}\right]\right)$

et $\begin{pmatrix} \lambda_0 \\ \vdots \\ \lambda_{n-1} \end{pmatrix} = \left(\mathrm{tr}(x^{i+j})\right)^{-1} \begin{pmatrix} \mathrm{tr}(z\,x^0) \\ \vdots \\ \mathrm{tr}(z\,x^{n-1}) \end{pmatrix}$

donc $\lambda_i \in \mathbb{Z}\left[\frac{1}{d}\right]$ et $z \in \mathbb{Z}\left[\frac{1}{d}\right][x]$

(2) π_α est unitaire, On peut faire une division euclidienne

(3). Soit $p \nmid d$

puisque $p \nmid d$ $\quad \dfrac{\mathcal{O}_K}{p\mathcal{O}_K} = \dfrac{\mathcal{O}_K\left[\frac{1}{d}\right]}{p\mathcal{O}_K\left[\frac{1}{d}\right]}$

$$= \frac{\mathbb{Z}\left[\frac{1}{d}\right][X]/(\pi_\alpha)}{p\mathbb{Z}\left[\frac{1}{d}\right][X]/(\pi_\alpha)}$$

$$= \mathbb{F}_p\left[\frac{1}{d}\right][X]/(\bar{\pi}_\alpha)$$

or $p \nmid d$ donc $\frac{1}{d} \in \mathbb{F}_p$

donc $\dfrac{\mathcal{O}_K}{p\mathcal{O}_K} = \mathbb{F}_p[X]/(\bar{\pi}_\alpha)$.

On écrit $\bar{\pi}_\alpha = \prod_{i=1}^{r} R_i$ où R_i est irréductible dans $\mathbb{F}_p[X]$

On a $\deg(\bar{\pi}_\alpha) = \bar{d}$ donc $\deg(\bar{\pi}_\alpha) \neq 0$ dans $\mathbb{F}_p$

donc $R_i \neq R_j$ pour $i \neq j$

On a alors $\mathbb{F}_p[X]/(\bar{\pi}_\alpha) = \prod_{i=1}^{r} \mathbb{F}_p[X]/(R_i)$

et puisque R_i est irréductible $\mathbb{F}_p[X]/(R_i)$ est réduit donc $\mathcal{O}_K/p\mathcal{O}_K$ est réduit

d'autre part On a $\mathcal{O}_K/p\mathcal{O}_K = \prod_{i=1}^{g} \mathcal{O}_K/\mathfrak{p}_i^{e_i}$ où $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$

donc $\dfrac{\mathcal{O}_K}{\mathfrak{p}_i^{e_i}}$ est réduit i.e $e_i = 1$ et p non ramifié

Corollaire 1 : pour $K = \mathbb{Q}(\alpha)$, $\alpha \in \mathcal{O}_K$ il n'y a qu'un nombre fini de p non ramifié dans K

On énonce maintenant un théorème très puissant que l'on ne démontrera pas.

On rappelle que dans un corps de nombre galoisien et pour $p \in \mathbb{Z}$ premier fixé

$\mathrm{Frob}_p = \{\mathrm{Frob}_P,\ P \supset (p)\}$ est une classe de conjugaison

Si $\mathrm{Gal}(K/\mathbb{Q})$ est abélien, on note $\mathrm{Frob}_p = \mathrm{Frob}_P$ pour $P \supset (p)$ quelconque.

Théorème 1 (Tchebotarev) : Soit K un corps de nombre galoisien et $C \subset \mathrm{Gal}(K/\mathbb{Q})$ une classe de conjugaison alors il existe une infinité de p premier t.q $\mathrm{Frob}_p = C$

On s'intéresse maintenant aux extensions cyclotomique :

Def : On pose $\zeta_n = e^{\frac{2i\pi}{n}}$ et $K_n = \mathbb{Q}(\zeta_n)$ c'est une extension abélienne. Pour $g \in \mathrm{Gal}(K_n/\mathbb{Q})$, on a $g(\zeta_n) = \zeta_n^k$ où $k \in (\mathbb{Z}/n\mathbb{Z})^\times$. On pose $\chi : \mathrm{Gal}(K_n/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$, $g \mapsto k$.

χ est un morphisme de groupe injectif, en particulier K_n est abélien.

On note ϕ_n le n-ème polynôme cyclotomique.

Théorème 2 : Soit $p \nmid n$ alors p est non ramifié dans K_n et

$$\chi(\mathrm{Frob}_p) = p\ [n]$$

Soit $p \nmid n$

Déma : On a $\pi_{\xi_n} \mid \phi_n \mid X^n - 1$ dans $\mathbb{Z}[X]$ donc

$\operatorname{disc}(\pi_{\xi_n}) \mid \operatorname{disc}(X^n - 1)$ or $\operatorname{disc}(X^n - 1) \wedge p = 1$

donc $p \nmid \operatorname{disc}(\pi_{\xi_n})$ donc d'après le lemme 1

p est non ramifié dans K_n.

On fixe $P \supset (p)$

Soit $g = \operatorname{Frob}_P$ et $h = \chi(g)$

On a $g(\xi_n) = \xi_n^h$

et $g(\xi_n) = \bar{\xi}_n^P$ [P]

Or dans $O_K/P[X]$ $X^n - 1$ est séparable et

$X^n - 1 = \prod_{i=0}^{n-1} (X - \bar{\xi}_n^i)$ donc $\bar{\xi}_n^i \neq \bar{\xi}_n^j$ si $i \neq j$

Finalement $\xi_n^h = \xi_n^p$ i.e $p \equiv h\,[n]$

Corollaire 2 : $[K_n, \mathbb{Q}] = \varphi(n)$, χ est un isomorphisme de groupe et ϕ_n est irréductible dans $\mathbb{Q}[X]$

Déma : On $|\mathrm{Gal}(K_n, \mathbb{Q})| = \deg(\pi_{\xi_n}) = [K_n, \mathbb{Q}]$ et $\pi_{\xi_n} \mid \phi_n$

donc il suffit de m.q χ est surjectif or On a pour $h \in (\mathbb{Z}/n\mathbb{Z})^\times$ $h = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ pour $p_i \nmid n$

donc pour $g = \operatorname{Frob}_{p_1}^{\alpha_1} \cdots \operatorname{Frob}_{p_n}^{\alpha_n}$ $\chi(g) = h$ d'après le théorème 2

Propriété 1 : Dans K_p, $(1-\zeta_p)$ est l'unique idéal premier contenant p et $p\mathcal{O}_{K_p} = (1-\zeta_p)^{p-1}$

Demo : On a $p = \Phi_p(1) = \prod_{1 \le k \le p-1} (1-\zeta_p^k)$

or $\dfrac{1-\zeta_p^k}{1-\zeta_p} = \sum_{j=0}^{k-1} \zeta_p^j \in \mathcal{O}_{K_p}$

et $\dfrac{1-\zeta_p}{1-\zeta_p^k} = \sum_{j=0}^{i-1} \zeta_p^{kj} \in \mathcal{O}_{K_p}$ où $ki \equiv 1 \ [p]$

donc $p = u(1-\zeta_p)^{p-1}$ où $u \in \mathcal{O}_{K_p}^*$

donc $p\mathcal{O}_{K_p} = (1-\zeta_p)^{p-1}$ il reste à montrer que

$(1-\zeta_p)$ est un idéal premier.

On a $[K_p : \mathbb{Q}] = p-1 = efg$ or $e \ge p-1$ donc $e = p-1$, $f = 1$, $g = 1$

donc $(1-\zeta_p)$ est premier

2) Théorème de Kronecker - Weber

Théorème 3 (Kronecker - Weber) : Tout corps de nombre abélien est inclus dans un corps cyclotomique

On montre ici une version plus faible mais suffisante pour l'objectif final.

Théorème 4 (Kronecker - Weber faible) : Soit K un corps de nombre abélien et p premier t.q :

* $[K, \mathbb{Q}]_p = 1$
* $\forall q \neq p$ premier q est non ramifié dans K

alors $K \subset K_p$.

On commence la preuve de Théorème 4 par un lemme :

lemme 2 : Soit $\mathbb{Q} \subset K' \subset K$ des corps de nombre galoisien et $p \subset P' \subset P$ des idéaux premier des K' et K alors la restriction de $Gal(K/\mathbb{Q}) \to Gal(K'/\mathbb{Q})$ induit une surjection de $D_P \to D_{P'}$ et de $I_P \to I_{P'}$

Déno : Soit $g \in D_{P'}$, Soit $h \in Gal(K/\mathbb{Q})$ t.q $h|_{K'} = g$

On sait que $Gal(K''/K')$ agit transitivement sur les idéaux premier contenant P'. On peut donc choisir $h' \in Gal(K/K')$ t.q $h'(h(p)) = p$ On a alors $h'h(p) = p$ et $h'h|_{K'} = g$ donc $h'h \in D_p$ et s'envoie sur g

Soit $g \in I_{\mathfrak{p}'}$ et $h \in D_{\mathfrak{p}}$ t.q $h|_{K'} = g$

On sait que $D_{\mathfrak{p}} \cap \mathrm{Gal}(K/K') \to \mathrm{Gal}\left(\frac{O_{K'}}{\mathfrak{p}}, \frac{O_{K'}}{\mathfrak{p}'}\right)$ est une surjection. Soit $h' \in D_{\mathfrak{p}} \cap \mathrm{Gal}(K/K')$ t.q $h' = h^{-1}[\mathfrak{p}]$

On a alors $h'h \in I_{\mathfrak{p}}$ et $h'h|_{K'} = g$.

Lemme 3: Soit K vérifiant les hypothèse du théorème 4 pour $\mathfrak{p}$
Alors $L = K(\zeta_p)$ vérifie les mêmes hypothèses que K et
On peut se ramener à $K_{\mathfrak{p}} \subset K$.

Démo: On a $\mathrm{Gal}(L/\mathbb{Q}) \hookrightarrow \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(K_{\mathfrak{p}}/\mathbb{Q})$

$$g \longmapsto (g|_K, g|_{K_{\mathfrak{p}}}).$$

donc $L/\mathbb{Q}$ est abélien et $[L,\mathbb{Q}] \mid [K,\mathbb{Q}][K_{\mathfrak{p}},\mathbb{Q}]$

donc $[L,\mathbb{Q}] \wedge p = 1$

Soit $q \neq \mathfrak{p}$ premier et $\mathcal{Q} \supset (q)$ idéal premier de O_L

On va m.q $|I_{\mathcal{Q}}| = 1$

On a $I_{\mathcal{Q}} \hookrightarrow I_{\mathcal{Q}\cap K} \times I_{\mathcal{Q}\cap K_{\mathfrak{p}}}$

$$g \longmapsto (g|_K, g|_{K_{\mathfrak{p}}}).$$

On a bien $g|_K$ et $g|_{K_{\mathfrak{p}}}$ dans $I_{\mathcal{Q}\cap K}$ et $I_{\mathcal{Q}\cap K_{\mathfrak{p}}}$ respectivement d'après le lemme 2.

or $I_{\mathcal{Q}\cap K}$ et $I_{\mathcal{Q}\cap K_{\mathfrak{p}}}$ sont triviaux car q non ramifié dans K par hypothèse et non ramifié dans $K_{\mathfrak{p}}$ par le Théorème 2. finalement $I_{\mathcal{Q}} \hookrightarrow \{1\}$ donc $I_{\mathcal{Q}} = 1$ et q non ramifié dans L.

Lemme 4 : Soit $P \supset (p)$ premier alors $I_p = Gal(K/\mathbb{Q})$.

Démo : On considère $K' = K^{I_p}$ c'est une extension galoisienne car $Gal(K/\mathbb{Q})$ est abélien. On note $P' = P \cap K'$

On a d'après le lemme 2 $I_p \twoheadrightarrow I_{P'}$ par restriction or par définition la restriction d'un élément de I_p à K' est trivial donc $I_{P'} = 1$ et p non ramifié dans K'

$\forall q \neq p$ q est non ramifié dans K' sinon il le serait dans K. finalement K' n'a aucun nombre premier ramifié donc $K' = \mathbb{Q}$ d'après le théorème de Minkowski (Admis)

On en déduit $I_p = Gal(K/\mathbb{Q})$.

propriété 2 : Soit K un corps de nombre galoisien et $p \subset P$ premier avec P idéal premier de O_K. On note $\mathbb{F}$ le corps fini O_K/P. Alors il existe un morphisme de $I_p \to \mathbb{F}^*$ dont le noyau est un p-groupe.

Démo : Soit $x \in P \setminus P^2$ alors $P^2 \subsetneq (x) + P^2 \subseteq P$

or O_K est un anneau de dedekind donc $(x) + P^2 = P$

et $P/P^2 = Vect_{\mathbb{F}}(\bar{x})$ On a alors $I_p \supset P/P^2$ linéairement.

En effet I_p agit trivialement sur $\mathbb{F}$ par définition

donc $\mathbb{F} I_p$ agit par $g(\lambda \bar{x}) = \lambda\, \overline{g(x)} = \lambda_g \lambda \bar{x}$

donc $I_p \to \mathbb{F}^*$ (λ_g non nul sinon $g(P) \subset P^2$ or $g(P) = P$)

$g \to \lambda_g$

On a construit notre morphisme, on s'intéresse maintenant à son noyau.

On note S le noyau en question et $S_i = \{ g \in S,\ g \equiv Id\ [\mathfrak{p}^i] \}$

On commence par m-q tout éléments de S agit trivialement sur $\mathfrak{p}^i/\mathfrak{p}^{i+1}$. Soit $g \in S$, g agit trivialement sur $\mathfrak{p}/\mathfrak{p}^2$ i-e $g(x) - x \in \mathfrak{p}^2$. On a $\mathfrak{p}^i = (x^i) + \mathfrak{p}^{i+1}$ $(x^i \notin \mathfrak{p}^{i+1})$.

donc l'action de g sur $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ se résume à celle de g sur $\bar{x}^i$

On a $$g(x^i) - x^i = \underbrace{(g(x) - x)}_{\in \mathfrak{p}^2} \underbrace{\left(\sum_{j=0}^{i-1} g(x)^j\, x^{i-j-1} \right)}_{\mathfrak{p}^{i-1}}$$

donc $g(x^i) - x^i \in \mathfrak{p}^{i+1}$

et g agit trivialement sur $\mathfrak{p}^i/\mathfrak{p}^{i+1}$

On a $\dfrac{S_i}{S_{i+1}} \hookrightarrow Aut\left(\mathcal{O}_K/\mathfrak{p}^{i+1}\right)$ on note G_i l'image

On peut alors injecter G_i dans un p-groupe. En effet

$G_i \hookrightarrow Aut_{\mathbb{Z}}\left(\mathcal{O}_K/\mathfrak{p}^{i+1},\ \mathfrak{p}^i/\mathfrak{p}^{i+1}\right)$

$g \longmapsto g - Id$

vérifion que pour $g \in G_i$ $g - Id$ est d'image dans $\mathfrak{p}^i/\mathfrak{p}^{i+1}$

On sait que $g \equiv Id\ [\mathfrak{p}^i]$ i-e $g(x) - x \in \mathfrak{p}^i$

donc $g - Id \in Hom_{\mathbb{Z}}\left(\mathcal{O}_K/\mathfrak{p}^{i+1},\ \mathfrak{p}^i/\mathfrak{p}^{i+1}\right)$

Il reste à vérifier que c'est un morphisme de groupe.

On a $gh - Id = g(h - Id) + g - Id$

or $Im(h - Id) \subset \frac{P^i}{P^{i+1}}$ et $g \in S$ donc

g agit trivialement sur $\frac{P^i}{P^{i+1}}$ donc

$g(h - Id) = h - Id$

finalement $\frac{S_i}{S_{i+1}} \hookrightarrow \underbrace{Hom_{\mathbb{Z}}\left(\frac{O_K}{P^{i+1}}, \frac{P^i}{P^{i+1}}\right)}_{p\text{-groupe}}$

donc $\frac{S_i}{S_{i+1}}$ est un p-groupe.

de plus pour $g \in S \setminus \{Id\}$ $\exists N \in \mathbb{N}$ $g \notin S_N$.

En effet Soit $x \in O_K$ $\exists$ $g(x) \neq x$ alors $\exists N \in \mathbb{N}$

$g(x) - x \in P^N$ et $g \notin S_N$ S est fini donc $\exists N \in \mathbb{N}$

$S_N = 1$

finalement $|S| = \prod^{N} |\frac{S_i}{S_{i+1}}|$

donc S est un p-groupe.

Preuve du théorème 4

D'après le lemme 4 $I_p = Gal(K/\mathbb{Q})$ or

$|I_p| \mid p^\alpha(p^t - 1)$ où $p^\alpha = |S|$ on a $f = 1$ et $|I_p| \wedge p = 1$ par hypothèse

donc $|I_p| \mid p - 1$ or $|I_p| \geq p - 1$ car $K_p \subset K$

donc $|I_p| = p - 1$ et $K = K_p$.