THEORÈME DE DIRICHLET FAIBLE.

Leçons : 120, 121, 141

Références : Algèbre 1, S. Francinou, H. Gianella, S. Nicolas p. 435.
(Gozard p. 84)

Théorème

Soit $n \geq 1$, il existe une infinité de nombres premiers de la forme $\lambda n+1$, avec λ entier.

Résumé

- Pour $\Phi_1 = X-1$
  $\Phi_n = \prod_{\substack{1 \leq k \leq n \\ k \wedge n = 1}} \left(X - e^{\frac{2ik\pi}{n}}\right)$ les polynômes cyclotomiques.

I - Pour tout $n \in \mathbb{N}^*$, Φ_n est à coefficients entiers.

II - Soit p un nombre premier.
Pour $a \in \mathbb{Z}$, si $p \mid \Phi_n(a)$ mais aucun $\Phi_d(a)$ pour $d \mid n$ strictement, alors $p \equiv 1 \mod n$.

III - Posons $P = \{p \in \mathbb{N}, p \text{ premier et } p \equiv 1 \mod n\}$.
Montrons par l'absurde que P est infini.

I | • Montrons dans un premier temps que, pour $n \geq 1$,

$$X^n - 1 = \prod_{d \mid n} \Phi_d.$$

• On définit : U_n l'ensemble des racines n-ièmes de 1.
P_n l'ensemble des racines n-ièmes primitives de 1.

• On a alors :

* $X^n - 1 = \prod_{\xi \in U_n} (X - \xi)$
* $\Phi_n = \prod_{\xi \in P_n} (X - \xi)$.
* si $\xi \in U_n$, l'ordre d de ξ divise n et $\xi \in P_d$: $U_n = \bigsqcup_{d \mid n} P_d$.

- Des lors, $X^n - 1 = \prod_{d|n} \left(\prod_{\xi \in P_d} (X - \xi) \right) = \prod_{d|n} \Phi_d$.

- On peut alors montrer que $\Phi_n \in \mathbb{Z}[X]$ par récurrence :

  * si $n=1$, $\Phi_1 = X - 1 \in \mathbb{Z}[X]$.

  * si $n \in \mathbb{N}^*$ et $\Phi_k \in \mathbb{Z}[X]$ pour tout $k < n$, alors

$$X^n - 1 = \prod_{d|n} \Phi_d$$

$$\underbrace{X^n - 1}_{\in \mathbb{Z}[X]} = \Phi_n \cdot \underbrace{\prod_{\substack{d|n \\ d \neq n}} \Phi_d}_{\in \mathbb{Z}[X]}$$

donc $\Phi_n \in \mathbb{Z}[X]$, car c'est ~~le quotient de la division euclidienne~~ NON
de $X^n - 1$ par $\prod_{\substack{d|n \\ d \neq n}} \Phi_d$. car les deux autres sont unitaires
et que $X^n - 1 \in \mathbb{Z}[X]$
et $\gamma(PQ) = \gamma(P)\gamma(Q)$
PGCD des coeff.

II] - Soit p premier vérifiant $p \mid \Phi_n(a)$ mais pas $\Phi_d(a)$ $(d|n, d \neq n)$.

- On sait que $p \mid \Phi_n(a)$ et $\Phi_n \mid X^n - 1$.
Donc $p \mid a^n - 1$, et dans $\mathbb{Z}/p\mathbb{Z}^*$, l'ordre (multiplicatif !) de $\bar{a}$ divise donc n.

- Cet ordre est exactement n car :

  * si $d|n$, $d \neq n$, alors $\bar{a}^d - 1 = \prod_{d'|d} \overline{\Phi_{d'}(a)}$

  * et si $d' \mid d$, alors $d' \mid n$.

  * comme $\overline{\Phi_{d'}(a)} \neq 0$ par hypothèse, $\bar{a}^d - 1 \neq 0$.

  → l'ordre de $\bar{a}$ est donc n.

- Le théorème de Lagrange donne alors : $\text{ordre}(\bar{a}) \mid p - 1$.
ie. $p = \lambda n + 1$ pour un certain λ entier

III] • Supposons $\mathcal{P} = \{p_1, \dots, p_q\}$ fini.

• On cherche alors p premier vérifiant les hypothèses de II et n'appartenant pas à $\mathcal{P}$.

• Pour s'assurer que $p \notin \mathcal{P}$, on va changer n en $N = n p_1 p_2 \cdots p_q$.
→ dès lors, si $p \equiv 1 \bmod N$, $p \equiv 1 \bmod n$ et $p \notin \mathcal{P}$.

• Il s'agit donc de trouver $a \in \mathbb{Z}$ et p premier tels que :
$$p \mid \Phi_N(a) \quad \text{et ne divise pas} \quad B(a) = \prod_{\substack{d \mid N \\ d < N}} \Phi_d(a).$$

• B et Φ_N n'ont aucune racine en commun donc $B \wedge \Phi_N = 1$ sur $\mathbb{C}[X]$ et d'après le théorème de Bezout, il existe $U, V \in \mathbb{Q}[X]$ tels que :
$$U\Phi_N + VB = 1$$

on passe de $\mathbb{Z}[X]$ à $\mathbb{Q}[X]$ car $B, \Phi_N \in \mathbb{Q}[X]$ et que le pgcd est invariant par extension de corps (égalité de la div. euclid.) (par unicité de la division euclidienne !)

• On choisit alors ensuite $a \in \mathbb{Z}$ tel que :

i - $aU, aV \in \mathbb{Z}[X]$ (possible car ppcm(coeff(U,V)) marche).

ii - $\Phi_N(a) \neq 0$ et $\Phi_N(a) \neq \pm 1$ (possible car Φ_N non constant)

On a donc

(*) $\quad a = U'(a)\Phi_N(a) + V'(a)B(a) \quad$ où $U', V' = aU, aV$.

• Cherchons maintenant p : soit $p \mid \Phi_N(a)$ premier.
Alors $p \mid a^N - 1$ car $\Phi_N \mid X^N - 1$, donc $\bar{a}^N = 1$.
→ a est donc inversible dans $\mathbb{Z}/p\mathbb{Z}$, d'où $a \wedge p = 1$.

• Donc p ne divise pas $B(a)$, car si non, il diviserait a d'après (*).

• En résumé : $\left.\begin{array}{l} p \mid \Phi_N(a) \\ p \nmid \Phi_d(a) \text{ pour } d \mid n,\ d \neq n \\ p \notin \mathcal{P} \end{array}\right\}$ $p \in P$

⇒ absurde, donc $\mathcal{P}$ est infini.