Sous groupes finis d'un corps commutatif

Ref Perrin 104 121 142

Lemme : Si $(G,\cdot)$ est un groupe commutatif, $r \geq 2$ un entier et $g_1, \dots, g_r$ des éléments deux à deux distincts de G d'ordre respectifs $m_1, \dots, m_r$, il existe dans G un élément g_0 d'ordre égal au ppcm de ces ordre.

Théorème : Tout sous groupes fini du groupe multiplicatif $\mathbb{K}^*$, $\mathbb{K}$ étant un corps commutatif est cyclique

Corollaire : $\mu_n(\mathbb{K}) = \{\lambda \in \mathbb{K}, \lambda^n = 1\}$ est un sous groupe cyclique de $\mathbb{K}^*$.

plan : 1) preuve lemme par récurrence
2) preuve théorème
3) preuve corollaire

---

1) On procède par récurrence sur $r \geq 2$.

Pour $r=2$, on procède comme suit. Si $\mathcal{O}(g_1)$ (l'ordre de g_1) et $\mathcal{O}(g_2)$ sont premiers entre eux, $g_0 = g_1 g_2$ est alors d'ordre $m_1 m_2 = ppcm(m_1, m_2)$

Si $\mathcal{O}(g_1) \wedge \mathcal{O}(g_2) \neq 1$, l'idée est de se ramener au cas de figure.

On écrit les décompositions en facteurs premiers de m_1 et m_2 sous la forme :

$$m_1 = \prod_{i=1}^{k} p_i^{\alpha_i} \prod_{i=k+1}^{r} p_i^{\alpha_i} \quad \text{et} \quad m_2 = \prod_{i=1}^{k} p_i^{\beta_i} \prod_{i=k+1}^{r} p_i^{\beta_i}$$

où les facteurs p_i ont été regroupés de sorte que $\alpha_i > \beta_i$ pour $1 \leq i \leq k$ et $\alpha_i \leq \beta_i$ pour $k+1 \leq i \leq r$.

Les exposants α_i, β_i étant positifs ou nuls

↳ car si l'une des conditions $\alpha_i > \beta_i$ ou $\alpha_i \leq \beta_i$ n'est jamais vérifiée alors le produit correspondant vaut 1.

Avec ces écritures, on a $ppcm(m_1, m_2) = \underbrace{\prod_{i=1}^{k} p_i^{\alpha_i}}_{q_1} \underbrace{\prod_{i=k+1}^{r} p_i^{\beta_i}}_{q_2} = q_1 q_2$.

où $q_1 \wedge q_2 = 1$.

et $m_1 = q_1 n_1$, $m_2 = q_2 n_2$.

Les éléments $g_1' = g_1^{n_1}$ et $g_2' = g_2^{n_2}$ sont alors d'ordre respectifs q_1 et q_2

et $g_0 = g_1' g_2'$ est d'ordre $q_1 q_2 = ppcm(m_1, m_2)$

Soit $r \geq 2$ et supposons le résultat acquis pour r.

Soient $g_1, \dots, g_{r+1}$ deux-à-deux distincts dans G d'ordre respectifs $m_1, \dots, m_{r+1}$.

L'hypothèse de récurrence nous dit qu'il $\exists g_0' \in G$ d'ordre $m_0' = \text{ppcm}(n_1, \dots, n_r)$

et le cas $r=2$, $\exists g_0$ d'ordre $\text{ppcm}(m_0', n_{r+1}) = \text{ppcm}(\text{ppcm}(n_1, n_2, \dots, n_r), n_{r+1})$

$= \text{ppcm}(n_1, \dots, n_{r+1})$

par associativité du ppcm.

2) Soit $(G, \cdot)$ un sous groupe d'ordre n de $\mathbb{K}^*$.

$\exists g_0 \in G$ d'ordre $m \leq n$ égal au ppcm des ordre des éléments de G d'après le lemme

L'ordre de tout élément de G divisant m, on en déduit que tout $g \in G$

est racine du polynôme $P = X^m - 1$, ce qui donne n racines distinctes

de P dans $\mathbb{K}$.

Or sur un corps commutatif, un polynôme de degré m a au plus m racines,

donc $n \leq m$.

donc $m = n$.

Le groupe G ayant un élément d'ordre n est cyclique.

3) $\mu_n(\mathbb{K})$ est le noyau du morphisme de groupe $\varphi_n \in \mathbb{K}^* \mapsto 1^n$.

C'est donc un sous groupe fini de $\mathbb{K}^*$ de cardinal au plus égal à n.

Par conséquent il est cyclique (d'après le théorème)

(Ex) Pour $\mathbb{K} = \mathbb{C}$, $\mu_n(\mathbb{C}) = \{ e^{\frac{2ik\pi}{n}}, 0 \leq k \leq n-1 \}$ est cyclique d'ordre n.

Pour $\mathbb{K} = \mathbb{R}$, $\mu_n(\mathbb{K}) = \begin{cases} \{1\} \text{ si } n \equiv 0 [2] \\ \{-1, 1\} \text{ si } n \equiv 1 [2] \end{cases}$

est cyclique d'ordre 1 ou 2.