101

Dev : Exposant d'un groupe abélien fini

K corps fini, G sous groupe fini de $K^*, \times$

G est cyclique.

{ X-ENS Alg 1 ex 2.8 p43
{ TEU TIP ex 1.10 et 1.11 p53

Soit K un corps commutatif, G sous-groupe fini de $(K^*, \times)$

Alors G est cyclique.

Etapes : 1) Soit G abélien fini, $a, b \in G$ tq $o(a) = n$ et $o(b) = m$

si $n \wedge m = 1$ alors $o(ab) = nm$ (X-ENS)

2) si $r = \bigvee_{g \in G} o(g)$ alors il existe un élément d'ordre r de G

3) K un corps, tout sous-groupe multiplicatif fini de K^* est cyclique.

Preuve : 1) Soit G commutatif, $\forall k \in \mathbb{N}$ $(ab)^k = a^k b^k$

donc $(ab)^{nm} = 1$ et $o(ab) \mid nm$.

Supposons $n \wedge m = 1$, montrons que $o(ab) = nm$

Soit $k \in \mathbb{N}$ tq $(ab)^k = 1$

$$\left((ab)^k\right)^n = 1 \Rightarrow a^{kn} b^{kn} = 1$$

$$\Rightarrow a^{kn} = 1 \quad \text{donc } o(a) = n \mid kn$$

or $n \wedge m = 1$ donc $n \mid k$ (Lemme de Gauss)

Par symétrie avec m, $m \mid k$

Comme $n \wedge m = 1$ alors $nm \mid k$

et comme $(ab)^{nm} = 1$ alors $o(ab) = nm$

Rq importante - Si m et n ne sont pas premiers

entre eux alors $o(ab) \mid mn$ mais n'est en général pas

égal. ex: $(\mathbb{K}-\mathrm{Vect})$ si $b = a^{-1}$

alors $ab = 1$ d'ordre 1

alors que $o(a) = o(b)$ et donc $\mathrm{ppcm}(o(a), o(b)) = n$.

ex: (TEU) dans U_n soit $a = e^{2i\pi/n}$ et $b = e^{-2i\pi/n}$

sont d'ordre n mais $ab = 1$.

2) Lemme : soit a élément d'ordre n, alors $\forall d \in D(n)$,

l'ordre de a^d est n/d (TEU p48)

→ dans G comm.

preuve - soit $n = dp$, on a :

$$(a^d)^k = 1 \Leftrightarrow a^{dk} = 1 \Leftrightarrow n \mid dk$$

$$\Leftrightarrow dp \mid dk$$

$$\Leftrightarrow p \mid k$$

d'où l'ordre de a^d est $p = \frac{n}{d}$.

Retour à notre problème : pour $x \in G$, soit $o(x)$ son ordre

décomposition de r en facteurs premiers $r = \prod_{i=1}^{k} p_i^{\alpha_i}$

(avec r ppcm des ordres de tous les éléments de G)

avec $p_1, \dots, p_k$ premiers distincts et $\alpha_1 \dots \alpha_k \in \mathbb{N}^*$

Soit $i \in [\![1, k]\!]$, soit v_{p_i} l'application valuation p_i-adique

$$r = \bigvee_{y \in G} o(y) \text{ et } \alpha_i = v_{p_i}(r) = \max_{y \in G} v_{p_i}(o(y))$$

donc il existe un élément $y_i \in G$ tq $v_i(o(y_i)) = \alpha_i$

d'où $o(y_i) = p_i^{\alpha_i} q_i$ avec $q_i \in \mathbb{N}^*$

D'après le lemme précédent, $x_i = y_i^{q_i}$ est d'ordre $p_i^{\alpha_i}$

Comme les x_i sont des éléments d'ordre premiers entre eux 2 à 2

d'après la question précédente (récurrence immédiate)

$$o(x_1 \dots x_\ell) = o(x_1) \dots o(x_\ell) = p_1^{\alpha_1} \dots p_\ell^{\alpha_\ell} = r$$

3) Soit G un groupe fini de $\mathbb{K}^*$ et n son cardinal.

L'ordre de tout élément de G divise n donc

$$r = \bigvee_{x \in G} o(x) \mid n.$$

$\mathbb{K}$ est commutatif donc G aussi par définition

Le polynôme $X^r - 1$ est de degré r et admet pour racines dans $\mathbb{K}$ les n éléments de G donc $n \leq r$.

D'après les questions précédentes, G commutatif, il existe un élément d'ordre r, d'où $r = n$

Donc le sous-groupe engendré par x est de cardinal $n = \text{card } G$

donc G engendré par x est donc cyclique.

Rem = Si G n'est pas abélien (gl) !

Le résultat est faux dans ce cas. Par exemple.

Soit $G = \mathfrak{S}_3$, ses éléments sont Id (ordre 1)

transpositions (ordre 2)

3-cycles (d'ordre 3)

d'où $r = 6$ mais il n'existe aucun élément d'ordre 6 !