Université Rennes 1, Année 2012-2013
Master 1 Math., Algèbre générale de base

Correction de l'exercice 8 de la feuille de td 1

Énoncé

Soit G un groupe abélien fini. Pour tout $x \in G$, on note $\omega(x)$ l'ordre de x.

(1) Soit $(x, y) \in G^2$, $m = \omega(x)$ et $n = \omega(y)$.

(i) Lorsque m et n sont premiers entre eux, montrer que $\omega(xy) = mn$.

(ii) Si on ne suppose plus m premier avec n, a-t-on $\omega(xy) = \mathrm{ppcm}(m, n)$?

(2) Pour $(m, n) \in (\mathbb{N}_\star)^2$, montrer qu'il existe $(m', n') \in (\mathbb{N}_\star)^2$ tel que

$$m' \mid m, \quad n' \mid n, \quad \mathrm{pgcd}(m', n') = 1 \quad \text{et} \quad \mathrm{ppcm}(m, n) = m'n'$$

(3) On définit l'*exposant* d'un groupe fini G, noté $\exp G$, comme le plus petit entier $n \geqslant 1$ tel que $x^n = 1$, pour tout élément x de G. Montrer qu'il existe $z \in G$ tel que $\exp G = \omega(z)$.

(4) En déduire qu'un sous-groupe fini du groupe multiplicatif d'un corps est cyclique.

Correction

(1.i) Soit $r = \omega(xy)$. Ayant $(xy)^{mn} = (x^m)^n (y^n)^m = (1)^n (1)^m = 1$, $r \mid mn$. En outre, $1 = ((xy)^r)^m = (x^m)^r y^{rm} = y^{rm}$, autrement dit $n \mid rm$, or n est premier à m, donc $n \mid r$. De façon similaire, $n \mid r$ et, à nouveau puisque m est premier à n, $mn \mid r$, d'où l'égalité annoncée.

(1.ii) Clairement non. Un contre-exemple est donné en considérant un élément x d'ordre $n \neq 1$ et $y = x^{-1}$, également d'ordre n. Alors $\omega(xx^{-1}) = 1 \neq n = \mathrm{ppcm}(n, n)$.

(2) On note $\mathcal{P}$ l'ensemble des nombres premiers, qui constitue un ensemble de représentants des éléments irréductibles de l'anneau factoriel $\mathbb{Z}$. Ainsi, il existe $(a_p)_{p\in\mathcal{P}}$ et $(b_p)_{p\in\mathcal{P}} \in \mathbb{N}^{(\mathcal{P})}$ telles que $m = \prod_{p\in\mathcal{P}} p^{a_p}$ et $n = \prod_{p\in\mathcal{P}} p^{b_p}$. On vérifie alors que $m' = \prod_{p\in\mathcal{P}} p^{\alpha_p}$ et $n' = \prod_{p\in\mathcal{P}} p^{\beta_p}$, où

$$\alpha_p = \begin{cases} a_p & \text{si } a_p \geqslant b_p \\ 0 & \text{sinon} \end{cases} \qquad \text{et} \qquad \beta_p = \begin{cases} b_p & \text{si } b_p > a_p \\ 0 & \text{sinon} \end{cases}$$

conviennent.

(3) Posons $M = \mathrm{ppcm}\{\omega(x) \ / \ x \in G\}$. D'après le théorème de Lagrange, $x^M = 1$, pour tout $x \in G$, ainsi $\exp G \leqslant M$. Montrons alors que cette borne est atteinte. Soit $p_1, \ldots, p_k \in \mathcal{P}$ et $a_1, \ldots, a_k \in \mathbb{N}_\star$ tels que $M = \prod_{i=1}^n p_i^{a_i}$. Pour $i \in [\![1, n]\!]$, il existe $x_i \in G$, tel que $\omega(x_i) = p_i^{a_i}$ (en effet, par définition de M, il existe $y_i \in G$ tel que $\omega(y_i) = p_i^{a_i} q$, avec q premier à p_i, et $x_i = y^q$ convient). Alors $x = \prod_{i=1}^n x_i$ vérifie $\omega(x) = M$, d'après la question (1.i).

Finalement on ne se sert pas de la question (2), qui aurait permis de se limiter à l'introduction des y_i pour la construction d'un élément de G d'ordre M.

(4) Soit G un sous-groupe fini, de cardinal n, du groupe multiplicatif d'un corps k. Il s'agit donc de montrer l'existence d'un élément d'ordre n dans G. D'après la question (3), il existe $x_0 \in G$ tel que $\omega(x_0) = \exp G$ et $\exp G \leqslant \mathrm{Card} G = n$, d'après le théorème de Lagrange. En outre, pour $x \in G$, $x^{\exp G} = 1$. Or, dans un corps (et plus généralement dans un anneau commutatif intègre) le nombre de racines, comptées avec multiplicité, d'un polynôme est majoré par son degré ; ainsi $n \leqslant \exp G$. Finalement $\omega(x_0) = n$ et G est cyclique engendré par x_0.