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

Feuille d'exercices 1 : (indications de) correction, suite

Exercice 8

(1) Attention, bien que G est abélien l'énoncé de l'exercice utilise la notation multiplicative pour la loi de G (on lit « xy »).

(i) Il suffit de montrer que mn est le plus petit (au sens de l'ordre $\leq$, ou de la divisibilité, dans $\mathbb{N}$) entier k tel que $(xy)^k = 1$. D'abord, comme x et y commutent et $x^m = y^n = 1$, on a $(xy)^{mn} = x^{mn}y^{mn} = 1$. De plus, si $(xy)^k = 1$ alors $x^k = y^{-k}$. En élevant à la puissance m, resp. n, on trouve $y^{-mk} = 1$, resp. $x^{nk} = 1$. Par propriété de $\omega(y)$, resp. de $\omega(x)$, on obtient $n \mid mk$ et $m \mid nk$. Comme m et n sont premiers entre eux, par le lemme de Gauss on trouve $n \mid k$ et $m \mid k$. Comme m et n sont premiers entre eux (encore), finalement $mn \mid k$.

(ii) Non, bien sûr, comme on le voit en prenant $y = x^{-1}$...

(2) Écrivons les décompositions en facteurs irréductibles $m = \prod p^{\alpha_p}$ et $n = \prod p^{\beta_p}$. On a alors $\text{ppcm}(m, n) = \prod p^{\gamma_p}$ où $\gamma_p = \max(\alpha_p, \beta_p)$. Notons I l'ensemble des p tels que $\alpha_p \geq \beta_p$ et J l'ensemble des p tels que $\beta_p > \alpha_p$. Notons m' le produit des p^{α_p} pour $p \in I$ et n' le produit des p^{β_p} pour $p \in J$. Comme I et J sont disjoints, on a $\text{pgcd}(m', n') = 1$. Comme I et J contiennent tous les facteurs premiers de m et n, on a $m'n' = \text{ppcm}(m, n)$. Enfin il est clair que $m' \mid m'$ et $n' \mid n$.

(3) Il est clair par définition du ppcm que pour tout $z \in G$ on a $\omega(z) \mid \exp(G)$. Il nous suffit donc de trouver $z \in G$ tel que $\exp(G) \mid \omega(z)$. Écrivons $G = \{g_1, \ldots, g_t\}$ où $t = |G|$, et soit m_s l'ordre de g_s. En utilisant le même procédé que dans la question (2), on peut trouver des entiers m'_s premiers entre eux deux à deux, avec $m'_s \mid m_s$ pour tout s, tels que $m'_1 \ldots m'_s = \exp(G)$. Si l'on écrit $m_s = d_s m'_s$, on a $\omega((g_s)^{d_s}) = m'_s$. D'après la question (1)(i), ici encore étendue au cas d'un nombre fini d'éléments d'ordre premiers entre eux deux à deux, on voit que $g := (g_1)^{d_1} \ldots (g_t)^{d_t}$ est d'ordre égal au produit des m'_s, c'est-à-dire $\exp(G)$.

(4) Notons $n = \text{card}(G)$ et $e = \exp(G)$. On sait que $g^n = 1$ pour tout $g \in G$, donc n est un multiple commun des $\omega(g)$ et en conséquence $e \mid n$. Si G est sous-groupe fini du groupe multiplicatif du corps k, le fait que $g^e = 1$ pour tout g montre que G est sous-groupe du groupe μ_e des racines e-ièmes de l'unité dans k. Comme μ_e est l'ensemble des racines du polynôme $X^e - 1$ on a $\text{card}(\mu_e) \leq e$. Finalement

$$n = \text{card}(G) \leq \text{card}(\mu_e) \leq e \leq n.$$

Donc on a égalité partout, $e = n$ et $G = \mu_e$. D'après la question (3) il existe $g \in G$ d'ordre e et G est cyclique.

Exercice 11

(3) On va noter θ_h au lieu de $\theta(h)$ la conjugaison par h. On a vu que tout élément de G peut s'écrire de manière unique $g = nh$ avec $n \in N$ et $h \in H$. De plus, pour calculer le produit de $g = nh$ par $g' = n'h'$ on écrit :

$$nhn'h' = nhn'h^{-1}hh' = (nhn'h^{-1})(hh')$$

ce qui met le produit sous la forme $n''h''$ avec $n'' = nhn'h^{-1}$ (se rappeler que $hn'h^{-1} \in N$) et $h'' = hh'$. Comme $hn'h^{-1} = \theta_h(n')$, finalement on a :

$$(nh)(n'h') = n\theta_h(n')hh'.$$

En résumé G est entièrement décrit, à isomorphisme près, à partir de N, H et θ par : son ensemble sous-jacent $G = N \times H$ ensemble des couples (n, h), et sa multiplication $(n, h).(n', h') = (n\theta_h(n'), hh')$.

(4) Il n'y a pas de grande difficulté.