Université M. Ismail – Faculté des Sciences – Département de Mathématiques

Corrigé de l'épreuve d'Algèbre 6 - SMA4 / Session Ordinaire – 2019-2020

Exercice 1.

1. Soit H et K deux sous-groupes de $(\mathbb{Z},+)$, distincts de $\{0\}$, donc il existe $m,n \in \mathbb{N}^*$ tel que $H = m\mathbb{Z}$ et $K = n\mathbb{Z}$. On a alors $mn \in H \cap K$ et donc $H \cap K \neq \{0\}$; par suite $\mathbb{Z}$ n'est pas le produit direct de H par K.

2. Soit G un groupe d'ordre 4 tel que $\forall x \in G\backslash\{e\}$. $o(x) = 2$, i.e. $x = x^{-1}$. G est alors abélien (voir TD). Soit H et K deux sous-groupes distincts et propres de G. Puisque G est abélien, on a $\forall h \in H, \forall k \in K, hk = kh$ et HK est un sous-groupe de G. Par ailleurs, d'après le théorème de Lagrange et l'hypothèse, Il s'ensuit que $|H| = |K| = 2$ et que $H \cap K = \{e\}$, et donc il existe deux éléments distincts $x, y \in G\backslash\{e\}$ tel que $H =< x >= \{e, x\}$ et $K =< y >= \{e, y\}$ et $HK = \{e, x, y, xy\} = G$ car $|HK| = |G|$. Donc G est le produit direct de H par K.

3. voir le cours.

Exercice 2.

1. (a-) $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$.
   $o(\overline{0}) = 1 = 2^0$, $o(\overline{1}) = 4 = 2^2$, $\overline{2} \neq \overline{0}$ et $2 \times \overline{2} = \overline{0}$ d'où $o(\overline{2}) = 2 = 2^1$.
   $\overline{3} \neq \overline{0}$, $2 \times \overline{3} \neq \overline{0}$, $3 \times \overline{3} \neq \overline{0}$ et $4 \times \overline{3} = \overline{0}$ d'où $o(\overline{3}) = 4 = 2^2$. Donc $\mathbb{Z}/4\mathbb{Z}$ est un 2-groupe.

   (b-) Dans $\mathbb{Z}/6\mathbb{Z}$, $o(\overline{1}) = 6$, or, il n'existe aucun nombre premier dont 6 est une puissance. Donc, ce n'est pas un p-groupe.
   On a $pgcd(2,3) = 1$ donc $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ est isomorphe à $\mathbb{Z}/6\mathbb{Z}$, par suite ce n'est pas un p-groupe.

2. Soit G un groupe cyclique d'ordre n. Il existe alors $a \in G$ tel que $G =< a >$. Si G est un p-groupe, tout élément de G est d'ordre une puissance de p, en particulier $o(a)$ est une puissance de p. Or, $o(a) = |G| = n$ d'où n est une puissance de p. Réciproquement, on suppose qu'il existe $k \in \mathbb{N}$, tel que $n = p^k$, soit $x \in G$, d'après le théorème de Lagrange, $o(x)/|G|$, i.e. $o(x)/p^k$ et puisque p est premier, on a alors $o(x) = p^\alpha$ avec $0 \leq \alpha \leq k$. Ainsi G est un p-groupe.

3. Tout sous-groupe H d'un p-groupe G est un p-groupe car tout élément de H est un élément de G.

4. Soit G, G' deux p-groupes. Soit $(a, b) \in G \times G'$, donc il existe $k, k' \in \mathbb{N}$ tel que $o(a) = p^k$ et $o(b) = p^{k'}$. $o((a, b)) = ppcm(o(a), o(b)) = ppcm(p^k, p^{k'}) = p^{sup(k,k')}$. Donc $G \times G'$ est un p-groupe.

5. (a-) Soit $y \in f(G)$, il existe $a \in G$ tel que $y = f(a)$. Comme G est un p-groupe, donc il existe $k \in \mathbb{N}$ tel que $o(a) = p^k$. D'où $a^{p^k} = e$, et, par l'homomorphisme f, on obtient $y^{p^k} = (f(a))^{p^k} = f(a^{p^k}) = f(e) = e'$. Ainsi, $o(y)$ divise p^k, et puisque p est premier, on en déduit que $o(y) = p^\alpha$, avec $0 \leq \alpha \leq k$. Donc $f(G)$ est un p-groupe.

   (b-) R est une relation d'équivalence compatible avec la loi de G, donc G/R muni de la loi quotient est un groupe et la surjection canonique $\pi : G \to G/R$ tel que $\pi(x) = \overline{x}$ est un homomorphisme. Si G est un p-groupe, on conclut d'après (a-) que $\pi(G) = G/R$ est un p-groupe.

6. Soit $a \in G$ alors $\overline{a} \in G/Kerf$, or, par hypothèse, G/R est un p-groupe, il existe alors $k \in \mathbb{N}$ tel que $o(\overline{a}) = p^k$, d'où $\overline{a^{p^k}} = \overline{a}^{p^k} = \overline{e}$, donc $a^{p^k} \in Kerf$; de même puisque $Kerf$ est un p-groupe, il existe $l \in \mathbb{N}$ tel que $o(a^{p^k}) = p^l$. On a alors $(a^{p^k})^{p^l} = e$, autrement dit, $a^{p^{k+l}} = e$, ainsi $o(a)$ divise p^{k+l} et, puisque p est premier, on a $o(a) = p^\alpha$ avec $0 \leq \alpha \leq k + l$. Ce qui prouve que G est un p-groupe.