Corrigé de l'examen du cours "Arithmétique et groupes" (Maths 209)

Exercice 1.

1. a) On observe que $(dx)^2 - a(dy)^2 - b(dz)^2 = d^2(x^2 - ay^2 - bz^2)$ donc (dx, dy, dz) est également une solution de (1); elle est non triviale car $d \neq 0$ donc l'un des nombres dx, dy, dz est non nul.

b) Si (x', y', z') est une solution non triviale de (1), alors le p.g.c.d. de (x', y', z') est un entier $d > 0$. Comme dans a), on observe alors que $(x'/d, y'/d, z'/d)$ est une solution non triviale de (1). Il suffit alors de poser $x = x'/d, y = y'/d, z = z'/d$.

2. a) Si p divise y, alors comme $x^2 - ay^2 - bz^2 = 0$, il divise $x^2 - bz^2$; comme p divise b, il divise x^2 donc aussi x puisque p est premier.

b) D'après a), si p divise y il divise x. Mais alors p^2 divise x^2 et p^2 divise ay^2 donc p^2 divise bz^2. Comme $b = pu$ avec u non divisible par p (parce que p^2 ne divise pas b), on obtient que p divise uz^2 donc p divise z^2, puis p divise z.

c) Cela résulte immédiatement de b).

d) Comme p divise b et $x^2 - ay^2 - bz^2 = 0$, on obtient que $x^2 - ay^2$ est divisible par p. On a donc $\bar{x}^2 = \bar{a}\bar{y}^2$ dans $\mathbf{Z}/p\mathbf{Z}$. Mais d'après c), p ne divise pas y donc comme p est premier, $\bar{y}$ possède un inverse $\bar{z}$ dans $\mathbf{Z}/p\mathbf{Z}$. On obtient alors $(\bar{x}\bar{z})^2 = \bar{a}$ d'où le résultat avec $\bar{c} = (\bar{x}\bar{z})$.

Remarque : en combinant 2d) et 1)b), on obtient que si (1) possède une solution non triviale et si p est un nombre premier qui divise b tel que p^2 ne divise pas b, alors a est un carré modulo p. En particulier si b n'a pas de facteur premier au carré dans sa décomposition en facteurs premiers, le lemme chinois donne que a est un carré modulo b (résultat dû à Legendre).

Exercice 2.

a) Oui : en effet les règles de calcul dans $\mathbf{Z}/p\mathbf{Z}$ donnent que $(xy)^2 = x^2y^2$ pour tous x, y de $(\mathbf{Z}/p\mathbf{Z})^*$.

b) On cherche les x tels que $x^2 = \bar{1}$ (attention : le neutre est ici $\bar{1}$ et pas $\bar{0}$ car c'est la structure multiplicative qu'on regarde) dans $(\mathbf{Z}/p\mathbf{Z})^*$. Cela équivaut à $(x - \bar{1})(x + \bar{1}) = 0$. Comme p est premier, tout élément non nul de $\mathbf{Z}/p\mathbf{Z}$ est inversible, donc la dernière égalité implique $x = \bar{1}$ ou $x = -\bar{1}$. Le noyau de f est donc $\{\pm\bar{1}\}$ (noter que $\bar{1} \neq -\bar{1}$ car $p \neq 2$).

c) Si x appartient à l'image de f, alors $x = y^2$ avec $y \in (\mathbf{Z}/p\mathbf{Z})^*$. Ainsi $x^{(p-1)/2} = y^{p-1}$. Or, le théorème de Lagrange (ou le petit théorème de Fermat dans ce cas particulier) dit que $y^{p-1} = \bar{1}$.

d) On écrit $x = u^r$ avec $r \in \mathbf{Z}$. Alors $u^{r(p-1)/2} = \bar{1}$. Comme u engendre le groupe multiplicatif $(\mathbf{Z}/p\mathbf{Z})^*$, son ordre est $p-1$. Ainsi $r(p-1)/2$ est un multiple de $p-1$, ce qui signifie que r est pair, soit $r = 2k$ avec k entier. Alors $x = (u^k)^2$ est bien dans l'image de f.

Exercice 3.

a) Déjà $\bar{0}$ est bien dans H. Si x et y sont dans H, alors $6(x+y) = 6x+6y = \bar{0}+\bar{0} = \bar{0}$ donc $x+y$ est dans H. Si x est dans H, alors $6(-x) = -6x = -\bar{0} = \bar{0}$ donc $-x$ est dans H. Finalement H est un sous-groupe de G.

b) Soit $\bar{x}$ un élément de G avec $x \in \{0, ..., 17\}$. Dire que x est dans H, c'est dire que $6x$ est divisible par 18 ou encore que x est divisible par 3. Finalement $H = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \bar{12}, \bar{15}\}$ est de cardinal 6.

c) Si $x \in H'$, alors $6x = \bar{0}$ d'après le théorème de Lagrange donc $x \in H$. Ainsi $H' \subset H$ et comme H et H' ont le même cardinal, on a $H = H'$.

d) Soit x un élément d'ordre 6 dans G. Alors $6x = \bar{0}$ donc $x \in H$. Mais dans H il y a deux éléments d'ordre 6 : on peut le vérifier directement ou noter que H est cyclique de cardinal 6, donc il possède $\varphi(6) = 2$ générateurs.