2M220 – Arithmétique

Partiel du 27 octobre

Corrigé

Exercice 1

1. C'est le théorème 1.1 du cours.

2. Une vérification directe montre que l'entier 401 n'est divisible par aucun nombre premier inférieur ou égal à $\sqrt{401} < 21$, d'où sa primalité (cf. le lemme 1.2 du cours).

3. Le carré d'un entier étant congru à $0, 1, 2$ ou 4 modulo 7, si 7 ne divisait pas a, l'entier $a^2 + b^2$ serait alors congru à $1, 2, 3, 4, 5$ ou 6 modulo 7, ce qui est exclu. Par symétrie, l'entier 7 divise également b.

4. On a les identités

$$94 = 81 + 9 + 3 + 1 = 1 \cdot 3^4 + 0 \cdot 3^3 + 1 \cdot 3^2 + 1 \cdot 3 + 1,$$

d'où l'écriture $94 = (10111)_3$.

Exercice 2 – En appliquant l'algorithme d'Euclide, on obtient le tableau suivant (cf. page 18 du polycopié du cours):

	1	10	1	3	
4512	4128	384	288	96	0
1	0	1	-10	11	
0	1	-1	11	-12	

On en déduit l'identité $d = 96$ ainsi que la relation

$$11a - 12b = d.$$

Exercice 3

1. Le groupe G est (cyclique) d'ordre 18. D'après le théorème de Lagrange (cf. les théorèmes 2.1, 2.2 et 2.3 du cours), l'ordre d'un élément de G divise 18 et peut donc être égal à $1, 2, 3, 6, 9$ ou 18 (le groupe G étant cyclique, toutes ces possibilités se réalisent).

2. L'ordre de l'élément $\bar{8}$ est le plus petit entier $n > 0$ tel que $n\bar{8} = \bar{0}$ (cf. le point 2 du théorème 2.2 du cours). Cette dernière condition étant remplie si et seulement si 18 divise $8n$, on obtient $n = 9$.

3. D'après le théorème 2.5 du cours, un élément $x = \bar{n}$ de G est un générateur si et seulement si n est premier avec 18, ce qui donne les six éléments $\bar{1}, \bar{5}, \bar{7}, \overline{11}, \overline{13}$ et $\overline{17}$.

4. Les deux groupes ne sont pas isomorphes. En effet, G possède un élément d'ordre 18 (car il est cyclique), là où l'ordre d'un quelconque élément de $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ est un diviseur de 6.

Exercice 4

1. En posant (par exemple) $x = \bar{p} \in A$, les relations $x \neq \bar{0}$ et $x^2 = \bar{0}$ impliquent que l'anneau A n'est pas intègre.

2. D'après le corollaire 4.1 du cours, le groupe $A^\times$ est d'ordre $\varphi(p^2) = p(p-1)$.

3. L'élément $x = \bar{p}$ du point 1 convient.

4.1. Le groupe $A^\times$ étant abélien, quels que soient $x, y \in A^\times$, on a les identités

$$f(xy) = (xy)^\ell = x^\ell y^\ell = f(x)f(y).$$

L'application f est donc un homomorphisme de groupes.

4.2. Le groupe G étant fini, l'homomorphisme f est bijectif si et seulement s'il est injectif, ce qui se traduit par la trivialité de $\ker(f)$. Un élément $x \in A^\times$ appartient à $\ker(f)$ si et seulement si $x^\ell = \bar{1}$, i.e. si son ordre d divise ℓ. Par ailleurs, le théorème de Lagrange affirme que d divise $p(p-1)$. En particulier, si ℓ ne divise pas $p(p-1)$ alors on obtient $d = 1$ et, par suite, $x = \bar{1}$. Cette dernière condition entraîne donc la bijectivité de f (elle en est en fait équivalente).

5.1. D'après le théorème 4.1 du cours, pour $p = 3$, on a l'identité

$$A^\times = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}.$$

5.2. Le théorème de Lagrange affirme qu'un élément x de $A^\times$ est d'ordre $1, 2, 3$ ou 6. Pour $x = \bar{2}$, les relations $x^1 = \bar{2} \neq \bar{1}, x^2 = \bar{4} \neq \bar{1}$ et $x^3 = \bar{8} \neq \bar{1}$ impliquent que x est d'ordre 6 et engendre donc $A^\times$.

5.3. Le groupe $A^\times$ étant cyclique, engendré par $x = \bar{2}$ (cf. le point précédent), le théorème 2.5 du cours affirme que les éléments $x^1 = \bar{2}$ et $x^5 = \overline{32} = \bar{5}$ forment une liste exhaustive de ses générateurs.