Anneaux et arithmétique

Contrôle continu 1
Éléments de correction.

Exercice 1

1. Si $ab = ca = 1$ alors on a $b = (ca)b = c(ab) = c$.
2. (a) Fait en TD.
   (b) Si on pose $b(f)(x) := \int_0^x f(t)dt$ alors $ab = 1$ donc a est inversible à gauche. Comme $ba \neq 1$ on a par la question 1 que a n'est pas inversible à droite. Enfin, a admet une infinité (non dénombrable) d'inverses à gauche donnés par $b_y(f)(x) := \int_y^x f(t)dt$, pour y parcourant $\mathbb{R}$.

Exercice 2

1,2. Fait en TD (remplacer i par $i\sqrt{17}$).

3. Comme en TD, on montre qu'un tel automorphisme f doit préserver $\mathbb{Z}$; de plus $f(i\sqrt{17})^2 = f(-17) = -17$ et donc on a $\mathrm{Aut}(\mathbb{Z}[i\sqrt{17}] = \{\mathrm{id}, i\sqrt{17} \mapsto -i\sqrt{17}\}$.
4. On considère (comme en TD) $N : z = a + i\sqrt{17} \mapsto (a + i\sqrt{17})(a - i\sqrt{17}) = a^2 + 17b^2 \in \mathbb{N}$ et on remarque que z est inversible si et seulement si $N(z) = 1$. De fait, les inversibles sont solutions (entières !) de l'équation $a^2 + 17b^2 = 1$, d'où le résultat.

Exercice 3

1. On sait qu'il existe un unique morphisme d'anneaux $\mathbb{Z} \to \mathbb{A}$; son noyau étant un idéal de $\mathbb{Z}$, il est de la forme $n\mathbb{Z}$ avec $n \geq 0$. Si $n = 0$, notre morphisme est injectif donc on est dans le cas (i), sinon on a bien $n1_{\mathbb{A}} = 0$ donc on vérifie (ii) avec $n \geq 1$.
2. (a) On remarque que pour $0 \leq k \leq p$, $\mathbf{C}_p^k = \dfrac{p!}{k!(p-k)!}$ donc p divise $k!(p-k)!\mathbf{C}_p^k$. Or, si $k \neq 0, p$ on sait que p est premier avec le produit $k!(p-k)!$ (il s'agit d'un produit de termes strictement plus petits que le nombre premier p) et donc par théorème de Gauss, $p | \mathbf{C}_p^k$, d'où le résultat.
   (b) Le fait que F soit un morphisme découle de la question précédente. Si $\mathbb{A} = \mathbb{Z}/p\mathbb{Z}$ alors par théorème de Lagrange (l'ordre d'un élément divise l'ordre du groupe) appliqué à $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$, F est l'application identité.

Exercice 4

1. L'égalité $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$ est équivalente à l'existence de $p, q \in \mathbb{Z}$ tels que $1 = np + mq$. Ainsi, par théorème de Bézout, $n\mathbb{Z}$ et $m\mathbb{Z}$ sont étrangers si et seulement si $n \wedge m = 1$.

arnaud.girand@ens-rennes.fr

2. Si I et J sont maximaux distincts, alors il existe $a \in J$ tel que $a \notin I$; ainsi $a \in I + J$ qui est donc un idéal contenant strictement I. Par maximalité, $I + J = \mathbb{A}$.

3. Fait en TD.

arnaud.girand@ens-rennes.fr