Université Aix-Marseille 2018–2019

Licence – Mathématiques
Algèbre 2

Interrogation 5
corrigé

SUJET A

Question 1
Soit A un anneau. Un idéal $I \subset A$ est un sous-groupe pour l'addition, stable par multiplication par tout élément de A.

Question 2
Supossons par l'absurde que $a \in A$ est simultanément inversible et diviseur de zéro. Il existe donc $b \in A$ et $c \in A \setminus \{0\}$ tels que $a.b = 1$ et $c.a = 0$. Mais alors $0 = 0.b = c.a.b = c$, contredisant l'hypothèse $c \neq 0$.

Question 3
Si n n'est pas premier, alors il existe $k_1, k_2 \in [\![1, n-1]\!]$ tels que $k_1.k_2 = n$. On a alors $\overline{k}_1, \overline{k}_2 \neq \overline{0}$, mais $\overline{k}_1.\overline{k}_2 = \overline{0}$. L'anneau $\mathbb{Z}/n\mathbb{Z}$ n'est alors pas intègre.

Réciproquement, si $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre, alors il existe $\overline{k}_1, \overline{k}_2 \neq \overline{0}$, c'est-à-dire tels que n ne divise ni k_1 ni k_2, avec $\overline{k}_1.\overline{k}_2 = \overline{0}$, c'est-à-dire tel que n divise $k_1.k_2$. Mais alors $\operatorname{pgcd}(k_1, n) \neq \pm n$ car n ne divise pas k_1 et $\operatorname{pgcd}(k_1, n) \neq \pm 1$ car si k_1 et n étaient premiers entre eux, alors n diviserait k_2 d'après le lemme de Gauss. On en déduit que n possède un diviseur autre que $\pm 1, \pm n$ et qu'il n'est donc pas premier.

SUJET B

Question 1
Soit A un anneau unitaire. Un élément $a \in A$ est inversible si il existe $b \in A$ tel que $a.b = b.a = 1_A$.

Question 2
Supposons que I contient un élément d inversible. Alors pour tout $a \in A$, on a $a = a.(d^{-1}.d) = (a.d^{-1}).d \in I$ puisque I est stable par multiplication par tout élément de A. On a donc $A \subset I$ et donc $I = A$.

Question 3
Soit $k \in \mathbb{Z}^*$ tel que $\operatorname{pgcd}(k, n) = 1$. D'après le théorème de Bachet-Bézout, il existe alors $u, v \in \mathbb{Z}$ tels que $u.k + v.n = 1$ et on a $\overline{1} = \overline{u}.\overline{k} + \overline{v}.\overline{n} = \overline{u}.\overline{k} = \overline{v}.\overline{u}$. On en déduit que $\overline{k}$ est inversible.

Réciproquement, si $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ est inversible, alors il existe $\overline{k}' \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{k}.\overline{k}' = \overline{1}$. On a alors $\overline{k.k'} = \overline{1}$ et il existe donc $d \in \mathbb{Z}$ tel que $k.k' - 1 = d.n$. Cela donne une relation de Bézout $k'.k - d.n = 1$ entre k et n qui sont donc premiers entre eux.