Examen

CORRIGÉ

Solution 1. —

1. (a) C'est le théorème chinois puisque $n = 3 \times 11 \times 17$.
   (b) Le cardinal de $(\mathbf{Z}/n\mathbf{Z})^\times$ est $\varphi(n) = \varphi(3)\varphi(11)\varphi(17) = 2 \times 10 \times 16 = 320$.
2. (a) L'ordre de $2 \pmod{11}$ divise 10, d'après le théorème de Lagrange dans le groupe $(\mathbf{Z}/11\mathbf{Z})^\times$. On a $2^2 \not\equiv 1 \pmod{11}$ et $2^5 \equiv -1 \pmod{11}$ donc l'ordre de $2 \pmod{11}$ est 10.
   (b) L'ordre de $3 \pmod{17}$ divise 16. On a $3^2 \equiv 9 \pmod{17}$ et $3^4 \equiv -4 \pmod{17}$ donc $3^8 \equiv -1 \pmod{17}$. L'ordre de $3 \pmod{17}$ ne divise pas 8 et divise 16.
   (c) $(1 \pmod 3, 2 \pmod{11}, 3 \pmod{17})^k = (1^k \pmod 3, 2^k \pmod{11}, 3^k \pmod{17}) = (1,1,1)$ si et seulement si k est divisible par 1, par 10, et par 16, c'est-à-dire, si et seulement si $80 = \operatorname{ppcm}(1,10,16)$ divise k.
   (d) On remarque que $343 \equiv 1 \pmod 3$, $343 \equiv 2 \pmod{11}$, $343 \equiv 3 \pmod{17}$. D'où le résultat, en utilisant l'isomorphisme de groupes entre $(\mathbf{Z}/n\mathbf{Z})^\times$ et $\big(\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/11\mathbf{Z} \times \mathbf{Z}/17\mathbf{Z}\big)^\times = \mathbf{Z}/3\mathbf{Z}^\times \times \mathbf{Z}/11\mathbf{Z}^\times \times \mathbf{Z}/17\mathbf{Z}^\times$.
3. (a) Soit x premier avec n. Pour $p = 3, 11, 17$, on a $x^{p-1} \equiv 1 \pmod p$, car $(p,x) = 1$. Dans ce cas $p-1$ divise 80 donc $x^{80} \equiv 1 \pmod p$, puis par le Lemme de Gauss (ou le théorème chinois), $x^{80} \equiv 1 \pmod n$.
   (b) Soit $x \in \mathbf{Z}$. Si $p = 3, 11$ ou 17 divise x alors $x^m \equiv x \equiv 0 \pmod p$. Sinon, si $p \nmid x$, $x^{p-1} \equiv 1 \pmod p$ et $x^{m-1} \equiv 1 \pmod p$, puisque $p-1$ divise $m-1$. Donc $x^m \equiv x \pmod p$. Dans tous les cas $x^m \equiv x \pmod p$. On a donc $x^m \equiv x \pmod n$.
   (c) 80 divise $560 = n-1$, donc $x^n \equiv x \pmod n$, pour tout entier x.

Solution 2. —

1. (a) $X^2 - 10 = X^2 - 3 \pmod 7$. Le polynôme $X^2 - 3$ n'a pas de racine dans $\mathbf{Z}/7\mathbf{Z}$ (les carrés de $\mathbf{Z}/7\mathbf{Z}$ sont $0, 1, 2, 4$) donc est irréductible dans $\mathbf{Z}/7\mathbf{Z}[X]$ et a fortiori dans $\mathbf{Z}[X]$.
   Autre réponse : critère d'Eisenstein avec $p = 2$ ou $p = 5$.
   (b) $\sqrt{10}$ est racine de $P = X^2 - 10$ irréductible dans $\mathbf{Q}[X]$ donc $\sqrt{10} \notin \mathbf{Q}$, sinon $X - \sqrt{10}$ diviserait $X^2 - 10$ dans $\mathbf{Q}[X]$. $X^2 - 10$ *est le polynôme minimal de* $\sqrt{10}$.
2. (a) Si $x = a + b\sqrt{10} = c + d\sqrt{10}$, alors $(a-c) + (b-d)\sqrt{10} = 0$ et le polynôme $(a-c) + (b-d)X$ annule $\sqrt{10}$. Il est donc divisible par $X^2 - 10$ et est donc nul. Donc $a = c$ et $b = d$.
   (b) A est clairement un sous-groupe de $\mathbf{R}$ image de $\mathbf{Z}^2$ par $(a,b) \mapsto a + b\sqrt{10}$. Par ailleurs, $1 \in \mathbf{Z} \subset A$.
   Si $x = a + b\sqrt{10}$ et $y = c + d\sqrt{10}$, alors $xy = (ac + 10bd) + (ad + bc)\sqrt{10} \in A$. A est un sous-groupe additif stable par produit, contenant 1, c'est donc un sous-anneau de $\mathbf{R}$.
3. (a) On a $N(xy) = (ac + 10bd)^2 - 10(ad + bc)^2 = (a^2 - 10b^2)(c^2 - 10d^2)$.
   (b) Si $xy = 1$ alors $N(x)N(y) = N(1) = 1$ donc $N(x) = \pm 1$ car $N(x)$ est inversible dans $\mathbf{Z}$. Réciproquement, si $N(x) = \varepsilon = \pm 1$, alors l'inverse de $x = a + b\sqrt{10}$ est $x' = \varepsilon \cdot (a - b\sqrt{10})$.
4. (a) On vérifie que $N(3 + \sqrt{10}) = 3^2 - 10 = -1$ et $N(19 + 6\sqrt{10}) = 19^2 - 360 = 1$.
   (b) On a $x_0 = 3 + \sqrt{10} > 1$ donc $(x_0^n)_n$ est une suite strictement croissante, donc infinie, d'éléments de $A^\times$.
   (c) De même $x_0^{-n} = (\sqrt{10} - 3)^n \underset{n \to \infty}{\to} 0^+$. Donc $0 \leq \inf\{x \in A^\times \mid x > 0\} \leq \inf\{x_0^{-n}, n \in \mathbf{N}\} = 0$.
5. (a) Si $a = 10k + u$ alors $a^2 - 10b^2 \equiv u^2 \pmod{10}$. Mais 2 ou -2 n'est pas un carré modulo 10 (les carrés sont $1, 4, 5, 6, 9$).
   (b) Si $2 = xy$ alors $N(x)N(y) = 4$. Mais alors, si x et y ne sont pas inversibles, on doit avoir $N(x) = N(y) = \pm 2$, ce qui est impossible. Donc x ou y est inversible et 2 divise x ou y.
6. On a $(4 + \sqrt{10})(4 - \sqrt{10}) = 2 \times 3$. Mais $N(4 + \sqrt{10}) = 6$. Donc $4 + \sqrt{10}$ est irréductible, sinon, il aurait un diviseur de norme ± 2. De la même façon $4 - \sqrt{10}$ est irréductible. La décomposition en irréductibles de 6 n'est pas unique. A n'est pas factoriel.