Examen

Mercredi 15 mai 2024 - Durée 2h
Corrigé

Solution 1. —

1. *Il existe un corps de cardinal* 36.
   Faux. Le cardinal d'un corps est une puissance d'un nombre premier.
2. Vrai. On a $2^4 = 3$ et $2^6 = -1$. Donc l'ordre de 2 ne divise ni 4, ni 6. Il divise 12 (th. de Lagrange) donc est égal à 12. 2 est donc un générateur de $(\mathbf{Z}/13\mathbf{Z})^*$.
3. Faux. $x = 43$ est bien une solution particulière. Deux solutions x et x' vérifient $x \equiv x' \pmod 8$ et $x \equiv x' \pmod{12}$, c'est-à-dire, $24 = \text{ppcm}(8,12) | x - x'$. Ainsi les solutions sont $x \equiv 43 \pmod{24} \equiv 19 \pmod{24}$.

Solution 2. —

1. $\mathbf{Z} + \alpha\mathbf{Z}$ est un sous-anneau de $\mathbf{C}$, (puisque $(a+\alpha a')(b+\alpha b') = ab - pa'b' + \alpha(ab' + a'b)$), contenant α, donc contient dans $\mathbf{Z}[\alpha]$. D'un autre côté, $\mathbf{Z}[\alpha]$ contient $\mathbf{Z}$ et $\alpha\mathbf{Z}$.
2. On a

$$\begin{aligned}\Phi((x,y)-(x',y')) = \Phi((x-x',y-y')) = (x-x') + (y-y')\alpha &= (x+y\alpha) - (x'+y'\alpha) \\ &= \Phi((x,y)) - \Phi((x',y')),\end{aligned}$$

   donc Φ est un morphisme de groupes, surjectif par définition. Soit $x, y \in \mathbf{Z}$ tels que $x + \alpha y = 0$. Si $y \neq 0$, alors $\alpha = -\frac{x}{y} \in \mathbf{Q}$, ce qui n'est pas possible, puisque $\alpha \in \mathbf{C} - \mathbf{R}$. On a donc $y = 0$ et $x = -\alpha y = 0$. Donc $\Phi(z) = 0 \Leftrightarrow z = 0$ et Φ est un isomorphisme.
3. On a $\alpha\mathbf{Z}[\alpha] = \alpha\mathbf{Z} + \alpha^2\mathbf{Z} = p\mathbf{Z} + \alpha\mathbf{Z}$. On déduit que α divise $a + b\alpha$ dans $\mathbf{Z}[\alpha]$ si et seulement si p divise a.
4. Soit $b = b_1 + \alpha b_2$ et $c = c_1 + \alpha c_2$. $bc \in \alpha\mathbf{Z}[\alpha]$ si et seulement si p divise $b_1 b_2 - p c_1 c_2$, c'est-à-dire, p divise $b_1 c_1$. p est premier donc p divise $b_1 c_1$ si et seulement si p divise b_1 ou p divise c_1. On en déduit que α divise bc si et seulement si α divise b ou α divise c.
   Par ailleurs α n'est pas inversible car $\alpha\mathbf{Z}[\alpha] \neq \mathbf{Z}[\alpha]$, donc α est premier.

Solution 3. —

1. (a) On calcule $(a+ib)\cdot(x+iy) = (ax-by) + i(ay+bx)$. On a donc $m - (ax-by) = i(ay+bx)$. Comme $(1,i)$ est libre dans $\mathbf{Q}(i)$, on a donc $m - (ax-by) = ay + bx = 0$.
   (b) Si $(x,y) = \lambda(-a,b)$ alors $ay + bx = \lambda(ab - ba) = 0$. Réciproquement si $ay + bx = 0$ alors b divise ay donc b divise y (lemme de Gauss), donc il existe $\lambda \in \mathbf{Z}$, tel que $y = \lambda b$. Mais alors $0 = ay + bx = b(\lambda a + x)$ et $x = -\lambda a$. Donc $(x,y) = \lambda(-a,b)$. On a donc l'égalité demandée.
   (c) $m \in \ker\Phi$ si et seulement si il existe $z = x + iy \in \mathbf{Z}[i]$, tel que $m = (a+ib)(x+iy)$. On a donc $ay + bx = 0$, c'est-à-dire, $(x,y) = \lambda(a,-b), \lambda \in \mathbf{Z}$. Mais alors $m = ax - by = \lambda(a^2+b^2) \in (a^2+b^2)\mathbf{Z}$. Réciproquement si $m = \lambda(a^2+b^2)$, on a $m = \lambda(a+ib)(a-ib) \in (a+ib)$.
2. (a) Calculons, comme dans la question précédente, on obtient $bu - av = t$ et $au + bv = 1$.
   (b) $\Phi(t_0) \equiv i \pmod{(a+ib)}$ si et seulement si il existe $u, v \in \mathbf{Z}$, tels que $i - t_0 = (a+ib)(v+iu)$. Considérons $u_0, v_0 \in \mathbf{Z}$ tels que $au_0 + bv_0 = 1$, ce qui est possible car $(a,b) = 1$ et posons $t_0 = bu_0 - av_0$, alors $\Phi(t_0) \equiv i \pmod{(a+ib)}$.

(c) On obtient $\Phi(x+t_0y) \equiv x+y\Phi(t_0) \equiv x+iy \pmod{(a+ib)}$, donc Φ est surjective. On a alors

$$\mathbf{Z}[i]/(a+ib) = \mathrm{Im}\,\Phi \simeq \mathbf{Z}/\ker\Phi = \mathbf{Z}/(a^2+b^2)\mathbf{Z}.$$

3. Les deux anneaux sont isomorphes donc en bijection et ont même cardinal, c'est-à-dire, a^2+b^2.
4. Considérons le morphisme canonique de $\mathbf{Z}[i]$ vers $\mathbf{Z}[i]/(a+ib)$ défini par $\Psi(x+iy) = (x+iy) \pmod{(a+ib)}$. On a alors $\Psi(x+iy) = \Phi(x+t_0y)$. On déduit que $(a+ib)$ divise $x+iy$ si et seulement si $\Psi(x+iy) = 0$, c'est-à-dire, $x+t_0y \in \ker\Phi$, c'est-à-dire, a^2+b^2 divise $x+t_0y$.

Solution 4. —

1. On a $X^8-1 = (X^2-1)\cdot P$.
2. (a) On a bien $P = (1+X^2)(1+X^4) = 1+X^2+X^4+X^6 \in \mathbf{Z}[X]$
   (b) $\Phi_4 = 1+X^2$ est irréductible dans $\mathbf{Q}[X]$ car il n'a pas de racine réelle. $\Phi_8 = X^4+1$ est irréductible sinon $\Phi_8(X+1)$ ne le serait pas. Mais $\Phi_8(X+1) = X^4+4X^3+6X^2+4X+2$. Donc $\Phi_8(X+1)$ est irréductible, d'après le critère d'Eisenstein. Ainsi $P = (1+X^2)(1+X^4)$ est la factorisation de P en produits d'irréductibles dans $\mathbf{Q}[X]$.
3. (a) Les racines de P vérifient donc $x^{(p-1)/2} = 1$. Ce sont des carrés de K.
   (b) Les racines de P sont les racines de X^8-1 sauf celles de X^2-1 : $\{-1 = 4^2, 1 = 1^2\}$. On obtient donc tous les autres carrés de K^*. Les racines sont donc $2^2 = 4, 3^2 = 9, 5^2 = 8, 6^2 = 2, 7^2 = 15, 8^2 = 13$.
4. (a) On a $X^6+X^4+X^2+1 = (X^3-X)^2+1$ donc $(P, X^3-X) = 1$.
   (b) Les facteurs irréductibles de P sont donc tous de degré 2, car P divise $X^{p^2}-X$.
   (c) On sait que $P = (X^2+1)(X^4+1)$. Mais $X^4+1 = (X^2-1)^2-X^2 = (X^2-X-1)(X^2+X-1)$. Ainsi $P = (X^2+1)(X^2+X-1)(X^2-X-1)$.