

*Solutions MP/MP**
Algèbre Générale

Solution 1. Soit $(x, y) \in G^2$. On a d'abord

$$x \cdot y = (x \cdot y)^{p+1} (x \cdot y)^{-p} \quad (1)$$

$$= x^{p+1} \cdot y^{p+1} \cdot y^{-p} \cdot x^{-p} \quad (2)$$

$$= x^{p+1} \cdot y \cdot x^{-p} \quad (3)$$

On cherche maintenant à montrer que x^{p+1} et y commutent. On a

$$y^{p+2} \cdot x^{p+2} = (y \cdot x)^{p+2} \quad (4)$$

$$= (y \cdot x)^{p+1} \cdot y \cdot x \quad (5)$$

$$= y^{p+1} \cdot x^{p+1} \cdot y \cdot x \quad (6)$$

Donc on a $y \cdot x^{p+1} = x^{p+1} \cdot y$. En reportant dans (3), on a $x \cdot y = y \cdot x$ et donc

G est abélien.

(7)

■

Remarque 1.

- Pour (Σ_3, \cdot) , on a f_0, f_1 et f_6 des morphismes mais Σ_3 n'est pas commutatif.
- Si f_2 est un morphisme, alors on a $(x \cdot y)^2 = x \cdot y \cdot x \cdot y = x^2 \cdot y^2$ d'où $y \cdot x = x \cdot y$.

Solution 2. A est non vide car $\omega(e_G) = 1$ et $e_G \in A$. Soit $x \in A$ tel que $\omega(x) = 2p + 1$. Soit $k \in \mathbb{Z}$, on a

$$x^{2k} = e_G \Leftrightarrow 2p + 1 \mid 2k \quad (8)$$

$$\Leftrightarrow 2p + 1 \mid k \quad (9)$$

d'après le théorème de Gauss.

Ainsi, $\omega(x^2) = 2p + 1$ et $x^2 \in A$, donc

$$\begin{array}{ccc} \varphi : & A & \rightarrow A \\ & x & \mapsto x^2 \end{array} \quad (10)$$

est bien définie. Soit $x \in A$, il existe $p \in \mathbb{N}$ tel que $x^{2p+1} = e_G$ donc $x^{2p+2} = x$ d'où $(x^{p+1})^2 = x$. Il suffit donc de vérifier que $x^{p+1} \in A$ pour montrer que l'application est surjective. Comme A est fini, elle sera bijective.

On a $gr\{x^{p+1}\} \subset gr\{x\}$ et $(x^{p+1})^2 = x$ donc $gr\{x\} = gr\{x^{p+1}\}$ donc $\omega(x) = \omega(x^{p+1}) = 2p + 1$ et donc $x^{p+1} \in A$.

Donc A est bijective.

(11)

■

Solution 3. On note $m = \theta(\sigma)$. On suppose que σ se décompose en produit de cycle de longueur l_1, \dots, l_m avec $l_1 + \dots + l_m = n$. Comme

$$(a_1, \dots, a_l) = [a_1, a_2] \circ [a_2, a_3] \circ \dots \circ [a_{l-1}, a_l] \quad (12)$$

Donc σ se décompose en $\sum_{i=1}^m (l_i - 1) = n - m$ transpositions. Montrons par récurrence sur k , $\mathcal{H}(k)$: "Un produit de k transpositions possède au moins $n - k$ orbites".

Pour $k = 0$, $\sigma = id$ possède n orbites.

Pour $k = 1$, soit τ une transposition, on a $\theta(\tau) = n - 2 + 1 = n - 1$.

Soit $k \in \mathbb{N}$, supposons \mathcal{H}_k , soit $\sigma \in \Sigma_n$ qui se décompose en produit de $k + 1$ transpositions.

$$\sigma = \underbrace{\tau_1 \circ \dots \tau_k}_{\sigma'} \circ \tau_{k+1} \quad (13)$$

D'après \mathcal{H}_k , on a $\theta(\sigma') \geq n - k$. Notons $\tau_{k+1} = [a, b]$.

Si a et b appartiennent à la même orbite. On note (a_1, \dots, a_r) le cycle correspondant avec $a_r = a$ et $a_s = b$ où $s \in \llbracket 1, n - 1 \rrbracket$. On a

$$\begin{cases} (a_1, \dots, a_{r-1}, a_r) \circ [a, b](a_i) = a_{i+1} & \text{où } i \notin \{r, s\} \\ (a_1, \dots, a_{r-1}, a_r) \circ [a, b](a_r) = a_{s+1} \\ (a_1, \dots, a_{r-1}, a_r) \circ [a, b](a_s) = a_1 \end{cases} \quad (14)$$

On n'a pas perdu d'orbites, donc $\theta(\sigma) \geq n - k - 1$.

Si a et b n'appartiennent pas à la même orbite, notons (a_1, \dots, a_r) et (b_1, \dots, b_s) ces orbites avec $a = a_r$ et $b = b_s$. On a

$$\begin{cases} \underbrace{(a_1, \dots, a_{r-1}, a_r) \circ (b_1, \dots, b_s) \circ [a_r, b_s]}_{\sigma''}(a_i) = a_{i+1} & \text{où } i \in \llbracket 1, \dots, r - 1 \rrbracket \\ (a_1, \dots, a_{r-1}, a_r) \circ (b_1, \dots, b_s) \circ [a_r, b_s](b_j) = b_{j+1} & \text{où } j \in \llbracket 1, \dots, s - 1 \rrbracket \\ (a_1, \dots, a_{r-1}, a_r) \circ (b_1, \dots, b_s) \circ [a_r, b_s](a_r) = b_1 \\ (a_1, \dots, a_{r-1}, a_r) \circ (b_1, \dots, b_s) \circ [a_r, b_s](b_s) = a_1 \end{cases} \quad (15)$$

Donc

$$\sigma'' = (a_1, \dots, a_r, b_1, \dots, b_s) \quad (16)$$

On a perdu une orbite et donc $\theta(\sigma) \geq n - k - 1$.

D'où le résultat par récurrence sur k .

(17)

■

Solution 4. On note par \bar{k} les éléments de $\mathbb{Z}/n\mathbb{Z}$ et par \tilde{l} les éléments de $\mathbb{Z}/m\mathbb{Z}$.

Soit f un morphisme. On pose $f(\bar{1}) = \tilde{x}$ où $x \in \llbracket 0, m - 1 \rrbracket$. On a donc $nf(\bar{1}) = f(\bar{0}) = \tilde{0}$.

On a donc $\tilde{n}x = \tilde{0}$ donc $m \mid nx$. On écrit $m = m_1(m \wedge n)$ et $n = n_1(m \wedge n)$. D'après le théorème de Gauss, on a donc $m_1 \mid x$. Donc $x = km_1$ avec $k \in \llbracket 0, (n \wedge m) - 1 \rrbracket$.

Réciproquement, soit $k \in \llbracket 0, (n \wedge m) - 1 \rrbracket$. On définit

$$\begin{aligned} f_k : \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/m\mathbb{Z} \\ \bar{l} &\mapsto \widetilde{lk m_1} \end{aligned} \quad (18)$$

Si $\bar{l} = \bar{l}'$, alors $n \mid l - l'$ et donc $nm_1 \mid (l - l')km_1$ puis $n_1(n \wedge m)m_1 \mid (l - l')km_1$ donc $m \mid (l - l')km_1$ d'où $\widetilde{lk m_1} = \widetilde{l'k m_1}$ donc f est bien définie et c'est évidemment un morphisme.

Soit $k, k' \in \llbracket 0, n \wedge m - 1 \rrbracket$ avec $k \neq k'$. Si $\widetilde{km_1} = \widetilde{k'm_1}$ alors $m \mid (k - k')m_1$ et donc $n \wedge m \mid k - k'$ et $|k - k'| < n \wedge m$ donc $k = k'$ ce qui est absurde. Ainsi, les f_k sont distincts.

On a donc $n \wedge m$ morphismes.

(19)

■

Remarque 2. Exemple pour l'exercice précédent : morphisme de $\mathbb{Z}/4\mathbb{Z}$ dans $\mathbb{Z}/6\mathbb{Z}$. On a $f(\bar{1}) = \widetilde{x}$ d'où $\widetilde{4x} = \widetilde{0}$ donc $3 \mid x$ d'où $x \in \{0, 3\}$. On a donc le morphisme trivial $f_0 : \bar{l} \mapsto \widetilde{0}$ et $f_1 : \bar{l} \mapsto \widetilde{3l}$.

Solution 5. On considère $H = \{x \in G \mid x^2 = e_G\}$. Si $x \notin H$, alors $x^{-1} \neq x$ et donc

$$P = \prod_{x \in H} x \quad (20)$$

H est le noyau du morphisme $x \mapsto x^2$ (morphisme car G est abélien) donc H est un sous-groupe. Soit K un sous-groupe de H et $a \in H \setminus K$. Montrons que $K \cup aK$ est un sous-groupe de H .

On a $e_G \in K \cup aK$. Soit $x \in K \cup aK \subset H$, on a $x^{-1} = x \in K \cup aK$. Soit $(x_1, x_2) \in (K \cup aK)^2$, si $(x_1, x_2) \in K^2$, c'est ok. Si $(x_1, x_2) \in (aK)^2$, on note $x_1 = a \cdot k_1$ et $x_2 = a \cdot k_2$ avec $(k_1, k_2) \in K^2$. On a $x_1 \cdot x_2 = a^2 \cdot k_1 \cdot k_2 = k_1 \cdot k_2 \in K$. Si $x_1 \in K$ et $x_2 \in aK$, alors $x_1 \cdot x_2 = a \cdot k_1 \cdot k_2 \in aK$. Donc $K \cup aK$ est un sous-groupe de H .

Soit $x \in K \cap aK$, il existe $(k_1, k_2) \in K^2$ tel que $k_1 = a \cdot k_2$ et $a \in K$ ce qui est impossible. Donc $K \cap aK = \emptyset$.

On construit alors par récurrence K_n : on pose $K_0 = \{e_G\}$ et à l'étape n , si $K_n = H$ on arrête, sinon il existe $a_{n+1} \in H \setminus K_n$ et on pose $K_{n+1} = K_n \cup a_{n+1}K$. Alors $|K_{n+1}| = 2|K_n|$. Comme H est fini, il existe $n_0 \in \mathbb{N}$ tel que $H = K_{n_0}$. On a alors $|H| = 2^{n_0}$.

Ainsi, si $n_0 = 0$, on a $H = \{e_G\}$ et

$P = e_G$

(21)

Si $n_0 = 1$, on a $H = \{e_G, a_1\}$ et

$P = a_1 \neq e_G$

(22)

Si $n_0 \geq 2$, comme chaque a_k apparaît un nombre pair de fois dans le produit, on a

$$P = e_G \quad (23)$$

■

Solution 6. Soit $x_0 \in \mathbb{R}$. $(\overline{kx_0})_{0 \leq k \leq n}$ ne sont pas deux à deux distincts. Donc il existe $l \neq l' \in \llbracket 0, n \rrbracket^2$ tel que $\overline{lx_0} = \overline{l'x_0}$ d'où $0 < |l - l'| \leq n$. Donc il existe $j \in \llbracket 1, n \rrbracket$ avec $jx_0 \in G$. Ainsi, $n!x_0 \in G$ (itéré de jx_0). Ce raisonnement est vrai pour $x = \frac{x_0}{n!}$ donc $x_0 \in G$. Ainsi,

$$G = \mathbb{R} \quad (24)$$

■

Solution 7. Soit f un isomorphisme de $\mathbb{Z}/n\mathbb{Z}$ dans lui-même. Soit $k \in \llbracket 0, n-1 \rrbracket$, on a $f(\overline{k}) = \overline{kf(1)}$. Par isomorphisme, $\omega(f(1)) = \omega(1) = n$. Notons alors $\overline{x} = f(1)$ avec $x \in \llbracket 0, n-1 \rrbracket$.

Si $x \wedge n = 1$, il existe $(u, v) \in \mathbb{Z}^2$ tel que $ux + vn = 1$, donc $u\overline{x} = \overline{1} \in \text{gr}\{\overline{x}\}$. Ainsi, $\mathbb{Z}/n\mathbb{Z} = \text{gr}\{\overline{x}\}$ (car les éléments de $\mathbb{Z}/n\mathbb{Z}$ sont des itérés de $\overline{1}$) donc $\omega(\overline{x}) = n$.

Réciproquement, si $\omega(\overline{x}) = n$, $\overline{1} \in \text{gr}\{\overline{x}\}$ donc il existe $u \in \mathbb{Z}$ tel que $u\overline{x} = \overline{1} = \overline{ux}$. Donc $n \mid ux - 1$, c'est-à-dire qu'il existe $v \in \mathbb{Z}$ tel que $ux - 1 = vn$, d'où $ux + vn = 1$. D'après Bézout, on a $x \wedge n = 1$. Finalement, on a $\omega(\overline{x}) = n$ si et seulement si $x \wedge n = 1$.

Ainsi, les isomorphismes sont nécessairement de la forme

$$f_x : \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \rightarrow & \mathbb{Z}/n\mathbb{Z} \\ \overline{k} & \mapsto & \overline{kx} \end{array} \quad (25)$$

où $x \in \llbracket 0, n-1 \rrbracket$ et $x \wedge n = 1$.

Réciproquement, si $x \in \llbracket 0, n-1 \rrbracket$ est tel que $x \wedge n = 1$, f_x est évidemment un morphisme. Si $\overline{k} \in \ker(f_x)$, on a $f_x(\overline{k}) = \overline{0}$ si et seulement si $\overline{kx} = \overline{0}$ si et seulement si $n \mid kx$ et comme $n \wedge x = 1$, d'après le théorème de Gauss, on a $n \mid k$ donc $\overline{k} = \overline{0}$ donc $\ker(f_x) = \{\overline{0}\}$. Donc f_x est injective, donc bijective car $|\mathbb{Z}/n\mathbb{Z}| = |\mathbb{Z}/n\mathbb{Z}| = n$. ■

Solution 8. Si $y \in \text{Im}\varphi$, y possède $|\ker \varphi|$ antécédents. En effet, il existe $x_0 \in G$ tel que $y = \varphi(x_0)$. Pour tout $x \in G$, on a $\varphi(x) = y$ si et seulement si $\varphi(x) = \varphi(x_0)$ si et seulement si $\varphi(x_0^{-1} \cdot x) = e_G$ si et seulement si $x_0^{-1} \cdot x \in \ker \varphi$ si et seulement si $x \in x_0 \ker \varphi$. Comme

$$g : \begin{array}{ccc} \ker \varphi & \rightarrow & x_0 \ker \varphi \\ x & \mapsto & x \cdot x_0 \end{array} \quad (26)$$

est bijective, on a $|\ker \varphi| = |x_0 \ker \varphi|$. Ainsi, on a $|G| = |\text{Im}\varphi| \times |\ker \varphi|$.

Dans tous les cas, on a $\ker \varphi \subset \ker \varphi^2$ et $\text{Im} \varphi^2 \subset \text{Im} \varphi$. On a ensuite

$$\text{Im} \varphi^2 = \text{Im} \varphi \iff |\text{Im} \varphi^2| = |\text{Im} \varphi| \quad (27)$$

$$\iff |\ker \varphi^2| |\text{Im} \varphi^2| = |\ker \varphi^2| |\text{Im} \varphi| = |G| = |\ker \varphi| |\text{Im} \varphi| \quad (28)$$

$$\iff |\ker \varphi^2| = |\ker \varphi| \quad (29)$$

$$\iff \boxed{\ker \varphi^2 = \ker \varphi} \quad (30)$$

■

Solution 9. On considère

$$\begin{aligned} f : G &\rightarrow G \\ x &\mapsto x^m \end{aligned} \quad (31)$$

l'exercice revient à montrer que f est bijective. D'après le théorème de Bézout, il existe $(a, b) \in \mathbb{Z}^2$ tel que $am + bn = 1$. Soit $y \in G$, on a

$$y^1 = y = y^{am+bn} = y^{am} \cdot \underbrace{y^{bn}}_{=e_G} = y^{am} = (y^a)^m \quad (32)$$

Donc f est surjective et comme G est fini,

$$\boxed{f \text{ est bijective.}} \quad (33)$$

■

Solution 10.

1. On a $e_G \in S_g$, si $(x, y) \in S_g^2$ alors $x \cdot y \cdot g = x \cdot g \cdot y = g \cdot x \cdot y$ donc $x \cdot y \in S_g$ et si $x \in S_g$ alors $x \cdot g = g \cdot x$ implique $g \cdot x^{-1} = x^{-1} \cdot g$ en multipliant par l'inverse de x à gauche et à droite donc

$$\boxed{x^{-1} \in S_g} \quad (34)$$

2. Soit $(h, h') \in G^2$. On a $h \cdot g \cdot h^{-1} = h' \cdot g \cdot h'^{-1}$ si et seulement si $g \cdot h^{-1} \cdot h' = h^{-1} \cdot h \cdot g$ si et seulement si $h^{-1} \cdot h \in S_g$ si et seulement si $h' \in hS_g$. Or $|hS_g| = |S_g|$ car

$$\begin{aligned} I_h : S_g &\rightarrow hS_g \\ x &\mapsto h \cdot x \end{aligned} \quad (35)$$

est bijective de réciproque $I_{h^{-1}}$. Soit la relation d'équivalence \mathcal{R}_0 sur G définie par $h\mathcal{R}_0 h'$ si et seulement si $h \cdot g \cdot h^{-1} = h' \cdot g \cdot h'^{-1}$. Chaque classe à $|S_g|$ éléments et il y a $|C(g)|$ classes dans G d'où

$$\boxed{|G| = |S_g| |C(g)|} \quad (36)$$

3. On a $Z(G) = \cap_{g \in G} S_g$ donc $Z(G)$ est un sous-groupe et pour tout $g \in G$,

$$\boxed{Z(G) \subset S_g} \quad (37)$$

4. Pour $x \in G$, on note $\bar{x} = \{h \cdot x \cdot h^{-1} \mid h \in G\} = C(x)$.

On a $|\bar{x}| = 1$ si et seulement si pour tout $h \in G$, $h \cdot x \cdot h^{-1} = x$ si et seulement si $x \in Z(G)$.

Soit \mathcal{A} une partie de G telle que $(\bar{x})_{x \in \mathcal{A}}$ forme une partition de $G \setminus Z(G)$. On a

$$|G| = p^\alpha = |Z(G)| + \sum_{x \in \mathcal{A}} |C(x)| \quad (38)$$

Si $x \in \mathcal{A}$, $x \notin Z(G)$ donc $|S_x| < |G|$ (car $x \in Z(G)$ si et seulement si $S_x = G$) et donc

$$|C(x)| = \frac{|G|}{|S_x|} \quad (39)$$

d'après 2. Donc $|C(x)| = p^\beta$ avec $\beta \in \llbracket 1, \alpha \rrbracket$ car $|C(x)| \neq 1$. Donc

$$p \mid \sum_{x \in \mathcal{A}} |C(x)| \quad (40)$$

d'où

$$p \mid |Z(G)| \quad (41)$$

donc

$$\boxed{|Z(G)| \neq 1} \quad (42)$$

5. On a

$$p^2 = |Z(G)| + \sum_{x \in \mathcal{A}} |C(x)| \quad (43)$$

D'après la question 4, on a $|Z(G)| \neq 1$ et $|Z(G)| \mid |G|$.

Si $Z(G) \neq G$, alors $|Z(G)| = p$. Pour $x \in \mathcal{A}$, $Z(G) \subset S_x \neq G$ donc $|S_x| = p$ (car $|S_x| \mid |G|$) et donc $Z(G) = S_x$. Or $x \in S_x$ et $x \notin Z(G)$ ce qui n'est pas possible, donc $|Z(G)| = p^2$ et $Z(G) = G$.

$$\boxed{\text{Donc } G \text{ est abélien.}} \quad (44)$$

S'il existe un élément d'ordre p^2 . G est cyclique et est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$. Sinon, pour tout $x \in G \setminus \{e_G\}$, on a $\omega(x) = p$. Soit $x_1 \in G \setminus \{e_G\}$ et $x_2 \in G \setminus \text{gr}\{x_1\}$. Soit

$$\begin{aligned} f : (\mathbb{Z}/p\mathbb{Z})^2 &\rightarrow G \\ (\bar{k}, \bar{l}) &\mapsto x_1^k \cdot x_2^l \end{aligned} \quad (45)$$

f est bien définie car si $\bar{k} = \bar{k}'$ et $\bar{l} = \bar{l}'$, on a $p \mid k - k'$ et $p \mid l - l'$ donc $x_1^k \cdot x_2^l = x_1^{k'} \cdot x_2^{l'}$. Comme G est abélien, f est un morphisme.

Montrons que f est injective. Soit $(\bar{k}, \bar{l}) \in \ker(f)$ avec $(k, l) \in \llbracket 0, p-1 \rrbracket^2$, on a $x_1^k \cdot x_2^l = e_G$ donc $x_2^l = x_1^{-k}$. Si $l \in \llbracket 1, p-1 \rrbracket$ or p est premier donc $l \wedge p = 1$ donc il existe $(u, v) \in \mathbb{Z}^2$ tel que $lu + pv = 1$. Alors on a

$$x_2 = x_2^{lu+pv} = x_2^{lu} \cdot x_2^{pv} = x_2^{lu} = x_1^{-k} \in \text{gr}\{x_1\} \quad (46)$$

ce qui n'est pas possible. Donc $\bar{l} = \bar{0}$ et de même $\bar{k} = \bar{0}$ donc f est injective et ainsi $|\mathbb{Z}/p^2\mathbb{Z}| = |G|$ donc

$f \text{ est un isomorphisme.}$

(47)

■

Remarque 3. Les groupes de cardinal p^3 ne sont pas nécessairement abélien, par exemple le groupe des isométries du carré \mathcal{D}_4 de cardinal 8.

Solution 11. Soit f un morphisme de $(\mathbb{Z}, +)$ dans (\mathbb{Q}_+^*, \times) . Pour tout $n \in \mathbb{Z}$, $f(n) = f(1)^n$ donc il existe $r_0 \in \mathbb{Q}_+^*$ tel que $f(1) = r_0$ donc

$f: n \mapsto r_0^n$

(48)

Soit f un morphisme de $(\mathbb{Q}, +)$ dans (\mathbb{Q}_+^*, \times) . Pour tout $a \in \mathbb{N}^*$, $f(1) = f(\frac{1}{a})^a$. Pour tout p premier, on a $\nu_p(f(1)) = a\nu_p(f(\frac{1}{a}))$ donc pour tout $a \in \mathbb{N}^*$, $a \mid \nu_p(f(1))$ donc $\nu_p(f(1)) = 0$ pour tout p premier, donc $f(1) = 1$. Ainsi, pour tout $n \in \mathbb{Z}$, $f(n) = f(1)^n = 1$ et $f(b \times \frac{a}{b}) = f(a) = 1 = f(\frac{a}{b})^b$ donc $f(\frac{a}{b}) = 1$. Donc

$f: r \mapsto 1$

(49)

■

Solution 12. On a $xy = y^2x$, $x^2y = xy^2x = y^4x^2$, $x^3y = x^2y^2x = xy^4x^2 = y^8x^3$, $x^5y = y^{32}x^5$ donc $y^{31} = e_G$ et $\omega(y) = 31$.

Tout élément de G peut s'écrire $y^\lambda x^\mu$ avec $(\lambda, \mu) \in \llbracket 0, 30 \rrbracket \times \{0, 4\}$. Soit

$$\begin{aligned} f: \llbracket 0, 30 \rrbracket \times \llbracket 0, 4 \rrbracket &\rightarrow G \\ (\lambda, \mu) &\mapsto y^\lambda x^\mu \end{aligned} \quad (50)$$

est surjective par construction. Soit $((\lambda, \mu), (\lambda', \mu')) \in (\llbracket 0, 30 \rrbracket \times \llbracket 0, 4 \rrbracket)^2$ tel que $y^\lambda x^\mu = y^{\lambda'} x^{\mu'}$ donc $y^{\lambda-\lambda'} = x^{\mu'-\mu}$ d'où $y^{5(\lambda-\lambda')} = x^{5(\mu'-\mu)} = e_G$. Or $\omega(y) = 31$ donc $31 \mid 5(\lambda - \lambda')$ et d'après le théorème de Gauss, $31 \mid \lambda - \lambda'$. Or $(\lambda, \lambda') \in \llbracket 0, 30 \rrbracket^2$ donc $\lambda = \lambda'$ et de même $\mu = \mu'$ donc f est injective donc bijective et

$|G| = 155$

(51)

Soit G' un autre tel groupe engendré par x' et y' , on forme

$$\begin{aligned} g : \quad G &\rightarrow G \\ y^p x^\mu &\mapsto y'^\lambda x'^\mu \end{aligned} \quad (52)$$

et on vérifie que g est un isomorphisme. ■

Solution 13.

1. Soit $i \in \llbracket 1, r \rrbracket$, il existe nécessairement $y_i \in G$ tel que $\nu_{p_i}(\omega(y_i)) = p_i^{\alpha_i}$ (où ν_p est la valuation p -adique), sinon on ne pourrait pas avoir ce terme dans le ppcm. Donc

$$\boxed{p_i^{\alpha_i} \mid \omega(y_i)} \quad (53)$$

2. Il existe $n \in \mathbb{N}$ tel que $\omega(y_i) = p_i^{\alpha_i} n$. Posons $x_i = y_i^n \in G$. Alors pour $k \in \mathbb{N}$,

$$x_i^k = e_G \iff y_i^{nk} = e_G \iff \omega(y_i) \mid nk \iff p_i^{\alpha_i} \mid k \quad (54)$$

Donc

$$\boxed{\omega(x_i) = p_i^{\alpha_i}} \quad (55)$$

3. On pose $x = \prod_{i=1}^r x_i$. Soit $k \in \mathbb{N}$, alors

$$x^k = e_G \iff \prod_{i=1}^r x_i^k = e_G \quad (56)$$

Pour $i \in \llbracket 1, r \rrbracket$, on met le tout à la puissance $M_i = \prod_{\substack{j=1 \\ j \neq i}}^r p_j^{\alpha_j}$. On a alors, pour tout $i \in \llbracket 1, r \rrbracket$,

$$x_i^{kM_i} = e_G \iff p_i^{\alpha_i} \mid kM_i \iff p_i^{\alpha_i} \mid k \quad (57)$$

la dernière équivalence venant du théorème de Gauss. Donc pour tout $i \in \llbracket 1, r \rrbracket$, $p_i^{\alpha_i} \mid k$, ce qui équivaut donc à $N \mid k$ et donc

$$\boxed{\omega(x) = N} \quad (58)$$

■

Solution 14. Sur un corps commutatif, un polynôme de degré n admet au plus n racines. Montrons qu'il existe $x_1 \in \mathbb{K}^*$ tel que $\omega(x_1) = |\mathbb{K}^*|$. Par définition de N , pour tout $x \in \mathbb{K}^*$, $\omega(x) \mid N$. D'où $x^N = 1_{\mathbb{K}}$. Donc x est racine de $X^N - 1$. Ainsi, $|\mathbb{K}^*| \leq N$. Par ailleurs, $N \mid |\mathbb{K}^*|$ car pour tout $x \in \mathbb{K}^*$, $x^{|\mathbb{K}^*|} = 1_{\mathbb{K}^*}$. Donc $|\mathbb{K}^*| = N$ et ainsi

$$\boxed{\mathbb{K}^* = \text{gr} \{x_1\}} \quad (59)$$

On a $|\mathbb{Z}/13\mathbb{Z}^*| = 12$ donc pour tout $\bar{x} \in (\mathbb{Z}/13\mathbb{Z})^*$, $\omega(\bar{x}) \in \{1, 2, 3, 4, 6, 12\}$. On a $\bar{2}^2 = \bar{4}$, $\bar{2}^3 = \bar{8}$, $\bar{2}^4 = \bar{16} = \bar{3}$, $\bar{2}^6 = \bar{12}$ donc $\omega(\bar{2}) = 12$ et

$$\mathbb{Z}/13\mathbb{Z}^* = \text{gr} \{ \bar{2} \} = \{ \bar{2}^k \mid k \in \llbracket 0, 11 \rrbracket \} \quad (60)$$

■

Solution 15.

1. Soit $(x, y) \in G^2$, on a $(x \cdot y)^2 = (x \cdot y) \cdot (x \cdot y) = e_G$ donc $x \cdot y = y^{-1} \cdot x^{-1}$ et comme $x^2 = e_G$, $x^{-1} = x$ d'où $xy = yx$ et

$$G \text{ est abélien.} \quad (61)$$

2. Soit (x_1, \dots, x_n) une famille génératrice minimale de G : pour tout $x \in G$, il existe $(\varepsilon_i) \in \{0, 1\}^n$ tel que $x = \prod_{i=1}^n x_i^{\varepsilon_i}$ (car G est abélien). Soit

$$\begin{aligned} f : (\mathbb{Z}/2\mathbb{Z})^n &\rightarrow G \\ (\bar{\varepsilon}_1, \dots, \bar{\varepsilon}_n) &\mapsto \prod_{i=1}^n x_i^{\varepsilon_i} \end{aligned} \quad (62)$$

Si pour tout $i \in \llbracket 1, n \rrbracket$ on a $\bar{\varepsilon}_i = \bar{\varepsilon}'_i$, alors $x^{\varepsilon_i} = x^{\varepsilon'_i}$ car $x_i^2 = e_G$ et $2 \mid \varepsilon_i - \varepsilon'_i$. Donc f est bien définie.

f est clairement un morphisme (car G est abélien). D'après la première question, f est surjective. Montrons que f est injective. Soit $(\bar{\varepsilon}_1, \dots, \bar{\varepsilon}_n)$ tel que $\prod_{i=1}^n x_i^{\varepsilon_i} = e_G$. Soit $i \in \llbracket 1, n \rrbracket$, supposons ε_i impair, on a alors $x_i = \varepsilon_i = x_i$. D'où $x_i = \prod_{j=1}^n x_j^{-\varepsilon_j} = \prod_{j=1}^n x_j^{\varepsilon_j}$ car $x^2 = e_G$. Donc $x_i \in \text{gr}(x_j, j \in \llbracket 1, n \rrbracket, j \neq i)$, ce qui contredit le caractère minimal de (x_1, \dots, x_n) .

$$\text{Ainsi, } f \text{ est injective donc est un isomorphisme.} \quad (63)$$

■

Remarque 4. En notant $+$ la loi sur G , on peut définir

$$\begin{aligned} f : \mathbb{Z}/2\mathbb{Z} \times G &\rightarrow G \\ (\varepsilon, x) &\mapsto x^\varepsilon \end{aligned} \quad (64)$$

. Alors $(G, +, \cdot)$ est un $\mathbb{Z}/2\mathbb{Z}$ -espace vectoriel, de dimension finie n car G est fini, et le choix d'une base réalise un isomorphisme de $((\mathbb{Z}/2\mathbb{Z})^n, +)$ dans $(G, +)$.

Remarque 5. Par isomorphisme, on a

$$\prod_{x \in G} x = f \left(\sum_{(\bar{\varepsilon}_1, \dots, \bar{\varepsilon}_n) \in (\mathbb{Z}/2\mathbb{Z})^n} (\bar{\varepsilon}_1, \dots, \bar{\varepsilon}_n) \right) \quad (65)$$

Pour $n = 1$, on a $\bar{0} + \bar{1} = \bar{1}$, pour $n = 2$, on a $(\bar{0}, \bar{0}) + (\bar{0}, \bar{1}) + (\bar{1}, \bar{0}) + (\bar{1}, \bar{1}) = (\bar{0}, \bar{0})$.
 Pour $n > 2$, $\bar{1}$ apparaît 2^{n+1} fois sur chaque coordonnée (donc un nombre pair de fois), donc la somme fait $(\bar{0}, \dots, \bar{0})$.

Solution 16.

1. Si G est abélien, on a

$$D(G) = \{e_G\} \quad (66)$$

2. Soit $\sigma \in \mathcal{A}_n$, σ se décompose en un produit d'un nombre pair de transpositions. Soient $[a, b]$ et $[c, d]$ deux transpositions.
 - Si $\{a, b\} = \{c, d\}$, alors $[a, b] \circ [c, d] = id$.
 - Si $a \in \{c, d\}$, supposons par exemple $a = c$ et $b \neq d$. On a alors $[a, b] \circ [c, d] = [a, b] \circ [a, d] = [b, a, d]$.
 - Si $\{a, b\} \cap \{c, d\} = \emptyset$, on a

$$[a, b] \circ [c, d] = [a, b] \circ \underbrace{[b, c] \circ [b, c]}_{=id} \circ [c, d] = [a, b, c] \circ [b, c, d] \quad (67)$$

$$\text{Donc les 3-cycles engendrent } \mathcal{A}_n. \quad (68)$$

3. On a

$$\sigma \circ (a_1, a_2, a_3) \circ \sigma^{-1} = (\sigma(a_1), \sigma(a_2), \sigma(a_3)) \quad (69)$$

On peut trouver $\sigma: \llbracket 1, n \rrbracket \rightarrow \llbracket 1, n \rrbracket$ telle que a_i soit envoyé sur b_i pour $i \in \{1, 2, 3\}$ et les éléments $\llbracket 1, n \rrbracket \setminus \{a_1, a_2, a_3\}$ dans $\llbracket 1, n \rrbracket \setminus \{b_1, b_2, b_3\}$.

$$\text{Donc les 3-cycles sont conjugués dans } \Sigma_n. \quad (70)$$

Si $n \geq 5$ et σ impair, soit $(c_1, c_2) \in \llbracket 1, n \rrbracket \setminus \{a_1, a_2, a_3\}$. $\sigma' = \sigma \circ [c_1, c_2]$ est pair et $\sigma'(a_i) = b_i$.

$$\text{Donc les trois cycles sont conjugués dans } \mathcal{A}_n \text{ pour } n \geq 5. \quad (71)$$

C'est cependant faux pour $n = 3$ et $n = 4$.

4. Soit $(\sigma, \sigma') \in \Sigma_n^2$. En notant \mathcal{E} la signature d'une permutation (morphisme de (Σ_n, \circ) dans $(\{-1, 1\}, \times)$), on a

$$\mathcal{E}(\sigma \circ \sigma^{-1} \circ \sigma' \circ \sigma'^{-1}) = 1 \quad (72)$$

donc $\sigma \circ \sigma^{-1} \circ \sigma' \circ \sigma'^{-1} \in \mathcal{A}_n$. Donc $D(\Sigma_n) \subset \mathcal{A}_n$.

Soit ensuite (a_1, a_2, a_3) un 3-cycle. On a $(a_1, a_3, a_2)^2 = (a_1, a_2, a_3)$ puis $(a_1, a_3, a_2)^{-1} = (a_1, a_2, a_3)$. Ainsi, on a

$$\sigma \circ (a_1, a_3, a_2) \circ \sigma^{-1} \circ (a_1, a_2, a_3) = (a_1, a_3, a_2)^2 = (a_1, a_2, a_3) \quad (73)$$

On pose $\sigma = [a_2, a_3]$, et alors (a_1, a_2, a_3) est un commutateur. Ainsi, $(a_1, a_2, a_3) \in D(\Sigma_n)$ et donc $\mathcal{A}_n \subset D(\Sigma_n)$ (d'après la première question).

Finalement, on a

$$\boxed{D(\Sigma_n) = \mathcal{A}_n} \quad (74)$$

■

Remarque 6. Pour $n \geq 5$, on a $D(\mathcal{A}_n) = \mathcal{A}_n$.

Solution 17.

1. Pour $g \in G$, τ_g est bijective de réciproque $\tau_{g^{-1}}$. On a notamment $\tau_{g \cdot g'} = \tau_g \circ \tau_{g'}$ donc τ est un morphisme. Si $g \in G$ est tel que $\tau_g = id$, pour tout $x \in G$, on a $gx = x$ donc $g = e_G$. Donc τ est un morphisme injectif et G est isomorphe à $\text{Im } \tau = \tau(G)$, sous-groupe de $\Sigma(G)$, lui-même isomorphe à Σ_n .

2. Soit

$$\begin{aligned} f : \Sigma_n &\rightarrow GL_n(\mathbb{C}) \\ \sigma &\mapsto (\delta_{i, \sigma(j)})_{1 \leq i, j \leq n} = P_\sigma \end{aligned} \quad (75)$$

P_σ est la matrice de permutation associée à σ . f est un morphisme, et est injectif, donc

$$\boxed{G \text{ est isomorphe à un sous-groupe de } GL_n(\mathbb{C}).} \quad (76)$$

■

Solution 18. Soit $(x, y, z, t) \in \mathbb{N}^4$ tel que $x^2 + y^2 + z^2 = 8t + 7$. Dans $\mathbb{Z}/8\mathbb{Z}$, on a $\bar{0}^2 = \bar{0}$, $\bar{1}^2 = \bar{1}$, $\bar{2}^2 = \bar{4}$, $\bar{3}^2 = \bar{1}$, $\bar{4}^2 = \bar{0}$, $\bar{5}^2 = \bar{1}$, $\bar{6}^2 = \bar{4}$ et $\bar{7}^2 = \bar{1}$. Donc la somme de 3 de ces classes ne donnent pas $\bar{7}$.

Par récurrence, prouvons la propriété. Soit $(x, y, z, t) \in \mathbb{N}^4$ tel que $x^2 + y^2 + z^2 = (8t + 7)4^{n+1}$. Parmi x, y, z les trois sont pairs ou deux d'entre eux sont impairs. Si x, y impairs et z pair, on écrit $x = 2x' + 1, y = 2y' + 1, z = 2z'$, alors $x^2 + y^2 + z^2 \equiv 2[4]$ mais $(8t + 7)4^{n+1} \equiv 0[4]$: contradiction. Nécessairement, x, y et z sont pairs. En divisant par 4, on se ramène donc à l'hypothèse de récurrence.

$$\boxed{\text{D'où le résultat par récurrence.}} \quad (77)$$

■

Solution 19. On raisonne sur $\mathbb{Z}/7\mathbb{Z}$. On a $\overline{10^{10^n}} = \overline{3^{10^n}}$. Dans le groupe $((\mathbb{Z}/7\mathbb{Z})^*, \times)$, $\bar{3}$ a un ordre qui divise $|\mathbb{Z}/7\mathbb{Z}^*| = 6$. On a $\bar{3}^2 = \bar{2}$, $\bar{3}^3 = \bar{-1}$ et $\bar{3}^6 = \bar{1}$. Donc $\bar{3}^{6k} = \bar{1}$, $\bar{3}^{6k+1} = \bar{3}$, $\bar{3}^{6k+2} = \bar{2}$, $\bar{3}^{6k+3} = \bar{-1}$, $\bar{3}^{6k+4} = \bar{4}$ et $\bar{3}^{6k+5} = \bar{5}$.

On se place maintenant dans $\mathbb{Z}/6\mathbb{Z}$: $\overline{10} = \bar{4}$, $\overline{10^2} = \bar{4}$ et donc par récurrence sur $n \in \mathbb{N}^*$, $\overline{10^n} = \bar{4}$. Donc il existe $k \in \mathbb{Z}$ tel que $10^n = 6k + 4$. Ainsi,

$$\boxed{\overline{10^{10^n}} = \bar{4}} \quad (78)$$

■

Solution 20.

1. On a $F_1 = 5$ et $2 + \prod_{k=0}^0 F_k = 2 + 3 = 5$. Soit $n \geq 1$, supposons que $F_n = 2 + \prod_{k=0}^{n-1} F_k$. Alors

$$F_{n+1} - 2 = 2^{2^{n+1}} - 1 = (2^{2^n})^2 - 1 \quad (79)$$

$$= (2^{2^n} + 1)(2^{2^n} - 1) \quad (80)$$

$$= F_n(F_n - 2) \quad (81)$$

$$= F_n \times \prod_{k=0}^{n-1} F_k \quad (82)$$

$$= \prod_{k=0}^n F_k \quad (83)$$

d'où le résultat par récurrence.

(84)

2. Soit p un facteur premier de F_n . S'il existe $k \in \llbracket 0, n-1 \rrbracket$ tel que $p \mid F_k$, alors d'après la première question on a $p \mid F_n - \prod_{k=0}^{n-1} F_k = 2$. Donc $p = 2$. Or F_n est impair, donc non divisible par deux, ce qui est absurde. Donc p ne divise aucun F_k pour $k \in \llbracket 0, n-1 \rrbracket$. Les F_n étant distincts deux à deux,

il existe donc une infinité de nombres premiers.

(85)

■

Remarque 7. Si $n \neq m$ alors $F_n \wedge F_m = 1$.

Solution 21.

1. On teste uniquement les puissances qui divisent 32 : 2, 4, 8, 16, 32. On a $\bar{5}^2 = \bar{-7}$, $\bar{5}^4 = \bar{-15}$, $\bar{5}^8 = \bar{1}$. Donc

$\omega(\bar{5}) = 8$

(86)

2. On note

$$\begin{aligned} \psi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} &\rightarrow U \\ (\dot{k}, \tilde{l}) &\mapsto \overline{-1}^k \times \bar{5}^l \end{aligned} \quad (87)$$

On a $\omega(\overline{-1}) = 2$ et $\gamma(\bar{5}) = 8$ donc ψ est bien définie. ψ est bien un morphisme de groupes. Soit $(\dot{k}, \tilde{l}) \in \ker(\psi)$, on a $\overline{-1}^k \times \bar{5}^l = \bar{1}$. Si $\dot{k} = \dot{1}$, alors $\overline{-1}^k = \overline{-1} = \bar{5}^{-l} = \bar{5}^l \in \text{gr}\{\bar{5}\}$. Donc $\bar{5}^{2l} = \bar{1}$ et ainsi $8 \mid 2l$ d'où $4 \mid l$. Mais alors $l \in \{0, 4\}$ ce

qui est impossible. Donc $\dot{k} \neq \dot{1}$. De ce fait, $\dot{k} \neq \dot{1}$. Ainsi, $\bar{5}^l = \bar{1}$ donc $\tilde{l} = \tilde{0}$. Ainsi, $\ker(\psi) = \{(\dot{0}, \tilde{0})\}$ donc ψ est injective, puis bijective car $|\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}| = |U|$. Donc

$$U = \text{gr} \{ \overline{-1}, \bar{5} \} \quad (88)$$

■

Remarque 8. U n'est pas cyclique car, par isomorphisme, ses éléments ont un ordre qui divise 8.

Solution 22.

1. Soit

$$\begin{aligned} f : G_n \times G_m &\rightarrow U_{nm} \\ (\xi, \xi') &\mapsto \xi \times \xi' \end{aligned} \quad (89)$$

Soit $(\xi, \xi') \in G_n \times G_m$, Soit $k \in \mathbb{Z}$ tel que $(\xi \times \xi')^k = 1$. Alors $(\xi \times \xi')^{km} = 1$ d'où $\xi^{km} = 1$ donc $n \mid km$ et $n \mid k$ d'après le théorème de Gauss. De même pour n , on a $m \mid k$ et donc $nm \mid k$. La réciproque est immédiate : $\xi \times \xi' \in G_{nm}$. Donc $f(G_n \times G_m) \subset G_{nm}$ et $|G_n \times G_m| = \varphi(n) \times \varphi(m) = \varphi(nm) = |G_{nm}|$ où φ est l'indicatrice d'Euler.

Montrons que f est injective : soit $(x, y, x', y') \in G_n^2 \times G_m^2$ tel que $xx' = yy'$. On a alors $x^m = y^m$ et $x'^n = y'^n$ d'où $(xy^{-1})^m = 1$ d'où $\omega(xy^{-1}) \mid m$ et $\omega(xy^{-1}) \mid n$. Donc $\omega(xy^{-1}) = 1$ donc $x = y$ et en reportant, on a $x' = y'$. Donc f est injective puis bijective (égalité des cardinaux).

On a alors

$$\mu(n)\mu(m) = \sum_{\xi \in G_n} \xi \times \sum_{\xi' \in G_m} \xi' \quad (90)$$

$$= \sum_{(\xi, \xi') \in G_n \times G_m} \xi \xi' \quad (91)$$

$$= \sum_{\xi \in G_{nm}} \xi \quad (92)$$

$$= \boxed{\mu(nm)} \quad (93)$$

2. On a $\mu(1) = 1$. Soit p premier. On a

$$\sum_{k=0}^{p-1} e^{\frac{2ik\pi}{p}} = 0 \quad (94)$$

donc

$$\mu(p) \sum_{k=1}^{p-1} e^{\frac{2ik\pi}{p}} = -1 \quad (95)$$

Soit alors $\alpha \in \mathbb{N}$ avec $\alpha \geq 2$, on a

$$\mu(p^\alpha) = \sum_{\substack{k=1 \\ k \wedge p=1}}^{p^\alpha} e^{\frac{2ik\pi}{p^\alpha}} = \sum_{k=1}^{p^\alpha} e^{\frac{2ik\pi}{p^\alpha}} - \sum_{k=1}^{p^{\alpha-1}} e^{\frac{2ik\pi}{p^{\alpha-1}}} = 0 \quad (96)$$

Si $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, s'il existe $i \in \llbracket 1, r \rrbracket$ tel que $\alpha_i \geq 2$ alors $\mu(n) = 0$. Sinon, on a

$$\mu(n) = \prod_{i=1}^r \mu(p_i) = (-1)^r \quad (97)$$

3. Soit $(f, g) \in (\mathbb{C}^{\mathbb{N}^*})^2$, on a

$$(f \star g)(n) = \sum_{d_1 d_2 = n} f(d_1) g(d_2) \quad (98)$$

$$= \sum_{d_1 d_2 = n} g(d_1) f(d_2) \quad (99)$$

$$= (g \star f)(n) \quad (100)$$

$$\text{Donc } \star \text{ est commutative.} \quad (101)$$

Soit $(f, g, h) \in (\mathbb{C}^{\mathbb{N}^*})^3$, on a

$$(f \star (g \star h))(n) = \sum_{d_1 d = n} f(d_1) (g \star h)(d) \quad (102)$$

$$= \sum_{d_1 d = n} \left[f(d_1) \times \sum_{d_2 d_3 = d} g(d_2) h(d_3) \right] \quad (103)$$

$$= \sum_{d_1 d_2 d_3 = n} f(d_1) g(d_2) h(d_3) \quad (104)$$

$$= ((f \star g) \star h)(n) \quad (105)$$

$$\text{donc } \star \text{ est associative.} \quad (106)$$

On vérifie maintenant que l'élément neutre est $e : \mathbb{N}^* \rightarrow \mathbb{C}$ qui à 1 associe 1 et 0 si $n \geq 2$. Soit

$$\begin{aligned} \psi : \mathbb{N} &\rightarrow \mathbb{Z} \\ n &\mapsto \sum_{d|n} \mu(d) \end{aligned} \quad (107)$$

On a $\psi(1) = 1$. Soit $n \geq 2$ avec $n = \prod_{i=1}^r p_i^{\alpha_i}$. Les diviseurs de n sont dans $D = \{\prod_{i=1}^r p_i^{\beta_i} \mid \beta_i \leq \alpha_i\}$. Ainsi, $\psi(n) = \sum_{d \in D} \mu(d)$. Or $\mu(d)$ vaut 0 s'il existe

$\beta_i \geq 2$ et $(-1)^k$ si k β_i valent 1 et les autres 0. Il y a $\binom{r}{k}$ choix possibles pour que k β_i valent 1. Ainsi,

$$\psi(n) = \sum_{k=0}^r 1^{r-k} (-1)^k \binom{r}{k} = 0 \quad (108)$$

Donc $\mu \star 1 = e$, et $\mu^{-1} = 1 : n \mapsto 1$ pour tout $n \in \mathbb{N}$.

4. On note

$$\begin{aligned} id : \mathbb{N}^* &\rightarrow \mathbb{N}^* \\ n &\mapsto n \end{aligned} \quad (109)$$

Alors

$$\sum_{d|n} d\mu\left(\frac{n}{d}\right) = (\mu \star id)(n) \quad (110)$$

$$= (id \star \mu)(n) \quad (111)$$

$$= (1 \star (\varphi \star \mu))(n) \quad (112)$$

$$= \boxed{\varphi(n)} \quad (113)$$

la troisième égalité venant du fait que $id = 1 \star \varphi$ car $n = \sum_{d|n} \varphi(d)$. ■

Solution 23. Pour $k \in \llbracket 1, p-1 \rrbracket$, on a

$$\binom{p+k}{k} = \frac{(p+k) \times \cdots \times (p+1)}{k \times \cdots \times 1} = 1 + \alpha kp \quad (114)$$

car $(p+k) \times \cdots \times (p+1) = k! + p \times \text{qqch}$. On a $p \mid \binom{p}{k}$ donc

$$\sum_{k=1}^{p-1} \binom{p}{k} \binom{p+k}{k} \equiv \sum_{k=1}^{p-1} \binom{p}{k} [p^2] \quad (115)$$

Pour $k=0$, on a $\binom{p}{0} \binom{p}{0} = 1$ et pour $k=p$, on a $\binom{p}{p} \binom{2p}{p} = \binom{2p}{p}$. Et

$$\sum_{k=1}^{p-1} \binom{p}{k} = \sum_{k=0}^p \binom{p}{k} - 2 = 2^p - 2 \quad (116)$$

Il reste donc à prouver que $\binom{2p}{p} \equiv 2[p^2]$.

Or

$$\binom{2p}{p} = \sum_{k=0}^p \binom{p}{k} \binom{p}{p-k} \equiv 2[p^2] \quad (117)$$

la première égalité venant de l'égalité du terme en X^p dans $(1+X)^{2p} = (1+X)^p(1+X)^p$, et la deuxième venant du fait que seuls les termes en $k=0$ et $k=p$ ne contiennent pas de p^2 , et valent chacun 1.

Finalement, on a

$$\sum_{k=0}^p \binom{p}{k} \binom{p+k}{k} \equiv 2^p - 2 + 1 + 2[p^2] \equiv 2^p + 1[p^2] \quad (118)$$

■

Solution 24.

1. Soit G un sous-groupe de (\mathbb{U}, \times) . On note $|G| = d$. On a donc $G \subset \mathbb{U}_d$ car pour tout $x \in G$, $x^d = 1$.

$$\text{Donc } G = \mathbb{U}_d \text{ est cyclique.} \quad (119)$$

2. On pose

$$\begin{aligned} \psi : SO_2(\mathbb{R}) &\rightarrow (\mathbb{U}, \times) \\ R_\theta &\mapsto e^{i\theta} \end{aligned} \quad (120)$$

qui est un isomorphisme. Donc les sous-groupes de $SO_2(\mathbb{R})$ sont les G_n pour $n \geq 1$ avec

$$G_n = \left\{ R_{\frac{2k\pi}{n}} \mid k \in \llbracket 0, n-1 \rrbracket \right\} \quad (121)$$

3. φ est bilinéaire et symétrique. Pour tout $X \in \mathbb{R}^2$, on $\varphi(X, X) = \sum_{M \in G} \|MX\|^2 \geq 0$ et si $\varphi(X, X) = 0$, on a pour tout $M \in G$, $X = 0$. Notamment, $I_2 \in G$ et donc $X = 0$.

$$\text{Donc } \varphi \text{ est bien un produit scalaire.} \quad (122)$$

Pour tout $(M_0, X, Y) \in G \times (\mathbb{R}^2)^2$, on a $\varphi(M_0X, M_0Y) = \sum_{M \in G} \langle MM_0X, MM_0Y \rangle$ et $M \mapsto MM_0$ est bijective de G dans G donc $\varphi(M_0X, M_0Y) = \varphi(X, Y)$.

Soit \mathcal{B}_0 la base canonique de \mathbb{R}^2 et \mathcal{B}_1 une base orthonormée pour φ . On note $P_0 = \text{mat}_{\mathcal{B}_0 \rightarrow \mathcal{B}_1}$.

Pour tout $M \in G$, $P_0^{-1}MP_0$ est la matrice d'une isométrie pour φ dans une base orthonormée pour φ . Donc $P_0^{-1}MP_0$ est orthogonale, et $\det(P_0^{-1}MP_0) = 1$ car pour tout $M \in G$, $\det(M) = 1$. Ainsi, $\{P_0^{-1}MP_0 \mid M \in G\}$ est un sous-groupe fini de $SO_2(\mathbb{R})$, donc cyclique. Il est isomorphe à G donc

$$G \text{ est cyclique.} \quad (123)$$

■

Solution 25.

1. On a $1 = 1 + 0\sqrt{2} \in E$. On remarque ensuite que pour tout $s = x + y\sqrt{2} \in E$, on a $ss^{-1} = 1$ avec $s^{-1} = x - y\sqrt{2} \in E$. Soit $(s, s') \in E^2$ avec $s = x + y\sqrt{2}$ et $s' = x' + y'\sqrt{2}$. Notons déjà que $x + y\sqrt{2} > 0$ car $x = \sqrt{1 + 2y^2} > |y|\sqrt{2}$. On a donc

$$ss' = \underbrace{xx' + 2yy'}_{\in \mathbb{Z}} + \sqrt{2} \underbrace{(yx' + y'x)}_{\in \mathbb{Z}} \quad (124)$$

On a $xx' \in \mathbb{N}$ et $x > \sqrt{2}|y| \geq 0$ et $x' > \sqrt{2}|y'| \geq 0$ donc $xx' > 2|yy'|$ et ainsi $xx' + 2yy' \in \mathbb{N}^*$. Enfin, on a

$$(xx' + 2yy')^2 - 2(yx' + y'x)^2 = (xx')^2 + 4(yy')^2 - 2(yx')^2 - 2(y'x)^2 \quad (125)$$

$$= (x^2 - 2y^2)(x'^2 - 2y'^2) \quad (126)$$

$$= 1 \quad (127)$$

Donc $ss' \in E$. Finalement,

$E \text{ est un sous-groupe de } (\mathbb{R}_+^*, \times).$

(128)

2. \ln est un isomorphisme de E sur $\ln(E)$, sous-groupe de $(\mathbb{R}, +)$. On sait que si

$$\underbrace{\inf(\ln(E) \cap \mathbb{R}_+)}_{\alpha} > 0 \quad (129)$$

alors $\ln(E) = \alpha\mathbb{Z}$ (sous-groupe de $(\mathbb{R}, +)$ dans le cas $\alpha > 0$, pour rappel si $\alpha = 0$ alors le sous-groupe est dense dans \mathbb{R}). On cherche la borne inférieure de $E \cap]1 + \infty[$ que l'on note β . β existe car cet ensemble est non vide, par exemple $3 + 2\sqrt{2}$ y appartient.

Si $\beta = 1$, on peut trouver une suite de termes de E strictement décroissante convergeant vers 1. Alors pour tout $n \in \mathbb{N}$, on a

$$1 < x_{n+1} + y_{n+1}\sqrt{2} < x_n + y_n\sqrt{2} \quad (130)$$

On sait que

$$x_n - y_n\sqrt{2} = (x_n + y_n\sqrt{2})^{-1} < 1 < x_n + y_n\sqrt{2} \quad (131)$$

donc $-y_n\sqrt{2} < 1 - x_n < 0$ donc $y_n > 0$. Ainsi,

$$y_n = \sqrt{\frac{x_n^2 - 1}{2}} \quad (132)$$

Si $x_{n+1} \geq x_n$, alors $y_{n+1} \geq y_n$ d'où $x_{n+1} + \sqrt{2}y_{n+1} > x_n + \sqrt{2}y_n$ ce qui est absurde. Donc $x_{n+1} < x_n$ et on obtient une suite strictement décroissante d'entiers naturels ce qui est impossible. Donc $\beta > 1$ et

$E = \{(x_0 + y_0\sqrt{2})^n \mid n \in \mathbb{Z}\} \text{ est monogène.}$

(133)

On peut identifier β :

$$x_0 = \min \left\{ x \in \mathbb{N}^* \setminus \{1\}, \exists y \in \mathbb{Z}, x + y\sqrt{2} \in E \cap], +\infty[\right\} \quad (134)$$

Donc $\beta = 3 + 2\sqrt{2}$ Finalement, $x^2 - 2y^2 = 1$ avec $x \in \mathbb{N}, y \in \mathbb{N}$ si et seulement s'il existe $n \in \mathbb{N}$ tel que $x_n + y_n\sqrt{2} = \beta^n$. ■

Remarque 9. En fait, on a

$$\begin{cases} x_n &= \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2k} 2^{2k} 3^{n-2k} \\ y_n &= \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n}{2k+1} 2^{2k+1} 3^{n-2k-1} \end{cases} \quad (135)$$

Solution 26. On a $7 \mid n^n - 3$ si et seulement si $\bar{n}^n = \bar{3}$ dans $\mathbb{Z}/7\mathbb{Z}$. $(\mathbb{Z}/7\mathbb{Z}^*, \times)$ est un groupe de cardinal 6. Donc l'ordre de ses éléments divisent 6, et sont donc 1, 2, 3 ou 6. Notamment, on vérifie que $\omega(\bar{3}) = 6$ et donc le groupe engendré par $\bar{3}$ est exactement $(\mathbb{Z}/7\mathbb{Z}^*, \times)$. Ainsi,

$$(\mathbb{Z}/7\mathbb{Z}^*, \times) = \left\{ \bar{3}^k \mid k \in \llbracket 0, 5 \rrbracket \right\} \quad (136)$$

(c'est un groupe cyclique). Les générateurs sont $\left\{ \bar{3}^k, k \wedge 6 = 1 \right\} = \left\{ \bar{3}, \bar{3}^5 = \overline{-2} = \bar{5} \right\}$. Donc $\bar{n} = \bar{3}$ ou $\bar{n} = \bar{5}$.

Si $\bar{n} = \bar{3}$, $\bar{3}^n = \bar{3}$ si et seulement si $n \equiv 1[6]$ donc $n \equiv 3[7]$ et $n \equiv 1[6]$. D'après le théorème des restes chinois, on vérifie que ceci équivaut à $n \equiv 31[42]$. La réciproque est immédiate.

Si $\bar{n} = \bar{5}$, $\bar{5}^n = \bar{3}$ si et seulement si $n \equiv 5[6]$ et $n \equiv 5[7]$. D'après le théorème des restes chinois, on vérifie que ceci équivaut à $n \equiv 5[42]$.

Donc les solutions sont $n \in \mathbb{N}^*$ tels que $n \equiv 31[42]$ ou $n \equiv 5[42]$.

(137) ■

Solution 27. On a

$$\sum_{k=1}^{p-1} \frac{1}{k} + \frac{1}{p-k} = \frac{2a}{(p-1)!} \iff \sum_{k=1}^{p-1} \frac{p}{k(p-k)} = \frac{2a}{(p-1)!} \quad (138)$$

$$\iff \sum_{k=1}^{p-1} \frac{p(p-1)!}{k(p-k)} = 2a \quad (139)$$

$$\iff \underbrace{p \sum_{k=1}^{p-1} \frac{(p-1)!^3}{k(p-k)}}_{\in \mathbb{N}} = 2a \underbrace{(p-1)!^2}_{p \wedge (p-1)!^2 = 1} \quad (140)$$

donc $p \mid a$ d'après le théorème de Gauss.

On écrit alors $a = p \times b$ avec $b \in \mathbb{N}$. On a alors

$$\sum_{k=1}^{p-1} \frac{1}{k(p-k)} = \frac{2b}{(p-1)!} \quad (141)$$

comme $(p-1)!, k$ et $p-k$ ($1 \leq k \leq p$) sont inversibles dans $\mathbb{Z}/p\mathbb{Z}$, on a alors

$$\sum_{k=1}^{p-1} \overline{-k}^{-2} = \overline{2b} \times \underbrace{\overline{(p-1)!}^{-1}}_{=-1} \quad (142)$$

d'après le théorème de Wilson.

Donc

$$\overline{2b} = \sum_{k=1}^{p-1} \overline{k}^{-2} \quad (143)$$

Comme

$$\begin{aligned} f : \mathbb{Z}/p\mathbb{Z}^* &\rightarrow \mathbb{Z}/p\mathbb{Z}^* \\ \overline{k} &\mapsto \overline{k}^{-1} \end{aligned} \quad (144)$$

est bijective, on a

$$\overline{2} \times \overline{b} = \sum_{k=1}^{p-1} \overline{k}^2 = \overline{\frac{p(p-1)(2p-1)}{6}} \quad (145)$$

Or $p \geq 5$ est premier, donc $p-1$ est pair et p est congru à 1 ou 2 modulo 3. Donc $p-1 \equiv 0[3]$ ou $2p-1 \equiv 0[3]$ donc $\frac{(p-1)(2p-1)}{6} \in \mathbb{N}$. Ainsi,

$$\overline{2} \times \overline{b} = \sum_{k=1}^{p-1} \overline{k}^2 = \overline{p} \times \frac{\overline{(p-1)(2p-1)}}{6} = 0 \quad (146)$$

et donc $p \mid b$ par le théorème de Gauss. Donc

$$\boxed{p^2 \mid a} \quad (147)$$

■

Solution 28. Les racines réelles de P ont une multiplicité paire, le coefficient dominant est positif (car la limite en $+\infty$ est positive) et les racines complexes non réelles sont 2 à 2 conjuguées :

$$(X - \alpha)(X - \overline{\alpha}) = X^2 - 2\Re(\alpha)X + |\alpha|^2 = (X - \Re(\alpha))^2 + |\Im(\alpha)|^2 \quad (148)$$

avec $\Im(\alpha) \neq 0$.

$$\boxed{\text{D'où le résultat en décomposant } P \text{ sur } \mathbb{C}[X].} \quad (149)$$

■

Solution 29.

1. $G = \mathbb{Z} + \alpha\mathbb{Z}$ est un sous-groupe de \mathbb{R} engendré par α et 1. S'il existait $a \in \mathbb{R}_+^*$ tel que $G = a\mathbb{Z}$, alors il existait $(n, m) \in (\mathbb{Z}^*)^2$ tel que $1 = na$ et $\alpha = ma$, d'où $\alpha = \frac{m}{n} \in \mathbb{Q}$ ce qui est absurde. Donc G est dense dans \mathbb{R} .

Le fait que $\mathbb{Z} + \alpha\mathbb{N}$ est dense dans \mathbb{R} est alors immédiate.

(150)

2. Posons $\beta = \frac{\alpha}{2\pi} \notin \mathbb{Q}$. Alors $\mathbb{Z} + \beta\mathbb{N}$ est dense dans \mathbb{R} . Soit $c < d \in \mathbb{R}^2$. Comme $\frac{c}{2\pi} < \frac{d}{2\pi}$, il existe $x \in \mathbb{Z} + \beta\mathbb{N} \cap]\frac{c}{2\pi}, \frac{d}{2\pi}[$ et alors $2\pi x \in 2\pi\mathbb{Z} + \alpha\mathbb{N} \cap]c, d[$. On pose $c = \arcsin(a)$ et $d = \arcsin(b)$ avec $a < b$. On a bien $c < d$ car \arcsin est strictement croissante.

Alors il existe $(m, n) \in \mathbb{Z} \times \mathbb{N}$ tel que $2\pi m + \alpha n = 2\pi x \in]c, d[$ donc $\sin(2\pi x) = \sin(2\pi m + \alpha n) = \sin(\alpha n) \in]a, b[$.

Donc $(\sin(n\alpha))_{n \in \mathbb{N}}$ est dense dans $] -1, 1[$.

(151)

En particulier, cela vaut pour $\alpha = 1$ car $\pi \notin \mathbb{Q}$. Donc $(\sin(n))_{n \in \mathbb{N}}$ est dense dans $[-1, 1]$.

3. Soit $n \in \mathbb{N}$. 2^n commence par 7 en base 10 si et seulement s'il existe $p \in \mathbb{N}$ avec

$$7 \times 10^p \leq 2^n < 8 \times 10^p \iff \ln(7) + p \ln(10) \leq n \ln(2) < \ln(8) + p \ln(10) \quad (152)$$

$$\iff \frac{\ln(7)}{\ln(10)} \leq \frac{n \ln(2)}{\ln(10)} - p < \frac{\ln(8)}{\ln(10)} \quad (153)$$

On a alors

$$p = \left\lfloor \frac{n \ln(2)}{\ln(10)} \right\rfloor \in \mathbb{N} \quad (154)$$

On étudie donc $\mathbb{N} \frac{\ln(2)}{\ln(10)} + \mathbb{Z}$. Supposons que $\frac{\ln(2)}{\ln(10)} = \frac{p}{q} \in \mathbb{Q}$. Alors on a $2^q = 10^p$ mais comme $p \neq 0$, on a $5 \mid 10^p$ mais $5 \nmid 2^q$, donc $\frac{\ln(2)}{\ln(10)} \notin \mathbb{Q}$.

On sait que

$$u_n = n \frac{\ln(2)}{\ln(10)} - \left\lfloor \frac{n \ln(2)}{\ln(10)} \right\rfloor \in \left] \frac{\ln(7)}{\ln(10)}, \frac{\ln(8)}{\ln(10)} \right[\quad (155)$$

Par densité, on peut donc construire par récurrence $(u_{n_p})_{p \in \mathbb{N}}$ telle que

$$\frac{\ln(7)}{\ln(10)} < u_{n_{p+1}} < u_{n_p} < \frac{\ln(8)}{\ln(10)} \quad (156)$$

Donc on a bien une infinité de puissance de 2 commençant par 7 en base 10.

(157)

■

Remarque 10. $(e^{in\alpha})_{n \in \mathbb{N}}$ est de la même façon dense dans \mathbb{U} . On peut montrer qu'elle est équirépartie, c'est à dire que pour tout $a < b \in [0, 2\pi[$, on a

$$\lim_{N \rightarrow +\infty} \left| \left\{ n \in \llbracket 1, N \rrbracket \left| n\alpha - \frac{\lfloor 2\pi n\alpha \rfloor}{2\pi} \in]a, b[\right\} \right| \times \frac{1}{N} = \frac{b-a}{2\pi} \quad (158)$$

Remarque 11. Par équirépartition dans $[0, 1[$ des

$$\left\{ n \frac{\ln(2)}{\ln(10)} - \left\lfloor \frac{n \ln(2)}{\ln(10)} \right\rfloor \mid n \in \mathbb{N} \right\} \quad (159)$$

la probabilité pour qu'une puissance de 2 commence par k en base 10 est ($k \in \llbracket 1, 9 \rrbracket$)

$$\frac{\ln(k+1) - \ln(k)}{\ln(10)} = \frac{\ln(1 + \frac{1}{k})}{\ln(10)} \quad (160)$$

Solution 30.

1. Pour $\alpha = a + ib$, on définit le module au carré : $|\alpha|^2 = a^2 + b^2$. Soit $\beta = c + id \neq 0$. Si $\alpha = \beta q + r$ avec $q, r \in \mathbb{Z}[i]^2$ et $|r|^2 < |\beta|^2$, alors $|\alpha - \beta q|^2 < |\beta|^2$ et $\beta \neq 0$ donc

$$\left| \underbrace{\frac{\alpha}{\beta}}_{\in \mathbb{C}} - \underbrace{q}_{\in \mathbb{Z}[i]} \right| < 1 \quad (161)$$

On pose $\frac{\alpha}{\beta} = x + iy$. On pose

$$u_x = \begin{cases} \lfloor x \rfloor & \text{si } x \in [\lfloor x \rfloor, \lfloor x \rfloor + \frac{1}{2}[\\ \lfloor x \rfloor + 1 & \text{si } x \in [\lfloor x \rfloor + \frac{1}{2}, \lfloor x \rfloor + 1[\end{cases} \quad (162)$$

et de même pour u_y . On a alors $q = u_x + iu_y \in \mathbb{Z}[i]$ et

$$\left| \frac{\alpha}{\beta} - q \right|^2 = |x - u_x|^2 + |y - u_y|^2 \leq 2 \times \left(\frac{1}{2} \right)^2 = \frac{1}{2} < 1 \quad (163)$$

On pose donc $r = \alpha - \beta q \in \mathbb{Z}[i]$ et ainsi

l'anneau $\mathbb{Z}[i]$ est euclidien.

(164)

2. Soit A un anneau euclidien et I un idéal de A non réduit à $\{0\}$. Il existe $x \in I$ tel que

$$v(x_0) = \min\{v(x) \mid x \in I \setminus \{0\}\} \quad (165)$$

On a $x_0A \subset I$. Soit $x \in I$. Il existe $q, r \in A$ tel que

$$x = x_0q + r \quad (166)$$

avec $v(r) < v(x_0)$ ou $r = 0$. Or $r \in I$ donc $r = 0$. Ainsi $x \in x_0A$ et donc $I = x_0A$.

Donc tout anneau euclidien est principal.

(167)

■

Remarque 12. *C'est encore vrai avec $\mathbb{Z}[i\sqrt{2}] = \{a + ib\sqrt{2} \mid (a, b) \in \mathbb{Z}^2\}$.*

Solution 31.

1. Si $\bar{x} = \bar{y}^2$ est un carré, d'après le petit théorème de Fermat, on a $\bar{x}^{\frac{p-1}{2}} = \bar{y}^{p-1} = \bar{1}$. Soit

$$f : \mathbb{Z}/p\mathbb{Z}^* \rightarrow \mathbb{Z}/p\mathbb{Z}^* \\ \bar{y} \mapsto \bar{y}^2 \quad (168)$$

f est un morphisme multiplicatif, $\text{Im}(f)$ est un sous-groupe de $(\mathbb{Z}/p\mathbb{Z}^*, \times)$.

Comme \mathbb{F}_p est un corps, chaque carré possède exactement deux antécédents. Il y a $p - 1$ antécédents, donc il y a $\frac{p-1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}^*$. Donc $|\text{Im}(f)| = \frac{p-1}{2}$ et si \bar{x} est un carré, x est racine de $X^{\frac{p-1}{2}} - \bar{1}$. Le polynôme $X^{\frac{p-1}{2}} - \bar{1}$ possède au plus $\frac{p-1}{2}$ racines et tout carré est racine. Donc les racines sont exactement les carrés et

$\bar{x}^{\frac{p-1}{2}} = \bar{1}$ si et seulement si \bar{x} est un carré.

(169)

2. On a $p \equiv 1[4]$ si et seulement si $\frac{p-1}{2}$ est pair si et seulement si $(-1)^{\frac{p-1}{2}} = \bar{1}$ si et seulement si $\bar{-1}$ est un carré dans \mathbb{F}_p . Supposons qu'il y ait un nombre fini de nombres premiers p_1, \dots, p_r tous congrus à 1 modulo 4. On pose $n = (p_1 \times \dots \times p_r)^2 + 1$. Soit p un facteur premier de n , on a $n \equiv 1[n_i]$ donc $p \notin \{p_1, \dots, p_r\}$. Dans $\mathbb{Z}/p\mathbb{Z}$, on a $\bar{n} = \bar{0}$ donc $\bar{-1} = \overline{p_1 \times \dots \times p_r}^2$ donc $p \equiv 1[4]$ ce qui est une contradiction.

Donc il y a une infinité de nombres premiers congrus à 1 modulo 4.

(170)

■

Solution 32.

1. On pose $P_1 = \sum_{i=0}^n r'_i X^i$, et $\nu_p(r'_i)$ est positif par définition de $c(P)$. Donc

$P_1 \in \mathbb{Z}[X]$

(171)

Pour tout $p \in \mathcal{P}$, il existe $i_0 \in \llbracket 1, n \rrbracket$ tel que

$$\min_{i \in \llbracket 1, n \rrbracket} \nu_p(r_i) = \nu_p(r_{i_0}) \quad (172)$$

et $\nu_p(r'_{i_0}) = 0$ donc $p \nmid r'_{i_0}$ donc

$$\bigwedge_{i=1}^n r'_i = 1 \quad (173)$$

Si on a $P = \alpha_1 P_1 = \alpha_2 P_2$ avec les conditions requises, soit $p \in \mathcal{P}$, si $\nu_p(\alpha_2) > \nu_p(\alpha_1)$, alors p divise tous les coefficients de P_1 ce qui n'est pas possible, donc $\nu_p(\alpha_2) = \nu_p(\alpha_1)$. Ceci étant vrai pour tout $p \in \mathcal{P}$, on a aussi $\alpha_1 = \alpha_2$ et donc $P_1 = P_2$.

Donc l'écriture est unique.

(174)

2. On a $P = c(P)P_1$ et $Q = c(Q)Q_1$ donc $PQ = c(P)c(Q)P_1Q_1$ et $P_1Q_1 \in \mathbb{Z}[X]$.
 Soit $p \in \mathcal{P}$ divisant tous les coefficients de P_1Q_1 . On définit, si $R = \sum_{i \in \mathbb{N}} \gamma_i X^i \in \mathbb{Z}[X]$, $\bar{R} = \sum_{i \in \mathbb{N}} \overline{\gamma_i} X^i \in \mathbb{Z}/p\mathbb{Z}[X]$. $R \mapsto \bar{R}$ est un morphisme d'anneaux. Par hypothèse, on a $\overline{P_1Q_1} = \bar{0} = \overline{P_1Q_1}$ et par intégrité de $\mathbb{Z}/p\mathbb{Z}[X]$, on a $\bar{P_1} = \bar{0}$ ou bien $\bar{Q_1} = \bar{0}$, ce qui est exclu par les hypothèses. Donc

$c(PQ) = c(P)c(Q)$

(175)

3. Soit alors P irréductible dans $\mathbb{Z}[X]$ (les inversibles de $\mathbb{Z}[X]$ étant -1 et 1). Posons

$$P = QR \in \mathbb{Q}[X]^2 \quad (176)$$

$$= c(Q)c(R) \underbrace{Q_1 R_1}_{\in \mathbb{Z}[X]} \quad (177)$$

Or $c(Q)c(R) = c(P)$ d'après le lemme de Gauss et nécessairement, $c(P) = 1$. Donc $P = Q_1 R_1$, et alors $Q_1 = \pm 1$ et $R_1 = \pm 1$, et Q ou R est constant,

donc P est irréductible sur $\mathbb{Q}[X]$.

(178)

Pour la réciproque, on a $2X$ est irréductible sur $\mathbb{Q}[X]$ car de degré 1, mais pas sur $\mathbb{Z}[X]$ car ni 2 ni X ne sont inversibles.

4. Soit $\theta = \frac{2\pi p}{q}$ avec $p \wedge q = 1$ et $\cos(\theta) \in \mathbb{Q}$. Sur $\mathbb{C}[X]$, on a $P = (X - e^{i\theta})(X - e^{-i\theta}) = X^2 - 2\cos(\theta)X + 1 \in \mathbb{Q}[X]$.

Et $e^{i\theta} \neq e^{-i\theta}$ car $\theta \not\equiv 0[\pi]$. On a $\theta = \frac{2\pi p}{q}$ donc $e^{i\theta} \in \mathbb{U}_q$, et $e^{i\theta}$ et $e^{-i\theta}$ sont des racines de A . Donc, dans $\mathbb{C}[X]$, on a $P \mid A$ et $A \in \mathbb{Q}[X]$, donc il existe $B \in \mathbb{Q}[X]$ tel que

$$\underbrace{A}_{\in \mathbb{Q}[X]} = \underbrace{B}_{\in \mathbb{C}[X]} \times \underbrace{P}_{\in \mathbb{Q}[X]} \quad (179)$$

Or B s'obtient par la division euclidienne de A par P , qui est indépendante du corps de référence, il vient $B \in \mathbb{Q}[X]$ et donc $A \mid P$ dans $\mathbb{Q}[X]$.

On a $c(A) = 1 = c(B)c(P)$ et $A = c(B)c(P)B_1P_1 = B_1P_1 \in \mathbb{Z}[X]$ et le coefficient dominant de A est donc 1. Donc le coefficient dominant de B_1 et de P_1 est aussi 1. En reportant, on a $P = P_1 \in \mathbb{Z}[X]$.

Donc $2\cos(\theta) \in \mathbb{Z} \cap [-2, 2]$ donc $\cos\{\theta\} \in \{-\frac{1}{2}, \frac{1}{2}, 0\}$ (-1 et 1 ne peuvent y être car on a supposé $\theta \not\equiv 0[\pi]$). Les solutions sont donc

$$\theta \in \left\{0, \frac{\pi}{3}, \frac{\pi}{2}, \frac{2\pi}{3}, \pi, \frac{4\pi}{3}, \frac{3\pi}{2}, \frac{5\pi}{3}\right\} \quad (180)$$

(en rajoutant $\theta = 0$ et π).

■

Remarque 13. On a $\frac{\arccos(\frac{1}{3})}{\pi} \notin \mathbb{Q}$ car $\cos(\theta) = \frac{1}{3}$ n'est pas dans l'ensemble solutions.

Solution 33.

1. Soit $P = a \prod_{i=1}^s (X - a_i)^{\alpha_i}$ avec les a_i distincts et $\alpha_i \geq 1$. a_i est racine de P' de multiplicité $\alpha_i - 1$. Il manque donc s racines. Si $\alpha = 0$, le résultat est évident, sinon on pose

$$\begin{aligned} f : \mathbb{R} &\rightarrow \mathbb{R} \\ x &\mapsto P(x)e^{\frac{x}{\alpha}} \end{aligned} \quad (181)$$

et on a pour tout $x \in \mathbb{R}$,

$$f'(x) = \frac{e^{\frac{x}{\alpha}}}{\alpha} (P(x) + \alpha P'(x)) \quad (182)$$

Comme P est scindé sur \mathbb{R} , P' est scindé sur \mathbb{R} (appliquer le théorème de Rolle entre les racines distinctes de P), donc f' s'annule $s - 1$ fois entre les racines de P donc

$$P + \alpha P' \text{ aussi.} \quad (183)$$

La dernière racine est réelle car sinon, le conjugué de la racine complexe supposée serait aussi racine.

2. On pose $R = \mu \prod_{i=0}^r (X - \beta_i)$. On pose

$$\begin{aligned} \Delta : \mathbb{R}[X] &\rightarrow \mathbb{R}[X] \\ P &\mapsto P' \end{aligned} \quad (184)$$

On a alors

$$\sum_{i=0}^r a_i P^{(i)} = \sum_{i=0}^r a_i \Delta^i(P) = R(\Delta)(P) = \mu \prod_{i=0}^r (\Delta - \beta_i \text{id})(P) \quad (185)$$

Par récurrence sur r , on montre que

$$\prod_{i=0}^r (\Delta - \beta_i id)(P) \text{ est scindé} \quad (186)$$

d'après la première question. ■

Remarque 14. On a aussi pour tout $\lambda \in \mathbb{R}$, $P' + \lambda P$ est aussi scindé sur \mathbb{R} si P est scindé sur \mathbb{R} .

Solution 34. Soit $F = \frac{P'}{P}$ définie sur $\mathbb{R} \setminus \{a_1, \dots, a_n\}$ où a_i sont les racines de P . On note α le coefficient dominant de P , et on a

$$P' = \alpha \sum_{i=1}^n \left(\prod_{\substack{j=1 \\ j \neq i}}^n (X - a_j) \right) \quad (187)$$

On a donc $F = \sum_{i=1}^n \frac{1}{X - a_i}$ et on a

$$F' = - \sum_{i=1}^n \frac{1}{(X - a_i)^2} = \frac{P''P - P'P'}{P^2} \quad (188)$$

Pour $x \notin \{a_1, \dots, a_n\}$, on a

$$(n-1)(P'^2(x))(x) \geq nP(x)P''(x) \iff n(P''(x)P(x) - P'^2(x)) \leq -P'^2(x) \quad (189)$$

$$\iff \frac{P'^2(x)}{P^2(x)} \leq n(P''(x)P(x) - P'^2(x)) \times \frac{1}{P^2(x)} \quad (190)$$

$$\iff F^2(x) \leq n(-F'(x)) \quad (191)$$

$$\iff \left(\sum_{i=1}^n \frac{1}{(X - a_i)} \right)^2 \leq n \times \sum_{i=1}^n \frac{1}{(X - a_i)^2} \quad (192)$$

qui est l'inégalité de Cauchy-Schwarz dans \mathbb{R}^2 avec $(1 \dots 1)$ et $(\frac{1}{x-a_1} \dots \frac{1}{x-a_n})$. ■

Remarque 15. Si $P = \alpha(X - a_1)^{m_1}(X - a_r)^{m_r}$, alors

$$\frac{P'}{P} = \sum_{i=1}^r \frac{m_i}{X - a_i} \quad (193)$$

Solution 35.

1. $P' \in \mathbb{C}[X]$ et $\deg(P') = \deg(P) - 1$. On a $P \wedge P' = 1$ car P est irréductible sur $\mathbb{Q}[X]$. Comme le pgcd est obtenu par l'algorithme d'Euclide qui est indépendant du corps de référence, on a $P \wedge P' = 1$ sur $\mathbb{C}[X]$ donc

$$\boxed{P \text{ n'a que des racines simples sur } \mathbb{C}.} \quad (194)$$

2. Notons $P \in \mathbb{Q}[X]$ le polynôme minimal de α sur \mathbb{Q} (défini car $A(\alpha) = 0$ donc α est algébrique). Comme $A(\alpha) = 0$, on a $P \mid A$ et P est irréductible sur $\mathbb{Q}[X]$. Si $\alpha \notin \mathbb{Q}$, on a $\deg(P) \geq 2$, on peut donc décomposer sur $\mathbb{Q}[X]$:

$$A = P^r \times P_1^{r_1} \times \dots \times P_s^{r_s} \quad (195)$$

avec les P_i irréductibles sur $\mathbb{Q}[X]$ non associés.

α n'est pas racine d'un P_i car sinon $P \mid P_i$ ce qui est impossible. α est racine simple de P donc $m(\alpha) = r > \frac{\deg(A)}{2}$. Par ailleurs, $\deg(P)^r \geq 2r > \deg(A)$ ce qui est impossible.

Donc

$$\alpha \in \mathbb{Q} \quad (196)$$

■

Solution 36. Soit $x \in A$. Il existe $(n, m) \in \mathbb{N}^2$ avec $n < m$ tel que $x^n = x^m$. Alors $x^{m-n} = e_G \in A$.

$$\begin{aligned} f : \mathbb{N}^* &\rightarrow A \\ n &\mapsto x^n \end{aligned} \quad (197)$$

n'est pas injective, car \mathbb{N}^* est infini et A est fini. Or $m - n \in \mathbb{N}^*$ donc

$$x^{m-n} = e_G \Rightarrow x = x \cdot x^{m-n-1} = e_G \quad (198)$$

donc $x^{-1} = x^{m-n-1} \in A$ et ainsi

$$\boxed{A \text{ est un sous-groupe.}} \quad (199)$$

■

Solution 37. Pour $\alpha = 0$, on a $1 + p \equiv 1 + p[p^2]$. Pour $\alpha = 1$, on a

$$(1 + p)^p = \sum_{k=0}^p \binom{p}{k} p^k = 1 + p^2 + \binom{p}{2} p^2 \sum_{k=3}^p \binom{p}{k} p^k \quad (200)$$

Or $\binom{p}{2} p^2 = \frac{p(p-1)p^2}{2} \equiv 0[p^3]$ car p est premier plus grand que trois donc impair, et la somme est aussi congrue à 0 modulo p^3 .

Soit $\alpha \geq 1$, supposons que l'on ait

$$(1+p)^p \equiv 1 + p^{\alpha+1}[p^{\alpha+2}] \quad (201)$$

Il existe $l \in \mathbb{N}$ tel que

$$(1+p)^{p^\alpha} = 1 + p^{\alpha+1} + lp^{\alpha+2} \quad (202)$$

Alors

$$(1+p)^{p^{\alpha+1}} = (1 + \underbrace{p^{\alpha+1} + lp^{\alpha+2}}_x)^p \quad (203)$$

Or

$$(1+x)^p = \sum_{k=0}^p \binom{p}{k} x^k = 1 + px + \sum_{k=2}^p \binom{p}{k} x^k = 1 + p^{\alpha+2} + lp^{\alpha+3} + \underbrace{\sum_{k=2}^p \binom{p}{k} x^k}_{\text{divisible par } x^2} \quad (204)$$

Comme $p^{\alpha+1} \mid x$, $p^{2\alpha+2} \mid x^2$ avec $2\alpha+2 \geq \alpha+3$ ($\alpha \geq 1$). D'où

$$p^{\alpha+3} \mid x^2 \mid \sum_{k=2}^p \binom{p}{k} x^k \quad (205)$$

et donc

$$(1+p)^{p^{\alpha+1}} \equiv 1 + p^{\alpha+2}[p^{\alpha+3}] \quad (206)$$

■

Remarque 16. Pour $p=2, \alpha=1$, on a $3^2 = 9 \not\equiv 5[8]$.

Solution 38. Si $7 = 2x^2 - 5y^2$, on a $\bar{0} = 2\bar{x}^2 - 5\bar{y}^2 = \bar{2}(\bar{x}^2 + \bar{y}^2)$ dans $\mathbb{Z}/7\mathbb{Z}$. Comme 2 et 7 sont premiers entre eux donc $\bar{2}$ est inversible. Donc $\bar{x}^2 + \bar{y}^2 = \bar{0}$. La seule possibilité est $\bar{x} = \bar{0}$ et $\bar{y} = \bar{0}$. Donc $7 \mid x$ et $7 \mid y$. Si $x = 7k$ alors $x^2 = 49k^2$ donc $49 \mid x^2$ et $49 \mid y^2$ donc $49 \mid 2x^2 - 5y^2 = 7$ ce qui est faux.

Ainsi, pour tout $(x, y) \in \mathbb{Z}^2$,

$$7 \neq 2x^2 - 5y^2 \quad (207)$$

■

Solution 39. \mathbb{F}_{19} est un corps car 19 est premier. On a donc $\bar{x}^3 = \bar{1}$ si et seulement si $(x - \bar{1})(x^2 + x - \bar{1}) = \bar{0}$. On a donc $x = \bar{1}$ ou $x^2 + x - \bar{1} = \bar{0}$. On a

$$x^2 + x - \bar{1} = (x + \bar{2}^{-1})^2 + \bar{3} \times \bar{4}^{-1} = (x + \bar{10})^2 + \bar{3} \times \bar{50} \quad (208)$$

Donc $(x + \bar{10})^2 = \bar{4}$ d'où

$$x = \bar{-8} = \bar{11} \text{ ou } x = \bar{-12} = \bar{7}. \quad (209)$$

■

Solution 40.

1. m est inversible si et seulement si $m \wedge 2^n = 1$ si et seulement si $m \wedge 2 = 1$ si et seulement si m est impair.

$$\boxed{\text{Il y a donc } 2^{n-1} \text{ inversibles.}} \quad (210)$$

2. On a $5^{2^{3-3}} = 5 \equiv 1 + 2^2[2^3]$. Par récurrence, soit $n \geq 3$. Il existe $k \in \mathbb{Z}$ avec $5^{2^{n-3}} = 1 + 2^{n-1} + k2^n$ donc

$$\boxed{5^{2^{n-1}} = 1 + 2^n + k2^{n+1} + 2^{2n-2}(1 + 2k)^2 \equiv 1 + 2^n[2^{n+1}]} \quad (211)$$

car $2n - 2 \geq n + 1$ ($n \geq 3$).

3. On a $5^{2^{n-2}} \equiv 1 + 2^n[2^{n+1}] \equiv 1[2^n]$ et $5^{2^{n-3}} \not\equiv 1[2^n]$.

$$\boxed{\text{Donc l'ordre de } \bar{5} \text{ est } 2^{n-2}.} \quad (212)$$

4. $\text{gr } \{\bar{-1}\} = \{\bar{-1}, \bar{1}\}$. $\bar{5}$ n'engendre pas $\bar{-1}$ car si $\bar{5}^k = \bar{-1}$, on a $\bar{5}^{2k} = \bar{1}$ d'où $2^{n-2} \mid 2k$ donc $2^{n-3} \mid k$. Ainsi, $k \in \{2^{n-3}, 2^{n-2}, 2^{n-1}\}$. Mais $\bar{5}^{2^{n-2}} = \bar{1}$, $\bar{5}^{2^{n-3}} = \bar{1} + 2^{n-1} \neq \bar{-1}$ donc un tel k n'existe pas.

Posons

$$\begin{aligned} \varphi : (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}, +) &\rightarrow (\mathbb{Z}/2^n\mathbb{Z}^\times, \times) \\ (\tilde{a}, \tilde{b}) &\mapsto \bar{-1}^{\tilde{a}} \bar{5}^{\tilde{b}} \end{aligned} \quad (213)$$

Elle est bien définie car $\omega(\bar{-1}) = 2$ et $\omega(\bar{5}) = 2^{n-2}$. C'est évidemment un morphisme, on a égalité des cardinaux des ensembles de départ et d'arrivée, et on vérifie qu'elle est injective, et donc

$$\boxed{\text{c'est un isomorphisme.}} \quad (214)$$

■

Solution 41. Soit $(x, x') \in G^2$ tel que $x \cdot x' = e$. Alors

$$e \cdot x = x \cdot x' \cdot x = x \cdot e \cdot x' \cdot x \quad (215)$$

si et seulement si

$$e \cdot x \cdot x' = e = x \cdot e \cdot x' \cdot x \cdot x' = x \cdot e \cdot x' \quad (216)$$

Soit $(x, x', x'') \in G^3$ tel que $x \cdot x' = e$ et $x' \cdot x'' = e$. On a alors

$$x \cdot x' \cdot x'' = x \cdot e = x = e \cdot x'' \quad (217)$$

Donc $x = e \cdot x''$ et $e = e \cdot x'' \cdot x'$. Si on prouve que $e \cdot x'' = x''$, alors $x = x''$ et $x' \cdot x = e$.

Montrons donc que pour tout $x \in G$, $e \cdot x = x$. Notons que s'il existe $e' \in G$ tel que pour tout $x \in G$, $e' \cdot x = x$, alors $e' \cdot e = e' = e$. Il vient donc

$$x' \cdot x = x' \cdot e \cdot x'' = x' \cdot x'' = e \quad (218)$$

Donc pour tout $x \in G$, l'élément x' est inverse à droite et à gauche : $x \cdot x' = e$.

Donc

$$x \cdot x' \cdot x = e \cdot x = x \cdot x' \cdot x = x \cdot e = x \quad (219)$$

Et donc e est neutre à gauche. Finalement,

(G, \cdot) est un groupe.

(220)

■

Remarque 17. Si $f: \mathbb{R} \rightarrow \mathbb{R}$ est surjective, on peut définir

$$\begin{aligned} g: \mathbb{R} &\rightarrow \mathbb{R} \\ y &\mapsto f(x) \end{aligned} \quad (221)$$

pour un certain $x \in \mathbb{R}$. On a $f \circ g = \text{id}$. Si f n'est pas injective : s'il existait $h: \mathbb{R} \rightarrow \mathbb{R}$ telle que $h \circ f = \text{id}$, soit $(x, x') \in \mathbb{R}^2$ telle que $f(x) = f(x')$. En composant par h , on aurait $x = x'$ donc f serait injective ce qui n'est pas.

On peut donc avoir un inverse à droite mais pas à gauche.

Solution 42. Soit $n \in \mathbb{N}^*$.

$$\underbrace{1 \dots 1}_{n \text{ fois en base } 10} = 1 + 10 + \dots + 10^{n-1} = \frac{10^n - 1}{9} \quad (222)$$

On a

$$21 \mid \frac{10^n - 1}{9} \iff 3 \mid \frac{10^n - 1}{9} \text{ et } 7 \mid \frac{10^n - 1}{9} \quad (223)$$

$$\iff 27 \mid 10^n - 1 \text{ et } 7 \mid 10^n - 1 \quad (224)$$

car $7 \wedge 9 = 1$. Dans $\mathbb{Z}/7\mathbb{Z}$, on a $\overline{10} = \overline{3}$ donc pour tout $k \in \mathbb{N}$, $\overline{10}^{6k} = \overline{1}$ d'après le petit théorème de Fermat. Dans $\mathbb{Z}/27\mathbb{Z}$, $\tilde{10}$ est inversible car $10 \wedge 27 = 1$. $((\mathbb{Z}/27\mathbb{Z})^\times, +, \times)$ comporte 18 éléments donc pour tout $k' \in \mathbb{N}$, on a $\tilde{10}^{18k'} = \tilde{1}$.

Lorsque $81 \mid n$, on a $21 \mid 1 \dots 1$.

Cherchons plus précisément les ordres de $\overline{10}$ dans le groupe $((\mathbb{Z}/7\mathbb{Z})^*, \times)$ et de $\tilde{10}$ dans $((\mathbb{Z}/27\mathbb{Z})^\times, \times)$. Dans $(\mathbb{Z}/7\mathbb{Z})^*$, groupe de cardinal 6, on vérifie que l'ordre de 10 est 6. Dans l'autre groupe, on vérifie que l'ordre de $\tilde{10}$ est 3. Ainsi, $21 \mid 1 \dots 1$ si et seulement si $6 \mid n$. Il y a donc une infinité de multiples de 21 qui s'écrivent avec uniquement des 1 en base 10. ■

Remarque 18. Il suffit de trouver l'ordre de 10 dans les deux ensembles et de prendre le ppcm.

Solution 43.

1. $X^d - 1$ a au plus d racines dans \mathbb{K} . Pour tout $k \in \llbracket 0, d-1 \rrbracket$, x_0^k est racine de $X^d - 1_{\mathbb{K}}$ car $\text{gr}\{x_0\}$ a pour cardinal d . Donc les racines sont exactement les puissances de x_0 .

Soit $x \in \mathbb{K}^*$ d'ordre d . On a $x \in \text{gr}\{x_0\}$ car $x^d = 1$ (racine du polynôme de $X^d - 1_{\mathbb{K}}$). Or, dans le groupe cyclique engendré par x_0 ,

$$\boxed{\text{il y a } \varphi(d) \text{ éléments.}} \quad (225)$$

2. On a ou bien $\varphi(d)$ ou bien aucun élément d'ordre d dans \mathbb{K} . Soit d tel que $d \mid n$, on note $H_d = \{x \in K \mid \omega(x) = d\}$. On a

$$\mathbb{K}^* = \bigcup_{d \mid n} H_d \quad (226)$$

Alors

$$n = \sum_{d \mid n} |H_d| \leq \sum_{d \mid n} \varphi(d) = n \quad (227)$$

Alors pour tout d tel que $d \mid n$, on a $|H_d| = \varphi(d)$. En particulier, on a $|H_n| = \varphi(n) \geq 1$ donc H_n est non vide. Donc il existe (au moins) un élément d'ordre n , donc

$$\boxed{(\mathbb{K}^*, \times) \text{ est cyclique.}} \quad (228)$$

■

Solution 44.

1. Soit $x \in M$. On a $\bar{1} - \bar{x}^{-1}$ si et seulement si $\bar{x} = \bar{1}$ et $\bar{1} - \bar{x}^{-1} = \bar{1}$ si et seulement si $\bar{x} = \bar{0}$, ce qui n'est pas possible pour les deux cas.

$$\boxed{\text{Donc } f \text{ est bien définie.}} \quad (229)$$

Soit $x \in M$, on a

$$f^2(x) = f(\bar{1} - \bar{x}^{-1}) \quad (230)$$

$$= \bar{1} - (\bar{1} - \bar{x}^{-1})^{-1} \quad (231)$$

$$= (\bar{1} - \bar{x}^{-1})^{-1}(\bar{1} - \bar{x}^{-1} - \bar{1}) \quad (232)$$

$$= -\bar{x}^{-1}(\bar{1} - \bar{x}^{-1})^{-1} \quad (233)$$

Donc

$$f^3(x) = \bar{1} - (\bar{1} - (\bar{1} - \bar{x}^{-1})^{-1})^{-1} \quad (234)$$

$$= \bar{1} - (-x\bar{x}^{-1}(\bar{1} - \bar{x}^{-1})^{-1})^{-1} \quad (235)$$

$$= \bar{1} + \bar{x}(\bar{1} - \bar{x}^{-1}) \quad (236)$$

$$= \bar{1} + \bar{x} - \bar{1} \quad (237)$$

$$= \bar{x} \quad (238)$$

Donc

$$f^3 = id_M \quad (239)$$

2. Soit $x \in M$, on a

$$f(x) = x \iff \bar{1} - \bar{x}^{-1} = x \quad (240)$$

$$\iff \bar{x}^2 - \bar{x} + \bar{1} = \bar{0} \quad (241)$$

$$\iff (\bar{x} - \bar{2}^{-1})^2 + \bar{3} \times \bar{4}^{-1} = \bar{0} \quad (242)$$

$$\iff \bar{-3} = (\bar{2}\bar{x} - \bar{1})^2 \quad (243)$$

f admet un point fixe si et seulement $\bar{-3}$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$ car $\bar{y} = \bar{2}\bar{x} - \bar{1}$ si et seulement si $\bar{x} = \bar{2}^{-1}(\bar{y} + \bar{1})$.

Donc

$\bar{-3} \text{ est un carré dans } \mathbb{Z}/p\mathbb{Z} \text{ si et seulement si } f \text{ admet un point fixe.}$

(244)

3. Comme p est premier plus grand que 5, on a $p \equiv 1$ ou $2[3]$ donc $p - 2 \equiv 0$ ou $2[3]$ car $f^3 = id_M$, les longueurs des cycles qui composent f valent 1 ou 3.

Si f n'a pas de point fixe, tous les cycles sont de longueur 3, donc $3 \mid p - 2$ donc $p \equiv 2[3]$. Si $p \equiv 2[3]$, alors $3 \mid p - 2$, le nombre de points fixes est un multiple de 3 donc aussi du nombre de racine carrés de $\bar{-3}$. Et puisque l'on est dans un corps, il y a au plus 2 racines de $\bar{-3}$. Donc si $p \equiv 2[3]$, il n'y a pas de point fixe.

Donc

$\bar{-3} \text{ est un carré dans } \mathbb{Z}/p\mathbb{Z} \text{ si et seulement si } p \equiv 1[3].$

(245)

■

Solution 45. Soit $x \in \mathbb{R}$. Supposons que x possède un développement décimal périodique. Alors il existe $(n_0, T) \in \mathbb{N} \times \mathbb{N}^*$ tels que pour tout $n \geq n_0$, $a_{n+T} = a_n$. On a alors

$$|x| = \underbrace{b_m \dots b_0, a_0 \dots a_{n_0-1}}_{\in \mathbb{Q}} + \frac{1}{10^{n_0-1}} \underbrace{(0, a_{n_0} \dots a_{n_0+T-1} a_{n_0} \dots)}_{=y} \quad (246)$$

$$10^T y - y = a_{n_0} \dots a_{n_0+T-1} \in \mathbb{N} \quad (247)$$

et donc

$$y = \frac{a_{n_0} \cdots a_{n_0+T-1}}{10^T - 1} \in \mathbb{Q} \quad (248)$$

Donc $x \in \mathbb{Q}$.

Réciproquement, soit $x = \frac{p}{q} \in \mathbb{Q}$ avec $q \in \mathbb{N}^*$. Il existe $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $p = aq + b$ avec $b \in \llbracket 0, q-1 \rrbracket$. Si $b = 0$, on arrête. On a sinon

$$x = a + \frac{1}{10^k} \frac{10^k b}{q} \quad (249)$$

où $k = \min\{m \geq 1 \mid 10^m b > q\}$. On réitère l'algorithme avec $\frac{10^k b}{q}$ car on a $\left\lfloor \frac{10^k b}{q} \right\rfloor \in \llbracket 1, 9 \rrbracket$ par définition de k .

Il y a q restes possibles dans la division euclidienne par q . Ainsi, au bout d'au plus de $q + 1$ itérations, on retrouve un reste précédent. Par unicité de la division euclidienne, on obtient un développement décimal périodique.

Donc

$x \in \mathbb{Q} \text{ si et seulement si } \exists n_0 \in \mathbb{N}, \exists T \in \mathbb{N}^*, \forall n \geq n_0, a_{n+T} = a_n.$

(250)

■

Remarque 19. On peut écrire $q = 2^a 5^b q'$ avec $q' \wedge 2 = q' \wedge 5 = 1$. On se ramène alors à $q \wedge 2 = q \wedge 5 = 1$. En reportant dans l'écriture décimale de x , on a

$$\frac{\alpha}{q} = \frac{\beta}{10^T - 1} \quad (251)$$

avec $\alpha \wedge q = 1$. On a donc $q \mid 10^T - 1$ d'après le lemme de Gauss. T revient donc à l'ordre de $\overline{10}$ dans $((\mathbb{Z}/q\mathbb{Z})^\times, \times)$ qui contient $\varphi(q)$ éléments. Par défaut, on a donc $T = \varphi(q)$.

Solution 46.

1. Soit $m \in \mathbb{Z}$. Si $m \in \llbracket 0, n-1 \rrbracket$, on a $H_n(m) = 0 \in \mathbb{Z}$. Si $m \geq n$, on a $H_n(m) = \binom{m}{n} \in \mathbb{Z}$. Si $m < 0$, on a

$$H_n(m) = \frac{m(m-1) \cdots (m-n+1)}{n!} = (-1)^n \binom{-m+n-1}{-m-1} \in \mathbb{Z} \quad (252)$$

Donc

$H_n(\mathbb{Z}) \subset \mathbb{Z}$

(253)

2. Supposons qu'il existe $n \in \mathbb{N}$ et $(a_0, \dots, a_n) \in \mathbb{Z}^{n+1}$ et $P = \sum_{k=0}^n a_k H_k$. On a $H_k(\mathbb{Z}) \subset \mathbb{Z}$ donc $P(\mathbb{Z}) \subset \mathbb{Z}$. Supposons $P(\mathbb{Z}) \subset \mathbb{Z}$. $(H_k)_{k \in \mathbb{N}}$ est une base étagée en degré de $\mathbb{C}[X]$. Donc il existe $(a_0, \dots, a_n) \in \mathbb{C}^{n+1}$ tel que $P = \sum_{k=0}^n a_k H_k$. Par

réurrence, on a $P(0) = a_0 \in \mathbb{Z}$. Soit $k \in \llbracket 0, n-1 \rrbracket$, supposons $(a_0, \dots, a_k) \in \mathbb{Z}^{k+1}$. On a alors

$$P(k+1) = \underbrace{\sum_{i=0}^k \underbrace{a_i}_{\in \mathbb{Z}} H_i + a_{k+1}}_{\in \mathbb{Z}} \underbrace{H_{k+1}(k+1)}_{=1} \quad (254)$$

Donc $a_{k+1} \in \mathbb{Z}$.

Donc

$$P(\mathbb{Z}) \subset \mathbb{Z} \text{ si et seulement si } \exists n \in \mathbb{N}, \exists (a_0, \dots, a_n) \in \mathbb{Z}^{n+1}, P = \sum_{k=0}^n a_k H_k.$$

(255)

■

Remarque 20. Les translation $X + \alpha$ sont les seules pour lesquelles on a $(X + \alpha)(\mathbb{Z}) = \mathbb{Z}$. En effet, si $P \in \mathbb{C}[X]$ est tel que $P(\mathbb{Z}) = \mathbb{Z}$, on a $P \in \mathbb{Q}[X]$ d'après ce qui précède. Si $\deg(P) \geq 2$, quitte à remplacer P par $-P$, on peut supposer le coefficient dominant de P strictement positif. On a alors $\lim_{x \rightarrow +\infty} P'(x) = +\infty$ donc il existe $A > 0$ tel que P est strictement croissant sur $[A, +\infty[$. De plus, $P(x+1) - P(x) \rightarrow +\infty$ quand $x \rightarrow +\infty$. Donc il existe $A' > 0$ tel que $P(x+1) > P(x) + 1$. Pour $n \geq \max(A, A')$, on a $P(n+1) \geq P(n) + 2$ ce qui contredit $P(\mathbb{Z}) = \mathbb{Z}$. Donc le degré de P est inférieur à 1.

Solution 47. Le coefficient en X^k s'écrit $a_{k-1} - \alpha a_k \in \mathbb{Q}$. Si $a_k \in \mathbb{Q}$, on a donc $a_{k-1} \in \mathbb{Q}$. Il est donc impossible d'avoir deux coefficients consécutifs rationnels. Or $x_{n-1} \in \mathbb{Q}$ car c'est le coefficient dominant de P . Donc

$$\alpha \text{ est nécessairement racine simple.}$$

(256)

■

Solution 48. Soit $\Delta = P \wedge P' = \Delta$. On a $\deg(\Delta) \in \{1, 2, 3, 4\}$ car $\Delta \mid P'$.

Si $\deg(\Delta) = 4$, alors $\Delta = P'$ (car associé). Donc il existe $\beta \in \mathbb{C}$ d'où $\underbrace{P}_{\in \mathbb{Q}[X]} = (X - \beta) \underbrace{P'}_{\in \mathbb{Q}[X]}$. Par division euclidienne, $X - \beta \in \mathbb{Q}[X]$ et $\beta \in \mathbb{Q}$ d'après l'algorithme de la division euclidienne.

Si $\deg(\Delta) = 1$, on a $P = X - \beta$ avec $\beta \in \mathbb{Q}$ racine de P .

Si $\deg(\Delta) = 2$, si $\Delta = (X - \beta)^2$, on a $\Delta' = 2(X - \beta) \in \mathbb{Q}[X]$ donc $\beta \in \mathbb{Q}$ racine de Δ donc de P . Si $\Delta = (X - \alpha_1)(X - \alpha_2)$ avec $\alpha_1 \neq \alpha_2$. α_1 et α_2 sont racines doubles de P donc $P = (X - \beta) \underbrace{(X - \alpha_1)^2 (X - \alpha_2)^2}_{=\Delta^2 \in \mathbb{Q}[X]}$ Par division euclidienne, $X - \beta \in \mathbb{Q}[X]$ et donc

$\beta \in \mathbb{Q}$.

Si $\deg(\Delta) = 3$, si $\Delta = (X - \beta)^3$, on a $\Delta^{(2)} = 6(X - \beta) \in \mathbb{Q}[X]$ donc $\beta \in \mathbb{Q}$. Si $\Delta = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$ avec α_1, α_2 et α_3 distinctes. α_1, α_2 et α_3 seraient racines doubles de P ce qui contredit $\deg(P) = 5$. Si $\Delta = (X - \alpha)^2(X - \beta)$, α est racine triple de P et β racine double de P donc $P = (X - \alpha)^3(X - \beta)^2 \in \mathbb{Q}[X]$. Par division euclidienne, $(X - \alpha)(X - \beta) \in \mathbb{Q}[X]$ et

$$X - \alpha = \frac{\Delta}{(X - \alpha)(X - \beta)} \in \mathbb{Q}[X] \quad (257)$$

donc $\alpha \in \mathbb{Q}$.

Donc

P admet au moins une racine rationnelle.

(258)

■

Solution 49.

1. $1 \in \mathbb{Z}[i], 0 \in \mathbb{Z}[i], i \in \mathbb{Z}[i]$. Soit $(a, b, a', b') \in \mathbb{Z}^4$:

$$\begin{cases} (a + ib) - (a' + ib') = (a - a') + i(b - b') \in \mathbb{Z}[i] \\ (a + ib) \times (aa' - bb') + i(ab' + ba') \in \mathbb{Z}[i] \end{cases} \quad (259)$$

Donc $\mathbb{Z}[i]$ est un sous-anneau de \mathbb{C} contenant i .

Soit A un sous anneau de \mathbb{C} contenant i . A est stable par x donc $i^4 = 1 \in A$. A est stable par $+$ donc $\mathbb{Z} \subset A$, puis $i\mathbb{Z} \subset A$ donc $\mathbb{Z}[i] \subset A$.

$\mathbb{Z}[i]$ est donc le plus petit sous anneau de \mathbb{C} contenant i .

(260)

2. Si $|z|^2 = 1$ c'est-à-dire $a^2 + b^2 = 1$, alors

$$\frac{1}{z} = \frac{a - ib}{|z|^2} = a - ib \in \mathbb{Z}[i] \quad (261)$$

Si z est inversible dans $\mathbb{Z}[i]$, il existe $' \in \mathbb{Z}[i]$ tel que $zz' = 1$ donc $|z|^2|z'|^2 = 1$ donc $|z|^2 = 1$. Donc

z est inverse dans $\mathbb{Z}[i]$ si et seulement si $|z|^2 = 1$.

(262)

Soit $(a, b) \in \mathbb{Z}^2$. Si $|a| \geq 2$ ou $|b| \geq 2$, alors $a^2 + b^2 \geq 4$ donc si $|z|^2 = 1$, alors $a^2 + b^2 = 1$ et $(|a| = 1 \text{ et } |b| = 0)$ ou $(|a| = 0 \text{ et } |b| = 1)$. Donc

$U = \{1, -1, i, -i\}$

(263)

3. (a) Si $x \in \mathbb{R}$, il existe $n \in \mathbb{Z}$ tel que $|x - n| \leq \frac{1}{2}$ (faire un dessin et le montrer grâce aux parties entières). Soit alors $z_0 = x_0 + iy_0 \in \mathbb{C}$, on prend un $(a, b) \in \mathbb{Z}^2$ tel que $|x_0 - a| \leq \frac{1}{2}, |y_0 - b| \leq \frac{1}{2}$. Et pour $z = a + ib \in \mathbb{Z}[i]$, on a

$$|z - z_0|^2 = (x_0 - a)^2 + (y_0 - b)^2 \leq \frac{1}{2} \quad (264)$$

- (b) Soit $(q, r) \in \mathbb{Z}[i]^2$, on a $z_1 = qz_2 + r$ si et seulement si $\frac{z_1}{z_2} - q = \frac{r}{z_2}$. On a $|r| < |z_1|$ si et seulement si $\left| \frac{z_1}{z_2} - q \right| < 1$. On a $\frac{z_1}{z_2} \in \mathbb{C}$ donc d'après 3.(a), il existe $q \in \mathbb{Z}[i]$ tel que $\left| \frac{z_1}{z_2} - q \right| \leq \frac{\sqrt{2}}{2} < 1$. On pose alors $r = z_1 - qz_2 \in \mathbb{Z}[i]$ par stabilité. Il vient donc $|r| < |z_2|$. Ainsi,

$$\exists (q, r) \in \mathbb{Z}[i]^2, z_1 = qz_2 + r \text{ et } |r| < |z_1|. \quad (265)$$

Si $z_2 = 1$ et $z_1 = \frac{1+i}{2}$, on peut prendre $q \in \{0, 1, i, 1+i\}$. Donc

$$\text{il n'y a pas unicité.} \quad (266)$$

- (c) Soit $I \neq \{0\}$ un idéal de $\mathbb{Z}[i]$. On note $n_0 = \min \{|z|^2 \mid z \in I \setminus \{0\}\}$ (partie non vide de \mathbb{N}^*). Soit $z_0 \in I \setminus \{0\}$ tel que $|z_0|^2 = n_0$. On a directement $z_0\mathbb{Z}[i] \subset I$ (I est un idéal).

Réciproquement, soit $z \in I$, d'après 3.(b), il existe $(q, r) \in \mathbb{Z}[i]^2$ tel que

$$r = \underbrace{z}_{\in I} - \underbrace{z_0}_{\in I} \underbrace{q}_{\in \mathbb{Z}[i]} \in I \quad (267)$$

et $|r|^2 < n_0$. Nécessairement, $r = 0$ et $z = z_0q \in z_0\mathbb{Z}[i]$. Donc $I = z_0\mathbb{Z}[i]$. Finalement,

$$\mathbb{Z}[i] \text{ est principal.} \quad (268)$$

4. Si $|z|^2 = 1$, alors $z \in U$ donc c'est bon. On travaille ensuite par récurrence sur $n \in \mathbb{N}^*$. Supposons que la décomposition existe pour $z \in \mathbb{Z}[i]$ avec $|z|^2 \leq n$. Soit $z \in \mathbb{Z}[i]$ tel que $|z|^2 = n + 1$. On a $|z|^2 \geq 2$ donc $z \in U$. Si z est irréductible, c'est bon. Sinon, il existe $(z_1, z_2) \in \mathbb{Z}[i]^2$ tel que $z = z_1z_2$ et z_1 et z_2 non inversibles. Alors $|z_1|^2 \geq 2$ et $|z_2|^2 \geq 2$. Or $|z|^2 = n + 1 = |z_1|^2|z_2|^2$ donc $|z_1|^2 \leq n$ et $|z_2|^2 \leq n$. Par hypothèse de récurrence, on peut décomposer z_1 et z_2 , donc z est décomposable

$$\text{D'où le résultat par récurrence.} \quad (269)$$

Pour l'unicité, soit $z \in \mathbb{Z}[i] \setminus \{0\}$ tel que $z = u \prod_{\rho \in \mathcal{P}_0} \rho^{\nu_\rho(z)} = v \prod_{\rho \in \mathcal{P}_0} \rho^{\mu_\rho(z)}$. Le théorème de Gauss est valable dans $\mathbb{Z}[i]$, car c'est un anneau principal. S'il existe $\rho_0 \in \mathcal{P}_0$ tel que $\nu_{\rho_0}(z) < \mu_{\rho_0}(z)$, alors

$$\rho_0 \mid \prod_{\rho \in \mathcal{P}_0 \setminus \{\rho_0\}} \rho^{\nu_\rho(z)} \quad (270)$$

ce qui est proscrit par le théorème de Gauss. On a donc pour tout $\rho \in \mathcal{P}_0$, $\nu_\rho(z) = \mu_\rho(z)$. En reportant, on a $u = v$.

D'où l'unicité de la décomposition.

(271)

■

Solution 50.

1. On a $\bar{1} \in R$. Soit $(\bar{x}_1, \bar{x}_2) \in R^2$, il existe $(\bar{y}_1, \bar{y}_2) \in (\mathbb{F}_p^*)^2$ tel que $\bar{x}_1 = \bar{y}_1^2$ et $\bar{x}_2 = \bar{y}_2^2$.
On a alors

$$\bar{x}_1 \bar{x}_2^{-1} = (\bar{y}_1 \bar{y}_2^{-1})^2 \in R \quad (272)$$

donc

R est un sous groupe de (\mathbb{F}_p^*, \times) .

(273)

Soit

$$\begin{aligned} \varphi : \mathbb{F}_p^* &\rightarrow \mathbb{F}_p^* \\ \bar{y} &\mapsto \bar{y}^2 \end{aligned} \quad (274)$$

On a $\text{Im}(\varphi) = R$. Comme \mathbb{F}_p est un corps, chaque éléments de R a exactement 2 antécédents par φ . Donc $|R| = \frac{|\mathbb{F}_p^*|}{2} = \frac{p-1}{2}$.

S'il existe $\bar{y} \in \mathbb{F}_p^*$ tel que $\bar{a} = \bar{y}^2$, on a $\bar{a}^{\frac{p-1}{2}} = \bar{y}^{p-1} = \bar{1}$ par le théorème de Fermat.

Réciproquement, si $\bar{a}^{\frac{p-1}{2}} = \bar{1}$, $X^{\frac{p-1}{2}} - \bar{1}$ admet au plus $\frac{p-1}{2}$ racines dans \mathbb{F}_p^* . Tous les éléments de R sont racines de ce polynôme, ce sont donc ses seules racines. Donc $a \in R$.

Donc $a \in R$ si et seulement si $a^{\frac{p-1}{2}} = 1$.

(275)

2. Si $p = a^2 + b^2$, alors $\bar{0} = \bar{a}^2 + \bar{b}^2$. Si $\bar{a} = \bar{b} = \bar{0}$, on a $p \mid a$ et $p \mid b$ donc $p^2 \mid p$ ce qui est exclu. Par exemple, si $\bar{a} \neq \bar{0}$, on a $\bar{1} = -\bar{b}^2 \bar{a}^{-2}$ donc $\overline{-1} = (\bar{a}^{-1} \bar{b})^2 \in R$ d'après 1. On a donc $(\overline{-1})^{\frac{p-1}{2}} = \bar{1}$ si et seulement si $2 \mid \frac{p-1}{2}$ (car p est premier plus grand que 3) d'où $4 \mid p-1$ donc

$p \equiv 1[4]$

(276)

3. On a $|\mathbb{F}_p| = p$, $E(\sqrt{p}) \leq \sqrt{p} < E(\sqrt{p}) + 1$ et $|\{0, \dots, E(\sqrt{p})\}|^2 = (E(\sqrt{p}) + 1)^2 > p$ (p est premier, ce n'est pas un carré) donc (cardinalité)

$$\boxed{f \text{ n'est pas injective.}} \quad (277)$$

Donc il existe

$$((a_1, b_1), (a_2, b_2)) \in (\{0, \dots, E(\sqrt{p})\}^2)^2 \quad (278)$$

avec $(a_1, b_1) \neq (a_2, b_2)$ et $f(a_1, b_1) = f(a_2, b_2)$. Donc

$$\overline{a_1} - \overline{kb_1} = \overline{a_2} - \overline{kb_2} \Rightarrow \overline{a_1} - \overline{a_2} = \overline{k}(\overline{b_1} - \overline{b_2}) \quad (279)$$

Si $\overline{b_1} = \overline{b_2}$, alors $\overline{a_1} = \overline{a_2}$ donc $p \mid b_1 - b_2$ et $p \mid a_1 - a_2$ donc $(a_1, b_1) = (a_2, b_2)$ ce qui n'est pas vrai. Donc $\overline{b_1} \neq \overline{b_2}$. Posons $b_0 = b_1 - b_2$ et $a_0 = a_1 - a_2$. On a $\overline{b_0} \neq \overline{0}$. Il vient donc $(|a_0|, |b_0|) \in \llbracket 1, E(\sqrt{p}) \rrbracket^2$, $\overline{a_0} = \overline{k}\overline{b_0}$ donc

$$\boxed{\overline{k} = \overline{a_0}\overline{b_0}^{-1}} \quad (280)$$

4. Si $p \equiv 1[4]$, en remontant les calculs, on a $(-1)^{\frac{p-1}{2}} = \overline{1}$ donc $\overline{-1} \in R$ et il existe $\overline{k} \in \mathbb{F}_p^*$ tel que $\overline{-1} = \overline{k}^2$. Alors d'après 3., il existe (a_0, b_0) tels que $\overline{k} = \overline{a_0}\overline{b_0}^{-1}$. Il vient alors $\overline{-1} = \overline{a_0}^2(\overline{b_0}^{-1})^2$ donc $\overline{-b_0}^2 = \overline{a_0}^2$. On a

$$p \mid a_0^2 + b_0^2 \in \llbracket 2, 2E(\sqrt{p}) \rrbracket^2 \subset \llbracket 2, 2p - 1 \rrbracket \quad (281)$$

Nécessairement, $a_0^2 + b_0^2 = p$ et

$$\boxed{p \text{ est somme de deux carrés.}} \quad (282)$$

■

Solution 51.

1. Soit $(m, n) \in A^2$. Il existe $(a, b, c, d) \in \mathbb{N}^4$ tel que $m = a^2 + b^2 = |a + ib|^2$ et $n = c^2 + d^2 = |c + id|^2$. Donc

$$\boxed{m \times n = |ac - bd6i(bc + ad)|^2 = (ac - bd)^2 + (bc + ad)^2 \in A} \quad (283)$$

2. On a

$$\boxed{n = \underbrace{\prod_{p \in \mathcal{P}_1} p^{\nu_p(n)}}_{\in A \text{ car } \mathcal{P}_1 \subset A} \times \underbrace{\prod_{p \in \mathcal{P}_2} p^{\nu_p(n)}}_{= \prod_{p \in \mathcal{P}_2} p^{2\alpha_p} \in A} \in A} \quad (284)$$

3. Soit $n \in A$, il existe $(a, b) \in \mathbb{N}^2$ avec $n = a^2 + b^2$. Soit $p \in \mathcal{P}_1 \cup \mathcal{P}_2$, on a $p \mid a^2 + b^2$ donc $\overline{a^2 + b^2} = \bar{0}$ dans $\mathbb{Z}/p\mathbb{Z}$. Si $p \nmid a$ ou $p \nmid b$, alors $1 + \frac{b^2}{a^2} = \bar{0}$ donc $\overline{-1} \in R$ (résidus quadratiques, voir exercice précédent). Donc $p = 2$ ou $p \equiv 1[4]$.
Si $p \mid a$ et $p \mid b$, $a = p^k a'$, $b = p^l b'$ avec $p \nmid a'$ et $p \nmid b'$. On suppose $1 \leq k \leq l$ (quitte à échanger a et b). On a

$$a^2 + b^2 = p^{2k}(a'^2 + p^{2(l-k)}b'^2) = n \quad (285)$$

donc

$$p \mid a'^2 + p^{2(l-k)}b'^2 \quad (286)$$

et $\overline{a'^2 + p^{2(l-k)}b'^2} = \bar{0}$. Nécessairement, $l = k$. De même $p \in \mathcal{P}_1$. Par contraposée, ν_p est pair.

D'où la réciproque.

(287)

■

Solution 52. On a $2p \mid k - 1$ si et seulement si $2 \mid k - 1$ et $p \mid k - 1$. Comme $k \mid 2^p - 1$ impair donc k est impair et $2 \mid k - 1$. De plus, dans le groupe $(\mathbb{Z}/k\mathbb{Z})^*$, $k \mid 2^p - 1$ donc $\bar{2}^p = \bar{1}$. Ainsi l'ordre de 2 divise p et $\bar{2} \neq \bar{1}$ car p est premier donc l'ordre de 2 est p . Par le petit théorème de Fermat, $\bar{2}^{k-1} = \bar{1}$ et $\bar{2}$ est inversible dans $\mathbb{Z}/k\mathbb{Z}$ donc $p \mid k - 1$. ■