INDICATIONS

▷**1)** On peut élever à une puissance entière (pas fractionnaire) et essayer d'éliminer y puis z pour trouve une relation sur x. Attention, a priori les éléments ne commutent pas.

▷**3)** Exprimer la négation de la conclusion : $\exists x \in H \setminus K$ et...

▷**4)** Les éléments de $\mathrm{Aut}(G)$ sont des bijections de G dans G, pas des éléments de G.

▷**6)** b) : $\chi(\bar{2}) = \xi^2 \ldots$

▷**9)** Non.

▷**10)** L'application est bijective, donc $\prod(ax) = \prod x$ si on fait le produit sur tous les éléments du groupe.

▷**12)** Si $\sigma(k) = 2^k \mod 53$, c'est que $\sigma^n(k) = 2^n k \mod 53$.

▷**14)** 0,2,4,6,7,9,11 → **1**,2,4,6,7,9,11.
$A = a_0 + \{0, d, 2d \ldots (k-1)d\}$; $A + d = a_0 + \{d, 2d \ldots (k-1)d;\ k\,d\}$.

▷**16)** Soit I un idéal différent de $\{0\}$ et A et $x \in I, x \neq 0$, montrer que x n'est pas inversible.
Si $E_{i,j}$ est la matrice qui a un "1" en position (i,j) et 0 partout ailleurs, évaluer $E_{i,j} \times A \times E_{k,\ell}$ où $A \in \mathcal{I}$ est une matrice non nulle.

▷**18)** $143 \mid 11\ldots 1 = \dfrac{10^n - 1}{9} \iff 10^n \equiv 1 \mod 143$.

▷**19)** Respectivement : groupe, anneau (non commutatif), pas groupe (certains éléments ne sont pas inversibles pour $\circ$) [on dit "monoïde"]

▷**20)** C'est l'idéal des polynômes qui font 0 au point (0,0). Un générateur éventuel diviserait et X et Y.
Les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont ses sous-groupes, qui sont cycliques aussi (remonter à $\mathbb{Z}$).

▷**22)** Vérifier que $a^2 - 2b^2$ ne donne jamais 0 (sauf si $a = b = 0$).

▷**23)** $d^2 \mid a^2 - 2b^2 \mid a$ et b donc $d^2 \mid d$.
La suite (a_n, b_n) ne peut pas décroître indéfiniment en restant > 0 puisque ce sont des entiers (principe de la descente infinie, inventé par Pierre de Fermat).

▷**25)** $(\sqrt{2} + \sqrt{3})^4 - 10(\sqrt{2} + \sqrt{3})^2 + 1 = 0$.
$\cos\frac{20}{7} = -\cos\frac{\pi}{7} = -\cos\frac{15}{7}$. Or $\cos(4x) = 8\cos^4 x - 8\cos^2 x + 1, \cos(3x) = 4\cos^3 x - 3\cos x$. Pour finir, le polynôme $8t^4 + 4t^3 - 8t^2 - 3t + 1$ n'est certainement pas irréductible (racine évidente...). Finalement on trouve $8t^3 - 4t^2 - 4t + 1$ qui est irréductible car ses racines $\cos\frac{(2k+1)}{7}$, $k = 0, 1, 2$, sont irrationnelles.
$\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)^2 + I_2 = O_2$. Cette matrice engendre une sous-algèbre isomorphe à $\mathbb{C}$.

▷**26)** Un "monoïde" est un ensemble muni d'une loi interne et associative. C'est mieux que rien.
Dans $\aleph$ on a $64 = 8 \times 8 = 4 \times 4 \times 4$, deux décompositions irréductibles et distinctes.

▷**27)** Ils sont premiers entre eux. On trouve les coefficients de Bezout $\frac{1}{3}\left(X^3 - X^2 - X + 1\right), \frac{1}{3}\left(2 - X^2\right)$.
Le plus simple est sans doute d'écrire les divisions successives de l'algorithme d'Euclide et de remonter.

$$\begin{aligned} X^4 + X^2 + 1 &= (X-1)(X^3 + X^2 + X + 1) + (X^2 + 2) \\ X^3 + X^2 + X + 1 &= (X+1)(X^2 + 2) - (X+1) \\ X^2 + 2 &= -(X-1)(-(X+1)) + 3 \end{aligned}$$

d'où $3 = (X^2+2) + (X-1)(-(X+1))$ où on injecte que $-(X+1) = (X^3+X^2+X+1) - (X+1)(X^2+2)$, etc.
L'algorithme proposé est plus rapide mais mystérieux.

▷**28)** On a (quitte à multiplier par une puissance de 10)

$$r = N + \overline{0, x_1 \ldots x_k x_1 \ldots x_k x_1 \ldots x_k \ldots} = N + \overline{x_1 \ldots x_k} \times \left(10^{-k} + 10^{-2k} + \ldots\right).$$

▷**29)** On peut identifier deux polynômes (dans $\mathbb{C}[X]$ par l'ensemble de leurs racines (+ coefficient dominant). $\Phi_p(X) = 1 + X + \ldots X^{p-1}$ pour p premier.

▷**30)** Ranger les entiers $1 \ldots n$ selon la valeur de leur pgcd avec $n = p^m$, qui peut valoir $1, p, p^2 \ldots$ ou p^m ; la valeur 1 vaut pour tous les cas sauf les multiples de p, la valeur p pour les multiples de p sauf les multiples de p^2, etc...

▷**32)** $p \mid \dfrac{p \times (p-1)!}{k!(p-k)!}$ parce que $k!(p-k)!$ divise $(p-1)!$ (on utilise le thm de Gauss)

▷**33)** Prendre q en "arrondissant" le quotient $z/z' \in \mathbb{C}$ aux coordonnées entières les plus proches.