Corrigé de l'examen du 9 novembre 2021

Ex 1

1. La loi est commutative, car.

$$x * y = y * x \quad \forall x, y \in \mathbb{R}.$$

La loi est associative, car.

$$(x * y) * z = x * (y * z) = \sqrt[3]{x^3 + y^3 + z^3}$$

$$\forall x, y, z \in \mathbb{R}$$

Le neutre pour la loi $*$ est 0, car.

$$x * 0 = \sqrt[3]{x^3 + 0^3} = x \quad \forall x \in \mathbb{R}$$

2. Tout élément $x \in \mathbb{R}$ est inversible d'inverse $-x$, car $x * (-x) = \sqrt[3]{x^3 + (-x)^3} = \sqrt[3]{x^3 - x^3} = 0$.

Ex 2

$$\begin{cases} 5x \equiv 2 \mod 9 \\ 2x \equiv 1 \mod 13 \end{cases} \iff \begin{cases} x \equiv 4 \mod 9 \\ x \equiv 7 \mod 13 \end{cases}$$

On multiplie la première congruence avec l'inverse de $5 \mod 9$ $(= 2)$ et la deuxième congruence avec l'inverse de $2 \mod 13$ $(= 7)$.

On écrit le tableau des solutions de la deuxième congruence

$x \equiv 7 \mod 13$	7	20	33	46	59	72	85
$\mod 9$	7	2	6	1	5	0	4

solution $x \equiv 85 \mod 9 \cdot 13 = 117$

L'ensemble des solutions est donc

$$\{x = 85 + 117k \mid k \in \mathbb{Z}\}.$$

Ex 3

1. Un homomorphisme f est déterminé par l'image $f(1) = \bar{a} \in \mathbb{Z}/100\mathbb{Z}$.

En effet si $f(1) = \bar{a}$, alors $f(n) = \overline{an}$ $\forall n \in \mathbb{Z}$.

2. $\bar{a} \in \mathbb{Z}/100\mathbb{Z}$ peut prendre toutes les valeurs dans $\mathbb{Z}/100\mathbb{Z}$, donc il y a 100 homomorphismes

3. Il n'y a pas d'homomorphisme injectif, car $|\mathbb{Z}| = +\infty$ et $|\mathbb{Z}/100\mathbb{Z}| = 100$. Il n'existe pas d'application injective d'un ensemble infini dans un ensemble fini.

4. f est surjectif $\Leftrightarrow$ $\operatorname{im} f = \mathbb{Z}/100\mathbb{Z}$

Or $\operatorname{im}(f) = \langle f(1) \rangle$. Donc f surjectif $\Leftrightarrow$ $f(1)$ est un générateur de $\mathbb{Z}/100\mathbb{Z}$.

D'après le cours $\mathbb{Z}/n\mathbb{Z}$ a $\varphi(n)$ générateurs.

donc $\varphi(100) = 40$ générateurs.

Il y a donc 40 homomorphismes surjectifs

Ex 4

. $20 \equiv 1 \mod 19$ donc $20^{21} \equiv 1^{21} \equiv 1 \mod 19$.

. Théorème de Fermat $\qquad 21 \equiv 2 \mod 19$

$$2^{18} \equiv 1 \mod 19$$

donc $2^{20} \equiv 2^{18+2} \equiv 2^2 \equiv 4 \mod 19$

D'où : $20^{21} + 21^{20} \equiv 1 + 4 = 5 \mod 19$

Ex 5 1. L'algorithme d'Euclide étendu donne.

$$8 \cdot 11 - 3 \cdot 29 = 1.$$

donc les entiers vérifiant la relation

$$8x + 29y = 1$$

sont de la forme $\begin{cases} x = 11 + 29k \\ y = -3 - 8k \end{cases}$

pour un entier $k \in \mathbb{Z}$.

2. L'inverse de $\overline{8}$ dans $(\mathbb{Z}/29\mathbb{Z})^*$ est $\overline{11}$

3. On multiplie l'égalité $8z \equiv 3 \mod 29$ avec 11, sachant que $8 \cdot 11 \equiv 1 \mod 29$.

donc on obtient $z \equiv 33 \mod 29$.

Le plus petit entier z vérifiant cette égalité est donc 4.