Exercice 15 – Soient $x, y, z \in \mathbf{Z}$. Montrer :

1. $x^2 \equiv 0, 1, 4 \pmod 8$.

Soit $n = n_1 n_2 \cdots n_k \in \mathbb{Z}$ t.q. $\gcd(n_i, n_j) = 1$,

(Thm du reste chinois)

alors on a

① $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$

② $\begin{cases} x \equiv a_1 \mod n_1 \\ x \equiv a_2 \mod n_2 \\ \vdots \\ x \equiv a_j \mod n_k \end{cases}$ a une unique solution modulo n.

$\Leftrightarrow \quad x \equiv a \mod n$

③ $a \equiv b \mod n$ si et seulement si $a \equiv b \mod n_i$

(1) $x^2 \equiv 0, 1, 4 \mod 8$.

x	0	1	2	3	4	-3	-2	-1	mod 8
x^2	0	1	4	1	0	1	4	1	

(2) Si $4 \mid (x^2+y^2+z^2)$, alors $2 \mid x$, $2 \mid y$ et $2 \mid z$.

$x^2 \equiv 0, 1 \mod 4$

8 choix possibles :

$\{0,1\} \times \{0,1\} \times \{0,1\}$

$\|\|$ $\|\|$ $\|\|$

x^2 y^2 z^2

$x^2 \equiv y^2 \equiv z^2 \equiv 0 \mod 4$

$\Leftrightarrow \quad x \equiv y \equiv z \equiv 0 \mod 2$

(3) Si $x^2+y^2+z^2 \equiv 3 \bmod 4$, alors $2\nmid x$, $2\nmid y$, $2\nmid z$ et $x^2+y^2+z^2 \equiv 3 \bmod 8$.

$x \equiv y \equiv z \equiv 1 \bmod 4$

$2\nmid x \iff$ **$x \equiv 1 \bmod 2 \Rightarrow x^2 \equiv 1 \bmod 8$**

d'après le tableau de $x^2 \bmod 8$

idem pour y^2 et z^2. Donc $x^2+y^2+z^2 \equiv 1+1+1 \equiv 3 \bmod 8$

(4) $x^2+y^2+z^2 \neq 4^k(8l+7)$ $(k, l \in \mathbb{N})$

Si $k \geq 1$, $4 \mid (x^2+y^2+z^2)$ $\overset{\text{d'après (2)}}{\Rightarrow}$ $2\mid x$ et $2\mid y$ et $2\mid z$

$x = 2^k x_1$, $y = 2^k y_1$, $z = 2^k z_1$.

$x^2+y^2+z^2 = 4x_1^2 + 4y_1^2 + 4z_1^2 = 4(x_1^2+y_1^2+z_1^2) = 4^k(8l+7)$

$\Rightarrow x_1^2+y_1^2+z_1^2 = 4^{k-1}(8l+7)$

Si $k-1=0$, on gagne ✓✓

Si $k-1 \geq 1$, $4 \mid (x_1^2+y_1^2+z_1^2)$

$x_1 = 2x_2$, $y_1 = 2y_2$, $z_1 = 2z_2 \Rightarrow x_2^2+y_2^2+z_2^2 = 4^{k-2}(8l+7)$

et $x = 2x_1 = 4x_2$

$x = 2x_1 = 2(2x_2) = 2(2(2x_3)) \cdots = 2^k x_k$.

$y = \cdots = 2^k y_k$

$z = \cdots = 2^k z_k$.

et $x_k^2+y_k^2+z_k^2 = 8l+7$.

Plan

① Ex 16 de la feuille 3

② Résumé

③ Ex 7, Ex 11 de la feuille 1

Ex 16 Mq $2^{2^{6n+2}}+3$ est divisible par 19.

$2^{2^{6n+2}} \equiv -3 \mod 19$ $\quad 2^4 \equiv -3 \mod 19$

$a \equiv b \mod c \iff c \mid (a-b)$

$2^{18} \equiv 1 \mod 19$ par le petit thm de Fermat

(pgcd(2, 19) = 1 et 19 est premier)

$2^{6n+2} = 18k + r$ $\quad 2^{2^{6n+2}} = 2^{18k+r} = (2^{18})^k \cdot 2^r \equiv 2^r \mod 19$

$2^{6n+2} \equiv 4 \mod 18$ $\quad 18 = 2 \times 3^2$

⇕

$2^{6n+2} \equiv 4 \mod 9$

$2^{6n+2} \equiv 0 \mod 2$

$2^{6n+2} = (2^6)^n \cdot 2^2$

$= (64)^n \cdot 4 \equiv ? \mod 9$

$\equiv 1^n \cdot 4 \equiv 4 \mod 9$

$a \equiv b \mod k$

$c \equiv d \mod k$

$\Rightarrow$

$a+c \equiv b+d \mod k$

$ac \equiv bd \mod k$

$k \mid (a-b)$
$k \mid (c-d)$

$ac - bd = (a-b)c + b(c-d)$
est divisible par k.

Résumé

① définitions de base : divisibité, pgcd, ppcm, ...

② Valuation p-adique

$v_p(a) = k \iff p^k \mid a$ mais $p^{k+1} \nmid a$

appli : . divisibité : $a \mid b \iff v_p(a) \leq v_p(b)$ pour tout p premier

$a^{k_1} \mid b^{k_2} \Rightarrow a^{k_3} \mid b^{k_4}$ $\quad v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$

. $2\sqrt{3}$ n'est pas rationnel.

$\mathbb{Q} = \{ \frac{a}{b} \mid$ pour $a, b \in \mathbb{Z}, b \neq 0 \}$.

$2\sqrt{3} = \frac{a}{b} \iff 3 = \frac{a^2}{b^2}$ $\quad 3b^2 = a^2$

$v_p(3) + 2v_p(b) = 2v_p(a)$

On prend $p=3$. $\quad 1 + 2v_3(b) = 2v_3(a)$

$\frac{a + b\sqrt{c}}{c + d} = \frac{p}{q}$.

③ l'algorithme d'Euclide et relation de Bézout.

a, b t.q. $\text{pgcd}(a,b) = d$.

$\Rightarrow \exists u, v \in \mathbb{Z}$ t.q. $au + bv = d$.

Appli. ① trouver l'inverse $a \in (\mathbb{Z}/n\mathbb{Z})^*$

($\text{pgcd}(a, n) = 1$) $au + nv = 1$

$au \equiv 1 \mod n$.

② résoudre les équations de congruences

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases} \qquad \text{pgcd}(m, n) = 1$$

$um + vn = 1$

$$\begin{cases} x \equiv 0 \mod m \\ x \equiv 1 \mod n \end{cases} \quad \uparrow \; um$$

$$\begin{cases} x \equiv 1 \mod m \\ x \equiv 0 \mod n \end{cases} \quad \uparrow \; vn$$

$x \equiv bum + avn \mod mn$

④ le thm des restes chinois.

Congruence module mn $\Leftrightarrow$ Congruence module m

+

Congruence module n.

$\text{pgcd}(m, n) = 1$

⑤ le petit thm de Fermat : $a^b \equiv ? \mod p$.

pgcd $(a,p) = 1$ et p est premier

$$a^{p-1} \equiv 1 \mod p$$

$$a^b \equiv a^{k(p-1)+r} \equiv a^r \mod p$$

$$\text{pgcd}(a,b) = \prod_{p \text{ premier}} p^{\min\{v_p(a),\, v_p(b)\}}$$

$$\text{ppcm}(a,b) = \prod_{p \text{ premier}} p^{\max\{v_p(a),\, v_p(b)\}}$$

Ex 11 de la feuille 1.

Soit $n \geq 1$ un entier.

1. Si $2 \nmid n$, alors on a $2 \nmid (3^n - 1)/2$.

$$2 \mid \frac{3^n - 1}{2} \iff \frac{3^n - 1}{2} = 2k \iff 3^n - 1 = 4k$$

$$\iff 4 \mid 3^n - 1$$

$n = 2k+1$.

$$3^n = (3^{2k+1}) = 9^k \cdot 3 \equiv 3 \mod 4.$$

$$3^n - 1 \equiv 2 \mod 4.$$

$3^n - 1 \equiv ? \mod 4$

n

$(-1)^n - 1 \equiv -2 \mod 4$

$\equiv 2 \mod 4.$

2. Supposer n est pas premier.

$n = pq$ $\quad p \neq 1,\ q \neq 1$ (parce que $2 \nmid n$)

$3^p \equiv 3^q \equiv 3 \mod 4.$

$3^n \equiv 1 \mod 4$ puis que.

$n = p+q$

$3^n = 3^p \cdot 3^q.$

$3^n = (3^p)^q \equiv 3^q \equiv 3 \mod 4.$

$a^m - 1 = (a-1)(1 + a + a^2 + \cdots + a^{m-1})$

$a = 3^p, \quad m = q.$

$$\frac{3^{pq} - 1}{2} = \frac{(3^p - 1)}{2} \cdot (1 + 3^p + 3^{2p} + \cdots + 3^{p(q-1)})$$

3. $2 \nmid \dfrac{3^n + 1}{2} \iff 4 \nmid 3^n + 1$

$\Leftarrow$ $3^n \neq -1 \mod 9$.

$3 \equiv -1 \mod 9$.

$3^n \equiv (-1)^n \mod 9$. $2 \mid n$, $(-1)^n = 1$.

9. $a^{2k+1} + 1 = (a+1)(a^{2k} - a^{2k-1} + \dots + 1)$

Ex 7 de la feuille 1.

la formule du binôme.

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$$

$(a+b)(a+b)\cdots(a+b)$

$169 = 13^2$. $13^2 \mid 3^{3n+3} - 26n - 27$

$\Leftrightarrow 2 v_p(13) \leq v_p(3^{3n+3} - 26n - 27)$

$\Leftrightarrow 2 \leq v_p(3^{3n+3} - 26n - 27)$

$26 = 13 \times 2$

$27 = 13 \times 2 + 1$

$3^{3n+3} = 3^{3(n+1)}$

$a^{b+c} = a^b \cdot a^c$

$a^{bc} = (a^b)^c$

3^{n+1} 3^{n+1}

$= 27^{n+1} = (13\times 2+1)^{n+1}$

$= \sum_{k=0}^{n+1} \binom{n+1}{k} 2^k 13^k - 26n - 27$

$= \sum_{k=2}^{n+1} \binom{n+1}{k} 2^k 13^k$

Exs de la feuille 3

$\begin{cases} 3^{15} \equiv ? \mod 2^3 \\ 3^{15} \equiv ? \mod 5^3 \end{cases}$

$1000 = 2^3 \cdot 5^3$

$\text{pgcd}(2^3, 5^3) = 1$

$(\Rightarrow) \quad 3^{15} \equiv ? \mod 1000$

$3^{\varphi} \equiv 1 \mod 8$

$3^{\varphi} \equiv 1 \mod 125$

$3^2 \equiv 1 \mod 8.$

$3^5 \equiv 81 \times 3 = 243$

$\equiv -7 \mod 125$

$3^{15} \quad 3^{\varphi} \equiv \square \mod 125$

$3^{15} = 3^{5\times 3} = (3^5)^3 = (-7)^3 \mod 125.$

Ex1. $36000 = 6 \times 6 \times 1000 = 2^2 \times 3^2 \times 2^3 \times 5^3 = 2^5 \times 3^2 \times 5^3$

le nombre des diviseurs positifs: $(5+1)(2+1)(3+1)$

$2^i 3^j 5^k$

$0 \le i \le 5$

$0 \le j \le 2$

$0 \le k \le 3$

la somme:

$$\sum 2^i 3^j 5^k$$

$$= \sum (1+2+2^2+\dots+2^5)(1+3+3^2)(1+5+5^2+5^3)$$

Ex2. $42x + 26y = 4$

$42x \equiv 4 \mod 26.$

(x, y)

① $21x + 13y = 2.$

$2(x_0 + 13y_0 = 1.$

$2(2x_0) + 13(2y_0) = 2$

② $42 = 26 + 16$

$26 = 16 + 10$

$16 = 10 + 6$

$10 = 6 + 4.$

$6 = 4 + 2$

$4 = 10 - 6$

$= 10 - (16 - 10)$

$= 2 \times 10 - 16$

$= 2 \times (26 - 16) - 16$

$= 2 \times 26 - 3 \times 16$

$= 2 \times 26 - 3 \times (42 - 26)$

$= 5 \times 26 - 3 \times 42.$

$42x' + 26y' = 0$. homogène.

$x' = 26t$

$y' = -42t$.

~~$x = x_0$~~ $x = x_0 + x'$

$= -3 + 13t$

$y = 5 + (-21)t$.

Ex3. $56 = 7 \times 2^3$

$\sqrt[3]{56}$ n'est pas rationnel.

$56 = \frac{b^3}{a^3}$ $\quad a^3 \cdot 56 = b^3$.

$3v_p(a) + v_p(56) = 3v_p(b)$

$3v_p(a) + 3v_p(2) + v_p(7) = 3v_p(b)$

$p = 7$.

Ex4. Déterminer l'ensemble

$\{a \in \mathbb{Z} \mid$ la congruence $ax \equiv 6 \pmod{20}$ a une solution $x \in \mathbb{Z}\}$

a_0 $\quad a_0 + 20t$

Si $\text{pgcd}(a, 20) \overset{2,5}{=} 1$.

$a^{-1} \cdot ax \equiv a^{-1} \cdot 6$.

a^{-1} l'inverse de a mod 20.

$ax \equiv 6 \mod 20$.

$2x \equiv 6 \mod 20$. $\Leftrightarrow$ $2x - 6 = 20k$.

$x - 3 = 10k$.

$x \equiv 3 \mod 10$.

$4x \equiv 6 \mod 20$

$7x \equiv 3 \mod 10$.

7 est inversible mod 10.

$ax \equiv b \mod 20$.

$d = \text{pgcd}(a, 20)$

$0 \quad 20$.

$\frac{a}{d} x \equiv \frac{b}{d} \mod \frac{20}{d}$.

$(a, b, c \in \mathbb{Z})$.

La congruence $ax \equiv b \mod c$ a une solution $x \in \mathbb{Z}$

$\iff \text{pgcd}(a, c) \mid b$.

"$\Leftarrow$" Si $\text{pgcd}(a, c) \mid b$., on divise $ax \equiv b \mod c$

par $\text{pgcd}(a, c)$. $a_0 := \frac{a}{\text{pgcd}(a,c)}$ est inversible mod $c_0 = \frac{c}{\text{pgcd}(a,c)}$

Donc on a $a^{-1} \cdot a_0 \equiv 1 \mod c_0$.

$a^{-1} \cdot a_0 x \equiv a^{-1} b_0 \mod c_0$

$x \equiv a^{-1} b_0 \mod c_0$.

"$\Rightarrow$" $ax \equiv b \mod c \Rightarrow ax - b = ck \quad k \in \mathbb{Z}$.

$\Rightarrow b = ax - ck$.

$\Rightarrow \quad \text{pgcd}(a,c) \mid b.$

$\{ ax + cy \mid \quad x,y \in \mathbb{Z} \} = \{\text{les multiples de pgcd}(a,c)\}$

Exo $\quad a \in \{\ldots\} \quad$ ssi $\quad \text{pgcd}(a,20) \mid 6$

$\downarrow$

ssi $\quad \text{pgcd}(a,20) = 2$ ou 1. $\qquad \text{pgcd}(20,6) = 2$

Exo

$$\begin{cases} 7x \equiv 24 \mod 30 \\ 6x \equiv 4 \mod 22 \end{cases} \Leftrightarrow 3x \equiv 2 \mod 11.$$

$7 \times 3 + 1 = 7 \times 13. \qquad 7 \times 13 \equiv 1 \mod 30.$

$12, \qquad 3 \times 4 \equiv 1 \mod 11.$

$13 \times 7 \times x \equiv 24 \times 7 \mod 30$

14

$$\begin{cases} x \equiv 24 \times 7 \mod 30 \\ x \equiv 8 \mod 11 \end{cases}$$

$\mod 30 \times 11.$

Feuille 4.

Ex1 $\quad n \geq 0. \qquad F_n = 2^{2^n} + 1.$

Mq $\quad (F_m, F_n) = 1 \quad$ si $\quad m \neq n.$

On peut supposer que $m < n$. $F_m < F_n$

$F_n = 2^{2^n} + 1 = \left(2^{2^m}\right)^{2^{n-m}} + 1 \equiv (-1)^{2^{n-m}} + 1 \equiv 2 \mod F_m$

$a^{bc} = (a^b)^c \qquad 2^{2^m} \equiv -1 \mod F_m$

$F_n \equiv 2 \mod F_m$

$\text{pgcd}(F_n, F_m) \mid 2$ $\qquad$ $\text{pgcd}(F_n, F_m) = 1$ ou 2 ×.

F_n et F_m impairs

$\text{pgcd}(F_n, F_m) = 1.$

$\log_2(\log_2(x))$ nombres premiers compris entre 1 et $x > 2$.

$m = 0$ $\quad F_0 = 3.$

$F_0, F_1, \ldots, F_m$ $\qquad \boxed{\text{pgcd}(F_i, F_j) = 1.}$

p

Il y a au moins $m+1$ nombres premiers compris entre 1 et $F_m = 2^{2^m} + 1.$

$F_m = x$

$m \sim \log_2(\log(x))$

Prenons F_{m_0} le plus grand nombre de Fermat entre 1 et x, i.e. $2^{2^{m_0}}+1 \leq x \leq 2^{2^{m_0+1}}$

$x < 2^{2^{m_0+1}}+1$
$\Leftrightarrow x \leq 2^{2^{m_0+1}}$

$$\log_2(2^{2^{m_0}}+1) \leq \log_2 x < \log_2(2^{2^{m_0+1}}+1)$$

$$\log_2 x \leq \log_2(2^{2^{m_0+1}})$$

$\log_2 2 = 1$

$$= 2^{m_0+1}$$

$\log e^2 = 2$.
↳ veut dire $\log_e$

$$\log_2(\log_2 x) \leq (m_0+1)$$

$$m_0+1 \geq \log_2(\log_2 x)$$

Ex2. $a, b \in \mathbb{Z}$.

① Si $2 \nmid a$, $5 \nmid a$. on a $a^{100} \equiv 1 \mod 1000$.

$1000 = 10^3 = (2\times 5)^3 = 2^3 \times 5^3$

Il faut et il suffit de montrer que $a^{100} \equiv 1 \mod 2^3$ / $\mod 5^3$

(Thm chinois)

$a^{100} \equiv 1 \mod 8$

$a^{100} \equiv 1 \mod 5^3$

$0, 1, 2, 3, 4, 5, 6, 7$

$x \equiv 0, 1, 2, 3, 4, -3, -2, -1 \mod 8$

$x^2 \equiv 0, 1, 4, \_$

$2 \nmid a \Rightarrow a^2 \equiv 1 \mod 8$.

$a^{100} = (a^2)^{50} \equiv 1 \mod 8$.

$$\begin{cases} x \equiv a \mod p \\ x \equiv b \mod q \end{cases} \iff x \equiv c \mod pq.$$

pour c unique mod pq.

$\gcd(p,q) = 1$.

$$\begin{cases} x \equiv 1 \mod 5^3 \\ x \equiv 1 \mod 2^3 \end{cases} \iff x \equiv 1 \mod 1000$$

$$\begin{cases} a^{100} \equiv 1 \mod 5^3 \\ a^{100} \equiv 1 \mod 2^3 \end{cases} \iff a^{100} \equiv 1 \mod 1000$$

$$\mathbb{Z}/pq\mathbb{Z} = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

( ) (_ , _)

$a^{100} \equiv 1 \mod 5^3$.

la fonction d'Euler.

$5 \nmid a$, a est inversible mod 5^3.

$a^{\varphi(5^3)} \equiv 1 \mod 5^3$.

$\varphi(p^k) = p^k - p^{k-1}$

$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$

$\varphi(5^3) = 5^3 - 5^2$

$= 5^2(5-1) = 100.$

$\varphi(d)$ = le nombre de d qui est premier à n entre $[0, n-1]$

$$\begin{cases} a^{100} \equiv 1 \mod 5^3 \\ a^{100} \equiv 1 \mod 2^3 \end{cases} \iff a^{100} \equiv 1 \mod 1000.$$

2. b.

$$\begin{cases} 2\nmid b, & 5 \mid b \\ 2 \mid b, & 5 \mid b \\ \hline 2 \mid b, & 5 \nmid b \\ \hline 2 \nmid b, & 5 \nmid b \end{cases} \longrightarrow \begin{cases} b^{100} \equiv 0 \mod 2^3 \\ b^{100} \equiv 0 \mod 5^3 \end{cases} \iff b^{100} \equiv 0 \mod 1000$$

$$\begin{cases} b^{100} \equiv 1 \mod 2^3 \\ b^{100} \equiv 0 \mod 5^3 \end{cases} \iff b^{100} \equiv [\,] \mod 1000$$ (625)

$$b^{100} \equiv 1 \mod 1000.$$

Ex3. ① $a^{12} \equiv ? \mod 7$ pour $a \in \mathbb{Z}$.

$a^{12} \equiv ? \mod 13$

$a^{12} \equiv ? \mod 91$

② $a^6 \equiv ? \mod 7$

$a^6 \equiv ? \mod 13$

$a^6 \equiv ? \mod 91$

③ Si $n \geq 1$ est un entier t.q. $n \equiv 1 \mod 12$, alors $a^n \equiv a \mod 91$.

$a^{12} \equiv 0 \mod 7$

$a^{12} \equiv 1 \mod 13.$

$\Rightarrow a^{12} \equiv 1 \mod 91$

$7u + 13v = 1$

$$\begin{cases} x \equiv 0 \mod 7 \\ x \equiv 1 \mod 13 \end{cases} \iff x \equiv 14 \mod 91$$

$\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z} \iff \mathbb{Z}/91\mathbb{Z}.$

$(a, b) \hookrightarrow c$

$$\boxed{\begin{array}{l} c \equiv a \mod 7 \\ c \equiv b \mod 13 \end{array}}$$

$13 = 2 \times 7 + (-1)$

$1 = 2 \times 7 - 13.$

$$\begin{cases} 14 \equiv 0 \mod 7 \\ 14 \equiv 1 \mod 13 \end{cases}$$

---

2. $13 \mid a, \quad a^6 \equiv 0 \mod 13.$

$13 \nmid a. \quad a^6 \equiv \pm 1 \mod 13.$ $\boxed{a^6 \equiv -1 \mod 13}$

$a^{12} \equiv 1 \mod 13.$

$(a^6)^2 \equiv 1 \mod 13$

$a^6 = (a^2)^3$
$\equiv (-1)^3$
$\equiv -1 \mod 13.$

$x^2 \equiv 1 \mod 13$

x	0	± 1	± 2	± 3	± 4	± 5	± 6
x^2	0	1	4	$+4$	3	-1	-3

$\mod 13.$

$a, -a.$

$a^2 = (-a)^2.$

$x^2 \equiv 1 \iff x \equiv \pm 1 \mod 13.$

$\begin{cases} a^6 \equiv 0, 1, -1 \mod 13 \\ a^6 \equiv 0, 1 \mod 7. \end{cases}$ $\Rightarrow a^6 \equiv ? \mod 91$

$\mod 13$ / $\mod 7$	0	1	-1
0	0	14	-14
1	-13	1	-25

$\hookrightarrow \mod 91$

$\begin{cases} x \equiv -1 \mod 13 \\ x \equiv 1 \mod 7. \end{cases}$ $\iff x \equiv ? \mod 91.$

$7 \times 2 - 13 = 1.$

$$X \equiv 7 \times 2 \times (-1) - 13 \times 1 \equiv -25$$

3. $a^n \equiv a \mod 91$.

$n = 12k+1$

$$\begin{cases} a \equiv b \mod p \\ a \equiv b \mod q \end{cases} \iff a \equiv b \mod pq.$$

$\gcd(\varphi, 8) = 1$

$a^n \equiv a \mod 91 \iff \begin{cases} a^n \equiv a \mod 13 \\ a^n \equiv a \mod 7. \end{cases}$

$n = 12k+1$

$(a^{12})^k \equiv 1 \mod 13$. Si $13 \nmid a$ $\Rightarrow a^{12k+1} \equiv a \mod 13$.

$(a^{12})^k \equiv 0 \mod 13$ Si $13 \mid a$

Ex 4. φ : fonction d'Euler

① pour p premier $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$

$\varphi(p^k) = |(\mathbb{Z}/p^k\mathbb{Z})^*|$

② Si $\gcd(a,b) = 1$, $\varphi(ab) = \varphi(a)\varphi(b)$

1. $\varphi(n)$: ① factoriser $n = \prod p_i^{k_i}$

② $\varphi(n) = \prod \varphi(p_i^{k_i}) = \prod (p_i^{k_i} - p_i^{k_i-1})$

$64 = 2^6$ $\quad \varphi(64) = \varphi(2^6) = 2^6 - 2^5 = 2^5(2-1) = 32.$

$125 = 5^3$ $\quad \varphi(5^3) = 5^3 - 5^2 = 5^2(5-1) = 25 \times 4 = 100$

$100 = 2^2 \times 5^2$ $\quad \varphi(2^2 \cdot 5^2) = \varphi(2^2) \cdot \varphi(5^2) = (2^2-2)(5^2-5)$

$= 2 \times 20 = 40$

$108 = 2 \times 54 = 2 \times 2 \times 3^3 = 2^2 \times 3^3$ $\quad \varphi(108) = \varphi(2^2) \cdot \varphi(3^3)$

$= (2^2-2)(3^3-3^2)$

$= 2 \times (27-9)$

$= 2 \times 18 = 36.$

2. $\dfrac{\varphi(2n)}{\varphi(n)}$ Soit $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ où p_i sont premiers

① $2n = 3 \cdot p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ si $3 \mid n$

② $2n = 2^{k_1+1} p_2^{k_2} \dots p_r^{k_r}$ si $2 \mid n$ et $p_1 = 3$.

① $\varphi(2n) = \varphi(3)\varphi(p_1^{k_1} \dots) = \varphi(3)\varphi(n)$

$\dfrac{\varphi(2n)}{\varphi(n)} = \varphi(3) = 3 - 1 = 2.$

② $\varphi(2n) = \varphi(2^{k_1+1})\varphi(p_2^{k_2} \dots p_r^{k_r})$

$$= (3^{k_1+1} - 3^{k_1})\, \varphi(p_2^{k_2} \cdots p_r^{k_r})$$

$$\varphi(n) = \varphi(3^{k_1})\, \varphi(p_2^{k_2} \cdots p_r^{k_r})$$

$$= (3^{k_1} - 3^{k_1-1})\, \varphi(p_2^{k_2} \cdots p_r^{k_r})$$

$$\frac{\varphi(2n)}{\varphi(n)} = \frac{3^{k_1+1} - 3^{k_1}}{3^{k_1} - 3^{k_1-1}} = 3.$$

$\frac{\varphi(6n)}{\varphi(n)}$: $2 \mid n$ $\quad 2 \nmid n$

$3 \mid n$ $\quad 3 \nmid n$

① $2 \mid n$ et $3 \mid n$ $\quad \frac{\varphi(6n)}{\varphi(n)} = \left[\frac{\varphi(2^{k_1+1})}{\varphi(2^{k_1})}\right]\left[\frac{\varphi(3^{k_2+1})}{\varphi(3^{k_2})}\right] = 2 \times 3 = 6$

② $2 \mid n$ et $3 \nmid n$ $\quad \frac{\varphi(6n)}{\varphi(n)} = \frac{\varphi(2n)\cdot\varphi(3)}{\varphi(n)} = 2 \times 2 = 4$

③ $2 \nmid n$ et $3 \mid n$ $\quad \frac{\varphi(6n)}{\varphi(n)} = \frac{\varphi(3n)\cdot\varphi(2)}{\varphi(n)} = 3 \times 1 = 3$

④ $2 \nmid n$ et $3 \nmid n$. $\quad \varphi(6n) = \varphi(6)\cdot\varphi(n) \Rightarrow \frac{\varphi(6n)}{\varphi(n)} = \varphi(6) = \varphi(3)\varphi(2) = 2.$

3. $\varphi(n) = \frac{n}{2}$ ssi $n = 2^k$ avec $k \geq 1$.

$\Leftrightarrow$

" $\Leftarrow$ " Si $n = 2^k$, $\varphi(n) = \varphi(2^k) = 2^k - 2^{k-1} = 2^{k-1} = \frac{2^k}{2} = \frac{n}{2}$.

" $\Rightarrow$ " $n = \prod p_i^{k_i} = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$

$$\varphi(n) = \prod p_i^{k_i - 1}(p_i - 1)$$

$$\frac{n}{2} = \frac{\prod p_i^{k_i}}{2}$$

$$\varphi(a) = \frac{n}{2} \Rightarrow \prod p_i^{k_i - 1}(p_i - 1) = \frac{1}{2}\prod p_i^{k_i}$$

$$\Rightarrow \prod (p_i - 1) = \frac{1}{2}\prod p_i$$

On peut supposer $p_1 = 2$ Si $r \geq 2$.

$$\prod_{i=1}^{r} (p_i - 1) = \prod_{i=2}^{r} p_i$$

$$(p_2 - 1) \cdots (p_r - 1) = p_2 p_3 \cdots p_r$$

$2 - 1$

$p_i - 1 < p_i$

$\prod (p_i - 1) < \prod p_i$: contradiction.

Donc on a $r = 1$.

4. $\varphi(n) = 4$ $\quad n = p_1^{k_1} \cdots p_r^{k_r}$

$$p_1^{k_1 - 1}(p_1 - 1)\, p_2^{k_2 - 1}(p_2 - 1) \cdots p_r^{k_r - 1}(p_r - 1) = 4.$$

$4 = 2 \times 2 = 4 \times 1$

$p_i - 1 = 1, 2, 4 \Rightarrow p_i = 2, 3, 5$

$p_j^{k_j - 1} = 1, 2, 4. \Rightarrow$

$p_j^{k_j - 1} = p_j^0, 2^1, 2^2$

Si $p_i - 1 = 1 \Rightarrow p_i = 2$, $(p_i^{k_i-1})(p_i-1) = 2^{k_i-1}$

$\begin{cases} k_i - 1 = 2 & \varphi(n) = 4, \text{ et } n = 2^3 \\ k_i - 1 = 1 & 2^{k_i-1} = 2 \quad 3-1=2. \end{cases}$

$\varphi(8) = \varphi(3)\varphi(4)$

$= 2 \times 2 = 4.$

$n = 12.$

$p_i = 3.$ $(p_i^{k_i-1})(p_i-1) = 3^{k_i-1} \cdot 2 \Rightarrow k_i = 1.$

$2^2 - 2 = 2.$

φ.

$n = 3 \times 4 = 12.$

$p_i = 5.$ $(p_i^{k_i-1})(p_i-1) = 5^{k_i-1} \cdot 4 \Rightarrow k_i - 1 = 0.$

$\varphi(n)$ $\varphi(2) = 1$

$\varphi(5) = 4.$

$\varphi(10) = 4.$

$2 \nmid n$ $\varphi(2n) = \varphi(n)$

$\varphi(n) = 4.$

$\varphi(2n) = 4.$

$n = 5, 8, 10, 12.$

Exo (5). $a^m \equiv 1 \mod 77$ pour tout $a \in (\mathbb{Z}/77\mathbb{Z})^*$

$\Leftrightarrow \text{pgcd}(a, 77) = 1$

Trouver m minimum.

$77 = 7 \times 11$ $\quad \varphi(7) = 6 \quad a^{\varphi(7)} \equiv 1 \mod 7$

$\varphi(11) = 10 \quad a^{\varphi(11)} \equiv 1 \mod 11.$

$n = \text{ppcm}(\varphi(7), \varphi(11)) = 30$

$a^{30} = (a^6)^5 \equiv 1 \mod 7$ $\Rightarrow a^{30} \equiv 1 \mod 77$

$a^{30} = (a^{10})^3 \equiv 1 \mod 11$

30 est minimum

(6) remplacer 77 par 385

$385 = 5 \times 7 \times 11.$

m minimum $= \text{ppcm}(\varphi(5), \varphi(7), \varphi(11))$

$= 60$

Exo (1) $\left|(\mathbb{Z}/17\mathbb{Z})^*\right| = 16$

a générateur $\in (\mathbb{Z}/17\mathbb{Z})^* \Leftrightarrow$ $a^{16} = 1 \in (\mathbb{Z}/17\mathbb{Z})^*$

$a^{16} \equiv 1 \mod 17$

Soit m l'ordre de a.
m minimum tel que
$a^m \equiv 1$

$a^d \neq 1$ pour $d < 16$.

Si $a^u \equiv 1 \Rightarrow m \mid u$

$16 = 2^4$ $\quad 2^i \quad 2^3$

$i \leq 3 \quad 2^i \equiv 1 \Rightarrow 2^3 \equiv 1$

Si $a^{2^3} \not\equiv 1 \Rightarrow a$ est un générateur.

~~$n = 3^2 \cdot 2^2$~~ $\quad a^{\boxed{\frac{n}{p}}} \not\equiv 1$

$3^i 2^j \quad (k_1, k_2, \dots, k_r)$

$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$

$p_1^{k_1} p_2^{k_2} \dots p_i^{k_i - 1} \dots p_r^{k_r}$

$(k_1, k_2, \dots, k_i - 1, \dots k_r)$

$a^n \equiv 1$

$\boxed{a^{\frac{n}{p}} \not\equiv 1.}$

$(k_1, k_1, \dots, k_i - 2, \dots k_r)$

$a^8 \neq 1$?

$a = 2$

$a^2 = 4$

$a^4 = 4^2 = 16 = -1.$

$a^8 = (a^4)^2 = 1.$

$q = 3 \mod 17$

$a^2 = 9 = -8$

$a^4 = 64 \equiv -4$

$a^8 = (-4)^2 = 16 \mod 17$

$\neq 1$

(2). $|(\mathbb{Z}/27)^*| = \varphi(27) = \varphi(3^3) = 3^3 - 3^2$

$= 3^2(3-1)$

$= 18$

a générateur $\Leftrightarrow$ $a^{\frac{18}{p}} \neq 1$ pour $p \mid 18$

$18 = 3^2 \times 2$

$3^i \cdot 2^j$

$(2,1)$

$(1,1)$

$(2,0)$

$a^6 \neq 1 \mod 18$

$a^9 \neq 1 \mod 18$

$a = 2.$

$a = 2$ est un générateur.

$a=1$

Ce groupe = $\{ a^k \mid k \in \{0,1,\dots\}$, ordre de $a \}$

Exo. $x^2 \equiv 1 \mod n$.

$\Leftrightarrow$ $n \mid (x-1)(x+1)$

$p \mid (x-1)(x+1)$

$x \equiv 1 \mod 2^{r-1}$ ou $\mod \frac{n}{2}$

$r-1$ $\frac{n}{2}$.

$x \equiv -1 \mod 2$

$1, 1+\frac{n}{2}$.

$x \mod n$.

$x \equiv 1 \mod 2$

$x \equiv ? \mod 4$

$x \equiv ? \mod 6$

Ex 7. $x^2 - x \equiv 0 \mod n$. $x^2 - 1$

$n \mid x(x-1)$

(1) $n = p^r$ $\quad p^r \mid x(x-1)$

k f.s.

$p^{r-k} \mid x$ $\quad p^k \mid (x-1)$

$\gcd(p^{r-k}, p^k) \mid x - (x-1)$

$\| \; 1.$

$1, p^r$

$p^r, 1.$

$p^r \mid x$ ou $p^r \mid x-1$

$x \equiv 0, 1 \mod n.$

2. $n = 10 = 2 \times 5$

$x \equiv 0, 1 \pmod 2$

$x \equiv 0, 1 \pmod 5$

4 : 2×2 solutions

$\begin{cases} x \equiv 0 \pmod 2 \\ x \equiv 1 \pmod 5 \end{cases}$ $\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 0 \pmod 5 \end{cases}$ $\begin{cases} x \equiv 0 \pmod 2 \\ x \equiv 0 \pmod 5 \end{cases}$ $\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 1 \pmod 5 \end{cases}$

3. $n = 2^t \cdot 5^t \quad (t = 2, 3)$

$x \equiv 0, 1 \pmod{2^t}$

$x \equiv 0, 1 \pmod{5^t}$

4. $n = 840 = 8 \times 105 = 2^3 \cdot 3 \cdot 5 \cdot 7.$

$x \equiv 0, 1 \pmod{2^3}$ $\quad 2 \times 2 \times 2 \times 2 = 16.$

$x \equiv 0, 1 \pmod 3$

$x \equiv 0, 1 \pmod 5$

$x \equiv 0, 1 \pmod 7.$

$f : x \longmapsto x^e$

$(x^e)^d \equiv x \mod n$

X

$g : y \longmapsto y^d$

$(x^d)^e = x \mod n$

$f \circ g$ $g \circ f$ sont Id

$n = pq$ $x^{p-1} \equiv 1 \mod p$ pour $p \nmid x$

$x^p \equiv x \mod p$ pour tout x

$x^q \equiv x \mod q$.

$x^{de} \equiv x \mod p \Rightarrow x^{de} \equiv x \mod pq$

$x^{de} \equiv x \mod q$ thm chinois

Si $de - 1$ est un multiple de $p-1$

& $q-1$.

$de \equiv 1 \mod \text{ppcm}(p-1)(q-1)$

$e = 37$

$n = 65 = 13 \times 5$

$p \quad q$

$\text{ppcm}(12, 4) = 12$

$de \equiv 1 \mod 12$

$37 \equiv 1 \mod 12$

$d \equiv 1 \mod 12$.

$f : x \mapsto x^e \mod n$.

$n = 77 = 7 \times 11$

$p \quad q$

$\text{ppcm}(6, 10) = 30$

$de \equiv 1 \mod 30$

$e = 37 \equiv 7 \mod 30$

$d \cdot 7 \equiv 1 \mod 30$, d est l'inverse

$d \in (\mathbb{Z}/30\mathbb{Z})^*$

$30 = 7 \times 4 + 2$

$7 = 3 \times 2 + 1$

$1 = 7 - 3 \times 2$

$= 7 - (30 - 7 \times 4) \times 3$

$= (3 \times 7) - 3 \times 30$

$q \equiv 13 \cdot 7 \mod 30$

$d \equiv 13 \mod 30$

$f: \quad x \mapsto x^7$

$g: \quad y \mapsto y^{13}$

$3 \equiv x^7$

$x \equiv (x^7)^{13} = 3^{13} \mod 30.$

Ex 9. $\frac{1}{7} = 0,142857\,142857\,\ldots\ldots$ (*)

$142857 =$

$10^6 \cdot \frac{1}{7} = 142857,\ 142857\,142857\cdots$

$\frac{1}{7} \qquad 0,\ 142857\,142857\cdots$

$\boxed{(10^6-1)\cdot\frac{1}{7} = 142857}$ $\quad \frac{n}{7}\cdot(10^6-1) = \ldots$

$\frac{1}{13}(10^d - 1)$ $\quad 10^d \equiv 1 \pmod{13}$.

$999\ldots9$ $\quad (24132)^*$

d

$0,\overline{123085}$

$0,585$

$142857 \longrightarrow 714285$

$abcdef \longrightarrow fabcde$

$142857 \longrightarrow 428571.$

$142857 \times 10 - (10^6 - 1) = (10^6 - 1)\left(\frac{10}{7} - 1\right)$

$= (10^6 - 1)\cdot\frac{3}{7}$

$428570 + 7 \times 10 - 4 \times (10^6 - 1) = (10^6 - 1)\left(10\cdot\frac{3}{7} - 4\right)$

$4285770 - 4000000 + 4.$ $\quad = (10^6 - 1)\frac{2}{7}$

Feuille 5

Groupe $(G, *)$

① associativité : $(a*b)*c = a*(b*c)$

e

① associativité

② ~~neutre élém~~ élément neutre

③ inverse

$e * a = a * e = a$ pour tout a

tout a, il existe a^{-1}

$a * a^{-1} = a^{-1} * a = e$.

$\mathbb{N} = \{0, 1, 2, \dots\}$ $+$

$0 + 0 = 0 + 0 = 0$. $\quad 0 + a = a + 0 = 0$

$a * a^{-1} = a^{-1} * a = e$.

$n > 0 \in \mathbb{N}$ $\quad n + [(-n)] = 0$

$(\mathbb{N}, +)$ n'est pas un groupe.

$(\mathbb{Z}, +)$

① associativité

② élément neutre 0

③ inverse ?

$n \in \mathbb{Z}$, $-n$ est l'inverse de n.

$(\mathbb{Z}/10\mathbb{Z}, \cdot)$ ① associative ✓.

② élément neutre

$1 \cdot n = n \cdot 1 = n$.

↳ élément neutre

③ inverse ?

$2 \in \mathbb{Z}/10\mathbb{Z}$? $\nexists$

$\frac{1}{2} \notin \mathbb{Z}/10\mathbb{Z}$.

$(\mathbb{R}/2\mathbb{Z}, \cdot)$ ① ✓

② 1 ✓.

③ $a \in \mathbb{R}/\{0\}$.

$a^{-1} \in \mathbb{R}/\{0\}$.

Ex2. $g, h \in 2\mathbb{Z}$ (" + ").

$g+h \in 2\mathbb{Z}$.

$H \subseteq G$ est un sous-groupe de H

si :

- $e \in H$, et pour toute $a, b \in H$

$a+b \in H$

et $a^{-1} \in H$.

- $H \neq \emptyset$, et pour toute $a, b \in H$

$a * b^{-1} \in H$.

$2\mathbb{Z}$ est un sous groupe de $(\mathbb{Z}, +)$

① $0 \in 2\mathbb{Z}$

② $\forall a, b \in 2\mathbb{Z}$, $a+b \in 2\mathbb{Z}$

$a = 0 \mod 2$

$b = 0 \mod 2$

$a+b \equiv 0 \mod 2$.

③ $a \in 2\mathbb{Z}$. $-a \in 2\mathbb{Z}$.

$2\mathbb{Z}$ est un sous groupe de $\mathbb{Z}$.

$2\mathbb{Z} \longrightarrow \mathbb{Z}$

isomorphisme = morphisme + bijectif.

morphisme: $f: G \to G'$

$f(gh) = f(g) f(h)$.

G G'.

f est un isomorphisme $\Leftrightarrow$

f a un inverse (morphisme).

$f^{-1} : G' \longrightarrow G$

$f \circ f^{-1} = id_G$

$f^{-1} \circ f = id_{G'}$

$\mathbb{Z} \longrightarrow 2\mathbb{Z}.$

$f : a \mapsto 2a$

f est isomorphisme.

① f est un morphisme.

$f(a+b) = f(a) + f(b)$

$2(a+b) = 2a + 2b$

f est bijective ?

$a \longmapsto 2a$ $\quad b = 2a$

$g: \frac{b}{2} \longleftarrow b \quad a = \frac{b}{2}$

$b \in 2\mathbb{Z}$.

$f \circ g$ $\qquad$ $g \circ f$

f: morphisme de groupe $\quad G \times H$

$G \longrightarrow G'$ $\quad \{(a,b)\}$

$(a,y) + (a',b') = (a+a', b+b')$

$g: G' \longrightarrow G$ t.q.

$g \circ f = id_G$

mais $f \circ g = id_{G'}$

$\mathbb{Z} \longrightarrow \mathbb{Z} \oplus \mathbb{Z}$

$f: a \longmapsto (a, 0)$

$g: a \longleftarrow (a,b)$

f est un morphisme $\Leftrightarrow$ de groupe

f est injective $\Leftrightarrow$ $\ker f$ est nul.

Ex) $G = (\mathbb{Z}^2, +)$

$$H = \{(a,b) \in \mathbb{Z}^2 \mid a \equiv b \pmod 2\}$$

H est un sous groupe ?

① $(0,0)$ est l'élément neutre $\in G$.

$(0,0) \in H$

② $(a,b) \in H$, $(a',b') \in H$.

$(a+a', b+b') \in H$?

$a \equiv b \bmod 2$ $\Rightarrow$ $a+a' \equiv b+b' \bmod 2$.

$a' \equiv b' \bmod 2$.

③ $(a,b) \in H$, $(-a,-b)$ est l'inverse de (a,b)

$\in G$ $(-a,-b) \in H$ ✓.

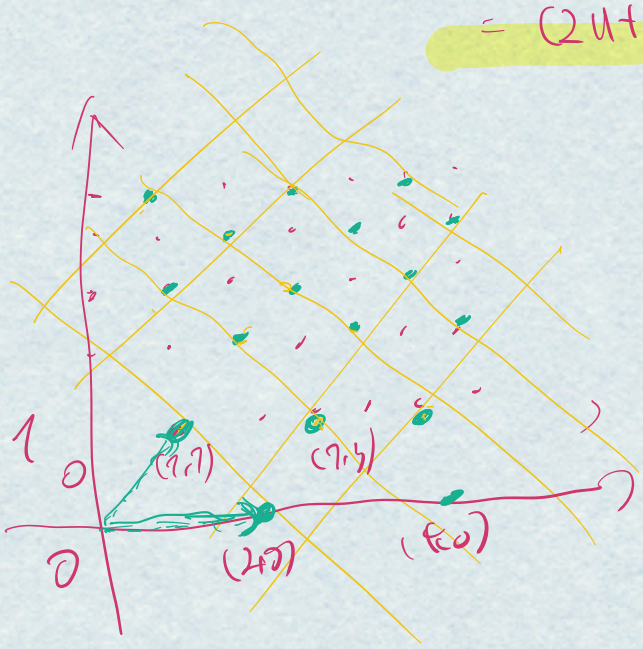
$a \equiv b \bmod 2$ $\Rightarrow$ $-a \equiv b \bmod H$.

H est un ss-groupe de G.

$f : \mathbb{Z}^2 \to H$

$(u, v) \mapsto u(2,0) + v(1,1)$

$= (2u+v, v).$



points entiers.

H

f

$\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}.$

$a \mapsto (a, 0).$

$\{1, 6\}$

$\{(1,0), (6,0)\}$

$\mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/25\mathbb{Z}$

$a \mapsto a.$

$5 \mapsto 5$

Ex3. $G = \mathbb{Z}^2$ $\quad H = \{(a,b) \in \mathbb{Z}^2 \mid a \equiv b \bmod 2\}$.

$f : \mathbb{Z}^2 \to H$

$(u,v) \mapsto u(2,0) + v(1,1)$

$(2u+v, v)$

① f est un morphisme. $\quad f(ab) = f(a) \cdot f(b)$

$\forall\ (u,v)\ (u',v')$

$f((u,v) + (u',v')) = f(u,v) + f(u',v')$ ✓.

Trouver l'inverse de f :

$(u,v) \mapsto (2u+v, v) = (a,b)$ $\quad \in H$

$\begin{cases} 2u+v = a \\ v = b \end{cases}$

$\Rightarrow \begin{cases} v = b \\ u = \dfrac{a-b}{2} \end{cases}$

$H \to G$

$(a,b) \mapsto \left(\dfrac{a-b}{2}, b\right)$

Ex4. Soit $(G,*)$ un groupe. Décrire tous les morphisme de groupes

$\mathbb{Z} \to (G,*)$ et $\mathbb{Z}^2 \to (G,*)$

f morphisme $\Rightarrow f(e) = e$

$f(a^{-1}) = (f(a))^{-1}$

$f(ab) = f(a) f(b)$

$f : \mathbb{Z} \to (G,*)$

$1 \mapsto a$

$n > 0 \in \mathbb{Z}$ $\quad f(n) = f(n-1+1) = f(n-1) + f(1)$

$= f(n-2+1) + f(1)$

$= \underbrace{f(1) + f(1) \cdots + f(1)}_{n \text{ fois}}$

$= \underbrace{a * a * a * \cdots * a}_{n \text{ fois}}$

$f(e) = f(e) \cdot f(e)$

$(f(e))^{-1} f(e) = (f(e))^{-1} \cdot f(e)$

$e = f(e)$

$f(e) = f(a) f(a^{-1})$

$e = f(a) f(a^{-1})$

$0 \longmapsto e_G$

$-1 \longmapsto a^{-1}$

-2

-3

$\vdots$

$-n$

$f(-n) = f(-1-1-1 \cdots -1)$

$= f(-1) * \cdots f(-1)$ (n fois)

$= a^{-1} * a^{-1} \cdots a^{-1}$.

$f : \mathbb{Z} \longrightarrow (G, *)$

$n \longmapsto a^n$

$g : \mathbb{Z}^2 \longrightarrow (G, *)$

$g(ab) = g(a)\, g(b)$

(a,b)

$g(1,0) \longmapsto u$ | $g(-1,0) \longmapsto u^{-1}$

$g(0,1) \longmapsto v$ | $g(0,-1) \longmapsto v^{-1}$

$= a(1,0) \; tb(0,1)$

$g(a,b) = g(a(1,0) + b(a1))$

$= g(a(1,0)) * g(b(a1))$

$= u^a * v^b$

$a \in \mathbb{Z}$.

$(1,0) + (1,0) \cdots + (1,0)$ (a fois) pour $a > 0$.

$a = 0$. $\quad a(1,0) = (0,0)$

$-a(1,0) = (-1,0) + (-1,0) \cdots + (-1,0)$ (a fois)

$(a > 0)$.

Ex 5. M_6 : $f : \mathbb{Z} \to \mathbb{Z}$ est un morphisme ssi $\exists a \in \mathbb{Z}$ t.q. $f(x) = ax$. $\forall x \in \mathbb{Z}$.

(Cor de Ex 4)

$f(1) = a$.

$f(x) = ax$.

$\{x \in \mathbb{Z} \mid f(x) = 0\} = \{x \in \mathbb{Z} \mid ax = 0\}$

$\ker(f) = \{ x \in \mathbb{Z} \mid \dots \} = \begin{cases} \mathbb{Z} & (a=0) \\ \{0\} & (a \neq 0) \end{cases}$ ou

$\mathrm{Im}(f) = \{ y \in \mathbb{Z} \mid \exists x \in \mathbb{Z}.\ f(x) = y \} = \{ ax \mid x \in \mathbb{Z} \}$.

f est un isomorphisme $\Leftrightarrow$ f est injectif et surjectif

$\Leftrightarrow$ $\ker f = \{0\}$ et $\mathrm{Im} f = \mathbb{Z}$.

$\Leftrightarrow$ $a \neq 0$ et $a = \pm 1$

$\Leftrightarrow$ $a = \pm 1$.

Ex. $x^2 \equiv -1$ mod p ($p \geq 2$ premier) ssi $p \equiv 1 \bmod 4$.

1. $a^2 \equiv -1 \bmod p$.

(1) $a^4 \equiv 1 \bmod p$

$a \not\equiv 1$ $\quad a^2 \not\equiv 1$ $\quad a^3 \not\equiv 1$

$a^3 = a \cdot a^2 \equiv a \cdot (-1) \equiv -a \not\equiv 1 \bmod p$

(2) $p \equiv 1 \bmod 4$

$4 \mid (p-1)$ $\quad a^{p-1} \equiv 1 \bmod p$

$a^n \equiv 1$ mod p $\quad 4 \mid (p-1)$

2. (1) $p \equiv 1 \bmod 4$.

$f(x) = x^{p-1} - 1$

$p-1$ solutions dans $\mathbb{Z}/p\mathbb{Z}$

$x^{p-1} \equiv 1 \mod p \quad x \in \{1, 2, 3, \dots, p-1\}$

2) $f(x) = \left(x^{\frac{p-1}{2}} - 1\right)\left(x^{\frac{p-1}{2}} + 1\right)$

3) f de degré $p-1$.

f a $p-1$ solution dans $\mathbb{Z}/p\mathbb{Z}$

On a une racine $x^{\frac{p-1}{2}} + 1 \mod p$

$$r^{\frac{p-1}{2}} \equiv -1 \mod p.$$

$p \equiv 1 \mod 4$

$$\left(r^{\frac{p-1}{4}}\right)^2 \equiv -1 \mod p.$$

x

Ex6 $f : \mathbb{Z}^2 \to \mathbb{Z}^2$

Mq : f est un morphisme de groupes ssi $\exists\, a, b, c, d \in \mathbb{Z}$,

t.q. $f(x,y) = (ax+by, cx+dy) \quad \forall (x,y) \in \mathbb{Z}^2$.

$\ker f = ?$ $\quad Im = f$

D'après ex 5, il faut choisir $f(1,0)$ $f(0,1)$

$f(1,0) = (a, c)$ $\quad f(0,1) = (b, d)$

$\forall (m,n) \in \mathbb{Z}^2 \quad f(m,n) = m(1,0) + n(0,1)$

$f(m(1,0) + n(0,1)) = mf(1,0) + nf(0,1) = m(a,c) + n(b,d)$

$= (ma + nb, mc + nd)$

$f((1,0) + (1,0) + \dots + (1,0) + (0,1) + (0,1) + \dots + (0,1))$

$= f(1,0) + f(1,0) + \dots + f(0,1)$

$\ker f = \{ x \in \mathbb{Z}^2 \mid f(x) = (0,0) \}$

$f(x,y) = (ax+by, cx+dy) = (0,0)$

$\Rightarrow \begin{cases} ax+by = 0 \\ cx+dy = 0 \end{cases}$

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ $\qquad \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad-bc$

Si $ad-bc \neq 0$ $\qquad \ker f = \{(0,0)\}$

Si $ad-bc = 0$ On suppose que $\begin{cases} ax+by=0 \\ cx+dy=0 \end{cases} \iff ax+by=0$

$\operatorname{rang} A = 2 \Rightarrow \ker f = \{(0,0)\}$

$\operatorname{rang} A = 0 \Rightarrow \ker f = \mathbb{Z}^2$

$\operatorname{rang} A = 1 \Rightarrow$ eqs $ax+by=0$

$$\frac{ax}{\operatorname{pgcd}(a,b)} + \frac{by}{\operatorname{pgcd}(a,b)} = 0.$$

$$\begin{cases} x = \dfrac{b}{\operatorname{pgcd}(a,b)} \cdot t \\ y = -\dfrac{a}{\operatorname{pgcd}(a,b)} \cdot t \end{cases} \qquad t \in \mathbb{Z}.$$

f est iso ?

$f(x,y) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$

f est inversible dans $\mathbb{R}^2$ Si $\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad-bc \neq 0$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x' \\ y' \end{pmatrix}$

$$\begin{cases} x = \dfrac{x'd - y'b}{ad-bc} \\ y = \dfrac{ay' - cx'}{ad-bc} \end{cases}$$

$ad-bc$

$g: (x',y') \mapsto \left(\frac{x'd-y'b}{ad-bc}, \frac{ay'-cx'}{ad-bc}\right)$

$g: \mathbb{R}^2 \to \mathbb{R}^2$ $\quad \frac{1}{ad-bc}\begin{pmatrix} d & b \\ -c & a \end{pmatrix}\begin{pmatrix} x' \\ y' \end{pmatrix}$

$g: \mathbb{Z}^2 \to \mathbb{Z}^2 \iff (ad-bc) \mid \operatorname{pgcd}(a,b,c,d)$

$\operatorname{pgcd}(a,b,c,d) = e$ $\quad a = a'e$, $b = b'e$, $c = c'e$, $d = d'e$.

$ad-bc = a'd'e^2 - b'c'e^2$.

$e^2(a'd'-b'c') \mid e$

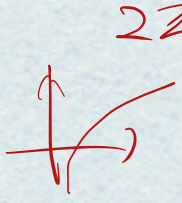
$e = 1$ et $a'd'-b'c' = \pm 1$

$\iff \det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \pm 1$

f est un isomorphisme $\iff ad-bc = \pm 1$.

Ex7. 1. $(\mathbb{R},+)$ et $(\mathbb{R}_{>0},\cdot)$

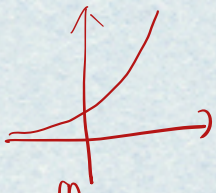
$f: \mathbb{R}_{>0} \to \mathbb{R}$, $x \mapsto \log x$



$\exp: \mathbb{R} \to \mathbb{R}_{>0}$, $a \mapsto \exp(a)$

$\exp(a+b) = \exp(a) \cdot \exp(b)$ ✓

exp ✓



$\mathrm{Im}(\exp) = \mathbb{R}_+^*$

2. $(\mathbb{Z}/4\mathbb{Z}, +)$ et $(\mathbb{Z}/2\mathbb{Z}, +) \times (\mathbb{Z}/2\mathbb{Z}, +)$

On suppose que f est un isomorphisme.

ordre $(a) = 4$ $\quad 4a = 0 \quad 2a \neq 0 \quad a \neq 0$

ordre $(f(a)) = 4 \quad 4f(a) = 0 \quad 2f(a) \neq 0 \quad f(a) = 0$

$f(4a) = 0 \quad f(2a) \neq 0 \quad f(a) = 0$

$f(x) = 0 \iff x = 0$

$1 \in \mathbb{Z}/4\mathbb{Z}$ ordre $(1) = 4$.

$(0,0)$

$(1,0) + (1,0) = (2,0) = (0,0)$

$(0,1) + (0,1) = (0,2) = (0,0)$

$(1,1) + (1,1) = (2,2) = (0,0)$

3. $(\mathbb{Z}/6\mathbb{Z}, +)$ et $(\mathbb{Z}/2\mathbb{Z}, +) \times (\mathbb{Z}/3\mathbb{Z}, +)$

$C \hookrightarrow (a, b)$

pgcd $(2,3) = 1$

$C \equiv a \mod 2$

$C \equiv b \mod 3.$

$C = 0 \mod 2$

$f(c) = (a,b)$ t.q. $\begin{cases} c \equiv a \pmod 2 \\ c \equiv b \pmod 3 \end{cases}$ donné par

$f(c') = (a',b')$

le thm chinois ✓

$f(c+c') = (a,b) + (a'+b')$

$\begin{cases} c \equiv a \pmod 2 \\ c \equiv b \pmod 3 \end{cases}$ $\begin{cases} c' \equiv a' \pmod 2 \\ c' \equiv b' \pmod 3 \end{cases}$

$\begin{cases} c+c' \equiv a+a' \pmod 2 \\ c+c' \equiv b+b' \pmod 3 \end{cases}$

---

4. $\text{pgcd}(m,n) = 1$ $(m,n \geq 1)$.

$(\mathbb{Z}/mn\mathbb{Z}, +) \cong (\mathbb{Z}/m\mathbb{Z}, +) \times (\mathbb{Z}/n\mathbb{Z}, +)$.

Thm chinois.

$\text{pgcd}(m,n) = d > 1$

dans $\mathbb{Z}/mn\mathbb{Z}$, on a un élément 1 qui a pour ordre mn.

On veut montrer que $\text{l'ordre}(f(1)) < mn$.

$f(1) = (a,b) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

$mn(a,b) = n(ma, mb) = n(0, mb) = (0, nmb)$

$= (0,0)$.

$m \cdot n = \text{pgcd}(m,n)\ \text{ppcm}(m,n)$

$\text{ppCm}_{(m,n)}(a,b) = \left(\text{ppcm}_{(m,n)}(a), \text{ppcm}_{(m,n)}(b)\right) = (0,0)$

5. $(\mathbb{Z}/4\mathbb{Z}, +)$ et $(\mathbb{Z}/5\mathbb{Z}\setminus\{0\}, \cdot)$

$(\mathbb{Z}/5\mathbb{Z})^*$

$2, -1, -2, 1 \quad \text{mod } 5$

$2, 2^2, 2^3, 2^4$

2 est un generateur de $(\mathbb{Z}/5\mathbb{Z})^*$.

$(\mathbb{Z}/5\mathbb{Z})^*$ est un groupe cyclique d'ordre 4.

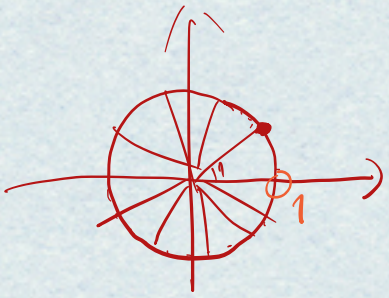
$\simeq \mathbb{Z}/4\mathbb{Z}$.

$2 \longleftrightarrow 1$

6. $(\mathbb{R}\setminus\{0\}, \cdot) \qquad (\mathbb{C}\setminus\{0\}, \cdot)$

$\underbrace{x \cdot x \cdot x \cdot x \cdot x \cdots x}_{n} = 1 \qquad \underline{x^n = 1}$

$n=4 \qquad x^4 = 1 \qquad i, -1, -i, 1$



Ex8. G groupe. Mq. $\forall g \in G$

$$f : \begin{array}{ccc} G & \to & G \\ h & \mapsto & ghg^{-1} \end{array}$$

est un automorphisme de groupe.

On doit montrer :

$h_1, h_2 \in G$. $f(h_1 h_2) = f(h_1) \cdot f(h_2)$

$$gh_1h_2g^{-1} = gh_1g^{-1} \cdot gh_2g^{-1}$$
$$= gh_1(g^{-1}g)h_2g^{-1}$$
$$= gh_1h_2g^{-1}$$

$$f^{-1} : \begin{array}{ccc} G & \to & G \\ h & \mapsto & g^{-1}hg \end{array}$$

$$f \circ f^{-1} = id_G$$

$$f^{-1} \circ f = id_G$$

$$G \xrightarrow{f^{-1}} G \xrightarrow{f} G$$
$$h \mapsto g^{-1}hg \mapsto g(g^{-1}hg)g^{-1}$$
$$\qquad\qquad\qquad\quad \| \; h$$

$$G \xrightarrow{f} G \xrightarrow{f^{-1}} G$$
$$h \mapsto ghg^{-1} \mapsto g^{-1}(ghg^{-1})g$$
$$\qquad\qquad\qquad\quad \| \; h$$

Ex4. Soit G un groupe t.q. $g^2 = e$ $\forall g \in G$.

Mq G est abélien.

déf : $g, h \in G$

Rappel : G est abélien

$$g*h = h*g$$

But :

$gh = hg \quad \forall g, h \in G.$ $\qquad$ $g^{-1} = g \quad \forall g \in G$

$\Leftrightarrow$

$$ghg^{-1} = hgg^{-1} = ghg^{-1} = h.$$

$\Leftrightarrow$ $\quad ghg = h$

$\Leftrightarrow$ $\quad ghgh = h \cdot h = e$

$(gh)^2$

Ex10 Soit G un groupe. Mq. l'application

$g \mapsto g^{-1}$ est un morphisme de groupes $G \to G$

ssi G est abélien.

$g \mapsto g^{-1}$ est un morphisme

$\Leftrightarrow \forall g, h \in G.$

$(gh)^{-1} = g^{-1} \cdot h^{-1}$

$\Leftrightarrow \forall g, h \quad h^{-1} g^{-1} = g^{-1} \cdot h^{-1}$

G abélien

$\Leftrightarrow \forall g, h \in G.$

$gh = hg$

en prenant g^{-1}, h^{-1} au lieu de g, h.

$g^{-1} h^{-1} = h^{-1} g^{-1}.$

$(gh)(h^{-1} g^{-1}) = e.$

$(gh)^{-1}.$

Ex 11 $f_1 : (\mathbb{C}\setminus\{0\}, \cdot) \longrightarrow (\mathbb{R}\setminus\{0\}, \cdot)$, $f_1(z) = |z|$.

$a+bi \longmapsto a^2+b^2$

"homo"

$|z| = z \cdot \bar{z}$

$a^2+b^2 = (a+bi)(a-bi)$

$a+bi,\ c+bi \in \mathbb{C}\setminus\{0\}$.

$f((a+bi)(c+di)) = f(a+bi)\, f(c+bi)$

$(a+bi)(c+di)\,(a-bi)(c-di) = (a+bi)(a-bi)\,(c+di)(c-di)$

$\ker f = \{ g \in G \mid f(g) = e \}$

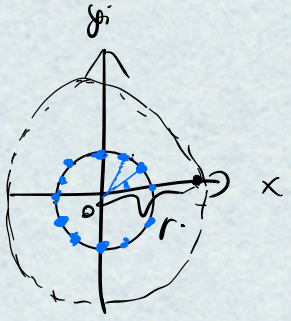
$= \{ a+bi \in \mathbb{C}\setminus\{0\} \mid a^2+b^2 = 1 \}$

sous-ensemble.

$\mathrm{Im} f = \mathbb{R}^+\setminus\{0\}$

$= \{ a \in \mathbb{R} \mid a > 0 \}$.

$r \in \mathbb{R}\setminus\{0\}$.



f est [surjective]. $de^{i\frac{2\pi t}{n}} \mid t = 0, 1, \ldots, n-1\}$

$|z^n| = |z|^n = 1$!!

Ex 13. Soit $n \geq 1$ un entier. Mq $\mu_n := (\{ z \in \mathbb{C} \mid z^n = 1 \}, \cdot)$ est un groupe cyclique d'ordre n. Trouver $(\mathbb{Z}/n\mathbb{Z}, +) \xrightarrow{\sim} \mu_n$.

Pour $d \mid n$, $\mu_d \subset \mu_n$ est un sous-groupe de μ_n. (cyclique d'ordre d).

↑ positif

$\mathbb{Z}/n\mathbb{Z} \longrightarrow \mu_n$

$e^{\frac{2\pi}{}}$

$\mapsto e^{\frac{i\pi}{n}}$

Ex 11.

$$f_1 : (\mathbb{C}\setminus\{0\}, \cdot) \to (\mathbb{R}\setminus\{0\}, \cdot)$$

$$z \longmapsto |z|$$

$$a+bi \longmapsto \sqrt{a^2+b^2}$$

$\sqrt{ab} = \sqrt{a}\cdot\sqrt{b}$

$a, b \in \mathbb{R}_{\geq 0}$

Norm : $a+bi \longmapsto a^2+b^2$

$$f_2 : (\mathbb{Z}^2, +) \longrightarrow (\mathbb{Z}, +)$$

$$(a,b) \longmapsto a-b$$

Il faut vérifier $(a,b)\ (c,d) \in \mathbb{Z}^2$

$$f_2((a,b)+(c,d)) = f_2(a,b) + f_2(c,d)$$

Mais $f_2(a+c, b+d) = a+c-(b+d)$

et $f_2(a,b) + f_2(c,d) = a-b+c-d$

Donc $f_2((a,b)+(c,d)) = f_2(a,b) + f_2(c,d)$

Donc f_2 est un morphisme de groupes

Par le thm d'homomorphisme.

$\ker f_2 = \{(a,b) \in \mathbb{Z}^2 \mid a-b=0\}$

$= \{(a,a) \in \mathbb{Z}^2\} \overset{\text{notation}}{=} \mathbb{Z}(1,1)$

$\text{Im} f_2 = \mathbb{Z}^2/\ker f_2$

$\mathbb{Z} = \mathbb{Z}^2/\mathbb{Z}(1,1)$

$f : a-b \leftarrow (a,b)$

$x \mapsto (x,0)$

$\mathrm{Im} f_2 = \mathbb{Z}$ f_2 est surjectif, parce que ↓

$\forall a \in \mathbb{Z}$ $f(a,0) = a$.

Vérifier que g est l'inverse de f :

$f_3 : (\mathbb{Z}^2, +) \to (\mathbb{Z}/2\mathbb{Z}, +)$

$(a,b) \mapsto a-b \mod 2$.

$f \circ g$: $x \mapsto (x,0) \mapsto x$ id ✓

$g \circ f$: $(a,b) \mapsto a-b \mapsto (a-b,0)$ id

mais $(a,b) - (a-b,0) = (b,b) \in \mathbb{Z}(1,1)$

Donc g est l'inverse de f.

f_3 est un morphisme de groupes ?

On prend (a,b) $(c,d) \in \mathbb{Z}^2$

$f_3((a,b)+(c,d)) = f_3(a+c, b+d)$

$= a+c-(b+d) \mod 2$

Mais $f_3(a,b) + f_3(c,d) = (a-b) + (c-a) \mod 2$

Donc f_3 est un morphisme de groupes.

$\mathrm{Im} f_3 = \mathbb{Z}/2\mathbb{Z}$ Surjectif

$(0,0) \mapsto 0 \mod 2$

$(1,0) \mapsto 1 \mod 2$.

$\ker f_3 = \{(a,b) \in \mathbb{Z}^2 \mid a-b \equiv 0 \mod 2\}$

$= \{(a,b) \in \mathbb{Z}^2 \mid a \equiv b \mod 2\}$.

$f_4 : (\mathbb{Z}^2, +) \to (\mathbb{Z}, +) \times (\mathbb{Z}/2\mathbb{Z}, +)$

$(a,b) \mapsto (a-b, b \mod 2)$

f_4 est un morphisme de groupes.

$\ker f_4 = \{(a,b) \in \mathbb{Z}^2 \mid a-b=0,\ b \equiv 0 \bmod 2\}$.

$b = 2k$ pour $k \in \mathbb{Z}$.

$a = b = 2k$.

$= \{(2k, 2k) \in \mathbb{Z}^2\}$ notation $= \mathbb{Z}(2,2)$

$\operatorname{Im} f_4 = \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. surjectif.

$\operatorname{Im} f_4 = \mathbb{Z}^2 / \ker f_4$

$\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}^2 / \mathbb{Z}(2,2)$

$f : (a-b, b \bmod 2) \leftarrow (a,b)$

$g : (x, y \bmod 2) \mapsto (x+y, y)$

$f_5 : (\mathbb{Z}^3, +) \to (\mathbb{Q}_{>0}, \cdot)$

$(a,b,c) \mapsto 2^a 3^b 5^c$

$x \mapsto a^x$

OPS $y = \alpha 1$

$a^{x+y} = a^x \cdot a^y$

$\ker f_5 = \{(0,0,0)\}$.

$\operatorname{Im} f_5 = \{2^a 3^b 5^c \mid (a,b,c) \in \mathbb{Z}^3\}$

$(a,b) \xmapsto{f} (a-b, b \bmod 2) \xmapsto{g}$

$(a-b+b_0, b_0)$

où $b \equiv b_0$ et $b_0 \in \{0,1\}$

$(a,b) - (a-b+b_0, b_0) = (b-b_0, b-b_0)$

$f_6 : (\mathbb{Z}^3, +) \to (\mathbb{Q}_{>0}, \cdot)$

$6 = 2 \cdot 3$

$6^c = 2^c \cdot 3^c$

$(a,b,c) \mapsto 2^{a+c} \cdot 3^{b+c}$

$2^{a+c} \cdot 3^{b+c} = 1 \Rightarrow \begin{cases} 2^{a+c} = 1 \\ 3^{b+c} = 1 \end{cases}$

$\ker f_6 = \{(a,b,c) \mid a+c=0 \text{ et } b+c=0\}$.

$= \{(-c, -c, c) \mid c \in \mathbb{Z}\}$ notation. $= \mathbb{Z}(-1,-1,1)$.

$\operatorname{Im} f_6 = \{2^u 3^v \mid u, v \in \mathbb{Z}\}$

$\begin{cases} a+c=u \\ b+c=v \end{cases}$ $\boxed{\begin{cases} a+c=u \\ b+c=v \end{cases}}$

Ex12. Soit $g \in G$ d'ordre fini $= n$, soit $f : G \to H$ un morphisme de groupes.

définition de l'ordre de g.

$g^n = e$ mais $g^k \neq e$ pour $1 < k < n$.

l'ordre de G est le nombre d'éléments dans G.

Mq. l'ordre de $f(g)$ divise l'ordre de g.

Si f est injectif, mq. l'ordre de $f(g)$ = l'ordre de g.

Si $g^m = e \Rightarrow n \mid m$.

Sinon $m = nk + r$, $0 < r < n$ (division euclidienne)

$$g^m = g^{nk+r} = (g^n)^k \cdot g^r$$

$$e = g^r$$

contradiction.

l'ordre de $f(g)$ divise n $\iff$ $f(g)^n = e$

l'ordre de h divise M $\iff$ $h^M = e$.

Il faut vérifier $\in G$

$$(f(g))^n = e.$$

Mais $(f(g))^n = f(g^n) = f(e_G) = e_H$

$$f(e_G \cdot e_G) = f(e_G) \cdot f(e_G)$$

e_G

$f(e_G)$

$f(e_G)^{-1} \cdot f(e_G) = f(e_G)^{-1} \cdot f(e_G) \cdot f(e_G)$

$e_H = f(e_G)$

Si f est injectif,

$f(g), f(g)^2, f(g)^3, \dots, f(g)^n$

$\| \quad \| \quad \| \quad \| \quad \|$

$f(g^2), f(g^3), \dots, f(g^n)$

Si $f(g)^k = e$ avec $0 < k < n$.

$f(g^k) = e$

Mais f est injectif $\Rightarrow g^k = e$ $0 < k < n$.

contredire le fait que l'ordre de $g = n$.

Ex 14. Définir un morphisme de morphismes

$(\mathbb{Z}, +) \xrightarrow{\sim} (\mathbb{Z}^2, +)/\mathbb{Z}(1,1)$

$(\mathbb{Z}, +) \times (\mathbb{Z}/2\mathbb{Z}, +) \xrightarrow{\sim} (\mathbb{Z}^2, +)/\mathbb{Z}(2,1)$

$G/H = \{gH\}$

$G \to G/H$

$f : G \to G'$

$\operatorname{Im} f \simeq G/\ker f$

Thm d'homomorphisme.

$g \mapsto g+H$

Ex15 $G := ((\mathbb{Z}/16\mathbb{Z})^*, \cdot)$

1. L'ordre de G $= |G| = \varphi(16) = \varphi(24)$
$= 2^4 - 2^3 = 8.$

2. ~~0, ±1, ±2, ±3, ±4, ±5, ±6, ±7, 8~~ mod 16.

$\{\pm 1, \pm 3, \pm 5, \pm 7\} = G$

	ordre
1	1
-1	2
3	4
-3	4
5	4
-5	4
7	2
-7	2

$49 = 16 \times 3 + 1$

3, -7, -5, 1

-7, 1

3. G n'est pas cyclique parce qu'il n'y a pas d'éléments d'ordre 8.

4. f est un isomorphisme.

Anneaux

Un anneau (unitaire) est $(A, +, \cdot)$

① $(A,+)$ est un groupe abélien.

0 ↑ élément neutre

$-a$ est l'inverse additif de a.

② $\forall a,b,c \in A,\ (a\cdot b)\cdot c = a\cdot(b\cdot c)$

③ unité 1. $\forall a \in A,\ 1\cdot a = a\cdot 1$

④ (Distributivité). $(a+b)\cdot c = (a\cdot c)+(b\cdot c)$

$a\cdot(b+c) = (a\cdot b)+(a\cdot c)$

Morphisme d'anneaux $(+,\cdot)$

$f : A \to B$

① $f(a+b) = f(a)+f(b)$

② $f(ab) = f(a)f(b)$

③ $f(1_A) = 1_B$

Ex 1 (Feuille 6)

$f : A \to B$ un morphisme d'anneaux.

Mq $f(A^*) \subset B^*$ et $f(a^{-1}) = f(a)^{-1}$ $\forall a \in A^*$.

$A^* = \{ a \in A \mid \exists\, a^{-1} \text{ t.q. } a\cdot a^{-1} = a^{-1}a = 1 \}$

$\mathbb{Z}/n\mathbb{Z}$. $(\mathbb{Z}/n\mathbb{Z})^* = \{ a \in \mathbb{Z}/n\mathbb{Z} \mid pgcd(a,n) = 1 \}$.

$\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. $Hom(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z})$

$f : a \mapsto (a, 0)$.

$g : a \longmapsto (a, b)$

$g \circ f = id_{\mathbb{Z}/2\mathbb{Z}}$.

$f \circ g \neq id_{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}}$.

Si $a \in A^*$, il existe $a^{-1} \in A$ t.q

$$a \cdot a^{-1} = a^{-1} \cdot a = 1_A$$

$$f(a \cdot a^{-1}) = f(a) \cdot f(a^{-1}) = f(a^{-1}) f(a) = f(1_A) = 1_B$$

Donc $f(a)^{-1} = f(a^{-1})$

Ex2.

$M \in M_n(A)$ est inversible $\iff \det(M) \in A$ est inversible.

$A = \mathbb{R}$

$M_n(\mathbb{R})$

Ex3 A anneau. Décrire tous les morphisme d'anneaux

$\mathbb{Z} \to A$

$f : \mathbb{Z} \to A$

$\boxed{f(1)} = 1_A$

$f(-1) = -f(1) = -1_A$

$f(n) = \underbrace{f(1) + f(1) + f(1) + \dots}_{n \text{ fois}}$

$= n \cdot 1_A$

$f(-n) = n \cdot (-1_A)$

$A = \mathbb{Z}/4\mathbb{Z}$

$\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$

$a \longmapsto a \bmod 4.$

$\delta \mapsto 0$ $\quad \delta \in \mathbb{Z}/4\mathbb{Z}$

Exo Ug. $f: \mathbb{Z} \to \mathbb{Q}$ (resp. $f: \mathbb{Q} \to \mathbb{Q}$) est un morphisme d'anneaux, alors on a $f(x) = x$ pour tout $x \in \mathbb{Z}$ (resp. pour tout $x \in \mathbb{Q}$).

$f: \mathbb{Q} \to \mathbb{Q}$ $\quad f(1) = 1$

$f(n) = \underbrace{f(1) + f(1) + \dots + f(1)}_{n \text{ fois}}$

$= n$

$f(-1) = -1$

$f(-n) = -n.$

$f(x) = x \quad \forall x \in \mathbb{Z}.$

$\forall \frac{m}{n} \in \mathbb{Q} \quad (m, n \in \mathbb{Z}, n \neq 0)$

$f(\frac{m}{n}) = f(m \cdot n^{-1}) = f(m) \cdot f(n^{-1})$

$= f(m) f(n)^{-1}$

$= m \cdot n^{-1}$

$= \frac{m}{n}.$

Donc $f(x) = x$ pour tout $x \in \mathbb{Q}$.

Exo Si f: morphisme d'anneaux $\mathbb{Q} \to A$

$f(1) = 1_A$ $\quad f(-1) = -1_A$

$n \in \mathbb{N}$ $\quad f(n) = n \cdot 1_A$ $\quad f(-n) = n \cdot (-1_A)$

$f(\frac{m}{n}) = f(m) \cdot f(n^{-1}) = m \cdot 1_A \cdot (n \cdot 1_A)^{-1}$

$A = \mathbb{Z}/n\mathbb{Z}$. $n = 2021$

$f\left(\frac{1}{2021}\right)$ n'existe pas !

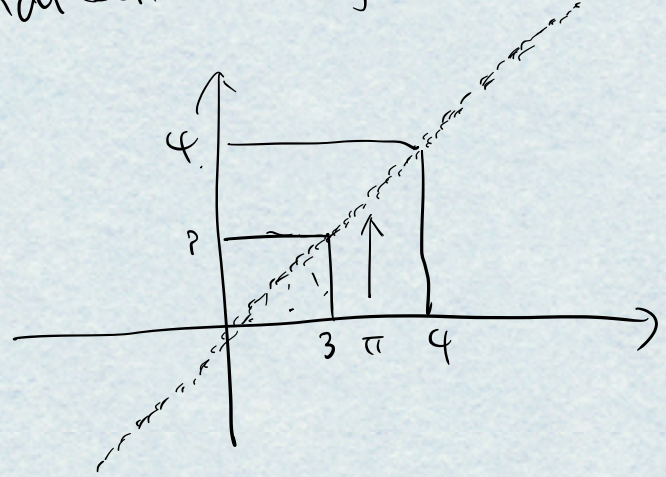
Il n'y a pas de morphismes d'anneaux

$\mathbb{Q} \to \mathbb{Z}/2021\mathbb{Z}$

Ex6. $f: \mathbb{R} \to \mathbb{R}$ morphisme d'anneaux.

alors $f(x) = x \quad \forall x \in \mathbb{R}$.

(Indication : $f(x) > 0$ pour tout $x > 0$)



f.

$\forall x > 0$

$x = \sqrt{x} \cdot \sqrt{x}$

$f(x) = f(\sqrt{x} \cdot \sqrt{x})$

$= f(\sqrt{x}) \cdot f(\sqrt{x})$

> 0

f est strictement croissante :

Si $x > y$

Mq : $f(x) > f(y)$

$x - y > 0$

$f(x-y) > 0$

$\Vert$

$f(x) - f(y) > 0$

$\forall x \in \mathbb{R}$

$a_n \to x \in$ br. $\subset$ rationnel $\subset$ réel.

$a_1\ a_2 \dots a_n \dots \mid \dots b_n \dots b_2\ b_1$

x

$a_1 < a_2 < \dots < a_n \dots < x < \dots b_n < b_{n-1} < \dots b_1.$

$a_n \to x$

$b_n \to x.$

$f(a_1) < f(a_2) \dots < f(a_n) < \dots f(x) = f(x) < \dots f(b_n) \dots f(b_1)$

$a_1 < a_2 \dots < a_n \dots < f(x) < \dots b_n < \dots < b_1.$

$x = f(x)$

$f(x) = \bigcap_{n \to \infty} [a_n, b_n] = x.$

$f(x) = 1 \quad \forall x \in \mathbb{R}.$

$(\mathbb{Z}/mn\mathbb{Z}, +) \overset{?}{=} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

Si $\text{pgcd}(m,n) = 1$ oui ✓

Si $\text{pgcd}(m,n) = d > 0$ non.

$\mathbb{Z}/20\mathbb{Z} \neq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$

groupe cyclique d'ordre 2.

il n'y a pas d'élément

$1 \in \mathbb{Z}/20\mathbb{Z}$

d'ordre 20.

$\text{ppcm}(2,10) \cdot x = 0$ mm

$x \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Feuille 6

Ex 7. Soit A un anneau.

$$\mathbb{Z}[X] \longrightarrow A$$

$$\mathbb{Z}[X] = \{ a_0 + a_1 X + \cdots + a_n X^n \mid a_i \in \mathbb{Z}, n \geq 0 \}$$

$$\mathbb{Z} \to A$$

$$1 \mapsto 1_A$$

$$-1 \mapsto -1_A$$

$$n \mapsto \underbrace{1_A + \cdots + 1_A}_{n \text{ fois}}$$

$$-n \mapsto \underbrace{-1_A + \cdots + (-1_A)}_{n \text{ fois}}$$

f : un morphisme de groupes

$$f(a^{-1}) = (f(a))^{-1}$$

$a \in G$. $\quad f(aa^{-1}) = f(a^{-1}a) = f(e)$

$f(a) f(a^{-1}) = f(a^{-1}) f(a) = e$

$$f(a_0 + a_1 X + \cdots + a_n X^n)$$

$$= f(a_0) + f(a_1) \cdot f(X) + \cdots + f(a_n) \cdot f(X^n)$$

$f(xy) = f(x) \cdot f(y)$ $\quad$ $(f(X))^n$

$$f(X^n) = f(\underbrace{X \cdot X \cdots X}_{n \text{ fois}})$$

$$= \underbrace{f(X) \cdot f(X) \cdots f(X)}_{n \text{ fois}}$$

$$= a_0 + a_1 f(X) + \cdots + a_n f(X)^n$$

(Si $f(X) = b \in \mathbb{Z}$.

$\hookrightarrow = a_0 + a_1 b + \cdots + a_n b^n$.

$$f(a^{-1}) = (f(a))^{-1}$$

En revanche, si on fixe $b \in \mathbb{Z}$.

et on définit une application $\mathbb{Z}[x] \to A$

$$f : \quad a_0 + \dots + a_n x^n \longmapsto a_0 1_A \dots + a_n b^n$$

On vérifie que f est un morphisme d'anneaux

Ex 8 A est un corps.

Corp : Un anneau commutatif t.q. $A^* = A \setminus \{0\}$.

$ab = ba \quad \forall a, b \in A$.

Montrer : Si $f : A \to B$ est un morphisme d'anneaux où A est un corps et $B \neq \{0\}$, alors f est injectif.

injectif $\overset{\text{déf}}{=}$: $f(a) = f(b) \Rightarrow a = b$

Si f est un morphisme de groupes abéliens

$$f(a) - f(b) = 0 \iff f(a-b) = 0$$

Injectivité : $f(a-b) = 0 \Rightarrow a - b = 0$

$\forall a, b \in G$.

Équivaut à : $f(a)=0 \Rightarrow a=0 \quad \forall a \in G$.

Équivaut à : $\ker f = \{0\}$

Mais $f(A^*) \subset B^*$

$\|$

$f(A \setminus \{0\}) \subset B^*$

Si $a \neq 0$ $f(a)$ est inversible dans $B \setminus \{0\}$.

En particulier, $f(a) \neq 0$.

Donc $\ker f = \{0\}$.

Exo. idéal $I \subset A$.

A/I.

$(a+I)(b+I) = ab+I$

$\|$? $\|$

$(a'+I)(b'+I) = a'b'+I$.

idéal I : sous-groupe de A.

$\forall x \in I, \forall a \in A, \quad ax \in I$

$xa \in I$.

$\Rightarrow$

$AI \subset I$

$IA \subset I$. (M).

A/I.

$f: A \to B$.

$A/\ker f \cong \operatorname{Im} f$.

$(m) = \{mk \mid k \in \mathbb{Z}\} \subseteq \mathbb{Z}$.

principal ideal domain

$(10, 12) = (10) + (12)$

principal

$= \{10k_1 + 12k_2 \mid k_1, k_2 \in \mathbb{Z}\}$ Common principal

$= \{mk \mid k \in \mathbb{Z}\}$

$= \{2k \mid k \in \mathbb{Z}\}$.

$(m) + (n) = (\gcd(m, n))$

$\{mk_1 + nk_2 \mid k_1, k_2 \in \mathbb{Z}\} = \{\gcd(m,n)\, k \mid k \in \mathbb{Z}\}$

"$\subseteq$" $\gcd(m,n) \mid m$, $d \mid mk_1$

$\gcd(m,n) \mid n$, $d \mid nk_2$

Donc $\gcd(m,n) \mid (mk_1 + nk_2)$

"$\supseteq$" par l'algorithme d'Euclide.

Cette relation de Bézout : $\text{pgcd}(m,n) = mk_1' + nk_2'$

$$\text{pgcd}(m,n)\,k = mk_1'k + nk_2'k.$$

$(10) \cap (12) = (\text{ppcm}(10,12)) = (60)$

Si $m \mid k$ $\Rightarrow$ $\text{ppcm}(m,n) \mid k$

$n \mid k$

$(10)\cdot(12) = \{10k_1 \cdot 12m_1 + 10k_2 \cdot 12m_2 + \dots + 10k_n \cdot 12k_n\}$.

$= (120)$

$\boxed{IJ} = \{ij \mid i \in I, j \in J\}$ $\times$.

$\boxed{\begin{matrix} i_1j_1 \\ + \\ i_2j_2 \end{matrix}} = \{\sum i_ij_i\}$.

Exo. Décrire tous les idéaux d'un corps K.

A : $\{0\}$ est un idéal

A est un idéal.

K : $\{0\}$ est un idéal

K est un idéal.

Si on suppose $I \neq \{0\}$ un idéal de K.

$a \in I$ $\quad a^{-1} \cdot a = 1 \in I$

$\neq 0$.

$\forall k \in K, \quad k \cdot 1 \in I$.

Ex 11 A sous-anneau de B ? $(A \subseteq B)$

① A sous-groupe de B :

$a, b \in A, \quad a+b \in A$ et $-a \in A$

$0 \in A$.

② clos par rapport à la multiplication

$a, b \in A \Rightarrow ab \in A$.

③ Unité : $1_B \in A$.

1) $A = \mathbb{Q} + \mathbb{Q}\sqrt{6} = \{ a + b\sqrt{6} \mid a, b \in \mathbb{Q} \}$.

$(a + b\sqrt{6}) + (a' + b'\sqrt{6}) = (a+a') + (b+b')\sqrt{6}$.

$-(a + b\sqrt{6}) = -a - b\sqrt{6}$.

$0 \in A$.

2). $(a + b\sqrt{6})(a' + b'\sqrt{6}) = (aa' + 6bb') + (ab' + ba')\sqrt{6}$

2). $1+0\sqrt{6} \in A$.

2. l'écriture $a+b\sqrt{6}$ est unique.

On suppose que $a+b\sqrt{6} = a'+b'\sqrt{6}$ (*)

avec $a, b, a', b' \in \mathbb{Q}$

(*) implique que $a - a' = (b'-b)\sqrt{6}$

Si $b'-b \neq 0$, $\sqrt{6} = \dfrac{a-a'}{b'-b}$

↑ irrationnel ↑ rationnel Contradiction

$b'-b=0 \Rightarrow a-a'=0$

3. $\sigma : A \to A$

$a+b\sqrt{6} \mapsto a-b\sqrt{6}$ est un iso d'anneaux.

① σ est bien un anneau:

D'abord, σ est bien définie

(l'écriture $a+b\sqrt{6}$ est unique)

On doit vérifier: pour $x, y \in A$

1) $\sigma(x+y) = \sigma(x) + \sigma(y)$

2) $\sigma(xy) = \sigma(x)\sigma(y)$

3) $\sigma(1_A) = 1_A$

On peut écrire $x = a+b\sqrt{6}$

$y = a'+b'\sqrt{6}$

1) ✓

2) ✓

3)

bijectif ?

$A \xrightarrow{\sigma} A \xrightarrow{\sigma} A$

$a+b\sqrt{6} \mapsto a-b\sqrt{6} \mapsto a+b\sqrt{6}$

$\sigma^2 = id_A$

Donc σ est un isomorphisme d'anneaux

4. $A \to \mathbb{C}$

$f : 1 \mapsto 1$

$f:$

$-1 \longmapsto -1$

$n \longmapsto n$

$\frac{n}{k} \longmapsto \frac{n}{k}.$

$f(a+b\sqrt{6}) = f(a) + f(b\sqrt{6})$

$= f(a) + f(b)\, f(\sqrt{6})$

$= a + b\, f(\sqrt{6})$

$(\sqrt{6})^2 = 6 \qquad f((\sqrt{6})^2) = f(6)$

$\left(f(\sqrt{6})\right)^2 = 6$

$f(\sqrt{6}) = \sqrt{6}$ ou $-\sqrt{6}$

$id: \quad a+b\sqrt{6} \longmapsto a+b\sqrt{6}$

$\sigma: \quad a+b\sqrt{6} \longmapsto a-b\sqrt{6}$

$\mathrm{Hom}(A \to \mathbb{C}) = \{id, \sigma\}$

5. A est un corps.

Si $a+b\sqrt{6} \neq 0 \quad \in A \subseteq \mathbb{R}$.

$$\frac{1}{a+b\sqrt{6}} = \frac{(a-b\sqrt{6})}{(a+b\sqrt{6})(a-b\sqrt{6})} = \frac{a-b\sqrt{6}}{a^2-6b^2} \in A$$

$$= \frac{a}{a^2-6b^2} + \left(\frac{-b}{a^2-6b^2}\right)\sqrt{6} \in A$$

7. Exo. Mq : $A = \mathbb{Q}+\mathbb{Q}\sqrt{6} \cong \mathbb{Q}[X]/(X^2-6)$

↑ isomorphisme.

Thm d'homomorphisme :

$$f : B \to B'$$

$$B/\ker f \cong \operatorname{Im} f.$$

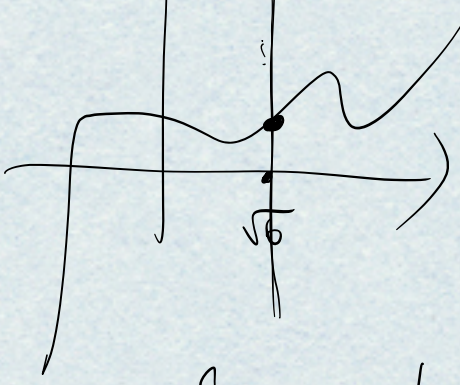
On veut définir $f : \mathbb{Q}[X] \to \mathbb{Q}+\mathbb{Q}\sqrt{6}$ t.q.

$\operatorname{Im} f = \mathbb{Q}+\mathbb{Q}\sqrt{6}$ et $\ker f = (X^2-6)$.
(i.e. f est surjective)

$$g(X) \mapsto g(\sqrt{6})$$

$$a_n X^n + a_{n-1}\cdot X^{n-1} + \dots a_0 \mapsto a_n(\sqrt{6})^n + a_{n-1}(\sqrt{6})^{n-1} + \dots + a_0$$

↑



$a+bX \mapsto a+b\sqrt{6}$

- f est surjectif.

$$\ker f = \{ g \in \mathbb{Q}[X] \mid g(\sqrt{6}) = 0 \}.$$

$\| ?$

$$(X^2-6) = \{ (X^2-6)g' \in \mathbb{Q}[X] \mid g' \in \mathbb{Q}[X] \}$$

$\cap$ $\cup$ "$\cup$": $f((X^2-6)g') = \underbrace{((\sqrt{6})^2-6)}_{0} g'(\sqrt{6}) = 0$

"$\cap$": $\ker f \subseteq (X^2-6)$. $\quad (X-\sqrt{6})(X+\sqrt{6}) = X^2-6$

$g(\sqrt{6}) = 0 \Rightarrow g = (X^2-6)g'$

$\sqrt{6}$ est une racine de g. $\Leftrightarrow$ $X-\sqrt{6} \mid g$

(dans $\mathbb{R}$) $\qquad$ $\mathbb{R}[X]$

$$g(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$$

$$g(\sqrt{6}) = a_n (\sqrt{6})^n + a_{n-1} (\sqrt{6})^{n-1} + \cdots + a_0$$

$$= \sum_{i \text{ pair}} a_i (\sqrt{6})^i + \sum_{j \text{ impair}} a_j (\sqrt{6})^j$$

$$= 0 \Rightarrow \quad 0 \qquad\qquad 0$$

$$g(-\sqrt{6}) = \sum_{i \text{ pair}} a_i (\sqrt{6})^i - \sum_{j \text{ impair}} a_j (\sqrt{6})^j$$

$$= 0$$

$(X + \sqrt{6}) \mid g$ dans $\mathbb{R}[X]$

$(X - \sqrt{6})(X + \sqrt{6}) \mid g$ dans $\mathbb{R}[X]$

$\Downarrow$

$(X^2 - 6) \mid g$ dans $\mathbb{Q}[X]$

$(X^2 - 6) g' = g$ dans $\mathbb{Q}[X]$.

dans $\mathbb{R}[X]$

$$\mathbb{Q} + \mathbb{Q}\sqrt{6} \cong \mathbb{Q}[X] / (X^2 - 6)$$

$K[X]$

$\mathbb{C}[X]$ $\mathbb{Q}[X]$ $\mathbb{R}[X]$ $\mathbb{Z}$

$a = bk + r$

$a = bk + r$ $\quad 0 \leq r < b$

$0 \leq \deg r < \deg b$

$ab = 0 \Rightarrow a = 0$ ou $b = 0$

(anneaux intègres)

anneaux euclidien $\Rightarrow$ anneau principal $\Rightarrow$ anneau factoriel

$\forall I$ idéal

$I = (a)$

$(a) = \{ka \mid k \in A\}$

Ex12. Définir un isomorphisme d'anneaux

$$\mathbb{R}[X]/(X^4-1) \xrightarrow{\sim} \mathbb{R} \times \mathbb{R} \times \mathbb{C}$$

$\text{pgcd}(m,n) = 1$ $\qquad \mathbb{Z}/mn\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

$a \bmod mn \longmapsto (a \bmod m, a \bmod n)$

$X^4 - 1 = (X^2-1)(X^2+1) = (X-1)(X+1)(X^2+1)$ dans $\mathbb{R}[X]$

$\mathbb{R}[X]/(X^4-1) \xrightarrow{\sim} \mathbb{R}[X]/(X-1) \times \mathbb{R}[X]/(X+1) \times \mathbb{R}[X]/(X^2+1)$

$\mathbb{R}[X]/(X-1) \longrightarrow \mathbb{R}$

$r \longmapsto r$

$\mathbb{R}[X]/(X^2+1) \longrightarrow \mathbb{C}$

$\mathbb{R} + \mathbb{R}i$

$\mathbb{R}[X] \xrightarrow{ev_1} \mathbb{R}$

$g(X) \longmapsto g(1)$

$\mathbb{Q}[X]/(X^2-6) \longrightarrow \mathbb{Q} + \mathbb{Q}\sqrt{6}$

$\ker(ev_1) = (X-1)$

Thm d'homomorphisme : $\mathbb{R}[X]/\ker ev_1 \simeq \operatorname{Im} ev_1$

$\mathbb{R}$

Ex 14

$\mathbb{R}[X]/(X-1)$ $\quad \mathbb{Z}/n\mathbb{Z}$.

$\mathbb{Z}/(n)$

$\mathbb{R}[X]/(X-1)\mathbb{R}[X]$

$\mathbb{F}_3$

$f = X^3 - X + 1 \in \mathbb{F}_3[X]$

$\mathbb{Z}/3\mathbb{Z}$

$\{0, 1, 2\}$ $\quad \mathbb{F}_3[X] \to \mathbb{F}_3[X]/(f)$ $\quad \alpha = X + (f)$

$x \mapsto \alpha$

$\bar{X}^3 - \bar{X} + \bar{1} = \bar{0}$

$\mathbb{Z}/9\mathbb{Z}$

$\bar{3} = \bar{12}$

1. $\Leftrightarrow$ f est irréductible.

$(X-a) \mid f \Leftrightarrow f(a) = 0$

$f(0) \neq 0 \quad f(1) \neq 0 \quad f(2) \neq 0$

f n'a pas de racines dans $\mathbb{F}_3$.

f est irréductible (parce que $\deg f = 3$.)

$K[X]/(f)$ un espace vectoriel de dimension $= \deg f$.

sur K.

$\{1, X, X^2, \dots, X^{\deg f - 1}\}$ forme une base.

$\{1, \alpha, \alpha^2\}$

$\{ a_0 + a_1\alpha + a_2\alpha^2 \mid a_0, a_1, a_2 \in \mathbb{F}_3 \}$.

$3 \times 3 \times 3 = 27$

2. $|K^*| = 27 - 1 = 26$

$a \in K^*$ $\quad a^n = 1$

Thm de Lagrange. $\quad a^{|K^*|} = 1$.

ordre $(a) \mid 26$

ord $(a) = 1, 2, 13, 26$.

$\{1\}$ $\quad \{2\}$ $a^2 = 1$, $a \neq 1$ $\Downarrow$ $a^2 - 1 = 0$, $(a-1)(a+1) = 0$, $a + 1 = 0$

13, 26 : les éléments qui ne sont pas dans $\mathbb{F}_3$.

3. $\alpha^{13} \neq 1$.

$\alpha^3 - \binom{3}{1}\alpha^2 + \binom{3}{2}\alpha - 1^3$ (dans $\mathbb{F}_3$: $\binom{3}{1} = 0$; dans $\mathbb{F}_3$: $\binom{3}{2} = 0$)

$\alpha^3 - \alpha + 1 = 0$ // dans $\mathbb{F}_3[X]/(f)$

$\alpha^3 = \alpha - 1$

$$\alpha^4 = (\alpha^3)^3 = (\alpha-1)^3 = \alpha^3 - 1$$
$$= \alpha + 1$$

$$\alpha^{12} = \alpha^9 \cdot \alpha^3 = (\alpha+1)(\alpha-1) = \alpha^2 - 1$$

$$\alpha^{13} = \alpha^{12} \cdot \alpha = (\alpha^2-1)\alpha = \alpha^3 - \alpha = -1$$

Points importants algèbre

① définitions.

② analogie entre $K[X]$ et $\mathbb{Z}$.

($K[X]/(f)$ et $\mathbb{Z}/(n)$ $\mathbb{Z}/n\mathbb{Z}$).

③. (1) Savoir décider si une application donnée est un morphisme de groupes / anneaux (ou éventuellement un isomorphisme!)

a) morphisme + bijectif

b) Thm d'homomorphisme.

2) décider si deux groupes (anneaux) sont isomorphes ou pas, et pourquoi.

No : définir une application
montrer que c'est un morphisme, bijectif.

n'est pas un iso : e.g. . trouver un élément d'ordre n dans A mais pas dans B

A n'est pas isomorphe à B.

- A est cyclique. B n'est pas cyclique.
- $|A| \neq |B|$.

3) décider si un groupe concret est cyclique ou pas, trouver tous les générateurs.

$|G|$

a est un générateur de G

ssi $\text{ordre}(a) = |G|$.

$\Leftrightarrow$ $a^{\frac{|G|}{p}} \neq e$ où p est un diviseur premier de $|G|$.

$a^{k_1} = e \Rightarrow a^{k_1 k_2} = e$.

4) Savoir déterminer l'ordre de a^m à partir de l'ordre de a.

(Si on note l'ordre $(a) = d$.)

$$(a^m)^k = e$$

(e.g. Ex 1) Feuille 7)

$$a^{mk} = e \Rightarrow d \mid mk$$

k le plus petit.

$mk = \text{PPCM}(m, d)$.

$$k = \frac{\text{PPCM}(m,d)}{m} = \frac{d}{\text{PGCD}(m,d)}$$

réductible ?

$\mathbb{Z}$ est un groupe cyclique engendré par 1 (ou -1)

$1 + 1 \dots + 1$ (n fois.)

$\mathbb{Z}/n\mathbb{Z}$.

$(-1) + (-1) + \dots + (-1)$

1 fois

$\mathbb{Z}^2$. $(1,0)$ $(0,1)$

G/H $\quad aH$

aH.

$abH = (aH).(bH)$

$(\mathbb{Z}/23\mathbb{Z})^*$ $\quad 22 = 2 \times 11$.

$a^{22} = 1 \mod 23$

$(-1)^{22} = 1$. $\quad a^2 \neq 1$ et $a^{11} \neq 1$.

"module" sur un anneau.

$\mathbb{Z} \oplus \mathbb{Z}$. $\quad \mathbb{Z}^2$.

$(1,0)$

(cont)

$\{a\}, \{b\}, \{c\}$.

$\mathbb{Z}^2$

$\{b\}$

$\{(0,1), (1,0)\}$ $\{(1,0), (0,-1)\}$

$\mathbb{Z}/n\mathbb{Z}$.

"1"

"-1"

$(\mathbb{Z}/n\mathbb{Z})^*$ cyclique ou pas?

Voir 5.5 du poly.

$\mathbb{Z}$ $\mathbb{Z}/n\mathbb{Z}$

$K(X)$.