

Correction examen: Algèbre et arith.

Exercice 1

a/ Soit G un groupe d'ordre 4 (noté multiplicativement).
 et soit $G = \{e, a_1, a_2, a_3\}$ avec e : élément neutre du groupe G .
 On sait d'après le thm de Lagrange que l'ordre a_1 , l'ordre a_2 ,
 l'ordre de a_3 divise l'ordre du groupe G i.e., divise 4.
 deux cas se présentent :

1^{er} cas:

L'un des éléments, disons a_1 est d'ordre 4
 dans ce cas on a $G = \langle a_1 \rangle = \{a_1, a_1^2, a_1^3, a_1^4 = e\}$

$\Rightarrow G \simeq \mathbb{Z}_4 = \langle \bar{1} \rangle = \{\bar{1}, \bar{2}, \bar{3}, \bar{0}\}$ (G : cyclique d'ordre 4)

2^{ème} cas

Tous les éléments a_1, a_2, a_3 sont d'ordres 2, dans ce cas
 $a_1^2 = a_2^2 = a_3^2 = e$. la table du groupe est de la forme

	e	a_1	a_2	a_3
e	e	a_1	a_2	a_3
a_1	a_1	e	a_3	a_2
a_2	a_2	a_3	e	a_1
a_3	a_3	a_2	a_1	e

Ce groupe (dit groupe de Klein) est non-cyclique
 est isomorphe au groupe $\mathbb{Z}_2 \times \mathbb{Z}_2$
 avec $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1})\}$

b/ si $(G:H) = 2 \Rightarrow (G/H)_g = \{H, G \setminus H\} = (G/H)$
 deux classes seulement: H et $G \setminus H$

et on a $\forall x \in G, xH = Hx = G \setminus H$ si $x \in G \setminus H \Rightarrow H \triangleleft G$.
 et $xH = Hx = H$ si $x \in H$

Pour $H = \langle (123) \rangle = \{(123), (132), (1)\}$ et $|S_3| = 3! = 6$
 $\Rightarrow (S_3:H) = \frac{|S_3|}{|H|} = \frac{6}{3} = 2 \Rightarrow H = \langle (123) \rangle \triangleleft S_3$

et on a $S_3/H = \{H, G \setminus H\} = \{\langle (123) \rangle, S_3 - \langle (123) \rangle\}$
 $= \{\langle (123) \rangle, \{(1, 2, 3)\}\}$

①

Exercice 2

a/ Montrons que $\bar{a} = a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ est inversible $\Leftrightarrow \text{pgcd}(a, n) = 1$.

Si $\bar{a}$ est inversible $\Rightarrow \exists \bar{b} \in \mathbb{Z}/n\mathbb{Z}$ tq $\bar{a} \odot \bar{b} = \bar{1}$

$$\Rightarrow \overline{a \times b} = \bar{1} \Rightarrow \exists k \in \mathbb{Z} \quad a \times b - 1 = k \cdot n$$

$$\Rightarrow a \times b - k \cdot n = 1 \Rightarrow \text{pgcd}(a, n) = 1$$

avec $u = b$ et $v = -k$.

Inversement, si $\text{pgcd}(a, n) = 1 \Rightarrow \exists u, v \in \mathbb{Z} : au + nv = 1$

Par passage aux classes, on obtient: $\overline{au + nv} = \bar{1}$

$$\Rightarrow \overline{au} \oplus \overline{nv} = \bar{1} \Rightarrow \bar{a} \odot \bar{u} = \bar{1} \quad (\text{car } \overline{nv} = \bar{0})$$

$$\Rightarrow \bar{a}^{-1} = \bar{u}$$

- Calcul de $\bar{g}^{-1}$ dans $\mathbb{Z}/11\mathbb{Z}$.

par Alg. d'Euclide et Euclide étendu

On a

$$11 = 9 \times 1 + 2$$

$$9 = 2 \times 4 + 1$$

$$\Rightarrow 1 = 9 - 2 \times 4$$

$$= 9 - (11 - 9 \times 1) \times 4$$

$$= 9 - 11 \times 4 + 9 \times 4 = 5 \times 9 + 11 \times (-4)$$

$$\Rightarrow \overline{5 \times 9 + 11 \times (-4)} = \bar{1}$$

$$= \bar{5} \odot \bar{9} + \bar{0} = \bar{5} \odot \bar{9} \quad (\text{car } \overline{11 \times 4} = \bar{0})$$

$$\Rightarrow \bar{9}^{-1} = \bar{5}, \text{ En effet } \bar{9} \odot \bar{5} = \overline{45} = \bar{1} \quad [11] = \bar{0}$$

b/ Résolution de l'équation $ax \equiv b [n]$

In first, On calcul $\text{pgcd}(a, n)$

* If $\text{gcd}(a, n) = 1 \Rightarrow$ There is exactly one solution

we find c such that $\bar{a} \odot \bar{c} = \bar{1} \Rightarrow \bar{a}^{-1} = \bar{c}$

$$\Rightarrow x \equiv \bar{a}^{-1} \odot \bar{b} = \bar{c} \odot \bar{b}$$

(To find c use the extended Euclidean Algorithm

to compute $\text{gcd}(a, n) = 1 \Rightarrow \exists u, v \in \mathbb{Z} : au + nv = 1$

$$\Rightarrow \overline{au} \oplus \bar{0} = \bar{1} \Rightarrow \bar{a} \odot \bar{u} = \bar{1} \Rightarrow \bar{c} = \bar{u}$$

* Si $\text{pgcd}(a, n)$ ne divise pas b alors l'équation n'admet pas de solutions, car l'équation: $ax \equiv b [n]$ sur $\mathbb{Z}/n\mathbb{Z}$ est équivalente à l'équation: $ax - b = k \cdot n, k \in \mathbb{Z}$
 $\Leftrightarrow ax + kn = b$, donc il faut que $\text{pgcd}(a, n) \mid b$

* Si $\text{pgcd}(a, n) = g \neq 1$ avec $g \mid b$ then there are g solutions
Infirist,

On divise l'équation $ax \equiv b [n]$ par g

ce $a' = \frac{a}{g}, b' = \frac{b}{g}, n' = \frac{n}{g}$

et on obtient $a'x' \equiv b' [n']$ (*) ($\text{pgcd}(a', n') = 1$)
 Si x' est solution de l'équation * $\Rightarrow \bar{a'}^{-1}$ existe

les autres solutions sont: $x \leftarrow x' + i n'$ for $0 \leq i < g$.

c/ On a $143 = 11 \times 13$ par suite l'équation 2) $11x \equiv 3 \pmod{143}$
 on a $\text{pgcd}(11, 143) = 11$ et $11 \nmid 3$ donc l'équation n'admet pas de solutions.

- L'équation $7x \equiv 3 \pmod{143}$ admet une seule solution
 car $\text{pgcd}(7, 143) = 1$ et $1 \mid 3$

On a $x \equiv \bar{7}^{-1} \otimes \bar{3} \pmod{143}$

(On a $143 = 7 \times 20 + 3 \Rightarrow 1 = 7 - 3 \times 2$
 $7 = 3 \times 2 + 1 \Rightarrow 1 = 7 - (143 - 7 \times 20) \times 2$
 $= 7 - 143 \times 2 + 7 \times 20 \times 2$
 $= 41 \times 7 - 143 \times 2$

alors $x \equiv 41 \otimes 3 [143] = 123 [143] \checkmark$
 $\Rightarrow \bar{7}^{-1} = \bar{41}$

3/ l'équation $11x \equiv 22 \pmod{143}$ admet 11 solutions

Exercice 3

a/ Soit $m, n \in \mathbb{N}^*$. On a $m\mathbb{Z} + n\mathbb{Z} = \{mk + nl \mid k, l \in \mathbb{Z}\}$ est un s/gpe de $\mathbb{Z}$. En effet, $m\mathbb{Z} + n\mathbb{Z} \neq \emptyset$ car $0, m, n, \dots \in m\mathbb{Z} + n\mathbb{Z}$. Et si $x = mk_1 + nl_1, y = mk_2 + nl_2 \in m\mathbb{Z} + n\mathbb{Z}$

$$\begin{aligned} \text{On a bien } x + (-y) &= (mk_1 + nl_1) - (mk_2 + nl_2) \\ &= m(k_1 - k_2) + n(l_1 - l_2) \in m\mathbb{Z} + n\mathbb{Z} \end{aligned}$$

Donc $m\mathbb{Z} + n\mathbb{Z}$ est un s/gpe de $\mathbb{Z}$.

Comme tout s/gpe de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$,

Soit que $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$, On montre que $d = \text{pgcd}(m, n)$.

Tout d'abord, $m \in m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z} \Rightarrow m \in d\mathbb{Z}$

$$\Rightarrow m = dk, k \in \mathbb{Z} \Rightarrow d \mid m.$$

De même, $n \in m\mathbb{Z} + n\mathbb{Z} \Rightarrow n \in d\mathbb{Z} \Rightarrow n = dt, t \in \mathbb{Z}$

$$\Rightarrow d \mid n.$$

Soit $d' \in \mathbb{Z}$ tq $d' \mid n$ et $d' \mid m \Rightarrow n = d'n_1$ et $m = d'm_1$

$$\text{On a donc } m\mathbb{Z} + n\mathbb{Z} = d'm_1\mathbb{Z} + d'n_1\mathbb{Z} = d'\mathbb{Z}$$

$$\Rightarrow d'(m_1\mathbb{Z} + n_1\mathbb{Z}) = d'\mathbb{Z} \Rightarrow d' \in d\mathbb{Z} \Rightarrow d' \mid d$$

donc d est le plus grand diviseur de m et n

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

* calcul $\text{pgcd}(726, 275)$ et $u, v \in \mathbb{Z}$: $726u + 275v = \text{pgcd}(726, 275)$

$$726 = 275 \times 2 + 176$$

$$\Rightarrow \text{pgcd}(726, 275) = 11$$

$$275 = 176 \times 1 + 99$$

$$11 = 77 - 22 \times 3$$

$$176 = 99 \times 1 + 77$$

$$= 77 - (99 - 77) \times 3$$

$$99 = 77 \times 1 + 22$$

$$= 77 \times 4 - 99 \times 3$$

$$77 = 22 \times 3 + 11$$

$$= (176 - 99) \times 4 - 99 \times 3$$

$$22 = 11 \times 2$$

$$= 176 \times 4 - 7 \times 99$$

$$= 176 \times 4 - (275 - 176) \times 7 = 176 \times 11 - 275 \times 7$$

$$= (726 - 275 \times 2) \times 11 - 275 \times 7 = 11 \times 726 + (-29) \times 275$$

$$\textcircled{4} \Rightarrow \boxed{m = 11, n = -29}$$

b/ On suppose que $\text{pgcd}(m, n) = 1 \Rightarrow \exists u, v \in \mathbb{Z} \text{ t.q. } mu + nv = 1.$

On pose $m_1 = mu$ et $n_1 = nv$ et soit $x = x_1 n_1 + x_2 m_1$
 $x = x_1 nv + x_2 mu.$

On a $x[m] \equiv x_1 nv$ mais comme $nv = 1 - mu$

$$\Rightarrow x[m] \equiv x_1(1 - mu)[m] \equiv x_1[m]$$

De même, $x[n] \equiv x_2 mu[n]$ mais $mu = 1 - nv$

$$\text{donc } x_2 mu[n] \equiv x_2(1 - nv)[n] \equiv x_2[n]$$

Dnc $\begin{cases} x \equiv x_1[m] \\ \text{et } x \equiv x_2[n] \end{cases}$ est solution
du système
en question.

Pour $m=5, n=7$

$$\begin{aligned} \text{on a } 7 &= 5 \times 1 + 2 & 1 &= 5 - 2 \times 2 \\ 5 &= 2 \times 2 + \boxed{1} \uparrow & &= 5 - (7-5) \times 2 = 3 \times 5 - 7 \times 2 \\ & & \Rightarrow & \boxed{u=3, v=-2} \end{aligned}$$

$$\text{On pose } m_1 = mu = 5 \times 3 = 15$$

$$n_1 = nv = 7(-2) = -14$$

$$\text{et soit } x = n_1 x_1 + x_2 m_1 = -14 \times 1 + 2 \times 15 \\ = 30 - 14 = 16$$

$$\text{et on a bien } \begin{aligned} 16[5] &\equiv 1[5] \\ 16[7] &\equiv 2[7] \end{aligned} \quad \text{i.e. } \begin{cases} 16 \equiv 1[5] \\ 16 \equiv 2[7] \end{cases}$$

(5)