Feuille de TD n° 7

Groupes $\mathbb{Z}/n\mathbb{Z}$, géométrie

15 avril 2022

Pour commencer . . .

Exercice 1.
Décrire (cardinal, commutatif ou non, cyclique ou non, ordre des éléments) les groupes suivants :

1. $\mathbb{Z}/7\mathbb{Z}$
2. $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
3. $\mathbb{Z}/8\mathbb{Z}$
4. $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/8\mathbb{Z}$ sont-ils isomorphes ?

---

1. C'est un groupe à 8 éléments. Il est commutatif. Il est cyclique, car engendré par $\overline{1}$.
   Il a 1 élément d'ordre 1, et 6 élément d'ordre 7.
2. C'est un groupe à 8 éléments. Il est commutatif.
   Il a 1 élément d'ordre 1, 3 éléments d'ordre 2, 4 éléments d'ordre 4.
   Ce groupe n'est donc pas cyclique, car il ne possède pas d'éléments d'ordre 8.
3. C'est un groupe à 8 éléments. Il est commutatif. Il est cyclique, car engendré par $\overline{1}$.
   Il a 1 élément d'ordre 1, 1 élément d'ordre 2, 2 éléments d'ordre 4, 4 éléments d'ordre 8.
4. Non, l'un a des éléments d'ordre 8 et l'autre n'en a pas.

Exercice 2. Soit $n \geq 2$.

1. Calculer $\overline{2.3.5.7}$ dans $\mathbb{Z}/9\mathbb{Z}$.
2. Calculer $(\overline{3})^{6^{30}}$ et $(\overline{2})^{7^5}$ dans $\mathbb{Z}/10\mathbb{Z}$.
3. Soit $n \geq 2$.
   Calculer $\sum_{x\in\mathbb{Z}/n\mathbb{Z}} x$.
4. On suppose que n n'est pas un nombre premier.
   Calculer $\Pi_{x\in\mathbb{Z}/n\mathbb{Z}\, x\neq\overline{0}} x$.

---

1. Dans $\mathbb{Z}/9\mathbb{Z}$, on a $\overline{2.3.5.7} = \overline{2.3.(-4).(-2)} = \overline{6.8} = \overline{6.(-1)} = \overline{-6} = \overline{3}$.
2. Dans $\mathbb{Z}/10\mathbb{Z}$, on a $\overline{3}^2 = \overline{9} = \overline{-1}$. Donc, $\overline{3}^4 = \overline{1}$.
   Ainsi, on a $\overline{3}^{4n} = \overline{1}$.
   On regarde donc 6^{30} modulo 4.
   Dans $\mathbb{Z}/4\mathbb{Z}$, on a $\overline{6}^3 0 = \overline{0}$.
   Donc, $\overline{3}^{6^{30}} = \overline{1}$.
   Dans $\mathbb{Z}/10\mathbb{Z}$, on a $\overline{2}^2 = \overline{4}$, $\overline{2}^3 = \overline{8}$, $\overline{2}^4 = \overline{4}$, $\overline{2}^5 = \overline{32} = \overline{2}$.
   Ainsi, la suite des $(\overline{2}^m)_{m\geq 1}$ est périodique de période 4.
   On regarde donc 7^5 modulo 4.
   Dans $\mathbb{Z}/4\mathbb{Z}$, on a $\overline{7}^5 = \overline{3}^5 = \overline{(-1)}^5 = \overline{-1} = \overline{3}$.
   Donc, $\overline{2}^{7^5} = \overline{2}^3 = \overline{8}$.
3. C'est une somme finie, de n termes.
   On a $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$.
   Si n est impair, cet entier est divisible par n, donc il est congru à 0 modulo n.
   Ainsi, $\sum_{x\in\mathbb{Z}/n\mathbb{Z}} x = \overline{0}$.
   Si n est pair, on a $\frac{n(n+1)}{2} = n\frac{n}{2} + \frac{n}{2}$. Comme n est pair, on a $n|n\frac{n}{2}$, donc $\frac{n(n+1)}{2}$ est congru à $\frac{n}{2}$ modulo n.
   Ainsi, $\sum_{x\in\mathbb{Z}/n\mathbb{Z}} x = \overline{n/2}$.
   Autre méthode : Pour tout $k \in \mathbb{Z}$, on a $\overline{n-k} = -\overline{k}$.
   Si n est impair, l'opposé de $\overline{k} \in \{\overline{1}, \ldots, \overline{\frac{n-1}{2}}\}$ est $\overline{n-k} \in \{\overline{\frac{n-1}{2}+1}, \ldots, \overline{n-1}\}$.
   On écrit $\sum_{x\in\mathbb{Z}/n\mathbb{Z}} x = \overline{0} + \sum_{k=1}^{\frac{n-1}{2}} \overline{k} + \sum_{m=\frac{n-1}{2}+1}^{n-1} \overline{m} = \sum_{k=1}^{\frac{n-1}{2}} \overline{k} - \overline{k} = \overline{0}$.
   Si n est pair, l'opposé de $\overline{k} \in \{\overline{1}, \ldots, \overline{\frac{n}{2}-1}\}$ est $\overline{n-k} \in \{\overline{\frac{n}{2}+1}, \ldots, \overline{n-1}\}$. Par contre, l'opposé de $\overline{n/2}$ est $\overline{n/2}$.
   On a donc $\sum_{x\in\mathbb{Z}/n\mathbb{Z}} x = \overline{0} + \sum_{k=1}^{\frac{n}{2}-1} \overline{k} + \overline{n/2} + \sum_{m=\frac{n}{2}+1}^{n-1} \overline{m} = \overline{n/2} + \sum_{k=1}^{n/2-1} \overline{k} - \overline{k} = \overline{n/2}$.
4. Si n n'est pas premier, on a $n = ab$ avec $2 \leq a, b < n$. Donc, $a \times b$ divise $(n-1)!$. Donc, n divise $(n-1)!$.
   Ainsi, $\Pi_{x\in\mathbb{Z}/n\mathbb{Z}\, x\neq\overline{0}} x = \overline{(n-1)!} = \overline{0}$.

Exercice 3.

1. Développer $(x^2 + x - \overline{1})(x^2 - x - \overline{1})$ et $(x^2 + \overline{2})(x^2 - \overline{2})$ dans $\mathbb{Z}/3\mathbb{Z}$.
2. Développer $(x^2 + x - \overline{1})(x^2 - x - \overline{1})$ et $(x^2 + \overline{2})(x^2 - \overline{2})$ dans $\mathbb{Z}/5\mathbb{Z}$
   Que remarque-t-on ?

1. On a $(x^2+x-\overline{1})(x^2-x-\overline{1}) = x^4+\overline{1}$ et $(x^2+\overline{2})(x^2-\overline{2}) = x^4-\overline{1}$
2. On a $(x^2+x-\overline{1})(x^2-x-\overline{1}) = x^4+2\overline{x}^2+\overline{1}$ et $(x^2+\overline{2})(x^2-\overline{2}) = x^4+\overline{1}$.
   On a des produits de polynômes de degré 2 qui donnent des résultats différents selon l'ensemble $\mathbb{Z}/n\mathbb{Z}$ choisi.

Exercice 4.
Soient $a, b, c \in \mathbb{Z}$.

1. Trouver des valeurs de a, b, c telles que $ax+by=c$ n'ait pas de solutions dans $\mathbb{Z}$, mais telles que $\overline{a}\overline{x}+\overline{b}\overline{y}=\overline{c}$ ait des solutions dans $\mathbb{Z}/n\mathbb{Z}$, pour un certain $n \geq 2$.
2. Soit $n \geq 2$. On s'intéresse à l'équation $\overline{a}\overline{x}+\overline{b}\overline{y}=\overline{c}$ dans $\mathbb{Z}/n\mathbb{Z}$.
   Si $pgcd(a,n)=1$, montrer que l'équation possède n solutions, que l'on écrira.
3. Si $pgcd(b,n)=1$, montrer que l'équation possède n solutions, que l'on écrira.
4. On suppose que $pgcd(a,n) \neq 1$ et que $pgcd(b,n) \neq 1$. Soit $d = pgcd(a,b,n)$. Montrer que si d ne divise pas c, alors l'équation n'admet pas de solutions dans $\mathbb{Z}/n\mathbb{Z}$.
5. Donner un exemple.

1. $7x+7y=5$ n'a pas de solutions dans $\mathbb{Z}$, mais $\overline{x}+\overline{y}=\overline{1}$ a des solutions dans $\mathbb{Z}/2\mathbb{Z}$.
2. Si $pgcd(a,n)=1$, on a vu d'après le cours que $\overline{a}$ possède un inverse pour $\times$ dans $\mathbb{Z}/n\mathbb{Z}$. Cet inverse existe d'après le théorème de Bézout, et il se calcule avec l'algorithme d'Euclide étendu.
   Posons $\overline{a'}$ l'inverse de $\overline{a}$ pour $\times$. Alors, on a
   $\overline{a}\overline{x}+\overline{b}\overline{y}=\overline{c} \Leftrightarrow \overline{a'}(\overline{a}\overline{x}+\overline{b}\overline{y}) = \overline{a'}\overline{c}$
   $\Leftrightarrow \overline{x}+\overline{a'b}\overline{y} = \overline{a'c}$
   $\Leftrightarrow \overline{x} = \overline{a'c}-\overline{a'b}\overline{y}$. Donc, cette équation possède des solutions.
   L'ensemble des solutions est $\{(\overline{a'c}-\overline{a'b}\overline{y}, \overline{y}), \overline{y} \in \mathbb{Z}/n\mathbb{Z}\}$. On a donc exactement n solutions.
3. Si $pgcd(b,n)=1$, on obtient un résultat similaire en utilisant $\overline{b'}$ l'inverse de $\overline{b}$ pour $\times$.
4. On "remonte" dans $\mathbb{Z}$:
   On a $\overline{a}\overline{x}+\overline{b}\overline{y}=\overline{c}$ ssi il existe $k \in \mathbb{Z}$ tel que $ax+by+kn=c$.
   Comme $d = pgcd(a,b,n)$, cela implique que $d|ax+by+kn=c$.
   Ainsi, si d ne divise pas c, l'équation n'a pas de solutions dans $\mathbb{Z}/n\mathbb{Z}$.
   L'équation $\overline{6}\overline{x}+\overline{12}\overline{y}=\overline{5}$ n'a donc pas de solutions dans $\mathbb{Z}/10\mathbb{Z}$.

Exercice 5. 1. Résoudre l'équation diophantienne modulaire : $x \equiv 4 \bmod (6)$ et $x \equiv 7 \bmod 11$.

Trouver un isomorphisme entre les groupes suivants :

1. $\mathbb{Z}/15\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.
2. $\mathbb{Z}/100\mathbb{Z}$ et $\mathbb{Z}/4Z \times \mathbb{Z}/25\mathbb{Z}$

On écrira à chaque fois ϕ et sa bijection réciproque ϕ^{-1}.

1. On utilise le théorème d'isomorphisme chinois.
   On recherche d'abord une solution particulière x_0.
   Les entiers 6 et 11 sont premiers entre eux.
   On trouve comme relation de Bézout : $2.6-11=1$.
   Ainsi, une solution particulière est $x_0 = 4.(-11)+7.(12) = -44+84 = 40$.
   On a donc : ($x \equiv 4 \bmod (6)$ et $x \equiv 7 \bmod 11$) ssi $x \equiv 40 \bmod (66)$.
   Donc, l'ensemble des solutions est $40+66\mathbb{Z}$.
2. On a $\phi(\widehat{c}) = (\overline{c}, \tilde{c})$ et $\phi^{-1}(\overline{a}, \tilde{b}) = \widehat{10a+6b}$.
   Pour déterminer ϕ^{-1} il faut déterminer l'image de $(\overline{1}, \tilde{0})$ et $(\overline{0}, \tilde{1})$ (ici $\overline{10}$ et $\overline{6}$).
   On les détermine soit en testant certaines valeurs, soit avec l'algorithme d'Euclide.
   Comme on a $2.3+(-1).5=1$, on obtient d'après le cours les valeurs de $\widehat{-5} = \widehat{10}$ et $\widehat{6}$ dans $\mathbb{Z}/15\mathbb{Z}$.
3. On a $\phi(\widehat{c}) = (\overline{c}, \tilde{c})$ et $\phi^{-1}(\overline{a}, \tilde{b}) = \widehat{76a+25b}$.
   Pour déterminer ϕ^{-1} il faut déterminer l'image de $(\overline{1}, \tilde{0})$ et $(\overline{0}, \tilde{1})$ (ici $\widehat{76}$ et $\widehat{25}$).
   On les détermine soit en testant certaines valeurs, soit avec l'algorithme d'Euclide.
   Comme on a $1.25+(-6).4=1$, on obtient d'après le cours les valeurs de $\widehat{-24} = \widehat{76}$ et $\widehat{25}$ dans $\mathbb{Z}/100\mathbb{Z}$.

■ *Un peu de Géométrie . . .*

Exercice 6. On considère le plan affine muni d'un repère orthonormé $\left(O, \overrightarrow{i}, \overrightarrow{j}\right)$. On définit deux droites par une équation cartésienne :

$$(D_1) \ : \ 2x-y+1=0 \quad \text{et} \quad (D_2) \ : \ x+y+5=0.$$

1. Déterminer une équation cartésienne de la droite (D) passant par le point d'intersection de (D_1) et (D_2), ainsi que par le point A de coordonnées $(-1, 2)$.
2. Déterminer la distance du point $M\,(2, 3)$ à la droite (D).

---

1. On commence par déterminer le point d'intersection I des deux droites. Pour cela, on résout
$$\left\{\begin{array}{rl} 2x-y+1 &= 0 \\ x+y+5 &= 0 \end{array}\right. \iff \left\{\begin{array}{rl} y &= 2x+1 \\ 3x+6 &= 0 \end{array}\right. \iff \left\{\begin{array}{rl} y &= -3 \\ x &= -2 \end{array}\right. .$$
Le point d'intersection est donc $I\,(-2, -3)$. Il reste à déterminer a, b, $c \in \mathbb{R}$ tels que
$$\left\{\begin{array}{rl} a(-1)+b(2)+c &= 0 \\ a(-2)+b(-3)+c &= 0 \end{array}\right. \iff \left\{\begin{array}{rl} -7a+5c &= 0 \\ -7b-c &= 0 \end{array}\right. .$$
On choisit $c = 7$ et on obtient l'équation cartésienne $5x - y + 7 = 0$ pour la droite (D).
2. Un vecteur directeur de (D) est $\overrightarrow{u}$ de coordonnées $(-1, -5)$. Le projeté orthogonal de $\overrightarrow{OM}$ sur (D) est le point P tel que
$$\overrightarrow{OP} = \frac{\overrightarrow{OM}\cdot\overrightarrow{u}}{\|\overrightarrow{u}\|^2}\overrightarrow{u} = \frac{-13}{26}\overrightarrow{u} = -\frac{1}{2}\overrightarrow{u}.$$
On obtient grâce à Pythagore
$$\mathrm{d}(M, D) = \left\|\overrightarrow{MP}\right\| = \sqrt{\left\|\overrightarrow{OM}\right\|^2 - \left\|\overrightarrow{OP}\right\|^2} = \sqrt{13 - \frac{26}{4}} = \sqrt{\frac{13}{2}}.$$

Exercice 7 (Lignes de niveau)**.**

1. Soient A, B et C trois points non alignés du plan. Soit G l'isobarycentre de A, B et C (le centre de gravité du triangle ABC).
   (a) Montrer que pour tout point M du plan,
   $$MA^2 + MB^2 + MC^2 = 3MG^2 + GA^2 + GB^2 + GC^2.$$
   (b) En déduire une expression de $GA^2 + GB^2 + GC^2$ en fonction des longueurs AB, AC et BC.
   (c) Soit $k \in \mathbb{R}$, quel est l'ensemble des points M du plan tels que $MA^2 + MB^2 + MC^2 = k$?
2. Soient A et B deux points du plan et soit $k \in \mathbb{R}$. Déterminer l'ensemble des points M du plan tels que $AM = kBM$.
   Indication : Dans le cas où $k \neq 1$, mettre l'égalité au carré et introduire le barycentre G de $\left\{(A, 1),\, (B, -k^2)\right\}$.

---

1. (a) On a d'abord
   $$\begin{aligned} MA^2 = \overrightarrow{MA}\cdot\overrightarrow{MA} &= \left(\overrightarrow{MG}+\overrightarrow{GA}\right)\cdot\left(\overrightarrow{MG}+\overrightarrow{GA}\right) \\ &= MG^2 + 2\overrightarrow{MG}\cdot\overrightarrow{GA} + GA^2. \end{aligned}$$
   On écrit la même chose pour MB^2 et MC^2, et on obtient
   $$MA^2+MB^2+MC^2 = 3MG^2+GA^2+GB^2+GC^2+2\overrightarrow{MG}\cdot\left(\overrightarrow{GA}+\overrightarrow{GB}+\overrightarrow{GC}\right).$$
   Or $\overrightarrow{GA}+\overrightarrow{GB}+\overrightarrow{GC} = 0$, ce qui donne le résultat.
   (b) On utilise la précédente formule avec $M = A$, $M = B$ et $M = C$ et on somme :
   $$2\left(AB^2 + AC^2 + BC^2\right) = 3AG^2 + 3BG^2 + 3CG^2 + 3\left(GA^2 + GB^2 + GC^2\right),$$
   c'est-à-dire
   $$GA^2 + GB^2 + GC^2 = \frac{1}{3}\left(AB^2 + AC^2 + BC^2\right).$$
   (c) Finalement,
   $$MA^2 + MB^2 + MC^2 = k \iff 3MG^2 = k - \frac{1}{3}\left(AB^2 + AC^2 + BC^2\right).$$
   Donc si $k < \frac{1}{3}\left(AB^2 + AC^2 + BC^2\right)$, l'ensemble recherché est l'ensemble vide. Si $k = \frac{1}{3}\left(AB^2 + AC^2 + BC^2\right)$, c'est le point G. Si $k > \frac{1}{3}\left(AB^2 + AC^2 + BC^2\right)$, c'est le cercle de centre G et de rayon $R = \frac{1}{3}\sqrt{3k - (AB^2 + AC^2 + BC^2)}$.
2. Si $k = 1$, on obtient la médiatrice de $[AB]$. De plus, si $k < 0$ il n'y a pas de solutions et si $k = 0$, on obtient le point A. Supposons maintenant que $k \neq 1$ et $k > 0$. On a $AM = kBM$ si et seulement si $AM^2 - k^2BM^2 = 0$. On définit G le barycentre de $\left\{(A, 1),\, (B, -k^2)\right\}$, on a donc $\overrightarrow{GA} - k^2\overrightarrow{GB} = 0$ et $AG = k^2BG$. D'où
   $$\begin{aligned} AM^2 - k^2BM^2 = 0 &\iff \left(\overrightarrow{AG}+\overrightarrow{GM}\right)\cdot\left(\overrightarrow{AG}+\overrightarrow{GM}\right) - k^2\left(\overrightarrow{BG}+\overrightarrow{GM}\right)\cdot\left(\overrightarrow{BG}+\overrightarrow{GM}\right) = 0 \\ &\iff AG^2 - k^2BG^2 + 2\overrightarrow{GM}\cdot\left(\overrightarrow{AG} - k^2\overrightarrow{BG}\right) + (1-k^2)GM^2 = 0 \\ &\iff GM^2 = \frac{1}{k^2-1}\left(AG^2 - k^2BG^2\right) = k^2BG^2. \end{aligned}$$
   On obtient le cercle de centre G et de rayon kBG.