Corrigé DS 3 : *Arithmétiques. Groupes cycliques. Suites numériques.*

MPSI-Maths.
Mr Mamouni & El Hassani : *myismail1@menara.ma*

Source disponible sur :
©http://www.chez.com/myismail

Lundi 10 Décembre 2007.

Durée: 3 heures 30mn.

Problème 1. (Fonction indicatrice d'Euler.)

1) n **est premier** $\iff k \wedge n = 1,\ \forall\, 1 \leq k \leq n \iff \varphi(n) = 1$.

2) $k \wedge n = 1 \iff \exists u, v \in \mathbb{Z}$ **tel que** $nu + kv = 1$
$\iff \exists v \in \mathbb{Z}$ **tel que** $kv \equiv 1\ [n]$
$\iff \exists v \in \mathbb{Z}$ **tel que** $\overline{k}\,\overline{v} = 1$
$\iff \overline{k}$ **est inversible dans** $\mathbb{Z}/n\mathbb{Z}$

3) $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ **est un corps** $\iff \forall\, 1 \leq k \leq n, \overline{k}$ **est inversible dans** $\mathbb{Z}/n\mathbb{Z}$
$\iff \forall\, 1 \leq k \leq n,\ k \wedge n = 1$
$\iff n$ **est premier**

4) $\mathbf{card}U\,(\mathbb{Z}/n\mathbb{Z}) = \mathbf{card}\{k \in [|1, n|]$ **tel que** $k \wedge n = 1\} = \varphi(n)$

5) **Soit** $(m, n) \in \mathbb{N}^*$ **tel que** $n \wedge m = 1$.

a) **On vérifie d'abord que** $\theta(\overline{1}, \overline{1}) = \overline{1},\ \theta(\overline{a} + \overline{c}, \overline{b} + \overline{d}) = \varphi(\overline{a}, \overline{b}) + \varphi(\overline{c}, \overline{d})$ **et enfin** $\theta(\overline{a}\,\overline{c}, \overline{b}\,\overline{d}) = \theta(\overline{a}, \overline{b})\,\theta(\overline{c}, \overline{d})$
Injection : Montrer que Ker $(\theta) = \{(\overline{0}, \overline{0})\}$.
Surjection : Les ensembles de départ et d'arrivées ont même cardinal.

b) $\overline{x}$ **inversible dans** $\mathbb{Z}/n\mathbb{Z}$, $\overline{y}$ **inversible dans** $\mathbb{Z}/m\mathbb{Z}$, **est evident par définition de l'inversiblilié.**
$(\overline{x}, \overline{y})$ **inversible dans** $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \iff \theta(\overline{x}, \overline{y})\overline{xy}$ **inversible dans** $\mathbb{Z}/nm\mathbb{Z}$, **car** θ **est un isomorphisme.**

c) **D'aprés la question précédente, on a :**

$$\begin{aligned}\varphi(nm) &= \textbf{card}\,(U(\mathbb{Z}/nm\mathbb{Z}))\\ &= \textbf{card}\,(U(\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}))\\ &= \textbf{card}\,(U(\mathbb{Z}/n\mathbb{Z})\times U(\mathbb{Z}/m\mathbb{Z}))\\ &= \varphi(n)\varphi(m)\end{aligned}$$

6) Par récurrence sur r.

7) $$\begin{aligned}\varphi(p^\alpha) &= \textbf{card}\{k\in[|1,p^\alpha|] \textbf{ tel que } k\wedge p^\alpha = 1\}\\ &= p^\alpha - \textbf{card}\{k\in[|1,p^\alpha|] \textbf{ tel que } k\wedge p \neq 1\}\\ &= p^\alpha - \textbf{card}\{k\in[|1,p^\alpha|] \textbf{ tel que } p \textbf{ divise } k\}\\ &= p^\alpha - \textbf{card}\{k=qp \textbf{ tel que } q\in[|1,p^{\alpha-1}|]\}\\ &= p^\alpha - p^{\alpha-1}\end{aligned}$$

8) ***Application :***

a) Posons $n=\prod_{i=1}^{r} p_i^{\alpha_i}$, avec $p_1<\cdots<p_r$, donc $\varphi(n)=\varphi\left(\prod_{i=1}^{r} p_i^{\alpha_i}\right)=\prod_{i=1}^{r}\varphi(p_i^{\alpha_i})=\prod_{i=1}^{r} p_i^{\alpha_i-1}(p_i-1)$, si $\varphi(n)$ divise n, alors $\prod_{i=1}^{r}(p_i-1)$, qui est pair divise $\prod_{i=1}^{r} p_i$, ceci est impossible si $r\geq 3$ car 4 divisera $\prod_{i=1}^{r} p_i$, le seul cas possible est $r=2$ avec $p_1=2, p_2=3$.

b) Le nombre de fractions $\frac{k}{n}$, tel que $1\leq k\leq n$ qu'on peut mettre sous la forme $\frac{a}{d}$, avec $a\wedge d=1$ est $\varphi(d)$, or au total il y a exactement n fraction, donc $\sum_{d \textbf{ divise } n}\varphi(d)=n$.

Problème 2. (Groupes cycliques)

1) Soit $(x,y)\in G^2$, or $G=\langle a\rangle$, donc $\exists(p,q)\in\mathbb{Z}^2$ tel que $x=a^p, y=a^q$, donc $x.y=a^{p+q}=y.x$.

2) Posons $p=kq$, donc $x\in\langle a^p\rangle\Longrightarrow x=a^{\alpha p}=a^{\alpha kq}\in\langle a^q\rangle$.

3) **a)** On a $o(a)=n$, donc $a^n=e$ et $(a^k)^{\frac{n}{n\wedge k}}=(a^n)^{\frac{k}{n\wedge k}}=e$, d'où $m=o(a^k)$ divise $\frac{n}{n\wedge k}$, d'autre part $a^{mk}=(a^k)^m=e$, donc $o(a)=n$ divise mk, donc $\frac{n}{\frac{n}{n\wedge k}}$ divise $m\frac{k}{\frac{n}{n\wedge k}}$, or $\frac{n}{n\wedge k}\bigwedge\frac{k}{n\wedge k}$, donc $\frac{n}{n\wedge k}$ divise m.

b) $G=\langle a^k\rangle\Longleftrightarrow \textbf{card}G=o(a^k)\Longleftrightarrow n=\frac{n}{n\wedge k}\Longleftrightarrow k\wedge n=1$.

c) Le nombre des générateurs de G est celui des entier k, tel que $1\leq k\leq n$ tel que $k\wedge n=1$, c'est à dire $\varphi(n)$.

4) Il est clair que $1\in\mathbb{U}_n$. Soit $z_1,z_2\in\mathbb{U}_n$, alors $(z_1z_2^{-1})^n=\frac{z_1^n}{z_2^n}$, donc $z_1z_2^{-1}\in\mathbb{U}$, d'où $\mathbb{U}$ est un sous-groupe de $(\mathbb{C}^*,\times)$.
D'autre part : $\mathbb{U}_n=\{e^{i\frac{2k\pi}{n}},\ 0\leq k\leq n-1\}=<w>$ où $w=e^{i\frac{2\pi}{n}}$, donc monogène, or il est fini de cardinal, n, donc cyclique.
Il y exactement $\varphi(n)$ racines $n^{\text{ème}}$ primitives de l'unité, ce sont les w^k tel que , $1\leq k\leq n$ et $k\wedge n=1$..
Pour $n=3, w=j$, les racines primitives sont j et j^2.
Pour $n=4, w=i$, les racines primitives sont i et $i^3=-i$.

5) **a)** Il est trés simple de montrer que H_d est un sous groupe de $(G,.)$, en vérifiant que, $e\in H(e^d=e)$ et que si $(x,y)\in H^2$, $(x^d=y^d=e)$, alors $x.y^{-1}\in H_d$ car $(x.y^{-1})^d=x^dy^{-d}=e$. Montrons maintenant que $H_d=\langle a^{\frac{n}{d}}\rangle$, par double inclusion, en utilisant surtout que $o(a)=n$.

- $x\in H_d\subset G=\langle a\rangle\Longrightarrow x=a^p, x^d=e$
  $\Longrightarrow x=a^p, a^{pd}=e$
  $\Longrightarrow x=a^p$ et n divise pd
  $\Longrightarrow x=a^p$ et $\frac{n}{d}$ divise $p=k\frac{n}{d}$
  $\Longrightarrow x=a^{k\frac{n}{d}}\in\langle a^{\frac{n}{d}}\rangle$
- Inversement, $x\in\langle a^{\frac{n}{d}}\rangle\Longrightarrow x=a^{k\frac{n}{d}}\Longrightarrow x^d=a^{nk}=e$
  $\Longrightarrow x\in H_d$

b) Soit H un sous groupe de $(G,.)$.

i. Cette question a été déjà traité en TD, les étapes à suivre sont les suivantes.

– **Montrer que f est un morphisme de groupe.**
– **En déduire que $f^{-1}(H)$ est un sous-groupe de $(\mathbb{Z},+)$, donc de la forme $p\mathbb{Z}$.**
– **Montrer par double inclusion que $H=\langle a^p\rangle$.**

ii. **Puisque $p\wedge n$ divise p, alors $\langle a^p\rangle\subset\langle a^{p\wedge n}\rangle$, d'autre part**

$$\begin{aligned}\textbf{card}\,\langle a^{p\wedge n}\rangle &= o(a^{p\wedge n})=\frac{n}{n\wedge(p\wedge n)}=\frac{n}{p\wedge n}=o(a^p)\\ &=\textbf{card}\,\langle a^p\rangle\end{aligned}$$

6) **La surjection découle de la question 5.b.ii), car pour tout $h\in\mathcal{H},\exists d=p\wedge n\in\mathcal{D}_n$ tel que $H=H_d$.**
L'injection, soit $d_1,d_2\in\mathcal{D}_n$,

$$\begin{aligned}\Phi(d_1)=\Phi(d_2) &\Longrightarrow H_{d_1}=H_{d_2}\\ &\Longrightarrow \left\langle a^{\frac{n}{d_1}}\right\rangle=\left\langle a^{\frac{n}{d_2}}\right\rangle\\ &\Longrightarrow o(\tfrac{n}{d_1})=o(\tfrac{n}{d_1})\\ &\Longrightarrow \frac{n}{n\wedge\frac{n}{d_1}}=\frac{n}{n\wedge\frac{n}{d_2}}\\ &\Longrightarrow d_1=d_2\end{aligned}\quad,$$

donc Φ est bijective.

7) **Comme Φ est bijective, alors le nombre de sous groupes dans G, est égale a celui des diviseurs de $n=p^\alpha$, qui sont les p^k tel que $0\le k\le\alpha$, il y en a exactement $\alpha+1$.**

Problème 3. (Étude d'une suite récurrente)

Préliminaire : Étudier la foction $\ln(1+x)-x$ sur $[-1,+\infty[$.

1) **a)** $1-u_{n+1}=(1-u_n)(1-\delta u_n)$.

b) **On montre d'abord (facile) par récurrence que $0\le u_n\le 1$, donc (u_n) est croissante, car $u_{n+1}-u_n=\delta u_n(1-u_n)$, d'où $u_n\ge u_0=a$.**

c) **(u_n) est croissante, majorée par 1, donc converge versl l tel que $0=\delta l(1-l)$ or $u_n\ge\delta>0$, donc $l\ge\delta>0$, d'où $l=1$.**

2) **a)** $1-u_{n+1}=(1-\delta u_n)(1-u_n)\le(1-\delta a)(1-u_n)$, **car** $a\le u_n\le 1$.

b) **Par récurrence.**

c) $0\le,\delta,u_k\le 1\Longrightarrow 1-\delta u_k\ge 1-\delta\ge 0\Longrightarrow$
$\ln x_{k+1}-\ln x_k=\ln\dfrac{1-\delta u_k}{1-\delta}\ge 0$, **d'autre part :**

$$\ln\frac{1-\delta u_k}{1-\delta}=\ln\left(1+\frac{\delta(1-u_k)}{1-\delta}\right)\le\frac{\delta(1-u_k)}{1-\delta}\le\frac{\delta}{1-\delta}(1-a)q^k.$$

d) $S_{n+1}-S_n=\ln x_{n+1}-\ln x_n\ge 0$, **donc S_n est croissante, d'autre part**

$$\begin{aligned}S_n &\le\sum_{k=0}^{n-1}\frac{\delta}{1-\delta}(1-a)q^k\\ &=\frac{\delta}{1-\delta}(1-a)\frac{1-q^n}{1-q}\\ &\le\frac{\delta}{1-\delta}(1-a)\frac{1}{1-q}\end{aligned}$$

donc majorée et par suite converge.

e) **S_n est une somme téléscopique, avec $S_n=\ln x_n-\ln x_0$ qui converge vers S, donc $\ln x_n=S_n+\ln x_0$ converge vers $S+\ln x_0$, d'où x_n converge vers $\mu=\mathrm{e}^S x_0==\mathrm{e}^S(1-a)>0$, donc $x_n=\dfrac{1-u_n}{(1-\delta)^n}\sim\mu$, donc $1-u_n\sim\mu(1-\delta)^n$.**

3) **a)** **On a :**

$$\begin{aligned}\frac{y_{k+1}}{y_k} &=\frac{u_{k+1}}{u_k}\frac{1-u_k}{1-u_{k+1}}\frac{(1+\delta)^n}{(1+\delta)^{n+1}}\\ &=\frac{1+\delta(1-u_k)}{(1+\delta)(1-\delta u_k)}\\ &=\frac{(1+\delta)(1-\delta u_k)+\delta^2u_k}{(1+\delta)(1-\delta u_k)}\\ &=1+\frac{\delta^2u_k}{(1+\delta)(1-\delta u_k)}\end{aligned}$$

b) **On remarque d'abord que :**

$$\begin{aligned}\ln\left(\frac{(1-a)y_n}{a(1-u_n)(1+\delta)^n}\right) &=\ln\left(\frac{y_n}{(1-u_n)(1+\delta)^n}\right)-\ln\left(\frac{a}{1-a}\right)\\ &=\ln y_n-\ln y_0\\ &=T_n\end{aligned}$$

Il sufit donc de montrer que $0 \leq T_n = \sum_{k=0}^{n-1} \ln \frac{y_{k+1}}{y_k} \leq \frac{n\delta^2}{1-\delta^2}$.

En effet,

$\frac{y_{k+1}}{y_k} = 1 + \frac{\delta^2 u_k}{(1+\delta)(1-\delta u_k)} \geq 1 \Longrightarrow \ln \frac{y_{k+1}}{y_k} \geq 0 \Longrightarrow T_n \geq 0.$

D'autre part,
$$\begin{aligned} \ln \frac{y_{k+1}}{y_k} &= \ln\left(1 + \frac{\delta^2 u_k}{(1+\delta)(1-\delta u_k)}\right) \\ &\leq \frac{\delta^2 u_k}{(1+\delta)(1-\delta u_k)} \\ &= \frac{\delta^2}{(1-\delta^2)} \cdot \frac{u_k(1-\delta)}{1-\delta u_k} \\ &= \frac{\delta^2}{(1-\delta^2)} \cdot \frac{u_k - \delta u_k}{1-\delta u_k} \\ &\leq \frac{\delta^2}{(1-\delta^2)} \end{aligned}$$

Donc, $T_n = \sum_{k=0}^{n-1} \ln \frac{y_{k+1}}{y_k} \leq \sum_{k=0}^{n-1} \frac{\delta^2}{(1-\delta^2)} = n\frac{\delta^2}{(1-\delta^2)}$.

4) **a)** $\left[\frac{t}{\delta}\right] \leq \frac{t}{\delta} \leq \left[\frac{t}{\delta}\right] + 1 \Longrightarrow \left[\frac{t}{\delta}\right]\delta \leq t \leq \left(\left[\frac{t}{\delta}\right] + 1\right)\delta.$

b) $\left[\frac{t}{\delta}\right]\delta \leq t \leq \left(\left[\frac{t}{\delta}\right] + 1\right)\delta \Longrightarrow t - \delta \leq \left[\frac{t}{\delta}\right]\delta \leq t,$

donc $\lim_{\delta\to 0}\left[\frac{t}{\delta}\right]\delta = t.$

$\ln(1+\delta)^{\left[\frac{t}{\delta}\right]} = \left[\frac{t}{\delta}\right]\ln(1+\delta) = \left(\left[\frac{t}{\delta}\right]\delta\right)\frac{\ln(1+\delta)}{\delta} \longrightarrow t.$

Donc $\lim_{\delta\to 0}(1+\delta)^{\left[\frac{t}{\delta}\right]} = \mathrm{e}^t.$

c) **Posons** $n = \left[\frac{t}{\delta}\right]$, **donc** $n\delta^2 = \left(\left[\frac{t}{\delta}\right]\delta\right)\delta \longrightarrow 0,$

or $0 \leq T_n = \ln y_n - \ln y_0 \leq \frac{n\delta^2}{1-\delta^2}$, **d'où** $\lim_{\delta\to 0} y_n = y_0$, **d'autre part** $y_n = \frac{u_n}{(1-u_n)(1+\delta)^n}$, **donc** $u_n = \frac{y_n}{y_n + \frac{1}{(1+\delta)^n}} \longrightarrow \frac{y_0}{y_0 + \mathrm{e}^{-t}}$, **avec** $y_0 = \frac{a}{1-a}$.

Exercice. (Groupe symétrique)

Vu en TD

1) $(\alpha\sigma\alpha^{-1})\alpha(i_1) = (\alpha\sigma)(i_1) = \alpha(i_2)$, **et ainsi de suite.**

2) **(1 3 2)(1 2 3 4)(1 2 3)=(3 1 2 4), prendre** $\alpha = (1\ 3\ 2)$ **et** $\sigma = (1\ 2\ 3\ 4)$.

3) $(1\ 2\ 3\ 4)^2 = (1\ 3)(2\ 4)$ **et** $(1\ 2\ 3\ 4)^3 = (1\ 4\ 3\ 2)$.

Fin.