Exercices L2

Nathan Fournié

Université Paul Sabatier

Le document ci-présent n'a aucune ambition mathématiques, sa seule fonction et d'entrainer son auteur à la maitrise du langage Latex et, de lui faire passer le temps. Rien de ce qui pourra être lu ici ne devra être pris avec certitude. L'existence de coquilles et erreurs est donc évidente, autant sur le fond que sur la forme.

Groupes et Anneaux élémentaires.

TD-3 : Sous-groupes et morphismes.

Exercice 1:

Soit G un groupe et $x \in G$, on utilsera la notation multiplicative.
1) Montrer que $\langle x \rangle = \{x^k, k \in \mathbb{Z}\}$
2) Montrer que l'ordre de x est $min\{n \in \mathbb{N}^*, x^n = e_G\}$
3) Soit $p \in \mathbb{N}$ l'ordre de x, soit $s \in \mathbb{N}$ tel que $x^s = e_G$. Montrer que s est un multiple de n
4) Montrer que si x est un élément d'ordre n il existe un morphisme $f : \mathbb{Z}/n\mathbb{Z} \leftarrow G$ entièrement déterminé pas $f(\dot{1}) = x$.

Solution :

1) Soit $u \in \{x^k, k \in \mathbb{Z}\}$. Alors $\exists k \in \mathbb{Z}$ tq: $u = x^k$. Soit p l'ordre de x. Alors $u^p = x^{kp} = (x^p)^k = e_G^k = e_G$ et donc : $u^{p+1} = x \in \langle x \rangle$
L'autre inclusion est par définition.

2) On doit montrer que $card\{x^k, k \in \mathbb{Z}\} = min\{n \in \mathbb{N}^*, x^n = e_G\}$
or $\{x^k, k \in \mathbb{Z}\} = \{e_G, x, x^2, ..., x^{p-1}\}$ avec p l'ordre de x.
Donc, $card(\{x^k, k \in \mathbb{Z}\}) = p$
Il nous reste à montrer que p appartient à $\{n \in \mathbb{N}^*, x^n = e_G\}$ et que c'est le plus petit.

• Montrons que $p \in \{n \in \mathbb{N}^*, x^n = e_G\}$.
On a que : $p \in \langle x \rangle$ donc $\exists j \in [\![0; p]\!]$ tq: $x^p = x^j$.
Alors : $x^{p-j} = e_G$. Donc $card(\{x^k, k \in \mathbb{Z}\}) = p_j$, donc $j = 0$.

• Montrons que p est le minimum.
Soit $j \in \mathbb{N}$ tq: $x^j = e_G$.
Supposons par l'absurde que $j < p$. Alors :
$\{x^k, k \in \mathbb{Z}\} = \{e_G, x, x^2, ..., x^{j-1}\}$ et $card(\{x^k, k \in \mathbb{Z}\}) = j < p$ *Absurdus*

4) $$\begin{array}{rccc} f: & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & G \\ & x & \longmapsto & x^3 \end{array}$$

Exercice 2 :

Soient G_1 et G_2 deux groupes. Soient $(x, y) \in G_1 \times G_2$ d'odre respectif m et n. Montrez que $(x, y) \in G_1 \times G_2$ est d'ordre $ppcm(m, n)$.

Solution :
Nous allons montrer que l'entier p qui vérifie la relation suivante : $(x, y)^p = (e_{G_1}, e_{G_2})$ ne peut qu'être un multiple de n et de m, puis, comme l'ordre est le plus petit, il ne peut qu'être le *ppcm* de n et m.

• Soit $p \in \mathbb{N}$ $tq:$ $\exists$ $k, k' \in \mathbb{N}$ $tq:$ $p = kn = k'm$
Alors, $(x,y)^p = (x^p, y^p) = (x^{km}, y^{k'n}) = ((x^m)^k, (y^n)^{k'}) = (e_{G_1}^k, e_{G_2}^{k'}) = (e_{G_1}, e_{G_2})$

• soit $r \in \mathbb{N}$ $tq:$ $\exists\, k, k', a \in \mathbb{N}$ $tq:$ $r = km = k'n + a$ avec $a < m$
Alors : $(x,y)^r = (x^{km}, y^{k'n+a}) = (e_{G_1}, e_{G_2} y^{k'n+a}) = (e_{G_1}, y^{k'n+a})$
or $y^{k'n+a} \neq e_{G_2}$ car $a < m$

Exercice 3:

Soient $a, b \in \mathbb{Z}$. Montrez que le sous groupes engendré par a, b dans $(\mathbb{Z}, +)$ est $pdgc(a,b)\mathbb{Z}$.

Solution:
On sait déjà que $pdcd(a,b)\mathbb{Z}$ est un groupe de la forme : $a\mathbb{Z} + b\mathbb{Z}$. Il suffit alors de montrer que c'est le plus petit groupe contenant le couple (a,b).

• Soit H un groupe contenant (a,b). Montrons que : $a\mathbb{Z} + b\mathbb{Z} \in H$.
Soit $u \in a\mathbb{Z} + b\mathbb{Z}$. Alors: $u = an + an'$ avec $n, n' \in \mathbb{Z}$
or $an \in H$ et $bn \in H$ donc, H étant un groupe, $u \in H$.

Exercice 4:

Soit $\dot{a} \in \mathbb{Z}/n\mathbb{Z}$ avec $0 \leq a < n$. Montrer que l'ordre de $\dot{a}$ est $p = \frac{ppcm(a,n)}{a}$

Solution :
On veut trouver l'ensemble des $p \in \mathbb{N}$ tq $p\dot{a} = \dot{0}$, l'ordre sera son minimum.

• Dans un premier temps, on a : $p\dot{a} = pa\dot{1} = \dot{pa}$
Donc, $p\dot{a} = \dot{0} \Leftrightarrow \dot{pa} = \dot{0}$
Donc, $pa \in n\mathbb{Z}$ mais, comme $pa \in a\mathbb{Z}$ alors, $pa \in ppcm(a,n)\mathbb{Z}$ donc,
$p \in \frac{ppcm(a,n)}{a}\mathbb{Z}$
or, $min(\frac{ppcm(a,n)}{a}\mathbb{Z}) = \frac{ppcm(a,n)}{a}$

Exercice 5:

Trouver l'ordre de $\dot{2}$ dans $(\mathbb{Z}/11\mathbb{Z}\backslash\dot{0}, \times)$ et en déduire que $(\mathbb{Z}/11\mathbb{Z}\backslash\{\dot{0}\}, \times)$ est isomorphe à $(\mathbb{Z}/10\mathbb{Z}, +)$.

Solution:
On remarque que $2^10 = 1024 = 93 \times 11 + 1$ donc que 10 est l'ordre de $\dot{2}$ dans $\mathbb{Z}/11\mathbb{Z}$.

• On pose alors : $\begin{array}{rccc} f: & (\mathbb{Z}/10\mathbb{Z}, +) & \longrightarrow & (\mathbb{Z}/11\mathbb{Z}\backslash\{\dot{0}\}, \times) \\ & \dot{x} & \longmapsto & \dot{2}^x \end{array}$
Il reste à montrer que f représente bien un morphisme bijectif de groupe.

• Montrons que f est bien un morphisme de groupe.
Soit $\dot{x}, \dot{y} \in (\mathbb{Z}/10\mathbb{Z}, +)$ Alors :
$f(\dot{x} + \dot{y}) = \dot{2}^{x+y} = \dot{2}^x \dot{2}^y = f(\dot{x})f(\dot{y})$

• Montrons que f est bien bijectif.
Soit $\dot{u} \in Ker(f)$, alors : $f(\dot{u}) = \dot{2}^u = \dot{1}$ donc $\dot{u} = \dot{0}$.
f est injective.
f est évidemment surjective, donc f est bien bijective.

Exercice 6:

Dessiner le treillis des sous-groupes de $\mathbb{Z}/12\mathbb{Z}$

Solution:
Je suis incapable de faire un trellis sur Latex, mais on à les inclusions suivantes :
$\{0\} \subset \mathbb{Z}/2\mathbb{Z} \subset \mathbb{Z}/4\mathbb{Z} \subset \mathbb{Z}/12\mathbb{Z}$
et:
$\{0\} \subset \mathbb{Z}/3\mathbb{Z} \subset \mathbb{Z}/6\mathbb{Z} \subset \mathbb{Z}/12\mathbb{Z}$
et
$\mathbb{Z}/2\mathbb{Z} \subset \mathbb{Z}/6\mathbb{Z}$

Exercice 7:

Soit G un groupe de cardinal p, un nombre premier. Montrer que G est isomorphe à $\mathbb{Z}/p\mathbb{Z}$

Solution:
Il suffit de montrer qu'il existe un $x \in G$ d'ordre p.

• Soit $x \in G$. Alors, $\langle x \rangle \subset G$.
D'après le théoreme de Lagrange, $r = card(\langle x \rangle)$ divise p.
Donc $r = 1$, soit $r = p$. De deux chose l'une :
Si $r = p$, alors c'est finit.
Si $r = 1$, alors $x = 1$, donc il existe $y \in G$ différent de x tel que : $card(\langle x \rangle) = p$.

Exercice 8:

Soit $S^1 = \{z \in \mathbb{C}, |z| = 1\}$
Soit $f : \mathbb{R} \to S^1$ tel que $f(x) = e^{ix}$.
1) Montrer que S^1 est un sous groupe de $\mathbb{C}^*$
2) Montrer que f est un morphisme surjectif.
3) Trouver $ker(f)$.
4) Montrer que $f(x)$ est d'ordre fini ssi $x \in \pi\mathbb{Q}$.

Solution:

1) Soit $x, y \in S^1, \quad |xy^{-1}| = \frac{|x|}{|y|} = 1$

2) Soit $x, y \in S^1, \quad f(x+y) = e^{i(x+y)} = e^{ix}e^{iy} = f(x)f(y)$

3) Soit $u \in ker(f)$, alors $e^{iu} = 1$, donc $u \in \{2k\pi, k \in \mathbb{N}\}$

4) Montrons que $f(x)$ est d'ordre fini ssi $x \in \pi\mathbb{Q}$.

• $\Rightarrow$ Si $f(x)$ est d'ordre n.
Alors : $f(x)^n = 1$, donc $(e^{ix})^n = e^{inx} = 1$, donc $nx \in ker(f)$, donc $x = \frac{2k\pi}{n} \in \pi\mathbb{Q}$.

• $\Leftarrow$ Si $x \in \pi\mathbb{Q}$, alors il existe $a, b \in \mathbb{N}$ tel que $x = \frac{a}{b}\pi$.
puis, $(e^{i\frac{a}{b}\pi})^b = e^{ia\pi} = 1$ car appartient au $ker(f)$.

Exercice 9:

Pour tout $n \in \mathbb{N}^*$, soit $C_n = \{e^{2ik\pi/n} \mid 0 \leq k \leq n-1\}$.
1) Montrer que C_n est un sous groupe de $\mathbb{C}^*$.
2) Montrer que C_d est un sous groupe de C_n ssi d divise n.
3) Soit H un sous groupe de C_n. Montrer qu'il existe d tel que $H = C_d$.
4) Montrer que le sous-groupe $C_m \cup C_n$ est $C_{ppcm(m,n)}$.
5) Montrer que C_n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Solution :

1) Soit $x, y \in C_n$ avec $x = e^{2ik\pi/n}$ et $y = e^{2ik'\pi/n}$
Alors, $xy^{-1} = e^{2ik\pi/n}e^{-2ik\pi/n} = e^{2i\pi(k-k')/n} \in C_n$

2)
• $\Rightarrow$ Soit C_d un sous groupe de C_n.Comme C_d est fini et de cardinal d, on conclu avec le théoreme de Lagrange.
• $\Leftarrow$ Supposons que d divise n et montrons que C_d est un sous groupe de C_n.
Soit $u \in C_d$, Alors $u = e^{2ik\pi/d}$ or $n = pd$ pour $d \in \mathbb{N}$.
Donc, $u = e^{2ik\pi/(n/p)} = u = e^{2ikp\pi/n} \in C_n$
Donc, $C_d \subset C_n$.
Soit $u, v \in C_d$. Alors: $uv^{-1} = e^{2ik\pi/d}e^{-2ik\pi/d} = e^{2i\pi(k-k')/d} \in C_d$

Exercice 10:

1) Soit $n \in \mathbb{N}^*$. Pour tout diviseur d de n, montrer que $H_d = \{\dot{k} \mid \dot{dk} = 0\}$ est l'unique sous groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$

2) Expliquer pourquoi la question précedente peut se déduire de l'exercice 9.

Solution: ???

Exercice 11:

Soient m et n deux entiers premiers entre eux. Pour $x \in \mathbb{Z}$, on pose : $\bar{x} = x+m\mathbb{Z}$, $\tilde{x} = x + n\mathbb{Z}$,$\hat{x} = x + mn\mathbb{Z}$.
1) Montrer que $(\bar{1}, \tilde{1})$ est un élément d'ordre mn
En déduire qu'il existe un isomorphisme $f : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ donné par : $f(\tilde{k} = (\bar{k}, \hat{k}$.
3) On prend $m = 4$, $n = 7$, calculer $f(\tilde{20}$ et $f^{-1}(\bar{2}, \tilde{5})$.
4) Comprendre que cet isomorphisme donne une preuve du théoreme chinois.

Solution : ???

Exercice 12:

1) Donner tous les générateurs possibles de $\mathbb{Z}/6\mathbb{Z}$.
2) Pour chacun des groupes additifs suivant, dire si il est monogène:
$\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$

Solution:

1) Les générateur de $\mathbb{Z}/n\mathbb{Z}$ Sont les classes d'équivalences des entiers k premiers avec n, donc pour $\mathbb{Z}/6\mathbb{Z}$ on a 1 et 5.

2)
Pour $\mathbb{Z}$, 1 est générateur, donc le groupe est monogène.
Pour $\mathbb{R}$, si il était monogène, alors il serait de isomorphe à $\mathbb{Z}$...
Pour $\mathbb{Z}^2$, Soit $(a, b) \in \mathbb{Z}^2$, si $a = 0$ alors $(1, 0)$ n'appartient pas à $< (a, b) >$, donc il n'y a pas de générateurs possibles.
Pour $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$, comme 3 et 7 sont premiers entre eux, le groupe est isomorphe à $\mathbb{Z}/21\mathbb{Z}$, donc monogène. Pour$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ ...Je ne sais pas.