Université de Bordeaux **Algèbre 3**
Licence de Sciences et Technologies
2014-2015

Corrigé de l'examen du 19 mai 2015.

Exercice 1. Soit

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 6 & 7 & 4 & 8 & 9 & 3 & 10 & 2 & 1 \end{pmatrix} \in S_{10}.$$

1. Déterminer la décomposition de σ en produit de cycles à supports disjoints.

   $\sigma = (1\,5\,8\,10)\,(2\,6\,9)\,(3\,7)\,(4)$
   $= (1\,5\,8\,10)\,(2\,6\,9)\,(3\,7)$ si l'on adopte la convention de ne pas écrire les cycles de longueur 1.

2. Déterminer l'ordre de σ.
   Rappelons que l'ordre d'un cycle est égal à sa longueur. Les cycles apparaissant dans la décomposition de σ sont donc respectivement d'ordre 4, 3 et 2. Comme ils sont de supports deux à deux disjoints, ils commutent et leur produit a pour ordre le *ppcm* de 4, 3 et 2, soit 12.

3. Calculer σ^{2015}.
   $\sigma^{2015} = \sigma^{167\times 12+11} = \sigma^{11} = \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 9 & 7 & 4 & 1 & 2 & 3 & 5 & 6 & 8 \end{pmatrix}$.

Exercice 2. On rappelle que la partie entière d'un nombre rationnel x, notée $\lfloor x \rfloor$, est l'unique entier n tel que

$$n \leq x < n+1$$

et que sa partie fractionnaire, notée $\{x\}$ est définie par

$$\{x\} = x - \lfloor x \rfloor.$$

1. Soit b un entier naturel non nul.

   (a) Donner une expression simple de $\left\{\frac{n}{b}\right\}$ pour tout $n \in \mathbb{Z}$, en utilisant la division euclidienne par b.
   Si $n = bq + r$ avec $(q,r) \in \mathbb{Z}^2$ et $0 \leq r < b$, alors $\frac{n}{b} = q + \frac{r}{b}$, d'où

   $$\lfloor \frac{n}{b} \rfloor = q \quad \text{et} \quad \left\{\frac{n}{b}\right\} = \frac{r}{b}.$$

   (b) Montrer que pour tous $(m,n) \in \mathbb{Z}^2$ on a

   $$\left\{\frac{m}{b}\right\} = \left\{\frac{n}{b}\right\} \Leftrightarrow m \equiv n \mod b.$$

   D'après la question précédente, $\left\{\frac{m}{b}\right\} = \left\{\frac{n}{b}\right\}$ si et seulement si m et n ont même reste dans la division euclidienne par b, d'où la conclusion.

2. Soit $x = \frac{a}{b} \in \mathbb{Q}^*$ avec a et b entiers, $b \geq 1$ et $a \wedge b = 1$.

   (a) On note $\overline{k}$ la classe modulo b d'un entier k. Montrer que l'application

   $$\begin{array}{rccc} f: & \mathbb{Z}/b\mathbb{Z} & \to & \mathbb{Z}/b\mathbb{Z} \\ & \overline{k} & \mapsto & \overline{ka} \end{array}$$

   est un automorphisme de $(\mathbb{Z}/b\mathbb{Z}, +)$, c'est-à-dire un morphisme de groupes bijectif de $(\mathbb{Z}/b\mathbb{Z}, +)$ dans lui-même.

   C'est clairement un morphisme de groupes car pour tous $x = \overline{k}$ et $y = \overline{\ell}$ dans $\mathbb{Z}/b\mathbb{Z}$, on a

   $$f(x+y) = \overline{(k+\ell)a} = \overline{ka} + \overline{\ell a} = f(x) + f(y).$$

   Son noyau est l'ensemble des $x = \overline{k}$ dans $\mathbb{Z}/b\mathbb{Z}$ tels que $f(x) = \overline{ka} = \overline{0}$, c'est-à-dire tels que b divise ka. Comme a et b sont premiers entre eux, cette dernière condition équivaut, via le lemme de Gauss, à la condition que b divise k, c'est-à-dire $\overline{k} = \overline{0}$. Le morphisme f est donc injectif, et par conséquent bijectif, comme toute application injective d'un ensemble fini dans lui-même.

   (b) Montrer que $\sum_{k=0}^{b-1} \left\{ \frac{ka}{b} \right\} = \frac{b-1}{2}$.

   Le résultat précédent montre en particulier que l'application

   $$\begin{array}{ccc} \{0, 1, \ldots, b-1\} & \longrightarrow & \{0, 1, \ldots, b-1\} \\ k & \longmapsto & \text{reste de la division euclidienne de } ka \text{ par } b \end{array}$$

   est une bijection. En utilisant l'équivalence $\left\{ \frac{m}{b} \right\} = \left\{ \frac{n}{b} \right\} \Leftrightarrow m \equiv n \mod b$ établie à la première question on en déduit que

   $$\sum_{k=0}^{b-1} \left\{ \frac{ka}{b} \right\} = \sum_{r=0}^{b-1} \left\{ \frac{r}{b} \right\} = \sum_{r=0}^{b-1} \frac{r}{b} = \frac{1}{b} \frac{b(b-1)}{2} = \frac{b-1}{2}.$$

Exercice 3. On rappelle que pour tout entier naturel non nul n, l'ensemble $(\mathbb{Z}/n\mathbb{Z})^\times$ des éléments de l'anneau $\mathbb{Z}/n\mathbb{Z}$ qui sont inversibles pour la multiplication est un groupe, la loi de groupe étant induite par la multiplication de $\mathbb{Z}/n\mathbb{Z}$.

1. Soit n un entier naturel non nul. Montrer que pour tout entier naturel a les propriétés suivantes sont équivalentes :

   (a) $a \wedge n = 1$,

   (b) la classe de a dans $\mathbb{Z}/n\mathbb{Z}$ est inversible pour la multiplication,

   En utilisant le théorème de Bézout, on a les équivalences suivantes :

   $$\begin{aligned} a \wedge n = 1 &\Leftrightarrow \exists\, (u, v) \in \mathbb{Z}^2 \mid au + nv = 1 \\ &\Leftrightarrow \exists\, u \in \mathbb{Z} \mid au \equiv 1 \mod n \\ &\Leftrightarrow \exists\, \overline{u} \in \mathbb{Z}/n\mathbb{Z} \mid \overline{a}\,\overline{u} = \overline{1}, \text{ en notant } \overline{u} \text{ la classe modulo } n \text{ d'un entier } u, \\ &\Leftrightarrow \overline{a} \text{ inversible pour la multiplication dans } \mathbb{Z}/n\mathbb{Z}. \end{aligned}$$

2. On s'intéresse dans cette question au groupe $G = (\mathbb{Z}/17\mathbb{Z})^\times$ des éléments de $\mathbb{Z}/17\mathbb{Z}$ inversibles pour la multiplication.

   (a) Quel est l'ordre de G ? Quels sont les ordres possibles pour un élément de G ?

   $(\mathbb{Z}/17\mathbb{Z})^\times$ est un groupe d'ordre $\varphi(17) = 17 - 1 = 16$ car 17 est premier. Les ordres possibles pour un élément de ce groupe sont donc 1, 2, 4, 8 et 16.

   (b) On note $\overline{10}$ la classe de 10 modulo 17. Vérifier que $\overline{10}$ appartient à G et déterminer son ordre. Le groupe G est-il cyclique ?

   L'ordre de la classe de 10 modulo 17 dans le groupe $(\mathbb{Z}/17\mathbb{Z})^\times$ vaut 2, 4, 8 ou 16 (on exclut 1 d'emblée, puisque $10 \not\equiv 1 \mod 17$). Pour le déterminer, il suffit, par élévations au carré successives, de calculer 10^2, 10^4 et 10^8 modulo 17. On trouve :

   - $10^2 = 100 \equiv -2 \mod 17$,
   - $10^4 \equiv 4 \mod 17$,
   - $10^8 \equiv 16 \equiv -1 \mod 17$.

   Par conséquent, 10 est d'ordre 16 dans $(\mathbb{Z}/17\mathbb{Z})^\times$, ce qui prouve en particulier que $(\mathbb{Z}/17\mathbb{Z})^\times$ est cyclique.

3. On s'intéresse dans cette question au groupe $H = (\mathbb{Z}/16\mathbb{Z})^\times$ des éléments de $\mathbb{Z}/16\mathbb{Z}$ inversibles pour la multiplication.

   (a) Quel est l'ordre de H ?
   Les éléments inversibles modulo 16 sont les classes des entiers premiers à 16, c'est-à-dire les classes des entiers impairs, qui sont au nombre de 8 (on peut aussi appliquer la formule $\phi(p^a) = p^{a-1}(a-1)$ pour p premier et a entier naturel non nul).

   (b) Montrer que H n'est pas cyclique.
   Soit $a = 2k + 1$ un entier impair. Alors

$$a^2 = 4k^2 + 4k + 1 = 4\underbrace{k(k+1)}_{\text{pair}} + 1 \equiv 1 \mod 8.$$

   Autrement dit, $a^2 = 8\ell + 1$, pour un certain $\ell \in \mathbb{Z}$ et

$$a^4 = 64\ell^2 + 16\ell + 1 \equiv 1 \mod 16.$$

   Les éléments de H, qui sont les classes modulo 16 des entiers impairs, sont donc d'ordre au plus 4. En particulier, H ne contient pas d'élément d'ordre 8 et n'est donc pas cyclique.

Exercice 4. Soit $(A, +, \cdot)$ un anneau commutatif unitaire non réduit à $\{0\}$. On dit qu'un élément a non nul de A est un *diviseur de zéro* s'il existe un élément b non nul de A tel que $ab = 0$, et qu'il est inversible s'il existe $c \in A$ tel que $ac = 1$. À tout élément a de $A \setminus \{0\}$ on associe l'application

$$\begin{array}{rccc} m_a : & A & \to & A \\ & x & \mapsto & a \cdot x \end{array}$$

de multiplication par a.

1. Montrer que l'application m_a est un morphisme du groupe additif $(A, +)$.
   C'est une conséquence immédiate de la distributivité de la multiplication sur l'addition :

$$\forall (x, y) \in A^2, m_a(x + y) = a(x + y) = ax + ay = m_a(x) + m_a(y).$$

2. Montrer que $\ker m_a \neq \{0\}$ si et seulement si a est un diviseur de zéro.
   Pour tout $a \in A \setminus \{0\}$ on a les équivalences :

$$\begin{aligned} \ker m_a \neq \{0\} &\Leftrightarrow \exists 0 \neq b \in A \mid m_a(b) = 0 \\ &\Leftrightarrow \exists 0 \neq b \in A \mid ab = 0 \\ &\Leftrightarrow a \text{ est un diviseur de zéro.} \end{aligned}$$

   Autrement dit, m_a est injectif si et seulement si $a \in A \setminus \{0\}$ n'est pas un diviseur de zéro.

3. À quelle condition le morphisme m_a est-il surjectif ?
   Le morphisme m_a est surjectif si et seulement si a est inversible. en effet :

   - Si m_a est surjectif, alors en particulier $1 \in m_a(A)$, ce qui signifie qu'il existe $b \in A$ tel que
   $$1 = m_a(b) = ab$$
   c'est-à-dire que a est inversible.
   - Inversement, si a est inversible, d'inverse a^{-1}, on a, pour tout $b \in A$
   $$b = a(a^{-1}b) = m_a(a^{-1}b) \in m_a(A),$$
   ce qui signifie que m_a est surjectif.

4. On suppose A de **cardinal fini**. En utilisant les questions précédentes, montrer qu'un élément non nul de A est soit inversible soit diviseur de zéro.
   Si A est fini, alors l'application $m_a : A \to A$ est injective si et seulement si elle est surjective. Autrement dit, d'après les questions précédentes, un élément $a \in A \setminus \{0\}$ est inversible si et seulement si il n'est pas diviseur de zéro.

5. Donner un exemple d'anneau infini et d'un élément non nul de cet anneau qui ne soit ni inversible ni diviseur de zéro.
   Dans $A = \mathbb{Z}$, l'élément 2 n'est ni inversible, ni diviseur de zéro.

Exercice 5. Soit $\mathbb{D}$ l'ensemble des nombres décimaux, c'est-à-dire

$$\mathbb{D} = \{x \in \mathbb{Q} \mid \exists n \in \mathbb{N} \text{ tel que } 10^n x \in \mathbb{Z}\}.$$

1. Montrer que la différence et le produit de deux éléments de $\mathbb{D}$ sont encore des éléments de $\mathbb{D}$. En déduire que $\mathbb{D}$ est un sous-anneau de $\mathbb{Q}$.
   Soient x et y deux éléments de $\mathbb{D}$. Il existe donc deux entiers naturels n et m tels que
   $$10^n x \in \mathbb{D} \text{ et } 10^m y \in \mathbb{D}.$$
   Par suite, on a :
   - $10^{n+m}(x-y) = 10^m \underbrace{(10^n x)}_{\in\mathbb{Z}} - 10^n \underbrace{(10^m y)}_{\in\mathbb{Z}} \in \mathbb{Z}$ donc $x - y \in \mathbb{D}$,
   - $10^{n+m}xy = \underbrace{(10^n x)}_{\in\mathbb{Z}} \underbrace{(10^m y)}_{\in\mathbb{Z}} \in \mathbb{Z}$ donc $xy \in \mathbb{D}$.

   Par ailleurs, 0 et 1 appartiennent trivialement à $\mathbb{D}$, ce qui achève de montrer que $\mathbb{D}$ est un sous-anneau de $\mathbb{Q}$.

2. Soit I un idéal de $\mathbb{D}$. Rappelons que cela signifie que $(I,+)$ est un sous-groupe de $(\mathbb{D},+)$ et que pour tout $a \in \mathbb{D}$ et tout $x \in I$ on a $ax \in I$.

   (a) Montrer que $I \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$.

   Si x et y sont deux éléments de $I \cap \mathbb{Z}$, alors leur différence appartient à I, puisque $(I,+)$ est un sous-groupe de $(\mathbb{D},+)$, et à $\mathbb{Z}$, comme différence de deux éléments de $\mathbb{Z}$, donc à $I \cap \mathbb{Z}$. Par conséquent, $(I \cap \mathbb{Z},+)$ est un sous-groupe de $(\mathbb{Z},+)$.

   Par ailleurs, si $x \in I \cap \mathbb{Z}$ et $a \in \mathbb{Z} \subset \mathbb{D}$, alors ax appartient à I car I est un idéal $\mathbb{D}$. De plus, ax appartient évidemment à $\mathbb{Z}$ comme produit de deux éléments de $\mathbb{Z}$. Donc ax appartient à $I \cap \mathbb{Z}$.

   En conclusion, $I \cap \mathbb{Z}$ est bien un idéal de $\mathbb{Z}$.

   (b) En utilisant un résultat du cours, montrer qu'il existe $d \in \mathbb{N}$ tel que $I \cap \mathbb{Z} = d\mathbb{Z}$.

   On a vu en cours que les sous-groupes, et a fortiori les idéaux, de $\mathbb{Z}$ sont tous de la forme $d\mathbb{Z}$, pour un entier naturel d convenable. Par conséquent, il existe $d \in \mathbb{N}$ tel que $I \cap \mathbb{Z} = d\mathbb{Z}$.

   (c) Montrer que $I = d\mathbb{D}$ (on procédera par double inclusion).

   Clairement $d \in d\mathbb{Z} = I \cap \mathbb{Z} \subset I$, donc d appartient à I et par suite, da appartient à $\mathbb{D}$ pour tout $a \in \mathbb{D}$ puisque I est un idéal de $\mathbb{D}$. Donc $d\mathbb{D} \subset I$.

   Inversement, si x est un élément de $I \subset \mathbb{D}$ alors, il existe $n \in \mathbb{N}$ tel que $10^n x \in I \cap \mathbb{Z} = d\mathbb{Z}$. autrement dit, il existe $n \in \mathbb{N}$ et $k \in \mathbb{Z}$ tels que $10^n x = dk$. Par suite, $x = d \underbrace{\frac{k}{10^n}}_{\in \mathbb{D}} \in d\mathbb{D}$.

   Donc $I \subset d\mathbb{D}$.