Algèbre 2 – Correction du partiel du 21 mars 2019

Exercice 1 (**4p**)

1. (**1,5p**) Énoncer et démontrer le théorème de Lagrange.

   Solution : Voir le poly.

2. (**2,5p**) Énoncer et démontrer les cinq corollaires au théorème de Lagrange faits en cours.

   Solution : Voir le poly.

Exercice 2 (**8p**) Soit $n \in \mathbb{N}^*$. Désignons par $\mathbb{Z}_n^\times$ l'ensemble des éléments de $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ qui sont inversibles par rapport à la multiplication.

1. (**1p**) Montrer que $(\mathbb{Z}_n^\times, \cdot)$ est un groupe.

   Solution : D'après la définition d'un groupe il faut démontrer que :

   (a) la multiplication $\cdot$ est une lci sur $\mathbb{Z}_n^\times$.

   (b) la multiplication $\cdot$ sur $\mathbb{Z}_n^\times$ est associative.

   (c) la multiplication $\cdot$ admet un élément neutre *dans* $\mathbb{Z}_n^\times$.

   (d) tout élément $x \in \mathbb{Z}_n^\times$ admet un élément symétrique *dans* $\mathbb{Z}_n^\times$ par rapport à la multiplication.

   Pour (a) : remarquer que, si x, $y \in \mathbb{Z}_n^\times$ alors, par la définition de $\mathbb{Z}_n^\times$, il existe x', $y' \in \mathbb{Z}_n$ tels que $xx' = [1]_n$, $yy' = [1]_n$. Mais alors $(xy)(x'y') = [1]_n$, donc xy est inversible, c'est à dire $xy \in \mathbb{Z}_n^\times$.
   Pour (b) : d'après un théorème de cours la multiplication est associative sur $\mathbb{Z}_n$, en particulier elle sera associative sur le sous-ensemble $\mathbb{Z}_n^\times \subset \mathbb{Z}_n$.
   Pour (c) : $[1]_n$ est élément neutre pour la multiplication même sur $\mathbb{Z}_n$, en particulier sur $\mathbb{Z}_n^\times$. Évidemment $[1]_n \in \mathbb{Z}_n^\times$.
   Pour (d) : Soit $x \in \mathbb{Z}_n^\times$. D'après la définition de $\mathbb{Z}_n^\times$, il existe $x' \in \mathbb{Z}_n$ tel que $xx' = [1]_n = x'x$ (la multiplication sur $\mathbb{Z}_n$ étant commutative).
   Mais alors on aura aussi $x' \in \mathbb{Z}_n^\times$ (parce qu'il admet x comme inverse). En conclusion x admet un inverse *dans* $\mathbb{Z}_n^\times$.

2. (**1p**) Préciser un isomorphisme de groupes additifs $f : \mathbb{Z}_{20} \to \mathbb{Z}_4 \times \mathbb{Z}_5$. Énoncer le théorème utilisé. Montrer que $(\mathbb{Z}_4 \times \mathbb{Z}_5, +)$ est un groupe cyclique et préciser un générateur de ce groupe.

   Solution : Puisque 4 et 5 sont premier entre eux, le théorème des restes chinois fournit un isomorphisme

   $$f : \mathbb{Z}_{20} \to \mathbb{Z}_4 \times \mathbb{Z}_5$$

   donné explicitement par

   $$f([k]_{20}) := ([k]_4, [k]_5).$$

   Pour l'énoncé du théorème des restes chinois : voir le poly.
   Le groupe $\mathbb{Z}_{20}$ est un groupe cyclique, et un générateur de ce groupe est (d'après le cours) la classe $[1]_{20}$. Puisque f est un isomorphisme, le groupe $\mathbb{Z}_4 \times \mathbb{Z}_5$ sera aussi cyclique admettant $f([1]_{20}) = ([1]_4, [1]_5)$ comme générateur.

3. (**1p**) Écrire explicitement $\mathbb{Z}_{20}^{\times}$ et la table de la lci de ce groupe multiplicatif.

   Solution :
   D'après le cours $[k]_{20} \in \mathbb{Z}_{20}^{\times}$ si et seulement si $\text{pgcd}(k, 20) = 1$. On obtient donc

   $$\mathbb{Z}_{20}^{\times} = \{[1]_{20}, [3]_{20}, [7]_{20}, [9]_{20}, [11]_{20}, [13]_{20}, [17]_{20}, [19]_{20}\}.$$

   La table du groupe est :

$\cdot$	[1]	[3]	[7]	[9]	[11]	[13]	[17]	[19]
[1]	[1]	[3]	[7]	[9]	[11]	[13]	[17]	[19]
[3]	[3]	[9]	[1]	[7]	[13]	[19]	[11]	[17]
[7]	[7]	[1]	[9]	[3]	[17]	[11]	[19]	[13]
[9]	[9]	[7]	[3]	[1]	[19]	[17]	[13]	[11]
[11]	[11]	[13]	[17]	[19]	[1]	[3]	[7]	[9]
[13]	[13]	[19]	[11]	[17]	[3]	[9]	[1]	[7]
[17]	[17]	[11]	[19]	[13]	[7]	[1]	[9]	[3]
[19]	[19]	[17]	[13]	[11]	[9]	[7]	[3]	[1]

4. (**2p**) Pour chaque élément $\xi = [k] \in \mathbb{Z}_{20}^{\times}$ préciser l'ordre de ξ et le sous-groupe cyclique engendré par ξ. Est-ce que $(\mathbb{Z}_{20}^{\times}, \cdot)$ est un groupe cyclique ?

   Solution : Nous avons :

   $$\langle [1] \rangle = \{[1]\},\ \text{ord}([1]) = 1.$$
   $$\langle [3] \rangle = \{[1], [3], [9], [7]\},\ \text{ord}([3]) = 4.$$
   $$\langle [7] \rangle = \{[1], [7], [9], [3]\},\ \text{ord}([7]) = 4.$$
   $$\langle [9] \rangle = \{[1], [9]\},\ \text{ord}([9]) = 2.$$
   $$\langle [11] \rangle = \{[1], [11]\},\ \text{ord}([11]) = 2.$$
   $$\langle [13] \rangle = \{[1], [13], [9], [17]\},\ \text{ord}([13]) = 4.$$
   $$\langle [17] \rangle = \{[1], [17], [9], [13]\},\ \text{ord}([17]) = 4.$$
   $$\langle [19] \rangle = \{[1], [19]]\},\ \text{ord}([19]) = 2.$$

   Nous constatons qu'aucun sous-groupe cyclique de $\mathbb{Z}_{20}^{\times}$ ne coïncide avec $\mathbb{Z}_{20}^{\times}$ (argument équivalent : $\mathbb{Z}_{20}^{\times}$ ne contient aucun élément d'ordre $|\mathbb{Z}_{20}^{\times}| = 8$), donc $\mathbb{Z}_{20}^{\times}$ n'est pas cyclique.

5. (**1p**) Préciser un isomorphisme $\phi : \mathbb{Z}_{20}^{\times} \to \mathbb{Z}_4^{\times} \times \mathbb{Z}_5^{\times}$. Énoncer le théorème utilisé.

   Solution : Puisque 4 et 5 sont premier entre eux, la version multiplicative du théorème des restes chinois fournit un isomorphisme

   $$\phi : \mathbb{Z}_{20}^{\times} \to \mathbb{Z}_4^{\times} \times \mathbb{Z}_5^{\times}$$

   donné explicitement par

   $$\phi([k]_{20}) := ([k]_4, [k]_5).$$

   Pour l'énoncé de la version multiplicative du théorème des restes chinois : voir le poly.

6. (**1p**) Montrer que $\mathbb{Z}_4^{\times}$, $\mathbb{Z}_5^{\times}$ sont des groupes cycliques, et préciser des isomorphismes

   $$\alpha : (\mathbb{Z}_2, +) \to (\mathbb{Z}_4^{\times}, \cdot),\ \beta : (\mathbb{Z}_4, +) \to (\mathbb{Z}_5^{\times}, \cdot).$$

Solution : Le groupe multiplicatif $\mathbb{Z}_4^\times = \{[1]_4, [3]_4\}$ admet $[3]_4$ comme générateur (parce que $\langle [3]_4 \rangle = \{[1]_4, [3]_4\}$), et le groupe multiplicatif $\mathbb{Z}_5^\times = \{[1]_5, [2]_5, [3]_5, [4]_5\}$ admet $[2]_5$ comme générateur (parce que $\langle [2]_5 \rangle = \{[1]_4, [2]_5, [4]_5, [3]_5\}$). D'après le cours on obtient les isomorphismes $\alpha : (\mathbb{Z}_2, +) \to (\mathbb{Z}_4^\times, \cdot)$, $\beta : (\mathbb{Z}_4, +) \to (\mathbb{Z}_5^\times, \cdot)$ définis par

$$\alpha([k]_2) := [3]_4^k,\ \beta([k]_4) := [2]_5^k.$$

Les isomorphismes de ce type ont été notés g_x en cours (voir le chapitre sur les sous-groupes cycliques).

7. (**1p**) Préciser un isomorphisme $\psi : (\mathbb{Z}_2 \times \mathbb{Z}_4, +) \to (\mathbb{Z}_{20}^\times, \cdot)$, et justifier votre réponse.

   Solution : Soit (α, β) l'isomorphisme

   $$(\alpha, \beta) : \mathbb{Z}_2 \times \mathbb{Z}_4 \to \mathbb{Z}_4^\times \times \mathbb{Z}_5^\times,\ (\alpha, \beta)(x, y) := (\alpha(x), \beta(y)).$$

   la composition $\psi := \phi^{-1} \circ (\alpha, \beta)$ sera un isomorphisme $\mathbb{Z}_2 \times \mathbb{Z}_4 \to \mathbb{Z}_{20}^\times$. Cette composition est bien un isomorphisme en tant que composition d'isomorphismes.

Exercice 3 (**13p**) Soit $(\mathfrak{S}_4, \circ)$ le groupe symétrique de degré 4 (le groupe symétrique de l'ensemble $\{1, 2, 3, 4\}$).

1. (**2p**) Écrire explicitement les éléments de $\mathfrak{S}_4$ en décomposant chaque élément en produit de cycles disjoints. Préciser l'ordre et la signature de chaque élément de $\mathfrak{S}_4$.

   Solution :
   D'après le cours $\mathfrak{S}_4$ contient : id, six 2-cycles, huit 3-cycles, 6 4-cycles, et trois permutations qui s'écrivent comme produit de deux 2-cycles disjoints. Voici la liste :

   id, (1 2), (1 3), (1 4), (2 3), (2 4), (3 4), (1 2 3), (1 3 2), (1 2 4), (1 4 2), (1 3 4), (1 4 3), (2 3 4), (2 4 3),

   (1 2 3 4), (1 3 2 4), (1 2 4 3), (1 4 3 2), (1 3 4 2), (1 4 2 3), (1 2)(3 4), (1 3)(2 4), (1 4)(2 3).

   Comment nous avons obtenu la liste des 4-cycles ? En cours nous avons étudié la correspondance entre arrangements et cycles. Cette correspondence n'est pas injective. A chaque k-cycle correspondent k arrangements. Etant donné un cycle τ, on obtient un arrangement qui définit τ en choisissant un élément de $\mathrm{supp}(\tau)$, qui va figurer comme premier élément de l'arrangement. Dans notre cas : tout 4-cycle τ est associé à un arrangement (de 4 éléments parmi $\{1, 2, 3, 4\}$) qui commence par 1, et cet arrangement est uniquement déterminé par τ. Sur la 1ère position on a écrit donc 1. Sur les positions 2, 3, 4 on a écrit d'abord les éléments 2, 3, 4 dans cette ordre, et puis on a appliqué toutes les permutations possibles à cette liste de trois éléments.
   L'ordre de l'identité est 1 et sa signature et 1.
   Les 2-cycles sont permutations d'ordre 2 et signature -1.
   Les 3-cycles sont permutations d'ordre 3 et signature 1.
   Les 4-cycles sont permutations d'ordre 4 et signature -1.
   Les permutations qui s'écrivent comme produit de deux 2-cycles disjoints (apr exemple (1 2)(3 2)) sont permutations d'ordre $\mathrm{ppcm}(2, 2) = 2$ et signature $(-1)(-1) = 1$. Voir le cours.

2. (**1p**) Quels sont les ordres possibles des sous-groupes de $\mathfrak{S}_4$? Énoncer le corollaire utilisé.

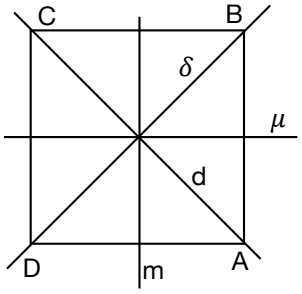
   Solution :
   D'après le 1er corollaire au théorème de Lagrange, l'ordre d'un sous-groupe de $\mathfrak{S}_4$ est un diviseur de $|\mathfrak{S}_4| = 24$. Donc les ordres possibles sont : 1, 2, 3, 4, 6, 8, 12, 24.

3. (**1p**) Montrer que $\mathfrak{S}_4$ admet un sous-groupe normal A d'ordre 12, et préciser un isomorphisme $\mu : \mathfrak{S}_4/A \to \mathrm{U}_2$.

   Solution : La signature définit un épimorphisme $\varepsilon : \mathfrak{S}_4 \to \mathrm{U}_2 = \{\pm 1\}$ dont le noyau est un sous-groupe normal d'indice 2 $A_4 \subset \mathfrak{S}_4$ (voir le cours). Donc il suffit donc de prendre $A = A_4 = \ker(\varepsilon)$.

4. (**2p**) Montrer que $\mathfrak{S}_4$ admet plusieurs sous-groupes d'ordre 8. *Indication : Chercher des sous-groupes isomorphes au groupe des isométries d'un carré.*

   Solution :
   Soit $\{A, B, C, D\}$ l'ensemble des sommets d'un carré dans le plan (écrits en respectant le sens trigonométrique), et soit O le centre de symétrie de ce carré. Soient $d = (AC)$, $\delta = (BD)$ les diagonales du carré. Soit m l'axe de symétrie parallèle à (AB), et μ l'axe de symétrie parallèle à (BC).



   Le groupe des isométries qui laissent invariant l'ensemble $\{A, B, C, D\}$ est (voir le TD) :

$$D_4 := \{\mathrm{id}, R_{\pi/2}, R_\pi, R_{3\pi/2}, S_d, S_\delta, S_m, S_\mu\}$$

   Chaque isométrie $f \in D_4$ induit une permutation $\Sigma(f) \in \mathfrak{S}(\{A, B, C, D\})$ sur l'ensemble des sommets, et l'application $\Sigma : D_4 \to \mathfrak{S}(\{A, B, C, D\})$ est un morphisme de groupes. On peut identifier l'ensemble $\{A, B, C, D\}$ avec $\{1, 2, 3, 4\}$ en indexant les sommets, et alors on va obtenir un monomorphisme $\Sigma : D_4 \to \mathfrak{S}_4$. Par exemple, en utilisant la bijection $1 \mapsto A$, $2 \mapsto B$, $3 \mapsto C$, $4 \mapsto D$ on obtient :

$$\Sigma(\mathrm{id}_{\mathbb{R}^2}) = \mathrm{id},\ \Sigma(R_{\pi/2}) = (1\,2\,3\,4),\ \Sigma(R_\pi) = (1\,3)(2\,4),\ \Sigma(R_{3\pi/2}) = (1\,4\,3\,2),$$

$$\Sigma(S_d) = (2\,4),\ \Sigma(S_\delta) = (1\,3),\ \Sigma(S_m) = (1\,4)(2\,3),\ \Sigma(S_\mu) = (1\,2)(3\,4).$$

   Puisque l'image d'un morphisme est un sous-groupe, on obtient le sous-groupe d'ordre 8

$$H = \{\mathrm{id}, (1\,2\,3\,4), (1\,3)(2\,4), (1\,4\,3\,2), (2\,4), (1\,3), (1\,4)(2\,3), (1\,2)(3\,4)\} \subset \mathfrak{S}_4.$$

   En changeant l'indexation des sommets, on va obtenir d'autres sous-groupes d'ordre 8. Tous les sous-groupes ainsi obtenus seront conjugués dans $\mathfrak{S}_4$ (sont les images de H par des automorphismes intérieurs de $\mathfrak{S}_4$).

5. (**2p**) Montrer que $\mathfrak{S}_4$ admet plusieurs sous-groupes d'ordre 6. *Indication : Chercher des sous-groupes isomorphes à $\mathfrak{S}_3$.*

   Solution :
   Pour chaque $i \in \{1, 2, 3, 4\}$ on obtient un sous-groupe $H_i \subset \mathfrak{S}_4$ défini par

$$H_i := \{\sigma \in \mathfrak{S}_4 |\ \sigma(i) = i\}.$$

Donc H_i est le sous-groupe des permutations qui laissent i invariant et s'identifie au groupe des permutation du sous-ensemble à trois éléments $\{1,2,3,4\} \setminus \{i\}$. Par exemple

$$H_4 = \{\mathrm{id}, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\} \subset \mathfrak{S}_4.$$

H_i est évidemment un sous-groupe de $\mathfrak{S}_4$:
— Evidemment $\mathrm{id} \in H_i$.
— Si σ, $\lambda \in H_i$ alors $\sigma(i) = i$, $\lambda(i) = i$, donc $(\sigma \circ \lambda)(i) = i$, donc $\sigma \circ \lambda \in H_i$.
— Soit $\sigma \in H_i$, i.e. $\sigma(i) = i$. Il en résulte $\sigma^{-1}(i) = i$, donc $\sigma^{-1} \in H_i$.

6. (**2p**) Montrer (en précisant le corollaire utilisé) que tout sous-groupe $H \subset \mathfrak{S}_4$ d'ordre 2 ou 3, est cyclique, et donner la liste complète de ces sous-groupes.

   Solution : 2 et 3 sont premiers, donc tous groupe d'ordre 2 ou 3 est cyclique d'après le 3ème corollaire au théorème de Lagrange.
   Pour écrire les sous-groupes (cycliques) d'ordre 2, il faut identifier dans la liste des éléments de $\mathfrak{S}_4$ les éléments d'ordre 2. Ces éléments sont les six 2-cycles, et les trois permutations qui s'écrivent comme produit de deux 2-cycles disjoints. On obtient la liste des sous-groupes d'ordre 2 :

   $$\langle(1\,2)\rangle,\ \langle(1\,3)\rangle,\ \langle(1\,4)\rangle,\ \langle(2\,3)\rangle,\ \langle(2\,4)\rangle,\ \langle(3\,4)\rangle,\ \langle(1\,2)(3\,4)\rangle,\ \langle(1\,3)(2\,4)\rangle,\ \langle(1\,4)(2\,3)\rangle.$$

   Les éléments d'ordre 3 sont les 3-cycles. Remarquer que, pour tout 3-cycle τ, τ et τ^2 engendrent le même sous-groupe. On obtient donc quatre sous-groupes d'ordre 3, à savoir :

   $$\langle(1\,2\,3)\rangle,\ \langle(1\,2\,4)\rangle,\ \langle(1\,3\,4)\rangle,\ \langle(2\,3\,4)\rangle.$$

7. (**1p**) Donner la liste complète de tous les sous-groupes *cycliques* d'ordre 4 de $\mathfrak{S}_4$.

   Solution :
   Les seuls éléments d'ordre 4 dans $\mathfrak{S}_4$ sont les six 4-cycles. Remarquer que, pour tout 4-cycle τ, τ et τ^3 engendrent le même sous-groupe. On obtient donc trois sous-groupes cycliques d'ordre 4, à savoir :

   $$\langle(1\,2\,3\,4)\rangle,\ \langle(1\,3\,2\,4),\ \langle(1\,2\,4\,3)\rangle.$$

8. (**2p**) Donner la liste complète de tous les sous-groupes d'ordre 4 de $\mathfrak{S}_4$ *qui ne sont pas cycliques.*

   Solution : D'après le TD, tout groupe d'ordre 4 qui n'est pas cyclique est abélien, est isomorphe à $\mathbb{Z}_2 \times \mathbb{Z}_2$, et s'écrit sous la forme $\{e, a, b, ab\}$, où $a^2 = b^2 = e$ et $ab = ba$. Donc, pour donner la liste des sous-groupes d'ordre 4 de $\mathfrak{S}_4$ qui ne sont pas cycliques, il faut trouver (dans $\mathfrak{S}_4$) *les paires d'éléments d'ordre 2 qui commutent.* Deux 2-cycles commutent si et seulement s'ils sont disjoints. Deux permutations arbitraires du type $(i\,j)(k\,l)$ (avec i, j, k, l distincts) commutent.
   On obtient les sous-groupes :

   $$\{\mathrm{id}, (1\,2), (3\,4), (1\,2)(3\,4)\},\ \{\mathrm{id}, (1\,3), (2\,4), (1\,3)(2\,4)\},\ \{\mathrm{id}, (1\,4), (2\,3), (1\,4)(2\,3)\},$$

   $$\{\mathrm{id}, (1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3)\}.$$