Les exercices étoilés (*) s'adressent aux seuls étudiants inscrits à l'unité MO12

Corrigé de la feuille d'exercices 1

Exercice 1. *Etude des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$:*

(i) Montrez que tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$;

(ii) Montrez que tout sous-groupe d'un groupe cyclique est cyclique;

(iii) Montrez que pour $d|n$, il existe un unique sous-groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$;

(iv) Donnez le cardinal du sous-groupe engendré par k dans $\mathbb{Z}/n\mathbb{Z}$;

(v) Montrez que $n = \sum_{d|n} \varphi(d)$ où $\phi(d)$ est l'indicatrice d'Euler, c'est à dire le nombre de générateurs de $\mathbb{Z}/d\mathbb{Z}$.

(vi) Montrez que tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique.

Preuve: (i) Soit G un groupe cyclique de cardinal n et g un générateur. On note la loi de G multiplicativement. Par définition tout élément de G est de la forme g^k. On considère alors le morphisme $\phi : \mathbb{Z} \longrightarrow G$ défini par $\phi(k) = g^k k$; c'est clairement un morphisme de groupe et surjectif par définition d'un groupe cyclique. Etudions son noyau, qui est un sous-groupe de $\mathbb{Z}$, donc de la forme $m\mathbb{Z}$. Ainsi ϕ induit un isomorphisme $\mathbb{Z}/m\mathbb{Z}$ sur G, par cardinalité on en déduit $m = n$.

(ii) Soit H un sous-groupe de G et $\varphi : \mathbb{Z} \longrightarrow G \longrightarrow G/H$, l'application composée de ϕ et du morphisme de réduction $G \longrightarrow G/H$. On rappelle que G étant commutatif, H est forcément distingué et G/H est alors naturellement muni d'une structure de groupe (cf. le cours). Le noyau de φ est un sous-groupe de $\mathbb{Z}$ donc de la forme $d\mathbb{Z}$, contenant $\operatorname{Ker}\phi = n\mathbb{Z}$, on en déduit donc que d divise n. Ainsi H est cyclique, un générateur étant g^d, son ordre est ainsi n/d.

(iii) Soit donc H un sous-groupe de G d'ordre d; il est cyclique d'après (ii), on note $h = g^k$ avec $0 \leqslant k < n$, un générateur. D'après la relation de Bezout H contient le groupe engendré par g^δ où $\delta = (n, k)$ et il est clairement contenu dans celui-ci. En outre ce dernier est évidement d'ordre $n/\delta = d$. En résumé H est isomorphe au sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par n/d.

(iv) On vient de voir dans le point précédent que l'ordre du sous-groupe engendré par k est égal à $n/(n, k)$.

(v) Chaque élément de $\mathbb{Z}/n\mathbb{Z}$ engendre un sous-groupe, soit $n = \sum_H g(H)$ où la somme est indexée par les sous-groupes H de $\mathbb{Z}/n\mathbb{Z}$ et $g(H)$ est le cardinal des générateurs de H. D'après ce que l'on vient de voir, l'ensemble des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ est indexée par les diviseurs d de n, où à un diviseur d on associe le sous-groupe H engendré par n/d. D'après (iv), l'ensemble des générateurs de (n/d) est en bijection avec l'ensemble $0 \leqslant \lambda < n$ tel que $(\lambda, n) = n/d$, soit en divisant par n/d, avec l'ensemble des $0 \leqslant \alpha < d$ premier avec d, i.e l'ensemble des générateurs de $\mathbb{Z}/d\mathbb{Z}$, d'où le résultat.

(vi) Soit donc G un sous-groupe fini du groupe multiplicatif d'un corps K (commutatif), et soit n le cardinal de G. Si $g \in G$, son ordre est un diviseur de n car le sous-groupe engendré par g est de cardinal son ordre, et le cardinal d'un sous-groupe divise le cardinal du groupe (cf.

cours). Ainsi pour d divisant n, on note A_d (resp. H_d) l'ensemble des éléments de G d'ordre d (reps. divisant d): en particulier on a $H_d = \{g \in G \ / \ g^d = 1\}$. Le corps K étant commutatif, on a $|H_d| \leqslant d$, car le polynôme $X^d - 1$ y a au plus d racines. En outre si $A_d \neq$, alors $|H_d| = d$ car tout élément de A_d engendre un sous-groupe d'ordre d dans lequel tout élément g est tel que $g^d = 1$. Or $A_d \subset H_d$ soit $|A_d| \leqslant \varphi(d)$, l'inégalité $|A_d| \geqslant \varphi(d)$ étant évidente. En résumé soit A_d est vide soit son cardinal est égal à $\varphi(d)$. En reprenant le comptage de la question précédente, $G = \coprod_{d|n} A_d$, on obtient

$$n = \sum_{d|n} \epsilon(d)\varphi(d)$$

où $\epsilon(d)$ est nul si A_d est vide, et égal à 1 sinon. En comparant cette égalité avec celle de (v), on en déduit que $\epsilon(d) = 1$ pour tout $d|n$, soit A_d non vide et en particulier A_n, cqfd.

□

Exercice 2. *(i) Donnez l'ordre de k dans $\mathbb{Z}/n\mathbb{Z}$ et déduisez-en le cardinal de l'ensemble des éléments d'ordre d (resp. d'ordre divisant d) dans $\mathbb{Z}/n\mathbb{Z}$.*

(ii) Donnez le cardinal de l'ensemble des éléments d'ordre divisant d dans $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

(iii) Pour $d = pq$ avec p et q premiers divisant n, donnez le nombre d'éléments d'ordre d dans $(\mathbb{Z}/n\mathbb{Z})^2$;

Preuve : (a) On rappelle que le groupe engendré par k dans $\mathbb{Z}/n\mathbb{Z}$ est celui engendré par $k \wedge n$. En effet comme k est un multiple de $k \wedge n$, on a l'inclusion $(k) \subset (k \wedge n)$. Réciproquement on écrit une relation de Bezout $uk + vn = n \wedge k$ de sorte que modulo n, $n \wedge k$ appartient au groupe engendré par k et donc $(k \wedge n) \subset (k)$. On en déduit alors que l'ordre de k dans $\mathbb{Z}/n\mathbb{Z}$ qui est par définition le cardinal du groupe engendré par k, est $\frac{n}{n \wedge k}$.

(b) Remarquons tout d'abord que si d ne divise pas n, d'après (a) il n'y a aucun élément d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$. Si d divise n, tous les éléments d'ordre d appartiennent au groupe engendré par $(\frac{n}{d})$ qui est isomorphe, en tant que groupe cyclique d'ordre d, à $\mathbb{Z}/d\mathbb{Z}$. Ainsi les éléments d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ sont en bijection avec les éléments d'ordre d de $\mathbb{Z}/d\mathbb{Z}$ qui sont en nombre $\varphi(d)$, où φ est l'indicatrice d'Euler; on rappelle en effet que les éléments d'ordre d de $\mathbb{Z}/d\mathbb{Z}$ en sont les générateurs et correspondent aux entiers $1 \leqslant k < d$ premiers avec d.

Cherchons maintenant les éléments d'ordre divisant d dans $\mathbb{Z}/n\mathbb{Z}$ qui sont donc d'ordre divisant $d \wedge n$ et qui appartiennent au groupe engendré par $\frac{n}{n \wedge d}$ isomorphe à $\mathbb{Z}/(n \wedge d)\mathbb{Z}$. Ainsi, comme précédemment, les éléments d'ordre divisant d de $\mathbb{Z}/n\mathbb{Z}$ sont en bijection avec les éléments d'ordre divisant $n \wedge d$ de $\mathbb{Z}/(n \wedge d)\mathbb{Z}$, qui sont en nombre $n \wedge d$.

(c) Notons pour tout entier e, A_e (resp. B_e) l'ensemble des éléments de $(\mathbb{Z}/n\mathbb{Z})^2$ d'ordre e (resp. d'ordre divisant e) et soit a_e (resp. b_e) son cardinal. Un élément (x, y) appartient à A_e si et seulement si x et y sont d'ordre divisant e dans $\mathbb{Z}/n\mathbb{Z}$, de sorte que pour tout e, $b_e = (e \wedge n)^2$. Par ailleurs B_d est la réunion disjointe de $A_d \coprod A_p \coprod A_q \coprod A_1$, où A_1 est réduit à l'élément nul. De même B_p (resp. B_q) est la réunion disjointe de $A_p \coprod A_1$ (resp. $A_q \coprod A_1$). En prenant les cardinaux, on obtient alors:

- $b_d = (n \wedge d)^2 = a_d + a_p + a_q + 1$,
- $b_p = (n \wedge p)^2 = a_p + 1$ et $b_q = (n \wedge q)^2 = a_q + 1$,

soit $a_d = (n \wedge (pq))^2 - (n \wedge p)^2 - (n \wedge q)^2 + 1$.

□

Exercice 3. *Soit $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ l'application qui à $k \in \mathbb{Z}$ associe sa classe modulo n et m. Précisez le noyau et l'image de π. Donnez alors l'ensemble des $k \in \mathbb{Z}$ tels que*

(i) $k \equiv 2 \bmod 5$ *et* $k \equiv 4 \bmod 7$*;*

(ii) $k \equiv 3 \bmod 10$ *et* $k \equiv 2 \bmod 6$*;*

(iii) $k \equiv 4 \bmod 10$ *et* $k \equiv 2 \bmod 6$*;*

Que peut-on dire de la congruence de k *modulo* 10 *sachant* $k \equiv 3 \bmod 6$ *?*

Preuve : Il s'agit de redémontrer le théorème chinois, c'est à dire que $\mathrm{Ker}\,\pi = (n \vee m)$ où $n \vee m$ est le ppcm de n et m, et $\mathrm{Im}\,\pi = \{(a,b) \ / \ (n \wedge m) | b - a \ \}$. Il est tout d'abord évident que π est un morphisme de groupes; en outre si $k \in \mathrm{Ker}\,\pi$, alors il est divisible d'après le lemme de Gauss par $n \vee m$ de sorte que $\mathrm{Ker}\,\pi \subset (n \vee m)$, l'inclusion réciproque étant évidente. Soit maintenant a, b tels que $b - a$ est divisible par le pgcd (n, m). On écrit une relation de Bezout $un + vm = (n, m)$ et on pose $k = u\frac{n}{(n,m)}b + v\frac{m}{(n,m)}b$. On a alors $k = un\frac{(b-a)}{(n,m)} + a \equiv a \bmod n$; de même on a $k = vm\frac{(a-b)}{(n,m)} + b \equiv b \bmod m$, de sorte que l'ensemble donné est inclus dans l'image de π. La réciproque est évidente car $k = a + \lambda n = b + \mu m$ soit $(b - a) = \lambda n - \mu m$ qui est donc divisible par (n, m). En particulier lorsque n et m sont premiers entre eux, π induit un isomorphisme $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

(i) 5 et 7 sont premiers entre eux, on trouve la solution particulière $k = 32$, l'ensemble des solutions est alors $32 + \lambda 35$ avec $\lambda \in \mathbb{Z}$;

(ii) $(6, 10) = 2$ or 2 ne divise pas $3 - 2 = 1$, il n'y a donc pas de solutions;

(iii) cette fois-ci $2 = (6, 10)$ divise $4 - 2$; une solution particulière est $k = 14$, l'ensemble des solutions est alors $14 + 30\lambda$ avec $\lambda \in \mathbb{Z}$.

D'après ce qui précéde si $k \equiv 3 \bmod 6$, on a alors $k \equiv a \bmod 10$ avec $a - 3$ divisible par 2, soit $a = 1, 3, 5, 7, 9$.

□

Exercice 4. *Résoudre dans* $\mathbb{Z}$ *les congruences suivantes:*

(i) $3x \equiv 4 \bmod 7$*;*

(ii) $9x \equiv 12 \bmod 21$*;*

(iii) $103x \equiv 612 \bmod 676$*.*

Preuve : (i) 3 étant premier avec 7, il est inversible dans $\mathbb{Z}/7\mathbb{Z}$; on calcule rapidement que $3.5 \equiv 1 \bmod 7$, i.e. $5 = 1/3$ dans $\mathbb{Z}/7\mathbb{Z}$ de sorte que l'équation s'écrit $x \equiv 20 \bmod 7$ soit $x \equiv -1 \bmod 7$;

(ii) d'après le théorème chinois, il suffit de vérifier l'équation modulo 3 et 7. Modulo 3 l'équation s'écrit $0.x \equiv 0 \bmod 3$ et est donc toujours vérifiée. Modulo 7, on obtient $2x \equiv -2 \bmod 7$; l'inverse de 2 dans $\mathbb{Z}/7\mathbb{Z}$ est -3, soit donc $x \equiv -1 \bmod 7$. Le résultat final est donc $x \equiv -1 \bmod 7$;

(iii) on calcule rapidement $676 = 2^2.13^2$; par le théorème chinois, on est donc ramené à résoudre $-x \equiv 0 \bmod 4$ et $103x \equiv 105 \bmod 169$. L'algorithme d'euclide fournit $64.103 - 39.169 = 1$ soit donc $x \equiv 64.105 \bmod 69$ soit $x \equiv -40 \bmod 169$ et donc $x \equiv -40 \bmod 676$.

On peut aussi résoudre la congruence $103x \equiv 105 \bmod 13^2$ de proche en proche, de la façon suivante. On la résoud tout d'abord modulo 13 soit $2x \equiv 4 \bmod 13$ soit $x \equiv 2 \bmod 13$. On écrit alors $x = 2 + 13k$ et on est donc ramené à résoudre $206 + 13.103k \equiv 105 \bmod 13^2$ soit $13.103k \equiv -13.8 \bmod 13^2$ soit en simplifiant par 13, $103k \equiv -8 \bmod 13$, soit $2k \equiv -8 \bmod 4$ et donc $k \equiv -4 \bmod 13$ et donc finalement $x \equiv 2 - 4.13 \bmod 13^2$.

□

Exercice 5. *Montrez en utilisant le théorème chinois que* $n^7 \equiv n \bmod 42$.

Preuve: On a $42 = 2.3.7$, il suffit alors de verifier la congruence modulo 2, 3 et 7. Pour 2 et 3, on a clairement $n^7 \equiv n$ et pour 7 le résultat découle du petit théorème de Fermat.

□

Exercice 6. *Donnez les morphismes de groupe* $\mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z}$ *puis ceux de* $\mathbb{Z}/12\mathbb{Z} \longrightarrow \mathbb{Z}/15\mathbb{Z}$. *Trouvez une condition nécessaire et suffisante sur* m *et* n *pour que tout morphisme* $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ *soit nul.*

Preuve : On rappelle qu'un morphisme d'un groupe cyclique de cardinal n dans un groupe G est complètement déterminé par l'image g d'un générateur quelconque telle $g^n = 1_G$, soit g d'ordre divisant n. Dans le premier cas comme 3 et 4 sont premiers entre eux, les seuls éléments d'ordre divisant 3 dans $\mathbb{Z}/4\mathbb{Z}$ sont le seul d'ordre 1 à savoir 0 de sorte que tout morphisme $\mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z}$ est nul.

Dans $\mathbb{Z}/15\mathbb{Z}$ les éléments d'ordre divisant 12 sont donc d'ordre divisant $12 \wedge 15 = 3$ et sont donc $0, 5, 10$, ce qui donne 3 morphismes distincts.

D'après les raisonnements ci-dessus, on en déduit donc qu'une CNS pour qu'il n'y ait pas de morphisme non nul $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ est donc $n \wedge m = 1$.

□

Exercice 7. *Définition, exemples, applications*

*(1) En utilisant la proposition (**??**), justifiez, pour* n *divisant* n', *l'écriture* $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^{n'}}$ *et donnez un sens à:*

$$\overline{\mathbb{F}}_p = \bigcup_{n>1} \mathbb{F}_{p^{n!}}.$$

(2) Montrez les isomorphismes suivant et donnez un générateur du groupe des inversibles des corps en question:

(i) $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(X^2 + X + 1)$;

(ii) $\mathbb{F}_8 \simeq \mathbb{F}_2[X]/(X^3 + X + 1)$;

(iii) $\mathbb{F}_{16} \simeq \mathbb{F}_2[X]/(X^4 + X + 1)$; *donner dans cet isomorphisme l'image de* $\mathbb{F}_4 \subset \mathbb{F}_8$ *et en déduire* $\mathbb{F}_{16} \simeq \mathbb{F}_2[X, Y]/(Y^2 + Y + 1, X^2 + X + 1)$.

(iv) $\mathbb{F}_9 \simeq \mathbb{F}_3[X]/(X^2 + X - 1)$.

Preuve (1) On rappelle que $\mathbb{F}_{p^n}$ est à priori **un** corps de décomposition de $X^{p^n} - X$; afin de fixer précisément les choses, il est pratique de se donner une clôture algébrique $\overline{\mathbb{F}}_p$ dont l'existence est donnée de manière théorie et de noter $\mathbb{F}_{p^n}$ **le** corps de décomposition dans $\overline{\mathbb{F}}_p$ du polynôme $X^{p^n} - X$.
Pour $n' = kn$, on a $p^{n'} - 1 = (p^n - 1)N$ avec $N = (p^n)^{k-1} + \cdots + 1$ et donc

$$X^{p^{n'}} - X = X(X^{p^{nk}-1} - 1) = X(X^{p^n-1} - 1)(X^{(p^n-1)(N-1)} + \cdots + 1)$$

et donc $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^{n'}}$.

Réciproquement supposons $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^{n'}}$; on a vu que $\mathbb{F}_{p^n}^\times$ est cyclique d'ordre $p^n - 1$ de sorte que d'après le théorème de Lagrange implique que $p^n - 1$ divise $p^{n'} - 1$. On effectue la division euclidienne $n' = kn + r$, soit $p^{n'} - 1 \equiv 1^k p^r - 1 \bmod (p^n - 1)$ soit $r = 0$ et donc n divise n'.

Evidemment $\bigcup_{n=1}^{N} \mathbb{F}_{p^{n!}} = \mathbb{F}_{p^{N!}}$ de sorte que $k = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^{n!}}$ est une réunion croissante de corps et est donc un corps; en effet pour $x, y \in k$, il existe n tels que $x, y \in \mathbb{F}_{p^{n!}}$ et $x+y, xy$ sont définis dans $\mathbb{F}_{p^{n!}}$. Il est en outre immédiat que k est algébrique sur $\mathbb{F}_p$ car tout $x \in k$ est un élément d'un $\mathbb{F}_{p^{n!}}$ pour n assez grand. Il reste alors à voir que k est algébriquement clos; soit donc $P(X) \in k(X)$ irréductible et soit $\mathbb{F}_{p^m}$ une extension contenant les coefficients de P et soit L un corps de rupture de P dans $\overline{\mathbb{F}}_p$ sur $\mathbb{F}_{p^m}$; L est alors une extension finie de $\mathbb{F}_{p^m}$ et est donc égale à un certain $\mathbb{F}_{p^r}$ et donc inclus dans $\mathbb{F}_{p^{r!}} \subset k$. Ainsi tout polynôme irréductible sur k est de degré 1 soit k algébriquement clos.

(2) (i) On vérifie rapidement que X^2+X+1 n'a pas de racines dans $\mathbb{F}_2$, étant de degré 2 il y est alors irréductible de sorte que $\mathbb{F}_2[X]/(X^2+X+1)$ est un corps, une extension de degré 2 de $\mathbb{F}_2$ et donc isomorphe à $\mathbb{F}_4$ qui par convention est **le** corps de cardinal 4 contenu dans une clôture algébrique $\overline{\mathbb{F}}_2$ de $\mathbb{F}_2$ fixée une fois pour toute. Comme $\mathbb{F}_4^\times \simeq \mathbb{Z}/3\mathbb{Z}$, tout élément autre que $0, 1$ est un générateur de $\mathbb{F}_4^\times$, soit X et $X+1$.

(ii) De même, on vérifie que X^3+X+1 n'a pas de racines dans $\mathbb{F}_2$; étant de degré 3 il est alors irréductible sur $\mathbb{F}_2$ de sorte que $\mathbb{F}_2[X]/(X^3+X+1)$ est un corps de cardinal 8 et donc isomorphe à $\mathbb{F}_8$. Comme $\mathbb{F}_8^\times \simeq \mathbb{Z}/7\mathbb{Z}$ tout élément autre que $0, 1$ est un générateur du groupe des inversibles, par exemple X.

(iii) Encore une fois X^4+X+1 n'a pas de racines sur $\mathbb{F}_2$ mais cela ne suffit pas pour conclure à son irréductibilité; il nous faut montrer que X^4+X+1 n'a pas de racines dans $\mathbb{F}_4$. Soit donc $x \in \mathbb{F}_4$ n'appartenant pas à $\mathbb{F}_2$; on a alors $x^3 = 1$ de sorte que $x^4+x+1 = x+x+1 = 1 \neq 0$. Ainsi X^4+X+1 n'a pas de racines dans les extensions de degré $\leqslant 4/2$ de $\mathbb{F}_2$ et est donc irréductible sur $\mathbb{F}_2$ de sorte que $\mathbb{F}_2[X]/(X^4+X+1)$ est un corps de cardinal 16 qui est donc isomorphe à $\mathbb{F}_{16}$.
Soit $\chi = X^2+X$, on a alors $\chi^2 = X^4+X^2$ et $\chi^2+\chi+1 = 0$ et $\chi^3 = 1$ de sorte que le sous ensemble $\{0, \chi, \chi^2, \chi^3\}$ de $\mathbb{F}_{16}$ correspond au sous-corps $\mathbb{F}_4$. En outre $X^2+\chi X+1$ n'a pas de racines dans $\mathbb{F}_2[\chi]$ et il y est donc irréductible de sorte que $\mathbb{F}_{16} \simeq \mathbb{F}_2[X,Y]/(Y^2+Y+1, X^2+YX+1)$.

(iv) A nouveau X^2+X-1 n'a pas de racines dans $\mathbb{F}_3$, il y est donc irréductible et $\mathbb{F}_9 \simeq \mathbb{F}_3[X]/(X^2+X-1)$. En outre $\mathbb{F}_9^\times \simeq \mathbb{Z}/8\mathbb{Z}$ de sorte qu'il y a $\varphi(8) = 4$ générateurs et donc 4 non générateurs. On a $X^4 = (X-1)^2 = X^2-2X+1 = -3X+2 = -1$ et X est un générateur de $\mathbb{F}_9^\times$.

□

Exercice 8. *Etude de* $(\mathbb{Z}/n\mathbb{Z})^\times$*:*

(a) Montrez que $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ *est isomorphe à* $(\mathbb{Z}/n\mathbb{Z})^\times$*. En déduire que* $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ *est abélien.*

(b) Soit $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$*. Prouver que* $(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$*.*

(c) Soit p *premier impair et* $\alpha \geqslant 2$*.*

(i) Montrez que pour tout $k \in \mathbb{N}$*, il existe* $\lambda \in \mathbb{N}\backslash\{0\}$ *premier avec* p *tel que* $(1+p)^{p^k} = 1+\lambda p^{k+1}$*. En déduire l'ordre de* $1+p$ *dans* $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$*.*

(ii) Montrez que $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$*;*

(iii) En considérant le morphisme naturel, $\psi : (\mathbb{Z}/p^\alpha\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$*, montrez que* $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ *contient un élément* x *d'ordre* $p-1$*:*

(iv) Montrez $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/(\varphi(p^\alpha)\mathbb{Z} \simeq \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$*;*

- *Le cas de 2.*

  (i) Déterminer $(\mathbb{Z}/2\mathbb{Z})^\times$ *et* $(\mathbb{Z}/4\mathbb{Z})^\times$*;*

  (ii) Soit $\alpha \geqslant 3$ *et* $k \in \mathbb{N}$*. Montrez que* $5^{2^k} = 1 + \lambda 2^{k+2}$ *avec* λ *impair. En déduire l'ordre de* 5 *dans* $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$*.*

  (iii) En considérant le morphisme canonique de $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ *dans* $(\mathbb{Z}/4\mathbb{Z})^\times$*, montrer que* $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{\alpha-2})$*.*

Preuve: (a) Considérons les deux morphismes de groupes suivant

$$\begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z})^\times & \xrightarrow{\phi} & \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \\ a & \longmapsto & k \mapsto ak \end{array}$$

$$\begin{array}{ccc} \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) & \xrightarrow{\psi} & (\mathbb{Z}/n\mathbb{Z})^\times \\ \varphi & \longmapsto & \varphi(1) \end{array}$$

On vérifie aisément que sont des morphismes inverses l'un de l'autre, ce sont donc des isomorphismes.
Remarque: La morale de cette question est qu'un morphisme d'un groupe cyclique vers un groupe, est caractérisé par la donnée de l'image d'un générateur.

(b) Le lemme chinois donne

$$\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z} \tag{1}$$

le résultat découle alors du fait que cet isomorphisme induit l'isomorphisme $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq \prod_{i=1}^{r} \mathrm{Aut}(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})$. En effet soit $\phi \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$; ϕ est caractérisé par $\phi(1)$. Par l'isomorphisme (**??**), 1 s'envoie sur $(1, \cdots, 1)$. Notons $e_i = (0, \cdots, 0, 1, 0, \cdots, 0)$, il suffit alors de montrer que $\phi(e_i)$ appartient au sous-groupe engendré par e_i. Or $p_i^{\alpha_i} e_i = 0$ donc $p_i^{\alpha_i}\phi(e_i)$ de sorte que $\phi(e_i)$ est d'ordre une puissance de p_i, d'où le résultat.

(c) (i) On raisonne par récurrence: pour $k = 0$, $(1+p)^{p^0} = 1+p = 1+p^{0+1}$ et pour $k = 1$ par la formule du binôme de Newton, on a $(1+p)^p = 1+p^2\lambda_1$ avec $\lambda_1 = (1+p(p-1)/2+\cdots+p^{p-2})$, soit $\lambda_1 \equiv 1 \bmod p$. Supposons donc le résultat vrai au rang k:

$$(1+p)^{p^{k+1}} = (1+\lambda_k p^{k+1})^p = 1+\lambda_{k+1}p^{k+2}$$

en posant $\lambda_{k+1} = \lambda_k + p^k \sum_{\alpha=2}^{p} \binom{\alpha}{p} \lambda_k^\alpha p^{(\alpha-2)(k+1)}$. Comme $k > 1$, on a $\lambda_{k+1} \equiv \lambda_k \bmod p$.

Ainsi $(1+p)^{p^{\alpha-1}} \equiv 1 \bmod p^\alpha$ de sorte que l'ordre de $(1+p)$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ divise $p^{\alpha-1}$ et donc de la forme p^k pour $k \leqslant \alpha - 1$. En outre on a $(1+p)^{p^k} = 1+\lambda_k p^{k+1}$ avec λ_k non divisible par p; en particulier $(1+p)^{p^{\alpha-2}} \not\equiv 1 \bmod p^\alpha$, de sorte que l'ordre de $1+p$ est $p^{\alpha-1}$.

(ii) D'après l'exercice précédent, $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p-1$.

(iii) Le morphisme ψ est clairement surjectif. Soit donc y un antécédent d'un générateur h de $(\mathbb{Z}/p\mathbb{Z})^\times$; l'ordre m de y est alors un multiple de $p-1$ (car $1 = \psi(y^m) = h^m$): $m = (p-1)k$, de sorte que $x = y^k$ est d'ordre $p-1$. En outre le noyau de ψ est le groupe engendré par $(1+p)$ de sorte que $\psi(x)$ est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$.

(iv) Soit $u = (1+p)x$ et soit m son ordre; $1 = \psi(u^m) = \psi(u)^m = \psi(x)^m$, soit $p-1$ divise m et donc $u^m = (1+p)^m$ soit $p^{\alpha-1}$ divise m. En outre $u^{(p-1)p^{\alpha-1}} = 1$ et donc u est un générateur de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.

(d) (i) On a de manière directe $(\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$ et $(\mathbb{Z}/4\mathbb{Z})^\times = \{1, -1\} \simeq \mathbb{Z}/2\mathbb{Z}$.

(ii) On raisonne à nouveau par récurrence, les cas $k = 0$ et $k = 1$ étant directs. Supposons donc que $5^{2^k} = 1+\lambda_k 2^{k+2}$ avec λ_k impair. On a alors $5^{2^{k+1}} = (1+\lambda_k 2^{k+2})^2 = 1+2^{k+3}(\lambda_k+2^{k+1}\lambda_k^2)$ d'où le résultat en posant $\lambda_{k+1} = \lambda_k + \lambda_k^2 2^{k+1} \equiv \lambda_k \bmod 2$. Comme précédemment, on en déduit que 5 est d'ordre $2^{\alpha-2}$ dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$.

(iii) Le morphisme canonique $\phi : (\mathbb{Z}/2^\alpha\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/4\mathbb{Z})^\times$ induit un isomorphisme de $\{1, -1\}$ sur $(\mathbb{Z}/4\mathbb{Z})^\times$. On en déduit donc un isomorphisme $f : (\mathbb{Z}/2^\alpha\mathbb{Z}) \longrightarrow \operatorname{Ker}\phi \times \{1, -1\}$ avec $f(x) = (x, 1)$ pour $x \equiv 1 \bmod 4$ et $f(x) = (-x, -1)$ pour $x \equiv 3 \bmod 4$. En outre $\operatorname{Ker}\phi$ contient le groupe engendré par 5 et pour des raisons de cardinalité, on a $\operatorname{Ker}\phi = (5)$ qui est donc cyclique d'ordre $2^{\alpha-2}$, d'où le résultat.

□

Exercice 9. *Pour $n > 0$, on note $\mathcal{S}_n$ le groupe des permutations de l'ensemble $\{1, \cdots, n\}$, et $\mathcal{A}_n$ son sous-groupe des permutations paires.*

(a) Montrez que $\mathcal{S}_n$ est engendré par les systèmes suivants et pas par un sous-ensemble strict:

(i) les transpositions $(1, i)$ pour $i = 2, \cdots, n$;

(ii) les transpositions $(i, i + 1)$ pour $i = 1, \cdots, n - 1$;

(iii) le cycle $c_n = (1, \cdots, n)$ et la transposition $\tau = (1, 2)$.

(b) Montrez que $\mathcal{A}_n$ pour $n \geqslant 3$, est engendré par les 3-cycles.

Preuve: (a) On part du fait que $\mathcal{S}_n$ est engendré par les transpositions $(i\ j)$. La technique est alors de montrer que toutes ces transpositions appartiennent au sous-groupe engendré par les éléments que l'on considère.

(i) On a $(i\ j) = (1\ i) \circ (1\ j) \circ (1\ i)$; de plus si $2 \leqslant i_0 \leqslant n$, i_0 est laissé fixe par toutes les transpositions $(1\ i)$ pour $i \neq i_0$ de sorte que $\mathcal{S}_n$ ne peut pas être engendré par un sous-ensemble strict de celui considéré.

(ii) Pour $1 \leqslant i < j - 1 \leqslant n - 1$, on a $(i\ j) = (j - 1\ j) \circ (i\ j - 1) \circ (j - 1\ j)$, le résultat découle alors d'une récurrence simple sur $j - i$; soit $1 \leqslant i - 0 < n$, l'intervalle $\{1, \cdots, i_0\}$ est laissé globalement stable par tous les éléments $(i, i + 1)$ pour $i \neq i_0$, de sorte que $\mathcal{S}_n$ ne peut pas être engendré par un sous-ensemble strict de celui considéré.

(iii) On a $(i, i + 1) = c_n^{i-1} \circ \tau \circ c_n^{-i+1}$; le résultat découle alors de (ii).

(b) Le résultat est clair pour $n = 3$. Pour $n \geqslant 4$, si $a \neq b$ et $b \neq c$ alors $(a\ b) \circ (b\ c) = (a\ b\ c)$; ainsi si a, b, c, d sont deux à deux distincts, $(a\ b) \circ (c\ d) = (a\ b\ c) \circ (b\ c\ d)$, d'où le résultat.

□

Exercice 10. *Etude des décompositions en cycles à supports disjoints de certains éléments de $\mathcal{S}_n$.*

(a) Donnez la décomposition en cycles à supports disjoints de $(1\ 2\ 3) \circ (2\ 4) \circ (1\ 3)$ et de $(1\ 2\ \cdots\ n-1) \circ (1\ n)$.

(b) Classes de conjugaisons

(i) Quelle est la décomposition en cycles à supports disjoints de $\sigma s \sigma^{-1}$ en fonction de celle de s ?

(ii) Quel est l'ordre maximal d'un élément de $\mathcal{S}_5$?

(iii) Quelle est la décomposition en cycles à supports disjoints de c^k, où $c = (1, \cdots, n)$?

(c) Commutants:

(i) Donnez le centre de $\mathcal{S}_n$ et celui de $\mathcal{A}_n$.

(ii) Quel est le commutant de $c = (1, \cdots, n)$?

(iii) Donnez une formule du cardinal du commutant de $\sigma \in \mathcal{S}_n$ en fonction de sa décomposition en cycles à supports disjoints.

Preuve: (a) $\sigma = (1\ 2\ 3) \circ (2\ 4) \circ (1\ 3)$ est bien une décomposition en cycles mais pas à supports disjoints; on vérifie sans peine que $\sigma = (3\ 2\ 4)$. De même $(1\ 2\ \cdots\ n{-}1) \circ (1\ n) = (1\ n\ 2\ \cdots\ n{-}1)$.

(b) (i) Si c est un cycle de longueur l: $c = (x_1\ x_2\ \cdots\ x_l)$ alors pour tout $\sigma \in \mathcal{S}_n$, $\sigma \circ c \circ \sigma^{-1}$ est le cycle de longueur l: $(\sigma(x_1)\ \sigma(x_2)\ \cdots\ \sigma(x_l))$. Ainsi si $s = c_1 \circ \cdots \circ c_r$ est la décomposition en cycle à supports disjoints de s alors $\sigma \circ s \circ \sigma^{-1} = (\sigma \circ c_1 \sigma^{-1}) \circ \cdots \circ (\sigma \circ c_r \circ \sigma^{-1})$ est celle de $\sigma \circ s \circ \sigma^{-1}$.

(ii) Si $\sigma = c_1 \circ \cdots \circ c_r$ est la décomposition en cycles à supports disjoints de σ, chaque cycle est d'ordre sa longueur et ces cycles commutent car leurs supports sont disjoints, d'où l'ordre de σ est le ppcm des longueurs des cycles c_i pour $1 \leqslant i \leqslant r$. En particulier dans $\mathcal{S}_5$, on trouve que l'ordre maximal d'un élément est 6.

(iii) Soit $x \in \{1, \cdots, n\}$ et cherchons quel est le cardinal de l'orbite de x sous c^k:

$$(c^k)^i(x) = x \iff n | ki \iff \frac{n}{(n,k)} | i$$

de sorte que l'orbite de x sous c^k est toujours de longueur $n/(n,k)$. La décomposition en cycles à supports disjoints de c^k est donc constitué de (n,k) cycles de longueur $n/(n,k)$.

(c) (i) Pour $n = 1, 2$, $\mathcal{S}_n$ est commutatif. Soit donc $n \geqslant 3$ et soit σ dans le centre de $\mathcal{S}_n$. On a alors $\sigma \circ (i\ j) \circ \sigma^{-1} = (\sigma(i)\ \sigma(j)) = (i\ j)$ de sorte que pour tout $i \neq j$, on a $\sigma(\{i,j\}) = \{i,j\}$. Comme $n \geqslant 3$, pour i, j, k distintcs deux à deux, on a $\{i\} = \{i,j\} \cap \{i,k\}$ et donc $\{\sigma(i)\} = \{\sigma(i), \sigma(j)\} \cap \{\sigma(i), \sigma(k)\} = \{i,j\} \cap \{i,k\} = \{i\}$, soit $\sigma = \mathrm{Id}$.

Pour $n \leqslant 3$, $\mathcal{A}_n$ est commutatif; soient donc $n \geqslant 4$ et σ dans le centre de $\mathcal{A}_n$. Pour tout a, b, c des éléments deux à deux distincts de $\{1, \cdots, n\}$, on a $\sigma \circ (a\ b\ c) \circ \sigma^{-1} = (\sigma(a)\ \sigma(b)\ \sigma(c)) = (a\ b\ c)$ et donc $\{a, b, b\} = \{\sigma(a), \sigma(b), \sigma(c)\}$. Comme $n \geqslant 4$, soient a, b, c, d des éléments deux à deux distincts; $\{a\} = \{a, b, c\} \cap \{a, b, d\} \cap \{a, c, d\}$. En procédant comme précédemment, on en déduit à nouveau que $\sigma = \mathrm{Id}$.

(ii) Soit σ dans le commutant de c; $\sigma \circ c \circ \sigma^{-1} = (\sigma(1)\ \sigma(2)\ \cdots\ \sigma(n)) = (1\ 2\ \cdots\ n)$ de sorte que $\sigma(i) = c^{i-1} \circ \sigma(1)$ soit $\sigma = c^k$ avec $k = \sigma(1)$.

(iii) On écrit la décomposition en cycles à supports disjoints de σ sous la forme $\sigma = \prod_{i,j} c_i^j$ où c_i^j est un cycle de longueur j. On en déduit alors que s est dans le commutant de σ, si et seulement si pour tout i, j, il existe un k tel que $s \circ c_i^j s^{-1} = c_k^j$, i.e. s induit une permutation des c_i^j pour tout j fixé. Si on note r_j le nombre de cycles c_i^j de longueur j, on a $\prod_{j=1}^n (r_j!)$ telle permutation. Une telle permutation ν étant fixé, dénombrons les s qui l'induisent, i.e. telle que $s \circ c_i^j \circ s^{-1} = c_{\nu(i)}^j$. La donnée d'un tel s est caractérisée par les $s(a_i^j)$ dans le support de $c_{\nu(i)}^j$ où a_i^j est dans le support de c_i^j; pour i, j fixé, on a donc j choix. Finalement le commutant de σ est donc de cardinal $\prod_{j=1}^n (r_j)! j^{r_j}$.

□

Exercice 11. *Nous allons étudier la simplicité de* $\mathcal{A}_n$.

(a) Etudiez les cas $n \leqslant 4$.

(b) $n = 5$*: soit* H *un sous-groupe distingué de* $\mathcal{A}_5$ *non trivial:*

(i) montrez que les éléments d'ordre 2 *sont conjugués dans* $\mathcal{A}_5$*;*

(ii) montrez que si H *contient un* 5*-cycle, il les contient tous,*

(iii) en déduire que $H = \mathcal{A}_5$*, i.e. que* $\mathcal{A}_5$ *est simple*

(c) $n \geqslant 5$*: soit* H *un sous-groupe distingué de* $\mathcal{A}_n$ *non trivial et soit* $\sigma \in H$ *différent de l'identité. Soit alors* $a \in \{1, \cdots, n\}$ *tel que* $b = \sigma(a) \neq a$.

(i) Soient $c \in \{1, \cdots, n\} \backslash \{a, b, \sigma(b)\}$ *et* $\tau = (acb)$*. Montrez que* $\rho = \tau\sigma\tau^{-1}\sigma^{-1}$ *"dérange" au plus* 5 *éléments et que* $\rho \neq \mathrm{Id}$.

(ii) Soit $E \subset \{1, \cdots, n\}$ *de cardinal* 5 *contenant le support de* ρ*. En considérant l'application* $i : \mathcal{A}_5 \simeq \mathcal{A}(E) \longrightarrow \mathcal{A}_n$ *définie par* $i(\sigma)_{|E} = \sigma$ *et* $i(\sigma)_{\{1,\cdots,n\}\backslash E} = \mathrm{Id}$ *et en remarquant que* $\rho \in H$*, montrez la simplicité de* $\mathcal{A}_n$.

(iii) En déduire que $D(\mathcal{A}_n) = D(\mathcal{S}_n) = \mathcal{A}_n$.

(d) Montrez que pour $n \geqslant 5$*, les seuls sous-groupes distingués de* $\mathcal{S}_n$ *sont:* $\{\mathrm{Id}\}$*,* $\mathcal{A}_n$ *et* $\mathcal{S}_n$*. En déduire que si* H *est un sous-groupe de* $\mathcal{S}_n$ *avec* $n \geqslant 5$*, d'indice* k *avec* $1 < k < n$*, alors* $k = 2$ *et* $H \simeq \mathcal{A}_n$.

Preuve: (a) On vérifie immédiatement que le groupe

$$V_4 = \{Id, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

est un sous-groupe distingué de $\mathcal{A}_4$ qui n'est donc pas simple.

(b) (i) Les éléments d'ordre 2 dans $\mathcal{A}_5$ sont de la forme $\sigma = (a\ b)(c\ d)$ pour a, b, c, d distincts deux à deux. Soit alors $\sigma' = (a'\ b')(c'\ d')$ pour des éléments a', b', c', d' distincts deux à deux et soit $s \in \mathcal{S}_5$ tel que $s(a) = a'$, $s(b) = b'$, $s(c) = c'$ et $s(d) = d'$. Si on note e et e' les éléments restant, on a forcément $s(e) = e'$. On a alors $\sigma' = s \circ \sigma \circ s^{-1}$. Considérons aussi $t = (c'\ d') \circ s$, on a encore $\sigma' = t \circ \sigma \circ t^{-1}$ et s ou t appartient à $\mathcal{A}_5$; on a donc montré que deux éléments quelconques d'ordre 2 de $\mathcal{A}_5$ étaient conjugués dans $\mathcal{A}_5$ et pas seulement dans $\mathcal{S}_5$.

(ii) Soit $c = (1\ a\ b\ c\ d)$ un 5-cycle et soit $\sigma, \tau \in \mathcal{S}_5$ défini par $\sigma(1) = 1 = \tau(1)$, $\sigma(a) = 2 = \tau(b)$, $\sigma(b) = 3 = \tau(d)$, $\sigma(c) = 4 = \tau(a)$ et $\sigma(d) = 5 = \tau(c)$. On a alors $\sigma \circ c \circ \sigma^{-1} = (1\ 2\ 3\ 4\ 5) = \tau \circ c^2 \circ \tau^{-1}$ et $\tau = (2\ 4\ 5\ 3) \circ \sigma$, de sorte que σ ou τ appartient à $\mathcal{S}_5$. Finalement si un sous-groupe distingué H de $\mathcal{A}_5$, contient un 5-cycle, il contient le 5-cycle $(1\ 2\ 3\ 4\ 5)$ et les contient donc tous.

(iii) Nous allons montrer que $H = \mathcal{A}_5$ par des raisons de cardinalité; $\mathcal{A}_5$ contient 60 éléments dont $15 = \binom{2}{5}\binom{2}{3}/2$ éléments d'ordre 2, $20 = 2\binom{3}{5}$ éléments d'ordre 3 et 24 éléments d'ordre 5. Si H contient un élément d'ordre 3 (resp. 2, resp. 5) alors il les contients tous car ils sont tous conjugués dans $\mathcal{A}_5$ et que H est distingué. D'après le théorème de Lagrange, le cardinal de H divise 60. On en déduit donc que H ne peut contenir des éléments tous du même ordre (autre que l'identité) car $25 = 24 + 1$, $21 = 20 + 1$ et $16 = 15 + 1$ ne divisent pas 60. On en déduit alors que le cardinal de H est supérieur ou égal à $1 + 15 + 20 = 36 \geqslant 60/2$ soit $H = \mathcal{A}_5$.

(c) (i) $\rho = \tau \circ (\sigma\tau^{-1}\sigma^{-1})$ appartient à H et $\rho = (a\ c\ b) \circ (\sigma(a)\ \sigma(b)\ \sigma(c))$ de sorte que le support de ρ est inclu dans $\{a, b, c, \sigma(b), \sigma(c)\}$ et est donc de cardinal inférieur ou égal à 5. De plus $\rho \neq \mathrm{Id}$ car $\rho(b) = \tau \circ \sigma(b) \neq b$ car $c \neq \sigma(b)$.

(ii) Soit $H' = i^{-1}(H)$ qui est donc distingué dans $\mathcal{A}_5$ et n'est pas réduit à l'identité car $\rho_{|E} \neq \mathrm{Id}$, d'où $H' = \mathcal{A}_5$. Soit alors c un 3-cycle de $\mathcal{A}_5$; $i(c)$ est aussi un 3-cycle dans H. Comme les 3-cycles sont conjugués dans $\mathcal{A}_n$, H les contient tous, et comme ils engendrent $\mathcal{A}_n$ alors $H = \mathcal{A}_n$.

(iii) On a bien sûr $D(\mathcal{A}_n) \subset D(\mathcal{S}_n) \subset \mathcal{A}_n$ et $\mathcal{D}(\mathcal{A}_n)$ est un sous-groupe distingué de $\mathcal{A}_n$ non réduit à l'identité car $\mathcal{A}_n$ n'est pas abélien pour $n \geqslant 5$; on en déduit donc $\mathcal{A}_n = D(\mathcal{A}_n)$.

(d) Soit H un sous-groupe distingué de $\mathcal{S}_n$, alors $H \cap \mathcal{A}_n$ est un sous-groupe distingué de $\mathcal{A}_n$, il est donc égal à $\mathcal{A}_n$ ou bien il est réduit à l'identité. Traitons séparément ces deux cas:

- $H \cap \mathcal{A}_n = \mathcal{A}_n$: $\mathcal{A}_n$ étant d'indice 2 dans $\mathcal{S}_n$, le théorème de Lagrange nous donne $H = \mathcal{A}_n$ ou $H = \mathcal{S}_n$;

- $H \cap \mathcal{A}_n = \{\mathrm{Id}\}$: la signature restreinte à H donne alors un morphisme injectif de H vers $\mathbb{Z}/2\mathbb{Z}$, de sorte que si H n'est pas réduit à l'identité, il est de la forme $\{\mathrm{Id}, \tau\}$ avec τ d'ordre 2 vérifiant pour tout $\sigma \in \mathcal{S}_n$, $\sigma\tau\sigma^{-1} = \tau$ soit τ appartient au centre de $\mathcal{S}_n$ qui comme on l'a vu est réduit à l'identité.

Soit donc H un sous-groupe de $\mathcal{S}_n$ d'indice k avec $1 < k < n$; on considère l'action de $\mathcal{S}_n$ sur $\mathcal{S}_n/H$ par translation à gauche. On obtient ainsi un morphisme non trivial $\phi : \mathcal{S}_n \longrightarrow \mathcal{S}_k$ qui pour des raisons de cardinalité ne peut pas être injetif; le noyau $\mathrm{Ker}\,\phi$ est alors un sous-groupe distingué de $\mathcal{S}_n$ distinct de $\mathcal{S}_n$ soit $\mathrm{Ker}\,\phi = \mathcal{A}_n$. Or comme $g\overline{h} = \overline{gh} = \overline{h}$ pour tout $g \in \mathrm{Ker}\,\phi$, on en déduit que $\mathrm{Ker}\,\phi \subset H$ et donc $\mathcal{A}_n \subset H$ soit $H = \mathcal{A}_n$ car les sous-groupes de $\mathcal{S}_n$ contenant $\mathcal{A}_n$ sont d'indice divisant 2, soit $H = \mathcal{A}_n$ ou $H = \mathcal{S}_n$, or $H = \mathcal{S}_n$ est exclu.

□

Exercice 12. *Montrez que $PGL_2(\mathbb{F}_3) \simeq \mathcal{S}_4$ et $PGL_2(\mathbb{F}_5) \simeq \mathcal{S}_5$.*

Preuve: (a) On fait agir $PGL_2(\mathbb{F}_3)$ sur $\mathbb{P}^1(\mathbb{F}_3)$ naturellement, i.e. $M.\overline{\binom{x}{y}} := \overline{M\binom{x}{y}}$; $\mathbb{P}^1(\mathbb{F}_3)$ étant de cardinal 4, on en déduit un morphisme $PGL_2(\mathbb{F}_3) \longrightarrow \mathcal{S}_4$ qui est injectif; en effet si pour tout vecteur v de $\mathbb{F}_3^2$, v est vecteur propre pour une valeur propre λ_v de M, c'est un exercice classique d'algèbre linéaire de montrer que λ_v est indépendant de v et donc $M = \lambda\mathrm{Id}$. Or $PGL_2(\mathbb{F}_3)$ est de cardinal $(9-1)(9-3)/2 = 24$, d'où le résultat.

(b) On fait de même agir $PGL_2(\mathbb{F}_5)$ sur $\mathbb{P}^1(\mathbb{F}_5)$ et on obtient ainsi un morphisme injectif $PGL_2(\mathbb{F}_5) \longrightarrow \mathcal{S}_6$. En outre $PGL_2(\mathbb{F}_5)$ est de cardinal 120; le résultat découle alors du fait général suivant: tout sous-groupe d'indice n de $\mathcal{S}_n$ est isomorphe à $\mathcal{S}_{n-1}$.

□

Exercice 13. *Un p-groupe est un groupe de cardinal une puissance de p (p premier). Montrez que le centre d'un p-groupe n'est pas réduit à l'élément neutre et en déduire qu'un p-groupe G possède des sous-groupes distingués de tous ordres (divisant $|G|$ bien sûr!).*

Preuve: On fait agir G sur lui-même par automorphismes intérieurs. L'équation aux classes s'écrit: $|G| = \sum_{x \in \mathcal{O}} |x|$, où $\mathcal{O}$ désigne l'ensemble des orbites. En mettant de côté les orbites de cardinal 1, on obtient $|G| = |Z_G| + \sum_{x \in \mathcal{O}^1} |x|$, où $\mathcal{O}^1$ désigne l'ensemble des orbites de cardinal strictement supérieur à 1; en effet une orbite x est réduite à un élément g si et seulement si g appartient au centre Z_G de G. En outre $|x| = [G : G_x]$, où G_x est le stabilisateur d'un élément quelconque de l'orbite de x; ces stabilisateurs sont tous conjugués sous G. Ainsi $|x|$ est divisible

par p et donc $Z_G \equiv 0 \bmod p$; en notant que $|Z_G| \geqslant 1$ car l'élément neutre appartient au centre de G, on en déduit que $|Z_G| \geqslant p$, i.e. Z_G n'est pas réduit à l'élément neutre.
Montrons qu'un p-groupe G admet des sous-groupes de tout ordre divisant $|G|$; on raisonne par récurrence sur r tel que $|G| = p^r$. Si $r = 1$ le résultat est évident; supposons le résultat vrai jusqu'au rang r. Soit $0 < s < r$. D'après ce qui précède, le centre de G n'est pas réduit à l'élément neutre. Si G n'est pas commutatif, le résultat découle par exemple des théorèmes de structure des groupes abéliens de type fini. Supposons donc $Z_G \neq G$, de cardinal p^k. Si $s \geqslant k$, le résultat découle du fait que Z_G commutatif, possède un sous-groupe de cardinal p^k. Supposons $k < s$; d'après l'hypothèse de récurrence, G/Z_G possède un sous-groupe $\overline{H}$ de cardinal p^{k-s} et $\pi^{-1}(\overline{H})$, où $\pi : G \longrightarrow G/Z_G$ est le morphisme naturel, est un sous-groupe de cardinal p^s.

□

Exercice 14. *Soit G un groupe fini, p le plus petit facteur premier de $|G|$, H un sous groupe d'indice p. Montrer que H est distingué dans G.*

Preuve: On fait agir H sur $E = G/H$ par translation à gauche; l'équation aux classes s'écrit $p = \sum_{x\in\mathcal{O}} |x|$, où $\mathcal{O}$ désigne l'ensemble des orbites. On sépare cette somme en deux en différentiant les orbites de cardinal 1: $p = k + \sum_{x\in\mathcal{O}^1}[G : G_x]$, où $\mathcal{O}^1$ est l'ensemble des orbites de cardinal supérieur strictement à 1, et G_x est le stabilisateur d'un élément quelconque de l'orbite x; G_x est un sous-groupe de G et d'après le théorème de Lagrange, $[G : G_x]$ est un diviseur de $|G|$ et est donc supérieur ou égal à p. Or on a $k \geqslant 1$ car H est stable sous l'action de H; ainsi $\mathcal{O}^1$ est vide, soit toutes les orbites sont de cardinal 1, i.e. H est distingué dans G; en effet pour tout $g \in G$, on a $\overline{hg} = \overline{g}$, i.e. pour tout $(g, h) \in G \times H$, il existe $h_1 \in H$ tel que $hg = gh_1$, soit $gHg^{-1} \subset H$.

□

Exercice 15. *Soit H un sous-groupe d'indice n de $\mathcal{S}_n$. Montrer que H est isomorphe à $\mathcal{S}_{n-1}$. Indication: On traitera les cas $n \leqslant 4$ séparèment. Pour $n \geqslant 5$ considérer "le" morphisme $\phi : \mathcal{S}_n \to \mathcal{S}(\mathcal{S}_n/H)$. Montrer que ϕ est injectif et donner l'image de H.*

Preuve: Considérons le cas $n \geqslant 5$ de sorte que $\mathcal{A}_n$ est simple et que les sous-groupes distingués de $\mathcal{S}_n$ sont $\{1\}$, $\mathcal{A}_n$ et $\mathcal{S}_n$. On considère l'action par translation à gauche de $\mathcal{S}_n$ sur $\mathcal{S}_n/H$, ce qui donne un morphisme $\varphi : \mathcal{S}_n \longrightarrow \mathcal{S}(\mathcal{S}_n/H)$; son noyau qui est un sous-groupe distingué. Or si $\sigma \in \operatorname{Ker}\varphi$, on a $\overline{\sigma h} = \overline{h}$, soit $\sigma \in H$, de sorte que $\operatorname{Ker}\varphi \subset H$; or H étant d'indice n dans $\mathcal{S}_n$, $\operatorname{Ker}\varphi$ ne peut qu'être le sous-groupe trivial. Ainsi $\varphi(H)$ est un sous-groupe de cardinal $(n-1)!$, laissant stable l'élément $\overline{\mathrm{Id}}$, de sorte que $\varphi(H)$ est inclu dans un sous-groupe de $\mathcal{S}(\mathcal{S}_n/H)$ isomorphe à $\mathcal{S}_{n-1}$; par cardinalité on en déduit $H \simeq \mathcal{S}_{n-1}$.

□

Exercice 16. *(*) On va montrer le théorème de Wedderburn, à savoir que tout corps fini est commutatif.*

(i) Soit k un corps fini et Z son centre de cardinal q; montrez que q est une puissance d'un nombre premier p et que $|k| = q^n$, pour $n \in \mathbb{N}$.

(ii) On suppose k non commutatif, soit $n > 1$, et on fait opérer $k^\times$ sur lui-même par automorphismes intérieurs. On note $\omega(x)$ l'orbite de $x \in k^\times$ et $k_x^\times$ son stabilisateur. Montrez que $|k_x| = q^d$ pour un diviseur d de n et donnez le cardinal de $\omega(x)$.

(iii) Soit $\Phi_n(X)$ le n-ième polynôme cyclotomique; montrez que $\Phi_n(q)$ divise le cardinal de $\omega(x)$ pour $x \notin Z$.

(iv) En écrivant l'équation aux classes montrez que $\Phi_n(q)$ divise $q-1$.

(v) Montrez que si $z \in \mathbb{C}$ est de module 1, alors $|q-z| > q-1$ et conclure.

Preuve : (i) k est un Z-espace vectoriel de dimension finie n, soit $|k| = |Z|^n$.

(ii) On considère le morphisme de groupe $y \in k^\times \longrightarrow (x \mapsto yxy^{-1}) \in \mathcal{S}(k^\times)$; soit $\omega(x) = \{yxy^{-1} \ / \ y \in k^\times\}$ l'orbite de x et $k_x^\times = \{y \in k^\times \ / \ xy = yx\}$ le stabilisateur de x: on note $k_x = k_x^\times\{0\}$. D'après le théorème de Lagrange, le cardinal de $k_x^\times$ divise q^n-1; en outre k_x est un Z-espace vectoriel de dimension d soit $|k_x| = q^d$ avec q^d-1 divisant q^n-1. Or si $n = ad+r$ avec $0 \leqslant r < d$ alors $q^n - 1 = (q^d)^a q^r - 1 \equiv q^r - 1 \bmod q^d - 1$ et donc $r = 0$ soit d divise n.
Remarque: Pour ceux qui sont familiers des espaces vectoriels sur des corps non commutatifs, on aurait pu dire que k est un k_x-espace vectoriel, soit $q^n = (q^d)^r$ et donc d divise n.

Ainsi l'orbite de x est de cardinal $\frac{q^n-1}{q^d-1}$ et donc $x \in Z$ si et seulement si $d = n$.

(iii) Pour $x \notin Z$ alors $d|n$ et $d \neq n$. Or on a $\frac{X^n-1}{X^d-1} = \Phi_n(X) \prod_{\substack{d'|n \\ n \neq d'|d}} \Phi_{d'}(X)$ et donc $\Phi_n(q)$ divise $\frac{q^n-1}{q^d-1}$.

(iv) L'équation aux classes s'écrit

$$q^n - 1 = q - 1 + \sum_{n \neq d|n} \alpha_d \frac{q^n-1}{q^d-1}$$

où α_d est le nombre d'orbites de cardinal $\frac{q^n-1}{q^d-1}$ de sorte que $\Phi_n(q)$ divise $q-1$.

(v) Pour tout $z \neq 1$ de module 1, on a $|q-z| > q-1$ et donc pour $n > 1$, on a $\Phi_n(q) > q-1$ et ne peut donc pas diviser $q-1$, de sorte que $n = 1$ et donc $k = Z$ est commutatif.