Partiel du 11 décembre 2018

Exercice 1. Le groupe multiplicatif $(\mathbb{Z}/11\mathbb{Z})^*$ est-il cyclique ? Si oui, donner un générateur, et si non, donner un court argument.

Éléments de correction de l'exercice 1. Le groupe multiplicatif $(\mathbb{Z}/11\mathbb{Z})^*$ est cyclique car c'est le groupe multiplicatif du corps fini $\mathbb{Z}/11\mathbb{Z}$.

La classe de 2 est un générateur. En effet $2^5 = 32 \equiv -1 \mod 11$ donc 2 est bien d'ordre 10 dans $(\mathbb{Z}/11\mathbb{Z})^*$.

Exercice 2.

a) Soient G un groupe et $Z(\mathrm{G})$ son centre. Supposons que $\mathrm{G}/Z(\mathrm{G})$ soit cyclique. Montrer que G est abélien.
   Donner un exemple de groupes $\mathrm{H} \lhd \mathrm{G}$ tels que H et G/H soient abéliens mais pas G.

b) Montrer que si $|\mathrm{G}| = pq$, pour p et q des nombres premiers, alors G est abélien ou $Z(\mathrm{G}) = 1$.

Éléments de correction de l'exercice 2. Voir feuille d'exercices 3

Exercice 3. Montrer que $\mathrm{GL}_2(\mathbb{F}_2)$ est isomorphe à $\mathcal{S}_3$.

Éléments de correction de l'exercice 3. Chaque élément $A \in \mathrm{GL}_2(\mathbb{F}_2)$ correspond à une bijection linéaire de $(\mathbb{F}_2)^2$, et donc à une permutation des trois vecteurs non nuls $v_1 = (1,0)$, $v_2 = (0,1)$ et $v_3 = (1,1)$. Autrement dit il existe $\sigma_A \in \mathcal{S}_3$ telle que $A(v_i) = v_{\sigma_A(i)}$. L'application qui à $A \in \mathrm{GL}_2(\mathbb{F}_2)$ fait correspondre $\sigma_A \in \mathcal{S}_3$ est l'isomorphisme recherché.

Exercice 4. Considérons les deux éléments suivants du groupe symétrique $\mathcal{S}_9$

$$\sigma_1 = (1\,2)(3\,4\,5)(6\,7\,8\,9) \qquad\qquad \sigma_2 = (1\,2\,3\,4)(5\,6\,7)(8\,9)$$

Justifier pourquoi σ_1 et σ_2 sont conjugués, puis exhiber une permutation $\omega \in \mathcal{S}_9$ telle que $\sigma_2 = \omega\sigma_1\omega^{-1}$.

Quel est le cardinal (une expression sous forme de produit d'entiers suffit) de la classe de conjugaison de σ_1 dans $\mathcal{S}_9$?

Éléments de correction de l'exercice 4. Les décompositions canoniques des permutations σ_1 et σ_2 font intervenir des cycles de même longueur (2, 3 et 4), ces deux permutations sont donc conjuguées. En écrivant

$$\sigma_1 = (1\,2)(3\,4\,5)(6\,7\,8\,9) \qquad\qquad \sigma_2 = (8\,9)(5\,6\,7)(1\,2\,3\,4)$$

on trouve parmi de nombreux choix possibles $\omega = (1\,8\,3\,5\,7\,2\,9\,4\,6)$

Le cardinal de la classe de conjugaison s'obtient en calculant le nombre de permutations de $\mathcal{S}_9$ de type 2, 3, 4 :

- $(9 \cdot 8)/2 = 9 \cdot 4$ choix possibles pour la transposition ;
- $2 \cdot (7 \cdot 6 \cdot 5)/6 = 7 \cdot 5 \cdot 2$ choix possibles pour le 3-cycle ;
- 6 choix possibles pour le 4-cycle.

soit finalement $9 \cdot 8 \cdot 7 \cdot 6 \cdot 5$ choix possibles.

Exercice 5. Soient $p \neq q$ deux nombres premiers. Montrer que tout groupe d'ordre pq n'est pas simple.

Éléments de correction de l'exercice 5.

Voir feuille d'exercices 4

Exercice 6. Montrer que le groupe symétrique $\mathcal{S}_3$ est isomorphe à son groupe d'automorphisme $\mathrm{Aut}(\mathcal{S}_3)$.

Éléments de correction de l'exercice 6. L'application qui à σ fait correspondre l'automorphisme intérieur $\sigma' \mapsto \sigma\sigma'\sigma^{-1}$ est un morphisme injectif de $\mathcal{S}_3$ dans $\mathrm{Aut}(\mathcal{S}_3)$, car le centre de $\mathcal{S}_3$ est trivial.

De plus un élément de $\mathrm{Aut}(\mathcal{S}_3)$ est déterminé par l'image des générateurs $(1\,2)$ et $(1\,3)$. Il y a donc au plus 6 choix possibles (choisir deux parmi les trois éléments d'ordre 2 de $\mathcal{S}_3$), donc en comparant les ordres on obtient que le morphisme ci-dessus est en fait un isomorphisme.

Exercice 7. Soient p un nombre premier et $a > 1$. En utilisant une action de groupe que l'on précisera montrer que tout groupe G d'ordre p^a admet un élément central (*i.e.* qui commute avec tout élément de G) d'ordre p.

Éléments de correction de l'exercice 7. Faisons agir G sur lui-même par conjugaison. Les orbites sont ou bien de cardinal 1 (pour chaque élément du centre), ou bien de cardinal une puissance de p non égale à 1. En écrivant G comme une union d'orbites on a donc $|Z(\mathrm{G})| \equiv 0 \mod p$, ce qui interdit à $Z(\mathrm{G})$ d'être trivial. Soit $g \in Z(\mathrm{G}) \smallsetminus \{1\}$, alors G est d'ordre p^b pour un certain $1 \leq b \leq a$. Alors $g^{p^{b-1}}$ appartient à $Z(\mathrm{G})$ et est d'ordre p.

Exercice 8.

(1) Montrer que $(\mathbb{Z}, +)$ n'est pas isomorphe à $(\mathbb{Z}^2, +)$ et que $(\mathbb{Q}, +)$ n'est pas isomorphe à $(\mathbb{Q}^2, +)$.
(2) Montrer que le groupe abélien $(\mathbb{Q}, +)$ n'est pas de type fini.
(3) Soit G un groupe de $(\mathbb{C}^*, \cdot)$ dont chaque élément est d'ordre fini. Est-il vrai que G est forcément fini ? de type fini ?
(4) Montrer que les sous-groupes de $(\mathbb{R}, +)$ sont soit de la forme $a\mathbb{Z}$, soit denses.
(5) Que dire de $\mathbb{Z}[\sqrt{2}]$?

Éléments de correction de l'exercice 8.

(1) Soit $\varphi\colon \mathbb{Z} \to \mathbb{Z}^2$ un morphisme. Posons $\varphi(1) = (a, b)$. Pour tout $n \in \mathbb{Z}$ on a

$$\varphi(n) = (na, nb).$$

L'image de φ est donc contenue dans une droite et φ n'est pas surjectif.

Pour tous $\frac{a}{b}$, $\frac{c}{d} \in \mathbb{Q} \smallsetminus \{0\}$ il existe m, $n \in \mathbb{Z} \smallsetminus \{0\}$ tel que

$$m\frac{a}{b} + n\frac{c}{d} = 0$$

(prendre $m = -bc$ et $n = ad$). Mais cette propriété n'est pas vraie dans $\mathbb{Q}^2$: considérer par exemple $(1, 0)$ et $(0, 1)$. Par suite $\mathbb{Q}$ et $\mathbb{Q}^2$ ne sont pas isomorphes.

(2) Soit $\mathrm{G} = \langle \frac{a_1}{b_1}, \frac{a_2}{b_2}, \ldots \frac{a_k}{b_k} \rangle$ un sous-groupe de $\mathbb{Q}$ de type fini. Tout élément de G peut s'écrire comme une fraction avec dénominateur égal au produit des b_i. En particulier G ne peut pas coïncider avec $\mathbb{Q}$.

(3) Soit G le groupe des racines de l'unité. On a
- G est un groupe de $(\mathbb{C}^*, \cdot)$ dont chaque élément est d'ordre fini ;
- G n'est pas fini ;
- G n'est pas de type fini.

(4) Soit G un sous-groupe de $\mathbb{R}$. Si G est trivial, alors $\mathrm{G} = 0\mathbb{Z}$ et il n'y a rien à montrer. Supposons donc G non trivial. Posons $a = \inf\{x \in \mathrm{G} \mid x > 0\}$.
- Supposons $a = 0$. Considérons $I =]x, x + \varepsilon[$ un intervalle ouvert. L'intervalle I contient un élément de G : par hypothèse il existe $y \in]0, \varepsilon/2[$ et l'un des multiples ny, $n \in \mathbb{Z}$, convient. Le groupe G est donc dense dans $\mathbb{R}$.
- Supposons $a > 0$. Dans ce cas l'inf est atteint, *i.e.* $a \in \mathrm{G}$. Soit $x \in \mathrm{G}$. On écrit $x = na + r$ avec n entier et $0 \leq r < a$. Mais alors $r = x - na \in \mathrm{G}$; par minimalité de a on obtient que $r = 0$. Par suite $x \in a\mathbb{Z}$ et $\mathrm{G} = a\mathbb{Z}$.

(5) Si le groupe $\mathbb{Z}[\sqrt{2}]$ était de la forme $a\mathbb{Z}$, alors 1 et $\sqrt{2}$ seraient tous les deux multiples entiers de a, donc a puis $\sqrt{2}$ seraient rationnels : contradiction. Le groupe $\mathbb{Z}[\sqrt{2}]$ est donc dense dans $\mathbb{R}$.

Exercice 9. Si G est un groupe, on peut faire agir G par conjugaison sur lui-même.

(1) Montrer que le centre $Z(\mathrm{G})$ de G est constitué des éléments dont l'orbite est réduite à un point.

(2) (i) Si G est un p-groupe, p premier, montrer que le centre de G n'est pas réduit à $\{1\}$.

(ii) Soit G un groupe tel que $\mathrm{G}/Z(\mathrm{G})$ soit cyclique. Montrer qu'alors G est abélien.

(3) Montrer que le groupe des matrices triangulaires supérieures unipotentes

$$G = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}_3(\mathbb{F}_p) \right\}$$

est un groupe non-abélien d'ordre p^3.

Éléments de correction de l'exercice 9.

(1) Montrons que le centre $Z(\mathrm{G})$ de G est constitué des éléments dont l'orbite est réduite à un point.

C'est la définition du centre :

$$Z(\mathrm{G}) = \{x \in \mathrm{G} \,|\, gxg^{-1} = x \text{ pour tout } g \in \mathrm{G}\}.$$

(2) (i) Si G est un p-groupe, p premier, montrons que le centre de G n'est pas réduit à $\{1\}$.

Notons Ω_i, $i \in I$, les orbites non réduites à un singleton. Puisque $|\Omega_i|$ divise $|G|$ chaque $|\Omega_i|$ est une puissance de p distincte de 1. En écrivant G comme une union disjointe d'orbites on obtient

$$|\mathrm{G}| = |Z(\mathrm{G})| + \sum_i |\Omega_i|$$

soit

$$0 \equiv |Z(\mathrm{G})| \bmod p.$$

Ceci montre que $|Z(\mathrm{G})| \neq 1$.

(ii) Soit G un groupe tel que $\mathrm{G}/Z(\mathrm{G})$ soit cyclique. Montrons qu'alors G est abélien.

Par hypothèse il existe un élément a de G dont la classe $\overline{a} \in \mathrm{G}/Z(\mathrm{G})$ engendre $\mathrm{G}/Z(\mathrm{G})$. Tout élément de G peut alors s'écrire $a^k h$ avec $k \in \mathbb{Z}$ et $h \in Z(\mathrm{G})$. Puisque

$$a^k h \cdot a^{k'} h' = a^{k+k'} hh' = a^{k+k'} h'h = a^{k'} h' a^k h$$

le groupe G est aélien.

(3) Montrons que le groupe des matrices triangulaires supérieures unipotentes

$$G = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}_3(\mathbb{F}_p) \right\}$$

est un groupe non-abélien d'ordre p^3.

Chacun des coefficients $*$ est un élément arbitraire de $\mathbb{F}_p$ d'où p^3 choix possibles ; de plus

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

ne commutent pas d'où le résultat.

Exercice 10. Soit G un groupe fini d'ordre $|\mathrm{G}| = p^a m$ avec p premier et $\mathrm{pgcd}(p, m) = 1$. Soient $S \subset \mathrm{G}$ un p-Sylow et H un sous-groupe de G. Montrer qu'il existe $g \in \mathrm{G}$ tel que $gSg^{-1} \cap \mathrm{H}$ soit un p-Sylow de H.

Éléments de correction de l'exercice 10. On a $|\mathrm{G}| = p^a m$ et $|\mathrm{H}| = p^b n$. On fait agir G (et donc également H) par translation sur l'ensemble X des classes à gauche de G modulo S. Notons que $g' \in \mathrm{Stab}(gS)$ équivaut à $g' \in gSg^{-1}$. Par ailleurs l'ensemble X est de cardinal m qui n'est pas un multiple de p. L'une des orbites Ω de X sous l'action de H est donc de cardinal p^c pour un certain

$c \leq b$. Mais comme de plus $|\mathrm{Stab}(x)| \cdot |\Omega| = |\mathrm{H}| = p^b n$ et $\mathrm{pgcd}(|\Omega|, p) = 1$ on a finalement $|\Omega| = n$ et $|\mathrm{Stab}(x)| = p^b$ comme attendu.

Exercice 11.

(1) Soient $\Bbbk$ un corps et G un groupe fini. Montrer qu'il existe un entier n tel que G soit isomorphe à un sous-groupe de $\mathrm{GL}_n(\Bbbk)$. [Indication : on pourra commencer par plonger G dans un groupe symétrique.]

(2) Soit $\mathbb{F}_p$ le corps à p éléments où p désigne un nombre premier. Montrer que le groupe des matrices triangulaires supérieures avec des 1 sur la diagonale est un p-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$.

Éléments de correction de l'exercice 11.

(1) Tout groupe fini se plonge dans un groupe symétrique $\mathcal{S}_n$ en faisant agir G sur lui-même par translation ce qui montre que $n = |\mathrm{G}|$ convient. De plus le groupe symétrique $\mathcal{S}_n$ se plonge dans $\mathrm{GL}(n, \Bbbk)$ pour tout corps $\Bbbk$ en faisant agir $\mathcal{S}_n$ sur les vecteurs d'une base de $\Bbbk^n$.

(2) Le cardinal de $\mathrm{GL}(\mathbb{F}_p)$ est (compter les base de $(\mathbb{F}_p)^n$

$$|\mathrm{GL}(n, \mathbb{F}_p)| = (p^n - 1)(p^n - p)(p^n - p^2) \ldots (p^n - p^{n-1}) = p^{1+2+\ldots+(n-1)} m$$

avec $\mathrm{pgcd}(m, p) = 1$. Or $p^{1+2+\ldots+(n-1)}$ est le cardinal du groupe des matrices triangulaires unipotentes.

Exercice 12.

a) Soit G un sous-groupe fini de $\mathbb{C}^*$. Montrer que $\mathrm{G} = \mathbb{U}_n$ où $n = [\mathrm{G} : 1]$.

b) Soient m, $n \in \mathbb{N}^*$. Déterminer le sous-groupe de $\mathbb{C}^*$ engendré par $\mathbb{U}_m$ et $\mathbb{U}_n$.

c) Soient n, p, $q \in \mathbb{N}^*$. À quelle condition a-t-on $\mathbb{U}_n \simeq \mathbb{U}_p \times \mathbb{U}_q$?

d) Pour un tel choix montrer que $\mathrm{Aut}(\mathbb{U}_n) \simeq \mathrm{Aut}(\mathbb{U}_p) \times \mathrm{Aut}(\mathbb{U}_q)$.

Éléments de correction de l'exercice 12.

a) Soit G un sous-groupe fini de $\mathbb{C}^*$. Montrons que $\mathrm{G} = \mathbb{U}_n$ où $n = [\mathrm{G} : 1]$.
Soit G un sous-groupe fini de $\mathbb{C}^*$. D'après le théorème de Lagrange on a $z^{[\mathrm{G}:1]} = 1$ pour tout $z \in \mathrm{G}$. Par suite G est contenu dans $\mathbb{U}_n$. Comme $[\mathrm{G} : 1] = [\mathbb{U}_n : 1] = n$ on obtient que $\mathrm{G} = \mathbb{U}_n$.

b) Soient m, $n \in \mathbb{N}^*$. Déterminons le sous-groupe de $\mathbb{C}^*$ engendré par $\mathbb{U}_m$ et $\mathbb{U}_n$.
Posons $M = \mathrm{ppcm}(m, n)$. Puisque n divise M, la condition $z^n = 1$ implique $z^M = 1$. Il en résulte que $\mathbb{U}_n \subset \mathbb{U}_M$ et de même que $\mathbb{U}_m \subset \mathbb{U}_M$. Le sous-groupe $\mathrm{H} = \mathbb{U}_n\mathbb{U}_m$, engendré par $\mathbb{U}_n$ et $\mathbb{U}_m$ est donc inclus dans $\mathbb{U}_M$ et est fini. L'inclusion $\mathrm{H} \subset \mathbb{U}_M$ assure que $[\mathrm{H} : 1] | M$. Le théorème de Lagrange assure que les ordres n et m de $\mathbb{U}_n$ et $\mathbb{U}_m$ divisent $[\mathrm{H} : 1]$. Ainsi $M = \mathrm{ppcm}(n, m)$ divise $[\mathrm{H} : 1]$. Finalement $M = [\mathrm{H} : 1]$ et $\mathrm{H} = \mathbb{U}_M$.

c) Soient n, p, $q \in \mathbb{N}^*$. Il est nécessaire que $p|n$ et $q|n$ afin que $\mathbb{U}_p$ et $\mathbb{U}_q$ soient des sous-groupes de $\mathbb{U}_n$. Comme $d \mapsto \mathbb{U}_d$ est un isomorphisme de l'ensemble ordonné des diviseurs de n sur l'ensemble ordonné des sous-groupes de $\mathbb{U}_n$ les conditions $\mathbb{U}_p \cap \mathbb{U}_q = \{1\}$ et $\mathbb{U}_p\mathbb{U}_q = \mathbb{U}_n$ équivalent à $\mathrm{pgcd}(p, q) = 1$ et $\mathrm{ppcm}(p, q) = n$ d'où $n = pq$.

d) Supposons que $n = pq$, n, p, $q \in \mathbb{N}^*$. Soit $\alpha \in \mathrm{Aut}(\mathbb{U}_n)$. Comme α est bijectif, $\alpha(\mathbb{U}_p)$ a le même ordre p que $\mathbb{U}_p$. Puisque $\mathbb{U}_p$ est le seul sous-groupe de $\mathbb{U}_n$ d'ordre p il est stable par α. Par restriction α induit un automorphisme β de $\mathbb{U}_p$. De même $\alpha(\mathbb{U}_q) = \mathbb{U}_q$ et par restriction α définit un élément γ de $\mathrm{Aut}(\mathbb{U}_q)$. On a donc une application

$$\phi\colon \mathrm{Aut}(\mathbb{U}_n) \to \mathrm{Aut}(\mathbb{U}_p) \times \mathrm{Aut}(\mathbb{U}_q), \qquad \alpha \mapsto (\beta, \gamma).$$

L'application ϕ est injective car tout élément de $\mathbb{U}_n$ est de la forme zz' avec $z \in \mathbb{U}_p$ et $z' \in \mathbb{U}_q$; de plus $\alpha(zz') = \beta(z)\gamma(z')$. L'application ϕ est surjective car la donnée de deux automorphismes β et γ de $\mathbb{U}_p$ et $\mathbb{U}_q$ détermine un automorphisme α de $\mathbb{U}_p \times \mathbb{U}_q = \mathbb{U}_n$ en posant $\alpha(z, z') = (\beta(z), \gamma(z'))$ (à vérifier). On a alors $\phi(\alpha) = (\beta, \gamma)$.
Enfin ϕ est un homomorphisme de groupes car la restriction de $\alpha_1 \circ \alpha_2$ au sous-groupe $\mathbb{U}_p$ est la composée $\beta_1 \circ \beta_2$ des restrictions de α_1 et α_2 et de même pour $\mathbb{U}_q$.

Exercice 13. Soit G un groupe abélien fini.

Supposons que pour tout diviseur d de l'ordre n de G, il existe un et un seul sous-groupe d'ordre d dans G. Montrer que G est cyclique.

Éléments de correction de l'exercice 13. Raisonnons par l'absurde. Supposons que G ne soit pas cyclique. Alors G est isomorphe à $(\mathbb{Z}/q_1\mathbb{Z}) \times (\mathbb{Z}/q_2\mathbb{Z}) \times \ldots \times (\mathbb{Z}/q_k\mathbb{Z})$ où $q_1|q_2|\ldots|q_k$ sont les invariants de G et $k \geq 2$. Il y a alors (au moins) deux sous-groupes distincts d'ordre q_1 : d'une part le facteur $\mathbb{Z}/q_1\mathbb{Z}$ et d'autre part l'unique sous-groupe d'ordre q_1 du facteur $\mathbb{Z}/q_2\mathbb{Z}$ associé au diviseur q_1 de q_2.

Exercice 14. Le but de cet exercice est de montrer que le centre du groupe $\mathrm{GL}_n(\mathbb{C})$ est le groupe des homothéties.

Une représentation ρ du groupe $\mathrm{GL}_n(\mathbb{C})$ est donnée par son action naturelle sur $\mathbb{C}^n$.

1. Montrer que la représentation ρ est irréductible.
2. Montrer que tout élément du centre de $\mathrm{GL}_n(\mathbb{C})$ est un morphisme de la représentation ρ, *i.e.* montrer que pour tout élément h du centre et pour tout élément M de $\mathrm{GL}_n(\mathbb{C})$ on a
$$\rho(M) \circ h = Mh = hM = h \circ \rho(M).$$
3. Conclure en utilisant le Lemme de Schur.

Éléments de correction de l'exercice 14. Puisque ρ est l'action naturelle de $\mathrm{GL}_n(\mathbb{C})$ sur $\mathbb{C}^n$, ρ est l'identité de $\mathrm{GL}_n(\mathbb{C})$ dans $\mathrm{GL}_n(\mathbb{C})$.

1. Si un sous-espace vectoriel V de $\mathbb{C}^n$ est stable par tous les éléments de $\mathrm{GL}_n(\mathbb{C})$, alors $V = \{0\}$ ou $V = \mathbb{C}^n$, *i.e.* ρ est irréductible.
2. Soit h un élément du centre de $\mathrm{GL}_n(\mathbb{C})$. Pour tout M dans $\mathrm{GL}_n(\mathbb{C})$ on a
$$\rho(M) \circ h = Mh = hM = h \circ \rho(M)$$
ainsi h est bien un morphisme de la représentation ρ.
3. Comme ρ est irréductible, le Lemme de Schur assure que $h = \lambda\mathrm{id}$ avec $\lambda \in \mathbb{C}^*$, *i.e.* h est une homothétie.

Exercice 15. Soit G un groupe abélien.

1. Si $\rho\colon \mathrm{G} \to \mathrm{GL}(V)$ est une représentation de G, montrer que tout élément G de G définit un G-morphisme $V \to V$.
2. En déduire que toute représentation irréductible de G est de dimension 1.
3. Donner toutes les représentations irréductibles de $\mathbb{Z}/n\mathbb{Z}$.

Éléments de correction de l'exercice 15.

1. Pour tous G, h et x dans G on a
$$g \cdot (h \cdot x) = (gh) \cdot x = (hg) \cdot x = h \cdot (g \cdot x)$$
c'est-à-dire l'application $\rho(g)\colon x \mapsto g \cdot x$ est un G-morphisme pour tout $g \in \mathrm{G}$.
2. On suppose que V est une représentation irréductible de G. Si $g \in \mathrm{G}$, alors, d'après 1. et le Lemme de Schur, $\rho(g) = \lambda\mathrm{id}$. De plus comme $\rho(g) \in \mathrm{GL}(V)$, λ est non nul. Par conséquent tout sous-espace vectoriel de V est stable par G donc est une sous-représentation de G. Puisque V est irréductible, $\dim V = 1$.
3. D'après 1. une représentation irréductible de $\mathbb{Z}/n\mathbb{Z}$ est un morphisme de groupes
$$\rho\colon \mathbb{Z}/n\mathbb{Z} \to \mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^*$$
Tout élément k de $\mathbb{Z}/n\mathbb{Z}$ est d'ordre divisant n ; par suite $\rho(k)$ est aussi d'ordre divisant n, *i.e.* $\rho(k)^n = 1$. Réciproquement pour tout racine $n$ième de l'unité ω l'application
$$\mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*, \qquad k \mapsto \omega^k$$
est une représentation de $\mathbb{Z}/n\mathbb{Z}$. On les obtient donc toutes ainsi.
Notons aussi que l'espace des représentations irréductibles de $\mathbb{Z}/n\mathbb{Z}$ peut être muni d'une structure de groupe qui le rend isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Exercice 16. Soit G un groupe fini. Soit H un sous-groupe abélien de G.

Montrer que toute représentation irréductible de G est de dimension au plus $[\mathrm{G} : H]$.

Indication : si V est une représentation irréductible de G*, c'est aussi une représentation de* H*. On pourra considérer la représentation de* G *engendrée par une sous-représentation de* H.

Éléments de correction de l'exercice 16.

Soit V une représentation irréductible de G. C'est aussi par restriction une représentation irréductible de H. Puisque H est abélien, V vu comme représentation de H se décompose en somme directe de représentations de H de degré 1. Soit v un vecteur directeur d'une de ces représentations et soit V' le sous-espace vectoriel de V engendré par les vecteurs de la forme $g \cdot v$ où G parcourt G. Il est clair que $V' \neq \{0\}$ est une sous-représentation de V du groupe G ; ainsi $V' = V$. Or si $g' = gh$ avec h dans H, alors par définition de v, $g' \cdot v$ et $g \cdot v$ sont colinéaires. Par conséquent V' est engendré par $[\mathrm{G} : H]$ vecteurs, et est donc de dimension au plus $[\mathrm{G} : H]$.

Exercice 17. Écrire la table des caractères de $\mathcal{S}_3$.

Éléments de correction de l'exercice 17.

cf feuille d'exercices

Exercice 18. Montrer que tout groupe non abélien admet une représentation irréductible de dimension > 1.

Éléments de correction de l'exercice 18.

Soit G un groupe dont toutes les représentations irréductibles sont de degré 1. La somme des carrés des dimensions des représentations irréductibles de G est égale au cardinal de G ; par suite les classes de conjugaisons de G sont toutes réduites à un élément. Autrement dit G est abélien.

Exercice 19. Montrer que si V est une représentation d'un groupe fini vérifiant $\langle \chi_V, \chi_V \rangle = 2$, alors V est somme de deux représentations irréductibles.

Éléments de correction de l'exercice 19.

Si $V = \oplus V_i^{a_i}$, alors $\langle \chi_V, \chi_V \rangle = 2$ si et seulement si deux a_i distincts sont non nuls et égaux à 1.