Préparation à l'agrégagion - TD d'algèbre
Julien Grivaux 20 septembre 2021

CORRIGÉ DE LA FEUILLE n° 1

Exercice 1

1. Posons $G = a\mathbb{Z} \cap b\mathbb{Z}$. Si $d = ppcm(a, b)$, d est un multiple de a et b donc $d\mathbb{Z} \subset G$. Réciproquement, tout élément de G est divisible par a et b est divisible par d. D'où $G = d\mathbb{Z}$.

2. Soit G le groupe engendré par a et b, et $d = pgcd(a, b)$. Comme d divise a et b, $a, b \in d\mathbb{Z}$ donc $G \subset \mathbb{Z}$. Réciproquement, en utilisant l'identité de Bezout, il existe u, v dans $\mathbb{Z}$ tels que $ua + vb = d$, donc $d \in G$ et par suite $d\mathbb{Z} \subset G$. D'où $G = d\mathbb{Z}$

Exercice 2

1. On cherche le plus petit entier k tel que $kd \equiv 0\ (n)$, c'est-à-dire le plus petit entier k tel que n divise kd. Soit $q = pgcd(d, n)$. La condition devient n/q divise kd/q mais comme n/q et d/q sont premiers entre eux, n/q divise k. Le plus petit k possible est donc n/q.

2. Construisons l'application inverse : à tout élément x de $\mathbb{Z}/n\mathbb{Z}$ on associe le morphisme f_x défini par $f_x(q) = qx$. C'est un morphisme de groupes. On a bien $f_x(1) = x$, et si f est un morphisme de groupes $f(q) = qf(1) = f_{f(1)}(q)$. Enfin, $f \circ g(1) = f(g(1)) = g(1)f(1)$ donc la composition des morphismes correspond à la multiplication dans $\mathbb{Z}/n\mathbb{Z}$ via cette bijection.

3. Si f est un automorphisme de groupe, comme 1 est inversible dans $(\mathbb{Z}/n\mathbb{Z}, \times)$, $f(1)$ aussi. Réciproquement, supposons $f(1)$ inversible, et soit x son inverse. Alors f_x et f sont des fonctions réciproques (car $f \circ f_x(1) = f_x \circ f(1) = xf(1) = 1$), donc f est inversible. On en déduit le résultat.

Exercice 3

1. ***a.*** Commençons par montrer que $\alpha \in G$. En raisonnant par l'absurde, si $\alpha \notin G$, il existe une suite strictement décroissante $(\alpha)_n$ d'éléments de G tels que $\lim \alpha_n = \alpha$. Mais alors $\alpha_n - \alpha_{n+1}$ est une suite d'éléments strictements positifs de G qui tend vers 0, ce qui contredit l'hypothèse. Soit maintenant x dans G. Supposons $x > 0$ et soit $n = \lfloor x/\alpha \rfloor$. Alors $x = n\alpha + y$ où $0 \leq y < \alpha$. Comme $\alpha \in G$, $y \in G$ donc $y = 0$ et $x = n\alpha$. Si x est négatif, on applique ce qui précède à $-x$ pour en déduire que x est un multiple entier négatif de α. Ceci montre que $G \subset \alpha\mathbb{Z}$ et comme l'inclusion en sens inverse est vraie, $G = \alpha\mathbb{Z}$.

b. Fixons une suite g_n d'éléments strictements positifs de G qui tend vers 0. Soit $x > 0$. Si $x \in G$, la suite $x + g_n$ est une suite d'éléments distincts de x qui a pour limite x. Si $x \neq G$, posons $k_n = \lfloor x/g_n \rfloor$. Alors $|x/g_n - k_n| < 1$ donc $|x - k_n g_n| < g_n$. La suite $k_n g_n$ d'éléments de G a donc pour limite x. Comme $x \neq G$, les éléments de la suite sont distincts de x. Si x est négatif, on applique le raisonnement précédent à $-x$.

2. ***a.*** Supposons a et b liés sur $\mathbb{Q}$. Cela signifie qu'il existe deux rationnels u et v tels que $ua + vb = 0$, donc b est un multiple rationnel de a. Considérons maintenant une suite $g_n = p_n a + q_n b$ d'éléments de $G_{a,b}$ qui tend vers 0. En écrivant $b = ra$ où $r \in \mathbb{Q}$, on a $g_n = (p_n + rq_n)a$. Si d est le dénominateur de r, $dg_n = (dp_n + drq_n)a$. La suite dg_n est ainsi une suite de multiples entiers de a qui tend vers 0, donc elle est nulle à partir d'un certain rang. Ceci montre que G n'est pas dense dans $\mathbb{R}$. Réciproquement supposons G non dense. Il existe alors $\alpha > 0$ et deux entpers p et q tels que $a = p\alpha$ et $b = q\alpha$, donc $qa - pb = 0$.

b. Considérons le morphisme de groupes $f : \mathbb{R} \to \mathbb{U}$ donné par $f(x) = \exp(2\mathbf{i}\pi x)$. Soit G un sous-groupe de $\mathbb{U}$. Alors $H = f^{-1}(G)$ est un sous-groupe de $\mathbb{R}$ et comme f est surjectif, $f(H) = G$. Si H est dense, alors $f(H)$ aussi (car f est continue). Si H n'est pas dense, H s'écrit $\mathbb{Z}\alpha$ pour $\alpha > 0$. Or, $1 \in H$ donc 1 est un multiple entier de α, c'est-à-dire $\alpha = 1/n$. On en déduit $f(H) = \{\exp(2\mathbf{i}k\pi/n), k \in \mathbb{Z}\}$, c'est à dire que G est le groupe des racines $n^{\text{èmes}}$ de l'unité. En particulier G est fini.

c. Oui : le groupe de toutes les racines de l'unité $f(\mathbb{Q})$.

Exercice 4

1. ***a.*** Comme G est fini, le sup est atteint donc il existe x tel que $d = \text{ord}(x)$, donc d divise n.

b. Soit $p = \text{ord}(y)$ et supposons que p ne divise pas d. Soit $k > 0$ tel que $(xy)^k = 1$. Alors $y^{-k} = x^k$. y^{-k} est d'ordre 1 ou p (car le groupe engendré par y est isomorphe à $\mathbb{Z}/p\mathbb{Z}$) donc x^k est d'ordre 1 ou p. Or l'ordre de x^k est un diviseur de d (car $\langle x^k \rangle \subset \langle x \rangle$) et comme p ne divise pas d, y^{-k} est d'ordre 1, c'est-à-dire $y^{-k} = 1$. Dans ce cas, k est un multiple de p mais comme $x^k = 1$, k est également un multiple de d. Comme p ne divise pas d, k est un multiple de pd, et donc $\text{ord}(xy) = pd > d$. Ceci contredit la définition de d. Remarque : on peut aussi utiliser que dans un groupe abélien, si x et y ont des ordres premiers entre eux, $\text{ord}(xy) = \text{ord}(x)\text{ord}(y)$.

c. Supposons que $\text{ord}(y)$ ne divise pas d. Soit $m = \text{ord}\,(y)$. Il existe donc un nombre premier p tel que le facteur p-premier de m ne divise pas d. On note p^r et p^s les facteurs p-premiers respectifs de m et d, on a donc $r > s$. On pose alors $z = y^{m/p^r}$, z est d'ordre p^r.

On recommence le même argument qu'à la question précédente en le raffinant un peu. Soit k tel que $(xz)^k = 1$. Alors $z^{-k} = x^k$. L'ordre de x^k est $d/\text{pgcd}(d, k)$ et celui de z^{-k} est $p^r/\text{pgcd}(p^r, k)$. Soit p^ℓ le facteur p-premier de k. On compare alors les facteurs p-premiers de $d/\text{pgcd}(d, k)$ et $p^r/\text{pgcd}(p^r, k)$. Si $\ell \leq s$, on obtient $p^{s-\ell}$ et $p^{r-\ell}$, ce qui est impossible. Si $s < \ell < r$, on obtient 1 (pas de facteur p-premier) et $p^{r-\ell}$, ce qui est également impossible. On en déduit que $\ell \geq r$, ce qui signifie que k est divisible par p^r. Dans ce cas $z^{-k} = 1$ et donc $x^k = 1$. k est donc multiple de d, donc de $p^{r-s}d > d$, ce qui contredit la définition de d.

d. Comme d est l'ordre de x, il divise le ppcm de tous les éléments de G. Réciproquement, on a démontré que tous les ordres des éléments de G divisaient l'ordre de x donc leur ppcm aussi.

2. Soit d l'indice de G et $P(X) = X^d - 1$. Pour tout x dans G, l'ordre de x divise d, en pariculier $x^d = 1$. Tous les éléments de G sont donc des racines de P. Comme $\mathbf{k}$ est un corps, P a au plus d racines donc $\#G \leq d$. Or d est un diviseur de $\#G$, donc $d = \#G$. Ceci signifie que G a un élément d'ordre égal à son cardinal, donc il est cyclique.

Exercice 5

1. ***a.*** Les éléments inversibles dans $\mathbb{Z}/p^N\mathbb{Z}$ sont les classes d'entiers premiers avec p. On peut les décrire comme l'ensemble $\{0, 1, 2, \ldots, p^N - 1\} \setminus \{0, p, 2p, \ldots, p^{N-1}\}$. Il y en a donc $p^N - p^{N-1}$.

b. $f(x)f(y) = (1 + xp^{N-1})(1 + yp^{N-1}) = (1 + (x + y)p^{N-1} + xyp^{2N-2}) \equiv 1 + (x + y)p^{N-1}\ (p^N)$ car $N \geq 2$, donc $f(x)f(y) = f(x + y)$.

c. $1 + p^{N-1} = f(1)$. Comme f est un morphisme de groupes, $f(1)^p = f(p) = 1$ donc $f(1)$ est d'ordre 1 ou p. Comme $f(1) \neq 1$, $f(1)$ est d'ordre p.

2. ***a.*** On procède par récurrence sur k. On utilisera le fait que p divise $\binom{p}{i}$ pour $1 \leq i \leq p - 1$. Si $k = 0$, l'égalité est vraie sans reste. Supposons vrai à l'ordre k. Alors

$$\begin{aligned}(1 + p)^{p^{k+1}} &= \left((1 + p)^{p^k}\right)^p = (1 + p^{k+1} + dp^{k+2})^p \\ &= (1 + p^{k+1})^p + \binom{p}{1}(1 + p^{k+1})^{p-1}dp^{k+2} + \ldots + (dp^{k+2})^p \\ &\equiv (1 + p^{k+1})^p \quad \mod p^{k+3}\end{aligned}$$

$$\equiv 1 + \binom{p}{1} p^{k+1} + \ldots + (p^{k+1})^p \mod p^{k+3}$$
$$\equiv 1 + p^{k+2} \mod p^{k+3}$$

Pour que ces égalités soient correctes, on a besoin à la première ligne que $p(k+2) \geq k+3$, puis à la dernière ligne que $p(k+1) \geq k+3$. La première inégalité est toujours valable pour $p \geq 2$, mais la seconde n'est valable que pour $p \geq 3$ (pour $p = 2$ et $k = 0$ elle n'est pas correcte, et on voit bien que $(1+2)^2 = 9$ n'est pas congru à $1 + 2^2 = 5$ modulo $2^3 = 8$).

b. On a $(1+p)^{p^{N-1}} = 1$ donc l'ordre de $1+p$ divise p^{N-1}. Or les seuls diviseurs possibles non triviaux de p^{N-1} sont les p^k pour $1 \leq k \leq N-2$ et pour ces valeurs de k, $(1+p)^{p^k} \neq 1$. On en déduit que $1+p$ est d'ordre p^{N-1}.

3. ***a.*** Evident car si x est inversible dans $\mathbb{Z}/p^N\mathbb{Z}$, sa classe dans $\mathbb{Z}/p\mathbb{Z}$ est également inversible (son inverse était la classe de l'inverse de x).

b. Comme $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique, on peut fixer un générateur y de ce groupe. Soit y' un relèvement de z dans $\mathbb{Z}/p^N\mathbb{Z}$. Si $(y')^k = 1$, $y^k = 1$ donc k est un multiple de $p-1$. L'ordre de y' est donc un multiple de $p-1$.

4. ***a.*** L'exposant du groupe est un multiple de tous les ordres des éléments du groupe qui divise le cardinal du groupe. Comme on a construit des éléments d'ordre p^{N-1} et multiple de $p-1$, l'exposant est un multiple de $p^{N-1}(p-1)$. Or c'est aussi un diviseur de $p^{N-1}(p-1)$, donc l'exposant est égal à $p^{N-1}(p-1)$.

b. L'exposant du groupe étant égal à son cardinal, le groupe est cyclique.

5. On a $\#(\mathbb{Z}/2^N\mathbb{Z})^\times = 2^N - 2^{N-1} = 2^{N-1}$. On reprend la stratégie précédente, mais au lieu de considérer $(1+2)^{2^k}$, on considère $(1+4)^{2^k}$. On peut montrer par récurrence que l'on a $5^{2^k} \equiv 1 + 2^{k+2} \mod 2^{k+3}$ en suivant la même méthode. L'ordre de 5 divise donc 2^{N-2}, est est par suite égal à 2^{N-2} car 5^{2^k} n'est jamais égal à 1 module 2^N si $k < N-2$. On considère alors le morphisme $f : \mathbb{Z}/2^{N-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to (\mathbb{Z}/2^N\mathbb{Z})^\times$ donné par $f(k,s) = 5^k \times \epsilon(s)$ où $\epsilon(0) = 1$ et $\epsilon(1) = -1$. C'est un morphisme de groupes. Si $f(k,s) = 1$, alors $f(k,s)$ est impair donc $s = 1$ et par suite $5^k = 1$ donc $k = 0 \mod 2^{N-2}$. On en déduit que f est injectif, et comme la source et le but ont même cardinal, f est un isomorphisme d'où $(\mathbb{Z}/2^N\mathbb{Z})^\times \simeq \mathbb{Z}/2^{N-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 6

Soit G un groupe fini, $\widehat{G}$ l'ensemble des caractères de G, et E l'espace vectoriel des fonctions de G dans $\mathbb{C}$. Une fonction f dans E est dite centrale si pour tout éléments g, h de E, $f(ghg^{-1}) = f(h)$.

1. ***a.*** Soit n le cardinal du groupe. Alors les caractères de G forment un sous-groupe des fonctions de G dans $\mathbb{U}_n$. Comme $\mathbb{U}_n$ et G sont finis, on obtient que $\widehat{G}$ est fini.

b. On procède par récurrence sur le nombre d'éléments de la famille. Soient $\chi_1, \ldots, \chi_d$ des caractères tels que $\sum_{i=1}^{d} \lambda_i \chi_i = 0$. Pour tous éléments x, y de G, $\sum_{i=1}^{d} \lambda_i \chi_i(xy) = 0$ donc $\sum_{i=1}^{d} (\lambda_i \chi_i(y)) \chi_i(x) = 0$. On en déduit $\sum_{i=1}^{d} \lambda_i (\chi_i(y) - \chi_1(y)) \chi_i = 0$. Comme le terme pour $i = 1$ disparaît dans la somme précédente, on peut utiliser l'hypothèse de récurrence et en déduire que $\lambda_i(\chi_i(y) \neq \chi_1(y)) = 0$. Pour chaque i, on peut fixer un y tel que $\chi_i(y) \neq \chi_1(y)$, ce qui donne $\lambda_i = 0$. Tous les λ_i sont nuls pour $i \geq 2$, et donc aussi λ_1.

c. Les éléments de $\widehat{G}$ forment une famille libre de E, donc $\#\widehat{G} \leq \dim E = \#G$.

2. ***a.*** Comme $\#\widehat{G} = \dim E$, les caractères forment une base de E. Comme les caractères sont des fonctions centrales, tout élément de E est une fonction centrale.

b. Pour h dans G, on considère la fonction f telle que $f(h) = 1$ et pour les autres valeurs f est nulle. Comme f est centrale, pour tout g dans G, $f(ghg^{-1}) = 1$ donc $ghg^{-1} = g$ ce qui entraîne que G est abélien.

3. On suppose maintenant que G est abélien. Pour tout g de E on définit un endomorphisme L_g de E par $L_g(f)(x) = f(gx)$.

a. On a $L_g L_h f(x) = L_h f(gx) = f(hgx) = L_{hg} f(x)$ donc $L_g L_h = L_{hg}$. Comme G est abélien, L_g et L_h commutent. Enfin $L_g^n = L_{g^n}$ donc pour $n = \mathrm{ord}(g)$, $L_g^n = \mathrm{Id}.L_g$ est donc d'ordre fini.

b. Le polynôme $X^n - 1$ est un polynôme scindé à racines simples sur $\mathbb{C}$. Comme il annule L_g, L_g est diagonalisable. Enfin, une famille d'endomorphismes diagonalisables qui commutent sont simultanément diagonalisables.

c. Soit f un vecteur propre commun des L_g. On peut alors écrire $L_g f = \lambda(g) f$ où $\lambda(g)$ est la valeur propre associée, c'est-à-dire pour tout x dans G, $f(gx) = \lambda(g) f(x)$. On a alors $f(g) = \lambda(g) f(1)$. Comme f est non nulle, $f(1)$ non plus. On a alors $\lambda(gh) = f(gh)/f(1) = \lambda(g) f(h)/f(1) = \lambda(g)\lambda(h)$ donc $f/f(1) = \lambda$ est un caractère.

d. La diagonalisation simultanée des L_g fournie une base de E formée de caractères de G. On en déduit $\#G = \dim E \leq \#\widehat{G}$, et donc en utilisant 1.c, $\#G = \#\widehat{G}$.

Exercice 7

1. ***a.*** Comme $H \cap \langle \overline{x} \rangle = \{e\}$, l'application $\langle x \rangle \to G \to G'$ est injective, d'où le résultat.

b. Comme H est maximal, le groupe engendré par g et H intersecte non trivialement $\langle x \rangle$. Ceci signifie qu'il existe $k \in \mathbb{Z}$ et $h \in H$ tel que $g^k h$ est un élément non trivial de $\langle x \rangle$. L'entier k est non nul, s'il est négatif on peut prendre l'inverse pour obtenir un entier > 0.

c. On a $\bar{g}^m \in \langle \bar{x} \rangle$. Supposons $\bar{g}^m = e$. Soit $k > 0$ tel que $\bar{g}^k \in \langle \bar{x} \rangle$ et $\bar{g}^k \neq e$. Alors $\bar{\bar{g}}^k = 0$ donc k est un multiple de m, mais alors $\bar{g}^k = e$ et on obtient une contradiction. Donc $\bar{g}^m \neq e$. Enfin, $\mathrm{ord}(\bar{\bar{g}})$ est un diviseur de $\mathrm{ord}(\bar{g})$ car $\bar{g}^k = 0 \Rightarrow \bar{\bar{g}}^k = 0$.

d. On a $\bar{g}^m = \bar{x}^i$ donc en comparant les ordres, $\mathrm{ord}(\bar{g})/m = d/\mathrm{pgcdi, d}$. Or, $\mathrm{ord}(\bar{g}) | \mathrm{ord}(g) | d$, la dernière divisibilité résultant de l'exercice 4. On en déduit que $d/\mathrm{pgcd}(i, d)$ divise d/m, et donc que m divise $\mathrm{pgcd}(i, d)$, et donc a fortiori i.

e. On peut écrire $\bar{g}^m = \bar{x}^i$ où $i = mr$, donc $(\overline{gx^{-r}})^m = 1$. Si $y = gx^{-r}$, alors $\bar{\bar{y}} = \bar{\bar{g}}$ donc $\mathrm{ord}(\bar{\bar{y}}) = m$. Mais $\bar{y}^m = e$, on en déduit donc en utilisant 1-c que $y \in H$. Ceci signifie que $\overline{g} = x^r$.

2. ***a.*** L'injectivité est claire : si $hx^k = e$, alors $h \in \langle x \rangle$ donc $h = e$ et $x^k = e$. Pour la surjectivité, on a démontré que $\langle x \rangle \simeq G/H$. Si $g \in G$, on peut donc écrire $\bar{g} = \bar{x}^k$ pour un certain entier k, donc il existe h dans H tel que $g = hx^k$.

b. Récurrence.