# CORRIGÉ DE LA FEUILLE n° 2

## Exercice 1

**1.** ***a.*** Les entiers premiers avec $p^n$ sont tout ceux qui ne sont pas multiples de $p$. On obtient donc $p^n - \#\{p, 2p, 3p, \dots, p^n\} = p^n - p^{n-1}$.

***b.*** $\varphi(n)$ est exactement le nombre de générateurs de $\mathbb{Z}/n\mathbb{Z}$. Par le théorème chinois, $\mathbb{Z}/ab\mathbb{Z} = \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. Le résultat s'ensuit.

***c.*** Résulte directement des deux questions précédentes.

**2.** ***a.*** Le groupe $(\mathbb{Z}/n\mathbb{Z})^\star$ a $\varphi(n)$ éléments, d'où le résultat.

***b.*** On cherche à connaître $12^{42}$ modulo 100. Or $\varphi(100) = \varphi(2^2 \times 5^2) = 2 \times 5 \times 4 = 40$. Par contre 12 n'est pas premier avec 100. On écrit $12^4 2 = 3^{42} \times 4^{42}$. Alors $3^{42} = 9$ modulo 100. Pour le facteur $4^{42}$, on raisonne modulo 25. $\varphi(25) = \varphi(5^2) = 20$. Comme 4 et 25 sont premiers entre eux, $4^{42} \equiv 16$ modulo 25. Comme $4^{42} \equiv 0$ modulo 4, le théorème chinois entraîne que $4^{42} \equiv 16$ modulo 100. On en déduit $12^{42} \equiv 9 \times 16 \equiv 144 \equiv 44$ modulo 100.

***c.*** Supposons que $p$ ne divise pas $x$. Alors il ne divise pas $y$. On a $x^2 \equiv -y^2\ (p)$ et comme $y$ est inversible modulo $p$, $(x/y)^2 = -1$. Or $(x/y)^{p-1} \equiv 1\ (p)$ donc $(-1)^{\frac{p-1}{2}} \equiv 1\ (p)$. Or $(-1)^{\frac{p-1}{2}} = -1$ et on aboutit à une contradiction.

**3.** ***a.*** Si $\varphi(n) = d$, alors pour tout diviseur premier $p$ de $n$, soit $p - 1$ divise $d$, soit $p$ divise $d$. De plus, si $p$ intervient avec un exposant $k \geq 2$, alors $p^{k-1}$ divise $d$. Pour trouver les facteurs premiers possibles de $n$,

- On regarde tous les diviseurs $d'$ de $d$, puis regarde $d' + 1$. On sélectionne tous les $d' + 1$ qui sont premiers.
- On sélectionne tous les diviseurs premiers de $d$ aussi (il est possible d'en avoir déjà dans la liste précédente, par exemple si $d$ est divisible par 6, 3 va sortir deux fois).
- Ensuite pour chaque nombre premier $p$, l'exposant peut aller au maximum à 1 si $p$ ne divise pas $d$, sinon à $v_p(d) + 1$.

Mettons la technique en pratique. Dans les petits tableaux, on met en ligne le nombre premier, en colonne l'exposant, et à l'intérieur la valeur de $\varphi$.

1. $d = 1$. Le tableau donne

| | 2 |
|---|---|
| 0 | 1 |
| 1 | 1 |

donc les solutions sont $\{1, 2\}$.

– $d = 2$. Le tableau donne

| | 2 | 3 |
|---|---|---|
| 0 | 1 | 1 |
| 1 | 1 | 2 |
| 2 | 2 | $\star$ |

On obtient pour les solutions $2^a 3^b$ avec $(a, b) = (0, 1), (1, 1), (2, 0)$ c'est-à-dire $\{3, 6, 4\}$.

– $d = 3$. On recommence :

| | 2 | 3 |
|---|---|---|
| 0 | 1 | 1 |
| 1 | 1 | 2 |
| 2 | $\star$ | 6 |

Aucune solution ne convient.

– $d = 4$.

| | 2 | 3 | 5 |
|---|---|---|---|
| 0 | 1 | 1 | 1 |
| 1 | 1 | 2 | 4 |
| 2 | 2 | ⋆ | ⋆ |
| 3 | 4 | ⋆ | ⋆ |

On trouve $2^a 3^b 5^c$ avec comme solutions $(0,0,1)$, $(1,0,1)$, $(2,1,0)$, $(3,0,0)$, à savoir $\{5, 10, 12, 8\}$.

***b.*** La technique précédente montre clairement la finitude car le nombre de facteurs premiers de $n$ est fini et leurs exposants aussi.

***c.*** Si $\varphi(n)$ ne tend pas vers l'infini quand $n$ tend vers l'infini, comme $\varphi$ est à valeurs entières, il existe une infinité d'entiers $n_k$ tels que $\varphi(n_k)$ est constante. Ceci contredit 3.b.

## Exercice 2

**1.** ***a.*** Faisons agir $G$ par translation à gauche sur lui-même. L'action est le morphisme de groupes $G \to Fct(G, G)$ donné par $g \mapsto \sigma_g$, où $\sigma_g(g') = gg'$. Ce morphisme est injectif car si $\sigma_g = \mathrm{Id}$, nécessairement $g = e$. En identifiant les éléments de $G$ à $\{1, \ldots, n\}$, on obtient le résultat souhaité.

***b.*** On applique la construction précédente en numérotant la classe de $i$ dans $\mathbb{Z}/n\mathbb{Z}$ par $i+1$ (si $0 \leq i \leq n-1$). Alors $\sigma_1$ est la permutation $(1, 2, 3, \ldots, n)$. Le sous-groupe obtenu est donc le groupe engendré par le cycle $(1, 2, \ldots, n)$.

***c.*** Il suffit par 1.a de traiter le cas $G = \mathfrak{S}_n$. Soit $e_1, \ldots, e_n$ la base canonique de $\mathbb{R}^n$. À tout $\sigma$ dans $\mathfrak{S}_n$, on associe la matrice $M_\sigma$ définie par $M_\sigma(e_i) = e_{\sigma(i)}$. On voit facilement que c'est une action de groupe, qui est un plongement.

**2.** Soit $M$ une matrice de $G$ telle que $M \equiv \mathrm{I}_n\ (p)$. On peut alors écrire $M = \mathrm{I}_n + pR$ où $R$ est dans $M_n(\mathbb{Z})$. Comme $M$ est diagonalisables avec valeurs propres racines de l'unité (car $G$ est fini), $R$ également, et ses valeurs propres sont de module $< 2/p$. On en déduit que $R^N \to 0$ quand $N \to +\infty$, mais comme $R$ est à coefficients entiers, ceci implique que $R^N$ est nulle pour $N$ assez grand. $R$ étant diagonalisable, elle est nulle.

## Exercice 3

**1.** Soit $G$ un groupe fini agissant sur un espace fini $X$.

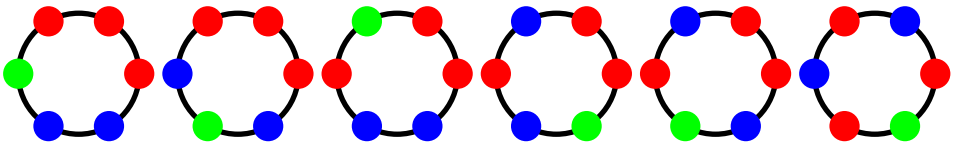
***a.*** Le lemme de Burnside dit que $\#X/G = \dfrac{1}{|G|} \displaystyle\sum_{g \in G} \#X^g$. Son intérêt est de pouvoir compter des objets identifiés par l'action d'un groupe *sans avoir besoin nécessairement de les expliciter*.

***b.*** $X^g$ est naturellement isomorphe à $X^{hgh^{-1}}$ via l'application $x \mapsto h.x$.

***c.*** On peut regrouper les éléments de $G$ par classes de conjuguaison, ce qui donne $\#X/G = \dfrac{1}{|G|} \displaystyle\sum_{[g] \in \mathrm{Cl}(G)} \#[g] \times \#X^g$.

**2.** ***a.*** Soit $X$ l'espace des applications $f : \mu_6 \to R, B, V$ telles que $\#f^{-1}(R) = 3, \#f^{-1}(B) = 2$ et $\#f^{-1}(V) = 1$. On a une action naturelle du groupe dihédral $D_{12}$ sur $X$, et l'espace des colliers s'identifie à $X/D_{12}$. On a $\#X = \binom{6}{3} \times \binom{3}{1} = 60$. On va maintenant regarder les orbites sous $D_{12}$. Pour cela, on remarque que toutes les orbites par rapport au sous-groupe $\mathbb{Z}/6\mathbb{Z}$ sont de cardinal 6, car la perle verte n'est jamais fixée par une rotation non triviale. On dispose ainsi que 10 orbites sous $\mathbb{Z}/6\mathbb{Z}$ qui sont les orbites de $(1)RRRVBB$, $(2)RRRBVB$, $(3)RRRBBV$, $(4)RRVRBB$, $(5)RRBRBV$, $(6)RRBRVB$, $(7)RRBBRV$, $(8)RRBVRB$, $(9)RRVBRB$, $(10)RBRBRV$. Dans cette notation, la valeur de la k-ème lettre est $f(\alpha^k)$ où $\alpha = \exp(2\mathbf{i}\pi/3)$. Soit $s$ l'élément canonique d'ordre 2 de $D_{12}$ donné par l'inversion. L'action de $s$ s'écrit $s(ABCDEF) = (AFEDCB)$ Alors $D_{12}$ est engendré par $\mathbb{Z}/6\mathbb{Z}$ et $g$. Il suffit donc de regarder comment $s$ agit sur les 10 $\mathbb{Z}/6\mathbb{Z}$ orbites. On voit que $(1) \to (3)$, $(2)$ est fixe, $(4) \to (7)$, $(5) \to (9)$,

(6) $\to$ (8) et (10) est fixe. On a ainsi 4 orbites à 12 éléments et 2 orbites à 6, soit 6 orbites en tout. Il y a donc 6 colliers possibles. De manière graphique, ce sont les six colliers suivants :



***b.*** On applique le lemme de Burnside. Pour ceci il faut lister les classes de conjuguaison dans $D_{12}$ et le nombre d'éléments fixés par chaque élément.

- La classe de l'identité (à ne pas oublier). Elle n'a qu'un élément, et tous les colliers sont fixés donc $\#X_g = 60$.
- La classe de $r$. Elle contient $r$ et $r^{-1}$. Aucun élément n'est fixé, car il n'y a qu'une perle verte.
- La classe de $r^2$. Elle contient $r^2$ et $r^{-2}$. Idem, aucun élément fixé.
- La classe de $r^3$, qui est réduite à $r^3$. Pas d'élément fixé.
- La classe de $s$, qui contient les 3 symétries $sr^{2k}$, $0 \leq k \leq 2$. On regarde maintenant combien de colliers sont fixés par $s$. Les conditions sont que les couples de perles $(1,5)$ et $(2,4)$ sont de même couleur. Ils sont donc de la forme $(\star RBBR\star)$ ou $(\star BRRB\star)$. Comme dans les deux perles restantes, il y n'y a que deux choix possible (une verte l'autre rouge), on trouve 4 possibilités.
- La classe de $rs$, qui contient les 3 symétries $rs$, $r^3s$ et $r^{-1}s$. $rs$ agit sur un élément $ABCDEF$ en le transformant en $FEDCBA$. Les colliers fixes sont donc de la forme $ABXXBA$. Il n'y a aucun élément fixe car une seule perle verte.

Le lemme de Burnside entraîne donc $\#X/D_{12} = \dfrac{1}{12}(60 + 3 \times 4) = 72/12 = 6$. La preuve est bien plus rapide, mais par contre elle ne produit pas une description explicite des orbites.

## Exercice 4

**1.** ***a.*** Soit $\sum_{n\geq 0} a_n t^n$ une série entière inversible. Alors $a_0 \neq 0$ car si $\sum_{n\geq 0} b_n t^n$ est l'inverse, $a_0 b_0 = 1$. Réciproquement, si $a_0 \neq 1$, on sait que $\sum_{n\geq 0} a_n t^n$ est inversible : les coefficients $b_n$ de l'inverse étant définis par récurrence par la formule $b_n = \dfrac{-1}{a_0} \sum_{k=1}^{n} a_k b_{n-k}$.

***b.*** Soit $I$ in idéal de $\mathbf{k}[[t]]$. Soit $n$ le plus grand entier tel que tous les éléments de $I$ soient divisibles par $t^n$. Alors il existe un élément de $I$ de la forme $f = a_n t^n + \ldots$ où $a_n \neq 0$. On peut donc écrire $f = t^n * g$ où $g$ est inversible et par suite $t^n \in I$ et donc $(t^n) \subset I$. Or par définition de $n$, $I \subset (t^n)$ donc $I = (t^n)$. $I$ est donc principal.

**2.** Dans ces deux anneaux, montrons que l'idéal engendré par $x$ et $y$ n'est pas principal. Supposons par l'absurde que $(x, y) = (f)$. Alors $f$ divise $x$ et $y$. Écrivons $f(x, y) = \sum_{p\geq 0} a_{pq} x^p y^q$. Comme $f \in (x, y)$, on peut écrire $f = xg + yh$ donc $a_{0,0} = 0$. Soit $\ell(x, y)$ la par

## Exercice 5

**1.** Soit $A$ un anneau euclidien. À tout couple d'éléments $(x, y)$ où $y$ est non nul, on associe le couple $(y, r)$, où $x = by + r$ est la division euclidienne de $x$ par $y$.

***a.*** Comme $r = x - by$, $r \in (x, y)$ donc $(y, r) \subset (x, y)$. En sens inverse, $x = by + r$ donc $x \in (y, r)$, d'où $(x, y) \subset (y, r)$.

***b.*** Soit $\nu$ le stathme de $A$. Alors si $r \neq 0$, $\nu(r) < \nu(y)$. La suite des stathmes du deuxième facteur est donc strictement décroissante (tant que $r > 0$), donc ce second facteur doit s'annuler à une étape de l'algorithme, car le stathme est positif.

***c.*** Par la question 1.a, $(x, y) = (d, 0) = d$ donc $d$ est le pgcd de $x$ et $y$.

**2.** On applique l'algorithme : $243 = 1 \times 198 + 45$ ; $198 = 4 \times 45 + 18$ ; $45 = 2 \times 18 + 9$ ; $18 = 2 \times 9$. On en déduit $d = 9$.

**Remarque** : l'algorithme d'Euclide permet de trouver des coefficients de Bezout $a$ et $b$ tels que $ax+by = d$ (c'est ce qu'on appelle l'algorithme de Bezout étendu). Pour ceci il suffit de remonter les calculs en sens inverse. Montrons comment faire dans un exemple pour ceci on doit décomposer 9 via la succession d'égalités $(9) = (18, 9) = (45, 18) = (198, 45) = (243, 198)$. On écrit

$$\begin{aligned} 9 &= 45 - 2 \times 18 \\ &= 45 - 2 \times (198 - 4 \times 45) \\ &= -2 \times 198 + 9 \times 45 \\ &= -2 \times 198 + 9 \times (243 - 198) \\ &= 9 \times 243 - 11 \times 198 \end{aligned}$$

**3.** On a $\left|\dfrac{22+\mathbf{i}}{97}\right| < 97$ donc la première étape de l'algorithme donne $(97, 22 + \mathbf{i})$. Ensuite, on voit $\dfrac{97}{22+\mathbf{i}} = \dfrac{97(22-\mathbf{i})}{485} = \dfrac{2134 - 97\mathbf{i}}{485}$. On fait la division euclidienne coordonnée par coordonnée. $2134 = 4 * 485 + 194$ et $97 = 0 * 485 + 97$. On a donc $97 = 4(22 + \mathbf{i}) + 9 - 4\mathbf{i}$ donc la seconde étape de l'algorithme donne $(22 + \mathbf{i}, 9 - 4\mathbf{i})$. On calcule à nouveau $\dfrac{22+\mathbf{i}}{9i-4\mathbf{i}} = \dfrac{194+97\mathbf{i}}{97} = 2 + \mathbf{i}$. On tombe donc sur $(2 + \mathbf{i}, 0)$ donc le pgcd est $2 + \mathbf{i}$.

**4.** Supposons $r > s$. Alors $\text{pgcd}(M_r, M_s) = \text{pgcd}(M_r - M_s, M_s)$. Or $M_r - M_s = 2^r - 2^s = 2^s M_{r-s}$. Comme $M_s$ est impair, on en déduit $\text{pgcd}(M_r, M_s) = \text{pgcd}(M_{r-s}, M_s)$. On peut appliquer ceci de manière répétée, ce qui permet de montrer que si $s = \alpha r + \beta$ est la division euclidienne de $s$ par $r$, alors $\text{pgcd}(M_r, M_s) = \text{pgcd}(M_\beta, M_s) = \text{pgcd}(M_s, M_\beta)$. Or $(s, \beta)$ est exactement l'image de l'algorithme d'Euclide appliqué à $(r, s)$. Ceci montre que la fonction $(r, s) \to \text{pgcd}(M_r, M_s)$ est invariante lorsqu'on applique l'algorithme d'Euclide au départ. De manière formelle,

$$\begin{array}{ccc} (r, s) & \longrightarrow & \text{pgcd}(M_r, M_s) \\ {\scriptstyle \text{Euclide}}\downarrow & & \| \\ (s, \beta) & \longrightarrow & \text{pgcd}(M_s, M_\beta) \end{array}$$

Comme l'algorithme termine à $(\text{pgcd}(r, s), 0)$, on obtient le résultat.

## Exercice 6

**1.** ***a.*** On a $\nu(1) = \nu(1) + \nu(1)$ donc $\nu(1) = 0$. Si $a \in A$ est inversible, il existe $b$ tel que $ab = 1$. Alors $\nu(a) + \nu(b) = 0$ et comme $\nu(a)$ et $\nu(b)$ sont positifs, $\nu(a) = \nu(b) = 0$. Réciproquement, si $\nu(a) = 0$, $a \neq 0$ donc $a$ est inversible dans $K$. Si $b$ est son inverse, $\nu(a) + \nu(b) = 0$ donc $\nu(b) = 0$ et $b \in A$.

***b.*** Soit $I$ un idéal non trivial de $A$. Si $a \in I$, $a$ est non inversible donc $\nu(a) \geq \nu(t)$. On a alors $\nu(a/t) = \nu(a) - \nu(t) \geq 0$ donc $a/t \in A$ et comme $a = t \times \dfrac{a}{t}$, $a \in (t)$.

***c.*** Si $a$ est un élément de valuation minimale de $I$, l'argument précédent montre que $I \subset (a)$. Mais comme $a \in I$, $I = (a)$.

***d.*** L'application $\nu : K^\star \to \mathbb{Z}$ est un morphisme de groupes. Son image est donc $\nu(t)\mathbb{Z}$. L'élément de valuation minimale $a$ dans $I$ satisfait donc $\nu(a) = s\nu(t)$ pour un entier $s > 0$. Alors $a/t^s$ est inversible, donc $(a) = (t^s)$.

**2.** ***a.*** On considère le corps des séries de Laurent formelles à coefficients dans $\mathbf{k}$, qui sont les séries formelles de la forme $\displaystyle\sum_{n\in\mathbb{Z}} a_n t^n$ où seuls un nombre fini de coefficients $a_n$ pour $n < 0$ sont non nuls. On vérifie facilement que c'est un corps en utilisant qu'une série entière dont le terme constant est non nul est inversible. La valuation est définie par $\nu\left(\displaystyle\sum_{n\in\mathbb{Z}} a_n t^n\right) = \inf\{k \in \mathbb{Z}, a_k \neq 0\}$.

***b.*** Le corps est essentiellement le même qu'à la question précédente (pour mais on demande cette fois que la série soit convergente dans un voisinage de 0. Il faut alors utiliser le théorème d'inversion des séries entières.