DM 19 – Groupes finis – Corrigé

1 Théorème de Cauchy

1. - Réflexivité. Soit $(g_c) \in E$. Alors, pour tout $c \in \mathbb{Z}/p\mathbb{Z}$, $g_c = g_{0+c}$. Donc, $(g_c)\mathscr{R}(g_c)$.
   - Symétrie. Soient (g_c) et (g'_c) dans E tels que $(g_c)\mathscr{R}(g'_c)$. Alors, il existe $a \in \mathbb{Z}/p\mathbb{Z}$ tel que $\forall c \in \mathbb{Z}/p\mathbb{Z}, g_c = g'_{c+a}$. Avec $b = -a$, on a donc $\forall c \in \mathbb{Z}/p\mathbb{Z}, g'_c = g_{c+b}$. Donc, $(g'_c)\mathscr{R}(g_c)$.
   - Transitivité. Soient (g_c), (g'_c) et (g''_c) dans E tels que $(g_c)\mathscr{R}(g'_c)$ et $(g'_c)\mathscr{R}(g''_c)$. Alors, il existe a et b dans $\mathbb{Z}/p\mathbb{Z}$ tels que pour tout $c \in \mathbb{Z}/p\mathbb{Z}$, $g_c = g'_{c+a}$ et $g'_c = g''_{c+b}$. Avec $d = a+b$, on a $\forall c \in \mathbb{Z}/p\mathbb{Z}$, $g_c = g''_{c+d}$. Donc, $(g_c)\mathscr{R}(g''_c)$.

2. D'abord, $H_{(g_c)}$ contient la classe $0 \in \mathbb{Z}/p\mathbb{Z}$. Soient $x, y \in H_{(g_c)}$. On a donc,

$$\forall c \in \mathbb{Z}/p\mathbb{Z}, g_{a+x-y} = g_{a-y} = g_a,$$

   en utilisant successivement que x et y sont dans $H_{(g_c)}$ (dans un sens et dans l'autre). Donc, $H_{(g_c)}$ est un sous-groupe de $\mathbb{Z}/p\mathbb{Z}$.

3. Les seuls sous-groupes de $\mathbb{Z}/p\mathbb{Z}$ sont $\{0\}$ et $\mathbb{Z}/p\mathbb{Z}$ lui-même (car le cardinal d'un tel sous-groupe doit diviser p).

   - Si $H_{(g_c)} = \mathbb{Z}/p\mathbb{Z}$, (g_c) est égal à tous ses translatés ; donc $\mathrm{cl}_{\mathscr{R}}((g_c))$ a pour cardinal 1.
   - Si $H_{(g_c)} = \{0\}$, alors l'application $f : \mathbb{Z}/^p\mathbb{Z} \to \mathrm{cl}_{\mathscr{R}}((g_c)), a \mapsto (g_{c+a})$, qui est surjective par définition, est aussi injective. En effet, si elle ne l'était pas, et si on avait $f(a) = f(b)$ avec a et b distincts dans $\mathbb{Z}/p\mathbb{Z}$, on aurait $a - b \in H_{(g_c)}$. Donc, dans ce cas, $\mathrm{cl}_{\mathscr{R}}((g_c))$ a pour cardinal p.

4. D'après ce qui précède, les $\mathscr{R}$-classes d'équivalence sont de cardinal 1 ou p. Notons r le nombre de classes de cardinal 1 et ℓ le nombre de classes de cardinal p. On a donc $|E| = r + \ell p$.

5. Remarquons déjà que $|E| = |G|^{p-1}$ (en effet, l'élément $g_{\overline{p-1}}$ est déterminé de façon unique par les éléments $g_{\overline{k}}$ pour $k \in [\![0, p-2]\!]$ et ces éléments sont quelconques). On en déduit que $p||E|$. D'après la question précédente, on a donc aussi $p \mid r$. Or, un élément de E dont la classe d'équivalence est de cardinal 1 est simplement une famille $(g_c)_{c\in\mathbb{Z}/p\mathbb{Z}}$ où tous les g_c sont les mêmes. L'ensemble de ces éléments est donc en bijection avec l'ensemble des $x \in G$ tels que $x^p = e$ (vu la définition de E). Or, si x vérifie cette équation, son ordre divise p : c'est donc 1 (et $x = e$) ou p. Autrement dit, le nombre N recherché vaut $N = r - 1$. Donc, $N \equiv -1\,[r]$.

2 Structure de $(\mathbb{Z}/n\mathbb{Z})^\times$

1. Soit $k \in [\![0, p^\alpha - 1]\!]$. La classe de k modulo p^α est inversible dans $\mathbb{Z}/p^\alpha\mathbb{Z}$ ssi k n'est pas divisible par p. Les classes non inversibles sont donc celles des entiers de la forme up, où $u \in [\![0, p^{\alpha-1} - 1]\!]$: il y en a $p^{\alpha-1}$. Et donc, le groupe des inversibles de $\mathbb{Z}/p^\alpha\mathbb{Z}$ est de cardinal $p^\alpha - p^{\alpha-1}$.

2.1 Étude de $\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^\times$ pour $p \neq 2$ et $\alpha \geq 2$

2. On le montre par récurrence sur $k \geq 1$.

   - Pour $k = 1$, on a par la formule du binôme que :

     $$(1+p)^p = \sum_{k=0}^{p} \binom{p}{k} p^k = 1 + p \times p + \binom{p}{2} p^2 + p^3 \sum_{k=3}^{p} \binom{p}{k} p^{k-3} = 1 + p^2 \left(1 + \binom{p}{2} + p \sum_{k=3}^{p} \binom{p}{k} p^{k-3}\right).$$

     Comme $\binom{p}{2}$ est divisible par p, la parenthèse à droite est congrue à 1 modulo p, de sorte qu'on a bien écrit $(1+p)^p$ sous la forme $1 + \lambda p^2$, avec $\lambda \wedge p = 1$.
   - Soit $k \geq 1$ pour lequel l'énoncé est vrai. On peut donc écrire $(1+p)^{p^k} = 1 + \lambda p^{k+1}$, où $\lambda \wedge p = 1$. Alors,

     $$(1+p)^{p^{k+1}} = (1 + \lambda p^{k+1})^p = \sum_{i=0}^{p} \binom{p}{i} \lambda^i p^{i(k+1)} = 1 + \lambda p^{k+2} + \sum_{i=2}^{p} \binom{p}{i} \lambda^i p^{i(k+1)}.$$

     Tous les termes dans la somme de droite sont divisibles par $p^{2(k+2)}$ donc par p^{k+3}. Ainsi, $(1+p)^{p^{k+1}}$ s'écrit $1 + \lambda p^{k+2} + \mu p^{k+3} = 1 + (\lambda + \mu p) p^{k+2}$, pour un certain entier μ. Comme λ et $\lambda + \mu p$ sont congrus modulo p, on a $(\lambda + \mu p) \wedge p = 1$, ce qui conclut la récurrence.

3. Déjà, $(1+p)^{p^{\alpha-1}}$ est de la forme $1 + \lambda p^\alpha$ donc vaut 1 modulo p^α. Ceci montre que l'ordre de la classe de $1+p$ dans $\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^\times$ divise $p^{\alpha-1}$. Cet ordre est donc un p^k, où $k \leq \alpha - 1$.
   Mais si $k < \alpha - 1$, $(1+p)^{p^k} = 1 + \lambda p^{k+1}$ n'est pas congru à 1 modulo p^α (sinon, on aurait $p^\alpha \mid \lambda p^{k+1}$, contredisant le fait que $\lambda \wedge p = 1$). Donc, l'ordre de la classe de $1+p$ dans $\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^\times$ est exactement $p^{\alpha-1}$.

4. Notons ω l'ordre de la classe de x dans $\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^\times$. Alors, x^ω est congru à 1 modulo p^α. En particulier, x^ω est congru à 1 modulo p, ce qui revient à dire que l'ordre de la classe de x dans $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ divise ω. Comme cet ordre vaut $p-1$, ω est divisible par $p-1$.

5. Avec les notations précédentes, on peut écrire $\omega = k(p-1)$. Alors, x^k est d'ordre $p-1$ dans $\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^\times$.

6. On commence par montrer un lemme qui nous sera utile.
   Si G est un groupe abélien et si x et y sont deux éléments de G d'ordres $\omega(x)$ et $\omega(y)$ premiers entre eux, alors l'ordre de xy est $\omega(x)\omega(y)$.
   En effet, considérons un entier k tel que $(xy)^k = e_G$. On a alors $x^k = y^{-k}$. En élevant à la puissance $\omega(x)$, il vient $y^{-k\omega(x)} = e_G$ et donc, $\omega(y) \mid k\omega(x)$. Comme $\omega(x)$ et $\omega(y)$ sont

supposés premiers entre eux, $\omega(y) \mid k$. Par le même argument, $\omega(x) \mid k$. Donc, $\omega(x)\omega(y) \mid k$. Réciproquement, on a bien $(xy)^{\omega(x)\omega(y)} = e_G$, ce qui montre le lemme.

On peut alors appliquer le lemme au groupe $\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^\times$, avec les éléments $1+p$ et y d'ordres respectifs $p^{\alpha-1}$ et $p-1$, premiers entre eux. L'ordre de $(1+p)y$ dans $\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^\times$ est donc $p^{\alpha-1}(p-1) = p^\alpha - p^{\alpha-1}$. Comme cet ordre est le cardinal de $\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^\times$, ce groupe est cyclique, engendré par $(1+p)y$.

2.2 Étude de $\left(\mathbb{Z}/2^\alpha\mathbb{Z}\right)^\times$

7. Le groupe $(\mathbb{Z}/2\mathbb{Z})^\times$ est réduit à la classe de 1.
Les classes inversibles modulo 4 sont celles de 1 et 3. Ainsi $(\mathbb{Z}/4\mathbb{Z})^\times$ est un groupe à 2 éléments, nécessairement isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

8. On procède par récurrence.

   - Pour $k=1$, on a $5^2 = 25 = 1+3\times 2^3$ et 3 est impair.
   - Supposons le résultat montré pour un $k \geq 1$. On écrit $5^{2^k} = (1+\lambda 2^{k+2})$ avec λ impair. Alors,
   $$5^{2^{k+1}} = (1+\lambda 2^{k+2})^2 = 1+\lambda 2^{k+3} + \lambda^2 2^{2k+4} = 1+(\lambda+\lambda^2 2^{k+1})2^{k+3}.$$
   L'entier $\lambda+\lambda^2 2^{k+1}$ a la même parité que λ donc est impair, ce qui conclut la récurrence.

9. Ainsi, $5^{2^{\alpha-2}}$ s'écrit $1+\lambda 2^\alpha$, qui vaut 1 modulo 2^α. Donc, l'ordre de 5 dans $\left(\mathbb{Z}/2^\alpha\mathbb{Z}\right)^\times$ divise $2^{\alpha-2}$. Il est donc de la forme 2^k, pour un $k \leq \alpha-2$.
Comme précédemment, si $k < \alpha-2$, $5^{2^k} = 1+\lambda 2^{k+2}$ avec un entier impair λ n'est pas congru à 1 modulo 2^α. Donc, l'ordre de 5 modulo 2^α est exactement $2^{\alpha-2}$.

10. ϕ est bien définie car la classe de 5 dans $\left(\mathbb{Z}/2^\alpha\mathbb{Z}\right)^\times$ est d'ordre $2^{\alpha-2}$ (et donc 5^k dépend uniquement de la classe de k modulo $2^{\alpha-2}$).
Soient $\varepsilon, \varepsilon' \in \{\pm 1\}$, soient k, ℓ des classes modulo $2^{\alpha-2}$. Pour montrer que ϕ est un morphisme, il s'agit de vérifier que
$$\varepsilon 5^k \times \varepsilon' 5^\ell = (\varepsilon\varepsilon')5^{k+\ell}$$
dans $\left(\mathbb{Z}/2^\alpha\mathbb{Z}\right)^\times$. Mais cette égalité est claire en considérant des entiers représentant k et ℓ.
Le groupe de gauche est de cardinal $2\times 2^{\alpha-2} = 2^{\alpha-1}$. C'est aussi le cardinal de $\left(\mathbb{Z}/2^\alpha\mathbb{Z}\right)^\times$. Donc, pour montrer que ϕ est un isomorphisme, il suffit de montrer que ϕ est injectif.
Considérons donc $(\varepsilon, k) \in \operatorname{Ker}\phi$. On a donc $\varepsilon 5^k = 1$, modulo 2^α. En passant au carré, $5^{2k} = 1$ modulo 2^α. Comme la classe de 5 est d'ordre $2^{\alpha-2}$ (modulo 2^α), on en déduit que $2^{\alpha-2}$ divise 2^k. Donc, $2^{\alpha-3}$ divise k ; donc k vaut $2^{\alpha-3}$ ou $2^{\alpha-2}$ (c'est-à-dire 0) modulo $2^{\alpha-2}$.

   - Dans le deuxième cas, k est nul modulo $2^{\alpha-2}$ et on en déduit que $\varepsilon = 1$ modulo 2^α, et donc finalement que $\varepsilon = 1$. Ainsi, (ε, k) est l'élément neutre de $\mathbb{U}_2 \times \left(\mathbb{Z}/2^{\alpha-2}\mathbb{Z}\right)^\times$.
   - Dans le premier cas, $k = 2^{\alpha-3}$. On sait déjà que $5^{2^{\alpha-3}}$ ne vaut pas 1 modulo 2^α. Et comme $5^{2^{\alpha-3}}$ s'écrit $1+\lambda 2^{\alpha-1}$ avec λ impair, on a
   $$-5^{2^{\alpha-3}} = -1-\lambda 2^{\alpha-1} \equiv -1-2^{\alpha-1}\,[2^\alpha].$$
   Ceci est non nul car $\alpha \geq 3$.

Ceci montre que le noyau de ϕ est trivial et conclut la démonstration de l'isomorphisme.

2.3 Quand $(\mathbb{Z}/n\mathbb{Z})^\times$ est-il cyclique ?

11. Le théorème des restes chinois (et une récurrence) nous dit que l'anneau $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à l'anneau produit $\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}$.
De plus, si A_1 et A_2 sont deux anneaux, les inversibles de $A_1 \times A_2$ sont les éléments de $A_1^\times \times A_2^\times$. En effet, un couple $(a_1, a_2) \in A_1 \times A_2$ est inversible ssi il existe $(b_1, b_2) \in A_1 \times A_2$ tel que $(a_1b_1, a_2b_2) = (1_{A_1}, 1_{A_2})$ ssi a_1 et a_2 sont inversibles. L'argument montre plus précisément qu'on a un isomorphisme de groupes $(A_1 \times A_2)^\times \cong A_1^\times \times A_2^\times$. Et on peut généraliser immédiatement à un produit de r anneaux.
Ainsi, le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$ est isomorphe au groupe des inversibles de $\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}$ (car ces anneaux sont isomorphes donc leur groupe des inversibles aussi), lui-même inversible à $\left(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}\right)^\times \times \cdots \times \left(\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}\right)^\times$.

12. Le fait que le produit de deux groupes cycliques d'ordre premier entre eux est cyclique a été fait en cours (proposition 2.6) ; on généralise à r groupes cycliques d'ordre premier entre eux pour obtenir l'implication droite-gauche.
Pour la réciproque, on raisonne par contraposée en supposant que deux des cardinaux ne sont pas premiers entre eux. Pour simplifier et par symétrie, on suppose que $|C_1|$ et $|C_2|$ ont un diviseur d commun, avec $d \geq 2$. Soit $x = (x_1, \ldots, x_n)$ un élément de $C_1 \times C_n$. L'entier $k = \dfrac{|C_1||C_2|}{d} \times |C_3| \times \cdots \times |C_n|$ est divisible par tous les $|C_i|$. Or, par le théorème de Lagrange, $x_i^{|C_i|} = e_{C_i}$. Donc, $x^k = e_{C_1 \times C_n}$. Ceci montre que l'ordre de tout élément de $C_1 \times \ldots \mathbb{C}_n$ divise strictement $\prod_{k=1}^{n} |C_k|$, donc que le produit $C_1 \times \cdots \times C_n$ n'est pas cyclique.

13. Notons $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$. On peut supposer que $p_1 = 2$, quitte à prendre α_1 égal à 0. Par une question précédente, le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à $\left(\mathbb{Z}/2^{\alpha_1}\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z}\right)^\times \times \cdots \times \left(\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}\right)^\times$.
Pour $k \geq 2$, on note $C_k = \left(\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}\right)^\times$. On sait que c'est un groupe cyclique de cardinal $p_k^{\alpha_k - 1}(p_k - 1)$. Et le groupe $\left(\mathbb{Z}/2^{\alpha_1}\mathbb{Z}\right)^\times$ est ou bien cyclique, ou bien produit de deux groupes cycliques par les questions précédentes. Dans tous les cas, on est parvenu à écrire $(\mathbb{Z}/n\mathbb{Z})^\times$ comme produit de groupes cycliques ; d'après la question précédente, ce groupe sera cyclique ssi tous les cardinaux des groupes cycliques obtenus sont deux à deux premiers entre eux. En particulier, un seul peut être de cardinal pair ; si $k \geq 2$, $p_k^{\alpha_k - 1}(p_k - 1)$ est pair et donc – pour que $(\mathbb{Z}/n\mathbb{Z})^\times$ soit cyclique – n doit avoir au plus un facteur premier impair. Si $\alpha_1 \geq 2$, le groupe $\left(\mathbb{Z}/2^{\alpha_1}\mathbb{Z}\right)^\times$ est aussi de cardinal pair. On obtient donc les possibilités suivantes :

    - Ou bien n a exactement un facteur premier impair. Alors, la valuation dyadique de n est au maximum 1 de sorte que n est de la forme p^k ou $2p^k$.
    - Ou bien n est une puissance de 2. Par la partie précédente, le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$ est cyclique ssi $n = 1, 2$ ou 4.

    Réciproquement, les calculs précédents montrent que si $n = 1, 2, 4$, p^k ou $2p^k$ avec p impair et $k \geq 1$, alors le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$ est cyclique.