

### Partie I: Préliminaires

1. Soit  $x, y, z \in \mathbb{N}^*$  tels que  $x \wedge y = 1$  et  $x \wedge z = 1$ , montrer que  $x \wedge yz = 1$  (On pourra utiliser l'égalité de Bezout)
2. Soient  $x, y_1, \dots, y_k \in \mathbb{N}^*$  tels que  $\forall i \in \llbracket 1, k \rrbracket, x \wedge y_i = 1$ , montrer que  $x \wedge \left( \prod_{i=1}^k y_i \right) = 1$

### Partie II: Ordre d'un produit

Soit  $G$  un groupe abélien fini de cardinal  $n$ .

3. Soit  $(a, b) \in G^2$  tels que  $\circ(a) = p$  et  $\circ(b) = q$  avec  $p \wedge q = 1$ , et soit  $s = \circ(ab)$ 
  - (a) Montrer que  $s$  divise  $pq$
  - (b) Montrer que  $(ab)^{sq} = e$ , en déduire que  $a^{sq} = e$  puis que  $p$  divise  $s$
  - (c) Montrer de même que  $q$  divise  $s$ .
  - (d) Montrer que  $s = pq$
4. Soit  $k \in \mathbb{N}$  tel que  $k \geq 2$  et  $a_1, \dots, a_k \in G$  tels que  $\circ(a_i) = n_i$  avec  $n_i \wedge n_j = 1$  si  $i \neq j$ .  
Montrer par récurrence sur  $k$  que  $\circ \left( \prod_{i=1}^k a_i \right) = \prod_{i=1}^k n_i$

### Partie III: Exposant d'un groupe abélien fini

Soit  $G$  un groupe abélien fini de cardinal  $n$ .

On appelle exposant de  $G$  l'entier  $r = \text{ppcm}_{g \in G}(\circ(g))$

5. Déterminer l'exposant de  $\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
6. Montrer que si  $G$  est cyclique alors  $r = n$ .
7. Soit  $r = p_1^{\alpha_1} \dots p_s^{\alpha_s}$  la décomposition en facteur premier de  $r$ .
  - (a) Montrer que pour tout  $i \in \llbracket 1, s \rrbracket$  il existe  $g_i \in G$  tel que  $\circ(g_i) = p_i^{\alpha_i} q_i$  avec  $p_i \wedge q_i = 1$
  - (b) Soit  $h_i = g_i^{q_i}$ . Montrer que  $\circ(h_i) = p_i^{\alpha_i}$
  - (c) Montrer en utilisant le préliminaire qu'il existe  $g \in G$  tel que  $\circ(g) = r$

### Partie IV: Les sous-groupes finis de $(\mathbb{K}^*, \times)$

Soit  $\mathbb{K}$  un corps. et  $G$  un sous groupe fini de  $(\mathbb{K}^*, \times)$ , de cardinal  $n$

Soit  $r$  l'exposant du groupe multiplicatif  $G$  et  $g \in G$  tel que  $\circ(g) = r$ .

**On admet que tout polynôme non nul  $P \in \mathbb{K}[X]$  admet au plus  $\deg(P)$  racines**

8. Montrer que  $r$  divise  $n$ .
9. Montrer que les éléments de  $G$  sont des racines du polynôme  $X^r - 1$  dans  $\mathbb{K}$ , en déduire que  $n \leq r$
10. Montrer que  $r = n$
11. En déduire que le groupe  $(G, \times)$  est cyclique.
12. Montrer que si  $\mathbb{K}$  est un corps fini alors le groupe multiplicatif  $(\mathbb{K}^*, \times)$  est cyclique
13. (a) Montrer que si  $p$  est un entier premier alors le groupe multiplicatif  $(\mathbb{Z}/p\mathbb{Z} \setminus \{0\}, \times)$  est cyclique;  
(b) Vérifier que  $\bar{3}$  est un générateur de  $(\mathbb{Z}/7\mathbb{Z} \setminus \{0\}, \times)$ , puis déterminer ses autres générateurs.

## Partie V: Le groupe $\left(\mathbb{U}\left(\mathbb{Z}/p^2\mathbb{Z}\right), \times\right)$ lorsque $p$ est premier

Soit  $p$  est un entier premier. Pour  $x \in \mathbb{Z}$  on notera par  $\hat{x}$  (respectivement  $\bar{x}$ ) la classe de  $x$  modulo  $p$  ( respectivement modulo  $p^2$ )

Soit  $b$  un entier dont la classe  $\hat{b}$  est d'ordre  $p-1$  dans  $\left(\mathbb{U}\left(\mathbb{Z}/p\mathbb{Z}\right), \times\right)$ .

14. Montrer que  $(b+p)^{p-1} - b^{p-1} \equiv p(p-1)b^{p-2} \pmod{p^2}$ , en déduire que  $p^2$  ne divise pas  $(b+p)^{p-1} - b^{p-1}$
15. Montrer par l'absurde que l'un au moins des deux entiers  $b^{p-1}$  ou  $(b+p)^{p-1}$  n'est pas congru à 1 modulo  $p^2$ .  
On notera  $c$  l'un des nombres  $b$  ou  $b+p$  de façon à ce que  $c^{p-1}$  ne soit pas congru à 1 modulo  $p^2$ .
16. Montrer que  $c^{p-1} \equiv b^{p-1} \pmod{p}$  et déduire qu'il existe  $q \in \mathbb{N}$  tel que  $c^{p-1} = 1 + qp$  avec  $p$  ne divise pas  $q$
17. Montrer qu'il existe  $k \in \mathbb{N}$ ,  $c^{p(p-1)} = 1 + kp^2$  avec  $p$  ne divise pas  $k$
18. En déduire que  $\bar{c}$  appartient à  $\mathbb{U}\left(\mathbb{Z}/p^2\mathbb{Z}\right)$ .
19. Soit  $r$  l'ordre de  $\bar{c}$  dans  $\left(\mathbb{U}\left(\mathbb{Z}/p^2\mathbb{Z}\right), \times\right)$ .
  - (a) Rappeler **Card** $\left(\mathbb{U}\left(\mathbb{Z}/p^2\mathbb{Z}\right)\right)$ , en déduire que  $r$  divise  $p(p-1)$
  - (b) Montrer que  $c^r \equiv 1 \pmod{p}$  et en déduire que  $(p-1)$  divise  $r$ .
  - (c) En déduire que  $r = p(p-1)$ .
  - (d) Montrer finalement que  $\bar{c}$  est un générateur de  $\left(\mathbb{U}\left(\mathbb{Z}/p^2\mathbb{Z}\right), \times\right)$ .
20. Application : Sachant que  $\hat{3}$  est un générateur de  $\left(\mathbb{U}\left(\mathbb{Z}/7\mathbb{Z}\right), \times\right)$ , déterminer un générateur de  $\left(\mathbb{U}\left(\mathbb{Z}/49\mathbb{Z}\right), \times\right)$ .

**L'EXPOSANT D'UN GROUPE**

**Partie I: Préliminaires**

1. Comme  $x \wedge y = 1$  et  $x \wedge z = 1$ , alors il existe  $u, v, \alpha, \beta \in \mathbb{Z}$  tels que

$$xu + yv = 1 \quad \text{et} \quad \alpha x + \beta z = 1$$

En multipliant membre à membre :  $(xu + yv)(\alpha x + \beta z) = 1$

On développe :  $(\alpha ux + \beta xz + \alpha vy)a + \beta v(yz) = 1$

Et d'après le théorème de Bézout :  $x \wedge (yz) = 1$

2. Par récurrence sur  $k \in \mathbb{N}^*$

— Pour  $k = 1$  rien à démontrer et le  $k = 2$  est traité dans la question précédente

— Soit  $k \geq 2$ . Supposons que pour tous  $x, y_1, \dots, y_k \in \mathbb{N}^*$  tels que  $\forall i \in \llbracket 1, k \rrbracket, x \wedge y_i = 1$ , alors  $x \wedge \left( \prod_{i=1}^k y_i \right) = 1$ .

Soit  $x, y_1, \dots, y_k, y_{k+1} \in \mathbb{N}^*$  tels que  $\forall i \in \llbracket 1, k+1 \rrbracket, x \wedge y_i = 1$ , alors, par hypothèse de récurrence on a  $x \wedge \left( \prod_{i=1}^k y_i \right) = 1$ . D'autre part  $x \wedge y_{k+1} = 1$ , alors, en appliquant le résultat précédent, on a  $x \wedge \left( \prod_{i=1}^{k+1} y_i \right) = 1$

**Partie II: Ordre d'un produit**

3. Soit  $(a, b) \in G^2$  tels que  $\circ(a) = p$  et  $\circ(b) = q$  avec  $p \wedge q = 1$ , et soit  $s = \circ(ab)$

(a) Les deux éléments  $a$  et  $b$  commutent, donc  $(ab)^{pq} = a^{pq}b^{pq} = e$ , donc  $s$  divise  $pq$

(b) On a  $(ab)^{sq} = ((ab)^s)^q = e$ . Comme  $(ab)^{sq} = a^{sq}b^{sq}$  et  $b^{sq} = e$ , alors on peut affirmer que  $a^{sq} = e$  puis que  $p$  divise  $sq$ . Mais  $p \wedge q = 1$ , donc, d'après le théorème de Gauss,  $p \mid s$

(c)  $p$  et  $q$  jouent un rôle symétrique. On a  $(ab)^{sp} = e$ , puis  $b^{sp} = e$ , donc  $q$  divise  $sp$ , ainsi  $q$  divise  $s$ .

(d) On a déjà montré que  $s \mid pq$ . D'autre part  $p \mid s$  et  $q \mid s$ , alors  $pq = \text{ppcm}(p, q) \mid s$ . Donc  $pq$  et  $s$  sont associés, voir qu'ils sont positifs, donc ils sont égaux

4. Par récurrence sur  $k \in \mathbb{N}$  tel que  $k \geq 2$

— Pour  $k = 2$ , c'est fait dans la question précédente

— Soit  $k \geq 2$ . Soit et  $a_1, \dots, a_k, a_{k+1} \in G$  tels que  $\circ(a_i) = n_i$  avec  $n_i \wedge n_j = 1$  si  $i \neq j$ . Par hypothèse de

récurrence  $a = \prod_{i=1}^k a_i$  est d'ordre  $\prod_{i=1}^k n_i$ . Or  $b = a_{k+1}$  est d'ordre  $n_{k+1}$  avec  $\left( \prod_{i=1}^k n_i \right) \wedge n_{k+1} = 1$ , donc

l'ordre de  $ab = \prod_{i=1}^{k+1} a_i$  est égal à  $\left( \prod_{i=1}^k n_i \right) \cdot n_{k+1} = \prod_{i=1}^{k+1} n_i$

**Partie III: Exposant d'un groupe abélien fini**

5. — Tout élément de  $\mathbb{Z}/4\mathbb{Z}$  est soit d'ordre 4, soit d'ordre 2, soit d'ordre 1, donc l'exposant de  $\mathbb{Z}/4\mathbb{Z}$  vaut le  $\text{ppcm}(1, 2, 4) = 4$

— Un élément de  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  est soit d'ordre 2, soit d'ordre 1, donc l'exposant de  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  égale 2

6. D'une part tout ordre d'un élément de  $G$  divise  $n$ , donc l'exposant  $r$  divise  $n$ . D'autre part  $G$  étant cyclique, donc il existe un élément de  $G$  d'ordre  $n$ , et par définition de  $r$  on a  $n$  divise  $r$ . Ainsi  $r = n$

7. Soit  $r = p_1^{\alpha_1} \dots p_s^{\alpha_s}$  la décomposition en facteur premier de  $n$ .

(a) On raisonne par l'absurde. Cela revient à supposer que si  $x$  est quelconque dans  $G$  alors son ordre  $\circ(x)$  est au plus divisible par  $p_i^{\alpha_i-1}$ . Mais dans ces conditions l'exposant de  $G$ , c'est-à-dire le  $\text{ppcm}$  des ordres  $\circ(g)$ , serait lui-même au plus divisible par  $p_i^{\alpha_i-1}$ , ce qui est absurde. Il existe donc un élément  $g_i$  de  $G$  dont l'ordre  $\circ(g_i)$ , est divisible au moins par  $p_i^{\alpha_i}$  (et donc exactement par  $p_i^{\alpha_i}$  sinon cela contredirait la factorisation de  $q$ ). On peut alors écrire  $\circ(g_i) = p_i^{\alpha_i} q_i$ , avec  $p_i \wedge q_i = 1$ .

(b) Soit  $k \in \mathbb{Z}$ . On a  $h_i^k = e$  équivaut à  $g_i^{q_i k} = e$ . Mais  $\circ(g_i) = q_i p_i^{\alpha_i}$ , donc  $h_i^k = e$  équivaut à  $q_i p_i^{\alpha_i} \mid q_i k \iff p_i^{\alpha_i} \mid k$ . Ainsi  $\circ(h_i) = p_i^{\alpha_i}$

**L'EXPOSANT D'UN GROUPE**

- (c) On vient de montrer que pour chaque  $i \in \llbracket 1, s \rrbracket$ , il existe  $h_i$  de  $G$  d'ordre  $p_i^{\alpha_i}$  avec les  $p_i^{\alpha_i}$  sont deux à deux premiers entre eux, d'après la partie II, l'élément  $h = \prod_{i=1}^s h_i$  est d'ordre  $\prod_{i=1}^s \circ(h_i) = \prod_{i=1}^s p_i^{\alpha_i} = r$

**Partie IV: Les sous-groupes finis de  $(\mathbb{K}^*, \times)$**

Soit  $\mathbb{K}$  un corps commutatif et  $G$  un sous groupe fini de  $(\mathbb{K}^*, \times)$ , de cardinal  $n$   
Soit  $r$  l'exposant du groupe multiplicatif  $G$  et  $g \in G$  tel que  $\circ(g) = r$ .

8. D'après le théorème de Lagrange l'ordre de chaque élément de  $G$  divise l'ordre de  $G$ , donc  $r$  divise  $n$ .
9. D'après la question précédente  $G$  est inclus dans l'ensemble des racines du polynôme  $X^r - 1$ . Un tel polynôme admet au plus  $r$  racines, donc  $n \leq r$
10.  $r$  divise  $n$  et  $r \geq n$ , alors  $r = n$
11. On a  $\text{Card}(\langle g \rangle) = \circ(g) = n$  et  $\langle g \rangle \subset G$ , donc  $G = \langle g \rangle$
12.  $\mathbb{K}^*$  est un sous-groupe multiplicatif fini, donc il est cyclique
13. (a)  $p$  étant un entier premier, alors  $\mathbb{Z}/p\mathbb{Z}$  est un corps fini, d'après la question précédente le groupe multiplicatif  $(\mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}, \times)$  est cyclique.
- (b) D'après le théorème de Lagrange,  $\circ(\bar{3})$  divise 6, donc  $\circ(\bar{3}) \in \{1, 2, 3, 6\}$ . Mais  $\bar{3} \neq \bar{1}$ ,  $\bar{3}^2 = \bar{2} \neq \bar{1}$  et  $\bar{3}^3 = \bar{6} \neq \bar{1}$ , donc  $\circ(\bar{3}) = 6$  et, par suite,  $\bar{3}$  est un générateur de  $(\mathbb{Z}/7\mathbb{Z} \setminus \{\bar{0}\}, \times)$ .  
Puisque  $(\mathbb{Z}/7\mathbb{Z} \setminus \{\bar{0}\}, \times)$  est d'ordre 6 et  $\bar{3}$  est un de ses générateurs, alors les autres générateurs sont  $\bar{3}^k$  avec  $k \in \llbracket 1, 6 \rrbracket$  et  $k \wedge 6 = 1$ , c'est-à-dire  $\bar{3}$  et  $\bar{3}^5 = \bar{4}$

**Partie V: Le groupe  $(\mathbb{U}(\mathbb{Z}/p^2\mathbb{Z}), \times)$  lorsque  $p$  est premier**

14. On fait appel à la formule de factorisation

$$(b+p)^{p-1} - b^{p-1} = p \sum_{k=0}^{p-2} (b+p)^k b^{p-2-k}$$

Or

$$\begin{aligned} \sum_{k=0}^{p-2} (b+p)^k b^{p-2-k} &\equiv \sum_{k=0}^{p-2} (b+p)^k b^{p-2-k} \quad [p] \\ &\equiv \sum_{k=0}^{p-2} b^{p-2} \quad [p] \\ &\equiv (p-1) b^{p-2} \quad [p] \end{aligned}$$

Donc

$$(b+p)^{p-1} - b^{p-1} \equiv p(p-1)b^{p-2} \quad [p^2]$$

Si  $p^2$  divise  $(b+p)^{p-1} - b^{p-1}$ , il divise  $p(p-1)b^{p-2}$ , puis  $p$  divise  $(p-1)b^{p-2}$ . Mais  $p$  est premier avec  $p-1$  et  $b$ , ce qui est absurde

15. Si les deux sont congrus à 1 modulo  $p^2$ , alors  $p^2$  divise  $(b+p)^{p-1} - b^{p-1}$ , ce qui contredit le résultat de la question précédente
16. Il est clair que  $b+p \equiv b \quad [p]$  et  $b \equiv b \quad [p]$ , donc par disjonction des cas,  $c^{p-1} \equiv b^{p-1} \quad [p]$ .  
Par hypothèse  $b^{p-1} \equiv 1 \quad [p]$ , donc on déduit que  $c^{p-1} \equiv 1 \quad [p]$  et, par définition, il existe  $q \in \mathbb{N}$  tel que  $c^{p-1} = 1 + qp$ . L'entier  $q$  n'est pas divisible par  $p$ , car sinon  $pq \equiv 0 \quad [p^2]$  puis  $c^{p-1} \equiv 1 \quad [p^2]$ , ce qui est absurde

L'EXPOSANT D'UN GROUPE

17. D'après la formule du binôme de Newton

$$\begin{aligned} c^{p(p-1)} &= (1 + qp)^p = \sum_{i=0}^p C_p^i p^i q^i \\ &= 1 + p^2 q + \sum_{i=2}^p C_p^i p^i q^i \\ &= 1 + p^2 \left( q + \sum_{i=2}^p C_p^i p^{i-2} q^i \right) \end{aligned}$$

On a bien  $c^{p(p-1)} = 1 + kp^2$  avec  $k = q + \sum_{i=2}^p C_p^i p^{i-2} q^i$ , comme  $p \geq 3$  alors  $p$  divise  $C_p^i p^{i-2}$  pour tout  $i \in \llbracket 2, p \rrbracket$ , alors  $k \equiv q \pmod{p}$ , donc  $p$  ne divise pas  $k$ .

18. D'après la question précédente  $\bar{c}^{p(p-1)} = \bar{1}$ , donc  $\bar{c}$  appartient à  $\mathbb{U} \left( \mathbb{Z}/p^2\mathbb{Z} \right)$ .

19. (a) **Card**  $\left( \mathbb{U} \left( \mathbb{Z}/p^2\mathbb{Z} \right) \right) = \varphi(p^2) = p(p-1)$ , donc  $r$  divise  $p(p-1)$

(b) On a  $c^r \equiv 1 \pmod{p^2}$ , donc  $p^2$  divise  $c^r - 1$ , puis par transitivité  $p$  divise  $c^r - 1$ , soit  $\widehat{c}^r = \widehat{1}$ , donc  $\circ(\widehat{c}) = \circ(\widehat{b}) = p-1$  divise  $r$

(c)  $p-1$  divise  $r$ , alors il existe  $s \in \mathbb{N}$  tel que  $r = s(p-1)$ . En outre  $r$  divise  $p(p-1)$ , donc  $s$  divise  $p$ , avec  $p$  premier, il vient alors que  $s = p$  ou  $s = 1$ . Si  $s = 1$ , alors  $r = p-1$ , ceci donne  $\bar{c}^{p-1} = \bar{1}$ , ce qui absurde. En déduire que  $r = p(p-1)$ .

(d)  $\bar{c}$  est d'ordre  $p(p-1)$  et **Card**  $\left( \mathbb{U} \left( \mathbb{Z}/p^2\mathbb{Z} \right) \right) = p(p-1)$ , donc  $\bar{c}$  est un générateur de  $\left( \mathbb{U} \left( \mathbb{Z}/p^2\mathbb{Z} \right), \times \right)$ .

20. On a  $3^6 \equiv 43 \pmod{49}$ , donc  $\bar{3}$  est un générateur de  $\left( \mathbb{U} \left( \mathbb{Z}/49\mathbb{Z} \right), \times \right)$ .