

Devoir maison N°1 (correction)

Partie I : Groupe $\mathbb{U}(\mathbb{Z}/p\mathbb{Z})$.

L'objectif de cette partie est de montrer que le groupe $\mathbb{U}(\mathbb{Z}/p\mathbb{Z})$ est cyclique.

- 1. a.** Soit $P \in K[X]$, $P = \sum_{i=0}^p a_i X^i$ et $\alpha \in K$ tel que $P(\alpha) = 0$. On a :

$$P(X) = P(X) - P(\alpha) = \sum_{i=0}^p a_i X^i - \sum_{i=0}^p a_i \alpha^i = \sum_{i=1}^p a_i X^i - \sum_{i=1}^p a_i \alpha^i = \sum_{i=1}^p a_i (X^i - \alpha^i) = (X - \alpha)Q(X).$$

Donc $(X - \alpha)$ divise P .

- b.** Récurrence sur $p = \deg P \in \mathbb{N}^*$.

Initialisation : Pour $p = 1$, la propriété est vraie.

Hérédité : Supposons le résultat est vraie au rang $p - 1$ et montrons le au rang p .

Si $\alpha \in K$ est une racine de P (le cas contraire est trivial), alors $P = (X - \alpha)Q$ avec $\deg Q = p - 1$. Par hypothèse de récurrence, Q a au plus $p - 1$ racines dans K donc P a au plus p racines dans K .

Conclusion : P admet au plus $\deg P$ racines dans K .

- 2. a.** D'après le théorème d'Euler, $k^{\varphi(p)} \equiv 1 \pmod{p}$ pour tout k premier avec p . Or $\varphi(p) = p - 1$ car p premier, donc le polynôme $X^{p-1} - 1$ a au moins $p - 1$ racines dans le corps $\mathbb{Z}/p\mathbb{Z}$ puisque les entiers k pour lesquels $k \wedge p = 1$ sont $1, \dots, p - 1$. Et d'après la question précédente, $X^{p-1} - 1$ a au plus $p - 1$ racines dans le corps $\mathbb{Z}/p\mathbb{Z}$. D'où $X^{p-1} - 1$ admet exactement $p - 1$ racines dans le corps $\mathbb{Z}/p\mathbb{Z}$.

- b.** d divise $p - 1$ donc $p - 1 = md$ avec $m \in \mathbb{N}^*$. On a $X^{p-1} - 1 = (X^d)^m - 1 = (X^d - 1)R(X)$ avec R un polynôme à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ et $\deg R = md - d = p - 1 - d$.

On a $X^{p-1} - 1$ admet exactement $p - 1$ racines dans $\mathbb{Z}/p\mathbb{Z}$. Le polynôme R admet au plus $p - 1 - d$ racines dans $\mathbb{Z}/p\mathbb{Z}$ et $X^d - 1$ a au plus d racines dans $\mathbb{Z}/p\mathbb{Z}$.

Puisque les racines de $(X^d - 1)R(X)$ sont les racines de $(X^d - 1)$ ou les racines de $R(X)$, alors nécessairement R admet exactement $p - 1 - d$ racines et par suite, $X^d - 1$ admet exactement d racines dans $\mathbb{Z}/p\mathbb{Z}$.

- 3. a.** Soit $k \in \mathbb{Z}$. On a

$$(ab)^k = e \implies a^k b^k = e \implies (a^k b^k)^r = e \implies a^{kr} b^{kr} = e \implies b^{kr} = e \implies s \text{ divise } kr \xrightarrow{\text{Gauss}} s \text{ divise } k.$$

De même, on obtient r divise k et par suite, $r \vee s$ divise k . De plus, $(ab)^{r \vee s} = e$ d'où ab est d'ordre $r \vee s = rs$.

- b.** Soit $k \geq 3$ un entier fixé. Soit r_i , $1 \leq i \leq k$ l'ordre de a_i avec $r_i \wedge r_j = 1$ pour $i \neq j$. Notons $c = \prod_{i=1}^k a_i$ et $r = r_1 \vee \dots \vee r_k$. On veut montrer le résultat suivant : l'ordre de c est égal à r .

On a :

$$\begin{aligned} c^r &= a_1^r \dots a_k^r \quad \text{car } a_i a_j = a_j a_i \text{ pour tout } i \neq j \\ &= e \dots e = e \quad \text{car chaque } r_i \text{ divise } r \text{ pour } 1 \leq i \leq k \end{aligned}$$

donc c est d'ordre fini et divise r .

Soit $m \in \mathbb{Z}$ tel que $c^m = e$. Posons, pour $1 \leq i \leq k$, $r'_i = r_1 \vee \dots \vee r_{i-1} \vee r_{i+1} \vee \dots \vee r_k$. On a

$$c^m = e \implies a_1^m \dots a_k^m = e \implies (a_1^m \dots a_k^m)^{r'_i} = e \implies a_1^{mr'_i} \dots a_k^{mr'_i} = e \implies a_i^{mr'_i} = e$$

donc r_i divise mr'_i . Or les r_i sont premiers entre eux deux à deux donc $r'_i = \prod_{\substack{j=1 \\ j \neq i}}^k r_j$. Par le lemme de Gauss,

puisque $r_i \wedge r'_i = 1$, on a r_i divise m pour tout $1 \leq i \leq k$ et par suite, r divise m . D'où c est d'ordre r .

- 4. a.** On a $p_j^{\alpha_j}$ divise $p-1$ donc d'après la question 2, le polynôme $X^{p_j^{\alpha_j}} - 1$ admet exactement $p_j^{\alpha_j}$ racines dans $\mathbb{Z}/p\mathbb{Z}$ et le polynôme $X^{p_j^{\alpha_j-1}} - 1$ admet exactement $p_j^{\alpha_j-1}$ racines dans $\mathbb{Z}/p\mathbb{Z}$.
Donc il y a $p_j^{\alpha_j} - p_j^{\alpha_j-1} = p_j^{\alpha_j-1}(p_j - 1)$ racines éléments $a \in \mathbb{Z}/p\mathbb{Z}$ tels que $a^{p_j^{\alpha_j}} = 1$ et $a^{p_j^{\alpha_j-1}} \neq 1$.
Puisque $p_j - 1 \geq 1$, il existe $x_j \in \mathbb{Z}/p\mathbb{Z}$ tel que $x_j^{p_j^{\alpha_j}} = 1$ et $x_j^{p_j^{\alpha_j-1}} \neq 1$.
- b.** L'ordre de x_j divise $p_j^{\alpha_j}$ donc x_j est de la forme $p_j^{\beta_j}$ avec $\beta_j \leq \alpha_j$.
Si $\beta_j \leq \alpha_j - 1$ alors $\alpha_j - 1 = \beta_j + \delta_j$ où $\delta_j \in \mathbb{N}$ donc
- $$x_j^{p_j^{\alpha_j-1}} = x_j^{p_j^{\beta_j+\delta_j}} = x_j^{p_j^{\beta_j} p_j^{\delta_j}} = \left(x_j^{p_j^{\beta_j}}\right)^{p_j^{\delta_j}} = 1$$
- ce qui contredit $x_j^{p_j^{\alpha_j-1}} \neq 1$ et par suite, $\beta_j \geq \alpha_j$. D'où $\beta_j = \alpha_j$ et x_j est d'ordre $p_j^{\alpha_j}$.
- c.** Chaque x_j est d'ordre $p_j^{\alpha_j}$ et les $p_j^{\alpha_j}$, $1 \leq j \leq m$ sont premiers entre eux deux à deux, donc d'après la question 3, x est d'ordre $\prod_{j=1}^m p_j^{\alpha_j}$ c-à-d x est d'ordre $p-1$.
- 5.** $\mathbb{U}(\mathbb{Z}/p\mathbb{Z})$ est un groupe d'ordre $p-1$ et il existe $x \in \mathbb{U}(\mathbb{Z}/p\mathbb{Z})$ d'ordre $p-1$ d'où le groupe $\mathbb{U}(\mathbb{Z}/p\mathbb{Z})$ est cyclique engendré par x .

Partie II : Carrés modulo n .

- 6. a.** On a :

$$\begin{aligned} \bar{a} \in \mathbb{U}(\mathbb{Z}/n\mathbb{Z}) &\iff \exists u \in \mathbb{Z}, \bar{a}u = \bar{1} \\ &\iff \exists (u, v) \in \mathbb{Z}^2, au + nv = 1 \\ &\stackrel{\text{Bézout}}{\iff} a \wedge n = 1. \end{aligned}$$

- b.** Si $\overline{-1} = \bar{1}$ alors $\bar{2} = \bar{0}$ donc p divise 2 ce qui est absurde car p est premier impair. Par suite $\overline{-1} \neq \bar{1}$.
- 7. a.** Soit $\alpha, \beta \in \mathbb{U}(\mathbb{Z}/p\mathbb{Z})$. On a $\sigma(\alpha\beta) = (\alpha\beta)^2 = \alpha^2\beta^2 = \sigma(\alpha)\sigma(\beta)$ car $\mathbb{U}(\mathbb{Z}/p\mathbb{Z})$ est abélien, donc σ est un morphisme de groupes.
- b.** $\alpha \in \ker(\sigma) \iff \sigma(\alpha) = \bar{1} \iff \alpha^2 = \bar{1} \iff \alpha = \bar{1} \text{ ou } \alpha = \overline{-1}$ car $\mathbb{Z}/p\mathbb{Z}$ est un corps.
D'où $\ker \sigma = \{\overline{-1}, \bar{1}\}$.
- c.** L'application $\sigma : \mathbb{U}(\mathbb{Z}/p\mathbb{Z}) \longrightarrow \text{Im } \sigma$ est surjective. Soit $y \in \text{Im } \sigma$, il existe $x \in \mathbb{U}(\mathbb{Z}/p\mathbb{Z})$ tel que
- $$\begin{array}{ccc} \alpha & \longmapsto & \alpha^2 \\ \sigma(x) = y. & \text{On a :} & \end{array}$$
- $$x' \in \sigma^{-1}(\{y\}) \iff \sigma(x') = \sigma(x) \iff \sigma(x'x^{-1}) = \bar{1} \iff x'x^{-1} \in \ker \sigma \iff x' \in (\ker \sigma).x.$$
- c-à-d $\sigma^{-1}(\{y\}) = (\ker \sigma).x$ donc $\text{Card } \sigma^{-1}(\{y\}) = \text{Card } (\ker \sigma).x$. Or l'application $h \longmapsto h.x$ est une bijection de $\ker \sigma$ sur $(\ker \sigma).x$ donc $\text{Card } \sigma^{-1}(\{y\}) = \text{Card } \ker \sigma$. Le lemme des bergers permet alors de conclure que : $\text{Card } \mathbb{U}(\mathbb{Z}/p\mathbb{Z}) = \text{Card } \ker \sigma \times \text{Card } \text{Im } \sigma$ d'où $\text{Card } \text{Im } \sigma = \frac{p-1}{2} = p'$.
- d. i.** $\text{Card } T = \text{Card } \mathbb{U}(\mathbb{Z}/p\mathbb{Z}) - \text{Card } \text{Im } \sigma = p-1-p' = p'$.
- ii.** Soit $\theta \in T$ fixé. Soit $s \in \text{Im } \sigma$ tel que $s' = \theta s \in \text{Im } \sigma$, alors $\theta = s's^{-1} \in \text{Im } \sigma$ ce qui est absurde car $\theta \notin \text{Im } \sigma$ et par suite, $\theta s \in T$. Ainsi, $\{\theta s, s \in \text{Im } \sigma\} \subset T$.
- De plus, $\text{Card } T = p' = \text{Card } \text{Im } \sigma$. Or l'application $s \longmapsto \theta s$ est une bijection de $\text{Im } \sigma$ sur $\{\theta s, s \in \text{Im } \sigma\}$, donc $\text{Card } \text{Im } \sigma = \text{Card } \{\theta s, s \in \text{Im } \sigma\}$ c-à-d $\text{Card } T = \text{Card } \{\theta s, s \in \text{Im } \sigma\}$. D'où l'égalité $T = \{\theta s, s \in \text{Im } \sigma\}$.

e. Il est clair que l'application $\chi_p : \mathbb{U}(\mathbb{Z}/p\mathbb{Z}) \longrightarrow \{-1, 1\}$ est surjective.

Soit α, β dans $\mathbb{U}(\mathbb{Z}/p\mathbb{Z})$. On va distinguer quatre cas :

- Si $\alpha, \beta \in \text{Im } \sigma$ alors $\alpha\beta \in \text{Im } \sigma$ donc $\chi_p(\alpha\beta) = 1 = \chi_p(\alpha)\chi_p(\beta) = 1 \times 1 = 1$.
- Si $\alpha, \beta \in T$ alors $\alpha = \theta s$ et $\beta = \theta s'$ avec $\theta \in T$ fixé et $s, s' \in \text{Im } \sigma$ donc $\alpha\beta = \theta^2 ss' \in \text{Im } \sigma$ et on a

$$\chi_p(\alpha\beta) = 1 = -1 \times -1 = \chi_p(\alpha)\chi_p(\beta).$$

- Si $\alpha \in \text{Im } \sigma$ et $\beta \in T$ alors $\alpha\beta = \delta \in T$ car sinon $\beta = \alpha^{-1}\delta \in \text{Im } \sigma$ ce qui est absurde et par suite,

$$\chi_p(\alpha\beta) = -1 = 1 \times -1 = \chi_p(\alpha)\chi_p(\beta).$$

- Si $\alpha \in T$ et $\beta \in \text{Im } \sigma$ (de même!).

D'où : pour tous α, β dans $\mathbb{U}(\mathbb{Z}/p\mathbb{Z})$, $\chi_p(\alpha\beta) = \chi_p(\alpha)\chi_p(\beta)$.

f. Soit $f : \mathbb{U}(\mathbb{Z}/p\mathbb{Z}) \longrightarrow \{-1, 1\}$ un morphisme de groupes surjectif.

- Si $\alpha \in \text{Im } \sigma$, il existe $\beta \in \mathbb{U}(\mathbb{Z}/p\mathbb{Z})$ tel que $\alpha = \beta^2$ donc $f(\alpha) = (f(\beta))^2 = 1$.
- Si $\alpha \in T$, alors comme f est surjectif, il existe $\theta \in \mathbb{U}(\mathbb{Z}/p\mathbb{Z})$ tel que $f(\theta) = -1$ donc $\theta \in T$ car sinon $f(\theta) = 1$ ce qui contredit le cas précédent et par suite, $\alpha = \theta s$ avec $s \in \text{Im } \sigma$. On a alors $f(\alpha) = f(\theta s) = f(\theta)f(s) = -1 \times 1 = -1$.

$$\text{Ainsi, } f(\alpha) = \begin{cases} 1 & \text{si } \alpha \in \text{Im } (\sigma) \\ -1 & \text{si } \alpha \in T \end{cases} \quad \text{d'où } f = \chi_p.$$

8. Soit $a \in \mathbb{Z}$ tel que $1 \leq a \leq 10$.

$\bar{a}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6} = \overline{-5}$	$\bar{7} = \overline{-4}$	$\bar{8} = \overline{-3}$	$\bar{9} = \overline{-2}$	$\bar{10} = \overline{-1}$
$\bar{a}^2$	$\bar{1}$	$\bar{4}$	$\bar{9}$	$\bar{5}$	$\bar{3}$	$\bar{3}$	$\bar{5}$	$\bar{9}$	$\bar{4}$	$\bar{1}$
$\left(\frac{a}{p}\right)$	1	-1	1	1	1	-1	-1	-1	1	-1

Partie III : Symbole de Legendre.

9. Le groupe $\mathbb{U}(\mathbb{Z}/p\mathbb{Z})$ est d'ordre $p-1$ donc d'après le cours, $\alpha^{p-1} = \bar{1}$ c-à-d $\alpha^{2p'} = \bar{1}$ donc $\alpha^{p'} \in \ker \sigma = \{\bar{-1}, \bar{1}\}$ d'où $\alpha^{p'} = \bar{1}$ ou $\bar{-1}$.

10. a. L'application $\psi : \mathbb{U}(\mathbb{Z}/p\mathbb{Z}) \longrightarrow \{\bar{-1}, \bar{1}\}$ est un morphisme de groupes (clair) et les groupes $\{\bar{-1}, \bar{1}\}$

$$\alpha \longmapsto \alpha^{p'}$$

et $\{-1, 1\}$ sont isomorphes, donc φ est un morphisme de groupes comme composée de deux morphismes de groupes.

Montrons que φ est surjectif. Soit $y \in \{-1, 1\}$.

- Si $y = 1$, on a $\varphi(\bar{1}) = 1$ puisque $\bar{1}^{p'} = \bar{1}$.
- Supposons $y = -1$. Si pour tout $\alpha \in \mathbb{U}(\mathbb{Z}/p\mathbb{Z})$ on a $\alpha^{p'} = \bar{1}$ alors le polynôme $X^{p'} - 1$ possède $p-1 = 2p'$ racines dans $\mathbb{U}(\mathbb{Z}/p\mathbb{Z})$ ce qui est absurde car le polynôme $X^{p'} - 1$ admet exactement p' racines dans $\mathbb{U}(\mathbb{Z}/p\mathbb{Z})$. Donc il existe $\alpha \in \mathbb{U}(\mathbb{Z}/p\mathbb{Z})$ tel que $\alpha^{p'} = \bar{-1}$ et $\varphi(\alpha) = -1$. D'où φ est surjectif.

b. φ est surjectif, par unicité (question 7), On a $\varphi = \chi_p$. Par suite, $\forall \bar{a} \in \mathbb{U}(\mathbb{Z}/p\mathbb{Z})$, $\varphi(\bar{a}) = \chi_p(\bar{a}) = \left(\frac{a}{p}\right)$.

- Si $\bar{a}^{p'} = \bar{1}$, alors $1 = \chi_p(\bar{a}) = \left(\frac{a}{p}\right)$.
- Si $\bar{a}^{p'} = \bar{-1}$, alors $-1 = \chi_p(\bar{a}) = \left(\frac{a}{p}\right)$.

Dans tous les cas, $a^{p'} \equiv \left(\frac{a}{p}\right) \pmod{p}$.

11. D'après la question précédente,

$$\begin{aligned}\left(\frac{-1}{p}\right) = 1 &\iff (-1)^{p'} \equiv 1 \pmod{p} \\ &\iff p' \equiv 0 \pmod{2} \\ &\iff p \equiv 1 \pmod{4}.\end{aligned}$$

et

$$\begin{aligned}\left(\frac{-1}{p}\right) = -1 &\iff (-1)^{p'} \equiv -1 \pmod{p} \\ &\iff p' \equiv 1 \pmod{2} \\ &\iff p \equiv 3 \pmod{4}.\end{aligned}$$

D'après : Agrégation interne 2000 (extrait).