L'isomorphisme chinois est en particulier un isomorphisme de groupes additifs. Comme le groupe des inversibles de l'anneau produit $A \times B$ est le groupe produit $A^\times \times B^\times$. On en déduit aussi :

COROLLAIRE 3.11. *Soient $m, n \in \mathbb{Z}$ premiers entre eux. L'isomorphisme chinois induit des isomorphismes de groupes $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ et $(\mathbb{Z}/mn\mathbb{Z})^\times \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. En particulier, on a $\varphi(mn) = \varphi(m)\varphi(n)$.*

4. Le théorème de Lagrange

Si A et B sont des parties d'un groupe G, on pose

$$AB = \{ab \mid a \in A,\, b \in B\} \subset G.$$

L'application $(A, B) \mapsto AB$ définit une loi de composition sur $\mathrm{P}(G)$, nous la noterons aussi $\bullet$. Elle est associative par associativité de la loi de G : on a $(AB)C = A(BC)$ pour tout $A, B, C \subset G$. Si $A_1, \ldots, A_n$ sont des $n \geq 1$ parties de G on a alors

$$A_1 A_2 \cdots A_n = \{a_1 a_2 \ldots a_n | a_i \in A_i \ \forall i = 1, \ldots, n\}.$$

Si $A = \{a\}$ est un singleton, on note aussi aB pour $\{a\}B$. La loi $\bullet$ sur $\mathrm{P}(G)$ admet manifestement pour élément neutre $\{1\}$, donc $(\mathrm{P}(G), \bullet)$ est un monoïde ! En revanche, ce n'est pas un groupe : pour $A \subset G$ on a $GA = AG = G$ si $A \neq \emptyset$, et $\emptyset A = A\emptyset = \emptyset$. Pour $A \subset G$, on pose néanmoins $A^{-1} = \{a^{-1} \mid a \in A\}$. On prendra garde qu'en général A^{-1} n'est pas un inverse de A pour $\bullet$ (*i.e.* $AA^{-1} \neq \{1\}$), contrairement aux conventions usuelles. On a en revanche les égalités $(AB)^{-1} = B^{-1}A^{-1}$ et $(A^{-1})^{-1} = A$.

LEMME 4.1. *Une partie H d'un groupe G un sous-groupe si, et seulement si, on a $H \neq \emptyset$, $HH = H$ et $H^{-1} = H$.*

DÉMONSTRATION — Supposons que H est un sous-groupe de G. On a $1 \in H$, donc $H \neq \emptyset$. On a $HH \subset H$, et aussi $H \subset HH$ en écrivant $h = 1\,h$, d'où $HH = H$. On a enfin $H^{-1} \subset H$, puis $H = (H^{-1})^{-1} \subset H^{-1}$, et donc $H = H^{-1}$. Réciproquement, un H comme dans l'énoncé est un sous-groupe : il ne manque que $1 \in H$, mais l'existence d'un élément $h_0 \in H$ entraîne bien $1 = h_0 h_0^{-1} \in HH^{-1} = HH = H$. □

DÉFINITION 4.2. *Soient G un groupe et H un sous-groupe. Une* classe à gauche *(resp.* à droite*) de H dans G est une partie de la forme gH (resp. Hg) pour un certain $g \in H$.*

L'involution $x \mapsto x^{-1}$ de G échange gH et Hg^{-1}, et induit une involution naturelle entre classes à gauche et classes à droite. Pour fixer les idées on se focalise sur les classes à gauche. On définit une relation $\sim_H$ sur G en posant

$$g \sim_H g' \ \Leftrightarrow\ \exists h \in H,\ g' = gh \ \Leftrightarrow\ g' \in gH.$$

C'est une relation déquivalence sur G : on a $g = g1$ avec $1 \in H$, $g' = gh$ avec $h \in H$ implique $g = g'h^{-1}$ avec $h^{-1} \in H$, et enfin $g' = gh$ et $g'' = g'h'$ avec $h, h' \in H$ entraîne $g'' = ghh'$ avec $hh' \in H$. Par définition, la classe d'équivalence de $g \in G$ pour $\sim_H$ est gH. Ainsi, les classes à gauche forment une partition de G (et deux classes à gauches sont soit disjointes, soit égales).

DÉFINITION 4.3. *On note G/H l'ensemble quotient de $\sim_H$. Autrement dit, G/H est le sous-ensemble de* $\mathrm{P}(G)$ *constitué des classes à gauche de H dans G. On appelle* indice *de H dans G le cardinal (fini ou infini) de G/H, et on le note $[G : H]$*

REMARQUE 4.4. On a une histoire parallèlle pour la relation d'équivalence $g \simeq_H g' \Leftrightarrow g' \in Hg$ ($\Leftrightarrow g^{-1} \sim_H (g')^{-1}$). On note $H\backslash G$ l'ensemble quotient de $\simeq_H$, constitué des classes à droite de H dans G, et on peut définir un indice à droite $[H : G] = |H\backslash G|$. Mais cet indice coïncide avec $[G : H]$ à cause de la bijection $A \mapsto A^{-1}$ entre classes à droite et classes à gauche.

THÉORÈME 4.5. *(Lagrange) Si H est un sous-groupe de G, on a une bijection ensembliste $G \sim H \times (G/H)$. En particulier, si deux des trois ensembles G, H et G/H sont finis, il en va de même du troisième, et on a l'égalité $|G| = |H|[G : H]$.*

DÉMONSTRATION — En effet, on sait que G est réunion disjointe de classes à gauches, et que l'ensemble de ces dernières est en bijection avec G/H. La dernière chose à observer, spécifique à la relation $\sim_H$, et que deux classes à gauche quelconques sont en bijection. En effet, la multiplication à gauche par $g \in G$ induit une bijection $H \to gH, h \mapsto gh$, de bijection réciproque la multiplication à gauche par g^{-1}. On en déduit l'énoncé. [6] □

On appelle aussi « Théorèmes de Lagrange » les corollaires suivants.

COROLLAIRE 4.6. *Si H est un sous-groupe du groupe G, alors $|H|$ divise $|G|$.*

COROLLAIRE 4.7. *Si G est un groupe fini, et si $g \in G$, alors $g^{|G|} = 1$.*

Le premier corollaire est immédiat, et le second s'en déduit car l'ordre d de g satisfait $d = |\langle g \rangle|$ (Proposition 3.2). Par exemple, appliqué au groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ avec p premier, il montre $n^{p-1} \equiv 1 \bmod p$ pour tout $n \in \mathbb{Z}$ premier à p, puis $n^p \equiv n \bmod p$ pour tout $n \in \mathbb{Z}$ (*petit théorème de Fermat*).

COROLLAIRE 4.8. *Tout groupe d'ordre premier p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.*

DÉMONSTRATION — Soient G d'ordre premier p et $g \in G - \{1\}$. L'ordre de g est > 1 et divise $|G| = p$, c'est donc p et on a $\langle g \rangle = G$. On conclut par le Corollaire 3.4. □

Une question réciproque naturelle est la suivante « si n divise $|G|$ alors est-ce que G possède un sous-groupe d'ordre n ? » Nous verrons par la suite que la réponse est négative en général, le plus petit contre-exemple ayant lieu dans le groupe alterné A_4, mais affirmative quand G est abélien (Gauss) ou quand n est une puissance

6. Donnons une seconde rédaction, équivalente mais plus pédestre. Choisissons $\{g_i\}_{i \in I}$ un système de représentants des classes à gauche de H dans G. Comme G est réunion disjointe de ses classes déquivalence pour $\sim_H$ on a $G = \coprod_{i \in I} g_i H$ et $I \sim G/H$. L'application $I \times H \to G, (i, h) \mapsto g_i h$ est alors bijective. En effet, elle est par définition surjective. Elle est aussi injective : si on a $g_i h = g_j h'$ avec $i, j \in I$ et $h, h' \in H$, on a $g_i H = g_j H$, donc $i = j$ par définition d'un système de représentants, puis $g_i h = g_i h'$, et donc $h = h'$.

d'un nombre premier (Sylow). Nous nous contenterons ici du cas particulier où n est premier, dû à Cauchy. [7]

THÉORÈME 4.9. *(Cauchy) Soient G un groupe fini et p un nombre premier divisant $|G|$. Alors G possède un élément d'ordre p.*

DÉMONSTRATION — Notons n_p le nombre d'éléments d'ordre p de G. On va montrer $n_p \equiv -1 \bmod p$, et en particulier $n_p \geq p-1 > 0$.

Le cas $p = 2$ est particulièrement simple. Pour $g \in G$ on a $g = g^{-1} \Leftrightarrow g^2 = 1 \Leftrightarrow g = 1$ ou g est d'ordre 2. Ainsi, si f désigne l'aplication $G \to G, g \mapsto g^{-1}$, alors f est une involution possédant $1 + n_2$ points fixes. On a donc $|G| \equiv 1 + n_2 \bmod 2$ par le Corollaire 1.9 Chap. 1, et on conclut car $|G|$ est pair.

Suivant J. Mc Kay, cette démonstration se généralise à tout p de la manière suivante. Soit $X = \{(g_1, g_2, \ldots, g_p) \in G^p \mid g_1 g_2 \cdots g_p = 1\}$. Notons que si on a $g_1 g_2 \cdots g_p = 1$, on a aussi $g_p g_1 g_2 \cdots g_{p-1} = 1$ en multipliant à gauche par g_p et à droite par g_p^{-1}. Autrement dit, la permutation circulaire $f : G^p \to G^p$, définie par $f(g_1, g_2, \ldots, g_p) = (g_p, g_1, g_2, \ldots, g_{p-1})$, préserve X, et vérifie $f^p = \mathrm{id}$. Les points fixes de f dans X sont les éléments $(g, g, \cdots, g)$ avec $g \in G$ et $g^p = 1$, donc il y en a $1 + n_p$. On a enfin $|X| = |G|^{p-1}$ car pour définir un élément de X il suffit de choisir arbitrairement $g_1, ..., g_{p-1}$ et de définir g_p comme l'inverse de $g_1 g_2 \cdots g_{p-1}$. On conclut par $|X| = |G|^{p-1} \equiv 0 \bmod p$ et $|X| \equiv 1 + n_p \bmod p$ (Corollaire 1.9 Chap. 1). □

5. Sous-groupes finis de $k^\times$ et $(\mathbb{Z}/n\mathbb{Z})^\times$

Le résultat principal de cette partie est le suivant :

THÉORÈME 5.1. *Si k est un corps, tout sous-groupe fini de $k^\times$ est cyclique.*

Un cas particulier facile est le cas $k = \mathbb{C}$. En effet, un exemple de sous-groupe fini de $\mathbb{C}^\times$ est le sous-groupe μ_n, qui est bien cyclique engendré par $e^{\frac{2i\pi}{n}}$. Réciproquement, par Lagrange, tout sous-groupe d'ordre n est inclus dans μ_n, donc égal à μ_n (et donc cyclique) pour des raisons de cardinal. Comme nous le verrons, le théorème est non trivial en revanche pour k général, notamment pour k est fini.

REMARQUE 5.2. Pour tout corps k et tout entier $n \geq 1$, l'ensemble

$$\mu_n(k) = \{x \in k^\times, x^n = 1\}$$

est un sous-groupe de $k^\times$. C'est aussi l'ensemble des racines dans k du polynôme $X^n - 1 \in k[X]$, on a donc $|\mu_n(k)| \leq n$. L'inégalité est stricte en général : par exemple on a $\mu_n(\mathbb{R}) = \{1\}$ pour n impair. Le théorème montre que $\mu_n(k)$ est toujours cyclique (et d'ordre d divisant n).

Montrons d'abord le lemme suivant :

7. Augustin-Louis Cauchy, *Mémoire sur les arrangements que l'on peut former avec des lettres données* (et sur les permutations ou substitutions à l'aide desquelles on passe d'un arrangement à un autre) (1845), œuvres complètes, série 2 tome 13 , https://gallica.bnf.fr/ark:/12148/bpt6k902053/f175.

LEMME 5.3. (Cauchy) *Soient G un groupe et $x, y \in G$ deux éléments qui commutent, d'ordres finis a et b. Si $(a, b) = 1$ alors xy est d'ordre ab.*

DÉMONSTRATION — Considérons $M = \langle x\rangle \cap \langle y\rangle$. C'est un sous-groupe de $\langle x\rangle$ et de $\langle y\rangle$. D'après Lagrange, $|M|$ divise $a = |\langle x\rangle|$ et $b = |\langle y\rangle|$ et donc $M = \{1\}$. (On peut d'ailleurs se passer de Lagrange ici en disant simplement que l'on a $m^a = m^b = 1$, et donc $m = 1$, pour tout m dans M.) Vérifions maintenant que xy est d'ordre ab. Soit $k \in \mathbb{Z}$. Comme $xy = yx$, on a $(xy)^k = x^k y^k$. En particulier, $(xy)^{ab} = 1$. Réciproquement, si $(xy)^k = 1$ alors $x^k = y^{-k} \in M = \{1\}$, et donc $x^k = y^{-k} = 1$. Ainsi, $a|k$ et $b|k$ puis $ab|k$ car $(a, b) = 1$. □

REMARQUE 5.4. Si on ne suppose plus que x et y commutent, alors xy peut être d'ordre quelconque, et ce même si G est fini : voir l'Exercice 2.20.

DÉMONSTRATION — (du Théorème) Soient k un corps et $G \subset k^\times$ un sous-groupe fini. Posons $n = |G|$. Il suffit de démontrer que, si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ est la décomposition en facteurs premiers de n, alors G possède un élément g_i d'ordre $p_i^{\alpha_i}$ pour tout i. En effet, le lemme ci-dessus assurera alors que l'élément $g_1 g_2 \cdots g_r$ est d'ordre n.

Considérons le polynôme $P = X^n - 1 \in k[X]$. Comme k est un corps, P admet au plus n racines dans k. D'autre part, le théorème de Lagrange assure que les n éléments de G sont racines de P : il est donc scindé à racines distinctes, égales aux éléments de G. On a montré l'égalité dans $k[X]$

$$X^{|G|} - 1 = \prod_{g \in G} (X - g). \tag{7}$$

Remarquons que si d est un diviseur de n, alors $X^d - 1$ divise $X^n - 1$ dans $k[X]$, le quotient étant $\sum_{i=0}^{n/d-1} X^{id}$. En particulier, $X^d - 1$ est aussi scindé à racines distinctes dans G. Pour tout i, il existe donc au moins une racine g_i de $X^{p_i^{\alpha_i}} - 1$ dans G qui n'est pas racine de $X^{p_i^{\alpha_i - 1}} - 1$. Un tel élément est donc d'ordre $p_i^{\alpha_i}$, ce qui conclut la démonstration. □

Le théorème suivant est démontré par Gauss quand $k = \mathbb{F}_p$ dans ses *Disquisitones Arithmeticae*.

COROLLAIRE 5.5. *(Gauss) Pour p premier, le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.*

Par exemple, les puissances successives de 2 modulo 11 sont (les classes de)

$$2, 4, 8, 5, 10, 9, 7, 3, 6, 1$$

et donc 2 est un générateur de $(\mathbb{Z}/11\mathbb{Z})^\times$. En revanche, ce n'est pas le cas de $5 \equiv 2^4$, qui est d'ordre $10/(10, 4) = 5$. Un entier a dont la classe dans $\mathbb{Z}/p\mathbb{Z}$ engendre $(\mathbb{Z}/p\mathbb{Z})^\times$ est appelé une *racine primitive modulo p*. Le théorème de Gauss assure l'existence de racines primitives modulo tout nombre premier p, mais de nombreuses questions persistent quant à leur construction. Par exemple, E. Artin a conjecturé que « *tout entier $a \neq -1$ qui n'est pas un carré est une racine primitive modulo p*

pour une infinité de nombres premiers p » . On ne connaît aucun entier a pour lequel cette conjecture est vraie ! [8]

REMARQUE 5.6. *Un isomorphisme de groupes* $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ *(il en existe par le corollaire) s'appelle un logarithme discret, par analogie avec l'isomorphisme* $\log : (\mathbb{R}_{>0}, \times) \xrightarrow{\sim} (\mathbb{R}, +)$.

Une première conséquence classique du théorème de Gauss concerne l'étude des puissances n-èmes dans $(\mathbb{Z}/p\mathbb{Z})^\times$. Pour $n \in \mathbb{Z}$, posons

$$(\mathbb{Z}/p\mathbb{Z})^{\times,(n)} = \{x^n \mid x \in (\mathbb{Z}/p\mathbb{Z})^\times\}$$

l'ensemble des puissances n-èmes. C'est manifestement un sous-groupe de $(\mathbb{Z}/p\mathbb{Z})^\times$, à savoir l'image du morphisme de groupes $(\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times, x \mapsto x^n$. Comme $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p-1$, le Lemme 3.7 montre :

COROLLAIRE 5.7. *Soient p premier,* $n \geq 1$ *un entier et* $m = (p-1, n)$.

(i) Le groupe $(\mathbb{Z}/p\mathbb{Z})^{\times,(n)}$ *est cyclique d'ordre* $\frac{p-1}{m}$*, et égal à* $(\mathbb{Z}/p\mathbb{Z})^{\times,(m)}$.

(ii) pour $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ *on a* $x \in (\mathbb{Z}/p\mathbb{Z})^{\times,(n)}$ *si, et seulement si,* $x^{\frac{p-1}{m}} = 1$.

Pour le (ii) on peut aussi dire que le polynôme $X^{\frac{p-1}{m}} - 1$ a au plus $\frac{p-1}{m}$ racines dans $\mathbb{Z}/p\mathbb{Z}$, et donc ses racines sont exactement les puissances n-èmes, par le (i).

EXEMPLE 5.8. (*Carrés*) Le groupe $(\mathbb{Z}/p\mathbb{Z})^{\times,(2)}$ est le groupe des *carrés* de $(\mathbb{Z}/p\mathbb{Z})^\times$. Pour $p > 2$, il est d'ordre $\frac{p-1}{2}$ d'après le corollaire ci-dessus (i). On a aussi

$$(\mathbb{Z}/p\mathbb{Z})^{\times,(2)} = \{\bar{i}^2 \mid 1 \leq i \leq \frac{p-1}{2}\},$$

car $(-i)^2 = i^2$, et donc tous les éléments de l'ensemble de droite sont distincts. Une application classique du (ii), due à Euler, est que -1 *est un carré modulo p si et seulement si* $p = 2$ *ou* $(-1)^{\frac{p-1}{2}} \equiv 1 \bmod p$*, i.e.* $p \equiv 1 \bmod 4$.

Décrivons enfin la structure de $(\mathbb{Z}/n\mathbb{Z})^\times$ pour $n \geq 1$ quelconque. D'après l'isomorphisme chinois (Corollaire 3.11) il suffit de traiter le cas où n est une puissance d'un nombre premier.

COROLLAIRE 5.9. *(i) Si p est premier impair, et* $m \geq 1$*, alors le groupe* $(\mathbb{Z}/p^m\mathbb{Z})^\times$ *est cyclique.*

(ii) Si $m \geq 2$ *on a* $(\mathbb{Z}/2^m\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}$.

Avant de montrer ce corollaire, commençons par établir une congruence utile.

LEMME 5.10. *Soit* $k \geq 0$ *un entier.*

(i) Si p est un nombre premier impair, alors $(1+p)^{p^k} \equiv 1 + p^{k+1} \bmod p^{k+2}$.

(ii) De plus, on a $(1+4)^{2^k} \equiv 1 + 2^{k+2} \bmod 2^{k+3}$.

DÉMONSTRATION — Si p est un nombre premier, on rappelle la congruence $\binom{p}{i} \equiv 0 \bmod p$ si $i = 1, \ldots, p-1$. On en déduit que pour $k \geq 1$, $a \equiv b \bmod p^k$ entraîne $a^p \equiv b^p \bmod p^{k+1}$, puis (i) et (ii), par récurrence sur k. □

8. En revanche, un théorème de Heath-Brown montre qu'il y a au plus 2 nombres premiers qui ne satisfont pas cette conjecture : D. R. Heath-Brown, « Artin's conjecture for primitive roots », Quart. J. Math. Oxford vol. 37 (1986), 27-38.