Sandrine CARUSO

Le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique

Référence : Francinou-Gianella-Nicolas, Oraux X-ENS, algèbre 1

Théorème. *Le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.*

Ce groupe est de cardinal $p-1$, il suffit donc de montrer qu'il a un élément d'ordre $p-1$. Tout d'abord, montrons que si q est un nombre premier et $\alpha > 0$ un entier tels que q^α divise $p-1$, alors $(\mathbb{Z}/p\mathbb{Z})^\times$ admet un élément d'ordre q^α.

Pour cela, on note, pour $x \in (\mathbb{Z}/p\mathbb{Z})^\times$, $y_x = x^{\frac{p-1}{q^\alpha}}$. D'après le petit théorème de Fermat, $y_x^{q^\alpha} = 1$, donc l'ordre de y_x est de la forme q^{r_x} avec $r_x \leqslant \alpha$. Soit $r = \max\{r_x, x \in (\mathbb{Z}/p\mathbb{Z})^\times\}$. Montrons que $r = \alpha$.

Pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^\times$, $y_x^{q^r} = 1$ c'est-à-dire $x^{\frac{p-1}{q^{\alpha-r}}} = 1$. Ainsi, tout élément de $(\mathbb{Z}/p\mathbb{Z})^\times$ est racine du polynôme $X^{\frac{p-1}{q^{\alpha-r}}} - 1$, qui a donc au moins $p-1$ racines distinctes dans le corps $\mathbb{Z}/p\mathbb{Z}$. Par conséquent, il est de degré au moins $p-1$, ce qui assure que $r = \alpha$. Donc $(\mathbb{Z}/p\mathbb{Z})^\times$ admet au moins un élément d'ordre q^α.

Maintenant, pour conclure, nous allons utiliser le lemme suivant.

Lemme. *Soit G un groupe abélien. On suppose que G admet un élément x d'ordre p et un élément y d'ordre q tels que p et q sont premiers entre eux. Alors xy est d'ordre pq.*

Démonstration. Soit k l'ordre de xy. Déjà, on a $(xy)^{pq} = (x^p)^q (y^q)^p = 1$, ce qui assure que k divise pq.

Ensuite, comme $(xy)^k = 1$, on a aussi $1 = (xy)^{qk} = x^{qk}$, et puisque x est d'ordre p, p divise qk. Or, p et q sont premiers entre eux donc p divise k. De même, q divise k. Le fait que p et q soient premiers entre eux implique alors encore que pq divise k.

Finalement, $k = pq$. □

En décomposant $p-1 = q_1^{\alpha_1} \cdots q_r^{\alpha_r}$ en facteurs premiers, on montre par récurrence que $(\mathbb{Z}/p\mathbb{Z})^\times$ admet un élément d'ordre $p-1$.

Application. *Soit p un nombre premier. Si $p \equiv 1 \pmod 4$, alors -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.*

Soit a un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$. L'hypothèse revient à dire que $\frac{p-1}{4}$ est entier. Soit alors $b = a^{\frac{p-1}{4}}$. Puisque a est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$, $a^{p-1} = 1$ mais $a^{\frac{p-1}{2}} \neq 1$, c'est-à-dire $b^4 = 1$ mais $b^2 \neq 1$: b^2 est une racine carrée de 1 qui n'est pas 1, donc $b^2 = -1$.

Remarque. Réciproquement, si -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$, alors $p = 2$ ou $p \equiv 1 \pmod 4$ (notons que si $p = 2$, -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$). En effet, si $p \neq 2$ et si $-1 = b^2$ dans $\mathbb{Z}/p\mathbb{Z}$, alors $(-1)^{\frac{p-1}{2}} = b^{p-1} = 1$, et donc $\frac{p-1}{2}$ est pair.