Corentin Bergeron ENS Rennes

Condition de cyclicité de $(Z/nZ)^\times$

Développement classique qui donne une condition nécéssaire et sufisante sur n pour que $(\mathbb{Z}/n\mathbb{Z})^\times$ soit cyclique. On sépare les cas p impair, le cas 2 et le cas général fait par théorème chinois.

Ce développment se recase très bien dans les leçons 104 (on utilise beaucoup les groupes finis), 108 (on donne une condition de cyclicité, ce qui renseigne sur la structure des générateurs), 120 et 121 (pour les lemmes et la décomposition en premier).

I - Le développement

Étape 1 : Cas $p > 2$

Lemme 1

Si $k \in \mathbb{N}$, $\exists \lambda_k \in \mathbb{N}^*$, $\lambda_k \wedge p = 1$ tel que

$$(1+p)^{p^k} = 1 + \lambda_k p^{k+1}.$$

Preuve :

On raisonne par récurrence sur k : $\star\star$

— $k = 0$: $\lambda_0 = 1$ convient.

— Si vrai au rang $k \in \mathbb{N}$

$$(1+p)^{p^{k+1}} = \left(1+\lambda_k p^{k+1}\right)^p = \sum_{i=0}^{p} \binom{p}{i} \left(\lambda_k p^{k+1}\right)^i = 1 + p^{k+2}\lambda_k + p^{k+2} \sum_{i=2}^{p} \binom{p}{i} p^{k(i-1)+i-2}$$

Pour $i \in [\![3, p]\!]$, comme $p \geqslant 3$, $p \mid p^{k(i-1)+i-2}$. Pour $i = 2$, on a $p \mid \binom{p}{2}$.

Ainsi

$$\lambda_{k+1} := \lambda_k + \sum_{i=2}^{p} \binom{p}{i} p^{k(i-1)+i-2}$$

est premier avec p.

Par le lemme, $(1+p)^{p^{\alpha-1}} = 1+\lambda_{\alpha-1}p^\alpha \equiv 1\,[p^\alpha]$ et $(1+p)^{p^{\alpha-2}} = 1+\lambda_{\alpha-2}p^{\alpha-1} \not\equiv 1\,[p^\alpha]$ (car $\lambda_{\alpha-1}\wedge$).$On en déduit que 1+p est un$ d'ordre $p^{\alpha-1}$.

Considérons l'application :

$$\begin{array}{rccc} \widetilde{\Psi} : & (\mathbb{Z}/p^\alpha\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^\times \\ & [x]_{p^\alpha} & \longmapsto & [x]_p \end{array}$$

induite par

$$\begin{array}{rccc} \Psi : & \mathbb{Z} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ & x & \longmapsto & [x]_p \end{array}$$

$\widetilde{\Psi}$ est bien définie et surjectif car $[x]_p$ inversible si et seulement si $x \wedge p = 1$ si et seulement si $[x]_{p^\alpha}$ est inversible.

Soit $x \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ tel que $\widetilde{\Psi}(x)$ engendre $(\mathbb{Z}/p\mathbb{Z})^\times$. On a alors :

$\widetilde{\Psi}(x)^{o(x)} = 1$ et par conséquent

$$p - 1 \mid o(x).$$

On possède donc un élément y d'ordre $p-1$ dans $\langle x \rangle$. Par commutativité,

$$o\big((1+p)y\big) = (p-1) \times p^{\alpha-1} = \varphi(p^\alpha).$$

Le groupe $\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est donc cyclique.

Étape 2 : Cas $p = 2$

On a de manière connue :

⋆ $(\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$.

⋆ $(\mathbb{Z}/4\mathbb{Z})^\times = \{-1, 1\} \simeq \mathbb{Z}/2\mathbb{Z}$

Passons donc au cas $\alpha \geq 3$.

Lemme 2

Si $k \in \mathbb{N}^*$, $\exists \lambda_k$ impair tel que

$$5^{2^k} = 1 + \lambda_k 2^{k+2}.$$

On considère l'application :

$$\widetilde{Phi} : (\mathbb{Z}/2^\alpha\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times,$$

obtenue de manière similaire que dans l'étape 2.

On a $|\ker(\widetilde{Phi})| = 2^{\alpha-2}$ et $5 \in \ker(\widetilde{Phi})$ est d'ordre $2^{\alpha-2}$ (comme pour (1+p) à l'étape 2), $donc \ker(\widetilde{Phi})$ est cyclique, engendré par 5.

En posant $H = \langle -1 \rangle$, $N = \ker(\hat{\varphi})$, on a $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times = HN$ (pour un raison de cardinalité) et $H \cap N = \{1\}$, d'où par critère de dévissage,

$$(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq H \times N.$$

Étape 3 : Cas général

On écrit $n = 2^\alpha p_1^{\alpha_1} \times \cdots \times p_r^{\alpha_r}$ avec $p_1, \ldots, p_r$ des premiers impairs 2 à 2 distincts et $\alpha, \alpha_1, \ldots, \alpha_r \geqslant 0$.
Par le théorème des restes chinois :

$$(\mathbb{Z}/m\mathbb{Z})^\times \simeq \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times \times (\mathbb{Z}/2^\alpha\mathbb{Z})^\times.$$

Or, puisqu'on travaille avec des groupes commutatifs, on a :

II - Remarques

1 - Attention pour les candidats un peu lent, ce développement peut être assez long, donc n'hésitez pas à racourcir certains arguments, quitte à avoir des questions après.

2 - Durant la présentation, je ne démontre pas le lemme pour le cas $p = 2$, puisqu'il est quasiment identique au premier. Attention cependant, il est essentiel de démontrer au moins l'un des deux lemmes (le premier est vraiement le meilleur à démontrer), car c'est là qu'est l'essence de la preuve.

3 - Pour l'étape 3, j'ai utilisé les propriétés de base de l'exposant dans le cas des groupes abéliens. Ce n'est pas forcément à connaître et on peut s'en tirer sans en parler (en faisant par l'absurde par exemple pour les cas ou les cardianux ne sont pas premiers entre eux, tec...), mais cela complique un peu les explications à mon goût. Les équivalences sont peut-être aussi un peu rapide, il faut juste bien se convaincre et au pire, le jury demandera plus d'explications.

4 - La justification de la bonne définition et de la surjectivité de $\widetilde{\Psi}$ n'est pas si immédiate que ça (on peut vite décrire un passage au quotient qui n'assure en rien la surjectivité), il faut donc bien avoir en tête l'argument (certes simple) de $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ ssi $x \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.

5 - Un exemple d'intérêt de savoir si $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique est son utilisation pour savoir si un polynôme cyclotomique est irréductible sur un corps fini. En effet, si $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique, alors Φ_n est réductible sur $\mathbb{F}_q$ (la réciproque est fausse, il faut que n et q soit premiers entre eux)

III - Références

[Per] : *Cours d'algèbre*, Daniel Perrin