Premier développement : Détermination des groupes d'ordre pq, $p < q$ premiers.

Référence : Perrin p27-28.

Nous noterons :

- $|G|$ le cardinal d'un groupe G.
- $\#\{E\}$ le cardinal de l'ensemble E.
- $Ord(x)$ l'ordre de l'élément $x \in G$.
- ϕ l'indicatrice d'Euler qui a un entier n associe le nombre d'entiers premier avec n qui le précèdent.
- $Aut(G)$ l'ensemble des automorphismes du groupe G dans lui-même.

Démontrons tout d'abord un résultat qui nous sera nécessaire par la suite :

Théorème :
$q = p^n$, *p premier,* $n \in \mathbb{N}$.
Le groupe multiplicatif $\mathbb{F}_q^*$ *est un groupe cyclique, donc isomorphe à* $\mathbb{Z}/(q-1)\mathbb{Z}$.

Preuve :
Notre but est d'exhiber l'existence d'un élément d'ordre $q-1$.
Par le théorème de Lagrange on a : $|\mathbb{F}_q^*| = \sum_{d|q-1} \#\ \{x \in \mathbb{F}_q^* \text{ d'ordre d }\}$.
Posons $\lambda(d) := \#\{x \in \mathbb{F}_q^* \text{ d'ordre d }\}$.

Soit $\lambda(d) = 0$.
Soit $\lambda(d) \neq 0$.
Dans ce cas, il existe un élément $x \in \mathbb{F}_q^*$ d'ordre d.

Le sous-groupe $< x >$ de $\mathbb{F}_q^*$ qu'il engendre est isomorphe à $\mathbb{Z}/d\mathbb{Z}$. Il contient $\phi(d)$ éléments d'ordre d. D'où la minoration :

$$\boxed{\phi(d) \leq \lambda(d)}.$$

D'autre part, pour tout élément a de $< x >$, $a^d = 1$ donc a est racine du polynôme $X^d - 1$. Or ce polynôme a au plus d racines et comme $|< x >| = d$, on l'égalité suivante : $\{$ racines de $X^d - 1\} =< x >$.
Soit $y \in \mathbb{F}_q^*$ d'ordre d, y vérifie $y^d = 1$ donc y est un élément de $< x >$ d'ordre d. Comme $< x >$ en possède $\phi(d)$, on a donc la majoration :

$$\boxed{\lambda(d) \leq \phi(d)}.$$

Pour finir, en suivant le même raisonnement on montre que,
$n = |\mathbb{Z}/n\mathbb{Z}| = \sum_{d|n} \lambda(d) = \sum_{d|n} \phi(d)$ car par propriété du groupe $\mathbb{Z}/n\mathbb{Z}$, $\lambda(d) \neq 0$ pour tout $d|n$.

Ainsi, on a :

$$q - 1 = |\mathbb{F}_q^*| = \lambda(q-1) + \sum_{d|q-1, d \neq q-1} \lambda(d) \leq \phi(q-1) + \sum_{d|q-1, d \neq q-1} \phi(d) = |\mathbb{Z}/(q-1)\mathbb{Z}| = q - 1.$$

Donc en particulier $\lambda(q-1) = \phi(q-1) \neq 0$.
Autrement dit, il existe un élément d'ordre $q-1$ dans $\mathbb{F}_q^*$, ce qui achève la démonstration.

■

. . . . . .

Passons à présent à la recherche des groupes d'ordre pq où p et q sont deux nombres premiers.
Soit G un tel groupe, $|G| = pq$.
On a l'existence, par le théorème de Cauchy, d'un élément g_p d'ordre p dans G et d'un élément g_q d'ordre q dans G.
Comme p et q sont premiers, on a $< g_p > \cong \mathbb{Z}/p\mathbb{Z}$ et $< g_q > \cong \mathbb{Z}/q\mathbb{Z}$.

- Par primalité, $< g_p > \cap < g_q >= \{0\}$.
- Soit n_q le nombre de q-Sylow dans G.
  Il suit par le théorème de Sylow :
  $n_q | p$ donc $n_q = 1$ ou p, puis $n_q \equiv 1[q]$ donc $n_q = 1$.
  Il existe donc un unique q-Sylow, $< g_q >$, distingué dans G.

– Enfin, on a $< g_p >.< g_q >= pq = |G|$

Nous sommes donc ammené à déterminer les produits semi-directs :
$\mathbb{Z}/q\mathbb{Z} \rtimes_\Phi \mathbb{Z}/p\mathbb{Z} = G$ où $\Phi : \mathbb{Z}/p\mathbb{Z} \to Aut(\mathbb{Z}/q\mathbb{Z}) \cong (\mathbb{Z}/q\mathbb{Z})^*$.
Or $(\mathbb{Z}/q\mathbb{Z})^* \cong \mathbb{Z}/(q-1)\mathbb{Z}$ par le théorème précédent.
Cherchons donc les morphismes :

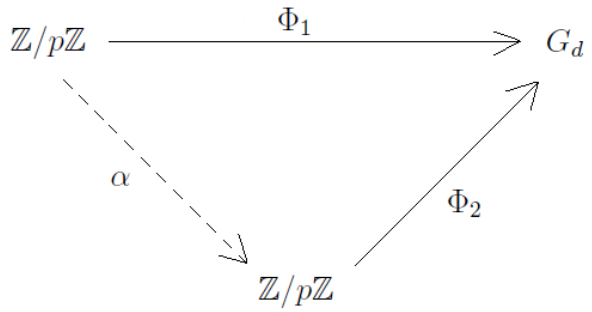
$$\begin{array}{rl} \Phi : & \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/(q-1)\mathbb{Z} \\ & 0 \longmapsto 0 \\ & \bar{x} \longmapsto \overline{\Phi(x)} \end{array}$$

Comme Φ est un morphisme, on a pour tout $\bar{x} \in \mathbb{Z}/p\mathbb{Z}$ non nul (donc $Ord(\bar{x}) = p$), $Ord(\overline{\Phi(x)})|Ord(\bar{x}) = p$. Donc $Ord(\overline{\Phi(x)})$ vaut 1 ou p.
Or on a aussi $Ord(\Phi(x))|q-1$ ce qui nous permet de distinguer deux cas.

– <u>Premier cas :</u>
Si p ne divise pas $q-1$ alors $Ord(\Phi(x)) = 1$ et Φ est trivial.
Dans ce cas, le produit est direct et par le théorème chinois $\boxed{G \cong \mathbb{Z}/pq\mathbb{Z}}$.

– <u>Second cas :</u>
Si $p|q-1$ alors $\mathbb{Z}/(q-1)\mathbb{Z}$ possède un unique sous-groupe d'ordre p : G_p.
On peut alors considérer des morphismes non triviaux.
Soient Φ_1, Φ_2 de tels morphismes. On va voir qu'ils construisent en fait le même produit semi-direct.
Par définition, on a Ker $\Phi_i = \{\vec{0}\}$ (sinon les morphismes sont triviaux).
Donc Im $\Phi_i \cong \mathbb{Z}/p\mathbb{Z}$ et par unicité Im Φ_1 =Im $\Phi_2 = G_p$.

On a le diagramme suivant :



où $\alpha := \Phi_1^{-1} \circ \Phi_2 \in Aut(G_d)$.

Dans ce cas, l'application

$$\begin{array}{rl} \Psi : & \mathbb{Z}/q\mathbb{Z} \rtimes_{\Phi_2} \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/q\mathbb{Z} \rtimes_{\Phi_1} \mathbb{Z}/p\mathbb{Z} \\ & (h,n) \longmapsto (h,\alpha(n)) \end{array}$$

est une bijection. Il reste à montrer que c'est un morphisme.

Pour tout $(h_1,h_2) \in (\mathbb{Z}/q\mathbb{Z})^2$ et tout $(n_1,n_2) \in (\mathbb{Z}/p\mathbb{Z})^2$, on a :

$$\begin{aligned} \psi[(h_1,n_1) \rtimes_{\Phi_2} (h_2,n_2)] &= \psi(h_1.\Phi_2(n1).h_2, n_1n_2) \\ &= (h_1.\Phi_2(n1).h_2, \alpha(n_1n_2)) \end{aligned}$$

$$\begin{aligned} \psi(h_1,n_1) \rtimes_{\Phi_1} (h_2,n_2) &= (h_1,\alpha(n_1)) \rtimes_{\Phi_1} (h_2,\alpha(n_2)) \\ &= (h_1.(\Phi_1 \circ \alpha)(n_1).h_2, \alpha(n_1)\alpha(n_2)) \\ &= (h_1.\Phi_2(n_1).h_2 \circ \alpha(n_1).h_2, \alpha(n_1n_2)) \end{aligned}$$

Ainsi, $\boxed{\mathbb{Z}/q\mathbb{Z} \rtimes_{\Phi_2} \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/q\mathbb{Z} \rtimes_{\Phi_1} \mathbb{Z}/p\mathbb{Z}}$.

Pour conclure, les groupes d'ordre pq, où $p < q$ premiers sont $\mathbb{Z}/pq\mathbb{Z}$ ou un produit semi-direct non commutatif.

■

Second développement : Irréductibilité des polynômes cyclotomiques dans $\mathbb{Z}[X]$

Référence : Gourdon-Algèbre p91-92

Nous noterons :
- $U_n = \{e^{2ik\pi/n} \mid k \in \mathbb{Z}\}$, le groupe multiplicatif formé par les racines n-ième de l'unité.
- Λ_n l'ensemble de ses générateurs (aussi appelés *racines primitives n-ième de l'unité*).
  On a $\Lambda_n = \{\omega^k \mid 0 \leq k \leq n-1$, premier avec $n\}$ pour n'importe quel générateur ω de U_n (p20 du Gourdon pour s'en convaincre).
- Φ_n le *polynôme cyclotomique d'indice n* définit par $\Phi_n = \prod_{\xi \in \Lambda_n} (X - \xi)$. Il est de degré $\varphi(n)$.

Par définition, les Φ_n ne sont pas irréductibles dans $\mathbb{C}[X]$ mais nous allons prouver le résultat suivant :

Théorème : *Pour tout entier naturel n non nul, Φ_n est irréductible dans $\mathbb{Z}[X]$*

Preuve :
Dans toute la preuve, on se fixe un entier naturel n non nul.
Nous allons montrer l'irréductibilité sur $\mathbb{Q}$ car, Φ_n étant primitif, si l'on montre l'irréductibilité dans $\mathbb{Q}[X]$ on l'aura alors dans $\mathbb{Z}[X]$.

Préliminaires : $\Phi_n \in \mathbb{Z}[X]$ (on pourra ainsi l'observer dans $\mathbb{Z}/p\mathbb{Z}[X]$).

Pour cela il nous faut prouver au préalable un lemme qui servira à nouveau plus loin :

Lemme : $X^n - 1 = \prod_{d|n} \Phi_d$.

Dém :
Notons $\omega := e^{2i\pi/n}$.
Pour tout $0 \leq k \leq n-1$, ω^k a un ordre d divisant n dans U_n donc appartient à U_d (car $(\omega^k)^d = 1$) et même à Λ_d.
Donc chaque $X - \omega^k$ divise Φ_d et divise donc le produit $\prod_{d|n} \Phi_d$.
Comme les $X - \omega^k$ pour tout $0 \leq k \leq n-1$ sont irréductibles (de degré 1) ils sont premiers entre eux (car $\mathbb{Q}[X]$ est factoriel) et leur produit divise également $\prod_{d|n} \Phi_d$.
On a donc montré que $X^n - 1 = \prod_{k=0}^{n-1}(X - \omega^k) \mid \prod_{d|n} \Phi_d$.
Enfin, comme les deux polynômes sont unitaires et de degrés égaux ($\sum_{d|n} deg(\Phi_d) = \sum_{d|n} \varphi(d) = n$) on conclut.

■

Revenons à la démonstration du fait qu'un polynôme cyclotomique est à coefficients entiers. Procédons par récurence sur $n \in \mathbb{N}^*$.
Pour $n = 1$, $\Phi_1 = X - 1 \in \mathbb{Z}[X]$.
Supposons le résultat vrai jusqu'au rang $n-1$ et montrons le au rang n.

Posons $P := \prod_{d|n, d \neq n} \Phi_d$, élément de $\mathbb{Z}[X]$ par hypothèse de récurrence.
En exploitant le lemme on obtient d'une part : $X^n - 1 = \Phi_n P$.
D'autre part, par division euclidienne dans $\mathbb{Z}[X]$ de $X^n - 1$ par P (on peut l'effectuer puisque P est unitaire) : $\exists Q, R \in \mathbb{Z}[X]$, $X^n - 1 = PQ + R$ avec $\deg(R) < \deg(P)$.

Par unicité du couple (Q, R) dans l'anneau euclidien $\mathbb{Q}[X]$ donc dans $\mathbb{Z}[X]$, $R = 0$ et $\Phi_n = Q \in \mathbb{Z}[X]$. Cela termine les préliminiaires.

. . . . . .

Passons à la preuve du théorème et supposons par l'absurde que l'on puisse écrire $\Phi_n = G_1 ... G_r$, une décompostition de Φ_n en produit d'irréductibles de $\mathbb{Q}[X]$.

Nous allons procéder en 4 étapes :
1/ on peut se ramener à écrire $\Phi_n = F_1 ... F_r$ où $F_i \in \mathbb{Z}[X]$ unitaires et irréductibles dans $\mathbb{Q}[X]$
2/ Soit $\xi \in \mathbb{C}$ une racine de F_1, $\exists i$, $F_i(\xi^p) = 0$ pour tout p premier ne divisant pas n
3/ $i = 1$
4/ $F_i(\xi^k) = 0$ pour tout k premier avec n.

1ère étape :
Pour tout i, il existe un $\alpha_i \in \mathbb{N}^*$ tel que $\alpha_i G_i \in \mathbb{Z}[X]$.
On a donc $\alpha_1...\alpha_r \Phi_n = (\alpha_1 G_1)...(\alpha_r G_r)$, produit de polynômes de $\mathbb{Z}[X]$.
Par le lemme de Gauss sur les contenus et comme Φ_n est unitaire, on obtient : $\alpha_1...\alpha_r = \prod_{i=0}^{r} c(\alpha_i G_i)$. Ainsi, $F_i := \alpha_i G_i / c(\alpha_i G_i)$ convient.

2ième étape :
Par hypothèse, ξ est une racine de F_1 donc de Φ_n. Donc $\xi \in \Lambda_n$.
Tout p premier ne divisant pas n est premier avec n et donc $\xi^p \in \Lambda_n$, d'où ξ^p est racine de Φ_n. Il existe donc i tel que $F_i(\xi^p) = 0$.
Nous allons maintenant voir qu'il s'agit encore de F_1.

3ième étape :
Cette partie nécessite deux résultats simple à démontrer.

Lemme 1 : Pour tout $F \in \mathbb{Z}[X]$, on a dans $\mathbb{Z}/p\mathbb{Z}[X]$: $\overline{F}(X^p) = \overline{F}(X)^p$
Dém :
Procédons par récurrence sur le degré m de F.
Si $m = 0$ c'est évident. Supposons le résultat vrai jusqu'au rang $m-1$ et montrons le au rang m.
On écrit $F = \sum_{k=0}^{m} a_k X^k = G + a_m X^m$ où G vérifie l'hypothèse de récurrence.
On a dans $\mathbb{Z}/p\mathbb{Z}[X]$:

$$\overline{F}^p = \overline{G}^p + \overline{a_m}^p X^{pm} + \sum_{k=1}^{p-1} \binom{p}{k} \overline{G}^k \overline{a_m}^{p-k} X^{(p-k)m}.$$

Or par Fermat, $\overline{a_m}^p = \overline{a_m}$ et $\forall 1 \leq k \leq n-1$, $p \mid \binom{p}{k}$, donc on en déduit en appliquant à G l'hypothèse de récurrence :

$$\overline{F}(X)^p = \overline{G}(X^p) + \overline{a_m}(X^p)^m = \overline{F}(X^p).$$

■

Lemme 2 : $\overline{\Phi_n}$ n'est divisible par aucun carré de polynôme non constant.
Dém :
Supposons $\overline{\Phi_n} = \overline{Q}^2 \overline{P}$. On a vu pendant les préliminaires qu'en posant $R := \prod_{d|n, d\neq n} \Phi_d$ on a $X^n - 1 = \Phi_n R$.
Donc $X^n - 1 = \overline{\Phi_n R} = \overline{Q}^2 \overline{S}$ (où $S = PR$), d'où par dérivation :

$$\overline{n} X^{n-1} = 2\overline{Q}\overline{Q}'\overline{S} + \overline{Q}^2 \overline{S}'$$

Donc $\overline{Q} \mid \overline{n}X^{n-1}$ et donc $\overline{n}X^n$. De plus, $\overline{Q} \mid X^n - 1$ donc $\overline{Q} \mid (\overline{n}X^n - \overline{n})$ donc finalement $\overline{Q} \mid \overline{n}$. Comme n a été supposé non nul, $\overline{Q}$ est constant.

■

Utilisons ces lemmes :
$F_1(X)$ et $F_i(X^p)$ ne sont pas premiers entre eux (Bezout en $X = \xi$ fournit une contradiction).
Comme F_1 est irréductible dans $\mathbb{Q}[X]$, $F_1(X) \mid F_i(X^p)$ dans $\mathbb{Q}[X]$ donc dans $\mathbb{Z}[X]$ (F_1 est unitaire). D'où, $\overline{F_1}(X) \mid \overline{F_i}(X^p) = \overline{F_i}(X)^p$ par le lemme 1.
Ainsi, un facteur $\overline{P}$ irréductible de $\overline{F_1}$ dans $\mathbb{Z}/p\mathbb{Z}$ divise à la fois $\overline{F_1}(X)$ et $\overline{F_i}(X)$.
Si $i \neq 1$, on aurait $\overline{P}^2 \mid \Phi_n$, ce qui est absurde par le lemme 2. Donc $i = 1$.

4ième étape : Soit k premier avec n. On peut écrire $k = p_1...p_s$ où les p_i sont premiers. Effectuons une récurrence sur s. Pour $s = 1$, c'est le résultat de la partie qui précède. Supposons le résultat vrai au rang $s-1$ et montrons le au rang s.
Comme k est premier avec n, $p_1...p_{s-1}$ aussi, donc par hypothèse de récurrence : $F_1(\xi^{p_1 \cdots p_{s-1}}) = 0$.
$\xi^{p_1 \cdots p_{s-1}}$ est donc une racine de F_1 et comme p_s est premier avec n, la partie précédente assure à nouveau que $F_1[(\xi^{p_1 \cdots p_{s-1}})^{p_s}] = 0$.

CONCLUSION :
On a $\Lambda_n = \{\xi^k \mid 0 \leq k \leq n-1$, premier avec $n\}$, donc tout élément de Λ_n est racine de F_1. Cela signifie qu'en fait $F_1 = \Phi_n$. Donc Φ_n est irréductible dans $\mathbb{Q}[X]$ donc dans $\mathbb{Z}[X]$.

■

Remarque : on retrouve également l'irréductibilité de $\Phi_p = 1 + ... + X^{p-1}$ par application du critère d'Eisenstein.
Applications : théorème de Dirichlet faible, théorème de Wedderburn... $\left(\frac{\mathbb{Z}}{d\mathbb{Z}}\right)$