Automorphismes de $\mathbb{Z}/n\mathbb{Z}$ (pages 24-25-26 du Perrin

Pierre Lissy

May 7, 2010

On se ramène par décomposition en facteurs premiers à rechercher les inversibles de $Z/(p^\alpha)Z$.

Lemme 1. *Si p est un nombre premier différent de 2 alors $Z^*_{p^\alpha} \simeq Z_{\varphi(p)}$.*

Proof. On a encore besoin d'un lemme.

Lemme 2. $(1+p)^{p^k} = 1 + \lambda * p^{k+1}$ *avec λ premier à p.*

Proof. Par récurrence sur k.

1. k=1: $(1+p)^p = \sum C_p^i p^i = 1 + p^2(1+u)$ avec u un multiple de p. Donc $\lambda = 1+u$ est premier à p.
2. Transition: $(1+p)^{p^{k+1}} = (1+\lambda p^k)^p = \sum C_p^i (\lambda p^k)^i = 1 + p^{k+2}(\lambda + u)$ avec u un multiple de p. Donc $\lambda + u$ est premier à p (sinon pb avec λ).

□

Du coup il est clair que l'élement $1+p$ est d'ordre $p^{\alpha-1}$ dans p^α puisque $(1+p)^{p^{\alpha-1}} = 1[p^\alpha]$ alors que $(1+p)^{p^{\alpha-2}} = 1 + \lambda * p^{\alpha-1}$. On considère le morphisme de groupe surjectif de $Z_p^(\alpha)^*$ vers $Z_p^* = Z_{p-1}$. On considère n'importe quel antécédent d'un générateur de Z_{p-1}, noté x. Alors l'ordre de x est un multiplie de $p-1$. En effet, on a que $x^k = 1$ implique que $\varphi(x)^k = 1$ et donc vu que l'ordre de $\varphi(x)$ est $p-1$, on a $(p-1)|k$.Il existe donc un y (qui est une certaine puissance de x) d'ordre $p-1$. L'ordre de y et l'ordre de $(1+p)$ sont premiers entre eux donc le produit $x(1+p)$ est d'ordre $o(x)o(1+p) = (p-1)p^{\alpha-1} = \varphi(p^\alpha)$ puisque l'on est dans un groupe commutatif. □

Reste à trouver les automorphismes des puissances de deux et on aura fini.

Lemme 3. $Z^*_{2^\alpha} \simeq Z_2 Z_{2^{\alpha-1}}$.

Ceci provient encore du lemme facilement démontrable:

Lemme 4. $5^{2^k} = 1 + \lambda 2^{k+2}$ *avec λ impair.*

Proof. Trivialement vrai pour k=1 et se transmet facilement: $5^{2^{k+1}} = (1+\lambda * 2^k)^2 = 1 + (\lambda^2)2^{2k+4} + (\lambda)2^{2k+3}$. □

On considère alors le morphisme surjectif $Z_2^(\alpha)^*$ vers $Z_2 = Z_4*$. Le noyau de φ, noté N est de cardinal $2^{\alpha-2}$ par surjectivité, donc est cyclique engendré par l'élement d'ordre $2^{\alpha-2}$ 5. On a alors que c'est un sous-groupe d'indice 2 (car on sait déjà que le groupe des inversibles est de cardinal $\varphi(2^\alpha)$), donc il est distingué et si on prend l'élement -1, il est pas dans le sous-groupe N puisque l'élement va valoir aussi -1 dans Z_2. Donc on a que $N * 1, -1 = G$, que les groupes sont d'intersection triviale et que l'u nest distingué, on a donc un produit semi-direct et même direct ici $Z^*_{2^\alpha} \simeq Z_2 Z_{2^{\alpha-1}}$.