Université Paris 7 - Denis Diderot 2018-2019

UFR de Mathématiques M1 - Arithmétique

Corrigé feuille d'exercices 1

Exercice 1 1) Soit d l'ordre de x_1x_2. Clairement $(x_1x_2)^{d_1d_2} = 1$donc d divise d_1d_2. Par ailleurs, puisque $(x_1x_2)^d = 1$, on a $x^d = y^{-d}$ et donc $x^{dd_2} = (y^{d_2})^{-d} = 1$ donc d_1 divise dd_2i, et donc divise d puisque $d1, d_2$ sont premiers entre eux. En échangeant x et y on arrive à d_2 divise d, et donc d_1d_2 divise d en utilisant de nouveau qu'ils sont premiers entre eux. 2) en décomposant d_1, d_2 en facteurs premiers on construit un élément d'ordre $PPCM(d_1, d_2)$ qui appartient au sous-groupe engendré par x_1 et x_2. Puisque on est dans un groupe cyclique, ce sous-groupe est lui même cyclique, et son ordre divise $PPCM(d_1, d_2)$, donc lui est égal par le point précédent.

Exercice 2 On peut adapter la preuve du cours que le groupe des inversibles dans $Z/p\mathbb{Z}$ est cyclique. On peut aussi poser

$$A = \{x \in (\mathbb{Z}/p^\alpha\mathbb{Z})^*, \text{ dont la réduction mod } p^2\text{est un générateur des inveribles}\}$$

et

$$B = \text{ensemble des générateurs de}(\mathbb{Z}/p^\alpha\mathbb{Z})^*$$

Clairement $B \subset A$. On sait que le cardinal de B est $\phi(\phi(p^\alpha)) = p^{\alpha-2}(p-1)\phi(p-1)$, tandis que celui de A est le produit de $(p-1)\phi(p-1)$ (nb de générateurs mod p^2) par $p^{\alpha-2}$ (nombre de façon de relever un élément mod p^2 en un élément mod p^α), donc ils ont aussi même cardinal.

Exercice 3 a) ± 1

b) D'après a), ± 1 sont les seuls éléments qui sont leur propre inverse mod p. Or $(p-1)!$ mod p est justement le produit de tous les éléments inversibles, donc ils s'annulent deux à deux, sauf 1 et -1.

Exercice 4 Si x engendre le groupe multiplicatif (tout élément non nul est une puissance de x), il engendre à fortiori l'extension (tout élément est $P(x)$ pour un certain polynôme P).

Exercice 5 Voir poly de cours

Exercice 6 Un polynôme homogène a toujours au moins $(0, 0, 0, \ldots, 0)$ comme racine, donc le nombre de racines est différent de 0. Par Chevalley-Warning il vaut 0 mod p, donc il vaut au moins p donc il existe une racine non-nulle.

Exercice 7 a) On sait que $x^q = x$ ssi $x \in \mathbb{F}_q$. Donc $x \mapsto x^q$ est $\mathbb{F}_q$-linéaire, et c'est un isomorphisme, donc il envoit une base sur une base.

b) $\phi(P) = P$, donc ses coefficients satisfont $a^q = a$ donc ils appartiennent à $\mathbb{F}_q$.

c) P est défini comme un produit, donc il s'annule ssi l'un des facteurs s'annule. Mais les $\alpha_i^{q^j}$, j fixé, forment une base, donc ces facteurs s'annulent seulement en $(0, 0, 0, \ldots, 0)$.

d) Le point précédent contredit la conclusion de Chevalley-Warning, il est donc otpimal.