Université Paris 7 - Denis Diderot 2018-2019

UFR de Mathématiques M1 - Arithmétique

Feuille d'exercices 1

Exercice 1 Montrer que si, dans un groupe commutatif, l'ordre de x_1 est d_1, l'ordre de x_2 est d_2, avec d_1 et d_2 premiers entre eux, alors l'ordre de x_1x_2 est d_1d_2. Montrer également que si, dans un groupe cyclique, l'ordre de x_1 est d_1, l'ordre de x_2 est d_2, alors l'ordre du sous-groupe engendré par x_1 et x_2 est égal au PPCM de d_1 et d_2.

Exercice 2 Soit $p \neq 2$ un nombre premier. Montrer que si la classe de $x \in \mathbb{Z}$ engendre $(\mathbb{Z}/p^2\mathbb{Z})^*$ alors elle engendre aussi $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$.

Exercice 3 Écrire les tables d'addition et de multiplication de l'anneau $\mathbb{Z}/4\mathbb{Z}$ et du corps $\mathbb{F}_4$.

Exercice 4 Théorème de Wilson.

a) Soit p un nombre premier. Résoudre $x^2 = 1$ dans $\mathbb{F}_p$.

b) En déduire le théorème de Wilson : pour tout entier p, p est premier si et seulement si $(p-1)! \equiv -1 \bmod p$.

Exercice 5 Générateurs des corps finis.

Soient p un nombre premier et $q = p^n$ $(n \geqslant 1)$ une puissance de p.

Si $x \in \mathbb{F}_q$, existe-t-il un lien entre le fait que x engendre l'extension $\mathbb{F}_q/\mathbb{F}_p$ et le fait que x engendre le groupe multiplicatif $\mathbb{F}_q^\times$?

Exercice 6 Théorème de Chevalley-Warning. Soit $\mathbb{F}_q$ un corps fini de caractéristique p.

a) À quelle condition sur l'entier $k \geqslant 0$ existe-t-il $x \in \mathbb{F}_q^\times$ tel que $x^k \neq 1$?

b) Déterminer, pour tout entier $k \geqslant 0$, la somme $\sum_{x \in \mathbb{F}_q} x^k$ (pour $k = 0$, on prendra la convention $0^0 = 1$).

c) On considère un polynôme $P \in \mathbb{F}_q[X_1, X_2, \cdots, X_n]$ et l'on définit $A = 1 - P^{q-1}$. Montrer que la fonction polynômiale $A : \mathbb{F}_q^n \to \mathbb{F}_q$ peut-être vue comme la fonction caractéristique d'un ensemble que l'on déterminera.

d) On suppose $\deg(P) < n$.
Déduire de ce qui précède que le nombre de solutions de l'équation $P(x_1, x_2, \ldots, x_n) = 0$, dans $\mathbb{F}_q^n$, est divisible par p.

e) On considère des polynômes $P_1, P_2, \cdots, P_r \in \mathbb{F}_q[X_1, X_2, \cdots, X_n]$ tels que $\sum_{i=1}^r \deg(P_i) < n$.
Généraliser le raisonnement précédent pour montrer que le nombre de racines communes aux polynômes $P_1, P_2, \cdots, P_r$, dans $\mathbb{F}_q^n$, est divisible par p.

Exercice 7 Corps quasi-algébriquement clos. Soient k un corps commutatif.

On dit que le corps k est *quasi-algébriquement clos* si tout polynôme homogène non constant à coefficients dans k, de degré strictement inférieur à son nombre de variables, possède une racine non nulle.

Montrer que tout corps fini est quasi-algébriquement clos.

Exercice 8 On veut montrer que l'hypothèse sur le degré dans le théorème de Chevalley-Warning ne peut pas être améliorée.

Soit $\mathbb{F}_q$ un corps fini et $n \geqslant 2$ un entier. On considère une base $(\alpha_1, \cdots, \alpha_n)$ du corps $\mathbb{F}_{q^n}$, vu comme $\mathbb{F}_q$-espace vectoriel et l'on considère le polynôme $P = \prod_{j=1}^{n}(\alpha_1^{q^j} X_1 + \alpha_2^{q^j} X_2 + \cdots + \alpha_n^{q^j} X_n)$.

a) Montrer que $(\alpha_1^q, \cdots, \alpha_n^q)$ est aussi une base du $\mathbb{F}_q$-espace vectoriel $\mathbb{F}_{q^n}$.

b) Pour tout polynome $R = \sum_{i=0}^{r} r_i X^i \in \mathbb{F}_{q^n}[X]$, on définit $\varphi(R) := \sum_{i=0}^{r} r_i^q X^i \in \mathbb{F}_{q^n}[X]$.
Déterminer $\varphi(P)$ et en déduire que $P \in \mathbb{F}_q[X_1, X_2, \cdots, X_n]$.

c) Résoudre, dans $\mathbb{F}_q^n$, l'équation $P(x_1, x_2, \cdots, x_n) = 0$.

d) Conclure.