TD 11

Exercice 1. À quoi est isomorphe le groupe additif d'un corps fini à q éléments ?

Exercice 2.

1. Combien le groupe $\mathbb{F}_7^\times$ a-t-il de générateurs ?
2. Faire la liste des éléments de $\mathbb{F}_7^\times$ et déterminer l'ordre de chacun d'eux.
3. Donner un isomorphisme entre $\mathbb{F}_7^\times$ et $\mathbb{Z}/6\mathbb{Z}$.

Exercice 3. Déterminer les automorphismes de $\mathbb{F}_4$.

Exercice 4. Déterminer les polynômes P irréductibles de degré 3 dans $\mathbb{F}_2[X]$. Montrer qu'à isomorphisme près, le quotient $\mathbb{F}_2[X]/(P)$ ne dépend pas du choix du polynôme irréductible de degré 3. Même question pour le degré 4.

Exercice 5. Soient q et q' deux nombres entiers qui peuvent s'écrire comme puissance d'un nombre premier. À quelle condition $\mathbb{F}_q$ admet-il un sous-corps isomorphe à $\mathbb{F}_{q'}$? Dans ce cas, combien en admet-il ?

Exercice 6. Soit K un corps fini. Montrer que toute fonction $K \to K$ est une fonction polynomiale. À quelle condition deux polynômes définissent-ils la même fonction polynomiale ?

Exercice 7. Soit p un nombre premier impair.

1. Montrer que le polynôme $P(X) = X^4+1$ est scindé sur le corps $\mathbb{F}_{p^2}$ (on pourra considérer les éléments d'ordre 8 du groupe multiplicatif du corps $\mathbb{F}_{p^2}$).
2. Si $\alpha \in \mathbb{F}_{p^2}$ est une racine de $P(X)$, montrer que les autres racines sont $-\alpha$, α^{-1} et $-\alpha^{-1}$, et que ces racines sont deux à deux distinctes.
3. Vérifier l'égalité $(\alpha+\alpha^{-1})^2 = 2$.
4. Montrer que $\alpha+\alpha^{-1}$ est dans le corps $\mathbb{F}_p$ si et seulement si $p \equiv \pm 1 \bmod 8$.
5. En déduire que 2 est un carré modulo p si et seulement si on a la congruence $p \equiv \pm 1 \bmod 8$.

Exercice 8. Soit K un corps. Étant donné $P(X) = a_d X^d + \cdots + a_1 X + a_0 \in K[X]$, on appelle *polynôme dérivé de* P le polynôme $P'(X) = d\cdot a_d X^{d-1} + \cdots + 2\cdot a_2 X + a_1 \in K[X]$.

1. Montrer que si K est de caractéristique nulle, $P' = 0$ si et seulement si P est constant.
2. Montrer que si K est de caractéristique $p > 0$, $P' = 0$ si et seulement s'il existe $Q \in K[X]$ tel que $P = Q(X^p)$.
3. Dans toute la suite, on se fixe un corps algébriquement clos L contenant K. Un polynôme $P \in K[X]$ est dit *séparable sur* K si ses racines (dans L) sont toutes de multiplicité 1. Montrer que P est séparable si et seulement si P et P' sont premiers entre eux dans $K[X]$.

4. Montrer que tout polynôme irréductible dans $K[X]$ est séparable si K est de caractéristique nulle ou si, étant de caractéristique $p > 0$, le morphisme $x \mapsto x^p$ est surjectif (on dit alors que le corps K est *parfait*).
5. Soit Frob : $R \mapsto R^p$ le morphisme de Frobenius $\mathbb{F}_p(T) \to \mathbb{F}_p(T)$. On pose $K = \operatorname{im} \mathrm{Frob} \subset \mathbb{F}_p(T)$ et $U = T^p = \mathrm{Frob}(T)$. Montrer que $X^p - U \in K[X]$ est irréductible et non séparable. (*Indication :* on pourra utiliser le critère d'Eisenstein).

Exercice 9.

1. Soit L/K une extension de corps finis (c'est-à-dire deux corps finis inclus l'un dans l'autre : $K \subset L$). Soit $x \in L^\times$ un générateur du groupe multiplicatif $L^\times$. Montrer qu'un sous-corps de L contenant K et x est nécessairement L.
2. Déduire de la question précédente que pour tout corps fini K et tout degré d, il existe un polynôme irréductible unitaire de degré d dans $K[X]$.

Exercice 10. Soit p un nombre premier. Le but de l'exercice est de démontrer, par récurrence sur $n \geq 1$ que tous les corps de cardinal p^n sont isomorphes.

1. Montrer le résultat pour $n = 1$.
2. On fixe n supérieur ou égal à 2 et K et K' deux corps de cardinal p^n. Soit ℓ un diviseur premier de n. Soit D (respectivement D') l'unique sous-corps de K (respectivement K') de cardinal $m = n/\ell$ (cf. exercice 5).
   a. Soit a un élément de $K \setminus D$; montrer que le sous-corps de K engendré par D et a est K ; en déduire que K est isomorphe au quotient de $D[X]$ par un polynôme irréductible P de degré ℓ qui divise $X^{p^n} - X$.
   b. Par l'hypothèse de récurrence, D et D' sont isomorphes ; soient ϕ un isomorphisme de D dans D' et Q l'image de P dans $D'[X]$. Montrer que Q possède une racine b dans K' et que le sous-corps engendré par D' et b est K'. En déduire que K et K' sont isomorphes.

Exercice 11. On appelle *poids* d'un élément $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{F}_2^n$ le nombre entier $w(\mathbf{b}) = w(b_1, \ldots, b_n) = |\{i \,|\, b_i = 1\}|$.

1. Montrer que $(\mathbf{b}, \mathbf{b}') \mapsto w(\mathbf{b} - \mathbf{b}')$ définit une distance sur $\mathbb{F}_2^n$, appelée *distance de Hamming*.
2. Si $C \subset \mathbb{F}_2^n$ est un sous-espace vectoriel, $d = \min\{w(\mathbf{b}) \,|\, \mathbf{b} \in C \setminus \{\mathbf{0}\}\}$ est appelé la *distance minimale* de C et on dit que C est un *code (linéaire, binaire) de paramètres* $(n, \dim C, d)$. Donner des exemples de codes de paramètres $(n, n, 1)$, $(n, 1, n)$ et $(2n, 2n - 1, 2)$.
3. Un code C est dit *parfait* si sa distance minimale est un entier impair $2t + 1$ et que les boules (pour la distance de Hamming) de rayon t centrées en les éléments de C forment une partition de $\mathbb{F}_2^n$. Montrer que si C est un code de paramètres (n, k, d), avec $d \geq 2t + 1$, on a l'inégalité suivante, appelée *borne de Hamming* : $\sum_{r=0}^{t} \binom{n}{r} \leq 2^{n-k}$ et que c'est une égalité si et seulement si C est parfait de distance minimale $2t + 1$. En déduire qu'un éventuel code de paramètres $(23, 12, 7)$ serait parfait.
4. Montrer que le $\mathbb{F}_2$-espace vectoriel engendré par les vecteurs $(1, 1, 0, 1, 0, 0, 0)$, $(0, 1, 1, 0, 1, 0, 0)$, $(0, 0, 1, 1, 0, 1, 0)$ et $(0, 0, 0, 1, 1, 0, 1)$ est un code parfait appelé *code de Hamming de longueur 7* et déterminer ses paramètres.