Corps finis et actions de groupes

Dans ce qui suit les corps et anneaux sont commutatifs.

Lemme 1. *Si k est un corps, toute k-algèbre A intègre de dim. finie est un corps.*

Dém. Soit $a \in A$ non nul. L'application k-linéaire $f : A \to A$, $x \mapsto ax$ est injective car A est intègre. Comme A est de dimension finie, f est bijective. En particulier il existe x tel que $ax = 1$ donc a est inversible.

Lemme 2. *Soit k un corps, $P \in k[X]$ un polynôme. Il existe une extension de corps K/k avec les propriétés :*

(i) *le polynôme P est scindé dans K, i.e. $P = \lambda(X - \alpha_1)\dots(X - \alpha_n)$ avec $\alpha_i \in K$,*

(ii) *l'extension K/k est engendrée par les racines de P, i.e. $K = k(\alpha_1, \dots, \alpha_n)$.*

Une telle extension est unique à isomorphisme près et est appelée un corps de décomposition de P sur k.

Dém. Soit Q un facteur irréductible de P et soit $K_1 = k[X]/(Q)$. C'est une k-algèbre intègre de dimension finie donc un corps (lemme 1). Notons α_1 la classe de X dans K_1. Par construction α_1 est une racine de Q dans K_1, et $K_1 = k(\alpha_1)$. Il en découle que dans K_1 on peut écrire $P = (X - \alpha_1)P_1$ avec $P_1 \in K_1[X]$. On recommence en prenant un facteur irréductible de P_1, etc. On construit ainsi une suite de corps $K_i = k(\alpha_1, \dots, \alpha_i)$ et $K := K_n$ convient. Passons à l'unicité. Soient $K = k(\alpha_1, \dots, \alpha_n)$, $L = k(\beta_1, \dots, \beta_n)$ deux extensions vérifiant (i) et (ii). Quitte à renuméroter les racines, on peut supposer que α_1 et β_1 sont racines de Q. On a alors $K_1 = k(\alpha_1) \simeq k[X]/(Q) \simeq k(\beta_1) = L_1$ ce qui donne un isomorphisme $\varphi_1 : K_1 \xrightarrow{\sim} L_1$. On construit par récurrence des isomorphismes $\varphi_i : K_i \xrightarrow{\sim} L_i$. Pour $i = n$ on trouve un k-isomorphisme entre K et L.

Théorème. (1) *Soit k un corps commutatif fini. Alors, la caractéristique de k est un nombre premier p. Le corps k est un $\mathbb{F}_p$-espace vectoriel de dimension finie n et son cardinal est égal à $q = p^n$. Tous les éléments $x \in k$ vérifient $x^q = x$. Le corps k est un corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$.*

(2) *Réciproquement, si p est un nombre premier, $n \geqslant 1$ un entier et $q = p^n$, alors un corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$ est un corps fini à q éléments.*

Remarque. On a vu que tout sous-groupe du groupe multiplicatif d'un corps est cyclique ; ceci s'applique au groupe des inversibles $k^\times$ d'un corps fini k, qui est donc cyclique donc isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$. En particulier, un générateur de $k^\times$ comme groupe est un générateur de k comme extension de $\mathbb{F}_p$, ce qui est un cas particulier (facile) du théorème de l'élément primitif pour les extensions finies séparables.

Exercice 1 (*« Le » corps à 16 éléments, extrait du sujet Math Géné 2007*)

1. (a) Comment peut-on construire $\mathbb{F}_{16}$?
   (b) Démontrer que le groupe multiplicatif $\mathbb{F}_{16}$ est formé des puissances successives d'un élément ω vérifiant l'égalité $\omega^4 + \omega^3 + 1 = 0$.
   (c) Démontrer que $\omega, \omega^2, \omega^4$ et ω^8 sont les racines du polynôme $X^4 + X^3 + 1$ dans $\mathbb{F}_{16}$.
   (d) Démontrer que la famille $(\omega, \omega^2, \omega^4, \omega^8)$ est une base de $\mathbb{F}_{16}$ sur $\mathbb{F}_2$.
2. (a) Soit $a \in \mathbb{F}_{16}$. Résoudre dans $\mathbb{F}_{16}$ l'équation $x^5 = a$, en discutant éventuellement selon la valeur de a.
   (b) Démontrer qu'il existe quatre éléments $\gamma \in \mathbb{F}_{16}$ tels que, pour chacun d'eux, la famille $(\gamma, \gamma^2, \gamma^4, \gamma^8)$ est une base de $\mathbb{F}_{16}$ sur $\mathbb{F}_2$ telle que le produit de deux de ses éléments appartient à la base ou est égal à 1. Expliquer rapidement pourquoi les calculs dans $\mathbb{F}_{16}$ sont plus faciles dans une telle base.

Les exercices suivants sont extraits de [H2G2$_1$], Ph. Caldero et J. Germoni, *Histoires hédonistes de groupes et de géométries*, tome 1, première édition, Calvage & Mounet, 2013.

Exercice 2 (*Cardinal de* $\mathrm{GL}_n(\mathbb{F}_q)$, [H2G2$_1$], *chap. VIII, prop. 1.1, p. 250*)

(1) Soient E un espace vectoriel de dimension finie sur un corps k, et $\mathscr{B}$ l'ensemble des bases ordonnées de E. Montrez que l'action naturelle de $\mathrm{GL}(E)$ sur $\mathscr{B}$ est libre et transitive.

(2) Calculez le cardinal de $\mathrm{GL}_n(\mathbb{F}_q)$ en dénombrant les bases de $(\mathbb{F}_q)^n$.

Exercice 3 (*Nombre de matrices diagonalisables dans* $\mathrm{M}_n(\mathbb{F}_q)$, [H2G2$_1$], *p. 262*)
Soit n et k deux entiers. On fixe k entiers $n_1, n_2, \ldots, n_k \geqslant 0$ tels que $\sum_{i=1}^k n_i = n$.

(1) Montrer qu'une matrice $A \in \mathrm{M}_n(\mathbb{F}_q)$ est diagonalisable si et seulement si $A^q = A$.

(2) Soient $n_1, \ldots, n_k$ des entiers $\geqslant 0$ dont la somme vaut n. Montrer que le nombre de familles $(E_1, \ldots, E_k)$ de sous-espaces tels que $E_1 \oplus \cdots \oplus E_k = \mathbb{F}_q^n$, $\dim E_i = n_i$ $(1 \leqslant i \leqslant k)$, est égal à

$$|\,\mathrm{GL}_n(\mathbb{F}_q)| / \prod_{i=1}^k |\,\mathrm{GL}_{n_i}(\mathbb{F}_q)|.$$

(*Indication : faire agir de façon naturelle* $\mathrm{GL}_n(\mathbb{F}_q)$ *sur l'ensemble des* k*-uplets de sous-espaces* $(E_1, \ldots, E_k)$ *tels que* $E_1 \oplus \cdots \oplus E_k = \mathbb{F}_q^n$ *et* $\dim E_i = n_i$*, montrer que l'action est transitive et regarder le stabilisateur.*)

(3) En déduire que le nombre de matrices diagonalisables de $\mathrm{M}_n(\mathbb{F}_q)$ est :

$$\sum_{\substack{n_1+\cdots+n_q=n \\ n_i \geqslant 0}} \frac{|\,\mathrm{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^q |\,\mathrm{GL}_{n_i}(\mathbb{F}_q)|}.$$

On trouve dans le livre [H2G2$_2$], Ph. Caldero et J. Germoni, *Histoires hédonistes de groupes et de géométries*, tome 2, Calvage & Mounet, 2015, la démonstration du fait que le cardinal de l'ensemble des matrices nilpotentes dans $\mathrm{M}_n(\mathbb{F}_q)$ est égal à $q^{n(n-1)}$. La preuve est assez délicate ; dans l'exercice suivant on présente le calcul plus facile du cardinal du sous-ensemble des matrices nilpotentes d'indice de nilpotence maximal.

Exercice 4 (*Nombre de matrices nilpotentes d'indice* n *dans* $\mathrm{M}_n(\mathbb{F}_q)$)

(1) Démontrez que l'ensemble des matrices nilpotentes d'indice n forme une orbite pour l'action de $\mathrm{GL}_n(\mathbb{F}_q)$ sur $\mathrm{M}_n(\mathbb{F}_q)$ par conjugaison.
Indication : si N *est nilpotente d'indice* n*, choisir* $x \in \mathbb{F}_q^n \smallsetminus \ker N^{n-1}$*, montrer que* $\{x, N(x), \ldots, N^{n-1}(x)\}$ *est une base de* $\mathbb{F}_q^n$*, et regarder la matrice de l'endomorphisme* N *dans cette base.*

(2) Soit N une matrice nilpotente d'indice n. Démontrez que l'ensemble des matrices $M \in \mathrm{M}_n(\mathbb{F}_q)$ telles que $NM = MN$ (le *commutant* de N dans $\mathrm{M}_n(\mathbb{F}_q)$) est égal à l'ensemble des polynômes en N. Démontrez qu'une telle matrice $M = a_0\mathbb{I}_n + a_1 N + \cdots + a_{n-1}N^{n-1}$ est inversible si et seulement si $a_0 \neq 0$.

(3) Déduisez-en que le cardinal de l'ensemble des matrices nilpotentes d'indice n dans $\mathrm{M}_n(\mathbb{F}_q)$ est égal à $(q^n - 1)(q^n - q)\ldots(q^n - q^{n-2})$.

Exercice 5 (*Cardinal de* $\mathrm{GL}_n(\mathbb{F}_q)$, [H2G2$_1$], *chap. VIII, prop. 1.1, p. 250, 2ème méthode*)

(1) On considère l'action naturelle de $\mathrm{GL}_n(\mathbb{F}_q)$ sur $(\mathbb{F}_q)^n \smallsetminus \{0\}$. Montrez que le stabilisateur du vecteur e_1 est de cardinal $q^{n-1}|\,\mathrm{GL}_{n-1}(\mathbb{F}_q)|$.

(2) Déduisez-en que $|\,\mathrm{GL}_n(\mathbb{F}_q)| = q^{n-1}(q^n - 1)|\,\mathrm{GL}_{n-1}(\mathbb{F}_q)|$ puis donnez une formule pour $|\,\mathrm{GL}_n(\mathbb{F}_q)|$.