COURS DE L'INSTITUT FOURIER

JEAN-RENÉ JOLY

Chapitre 1 Propriétés générales des corps finis

Cours de l'institut Fourier, tome 4 (1971), p. 1-13

<http://www.numdam.org/item?id=CIF_1971__4__A1_0>

Chapitre 1

Propriétés générales des corps finis

(1.1). Le théorème de Wedderburn.

Théorème 1 (Wedderburn). - Tout corps fini est commutatif.

Démonstration. Soit K un corps fini, et soit Z le centre de K, c'est-à-dire l'ensemble des $z \in K$ tels que $zx = xz$ pour tout $x \in K$; Z est un sous-corps de K, et $\mathrm{card}(Z) = q \geqslant 2$, puisque 0 et 1 sont dans Z. Considérons K comme espace vectoriel sur Z, et soit n la dimension de K sur Z ; on a $K \simeq Z^n$, donc

$$\mathrm{card}(K) = q^n . \tag{1}$$

Examinons maintenant le groupe multiplicatif K^* ; rappelons que deux éléments x_1 et x_2 de K^* sont dits conjugués (voir [La], pp. 19-23) s'il existe $y \in K^*$ tel que $x_2 = y^{-1} x_1 y$; la conjugaison est une relation d'équivalence dans K^* et partage K^* en classes de conjugaison; soit X un système de représentants de ces classes, et pour tout $x \in X$, soit C_x la classe de x : on a évidemment

$$\mathrm{card}(K^*) = \sum_{x \in X} \mathrm{card}(C_x) . \tag{2}$$

Les classes de conjugaison sont de deux types:

I) celles réduites à un élément, donc de la forme $C_z = \{z\}$, $z \in Z^*$; il y en a exactement

(3) $$\mathrm{card}(Z^*) = q - 1 ;$$

II) les autres, c'est-à-dire celles de la forme C_x, avec $x \in X' = X - Z^*$; pour chaque classe de ce deuxième type, soit N_x l'ensemble des $y \in K$ tels que $yx = xy$; N_x est un sous-corps de K, distinct de K et contenant Z ; si $d(x)$ désigne la dimension de N_x en tant qu'espace vectoriel sur Z, on a donc $1 \leq d(x) < n$, et $\mathrm{card}(N_x) = q^{d(x)}$; de plus, si $e(x)$ désigne la dimension de K sur N_x (en tant qu'espace vectoriel à gauche, par exemple), on vérifie sans peine que $d(x)e(x) = n$: $d(x)$ est donc un diviseur de n ; enfin, N_x^* est évidemment le normalisateur de x dans K^*, d'où (loc. cit.)

(4) $$\mathrm{card}(C_x) = \mathrm{card}(K^*) \big/ \mathrm{card}(N_x) = \frac{q^n - 1}{q^{d(x)} - 1} .$$

Comme, d'après (1), $\mathrm{card}(K^*) = q^n - 1$, les relations (3) et (4) permettent de réécrire (2) sous la forme suivante:

(5) $$q^n - 1 = q - 1 + \sum_{x \in X'} \frac{q^n - 1}{q^{d(x)} - 1} .$$

Cela étant, prouvons que K est commutatif: il s'agit de montrer que $K = Z$, ou encore que $n = 1$. Raisonnons par l'absurde, supposons que $n > 1$, et montrons que la relation (5) implique alors une contradiction. Rappelons que pour tout entier $d \geq 1$, on appelle $d^{\text{ième}}$ polynôme cyclotomique le polynôme $P_d(T) = \prod_{\zeta} (T - \zeta)$, le produit étant étendu à l'ensemble des ζ qui sont racines primitives $d^{\text{ièmes}}$ de l'unité dans C ; on a évidemment

(6) $$\prod_{d \mid n} P_d(T) = T^n - 1 ,$$

et cette formule permet, par récurrence, de calculer $P_d(T)$ pour toute valeur de d, et surtout de constater que $P_d(T)$ est un polynôme unitaire

à coefficients entiers. C'est le cas notamment pour $P_n(T)$, qui, d'autre part, divise évidemment le polynôme $(T^n - 1)/(T^d - 1)$ chaque fois que d est un diviseur de n différent de n . Cette dernière remarque prouve que dans la formule (5), tous les termes de la somme $\sum$ sont divisibles par $P_n(q)$, ainsi d'ailleurs que le membre de gauche: donc $P_n(q)$ doit diviser $q - 1$; mais, par définition, $P_n(q)$ est produit en nombre ≥ 1 de facteurs de la forme $q - \zeta$, où ζ est une racine primitive $n^{\text{ième}}$ de l'unité (d'où $\zeta \neq 1$, puisqu'on a supposé $n > 1$); pour chacun de ces facteurs, on a donc $|q - \zeta| > q - 1$ (*); a fortiori, $|P_n(q)| > q - 1$; or, nous venons de voir que $P_n(q)$ divise $q - 1$: contradiction. Ainsi, $n = 1$ et le corps fini K est commutatif, C.Q.F.D.

L'utilisation des polynômes cyclotomiques dans la démonstration du théorème de Wedderburn est due à Witt; pour plus amples détails sur les polynômes cyclotomiques, voir [La] , pp. 206-207, ou [VW] , vol. I, pp. 113-115.

(1.2). Classification des corps finis.

Désormais, corps signifiera corps commutatif; d'après le théorème 1, ceci est une convention "vide" en ce qui concerne les corps finis.

Théorème 2. - (i) Soit K un corps fini; la caractéristique de K est alors un nombre premier p , et le sous-corps premier de K s'identifie à $F_p = Z/pZ$; si $f = [K : F_p]$, et si on pose $q = p^f$, on a

$$\text{card}(K) = q ;$$

(*) faire une figure...

tout élément x de K vérifie l'égalité $x^q = x$, et on a donc la relation suivante:

$$X^q - X = \prod_{x \in K} (X - x) .$$

(ii) Inversement, soient p un nombre premier, f un entier $\geqslant 1$, posons $q = p^f$, et soit Ω_p une cloture algébrique de F_p ; il existe alors un sous-corps fini K et un seul de Ω_p tel que $\mathrm{card}(K) = q$: c'est l'ensemble des racines dans Ω_p du polynôme $X^q - X$.

(iii) Tout corps fini à $q = p^f$ éléments est isomorphe au corps K décrit en (ii).

Démonstration. (i) Si K, corps fini, était de caractéristique nulle, il contiendrait un sous-corps isomorphe à Q, qui est infini: absurde. La caractéristique de K est donc un nombre premier p, et l'égalité $\mathrm{card}(K) = q = p^f$ résulte du fait que $K \simeq (F_p)^f$ (pour la structure d'espace vectoriel). K^* est alors un groupe d'ordre $q - 1$, d'où $x^{q-1} = 1$ et a fortiori $x^q = x$ pour tout $x \in K^*$; mais cette dernière égalité est aussi vérifiée par $x = 0$, elle est donc vérifiée par tout $x \in K$. L'égalité polynomiale résulte alors de là, et du fait que les deux membres ont même degré, q.

(ii) L'unicité de K, sous-corps de Ω_p tel que $\mathrm{card}(K) = q$, résulte de (i) et du fait que dans Ω_p, le polynôme $X^q - X$ possède au plus q racines. Pour prouver son existence, définissons K comme l'ensemble des racines dans Ω_p de $X^q - X$: il faut démontrer deux choses:

que K est un corps: le seul point non évident est la stabilité de K

pour l'addition; mais ceci résulte de l'identité $x^{p^f} + y^{p^f} = (x+y)^{p^f}$, valable dans tout corps de caractéristique p, donc dans Ω_p ;

que card$(K) = q$: comme $F(X) = X^q - X$ est de degré q et se décompose complètement dans le corps algébriquement clos Ω_p, il s'agit de montrer que toutes les racines de $F(X)$ sont simples, ce qui résulte du fait que $F'(X) = qX^{q-1} - 1 = -1$ ne s'annule jamais (q est multiple de p, donc $q.1 = 0$ dans Ω_p).

(iii) Cette partie du théorème résulte de (i) et (ii), et du fait que deux clotures algébriques d'un corps donné (ici, F_p) sont isomorphes.

Par la suite, les lettres p, f et q garderont le plus souvent la signification qu'elles ont dans ce théorème 2, et F_q désignera "le" corps à q éléments (défini par q à isomorphisme près, d'après (iii)); pour $f = 1$ et $q = p$, on retombe sur la notation F_p.

Remarque. - Il résulte du théorème 2

que les éléments de F_q^* sont exactement les racines du polynôme $X^{q-1} - 1$; en particulier, que le produit de tous les éléments de F_q^* est égal au produit des racines de ce polynôme, donc à $(-1)^{q-1}.(-1) = (-1)^q = -1$.

Appliquons ceci à $F_p = Z/pZ$: nous retrouvons ces deux propriétés bien connues:

quels que soient p premier et a entier relatif non divisible par p, on a $a^{p-1} \equiv 1 \pmod p$ ("petit" théorème de Fermat);

quel que soit p premier, on a $(p-1)! \equiv -1 \pmod p$ (théorème de Wilson).

(1.3). Groupe additif et groupe multiplicatif d'un corps fini.

Théorème 3. - Soit K un corps fini à $q = p^f$ éléments.

(i) Le groupe additif de K est un groupe d'exposant p, somme directe de f groupes cycliques d'ordre p.

(ii) Le groupe multiplicatif K^* de K est un groupe cyclique d'ordre $q - 1$.

Démonstration. (i) K est en effet un espace vectoriel de dimension f sur son sous-corps premier $F_p \simeq Z/pZ$, d'où un isomorphisme de groupes additifs $K \simeq (Z/pZ)^f$.

(ii) Démontrons d'abord un lemme de théorie des groupes:

Lemme. - Soit G un groupe commutatif d'ordre fini, noté multiplicativement, et soit N le plus petit commun multiple des ordres de tous les éléments de G ; il existe alors un élément de G dont l'ordre est égal à N.

Prouvons ce lemme: soit $p_1^{a_1} p_2^{a_2} \dots p_m^{a_m}$ la décomposition de N en facteurs premiers; par définition de N, il existe pour chaque i ($1 \leq i \leq m$) un élément $y_i \in G$ d'ordre multiple de $p_i^{a_i}$; en élevant y_i à une puissance convenable, on obtient un élément $x_i \in G$ d'ordre égal à $p_i^{a_i}$; l'élément $x_1 x_2 \dots x_m \in G$ est alors d'ordre N, du fait que les entiers $p_i^{a_i}$ sont premiers entre eux deux à deux.

Prouvons maintenant (ii): soit N le plus petit commun multiple des ordres des éléments de K^* ; on a évidemment $N \leq q - 1$. D'autre part, tout $x \in K^*$ est (par définition de N) racine de l'équation $X^N - 1 = 0$: d'où (nombre de racines $\leq$ degré) $q - 1 \leq N$. Ainsi, $N = q - 1$. Appliquons alors le lemme: il existe dans K^* un élément w d'ordre $N = q - 1$

= l'ordre de K^* ; w est donc un générateur de K^*, et K^* est effectivement cyclique.

Remarque. - Pour une autre démonstration du fait que K^* est cyclique, voir par exemple [Se], chap. I, § 1.2.

(1.4). Puissances et racines de l'unité dans un corps fini.

D'abord quelques rappels relatifs aux groupes cycliques (finis!). Soit G un tel groupe, noté multiplicativement, et désignons par g l'ordre de G ; on sait (voir [VW], chap. I, § 7) que les sous-groupes de G sont en correspondance bijective avec les diviseurs positifs de g ; plus précisément, si H est un sous-groupe de G, l'ordre h de H divise g ; inversement, si un entier positif h divise g, il existe un et un seul sous-groupe H de G qui soit d'ordre h, et H est l'ensemble des $x \in G$ tels que $x^h = 1$. En outre, H et G/H sont évidemment cycliques. Cela étant:

Lemme. - Soient G un groupe cyclique d'ordre g, d un entier $\geqslant 1$ et $\overline{d} = (g, d)$ le plus grand commun diviseur de g et d. Désignons par ε l'endomorphisme de G défini par $x \longmapsto x^d$. Alors

(i) Le noyau N_d de ε est l'unique sous-groupe de G d'ordre égal à d ; étant donné $x \in G$, les assertions suivantes sont donc équivalentes:

(a) $x^d = 1$;

(b) $x^{\overline{d}} = 1$.

(ii) L'image G^d de ε est l'unique sous-groupe de G d'ordre égal à $g/\overline{d}$; étant donné $x \in G$, les assertions suivantes sont donc équivalentes:

(a') il existe $y \in G$ tel que $x = y^d$;

(b') x vérifie l'égalité $x^{g/\bar{d}} = 1$.

Démonstration. Si d divise g , on a $d = \bar{d}$, et le lemme résulte des rappels faits plus haut. Sinon, on a $d = k\bar{d}$, où k est premier avec g ; l'identité de Bezout $ag + bk = 1$ montre alors que l'application $x \longmapsto x^k$ est un automorphisme de G (d'inverse $x \longmapsto x^b$), d'où il résulte que $N_d = N_{\bar{d}}$ et $G^d = G^{\bar{d}}$: comme $\bar{d}$ divise g , on se trouve ramené au premier cas, et le lemme est démontré.

Appliquons ce lemme à $G = K^*$, groupe multiplicatif (cyclique!) d'un corps fini K ; l'endomorphisme ε est alors l'opération d'élévation à la puissance $d^{\text{ième}}$, et

$G^d = K^{*d}$ = le groupe des puissances $d^{\text{ièmes}}$ dans K^* ,

N_d = le groupe des racines $d^{\text{ièmes}}$ de l'unité contenues dans K .

Le lemme donne dans ces conditions:

Théorème 4. - Soient K un corps fini à $q = p^f$ éléments, d un entier $\geqslant 1$, et $\bar{d} = (q-1, d)$ le plus grand commun diviseur de $q - 1$ et d . Alors

(i) Le groupe des racines $d^{\text{ièmes}}$ de l'unité contenues dans K est l'unique sous-groupe d'ordre $\bar{d}$ de K^* ; pour que $x \in K^*$ soit racine $d^{\text{ième}}$ de l'unité, il faut et il suffit que x soit racine $\bar{d}^{\text{ième}}$ de l'unité.

(ii) Le groupe K^{*d} des puissances $d^{\text{ièmes}}$ dans K^* est l'unique sous-groupe d'ordre $(q - 1)/\bar{d}$ de K^* ; pour que $x \in K^*$ soit une puissance $d^{\text{ième}}$, il faut et il suffit que x vérifie le "critère d'Euler généralisé":

$$x^{(q-1)/\bar{d}} = 1 .$$

Enfin, le groupe quotient K^*/K^{*d} est d'ordre $\bar{d}$.

Remarque. - Soient p un nombre premier impair et a un entier relatif non divisible par p ; le théorème 4, appliqué à $K = F_p = Z/pZ$, à $d = 2$ et à $x =$ la classe de a modulo p , donne le critère d'Euler proprement dit (voir [HW] , p. 68): pour que a soit reste quadratique modulo p , c'est-à-dire pour que la congruence

$$Y^2 \equiv a \pmod{p}$$

admette une solution $y \in Z$, il faut et il suffit que a vérifie la congruence

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

(1.5). Extensions algébriques d'un corps fini.

Soient toujours p un nombre premier, f un entier $\geqslant 1$, q le nombre p^f , et $K = F_q$ "le" corps fini à q éléments. Soit d'autre part L une extension algébrique de K , de degré fini m : on a donc (toujours par des considérations de dimensions d'espaces vectoriels)

$$L = F_{q^m}.$$

Théorème 5. - L'extension L/K est cyclique (c'est-à-dire galoisienne à groupe de Galois cyclique). Le groupe de Galois $G(L/K)$ est engendré par le K-automorphisme $\sigma : x \longmapsto x^q$ de L , et les éléments de $G(L/K)$ sont les $\sigma^j : x \longmapsto x^{q^j}$ $(0 \leqslant j \leqslant m-1)$.

Démonstration. L'identité $x^{p^f} + y^{p^f} = (x+y)^{p^f}$, valable dans tout corps de caractéristique première p , montre que σ est un isomorphisme de L dans L , donc sur L , puisque L est fini; par ailleurs, le théorème 2, (i) prouve que $\sigma(x) = x$ pour tout $x \in K$: ainsi σ et plus

généralement toute puissance σ^j de σ est un K-automorphisme de L. Prouvons maintenant que $\sigma^j \neq 1$ pour tout j tel que $1 \leq j \leq m-1$: dans l'hypothèse contraire, on aurait $\sigma^j(x) = x$, c'est-à-dire $x^{q^j} = x$, pour tout $x \in L = F_{q^m}$; on aurait donc (théorème 2) $F_{q^m} \subset F_{q^j}$, ce qui est impossible, puisque $q^m = \mathrm{card}(F_{q^m}) > \mathrm{card}(F_{q^j}) = q^j$. Enfin, le théorème 2 montre de la même manière que $\sigma^m(x) = x^{q^m} = x$ pour tout $x \in L$, donc que $\sigma^m = 1$. Ainsi, le groupe des K-automorphismes de L contient au moins m éléments distincts: $1, \sigma, \sigma^2, \ldots, \sigma^{m-1}$, qui forment un groupe cyclique d'ordre m engendré par σ : comme $m = [L:K]$, ceci prouve à la fois que L/K est cyclique et que G(L/K) est le groupe cyclique engendré par σ : d'où le théorème.

Remarque 1. - Il est clair que le corps fini K est parfait: car l'isomorphisme $x \longmapsto x^p$ de K dans K est en fait surjectif; ceci implique que l'extension L/K est séparable. Par ailleurs, L/K est nécessairement normale: car si Ω_p est une cloture algébrique de F_p contenant L (et K), et si τ est un K-isomorphisme de L dans Ω_p, alors $\tau(L) = L$ = l'unique sous-corps de Ω_p contenant exactement q^m éléments (théorème 2, (ii)). L'ensemble de ces deux propriétés montre d'une autre manière que L/K est galoisienne (mais ne donne pas la structure de G(L/K)).

Remarque 2. - Le groupe multiplicatif L^* est cyclique: soit w un générateur de L^* ; il est clair que $L = K(w)$: ainsi, l'extension L/K est monogène, et w est un élément primitif pour cette extension.

Remarque 3. - Soit Ω_p une cloture algébrique de F_p contenant $K = F_q$, et soient L_1 et L_2 deux extensions de K contenues dans Ω_p et de degrés respectifs (finis) m_1 et m_2 (on a donc $L_1 = F_{q^{m_1}}$ et $L_2 = F_{q^{m_2}}$). Alors (exercice!)

pour que $L_1 \subset L_2$, il faut et il suffit que m_1 divise m_2 ; L_2 est dans ce cas l'unique extension de L_1 contenue dans Ω_p et de degré m_2/m_1 sur L_1 ; et inversement, L_1 est le sous-corps de L_2 invariant par l'automorphisme $x \longmapsto x^{q^{m_1}}$.

*

Mêmes notations que précédemment.

Théorème 6. - Soient Tr et N les applications trace et norme relatives à l'extension cyclique L/K (théorème 5), et posons

$$F(X) = X + X^q + \ldots + X^{q^{m-1}},$$

$$G(X) = X^{(q^m - 1)/(q - 1)} ;$$

alors

(i) Pour tout $x \in L$, $Tr(x) = F(x)$ et $N(x) = G(x)$.

(ii) L'application $Tr : L \longrightarrow K$ est surjective; si $x \in L$, les deux assertions suivantes sont équivalentes:

(a) $Tr(x) = 0$;

(b) il existe $y \in L$ tel que $x = y^q - y$.

(iii) L'application $N : L^* \longrightarrow K^*$ est surjective; si $x \in L^*$, les deux assertions suivantes sont équivalentes:

(a') $N(x) = 1$;

(b') il existe $y \in L^*$ tel que $x = y^{q-1}$.

Démonstration. (i) Si $x \in L$, les conjugués de x sur K sont x, x^q, ..., $x^{q^{m-1}}$ (théorème 5), donc $Tr(x) = x + x^q + \ldots + x^{q^{m-1}}$ et $N(x) = x.x^q. \ldots .x^{q^{m-1}} = x^{1 + q + \ldots + q^{m-1}} = x^{(q^m - 1)/(q - 1)}$, c.q.f.d.

(ii) Tr est évidemment une forme K-linéaire sur L ; si elle n'était pas surjective, elle serait nulle, et on aurait donc $Tr(x) = F(x) = 0$ pour tout $x \in L$: absurde, puisque $\deg(F) = q^{m-1} < q^m = \mathrm{card}(L)$. Ceci prouve la première partie de (ii), et montre en outre que le noyau de Tr est un hyperplan, dans L ; comme $Tr(y^q - y) = 0$ pour tout $y \in L$, il reste, pour démontrer l'équivalence de (a) et (b), à prouver que l'ensemble des éléments de L de la forme $y^q - y$ est également un hyperplan de L, et il suffit pour cela de remarquer que $y \longmapsto y^q - y$, qui est une application K-linéaire de L dans L, est de rang $m - 1$, puisque son noyau (égal évidemment à K) est de dimension 1.

(iii) N est un homomorphisme du groupe multiplicatif L^* dans le groupe multiplicatif K^* ; comme $q - 1$ divise $q^m - 1$, le théorème 4, appliqué à L, montre que le noyau de N est d'ordre $(q^m - 1)/(q - 1)$; comme L^* est lui-même d'ordre $q^m - 1$, l'image de N est nécessairement d'ordre $q - 1 = \mathrm{card}(K^*)$: d'où la surjectivité de N. Le noyau de N contenant évidemment tout élément de L^* de la forme $y^{q-1} = y^q/y$, et les éléments de cette forme constituant un sous-groupe de L^*, il reste, pour démontrer (iii), à prouver que ce sous-groupe est d'ordre précisément $(q^m - 1)/(q - 1)$: mais il suffit pour cela de remarquer que $y \longmapsto y^{q-1}$ est un homomorphisme de L^* dans L^* dont le noyau est exactement K^*, d'ordre $q - 1$, et dont l'image est donc d'ordre $\mathrm{card}(L^*)/\mathrm{card}(K^*) = (q^m - 1)/(q - 1)$, c.q.f.d.

Remarque. - La surjectivité de la trace résulte évidemment de façon générale du fait que l'extension L/K est séparable.

D'autre part, si, pour tout $y \in L$, on pose $D(y) = y^q - y$ et $\Delta(y) = y^{q-1}$, on voit immédiatement que les parties (ii) et (iii) du théorème 6 équivalent respectivement à dire que

$$0 \longrightarrow K \xrightarrow{\text{incl}} L \xrightarrow{D} L \xrightarrow{Tr} K \longrightarrow 0$$

et

$$1 \longrightarrow K^* \xrightarrow{\text{incl}} L^* \xrightarrow{\Delta} L^* \xrightarrow{N} K^* \longrightarrow 1$$

sont des suites exactes de groupes.