

# Cours ALGEBRE M1

Automne 2017

Vadim Schechtman

## Table de Matières

Noms 2

Chapitre 1. Anneaux, modules, catégories

§Pr. Anneaux, modules, catégories 3

Chapitre 2. Représentations linéaires de groupes finis.

§Rep. Représentations linéaires des groupes finis 7

Chapitre 3. Les corps

§EF. Extensions finies, algébriques 14

§Gal Théorie de Galois 18

§Fin. Corps finis 22

## NOMS

Carl Friedrich GAUSS (1777 - 1855)

Evariste GALOIS (1811 - 1832)

Ferdinand Georg FROBENIUS (1849 - 1917)

Issai SCHUR (1875 - 1941)

## Chapitre 1. ANNEAUX, MODULES, CATEGORIES

### §Pr. Anneaux, modules, catégories

**Pr.1.** *Un anneau* = un anneau associatif avec 1.

*Un anneau commutatif* = un anneau associatif commutatif avec 1.

**Exemple.** Un corps; tous nos corps seront commutatifs, sauf mention contraire explicite.

Soit  $A$  un anneau. Un  $A$ -module (à gauche).

Si  $A$  est un corps, un  $A$ -module est un espace vectoriel sur  $A$ .

Un  $\mathbb{Z}$ -module est la même chose qu'un groupe abélien.

Sous-modules  $N \subset M$  et modules quotients  $M/N$ .

**Exemple.**  $A$ -module libre  $A^{(I)}$  où  $I$  est un ensemble arbitraire. Nous nous intéresserons au cas de  $I$  fini; alors  $A^{(I)} = A^I = A^n$  où  $n = \text{Card } I$ .

**Pr. 2. Catégories.** *Une catégorie*  $\mathcal{C}$ :

une classe des objets  $Ob\mathcal{C}$  (au lieu de  $x \in Ob\mathcal{C}$  on écrit parfois simplement  $x \in \mathcal{C}$ );

pour tous  $x, y \in \mathcal{C}$  un ensemble des morphismes  $Hom(x, y) = Hom_{\mathcal{C}}(x, y)$ ;

les applications de composition

$$Hom(x, y) \times Hom(y, z) \longrightarrow Hom(x, z), (f, g) \mapsto gf \quad (2.1)$$

associatives:  $h(gf) = (hg)f$ ;

pour tout  $x \in \mathcal{C}$  le morphisme identique  $Id_x \in Hom(x, x)$  tels que pour tout  $f \in Hom(x, y)$

$$f \cdot Id_x = Id_y \cdot f = f.$$

Isomorphismes.

**Pr.3. Catégories des  $A$ -modules.**  $Ann$ : la catégorie des anneaux.  $AnnCom$ : la catégorie des anneaux commutatifs.

Pour  $A \in Ann$ ,  $A - Mod$ : la catégorie des  $A$ -modules à gauche.

Cette catégorie est *additive*, ce qui veut dire que  $Hom_A(M, N)$  sont des groupes abéliens et la composition (2.1) est bilinéaire.

Ici une application

$$f : X \times Y \longrightarrow Z$$

des groupes abéliens est dite bilinéaire si

$$\begin{aligned} f(x + x', z) &= f(x, z) + f(x', z); & f(x, z + z') &= f(x, z) + f(x, z'); \\ f(-x, z) &= f(x, -z) = -f(x, z) \end{aligned}$$

Si  $A$  est commutative,  $A - Mod$  est une catégorie  $A$ -linéaire, ce qui veut dire que  $Hom_A(M, N) \in A - Mod$  et les applications (2.1) sont  $A$ -bilinéaires.

Ici une application

$$f : X \times Y \longrightarrow Z$$

des  $A$ -modules est dite  $A$ -bilinéaire si elle est bilinéaire en tant qu'une application de groupes abéliens et en plus

$$f(ax, y) = f(x, ay) = af(x, y), \quad a \in A.$$

Image, noyau et conoyau d'un morphisme  $f : M \longrightarrow N$ .

**Exercice.** Propriétés universelles du noyau et conoyau.

Somme directe de  $A$ -modules.

**Pr.3. Produit tensoriel.** Soit  $A \in AnnCom$ ,  $M, N \in A - Mod$ . Leur produit tensoriel  $M \otimes_A N$  est le  $A$ -module muni d'une application canonique

$$f : M \times N \longrightarrow M \otimes_A N$$

$A$ -bilinéaire qui ait la propriété universelle suivante.

(P) Si  $K \in A - Mod$  et

$$g : M \times N \longrightarrow K$$

est une application  $A$ -bilinéaire, alors il existe l'unique  $h \in Hom(M \otimes_A N, K)$  telle que  $g = hf$ .

Notation: pour  $x \in M, y \in N, x \otimes y := f(x, y)$ .

Si  $A$  est un corps (le seul cas qui nous intéressera pour le moment), alors  $M \otimes_A N$  est caractérisé par la propriété

(P') Si  $M \cong A^n$  avec une base  $e_1, \dots, e_n$  et  $N \cong A^m$  avec une base  $f_1, \dots, f_m$  alors  $M \otimes_A N \cong A^{mn}$  avec une base  $\{e_i \otimes f_j, 1 \leq i \leq n, 1 \leq j \leq m\}$ .

**Construction de  $M \otimes_A N$ .** On prends le  $A$ -module libre  $L$  avec la base  $x \otimes y, x \in M, y \in N$  et on pose  $M \otimes_A N = L/L'$  où  $L' \subset L$  est le sous- $A$ -module engendré par tous

$$\begin{aligned} (x + x') \otimes y - x \otimes y - x' \otimes y, & \quad x \otimes (y + y') - x \otimes y - x \otimes y', \\ (ax) \otimes y - a(x \otimes y), & \quad x \otimes (ay) - a(x \otimes y), \quad a \in A. \end{aligned}$$

**Exercice.** Démontréz que

$$\text{Hom}_A(M \otimes_A N, K) \cong \text{Hom}_A(M, \text{Hom}_A(N, K)).$$

**Pr.4. Foncteurs. Functorialité de  $\text{Hom}$  et  $\otimes$ .**

Un foncteur  $F : \mathcal{C} \rightarrow \mathcal{C}'$ : une application

$$F : \text{Ob } \mathcal{C} \rightarrow \text{Ob } \mathcal{C}',$$

pour tous  $x, y$  des applications

$$F : \text{Hom}_{\mathcal{C}}(x, y) \rightarrow \text{Hom}_{\mathcal{C}'}(x, y)$$

telles que

$$F(\text{Id}_x) = \text{Id}_{F(x)}; F(fg) = F(f)F(g)$$

Transformation naturelle des foncteurs.

Équivalence de catégories.

Bicatégorie des catégories.

Foncteurs fidèles, pleins, pleinement fidèles.

Foncteurs contravariants.

Si  $x, y \in \text{Ob } \mathcal{C}$ , un morphisme  $f : \text{Hom}(x, y)$  induit pour tout  $z$  des applications

$$f_* : \text{Hom}(z, x) \rightarrow \text{Hom}(z, y)$$

et

$$f^* : \text{Hom}(y, z) \rightarrow \text{Hom}(x, z).$$

Donc chaque objet  $z \in \mathcal{C}$  induit les foncteurs

$$\text{Hom}(\cdot, z) : \mathcal{C} \rightarrow \mathcal{C}^{\sim} := \text{Hom}_{\text{cat}}(\mathcal{C}^{\text{opp}}, \text{Ens}) \quad (\text{Pr.4.1})$$

et

$$\text{Hom}(z, \cdot) : \mathcal{C}^{\text{opp}} \rightarrow \text{Hom}_{\text{cat}}(\mathcal{C}, \text{Ens}) \quad (\text{Pr.4.2})$$

**Exercice (lemme de Ionedá)** Les foncteurs (Pr.4.1) et (Pr.4.2) sont pleinement fidèles.

**Pr.5. Algèbre homologique.** Soit  $A \in \text{Ann}$ . Une suite (finie ou infinie) dans  $A - \text{Mod}$

$$C^* : \dots \rightarrow C^{i-1} \xrightarrow{d^{i-1}} C^i \xrightarrow{d^i} C^{i+1} \rightarrow \dots$$

est appelée un *complexe* si  $d^i d^{i-1} = 0$ , i.e.  $\text{Im } d^{i-1} \subset \text{Ker } d^i$  pour tout  $i$ .

Cohomologie:

$$H^i(C^*) = \text{Ker } d^i / \text{Im } d^{i-1}$$

La suite  $C^*$  est appelé exacte en  $C^i$  si  $H^i(C^*) = 0$ ;  $C^*$  appelé exacte si tous  $H^i(C^*) = 0$ .

Donc la suite  $0 \longrightarrow M \xrightarrow{f} N$  (resp.  $M \xrightarrow{f} N \longrightarrow 0$ ) est exacte ssi  $f$  est injectif (resp. surjectif).

Une suite exacte courte:

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0. \quad (5.1)$$

Suites exactes courtes scindées.

**Pr.6. Catégorie  $Vect_K$**  des espaces vectoriels de dimension finie sur un corps  $K$ .

Structure monoïdale symétrique: opérations  $\oplus$  et  $\otimes$  et leurs propriétés de commutativité, associativité et distributivité.

Espace dual  $V^*$ . Isomorphisme

$$\text{Hom}(V_1, V_2) \xrightarrow{\sim} V_1^* \otimes V_2.$$

## Chapitre 2. REPRESENTATIONS LINÉAIRES DE GROUPES FINIS

### §Rep. Représentations linéaires des groupes finis

**Rep. 0. Anneau du groupe.** Soit  $G$  un groupe,  $k$  un anneau commutatif.

L'anneau  $k[G]$  en tant qu'un  $k$ -module est le  $k$ -module libre de base  $e_g$ ,  $g \in G$ . La multiplication  $k[G] \times k[G] \rightarrow k[G]$  est  $k$ -bilineaire, avec

$$e_g \cdot e_h = e_{gh}.$$

Si  $1_G \in G$  est l'élément neutre de  $G$ ,  $e_{1_G}$  est l'unité dans  $k[G]$ .

**Exemple.** (a)  $G = \mu_2 = \{1, \sigma, \sigma^2 = 1\} \cong \mathbb{Z}/2\mathbb{Z}$ . Alors  $k[G] \cong k[T]/(T^2 - 1)$ .

(b) Plus généralement, pour

$$G = \mu_n = \{z \in \mathbb{C} \mid z^n = 1\} = \{1, \zeta, \dots, \zeta^{n-1}\} \cong \mathbb{Z}/n\mathbb{Z}, \quad \zeta = e^{2\pi i/n},$$

$$k[G] \cong k[T]/(T^n - 1).$$

**Exercice.** (a) Montrez que

$$\mathbb{R}[T]/(T^2 - 1) \xrightarrow{\sim} \mathbb{R} \oplus \mathbb{R}, \quad f(T) \mapsto (f(1), f(-1)).$$

(b) Montrez que

$$\mathbb{C}[T]/(T^n - 1) \xrightarrow{\sim} \mathbb{C}^n, \quad f(T) \mapsto (f(1), f(\zeta), \dots, f(\zeta^{n-1})).$$

**Rep. 1.** On va travailler sur le corps de nombres complexes  $\mathbb{C}$ .

Soi  $G$  un groupe. Une représentation de  $G$  est un couple  $(\rho, V)$  où  $V$  est un  $\mathbb{C}$ -espace vectoriel et  $\rho: G \rightarrow GL(V)$  un homomorphisme.

On dit aussi que  $\rho$  est une représentation de  $G$  dans  $V$ .

Une définition équivalente: une représentation de  $G$  dans  $V$  est une action gauche de  $G$  sur  $V$  telle que pour tout  $g \in G$  le morphisme de multiplication

$$g \cdot : V \rightarrow V, \quad x \mapsto gx$$

est  $\mathbb{C}$ -linéaire.

Une définition équivalente: une représentation de  $G$  dans  $V$  est une structure de  $k[G]$ -module à gauche sur  $V$ .

On va considérer que les groupes finis.

Toutes les représentations seront de dimension  $\dim V$  finie; elle est appelée aussi le degré de  $\rho$ .

**Exemple:** représentations de degré 1.

**Exemple.**  $G = \mu_n =$  groupe de déplacements du  $n$ -gone régulier  $\subset SO(2)$ .

**Rep. 2. Catégorie  $Rep(G)$ :** la catégorie des  $G$ -représentations de dimension finie de  $G$ .

Sous-représentations. Irréductibles.

La somme directe. Si  $(V_i, \rho_i) \in Rep(G)$ ,  $i = 1, 2$ , alors leur somme

$$(V_1 \oplus V_2, \rho_1 \oplus \rho_2)$$

est définie par

$$g(x_1, x_2) = (gx_1, gx_2),$$

ou, en plus de details,

$$(\rho_1 \oplus \rho_2)(g)(x_1, x_2) = (\rho_1(g)(x_1), \rho_2(g)(x_2)).$$

**Exemples.** (a) Toutes reps de degré 1 sont irréductibles.

(b)  $G = \mu_2 = \{1, \sigma\}$ ,  $V = \mathbb{R}^2$ ,  $\sigma(x, y) = (y, x)$ .  $V$  est la somme de deux irréductibles de degré 1:

$$V = V_+ \oplus V_-,$$

où

$$V_{\pm} = \mathbb{R} \cdot (1, \pm 1) \subset V$$

**Rep. 3. Structure monoïdale symétrique sur  $Rep(G)$ .**

Sommes et produits tensoriels de représentations.

Si  $\rho_i : G \rightarrow GL(V_i)$ ,  $i = 1, 2$  sont deux représentations, l'espace  $Hom_{\mathbb{C}}(V_1, V_2)$  admet une structure d'une représentation par la règle

$$(g \cdot f)(x) = gf(g^{-1}x)$$

On a

$$Hom_{\mathbb{C}}(V_1, V_2)^G = Hom_G(V_1, V_2)$$

Représentation duale  $V^*$ . Isomorphisme

$$Hom(V_1, V_2) \xrightarrow{\sim} V_1^* \otimes V_2.$$

**Rep. 3.1. Moyennisation.** Si  $V$  est une représentation de  $G$ ,  $n = |G|$ ,

$$m : V \rightarrow V^G, \quad m(x) = \frac{1}{n} \sum_{g \in G} gx$$

D'où:

$$m : Hom_{\mathbb{C}}(V_1, V_2) \rightarrow Hom_G(V_1, V_2)$$



**Rep. 4. Théorème.** Soit  $V$  une  $G$ -représentation,  $i : W \hookrightarrow V$  une sous-représentation. Alors il existe une sous-représentation (dite "supplémentaire")  $W' \subset V$  telle que

$$W \oplus W' \xrightarrow{\sim} V$$

**Preuve.** Choisissons un projecteur  $\mathbb{C}$ -linéaire  $p' : V \rightarrow W$ ,  $p' \circ i = \text{Id}_W$  et posons  $p = m(p')$ . Alors

$$pi(x) = \frac{1}{n} \sum_g gp'g^{-1}i(x) = \frac{1}{n} \sum_g gp'ig^{-1}(x) = x,$$

i.e.  $p$  est un projecteur  $G$ -équivariant. On pose  $W' = \text{Ker}(p)$ .  $\square$

**Rep. 4. Exercice.** Soit  $\rho$  une représentation dans l'espace  $V$ . Choisissons un produit scalaire hermitien  $(,)'$  sur  $V$ . Posons

$$(x, y) = \frac{1}{n} \sum_g (gx, gy)'$$

Montrez que  $(,)$  est un produit scalaire hermitien  $G$ -invariant, i.e.  $(x, y) = (gx, gy)$  pour tous  $g$ . (Notez que "défini positif" implique "non dégénéré".)

En utilisant le complément orthogonal, donnez une autre preuve du Thm Rep. 3.

Corollaire:

**Rep. 5. Théorème de Maschke.** Chaque représentation de  $G$  est une somme directe des représentations irréductibles.

**Rep. 6. Théorème** (lemme de Schur). Soit  $\rho, \rho'$  deux représentations irréductibles. (i) Chaque  $G$ -homomorphisme est soit 0, soit un isomorphisme.

(ii) Chaque  $G$ -isomorphisme  $f : \rho \xrightarrow{\sim} \rho$  est une homothétie (une multiplication par un scalaire). Donc  $\dim_{\mathbb{C}} \text{Hom}(\rho, \rho) = 1$ .

**Preuve.** (ii) Soient  $\rho : G \rightarrow GL(V)$ ,  $\lambda$  une valeur propre de  $f$ ,  $W \subset V$  le sous-espace propre correspondant. Si  $x \in W$ ,

$$f(gx) = gf(x) = \lambda gx,$$

donc  $W$  est une sous-représentation, d'où  $W = V$ .  $\square$

*Issai Schur* (1875, Mogilev, Russie - 1941, Tel Aviv, Palestine) Un grand mathématicien allemand, un élève de *Georg Frobenius* (1849 - 1917). Membre correspondant de l'Académie de Sciences de l'URSS (1929).

*Caractères.*

**Rep. 7. Définition.** Soit  $\rho$  une représentation de  $G$ .

$$\chi_\rho(g) = \text{Tr}\rho(g)$$

Propriétés élémentaires.

(a)

$$\chi_\rho(hgh^{-1}) = \chi_\rho(g)$$

(b) Si  $\rho_1 \cong \rho_2$ ,  $\chi_{\rho_1} = \chi_{\rho_2}$ .

(c)  $\chi_{\rho \oplus \pi} = \chi_\rho + \chi_\pi$ ;  $\chi_{\rho \otimes \pi} = \chi_\rho \chi_\pi$ .

(d) Toutes les valeurs propres de  $\rho(g)$  sont des racines  $n$ -èmes de l'unité,  $n = |G|$ . Donc

$$\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}$$

**Rep. 8.** Soient  $\rho_i : G \rightarrow V_i$  irréductibles,  $f \in \text{Hom}_{\mathbb{C}}(V_1, V_2)$ .

Rappelons que

$$m(f)(x) = \frac{1}{n} \sum_g \rho_2(g) f(\rho_1(g^{-1})x)$$

C'est un opérateur  $G$ -équivariant (on dit aussi "d'entrelacement").

**8.1. Lemme.** (a)  $m(f) = 0$  si  $\rho_i$  ne sont pas isomorphes.

(b) Si  $\rho_1 = \rho_2$ ,  $V = V_1 = V_2$  alors  $m(f)$  est une multiplication par  $\text{Tr}(f)/d$ , où  $d = \dim V$ .

En effet, (a) est clair d'après le lemme de Schur. Dans le cas (b)  $m(f)$  est une multiplication par  $\lambda$ . Or

$$d\lambda = \text{Tr}(m(f)) = n\text{Tr}(f),$$

d'où l'assertion.  $\square$

Écrivons cela sous une forme matricielle. Fixons des bases dans  $V_1$  et  $V_2$ ; par rapport aux ces bases  $\rho_i(g)$ ,  $f$  sont représentés par les matrices  $\rho_i(g)_{pq}$ ,  $f_{rs}$ . Alors  $m(f)$  est représenté par la matrice

$$m(f)_{ij} = \frac{1}{n} \sum_g \rho_2(g)_{ip} f_{pq} \rho_1(g^{-1})_{qj}$$

(la règle d'Einstein: la sommation sur les indices répétés est sous-entendue).

**8.2. Lemme.** Sous les hypothèses du Lemme 8.1, dans le cas (a) on a

$$\frac{1}{n} \sum_g \rho_2(g)_{ip} \rho_1(g^{-1})_{qj} = 0 \quad (\text{Rep.8.1})$$

pour tous  $i, j, p, q$ .

Dans le cas (b)

$$\frac{1}{n} \sum_g \rho(g)_{ip} \rho(g^{-1})_{qj} = \frac{1}{d} \delta_{ij} \delta_{pq} \quad (\text{Rep.8.2})$$

pour tous  $i, j, p, q$ .

**Preuve.** Dans le cas (a)  $m(f)_{ij} = 0$  pour tout  $f = (f_{pq})$ . Maintenant on utilise le fait évident:

si  $(x_i) \in \mathbb{C}^N$  est tel que pour tout  $(f_i) \in \mathbb{C}^N$ ,  $\sum f_i x_i = 0$  alors pour tout  $i$   $x_i = 0$ .

De même, dans le cas (b)

$$m(f)_{ij} = \frac{\text{Tr}(f)}{d} \delta_{ij} = \frac{1}{d} f_{pq} \delta_{pq} \delta_{ij}$$

pour tout  $f$ .  $\square$

**Rep. 9.** Introduisons un produit scalaire hermitien sur l'espace

$$\begin{aligned} \mathbb{C}[G] &= \{f : G \longrightarrow \mathbb{C}\}, \\ (f, g) &= \frac{1}{n} \sum_{x \in G} f(x) \overline{g(x)} \end{aligned} \quad (\text{Rep.9.1})$$

**Rep. 10. Théorème** (relations d'orthogonalité pour les caractères). Soit  $\rho_i, i = 1, 2$  deux représentations irréductibles de  $G$ . Alors

$$(\chi_{\rho_1}, \chi_{\rho_2}) = 0$$

si ils ne sont pas isomorphes.

Pour un  $\rho = \rho_i$

$$(\chi_{\rho}, \chi_{\rho}) = 1$$

**Preuve.** Appliquez (Rep.8.1) et (Rep.8.2).  $\square$

**Rep. 11. Corollaires.** (a) Soit

$$\pi = \oplus \rho_i$$

une décomposition d'une représentation en irréductibles. Alors la multiplicité d'une irréductible  $\rho_i$  dans  $\pi$  est égale à  $(\chi_{\pi}, \chi_{\rho_i})$ .

Donc ce nombre ne dépend pas d'une décomposition.

(b) Deux représentations ayant les mêmes caractères sont isomorphes.

**Rep. 12. Représentation régulière.**  $R = \mathbb{C}[G]$ ; elle a une base  $\{e_g\}_{g \in G}$  telle que

$$\rho(s)e_t = e_{st}$$

Donc son caractère  $\chi_\rho(g) = 0$  si  $g \neq e$  et  $\chi_\rho(e) = n = |G|$ .

**Rep. 12.1. Corollaires.** (a) La multiplicité d'une irréductible  $\rho : G \rightarrow GL(V_\rho)$  dans  $R$  est égale à  $\deg(\rho) = \dim V_\rho$ .

(b) Il existe qu'un nombre fini d'irréductibles non-isomorphes de dimensions  $n_i$ ; on a

$$\sum n_i^2 = n$$

En effet,

$$m(\rho, R) = (\chi_\rho, \chi_R) = \frac{1}{n} \sum_g \chi_\rho(g) \overline{\chi_R(g)} = \frac{1}{n} \chi_\rho(e) \overline{\chi_R(e)} = \chi_\rho(e) = \deg(\rho).$$

*Fonctions centrales et caractères*

**Rep. 13.** Une fonction  $f : G \rightarrow G$  est dit *centrale* si  $f(sts^{-1}) = f(t)$  pour tous  $s, t \in G$ .

L'espace des fonctions cenrales muni du produit scalaire (Rep. 9.1) sera noté  $C(G)$ .

**Rep. 14. Lemme.** Soient  $f$  une fonction centrale,  $\rho : G \rightarrow GL(V)$  une représentation. Définissons

$$\rho_f := \sum_{t \in G} f(t) \rho(t) \in \text{End}(V)$$

(a) L'application  $\rho_f$  est  $G$ -équivariante.

(b) Si  $\rho$  est irréductible de degré ( $= \dim V$ )  $d$ ,  $\rho_f$  est la multiplication par

$$\lambda = \frac{1}{d} \sum_t f(t) \chi_\rho(t) = \frac{n}{d} (\chi, \bar{f})$$

**Preuve.** (a) Exercice (montrez que  $\rho(s) \rho_f \rho(s)^{-1} = \rho_f$ ).

(b) Par le lemme de Schur,  $\rho_f$  est une homothétie avec une constante  $\lambda$ ; sa trace est  $d\lambda$ . D'un autre côté,

$$\text{Tr}(\rho_f) = \sum_t f(t) \text{Tr}(\rho(t)) = n(\chi, \bar{f}),$$

QED.  $\square$

**Rep. 15. Théorème.** *Les caractères des représentations irréductibles  $\chi_1, \dots, \chi_h$  forment une base orthonormée de  $C(G)$ .*

**Preuve.** Nous savons déjà que les caractères sont orthonormés. Il reste à montrer qu'ils engendrent  $C(G)$ .

Soit  $g \in C(G)$  orthogonale aux tous  $\chi_i$ . Montrons que  $g = 0$ . Posons  $f = \bar{g}$ . Pour chaque représentation  $\rho$ , considérons  $\rho_f$  comme dans le Lemme ci-dessus.

Par ce lemme,  $\rho_f = 0$  si  $\rho$  est irréductible, donc pour chaque  $\rho$ .

Maintenant prenons  $\rho = R$  (représentation régulière). Alors

$$0 = \rho_f(e_1) = \sum_t f(t)e_t,$$

d'où  $f(t) = 0$  pour tous  $t$ , donc  $g = 0$ .  $\square$

**Rep. 16. Corollaire.** *Le nombre des représentations irréductibles non-isomorphes =  $\dim C(G)$  = le nombre des classes de conjugaison dans  $G$ .*

**Rep. 17. Exemple - exercice.** Table de caractères de  $G = S_3$  (cf. [Ramis - Warusfel]). On 3 classes de conjugaison dans  $S_3$ :

$$C_0 = \{e\}, C_1 = \{(12), (23), (13)\}, C_3 = \{(123), (132)\}$$

On a deux caractères de degré 1: le trivial  $\chi_0$  et le signe  $\chi_1$ .

De  $6 = 1^2 + 1^2 + 2^2$  on conclut qu'on a encore qu'une irrep de degré 2, de caractère  $\chi_2$ .

La matrice  $C = (\chi_i(C_j))$  (table de caractères):

$$C = \begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & -1 \\ 2 & a & b \end{pmatrix}$$

Relations d'orthogonalité:

$$(\chi_i, \chi_j) = \sum_{k=0}^2 |C_k| \bar{\chi}_i(C_k) \cdot \chi_j(C_k), \quad i \neq j.$$

Il vient,

$$0 = (\chi_1, \chi_3) = 2 + 3a + 2b$$

et

$$0 = (\chi_2, \chi_3) = 2 - 3a + 2b,$$

d'où  $(a, b) = (0, -1)$ .

## Chapitre 3. CORPS

### §EF. Extensions finies, algébriques

**EF.1. Définitions de base.** *Un corps est un anneau  $K$  associatif commutatif avec 1 tel que tout  $x \in K$ ,  $x \neq 0$  est inversible.*

Condition équivalente:  $K$  ne contient pas des idéaux différents de 0 et  $K$ .

**Exemples.**  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ,  $\mathbb{Q}$ , etc.

**Notation.** Si  $K$  est un corps,  $K^*$ , *le groupe multiplicatif de  $K$* , est l'ensemble  $K \setminus \{0\}$  avec la multiplication de  $K$  en tant que la loi de composition.

**Lemme.** *Tout morphisme des corps est injectif.*

En effet, le noyau d'un tel morphisme est un idéal qui ne contient pas 1, donc il est trivial.  $\square$

Soit  $K$  un corps. Considérons l'unique morphisme

$$i : \mathbb{Z} \longrightarrow K, \quad i(n) = n \cdot 1_K$$

Il y a deux possibilités:

(i)  $i$  est injectif. Alors on dit que la caractéristique de  $K$  est égale à 0, Car  $K = 0$ .

Identifions  $\mathbb{Z}$  avec son image dans  $K$ ;  $K$  contient toutes les fractions  $m/n$ ,  $m, n \in \mathbb{Z}$ ,  $n \neq 0$ , donc  $\mathbb{Q} \subset K$ ; c'est le sous-corps minimal contenu dans  $K$ .

(ii) Ker  $i = (p)$  où  $p$  est premier car  $i(\mathbb{Z})$  est intègre. Alors on dit que la caractéristique de  $K$  est égale à  $p$ , Car  $K = p$ .

Dans ce cas  $p \cdot 1_K = 0$  et  $K \supset \mathbb{F}_p = i(\mathbb{Z})$  et  $\mathbb{F}_p$  est le sous-corps minimal contenu dans  $K$ .

Le sous-corps minimal  $K_0 \subset K$  est appelé le sous-corps premier; donc c'est soit  $\mathbb{F}_p$  soit  $\mathbb{Q}$ .

Tout automorphisme  $\sigma$  de  $K$  préserve  $K_0$  et

$$\sigma|_{K_0} = \text{Id}_{K_0}$$

**EF.2. Extensions.** Une extension de corps est une inclusion des corps  $K \subset L$ .

**Notation.** Une extension des corps  $K \subset L$  est parfois notée  $L/K$ . Ce n'est pas une quotient!

*Les sous-corps fixés*

Par  $\text{Aut}(L/K)$  on va noter le groupe d'automorphismes du corps  $L$ ,  $\sigma : L \xrightarrow{\sim} L$  tels que  $\sigma|_K = \text{Id}_K$ .

Si  $H \subset \text{Aut}(L/K)$  est un sous-groupe quelconque, on désigne

$$L^H := \{x \in L \mid \forall \sigma \in H \sigma(x) = x\}$$

C'est un corps,  $K \subset L^H \subset L$ .

*Degré*

On peut multiplier des éléments de  $L$  par des éléments de  $K$ , donc  $L$  est un espace vectoriel sur  $K$ . La dimension de cet espace est appelée *le degré* de l'extension et notée

$$[L : K] := \dim_K L$$

Donc c'est un nombre naturel ou  $\infty$ .

Si  $[L : K] < \infty$ , on dit que l'extension est *finie*.

**Proposition.** Si  $K_1 \subset K_2 \subset K_3$  sont des extension finies, alors

$$[K_3 : K_1] = [K_3 : K_2][K_2 : K_1]$$

**Exemples.**  $\mathbb{Q}(\sqrt{D})$ ,  $\mathbb{Q}(\sqrt{D}, \sqrt{D'})$ . Corps cyclotomiques  $\mathbb{Q}(\zeta_n)$ ,  $\zeta_n = e^{2\pi i/n}$ .

### EF.3. Éléments algébriques.

**EF.3.1. Exercice important.** (a) Montrez que si  $p$  est un nombre premier, alors  $\mathbb{Z}/p\mathbb{Z}$  est un corps.

(b) Soient  $K$  un corps,  $p(x) \in K[x]$   $p(x) \neq 0$ . Montrez que  $p(x)$  est un polynôme irréductible si et seulement si  $K[x]/(p)$  est un corps.

(Utilisez la division euclidienne ou le théorème de Bezout.)

$K \subset E$ ,  $\alpha \in E$  est dit *algébrique sur  $K$*  s'il existe  $f(x) \in K[x]$  tel que  $f(\alpha) = 0$ .

Soient  $K \subset E$  des corps,  $\alpha \in E$ . On désigne par  $K(\alpha) \subset E$  le sous-corps minimal de  $E$  contenant  $K$  et  $\alpha$ . On a

$$K(\alpha) = \{f(\alpha)/g(\alpha) \mid f, g \in K[x], g(\alpha) \neq 0\}$$

Voici une description plus explicite de ce corps.

Considérons le homomorphisme d'anneaux

$$\phi_\alpha : K[x] \longrightarrow E, \quad \phi(x) = \alpha, \quad \phi_K = \text{Id}_K$$

Donc si  $f(x) = \sum b_i x^i$ ,  $b_i \in K$ ,  $\phi_\alpha(f(x)) = f(\alpha)$ .

Soit  $I_\alpha = \text{Ker } \phi_\alpha$ . Puisque  $K[x]$  est un anneau principal,

$$I_\alpha = (p), \quad p \in K[x]$$

Soit

$$K[\alpha] := \phi_\alpha(K[x]) \subset E$$

L'homomorphisme  $\phi_\alpha$  induit un isomorphisme  $K[x]/I_\alpha \xrightarrow{\sim} K[\alpha]$ .

$K[\alpha]$  est un sous-anneau de  $E$  donc intègre, donc  $I_\alpha$  est un idéal premier.

Il y a deux possibilités.

(i)  $I_\alpha = 0$ , i.e. il n'existe pas d'un polynôme  $f(x) \in K[x]$  tel que  $f(\alpha) = 0$ . Dans ce cas  $\alpha$  est appelé *transcendent* sur  $K$ .

**Exemple.**  $K = \mathbb{Q} \subset E = \mathbb{R}$ ,  $\alpha = \pi$ .

Dans ce cas  $\phi_\alpha$  est une inclusion et induit un isomorphisme de corps

$$K(x) := \{f(x)/g(x) \mid f, g \in K[x], g \neq 0\} \xrightarrow{\sim} K(\alpha)$$

Ici  $K(x)$  est l'anneau de fractions d'anneau intègre  $K[x]$ .

(ii)  $I_\alpha = (p(x)) \neq 0$ . Dans ce cas  $\alpha$  est appelé *algébrique* sur  $K$ .

Un générateur  $p(x)$  de  $I_\alpha$  est appelé le *polynôme minimal* de  $\alpha$  sur  $K$  (il est défini à la multiplication par une constante  $c \in K^*$  près).

On a  $p(\alpha) = 0$  et si  $f(x) \in K[x]$ ,  $f(\alpha) = 0$  alors  $p(x) \mid f(x)$ .

Le polynôme  $p(x)$  est irréductible dans  $K[x]$ . Dans ce cas l'anneau quotient  $K[x]/(p)$  est un corps et le morphisme  $\phi_\alpha$  induit l'isomorphisme des corps.

$$\bar{\phi}_\alpha : K[x]/(p(x)) \xrightarrow{\sim} K[\alpha] = K(\alpha)$$

Explicitement, si

$$p(x) = x^n + c_{n-1}x^{n-1} + \dots + c_0$$

alors

$$K(\alpha) \cong \{b_0 + b_1x + b_2x^2 + \dots + b_{n-1}x^{n-1} \mid b_0, \dots, b_{n-1} \in K\}$$

comme les  $K$ -espaces vectoriels, donc

$$[K(\alpha) : K] = n = \deg p$$

**Proposition.** Soient  $\alpha \in E$ ,  $f(x) \in K[x]$  tels que  $f(\alpha) = 0$ . Alors  $f(x)$  est un polynôme minimal de  $\alpha$  si et seulement si  $f$  est irréductible sur  $K$ .

**Exemple.**  $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ .



**EF.4.** Réciproquement, soit  $K$  un corps,  $p(x) \in K[x]$  un polynôme irréductible. L'anneau  $K[x]$  étant principal,  $K' := K[x]/(p(x))$  est un corps.

Soit  $\alpha$  l'image de  $x$  sous la projection canonique

$$K[x] \longrightarrow K[x]/(p(x))$$

Alors  $K' = K(\alpha)$ ,  $[K' : K] = \deg p$ .

### EF.5. Extensions algébriques.

**Théorème.** Soient  $K \subset L$  une extension de corps,  $\alpha \in L$ . Alors  $\alpha$  est algébrique ssi  $\alpha$  est contenu dans une extension finie  $K' \supset K$ .

Une extension  $K \subset L$  est appelé *algébrique* si tout  $\alpha \in E$  est algébrique sur  $K$ .

**Corollaire.** Une extension finie est algébrique.

**Théorème.** Si  $K_1 \subset K_2 \subset K_3$  sont des corps,  $K_i$  algébrique sur  $K_{i-1}$ ,  $i = 2, 3$ , alors  $K_3$  est algébrique sur  $K_1$ .

**Théorème.** Soit  $K \subset L$  une extension de corps. Alors

$$K' = \{\alpha \in L \mid \alpha \text{ est algébrique sur } K\}$$

est un corps.

**EF.6. Les corps algébriquement clôs.** Un corps  $K$  est dit *algébriquement clôs* si chaque  $f(x) \in K[x]$  a une racine  $\alpha \in K$ . Alors chaque  $f$  se décompose en facteurs linéaires.

**Théorème.** Soit  $K \subset L$  une extension de corps avec  $L$  algébriquement clôs. Alors le corps

$$\bar{K} = \{\alpha \in L \mid \alpha \text{ est algébrique sur } K\}$$

est algébrique sur  $K$  et algébriquement clôs.

**Exemple.**  $\mathbb{Q} \subset \bar{\mathbb{Q}} \subset \mathbb{C}$ .

$\bar{\mathbb{Q}}$  est appelé *le corps de nombres algébriques*. Il est dénombrable.

**Théorème.** Chaque corps peut être plongé dans un corps algébriquement clôs.

**Exercice.** Un corps algébriquement clôs est infini.

**EF.7. Théorème.** Soient  $i : K \hookrightarrow K'$  avec  $K'$  algébriquement clôs;  $j : K \hookrightarrow L$  une extension algébrique. Alors il existe  $i' : L \hookrightarrow K'$  telle que  $i = i' \circ j$ .

(Preuve pour  $i$  finie.)

## Gal. Théorie de Galois

### *Extensions normales*

**Gal.1.** Une extension des corps  $K \subset L$  est dite *normale* si chaque polynôme irréductible  $f(x) \in K[x]$  ayant une racine  $\alpha \in L$  se décompose en facteurs linéaires dans  $L$ .

Voici un critère commode.

**Gal.2. Proposition.** *Une extension finie  $K \subset L$  est normale si et seulement si il existe  $f(x) \in K[x]$  tel que (i)*

*$f$  se décompose en facteurs linéaires dans  $L[x]$ :*

$$f(x) = c \prod_{i=1}^n (x - \alpha_i),$$

*tout  $\alpha_i \in L$ ;*

*(ii)  $L$  est engendré sur  $K$  par les racines de  $f$ :  $L = K(\alpha_1, \dots, \alpha_n)$ .*

On dit que  $L$  est le corps de décomposition de  $f(x)$ .

**Gal.3. Exemples.** (i) Chaque extension de degré 2 est normale.

(ii) L'extensions  $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$  et  $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$  sont de degré 2 donc normales, tandis que  $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$  n'est pas normale.

En effet  $f(x) = x^4 - 2$  a une racine  $\sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{2})$  tandis que les autres racines de  $f(x)$  sont complexes et n'appartiennent pas à  $\mathbb{Q}(\sqrt[4]{2})$ .

(iii) L'extension  $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$  n'est pas normale. Le corps de décomposition de  $f(x) = x^3 - 2$  est  $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ .

### *Polynômes et extensions séparables.*

**Gal.4. Exercice.** Soient  $K \subset L$  une extension des corps,  $L$  algébriquement clos,  $f(x) \in K[x]$ . Montrez que  $f(x)$  n'a pas des racines multiples dans  $L$  si et seulement si  $f(x)$  est première à  $f'(x)$  dans  $K[x]$ .

On dit qu'un polynôme  $f(x) \in K[x]$  est séparable si  $f(x)$  est première à  $f'(x)$ .

Soit  $K \subset L$  une extension des corps,  $\alpha \in L$  un élément algébrique sur  $K$ . On dit que  $\alpha$  est séparable sur  $K$  si son polynôme minimal  $f(x) \in K[x]$  est séparable.

Une extension algébrique  $K \subset L$  est appelée *séparable* si chaque  $\alpha \in L$  est séparable sur  $K$ .

**Gal.5. Proposition.** Supposons que  $L = K(\alpha)$ , et soit  $f(x) \in K[x]$  le polynôme minimal de  $\alpha$ . Alors  $L/K$  est séparable ssi  $f(x)$  est séparable.

**Gal.6.** Si  $K \subset K' \subset K''$ , alors  $K''/K$  est séparable ssi  $K''/K'$  et  $K'/K$  sont séparables.

### *Extensions galoisiennes*

**Gal.7.** Une extension finie  $K \subset L$  est appelée *galoisienne* si elle est normale et séparable.

**Gal.8. Corollaire.** Supposons que  $L = K(\alpha)$ , et soit  $f(x) \in K[x]$  le polynôme minimal de  $\alpha$ . Alors  $L/K$  est galoisienne ssi  $f(x)$  est séparable se décompose en facteurs linéaires dans  $L[x]$

Si  $L/K$  est galoisienne,

$$\text{Gal}(L/K) = \text{Aut}(L/K)$$

est appelé *le groupe de Galois de L sur K*.

Son ordre

$$|\text{Gal}(L/K)| = [L : K]$$

Pour une extension finie arbitraire

$$|\text{Aut}(L/K)| \leq [L : K]$$

Par exemple, le groupe  $\text{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$  est trivial.

**Gal.9. Théorème (E.Artin).** Soient  $L$  un corps,  $G$  un groupe fini d'automorphismes de  $L$ ,  $K = L^G$ . Alors l'extension  $L/K$  est galoisienne, et  $[L : K] = |G|$ .

Considérons l'application

$$\gamma : \{ \text{(Sous-groupes } H \subset G = \text{Aut}(L/K)) \} \longrightarrow \{ \text{(Sous-corps } L' : K \subset L' \subset L) \},$$

$$\gamma(H) = L^H$$

**Gal.10. Théorème principal de la Théorie de Galois.** Supposons que l'extension finie  $L/K$  soit galoisienne,  $G = \text{Gal}(L/K)$ . Alors l'application  $\gamma$  est une bijection. L'application inverse associée à un corps intermédiaire  $K \subset L' \subset L$  le groupe

$$G(L/L') := \{ \sigma \in G \mid \sigma|_{L'} = \text{Id}_{L'} \}$$

Si  $H \subset G$  est un sous-groupe, l'extension  $L/L^H$  est galoisienne et

$$\text{Gal}(L/L^H) = H.$$

Un sous-groupe  $H \subset G$  est normal ssi  $L^H/K$  est normale, donc galoisienne, avec

$$\text{Gal}(L^H/K) = G/H$$

En particulier  $L^G = K$ .

**Gal.10. Exemple. Extensions quadratiques.** Soient  $\beta \in K^* \setminus K^{*2}$ ,

$$K(\alpha) = K(\sqrt{\beta}) = K[x]/(x^2 - \beta)$$

Alors  $K(\alpha)/K$  est galoisienne, avec  $G = \text{Gal}(K(\alpha)/K) \cong \mathbb{Z}/2\mathbb{Z}$ . Le seul élément nontrivial  $\sigma \in G$  agit par  $\sigma(\alpha) = -\alpha$ .

**Gal.11. Exemple.**  $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) = K \subset \mathbb{Q}(\sqrt[3]{2}, \zeta_3 \sqrt[3]{2}, \zeta_3^2 \sqrt[3]{2}) = L$ , où  $\zeta_3 = e^{2\pi i/3}$ .

L'extension  $L/K$  est Galoisienne,

$$G = \text{Gal}(L/\mathbb{Q}) \cong S_3,$$

$K/\mathbb{Q}$  correspond à un sous-groupe  $H \subset G$  d'indice 3 qui ne soit pas normal.

**Gal.12. Exemple. Corps cyclotomiques.** Soit  $p$  premier,  $\zeta_p = e^{2\pi i/p}$ . Alors  $f_p(\zeta_p) = 0$  où

$$f_p(x) = 1 + x + \dots + x^{p-1} = \frac{x^p - 1}{x - 1}$$

**Gal.12.1. Lemme.** *Le polynôme  $f_p(x)$  est irréductible sur  $\mathbb{Q}$ .*

**Preuve.** Rappelons le

**Gal.12.2. Critère d'Eisenstein.** *Soit  $f(x) = a_0 + \dots + a_n x^n \in \mathbb{Z}[x]$ ,  $p$  un nombre premier. Supposons que*

- $(a_0, \dots, a_n) = 1$ ;
- $p \nmid a_n$ ;
- $p \mid a_i$  pour  $0 \leq i < n$ ;
- $p^2 \nmid a_0$ .

*Alors  $f(x)$  est irréductible sur  $\mathbb{Q}$ .*

En appliquant ce critère à  $g(x) = f_p(x + 1)$ , on obtient le lemme.  $\square$

Il s'en suit que

$$\mathbb{Q}(\zeta_p) = \mathbb{Q}[x]/(f_p)$$

Ici  $\mathbb{Q}(\zeta_p)$  désigne le sous-corps minimal de  $\mathbb{C}$  contenant  $\zeta_p$ .

Sur  $\mathbb{Q}(\zeta_p)$   $f_p(x)$  se décompose en facteurs linéaires:

$$f_p(x) = \prod_{j=1}^{p-1} (x - \zeta_p^j),$$

donc l'extension  $\mathbb{Q}(\zeta_p)/\mathbb{Q}$  est galoisienne.

Calculons son groupe de Galois

$$G_p = \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = \text{Aut}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$$

Si  $\sigma \in G_p$  alors

$$\sigma(\zeta_p) = \zeta_p^{\phi(\sigma)}$$

avec  $1 \leq \phi(\sigma) \leq p-1$ .

De là on obtient un homomorphisme

$$\phi : G_p \longrightarrow \mathbb{F}_p^*, \sigma \mapsto \phi(\sigma) \pmod{p}$$

On vérifie facilement que c'est un isomorphisme.

**Gal.13 Exercice.** Soit  $\zeta_n = e^{2\pi i/n}$ ; c'est un générateur du groupe

$$\mu_n = \{z \in \mathbb{C} \mid z^n = 1\}$$

Disons que  $x \in \mu_n$  est *une racine primitive n-ème de 1* si  $x$  est un générateur de  $\mu_n$ .

Montrez que  $\zeta_n^j$  est une racine primitive ssi  $(j, n) = 1$ .

**Gal.14. Exercice.** (a) Trouvez le polynôme minimal de  $\alpha = \sqrt{2} + \sqrt{3}$ .

(b) Montrez que  $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ .

(c) En admettant que l'extension  $\mathbb{Q}(\alpha)/\mathbb{Q}$  est galoisienne, calculez  $\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ .

## §Fin. Corps finis

**Fin.1.** Considérons le groupe  $\mathbb{F}_5^*$ . On a  $\text{Card}(\mathbb{F}_5^*)$ , donc a priori ce groupe peut être isomorphe à  $\mathbb{Z}/4\mathbb{Z}$  ou à  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .

Essayons le nombre 2: les restes  $2^a$  modulo 5 pour  $a = 1, 2, 3, 4$  sont 2, 4, 3, 1, donc  $\mathbb{F}_5^*$  est cyclique, avec un générateur  $\bar{2} = 2 \pmod{5}$ .

Cela est un phénomène général.

**Fin.2. Théorème (Euler)** Soient  $F$  un corps,  $A \subset F^*$  un sous-groupe fini. Alors  $A$  est cyclique.

**Fin.2.1. Lemme.** Soient  $A$  un groupe abélien,  $x, y \in A$  des éléments d'ordres  $a, b$ , tels que  $(a, b) = 1$ . Alors  $xy$  a l'ordre  $ab$ .

En effet, si  $B$  (resp.  $C$ ) est un sous-groupe engendré par  $x$  (resp.  $y$ ) alors l'ordre de  $B \cap C$  divise l'ordres de  $B$  et de  $C$ , donc  $B \cap C = \{1\}$ . Si  $(xy)^c = 1$  alors  $x^c, y^c \in B \cap C$  donc  $x^c = y^c = 1$ , donc  $a|c$  et  $b|c$ . Il s'en suit que  $(ab)|c$ , d'où l'assertion.

**Fin.2.2. Lemme.** Soient  $A$  un groupe abélien,  $x, y \in A$  des éléments d'ordres  $a, b$ . Alors il existe un  $z \in A$  d'ordre  $c := \text{ppcm}(a, b)$ .

En effet, on peut trouver des décompositions  $a = a'a''$ ,  $b = b'b''$  avec  $(a', b') = 1$  et  $c = a'b'$  (vérifier!). Alors  $x^{a''}$  (resp.  $y^{b''}$ ) est de l'ordre  $a'$  (resp.  $b'$ ), donc par le lemme précédent  $z = x^{a''}y^{b''}$  est de l'ordre  $c$ .

**Fin.2.3. Corollaire.** Soit  $A$  un groupe abélien fini,  $d$  le maximal des ordres d'éléments de  $A$ . Alors l'ordre de chaque élément de  $A$  divise  $d$ , donc  $x^d = 1$  pour chaque  $x \in C$ .

Revenons à notre théorème. Soit  $d$  le maximal des ordres d'éléments de  $A$ . D'après le corollaire précédent,  $x^d = 1$  pour chaque  $x \in A$ . D'autre part, l'équation  $t^d - 1 = 0$  ne peut pas avoir plus que  $d$  racines dans  $F$ , d'où  $d = \text{Card}(A)$ , donc  $A$  est cyclique.  $\square$

**Fin.3. Théorème (Fermat)** Soit  $F$  un corps de caractéristique  $p > 0$ .

Alors  $(x + y)^p = x^p + y^p$  pour tous  $x, y \in F$ .

En effet,

$$(x + y)^p = \sum_{i=0}^p \binom{p}{i} x^i y^{p-i}$$

Mais

$$\binom{i}{p} \equiv 0(p)$$

pour  $1 \leq i \leq p$  (vérifier!), d'où l'assertion.  $\square$

Il s'en suit que l'application  $\sigma : F \rightarrow F$ ,  $\sigma(x) = x^p$  est un morphisme de corps, nécessairement injectif; de même pour ses itérés  $\sigma^f$ ,  $\sigma^f(x) = x^{p^f}$ ,  $f \geq 1$ .

Le sous-corps fixé  $F_0 = \{x \in F \mid \sigma(x) = x\} \subset F$  contient  $\mathbb{F}_p$  par le petit Fermat. Puisque l'équation  $t^p - t = 0$  ne peut avoir plus que  $p$  racines dans  $F$ , Il s'en suit que  $F_0 = \mathbb{F}_p$ .

**Fin.4.** Soit  $F$  un corps fini. Sa caractéristique est nécessairement un nombre premier  $p$ ; on a  $\mathbb{F}_p \subset F$ . Si le degré  $[F : \mathbb{F}_p]$  est égale à  $f$ , alors  $F$  est un espace vectoriel sur  $\mathbb{F}_p$  de dimension  $f$ , donc  $\text{Card}(F) = p^f$ .

Réciproquement, pour chaque  $f \in \mathbb{Z}$ ,  $f \geq 1$ , on peut construire un corps  $F$  qui ait  $q = p^f$  éléments. Pour le faire, plongeons  $\mathbb{F}_p$  dans un corps  $\Omega$  algébriquement clos. Considérons le morphisme  $\sigma^f : \Omega \rightarrow \Omega$ ,  $\sigma^f(x) = x^q$ . Il est surjectif car  $\Omega$  est algébriquement clos, donc  $\sigma^f$  est un automorphisme de  $\Omega$ .

Considérons son sous-corps fixé  $F = \{x \in \Omega \mid x^q = x\} \subset \Omega$ ; il coïncide avec l'ensemble de racines du polynôme  $f(t) = t^q - t$  dans  $\Omega$ .

**Fin.5. Lemme.** Toutes les racines de  $f(t)$  sont distincts.

En effet, si  $\alpha \in \Omega$  est une racine multiple de  $f(t)$  alors  $f'(\alpha) = 0$  (démontrer!). D'autre part,

$$f'(t) = qt^{q-1} - 1 = -1$$

n'a pas de racines, donc  $f(t)$  n'a pas de racines multiples, cqfd.  $\square$

Ce lemme implique que  $\text{Card}(F) = q$ .

Soit  $F' \subset \Omega$  un sous-corps à  $q$  éléments. On a  $\text{Card}(F'^*) = q-1$ , donc  $x^{q-1} = 1$  pour chaque  $x \in F'$ ,  $x \neq 0$ , donc  $x^q = x$  pour chaque  $x \in F'$ . Il s'en suit que  $F' \subset F$ , donc  $F' = F$ .

Enfin, soit  $K$  un corps arbitraire à  $q$  éléments. Celui-ci est une extension algébrique de  $\mathbb{F}_p$  (de degré  $f$ ). Par la propriété générale, il existe un plongement  $\phi : K \hookrightarrow \Omega$  prolongeant l'inclusion  $\mathbb{F}_p \subset \Omega$ , puisque  $\Omega$  est algébriquement clos. Son image  $\phi(K)$  est un sous-corps à  $q$  éléments, donc  $\phi(K) = F$ . Donc  $\phi : K \xrightarrow{\sim} F$ .

On a prouvé

**Fin.6. Théorème.** Pour chaque nombre premier  $p$  et  $f \in \mathbb{Z}$ ,  $f \geq 1$  il existe un corps à  $q = p^f$  éléments. Ce corps est unique à isomorphisme près.

**Fin.7. Exercice.** Montrer que  $\mathbb{F}_q \subset \mathbb{F}_{q'}$  ssi  $q = p^f$ ,  $q' = p^{f'}$  et  $f|f'$ .

**Fin.8. Théorie de Galois.** Considérons une extension

$$F = \mathbb{F}_q \subset F' = \mathbb{F}_{q'} = \mathbb{F}_{q^n}$$

et l'automorphisme de Frobenius

$$Fr_q : \mathbb{F}_{q'} \xrightarrow{\sim} \mathbb{F}_{q'}, Fr_q(x) = x^q$$

Alors le corps fixe

$$F'^{Fr_q} = F$$

(voire l'argument ci-dessus), et  $Fr_q^n = \text{Id}_{F'}$ .

Plus généralement, si  $m|n$  alors le sous-corps fixe de  $Fr_{q^n} := Fr_q^n$  est le seul sous-corps  $\mathbb{F}_{q^m}$  à  $q^m$  éléments de  $F'$ .

Soit  $G \subset \text{Aut}(F'/F)$  le sous-groupe engendré par  $Fr_q$ ; on a montré que  $G$  est un groupe cyclique à  $n$  éléments.

**Proposition.**  $G = \text{Aut}(F'/F)$ .

**Preuve.** Soit  $\alpha$  un générateur de  $F'^*$ . Alors  $F' = F(\alpha)$ . Soit  $f(x) \in F[x]$  le polynôme minimal de  $\alpha$ ; donc  $\deg f = n$ . Un automorphisme quelconque  $\sigma \in \text{Aut}(F'/F)$  envoie  $\alpha$  sur une autre racine de  $f$  dans  $F'$ . Il s'en suit que

$$\text{Card } \text{Aut}(F'/F) \leq n = [F' : F]$$

(c'est un phénomène général). Or, on a déjà trouvé un sous-groupe  $G$  à  $n$  éléments dans  $\text{Aut}(F'/F)$ , donc  $G = \text{Aut}(F'/F)$ .  $\square$ .

Le polynôme  $g(x) = x^{q^n} - 1 \in F[x]$  se décompose en facteurs linéaires dans  $F'[x]$  et  $F'$  est engendré sur  $F$  par ses racines, donc l'extension  $F'/F$  est normale.

En plus,  $g(x)$  est un polynôme séparable et  $f(x)|g(x)$  donc  $f(x)$  est séparable. Donc l'extension  $F'/F$  est séparable.

Il s'en suit le

**Fin.9. Théorème.** L'extension  $F'/F$  est galoisienne. Le groupe de Galois  $G = \text{Gal}(F'/F)$  est un groupe cyclique à  $n$  éléments engendré par  $Fr_q$ .

On a des bijections des ensembles

$$\{m \in \mathbb{Z} \mid 1 \leq m \leq n, m|n\} \cong \{\text{sous-groupes de } G\} \cong \{\text{sous-corps } F \subset F'' \subset F'\}$$

Sous cette bijection à un nombre  $m|n$  correspond le sous-groupe cyclique

$$H_m = \langle Fr_q^m \rangle \subset G$$



d'ordre  $n/m$ ;  $G/H_m$  est un groupe cyclique d'ordre  $d = n/m$ ,

$$F'' = F'^{H_m} = \mathbb{F}_{q^m},$$

$$H_m = \text{Gal}(F'/F''), \quad G/H_m = \text{Gal}(F''/F).$$

□