VII. EXTENSIONS NORMALES, SÉPARABLES, GALOISIENNES. CORPS FINIS

Séances des 20, 21, 27 et 28 novembre

18. Extensions séparables et théorème de l'élément primitif

18.0. Morphismes d'une extension monogène. — Commençons par rappeler la proposition suivante, déjà énoncée en 16.5 (Chap. VI).

Proposition 18.0. — *Soit* K/k *une extension algébrique monogène, c.-à-d.,* $\mathrm{K} = k(\alpha)$ *avec* α *algébrique sur* k*. Soient* $\mathrm{P} = \mathrm{Irr}_k(\alpha)$*, le polynôme minimal de* α *sur* k*, et* $d = \deg \mathrm{P} = [\mathrm{K} : k]$*. Alors, pour toute extension* L/k*, le nombre de* k*-morphismes* $\mathrm{K} \to \mathrm{L}$ *est égal au nombre de racines distinctes de* P *dans* L*. Par conséquent, on a*

$$\#\,\mathrm{Hom}_{k\text{-}alg.}(\mathrm{K}, \mathrm{L}) \leqslant \deg \mathrm{P} = [\mathrm{K} : k],$$

avec égalité si et seulement si P *a* d *racines distinctes dans* L*.*

Démonstration. — Pour tout k-morphisme $\phi : \mathrm{K} \to \mathrm{L}$, $\phi(\alpha)$ est une racine de P dans L. Réciproquement, comme $\mathrm{K} \cong k[\mathrm{X}]/(\mathrm{P})$, alors toute racine β de P dans L définit un morphisme de k-algèbres $\phi_\beta : \mathrm{K} \to \mathrm{L}$ tel que $\phi_\beta(\alpha) = \beta$, et évidemment ces morphismes sont deux à deux distincts. Ceci prouve la proposition. □

18.1. Polynômes et extensions séparables. —

Définition 18.1. — Soit $\mathrm{P} \in k[\mathrm{X}]$ un polynôme **irréductible**. On dit que P est **séparable sur** k s'il vérifie la propriété suivante : ses racines $\alpha_1, \ldots, \alpha_n$ dans un corps de décomposition K de P sur k sont deux à deux distinctes, c.-à-d., chacune de multiplicité 1.

(0) Version du 28/11/06

Ceci ne dépend pas du corps de décomposition K. En effet, si K' est un autre corps de décomposition, il existe, d'après le théorème 17.2, un k-isomorphisme $\sigma : \mathrm{K} \xrightarrow{\sim} \mathrm{K}'$. On a $\sigma(\mathrm{P}) = \mathrm{P}$, puisque P est à coefficients dans k. D'autre part, on a dans $\mathrm{K}[\mathrm{X}]$, $\mathrm{P} = a(\mathrm{X} - \alpha_1) \cdots (\mathrm{X} - \alpha_n)$, où $a \in k$ est le coefficient dominant de P, et appliquant σ à cette égalité on obtient la décomposition $\mathrm{P} = \sigma(\mathrm{P}) = a(\mathrm{X} - \sigma(\alpha_1)) \cdots (\mathrm{X} - \sigma(\alpha_n))$. Par conséquent, les racines de P dans K' sont les $\sigma(\alpha_i)$, qui sont deux à deux distinctes.

Exemple 18.2. — On verra plus bas que si $\mathrm{car}(k) = 0$, alors tout polynôme irréductible est séparable. D'un autre côté, voici un exemple (en caractéristique $p > 0$) d'un polynôme irréductible non séparable.

Soit $\mathrm{K} = \mathbb{F}_p(\mathrm{T})$ et soit k le sous-corps $\mathbb{F}_p(\mathrm{T}^p)$. Considérons le polynôme

$$\mathrm{P} = \mathrm{X}^p - \mathrm{T}^p \in k[\mathrm{X}].$$

Dans $\mathrm{K}[\mathrm{X}]$ il se factorise en $\mathrm{P} = (\mathrm{X} - \mathrm{T})^p$. Ceci est sa décomposition en facteurs irréductibles dans $\mathrm{K}[\mathrm{X}]$ (qui est factoriel). Comme $\mathrm{T}^i \notin k$ pour $i = 1, \ldots, p-1$, on en déduit que P est **irréductible** dans $k[\mathrm{X}]$, mais il n'est pas séparable, puisque justement il a T comme racine de multiplicité p dans K.

Lemme 18.3. — *Soient* $\mathrm{P} \in k[\mathrm{X}]$ *séparable,* L *une extension de* k*, et* Q *un diviseur de* P *dans* $\mathrm{L}[\mathrm{X}]$*. Alors* Q *est séparable sur* L*.*

Démonstration. — Soit K un corps de décomposition de P sur L. Alors Q est scindé dans L et ses racines sont parmi celles de P donc sont deux à deux distinctes. □

Définition 18.4. — Soit $k \subset \mathrm{K}$ une extension algébrique.

1) On dit que $\alpha \in \mathrm{K}$ est **séparable sur** k si son polynôme minimal $\mathrm{Irr}_k(\alpha)$ est séparable sur k.

2) On dit que l'extension $k \subset \mathrm{K}$ **est séparable** si tout $\alpha \in \mathrm{K}$ est séparable sur k.

Proposition 18.5. — *Soient* $k \subset \mathrm{L} \subset \mathrm{K}$ *des extensions de corps. Si* K/k *est séparable,* L/k *et* K/L *le sont aussi.*

Démonstration. — Il est clair que L/k est séparable ; montrons que K/L l'est aussi. Soit $x \in \mathrm{K}$. Par hypothèse, $\mathrm{Irr}_k(x)$ est séparable. Or, il est multiple, dans $\mathrm{L}[\mathrm{X}]$, de $\mathrm{Irr}_{\mathrm{L}}(x)$. Donc ce dernier est séparable, d'après le lemme précédent. □

On a introduit plus haut la notion de séparabilité pour un polynôme $\mathrm{P} \in k[\mathrm{X}]$ **irréductible**. Pour la suite, il est commode d'étendre cette notion à un polynôme non constant quelconque, de la façon suivante.

Définition 18.6. — Soit $P \in k[X]$, non constant, et soit $P = P_1 \cdots P_r$ sa décomposition en facteurs irréductibles dans $k[X]$. On dit que P est **séparable** sur k si chaque P_i l'est.

Remarque 18.7. — 1) Ainsi, par exemple, les polynômes $(X-1)^3$ et $(X^2+1)^2$ sont séparables sur $\mathbb{Q}$, car leurs facteurs irréductibles le sont.

2) Revenons à l'exemple 18.2, avec $k = \mathbb{F}_p(T^p) \subset K = \mathbb{F}_p(T)$. Alors le polynôme

$$X^p - T^p = (X-T)^p \quad \text{est séparable sur K,}$$

alors qu'il ne l'est pas sur k. Ceci montre que la notion de séparabilité dépend du corps de base et explique la terminologie « séparable sur k ».

18.2. Racines multiples et séparabilité. — Élucidons maintenant la notion de polynôme séparable.

Définition 18.8. — Soit A une k-algèbre. Une **dérivation** de A est un endomorphisme k-linéaire $D : A \to A$ qui vérifie la *règle de Leibniz*, c.-à-d.,

$$\forall\, a, b \in A, \qquad D(ab) = D(a)b + aD(b).$$

Ceci entraîne, en particulier, $D(1) = D(1 \cdot 1) = D(1) + D(1)$, d'où $D(1) = 0$ et, par linéarité, $D(\lambda) = 0$ pour tout $\lambda \in k$.

Un exemple familier de dérivation est fourni par la dérivation des polynômes, bien connue sur $\mathbb{R}$, et qui est définie sur un corps k arbitraire de la façon suivante.

Définition 18.9 **(L'opérateur de dérivation)**. — Soit k un corps. Pour tout élément $P = a_0 + a_1X + \cdots + a_nX^n$ de $k[X]$, on pose

$$P' = a_1 + 2a_2X + \cdots + na_nX^{n-1}.$$

On l'appelle le **polynôme dérivé** de P. On notera D l'application $P \mapsto P'$; on voit facilement que c'est un endomorphisme k-linéaire de $k[X]$.

Lemme 18.10. — *Pour tout* $P, Q \in k[X]$*, on a* $D(PQ) = PD(Q) + D(P)Q$*, c.-à-d.,* $(PQ)' = PQ' + P'Q$.

Démonstration. — Les deux termes de l'égalité à démontrer étant bilinéaires en (P, Q), il suffit de vérifier cette égalité lorsque $P = X^m$ et $Q = X^n$. Dans ce cas, les deux termes valent $(m+n)X^{m+n-1}$. Ceci prouve le lemme. □

Proposition 18.11. — *Soit* $P \in k[X]$ *non constant. Les assertions suivantes sont équivalentes :*

1) P *a une racine multiple dans une extension de k (et donc dans tout corps de décomposition de* P *sur k) ;*

2) P *et* P' *ont une racine commune dans une extension de k ;*

3) *Le* pgcd *de* P *et* P′ *est de degré* $\geqslant 1$.

Démonstration. — Soit K un corps de décomposition de P sur k. Supposons que P ait dans K une racine α de multiplicité $n \geqslant 2$. Alors, $\mathrm{P} = (\mathrm{X}-\alpha)^n\mathrm{Q}$, avec $\mathrm{Q} \in \mathrm{K}[\mathrm{X}]$. D'après le lemme précédent, appliqué dans K[X], on obtient

$$(*) \qquad \mathrm{P}' = n(\mathrm{X}-\alpha)^{n-1}\mathrm{Q} + (\mathrm{X}-\alpha)^n\mathrm{Q}',$$

d'où $\mathrm{P}'(\alpha) = 0$. Ceci montre que 1) ⇒ 2).

Soit D un pgcd de P et P′. D'après le théorème de Bezout, il existe $\mathrm{A}, \mathrm{B} \in k[\mathrm{X}]$ tels que $\mathrm{AP} + \mathrm{BP}' = \mathrm{D}$. Si α est une racine commune de P et P′ dans une extension L de k, c'est aussi une racine de D, d'où $\deg \mathrm{D} \geqslant 1$. Ceci montre que 2) ⇒ 3).

Réciproquement, si D est de degré $\geqslant 1$, il admet une racine α dans une extension L de k, et α est une racine de P et P′, puisque D divise P et P′. Nécessairement, α est une racine multiple de P. En effet, on aurait sinon, dans L[X],

$$\mathrm{P} = (\mathrm{X}-\alpha)\mathrm{Q} \quad \text{avec} \quad \mathrm{Q}(\alpha) \neq 0,$$

d'où, d'après (∗) ci-dessus, $\mathrm{P}'(\alpha) = \mathrm{Q}(\alpha) \neq 0$. Donc, α est une racine de P dans L de multiplicité $\geqslant 2$. Soit K un corps de décomposition de P sur $k(\alpha)$. Alors, K est un corps de décomposition de P sur k, et P a une racine multiple dans K. Ceci prouve 3) ⇒ 1). La proposition est démontrée. □

Corollaire 18.12. — *Soit* $\mathrm{P} \in k[\mathrm{X}]$ **irréductible**. *Alors :* P *est séparable* ⇔ $\mathrm{P}' \neq 0$.

Démonstration. — Soit $\mathrm{D} = \mathrm{pgcd}(\mathrm{P}, \mathrm{P}')$. D'après la proposition précédente, il suffit de montrer que $\deg \mathrm{D} \geqslant 1 \Leftrightarrow \mathrm{P}' = 0$. L'implication ⇐ est évidente. Supposons $\deg \mathrm{D} \geqslant 1$. Comme P est irréductible, D est associé à P donc de degré $\deg \mathrm{P}$. D'autre part, P′ est nul ou bien de degré $< \deg \mathrm{P}$. Comme D divise P′, on a nécessairement $\mathrm{P}' = 0$. Ceci prouve le corollaire. □

Corollaire 18.13. — *Si* $\mathrm{car}(k) = 0$, *tout polynôme est séparable.*

Démonstration. — D'après la définition 18.6, il suffit de montrer que tout polynôme irréductible P est séparable. On peut supposer P unitaire, disons de degré d. Alors le terme dominant de P′ est $d\mathrm{X}^{d-1}$, non nul puisque $\mathrm{car}(k) = 0$. Donc P est séparable, d'après le corollaire précédent. □

18.3. Caractérisation de la séparabilité en termes de morphismes. — On peut caractériser les extensions séparables en termes de morphismes (théorème 18.15 ci-dessous). Ceci sera utile pour démontrer, dans le paragraphe suivant, le théorème de l'élément primitif 18.19 et son corollaire 18.21.

De plus, l'intérêt du théorème 18.15 ci-dessous apparaîtra plus clairement plus tard, lorsqu'on étudiera la théorie de Galois.

Définition 18.14. — Soit K/K_1 une extension de corps et soit $\tau : \mathrm{K}_1 \to \mathrm{L}$ un morphisme de corps (nécessairement injectif !). On note $\mathrm{Hom}_\tau(\mathrm{K}, \mathrm{L})$ l'ensemble des morphismes de corps $\phi : \mathrm{K} \to \mathrm{L}$ tels que $\phi|_{\mathrm{K}_1} = \tau$. Si l'on identifie K_1 à son image $\tau(\mathrm{K}_1)$, ce n'est autre que l'ensemble des K_1-morphismes de K vers L.

***Théorème 18.15* (Séparabilité sur k et k-morphismes)**. — *Soit* K/k *une extension de degré fini.*

1) *Pour toute extension* L/k*, on a l'inégalité :*

$$(*) \qquad \#\,\mathrm{Hom}_{k\text{-}alg.}(\mathrm{K}, \mathrm{L}) \leqslant [\mathrm{K} : k].$$

2) *Si* K/k *est séparable,* $(*)$ *est une égalité lorsque* L *est algébriquement clos.*

3) *S'il existe une extension* L/k *telle que l'égalité ait lieu, alors* K/k *est séparable.*

Démonstration. — Par hypothèse, $\mathrm{K} = k[x_1, \ldots, x_r]$. On va montrer 1) et 2) par récurrence sur r. Supposons $r = 1$, c.-à-d., $\mathrm{K} = k[x]$, et soit P le polynôme minimal de x sur k. D'après la proposition 18.0, le cardinal de $\mathrm{Hom}_{k\text{-alg.}}(\mathrm{K}, \mathrm{L})$ est le nombre de racines distinctes de P dans L, qui est $\leqslant \deg \mathrm{P} = [\mathrm{K} : k]$, d'où l'inégalité $(*)$.

De plus, si x est séparable sur k, l'égalité est obtenue dans $(*)$ si L est un corps de décomposition sur k de P. Ceci prouve 1) et 2) pour $r = 1$. On peut donc supposer $r \geqslant 2$ et le résultat établi pour $r - 1$.

Posons $k_1 = k[x_1]$. Alors $k \subset k_1 \subset \mathrm{K} = k_1[x_2, \ldots, x_r]$. Alors, d'une part,

$$(1) \qquad \#\,\mathrm{Hom}_{k\text{-alg.}}(k_1, \mathrm{L}) \leqslant [k_1 : k].$$

D'autre part, soit $\tau : k_1 \to \mathrm{L}$ un k-morphisme. Par hypothèse de récurrence, appliquée à l'extension K/k_1, on a

$$(2) \qquad \#\,\mathrm{Hom}_\tau(\mathrm{K}, \mathrm{L}) = \#\,\mathrm{Hom}_{k_1\text{-alg}}(\mathrm{K}, \mathrm{L}) \leqslant [\mathrm{K} : k_1].$$

Or, si $\phi : \mathrm{K} \to \mathrm{L}$ est un k-morphisme, alors sa restriction ϕ_1 à k_1 est un k-morphisme, et $\phi \in \mathrm{Hom}_{\phi_1}(\mathrm{K}, \mathrm{L})$. On a donc

$$(3) \qquad \#\,\mathrm{Hom}_{k\text{-alg}}(\mathrm{K}, \mathrm{L}) \leqslant \#\,\mathrm{Hom}_{k\text{-alg}}(k_1, \mathrm{L}) \cdot \#\,\mathrm{Hom}_{k_1\text{-alg}}(\mathrm{K}, \mathrm{L}),$$

avec égalité si et seulement si tout k-morphisme $\tau : k_1 \to \mathrm{L}$ se prolonge en un k-morphisme $\phi : \mathrm{K} \to \mathrm{L}$. Combiné avec (1), (2) et la multiplicativité des degrés, ceci donne :

$$(4) \qquad \#\,\mathrm{Hom}_{k\text{-alg.}}(\mathrm{K}, \mathrm{L}) \leqslant [\mathrm{K} : k_1][k_1 : k] = [\mathrm{K} : k],$$

ce qui prouve l'assertion 1).

Supposons de plus K/k séparable et L algébriquement clos. Alors, d'après le théorème 16.18, tout k-morphisme $k_1 \to \mathrm{L}$ se prolonge en un k-morphisme

$\phi : \mathrm{K} \to \mathrm{L}$, et donc (3) est une égalité. De plus, (1) et (2) sont des égalités d'après le cas $r = 1$ et l'hypothèse de récurrence. Donc (4) est une égalité. Ceci prouve l'assertion 2).

Montrons l'assertion 3). Supposons qu'il existe une extension L/k telle que (4) soit une égalité, et soit $x \in \mathrm{K}$ arbitraire. On peut prendre, dans le raisonnement précédent, $k_1 = k[x]$, et alors l'égalité dans (4) entraîne que les inégalités (1), (2) et (3) sont des égalités. En particulier, on a

$$\#\operatorname{Hom}_{k\text{-alg}}(k[x], \mathrm{L}) = [k[x] : k],$$

et d'après la proposition 18.0 ceci entraîne que x est séparable sur k. Ceci montre que K/k est séparable, et l'assertion 3) est démontrée. □

Théorème 18.16 **(Critère de séparabilité et transitivité)**. — *Soit* K/k *une extension de degré fini.*

1) *Soit* $x \in \mathrm{K}$. *Si* x *est séparable sur* k, *alors l'extension* $k[x]/k$ *est séparable.*

2) **(Transitivité)** *Soit* E *un corps intermédiaire entre* k *et* K. *Si* K/E *et* E/k *sont séparables, alors* K/k *l'est aussi.*

3) **(Critère de séparabilité)** *Si* $\mathrm{K} = k[x_1, \ldots, x_r]$ *avec chaque* x_i *séparable sur* k, *alors* K/k *est séparable.*

Démonstration. — 1) Supposons x séparable et soit L un corps de décomposition sur k de $\operatorname{Irr}_k(x)$. Alors $\operatorname{Irr}_k(x)$ a $\deg_k(x)$ racines distinctes dans L donc, d'après la proposition 16.5, on a

$$\#\operatorname{Hom}_{k\text{-alg.}}(k[x], \mathrm{L}) = \deg_k(x) = [k[x] : k].$$

Par conséquent, d'après le théorème précédent, l'extension $k \subseteq k[x]$ est séparable. Ceci prouve 1).

Soit L une clôture algébrique de K. Puisque E/k et K/E sont séparables alors, d'après le théorème précédent et le théorème 16.18, on a

$$\#\operatorname{Hom}_{k\text{-alg.}}(\mathrm{E}, \mathrm{L}) = [\mathrm{E} : k],$$

et tout k-morphisme $\tau : \mathrm{E} \to \mathrm{L}$ se prolonge en exactement $[\mathrm{K} : \mathrm{E}]$ morphismes $\mathrm{K} \to \mathrm{L}$. Par conséquent, on a

$$\#\operatorname{Hom}_{k\text{-alg.}}(\mathrm{K}, \mathrm{L}) = [\mathrm{K} : \mathrm{E}][\mathrm{E} : k] = [\mathrm{K} : k],$$

et donc, d'après le théorème précédent, l'extension K/k est séparable. Ceci prouve 2).

Enfin, 3) résulte de 1) et 2) par récurrence sur r. □

Corollaire 18.17. — *Soit* $\mathrm{P} \in k[\mathrm{X}]$ *un polynôme séparable, et* K *un corps de décomposition de* P *sur* k. *Alors* K/k *est séparable.*

Démonstration. — On peut supposer P unitaire. Soient $x_1, \ldots, x_r$ les racines de P dans K, alors $\mathrm{K} = k[x_1, \ldots, x_r]$. D'autre part, soit

$$\mathrm{P} = \mathrm{Q}_1 \cdots \mathrm{Q}_n$$

la décomposition de P en facteurs irréductibles, unitaires, dans $k[\mathrm{X}]$. Par hypothèse, chaque Q_j est séparable. Fixons $i \in \{1, \ldots, r\}$ et soit P_i le polynôme minimal de x_i sur k. Comme $\mathrm{P}(x_i) = 0$, alors P_i divise P donc est l'un des Q_j. Ceci montre que chaque x_i est séparable sur k, et donc K/k est séparable, d'après le théorème précédent. □

18.4. Le théorème de l'élément primitif. —

Définition 18.18. — On rappelle qu'une extension K/k est dite **monogène** si K est engendré sur k par un seul élément, c.-à-d., s'il existe $\xi \in \mathrm{K}$ tel que $\mathrm{K} = k(\xi)$. Dans ce cas, on dit que ξ est un **élément primitif** de K/k.

Théorème 18.19 **(Théorème de l'élément primitif)**. — *Soit* K/k *une extension* **séparable de degré fini**. *Alors* K *admet un élément primitif sur* k.

Démonstration. — On verra dans la section 20 que si k est un corps fini et K/k une extension de degré fini, alors le groupe multiplicatif $\mathrm{K}^\times$ est cyclique, et donc $\mathrm{K} = k[\xi]$ pour tout générateur ξ de $\mathrm{K}^\times$.

On peut donc supposer k infini. Posons $n = [\mathrm{K} : k]$ et soit L une clôture algébrique de K. Comme K/k est séparable, il existe des k-morphismes $\mathrm{K} \to \mathrm{L}$ deux à deux distincts $\tau_1, \ldots, \tau_n$. Alors $\mathrm{Ker}(\tau_i - \tau_j)$ est un sous-espace propre de K, pour tout $i \neq j$.

Lemme 18.20. — *Un espace vectoriel* V *sur un corps infini* k *n'est pas réunion finie de sous-espaces propres* $\mathrm{V}_1, \ldots, \mathrm{V}_t$.

Démonstration. — C'est clair si $t = 1$. Donc on peut supposer $t \geqslant 2$ et le résultat établi pour $t - 1$. Alors, il existe $u, v \in \mathrm{V}$ tels que $u \notin \mathrm{V}_t$ et $v \notin \mathrm{V}_1 \cup \cdots \cup \mathrm{V}_{t-1}$. Supposons

$$\mathrm{V} = \mathrm{V}_1 \cup \cdots \cup \mathrm{V}_t.$$

Alors $v \in \mathrm{V}_t$. Comme l'ensemble des $x_\mu := u + \mu v$, pour $\mu \in k$, est infini, il existe $\mu \neq \nu$ dans k tels que x_μ et x_ν appartiennent au même V_j. On ne peut avoir $j = t$, car sinon on aurait $u \in \mathrm{V}_t$, une contradiction. Donc $j < t$, et V_j contient $x_\mu - x_\nu = (\mu - \nu)v$ donc aussi v, une contradiction. Ceci prouve le lemme. □

On peut maintenant achever la preuve du théorème de l'élément primitif. D'après le lemme, il existe $x \in \mathrm{K}$ n'appartenant à aucun des $\mathrm{Ker}(\tau_i - \tau_j)$.

Alors, les $\tau_i(x)$ sont deux à deux distincts. Comme ce sont des racines, dans L, de $\mathrm{Irr}_k(x)$, ceci entraîne $\deg_k(x) \geqslant n$, et donc

$$n \leqslant \deg_k(x) = [k(x) : k] \leqslant [\mathrm{K} : k] = n.$$

Il en résulte que $k(x) = \mathrm{K}$. Le théorème est démontré. □

On aura besoin plus loin du raffinement suivant.

Proposition 18.21. — *Soit* K/k *une extension algébrique séparable. On suppose qu'il existe* $n \in \mathbb{N}^*$ *tel que* $\deg_k(x) \leqslant n$ *pour tout* $x \in \mathrm{K}$. *Alors* $[\mathrm{K} : k]$ *est de degré fini* $\leqslant n$, *donc* K/k *admet un élément primitif.*

Démonstration. — Prenant n le plus petit possible, on peut supposer qu'il existe $x \in \mathrm{K}$ tel que $\deg_k(x) = n$. Soit $y \in \mathrm{K}$ arbitraire. Comme l'extension $k \subseteq k[x, y]$ est séparable de degré fini, elle admet un élément primitif z. On a donc $k[x] \subseteq k[z]$, et cette inclusion est une égalité par maximalité de $\deg_k(x)$. Donc $k[x] = k[z] = k[x, y]$, d'où $y \in k[x]$. Ceci montre que $\mathrm{K} = k[x]$. Donc $[\mathrm{K} : k] = n$ et x est un élément primitif de K/k. □

Pour terminer cette section, signalons aussi la proposition suivante.

Proposition 18.22. — *Soit* K/k *une extension de degré fini. Alors* K/k *admet un élément primitif* $\Leftrightarrow$ *le nombre d'extensions intermédiaires est fini.*

Démonstration. — $\Rightarrow$ Supposons $\mathrm{K} = k[\xi]$ et soit $\mathrm{P} = \mathrm{Irr}_k(\xi)$. Soit $k \subseteq \mathrm{L} \subseteq \mathrm{K}$ une extension intermédiaire et soit $\mathrm{Q} = \mathrm{Irr}_{\mathrm{L}}(\xi)$. Alors $[\mathrm{K} : \mathrm{L}] = \deg \mathrm{Q}$. Observons que Q divise P dans L[X], donc a fortiori dans K[X]. Par conséquent, il n'y a qu'un nombre fini de possibilités pour Q.

Soit $\mathrm{L}' \subseteq \mathrm{L}$ le sous-corps de L engendré sur k par les coefficients de Q. Comme Q est irréductible dans L[X], il l'est aussi dans L'[X]. Par conséquent, $\mathrm{K} = \mathrm{L}'[\xi]$ est de degré $\deg \mathrm{Q}$ sur L'. On a donc

$$[\mathrm{K} : \mathrm{L}] = \deg \mathrm{Q} = [\mathrm{K} : \mathrm{L}'],$$

d'où $[\mathrm{L} : \mathrm{L}'] = 1$, c.-à-d., $\mathrm{L} = \mathrm{L}'$. Ceci montre que L est entièrement déterminé par la donnée de Q. Comme il n'y a qu'un nombre fini de tels Q, ceci prouve la finitude du nombre des extensions intermédiaires.

Démontrons maintenant l'implication $\Leftarrow$ sous l'hypothèse que k est **infini**. (On verra le cas des corps finis dans la section 20).

Choisissons un élément $\xi \in \mathrm{K}$ tel que $\deg_k(\xi)$ soit maximal, c.-à-d., tel que $k[\xi]$ soit de degré maximal parmi les extensions monogènes contenues dans K. Ceci est possible puisque K est de degré fini sur k. On va montrer que $k[\xi] = \mathrm{K}$.

Soit $\alpha \in \mathrm{K}$. Pour t variant dans k, posons $\xi_t = \xi + t\alpha$ et notons L_t le sous-corps de K engendré par ξ_t. Ces corps sont en nombre fini et donc, k étant

supposé infini, il existe des éléments $s \neq t$ dans k tels que $\mathrm{L}_s = \mathrm{L}_t$. Ce corps contient alors $(s-t)\alpha$, donc α, et aussi ξ. Donc,

$$k[\xi] \subseteq k[\xi, \alpha] \subseteq k[\xi_s].$$

La maximalité de $\deg_k(\xi)$ entraîne alors que les inclusions ci-dessus sont des égalités, d'où $\alpha \in k[\xi]$. Comme $\alpha \in \mathrm{K}$ était arbitraire, ceci montre que $k[\xi] = \mathrm{K}$. Le théorème est démontré. □

Remarque 18.23. — Soit $\mathrm{K} = \mathbb{F}_p(\mathrm{X}, \mathrm{Y})$ le corps des fractions rationnelles à deux variables sur $\mathbb{F}_p$, et soit k le sous-corps engendré par X^p et Y^p. On peut montrer que $[\mathrm{K} : k] = p^2$ et que tout $\alpha \in \mathrm{K}$ vérifie $\alpha^p \in k$, et donc $[k[\alpha] : k] \leqslant p$ (et $= p$ si $\alpha \notin k$). Ceci montre que l'extension $k \subset \mathrm{K}$ n'est pas monogène (car de degré p^2), donc admet une infinité de corps intermédiaires.

19. Extensions normales et galoisiennes

19.1. Extensions normales. —

Définition 19.1. — Soit K/k une extension algébrique. On dit que K/k est une extension **normale**, ou **quasi-galoisienne**, si : pour tout $\alpha \in \mathrm{K}$, le polynôme minimal $\mathrm{Irr}_k(\alpha)$ a toutes ses racines dans K.

Proposition 19.2. — *Soit* $\mathrm{P} \in k[\mathrm{X}]$ *de degré* $n \geqslant 1$ *et soit* K *un corps de décomposition de* P *sur* k. *L'extension* K/k *est quasi-galoisienne.*

Démonstration. — Soit $\alpha \in \mathrm{K}$ et soit $\mathrm{S} = \mathrm{Irr}_k(\alpha)$ son polynôme minimal sur k. Soit L un corps de décomposition sur K de S. Alors PS a toutes ses racines dans L et celles-ci engendrent L sur k. Par conséquent, L est un corps de décomposition de PS sur k. Montrons que $\mathrm{L} = \mathrm{K}$.

Soit β une racine de S dans L. D'après le théorème 16.1, il existe un (unique) k-isomorphisme $\tau : k[\alpha] \xrightarrow{\sim} k[\beta]$ tel que $\tau(\alpha) = \beta$. De plus, d'après le théorème d'unicité (17.3), τ se prolonge en un k-automorphisme σ de L.

Soient $x_1, \ldots, x_m$ les racines distinctes de P dans K ; alors K, resp. $\sigma(\mathrm{K})$, est le sous-corps de L engendré par les x_i, resp. les $\sigma(x_i)$. Or, pour chaque i, $\sigma(x_i)$ est une racine de $\sigma(\mathrm{P}) = \mathrm{P}$. On en déduit que σ induit une bijection f de $\{1, \ldots, m\}$ telle que $\sigma(x_i) = x_{f(i)}$, pour $i = 1, \ldots, m$. Il en résulte que $\sigma(\mathrm{K}) = \mathrm{K}$. Comme $\sigma(\alpha) = \tau(\alpha) = \beta$, on obtient ainsi que $\beta \in \mathrm{K}$. Ceci montre que S a toutes ses racines dans K, et donc $\mathrm{L} = \mathrm{K}$. La proposition est démontrée. □

19.2. Le groupe des k-automorphismes d'une extension. —

Définition 19.3. — 1) Soit K/k une extension algébrique. On note $\mathrm{Aut}(\mathrm{K}/k)$ le groupe des k-automorphismes de K, c.-à-d.,

$$\mathrm{Aut}(\mathrm{K}/k) = \{g \in \mathrm{Aut}(\mathrm{K}) \mid g(\lambda) = \lambda, \quad \forall\, \lambda \in k\}.$$

Si $[\mathrm{K} : k] < \infty$, il résulte du théorème 18.15 que $\#\,\mathrm{Aut}(\mathrm{K}/k) \leqslant [\mathrm{K} : k]$.

2) Posons $\mathrm{G} = \mathrm{Aut}(\mathrm{K}/k)$ et soit $\alpha \in \mathrm{K}$. L'ensemble $\{g(\alpha) \mid g \in \mathrm{G}\}$ des transformés de α par les éléments de G s'appelle **l'orbite** de α sous l'action de G, ou simplement la G-orbite de α, et se note $\mathrm{G}\alpha$. D'autre part,

$$\mathrm{G}_\alpha := \{g \in \mathrm{G} \mid g(\alpha) = \alpha\}$$

est un **sous-groupe** de G, appelé le **stabilisateur** de α. On le note parfois $\mathrm{Stab}_\mathrm{G}(\alpha)$. L'application $\mathrm{G} \to \mathrm{G}\alpha$, $g \mapsto g(\alpha)$ induit une **bijection**

$$\mathrm{G}/\mathrm{G}_\alpha \xrightarrow{\sim} \mathrm{G}\alpha,$$

où $\mathrm{G}/\mathrm{G}_\alpha$ désigne l'ensemble des classes à gauche $g\mathrm{G}_\alpha$, pour $g \in \mathrm{G}$.

Proposition 19.4. — *Soit* K/k *une extension algébrique et soit* $\alpha \in \mathrm{K}$.

1) *Pour tout* $g \in \mathrm{Aut}(\mathrm{K}/k)$, $g(\alpha)$ *est racine de* $\mathrm{Irr}_k(\alpha)$.

2) *Posons* $\mathrm{G} = \mathrm{Aut}(\mathrm{K}/k)$. *L'orbite* $\mathrm{G}\alpha$ *est un ensemble fini de cardinal* $\leqslant \deg_k(\alpha)$, *et* $\mathrm{Irr}_k(\alpha)$ *est divisible par le polynôme*

$$\prod_{\beta \in \mathrm{G}\alpha} (\mathrm{X} - \beta).$$

Démonstration. — Posons $\mathrm{P} = \mathrm{Irr}_k(\alpha)$ et écrivons $\mathrm{P} = \mathrm{X}^d + a_1\mathrm{X}^{d-1} + \cdots + a_d$, où $d = \deg_k(\alpha)$. Soit $g \in \mathrm{Aut}(\mathrm{K}/k)$. Alors

$$0 = g(\mathrm{P}(\alpha)) = g(\alpha)^d + a_1(g(\alpha))^{d-1} + \cdots + a_d = \mathrm{P}(g(\alpha)).$$

Ceci montre que $g(\alpha)$ est racine de P.

Par conséquent, $\mathrm{X} - g(\alpha)$ divise P, pour tout $g \in \mathrm{G} = \mathrm{Aut}(\mathrm{K}/k)$. Or, d'après l'unicité de la décomposition en facteurs irréductibles, P a au plus d diviseurs irréductibles distincts. Il en résulte que l'orbite $\mathrm{G}\alpha$ est finie, de cardinal $\leqslant d$, et que P est divisible par le produit des $\mathrm{X} - \beta$, pour $\beta \in \mathrm{G}\alpha$. La proposition est démontrée. □

Remarque 19.5. — Au vu de la proposition précédente, on est conduit à se demander si, pour tout $\alpha \in \mathrm{K}$, on a l'égalité

$$(*) \qquad \mathrm{Irr}_k(\alpha) = \prod_{\beta \in \mathrm{G}\alpha} (\mathrm{X} - \beta) \quad ?$$

En cas de réponse positive, on obtiendrait que la connaissance du groupe G (et de son action sur K) permet de déterminer, pour tout $\alpha \in \mathrm{K}$, le polynôme minimal $\mathrm{Irr}_k(\alpha)$ et donc la structure du sous-corps $k[\alpha] \subset \mathrm{K}$.

On va voir dans un instant qu'il faut imposer certaines hypothèses, assez naturelles, sur l'extension $k \subset \mathrm{K}$ pour que $(*)$ soit vraie. On verra ensuite que, sous ces hypothèses, la structure du groupe G et des ses sous-groupes détermine complètement la structure de l'extension K/k et des sous-corps intermédiaires.

Exemples 19.6. — 1) Une première obstruction, évidente, à $(*)$ est que K peut ne pas contenir suffisamment de racines de $\mathrm{Irr}_k(\alpha)$. Par exemple, soient $k = \mathbb{Q}$, $\mathrm{P} = \mathrm{X}^3 - 2$ et ξ l'une quelconque des racines de P dans $\mathbb{C}$. On a vu dans l'exemple 16.6 que ξ est la seule racine de P dans $\mathbb{Q}[\xi]$. Donc $g(\xi) = \xi$, pour tout $g \in \mathrm{G} := \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}[\xi])$, et comme $\mathbb{Q}[\xi]$ est engendré sur $\mathbb{Q}$ par ξ, on obtient que $\mathrm{G} = \{1\}$.

En fait, si $(*)$ est vérifiée, alors $\mathrm{Irr}_k(\alpha)$ a toutes ses racines dans K. Donc, pour que $(*)$ soit vérifiée pour tout $\alpha \in \mathrm{K}$, il est **nécessaire** de supposer que l'extension K/k soit **quasi-galoisienne**.

2) Une autre obstruction, plus subtile, est la suivante. Le terme de droite dans $(*)$ est un polynôme dont les racines sont deux à deux distinctes. Donc, l'égalité dans $(*)$ entraîne que α est séparable sur k. Ceci justifie, *a posteriori*, l'étude des polynômes et extensions séparables faite dans la section précédente.

19.3. Extensions galoisiennes. —

Définition 19.7. — Soit K/k une extension de degré fini. On dit que K/k est **galoisienne** si $\#\,\mathrm{Aut}(\mathrm{K}/k) = [\mathrm{K} : k]$. Dans ce cas, $\mathrm{Aut}(\mathrm{K}/k)$ est noté $\mathrm{Gal}(\mathrm{K}/k)$. De plus, pour tout $\alpha \in \mathrm{K}$, les éléments $g(\alpha)$, pour $g \in \mathrm{Gal}(\mathrm{K}/k)$, sont appelés les **conjugués** sur k de α (dans K).

Théorème 19.8 **(Caractérisation des extensions galoisiennes)**
Soit K/k *une extension de degré fini. Les conditions suivantes sont équivalentes :*

1) K/k *est* **galoisienne**, *c.-à-d.,* $\#\,\mathrm{Aut}(\mathrm{K}/k) = [\mathrm{K} : k]$ *;*

2) K/k *est* **normale** *et* **séparable** *;*

3) K *est le corps de décomposition sur* k *d'un polynôme séparable.*

Sous ces conditions, pour tout $\alpha \in \mathrm{K}$ *on a*

$$\mathrm{Irr}_k(\alpha) = \prod_{\beta \in \mathrm{G}\alpha} (\mathrm{X} - \beta).$$

Démonstration. — On a 3) $\Rightarrow$ 2) d'après la proposition 19.2 et le corollaire 18.17. L'implication 2) $\Rightarrow$ 3) est facile : écrivons $\mathrm{K} = k[x_1, \ldots, x_n]$ et notons P_i le polynôme minimal de x_i sur k. Comme K/k est séparable et normale, alors chaque P_i est séparable et a toutes ses racines dans K. Par conséquent, $\mathrm{P} = \mathrm{P}_1 \cdots \mathrm{P}_r$ est séparable sur k, et K est un corps de décomposition de P sur k.

Montrons que 2) $\Rightarrow$ 1). Supposons K/k normale et séparable et notons $\mathrm{G} = \mathrm{Aut}(\mathrm{K}/k)$ et $n = [\mathrm{K} : k]$. Soit L une clôture algébrique de K. D'après le théorème 18.15, il y a exactement n k-morphismes $g_1, \ldots, g_n$ de K dans L, et l'on a

$$\#\mathrm{G} \leqslant n = [\mathrm{K} : k].$$

L'égalité à établir est donc équivalente au fait que chaque g_i soit dans G, c.-à-d., applique K sur lui-même.

D'après le théorème de l'élément primitif, il existe $\xi \in \mathrm{K}$ tel que $\mathrm{K} = k[\xi]$. Soit P son polynôme minimal sur k. Fixons $i \in \{1, \ldots, n\}$. Alors $g_i(\xi)$ est racine de $g_i(\mathrm{P}) = \mathrm{P}$. Comme K/k est normale, P a toutes ses racines dans K, d'où $g_i(\xi) \in \mathrm{K}$ et donc $g_i(\mathrm{K}) \subseteq \mathrm{K}$. De même, on a $g_i^{-1}(\mathrm{K}) \subseteq \mathrm{K}$, d'où l'égalité

$$g_i(\mathrm{K}) = \mathrm{K}.$$

Il en résulte que $\mathrm{G} = \{g_1, \ldots, g_n\} = \mathrm{Hom}_{k\text{-alg}}(\mathrm{K}, \mathrm{L})$ est de cardinal $n = [\mathrm{K} : k]$, c.-à-d., K/k est galoisienne. Remarquons que le résultat établi montre que pour toute extension algébrique L/K, tout k-morphisme ϕ de K dans L applique nécessairement K dans lui-même. En effet, on peut plonger L dans une clôture algébrique L$'$ et considérer ϕ comme un k-morphisme $\mathrm{K} \to \mathrm{L}'$, d'où alors $\phi(\mathrm{K}) = \mathrm{K}$.

Montrons que 1) $\Rightarrow$ 2). Supposons K/k galoisienne, c.-à-d., supposons que $\mathrm{G} = \mathrm{Aut}(\mathrm{K}/k)$ soit de cardinal $n = [\mathrm{K} : k]$. Alors, d'après le théorème 18.15, K/k est séparable. Montrons que K/k est normale.

Soient $\alpha \in \mathrm{K}$ et P son polynôme minimal sur k. Soit L une clôture algébrique de K et soit β une racine de P dans L. Montrons que $\beta \in \mathrm{K}$.

D'après la proposition 16.5 (ou 18.0), il existe un (unique) k-isomorphisme

$$\tau : k[\alpha] \xrightarrow{\sim} k[\beta] \qquad \text{tel que} \quad \tau(\alpha) = \beta.$$

Comme L est algébriquement clos alors, d'après le théorème 16.18, τ se prolonge en un k-morphisme $\sigma : \mathrm{K} \to \mathrm{L}$. Or, d'après l'hypothèse, d'une part, et le théorème 18.15, d'autre part, on a l'égalité (1) et l'inégalité (2) ci-dessous :

$$[\mathrm{K} : k] \overset{(1)}{=} \#\,\mathrm{Aut}(\mathrm{K}/k) \overset{(*)}{\leqslant} \#\,\mathrm{Hom}_{k\text{-alg}}(\mathrm{K}, \mathrm{L}) \overset{(2)}{\leqslant} [\mathrm{K} : k].$$

Donc (2) est une égalité, ainsi que l'inégalité intermédiaire $(*)$. Donc notre σ ci-dessus appartient à $\mathrm{Aut}(\mathrm{K}/k)$, c.-à-d., applique K sur K. Donc

$$\beta = \sigma(\alpha) \in \mathrm{K}.$$

Ceci montre que K/k est normale, et achève la preuve de l'implication 1) $\Rightarrow$ 2), et du théorème. □

Lemme 19.9. — *Soient* R *un anneau et* τ *un automorphisme de* R. *Alors* τ *s'étend en un automorphisme* ϕ_τ *de* R[X], *défini par*

$$\phi_\tau(\mathrm{P}) = \tau(a_0) + \cdots + \tau(a_d)\mathrm{X}^d \qquad \textit{si} \quad \mathrm{P} = a_0 + \cdots + a_d\mathrm{X}^d;$$

et l'on a : $\phi_\tau(\mathrm{P}) = \mathrm{P} \Leftrightarrow \tau(a_i) = a_i$*, pour* $i = 0, \ldots, d$*. Par abus de notation, on écrira simplement* τ *au lieu de* ϕ_τ*.*

Démonstration. — On vérifie facilement que la formule indiquée définit un endomorphisme d'anneau de R[X], et c'est un automorphisme dont l'inverse est $\phi_{\tau^{-1}}$. La deuxième assertion est claire. □

***Théorème 19.10* (Artin).** — *Soient* K *un corps et* G *un sous-groupe fini de* Aut(K)*. Posons*

$$\mathrm{K}^{\mathrm{G}} = \{x \in \mathrm{K} \mid g(x) = x, \quad \forall\, g \in \mathrm{G}\};$$

c'est un sous-corps de K*. Alors, l'extension* $\mathrm{K}/\mathrm{K}^{\mathrm{G}}$ *est galoisienne, et l'on a*

$$\mathrm{Gal}(\mathrm{K}/\mathrm{K}^{\mathrm{G}}) = \mathrm{G} \qquad \textit{et} \qquad [\mathrm{K} : \mathrm{K}^{\mathrm{G}}] = \#\mathrm{G}.$$

Démonstration. — Il est clair que K^{G} est un sous-corps de K. Montrons que l'extension $\mathrm{K}/\mathrm{K}^{\mathrm{G}}$ est galoisienne. Soit $\alpha \in \mathrm{K}$; notons $\mathrm{A} = \mathrm{G}\alpha$ son orbite son G et soit $\mathrm{P} = \mathrm{P}_\alpha$ le polynôme suivant :

$$\prod_{\beta \in \mathrm{A}} (\mathrm{X} - \beta) \in \mathrm{K}[\mathrm{X}].$$

Alors, pour tout $g \in \mathrm{G}$, l'on a

$$g(\mathrm{P}) = \prod_{\beta \in \mathrm{G}\alpha} (\mathrm{X} - g(\beta)) = \prod_{\gamma \in \mathrm{A}} (\mathrm{X} - \gamma) = \mathrm{P},$$

et donc P est à coefficients dans K^{G}. Notons $k = \mathrm{K}^{\mathrm{G}}$ et soit $\mathrm{Irr}_k(\alpha)$ le polynôme minimal de α sur k. Posons, pour un instant, $\mathscr{G} = \mathrm{Aut}(\mathrm{K}/k)$. Comme $k = \mathrm{K}^{\mathrm{G}}$, alors $\mathrm{G} \subseteq \mathscr{G}$. On va voir plus bas que $\mathrm{G} = \mathscr{G}$. Commençons par la proposition suivante.

Proposition 19.11. — *On a* $\mathrm{Irr}_k(\alpha) = \mathrm{P}_\alpha = \prod_{\beta \in \mathrm{A}} (\mathrm{X} - \beta)$*, et donc* α *est séparable sur* k *et l'extension* K/k *est galoisienne.*

Démonstration. — On a $\mathrm{P}_\alpha \in k[\mathrm{X}]$ et $\mathrm{P}_\alpha(\alpha) = 0$, donc P_α est multiple de $\mathrm{Irr}_k(\alpha)$. D'autre part, d'après la proposition 19.4, $\mathrm{Irr}_k(\alpha)$ est divisible par le polynôme

$$\prod_{\gamma \in \mathscr{G}\alpha} (\mathrm{X} - \gamma),$$

qui est de degré $\geqslant \#\mathrm{G}\alpha$, puisque $\mathrm{G} \subseteq \mathscr{G}$. Il en résulte que

$$\mathrm{P}_\alpha = \mathrm{Irr}_k(\alpha) \qquad \text{et} \qquad \mathrm{G}\alpha = \mathscr{G}\alpha.$$

Donc $\mathrm{Irr}_k(\alpha)$ a des racines simples, toutes dans K, et ceci montre que l'extension K/k est séparable et normale, donc galoisienne (d'après 19.8). Ceci prouve la proposition. □

Achevons maintenant la démonstration du théorème d'Artin. Posons $n = [\mathrm{K} : k]$. Comme $\mathrm{G} \subseteq \mathscr{G} = \mathrm{Gal}(\mathrm{K}/k)$, on a, d'après le théorème 18.15,

$$\#\mathrm{G} \leqslant \#\mathscr{G} \leqslant [\mathrm{K} : k] = n.$$

De plus, pour tout $\alpha \in \mathrm{K}$, on vient de voir que

$$\deg_k(\alpha) = \deg \mathrm{P}_\alpha = \#\mathrm{G}\alpha \leqslant \#\mathrm{G}.$$

Donc, d'après la proposition 18.21, on a $[\mathrm{K} : k] \leqslant \#\mathrm{G}$. Combiné avec les inégalités précédentes, ceci entraîne que

$$\mathrm{G} = \mathscr{G} = \mathrm{Gal}(\mathrm{K}/k) \qquad \text{et} \qquad [\mathrm{K} : k] = \#\mathrm{G}.$$

Le théorème d'Artin est démontré. □

Corollaire 19.12. — *Soient* K/k *une extension galoisienne et* $\mathrm{G} = \mathrm{Gal}(\mathrm{K}/k)$. *Alors* $\mathrm{K}^{\mathrm{G}} = k$.

Démonstration. — On a $k \subseteq \mathrm{K}^{\mathrm{G}}$ et $[\mathrm{K} : k] = \#\mathrm{G}$ puisque K/k est galoisienne. Or, d'après le théorème d'Artin, on a aussi

$$[\mathrm{K} : \mathrm{K}^{\mathrm{G}}] = \#\mathrm{G},$$

et donc l'inclusion $k \subseteq \mathrm{K}^{\mathrm{G}}$ est une égalité. □

19.4. Correspondance de Galois. — Commençons par quelques rappels sur les groupes non abéliens.

Définition 19.13. — Soit G un groupe. Un sous-groupe H est dit **normal**, ou **distingué**, s'il vérifie $g\mathrm{H}g^{-1} = \mathrm{H}$, pour tout $g \in \mathrm{G}$. Dans ce cas, on écrira

$$\mathrm{H} \lhd \mathrm{G} \qquad \text{ou} \qquad \mathrm{G} \rhd \mathrm{H}.$$

(dans les deux cas, le triangle pointe vers H.)

Exemple 19.1. — Soit $\phi : \mathrm{G} \to \mathrm{G}'$ un morphisme de groupes. Son noyau $\mathrm{Ker}\,\phi = \{h \in \mathrm{G} \mid \phi(h) = 1\}$ est un sous-groupe normal. En effet, pour tout $h \in \mathrm{Ker}\,\phi$ et $g \in \mathrm{G}$, on a

$$\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = 1.$$

D'autre part, $\mathrm{Im}(\phi) = \phi(\mathrm{G})$ est un sous-groupe de G', non nécessairement normal.

Définition 19.14 **(Classes à gauche)**. — Soient G un groupe et H un sous-groupe quelconque (c.-à-d., pas nécessairement normal). Pour tout $g \in \mathrm{G}$, on pose

$$g\mathrm{H} := \{gh \mid h \in \mathrm{H}\}.$$

On l'appelle la **classe à gauche** de g modulo H. C'est la classe d'équivalence de g pour la relation d'équivalence :

$$g_1 \sim g_2 \Leftrightarrow g_1^{-1}g_2 \in \mathrm{H}.$$

On note G/H l'ensemble de ces classes à gauche, et $\pi : G \to G/H$ l'application $g \mapsto gH$. On voit que $\pi(g) = \pi(g') \Leftrightarrow g^{-1}g' \in H$.

Remarque 19.15. — On définit de façon analogue les classes à droite Hg. En général, on a $gH \neq Hg$, mais on a l'égalité si H est normal, car alors $Hg = g(g^{-1}Hg) = gH$.

De plus, si H est un sous-groupe normal, on peut munir G/H d'une unique structure de groupe, telle que $\pi : G \to G/H$ soit un morphisme. Rappelons la construction.

Proposition 19.16. — *Soit* H *un sous-groupe* **normal** *de* G.

1) *Il existe sur* G/H *une unique structure de groupe telle que* $\pi : G \to G/H$ *soit un morphisme de groupes. Elle est définie par*

$$(*) \qquad (g_1H)(g_2H) = g_1g_2H.$$

Le noyau de $\pi : G \to G/H$ *égale* H.

2) *Les sous-groupes (normaux) de* G/H *sont les* K/H, *pour* K *sous-groupe (normal) de* G *contenant* H.

Démonstration. — 1) Pour que π soit un morphisme de groupes, il est nécessaire que la multiplication de G/H vérifie $(*)$, d'où l'unicité.

Vérifions que la formule $(*)$ fait sens, c.-à-d., que l'élément $(g_1H)(g_2H)$ est bien défini. Pour $i = 1, 2$, soit g_i' un autre élément de g_iH. Alors, $g_i' = g_ih_i$ avec $h_i \in H$ et l'on a

$$g_1'g_2' = g_1h_1g_2h_2 = g_1g_2(g_2^{-1}h_1g_2)h_2.$$

Or, par hypothèse, $g_2^{-1}h_1g_2 \in H$ et il en résulte que $g_1'g_2'H = g_1g_2H$. On vérifie alors facilement que la multiplication définie par $(*)$ est associative, admet pour élément neutre la classe $1H = H$, et que l'inverse de gH est $g^{-1}H$. Donc, G/H est un groupe, et $(*)$ montre que $\pi : G \to G/H$ est un morphisme de groupes surjectif. Enfin, $\operatorname{Ker}\pi = \{g \in G \mid gH = H\}$ égale H. Ceci prouve le point 1). Le point2) est laissé au lecteur, cf. la discussion précédant le théorème 2.5 (Chap. I). □

Théorème 19.17 **(Propriété universelle du noyau)**. — *Soit* $\phi : G \to G'$ *un morphisme de groupes et soit* K *un sous-groupe normal de* G *contenu dans* $\operatorname{Ker}\phi$. *Notons* π *la projection* $G \to G/K$.

1) ϕ *se factorise de façon unique à travers* G/K, *c.-à-d., il existe un unique morphisme de groupes* $\overline{\phi} : G/K \to G'$ *tel que* $\overline{\phi} \circ \pi = \phi$, *c.-à-d., vérifiant* $\overline{\phi}(gK) = \phi(g)$ *pour tout* $g \in G$. *De plus, on a* $\operatorname{Ker}\overline{\phi} = (\operatorname{Ker}\phi)/K$.

2) *En particulier,* ϕ *induit un isomorphisme de groupes*

$$\overline{\phi} : G/\operatorname{Ker}\phi \xrightarrow{\cong} \phi(G).$$

Démonstration. — La démonstration est analogue à celle du théorème 2.16 (Chap. I) et est laissée au lecteur. □

Soit K/k une extension de degré fini galoisienne, et soit $\mathrm{G} = \mathrm{Gal}(\mathrm{K}/k)$. Pour tout sous-groupe H de G, le sous-corps

$$\mathrm{K}^{\mathrm{H}} = \{x \in \mathrm{K} \mid h(x) = x, \quad \forall\, h \in \mathrm{H}\}$$

contient k, puisque $k = \mathrm{K}^{\mathrm{G}} \subseteq \mathrm{K}^{\mathrm{H}}$. Donc K^{H} est un « corps intermédiaire » entre k et K.

***Théorème 19.18* (Correspondance de Galois).** — *Soit* K/k *une extension de degré fini galoisienne, et soit* $\mathrm{G} = \mathrm{Gal}(\mathrm{K}/k)$.

1) *Pour tout sous-groupe* H *de* G, *l'extension* $\mathrm{K}/\mathrm{K}^{\mathrm{H}}$ *est galoisienne, et* $\mathrm{Gal}(\mathrm{K}/\mathrm{K}^{\mathrm{H}}) = \mathrm{H}$.

2) *Réciproquement, soit* L *un corps intermédiaire. L'extension* K/L *est galoisienne,*

$$\mathrm{Gal}(\mathrm{K}/\mathrm{L}) = \{g \in \mathrm{G} \mid g(\ell) = \ell, \quad \forall\, \ell \in \mathrm{L}\}$$

est un sous-groupe H *de* G, *et l'on a* $\mathrm{L} = \mathrm{K}^{\mathrm{H}}$.

3) *Par conséquent, les applications*

$$\mathrm{H} \mapsto \mathrm{K}^{\mathrm{H}} \qquad \textit{et} \qquad \mathrm{L} \mapsto \mathrm{Gal}(\mathrm{K}/\mathrm{L})$$

sont des bijections réciproques entre les deux ensembles suivants :

$$\{\textit{corps intermédiaires } \mathrm{L}\} \leftrightarrow \{\textit{sous-groupes } \mathrm{H} \textit{ de } \mathrm{G}\}.$$

Si L *et* H *se correspondent, on a*

$$[\mathrm{K} : \mathrm{L}] = |\mathrm{H}| \qquad \textit{et} \qquad [\mathrm{L} : k] = \frac{|\mathrm{G}|}{|\mathrm{H}|} = |\mathrm{G}/\mathrm{H}|.$$

Ces deux bijections sont **décroissantes**, *c.-à-d.,*

$$\mathrm{H} \subseteq \mathrm{H}' \Leftrightarrow \mathrm{K}^{\mathrm{H}} \supseteq \mathrm{K}^{\mathrm{H}'} \qquad \textit{et} \qquad \mathrm{L} \subseteq \mathrm{L}' \Leftrightarrow \mathrm{Gal}(\mathrm{K}/\mathrm{L}) \supseteq \mathrm{Gal}(\mathrm{K}/\mathrm{L}').$$

4) *Si* L *correspond à* H *alors, pour tout* $g \in \mathrm{G}$, $g(\mathrm{L})$ *correspond à* $g\mathrm{H}g^{-1}$.

5) *Soient* L *un corps intermédiaire et* $\mathrm{H} = \mathrm{Gal}(\mathrm{K}/\mathrm{L})$. *Alors* L/k *est séparable et on a l'équivalence :*

$$\mathrm{L}/k \textit{ galoisienne} \quad \Leftrightarrow \quad \mathrm{L}/k \textit{ normale} \quad \Leftrightarrow \quad \mathrm{H} \textit{ normal dans } \mathrm{G}.$$

Dans ce cas, $\mathrm{Gal}(\mathrm{L}/k) \cong \mathrm{G}/\mathrm{H}$.

6) *Soient* L *un corps intermédiaire et* $\mathrm{H} = \mathrm{Gal}(\mathrm{K}/\mathrm{L})$. *Alors les bijections de* 3) *induisent une bijection entre l'ensemble des sous-extensions* $k \subseteq \mathrm{L}' \subseteq \mathrm{L}$ *et l'ensemble des sous-groupes* H' *de* G *contenant* H. *En particulier, il n'y a qu'un nombre fini de tels* L'.

Démonstration. — L'assertion 1) est le théorème d'Artin. Montrons l'assertion 2). Soit L un corps intermédiaire et soient $x \in \mathrm{K}$ et P le polynôme minimal de x sur L. Alors P divise $\mathrm{Irr}_k(x)$, qui par hypothèse a des racines simples, toutes dans K. Donc, il en est de même des racines de P, et ceci montre que K/L est séparable et normale, donc galoisienne. Son groupe de Galois est

$$\mathrm{H} = \mathrm{Aut}(\mathrm{K}/\mathrm{L}) = \{g \in \mathrm{Aut}(\mathrm{K}) \mid g(\ell) = \ell, \quad \forall\, \ell \in \mathrm{L}\},$$

c'est un sous-groupe de

$$\mathrm{G} = \mathrm{Aut}(\mathrm{K}/k) = \{g \in \mathrm{Aut}(\mathrm{K}) \mid g(x) = x, \quad \forall\, x \in k\},$$

et l'on a $\mathrm{L} = \mathrm{K}^{\mathrm{H}}$ d'après le corollaire 19.12. Ceci prouve l'assertion 2). L'assertion 3) résulte de 1) et 2), et de la multiplicativité du degré.

4) Si L correspond à H alors, pour tout $g \in \mathrm{G}$, on a

$$g(\mathrm{L}) = \{g(x) \mid hx = x,\ \forall\, h \in \mathrm{H}\} = \{y = g(x) \mid ghg^{-1}(y) = y,\ \forall\, h \in \mathrm{H}\};$$

donc $g(\mathrm{L})$ correspond à $g\mathrm{H}g^{-1}$.

5) Soient L un corps intermédiaire et $\mathrm{H} = \mathrm{Gal}(\mathrm{K}/\mathrm{L})$. Alors L/k est séparable, et donc l'on a :

$$\mathrm{L}/k \ \text{ galoisienne} \quad \Leftrightarrow \quad \mathrm{L}/k \ \text{ normale.}$$

Si $\mathrm{H} \lhd \mathrm{G}$ alors, d'après 4), on a $g(\mathrm{L}) = \mathrm{L}$ pour tout $g \in \mathrm{G}$. Donc, pour tout $\alpha \in \mathrm{L}$,

$$\mathrm{Irr}_k(\alpha) = \prod_{\beta \in \mathrm{G}\alpha} (\mathrm{X} - \beta)$$

a toutes ses racines dans L, donc L/k est normale.

Réciproquement, supposons L/k normale et soient $g \in \mathrm{G}$ et $x \in \mathrm{L}$. Alors, étant racine de racine de $\mathrm{Irr}_k(x)$, $g(x)$ appartient à L. Ceci montre que $g(\mathrm{L}) = \mathrm{L}$ pour tout $g \in \mathrm{G}$, et donc $\mathrm{H} \lhd \mathrm{G}$ d'après 4). Ceci prouve l'équivalence

$$\mathrm{L}/k \ \text{ galoisienne} \Leftrightarrow \mathrm{H} \lhd \mathrm{G}.$$

Supposons cette condition vérifiée. Alors, $\mathrm{Gal}(\mathrm{L}/k) = \mathrm{Aut}(\mathrm{L}/k)$ est de cardinal

$$[\mathrm{L} : k] = \frac{[\mathrm{K} : k]}{[\mathrm{K} : \mathrm{L}]} = |\mathrm{G}/\mathrm{H}|.$$

D'autre part, comme L est stable par tout $g \in \mathrm{G} = \mathrm{Gal}(\mathrm{K}/k)$, alors l'application de restriction

$$\mathrm{G} \xrightarrow{\mathrm{res}} \mathrm{Gal}(\mathrm{L}/k), \qquad g \mapsto g_{|\mathrm{L}}$$

est bien définie, et est un morphisme de groupes dont le noyau est

$$\{g \in \mathrm{G} \mid g_{|\mathrm{L}} = \mathrm{id}_{\mathrm{L}}\} = \mathrm{Gal}(\mathrm{K}/\mathrm{L}) = \mathrm{H}.$$

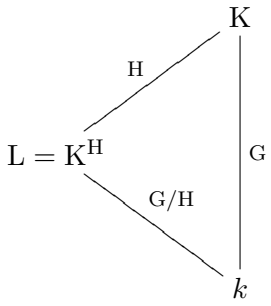
Il en résulte que l'application de restriction est surjective, et induit un isomorphisme de groupes

$$\mathrm{G}/\mathrm{H} \xrightarrow{\sim} \mathrm{Gal}(\mathrm{L}/k).$$

Ceci prouve le point 5).

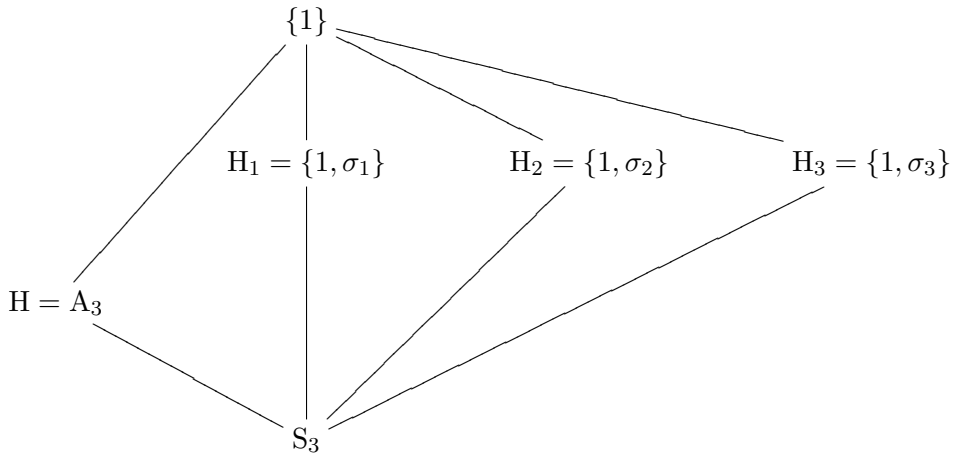
Enfin, le point 6) est une conséquence immédiate du point 3). Le théorème est démontré. □

Remarque 19.19. — On peut résumer le théorème, et en particulier le point 5), par le diagramme suivant :

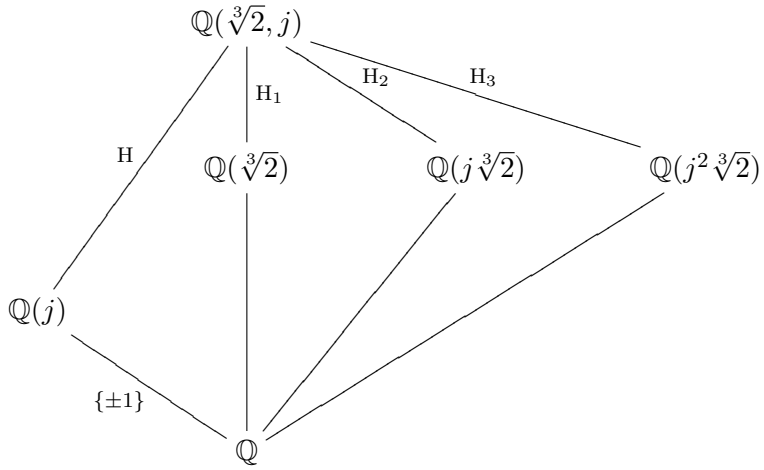


Ce diagramme, et les deux exemples qui suivent, sont empruntés au polycopié de Jan Nekovář [**Ne04**].

Exemple 19.20. — Posons $j = \exp(2i\pi/3)$ et notons $\sigma_1, \sigma_2, \sigma_3$ les trois transpositions de S_3. Alors les sous-groupes de S_3 :



correspondent aux sous-corps $\mathbb{Q} \subseteq \mathrm{L} \subseteq \mathbb{Q}(\sqrt[3]{2}, j)$:

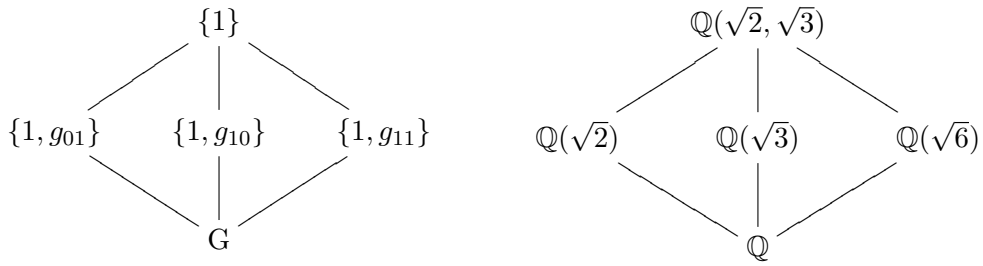


On a $\mathrm{H} = \mathrm{A}_3 \lhd \mathrm{S}_3$, et l'application signature $\varepsilon : \mathrm{S}_3 \to \{\pm 1\}$ induit un isomorphisme de groupes $\mathrm{Gal}(\mathbb{Q}(j)/\mathbb{Q}) \cong \mathrm{S}_3/\mathrm{A}_3 \cong \{\pm 1\}$.

Exemple 19.21. — Soit $\mathrm{K} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ et soit

$$\mathrm{G} = \mathrm{Gal}(\mathrm{K}/\mathbb{Q}) = \{g_{00}, g_{01}, g_{10}, g_{11}\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

On a la correspondance suivante entre sous-groupes de G et corps intermédiaires :



19.5. Clôture normale ou galoisienne. — On a vu les bonnes propriétés des extensions de degré fini galoisiennes et de leurs sous-extensions. Pour cette raison, étant donné une extension de degré fini arbitraire K/k, il est parfois utile de la plonger, si cela est possible, dans une extension plus grande L/k qui soit galoisienne. Comme une extension galoisienne est séparable, ainsi que toute sous-extension (cf. 18.5), une condition nécessaire est que K/k soit séparable. On va voir que cette condition est également suffisante.

***Théorème 19.22* (Clôture normale ou galoisienne).** — *Soit* K/k *une extension de degré fini. Alors* K *est contenu dans une extension* L*, de degré fini et normale sur* k*, minimale pour cette propriété, et unique à* K*-isomorphisme près. Un tel* L *s'appelle une* **clôture normale** *de* K/k*.*

De plus, si K/k *est* **séparable***, alors* L/k *est galoisienne et l'on dit que c'est une* **clôture galoisienne** *de* K/k*. En particulier, si* $\mathrm{car}(k) = 0$*, toute extension* K/k *de degré fini est contenue dans une extension galoisienne* L/k*.*

Démonstration. — Soit $\alpha_1, \ldots, \alpha_r$ un système de générateurs de K sur k et soit P_i le polynôme minimal sur k de α_i. Posons $\mathrm{P} = \mathrm{P}_1 \cdots \mathrm{P}_r$ et soit L un corps de décomposition de P sur K. C'est aussi un corps de décomposition de P sur k et donc l'extension L/k, de degré fini, est normale, d'après la proposition 19.2.

Elle est de plus minimale, au sens suivant. Soit L' une extension intermédiaire entre K et L, qui soit normale sur k. Alors L' contient $\alpha_1, \ldots, \alpha_r$, et donc toutes les racines de chaque $\mathrm{P}_i = \mathrm{Irr}_k(\alpha_i)$. Par conséquent, $\mathrm{L}' = \mathrm{L}$. Ceci montre que L est une extension de K normale sur k et minimale pour cette propriété.

De plus, L est unique à K-isomorphisme près. En effet, soit E une extension de K, normale sur k. Alors, E contient un corps de décomposition L' de P sur K. D'après le théorème 17.3, il existe un K-isomorphisme $\tau : \mathrm{L} \xrightarrow{\sim} \mathrm{L}'$. Si de plus, E est supposée minimale, alors $\mathrm{E} = \mathrm{L}'$ et donc E est K-isomorphe à L.

Enfin, si K/k est séparable, alors $\mathrm{P}_1, \ldots, \mathrm{P}_r$ et P sont séparables. Comme L est un corps de décomposition de P sur k, l'extension L/k est galoisienne, d'après le théorème 19.8. Ceci prouve le théorème. □

***Corollaire 19.23*.** — *Soit* $k \subset \mathrm{K}$ *une extension séparable de degré fini. Le nombre d'extensions intermédiaires* $k \subseteq \mathrm{L} \subseteq \mathrm{K}$ *est fini.*

Démonstration. — Soient $\widetilde{\mathrm{K}}$ une clôture galoisienne de K/k et $\mathrm{G} = \mathrm{Gal}(\widetilde{\mathrm{K}}/k)$. C'est un groupe fini, de cardinal $[\widetilde{\mathrm{K}} : k]$. D'après le point 6) du théorème 19.18, les extensions intermédiaires $k \subseteq \mathrm{L} \subseteq \mathrm{K}$ sont en bijection avec l'ensemble des sous-groupes de G contenant $\mathrm{H} = \mathrm{Gal}(\widetilde{\mathrm{K}}/\mathrm{K})$, qui est un ensemble fini. □

20. Corps finis

20.1. Cardinal et groupe multiplicatif d'un corps fini. — [(1)]

Soit k un corps fini. Son sous-corps premier est fini donc, d'après le paragraphe 15.2, k est de caractéristique $p > 0$. On identifiera son sous-corps

[(1)] La section 20 n'a pas été traitée le 28/11 mais le sera ultérieurement. La séance du 28/11 a été consacrée aux polynômes symétriques, qui figureront dans le polycopié du (dernier) chapitre VIII. On pourra consulter, en attendant, le chapitre 7 du cours 2005/06

premier à $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Tout corps contenant k a même sous-corps premier, donc est aussi de caractéristique p.

Lemme 20.1. — *Soient $k \subseteq k'$ deux corps finis, de cardinal q et q' respectivement.*

1) *On a $q' = q^n$, où $n = [k' : k]$.*
2) *Par conséquent, si $p = \mathrm{car}(k)$ et $m = [k : \mathbb{F}_p]$, alors $q = p^m$ et $q' = p^{mn}$.*

Démonstration. — 1) Comme k' est fini, c'est un k-espace vectoriel de dimension finie n. Alors $k' \cong k^n$ comme k-espace vectoriel, et donc $|k'| = |k|^n$. Ceci prouve 1).

Le même argument appliqué à $\mathbb{F}_p \subseteq k$ montre que $q = p^m$, d'où le lemme. □

Corollaire 20.2. — *Si k est un corps fini de caractéristique p, alors le cardinal de k est une puissance de p.*

***Théorème 20.3* (Groupe multiplicatif d'un corps fini)**. — *Soit k un corps fini de cardinal $q = p^n$. Le groupe multiplicatif $k^\times = k \setminus \{0\}$ est un groupe cyclique d'ordre $q - 1$.*

Démonstration. — $k^\times$ est un groupe abélien fini ; c'est donc un $\mathbb{Z}$-module de type fini et de torsion. D'après le théorème de structure des modules de type fini sur un anneau principal, il existe des entiers $d_1 \geqslant \cdots \geqslant d_r > 1$ tels que d_i divise d_{i-1}, pour $i = r, r-1, \ldots, 2$ et

$$k^\times \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_r\mathbb{Z}.$$

Alors, d'une part, $|k^\times| = d_1 d_2 \cdots d_r$ et, d'autre part, tout élément $x \in k^\times$ vérifie $x^d = 1$, où $d = d_1$. Or, comme $k[\mathrm{X}]$ est intègre, le polynôme $\mathrm{X}^d - 1$ a au plus d racines dans k. Il en résulte que $r = 1$ et $k^\times \cong \mathbb{Z}/d\mathbb{Z}$ est cyclique, d'ordre $d = |k^\times| = q - 1$. Ceci prouve le théorème. □

On rappelle qu'une extension K/k est dite monogène s'il existe $\xi \in \mathrm{K}$ tel que $\mathrm{K} = k(\xi)$; dans ce cas, on dit que ξ est un élément **primitif** de K/k.

***Théorème 20.4* (Théorème de l'élément primitif)**. — *On considère une extension $\mathbb{F}_q \subset \mathbb{F}_{q^n}$. Soit ξ un générateur du groupe multiplicatif $\mathbb{F}_{q^n}^\times$.*

1) *$\mathbb{F}_{q^n} = \mathbb{F}_q[\xi]$, c.-à-d., ξ est un élément primitif.*
2) *Le polynôme minimal $\mathrm{Irr}_{\mathbb{F}_q}(\xi)$ est de degré n.*

Démonstration. — 1) est clair car $\mathbb{F}_q[\xi]$ contient $\{1, \xi, \xi^2, \ldots, \xi^{q^n-1}\} = \mathbb{F}_{q^n}^\times$, ainsi que 0, donc égale $\mathbb{F}_{q^n}$. Le point 2) en découle car le degré de $\mathrm{Irr}_{\mathbb{F}_q}(\xi)$ est le degré sur $\mathbb{F}_q$ de $\mathbb{F}_q[\xi] = \mathbb{F}_{q^n}$, qui égale n. □

20.2. La formule du binôme. — Soient k, n deux entiers tels que $0 \leqslant k \leqslant n$. On rappelle la définition du coefficient binomial :

$$\binom{n}{k} := \frac{n!}{k!(n-k)!}.$$

(On le note aussi C_n^k.) C'est le nombre de façons de choisir k éléments dans un ensemble à n éléments. Pour $k = 0$ ou n, ceci vaut 1. On rappelle aussi la formule de Pascal (pour $k \geqslant 1$) :

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1},$$

qu'on obtient en remarquant que, quand on prend k éléments dans $\{1, \ldots, n\}$, on peut ou bien prendre, ou ne pas prendre, n. On rappelle aussi la formule du binôme, valable dans tout anneau commutatif.

***Lemme 20.5* (Formule du binôme).** — *Soient* A *un anneau commutatif et* $a, b \in$ A. *Pour tout* $n \geqslant 1$, *on a :*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$

Démonstration. — Par récurrence sur n, en utilisant la formule de Pascal. □

***Lemme 20.6*.** — *Soit* $p \in \mathbb{N}$ *un nombre premier. Alors* p *divise* $\binom{p}{k}$ *pour tout* $k = 1, \ldots, p-1$.

Démonstration. — p divise $p! = k!(p-k)!\binom{p}{k}$ et est premier avec $k!(p-k)!$, donc divise $\binom{p}{k}$. □

20.3. Endomorphismes de Frobenius. —

***Proposition 20.7* (L'endomorphisme de Frobenius Fr_p).** — *Soit* K *un corps de caractéristique* $p > 0$. *Alors l'application* $x \mapsto x^p$ *est un endomorphisme du corps* K, *noté* Fr_p. *De plus, si* K *est fini, alors* Fr_p *est un automorphisme de* K.

Démonstration. — Il est clair que $1^p = 1$ et $(ab)^p = a^p b^p$ pour tout $a, b \in$ K. L'égalité $(a+b)^p = a^p + b^p$ résulte de la formule du binôme et du lemme précédent. Donc, Fr_p est un morphisme de corps de K vers K, c.-à-d., un endomorphisme de corps de K. Il est bien sûr injectif, comme tout morphisme de corps. Par conséquent, si K est fini, Fr_p est bijectif donc un automorphisme de K. □

Corollaire 20.8 **(Les endomorphismes de Frobenius $\mathrm{Fr}_q = \mathrm{Fr}_{p^n}$)**

Soient K *un corps de caractéristique $p > 0$ et $n \geqslant 1$. L'application $\mathrm{Fr}_p^n := \mathrm{Fr}_p \circ \cdots \circ \mathrm{Fr}_p$ (n fois), qui à tout x associe x^{p^n}, est un endomorphisme du corps* K. *On le note aussi Fr_{p^n} ou Fr_q si $q = p^n$. Si* K *est fini, c'est un automorphisme de* K.

Démonstration. — Ceci résulte immédiatement de la proposition précédente. □

Corollaire 20.9. — *Soient p un nombre premier, $n \geqslant 1$ et $q = p^n$. Alors p divise $\binom{q}{i}$ pour tout $i = 1, \ldots, q-1$.*

Démonstration. — Plaçons-nous dans le corps $\mathrm{K} = \mathbb{F}_p(\mathrm{X})$ des fractions rationnelles sur $\mathbb{F}_p$ et notons π la projection $\mathbb{Z} \to \mathbb{F}_p$. D'une part, on a

$$(1+\mathrm{X})^q = \sum_{i=0}^{q} \pi\Big(\binom{q}{i}\Big)\,\mathrm{X}^i. \tag{1}$$

D'autre part, comme $\mathrm{Fr}_q = \mathrm{Fr}_p^n$ est un endomorphisme de K, l'on a

$$(1+\mathrm{X})^q = 1 + \mathrm{X}^q. \tag{2}$$

En comparant (1) et (2), on obtient que $\binom{q}{i} \equiv 0 \bmod p$, pour $i = 1, \ldots, q-1$. Ceci prouve le corollaire. □

20.4. Existence et unicité des corps $\mathbb{F}_{p^n}$. —

Lemme 20.10. — *Soient* K *un corps et τ un endomorphisme de* K. *Alors l'ensemble des éléments invariants*

$$\mathrm{K}^\tau := \{x \in \mathrm{K} \mid \tau(x) = x\}$$

est un sous-corps de K.

Démonstration. — C'est clair. □

Théorème 20.11 **(Existence et unicité de $\mathbb{F}_q$)**. — *Soient p un nombre premier, $n \geqslant 1$ et $q = p^n$. Soit* K *un corps de décomposition sur $\mathbb{F}_p$ du polynôme $\mathrm{X}^q - \mathrm{X}$. Alors, $|\mathrm{K}| = q$. Réciproquement, tout corps fini à q éléments est isomorphe à* K. *Par conséquent, il existe à isomorphisme près, un unique corps fini à q éléments. On le note $\mathbb{F}_q$ ou $\mathbb{F}_{p^n}$.*

Démonstration. — Soit K un corps de décomposition du polynôme $\mathrm{Q} := \mathrm{X}^q - \mathrm{X}$ sur $\mathbb{F}_p$. Le polynôme dérivé Q' égale -1 donc n'a pas de racines en commun avec Q. Par conséquent, d'après la proposition 18.11, Q a q racines distinctes dans K.

Or, le point-clé est que ces racines sont exactement les solutions de l'équation $x^q = x$, c.-à-d., les éléments de K fixés par l'endomorphisme Fr_q. Par

conséquent, ces racines forment un sous-corps K_1 de K, de cardinal q. Comme, par hypothèse, K est engendré par ces racines, on obtient $\mathrm{K} = \mathrm{K}_1$, et donc K est de cardinal q. Ceci prouve le point 1).

Réciproquement, supposons que L soit un autre corps fini de cardinal q. D'après le théorème 20.3, le groupe multiplicatif $\mathrm{L}^\times$ est cyclique, d'ordre $q-1$. Donc, tout élément $x \in \mathrm{L}^\times$ vérifie

$$x^{q-1} = 1 \quad \text{et donc} \quad x^q = x.$$

Donc, tout élément de $\mathrm{L} = \mathrm{L}^\times \cup \{0\}$ est une racine du polynôme $\mathrm{Q} = \mathrm{X}^q - \mathrm{X}$. Comme $|\mathrm{L}| = q$, alors Q a toutes ses racines dans L, et puisque leur ensemble égale L tout entier, L est un corps de décomposition de Q sur $\mathbb{F}_p$. Par conséquent, d'après le théorème 17.2, L est isomorphe à K. Le théorème est démontré. □

Théorème 20.12 **(Existence et unicité des extensions $\mathbb{F}_q \subseteq \mathbb{F}_{q^n}$)**

Soient p un nombre premier, $q = p^d$ et $q' = p^n$ deux puissances de p.

1) *S'il existe une extension $\mathbb{F}_q \subseteq \mathbb{F}_{q'}$ alors q' est une puissance de q, c.-à-d., n est un multiple de d.*

2) *Réciproquement, si $n = rd$, c.-à-d., si $q' = q^r$, alors le corps $\mathbb{F}_{q'}$ contient un* **unique** *sous-corps de cardinal q ; c'est le sous-corps des invariants de Fr_q.*

Démonstration. — 1) On a déjà vu (lemme 20.1) que si $\mathbb{F}_q \subseteq \mathbb{F}_{q'}$ alors $\mathbb{F}_{q'}$ est un $\mathbb{F}_q$-espace vectoriel de dimension finie r, d'où $q' = q^r$, c.-à-d., $n = dr$.

2) Réciproquement, supposons $n = dr$, c.-à-d., $q' = q^r$. D'après le théorème précédent, le polynôme

$$\mathrm{X}^{q'} - \mathrm{X} = \mathrm{X}^{q^r} - \mathrm{X}$$

est scindé dans $\mathbb{F}_{q'}$ et ses racines, deux à deux distinctes, sont exactement les éléments de $\mathbb{F}_{q'}$. D'autre part,

$$\begin{aligned} \mathrm{X}^{q^r} - \mathrm{X} &= \mathrm{X}^q - \mathrm{X} + \mathrm{X}^{q^2} - \mathrm{X}^q + \cdots + \mathrm{X}^{q^r} - \mathrm{X}^{q^{r-1}} \\ &= \mathrm{X}^q - \mathrm{X} + (\mathrm{X}^q - \mathrm{X})^q + \cdots + (\mathrm{X}^q - \mathrm{X})^{q^{r-1}}. \end{aligned}$$

Donc $\mathrm{X}^q - \mathrm{X}$ divise $\mathrm{X}^{q^r} - \mathrm{X}$ et a aussi toutes ses racines dans $\mathbb{F}_{q'}$. Ces racines sont exactement les points fixes dans $\mathbb{F}_{q'}$ de l'endomorphisme de Frobenius Fr_q, donc forment un sous-corps K de cardinal q, isomorphe à $\mathbb{F}_q$.

Enfin, supposons que L soit un autre sous-corps de $\mathbb{F}_{q'}$ de cardinal q. D'après le théorème 20.3, le groupe multiplicatif $\mathrm{L}^\times$ est cyclique, d'ordre $q-1$. Donc, tout élément $x \in \mathrm{L}^\times$ vérifie

$$x^{q-1} = 1 \quad \text{et donc} \quad x^q = x.$$

Par conséquent, les éléments de $\mathrm{L} = \mathrm{L}^\times \cup \{0\}$ sont exactement les racines dans $\mathbb{F}_{q'}$ du polynôme $\mathrm{X}^q - \mathrm{X}$. Il en résulte $\mathrm{L} = \mathrm{K}$. Le théorème est démontré. □

20.5. Groupe de Galois de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$. —

Lemme 20.13. — *Soit* G *un groupe fini.*

1) *Pour tout sous-groupe* H*, on a* $|\mathrm{G}| = |\mathrm{H}|\cdot|\mathrm{G/H}|$*. En particulier,* $|\mathrm{H}|$ *divise* $|\mathrm{G}|$*.*

2) *Soit* $g \in \mathrm{G}$*. L'ensemble* $\{n \in \mathbb{Z} \mid g^n = 1\}$ *est un sous-groupe non-nul de* $\mathbb{Z}$*, donc de la forme* $d\mathbb{Z}$*, pour un certain* $d \geqslant 1$*, appelé l'***ordre** *de* g*. On a* $d = 1 \Leftrightarrow g = 1$*. Le sous-groupe de* G *engendré par* g *est égal à* $\{1, g, \dots, g^{d-1}\}$ *; il est de cardinal* d *et isomorphe à* $\mathbb{Z}/d\mathbb{Z}$*. En particulier,* d *divise* n*.*

Démonstration. — On rappelle que G/H désigne l'ensemble des classes à gauche gH. C'est un ensemble fini, puisque G est fini. De plus, deux classes distinctes $g\mathrm{H} \neq g'\mathrm{H}$ sont disjointes. En effet, sinon il existerait $h, h' \in \mathrm{H}$ tels que $gh = g'h'$, et l'on aurait $g\mathrm{H} = g'\mathrm{H}$. De plus, chaque classe gH est de cardinal $|\mathrm{H}|$, puisque l'application $\mathrm{H} \mapsto g\mathrm{H}$, $h \mapsto gh$ est une bijection. Donc G est la réunion disjointe de $|\mathrm{G/H}|$ classes, chacune de cardinal $|\mathrm{H}|$. Le point 1) en résulte.

Soit $g \in \mathrm{G}$. On pose $g^0 = 1$. Comme G est fini, les éléments g^k, $k \geqslant 1$, ne peuvent être tous distincts. Donc il existe $r < s$ tels que $g^r = g^s$, d'où $g^{s-r} = 1$. Ceci montre que l'ensemble

$$\{n \in \mathbb{Z} \mid g^n = 1\}$$

n'est pas réduit à $\{0\}$. Comme $g^m g^n = g^{m+n}$, on voit que cet ensemble est un sous-groupe non nul de $\mathbb{Z}$, donc est de la forme $d\mathbb{Z}$, pour un unique $d \geqslant 1$, et le reste du point 2) s'obtient facilement. □

Théorème 20.14 **(L'isomorphisme** $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$**)**

Soient $n \geqslant 1$ *et* q *une puissance d'un nombre premier* p*. L'extension* $\mathbb{F}_q \subseteq \mathbb{F}_{q^n}$ *est galoisienne. Son groupe de Galois* $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ *est cyclique d'ordre* n*, engendré par l'automorphisme de Frobenius* Fr_q*.*

Démonstration. — $\mathbb{F}_{q^n}$ est un corps de décomposition du polynôme $\mathrm{Q} = \mathrm{X}^{q^n} - \mathrm{X}$ sur $\mathbb{F}_p$, donc a fortiori sur $\mathbb{F}_q$. De plus, Q a des racines distinctes dans $\mathbb{F}_{q^n}$ (puisque $\mathrm{Q}' = -1$) donc est séparable sur $\mathbb{F}_q$. Donc, d'après le théorème 19.8, l'extension $\mathbb{F}_q \subseteq \mathbb{F}_{q^n}$ est galoisienne, et l'on a

$$|\operatorname{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)| = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n.$$

D'autre part, Fr_q est un $\mathbb{F}_q$-automorphisme de $\mathbb{F}_{q^n}$, c.-à-d., un élément de $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$; soit d son ordre. L'égalité $\mathrm{Fr}_q^d = \mathrm{id}_{\mathbb{F}_{q^n}}$ équivaut à

$$\forall\, x \in \mathbb{F}_{q^n}, \quad x = \mathrm{Fr}_q^d(x) = x^{q^d}.$$

Comme le polynôme $X^{q^d} - X$ a au plus q^d racines, ceci entraîne que $d \geqslant n$. Par conséquent, $d = n$ et donc Fr_q est un générateur de $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$, qui est donc isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Le théorème est démontré. □

20.6. Polynômes irréductibles sur $\mathbb{F}_q$. — D'après le point 2) du théorème 20.4, on a la proposition suivante.

Proposition 20.15. — *Pour tout corps fini $\mathbb{F}_q$, et tout $n \geqslant 1$, il existe dans $\mathbb{F}_q[X]$ au moins un polynôme irréductible unitaire de degré n.*

Définition 20.16. — Pour tout $d \geqslant 1$, notons $I(d,q)$ l'ensemble des polynômes irréductibles unitaires de degré d dans $\mathbb{F}_q[X]$ et posons $i(d,q) = |I(d,q)|$.

Théorème 20.17. — *Pour tout $n \geqslant 1$, on a*

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in I(d,q)} P. \tag{1}$$

Par conséquent,

$$q^n = \sum_{d|n} d\, i(d,q). \tag{2}$$

Démonstration. — Fixons $n \geqslant 1$. On va démontrer le théorème en trois étapes.

1. Soient d divisant n et $P \in I(d,q)$. Le corps de rupture $\mathbb{F}_q[X]/(P)$ est de degré d sur $\mathbb{F}_q$, donc est isomorphe à $\mathbb{F}_{q^d}$. Par conséquent, P a au moins une racine α dans $\mathbb{F}_{q^d}$. Comme, d'après le théorème 20.14, l'extension $\mathbb{F}_q \subseteq \mathbb{F}_{q^d}$ est galoisienne, alors $P = \mathrm{Irr}_{\mathbb{F}_q}(\alpha)$ est scindé sur $\mathbb{F}_{q^d}$. Par conséquent, P divise le polynôme

$$X^{q^d} - X = \prod_{x \in \mathbb{F}_{q^d}} (X - x). \tag{$*_d$}$$

De plus, on a vu dans la preuve du théorème 20.12 que $X^{q^d} - X$ divise $X^{q^n} - X$. Ceci découle aussi de l'inclusion $\mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^n}$ (établie en 20.12), et de l'égalité

$$X^{q^n} - X = \prod_{x \in \mathbb{F}_{q^n}} (X - x). \tag{$*_n$}$$

Donc, P divise $Q_n := X^{q^n} - X$. Ceci montre que Q_n est divisible par le terme de droite de (1).

2. Réciproquement, soit R un facteur irréductible, unitaire, de degré d, de Q_n dans $\mathbb{F}_q[X]$ et soit α une racine de R dans $\mathbb{F}_{q^n}$. Alors $R = \mathrm{Irr}_{\mathbb{F}_q}(\alpha)$ et donc $\deg_{\mathbb{F}_q}(\alpha) = d$. Par conséquent, on a

$$\mathbb{F}_{q^d} \cong \mathbb{F}_q[\alpha] \subseteq \mathbb{F}_{q^n},$$

et, d'après le théorème 20.12, ceci entraîne que $d \mid n$. Ceci montre que Q_n n'a pas d'autres facteurs irréductibles que les $\mathrm{P} \in \mathrm{I}(d,q)$, pour $d \mid n$.

3. Enfin, les facteurs irréductibles de Q_n sont tous de multiplicité 1, puisque Q_n a des racines simples, d'après $(*_n)$. Ceci prouve l'égalité (1) du théorème, et l'égalité (2) en découle en prenant les degrés. □

***Théorème 20.18* (Polynômes irréductibles sur $\mathbb{F}_q$).** — *Soit* $\mathrm{P} \in \mathrm{I}(d,q)$ *et soit* $\alpha \in \mathbb{F}_{q^d}$ *une racine de* P. *Alors,*

$$\mathrm{P} = (\mathrm{X}-\alpha)(\mathrm{X}-\alpha^q)\cdots(\mathrm{X}-\alpha^{q^{d-1}}). \tag{3}$$

Démonstration. — D'après le théorème 20.14, l'extension $\mathbb{F}_q \subseteq \mathbb{F}_{q^d}$ est galoisienne, de groupe

$$\mathrm{G} := \mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q) = \{1, \mathrm{Fr}_q, \ldots, \mathrm{Fr}_q^{d-1}\} \cong \mathbb{Z}/d\mathbb{Z}.$$

D'autre part, d'après la proposition 19.4, l'on a :

$$\mathrm{P} = \mathrm{Irr}_{\mathbb{F}_q}(\alpha) = \prod_{\beta \in \mathrm{G}\alpha} (\mathrm{X}-\beta).$$

Comme $\deg \mathrm{P} = d$, l'orbite $\mathrm{G}\alpha$ a d éléments ; elle est donc formée des éléments $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$, qui sont deux à deux distincts. Ceci prouve le théorème. □

20.7. Le corps $\overline{\mathbb{F}}_p$. — Soit $(m_i)_{i\geqslant 1}$ une suite d'entiers $\geqslant 1$ tendant vers $+\infty$ et « suffisamment divisible » au sens suivant : pour tout $i \geqslant 1$, m_i divise m_{i+1}, et i divise m_i. On peut prendre, par exemple, $m_i = i!$.

Posons $\mathrm{K}_0 = \mathbb{F}_p$ et pour tout $i \geqslant 1$, soit K_i un corps de décomposition sur K_{i-1} du polynôme

$$\mathrm{X}^{p^{m_i}} - \mathrm{X}.$$

Alors, $\mathrm{K}_i \cong \mathbb{F}_{p^{m_i}}$ et on a une suite croissante

$$\mathrm{K}_0 \subseteq \mathrm{K}_1 \subseteq \mathrm{K}_2 \subseteq \cdots$$

On note $\overline{\mathbb{F}}_p$ la réunion des K_i.

***Proposition 20.19* (Premières propriétés de $\overline{\mathbb{F}}_p$).** —

1) *Pour tout* $d \geqslant 1$, $\overline{\mathbb{F}}_p$ *contient un unique sous-corps de cardinal* p^d *; on le notera* $\mathbb{F}_{p^d}(\overline{\mathbb{F}}_p)$.

2) *Fixons* $r \geqslant 1$ *et* $q = p^r$. *On a* $\overline{\mathbb{F}}_p = \bigcup_{n\geqslant 1} \mathbb{F}_{q^{n!}}(\overline{\mathbb{F}}_p)$.

Démonstration. — 1) Soient $d \geqslant 1$ et $q = p^d$. Par hypothèse, d divise m_d donc

$$\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^{m_d}} \subseteq \overline{\mathbb{F}}_p.$$

De plus, le polynôme $\mathrm{X}^q - \mathrm{X}$ a toutes ses racines, deux à deux distinctes, dans $\mathbb{F}_q$, et ces racines sont exactement les éléments de $\mathbb{F}_q$.

Par conséquent, $\mathbb{F}_q$ est l'unique sous-corps de $\overline{\mathbb{F}}_p$ de cardinal q. En effet, si L en est un autre alors, comme le groupe multiplicatif $\mathrm{L}^\times$ est cyclique d'ordre $q-1$, les éléments de L sont exactement les racines dans $\overline{\mathbb{F}}_p$ du polynôme $\mathrm{X}^q - \mathrm{X}$, c.-à-d., les élément de $\mathbb{F}_q$. Ceci prouve le point 1).

2) Pour tout $d \geqslant 1$, notons simplement $\mathbb{F}_{p^d}$ l'unique sous-corps de $\overline{\mathbb{F}}_p$ de cardinal p^d. Par définition, l'on a

$$\overline{\mathbb{F}}_p = \bigcup_{i \geqslant 1} \mathbb{F}_{p^{m_i}}.$$

Fixons $q = p^r$ et montrons que

$$(*) \qquad \bigcup_{i \geqslant 1} \mathbb{F}_{p^{m_i}} = \bigcup_{n \geqslant 1} \mathbb{F}_{q^{n!}}.$$

Pour tout $i \geqslant 1$, on a $\mathbb{F}_{p^{m_i}} \subseteq \mathbb{F}_{q^{m_i!}}$, puisque m_i divise $m_i!$. Ceci prouve l'inclusion $\subseteq$. Réciproquement, soit $n \geqslant 1$. Par hypothèse, $i = rn!$ divise $m_i = m_{rn!}$ et donc $\mathbb{F}_{q^{n!}} \subseteq \mathbb{F}_{p^{m_{rn!}}}$. Ceci prouve l'inclusion $\supseteq$, et donc l'égalité dans $(*)$. La proposition est démontrée. □

***Théorème 20.20* (Clôture algébrique de $\mathbb{F}_q$).** — 1) *$\overline{\mathbb{F}}_p$ est une clôture algébrique de $\mathbb{F}_q$, pour tout $q = p^d$.*

2) *Toute clôture algébrique de $\mathbb{F}_q$ est $\mathbb{F}_q$-isomorphe à $\overline{\mathbb{F}}_p$.*

Démonstration. — Fixons $q = p^d$ et désignons par $\mathbb{F}_q$ l'unique sous-corps de $\overline{\mathbb{F}}_p$ à q éléments.

1) Soit $x \in \overline{\mathbb{F}}_p$. Il existe $i \geqslant 1$ tel que $x \in \mathbb{F}_{p^{m_i}}$, et donc x est algébrique sur $\mathbb{F}_p$, et a fortiori sur $\mathbb{F}_q$. Donc, pour prouver 1), il suffit de montrer que $\overline{\mathbb{F}}_p$ est algébriquement clos. Soit $\mathrm{P} = \mathrm{X}^d + a_1\mathrm{X}^{d-1} + \cdots + a_d \in \overline{\mathbb{F}}_p[\mathrm{X}]$, non constant. Il existe $i \geqslant 1$ tel que $a_0, \ldots, a_d \in \mathbb{F}_{p^i}$. Soit K un corps de décomposition de P sur $\mathbb{F}_{p^i}$ et soit $r = [\mathrm{K} : \mathbb{F}_{p^i}]$. Alors K est isomorphe au sous-corps $\mathbb{F}_{p^{ir}}$ de $\overline{\mathbb{F}}_p$ et donc P est scindé sur ce sous-corps, a fortiori sur $\overline{\mathbb{F}}_p$. Ceci prouve que $\overline{\mathbb{F}}_p$ est une clôture algébrique de $\mathbb{F}_q$.

Posons $\mathrm{K} = \overline{\mathbb{F}}_p$ et, pour tout $n \geqslant 1$, désignons par K_n l'unique sous-corps de K de cardinal $q^{n!}$. Ainsi, K_1 est le corps $\mathbb{F}_q$ considéré dans le théorème, et l'on a, d'après la proposition précédente,

$$(1) \qquad \mathrm{K} = \bigcup_{n \geqslant 1} \mathrm{K}_n.$$

Considérons une extension $\mathbb{F}_q \subset \mathrm{L}$ et supposons que L soit une clôture algébrique de $\mathbb{F}_q$. Comme L est algébriquement clos, le polynôme $\mathrm{Q}_n := \mathrm{X}^{q^{n!}} - \mathrm{X} \in \mathrm{L}[\mathrm{X}]$ est scindé ; et comme ses racines sont simples, L contient un sous-corps

de cardinal $q^{n!}$. En raisonnant comme dans la preuve de la proposition précédente, on obtient que L contient un unique sous-corps de cardinal $q^{n!}$, dont les éléments sont les racines dans L de Q_n. Notons-le L_n. En particulier, L_1 égale $\mathbb{F}_q$, identifié à K_1.

D'autre part, soit $x \in \mathrm{L}$. Par hypothèse, x est algébrique sur $\mathbb{F}_q$; soit $d = \deg_{\mathbb{F}_q}(x)$ son degré. Alors le sous-corps $\mathbb{F}_q[x]$ de L est de cardinal q^d, donc est contenu dans L_d (puisque d divise $d!$). Par conséquent, on a

$$\mathrm{L} = \bigcup_{n \geqslant 1} \mathrm{L}_n. \tag{2}$$

Montrons maintenant, par récurrence sur n, qu'on peut prolonger l'identification $\mathrm{L}_1 = \mathrm{K}_1 = \mathbb{F}_q$ en un $\mathbb{F}_q$-isomorphisme $\tau_n : \mathrm{L}_n \xrightarrow{\sim} \mathrm{K}_n$.

Supposons l'assertion établie au cran n. Commençons par remarquer que $\tau_n(\mathrm{Q}_{n+1}) = \mathrm{Q}_{n+1}$, puisque les coefficients de Q_{n+1} sont dans $\mathbb{F}_p$. Observons ensuite que, comme L_{n+1}, resp. K_{n+1}, contient L_n, resp. K_n, et est formé des racines de Q_{n+1} dans L, resp. K, alors L_{n+1}, resp. K_{n+1}, est un corps de décomposition de Q_{n+1} sur L_n, resp. K_n. Par conséquent, d'après le théorème 17.3, τ_n se prolonge en un $\mathbb{F}_q$-isomorphisme $\tau_{n+1} : \mathrm{L}_{n+1} \xrightarrow{\sim} \mathrm{K}_{n+1}$.

On obtient ainsi une suite infinie $(\tau_1, \tau_2, \cdots)$ d'isomorphismes $\tau_n : \mathrm{L}_n \xrightarrow{\sim} \mathrm{K}_n$, tels que $\tau_1 = \mathrm{id}_{\mathbb{F}_q}$ et

$$\forall\, r \geqslant n, \quad \tau_r|_{\mathrm{L}_n} = \tau_n. \tag{3}$$

On définit alors $\tau : \mathrm{L} \to \mathrm{K}$ par la formule : $\tau(x) = \tau_n(x)$ si $x \in \mathrm{L}_n$. Ceci est bien défini d'après (3). Il est alors clair que τ est un morphisme de corps, donc est injectif. De plus, son image contient K_n, pour tout $n \geqslant 1$, donc égale K. Par conséquent, τ est un $\mathbb{F}_q$-isomorphisme de L sur K. Le théorème est démontré. □

TABLE DES MATIÈRES

Bibliographie

[Art] E. Artin, Galois Theory, nouvelle édition, Dover, 1998.

[AM] M. Atiyah, I. G. Macdonald, Commutative algebra, Addison-Wesley, 1969.

[BAlg] N. Bourbaki, Algèbre, Chapitres 4 à 7, Masson, 1981.

[BM] J. Briançon, Ph. Maisonobe, Éléments d'algèbre commutative (niveau M1), Ellipses, 2004.

[ChL] A. Chambert-Loir, Algèbre corporelle, Presses de l'École polytechnique, 2005.

[Die] J. Dieudonné, Cours de géométrie algébrique, tome 2, P.U.F., 1974.

[Dou] A. Douady, R. Douady, Algèbre et théories galoisiennes (2 tomes), Cedic Fernand Nathan, 1977, 2ème éd., Cassini, 2005.

[Elk] R. Elkik, Cours d'algèbre, Ellipses, 2002.

[Esc] J.-P. Escofier, Théorie de Galois, Dunod, 2000.

[Ja1] N. Jacobson, Basic algebra I, W. H. Freeman & Co., 1974.

[Ja2] N. Jacobson, Basic algebra II, W. H. Freeman & Co., 1980.

[La] S. Lang, Algebra, Addison-Wesley, 1965. Traduction française de la 3ème édition : Algèbre, Dunod, 2004.

[Ne04] J. Nekovář, Théorie de Galois, cours UPMC 2003/4, disponible à l'adresse : www.math.jussieu.fr/~nekovar/co/ln

[Pe1] D. Perrin, Cours d'algèbre, E.N.S.J.F. 1981, et 3ème édition, Ellipses, 1996.

[Pe2] D. Perrin, Géométrie algébrique - Une introduction, Inter Éditions/-CNRS Éditions, 1995.

[Sa] P. Samuel, Théorie algébrique des nombres, Hermann, 1967.

[Se] J.-P. Serre, Représentations linéaires des groupes finis, (3ème édition corrigée), Hermann, 1978.

[Ti] J.-P. Tignol, Galois' Theory of algebraic equations, World Scientific, 2001.