

**VIII. EXTENSIONS NORMALES,
SÉPARABLES, GALOISIENNES. CORPS FINIS**
SÉANCES DU 5, 6, 12 ET 13 NOVEMBRE

16. Extensions séparables et théorème de l'élément primitif

16.1. Polynômes et extensions séparables. — ⁽⁹⁾

Définition 16.1. — Soit $P \in k[X]$ un polynôme **irréductible**. On dit que P est **séparable sur k** s'il vérifie la propriété suivante : ses racines $\alpha_1, \dots, \alpha_n$ dans un corps de décomposition K de P sur k sont deux à deux distinctes, c.-à-d., chacune de multiplicité 1.

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 15.42, un k -isomorphisme $\sigma : K \xrightarrow{\sim} K'$. On a $\sigma(P) = P$, puisque P est à coefficients dans k . D'autre part, on a dans $K[X]$, $P = a(X - \alpha_1) \cdots (X - \alpha_n)$, où $a \in k$ est le coefficient dominant de P , et appliquant σ à cette égalité on obtient la décomposition $P = \sigma(P) = a(X - \sigma(\alpha_1)) \cdots (X - \sigma(\alpha_n))$. Par conséquent, les racines de P dans K' sont les $\sigma(\alpha_i)$, qui sont deux à deux distinctes.

Exemple 16.2. — On verra plus bas que si $\text{car}(k) = 0$, alors tout polynôme irréductible est séparable. D'un autre côté, voici un exemple (en caractéristique $p > 0$) d'un polynôme irréductible non séparable.

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

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

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

Lemme 16.3. — Soient $P \in k[X]$ séparable, L une extension de k , et Q un diviseur de P dans $L[X]$. Alors Q est séparable sur L .

⁽⁹⁾version du 4/11/07

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. \square

Définition 16.4. — Soit $k \subset K$ une extension algébrique.

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

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

Proposition 16.5. — Soient $k \subset L \subset K$ 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 $x \in K$. Par hypothèse, $\text{Irr}_k(x)$ est séparable. Or, il est multiple, dans $L[X]$, de $\text{Irr}_L(x)$. Donc ce dernier est séparable, d'après le lemme précédent. \square

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

Définition 16.6. — 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 16.7. — 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 16.2, 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 ».

16.2. Racines multiples et séparabilité. — Éluçidons maintenant la notion de polynôme séparable.

Définition 16.8. — Soit A une k -algèbre. Une **dérivation** de A est un endomorphisme k -linéaire $D : A \rightarrow A$ qui vérifie la *règle de Leibniz*, c.-à-d.,

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

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 16.9 (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 16.10. — *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. \square

Proposition 16.11. — *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 ≥ 1 .

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

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

d'où $P'(\alpha) = 0$. Ceci montre que 1) \Rightarrow 2).

Soit D un pgcd de P et P' . D'après le théorème de Bezout, il existe $A, B \in k[X]$ tels que $AP + BP' = D$. 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 $\deg D \geq 1$. Ceci montre que 2) \Rightarrow 3).

Réciproquement, si D est de degré ≥ 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 $L[X]$,

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

d'où, d'après (*) ci-dessus, $P'(\alpha) = Q(\alpha) \neq 0$. Donc, α est une racine de P dans L de multiplicité ≥ 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) \Rightarrow 1). La proposition est démontrée. \square

Corollaire 16.12. — Soit $P \in k[X]$ irréductible. Alors : P est séparable $\Leftrightarrow P' \neq 0$.

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

Corollaire 16.13. — Si $\text{car}(k) = 0$, tout polynôme est séparable.

Démonstration. — D'après la définition 16.6, 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 dX^{d-1} , non nul puisque $\text{car}(k) = 0$. Donc P est séparable, d'après le corollaire précédent. \square

16.3. Caractérisation de la séparabilité en termes de morphismes.

— On peut caractériser les extensions séparables en termes de morphismes (théorème 16.16 ci-dessous). Ceci sera utile pour démontrer, dans le paragraphe suivant, le théorème de l'élément primitif 16.20 et son corollaire 16.22.

De plus, l'intérêt du théorème 16.16 ci-dessous apparaîtra plus clairement plus tard, lorsqu'on étudiera la théorie de Galois.

Commençons par rappeler la proposition suivante, déjà énoncée en 15.39 (Chap. VII).

Proposition 16.14. — Soit K/k une extension algébrique monogène, c.-à-d., $K = k(\alpha)$ avec α algébrique sur k . Soient $P = \text{Irr}_k(\alpha)$, le polynôme minimal de α sur k , et $d = \text{deg } P = [K : k]$. Alors, pour toute extension L/k , le nombre de k -morphisms $K \rightarrow L$ est égal au nombre de racines distinctes de P dans L . Par conséquent, on a

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

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

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

Définition 16.15. — Soit K/K_1 une extension de corps et soit $\tau : K_1 \rightarrow L$ un morphisme de corps (nécessairement injectif!). On note $\text{Hom}_\tau(K, L)$ l'ensemble des morphismes de corps $\phi : K \rightarrow L$ tels que $\phi|_{K_1} = \tau$. Si l'on identifie K_1 à son image $\tau(K_1)$, ce n'est autre que l'ensemble des K_1 -morphisms de K vers L .

Théorème 16.16 (Séparabilité sur k et k -morphisms). — Soit K/k une extension de degré fini.

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

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

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, $K = k[x_1, \dots, x_r]$. On va montrer 1) et 2) par récurrence sur r . Supposons $r = 1$, c.-à-d., $K = k[x]$, et soit P le polynôme minimal de x sur k . D'après la proposition 16.14, le cardinal de $\text{Hom}_{k\text{-alg.}}(K, L)$ est le nombre de racines distinctes de P dans L , qui est $\leq \deg P = [K : k]$, 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 $r \geq 2$ et le résultat établi pour $r - 1$.

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

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

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

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

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

$$(3) \quad \# \text{Hom}_{k\text{-alg.}}(K, L) \leq \# \text{Hom}_{k\text{-alg.}}(k_1, L) \cdot \# \text{Hom}_{k_1\text{-alg.}}(K, L),$$

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

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

ce qui prouve l'assertion 1).

Supposons de plus K/k séparable et L algébriquement clos. Alors, d'après le théorème 15.54, tout k -morphisme $k_1 \rightarrow L$ se prolonge en un k -morphisme $\phi : K \rightarrow L$, 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 $x \in K$ 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

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

et d'après la proposition 16.14 ceci entraîne que x est séparable sur k . Ceci montre que K/k est séparable, et l'assertion 3) est démontrée. \square

Théorème 16.17 (Critère de séparabilité et transitivité). — *Soit K/k une extension de degré fini.*

- 1) *Soit $x \in K$. 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 $K = k[x_1, \dots, x_r]$ 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 $\text{Irr}_k(x)$. Alors $\text{Irr}_k(x)$ a $\deg_k(x)$ racines distinctes dans L donc, d'après la proposition 16.14, on a

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

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 15.54, on a

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

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

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

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 . \square

Corollaire 16.18. — *Soit $P \in k[X]$ 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, \dots, x_r les racines de P dans K , alors $K = k[x_1, \dots, x_r]$. D'autre part, soit

$$P = Q_1 \cdots Q_n$$

la décomposition de P en facteurs irréductibles, unitaires, dans $k[X]$. Par hypothèse, chaque Q_j est séparable. Fixons $i \in \{1, \dots, r\}$ et soit P_i le polynôme minimal de x_i sur k . Comme $P(x_i) = 0$, 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. \square

16.4. Le théorème de l'élément primitif. —

Définition 16.19. — 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 $\xi \in K$ tel que $K = k(\xi)$. Dans ce cas, on dit que ξ est un **élément primitif** de K/k .

Théorème 16.20 (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 18 que si k est un corps fini et K/k une extension de degré fini, alors le groupe multiplicatif K^\times est cyclique, et donc $K = k[\xi]$ pour tout générateur ξ de K^\times .

On peut donc supposer k infini. Posons $n = [K : k]$ et soit L une clôture algébrique de K . Comme K/k est séparable, il existe des k -morphisms $K \rightarrow L$ deux à deux distincts τ_1, \dots, τ_n . Alors $\text{Ker}(\tau_i - \tau_j)$ est un sous-espace propre de K , pour tout $i \neq j$.

Lemme 16.21. — Un espace vectoriel V sur un corps infini k n'est pas réunion finie de sous-espaces propres V_1, \dots, V_t .

Démonstration. — C'est clair si $t = 1$. Donc on peut supposer $t \geq 2$ et le résultat établi pour $t - 1$. Alors, il existe $u, v \in V$ tels que $u \notin V_t$ et $v \notin V_1 \cup \dots \cup V_{t-1}$. Supposons

$$V = V_1 \cup \dots \cup V_t.$$

Alors $v \in V_t$. 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 $u \in V_t$, 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. \square

On peut maintenant achever la preuve du théorème de l'élément primitif. D'après le lemme, il existe $x \in K$ n'appartenant à aucun des $\text{Ker}(\tau_i - \tau_j)$. Alors, les $\tau_i(x)$ sont deux à deux distincts. Comme ce sont des racines, dans L , de $\text{Irr}_k(x)$, ceci entraîne $\deg_k(x) \geq n$, et donc

$$n \leq \deg_k(x) = [k(x) : k] \leq [K : k] = n.$$

Il en résulte que $k(x) = K$. Le théorème est démontré. \square

On aura besoin plus loin du raffinement suivant.

Proposition 16.22. — Soit K/k une extension algébrique séparable. On suppose qu'il existe $n \in \mathbb{N}^*$ tel que $\deg_k(x) \leq n$ pour tout $x \in K$. Alors $[K : k]$ est de degré fini $\leq n$, donc K/k admet un élément primitif.

Démonstration. — Prenant n le plus petit possible, on peut supposer qu'il existe $x \in K$ tel que $\deg_k(x) = n$. Soit $y \in K$ 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 $K = k[x]$. Donc $[K : k] = n$ et x est un élément primitif de K/k . \square

Pour terminer cette section, signalons aussi la proposition suivante.

Proposition 16.23. — 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 $K = k[\xi]$ et soit $P = \text{Irr}_k(\xi)$. Soit $k \subseteq L \subseteq K$ une extension intermédiaire et soit $Q = \text{Irr}_L(\xi)$. Alors $[K : L] = \deg Q$. 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 $L' \subseteq L$ 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, $K = L'[\xi]$ est de degré $\deg Q$ sur L' . On a donc

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

d'où $[L : L'] = 1$, c.-à-d., $L = L'$. 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 18).

Choisissons un élément $\xi \in K$ 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 $k[\xi] = K$.

Soit $\alpha \in K$. 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 $L_s = L_t$. 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 $\alpha \in K$ était arbitraire, ceci montre que $k[\xi] = K$. Le théorème est démontré. \square

Remarque 16.24. — Soit $K = \mathbb{F}_p(X, Y)$ 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 $[K : k] = p^2$ et que tout $\alpha \in K$ vérifie $\alpha^p \in k$, et donc $[k[\alpha] : k] \leq p$ (et $= p$ si $\alpha \notin k$). Ceci montre que l'extension $k \subset K$ n'est pas monogène (car de degré p^2), donc admet une infinité de corps intermédiaires.

17. Extensions normales et galoisiennes

17.1. Extensions normales. —

Définition 17.1. — Soit K/k une extension algébrique. On dit que K/k est une extension **normale**, ou **quasi-galoisienne**, si : pour tout $\alpha \in K$, le polynôme minimal $\text{Irr}_k(\alpha)$ a toutes ses racines dans K .

Proposition 17.2. — Soit $P \in k[X]$ de degré $n \geq 1$ et soit K un corps de décomposition de P sur k . L'extension K/k est quasi-galoisienne.

Démonstration. — Soit $\alpha \in K$ et soit $S = \text{Irr}_k(\alpha)$ 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 $L = K$.

Soit β une racine de S dans L . D'après le théorème 15.35, 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 (15.44), τ se prolonge en un k -automorphisme σ de L .

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

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

Définition 17.3. — 1) Soit K/k une extension algébrique. On note $\text{Aut}(K/k)$ le groupe des k -automorphismes de K , c.-à-d.,

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

Si $[K : k] < \infty$, il résulte du théorème 16.16 que $\#\text{Aut}(K/k) \leq [K : k]$.

2) Posons $G = \text{Aut}(K/k)$ et soit $\alpha \in K$. L'ensemble $\{g(\alpha) \mid g \in G\}$ 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 $G\alpha$. D'autre part,

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

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

$$G/G_\alpha \xrightarrow{\sim} G\alpha,$$

où G/G_α désigne l'ensemble des classes à gauche gG_α , pour $g \in G$.

Proposition 17.4. — Soit K/k une extension algébrique et soit $\alpha \in K$.

- 1) Pour tout $g \in \text{Aut}(K/k)$, $g(\alpha)$ est racine de $\text{Irr}_k(\alpha)$.
- 2) Posons $G = \text{Aut}(K/k)$. L'orbite $G\alpha$ est un ensemble fini de cardinal $\leq \deg_k(\alpha)$, et $\text{Irr}_k(\alpha)$ est divisible par le polynôme

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

Démonstration. — Posons $P = \text{Irr}_k(\alpha)$ et écrivons $P = X^d + a_1X^{d-1} + \dots + a_d$, où $d = \deg_k(\alpha)$. Soit $g \in \text{Aut}(K/k)$. Alors

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

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

Par conséquent, $X - g(\alpha)$ divise P , pour tout $g \in G = \text{Aut}(K/k)$. 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 $G\alpha$ est finie, de cardinal $\leq d$, et que P est divisible par le produit des $X - \beta$, pour $\beta \in G\alpha$. La proposition est démontrée. \square

Remarque 17.5. — Au vu de la proposition précédente, on est conduit à se demander si, pour tout $\alpha \in K$, on a l'égalité

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

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

On va voir dans un instant qu'il faut imposer certaines hypothèses, assez naturelles, sur l'extension $k \subset K$ 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 17.6. — 1) Une première obstruction, évidente, à $(*)$ est que K peut ne pas contenir suffisamment de racines de $\text{Irr}_k(\alpha)$. Par exemple, soient $k = \mathbb{Q}$, $P = X^3 - 2$ et ξ l'une quelconque des racines de P dans \mathbb{C} . On a vu dans l'exemple 15.40 que ξ est la seule racine de P dans $\mathbb{Q}[\xi]$. Donc $g(\xi) = \xi$, pour tout $g \in G := \text{Aut}_{\mathbb{Q}}(\mathbb{Q}[\xi])$, et comme $\mathbb{Q}[\xi]$ est engendré sur \mathbb{Q} par ξ , on obtient que $G = \{1\}$.

En fait, si (*) est vérifiée, alors $\text{Irr}_k(\alpha)$ a toutes ses racines dans K . Donc, pour que (*) soit vérifiée pour tout $\alpha \in K$, 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.

17.3. Extensions galoisiennes. —

Définition 17.7. — Soit K/k une extension de degré fini. On dit que K/k est **galoisienne** si $\#\text{Aut}(K/k) = [K : k]$. Dans ce cas, $\text{Aut}(K/k)$ est noté $\text{Gal}(K/k)$. De plus, pour tout $\alpha \in K$, les éléments $g(\alpha)$, pour $g \in \text{Gal}(K/k)$, sont appelés les **conjugués** sur k de α (dans K).

Théorème 17.8 (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., $\#\text{Aut}(K/k) = [K : k]$;
- 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 $\alpha \in K$ on a

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

Démonstration. — On a 3) \Rightarrow 2) d'après la proposition 17.2 et le corollaire 16.18. L'implication 2) \Rightarrow 3) est facile : écrivons $K = k[x_1, \dots, x_n]$ 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, $P = P_1 \cdots P_r$ 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 $G = \text{Aut}(K/k)$ et $n = [K : k]$. Soit L une clôture algébrique de K . D'après le théorème 16.16, il y a exactement n k -morphisms g_1, \dots, g_n de K dans L , et l'on a

$$\#G \leq n = [K : k].$$

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 $\xi \in K$ tel que $K = k[\xi]$. Soit P son polynôme minimal sur k . Fixons $i \in \{1, \dots, n\}$. Alors $g_i(\xi)$ est

racine de $g_i(P) = P$. Comme K/k est normale, P a toutes ses racines dans K , d'où $g_i(\xi) \in K$ et donc $g_i(K) \subseteq K$. De même, on a $g_i^{-1}(K) \subseteq K$, d'où l'égalité

$$g_i(K) = K.$$

Il en résulte que $G = \{g_1, \dots, g_n\} = \text{Hom}_{k\text{-alg}}(K, L)$ est de cardinal $n = [K : k]$, 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 $K \rightarrow L'$, d'où alors $\phi(K) = K$.

Montrons que 1) \Rightarrow 2). Supposons K/k galoisienne, c.-à-d., supposons que $G = \text{Aut}(K/k)$ soit de cardinal $n = [K : k]$. Alors, d'après le théorème 16.16, K/k est séparable. Montrons que K/k est normale.

Soient $\alpha \in K$ 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 $\beta \in K$.

D'après la proposition 15.39 (ou 16.14), il existe un (unique) k -isomorphisme

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

Comme L est algébriquement clos alors, d'après le théorème 15.54, τ se prolonge en un k -morphisme $\sigma : K \rightarrow L$. Or, d'après l'hypothèse, d'une part, et le théorème 16.16, d'autre part, on a l'égalité (1) et l'inégalité (2) ci-dessous :

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

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

$$\beta = \sigma(\alpha) \in K.$$

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

Lemme 17.9. — Soient R un anneau et τ un automorphisme de R . Alors τ s'étend en un automorphisme ϕ_τ de $R[X]$, défini par

$$\phi_\tau(P) = \tau(a_0) + \dots + \tau(a_d)X^d \quad \text{si} \quad P = a_0 + \dots + a_dX^d;$$

et l'on a : $\phi_\tau(P) = P \Leftrightarrow \tau(a_i) = a_i$, pour $i = 0, \dots, d$. 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. \square

Théorème 17.10 (Artin). — Soient K un corps et G un sous-groupe fini de $\text{Aut}(K)$. Posons

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

c'est un sous-corps de K . Alors, l'extension K/K^G est galoisienne, et l'on a

$$\text{Gal}(K/K^G) = G \quad \text{et} \quad [K : K^G] = \#G.$$

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

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

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

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

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

Proposition 17.11. — On a $\text{Irr}_k(\alpha) = P_\alpha = \prod_{\beta \in A} (X - \beta)$, et donc α est séparable sur k et l'extension K/k est galoisienne.

Démonstration. — On a $P_\alpha \in k[X]$ et $P_\alpha(\alpha) = 0$, donc P_α est multiple de $\text{Irr}_k(\alpha)$. D'autre part, d'après la proposition 17.4, $\text{Irr}_k(\alpha)$ est divisible par le polynôme

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

qui est de degré $\geq \#G\alpha$, puisque $G \subseteq \mathcal{G}$. Il en résulte que

$$P_\alpha = \text{Irr}_k(\alpha) \quad \text{et} \quad G\alpha = \mathcal{G}\alpha.$$

Donc $\text{Irr}_k(\alpha)$ a des racines simples, toutes dans K , et ceci montre que l'extension K/k est séparable et normale, donc galoisienne (d'après 17.8). Ceci prouve la proposition. \square

Achevons maintenant la démonstration du théorème d'Artin. Posons $n = [K : k]$. Comme $G \subseteq \mathcal{G} = \text{Gal}(K/k)$, on a, d'après le théorème 16.16,

$$\#G \leq \#\mathcal{G} \leq [K : k] = n.$$

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

$$\deg_k(\alpha) = \deg P_\alpha = \#G\alpha \leq \#G.$$

Donc, d'après la proposition 16.22, on a $[K : k] \leq \#G$. Combiné avec les inégalités précédentes, ceci entraîne que

$$G = \mathcal{G} = \text{Gal}(K/k) \quad \text{et} \quad [K : k] = \#G.$$

Le théorème d'Artin est démontré. \square

Corollaire 17.12. — Soient K/k une extension galoisienne et $G = \text{Gal}(K/k)$. Alors $K^G = k$.

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

$$[K : K^G] = \#G,$$

et donc l'inclusion $k \subseteq K^G$ est une égalité. \square

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

Définition 17.13. — Soit G un groupe. Un sous-groupe H est dit **normal**, ou **distingué**, s'il vérifie $gHg^{-1} = H$, pour tout $g \in G$. Dans ce cas, on écrira

$$H \triangleleft G \quad \text{ou} \quad G \triangleright H.$$

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

Exemple 17.1. — Soit $\phi : G \rightarrow G'$ un morphisme de groupes. Son noyau $\text{Ker } \phi = \{h \in G \mid \phi(h) = 1\}$ est un sous-groupe normal. En effet, pour tout $h \in \text{Ker } \phi$ et $g \in G$, on a

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

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

Définition 17.14 (Classes à gauche). — Soient G un groupe et H un sous-groupe quelconque (c.-à-d., pas nécessairement normal). Pour tout $g \in G$, on pose

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

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

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

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

Remarque 17.15. — 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 $\pi : G \rightarrow G/H$ soit un morphisme. Rappelons la construction.

Proposition 17.16. — *Soit H un sous-groupe normal de G .*

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

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

Le noyau de $\pi : G \rightarrow G/H$ 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

$$g'_1g'_2 = g_1h_1g_2h_2 = g_1g_2(g_2^{-1}h_1g_2)h_2.$$

Or, par hypothèse, $g_2^{-1}h_1g_2 \in H$ et il en résulte que $g'_1g'_2H = g_1g_2H$. 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 $\pi : G \rightarrow G/H$ est un morphisme de groupes surjectif. Enfin, $\text{Ker } \pi = \{g \in G \mid gH = H\}$ égale H . Ceci prouve le point 1). Le point 2) est laissé au lecteur, cf. la discussion précédant le théorème 4.5 (Chap. I). \square

Théorème 17.17 (Propriété universelle du noyau). — *Soit $\phi : G \rightarrow G'$ un morphisme de groupes et soit K un sous-groupe normal de G contenu dans $\text{Ker } \phi$. Notons π la projection $G \rightarrow G/K$.*

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

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

$$\bar{\phi} : G/\text{Ker } \phi \xrightarrow{\cong} \phi(G).$$

Démonstration. — La démonstration est analogue à celle du théorème 4.10 (Chap. I) et est laissée au lecteur. \square

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

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

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

Théorème 17.18 (Correspondance de Galois). — Soit K/k une extension de degré fini galoisienne, et soit $G = \text{Gal}(K/k)$.

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

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

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

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

3) Par conséquent, les applications

$$H \mapsto K^H \quad \text{et} \quad L \mapsto \text{Gal}(K/L)$$

sont des bijections réciproques entre les deux ensembles suivants :

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

Si L et H se correspondent, on a

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

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

$$H \subseteq H' \Leftrightarrow K^H \supseteq K^{H'} \quad \text{et} \quad L \subseteq L' \Leftrightarrow \text{Gal}(K/L) \supseteq \text{Gal}(K/L').$$

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

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

$$L/k \text{ galoisienne} \Leftrightarrow L/k \text{ normale} \Leftrightarrow H \text{ normal dans } G.$$

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

6) Soient L un corps intermédiaire et $H = \text{Gal}(K/L)$. Alors les bijections de 3) induisent une bijection entre l'ensemble des sous-extensions $k \subseteq L' \subseteq L$ 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 $x \in K$ et P le polynôme minimal de x sur L . Alors P divise $\text{Irr}_k(x)$, 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

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

c'est un sous-groupe de

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

et l'on a $L = K^H$ d'après le corollaire 17.12. 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 $g \in G$, on a

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

donc $g(L)$ correspond à gHg^{-1} .

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

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

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

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

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

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

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

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

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

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

$$G \xrightarrow{\text{res}} \text{Gal}(L/k), \quad g \mapsto g|_L$$

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

$$\{g \in G \mid g|_L = \text{id}_L\} = \text{Gal}(K/L) = H.$$

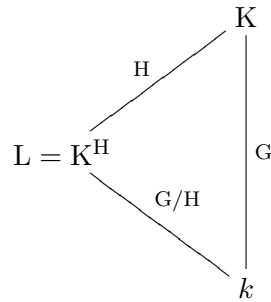
Il en résulte que l'application de restriction est surjective, et induit un isomorphisme de groupes

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

Ceci prouve le point 5).

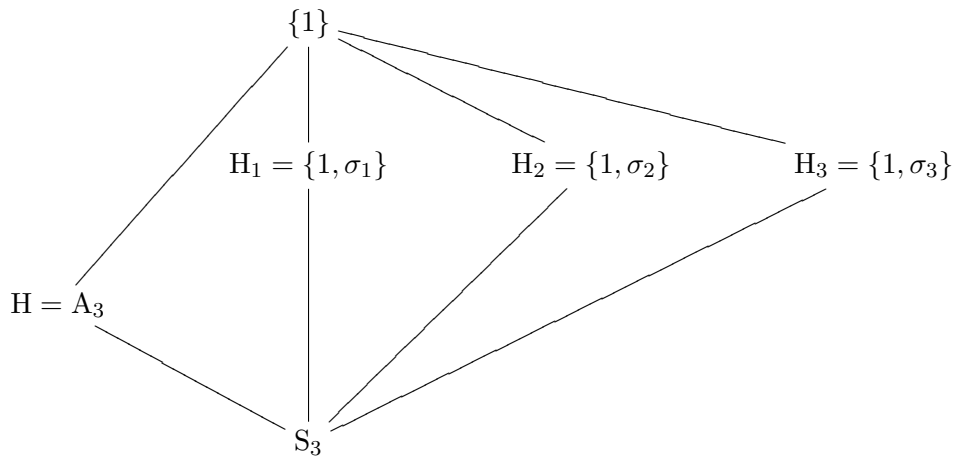
Enfin, le point 6) est une conséquence immédiate du point 3). Le théorème est démontré. \square

Remarque 17.19. — On peut résumer le théorème, et en particulier le point 5), par le diagramme suivant :

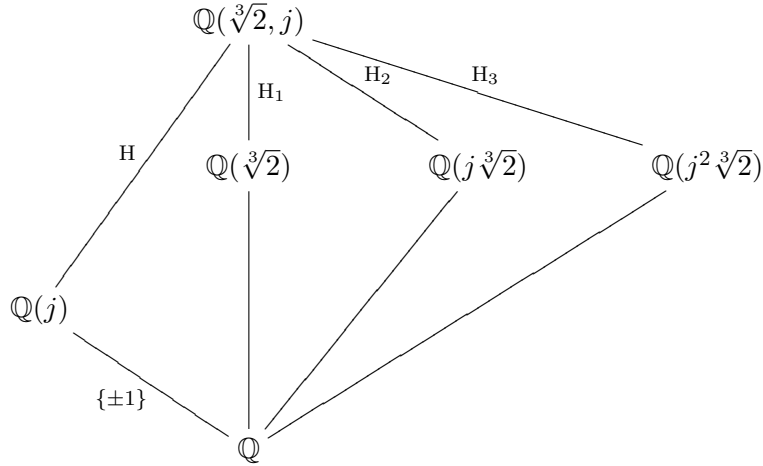


Ce diagramme, et les deux exemples qui suivent, sont empruntés au polycopié de Jan Nekovář [Ne04].

Exemple 17.20. — 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 $\mathbb{Q} \subseteq L \subseteq \mathbb{Q}(\sqrt[3]{2}, j)$:

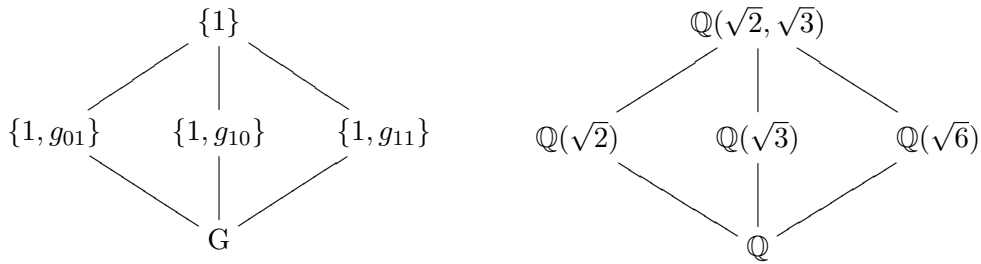


On a $H = A_3 \triangleleft S_3$, et l'application signature $\varepsilon : S_3 \rightarrow \{\pm 1\}$ induit un isomorphisme de groupes $\text{Gal}(\mathbb{Q}(j)/\mathbb{Q}) \cong S_3/A_3 \cong \{\pm 1\}$.

Exemple 17.21. — Soit $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ et soit

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

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



17.5. 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. 16.5), une condition nécessaire est que K/k soit séparable. On va voir que cette condition est également suffisante.

Théorème 17.22 (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 $\text{car}(k) = 0$, toute extension K/k de degré fini est contenue dans une extension galoisienne L/k .

Démonstration. — Soit $\alpha_1, \dots, \alpha_r$ un système de générateurs de K sur k et soit P_i le polynôme minimal sur k de α_i . Posons $P = P_1 \cdots P_r$ 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 17.2.

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 $\alpha_1, \dots, \alpha_r$, et donc toutes les racines de chaque $P_i = \text{Irr}_k(\alpha_i)$. Par conséquent, $L' = L$. 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 15.44, il existe un K -isomorphisme $\tau : L \xrightarrow{\sim} L'$. Si de plus, E est supposée minimale, alors $E = L'$ et donc E est K -isomorphe à L .

Enfin, si K/k est séparable, alors P_1, \dots, 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 17.8. Ceci prouve le théorème. \square

Corollaire 17.23. — Soit $k \subset K$ une extension séparable de degré fini. Le nombre d'extensions intermédiaires $k \subseteq L \subseteq K$ est fini.

Démonstration. — Soient \tilde{K} une clôture galoisienne de K/k et $G = \text{Gal}(\tilde{K}/k)$. C'est un groupe fini, de cardinal $[\tilde{K} : k]$. D'après le point 6) du théorème 17.18, les extensions intermédiaires $k \subseteq L \subseteq K$ sont en bijection avec l'ensemble des sous-groupes de G contenant $H = \text{Gal}(\tilde{K}/K)$, qui est un ensemble fini. \square

18. Corps finis

18.1. Cardinal et groupe multiplicatif d'un corps fini. — 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 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 18.1. — 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 $p = \text{car}(k)$ 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. \square

Corollaire 18.2. — Si k est un corps fini de caractéristique p , alors le cardinal de k est une puissance de p .

Théorème 18.3 (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 $d_1 \geq \dots \geq d_r > 1$ tels que d_i divise d_{i-1} , pour $i = r, r - 1, \dots, 2$ et

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

Alors, d'une part, $|k^\times| = d_1 d_2 \dots d_r$ et, d'autre part, tout élément $x \in k^\times$ vérifie $x^d = 1$, où $d = d_1$. Or, comme $k[X]$ est intègre, le polynôme $X^d - 1$ 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. \square

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

Théorème 18.4 (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 $\text{Irr}_{\mathbb{F}_q}(\xi)$ est de degré n .

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

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

Lemme 18.5. — Soient K un corps et τ un endomorphisme de K . Alors l'ensemble des éléments invariants

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

est un sous-corps de K .

Démonstration. — C'est clair. \square

Théorème 18.6 (Existence et unicité de \mathbb{F}_q). — Soient p un nombre premier, $n \geq 1$ et $q = p^n$. Soit K un corps de décomposition sur \mathbb{F}_p du polynôme $X^q - X$. Alors, $|K| = q$. 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 $Q := X^q - X$ 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 16.11, 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 $K = K_1$, 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 18.3, le groupe multiplicatif L^\times est cyclique, d'ordre $q-1$. Donc, tout élément $x \in L^\times$ vérifie

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

Donc, tout élément de $L = L^\times \cup \{0\}$ est une racine du polynôme $Q = X^q - X$. Comme $|L| = q$, 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 15.42, L est isomorphe à K . Le théorème est démontré. \square

Théorème 18.7 (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 18.1) 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

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

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

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

Donc $X^q - X$ divise $X^{q^r} - X$ 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 18.3, le groupe multiplicatif L^\times est cyclique, d'ordre $q - 1$. Donc, tout élément $x \in L^\times$ vérifie

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

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

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

Lemme 18.8. — *Soit G un groupe fini.*

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

2) *Soit $g \in G$. 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 $d \geq 1$, 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 $gH \neq g'H$ sont disjointes. En effet, sinon il existerait $h, h' \in H$ tels que $gh = g'h'$, et l'on aurait $gH = g'H$. De plus, chaque classe gH est de cardinal $|H|$, puisque l'application $H \mapsto gH$, $h \mapsto gh$ est une bijection. Donc G est la réunion disjointe de $|G/H|$ classes, chacune de cardinal $|H|$. Le point 1) en résulte.

Soit $g \in G$. On pose $g^0 = 1$. Comme G est fini, les éléments g^k , $k \geq 1$, 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 $d \geq 1$, et le reste du point 2) s'obtient facilement. \square

Théorème 18.9 (L'isomorphisme $\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$). — Soient $n \geq 1$ 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 $\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ 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 $Q = X^{q^n} - X$ sur \mathbb{F}_q , donc a fortiori sur \mathbb{F}_q . De plus, Q a des racines distinctes dans \mathbb{F}_{q^n} (puisque $Q' = -1$) donc est séparable sur \mathbb{F}_q . Donc, d'après le théorème 17.8, l'extension $\mathbb{F}_q \subseteq \mathbb{F}_{q^n}$ est galoisienne, et l'on a

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

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

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

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

18.4. Polynômes irréductibles sur \mathbb{F}_q . — D'après le point 2) du théorème 18.4, on a la proposition suivante.

Proposition 18.10. — Pour tout corps fini \mathbb{F}_q , et tout $n \geq 1$, il existe dans $\mathbb{F}_q[X]$ au moins un polynôme irréductible unitaire de degré n .

Définition 18.11. — Pour tout $d \geq 1$, 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 18.12. — Pour tout $n \geq 1$, on a

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

Par conséquent,

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

Démonstration. — Fixons $n \geq 1$. 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 18.9, l'extension $\mathbb{F}_q \subseteq \mathbb{F}_{q^d}$ est

galoisienne, alors $P = \text{Irr}_{\mathbb{F}_q}(\alpha)$ est scindé sur \mathbb{F}_{q^d} . Par conséquent, P divise le polynôme

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

De plus, on a vu dans la preuve du théorème 18.7 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 18.7), et de l'égalité

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

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 $R = \text{Irr}_{\mathbb{F}_q}(\alpha)$ 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 18.7, ceci entraîne que $d \mid n$. Ceci montre que Q_n n'a pas d'autres facteurs irréductibles que les $P \in I(d, q)$, 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. \square

Théorème 18.13 (Polynômes irréductibles sur \mathbb{F}_q). — Soit $P \in I(d, q)$ et soit $\alpha \in \mathbb{F}_{q^d}$ une racine de P . Alors,

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

Démonstration. — D'après le théorème 18.9, l'extension $\mathbb{F}_q \subseteq \mathbb{F}_{q^d}$ est galoisienne, de groupe

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

D'autre part, d'après la proposition 17.4, l'on a :

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

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

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

Posons $K_0 = \mathbb{F}_p$ et pour tout $i \geq 1$, soit K_i un corps de décomposition sur K_{i-1} du polynôme

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

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

$$K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots$$

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

Proposition 18.14 (Premières propriétés de $\overline{\mathbb{F}}_p$). —

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

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

Démonstration. — 1) Soient $d \geq 1$ 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 $X^q - X$ 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 L^\times est cyclique d'ordre $q - 1$, les éléments de L sont exactement les racines dans $\overline{\mathbb{F}}_p$ du polynôme $X^q - X$, c.-à-d., les éléments de \mathbb{F}_q . Ceci prouve le point 1).

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

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

Fixons $q = p^r$ et montrons que

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

Pour tout $i \geq 1$, 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 $n \geq 1$. 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. \square

Théorème 18.15 (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 $i \geq 1$ tel que $x \in \mathbb{F}_{p^{mi}}$, 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 $P = X^d + a_1X^{d-1} + \dots + a_d \in \overline{\mathbb{F}_p}[X]$, non constant. Il existe $i \geq 1$ tel que $a_0, \dots, a_d \in \mathbb{F}_{p^i}$. Soit K un corps de décomposition de P sur \mathbb{F}_{p^i} et soit $r = [K : \mathbb{F}_{p^i}]$. 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 $K = \overline{\mathbb{F}_p}$ et, pour tout $n \geq 1$, 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,

$$(1) \quad K = \bigcup_{n \geq 1} K_n.$$

Considérons une extension $\mathbb{F}_q \subset L$ et supposons que L soit une clôture algébrique de \mathbb{F}_q . Comme L est algébriquement clos, le polynôme $Q_n := X^{q^{n!}} - X \in L[X]$ 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 $x \in L$. 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

$$(2) \quad L = \bigcup_{n \geq 1} L_n.$$

Montrons maintenant, par récurrence sur n , qu'on peut prolonger l'identification $L_1 = K_1 = \mathbb{F}_q$ en un \mathbb{F}_q -isomorphisme $\tau_n : L_n \xrightarrow{\sim} K_n$.

Supposons l'assertion établie au cran n . Commençons par remarquer que $\tau_n(Q_{n+1}) = Q_{n+1}$, 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 15.44, τ_n se prolonge en un \mathbb{F}_q -isomorphisme $\tau_{n+1} : L_{n+1} \xrightarrow{\sim} K_{n+1}$.

On obtient ainsi une suite infinie (τ_1, τ_2, \dots) d'isomorphismes $\tau_n : L_n \xrightarrow{\sim} K_n$, tels que $\tau_1 = \text{id}_{\mathbb{F}_q}$ et

$$(3) \quad \forall r \geq n, \quad \tau_r|_{L_n} = \tau_n.$$

On définit alors $\tau : L \rightarrow K$ par la formule : $\tau(x) = \tau_n(x)$ si $x \in L_n$. 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 $n \geq 1$, donc égale K . Par conséquent, τ est un \mathbb{F}_q -isomorphisme de L sur K . Le théorème est démontré. \square

TABLE DES MATIÈRES

I. Les anneaux de la géométrie algébrique ou de la théorie des nombres	1
1. Courbes algébriques et fonctions polynomiales	1
1.1. Courbes algébriques	1
1.2. Fonctions polynomiales	2
1.3. Espaces tangents	4
1.4. Sous-variétés algébriques de \mathbb{C}^n	4
1.5. Morphismes	6
1.6. Fonctions rationnelles	7
1.7. Sujet du cours	8
2. Anneaux de nombres	8
2.1. Notations et définitions	8
2.2. Division euclidienne et conséquences	9
2.3. Solutions entières de $x^2 + y^2 = z^2$	13
2.4. Somme de deux carrés et entiers de Gauss	14
2.5. Les anneaux de nombres $\mathbb{Z}[\sqrt{n}]$	18
2.6. Les anneaux $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ et $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$	20
2.7. Entiers algébriques	21
II. Anneaux et modules	25
3. Anneaux et modules	25
3.0. Complément d'introduction	25
3.1. Anneaux	25
3.2. Morphismes	27
3.3. A-modules	28
4. Modules et anneaux quotients, théorèmes de Noether	31
4.1. Définition des modules quotients	31
4.2. Noyaux et théorèmes de Noether	34

5. Construction de modules ou d'idéaux	37
5.1. Sous-module ou idéal engendré	37
5.2. Sommes de sous-modules et sommes directes	38
5.3. Sommes et produits d'idéaux	39
5.4. Racine d'un idéal, et idéaux premiers	40
6. Modules libres	42
6.1. Définitions et exemples	42
6.2. Les modules libres $A^{(I)}$	44
III. Anneaux de polynômes, conditions de finitude	47
7. Anneaux de polynômes	47
7.1. Polynômes en une variable	47
7.2. Polynômes à n variables	49
8. Conditions de finitude	51
8.1. Union filtrante de sous-modules	51
8.2. Modules de type fini	52
8.3. Anneaux et modules noethériens	55
8.4. Le théorème de transfert de Hilbert	57
IV. Anneaux factoriels, principaux, euclidiens	
<i>Semaine du 1er octobre</i>	61
9. Anneaux factoriels	61
9.1. Une motivation	61
9.2. Anneaux intègres	61
9.3. Divisibilité, éléments irréductibles	62
9.4. Anneaux factoriels, lemmes d'Euclide et Gauss	65
9.5. Anneaux principaux et anneaux euclidiens	67
9.6. PPCM et PGCD dans un anneau factoriel	69
9.7. Corps des fractions d'un anneau intègre	71
9.8. Corps des fractions d'un anneau factoriel	73
9.9. Le théorème de transfert de Gauss	73
9.10. Sous-variétés algébriques fermées de \mathbb{C}^2	77
9.11. Exemples d'anneaux noethériens non factoriels	80
V. Extensions algébriques, théorème des zéros	
<i>Semaine du 8 octobre</i>	83
10. Extensions de corps	83
10.1. Généralités sur les extensions de corps	83
10.2. L'alternative algébrique/transcendant	85
10.4. Extensions algébriques et degré	86
10.5. Corps algébriquement clos	89
10.6. \mathbb{C} est algébriquement clos	89

11. Le théorème des zéros de Hilbert	91
11.1. Idéaux maximaux de $\mathbb{C}[X_1, \dots, X_n]$	91
11.2. Sous-variétés algébriques de \mathbb{C}^n	92
11.3. Composantes irréductibles	95
11.4. Topologie de Zariski	97
VI. Compléments sur les modules, théorème chinois, facteurs invariants	
<i>Séances du 15, 16 et 22 octobre</i>	99
12. Compléments sur les modules	99
12.1. Théorème de Zorn et conséquences	99
12.2. Rang d'un module libre de type fini	101
12.3. Annulateurs et modules de torsion	102
12.4. Modules d'homomorphismes et module dual	103
12.5. Suites exactes	104
12.6. Anneaux d'endomorphismes	105
13. Théorème chinois et applications	107
13.1. Idéaux étrangers	107
13.2. Théorème chinois des restes	110
13.3. Modules se décomposant en composantes primaires	111
13.4. Décomposition primaire des modules de torsion sur un anneau principal	113
14. Modules de type fini sur un anneau principal	118
14.1. Structure des modules de type fini sur un anneau principal ...	118
14.2. Un exemple	121
14.3. Réduction des matrices	122
14.4. Décomposition en somme de modules monogènes	129
14.5. Autre démonstration	134
VII. Extensions de corps : caractéristique, corps de rupture, corps de décomposition, clôtures algébriques	
<i>Séances du 23, 29 et 30 octobre</i>	137
15. Construction d'extensions de corps	137
15.1. Généralités sur les extensions de corps	137
15.2. Sous-corps premier et caractéristique	139
15.3. Endomorphismes de Frobenius	140
15.4. Éléments algébriques et polynômes minimaux	142
15.5. Extensions de degré fini	144
15.6. Corps de rupture d'un polynôme irréductible	145
15.7. Corps de décomposition d'un polynôme	147
15.8. Extensions algébriques et clôtures algébriques	150
15.9. Bases de transcendance	155

VIII. Extensions normales, séparables, galoisiennes. Corps finis

<i>Séances du 5, 6, 12 et 13 novembre</i>	159
16. Extensions séparables et théorème de l'élément primitif	159
16.1. Polynômes et extensions séparables	159
16.2. Racines multiples et séparabilité	160
16.3. Caractérisation de la séparabilité en termes de morphismes ...	162
16.4. Le théorème de l'élément primitif	165
17. Extensions normales et galoisiennes	167
17.1. Extensions normales	167
17.2. Le groupe des k -automorphismes d'une extension	167
17.3. Extensions galoisiennes	169
17.4. Correspondance de Galois	172
17.5. Clôture normale ou galoisienne	177
18. Corps finis	178
18.1. Cardinal et groupe multiplicatif d'un corps fini	178
18.2. Existence et unicité des corps \mathbb{F}_{p^n}	180
18.3. Groupe de Galois de \mathbb{F}_{q^n} sur \mathbb{F}_q	181
18.4. Polynômes irréductibles sur \mathbb{F}_q	182
18.5. Le corps $\overline{\mathbb{F}_p}$	184
Bibliographie	v

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.
- [Ca] J.-C. Carrega, Théorie des corps – La règle et le compas, Hermann, 1981, 2ème édition 1989.
- [ChL] A. Chambert-Loir, Algèbre corporelle, Éditions de l'École Polytechnique, 2005.
- [Co] H. S. M. Coxeter, Introduction to Geometry, 2nd edition, Wiley, 1969.
- [De] R. Dedekind, Sur la théorie des nombres entiers algébriques, Gauthier-Villars, 1877; traduit en anglais avec une introduction de J. Stillwell dans : Theory of algebraic integers, Cambridge Univ. Press, 1996.
- [Die] J. Dieudonné, Cours de géométrie algébrique, tome 2, P.U.F., 1974.
- [Dou] A. Douady, R. Douady, Algèbre et théories galoisiennes, Cedic Fernand Nathan, 1977, 2ème éd., Cassini, 2005.
- [Elk] R. Elkik, Cours d'algèbre, Ellipses, 2002.
- [Fu] W. Fulton, Algebraic Curves, Benjamin, 1969.
- [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/~nekoar/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.
- [Re] M. Reid, Undergraduate commutative algebra, Cambridge Univ. Press, 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.
- [vdW] B. L. van der Waerden, History of algebra from al-Khwarizmi to Emmy Noether, Springer Verlag, 1985.