**Cours d'algèbre commutative**

# 1 Premiers résultats sur les extension de corps

## 1.1 Extension de corps - extension finie et algébrique -degré

**Définition 1.1.** Soit $\mathbf{k}$ un corps. Une extension du corps $\mathbf{k}$ est la donnée d'un corps $\mathbb{K}$ et d'un morphisme de corps (non nul) $j : \mathbf{k} \to \mathbb{K}$ (il est donc injectif).
On note $\mathbb{K}/\mathbf{k}$ une telle extension.

**Remarque 1.2.** En pratique, $\mathbf{k}$ sera souvent une partie de $\mathbb{K}$ et donc l'application $j$ sera simplement l'application de l'inclusion.

Pour une extension $\mathbb{K}/\mathbf{k}$, $\mathbb{K}$ est un $\mathbf{k}$-espace vectoriel.

**Définition 1.3.** Une extension $\mathbb{K}/\mathbf{k}$ est dite finie si la dimension de $\mathbb{K}$ sur $\mathbf{k}$ est finie, et on note $[\mathbb{K} : \mathbf{k}]$ cette dimension. On appelle $[\mathbb{K} : \mathbf{k}]$ le degré de l'extension.
Une base de $\mathbb{K}$ sur $\mathbf{k}$ est appellée une base de l'extension.

**Proposition 1.4.** Soient $\mathbb{L}/\mathbb{K}$ et $\mathbb{K}/\mathbf{k}$ deux extension (et donc $\mathbb{L}/\mathbf{k}$ est une extension) alors on a équivalence entre :

1. L'extension $\mathbb{L}/\mathbf{k}$ est finie.
2. Les extensions $\mathbb{L}/\mathbb{K}$ et $\mathbb{K}/\mathbf{k}$ sont finies.

De plus, dans le cas où ces assertions sont vraies, on a

$$[\mathbb{L}/\mathbf{k}] = [\mathbb{L}/\mathbb{K}][\mathbb{K}/\mathbf{k}].$$

*Démonstration.* Supposons $[\mathbb{L}/\mathbf{k}]$ finie.
On a $\mathbb{K} \subseteq \mathbb{L}$ donc $\dim_{\mathbf{k}}(\mathbb{K}) \leq \dim_{\mathbf{k}}(\mathbb{L}) = [\mathbb{L} : \mathbf{k}]$, d'où la finitude de $[\mathbb{K} : \mathbf{k}]$.
D'autre part, si une famille $l_1, \ldots, l_p$ de $\mathbb{L}$ est libre sur $\mathbb{K}$, elle le sera sur $\mathbf{k}$. Ainsi, si $[\mathbb{L} : \mathbb{K}]$ était infini alors on pourrait construire une telle famille avec un cardinal aussi grand que l'on veut ce qui contredirait la finitude de $[\mathbb{L} : \mathbf{k}]$.
Voyons l'implication réciproque.
Soit $(l_1, \ldots, l_p)$ une base de $\mathbb{L}$ sur $\mathbb{K}$ et soit $(K_1, \ldots, K_q)$ une base de $\mathbb{K}$ sur $\mathbf{k}$. Le reste de la démonstration consiste à montrer que la famille $(K_j l_i \mid 1 \leq i \leq p,\ 1 \leq j \leq q)$ de $\mathbb{L}$ est libre et génératrice sur $\mathbf{k}$, ce que nous laissons en exercice. □

**Définition 1.5.** Soit $\mathbb{K}/\mathbf{k}$ une extension et soit $\alpha \in \mathbb{K}$. On dit que $\alpha$ est algébrique sur $\mathbf{k}$ s'il existe $P$ non nul dans $\mathbf{k}[x]$ tel que $P(\alpha) = 0$. Sinon $\alpha$ est dit transcendant. L'extension $\mathbb{K}/\mathbf{k}$ est dite algébrique si chaque $\alpha \in \mathbb{K}$ est algébrique.

**Définition 1.6.** Étant donné $\alpha \in \mathbb{K}$ algébrique sur $\mathbf{k}$, le générateur unitaire de l'idéal

$$\{P \in \mathbf{k}[x] \mid P \neq 0, P(\alpha) = 0\}$$

noté $\mu_\alpha$ (ou $\mu_{\alpha,\mathbf{k}}$ si nécessaire) est appelé polynôme minimal de $\alpha$ sur $\mathbf{k}$.

**Proposition 1.7.** Soient $\mathbb{K}/\mathbf{k}$ une extension et $\alpha \in \mathbb{K}$.

1. On a l'équivalence : $\alpha$ est algébrique sur $\mathbf{k} \iff$ l'extension $\mathbf{k}(\alpha)/\mathbf{k}$ est finie.
2. Dans le cas où $\alpha$ est algébrique, on a :
   — $\mu_\alpha \in \mathbf{k}[x]$ est irréductible,
   — $[\mathbf{k}(\alpha) : \mathbf{k}] = \deg(\mu_\alpha)$,
   — $\mathbf{k}(\alpha) = \mathbf{k}[\alpha]$.

*Démonstration.* Supposons $\alpha$ algébrique sur $\mathbf{k}$.
Considérons $\varphi : \mathbf{k}[x] \to \mathbb{K}$ tel que $\varphi(P) = P(\alpha)$. Alors $\ker(\phi)$ n'est rien d'autre que l'idéal considéré plus haut. Par conséquent

$$\mathbf{k}[x]/\langle \mu_\alpha \rangle \simeq \mathrm{Im}(\varphi) = \mathbf{k}[\alpha].$$

L'anneau $\mathbf{k}[\alpha]$ est intègre donc $\langle \mu_\alpha \rangle$ est premier et donc $\mu_\alpha$ est irréductible (car dans un anneau factoriel). Mais comme $\mathbf{k}[x]$ est principal, $\langle \mu_\alpha \rangle$ est maximal et donc $\mathbf{k}[x]/\langle \mu_\alpha \rangle$ est un corps ; ainsi $\mathbf{k}[\alpha]$ est un corps ce qui entraine l'égalité $\mathbf{k}[\alpha] = \mathbf{k}(\alpha)$.
Notons $d$ le degré de $\mu_\alpha$. Soit $P \in \mathbf{k}[x]$ alors par division euclidienne, on peut écrire

$$P = Q\mu_\alpha + a_0 \cdot 1 + a_1 \cdot x + \cdots + a_{d-1}x^{d-1}.$$

D'où $\overline{P} = \sum_0^{d-1} a_i \overline{x^i}$. On a donc une famille génératrice de $\mathbf{k}[x]/\langle \mu_\alpha \rangle$ donnée par : $\bar{1}$, …, $\overline{x^{d-1}}$. On voit alors qu'elle est libre car sinon on aurait un polynôme annulateur de $\alpha$ de degré inférieur. Ainsi $\dim(\mathbf{k}[x]/\langle \mu_\alpha \rangle) = d$.
Il reste la réciproque du 1. Notons $d = [\mathbf{k}(\alpha) : \mathbf{k}]$.
Alors la famille $1, \alpha, \ldots, \alpha^d$ est liée dans $\mathbf{k}(\alpha)$ donc il existe des $a_i \in \mathbf{k}$ tels que : $a_0 1 + a_1\alpha + \cdots + a_d\alpha^d = 0$, d'où l'existence d'un polynôme annulateur de $\alpha$ non nul dans $\mathbf{k}[x]$. □

La fin de cette démonstration montre en particulier que :

**Proposition 1.8.** Toute extension $\mathbb{K}/\mathbf{k}$ finie est algébrique.

La proposition précédente a aussi pour conséquence le résultat suivant.

**Corollaire 1.9.** Soit $\mathbb{K}/\mathbf{k}$ une extension.

1. Soit $M$ une partie de $\mathbb{K}$ formée d'éléments algébriques sur $\mathbf{k}$ alors l'extension $\mathbf{k}(M)/\mathbf{k}$ est algébrique et on a $\mathbf{k}[M] = \mathbf{k}(M)$.
   De plus, si $M$ est de cardinal fini alors l'extension $\mathbf{k}(M)/\mathbf{k}$ est finie.
2. Soit $E$ l'ensemble des éléments $\alpha \in \mathbb{K}$ qui sont algébriques sur $\mathbf{k}$. Alors $E$ est un sous-corps de $\mathbb{K}$ (et c'est une extension de $\mathbf{k}$).
3. Soit $E$ un corps intermédiaire $\mathbf{k} \subseteq E \subseteq \mathbb{K}$ alors : $\mathbb{K}/\mathbf{k}$ est algébrique si et s. si $\mathbb{K}/E$ et $E/\mathbf{k}$ le sont.

*Démonstration.* 1. Soit $\alpha \in \mathbf{k}(M)$, le but étant de montrer qu'il est algébrique sur $\mathbf{k}$. Il existe $y_1, \dots, y_d \in M$ tels que $x \in \mathbf{k}(y_1, \dots, y_d)$. Chaque $y_i$ est algébrique sur $\mathbf{k}$ donc sur $\mathbf{k}(y_1, \dots, y_{i-1})$, donc pour tout $i$, l'extension $\mathbf{k}(y_1, \dots, y_i)/\mathbf{k}(y_1, \dots, y_{i-1})$ est finie ce qui entraine la finitude de l'extension $\mathbf{k}(y_1, \dots, y_d)/\mathbf{k}$. Mais $\mathbf{k}(\alpha)$ est un sous-espace vectoriel de $\mathbf{k}(y_1, \dots, y_d)$, il est donc de dimension finie sur $\mathbf{k}$ et $\alpha$ est algébrique.

Montrons que $\mathbf{k}[M] = \mathbf{k}(M)$. Pour cela il suffit de montrer que $\mathbf{k}[M]$ est stable par inverse ce qui en fera un corps et la conclusion en découlera. Soit alors $\alpha \in \mathbf{k}[M]$, $\alpha \neq 0$. On sait que $\mathbf{k}[\alpha] = \mathbf{k}(\alpha)$ donc $\alpha^{-1} \in \mathbf{k}[\alpha] \subseteq \mathbf{k}[M]$.

Enfin, si $M = \{y_1, \dots, y_d\}$, on a vu que l'extension $\mathbf{k}(M)/\mathbf{k}$ est finie.

2. On a $E \subset \mathbf{k}(E)$. Par le 1., on a l'inclusion inverse.

3. Supposons $\mathbb{K}/\mathbf{k}$ algébrique.

   Alors tout élément de $\mathbb{K}$ admet un polynôme annulateur dans $\mathbf{k}[X] \setminus \{0\}$ donc dans $E[X] \setminus \{0\}$, donc $\mathbb{K}/E$ est algébrique. De même si $\alpha \in E$ alors $\alpha \in \mathbb{K}$ et il est algébrique sur $\mathbf{k}$.

   Réciproquement on suppose $\mathbb{K}/E$ et $\mathbb{K}/\mathbf{k}$ algébriques.

   Soit $\alpha \in \mathbb{K}$ et $\mu_{\alpha,E} = X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in E[X]$. On a $\mathbf{k} \subseteq \mathbf{k}(a_1, \dots, a_d) \subseteq \mathbf{k}(\alpha, a_1, \dots, a_d)$. Ces deux extensions sont finies : la première par 1 et la seconde parce que $\alpha$ est algébrique sur $\mathbf{k}(a_1, \dots, a_d)$, ce qui entraine la finitude de l'extension $k(\alpha, a_1, \dots, a_d)/\mathbf{k}$ et donc de la sous-extension $\mathbf{k}(\alpha)/\mathbf{k}$ et donc $\alpha$ est algébrique sur $\mathbf{k}$.

□

**Remarque 1.10.** Sur les nombres algébriques et transcendants réels (à compléter).

## 1.2 Corps de rupture

**Définition 1.11.** Soit $\mathbf{k}$ un corps et $P \in \mathbf{k}[X]$. Un corps de rupture de $P$ est une extension $\mathbb{K}$ telle qu'il existe $\alpha \in \mathbb{K}$ tel que $P(\alpha) = 0$.

**Proposition 1.12.** Un tel corps existe toujours.

*Démonstration.* On peut supposer $P$ irréductible (quitte à prendre un des facteurs de $P$). Soit $\mathbb{K} = \mathbf{k}[X]/\langle P \rangle$ et soit $\alpha$ la classe de $X$. On montre alors que $P(\alpha)$ est la classe de $P$ et est donc nul dans $\mathbb{K}$. □

**Remarque 1.13.** Avec les notations ci-dessus, $[\mathbb{K} : \mathbf{k}] = \deg(P)$.

Le corps de rupture précédent est le plus petit au sens suivant.

**Proposition 1.14.** Soit $P \in \mathbf{k}[X]$ irréductible et soit $\mathbb{L}$ un corps de rupture de $P$. Alors $\mathbb{L}$ est une extension de $\mathbb{K} = \mathbf{k}[X]/\langle P \rangle$ (au sens où $\mathbb{K}$ s'injecte dans $\mathbb{L}$ avec morphisme constant sur $\mathbf{k}$).

*Démonstration.* Soit $\alpha \in \mathbb{L}$ tel que $P(\alpha) = 0$.
Soit $\varphi : \mathbf{k}[X] \to \mathbb{L}, Q \mapsto Q(\alpha)$. On a vu que $\ker(\varphi) = \langle \mu_\alpha \rangle$ et $\mu_\alpha$ est irréductible.
On a un morphisme injectif induit par $\varphi : \mathbf{k}[X]/\langle \mu_\alpha \rangle \to \mathbb{L}$.
Par définition de $\mu_\alpha$, $\mu_\alpha$ divise $P$ mais ce dernier étant irréductible, il est égal à $\mu_\alpha$ à un multiple scalaire près, i.e. $\langle P \rangle = \langle \mu_\alpha \rangle$ ce qui entraine l'existence de l'injection de $\mathbb{K}$ dans $\mathbb{L}$ annoncée. □

## 1.3 Clôture algébrique

**Définition 1.15.** Un corps $\mathbb{K}$ est algébriquement clos si tout $P \in \mathbb{K}[X] \setminus \mathbb{K}$ possède une racine dans $\mathbb{K}$.

Ceci équivaut à dire que tout polynôme non constant de $\mathbb{K}[X]$ est scindé dans $\mathbb{K}[X]$.

**Définition 1.16.** Une clôture algébrique d'un corps $\mathbf{k}$ est une extension $\mathbb{K}/\mathbf{k}$ algébrique telle que $\mathbb{K}$ est algébriquement clos.

**Théorème 1.17.** Tout corps $\mathbf{k}$ admet une clôture algébrique.

La démonstration est basée sur le lemme suivant.

**Lemme 1.18.** Il existe une extension $\mathbb{L}/\mathbf{k}$ telle que pour tout $P \in \mathbf{k}[X] \setminus \mathbf{k}$, $P$ a une racine dans $\mathbb{L}$.

*Démonstration.* Soit $A = \mathbf{k}[X_P,\ P \in \mathbf{k}[X], \deg(P) \geq 1$. L'anneau $A$ est un anneau de polynômes à une infinité de variables.
Soit $J$ l'idéal de $A$ engendré par les $P(X_P)$ pour $P \in \mathbf{k}[X] \setminus \mathbf{k}$.
Montrons que $J \neq A$. Par l'absurde, supposons $J = A$. Alors $1 \in J$, i.e. on peut écrire

$$1 = Q_1 \cdot P_1(X_{P_1}) + \cdots + Q_r \cdots P_r(X_{P_r})$$

avec $P_1, \ldots, P_r \in \mathbf{k}[X] \setminus \mathbf{k}$ et $Q_1, \ldots, Q_r \in A$. Une telle relation fait intervenir un nombre fini de variables qu'on note $T_1, \ldots, T_n$, avec $T_i = X_{P_i}$. On a donc

$$1 = \sum_{i=1}^{r} Q_i(T_1, \ldots, T_n) \cdot P_i(T_i).$$

Soit $E$ une extension de $\mathbf{k}$ dans laquelle chaque $P_i$ a une racine notée $\alpha_i$ (possible en prenant un corps de rupture de $P_1$ avec une racine $\alpha_1$, puis on recommence avec $P_2 \in \mathbf{k}(\alpha_1)[X]$ qui a une racine $\alpha_2$ et on recommence dans $\mathbf{k}(\alpha_1, \alpha_2)[X]$). On applique alors $\varphi$ à l'égalité ci-dessus et on obtient $1 = 0$. Absurde.
Comme $J \neq A$, par le théorème de Krull, il existe un idéal maximal $m$ de $A$ contenant $J$.
Soit alors $E = A/m$ (anneau quotient). C'est un corps.
Notons $s : A \to E = A/m$ la projection canonique et $\sigma = s_{|\mathbf{k}} : \mathbf{k} \to E$.
Soit $P \in \mathbf{k}[X] \setminus \mathbf{k}$. On identifie $\mathbf{k}$ à $\sigma(\mathbf{k}) \subseteq A/m$ ; cette identification est possible car $\sigma$ est injective car $\mathbf{k} \cap m = (0)$ (sinon on aurait $m = A$). On alors $\sigma(P)(s(X_P)) = s(P(X_P)) = 0$ car $P(X_P) \in J \subset m$ ; donc $P$ identifié à $\sigma(P)$ admet une racine dans $E$. □

*Démonstration.* (du théorème) Soit $L_1$ une extension dans laquelle tout polynôme $P \in \mathbf{k}[X] \setminus \mathbf{k}$ admet une racine (possible par le lemme). Ensuite, soit $L_2$ une extension de $L_1$ dans laquelle tout polynôme $P \in L_1[X] \setminus L_1$ a une racine. On continue ainsi.
Soit alors $L_\infty = \bigcup_{n \in \mathbb{N}} L_n$. C'est une extension de $\mathbf{k}$. Soit $L$ l'ensemble des éléments de $L_\infty$ qui sont algébriques sur $\mathbf{k}$. $L$ est une extension algébrique (voir corollaire 1.9).
Montrons que $L$ est algébriquement clos. Soit $P \in L[X] \setminus L$, $P = \sum_{i=0}^{d} a_i X^i$. Chaque $a_i$ appartient à $L_\infty$ donc il existe $n$ tel que tous les $a_i$ soient dans $L_n$. Par suite, $P$ a une racine dans $L_{n+1}$ donc dans $L_\infty$. Notons $\alpha$ cette racine.
Les extensions $\mathbf{k} \subseteq \mathbf{k}(a_0, \ldots, a_d) \subseteq \mathbf{k}(\alpha, a_0, \ldots, a_d)$ sont algébriques, la première car les $a_i \in L$ et la seconde car $\alpha$ est une racine de $P \in \mathbf{k}(a_0, \ldots, a_d)[X]$ donc $\alpha$ est algébrique sur $\mathbf{k}$ et donc $\alpha \in L$. □

Le résultat suivant montre que la clôture algébrique est unique à $\mathbf{k}$-isomorphisme près.

**Théorème 1.19.**
1. Si $L_1/\mathbf{k}$ et $L_2/\mathbf{k}$ sont deux clôtures algébriques de $\mathbf{k}$ alors il existe un isomorphisme de corps $\varphi : L_1 \to L_2$ tel que $\varphi_{|\mathbf{k}} = \mathrm{Id}_{\mathbf{k}}$.
2. Soit $\mathbb{K}$ une clôture algébrique de $\mathbf{k}$ et soit $\sigma : \mathbf{k} \to L$ un morphisme, avec $L$ algébriquement clos. Alors il existe $\tau : \mathbb{K} \to L$ qui prolonge $\sigma$.

La démonstration de ce théorème va utiliser quelques résultats intermédiaires.

**Lemme 1.20.** Soit $\sigma : \mathbf{k} \to \mathbb{L}$ un morphisme de corps avec $\mathbb{L}$ algébriquement clos. Soient $\mathbb{K}/\mathbf{k}$ une extension et $x \in \mathbb{K}$ un élément algébrique sur $\mathbf{k}$. Alors il existe un morphisme de corps $\mathbf{k}(x) \to \mathbb{L}$ qui prolonge $\tau$.

*Démonstration.* Soit $P = \mu_x \in \mathbf{k}[X]$ le polynôme minimal de $x$. Le morphisme $\sigma$ induit un isomoprhisme

$$\theta_2 : \mathbf{k}[X]/\langle P\rangle \to \sigma(\mathbf{k})[X]/\langle \sigma(P)\rangle$$

où $\sigma(P) \in \mathbb{L}[X]$ est le polynôme obtenu en appliquant $\sigma$ aux coefficients de $P$. D'autre part on a un isomorphisme $\theta_1 : \mathbf{k}(x) \to \mathbf{k}[X]/\langle P\rangle$ et par la prop. 1.12, on a un morphisme de corps $\theta_3 : \sigma(\mathbf{k})[X]/\langle\sigma(P)\rangle \to \mathbb{L}$. La composée $\theta_3 \circ \theta_2 \circ \theta_1$ est bien un morphisme de corps entre $\mathbf{k}(x)$ et $\mathbb{L}$. De plus pour $z \in \mathbf{k}$, on a $\theta_3 \circ \theta_2 \circ \theta_1(z) = \theta_3 \circ \theta_2(z) = \theta_3(\sigma(z)) = \sigma(z)$. □

**Proposition 1.21.** Soit $\mathbb{K}/\mathbf{k}$ une extension algébrique et $\sigma : \mathbf{k} \to \mathbb{L}$ un morphisme de corps avec $\mathbb{L}$ algébriquement clos. Alors il existe un morphisme de corps $\mathbb{K} \to \mathbb{L}$ qui prolonge $\sigma$.

*Démonstration.* Soit $S$ l'ensemble des couples $(F, \tau)$ tels que $F$ est un corps intermédiaire $\mathbf{k} \subseteq F \subseteq \mathbb{K}$, et $\tau$ est un morphisme de corps de $F$ vers $\mathbb{L}$ qui prolonge $\sigma$.
Remarquons que $S$ est non vide puisqu'il contient le couple $(\mathbf{k}, \sigma)$. Dans $S$ on a une relation d'ordre (partielle) donnée par : $(F, \tau) \leq (F', \tau')$ si et s. si $F \subseteq F'$ et $\tau'$ prolonge $\tau$ à $F'$.
Pour cet ordre, vérifions que $S$ est inductif. En effet, soit $(F_n, \tau_n)_{n\in\mathbb{N}}$ une chaine croissante d'éléments de $S$. Alors soit $F' = \cup_{n\in\mathbb{N}} F_n$ et soit $\tau' : F' \to \mathbb{L}$ définie par restriction de $\tau_n$ pour tout $n$. Alors $(F', \tau')$ est une borne supérieure de la chaine en question.
Par le lemme de Zorn, $S$ admet un élément maximal $(F, \tau)$. Supposons par l'absurde que $F \neq \mathbb{K}$. Alors soit $x \in \mathbb{K} \setminus F$. On applique alors le lemme précédent $F(x)$ et $x \in F(x)$ ce qui donne un élément de $S$ plus grand que $F$, ce qui contredit la maximalité de $F$. Par conséquent $F = \mathbb{K}$. □

Avant la preuve du théorème, il reste un dernier lemme.

**Lemme 1.22.** Soit $\mathbb{K}/\mathbf{k}$ une extension algébrique et soit $\sigma : \mathbb{K} \to \mathbb{K}$ un morphisme de corps égal à l'identité sur $\mathbf{k}$. Alors $\sigma$ est bijectif.

*Démonstration.* Il suffit de montrer que $\sigma$ est surjectif. Soit donc $x \in \mathbb{K}$ et soit $P = \mu_x \in \mathbf{k}[X]$ son polynôme minimal. Soit $R$ l'ensemble des racines de $P$ dans $\mathbb{K}$ ($R$ contient au moins $x$). Soit $y \in R$. On a $P(y) = 0$. Par suite $P(\sigma(y)) = \sigma(P)(\sigma(y)) = \sigma(P(y))$ (car $\sigma$ ne modifie pas les coefficients de $P$). Ainsi $\sigma(y)$ est aussi une racine de $P$. Ceci signfie que $\sigma$ induit une application (injective) de $R$ dans $R$. Mais $R$ étant fini, cette application est bijective. Par conséquent, $x$ est dans l'image de $\sigma$. □

*Démonstration du théorème.* Le point 2 du théorème est une application directe de la proposition. Voyons le point 1. Par le point 2, il existe $\tau_1 : \mathbb{L}_1 \to \mathbb{L}_2$ et $\tau_2 : \mathbb{L}_2 \to \mathbb{L}_1$ deux morphismes de corps qui prolongent l'application d'inclusion de $\mathbf{k}$ dans $\mathbb{L}_1$ et de $\mathbf{k}$ dans $\mathbb{L}_2$. Par le lemme précédent $\tau_1 \circ \tau_2$ est un morphisme bijectif de $\mathbb{L}_2$ dans lui-même ce qui entraine la surjectivité de $\tau_1$ qui est donc un isomorphisme. □

### 1.4 Corps de décomposition

**Définition 1.23.** Soit $\mathbf{k}$ un corps et soit $\bar{\mathbf{k}}$ une clôture algébrique de $\mathbf{k}$ (unique à isomorphisme près). Soit $P \in \mathbf{k}[X]$ un polynôme de degré $n \geq 1$. Dans $\bar{\mathbf{k}}$, on peut décomposer $P = c\prod_{i=1}^{n}(X - \alpha_i)$ avec $c \in \mathbf{k}$ et $\alpha_i \in \bar{\mathbf{k}}$. Le corps $\mathbf{k}(\alpha_1, \ldots, \alpha_n)$ est appelé le corps de décomposition de $P$.

Comme le montre la proposition suivante, ce corps est le plus petit corps (à isomorphisme près) dans lequel $P$ est scindé.

**Proposition 1.24.** Soit $P \in \mathbf{k}[X]$ de degré $\geq 1$. Soit $\mathbb{L}/\mathbf{k}$ une extension telle que $P$ est scindé dans $\mathbb{L}$. Notons $\mathbb{K}$ le corps de décomposition de $P$. Alors il existe un morphisme injectif de corps $\mathbb{K} \to \mathbb{L}$ laissant $\mathbf{k}$ stable.

*Démonstration.* Considérons $\overline{\mathbb{L}}$ une clôture algébrique de $\mathbb{L}$. Alors l'inclusion $i : \mathbf{k} \to \mathbb{L}$ se prolonge en un morphisme injectif $j : \overline{\mathbf{k}} \to \overline{\mathbb{L}}$. Par conséquent l'image $L'$ de $\mathbb{K}$ par $j$ est un corps dans lequel $P$ est scindé. Ainsi $P$ est scindé dans $\mathbb{L}$ et dans $\mathbb{L}'$ qui sont des sous-corps de $\overline{\mathbb{L}}$. Par unicité de la décomposition d'un polynôme en facteurs irréductible (ici de degrés 1), les $j(\alpha_i)$ sont dans $\mathbb{L}$ (les $\alpha_i$ étant les racines de $P$ dans $\overline{\mathbf{k}}$). Ainsi la restriction de $j$ à $\mathbb{K}$ est un morphisme injectif de $\mathbb{K}$ dans $\mathbb{L}$. □

## 2 Résultant et discriminant

Dans cette partie, $A$ désigne un anneau commutatif.

### 2.1 Sur le déterminant

**Proposition 2.1.** Soit $M$ un $A$-module libre de rang $n$ muni d'une base $\mathcal{B} = (e_1, \ldots, e_n)$. Il existe une unique forme multilinéaire alternée $f : M^n \to A$ telle que $f(e_1, \ldots, e_n) = 1$. Si $(x_1, \ldots, x_n) \in M^n$ et si on écrit $x_j = \sum_{i=1}^{n} x_{ij}e_i$ avec $x_{ij} \in A$ alors

$$f(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} \varepsilon(\sigma) x_{\sigma(1)1} \cdots x_{\sigma(n)n} = \sum_{\sigma \in S_n} \varepsilon(\sigma) x_{1\sigma(1)} \cdots x_{n\sigma(n)}.$$

**Définition 2.2.** Avec les notations précédentes, $f(x_1, \ldots, x_n)$ est appelé déterminant de $(x_1, \ldots, x_n)$ par rapport à la base $\mathcal{B}$ et on note : $f(x_1, \ldots, x_n) = \det_{\mathcal{B}}(x_1, \ldots, x_n)$.

**Définition 2.3.** Soit $A = (a_{ij})$ une matrice $n \times n$ à coefficients dans $A$. Soit $M = A^n$ et soit $\mathcal{B} = (e_1, \ldots, e_n)$ la base canonique de $M$. On pose $a_j = \sum_{i=1}^{n} a_{ij}e_i$. On définit le déterminant de $A$, $\det(A) = \det_{\mathcal{B}}(a_1, \ldots, a_n)$.

On peut alors montrer que le déterminant ainsi défini a les mêmes propriétés que lorsque $A$ est un corps, en particulier :

— On a la formule de développement par rapport à une ligne ou une colonne.

— Avec les notations de la proposition, on a l'implication : $\det_{\mathcal{B}}(x_1,\dots,x_n)=0 \Rightarrow$ les $x_i$ sont liés.
— Si $A$ est intègre alors l'implication inverse est vraie.
— Voici un exemple qui montre que c'est faux si $A$ n'est pas intègre.
Soit $A=\mathbb{Z}/6\mathbb{Z}$ et $M=A^2$ muni de la base canonique $(e_1,e_2)$. Soient $x_1=e_1+e_2$ et $x_2=e_1+3e_2$.
On a $3x_1-3x_2=0$ alors que $\det_{\mathcal{B}}(x_1,x_2)=2\neq 0$ dans $A$.

Voyons un résultat utile pour la suite.

**Lemme 2.4.** Soit $M$ un $A$-module libre de rang $n$, muni d'une base $\mathcal{B}=(e_1,\dots,e_n)$. Soient $x_1,\dots,x_n\in M$ et $N$ le module engendré par les $x_i$. Notons $d=\det_{\mathcal{B}}(x_1,\dots,x_n)$. Alors pour tout $k=1,\dots,n$, $de_k\in N$.

*Démonstration.* On écrit $x_j=\sum_{i=1}^n x_{ij}e_i$ et on note $X$ la matrice $(x_{ij})$.
Pour tout $i=1,\dots,n$, le développement par rapport à la ligne $i$ de la matrice $X$ donne

$$d=\sum_{j=1}^n x_{ij}(-1)^{i+j}\det(X_{ij})$$

où $X_{ij}$ est la matrice obtenue à partir de $X$ en lui retirant la ligne $i$ et la colonne $j$.
D'autre part, soit $i,k\in\{1,\dots,n\}$ avec $i\neq k$. Soit $X'$ la matrice $n\times n$ obtenue en gardant toutes les lignes de $X$ sauf la ligne $k$ dans laquelle on met les coefficients de la ligne $i$ ; ainsi les lignes $i$ et $k$ de $X'$ sont égales et toutes les lignes de $X'$ (sauf la ligne d'indice $k$) sont celles de $X$. Alors $\det(X')=\det_{\mathcal{B}}(x_1,\dots,x_i,\dots,x_i,\dots,x_n)$ (l'un des $x_i$ est en position $k$) ce qui entraine, du fait que le déterminant est une forme alternée, $\det(X')=0$. Mais si on développe $X'$ par rapport à sa ligne $k$, cela donne :

$$0=\det(X')=\sum_{j=1}^n x_{ij}(-1)^{j+k}\det(X_{kj}).$$

En combinant les deux égalités obtenues, on peut écrire :

$$\forall i,k=1\dots,n,\qquad \delta_{ik}d=\sum_{j=1}^n x_{ij}(-1)^{j+k}\det(X_{kj}).$$

Par conséquent, pour $k=1,\dots,n$ :

$$\begin{aligned} de_k &= \sum_{i=1}^n \delta_{ik}de_i \\ &= \sum_{i=1}^n\sum_{j=1}^n x_{ij}(-1)^{j+k}\det(X_{kj})e_i \\ &= \sum_{j=1}^n (-1)^{k+j}\det(X_{kj})x_j. \end{aligned}$$

□

## 2.2 Résultant

Soient $P,Q\in A[T]$ qu'on écrit : $P=a_0+a_1T+\cdots+a_mT^m$ et $Q=b_0+b_1T+\cdots+b_nT^n$ avec $m,n\geq 1$. On ne suppose pas nécessairement $a_m$ et $b_n$ non nuls.

**Définition 2.5.** Le résultant de $P$ et $Q$, noté $R(P,Q) \in A$ est par définition le déterminant suivant :

$$R(P,Q) = \begin{vmatrix} a_m & a_{m-1} & \cdots & \cdots & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & a_m & a_{m-1} & \cdots & \cdots & \cdots & a_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & a_m & a_{m-1} & \cdots & \cdots & \cdots & a_0 \\ b_n & b_{n-1} & \cdots & \cdots & b_0 & 0 & \cdots & \cdots & 0 \\ 0 & b_n & b_{n-1} & \cdots & \cdots & b_0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & b_n & b_{n-1} & \cdots & \cdots & b_0 \end{vmatrix}.$$

C'est un déterminant $(m+n) \times (m+n)$ avec $n$ lignes formées des coefficients $a_i$ et de $n-1$ zéros ; et de $m$ lignes formées des $b_i$ et de $m-1$ zéros.

Remarquons que le produit des éléments de la diagonale est : $a_m^n b_0^m$.
Voici une interprétation du résultant en terme de déterminant.

**Proposition 2.6.** Soit $M = \{S \in A[T] \mid \deg(S) \leq m+n-1\}$. C'est un $A$-module libre de type fini dont une base est $\mathcal{B} = (T^{m+n-1}, \ldots, T, 1)$. Alors $R(P,Q)$ est le déterminant de la famille

$$T^{n-1}P, T^{n-2}P, \ldots, TP, T, T^{m-1}Q, T^{m-2}Q, \ldots, TQ, Q$$

par rapport à la base $\mathcal{B}$.

*Démonstration.* Facile. □

### 2.2.1 Le théorème principal

**Proposition 2.7.** On garde les notations précédentes avec $\deg(P) \leq m$ et $\deg(Q) \leq n$. Il existe $F, G \in A[T]$ non tous deux nuls tels que $R(P,Q) = FP + GQ$ avec $\deg(F) < n$ et $\deg(G) < m$.

*Démonstration.* Notons $R = R(P,Q)$. Comme ci-dessus, on considère le sous-$A$-module $M$ de $A[T]$ formé des polynômes de degré $\leq m+n-1$ et muni de la base canonique. On a vu que $R$ est le déterminant de la famille $\mathcal{F}$ formée de $T^{n-1}P, \ldots, TP, P, T^{m-1}Q, \ldots, TQ, Q$. On applique le lemme 2.4 à $e_k = 1$ et on obtient $R$ comme combinaison linéaire des $T^iP$ et des $T^jQ$ ce qui donne $R$ sous la forme annoncée $R = FP + GQ$ avec $\deg(F) < n$ et $\deg(G) < m$. Maintenant si $R \neq 0$ alors $F$ et $G$ ne peuvent pas être nuls en même temps. Et dans le cas où $R = 0$ alors la famille $\mathcal{F}$ est liée (propriétés du déterminant) ce qui entraine l'existence de $F$ et $G$ avec les bons degrés tels que $FP + GQ = 0$. □

**Théorème 2.8.** On garde les notations précédentes avec $P \in A[T]$ de degré $\leq m$ et $Q \in A[T]$ de degré $\leq n$. Considérons les deux conditions suivantes.

1. Le résultant $R := R(P,Q) \in A$ est nul.
2. Il existe $F, G \in A[T]$, non tous deux nuls, tels que $FP + GQ = 0$ avec $\deg(F) < n$ et $\deg(G) < m$.

Alors l'implication (1) $\Rightarrow$ (2) est vraie.
Si $A$ est intègre alors (2) $\Rightarrow$ (1) est vraie.
Supposons $A$ intègre et soit $\mathbb{K}$ son corps des fractions et supposons que $a_m$ et $b_n$ sont non nuls, alors les assertions (1) et (2) sont équivalentes aux deux assertions suivantes.

3. Le pgcd de $P$ et $Q$ dans $\mathbb{K}[X]$ est de degré non nul.
4. Les polynômes $P$ et $Q$ ont une racine commune dans une extension convenable de $\mathbb{K}$ (par exemple un corps contenant le corps de décomposition de $PQ$).

*Démonstration.* L'implication (1) $\Rightarrow$ (2) découle directement de la proposition précédente. Si on suppose (2) alors cela signifie que la famille $T^{n-1}P, \ldots, P, T^{m-1}Q, \ldots, Q$ est liée et le déterminant de cette famille dans la base des $T^i$ (avec $0 \leq i \leq m+n-1$) est nul car $A$ est intègre, i.e. $R(P,Q)$ est nul, d'où (1).
Supposons (2) vraie et (3) faux. Alors $P$ et $Q$ sont premiers entre eux dans $K[T]$, mais comme $FP = -GQ$, le théorème de Gauss implique que $P$ divise $G$ mais c'est impossible pour des questions de degré. Ainsi (2) $\Rightarrow$ (3) est vraie. Voyons la réciproque et supposons (3). Soit $D$ le pgcd de $P$ et $Q$ dans $\mathbb{K}[T]$. On peut écrire $P = DA$, $Q = DB$ avec $A, B \in \mathbb{K}[T]$ et $\deg(A) < m$ et $\deg(B) < n$. On a alors $BP = BDA = AQ$. Soit $e$ le produit des dénominateurs des coefficients de $A$ et $B$ alors :$eB \cdot P + (-eA) \cdot Q = 0$ avec $eB$ et $-eA$ dans $A[T]$ avec les bonnes conditions de degrés, d'où (2).
Pour finir, l'équivalence (3) $\iff$ (4) est triviale. □

**Remarque 2.9.** L'implication (2) $\Rightarrow$ (1) est fausse en général si $A$ n'est pas intègre. En effet, soient $P = T + 1$ et $Q = T + 3$ dans $\mathbb{Z}/6\mathbb{Z}[T]$. Leur résultant est $R = 2 \neq 0$ alors que $3P - 3Q = 0$.

### 2.2.2 Le résultant en fonction des racines

Notons $\Gamma = \mathbb{Z}[X_1, \ldots, X_m, Y_1, \ldots, Y_n, U_m, V_n]$.

**Théorème 2.10.** Soient $P = P(T) = U_m(T - X_1) \cdots (T - X_m)$, $Q = Q(T) = V_n(T - Y_1) \cdots (T - Y_n)$ dans $\Gamma[T]$. Dans l'anneau $\Gamma$, on a les égalités suivantes :

$$\begin{aligned} R(P,Q) &= U_m^n V_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (X_i - Y_j) \\ &= U_m^n \prod_{i=1}^{m} Q(X_i) \\ &= (-1)^{mn} V_n^m \prod_{j=1}^{n} P(Y_j). \end{aligned}$$

La preuve va nécessiter deux lemmes dont voici le premier.

**Lemme 2.11.** Avec les notation précédentes, $R := R(P,Q)$ (élément de $\Gamma$) est le produit de $U_m^n V_n^m$ par un polynôme homogène en les variables $X_i, Y_j$ de degré total $mn$.

*Démonstration.* Notons $a_i$ (resp. $b_j$) le coefficient du terme de degré $i$ (resp. $j$) de $P$ (resp. $Q$) en tant que polynôme en $T$. On a donc $a_m = U_m$ et pour $i < m$, $a_i = (-1)^{m-i} U_m S_{m-i}(X_1, \ldots, X_m)$. Ici $S_k$ désigne le $k$-ième polynôme symétrique élementaire en les $X_i$. Ainsi $S_1 = X_1 + \cdots + X_m, \ldots, S_m = X_1 \cdots X_m)$. Le polynôme symétrique $S_k$ est homogène de degré $k$ en les $X_i$ d'où $a_i$ est homogène de degré $m - i$ pour $i < m$. De même, on a $b_n = V_n$ et $b_j = (-1)^{n-j} V_n S_{n-j}(Y_1, \ldots, Y_n)$ et le coefficient $b_j$ est homogène de degré $n - j$ en les $Y_j$ pour $j < n$.
Notons $r_{ij}$ le terme générique de $R$. On sait que $r_{ij} = a_{m+i-j}$ pour $i \leq n$ et $r_{ij} = b_{i-j}$ pour $i > n$. Le déterminant $R$ est alors donné par :

$$R = \sum_{\sigma \in S_{m+n}} \varepsilon(\sigma) r_{1,\sigma(1)} \cdots r_{m+n,\sigma(m+n)}.$$

L'assertion sur les variables $U_m$ et $V_n$ est claire car les termes des $n$ premières lignes (resp. des $m$ dernières) sont tous produits de $U_m$ (resp. de $V_n$) par un polynôme en les $X_i, Y_j$.
Déterminons le degré total en les $X_i, Y_j$ d'un terme (non nul) de la somme ci-dessus. Pour $i \leq n$, $\deg(r_{i,\sigma(i)}) = \deg(a_{m+i-\sigma(i)}) = \sigma(i) - i$, et pour $i > n$, $\deg(r_{i,\sigma(i)}) = \deg(b_{i-\sigma(i)}) = n + \sigma(i) - i$. Le degré d'un terme est alors $mn + \sum_{i=1}^{m+n} \sigma(i) - i$ mais $\sum_{i=1}^{m+n} \sigma(i) - i = 0$ car $\sigma$ est une permutation donc il reste $mn$. □

Voici le deuxième lemme.

**Lemme 2.12.** Soit $R \in \mathbb{Z}[T_1, \ldots, T_n]$. On suppose que $R$ devient nul dans $\mathbb{Z}[T_1, \ldots, \widehat{T_i}, \ldots, T_n]$ quand on fait $T_i := T_j$ (le chapeau sur $T_i$ signifie que la variable $T_i$ est omise). Alors $T_i - T_j$ divise $R$.

*Démonstration.* On fait la division euclidienne de $R$ par $T_i - T_j$ relativement à la variable $T_i$ :

$$R = (T_i - T_j)S(T) + S'(T_1, \ldots, \widehat{T_i}, \ldots, T_n).$$

Quand on fait $T_i := T_j$, on obtient que $S'$ (qui n'a pas de $T_i$) devient nul et donc était nul avant la substitution. □

On peut maintenant démontrer le théorème.

*Démonstration du théorème.* Fixons $i \in \{1, \ldots, m\}$ et $j \in \{1, \ldots, n\}$, soit $\Gamma'$ l'anneau $\Gamma$ dans lequel on a enlevé la variable $Y_j$. On considère le morphisme d'anneau $\Phi : \Gamma \to \Gamma'$ qui à $Y_j$ associe $X_i$ et on note $\overline{P}$ et $\overline{Q}$ les images respectives de $P$ et $Q$ dans $\Gamma'$. Comme $\overline{P}$ et $\overline{Q}$ ont une racine commune (la racine $X_i = Y_j$) dans $\Gamma'$, leur résultant $\overline{R} = \Phi(R)$ est nul. Par le lemme précédent, $X_i - Y_j$ divise $R$ et ce pour tout $i, j$. Dans l'anneau factoriel $\Gamma$, les $X_i - Y_j$ sont irréductibles (car de degré 1) et ils sont distincts. Comme ils divisent tous $R$, leur produit le divise aussi. On a vu aussi dans le premier lemme que $U_m^n$ et $V_n^m$ divisent $R$. Par conséquent le polynôme $S := U_m^n V_n^m \prod_{i=1}^m \prod_{j=1}^n (X_i - Y_j)$ divise $R$. Comme $R$ et $S$ sont homogènes de mêmes degrés en les $U_m$, $V_n$ et $X_i, Y_j$ on a $R = \lambda S$ avec $\lambda \in \mathbb{Z}$.
Pour déterminer $\lambda$, on fait $(X_1, \ldots, X_m) = 0$ dans $R$. On obtient un déterminant égal à $U_m^n b_0^m = U_m^n V_n^m (-1)^{mn} \prod_{j=1}^n Y_j^m$. Mais ce terme est le terme obtenu dans $S$ quand on fait $(X_1, \ldots, X_m) = 0$ ce qui entraine $\lambda = 1$, i.e. $R = S$. On a donc la première égalité du théorème. Les deux autres égalités sont évidentes. □

**Corollaire 2.13.** On reprend les notations initiales $P, Q \in A[T]$. On suppose $A$ intègre et on note $\mathbb{K}$ son corps des fractions. Soit $\mathbb{L}/\mathbb{K}$ une extension dans laquelle le produit $PQ$ est scindé. On note $x_1, \ldots, x_m$ et $y_1, \ldots, y_n$ les racines de $P$ et $Q$ dans $\mathbb{L}$ (comptées avec leur multiplicité). On a les égalités suivantes dans $\mathbb{L}$.

$$\begin{aligned} R(P,Q) &= a_m^n b_n^m \prod_{i=1}^m \prod_{j=1}^n (x_i - y_j) \\ &= a_m^n \prod_{i=1}^m Q(x_i) \\ &= (-1)^{mn} b_n^m \prod_{j=1}^n P(y_j). \end{aligned}$$

*Démonstration.* S'obtient du théorème en spécialisant les variables. □

## 2.3 Discriminant

Soit $P \in \mathbf{k}[X]$ un polynôme de degré $n$ non nul. Soit $\mathbb{L}/\mathbf{k}$ une extension dans lequel $P$ est scindé. On note $x_1, \ldots, x_n$ les racines de $P$ dans $\mathbb{L}$ comptés avec leur multiplicité.

**Définition 2.14.** On pose $\delta = \prod_{1 \leq i < j \leq n} (x_i - x_j)$ et $\Delta = \delta^2$. Le nombre $\Delta$ (ou $\Delta(P)$) est appelé le discriminant de $P$.

**Remarque 2.15.** On a l'égalité

$$\Delta = (-1)^{n(n-1)/2} \prod_{i \neq j} (x_i - x_j).$$

A priori, $\Delta$ est dans $\mathbb{L}$ mais on verra que c'est un élément de $\mathbf{k}$.

**Exemple 2.16.** Le discriminant de $P = aX^2 + bX + c$ est $\Delta = \dfrac{b^2 - 4ac}{a^2}$. En effet, si on note $x_1, x_2$ ses racines (éventuellement confondues). Alors $\Delta = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = (-b/a)^2 - 4c/a = \frac{b^2-4ac}{a^2}$.

### 2.3.1 Cacul du discriminant

On garde les notations ambiantes et on suppose de plus que $P$ est unitaire :

$$P = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0.$$

On suppose que la caractéristique de $\mathbf{k}$ ne divise pas $n$.
On note $P'$ le polynôme dérivé de $P$ et on note $y_1, \ldots, y_{n-1}$ ses racines dans une extension où $P$ et $P'$ se décomposent. On a donc

$$P' = nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots a_1 = n \prod_{j=1}^{n-1} (X - y_j).$$

**Proposition 2.17.** On a les formules suivantes pour le discriminant $\Delta$ de $P$.

$$\begin{aligned}
\Delta &= (-1)^{n(n-1)/2} \prod_{i=1}^{n} P'(x_i), \\
&= (-1)^{n(n-1)/2} n^n \prod_{i,j} (x_i - y_j), \\
&= (-1)^{n(n-1)/2} n^n \prod_{j=1}^{n-1} P(y_j), \\
&= (-1)^{n(n-1)/2} R(P, P').
\end{aligned}$$

*Démonstration.* On dérive $P$ écrit sous la forme $P = \prod_{i=1}^{n} (X - x_i)$ :

$$P' = \sum_{i=1}^{n} (X - x_1) \cdots \widehat{(X - x_i)} \cdots (X - x_n)$$

où le chapeau signifie qu'on omet le terme correspondant. On obtient alors $P'(x_i) = \prod_{j, j \neq i} (x_i - x_j)$ ce qui donne $\prod_{i=1}^{n} P'(x_i) = \prod_{i,j,j \neq i} (x_i - x_j)$ et la première égalité provient de la remarque faite au paragraphe

précédent.
D'autre part, on a : $P'(x_i) = n\prod_{j=1}^{n-1}(x_i - y_j)$ d'où

$$\prod_{i=1}^{n} P'(x_i) = n^n \prod_{i,j}(x_i - y_j)$$

d'où la deuxième égalité.
On a aussi $P(y_j) = \prod_{i=1}^{n}(y_j - x_i)$ d'où $\prod_{j=1}^{n-1} P(y_j) = \prod_{i,j}(y_j - x_i) = \prod_{i,j}(x_i - y_j)$ (car $n(n-1)$ changements de signe) ce qui donne la troisième égalité.
Pour finir la dernière égalité provient du paragraphe 4.2.2. □

C'est la dernière égalité de cette proposition qui nous dit que le discriminant est bien dans le corps **k** de départ.

**Exercice 2.18.** Le discriminant de $P = X^3 + pX + q$ est $\Delta = -4p^3 - 27q^2$.
Celui de $P = X^n + pX + q$ est $\Delta = (-1)^{n(n-1)/2}(n^n q^{n-1} + (1-n)^{n-1}p^n)$.

# 3 Théorie de Galois

## 3.1 Plongements

On sait qu'un morphisme de corps est nécessairement injectif, on emploiera la terminologie : plongement. De plus si $\mathbb{K}$ et $\mathbb{K}'$ sont deux extensions d'un corps **k**, on parlera de **k**-plongement pour signifier un morphisme (injectif) $\varphi : \mathbb{K} \to \mathbb{K}'$ tel que $\varphi(x) = x$ pour tout $x \in \mathbf{k}$.
Dans ce paragraphe, on va fixer un corps **k** et un corps algébriquement clos $\Omega$ contenant **k** et quand on parlera d'extension $\mathbb{L}$ de **k**, ce sera un corps tel que $\mathbf{k} \subseteq \mathbb{L} \subset \Omega$ (ce n'est pas restrictif car on peut toujours trouver un corps algébriquement clos $\Omega$ contenant $\mathbb{L}$).

**Lemme 3.1.** Soient $\mathbf{k} \subseteq \mathbb{L} \subseteq \Omega$. Soit $N$ un entier et $\sigma_1, \ldots, \sigma_N$ des **k**-plongements de $\mathbb{L}$ dans $\Omega$ deux à deux distincts. Alors ils sont indépendants sur $\Omega$.

*Démonstration.* On procède par l'absurde et on suppose la famille liée. Quitte à renuméroter les $\sigma_i$ on peut supposer qu'il existe $r < N$ tel que

$$\sigma_{r+1} = \sum_{i=1}^{r} \lambda_i \sigma_i$$

avec $\lambda_i \in \Omega$ déterminés de façon unique. Fixons $y \in L$ non nul. Alors pour tout $x \in L$ on a applique l'égalité à $yx$ :

$$\sigma_{r+1}(x) = \sum_{i=1}^{r} \lambda_i \frac{\sigma_i(y)}{\sigma_{r+1}(y)} \sigma_i(x).$$

Par unicité des $\lambda_i$ on a donc pour tout $i = 1, \ldots, r$ :

$$\lambda_i \frac{\sigma_i(y)}{\sigma_{r+1}(y)} = \lambda_i.$$

Comme l'un des $\lambda_i$ est non nul, cela implique que pour un tel $i$ on ait $\sigma_i(y) = \sigma_{r+1}(y)$. Mais $y$ est quelconque (non nul) dans $\mathbb{L}$ donc $\sigma_i = \sigma_{r+1}$ ce qui contredit les hypothèse. □

**Proposition 3.2.** Soient $\mathbf{k} \subset \mathbb{L} \subset \Omega$ trois corps avec $[\mathbb{L} : \mathbf{k}] = n$ fini. Alors il y a au plus $n$ $\mathbf{k}$-plongements de $\mathbb{L}$ vers $\Omega$.

*Démonstration.* Notons $V$ l'espace vectoriel sur $\Omega$ des applications $\mathbf{k}$-linéaires de $\mathbb{L}$ vers $\Omega$. Soit $a_1, \ldots, a_n$ une $\mathbf{k}$-base de $\mathbb{L}$ et soit $\varphi : V \to \Omega^n$ définie par $\varphi(u) = (u(a_1), \ldots, u(a_n))$. On a facilement : $\varphi$ est linéaire et injective et surjective. Donc $V$ est de dimension $n$ sur $\Omega$.
Maintenant soit $N$ $\mathbf{k}$-plongements de $\mathbb{L}$ vers $\Omega$ deux à deux distincts alors (par le lemme) cela donne $N$ éléments linéairement indépendants de $V$ ce qui entraine $N \leq n$. □

**Corollaire 3.3.** Soit $\mathbf{k} \subset \mathbb{L} \subset \Omega$ avec $[\mathbb{L} : \mathbf{k}] = n$ fini. Soit $\sigma : \mathbf{k} \to \Omega$ un plongement. Alors il y a au plus $n$ $\mathbf{k}$-plongements de $\mathbb{L}$ vers $\Omega$ qui prolongent $\sigma$.

*Démonstration.* On a une injection $\mathbb{L} \to \bar{\mathbf{k}}$ (dans la clôture algébrique de $\mathbf{k}$ car $\mathbb{L}/\mathbf{k}$ est algébrique). En utilisant le théorème 1.19, $\sigma$ se prolonge en un morphisme $\tau$ de $\bar{\mathbf{k}}$ vers $\Omega$. On a donc $\tau(\mathbf{k}) \subset \tau(\mathbb{L}) \subset \Omega$ avec $[\tau(\mathbb{L}) : \tau(\mathbf{k})] = n$. On applique la proposition précédente pour dire qu'il y a au plus $n$ $\tau(\mathbf{k})$-plongements de $\tau(\mathbb{L})$ vers $\Omega$. Or on a une bijection entre les $\tau(\mathbf{k})$-plongements de $\tau(\mathbb{L})$ vers $\Omega$ et l'ensemble des plongements de $\mathbb{L}$ vers $\Omega$ qui prolonge $\sigma$ d'où le résultat voulu. □

Soit $P \in \mathbf{k}[X]$ un polynôme irréductible. Soit $\alpha \in \Omega$ une racine de $P$. Pour un plongement $\sigma : \mathbf{k} \to \Omega$, on note $\sigma^*(P) \in \Omega[X]$ le polynôme obtenu en appliquant $\sigma$ aux coefficients de $P$.

**Proposition 3.4.** Soit $\sigma : \mathbf{k} \to \Omega$ un plongement. Alors le nombre de plongements de $\mathbf{k}(\alpha)$ dans $\Omega$ qui prolongent $\sigma$ sur $\mathbf{k}$ est égal au nombres de racines distinctes de $P$ dans $\Omega$ (ou de $\sigma^*(P)$).

*Démonstration.* Soit $n$ le nombre de racines distinctes de $\sigma^*(P)$ dans $\Omega$. Soit $\beta$ une racine de $\sigma^*(P)$. On définit $\tau : \mathbf{k}(\alpha) \to \Omega$ par

$$\tau(\sum a_k \alpha^k) = \sum \sigma(a_k)\beta^k.$$

Cela définit un morphisme de corps tel que $\tau$ est égal à $\sigma$ sur $\mathbf{k}$ et ce pour chaque $\beta$. On obtient donc $n$ plongements de $\mathbf{k}(\alpha)$ dans $\Omega$ égaux à $\sigma$ sur $\mathbf{k}$. De plus, un plongement de $\mathbf{k}(\alpha)$ dans $\Omega$ qui prolonge $\sigma$ envoie $\alpha$ sur une racine de $\sigma^*(P)$.
Par conséquent, $n$ est exactement le nombre de plongements de $\mathbf{k}(\alpha)$ dans $\Omega$ qui prolongent $\sigma$.
Mais $n$ est aussi le nombre de racines distinctes de $P$ dans $\Omega$. En effet, soit $\mathbb{L} = \mathbf{k}(\alpha_1, \ldots, \alpha_t)$ le corps de décomposition de $P$ dans $\Omega$. On peut [1] prolonger $\sigma$ en $\varphi : \mathbb{L} \to \Omega$ et on a $\sigma^*(P) = \varphi^*(P)$. Si on écrit $P = \prod_{i=1}^t (X - \alpha_i)^{e_i}$ alors $\varphi^*(P) = \prod_{i=1}^t (X - \varphi(\alpha_i))^{e_i}$ ce qui donne le même nombre de racines distinctes. □

**Remarque 3.5.** On voit donc que le nombre de tels plongements est égal au nombres de racines du polynôme de départ et c'est égal à son degré s'il n'y a pas de racines multiples d'où la notion de séparabilité qui va suivre.

## 3.2 Extensions séparables

Dans ce paragraphe, $\Omega$ désigne toujours un corps algébriquement clos contenant $\mathbf{k}$.

**Définition 3.6.** Soit $P \in \mathbf{k}[X]$ un polynôme de degré $n$. On dit que $P$ est séparable sur $\mathbf{k}$ s'il possède $n$ racines distinctes dans $\Omega$ ; et inséparable dans le cas contraire.

1. En effet, $\sigma : \mathbf{k} \to \Omega$ se prolonge en une application $\bar{k} \to \Omega$ (cf. Théo. de 3.4) donc par restriction en $\varphi$.

**Exemple 3.7.** 1. Le polynôme $X^3 - 2 \in \mathbb{Q}[X]$ est séparable sur $\mathbb{Q}$.

2. Soit $p$ un nombre premier. Soit $X$ une indéterminée. Soit $\mathbb{L} = \mathbb{F}_p(X)$ le corps des fractions de $\mathbb{F}_p[X]$ et soit $\Omega$ un corps algébriquement clos contenant $\mathbb{L}$. Soit $\mathbf{k} = \mathbb{F}_p(X^p)$. C'est un sous-corps de $\mathbb{L}$.
   Considérons le polynôme $P = Y^p - X^p \in \mathbf{k}[Y]$.
   Dans $\mathbb{L}[Y]$, donc dans $\Omega[Y]$, on a : $P = (Y - X)^p$. Ainsi $P$ n'est pas séparable sur $\mathbf{k}$.
   Remarquons aussi que $P$ est irréductible dans $\mathbf{k}[Y]$. En effet si on avait $P = QR$ alors en regardant cette égalité dans $\mathbb{L}[X]$, on aurait $Q$ et $R$ qui seraient des puissances de $Y - X$. Par conséquent, le terme constant de $Q$ serait de la forme $(-1)^n X^n$ avec $n < p$ et ne serait donc pas dans $\mathbf{k}$.

**Proposition 3.8.** Soit $P \in \mathbf{k}[X]$. Alors $P$ est séparable si et s. si $P$ et $P'$ sont premiers entre eux (i.e. son discriminant est non nul).

*Démonstration.* Soit $n$ le degré de $P$. Si $P$ a $n$ racines distinctes $\alpha_i$ dans $\Omega$ alors on voit facilement que $P'$ ne s'annule en aucun $\alpha_i$. Réciproquement si $P$ n'est pas séparable alors on peut écrire $P = (X-\alpha)^k Q$ dans $\Omega[X]$. En dérivant, on constate que $\alpha$ est racine de $P'$, d'où $P$ et $P'$ ne sont pas premiers entre eux. □

**Corollaire 3.9.** Un polynôme irréductible $P \in \mathbf{k}[X]$ est séparable sur $\mathbf{k}$ si et s. si $P'$ n'est pas nul.

*Démonstration.* Supposons $P$ inséparable. Alors $P$ et $P'$ ont une racine commune $\alpha \in \Omega$. Puisque $P$ est irréductible, c'est le polynôme minimal de $\alpha$. D'où $P$ divise $P'$. Pour des questions de degré, ce n'est possible que si $P'$ est nul. Réciproquement, si $P'$ est nul alors $P$ et $P'$ ne sont pas premiers entre eux (1 n'est pas dans l'idéal engendré par $P$ et $P'$). □

**Corollaire 3.10.** Si $\mathbf{k}$ est de caractéristique 0 alors tout polynôme irréductible est séparable.

*Démonstration.* En effet, $P' = 0$ équivaut au fait que $P$ est constant. □

L'exemple 2 ci-dessus montre que c'est faux en caractéristique $p$ où on avait un polynôme irréductible inséparable.

**Corollaire 3.11.** Supposons $\mathbf{k}$ de caractéristique $p$. Soit $P \in \mathbf{k}[X]$ irréductible. Alors $P$ est inséparable si et s. si il existe $Q \in \mathbf{k}[X]$ tel que $P(X) = Q(X^p)$.

*Démonstration.* en exercice. □

**Définition 3.12.** Soit $\alpha \in \Omega$ un élément algébrique sur $\mathbf{k}$. On dit que $\alpha$ est séparable sur $\mathbf{k}$ s'il est racine d'un polynôme séparable sur $\mathbf{k}$. (On peut noter que c'est équivalent à dire que $\mu_\alpha$ est séparable.) Une extension (algébrique) $\mathbb{L}$ de $\mathbf{k}$ est dite séparable si tous les éléments de $\mathbb{L}$ sont séparables sur $\mathbf{k}$.

**Proposition 3.13.** Soit $\mathbb{L}$ une extension de $\mathbb{K}$ et $\mathbb{K}$ une extension de $\mathbf{k}$. Si $\mathbb{L}$ est séparable sur $\mathbf{k}$ alors $\mathbb{L}$ est séparable sur $\mathbb{K}$ et $\mathbb{K}$ l'est sur $\mathbf{k}$

*Démonstration.* Soit $\alpha \in \mathbb{L}$. Le polynôme $\mu_{\alpha,\mathbb{K}}$ divise $\mu_{\alpha,\mathbf{k}}$ et ce dernier est séparable donc le premier aussi. De plus l'inclusion $\mathbb{K} \subseteq \mathbb{L}$ implique que $\mathbb{K}$ est séparable sur $\mathbf{k}$. □

**Définition 3.14.** Un corps $\mathbf{k}$ est dit parfait si toutes ses extensions algébriques sont séparables.

Ceci équivaut à dire que tout polynôme $P \in \mathbf{k}[X]$ irréductible est séparable.
On a déjà vu (par un corollaire ci-dessus) que si $\mathbf{k}$ est de caractéristique nulle alors $\mathbf{k}$ est parfait.

**Lemme 3.15.** Soit $\mathbf{k}$ un corps de caractéristique non nulle $p$. Alors $\mathbf{k}$ est parfait si et s. si $\mathbf{k} = \mathbf{k}^p$ (i.e. tout élément de $\mathbf{k}$ possède une racine $p$-ième dans $\mathbf{k}$).

*Démonstration.* Supposons $\mathbf{k} = \mathbf{k}^p$. Soit $P \in \mathbf{k}[X]$ irréductible. Si $P$ n'est pas séparable alors il existe $Q = \sum q_i X^i \in \mathbf{k}[X]$ tel que $P(X) = Q(X^p)$. Par hypothèse, il existe existe $a_i \in \mathbf{k}$ tels que $a_i^p = q_i$ ce qui entraine $P = \sum_i a_i^p X_i^p = (\sum_i a_i X_i)^p$ ce qui contredit le fait pour $P$ d'être irréductible.
Réciproquement supposons $\mathbf{k} \neq \mathbf{k}^p$. Soit alors $a \in \mathbf{k}$ qui ne soit pas dans $\mathbf{k}^p$. Soit alors $P = X^p - a$. Il possède une unique racine $\alpha$ dans $\bar{\mathbf{k}}$ et dans $\bar{\mathbf{k}}[X]$, on a $P = (X - \alpha)^p$. Le polynôme $P$ est irréductible dans $\mathbf{k}[X]$. En effet, sinon soit $Q \in \mathbf{k}[X]$ un diviseur irréductible de $P$, $\deg(Q) \geq 2$ (sinon $Q = X - \alpha$). Le polynôme $Q$ n'est pas séparable ($\alpha$ est au moins racine double) et donc on peut écrire $Q(X) = R(X^p)$ mais alors $\deg(Q) > p$ ce qui est absurbe. On a donc $P \in \mathbf{k}[X]$ irréductible et non séparable. □

**Corollaire 3.16.** Tout corps fini est parfait.

*Démonstration.* Soit $\mathbf{k}$ un corps fini de caractéristique $p$. L'application $\gamma : \mathbf{k} \to \mathbf{k}, x \mapsto x^p$ est morphisme de corps. il est donc injectif. L'ensemble $\mathbf{k}$ étant de cardinal fini, $\gamma$ est bijectif ce qui signifie $\mathbf{k} = \mathbf{k}^p$ et on utilise le lemme. □

On a vu dans l'exemple du début que $\mathbb{F}_p(X)$ n'est pas un corps parfait.

### 3.2.1 Le théorème principal

**Théorème 3.17.** Soit $\mathbb{L}$ une extension finie sur $\mathbf{k}$ de degré $n$. Les assertions suivantes sont équivalentes.

1. L'extension $\mathbb{L}$ est séparable sur $\mathbf{k}$.
2. L'extension $\mathbb{L}$ est engendrée sur $\mathbf{k}$ par des éléments séparables.
3. Il existe exactement $n$ $\mathbf{k}$-plongements de $\mathbb{L}$ dans $\Omega$.
4. Il existe $\alpha \in \mathbb{L}$, élément séparable, tel que $\mathbb{L} = \mathbf{k}(\alpha)$.

L'implication (1) ⇒ (4) est ce qu'on appelle habituellement le **théorème de l'élément primitif**.
La preuve du théorème nécessitera le lemme suivant.

**Lemme 3.18.** Soit $V$ un espace vectoriel de dimension finie $d$ sur un corps $\mathbf{k}$ infini. Soit $V_1, \ldots, V_m$ une famille de sous-espaces vectoriels de $V$ tous distincts de $V$. Alors la réunion des $V_i$ est distincte de $V$.

*Démonstration.* Pour tout $i = 1, \ldots, m$ il existe une forme linéaire non nulle $f_i$ qui s'annulle sur $V_i$ (i.e. $V_i \subset \ker(f_i)$). Considérons alors la fonction (polynomiale dans des coordonnées) suivante : $F(x) = \prod_{i=1}^m f_i(x)$. Alors la réunion des $V_i$ est incluse dans $F^{-1}(0)$. Pour montrer le lemme, il suffit donc de montrer que $F$ n'est pas nulle sur $V$. Par l'absurde, supposons $F$ nulle. Le corps $\mathbf{k}$ étant infini, cela entraine que le polynôme $P_F \in \mathbf{k}[X_1, \ldots, X_d]$ correspondant est nul. Par intégrité de $\mathbf{k}[X_1, \ldots, X_d]$ cela implique que l'un des polynômes $P_{f_i}$ est nul ce qui entraine qu'une des fonctions $f_i$ est nulle. Absurde. □

Nous pouvons maintenant donner une :

*Démonstration du théorème.* L'implication (1) $\Rightarrow$ (2) est triviale car tout élément de $\mathbb{L}$ est supposé séparable.

Montrons (2) $\Rightarrow$ (3). Soit $\{\alpha_1, \ldots, \alpha_n\}$ une base de $\mathbb{L}$ sur $\mathbf{k}$ constituée d'éléments séparables. On a donc $\mathbb{L} = \mathbf{k}(\alpha_1, \ldots, \alpha_n)$. Considérons, pour chaque $i = 0, \ldots, n$, le corps $\mathbb{L}_i = \mathbf{k}(\alpha_1, \ldots, \alpha_i)$ ; avec la convention $\mathbb{L}_0 = \mathbf{k}$. Pour $i = 1, \ldots, n$, $\mathbb{L}_i = \mathbb{L}_{i-1}(\alpha_i)$. L'élément $\alpha_i$ est séparable sur $\mathbb{L}_{i-1}$ (voir prop. plus haut) de sorte que le polynôme minimal de $\alpha_i$ sur $\mathbb{L}_{i-1}$ est de degré $[\mathbb{L}_i : \mathbb{L}_{i-1}]$. Par suite, tout plongement de $\mathbb{L}_{i-1}$ dans $\Omega$ se prolonge de $[\mathbb{L}_i : \mathbb{L}_{i-1}]$ façons à $\mathbb{L}_i$ (voir dernière prop. de 5.1). Par conséquent, il y a

$$\prod_{i=1}^{n} [\mathbb{L}_i : \mathbb{L}_{i-1}] = [\mathbb{L} : \mathbf{k}] = n$$

plongements de $\mathbb{L}$ dans $\Omega$ qui prolongent l'application identité $\mathbb{K} \to \Omega$.

Montrons (3) $\Rightarrow$ (4). Considérons les $n$ $\mathbf{k}$-plongements de $\mathbb{L}$ dans $\Omega$ : $\sigma_1, \ldots, \sigma_n$. Supposons qu'il existe $\alpha \in \mathbb{L}$ tel que les $\sigma_i(\alpha)$ soient distincts deux à deux. Alors on a (au moins) $n$ $\mathbf{k}$-plongements de $\mathbf{k}(\alpha)$ dans $\Omega$ ce qui entraine que le polynôme minimal de $\alpha$ sur $\mathbf{k}$ est de degré au moins $n$ (voir dernière prop. de 5.1). Mais alors $[\mathbf{k}(\alpha) : \mathbf{k}] \geq n$. Mais comme $[\mathbb{L} : \mathbf{k}] = n$ et $\mathbf{k}(\alpha) \subseteq \mathbb{L}$, cela impose $\mathbb{L} = \mathbf{k}(\alpha)$.

Il nous reste donc à montrer qu'il existe un tel élément $\alpha$. On a deux cas.

Cas où $\mathbf{k}$ est fini. Dans ce cas, $\mathbb{L}$ est un corps fini et le groupe multiplicatif $\mathbb{L}^*$ est cyclique (admis pour le moment). On prend $\alpha$ un générateur de ce groupe. De plus $\alpha$ est séparable (voir dernier Cor. de 5.2).

Cas où $\mathbf{k}$ est infini. Pour tous $i \neq j$ dans $\{1, \ldots, n\}$, considérons l'ensemble $H_{i,j} = \{x \in \mathbb{L} \mid \sigma_i(x) = \sigma_j(x)\}$. Ce sont des sous-$\mathbf{k}$-espaces vectoriels de $\mathbb{L}$. Comme $\sigma_i \neq \sigma_j$, $H_{i,j} \neq \mathbb{L}$. Par le lemme précédent, la réunion $\bigcup H_{i,j}$ n'est pas égale à $\mathbb{L}$. On choisit alors $\alpha$ dans $\mathbb{L} \smallsetminus \bigcup H_{i,j}$. De plus $\alpha$ est séparable car son polynôme minimal (qui est de degré $n$) a $n$ racines distinctes dans $\Omega$ (par la dernière prop. de 5.1).

Il reste (4) $\Rightarrow$ (1). Par hypothèse on a $\mathbb{L} = \mathbf{k}(\alpha)$ avec $\alpha \in \mathbb{L}$ séparable. Il y a $n$ $\mathbf{k}$-plongements distincts de $\mathbb{L}$ dans $\Omega$ ; ici $n = [\mathbb{L} : \mathbf{k}(\alpha)]$ est le degré du polynôme $\mu_\alpha$. Soit maintenant $\beta \in \mathbb{L}$. Notons $m = [\mathbf{k}(\beta) : \mathbf{k}]$ et $r$ le nombre de $\mathbf{k}$-plongements $\mathbf{k}(\beta)$ dans $\Omega$ ; on a donc $r \leq m$. Un tel plongement se prolonge à son tour d'au plus $[\mathbb{L} : \mathbf{k}(\beta)]$ façons (cf. Cor. de 5.1). Si on avait $r < m$ alors le nombre de $\mathbf{k}$-plongements de $\mathbb{L}$ dans $\Omega$ serait $< n$ ce qui est faux. Ainsi $r = m$, i.e. (par la dernière prop. de 5.1) le degré de $\mu_\beta$ (qui est égal à $m$) est égal au nombre de ses racines distinctes ce qui entraine que $\beta$ est racine d'un polynôme séparable d'où (1). □

### 3.3 Extension normale et extension galoisienne

Dans ce paragraphe $\Omega$ désigne une clôture algébrique de $\mathbf{k}$.

**Définition 3.19.** Soit $\mathbb{L}$ une extension (algébrique) de $\mathbf{k}$ contenue dans $\Omega$.

- On dit que $\mathbb{L}$ est une extension normale de $\mathbf{k}$ si pour tout $\mathbf{k}$-plongement $\sigma$ de $\mathbb{L}$ dans $\Omega$, on a $\sigma(\mathbb{L}) = \mathbb{L}$.
- On dit que $\mathbb{L}$ est une extension galoisienne de $\mathbf{k}$ si $\mathbb{L}$ est normale et séparable.

**Définition 3.20.** Soit $\mathbb{L}$ une extension de $\mathbf{k}$ contenue dans $\Omega$. On appelle groupe de Galois de $\mathbb{L}$ sur $\mathbf{k}$, et on le note $\mathrm{Gal}(\mathbb{L}/\mathbf{k})$, le groupe des automorphismes de $\mathbb{L}$ qui laissent fixes les éléments de $\mathbf{k}$.

C'est un sous-groupe du groupe des automorphismes de $\mathbb{L}$.

**Exercice 3.21.**

- $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ est d'ordre 2 (son élément non trivial est la conjugaison complexe).
- $\mathrm{Gal}(\mathbb{R}/\mathbb{Q}) = \mathrm{Aut}(\mathbb{R}) = \{\mathrm{Id}_{\mathbb{R}}\}$.

**Proposition 3.22.** Soit $\mathbb{L}$ une extension finie de $\mathbf{k}$ contenue dans $\Omega$. On a toujours

$$|\mathrm{Gal}(\mathbb{L}/\mathbf{k})| \leq [\mathbb{L} : \mathbf{k}].$$

On a :

$$|\mathrm{Gal}(\mathbb{L}/\mathbf{k})| = [\mathbb{L} : \mathbf{k}] \iff \mathbb{L} \text{ est une extension galoisienne sur } \mathbf{k}.$$

*Démonstration.* L'inégalité découle directement de la prop. 1 de 5.1. Montrons l'équivalence. Posons $n = [L : \mathbf{k}]$. Supposons $\mathbb{L}$ galoisienne sur $\mathbf{k}$. Le groupe $\mathrm{Gal}(\mathbb{L}/\mathbf{k})$ est inclus dans l'ensemble des $\mathbf{k}$-plongements de $\mathbb{L}$ dans $\Omega$, mais les $\mathbb{L}$ étant normale, cette inclusion est une égalité. Comme $\mathbb{L}$ est séparable, le théorème précédent implique qu'il y a exactement $n$ tels plongements donc $\mathrm{Gal}(\mathbb{L}/\mathbf{k})$ est d'ordre $n$.
Réciproquement, supposons que $\mathrm{Gal}(\mathbb{L}/\mathbf{k})$ est d'ordre $n$. On sait qu'il y a au plus $n$ $\mathbf{k}$-plongements de $\mathbb{L}$ dans $\Omega$ donc il y en a exactement $n$ ce qui entraine que $\mathbb{L}$ est séparable sur $\mathbf{k}$ d'une part et d'autre part ces plongements fixent $\mathbf{k}$ et donc $\mathbb{L}$ est normale. □

**Proposition 3.23** (Critère de normalité)**.** Soit $\mathbb{L}$ une extension finie de $\mathbf{k}$ contenue dans $\Omega$. Alors $\mathbb{L}$ est normale si et s. si tout polynôme irréductible de $\mathbf{k}[X]$ ayant une racine dans $\mathbb{L}$ a toutes ses racines dans $\mathbb{L}$.

*Démonstration.* Supposons $\mathbb{L}$ normale. Soit $P \in \mathbf{k}[X]$ un polynôme irréductible et soit $\alpha \in \mathbb{L}$ une racine de $P$. Soit $\beta$ une racine quelconque de $P$ dans $\Omega$. Soit $\tau$ un $\mathbf{k}$-plongement de $\mathbf{k}(\alpha)$ dans $\Omega$. On peut prolonger $\tau$ en un morphisme $\Omega \to \Omega$ (voir dernière prop. de 3.4) puis en un plongement $\sigma$ de $\mathbb{L}$ dans $\Omega$. Puisque $\mathbb{L}$ est normale, on a $\sigma(\mathbb{L}) = \mathbb{L}$ ce qui entraine $\beta = \tau(\alpha) = \sigma(\alpha) \in \mathbb{L}$.
Réciproquement soit $\sigma : \mathbb{L} \to \Omega$ un $\mathbf{k}$-plongement. Soit $\alpha \in \mathbb{L}$. Notons $P \in \mathbf{k}[X]$ le polynôme minimal de $\alpha$ sur $\mathbf{k}$. Notons $\beta = \sigma(\alpha)$. On a alors $P(\beta) = \sigma(P(\alpha)) = 0$. $P$ est irréductible et a une racine dans $\mathbb{L}$ donc $\beta$ est aussi dans $\mathbb{L}$ ce qui montre $\sigma(\mathbb{L}) \subset \mathbb{L}$ mais comme $\mathbb{L}$ et $\sigma(\mathbb{L})$ sont deux $\mathbf{k}$-espaces vectoriels de même dimension finie, on a $\sigma(\mathbb{L}) = \mathbb{L}$. □

On peut voir la séparabilité et la normalité sous l'angle suivant :

**Proposition 3.24.** Soit $\mathbb{L}$ une extension finie de $\mathbf{k}$.

1. L'extension $\mathbb{L}/\mathbf{k}$ est séparable si et s. si pour tout $\alpha \in \mathbb{L}$, $\mu_\alpha$ est à racines simples dans $\Omega[X]$.
2. L'extension $\mathbb{L}/\mathbf{k}$ est normale si et s. si pour tout $\alpha \in \mathbb{L}$, $\mu_\alpha$ est scindé dans $\mathbb{L}[X]$.
3. L'extension $\mathbb{L}/\mathbf{k}$ est galoisienne si et s. si pour tout $\alpha \in \mathbb{L}$, $\mu_\alpha$ est scindé à racines simples dans $\mathbb{L}[X]$.

*Démonstration.* Le (1) a déjà été évoqué. Le (2) est une conséquence assez directe de la prop. précédente et le (3) n'est rien d'autre que (1) et (2). □

**Lemme 3.25.** On rappelle que $\Omega = \overline{\mathbf{k}}$ désigne une clôture algébrique de $\mathbf{k}$.

1. Soient $\alpha, \beta \in \Omega$. Les deux assertions suivantes sont équivalentes.
   (a) Il existe un $\mathbf{k}$-isomorphisme de corps $\sigma : \Omega \to \Omega$ (i.e. tel que $\sigma$ est égal à l'identité sur $\mathbf{k}$) tel que $\sigma(\alpha) = \beta$.
   (b) Les polynômes minimaux $\mu_\alpha$ et $\mu_\beta$ sont égaux.

2. De plus, si on note $\mathrm{Aut}_{\mathbf{k}}(\Omega)$ le groupe des $\mathbf{k}$-automorphismes du corps $\Omega$ alors pour tout $\alpha \in \Omega$,

$$\{\sigma(\alpha) \mid \sigma \in \mathrm{Aut}_{\mathbf{k}}(\Omega)\} = \mu_\alpha^{-1}(\{0\}).$$

*Démonstration.* Montrons (a) $\Rightarrow$ (b). Supposons qu'on ait un $\mathbf{k}$-morphisme $\sigma : \Omega \to \Omega$ tel que $\sigma(\alpha) = \beta$. Si on note $\mu_\alpha = \sum a_i X^i$ alors on aura : $\mu_\alpha(\beta) = \sum a_i \beta^i = \sigma(\sum a_i \alpha^i) = \sigma(\mu_\alpha(\alpha)) = \sigma(0) = 0$ donc $\mu_\beta | \mu_\alpha$. Ces polynômes sont irréductibles et unitaires donc égaux, d'où (b).
Réciproquement supposons que $\mu_\alpha = \mu_\beta$. Alors on obtient un $\mathbf{k}$-isomorphisme de corps $\mathbf{k}[\alpha] \simeq \mathbf{k}[\beta]$ (exercice) qui envoie $\alpha$ sur $\beta$. Cet isomorphisme se prolonge en un $\mathbf{k}$-morphisme $\mathbf{k}[\alpha] \to \Omega$ (par inclusion) puis en utilisant le 2ème théorème de 3.4, on peut prolonger ce morphisme en un $\sigma : \Omega \to \Omega$ ce qui donne (a).
Montrons l'inclusion $\subseteq$ dans (2). Soit donc $\beta = \sigma(\alpha)$ avec $\alpha \in \Omega$ et $\sigma \in \mathrm{Aut}_{\mathbf{k}}(\Omega)$. D'après le point (b), $\mu_\alpha = \mu_\beta$ annule $\beta$ d'où l'inclusion voulue. Réciproquement, soit $\beta$ une racine de $\mu_\alpha$ alors $\mu_\alpha | \mu_\beta$ et par suite $\mu_\alpha = \mu_\beta$ donc, par (a) il existe $\sigma \in \mathrm{Aut}_{\mathbf{k}}(\Omega)$ tel que $\sigma(\alpha) = \beta$ ce qui donne l'appartenance de $\beta$ à l'ensemble de gauche. □

**Définition 3.26.** Deux éléments $\alpha, \beta \in \Omega$ tels que $\mu_\alpha = \mu_\beta \in \mathbf{k}[X]$ sont dit conjugués sur $\mathbf{k}$.

Exemple : $\sqrt{2}$ et $-\sqrt{2}$ sont conjugués sur $\mathbb{Q}$ et leur polynôme minimal est $X^2 - 2$.

**Proposition 3.27.** Soit $\mathbb{L}$ une extension finie de $\mathbf{k}$ contenue dans $\Omega$. Les assertions suivantes sont équivalentes :

1. L'extension $\mathbb{L}$ est galoisienne sur $\mathbf{k}$.
2. $\mathbb{L}$ est le corps de décomposition d'un polynôme séparable de $\mathbf{k}[X]$.

*Démonstration.* Supposons (1). Alors par le théorème de 5.2.1, il existe $\alpha \in \mathbb{L}$ séparable tel que $\mathbb{L} = \mathbf{k}(\alpha)$. Soit $P$ le polynôme minimal de $\alpha$ alors $P$ divise un polynôme séparable, il est donc séparable. De plus, par la prop. précédente, toutes les racines de $P$ sont dans $\mathbb{L}$, i.e. $P$ est scindé dans $\mathbb{L}[X]$. Si on note $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ les racines de $P$ dans $\mathbb{L}$, et si on note $\mathbb{K} = \mathbf{k}(\alpha_1, \ldots, \alpha_n)$ le corps de décomposition de $P$ alors on a $\mathbb{L} = \mathbf{k}(\alpha) = \mathbb{K}$. D'où (2).
Supposons (2). Par hypothèse $\mathbb{L} = \mathbf{k}(\alpha_1, \ldots, \alpha_n)$ avec $P \in \mathbf{k}[X]$ séparable de racines les $\alpha_i$. L'extension $\mathbb{L}$ est donc séparable. Soit $\sigma : \mathbb{L} \to \Omega$ un $\mathbf{k}$-plongement. Alors $P(\sigma(\alpha_i)) = \sigma(P(\alpha_i)) = 0$ donc $\sigma(\alpha_i)$ est un des $\alpha_j$ ce qui entraine $\sigma(\mathbb{L}) \subset \mathbb{L}$. Comme ci-dessus, étant en dimension finie sur $\mathbf{k}$, cela entraine $\sigma(\mathbb{L}) = \mathbb{L}$ et donc $\mathbb{L}$ est normale, d'où (1). □

Voici résumé dans ce théorème une partie de ce qu'on a dit ici auquel on ajoute d'autres résultats.

**Théorème 3.28.** Soit $\mathbb{L}$ une extension finie de $\mathbf{k}$ contenue dans $\Omega$. Les assertions suivantes sont équivalentes.

1. L'extension $\mathbb{L}/\mathbf{k}$ est galoisienne.
2. Le corps $\mathbb{L}$ est le corps de décomposition d'un certain polynôme séparable de $\mathbf{k}[X]$.
3. $|\mathrm{Gal}(\mathbb{L}/\mathbf{k})| = [\mathbb{L} : \mathbf{k}]$.
4. Pour tout $\alpha \in \mathbb{L}$, on a $\mu_\alpha = \prod_{\beta \in \mathrm{Gal}(\mathbb{L}/\mathbf{k}) \cdot \alpha} (X - \beta)$ où $\mathrm{Gal}(\mathbb{L}/\mathbf{k}) \cdot \alpha = \{\sigma(\alpha) \mid \sigma \in \mathrm{Gal}(\mathbb{L}/\mathbf{k})\}$.
5. $\{\alpha \in \mathbb{L} \mid \forall \sigma \in \mathrm{Gal}(\mathbb{L}/\mathbf{k}), \sigma(\alpha) = \alpha\} = \mathbf{k}$.

*Démonstration.* Les équivalences (1) $\iff$ (2) $\iff$ (3) ont été démontrées.
Montrons (1) $\Rightarrow$ (5). Soit $\alpha \in \mathbb{L}$ tel que pour tout $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbf{k})$, $\sigma(\alpha) = \alpha$. Supposons par l'absurde $\alpha \notin \mathbf{k}$. Soit $P$ le polynôme minimal de $\alpha$. On sait que $P$ est séparable. Comme $\alpha \notin \mathbf{k}$, cela entraine l'existence d'au moins une autre racine $\beta$ de $P$. Il existe alors $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbf{k})$ tel que $\sigma(\alpha) = \beta$ (on peut utiliser le point (2) du lemme précédent pour un tel $\sigma$) ce qui est absurde.
Montrons (5) $\Rightarrow$ (4). Soit $\alpha \in \mathbb{L}$ et posons $Q = \prod_{\beta \in \mathrm{Gal}(\mathbb{L}/\mathbf{k})\cdot\alpha}(X - \beta)$. Le lemme ci-dessus nous dit que chaque $\beta \in \mathrm{Gal}(\mathbb{L}/\mathbf{k}) \cdot \alpha$ est une racine de $\mu_\alpha$ donc $Q$ divise $\mu_\alpha$. Puisque $\mu_\alpha$ est irréductible, il suffit de montrer que $Q \in \mathbf{k}[X]$ pour avoir $Q = \mu_\alpha$. Comme souvent, on étend l'action de $\mathrm{Gal}(\mathbb{L}/\mathbf{k})$ à $\mathbf{k}[X]$ et l'hypothèse (5) nous dit alors qu'un polynôme de $\mathbb{L}[X]$ est dans $\mathbf{k}[X]$ si et s. si il est laissé fixe par $\mathrm{Gal}(\mathbb{L}/\mathbf{k})$. Voyons que c'est bien le cas du polynôme $Q$ : soit $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbf{k})$,

$$\sigma^*(Q) = \prod_{\beta \in \mathrm{Gal}(\mathbb{L}/\mathbf{k})\cdot\alpha} (X - \sigma(\beta)) = \prod_{\gamma \in (\sigma\mathrm{Gal}(\mathbb{L}/\mathbf{k}))\cdot\alpha} (X - \gamma) = \prod_{\gamma \in \mathrm{Gal}(\mathbb{L}/\mathbf{k})\cdot\alpha} (X - \gamma) = Q.$$

Ainsi $Q \in \mathbf{k}[X]$ et par suite $Q = \mu_\alpha$.
Montrons (4) $\Rightarrow$ (1). Soit $\alpha \in \mathbb{L}$. Par hypothèse, $\mu_\alpha$ est à racines simples dans $\Omega[X]$. De plus, ses racines sont dans $\mathbb{L}$ car pour tout $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbf{k})$, $\sigma(\alpha) \in \mathbb{L}$. Ainsi $\mu_\alpha$ est scindé à racines simples dans $\mathbb{L}$ ce qui entraine (1). □

### 3.4 Groupe de Galois d'un polynôme

Dans ce paragraphe, on suppose que toutes les extensions algébriques de $\mathbf{k}$ sont séparables (i.e. tout polynôme irréductible est séparable ou encore $\mathbf{k}$ est parfait). On sait que c'est le cas si $\mathbf{k}$ est de caractéristique 0 ou bien si $\mathbf{k}$ est fini.
$\Omega$ désigne toujours une clôture algébrique de $\mathbf{k}$.

**Définition 3.29.** Soit $P \in \mathbf{k}[X]$. Soit $\mathbb{L}$ son corps de décomposition dans $\Omega$. On appelle groupe de Galois de $P$, noté $\mathrm{Gal}(P)$, le groupe de Galois $\mathrm{Gal}(\mathbb{L}/\mathbf{k})$.

**Proposition 3.30.** Soit $P \in \mathbf{k}[X]$. Soit $n$ le nombre de racines distinctes de $P$. On les numérote : $\alpha_1, \ldots, \alpha_n$. Alors pour tout $\sigma \in \mathrm{Gal}(f)$, $\sigma$ induit une bijection sur l'ensemble des $\alpha_i$ et donc une bijection $s_\sigma$ de $\{1, \ldots, n\}$.
L'application $\mathrm{Gal}(f) \to S_n, \sigma \mapsto s_\sigma$ est un morphisme injectif de groupe.

*Démonstration.* Soit $\sigma \in \mathrm{Gal}(f)$. Notons $A$ l'ensemble des racines de $P$. On a $0 = \sigma(P(\alpha_i)) = P(\sigma(\alpha_i))$ donc $\sigma(\alpha_i)$ est une racine de $P$. On a donc une application $A \to A$ induite par $\sigma$. Mais $\sigma$ est injective et $A$ est fini donc cette application est bijective. On a donc une permutation $s_\sigma \in S_n$ donnée par $\sigma(\alpha_i) = \alpha_{s_\sigma(i)}$.
Soient $\sigma, \sigma' \in \mathrm{Gal}(f)$. Alors pour $\alpha_i \in A$, $\alpha_{s_{\sigma'\circ\sigma}(i)} = \sigma'(\sigma(\alpha_i)) = \sigma'(\alpha_{s_\sigma(i)}) = \alpha_{s_{\sigma'}(s_\sigma(i))}$ d'où $s_{\sigma'} \circ s_\sigma = s_{\sigma'\circ\sigma}$ et on a bien un morphisme de groupes. De plus si $s_\sigma$ est l'identité alors pour tout $\alpha_i$, on aura $\sigma(\alpha_i) = \alpha_i$ pour tout $i$ ce qui entraine $\sigma(\alpha) = \alpha$ pour tout $\alpha \in \mathbb{L} = \mathbf{k}(\alpha_1, \ldots, \alpha_n)$ d'où l'injectivité de $\sigma \mapsto s_\sigma$. □

**Remarque 3.31.** Si on change la numérotation alors $\mathrm{Gal}(f)$ est transformé en un sous-groupe conjugué de $S_n$.
En effet, un changement de numérotation correspond à faire agir un élément $\tau \in S_n$, à faire agir $\mathrm{Gal}(f)$ puis à faire agir $\tau^{-1}$ pour revenir à la numérotation initiale.
Les détails sont laissés en exercice.

**Exercice 3.32.** Le polynôme $P \in \mathbf{k}[X]$ est irréductible si et s. si $\mathrm{Gal}(P)$ permute transitivement les racines de $P$.

**Proposition 3.33.** Soit $P \in \mathbf{k}[X]$ un polynôme séparable dont on note $\alpha_1, \ldots, \alpha_n \in \Omega$ les racines. On note $\delta = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)$. On rappelle que le discriminant de $P$ est $\Delta = \delta^2$.

1. Pour $\sigma \in \mathrm{Gal}(P)$, $\sigma(\delta) = \varepsilon(\sigma)\delta$ et $\sigma(\Delta) = \Delta$.
2. On a les équivalences :

$$\delta \in \mathbf{k}^* \iff \Delta \in (\mathbf{k}^*)^2 \iff \mathrm{Gal}(P) \subset A_n.$$

L'expression $\Delta \in (\mathbf{k}^*)^2$ signifie que $\Delta$ est le carré d'un élément non nul de $\mathbf{k}$ et rappelons que $A_n$ est le groupe alterné (sous-groupe de $S_n$ obtenu comme noyau de $\varepsilon : S_n \to \{-1, 1\}$).

*Démonstration.* Une fois la numérotation fixée, on identifie $\sigma \in \mathrm{Gal}(P)$ et $s_\sigma \in S_n$ et on alors

$$\sigma(\delta) = \prod_{i<j} (\alpha_{\sigma(i)} - \alpha_{\sigma(j)}) = \prod_{i<j} \mathrm{sign}(\sigma(i) - \sigma(j))(\alpha_i - \alpha_j) = \varepsilon(\sigma)\delta.$$

De cette égalité découle $\sigma(\Delta) = (\sigma(\delta))^2 = \delta^2 = \Delta$ (sinon on dit simplement que $\Delta \in \mathbf{k}$, ce qui a été vu dans le chapitre résultant/discriminant).
Si $\delta \in \mathbf{k}^*$ alors $\Delta$ est un carré dans $\mathbf{k}$ (trivial). Réciproquement si $\Delta = \lambda^2$ avec $\lambda \in \mathbf{k}^*$ alors $0 = \delta^2 - \lambda^2 = (\delta - \lambda)(\delta + \lambda)$ ce qui entraine que $\delta \in \mathbf{k}^*$.
Si $\mathrm{Gal}(P) \subseteq A_n$ alors pour tout $\sigma \in \mathrm{Gal}(P)$, on a $\sigma(\delta) = \delta$ donc par le point 5 du théorème de 5.3, cela signifie que $\delta \in \mathbf{k}$ et donc $\delta \in \mathbf{k}^*$ puisque les racines sont simples. Réciproquement si $\delta \in \mathbf{k}^*$ alors pour tout $\sigma \in \mathrm{Gal}(P)$, $\delta = \sigma(\delta) = \varepsilon(\sigma)\delta$ ce qui signifie $\sigma \in A_n$. □

**Lemme 3.34.** Soit $P \in \mathbf{k}[X]$ séparable. On suppose $P$ irréductible de degré $p$ premier. Alors $\mathrm{Gal}(P)$ vu comme sous-groupe de $S_p$ contient un $p$-cycle.

*Démonstration.* Le corps de rupture $\mathbb{K} = \mathbf{k}[X]/\langle P \rangle$ est de degré égal au degré de $P$, i.e. $[\mathbb{K} : \mathbf{k}] = p$. Si on note $\mathbb{L}$ le corps de décomposition de $P$ alors $[\mathbb{L} : \mathbf{k}] = [\mathbb{L} : \mathbb{K}] \times p$. Le point 2 du théorème de 5.3 nous assure que $\mathbb{L}/\mathbf{k}$ est galoisienne et donc l'ordre du groupe $\mathrm{Gal}(P)$ est égal à $[\mathbb{L} : \mathbf{k}]$ ce qui entraine que $p$ divise cet ordre. Par le théorème de Cauchy sur les groupes, $\mathrm{Gal}(P)$ contient un élément d'ordre $p$. Mais un élément d'ordre $p$ dans $S_p$ est un $p$-cycle d'où la conclusion. □

**Lemme 3.35.** Soient $\tau \in S_n$ une transposition et $\sigma \in S_n$ un $n$-cycle. Alors $\{\tau, \sigma\}$ engendre $S_n$.

*Démonstration.* Rappelons que si $\alpha = (a_1 a_2 \ldots a_k)$ est un $k$-cycle et si $\beta \in S_n$ est une permutation quelconque alors le conjugué $\beta c \beta^{-1}$ est le cycle $(\beta(a_1) \ldots \beta(a_k))$.
Soit $\tau = (i\ j)$. Quitte à remplacer $\sigma$ par une de ses puissances, on peut supposer que $\sigma(i) = j$.
Pour $s = 0, \ldots, n-1$, $\sigma^s \tau \sigma^{-s} = (\sigma^s(i)\sigma^s(j)) = (\sigma^s(i), \sigma^{s+1}(i))$.
Soient $r > s + 1$. On a alors la conjugaison suivante :

$$(\sigma^{r-1}(i)\sigma^r(i)) \cdots (\sigma^{s+1}(i)\sigma^{s+2}(i)) \cdot (\sigma^s(i)\sigma^{s+1}(i)) \cdot (\sigma^{s+1}(i)\sigma^{s+2}(i)) \cdots (\sigma^{r-1}(i)\sigma^r(i)) = (\sigma^r(i)\sigma^s(i)).$$

Pour voir que cette égalité est vraie, on pense au rappel ci-dessus qui nous dit que cette conjugaison est bien un 2-cycle et on voit que l'image de $\sigma^r(i)$ est $\sigma^s(i)$ ce qui donne la transposition voulue.
Par conséquent, on voit que toute transposition de $S_n$ est dans le sous-groupe $\langle \tau, \sigma \rangle$ ce qui montre que ce dernier est $S_n$. □

**Exemple 3.36.** Le groupe de Galois de $P = X^5 - 10X + 5 \in \mathbb{Q}[X]$ est $S_5$.

*Démonstration.* Par le critère d'Eiseinstein, on peut montrer que $P$ est irréductible dans $\mathbb{Q}[X]$. Comme on est en caractéristique nulle, cela entraine que $P$ est séparable. Le groupe de Galois $\mathrm{Gal}(P)$ contient donc un 5-cycle.
Son polynôme dérivé $P' = 5(X^4-2)$ permet une étude des variations de $P$ et montre que $P$ a exactement trois racines réelles et donc deux racines complexes (non réelles) conjuguées.
La conjugaison dans $\mathbb{C}$, restreinte à $\mathrm{Gal}(P)$ est une transposition dans $S_5$. Ainsi, $\mathrm{Gal}(P)$ contient un 5-cycle et une transposition, c'est donc $S_5$ tout entier par le lemme précédent. □

**Remarque 3.37.** On verra plus loin que ce polyôme n'est pas résoluble par radicaux, i.e. qu'on ne peut pas obtenir ses racines à partir d'éléments de $\mathbb{Q}$ en faisant opérer l'addition, la soustraction, la multiplication, la division et l'extraction de racine $n$-ième un nombre fini de fois.

Voici un autre outil qui peut aider à déterminer le groupe de Galois d'un polynôme de $\mathbb{Q}[X]$.

**Proposition 3.38** (Réduction modulo $p$)**.** Soit $p$ un nombre premier. Soit $P$ un polynôme unitaire séparable de degré $n$ dans $\mathbb{Z}[X]$. Notons $\overline{P} \in \mathbb{Z}/p\mathbb{Z}[X]$ le polynôme obtenu en réduisant modulo $p$ les coefficients de $P$. On suppose $\overline{P}$ séparable.
Soit $\overline{P} = \prod_{i=1}^{t} \overline{P_i}$ la décomposition de $\overline{P}$ en polynômes irréductibles dans $\mathbb{Z}/p\mathbb{Z}[X]$.
Pour $i = 1, \dots, t$, notons $n_i$ le degré de $\overline{P_i}$.
Alors $\mathrm{Gal}(P)$, vu comme sous-groupe de $S_n$, contient un élément du type $\prod_{i=1}^{t} \sigma_i$ où les $\sigma_i$ sont des cycles à supports disjoints avec $|\sigma_i| = n_i$.

*Démonstration.* Admis (car on ne l'utilisera pas directement dans ce cours). □

## 3.5 Quelques extensions galoisiennes particulières

### 3.5.1 Rappels sur les corps et les groupes finis

Les résultats énoncés ici ont probablement été vus au semestre précédent. Dans le soucis d'être complet, nous décidons de revoir quelques résultats dont certains utiles pour la suite.

**Définition 3.39.** Étant donné un corps $\mathbf{k}$, on appelle sous-corps premier de $\mathbf{k}$ l'intersection de tous les sous-corps de $\mathbf{k}$ (c'est le plus petit sous-corps de $\mathbf{k}$).

**Proposition 3.40.** Pour un corps $\mathbf{k}$, on a deux cas :

1. Si $\mathrm{car}(\mathbf{k}) = 0$ alors $\mathbf{k}$ contient $\mathbb{Z}$ et donc contient $\mathbb{Q}$ qui est donc le sous-corps premier de $\mathbf{k}$.
2. Si $\mathrm{car}(\mathbf{k}) = \mathrm{p} > 0$ alors $\mathbf{k}$ contient $\mathbb{F}_p$ qui est le sous-corps premier de $\mathbf{k}$.

**Proposition 3.41.** Soit $A$ un anneau (commutatif) de caractéristique $p$. Alors l'application $F_A : A \to A,\ a \mapsto a^p$ est un endomorphisme de $\mathbb{F}_p$-algèbres. On l'appelle **endomorphisme de Frobenius** de $A$.

*Démonstration.* Soient $a, b \in A$. On a clairement $(ab)^p = a^p b^p$ et $(a+b)^p = \sum_{k=0}^{p} \binom{k}{p} a^{p-k} b^k = a^p + b^p$ (car les autres termes disparaissent modulo $p$) ; enfin pour $a \in F_p$, $F_A(a) = a$ par le petit théorème de Fermat. □

**Remarque 3.42.** Si $\varphi : A \to B$ est un morphisme entre deux anneaux de caractéristique $p$ alors $\varphi \circ F_A = F_B \circ \varphi$.

Si $\mathbf{k}$ est un corps de caractéristique $p$, on note

$$\mathbf{k}^F = \{x \in \mathbf{k} \ ; \ \mathbb{F}_{\mathbf{k}}(x) = x\}$$

l'ensemble des points fixes de $\mathbb{F}_{\mathbf{k}}$.

**Lemme 3.43.** L'ensemble $\mathbf{k}^F$ est un sous-corps de $\mathbf{k}$ et on a : $\mathbf{k}^F = \mathbb{F}_p$.

*Démonstration.* On montre uniquement l'inclusion non triviale. Soit donc $x \in \mathbf{k}^F$. Alors $x$ est racine de $X^p - X$, i.e. $X - x | X^p - X$.
D'autre part pour tout $a \in \mathbb{F}_p$, $a^p = a$ donc $X - a$ divise $X^p - X$ ; ce qui entraine $\prod_{a \in \mathbb{F}_p}(X - a)$ divise $X^p - X$ et lui est donc égal ( car polynômes unitaires de même degré). Par unicité des facteurs irréductibles $X - x$ est l'un des $X - a$ avec $a \in \mathbb{F}_p$ d'où $x \in \mathbb{F}_p$. □

Pour $r \in \mathbb{N}^*$, l'ensemble

$$\mathbf{k}^{F^r} = \{x \in \mathbf{k} \ ; \ (F_{\mathbf{k}})^r(x) = x\}$$

des points fixes de $F_k \circ \cdots \circ F_k$ ($r$ fois) est un sous-corps de $\mathbf{k}$.

**Proposition 3.44.**

- Notons $\mathbb{K}$ une clôture algébrique de $\mathbb{F}_p$. Alors le corps $\mathbb{K}^{F^r}$ est le corps de décomposition du polynôme $X^{p^r} - X$ sur $\mathbb{F}_p$.
- Toute extension finie $\mathbf{k}$ de $\mathbb{F}_p$, de degré $d = [\mathbf{k} : \mathbb{F}_p]$, est un corps de décomposition de $X^{p^d} - X$ sur $\mathbb{F}_p$.

*Démonstration.* Soit $x \in \mathbb{K}$. On a $x \in \mathbb{K}^{F^r} \iff x$ est racine de $X^{p^r} - X$. Ainsi, $\mathbb{K}^{p^r}$ est l'ensemble des racines de $X^{p^r} - X$. Comme c'est un corps, c'est le corps de décomposition de $X^{p^r} - X$.
Réciproquement, soit $\mathbf{k}$ une extension finie (qu'on peut supposer incluse dans $\mathbb{K}$) de degré $d$. Alors $\mathbf{k}$ est isomorphe à $\mathbb{F}_p^d$ comme $\mathbb{F}_p$-espace vectoriel ce qui entraine $|\mathbf{k}| = p^d$. Son groupe multiplicatif $\mathbf{k}^*$ est donc de cardinal $p^d - 1$. Donc tout élément $x \in \mathbf{k}^*$ satisfait $x^{p^d} - 1 = 0$. Il s'ensuit que tout $x \in \mathbf{k}$ est racine de $X(X^{p^d} - 1) = X^{p^d} - X$. Ainsi $\mathbf{k}$ est un corps de décomposition de ce polynôme. □

**Remarque 3.45.** Pour $P \in \mathbf{k}[X]$, on a définit le corps de décomposition comme le sous-corps de $\overline{\mathbf{k}}$ engendré par les racines de $P$ ; on a vu que c'est le plus petit corps (à isomorphisme près dans lequel $P$ est scindé).
Quand on dit un corps de décomposition, cela signifie un corps sur lequel $P$ est scindé (c'est donc un corps dans lequel s'injecte le corps de décomposition de $P$).

**Corollaire 3.46.**

1. Étant donné un nombre premier $p$ et $r \in \mathbb{N}^*$, il existe un corps $\mathbb{F}_{p^r}$ de cardinal $p^r$, unique à isomorphisme près. C'est le corps de décomposition du polynôme $X^{p^r} - X$ sur $\mathbb{F}_p$.
2. Tout corps fini est de la forme $\mathbb{F}_{p^r}$ avec $p$ premier et $r \in \mathbb{N}^*$.

*Démonstration.* Le polynôme $P = X^{p^r} - X \in \mathbb{F}_p[X]$ est séparable (car $P' = -1$ est premier avec $P$) Notons $\mathbb{L}$ le corps de décomposition de ce polynôme. On a vu que $\mathbb{L} = (\overline{\mathbb{F}_p})^{F^r}$ dont le cardinal est celui des racines de $P$ dans $\overline{\mathbb{F}_p}$. Comme $P$ est séparable, le nombre de racines distinctes de $P$ est $p^r$, c'est donc le cardinal de $\mathbb{K}$.

Soit maintenant un corps fini $\mathbf{k}$. Il est donc de caractéristique non nulle. Notons la $p$. Notons $r = [\mathbf{k} : \mathbb{F}_p]$. D'après la proposition ci-dessus, $\mathbf{k}$ est un corps de décomposition de $X^{p^r} - X$. Ainsi $\mathbb{F}_{p^r}$ s'injecte dans $\mathbf{k}$. Mais comme ils ont le même cardinal $p^r$, ils sont donc égaux (à isomorphisme près). □

**Proposition 3.47.** On se donne $p \in \mathbb{N}$ premier et $r \in \mathbb{N}^*$.
L'extension $\mathbb{F}_{p^r}/\mathbb{F}_p$ est galoisienne et $\mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p)$ est cyclique d'ordre $r$ engendré par le morphisme de Frobenius $F$.

*Démonstration.* L'extension est galoisienne car $\mathbb{F}_{p^r}$ est le corps de décomposition du polynôme séparable $X^{p^r} - X$. Considérons $F$ l'endomorphisme de Frobenius de $\mathbb{F}_{p^r}$. C'est donc un automorphisme (car $\mathbb{F}_{p^r}$ est de cardinal fini) et c'est donc un élément de $\mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p)$.
Remarquons que $p^r = |\mathbb{F}_{p^r}| = p^d$ où $d = [\mathbb{F}_{p^r} : \mathbb{F}_p] = |\mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p)|$ donc $d = r$. On a $F^r = \mathrm{Id}$. De plus pour tout $s < r$, le sous-corps des points fixes de $F^s$ est l'ensemble des racines de $X^{p^s} - X$, qui est donc de cardinal $< p^r$. Par conséquent $F$ est bien d'ordre $r$. Ainsi $F$ engendre $\mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p)$ (car il est de cardinal $r$). □

Encore deux résultats qu'on donne sans preuve.

**Proposition 3.48.** Soit $\mathbf{k}$ un corps et $G \subset \mathbf{k}^*$ un sous-groupe fini de $\mathbf{k}^*$. Alors $G$ est cyclique.

**Proposition 3.49.** Tout groupe abélien fini est un produit de groupes cycliques.

### 3.5.2 Extension cyclotomique

**Définition 3.50.** Étant donné un corps $\mathbf{k}$ et un entier $n \in \mathbb{N}^*$, l'extension $n$-cyclotomique de $\mathbf{k}$ est le corps de décomposition du polynôme $X^n - 1$, qu'on notera $\mathbf{k}_n$.

Nous allons montrer la proposition suivante.

**Proposition 3.51.**

1. Pour tout corps $\mathbf{k}$, on a une injection de groupes
$$\mathrm{Gal}(\mathbf{k}_n/\mathbf{k}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*.$$
2. Si $\mathbf{k} = \mathbb{F}_p$ alors il existe $r \in \mathbb{N}^*$ tel que $\mathbf{k}_n = F_{p^r}$ et $\mathrm{Gal}(\mathbf{k}_n/\mathbf{k})$ est cyclique d'ordre $r$.
3. Si $\mathbf{k} = \mathbb{Q}$ alors on a un isomorphisme de groupes $\mathrm{Gal}(\mathbf{k}_n/\mathbf{k}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$.

*Démonstration.* L'extension $\mathbf{k}_n/\mathbf{k}$ On sait que $\mathrm{Gal}(\mathbf{k}_n/\mathbf{k})$ induit une bijection de l'ensemble $\Gamma_n$ des racines de $X^n - 1$ dans $\overline{\mathbf{k}}$. L'ensemble $\Gamma_n$ est en fait un groupe multiplicatif, sous-groupe fini de $\overline{\mathbf{k}}^*$, il est donc cyclique (voir les dernières prop. de 5.5.1).
On sait que $\mathrm{Gal}(\mathbf{k}_n/\mathbf{k})$ induit une bijection de $\Gamma_n$. On a donc un morphisme injectif de groupes
$$\mathrm{Gal}(\mathbf{k}_n/\mathbf{k}) \hookrightarrow \mathrm{Aut}(\Gamma_\mathrm{n}).$$
Soit $\zeta$ un générateur de $\Gamma_n$. Si $\sigma \in \mathrm{Gal}(\mathbf{k}_n/\mathbf{k})$ alors $\sigma(\zeta) \in \Gamma_n$, donc il existe $m_\sigma \in \mathbb{Z}$ unique modulo $n$, tel que $(m_\sigma, n) = 1$ et $\sigma(\zeta) = \zeta^{m_\sigma}$. On obtient donc une injection de groupes
$$\chi : \mathrm{Gal}(\mathbf{k}_n/\mathbf{k}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*, \quad \sigma \mapsto (m_\sigma \bmod \mathrm{n}).$$

En effet pour $\sigma, \sigma' \in \mathrm{Gal}(\mathbf{k}_n/\mathbf{k})$ et $q \in \mathbb{Z}$, $\sigma'(\sigma(\zeta^q)) = \sigma'(\zeta^{qm_\sigma}) = (\sigma'(\zeta))^{qm_\sigma} = (\zeta^q)^{m_{\sigma'}m_\sigma}$ d'où $\chi(\sigma'\circ\sigma) = m_\sigma m_{\sigma'} = \chi(\sigma)\chi(\sigma')$.
Supposons maintenant $\mathbf{k} = \mathbb{F}_p$, alors on a vu que $\mathbf{k}_n$ est nécessairement de la forme $\mathbb{F}_{p^r}$ et on conclut avec une prop. ci-dessus pour dire que le groupe de Galois est cyclique d'ordre $r$.
Supposons maintenant que $\mathbf{k} = \mathbb{Q}$.
Dans ce cas, $\mathbf{k}_n = \mathbb{Q}(e^{2i\pi/n})$. Montrons que le morphisme $\chi : \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^*$ construit à partir $\zeta = e^{2i\pi/n}$ est un isomorphisme. Comme on sait que c'est morphisme injectif, il suffit donc d'avoir

$$[\mathbb{Q}_n : \mathbb{Q}] = \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$$

où $\varphi$ désigne l'indicatrice d'Euler.
On pose

$$\Phi_n(X) = \prod_{0\leq a<n,(a,n)=1} (X - e^{2i\pi a/n}) = \prod_{\theta \text{ d'ordre } n} (X - \theta) \in \overline{Q}[X]$$

où le second produit est indexé par les racines primitives de l'unité.
On a donc $X^n - 1 = \prod_{d|n} \Phi_d(X)$ dans $\overline{\mathbb{Q}}[X]$ (exercice). Pour tout $\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ et toute racine primitive $\theta$ de 1, $\sigma(\theta)$ est encore une racine primitive de 1 donc $\Phi_n(X)$ est fixé par tout $\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$. Cela entraine $\Phi_n(X) \in \mathbb{Q}[X]$ (voir dernier théo. de 5.3).
Supposons qu'on ait : $\Phi_n(X)$ irréductible sur $\mathbb{Q}$.
Alors le corps de décomposition $\mathbb{L}$ de $\Phi_n$ s'injecte dans $\mathbb{Q}_n$ ainsi $[\mathbb{L} : \mathbb{Q}] \leq [\mathbb{Q}_n : \mathbb{Q}] \leq \phi(n)$. Mais $\Phi_n$ étant irréductible, c'est le polynôme minimal de $\zeta = e^{2i\pi/n}$ donc $[\mathbb{L} : \mathbb{Q}] = \deg(\Phi_n) = \varphi(n)$ ce qui entraine l'égalité voulue.
Il reste donc à montrer que $\Phi_n$ est irréductible sur $\mathbb{Q}$. □

D'abord un petit résultat intermédiaire :

**Lemme 3.52.** Soit $A$ un anneau intègre et $\mathbb{K}$ un corps contenant $A$. Soient $F, G \in A[X]$ avec $G$ unitaire. Supposons qu'il existe $H \in \mathbb{K}[X]$ tel que $F = GH$ alors $H \in A[X]$.

*Démonstration.* Laissée en exercice (il s'agit de faire la division euclidienne de $F$ par $G$, qui a lieu dans $A[X]$ car $G$ est unitaire). □

**Lemme 3.53.** Le polynôme $\Phi_n$ est à coefficients dans $\mathbb{Z}$. De plus, il est irréductible dans $\mathbb{Z}[X]$ (il est donc irréductible dans $\mathbb{Q}[X]$).

*Démonstration.* Montrons d'abord que $\Phi_n$ est dans $\mathbb{Z}[X]$. Cela se fait par récurrence sur $n$. On a $\Phi_1 = X - 1 \in \mathbb{Z}[X]$. Soit $n \geq 2$ tel que pour tout $m < n$, $\Phi_m \in \mathbb{Z}[X]$. On a l'égalité suivante : $X^n - 1 = \Phi_n \cdot \prod_{d|n;d\neq n} \Phi_d$. Par hypohtèse de récurrence, le produit des $\Phi_d$ est dans $\mathbb{Z}[X]$, on peut appliquer le lemme précédent (avec $\mathbb{K} = \mathbb{C}$ par exemple).
Montrons maintenant que $\Phi_n$ est irréductible dans $\mathbb{Z}[X]$. Soit $P \in \mathbb{Z}[X]$ un facteur irréductible de $\Phi_n$ et soit $Q \in \mathbb{Z}[X]$ tel que $\Phi_n = PQ$.
Soit $\alpha \in \mathbb{C}$ une racine de $P$ et montrons que pour tout nombre premier $p$ ne divisant pas $n$, on a $\alpha^p$ qui est aussi racine.
On suppose, par l'absurde, que c'est faux. Soit donc $p$ premier, premier avec $n$ tel $\alpha^p$ n'est pas racine de $P$. Mais $\alpha^p$ est une racine primitive de 1 donc racine de $\Phi_n$ et donc racine de $Q$. Par conséquent $\alpha$ est

racine du polynôme $T(X) = Q(X^p)$. Comme $P$ est irréductible, c'est le polynôme minimal de $\alpha$ donc $P|T = Q(X^p)$. Modulo $p$, l'égalité $\Phi_n = PQ$ s'écrit : $\overline{\Phi_n} = \overline{PQ}$ dans $\mathbb{F}_p[X]$.
De plus $\overline{Q(X^p)} = \overline{Q}^p$ ; comme $P$ divise $Q(X^p)$, $\overline{P}$ divise $\overline{Q}^p$ dans $\mathbb{F}_p[X]$.
Par conséquent, il existe $S \in \mathbb{F}_p[X]$ qui divise $\overline{P}$ et $\overline{Q}$. Ainsi, $S^2$ divise $\overline{\Phi_n}$ donc aussi $X^n - \bar{1}$. Or la dérivée de ce dernier dans $\mathbb{F}_p[X]$ est $\bar{n}X^{n-1}$ qui est premier avec $X^n - \bar{1}$ (car $p$ ne divise pas $n$). Par conséquent, $X^n - \bar{1}$ ne peut avoir un facteur carré non constant d'où la contradiction. Autrement dit $\alpha^p$ est racine de $P$.
Maintenant pour tout entier $k$ premier avec $n$, on écrit $k = p_1^{m_1} \cdots p_r^{m_r}$ et on applique le résultat précédent plusieurs fois pour montrer que $\alpha^k$ est racine de $P$. Cela montre que $\Phi_n$ divise $P$, et $P$ étant irréductible, on conclut que $\Phi_n = P$. □

### 3.5.3 Extension radicale

Soit $a \in \mathbf{k}^*$ et soit $n \in \mathbb{N}^*$. Notons $\Gamma_n \subset \overline{\mathbf{k}}$ le groupe des racines $n$-ièmes de 1.
Dans ce paragraphe, **on suppose que $\Gamma_n \subset \mathbf{k}$.**

Considérons le corps de décomposition $\mathbb{K}$ de $X^n - a \in \mathbf{k}[X]$.

**Lemme 3.54.** Si $\alpha \in \mathbb{K}$ est une racine de $X^n - a$ alors $\mathbb{K} = \mathbf{k}(\alpha)$.

*Démonstration.* En effet, on a $\mathbf{k}(\alpha) \subset \mathbb{K}$. De plus si pour tout $\zeta \in \Gamma_n$, $\alpha\zeta$ est aussi racine de $X^n - a$. On les obtient toutes ainsi (car il y en a $n$) et elles sont toutes dans $\mathbf{k}(\alpha)$ car $\Gamma_n \subset \mathbf{k}$ d'où l'égalité $\mathbf{k}(\alpha) = \mathbb{K}$ □

Dans la suite du paragraphe, on notera $\mathbf{k}[\sqrt[n]{a}]$ le corps de décomposition de $X^n - a$.
D'après ce qui vient d'être dit, c'est une extension galoisienne de $\mathbf{k}$.

Fixons $\zeta \in \Gamma_n$ un générateur et $\alpha \in \mathbb{K}$ une racine de $X^n - a$.
Ce qu'on vient de dire entraine que pour tout $\sigma \in \mathrm{Gal}(\mathbf{k}[\sqrt[n]{a}]/\mathbf{k})$, $\sigma(\alpha) = \alpha\zeta_\sigma$ pour un certain $\zeta_\sigma \in \Gamma_n$.

**Lemme 3.55.** L'application $\mathrm{Gal}(\mathbf{k}[\sqrt[n]{a}]/\mathbf{k}) \to \Gamma_n,\ \sigma \mapsto \zeta_\sigma$ est un morphisme (injectif) de groupes.

*Démonstration.* Soient $\sigma, \sigma' \in \mathrm{Gal}(\mathbf{k}[\sqrt[n]{a}]/\mathbf{k})$. Alors

$$(\sigma' \circ \sigma)(\alpha) = \sigma'(\alpha\zeta_\sigma) = \sigma'(\alpha)\zeta_\sigma = \alpha\zeta_{\sigma'}\zeta_\sigma$$

d'où $\alpha\zeta_{\sigma'\circ\sigma} = \alpha\zeta_{\sigma'}\zeta_\sigma$, i.e. $\zeta_{\sigma'\circ\sigma} = \zeta_{\sigma'}\zeta_\sigma$ □

Comme conséquence de ce lemme, nous avons :

$$\mathrm{Gal}(\mathbf{k}[\sqrt[n]{a}]/\mathbf{k}) \simeq \Gamma_m$$

pour une certain $m$ divisant $n$ (car tout sous-groupe de $\Gamma_n$ est un tel $\Gamma_m$). Ainsi $\mathrm{Gal}(\mathbf{k}[\sqrt[n]{a}]/\mathbf{k})$ est cyclique d'ordre $m = [\mathbf{k}[\sqrt[n]{a}] : \mathbf{k}]$.

**Proposition 3.56.** En gardant les notations ci-dessus, l'extension $\mathbf{k}[\sqrt[n]{a}]/\mathbf{k}$ est galoisienne engendrée par une racine $n$-ième de $a$ et on a un isomorphisme

$$\mathrm{Gal}(\mathbf{k}[\sqrt[n]{a}]/\mathbf{k}) \to \Gamma_m,\ \sigma \mapsto \frac{\sigma(\alpha)}{\alpha}$$

où $\alpha \in \overline{\mathbf{k}}$ est une racine de $X^n - a$ fixée. De plus $m$ est le plus petit entier tel que $\alpha^m \in \mathbf{k}$.
Réciproquement, toute extension $\mathbb{K}/\mathbf{k}$ de groupe de Galois cyclique d'ordre $n$ est de la forme $\mathbf{k}[\sqrt[n]{a}]$ pour un certain $a \in \mathbf{k}$.

*Démonstration.* Concernant la première partie de cette proposition, nous avons tout démontré sauf la condition sur $m$.
Montrons d'abord que $\alpha^m \in \mathbf{k}$. Soit $\gamma = \prod_\sigma \sigma(\alpha)$ (le produit se fait sur tous les $\sigma \in \mathrm{Gal}(\mathbf{k}[\sqrt[n]{a}]/\mathbf{k})$). Alors pour pour tout $\sigma' \in \mathrm{Gal}(\mathbf{k}[\sqrt[n]{a}]/\mathbf{k})$, $\sigma'(\gamma)\prod_\gamma \sigma'(\sigma(\alpha)) = \prod_\sigma \sigma(\alpha)$ (car l'ensemble des $\sigma' \circ \sigma$ est $\mathrm{Gal}(\mathbf{k}[\sqrt[n]{a}]/\mathbf{k})$). Ainsi $\gamma$ est fixé par tous les $\sigma' \in \mathrm{Gal}(\mathbf{k}[\sqrt[n]{a}]/\mathbf{k})$, ce qui entraine $\gamma \in \mathbf{k}$.
Or $\gamma = \alpha^m \prod_\sigma \zeta_\sigma$ d'où $\alpha^m \in \mathbf{k}$.
Montrons maintenant que $m$ est le plus petit entier pour lequel $\alpha^m \in \mathbf{k}$. Soit donc $q < m$ tel $\alpha^q \in \mathbf{k}$. Soit $\sigma$ un générateur de $\mathrm{Gal}(\mathbf{k}[\sqrt[n]{a}]/\mathbf{k})$. Notons $\psi$ l'isomorphisme $\mathrm{Gal}(\mathbf{k}[\sqrt[n]{a}]/\mathbf{k}) \to \Gamma_n$. Alors

$$\psi(\sigma^q) = (\psi(\sigma))^q = (\frac{\sigma(\alpha)}{\alpha})^q = \frac{\sigma(\alpha^q)}{\alpha^q} = \frac{\alpha^q}{\alpha^q} = 1.$$

Remarquons que $\sigma(\alpha^q) = \alpha^q$ car $\alpha^q \in \mathbf{k}$ par hypothèse. Le calcul précédent montrer que $\sigma^q = \mathrm{Id}$, i.e. $\mathrm{Gal}(\mathbf{k}[\sqrt[n]{a}]/\mathbf{k})$ est d'ordre $q < m$, absurde.
Montrons maintenant la seconde partie.
Soit donc $\mathbb{K}/\mathbf{k}$ une extension dont le groupe de Galois est cyclique d'ordre $n$. Soit $\sigma$ un générateur de $\mathrm{Gal}(\mathbb{K}/\mathbf{k})$ de sorte que $\mathrm{Gal}(\mathbb{K}/\mathbf{k}) = \{\mathrm{Id}, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$ et soit $\zeta$ une racine primitive $n$-ième de l'unité. Par le 1ere lemme de 5.1, les éléments de $\mathrm{Gal}(\mathbb{K}/\mathbf{k})$ sont linéairement indépendants sur $\mathbb{K}$. Par conséquent : $\mathrm{Id} + \zeta^{-1}\sigma + \cdots + \zeta^{1-n}\sigma^{n-1} \neq 0$. Ainsi il existe $x \in \mathbb{K}$ tel que $\alpha := x + \zeta^{-1}\sigma(x) + \cdots + \zeta^{1-n}\sigma^{n-1}(x) \neq 0$. Alors $\sigma(\alpha) = \zeta\alpha$ ce qui entraine $\sigma^i(\alpha) = \zeta^i\alpha$ pour tout $i = 0, \ldots, n-1$ ; et ces $\sigma^i(\alpha)$ sont deux à deux distincts. Par le théorème principal de 5.3 (point 4), on a :

$$\mu_\alpha = \prod_{i=0}^{n-1}(X - \sigma^i(\alpha)) = \prod_{i=0}^{n-1}(X - \zeta^i\alpha) = X^n - \alpha^n.$$

En particulier $a := \alpha^n \in \mathbf{k}^*$. De plus $\mathbf{k}[\alpha] \subset \mathbb{K}$ mais comme les deux sont de dimension $n$, on a égalité. □

Le corollaire suivant nous sera utile dans la suite.

**Corollaire 3.57.** Soit $\mathbf{k}$ un corps contenant $\Gamma_n$. Soit $\mathbb{K}/\mathbf{k}$ une extension engendrée par des éléments $\alpha_1, \ldots, \alpha_r$ tel que $\alpha_i^n \in \mathbf{k}$. Alors $\mathbb{K}/\mathbf{k}$ est galoisienne de groupe de Galois abélien.

*Démonstration.* L'extension est galoisienne car c'est le corps de décomposition du polynôme $(X^n - \alpha_1)\cdots(X^n - \alpha_r)$. Considérons l'application

$$\mathrm{Gal}(\mathbb{K}/\mathbf{k}) \to \prod_{i=1}^{r}\mathrm{Gal}(\mathbf{k}(\alpha_i)/\mathbf{k}),\ \sigma \mapsto (\sigma_{|\mathbf{k}(\alpha_1)}, \ldots, \sigma_{|\mathbf{k}(\alpha_r)}).$$

Elle est bien définie car chaque extension $\mathbf{k}(\alpha_i)/\mathbf{k}$ est galoisienne. Elle est injective car les $\alpha_i$ engendrent $\mathbb{K}$ et c'est un morphisme de groupes. Ainsi $\mathrm{Gal}(\mathbb{K}/\mathbf{k})$ est un sous-groupe d'un produit de groupes cycliques, il est donc abélien. □

## 3.6 Correspondance de Galois

Dans cette section, on établit une bijection remarquable entre les sous-extensions d'une extension galoisienne et les sous-groupes distingués de son groupe de Galois.

**Notation.** Étant donné un corps $\mathbb{K}$ et $G$ un sous-groupe du groupe des automorphismes de $\mathbb{K}$, on notera $\mathbb{K}^G = \{x \in \mathbb{K} \mid \forall \sigma \in G,\ \sigma(x) = x\}$.

**Proposition 3.58** (Lemme d'Artin)**.** Soit $G$ un sous-groupe fini du groupe des automorphismes d'un corps $\mathbb{K}$. Alors $\mathbb{K}^G$ est un corps contenu dans $\mathbb{K}$ et l'extension $\mathbb{K}^G \subset \mathbb{K}$ est de degré fini et galoisienne et son groupe de Galois est $\mathrm{Gal}(\mathbb{K}/\mathbb{K}^G) = G$.

*Démonstration.* $\mathbf{k} := \mathbb{K}^G$ est un corps : laissé en exercice ; il est contenu dans $\mathbb{K}$ par définition. Soit $\alpha \in \mathbb{K}$ et posons $P = \prod_{\beta \in G\cdot\alpha} (X - \beta)$. Pour tout $\sigma \in G$, $\sigma^*(P) = P$ ce qui entraine $P \in \mathbf{k}[X]$.
Dans ce cas, on a $\mu_\alpha$ qui divise $P$ donc $[\mathbf{k}(\alpha) : \mathbf{k}] \leq \deg(P) \leq |G|$.
Ainsi l'extension $\mathbb{K}/\mathbf{k}$ est (algébrique) séparable et pour tout $\alpha \in \mathbb{K}$, $[\mathbf{k}(\alpha) : \mathbf{k}] \leq |G|$.
Choisissons $\alpha \in \mathbb{K}$ de telle sorte que $[\mathbf{k}(\alpha) : \mathbf{k}]$ soit maximal. Nous allons montrer que $\mathbb{K} = \mathbf{k}(\alpha)$.
Soit $\beta \in \mathbb{K}$. L'extension $\mathbf{k}(\alpha, \beta)/\mathbf{k}$ est séparable (car tout $\gamma \in \mathbf{k}(\alpha, \beta) \subset \mathbb{K}$ est séparable) donc il existe $\gamma \in \mathbf{k}(\alpha, \beta)$ tel que $\mathbf{k}(\alpha, \beta) = \mathbf{k}(\gamma)$. On a alors $\mathbf{k}(\alpha) \subseteq \mathbf{k}(\gamma)$ mais par maximalité du degré de $\mathbf{k}(\alpha)/\mathbf{k}$, l'inclusion est une égalité. Autrement dit, $\mathbf{k}(\alpha) = \mathbf{k}(\alpha, \beta)$ i.e. $\beta \in \mathbf{k}(\alpha)$ et on a bien $\mathbb{K} = \mathbf{k}(\alpha)$.
On a trivialement $G \subseteq \mathrm{Gal}(\mathbb{K}/\mathbf{k})$. On a donc les inégalités suivantes (la dernière provenant de ce qu'on a fait juste avant) :

$$|G| \leq |\mathrm{Gal}(\mathbb{K}/\mathbf{k})| \leq [\mathbb{K} : \mathbf{k}] \leq |G|.$$

On en déduit à la fois que $\mathbb{K}/\mathbf{k}$ est galoisienne et que $\mathrm{Gal}(\mathbb{K}/\mathbf{k}) = G$. □

**Proposition 3.59.** Soit $\mathbb{K} \supset \mathbf{k}$ une extension galoisienne finie et soit $\mathbf{k} \subset \mathbb{K}' \subset \mathbb{K}$ une sous-extension.

1. L'extension $\mathbb{K}' \subset \mathbb{K}$ est galoisienne et on a $\mathbb{K}' = \mathbb{K}^{\mathrm{Gal}(\mathbb{K}/\mathbb{K}')}$.
2. Pour tout $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbf{k})$, on a :
$$\sigma \mathrm{Gal}(\mathbb{K}/\mathbb{K}')\sigma^{-1} = \mathrm{Gal}(\mathbb{K}/\sigma(\mathbb{K}')).$$
3. On a l'équivalence :
L'extension $\mathbf{k} \subset \mathbb{K}'$ est galoisienne $\iff$ $\mathrm{Gal}(\mathbb{K}/\mathbb{K}')$ est distingué dans $\mathrm{Gal}(\mathbb{K}/\mathbf{k})$.
Dans ce cas, on a un isomorphisme :
$$\mathrm{Gal}(\mathbb{K}/\mathbf{k})/\mathrm{Gal}(\mathbb{K}/\mathbb{K}') \simeq \mathrm{Gal}(\mathbb{K}'/\mathbf{k}).$$

*Démonstration.*
1. $\mathbb{K}$ est le corps de décomposition d'un polynôme séparable $P \in \mathbf{k}[X]$. Alors c'est aussi le corps de décomposition du même polynôme $P$ vu dans $\mathbb{K}'[X]$. Ainsi $\mathbb{K}/\mathbb{K}'$ est galoisienne. Le point 5 du théorème de 5.3 entraine alors l'égalité $\mathbb{K}' = \mathbb{K}^{\mathrm{Gal}(\mathbb{K}/\mathbb{K}')}$.
2. Soit $\tau \in \mathrm{Gal}(\mathbb{K}/\mathbf{k})$. On a $\tau \in \mathrm{Gal}(\mathbb{K}/\sigma(\mathbb{K}'))$ $\iff$ $(\forall \alpha \in \mathbb{K}',\ \tau(\sigma(\alpha)))$ $\iff$ $(\forall \alpha \in \mathbb{K}',\ \sigma^{-1}\tau\sigma(\alpha) = \alpha)$ $\iff$ $\sigma^{-1}\tau\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{K}')$.
3. Remarquons déjà qu'on a bien une inclusion $\mathrm{Gal}(\mathbb{K}/\mathbb{K}') \subset \mathrm{Gal}(\mathbb{K}/\mathbf{k})$ car si $\sigma$ est automorphisme de $\mathbb{K}$ fixant les éléments de $\mathbb{K}'$ alors il fixe ceux de $\mathbf{k}$.
Supposons $\mathrm{Gal}(\mathbb{K}/\mathbb{K}')$ dinstingué dans $\mathrm{Gal}(\mathbb{K}/\mathbf{k})$. Alors par (1) et (2) :
$$\forall \sigma \in \mathrm{Gal}(\mathbb{K}/\mathbf{k}),\ \sigma(\mathbb{K}') = \mathbb{K}^{\mathrm{Gal}(\mathbb{K}/\sigma(\mathbb{K}'))} = \mathbb{K}^{\sigma\mathrm{Gal}(\mathbb{K}/\mathbb{K}')\sigma^{-1}} = \mathbb{K}^{\mathrm{Gal}(\mathbb{K}/\mathbb{K}')} = \mathbb{K}'.$$

Ainsi $\mathbb{K}'$ est normale sur $\mathbf{k}$. Elle est aussi séparable (car pour tout $\alpha \in \mathbb{K}' \subset \mathbb{K}$, $\mu_\alpha \in \mathbf{k}[X]$ est séparable car $\mathbb{K}/\mathbf{k}$ est galoisienne) et donc $\mathbb{K}'/\mathbf{k}$ est galoisienne.
Réciproquement, supposons $\mathbb{K}'/\mathbf{k}$ galoisienne. Alors pour tout $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbf{k})$, $\sigma(\mathbb{K}') = \mathbb{K}'$. Par conséquent, on a une application

$$\mathrm{Gal}(\mathbb{K}/\mathbf{k}) \to \mathrm{Gal}(\mathbb{K}', \mathbf{k}) \ ; \ \sigma \mapsto \sigma_{|\mathbb{K}'}$$

et c'est un morphisme de groupes ; son noyau est formé des $\sigma$ qui fixent les éléments de $\mathbb{K}'$, i.e. le noyau est $\mathrm{Gal}(\mathbb{K}/\mathbb{K}')$ qui est donc distingué. Pour finir, voyons que ce morphisme est surjectif (ce qui fournira, par passage au quotient, l'isomorphisme voulu). On a $[\mathbb{K}/\mathbf{k}] = [\mathbb{K} : \mathbb{K}'][\mathbb{K}' : \mathbf{k}]$ ou encore $|\mathrm{Gal}(\mathbb{K}'/\mathbf{k})| = [\mathbb{K}' : \mathbf{k}] = \dfrac{[\mathbb{K} : \mathbf{k}]}{[\mathbb{K} : \mathbb{K}']} = |\mathrm{Gal}(\mathbb{K}/\mathbf{k})/\mathrm{Gal}(\mathbb{K}/\mathbb{K}')|$ ce qui implique la surjéctivité. □

Voici en conclusion ce que les deux propositions précédentes nous disent.
On fixe une extension galoisienne finie $\mathbb{K}/\mathbf{k}$ et on note $G = \mathrm{Gal}(\mathbb{K}/k)$.
On note $\mathcal{SE}(\mathbb{K})$ l'ensemble des sous-extensions $\mathbb{K}'$, avec $\mathbf{k} \subset \mathbb{K}' \subset \mathbb{K}$ et on note $\mathcal{SG}(G)$ l'ensemble des sous-groupes de $G$. On considère les application suivantes.

$$\Phi : \begin{array}{ccc} \mathcal{SE}(\mathbb{K}) & \to & \mathcal{SG}(G) \\ \mathbb{K}' & \mapsto & \mathrm{Gal}(\mathbb{K}/\mathbb{K}') \end{array} \quad \text{et} \quad \Psi : \begin{array}{ccc} \mathcal{SG}(G) & \to & \mathcal{SE}(\mathbb{K}) \\ H & \mapsto & \mathbb{K}^H \end{array}$$

**Théorème 3.60.** Ces applications sont des bijections réciproques. Elles renversent les inclusions et elles échangent sous-extensions galoisiennes et sous-groupes distingués.

## 3.7 Groupes résolubles et résolubles par radicaux

Dans ce paragraphe, nous allons caractériser les polynômes de $\mathbb{Q}[X]$ qui sont résolubles par radicaux. Pour cela, nous avons besoin d'une notion supplémentaire.

### 3.7.1 Clôture normale (galoisienne) d'une extension

La notion de corps de décomposition d'un polynôme a un analogue concernant les extensions de corps : c'est la notion de clôture normale.

**Proposition 3.61.** Soient $\mathbb{K}/\mathbf{k}$ une extension contenue dans $\overline{\mathbf{k}}$. Alors le corps engendré par les $\sigma(\mathbb{K})$ où $\sigma$ parcourt l'ensemble des $\mathbf{k}$-automorphismes de $\overline{\mathbf{k}}$ est une extension normale de $\mathbf{k}$ contenant $\mathbb{K}$, et c'est la plus petite.

*Démonstration.* Notons $\mathbb{L}$ l'extension en question. Soit $\tau : \mathbb{L} \to \overline{\mathbf{k}}$ un morphisme. Soit $x \in \mathbb{L}$. Alors par définition, $x$ dont le numérateur et le dénominateur sont des polynômes en les $\sigma(\alpha)$ avec $\sigma \in \mathrm{Aut}_{\mathbf{k}}(\overline{\mathbf{k}})$ et $\alpha \in \mathbb{K}$. Quand on applique $\tau$ à $x$, on obtient un élément du même type donc $\tau(x) \in \mathbb{L}$. Ainsi $\mathbb{L}$ est normale.
De plus soit $\mathbb{L}'$ est une autre extension normale de $\mathbf{k}$ contenant $\mathbb{K}$. Alors pour tout $\sigma \in \mathrm{Aut}_{\mathbf{k}}(\overline{\mathbf{k}})$, $\sigma(\mathbb{K}) \subset \sigma(\mathbb{L}') \subset \mathbb{L}'$ ce qui implique l'inclusion $\mathbb{L} \subset \mathbb{L}'$. □

Le corps $\mathbb{L}$ obtenu est appelé **clôture normale** de $\mathbb{K}$ sur $\mathbf{k}$.

**Lemme 3.62.** Soit $\mathbb{K} = \mathbf{k}(\alpha_1, \ldots, \alpha_r)$ une extension séparable (finie) de $\mathbf{k}$. Alors la côture normale $\mathbb{L}$ de $\mathbb{K}$ est égale à

$$\mathbb{L} = \mathbf{k}(\bigcup_{i=1}^{r} \{\alpha' \in \overline{\mathbf{k}};\ \alpha' \text{ est conjugué à } \alpha_i\}).$$

De plus $\mathbb{L}/\mathbf{k}$ est galoisienne.

*Démonstration.* Notons $A = \{\sigma(\alpha_i) \mid i = 1, \ldots, n,\ \sigma \in \mathrm{Aut}_{\mathbf{k}}(\overline{\mathbf{k}})\}$. Alors $\mathbb{L} = \mathbf{k}(A)$. En effet, pour tout $\sigma$, $\sigma(\mathbb{K}) \subset \mathbf{k}(A)$. Et $A$ est inclus dans la réunion des $\sigma(\mathbb{K})$ avec $\sigma \in \mathrm{Aut}_{\mathbf{k}}(\overline{\mathbf{k}})$. D'autre part, $\mathbb{L}/\mathbf{k}$ est normale. Voyons qu'elle est séparable. Soit $\beta = \sigma(\alpha_i)$ pour un $\sigma \in \mathrm{Aut}_{\mathbf{k}}(\overline{\mathbf{k}})$ et $i \in \{1, \ldots, n\}$. L'élément $\alpha_i$ est séparable donc $P = \mu_{\alpha_i}$ est scindé dans $\overline{\mathbf{k}}[X]$ et on a $P(\beta) = P(\sigma(\alpha_i)) = \sigma(P(\alpha_i)) = 0$ donc $\beta$ est séparable. L'extension $\mathbb{L}/\mathbf{k}$ est donc séparable. D'autre part, le petit calcul précédent montrer que $\sigma(\alpha_i)$ est conjugué à $\alpha_i$. Réciproquement tout conjugué à un $\alpha_i$ est du type $\sigma(\alpha_i)$ avec $\sigma \in \mathrm{Aut}_{\mathbf{k}}(\overline{\mathbf{k}})$ (voir le lemme de 5.3 sur les conjugués). □

Un polynôme $P \in \mathbb{Q}[X]$ est dit résoluble par radicaux si chaque racine de $P$ peut s'exprimer par une formule ne faisant intervenir que des nombres rationnels, les opérations arithmétiques usuelles (addition, soustraction, multiplication, division) et l'extraction de racines.
Cette définition manque de précision. Voici une façon plus rigoureuse de la formuler.

**Définition 3.63.** Une extension $\mathbb{L}/\mathbb{Q}$ (avec $\mathbb{L} \subset \mathbb{C}$) est dite par radicaux s'il existe une suite d'extensions

$$\mathbb{Q} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_r = \mathbb{L}$$

telle que pour tout $i \geq 1$, il existe $\alpha_i \in \mathbb{K}_i$ et $n_i \in \mathbb{N}^*$ tels que $\mathbb{K}_i = \mathbb{K}_{i-1}(\alpha_i)$ et $\alpha_i^{n_i} \in \mathbb{K}_{i-1}$.

**Définition 3.64.** Soit $P \in \mathbb{Q}[X]$. On dit qu'il est résoluble par radicaux s'il existe une extension $\mathbb{L}/\mathbb{Q}$ par radicaux telle que $P$ est scindé dans $\mathbb{L}[X]$.

**Définition 3.65.** Un groupe fini $G$ est dit résoluble s'il admet une suite décroissante

$$G = G_0 \supset G_1 \supset \cdots \supset G_r = \{1\}$$

formée de sous-groupes de $G$ tels que pour tout $i = 0, \ldots, r-1$, $G_{i+1}$ est distingué dans $G_i$ et $G_i/G_{i+1}$ est abélien.

**Lemme 3.66.** Soit $H$ un sous-groupe d'un goupe fini $G$.

1. Si $G$ est résoluble alors $H$ l'est.
2. Supposons $H$ distingué dans $G$. Alors : $G$ est résoluble si et s. si (H et G/H sont résolubles).

*Démonstration.* en exercice □

**Lemme 3.67.** Soit $G$ un groupe fini résoluble alors il existe une chaine

$$G = G_0 \supset G_1 \supset \cdots \supset G_r = \{1\}$$

formée de sous-groupes de $G$ tels que pour tout $i = 0, \ldots, r-1$, $G_{i+1}$ est distingué dans $G_i$ et $G_i/G_{i+1}$ est cyclique d'ordre premier.

*Démonstration.* Soit $\{1\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_r = G$ une chaîne comme dans la définition d'un groupe résoluble. On suppose que cette chaîne est la plus longue des chaînes de ce type (c'est possible puisque $G$ est fini).
Supposons par l'absurde qu'un facteur $F_i := G_{i+1}/G_i$ n'est pas un groupe cyclique d'ordre premier. Alors $F_i$ possède un sous-groupe propre et par suite $G$ possède un sous-groupe $H$ tel que $G_i \subseteq H \subseteq G_{i+1}$. $H$ est distingué dans $G_{i+1}$, car si $x \in G_{i+1}$ et $y \in H$, alors $\overline{x}^{-1}\overline{yx} = \overline{y}$ ($F_i$ est abélien). Il en résulte $x^{-1}yxy^{-1} \in G_i \subseteq H$ et $x^{-1}yx = \left(x^{-1}yxy^{-1}\right) y \in H$.
D'un autre côté, $H/G_i$ est abélien (sous-groupe de $F_i$) et $G_{i+1}/G$ est abélien car nous avons $G_{i+1}/H \simeq (G_{i+1}/G_i)\,/\,(H/G_i)$ et $(G_{i+1}/G_i)\,/\,(H/G_i)$ est abélien car c'est un quotient du groupe abélien $F_i$. Ainsi, on peut insérer $H$ entre $G_i$ et $G_{i+1}$ et obtenir une chaîne plus longue que celle du début. Absurde. □

Une dernière remarque avant le théorème.

**Remarque 3.68.** Pour tout polynôme $P \in \mathbb{Q}[X]$, l'extension $\mathbb{K}_P/\mathbb{Q}$ est galoisienne ; ou $\mathbb{K}_P$ désigne le corps de décomposition de $P$.

*Démonstration.* Écrivons $P = P_1^{m_1} \cdots P_e^{m_e}$ sous forme de produit de facteurs irréductibles dans $\mathbb{Q}[X]$. Soit $Q = P_1 \cdots P_e$. Alors $\mathbb{K}_P = \mathbb{K}_Q$. Chaque $P_i$ est séparable (car $\mathbb{Q}$ est parfait car de caractéristique 0). De plus les $P_i$ sont premiers entre eux deux à deux donc n'ont pas de racine commune dans $\mathbb{C}$. Ainsi $Q$ est séparable. Par suite $\mathbb{K}_Q/\mathbb{Q}$ est galoisienne. □

**Théorème 3.69.** Soit $P \in \mathbb{Q}[X]$. Alors $P$ est résoluble par radicaux si et s. si $\mathrm{Gal}(P)$ est résoluble.

*Démonstration.* Supposons $P$ résoluble par radicaux.
Notons $\mathbb{K}_P$ le corps de décomposition de $P$. Par hypothèse il existe une suite de corps

$$\mathbb{Q} = \mathbb{K}_1 \subset \mathbb{K}_2 \subset \cdots \subset \mathbb{K}_r$$

telle que pour $i = 2, \ldots, r$, il existe $\alpha_i \in \mathbb{K}_i$ et $n_i \in \mathbb{N}^*$ tels que $\mathbb{K}_i = \mathbb{K}_{i-1}(\alpha_i)$ et $\alpha_i^{n_i} \in \mathbb{K}_{i-1}$ et telle que $\mathbb{K}_P \subseteq \mathbb{K}_r$.
Soit $\mathbb{L}_0 = \mathbb{Q}$.
On pose $n = \mathrm{ppcm}\{\mathrm{n}_1, \ldots, \mathrm{n}_\mathrm{r}\}$ et $\mathbb{L}_1 = \mathbb{Q}_n$ le corps de décomposition de $X^n - 1$, et on définit $\alpha_1$ comme étant une racine primitive de $X^n - 1$.
Ensuite pour $i = 2, \ldots, r$, on définit $\mathbb{L}_i = \mathbb{L}_{i-1}(\{\alpha' \in \mathbb{C}\ ;\ \alpha' \text{ est conjugué de } \alpha_i\})$. Ainsi chaque $\mathbb{L}_i/\mathbb{Q}$ est galoisienne (on applique le lemme précédent). D'autre part chaque extension $\mathbb{L}_i/\mathbb{L}_{i-1}$ est galoisienne (par la correspondance de Galois) et de plus si $\alpha$ est un conjugué de $\alpha_i$ alors il existe $\sigma \in \mathrm{Aut}_{\mathbf{k}}(\overline{\mathbf{k}})$ tel que $\sigma(\alpha_i) = \alpha$. Par conséquent $\alpha^{n_i} = \sigma(\alpha_i^{n_i}) \in \sigma(\mathbb{K}_{i-1}) \subset \mathbb{L}_{i-1}$. On peut alors appliquer le corollaire de 5.5.3 et dire que $\mathrm{Gal}(\mathbb{L}_i/\mathbb{L}_{i-1})$ est abélien.
Noton alors $G_i = \mathrm{Gal}(\mathbb{L}_r/\mathbb{L}_i)$ pour $i = 0, \ldots, r$. On a donc

$$\mathrm{Gal}(\mathbb{L}_r/\mathbb{Q}) = G_0 \supset G_1 \supset \cdots \supset G_r = \mathrm{Gal}(\mathbb{L}_r/\mathbb{L}_r) = \{\mathrm{Id}\}.$$

Si on considère les extensions suivantes

$$\mathbb{Q} = \mathbb{L}_0 \subset \mathbb{L}_i \subset \mathbb{L}_r,$$

alors la correspondance Galois nous dit que $G_i = \mathrm{Gal}(\mathbb{L}_r/\mathbb{L}_i)$ est distingué dans $G_0 = \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ ce qui entraine que $G_i$ est un sous-groupe distingué de $G_{i-1}$ et on a

$$G_{i-1}/G_i \simeq \mathrm{Gal}(\mathbb{L}_i/\mathbb{L}_{i-1}).$$

Ainsi le quotient $G_{i-1}/G_i$ est abélien pour tout $i$. Par conséquent, le groupe $G_0$ est résoluble. De plus, on a $\mathbb{Q} \subset \mathbb{K}_P \subset \mathbb{L}_r$ d'où l'isomorphisme suivant :

$$\mathrm{Gal}(P) = \mathrm{Gal}(\mathbb{K}_P/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{L}_r/\mathbb{Q})/\mathrm{Gal}(\mathbb{L}_r/\mathbb{K}_p) = G_0/\mathrm{Gal}(\mathbb{L}_r, \mathbb{K}_P)$$

Autrement dit, $\mathrm{Gal}(P)$ est un quotient de $G_0$. Par un lemme précédent, cela implique que $\mathrm{Gal}(P)$ est résoluble.
Réciproquement, supposons que $\mathrm{Gal}(P)$ soit résoluble et montrons que $\mathbb{K}_P$ est inclus dans une extension par radicaux de $\mathbb{Q}$.
Notons $\mathbb{K}_P$ le corps de décomposition de $P$. Notons $N = [\mathbb{K}_P : \mathbb{Q}]$. On pose alors $\mathbb{K}' = \mathbb{K}(e^{2i\pi/N})$ et on note comme d'habitude $\mathbb{Q}_N = \mathbb{Q}(e^{2i\pi/N})$.
L'extension $\mathbb{K}'/\mathbb{Q}$ est galoisienne (car $\mathbb{K}'$ est le corps de décomposition de $(X^N - 1)P$) et $\mathbb{K}_P/\mathbb{Q}$ est aussi galoisienne (comme corps de décomposition de $P$). Par la correspondance de Galois,

$$\mathrm{Gal}(\mathbb{K}'/\mathbb{K}_p) \triangleleft \mathrm{Gal}(\mathbb{K}'/\mathbb{Q}) \text{ et } \mathrm{Gal}(\mathbb{K}'/\mathbb{Q})/\mathrm{Gal}(\mathbb{K}'/\mathbb{K}_P) \simeq \mathrm{Gal}(\mathbb{K}_P/\mathbb{Q}).$$

Or $\mathrm{Gal}(\mathbb{K}'/\mathbb{K}_P)$ est abélien (voir (1) de la prop. de 5.5.2) donc est résoluble ; de plus $\mathrm{Gal}(\mathbb{K}_P/\mathbb{Q}) = \mathrm{Gal}(P)$ est résoluble donc par le lemme ci-dessus $\mathrm{Gal}(\mathbb{K}'/\mathbb{Q})$ est résoluble. Par conséquent, son sous-groupe $G := \mathrm{Gal}(\mathbb{K}'/\mathbb{Q}_N)$ est aussi résoluble.
Nous allons donc montrer que l'extension $\mathbb{Q}_N \subset \mathbb{K}'$ est par radicaux (et comme $\mathbb{Q} \subset \mathbb{Q}_N$ l'est, çela entrainera que $\mathbb{Q} \subset \mathbb{K}'$ l'est aussi et on aura $\mathbb{K}_P \subset \mathbb{K}'$ ce qui conclura la démonstration).
Remarquons qu'on a : $[\mathbb{K}' : \mathbb{Q}_N] \leq [\mathbb{K}_P : \mathbb{Q}] = N$. En effet (par le théorème de l'élément primitif) on peut écrire $\mathbb{K}_P = \mathbb{Q}(\alpha)$. Notons $f \in \mathbb{Q}[X]$ son polynôme minimal. Alors $\deg(f) = N$. On a alors $\mathbb{K}' = \mathbb{Q}_N(\alpha)$ et si on note $g \in \mathbb{Q}_N[X]$ le polynôme minimal de $\alpha$, on aura $g|f$. Mais $\deg(g) = [\mathbb{K}' : \mathbb{Q}_N]$ et l'inégalité annoncée est vraie.
Par conséquent, $\mathbb{Q}_N$ contient toutes les racines de l'unité d'ordre $[\mathbb{K}' : \mathbb{Q}_N]!$.
Le groupe $G$ est résoluble donc on a une suite de sous-groupes

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_r = \{\mathrm{Id}\}$$

où les quotients $G_{i-1}/G_i$ sont cycliques (voir lemme ci-dessus). Par la correspondance de Galois, on obtient une suite d'extensions

$$\mathbb{Q}_N = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \cdots \subset \mathbb{K}_r = \mathbb{K}'$$

avec $\mathrm{Gal}(\mathbb{K}_i/\mathbb{K}_{i-1})$ cyclique dont on note l'ordre $n_i = [\mathbb{K}_i : \mathbb{K}_{i-1}]$. (Ces groupes sont bien cycliques ; en effet, on $\mathbb{K}_{i-1} \subset \mathbb{K}_i \subset \mathbb{K}'$ donc $G_{i-1}/G_i = \mathrm{Gal}(\mathbb{K}'/\mathbb{K}_{i-1})/\mathrm{Gal}(\mathbb{K}'/\mathbb{K}_i) \simeq \mathrm{Gal}(\mathbb{K}_i/\mathbb{K}_{i-1})$ et ce groupe est cyclique).
On a $n_i = [\mathbb{K}_i : \mathbb{K}_{i-1}]|[\mathbb{K}' : \mathbb{Q}_N]!$ donc $\mathbb{K}_{i-1}$ contient toutes les racines $n_i$-ièmes de 1 donc (par la prop. de 5.5.3) l'extension $\mathbb{K}_{i-1} \subset \mathbb{K}_i$ est radicale, i.e. de la forme $\mathbb{K}_= \sqrt[n_i]{a}$. L'extension $\mathbb{Q}_N \subset \mathbb{K}'$ est donc bien par radicaux. □

Terminons ce que nous avons commencé dans le paragraphe 5.4. Dans ce paragraphe, nous avons exhibé un polynôme de degré 5 dont le groupe de Galois est $S_5$. La proposition suivante permet alors de conclure que le polynôme en question n'est pas résoluble par radicaux.

**Proposition 3.70.** Lorsque $n \geq 5$, $S_n$ n'est pas résoluble.

*Démonstration.* Si $S_n$ était résoluble alors son sous-groupe $A_n$ le serait. Il suffit donc de montrer que $A_n$ n'est pas résoluble ; en particulier montrons que $A_n$ ne possède aucun quotient abélien [2].
Montrons, pour commencer, que $A_n$ est engendré par les 3-cycles. Il suffit de voir que le produit de deux transpositions $\tau = (ij)(kl)$ est un produit de 3-cycles. Si $\{i,j\} = \{k,l\}$ alors $\tau = \mathrm{Id}$. Si $\mathrm{card}(\{\mathrm{i},\mathrm{j}\} \cap \{\mathrm{k},\mathrm{l}\}) = 1$, par exemple si $j = k$, alors $\tau = (ijl)$. Enfin si $\{i,j\} \cap \{k,l\} = \emptyset$ alors $\tau = (ijk)(jkl)$.
Notons $D(A_n)$ le sous-groupe de $A_n$ engendré par les commutateurs $xyx^{-1}y^{-1}$ avec $x, y \in A_n$. On va montrer que $A_n = D(A_n)$. Pour cela, il suffit de montrer que tout 3-cycle est dans $D(A_n)$.
On a $(ijk) = (ij)(jk) = (ij)(ik)(ij)^{-1}(ik)^{-1}$ ce qui montre que $(ijk)$ est un commutateurs d'éléments de $S_n$. Voyons qu'on peut l'écrire comme commutateurs d'éléments de $A_n$. Comme $n \geq 5$, on peut trouver $l \neq m$ distincts de $i, j, k$. Alors (lm) commute avec $(ij)$ et $(ik)$ donc si on pose $\tau = (ij)(lm)$ et $\sigma = (ik)(lm)$ alors $\tau\sigma\tau^{-1}\sigma^{-1} = (ijk)$ et $(ijk)$ est bien dans $D(A_n)$.
Maintenant, supposons par l'absurde que $A_n$ possède un quotient abélien, i.e. il existe $H$ sous-groupe distingué propre de $A_n$ tel que $A_n/H$ est abélien. Alors pour $x, y \in A_n$, la classe de $xyx^{-1}y^{-1}$ dans ce quotient est alors triviale, i.e. $xyx^{-1}y^{-1} \in H$. Mais alors $D(A_n) \subset H$ et donc $A_n \subset H$ ce qui est absurde. □

# 4 Introduction à la géométrie algébrique : point de vue constructif

## 4.1 Noethérianité

**Définition 4.1.** Dans un anneau $A$, un idéal $I$ est dit de type fini s'il admet un système fini de générateurs.
Un anneau $A$ est dit noethérien si tout idéal de $A$ est de type fini.

En particulier tout anneau principal est noethérien ; ce qui est le cas de $\mathbf{k}[X]$ pour un corps $\mathbf{k}$ quelconque.

**Proposition 4.2.** Soit $A$ un anneau. Alors les conditions suivantes sont équivalentes.

1. $A$ est noethérien.
2. Toute suite croissante d'idéaux est stationnaire.
3. Toute famille non vide d'idéaux admet au moins un élément maximal pour l'inclusion (i.e. la famille contient un idéal qui n'est strictement inclus dans aucun autre).

*Démonstration.* (1) ⇒ (2) : soit $I_1 \subset I_2 \subset \cdots \subset I_k \subset \cdots$ une suite d'idéaux de $A$.
Soit alors $I = \sum_k I_k$ la somme des idéaux $I_k$. Alors $I$ est un idéal et par hypothèse, il admet un système fini de générateurs $f_1, \ldots, f_r$. Chaque $f_k$ est une somme finie d'éléments des $I_j$ donc il existe $m_k \in \mathbb{N}$ tel que $f_k \in I_{m_k}$.
Soit $m = \max\{m_1, \ldots, m_r\}$. Soit $k \geq m+1$ alors $I_k \subset I$ donc pour tout $f \in I_k$, $f$ est une combinaison des $f_j$ et $f$ est donc dans $I_m$. Ainsi $I_k \subset I_m$, autrement dit $I_k = I_m$.
(2) ⇒ (3) : Soit $F$ une famille non vide d'idéaux. Supposons par contraposée que cette famille n'a aucun élément maximal, i.e. tout élément de $F$ est inclus strictement dans un autre. Alors cela produit une chaine strictement croissante d'idéaux ce qui montre que (2) est faux.
(3) ⇒ (2) : Soit $I$ un idéal de $A$. Soit alors $F = \{J \subseteq I \mid J \text{ idéal de type fini}\}$. Cet ensemble est non vide car $\{0\} \in F$. Soit $I'$ un élément maximal de $F$. Si $I$ n'est pas de type fini alors il existe $x \in I \setminus I'$. Alors l'idéal $I' + \langle x \rangle$ est dans $F$ et contient strictement $I'$ ce qui contredit la maximalité de ce dernier. □

2. Il y a un résultat plus fort qui dit que $A_n$ est simple, i.e. ne possède aucun sous-groupe distingué

**Exemple** d'anneau non noethérien : $A = \mathbf{k}[X_i;\ i \in \mathbb{N}]$. Dans cet annean, si on pose $I_j = \langle X_0, \ldots, X_j \rangle$ alors les $I_j$ forment une suite strictement croissante.

Nous allons maintenant démontrer le

**Théorème 4.3** (Théorème de la base de Hilbert)**.** Soit $A$ un anneau noethérien alors $A[X]$ l'est également.

**Corollaire 4.4.**

1. Si $A$ est anneau noethérien alors $A[X_1, \ldots, X_n]$ est noethérien.
2. Si $\mathbf{k}$ désigne un corps alors l'anneau $\mathbf{k}[X_1, \ldots, X_n]$ est noethérien

*Démonstration.* Le (1) se fait par récurrence. Et le (2) provient du fait que $\mathbf{k}[X_1]$ est principal donc noethérien. □

Le point (2) de ce corollaire sera redémontrer à l'aide des bases de Gröbner.
Afin de démontrer le théorème, nous utiliserons le lemme suivant.

**Lemme 4.5.** Soit $I$ un idéal de $A[X]$. Pour $k \in \mathbb{N}$, on note $L_k(I)$ l'ensemble des coefficients dominants des polynômes de $I$ dont le degré est $k$, auquel on adjoint 0. Alors

1. Chaque $L_k(I)$ est un idéal de $A$.
2. Pour tout $k \in \mathbb{N}$, $L_k(I) \subseteq L_{k+1}(I)$.
3. Si $I' \subset A[X]$ est un idéal tel que $I \subseteq I'$ et $L_k(I) = L_k(I')$ pour tout $k \in \mathbb{N}$, alors $I = I'$.

*Démonstration (du lemme).*

1. Soient $a_1, a_2 \in L_k(I)$ les coefficients dominants de $P_1$ et $P_2$ et soit $\alpha \in A$. Si $\alpha a_1 + a_2 \neq 0$ alors c'est le coefficient dominant de $\alpha P_1 + P_2$ (qui est de degré $k$) donc appartient à $L_k(I)$ ; sinon $\alpha a_1 + a_2 = 0 \in L_k(I)$ aussi.
2. Si $a \in L_k(I)$ est le coefficient dominant de $P$ alors $XP$ a le même coefficient dominant et donc $a \in L_{k+1}(I)$.
3. Il suffit de montrer que $I' \subseteq I$. Soit $g = \sum_{i=0}^{r} a_i X^i \in I'$ de degré $r$. Alors $a_r \in L_r(I') = L_r(I)$. Donc il existe $f_r \in I$ de degré $r$ ayant $a_r$ comme coefficient dominant. Par conséquent $g - f_r \in I'$ et est de degré $\leq r - 1$. On réitère le procédé et on obtient finalement $g = f_0 + \cdots + f_r \in I$.

□

On est en mesure de démontrer le théorème.

*Démonstration (du théorème).* Soit $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ une suite croissante d'idéaux de $A[X]$.
Soit $F = \{L_i(I_j) \mid i, j \in \mathbb{N}\}$, c'est une famille d'idéaux de $A$.
Pour $i$ fixé, la suite des $L_i(I_j)$ est croissante et pour $j$ fixé également.
Montrons qu'il existe $j' \in \mathbb{N}$ tel que pour tout $j \geq j'$, $I_j = I_{j'}$. Pour ça, nous allons montrer que pour tout $i \in \mathbb{N}$, $L_i(I_j) = L_i(I_{j'})$ ce qui conclura par le lemme.
Comme $A$ est noethérien, $F$ admet un élément maximal $L_p(I_q)$.
Par conséquent pour tout $i \geq p$ et $j \geq q$, $L_i(I_j) = L_p(I_q)$.
D'autre part, toujours par noethérianité de $A$ : pour $i \in \{1, \ldots, p-1\}$ fixé, la suite $(L_i(I_j))_{j \in \mathbb{N}}$ est stationnaire donc il existe $j_i \in \mathbb{N}$ tel que pour $j \geq j_i$, $L_i(I_j) = L_i(I_{j_i})$.

On pose alors $j' = \max\{j_0, \ldots, j_{p-1}, q\}$.
Soit alors $j \geq j'$ et montrons que pour tout $i \in \mathbb{N}$, $L_i(I_j) = L_i(I_{j'})$. Si $i \in \{1, \ldots, p-1\}$ alors $L_i(I_j) = L_i(I_{j_i})$ et $L_i(I_{j_i}) = L_i(I_{j'})$ (car $j' \geq j_j$) ; et si $i \geq p$ alors $L_i(I_j) = L_p(I_q)$ et $L_i(I_{j'}) = L_p(I_q)$ (car $j' \geq q$). □

## 4.2 Ensembles algébriques affines

Dans toute cette section, sauf mention contraire, $\mathbf{k}$ désignera un corps (commutatif).
On adoptera la notation suivante : $\mathbf{k}[\underline{X}] = \mathbf{k}[X_1, \ldots, X_n]$.

**Définition 4.6.** Soit $n \in \mathbb{N}^*$. On appelle $\mathbf{k}^n$ l'espace affine de dimension $n$ sur $\mathbf{k}$, on le note parfois $\mathbb{A}_n(\mathbf{k})$.
Étant donné une partie $S \subset \mathbf{k}[X_1, \ldots, X_n]$, on définit

$$V(S) = \{(a_1, \ldots, a_n) \in \mathbf{k}^n \mid \forall P \in S,\ P(a_1, \ldots, a_n) = 0\}.$$

C'est le lieu des zéros défini par $S$. Un tel ensemble $V(S)$ est appelé ensemble algébrique affine (qu'on abrégera par EAA). On parle aussi de variété algébrique affine (d'où le V).

**Proposition 4.7.**

1. Si $S \subset T \subset \mathbf{k}[\underline{X}]$ alors $V(T) \subset V(S)$ (l'application $V$ est décroissante).
2. $V(\mathbf{k}[\underline{X}]) = \emptyset$ et $V(\emptyset) = \mathbf{k}^n$.
3. Pour $S \subset \mathbf{k}[\underline{X}]$, $V(S) = V(\langle S \rangle)$ ($\langle S \rangle$ désigne l'idéal engendré).
4. Soit $I \subset \mathbf{k}[\underline{X}]$ un idéal et $f_1, \ldots, f_r$ des générateurs alors $V(I) = V(\{f_1, \ldots, f_r\})$.

*Démonstration.* (1) et (2) sont faciles et laissés en exercices. Le (4) est une application directe de (3). Montrons (3). Comme $S \subset \langle S \rangle$, $V(\langle S \rangle) \subset V(S)$. Soit $a \in V(S)$. Soit $f \in \langle S \rangle$ alors $f$ s'écrit comme combinaison finie $f = \sum g_i s_i$ avec $g_i \in \mathbf{k}[\underline{X}]$ et $s_i \in S$. Alors $f(a)$ est clairement nul d'où $a \in V(\langle S \rangle)$. □

**Exemple 4.8.**

1. Dans $\mathbb{R}$, $V(X^2 + 1) = \emptyset$ ; dans $\mathbb{C}$, $V(X^2 + 1) = \{i, -i\}$.
2. Dans $\mathbb{R}^2$, $V(X^2 + Y^2 - 25)$ est le cercle de centre 0 et rayon 5.
3. Tout sous-espace vectoriel de $\mathbf{k}^n$ est un EAA.
4. Pour $a = (a_1, \ldots, a_n) \in \mathbf{k}^n$, $V(\{X_1 - a_1, \ldots, X_n - a_n\}) = \{a\}$.

**Proposition 4.9.**

1. Soit $(I_j)_{j \in J}$ une famille d'idéaux de $\mathbf{k}[\underline{X}]$ (finie ou non) alors

$$V\Big(\bigcup_{j \in J} I_j\Big) = V\Big(\sum_{j \in J} I_j\Big) = \bigcap_{j \in J} V(I_j).$$

2. Soient $I, J \subset \mathbf{k}[\underline{X}]$ deux idéaux alors

$$V(I \cap J) = V(I) \cup V(J).$$

*Démonstration.*

1. Pour tout $j_0$, $I_{j_0} \subset \sum_j I_j$ donc $V(\sum I_j) \subset V(I_{j_0})$ d'où $V(\sum I_j) \subset \cap V(I_j)$.
   Montrons $\cap V(I_j) \subset V(\cup I_j)$ : soit $a \in \cap V(I_j)$. Soit $f \in \cup I_j$. Alors $f \in I_j$ pour un certain $j$ d'où $f(a) = 0$.
   Montrons $V(\cup I_j) \subset V(\sum I_j)$ : soit $a \in V(\cup I_j)$. Soit $f \in \sum I_j$. Alors $f$ s'écrit comme une somme finie $f = \sum f_j$ avec $f_j \in I_j$. Alors $f(a) = \sum f_j(a) = 0$.
2. On a $I \cap J \subset I$ d'où $V(I) \subset V(I \cap J)$. De même, $V(J) \subset V(I \cap J)$ d'où $V(I) \cup V(J) \subset V(I \cap J)$. Voyons l'inclusion inverse. Soit $a \in V(I \cap J)$ et supposons que $a \notin V(J)$. Soit alors $f \in V(I)$. Il existe $g \in J$ tel que $g(a) \neq 0$. On a $fg \in I \cap J$ d'où $(fg)(a) = f(a)g(a) = 0$ or $g(a) \neq 0$ donc $f(a) = 0$. Ainsi $a \in V(I)$.

□

**Exemple 4.10.** Regardons quels sont les EAA en dimension 1. Soit $I$ un idéal de $\mathbf{k}[X]$. Ce dernier étant principal, on a $V(I) = V(f)$ pour un certain $f \in I$. Si $f = 0$ alors $V(f) = \mathbf{k}$. Si $f \neq 0$ alors $V(f)$ est de cardinal fini (en effet, un polynôme non constant possède un nombre fini de racines et si $f$ est constant alors $V(f)$ est vide). Ainsi, tout EAA de $\mathbf{k}$ est ou bien égal à $\mathbf{k}$ ou bien vide ou bien un nombre fini de points.
Réciproquement, toute partie finie $A \subset \mathbf{k}$ est un EAA car $A$ est l'union des $V(X - a)$ avec $a \in A$ et le (2) de la proposition nous dit qu'une union finie de EAA est un EAA.
En conclusion, si $A$ est une partie de $\mathbf{k}$ alors : $A$ est une EAA si et s. si $A$ est vide ou bien égal à $\mathbf{k}$ ou bien est de cardinal fini.

**Remarque 4.11.** Dans le point (2) de la proposition, l'égalité serait fausse (en général) si on prenait une union infinie. En effet, prenons l'exemple d'un ensemble $A \subset \mathbf{k}$ infini tel que $A \neq \mathbf{k}$.
Si (2) était vrai avec une union infinie alors on aurait : $A = \bigcup_{a \in A} V(X - a) = V\big(\bigcap_{a \in A} \langle (X - a) \rangle\big)$ mais ceci contredirait ce qu'on vient de voir car $A$ ne peut pas être un EAA.
Une autre façon de formuler ceci est de dire qu'une union quelconque d'EAA n'est pas nécessairement un EAA.

**Topologie de Zariski**.
Notons $\mathcal{E}$ l'ensemble des $V(I)$ où $I \subset \mathbf{k}[\underline{X}]$ est un idéal. La proposition précédente implique :
- $\mathcal{E}$ contient $\emptyset$ et $\mathbf{k}$.
- $\mathcal{E}$ est stable par réunion finie.
- $\mathcal{E}$ est stable par intersection quelconque.

Cela entraine que les éléments de $\mathcal{E}$ sont les fermés d'une certaine topologie qu'on appelle la topologie de Zariski de $\mathbf{k}^n$.
Autrement dit, si on note $T = \{\mathbf{k}^n \smallsetminus V \mid V \in \mathcal{E}\}$ alors $T$ est une topologie sur $\mathbf{k}^n$.

**Exercice 4.12.** Supposons que $\mathbf{k} = \mathbb{R}$ ou $\mathbf{k} = \mathbb{C}$. Alors $\mathbf{k}^n$ peut-être muni de la topologie euclidienne (qui est donnée par n'importe quelle norme ; sachant que toutes les normes sont équivalentes) et il est intéressant de comparer la topologie euclidienne et la topologie de Zariski. On peut montrer que

1. Si $U$ est un ouvert de Zariski alors $U$ est un ouvert dense dans $\mathbf{k}^n$ pour la topologie euclidienne.
2. Soient $U_1, \ldots, U_r$ un nombre fini d'ouverts de Zariski non-vides. Alors $U_1 \cap \cdots \cap U_r \neq \emptyset$.

Nous allons maintenant introduire une nouvelle application qui est un peu "inverse" de l'application $V$.

**Définition 4.13.** Soit $E \subset \mathbf{k}^n$ un sous-ensemble. On définit

$$I(E) = \{f \in \mathbf{k}[X_1, \ldots, X_n] \mid \forall a = (a_1, \ldots, a_n) \in E,\ f(a) = 0\}.$$

On l'appelle l'idéal défini par $E$.

*Démonstration ($I(E)$ est un idéal).* En effet, le polynôme nul appartient à $I(E)$ qui est donc non vide. De plus si $f, g \in I(E)$ et $q \in \mathbf{k}[\underline{X}]$ alors pour $a \in E$, $(qf + g)(a) = q(a)f(a) + g(a) = 0$ ce qui entraine $qf + g \in I(E)$. □

La notion de radical d'un idéal va jouer un rôle importante dans la suite. Voici la définition.

**Définition 4.14.** Soit $I \subset \mathbf{k}[\underline{X}]$. On pose

$$\sqrt{I} = \{f \in \mathbf{k}[\underline{X}] \mid \exists m \in \mathbb{N}^*,\ f^m \in I\}.$$

Cet ensemble est un idéal appelé le radical de $I$.
Un idéal $I$ est qualifié de radical si on a $I = \sqrt{I}$ (notons qu'on a toujours $I \subset \sqrt{I}$).

*Démonstration ($\sqrt{I}$ est un idéal).* $\sqrt{I}$ contient $I$ donc il est non vide. Soit $f \in \sqrt{I}$ et $q \in \mathbf{k}[\underline{X}]$. Par hypothèse, $f^m \in I$ pour un certain entier $m \geq 1$. Par conséquent $(qf)^m = q^m f^m \in I$.
Soient $f, g \in \sqrt{I}$. On a l'existence de deux entiers positifs non nuls $m, p$ tels que $f^m$ et $g^p$ soient dans $I$. Voyons que $(f+g)^{m+p} \in I$. On a : $(f+g)^{m+p} = \sum_{i,j \in \mathbb{N}, i+j=m+p} \binom{i}{m+p} f^i g^j$. Dans chaque terme de cette somme on a nécessairement $i \geq m$ ou $j \geq p$, donc chaque terme est dans $I$ et donc $(f+g)^{m+p} \in I$. □

**Proposition 4.15.**

1. $I(\emptyset) = \mathbf{k}[X]$ et $I(\mathbf{k}^n) = \{0\}$.
2. Si $E_1 \subset E_2 \subset \mathbf{k}^n$ alors $I(E_2) \subset I(E_1)$.
3. Soit $V \subset \mathbf{k}^n$ un EAA. Alors $V(I(V)) = V$.
4. Soit $E \subset \mathbf{k}^n$. Alors $I(E)$ est radical.
5. Soit $I \subset \mathbf{k}[\underline{X}]$ un idéal alors : $I \subset \sqrt{I} \subset I(V(I))$.
6. Soit $I \subset \mathbf{k}[\underline{X}]$ un idéal alors : $V(I) = V(\sqrt{I})$.
7. Soit $E \subset \mathbf{k}^n$ un ensemble. Alors $V(I(E))$ est égal à l'adhérence de Zariski de $E$.

*Démonstration.* On laisse (1) et (2) en exercice.
Montrons (3). On a trivialement $V \subset V(I(V))$ (tout point de $V$ est annulé par tout polynôme qui s'annule sur $V$). Comme $V$ est un EAA, il estiste un idéal $J$ tel que $V = V(J)$. On a alors trivialement $J \subset I(V)$. D'où par (2), $V(I(V)) \subset V(J) = V$.
Voyons (4). Soit $f \in \sqrt{I(E)}$. Alors $f^m \in I(E)$ pour une certain entier $m \geq 1$. Ainsi pour tout $a \in E$, $f^m(a) = 0$ donc $f(a) = 0$ et donc $f \in I(E)$. D'où l'inclusion $\sqrt{I(E))} \subset I(E)$. L'inclusion inverse est vrai pour n'importe quel idéal ce qui donne l'égalité.
Voyons (5). La première inclusion est triviale. Notons $J = I(V(I))$. On a trivialement $I \subset J$. Par conséquent $\sqrt{I} \subset \sqrt{J}$ mais $J$ étant radical, on obtient $\sqrt{I} \subset J$.
Voyons (6). On applique $V$ dans (5) ce qui donne : $V(I) \supset V(\sqrt{I}) \supset V(I(V(I))) = V(I)$ (par le (3)).
Voyons (7). On a trivialement $E \subset V(I(E))$. Ainsi $V(I(E))$ est un fermé qui contient $E$. Montrons que

c'est le plus petit. Soit $V$ un autre fermé de Zariski contenant $E$. Soit $J$ un idéal tel que $V = V(J)$. On a par hypothèse, $E \subset V = V(J)$. On applique $I$ et on obtient $I(V(J)) \subset I(E)$. On applique alors $V$ et on utilise (3) et cela donne : $V(I(E)) \subset V(I(V(J))) = V(J) = V$. Ainsi $V(I(E))$ est le plus petit fermé de Zariski contenant $E$. □

**Exemple 4.16.** Si $I = \langle X^2 + 1 \rangle \subset \mathbb{R}[X]$ alors

$$I(V(I)) = I(\emptyset) = \mathbb{R}[X] \neq I.$$

Si $I = \langle (X-1)^2 \rangle \subset \mathbb{R}[X]$ alors

$$I(V(I)) = I(\{1\}) = \langle X - 1 \rangle = \sqrt{I}.$$

On laisse les détails en exercices. On verra un peu plus loin ce que donne $I(V(I))$ en général dans le cas où $\mathbf{k}$ est algébriquement clos. Si $\mathbf{k}$ n'est pas algébriquement clos, on ne contrôle plus grand chose.

## 4.3 Théorème des zéros de Hilbert

Commençons par un petit lemme utile dans la suite.

**Lemme 4.17.** Tout corps algébriquement clos est infini.

*Démonstration.* Soit $\mathbb{K}$ un corps fini. C'est donc un sur-corps de $\mathbb{F}_p$ pour un certain nombre premier $p$. On suppose (par l'absurde) que $\mathbb{K}$ algébriquement clos. Alors pour tout $r \in \mathbb{N}^*$, $\mathbb{K}$ contient les racines de $X^{p^r} - X$ donc (voir le paragraphe 5.5.1) $\mathbb{K}$ contient $F_{p^r}$. Par conséquent le cardinal de $\mathbb{K}$ est $\geq p^r$ pour tout $r \geq 1$ ce qui contredit la finitude de $\mathbb{K}$. □

Remarquons aussi une chose :

**Lemme 4.18.** Si $\mathbf{k}$ est un corps infini et $P \in \mathbf{k}[X_1, \ldots, X_n$ alors $P$ est nul si et s. si la fonction polynomiale associée $f_P : \mathbf{k}^n \to k$ est nulle

*Démonstration.* Se fait par récurrence sur $n$. Si $n = 1$, c'est trivial. Supposons le résultat vrai au rang $n$ et soit $P \in \mathbf{k}[X_1, \ldots, X_{n+1}]$ dont la fonction associée est nulle.
Écrivons $P = \sum_{i=0}^{d} Q_i X_{n+1}^i$ où $Q_i \in \mathbf{k}[X_1, \ldots, X_n]$.

L'hypothèse sur $P$ nous dit que pour tout $a = (a_1, \ldots, a_n) \in \mathbf{k}^n$ et tout $\alpha \in \mathbf{k}$, $\sum_{i=1}^{d} Q_i(a)\alpha^i = 0$. Fixons $a = (a_1, \ldots, a_n) \in \mathbf{k}^n$. On obtient alors une fonction polynomiale nulle donnée par $\mathbf{k} \ni \alpha \mapsto P(a, \alpha) \in \mathbf{k}$ ce qui entraine que le polynôme $P(a, X_{n+1})$ est nul d'où, pour tout $i$, $Q_i(a) = 0$. L'hypothèse de récurrence entraine que chaque polynôme $Q_i$ est nul et donc $P$ est nul. □

**Lemme 4.19** (de normalisation de Noether)**.** Soit $n \geq 2$ et $\mathbf{k}$ un corps infini. Soit $f \in \mathbf{k}[X_1, \ldots, X_n]$ de degré $d \geq 1$. Alors il existe $(\lambda_1, \ldots, \lambda_{n-1}) \in \mathbf{k}^{n-1}$ tel que le coefficient devant $X_n^d$ dans

$$f(X_1 + \lambda_1 X_n, \ldots, X_{n-1} + \lambda_{n-1} X_n, X_n)$$

soit non nul.

*Démonstration.* Écrivons

$$f = \sum_{i_1,\dots,i_n} a_{i_1,\dots,i_n} X_1^{i_1} \cdots X_n^{i_n} \quad \text{(somme finie)}$$

avec $a_{i_1,\dots,i_n} \in \mathbf{k}$. Posons alors

$$g = \sum_{i_1+\cdots+i_n=d} a_{i_1,\dots,i_n} X_1^{i_1} \cdots X_n^{i_1}.$$

Par hypothèse $f$ est de degré $d$ donc $g$ est non nul. Notons que $g$ est homogène de degré $d$.
Montrons que $g(X_1,\dots,X_n,1) \in \mathbf{k}[X_1,\dots,X_n]$ n'est pas nul.
Par l'absurde, supposons qu'il est nul. Alors $g = (X_n-1)Q$ pour une certain $Q \in \mathbf{k}[X_1,\dots,X_n]$ (en effet, on peut faire une division euclidienne par $X_n - 1$ puis évaluer en $X_n = 1$ ; ou bien on peut aussi écrire $X_n = ((X_n-1)+1)$ dans le développement de $g$ et développer, puis évaluer en $X_n = 1$). Écrivons $Q = Q_{d-1} + Q'$ avec $Q_{d-1}$ homogène de degré $d-1$ et $Q'$ est de degré $< d-1$. Cela donne

$$g = (X_n-1)(Q_{d-1}+Q') = \underbrace{X_n Q_{d-1}}_{\text{homogène de degré } d} + \underbrace{X_n Q' - Q_{d-1} - Q'}_{\text{de degré } <d}.$$

Comme $g$ est homogène de degré $d$, on obtient :

$$0 = X_n Q' - Q_{d-1} - Q' = (X_n-1)Q' - Q_{d-1}$$

ou encore $Q_{d-1} = (X_n-1)Q'$.
On obtient une relation identique à celle obtenu ci-dessus mais en ayant perdu un degré. On peut réitérer le processus et obtenir

$$Q_1 = (X_n-1)\tilde{Q} \quad \text{avec } Q_1 \text{ homogène de degré 1.}$$

Mais ceci entraine $\tilde{Q}$ constant et $Q_1$ ne peut pas être homogène d'où l'absurdité. Finalement, le polynôme $g(X_1,\dots,X_{n-1},1)$ est bien non nul. Le lemme précédent entraine que la fonction associée est non nulle. Il existe donc $(\lambda_1,\dots,\lambda_{n-1}) \in \mathbf{k}^{n-1}$ tel que $g(\lambda_1,\dots,\lambda_{n-1},1) \neq 0$. Mais on se rend compte que ce nombre n'est rien d'autre que le coefficient devant $X_n^d$ dans $f(X_1+\lambda_1 X_n,\dots,X_{n-1}+\lambda_{n-1}X_n,X_n)$. En effet si on développe

$$\sum a_{i_1,\dots,i_n}(X_1+\lambda_1 X_n)^{i_1}\cdots(X_{n-1}+\lambda_{n-1}X_n)^{i_{n-1}}\cdot X_n^{i_n}$$

alors le terme devant $X_n^d$ sera

$$\sum_{i_1+\cdots+i_n=d} a_{i_1,\dots,i_n}\lambda_1^{i_1}\cdots\lambda_{n-1}^{i_{n-1}}$$

qui n'est rien d'autre que $g(\lambda_1,\dots,\lambda_{n-1},1)$. □

**Proposition 4.20** (Nullstellensatz faible)**.** Soit $\mathbf{k}$ un corps algébriquement clos et $I \subsetneq \mathbf{k}[\underline{X}]$ alors $V(I)$ est non vide.

*Démonstration.* La preuve se fait par récurrence sur $n$. Si $n = 1$ alors c'est trivial (tout polynôme non constant admet une racine).
Soit donc $n \geq 2$. Soit $g \in I$ alors, le corps $\mathbf{k}$ étant infini, par lemme précédent (quitte à diviser par le coefficient non nul en question) on peut écrire

$$g(X_1+\lambda_1,\dots,X_{n-1}+\lambda_{n-1}X_{n-1},X_n) = X_n^d + r(X_1,\dots,X_n)$$

avec $r(X_1,\dots,X_n)$ de degré $< d$ en $X_n$, ceci pour un certain $(\lambda_1,\dots,\lambda_{n-1}) \in \mathbf{k}^{n-1}$ fixé. Notons $J = \{f(X_1+\lambda_1,\dots,X_{n-1}+\lambda_{n-1}X_{n-1},X_n)\ ;\ f\in I\}$. Alors $J$ est un idéal de $\mathbf{k}[\underline{X}]$ et $J \neq \mathbf{k}[\underline{X}]$. De plus : $V(I)\neq\emptyset \iff V(J)\neq\emptyset$.
Par conséquent, quitte à remplacer $I$ par $J$ on peut supposer que $I$ contient un élément du type $X_n^d + r(X_1,\dots,X_n)$ avec $r$ de degré $< d$ en $X_n$ que l'on peut écrire aussi

$$g = X_n^d + g_{d-1}X_n^{d-1} + \cdots + g_0, \qquad g_i \in \mathbf{k}[X_1,\dots,X_{n-1}].$$

On pose alors $I' = I \cap \mathbf{k}[X_1,\dots,X_{n-1}]$. C'est un idéal de $\mathbf{k}[X_1,\dots,X_{n-1}]$ et qui est différent de $\mathbf{k}[X_1,\dots,X_{n-1}]$ (car sinon 1 serait dans $I' \subset I$). Par hypothèse de récurrence, il existe $a = (a_1,\dots,a_{n-1}) \in V(I')$.
Soit alors $J = \{f(a_1,\dots,a_{n-1},X_n)\ ;\ f\in I\}$ ; idéal de $\mathbf{k}[X_n]$.

— Si $J \subsetneq \mathbf{k}[X_n]$ alors $J = \langle P(X_n)\rangle$ avec $P$ non constant. Soit alors $a_n \in \mathbf{k}$ une racine de $P$ et on obtient que $(a_1,\dots,a_{n-1},a_n) \in V(I)$ qui est donc non vide

— Si $J = \mathbf{k}[X_n]$ alors $1 \in J$ donc il existe $f \in I$ tel que $f(a_1,\dots,a_{n-1},X_n) = 1$.
Écrivons $f = f_0 + f_1X_n + \cdots + f_kX_n^k$ avec $f_i \in \mathbf{k}[X_1,\dots,X_{n-1}]$. Alors $f_0(a) = 1$ et $f_1(a) = \cdots = f_k(a) = 0$.
Soit $R$ le résultant de $g$ et $f$ par rapport $X_n$. Alors $R \in \mathbf{k}[X_1,\dots,X_{n-1}]$ et $R \in I$ (car combinaison de $f$ et $g$) donc $R \in I'$ et donc $R(a) = 0$.
D'autre part $R(a)$ est le déterminant d'une matrice triangulaire inférieure avec des 1 sur la diagonale (le premier paquet de 1 est celui qui est devant $X_n^d$ dans $g$ et l'autre paquet de 1 provient de $f_0(a)$) ce qui donne $R(a) = 1$. D'où une absurdité. Ce cas est donc impossible.

□

**Théorème 4.21.** (Nullstellensatz fort) Soit $\mathbf{k}$ un corps algébriquement clos.
Soit $I \subset \mathbf{k}[X_1,\dots,X_n]$ un idéal. Alors $I(V(I)) = \sqrt{I}$.

**Lemme 4.22.** Soit $I$ un idéal de $\mathbf{k}[\underline{X}]$ ; on ne suppose pas $\mathbf{k}$ algébriquement clos.
Soit $\{f_1,\dots,f_s\}$ un système de générateurs de $I$ et soit $f \in \mathbf{k}[\underline{X}]$. Notons $T$ un nouvelle indéterminée. Alors

$$f \in \sqrt{I} \iff 1 \in \langle f_1,\dots,f_s,1-Tf\rangle \subset \mathbf{k}[X_1,\dots,X_n,T].$$

*Démonstration.*
$\Longrightarrow$ : Si $f^m \in I$ alors $1-T^mf^m = 1-(Tf)^m = (1-Tf)Q$ où $Q \in \mathbf{k}[\underline{X},T]$. D'où $1 = T^mf^m + Q\cdot(1-Tf)$ appartient à l'idéal voulu.
$\Longleftarrow$ : On écrit $1 = g_1(\underline{X},T)f_1 + \cdots + g_s(\underline{X},T)f_s + g(\underline{X},T)(1-Tf)$. On évalue en $T = 1/f$ et on obtient

$$1 = g_1(\underline{X},1/f)f_1 + \cdots + g_s(\underline{X},1/f)f_s.$$

On chasse les dénominateurs dans le membre de droite en multipliant par une puissance de $f$ assez grande et on obtient $f^m \in I$. □

*Démonstration du théorème.* On sait déjà que $\sqrt{I} \subset I(V(I))$.
Soit $f \in I(V(I))$. Soient $f_1,\dots,f_s$ des générateurs de $I$ sur $\mathbf{k}[\underline{X}]$. Via le lemme, le but est donc de montrer que 1 appartient à $J = \langle f_1,\dots,f_s,1-Tf\rangle \subset \mathbf{k}[\underline{X},T]$.
Montrons que $V(J) = \emptyset \subset \mathbf{k}^{n+1}$. Par l'absurde, soit $(a_1,\dots,a_n,\tau) \in V(J)$.

Si $(a_1, \ldots, a_n) \in V(I)$ alors $1 - \tau f(a) = 0$ i.e. $1 = 0$. Absurde.
Si $(a_1, \ldots, a_n) \notin V(I)$ alors il existe il existe $i \in \{1, \ldots, s\}$ tel que $f_i(a_1, \ldots, a_n) \neq 0$ mais alors $0 \neq f_i(a_1, \ldots, a_n) = f_i(a_1, \ldots, a_n, \tau) = 0$. Absurde.
Par le Nullstellensatz faible, $J = \langle 1 \rangle$. □

Le théorème suivant résume ce qui a été fait jusqu'ici.

**Théorème 4.23.**

1. Ici $\mathbf{k}$ est un corps quelconque. Notons $\mathcal{I}$ l'ensemble des idéaux de $\mathbf{k}[\underline{X}]$ et $\mathcal{EAA}$ l'ensemble des ensembles algébriques affines dans $\mathbf{k}^n$. Alors les applications

$$I : \mathcal{EAA} \to \mathcal{I} \qquad \text{et } V : \mathcal{I} \to \mathcal{EAA}$$

   sont deux application décroissantes telles que $V \circ I = \mathrm{Id}_{\mathcal{EAA}}$ ; en particulier $V$ est surjective et $I$ est injective.

2. Ici $\mathbf{k}$ est supposé algébriquement clos. Notons $\mathcal{IR}$ l'ensemble des idéaux radicaux de $\mathbf{k}[\underline{X}]$. Alors par restrictions, on obtient

$$I : \mathcal{EAA} \to \mathcal{IR} \qquad \text{et } V : \mathcal{IR} \to \mathcal{EAA}$$

   et ces applications sont deux bijections réciproques l'une de l'autre.

*Démonstration.* Dans le (1), tout a déjà été vu.
Concernant (2), on a vu que $I$ est bien à valeurs dans $\mathcal{IR}$ (voir point 4 dans la prop page 41). Le point 3 de cette même proposition nous dit que $V(I(V)) = V$ pour tout $V \in \mathcal{EAA}$ et le Nullstellensatz nous dit que $I(V(I)) = \sqrt{I} = I$ (si $I$ est radical). □

## 4.4 Dictionnaire Algèbre-Géométrie

On a vu la correspondance entre idéaux radicaux et ensembles algébriques affines. On va affiner cette correspondance d'une part et d'autre part voir ce que certaines opérations algébriques dans $\mathbf{k}[\underline{X}]$ entrainent d'un point de vue géométrique et topologique dans $\mathbf{k}^n$. Certains résultats ne seront valables qu'avec un corps algébriquement clos.
Tout d'abord un résultat assez naturel.

**Proposition 4.24.** Soit $E$ une sous-ensemble de $\mathbf{k}^n$. Alors $I(E) = I(\overline{E})$. Ici $\overline{E}$ désigne l'adhérence de Zariski de $E$.

Ce résultat dit que si un polynôme s'annule sur $E$ alors il s'annule sur son adhérence.

*Démonstration.* On a $E \subset \overline{E}$ donc $I(\overline{E}) \subset I(E)$.
Soit $f \in \mathbf{k}[\underline{X}]$ s'annulant sur $E$, i.e. $f \in I(E)$. Alors $E \subset V(f)$. Or $\overline{E}$ est, par définition, le plus petit fermé contenant $E$ donc $\overline{E} \subset V(f)$ ce qui signifie que $f \in I(\overline{E})$. □

Rappelons qu'un idéal propre $I \subsetneq \mathbf{k}[\underline{X}]$ est premier si : pour $f, g \in \mathbf{k}[\underline{X}]$, $fg \in I$ implique $f \in I$ ou $g \in I$. Il y a une notion très proche du côté des ensembles algébriques affines.

**Définition 4.25.** Un EAA $V \subset \mathbf{k}^n$ est dit irréductible si : pour tous EAA $V_1, V_2$, si $V = V_1 \cup V_2$ alors $V = V_1$ ou $V = V_2$.

**Proposition 4.26.** Soit $V \subset \mathbf{k}^n$ un EAA. Alors $V$ est irréductible si et seulement si $I(V)$ est un idéal premier.

*Démonstration.* Supposons $V$ irréductible et soient $f, g \in \mathbf{k}[\underline{X}]$ tels que $fg \in I(V)$. Alors $V \subset V(f) \cup V(g)$ ce qui entraine $V = (V \cap V(f)) \cup (V \cap V(g))$. L'hypothèse entraine, par exemple, $V = V \Cap V(f)$ ce qui implique $f \in I(V)$.
Réciproquement supposons $I(V)$ premier et supposons qu'on ait $V = V_1 \cup V_2$ comme union de deux EAA. Supposons, par exemple, que $V \neq V_2$ alors $V_2 \subsetneq V$ ce qui entraine $I(V) \subsetneq I(V_2)$ et montrons que $V = V_1$ (sachant qu'on a déjà $V_1 \subset V$). L'inclusion stricte précédente implique l'existence de $f \in I(V_2) \setminus I(V)$. Soit $g \in I(V_1)$. Alors $fg \in I(V)$ qui est premier donc $g \in I(V)$. Ainsi $I(V_1) \subset I(V)$ ce qui entraine (en appliquant l'opération $V$) que $V \subset V_1$. □

**Corollaire 4.27.** Supposons $\mathbf{k}$ est algébriquement clos. Alors les applications $I$ et $V$ échangent idéaux premiers et EAA irréductibles.

*Démonstration.* Si $V$ est irréductible alors, d'après la proposition précédente, $I(V)$ est premier.
Réciproquement soit $I$ un idéal premier. Montrons qu'il est radical. En effet si $f \in \mathbf{k}[\underline{X}]$ satisfait $f^m \in I$ pour un certain entier $m \in \mathbb{N}^*$ alors $f \cdot f^{m-1} \in I$ ce qui entraine $f \in I$ ou $f^{m-1} \in I$. De proche en proche, on arrive à $f \in I$. Ainsi $\sqrt{I} \subset I$ et donc $I = \sqrt{I}$.
Si on note $V = V(I)$ alors $I(V) = \sqrt{I} = I$ (par le Nullstellensatz) mais comme $I$ est premier, la proposition précédent nous dit que $V = V(I)$ est irréductible. □

**Remarque 4.28.** Plaçons nous dans le cas d'un idéal principal de $\mathbf{k}[\underline{X}]$ avec $\mathbf{k}$ algébriquement clos. Soit donc $I$ un idéal propre et $f$ un générateur de $I$. Dans $\mathbf{k}[\underline{X}]$ qui est factoriel, on peut décomposer

$$f = c \cdot f_1^{m_1} \cdots f_q^{m_q}$$

avec $c \in \mathbf{k}^*$, $m_i \in \mathbb{N}^*$ et $f_i$ premier.
Pour chaque $i$, $\langle f_i \rangle$ est un idéal premier et on a $V(\langle f_i \rangle) = V(f_i) = V(f_i^{m_i})$. On obtient alors $V(I) = \bigcup V(f_i)$ et puisque $\langle f_i \rangle$ est premier, chaque $V(f_i)$ est irréductible.
Nous allons voir que cette décomposition en variétés irréductibles est générale (avec un corps pas nécessairement algébriquement clos).

**Définition 4.29.** Soit $V \subset \mathbf{k}^n$ (on ne suppose pas $\mathbf{k}$ alg. clos). On dit que $V$ admet une décomposition en variétés irréductibles si on a : $V = V_1 \cup \cdots \cup V_q$ avec $V_i$ EAA irréductible.
De plus cette décomposition est dite minimale si pour tout $i, j$ tels que $i \neq j$, on a $V_i \not\subset V_j$.

**Proposition 4.30.** On ne suppose pas $\mathbf{k}$ algébriquement clos. Soit $V \subset \mathbf{k}^n$ un EAA. Alors $V$ admet une décomposition minimale en variétés irréductibles et elle est unique à l'ordre près des termes.

*Démonstration.* Montrons l'existence pour commencer. Si $V$ n'est pas irréductible alors on peut l'écrire $V = V_1 \cup V'$ avec $V_1, V' \subsetneq V$ Si $V_1$ n'est pas irréductible alors on peut l'écrire $V_1 = V_2 \cup V''$ avec $V_2 \subsetneq V_1$, etc. On obtient alors $\cdots \subsetneq V_2 \subsetneq V_1 \subsetneq V$ ce qui entraine $I(V) \subset I(V_1) \subset I(V_2) \subset \cdots$. De plus ces dernières inclusions sont strictes. En effet si on avait par exemple $I(V_1) = I(V_2)$ alors on aurait $V_1 = V(I(V_1)) = V(I(V_2)) = V_2$. Ainsi, on construit une chaine strictement croissante d'idéaux. Par noethérianité de $\mathbf{k}[\underline{X}]$ une telle chaine est finie. Cela entraine qu'on finit par avoir des $V_i$ irréductibles

dans une telle construction d'où l'existence d'une décomposition. Montrons qu'on peut la rendre minimale. En effet, si ça n'est pas le cas, il suffit de retirer tous les $V_i$ qui sont strictement inclus dans un autre et on obtient une décomposition minimale.

Montrons son unicité. Soient deux décompositions minimales $V = \bigcup_{i=1}^{q} V_i = \bigcup_{i=1}^{r} V_i'$. Pour chaque $V_i$ on a

$$V_i = V_i \cap V = V_i \cap (V_1' \cup \cdots \cup V_r') = (V_i \cap V_1') \cup \cdots \cup (V_i \cap V_r').$$

Comme $V_i$ est irréductible, on a $V_i = V_i \cap V_j'$ pour un certain $j$, i.e. $V_i \subset V_j'$. En faisant la même chose avec $V_j'$ on obtient $V_j' \subset V_k$ pour un certain $k$ d'où $V_i \subset V_j' \subset V_k$ mais par minimalité, cela entraine $V_i = V_k$ puis $V_i = V_j'$. On a montré que chaque $V_i$ est égal à l'un des $V_j'$. De façon symétrique, chaque $V_j'$ est égal à l'un des $V_i$ ce qui montre que $q = r$ et que ce sont les mêmes décompositions écrites dans un ordre éventuellement différent. □

Voici une conséquence immédiate d'une telle décomposition.

**Corollaire 4.31.** On suppose $\mathbf{k}$ alg. clos. Tout idéal radical $I \subset \mathbf{k}[\underline{X}]$ peut s'écrire comme intersection d'idéaux premiers $I = P_1 \cap \cdots \cap P_q$ avec $P_i \not\subset P_j$ si $i \neq j$ ; et cette décomposition est unique à l'ordre près des termes.

**Remarque 4.32** (pour la culture)**.** On peut se demander si on peut (comme dans le cas d'un idéal principal, voir la remarque plus haut) décomposer un idéal (quelconque) comme intersection d'idéaux plus "simples". La réponse est oui. C'est ce qu'on appelle la décomposition primaire qu'on n'étudiera pas ici.

Nous avons vu plus haut une correspondance entre idéaux premiers et EAA irréductibles. Il y en a une autre qui concerne les idéaux maximaux et les points.

**Proposition 4.33.** Étant donné un point $a = (a_1, \ldots, a_n) \in \mathbf{k}^n$, on note $m_a = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$.

1. Pour tout $a \in \mathbf{k}^n$, $m_a$ est un idéal maximal.
2. Pour tout $a \in \mathbf{k}^n$, $I(\{a\}) = m_a$ et $V(m_a) = \{a\}$.
3. Si $\mathbf{k}$ algébriquement clos alors tout idéal maximal de $\mathbf{k}[\underline{X}]$ est de la forme $m_a$ pour un $a \in \mathbf{k}^n$.

Comme conséquence immédiate, on a le corollaire suivant.

**Corollaire 4.34.** Supposons $\mathbf{k}$ algébriquement clos. Alors les applications $I$ et $V$ échangent idéaux maximaux (tous de la forme $m_a$) et points.

*Démonstration de la prop.*

1. Par division par exemple, on peut montrer que tout polynôme $f$ s'écrit sous la forme $f = f(a) + \sum_{i=1}^{n} q_i(X) \cdot (X_i - a_i)$. Cela montre que le morphisme (surjectif) d'anneaux $\mathbf{k}[\underline{X}] \to \mathbf{k}, f \mapsto f(a)$ a pour noyau $m_a$. Ainsi $\mathbf{k}[\underline{X}]/m_a$ est un corps donc $m_a$ est maximal.
2. On a trivialement $V(m_a) = \{a\}$. Pour l'autre égalité, on a aussi trivialement l'inclusion $m_a \subset I(\{a\})$. Par maximalité de $m_a$ cela implique l'égalité (car $I(\{a\}) \neq \mathbf{k}[\underline{X}]$).
3. Soit $I$ un idéal maximal. Alors par définition, $I \neq \mathbf{k}[\underline{X}]$. Par le Nullstellensatz faible, $V(I)$ contient au moins un point $a$, i.e. $\{a\} \subset V(I)$ ce qui implique par la version forte du Nullstellensatz, $\sqrt{I} = I(V(I)) \subset I(\{a\}) = m_a$. Or $I$ étant maximal (donc premier) il est radical ce qui entraine $I \subset m_a$. Par maximalité de $I$, on arrive à $I = m_a$.

□

Pour $1 \leq m \leq n$, on notera

$$\pi_m : \mathbf{k}^n \to \mathbf{k}^m,\ (a_1, \ldots, a_n) \mapsto (a_1, \ldots, a_m).$$

Étant donné un idéal $I \subset \mathbf{k}[X_1, \ldots, X_n]$, l'ensemble $I \cap \mathbf{k}[X_1, \ldots, X_m]$ est un idéal de $\mathbf{k}[X_1, \ldots, X_m]$ et à ce titre on peut regarder son lieu des zéros $V(I \cap \mathbf{k}[X_1, \ldots, X_m]) \subset \mathbf{k}^m$. On a alors le théorème de projection suivant.

**Théorème 4.35.** Soit $I \subset \mathbf{k}[X_1, \ldots, X_n]$ un idéal.
Notons $V = V(I) \subset \mathbf{k}^n$ et $I_m = I \cap \mathbf{k}[X_1, \ldots, X_m]$.

1. On a $\pi_m(V) \subset V(I_m)$.
2. Si $\mathbf{k}$ est algébriquement clos alors
$$\overline{\pi_m(V)} = V(I_m)$$
où $\overline{\pi_m(V)}$ désigne l'adhérence de Zariski dans $\mathbf{k}^m$.

*Démonstration.* 1. Soit $a' = \pi_m(a)$ avec $a = (a_1, \ldots, a_n) \in V$. Soit $f \in I_m$. Alors $f(a') = f(a)$ (car $f$ ne dépend pas des variables $X_{m+1}, \ldots, X_n$) et $f(a) = 0$ car $a \in V = V(I)$. L'inclusion en découle.

2. L'inclusion du (1) entraine l'inclusion $\overline{\pi_m(V)} \subset V(I_m)$ car $\overline{\pi_m(V)}$ est par définition le plus petit fermé contenant $\pi_m(V)$. Montrons l'inclusion inverse.
Rappelons qu'étant donné un ensemble de points $E$, son adhérence de Zariski est $\overline{E} = V(I(E))$.
Soit $f \in I(\pi_m(V))$ (remarquons que $f \in \mathbf{k}[X_1, \ldots, X_m]$). Pour tout $a \in V$, $f(a) = f(\pi_m(a)) = 0$.
Par conséquent, par le Nullstellensatz, il existe un entier $j \geq 1$ tel que $f^j \in I$ et donc $f^j \in I_m$.
Ainsi, $I(\pi_m(V)) \subset \sqrt{I_m}$ ce qui entraine $V(I_m) = V(\sqrt{I_m}) \subset V(I(\pi_m(V))) = \overline{\pi_m(V)}$.

□

**Remarque 4.36** (pour la culture)**.** Dans le théorème précédent, on peut facilement construire des exemples où l'égalité $\pi_m(V) = V(I_m)$ n'a pas lieu donc l'adhérence est nécessaire pour atteindre l'égalité en général et ce qui "manque" pour avoir l'égalité est petit dans le sens suivant :
il existe $W \subset \mathbf{k}^m$ un EAA tel que $W \subsetneq V(I_m)$ et $V(I_m) \smallsetminus W \subset \pi_m(V) \subset V(I_m)$.

Dans le résultat suivant, on s'intéresse à une autre opération. On se donne deux EAA $V = V(I), W = V(J)$ avec $W \subsetneq V$. Peut-on trouver un idéal dont le lieu des zéros est $\overline{V \smallsetminus W}$ ?
Voici deux exemples triviaux.

**Exemple 4.37.** 1. Dans $\mathbb{C}^2$, $V = V(X_1X_2)$ et $W = V(X_2)$. Alors $V$ est l'union des deux axes de coordonnées et $W$ est l'axe des abscisses et donc $V \smallsetminus W$ est l'axe des ordonnées privé de l'origine. Dans ce cas, $\overline{V \smallsetminus W}$ est égal à l'axe des ordonnées (pourquoi ?) et est donc égal à $V(X_1)$.

2. Toujours dans $\mathbb{C}^2$, $V = V(X_1)$ et $W = V(X_2)$, i.e. $V$ est l'axe des ordonnées et $W$ celui des abscisses. La différence $V \smallsetminus W$ est encore l'axe des ordonnées privé de l'origine et l'adhérence est l'axe des abscisses et est égal à $V(X_1)$.

On voit dans l'exemple 1 qu'on a $\overline{V(X_1X_2) \smallsetminus V(X_2)} = V(X_1)$ donc d'une certaine façon on a "quotienté" l'idéal de départ $\langle X_1X_2 \rangle$ par l'idéal $\langle X_2 \rangle$ pour obtenir l'idéal $\langle X_1 \rangle$ d'où la notion qui suit.

**Définition 4.38.** Soient $I, J \subset \mathbf{k}[\underline{X}]$ deux idéaux. On définit le quotient de $I$ par $J$

$$I : J = \{f \in \mathbf{k}[\underline{X}];\ \forall g \in J,\ fg \in I\}.$$

**Proposition 4.39.** Soient $I, J$ deux idéaux de $\mathbf{k}[\underline{X}]$.

1. On a $V(I) \setminus V(J) \subset V(I : J)$.
2. Si $\mathbf{k}$ est algébriquement clos alors $\overline{V(I) \setminus V(J)} = V(\sqrt{I} : J)$.

*Démonstration.* 1. Soit $a \in V(I) \setminus V(J)$ et soit $f \in I : J$. Puisque $a \notin V(J)$, il existe $g \in J$ tel que $g(a) \neq 0$. On a par définition de $I : J$, $fg \in I$. Donc $fg(a) = 0$ mais $g(a) \neq 0$ donc $f(a) = 0$ d'où l'égalité.

2. Comme $V(I) = V(\sqrt{I})$, on peut supposer $I$ radical et montrer que $\overline{V(I) \setminus V(J)} = V(I : J)$. L'inclusion du (1) entraine, par passage à l'adhérence, l'inclusion gauche-droite. Montrons l'inclusion inverse. Pour ça, soit $f \in I(V(I) \setminus V(J))$. Soit $g \in J$ alors $fg$ s'annule sur $(V(I) \setminus V(J)) \cup V(J) = V(I)$ donc par le Nullstellensatz, $fg \in \sqrt{I} = I$, ce qui montre que $f \in I : J$. On a donc l'inclusion $I(V(I) \setminus V(J)) \subset I : J$ d'où $V(I : J) \subset V(I(V(I) \setminus V(J))) = \overline{V(I) \setminus V(J)}$.

□

**Exercice 4.40.** Avec $I = \langle (X-1)^2(X-2) \rangle$ et $J = \langle (X-1) \rangle$, montrer que $V(\sqrt{I} : J) \neq V(I : J)$. Une des inclusions est-elle toujours vraie ?

**Corollaire 4.41.** Ici $\mathbf{k}$ n'est pas supposé alg. clos. Soient $V, W \subset \mathbf{k}^n$ deux EAA. Alors

$$I(V) : I(W) = I(V \setminus W).$$

*Démonstration.* Pour une inclusion on utilise le (1) de la prop. et pour l'autre, il n'y a pas de difficultés. On laisse les détails en exercice. □

Le tableau suivant résume ce qui a été fait jusqu'ici sur le lien entre algèbre et géométrie. Dans la colonne de gauche, *tous les idéaux sont (supposés) radicaux* et dans la colonne de droite on a des EEA.

| Algèbre | | Géométrie |
|---|---|---|
| $I$ | $\longrightarrow$ | V(I) |
| I(V) | $\longleftarrow$ | V |
| $I + J$ | $\longrightarrow$ | $V(I) \cap V(J)$ |
| $\sqrt{I(V) + I(W)}$ | $\longleftarrow$ | $V \cup W$ |
| $IJ$ | $\longrightarrow$ | $V(I) \cup V(J)$ |
| $\sqrt{I(V)I(W)}$ | $\longleftarrow$ | $V \cup W$ |
| $I \cap J$ | $\longrightarrow$ | $V(I) \cup V(J)$ |
| $I(V) \cap I(W)$ | $\longleftarrow$ | $V \cup W$ |
| $I : J$ | $\longrightarrow$ | $\overline{V(I) \setminus V(J)}$ |
| $I(V) : I(W)$ | $\longleftarrow$ | $\overline{V \setminus W}$ |
| $\sqrt{I \cap \mathbf{k}[X_1, \ldots, X_m]}$ | $\longleftrightarrow$ | $\overline{\pi_m(V(I))}$ |
| idéal premier | $\longleftrightarrow$ | EAA irréductible |
| idéal maximal | $\longleftrightarrow$ | point |

## 4.5 Bases de Gröbner

Dans $\mathbf{k}[X]$ on a la division euclienne (on a d'ailleurs aussi une division suivant les puissances croissantes) et cette division euclidienne permet entre autres, via l'algorithme de Bézout, de construire un générateur d'un idéal dont on connait un système fini de générateur.
Ce qu'on va faire ici est analogue. Dans $\mathbf{k}[X_1, \ldots, X_n]$, on va définir une forme de division, cette division dépendra de l'ordre choisi un peu comme dans le cas d'une variable où on décide de diviser suivant les

puissances croissantes ou décroissantes (Euclide) à la différence que dans le cas d'une variable, on n'a que deux ordres possibles alors que dans le cas de plusieurs variables, on en a une infinité et seuls certains (qualifiés de bons) seront utilisés ici. On aura alors un analogue de l'algorithme d'Euclide qui sera l'algorithme de Buchberger avec comme but : la construction d'une base de Gröbner d'un idéal donné par un système fini de générateurs. Cette base n'est pas unique (on peut la rendre unique en imposant des conditions supplémentaires mais elle dépendra toujours de l'ordre choisi pour les divisions). Elle permet par exemple de répondre à la question de savoir si un polynôme donné appartient ou bon à un idéal donné ; ou bien aussi elle rend constructive la notion d'élimination.

**Notations.** Dans la suite on notera fréquemment $X^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ où $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$.

### 4.5.1 Idéaux monomiaux

**Lemme 4.42** (de Dickson)**.** Tout idéal monomial admet un système fini de générateurs.

C'est une conséquence directe du théorème de la base d'Hilbert.
Nous allons néanmoins en fournir une preuve directe. Pour cela, nous donnons quelques résultats sur les idéaux monomiaux.

**Lemme 4.43.** Soit $A$ une partie non vide de $\mathbb{N}^n$ Soit $I$ l'idéal engendré par les $X^\alpha$ avec $\alpha \in A$. Alors pour tout $\beta \in \mathbb{N}^n$, $X^\beta \in I$ si et s. si il existe $\alpha \in A$ tel que $X^\alpha | X^\beta$.

*Démonstration.* Seul le sens direct est à démontrer. Soit $X^\beta$ un élément de $I$. Alors on peut l'écrire sous forme d'une somme finie $X^\beta = \sum_{\alpha \in A} q_\alpha X^\alpha$. En écrivant chaque $q_\alpha$ sous forme de combinaison linéaire de monômes, on obtient que $X^\beta$ est nécessairement un terme de la somme de droite d'où le résultat. □

**Lemme 4.44.** Soit $I$ un idéal monomial de $\mathbf{k}[\underline{X}]$. Soit $f \in \mathbf{k}[\underline{X}]$. Les conditions suivantes sont équivalentes.

1. $f \in I$.
2. Tous les termes de $f$ sont dans $I$.
3. $f$ est une combinaison linéaire sur $\mathbf{k}$ de monômes de $I$.

*Démonstration.* Supposons (1). Écrivons $f = \sum_\beta c_\beta X^\beta$ (somme finie avec $\beta \in \mathbb{N}^n$). Comme $f$ appartient à $I$, on peut écrire $f = \sum_i q_i X^{\alpha_i}$ avec $X^{\alpha_i} \in I$. Comme dans le lemme précédent, on voit que chaque terme de gauche apparait à droite, i.e. appartient à $I$ ce qui implique (2).
Les implications (2) ⇒ (3) ⇒ (1) sont triviales. □

*Démonstration (du lemme de Dickson).* La preuve se fait par récurrence sur $n$. Pour $n = 1$, c'est trivial.
Soit alors $I$ un idéal de $\mathbf{k}[X_1, \ldots, X_n, Y] = \mathbf{k}[\underline{X}, Y]$. Soit $J$ l'idéal de $\mathbf{k}[\underline{X}]$ engendré par les $X^\alpha$ tels qu'il existe $k \in \mathbb{N}$ tel que $X^\alpha Y^k \in I$.
Par hypothèse de récurrence, soit $\alpha_1, \ldots, \alpha_q \subset \mathbb{N}^n$ tel que $\{X^{\alpha_i};\ i = 1, \ldots, q\}$ engendre $J$.
Pour chaque $i = 1, \ldots, q$, il existe $m_i \in \mathbb{N}$ tel que $X^{\alpha_i} Y^{m_i} \in I$. Soit alors $m = \max\{m_1, \ldots, m_q\}$.
Pour chaque $k = 0, \ldots, m-1$, soit $J_k \subset \mathbf{k}[\underline{X}]$ l'idéal engendré par les $X^\alpha$ pour lesquels $X^\alpha Y^k \in I$.
Encore par hypothèse de récurrence, $J_k$ a un nombre fini de générateurs : $X^{\alpha_{k,1}}, \ldots, X^{\alpha_{k,q_k}}$.
Soit $M = X^\alpha Y^k \in I$.
Si $k \geq m$ alors $M$ est multiple d'un $X^{\alpha_i} Y^m$ lui même multiple de $X^{\alpha_i} Y^{m_i}$.
Si $k < m$ alors $M$ est multiple d'un $X^{\alpha_{k,j}} Y^k$. □

**Corollaire 4.45.** Soit $A \subset \mathbb{N}^n$ et $I$ l'idéal de $\mathbf{k}[\underline{X}]$ engendre par $\{X^\alpha;\ \alpha \in A\}$. Alors il existe $B \subset A$ fini tel que $I = \langle X^\alpha;\ \alpha \in B\rangle$.

*Démonstration.* Par le lemme de Dickson, $I$ admet un système fini de générateurs $\alpha_1, \ldots, \alpha_q$. Par le deuxième lemme du paragraphe, pour chaque $i$, il existe $\beta_i \in A$ tel que $X^{\beta_i} | X^{\alpha_i}$. On pose alors $B = \{\beta_1, \ldots, \beta_q\}$. □

### 4.5.2 Ordres monomiaux

Rappelons qu'une relation d'ordre $\leq$ sur un ensemble $A$ est une relation binaire qui est réflexive ($x \leq x$), transitive ($x \leq y$ et $y \leq z$ implique $x \leq z$) et antisymétrique ($x \leq y$ et $y \leq x$ implique $x = y$). Cette relation est dite totale si deux éléments sont toujours comparables, i.e. pour tous $x, y \in A$, $x \leq y$ ou $y \leq x$.
Deux exemples de base : $\mathbb{R}$ muni de la relation d'ordre usuelle est un ensemble totalement ordonné.
Pour un ensemble $X$, l'ensemble de ses parties $A = \mathcal{P}(X)$ muni de la relation d'inclusion $\subseteq$ est un ensemble ordonné mais la relation n'est en général pas totale. Question : à quelle condition sur $X$, cette relation est-elle totale ?

**Définition 4.46.** Un ordre monomial sur $\mathbb{N}^n$ ou de façon équivalente sur les monômes $X^\alpha$ est une relation d'ordre $\preceq$ totale qui satisfait la condition suivante :

$$\forall \alpha, \beta, \gamma \in \mathbb{N}^n,\ \alpha \preceq \beta \Longrightarrow \alpha + \gamma \preceq \beta + \gamma,$$

ou de façon équivalente : $X^\alpha \preceq X^\beta \Longrightarrow X^\alpha X^\gamma \preceq X^\beta X^\gamma$.
Un ordre monomial est dit bon si pour toute partie non vide de $\mathbb{N}^n$ a un minimum.

**Lemme 4.47.** Soit $\preceq$ un ordre monomial sur $\mathbb{N}^n$. Les conditions suivantes sont équivalentes.

1. L'ordre $\preceq$ est un bon ordre.
2. Toute suite décroissante est stationnaire.
3. Pour tout $\alpha \in \mathbb{N}^n$, $\alpha \succeq 0$.

*Démonstration.* Supposons (1). Alors si une suite strictement décroissante existait alors l'ensemble de ses éléments n'aurait pas de minimum ce qui contredirait (1). D'ou (2).
Supposons (2) et par l'absurde qu'il existe $\alpha$ tel que $0 \succ \alpha$. Alors pour $k \in \mathbb{N}$, $k\alpha = 0 + k\alpha \succ \alpha + k\alpha = (k+1)\alpha$ et on obtient une suite strictement décroissante ce qui contredit (2). On a donc (3).
Supposons (3). Soit $A$ une partie de $\mathbb{N}^n$. Par le corollaire du lemme de Dickson, il existe $B \subset A$ fini tel que pour tout $\alpha \in A$, il existe $\beta \in B$ tel que $\alpha \in \beta + \mathbb{N}^n$. L'hypothèse (3) entraine alors que $\alpha \succeq \beta$.
L'ensemble $B$ étant fini, il admet un minimum. C'est alors le minimum de $A$ d'où (1). □

Voici quelques exemples d'ordres monomiaux bons.

**Exemple 4.48.**

1. L'ordre lexicographique défini par : $\alpha \prec \beta \iff$ dans $\alpha - \beta$, la première composante non nulle est positive.
2. On fixe un bon ordre monomial $\preceq_0$. Soit $w \in \mathbb{Z}^n$ qu'on voit comme un système de poids. On définit $\preceq_w$ comme suit : $\alpha \prec_w \beta \iff (w \cdot \alpha < w \cdot \beta$ ou ( $w \cdot \alpha = w \cdot \beta$ et $\alpha \prec_0 \alpha))$.
   Ici $w \cdot \alpha = \sum_i w_i \alpha_i$ (c'est le produit scalaire canonique de $\mathbb{R}^n$).
   Exercice : On pourra montrer que cet ordre est bon si et s. si $w \in \mathbb{N}^n$.

### 4.5.3 Bases de Gröbner

Un ordre monomial $\preceq$ est toujours fixé. Il n'est pas supposé bon.
On introduit quelques notations. Soit $f = \sum_\alpha c_\alpha X^\alpha \in \mathbf{k}[\underline{X}]$ non nul.
C'est une somme finie, les $\alpha$ sont dans $\mathbb{N}^n$ et les $c_\alpha$ dans $\mathbf{k}$.
On fixe un ordre monomial $\preceq$ sur $\mathbb{N}^n$. On note :

— $\mathrm{Supp}(f) = \{\alpha \in \mathbb{N}^n;\ c_\alpha \neq 0\}$ (le support de $f$)
— $\exp_\preceq(f) = \max_\preceq(\mathrm{Supp}(f))$ (l'exposant dominant de $f$)
— $\mathrm{lm}_\preceq(f) = X^{\exp_\preceq(f)}$ (le monôme dominant = leading monomial)
— $\mathrm{lc}_\preceq(f) = c_{\exp_\preceq(f)}$ (le coefficient dominant = leading coefficient)
— $\mathrm{lt}_\preceq(f) = \mathrm{lc}_\preceq(f) \cdot \mathrm{lm}_\preceq(f)$.

Dans la suite, si aucune confusion n'est possible, on enlèvera $\preceq$ en indice et on écrira $\exp(f)$, $\mathrm{lm}(f)$, etc.
Voici quelques propriétés immédiates (laissées en exercice). Soient $f, g \in \mathbf{k}[\underline{X}]$ non nuls.

— $\exp(f+g) \preceq \max\{\exp(f), \exp(g)\}$.
— Si $\exp(f) \neq \exp(g)$ alors $\exp(f+g) = \max\{\exp(f), \exp(g)\}$.
— $\exp(f \cdot g) = \exp(f) + \exp(g)$ (ou de façon équivalente $\mathrm{lm}(f \cdot g) = \mathrm{lm}(f)\mathrm{lm}(g)$).

**Définition 4.49.** Soit $I \subset \mathbf{k}[\underline{X}]$ un idéal non nul. On définit

$$\mathrm{lm}(I) = \langle \{\mathrm{lm}(g);\ g \in I \setminus \{0\}\} \rangle$$

L'ensemble $\mathrm{lm}(I)$ est appelé l'idéal monomial associé à $I$ (et l'ordre $\preceq$).

**Définition 4.50.** Soit $I \subset \mathbf{k}[\underline{X}]$ un idéal non nul. On appelle base de Gröbner (ou Groebner) de $I$ (relativement à l'ordre $\preceq$) tout ensemble fini $\{g_1, \ldots, g_r\} \subset I$ tel que

$$\mathrm{lm}(I) = \langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_r) \rangle.$$

Le lemme de Dickson (plus précisément son corollaire) assure l'existence d'une base de Gröbner.
Dans le paragraphe suivant, nous énonçons un théorème de division (ou réduction) qui montrera qu'une base de Gröbner est un système de générateurs de l'idéal en question et nous verrons par la suite les propriétés particulières qu'il possède.

### 4.5.4 Divisions

Dans ce paragraphe, on fixe un ordre monomial $\preceq$ et on le suppose bon.

**Proposition 4.51.** Soient $f, f_1, \ldots, f_s \in \mathbf{k}[\underline{X}]$. Il existe $q_1, \ldots, q_s, r \in \mathbf{k}[\underline{X}]$ tels que

1. $f = q_1 \cdot f_1 + \cdots + q_s \cdot f_s + r$,
2. pour tout $i = 1, \ldots, s$, si $q_i \neq 0$ alors $\mathrm{lm}(f) \succeq \mathrm{lm}(q_i f_i)$,
3. si $r \neq 0$ alors pour tout monôme $m$ de $r$ et pour tout $i = 1, \ldots, s$, $\mathrm{lm}(f_i)$ ne divise pas $m$.

Le polynôme $r$ est appelé "un reste de la division de $f$ par les $f_i$" ou encore "une réduction de $f$ modulo $\{f_1, \ldots, f_s\}$".

Dans cet énoncé, les $q_i$ et $r$ ne sont pas uniques.

*Démonstration.* L'énoncé se fait par récurrence sur $\mathrm{lm}(f)$.
Si $\mathrm{lm}(f) = 1$, autrement dit si $f$ est un polynôme constant alors si l'un des $f_i$ est constant alors on peut écrire $f = \frac{f_i}{f} \cdot f_i$, et sinon on pose $r = f$.
On se donne maintenant $f$ tel que $\mathrm{lm}(f) \succ 1$ et on suppose que pour tout $f'$ tel que $\mathrm{lm}(f') \prec \mathrm{lm}(f)$, le résultat est vrai pour $f'$. Notons qu'une récurrence est possible car, l'odre $\preceq$ étant bon, le nombre de monômes strictement plus petits que $\mathrm{lm}(f)$ est fini.
Ecrivons $f' = f - \mathrm{lt}(f)$. On a alors deux cas possibles.

— Cas 1 : $\mathrm{lm}(f)$ est multiple d'un des $\mathrm{lm}(f_i)$.
Soit donc $j$ tel que $\mathrm{lm}(f_j)|\mathrm{lm}(f)$. Notons $\mathrm{lt}(f) = c \cdot X^\alpha$ et $\mathrm{lt}(f_j) = e \cdot X^\beta$ avec $c, e \in \mathbf{k}$ et $\alpha, \beta \in \mathbb{N}^n$ et notons $f'_j = f_j - \mathrm{lt}(f_j)$. On a alors

$$\begin{aligned} f &= f' + \mathrm{lt}(f) \\ &= f' + \frac{c}{e} X^{\beta-\alpha} \cdot \mathrm{lt}(f_j) \\ &= f' + \frac{c}{e} X^{\beta-\alpha} \cdot (f_j - f'_j) \\ &= (f' - \frac{c}{e} X^{\beta-\alpha} f'_j) + \frac{c}{e} X^{\beta-\alpha} \cdot f_j. \end{aligned}$$

Notons $f''$ le terme entre parenthèse, ce terme satisfait $\mathrm{lm}(f'') \prec \mathrm{lm}(f)$ (exo) et on peut lui appliquer l'hypothèse de récurrence. On peut donc l'écrire $f'' = \sum_i q'_i f_1 + r'$ avec les conditions requises sur les $q'_i$ et sur $r'$. On obtient alors

$$f = q'_1 f_1 + \cdots + \big(\frac{c}{e} X^{\beta-\alpha} + q'_j\big) f_j + \cdots q'_s f_s + r'.$$

Il reste à vérifier que les conditions sont satisfaites (exo).

— Cas 2 : $\mathrm{lm}(f)$ n'est multiple d'aucun $\mathrm{lm}(f_i)$.
On applique l'hypothèse de récurrence à $f'$ et cela donne $f' = \sum_i q'_i f_i + r'$. On obtient la décomposition suivante

$$f = q'_1 f_1 + \cdots + q'_s f_s + (r' + \mathrm{lt}(f))$$

décomposition qui convient (à vérifier en exo).

□

Dans une telle division, rien n'est unique. Cependant nous avons un résultat plus précis dans le cas où on divise par une base de Gröbner.

**Proposition 4.52.** Soit $G = \{g_1, \ldots, g_s\}$ une base de Gröbner d'un idéal $I \subset \mathbf{k}[\underline{X}]$. Alors étant donné $f \in \mathbf{k}[\underline{X}]$, il existe un unique couple $(g, r) \in \mathbf{k}[\underline{X}]^2$ tel que

1. $f = g + r$,
2. $g \in I$,
3. si $r \neq 0$ alors aucun des monômes constituants $r$ n'est divisible par un $\mathrm{lm}(g_i)$ (i.e. on ne peut pas réduire $r$ modulo $G$).

*Démonstration.* L'existence est assurée directement par la proposition de division de $f$ par $G$. Montrons l'unicité. Soit $(g', r')$ un autre couple avec les propriétés demandées. Alors $R = r - r'$ appartient à $I$. Si $R$ n'est pas nul alors $\mathrm{lm}(R)$ est dans $\mathrm{lm}(I)$ et donc (voir 2ème lemme de 6.5.1) est divisible par l'un des $\mathrm{lm}(g_i)$ ce qui est impossible vues les conditions sur $r$ et $r'$. Ainsi $R = 0$. D'où $r = r'$ et $g = g'$. □

Ainsi, grâce à ce résultat on peut dire "le reste d'une division de $f$ par $G$" car ce reste est uniquement déterminé lorsque $G$ est une base de Gröbner de $I$ (bien que la division en elle-même n'est pas forcément unique).
Comme première application des bases de Gröbner, nous avons le test d'appartenance à un idéal.

**Proposition 4.53.** Soit $G$ une base de Gröbner de $I$. Soit $f \in \mathbf{k}[\underline{X}]$. Alors

$$f \in I \iff \text{le reste de n'importe quelle division de } f \text{ par } G \text{ est nul.}$$

*Démonstration.* Le sens "$\Leftarrow$" est trivial. Montrons le sens direct. Supposons $f \in I$. Considérons une réduction modulo $G$ : $f = \sum_i q_i g_i + r$ (on a noté $g_i$ les éléments de $G$). Alors $r$ est dans $I$. Donc, s'il n'est pas nul, $\mathrm{lm}(r)$ est divisible par l'un des $\mathrm{lm}(g_i)$ ce qui est impossible par la division. □

### 4.5.5 Critère et algorithme de Buchberger

Dans ce paragraphe, un bon ordre monomial $\preceq$ est encore fixé.
Nous savons que tout idéal admet une base de Gröbner. Nous allons donner un algorithme de calcul d'une telle base à partir d'un système de générateurs donné. Pour cela, nous avons besoin des $S$-polynômes.

**Définition 4.54.** Soient $f, g \in \mathbf{k}[\underline{X}]$ non nuls.
Notons $\mathrm{lt}(f) = cX^\alpha$ et $\mathrm{lt}(g) = dX^\beta$ avec $c, d \in \mathbf{k}$ et $\alpha, \beta \in \mathbb{N}^n$. Définissons $\gamma = (\gamma_1, \ldots, \gamma_n) \in \mathbb{N}^n$ en posant $\gamma_i = \max\{\alpha_i, \beta_i\}$. On définit le $S$-polynôme de $f$ et $g$ :

$$S(f,g) = \frac{1}{c} X^{\gamma-\alpha} \cdot f \ - \ \frac{1}{d} X^{\gamma-\beta} \cdot g.$$

Ce $S$-polynôme est construit de telle sorte qu'on annule les monômes dominants de $f$ et $g$ de "façon minimale".

**Théorème 4.55** (Critère de Buchberger)**.** Soit $G = \{g_1, \ldots, g_s\}$ un système de générateurs d'un idéal $I$. Alors $G$ est une base de Gröbner de $I$ si et seulement si : pour tout couple $(i,j) \in \{1, \ldots, s\}$ tel que $i \neq j$, la réduction de $S(g_i, g_j)$ modulo $G$ donne un reste nul.

Pour démontrer ce théorème, nous avons besoin d'un lemme technique.

**Lemme 4.56.** Soient $f_1, \ldots, f_s$ des polynômes ayant le même monôme dominant : $\forall i,\ \mathrm{lm}(f_i) = X^\delta$.
Soient $c_1, \ldots, c_s \in \mathbf{k}$ tels que

$$\mathrm{lm}\Big(\sum_{i=1}^{s} c_i \cdot f_i\Big) \prec X^\delta.$$

Alors $\displaystyle\sum_{i=1}^{s} c_i \cdot f_i$ est une combinaison linéaire sur $\mathbf{k}$ des $S(f_j, f_k)$.
De plus pour tout $1 \leq j, k \leq s$, $\mathrm{lm}(S(f_j, f_k)) \prec X^\delta$.

*Démonstration.* Voyons d'abord la dernière affirmation du lemme. Pour tout $i$, notons $d_i = \mathrm{lc}(f_i)$.
Étant donné que $f_j$ et $f_k$ ont le même monôme dominant (à savoir $X^\delta$), on obtient

$$S(f_j, f_k) = \frac{1}{d_j} f_j - \frac{1}{d_k} f_k.$$

Le monôme d'exposant $\delta$ disparait ce qui donne $\mathrm{lm}(S(f_j, f_k)) \prec X^\delta$.
Montrons la première partie du lemme à présent.
Pour tout $i$, $c_i d_i = \mathrm{lc}(c_i f_i)$ et l'hypothèse entraine alors que

$$c_1 d_1 + \cdots + c_s d_s = 0.$$

Pour tout $i$, posons $p_i = \frac{1}{d_i} f_i$. Remarquons que $S(f_j, f_k) = p_j - p_k$. La somme télescopique suivante permet alors de conclure la démonstration :

$$\begin{aligned}\sum_{i=1}^{s} c_i f_i = \sum_{i=1}^{s} c_i d_i p_i &= c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \cdots \\ &\quad + (c_1 d_1 + \cdots + c_{s-1} d_{s-1})(p_{s-1} - p_s) + \underbrace{(c_1 d_1 + \cdots + c_s d_s)}_{=0} p_s.\end{aligned}$$

□

*Démonstration du Théorème.* L'implication gauche-droite est une conséquence directe de la dernière prop. de 6.5.4.
On suppose donc que chaque réduction de $S(g_i, g_j)$ modulo $G$ donne un reste nul. Commençons par une remarque : soient $j, k \in \{1, \ldots, s\}$ et soient $\alpha, \beta \in \mathbb{N}^n$ tels que $\mathrm{lm}(X^\alpha g_j) = \mathrm{lm}(X^\beta g_k) = X^\delta$. Alors

$$\begin{aligned}S(X^\alpha g_j, X^\beta g_k) &= \frac{1}{\mathrm{lc}(g_j)} X^{\delta - (\alpha + \exp(g_j))} X^\alpha g_j - \frac{1}{\mathrm{lc}(g_k)} X^{\delta - (\beta + \exp(g_k))} X^\beta g_k \\ &= \frac{1}{\mathrm{lc}(g_j)} X^{\delta - \exp(g_j)} g_j - \frac{1}{\mathrm{lc}(g_k)} X^{\delta - \exp(g_k)} g_k \\ &= X^{\delta - \gamma} \cdot \Big( \frac{1}{\mathrm{lc}(g_j)} X^{\gamma - \exp(g_j)} g_j - \frac{1}{\mathrm{lc}(g_k)} X^{\gamma - \exp(g_k)} g_k \Big) \\ &\quad (\text{où } \gamma = (\gamma_1, \ldots, \gamma_n) \text{ et } \gamma_i = \max\{\exp(g_j)_i, \exp(g_k)_i\} \ ) \\ &= X^{\delta - \gamma} S(g_j, g_k).\end{aligned}$$

De plus, d'après le lemme, $\mathrm{lm}(S(X^\alpha g_j, X^\beta g_k)) \prec X^\delta$.
Soit $f \in I$ que l'on peut donc écrire

$$f = \sum_{i=1}^{s} h_i g_i$$

avec $h_i \in \mathbf{k}[\underline{X}]$. Le but est de montrer qu'on peut obtenir une telle écriture avec $\mathrm{lm}(f) \succeq \mathrm{lm}(h_i g_i)$. En effet, si cette condition est remplie alors $\mathrm{lm}(f)$ est divisible par l'un des $\mathrm{lm}(g_i)$ et cela montrera qu'on a bien une base de Gröbner.
On suppose donc que $\mathrm{lm}(f) \prec \delta := \max\{\mathrm{lm}(h_1 g_1), \ldots, \mathrm{lm}(h_s g_s)\}$. Notons $e_i = \exp(h_i g_i)$ (pour les $h_i \neq 0$). On peut écrire

$$f = \sum_{e_i = \delta} \mathrm{lt}(h_i) g_i + \sum_{e_i = \delta} (h_i - \mathrm{lt}(h_i)) g_i + \sum_{e_i < \delta} h_i g_i.$$

Dans le membre de droite, les deux derniers termes ont un monôme dominant $\prec X^\delta$. Comme $\mathrm{lm}(f) \prec \delta$ cela implique dans le premier terme de droite, qu'on note $h$, le monôme dominant est $\prec X^\delta$. Écrivons $\mathrm{lt}(h_i) = c_i \cdot X^{\alpha(i)}$. On se retrouve avec $\mathrm{lm}(\sum_{e_i = \delta} c_i X^{\alpha(i)} g_i) \prec \delta$. On peut donc appliquer le lemme précédent. On obtient alors que $h$ s'écrit comme une combinaison linéaire à coefficients dans $\mathbf{k}$ des $S\big(X^{\alpha(j)} g_j, X^{\alpha(k)} g_k\big)$ pour lesquels $\mathrm{lm}\big(X^{\alpha(i)} g_i\big) = \delta$. En utilisant la remarque précédente, on peut réécrire $h$ comme combinaison linéaire de termes du type $X^{\delta - \gamma} S(g_j, g_k)$ et pour lesquels le monôme

dominant est $\prec \delta$.
L'hypothèse du théorème nous dit qu'on peut réécrire $h$ comme combinaison des $g_i$ avec des termes de monômes dominants $\prec \delta$ (cela vient des conditions d'une division). Au final on a réécrit $f = \sum_{i=1}^{s} h'_i g_i$ avec $\delta' := \max\{\mathrm{lm}(h'_1 g_1), \ldots, \mathrm{lm}(h'_s g_s)\} \prec \delta$. Si $\delta' \succ \mathrm{lm}(f)$, on recommence de la même manière. Ce processus s'arrête car l'ensemble $\{m \ ; \ m \text{ monôme}, \ \mathrm{lm}(f) \prec m \preceq \delta\}$ est fini car l'ordre $\preceq$ est bon. □

Ce critère permet de donner un algorithme de calcul d'une base de Gröbner d'un idéal en partant d'un système de générateurs donnés.

Algorithme de Buchberger

— On se donne $I = \langle g_1, \ldots, g_q \rangle$.
— Posons $G_0 = \{g_1, \ldots, g_q\}$.
— Pour chaque $(i, j)$ tel que $i \neq j$, on considère le reste d'une division de $S(g_i, g_j)$ par $G_0$.
Dès qu'on trouve un reste non nul, on le nomme $g_{q+1}$ et on pose $G_1 = \{g_1, \ldots, g_q, g_{q+1}\}$.
— On recommence avec $G_1$ et on construit ainsi une suite strictement croissante $G_0 \subset G_1 \subset \cdots$.

Par construction, $\mathrm{lm}(g_{q+1})$ n'est divisible par aucun autre $\mathrm{lm}(g_i)$. Cela donne une inclusion stricte d'idéaux monomiaux $M_0 = \langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_q) \rangle \subsetneq M_1 = \langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_{q+1}) \rangle \subsetneq \cdots$. Par noethérianité de $\mathbf{k}[\underline{X}]$, cette suite est finie. Cela signifie qu'il existe un $s \in \mathbb{N}$ pour lequel toutes les réductions des $S(g_i, g_j)$ avec $g_i, g_j \in G_s$ donnent un reste nul. Le critère de Buchberger implique que $G_s$ est une base de Gröbner de $I$.

### 4.5.6 Élimination de variables et quelques conséquences

On a vu dans la section précédente qu'une projection d'un EAA correspond, dans le cas d'un corps algébriquement clos, à une élimination de variables. Nous allons voir comment se fait une telle élimination. On considère un idéal $I \subset \mathbf{k}[X_1, \ldots, X_n]$ donné par des générateurs et on cherche à calculer des générateurs de l'idéal $I \cap \mathbf{k}[X_1, \ldots, X_m]$ avec $m \in \{1, \ldots, n-1\}$.

**Proposition 4.57.** (Élimination) Soit $\preceq$ un ordre monomial tel que pour $i \in \{m+1, \ldots, n\}$ et pour tout monôme $\mu$ en les variables $X_1, \ldots, X_m$ on ait $X_i \succ \mu$.
Soit $g_1, \ldots, g_r$ une base de Gröbner de $I$ relativement à $\preceq$. Quitte à réordonner les $g_i$, supposons que $g_1, \ldots, g_s \in \mathbf{k}[X_1, \ldots, X_m]$ et $g_{s+1}, \ldots, g_r \notin \mathbf{k}[X_1, \ldots, X_m]$. Alors $g_1, \ldots, g_s$ forment une famille génératrice de $I \cap \mathbf{k}[X_1, \ldots, X_m]$.

**Remarque 4.58.**

1. Un tel ordre est appelé un ordre qui élimine les variables $X_{m+1}, \ldots, X_n$. On remarquera qu'on met un poids plus grand sur les variables qu'on souhaite éliminer.
2. Pour un tel ordre, on a pour tout $f \in \mathbf{k}[X_1, \ldots, X_n]$ : $f \in \mathbf{k}[X_1, \ldots, X_m] \iff \mathrm{lm}_{\preceq}(f) \in \mathbf{k}[X_1, \ldots, X_m]$. Je laisse ce point en exercice.
3. Il y a plusieurs façons d'obtenir un tel ordre. Par exemple ça peut être l'ordre lexicographique inverse. On peut aussi prendre un ordre associé au système de poids suivant : $w \cdot (\alpha_1, \ldots, \alpha_n) = \alpha_{m+1} + \cdots + \alpha_n$.

4. Notons $\preceq'$ la restriction de $\preceq$ aux monômes $X_1^{\alpha_1}\cdots X_m^{\alpha_m}$. Alors on a même un résultat un peu plus précis : $g_1,\ldots,g_s$ forment une base de Gröbner de $I\cap\mathbf{k}[X_1,\ldots,X_m]$ relativement à $\preceq'$. Nous allons démontrer ce dernier point dans la preuve à suivre.

*Démonstration de la Prop.* Nous allons, en fait, démontrer la proposition et le quatrième point de la remarque en même temps. Pour cela, soit $f\in I\cap\mathbf{k}[X_1,\ldots,X_m]$. Considérons une division de $f$ par les $g_i$ relativement à l'ordre $\preceq$, division dont le reste est nul puisque $f\in I : f=\sum_{i=1}^r q_ig_i$ avec $\mathrm{lm}_\preceq(f)\succeq\mathrm{lm}_\preceq(q_ig_i)$ pour les $i$ tels que $q_i\neq 0$. Soit $i\geq s+1$. Si, pour un tel $i$, nous avons $q_i\neq 0$ alors (par le point 2 de la remarque) $\mathrm{lm}_\preceq(q_ig_i)=\mathrm{lm}_\preceq(q_i)\mathrm{lm}_\preceq(g_i)$ contient $X_j$ avec $j\geq m+1$, ce qui entraine $\mathrm{lm}_\preceq(f)\prec\mathrm{lm}_\preceq(q_ig_i)$ ce qui est impossible.
Par conséquent, on a une écriture du type $f=\sum_{i=1}^s q_ig_i$ avec $\mathrm{lm}_\preceq(f)\succeq\mathrm{lm}_\preceq(q_ig_i)$ si $q_i\neq 0$. De plus, si $q_i\notin\mathbf{k}[X_1,\ldots,X_m]$ alors $\mathrm{lm}_\preceq(q_i)$ contient un $X_j$ avec $j\geq m+1$ ce qui est impossible encore une fois. Par conséquent, tous les $q_i$ sont dans $\mathbf{k}[X_1,\ldots,X_m]$. Mais alors, $\mathrm{lm}_{\preceq'}(f)=\mathrm{lm}_\preceq(f)\succeq\mathrm{lm}_\preceq(q_ig_i)=\mathrm{lm}_{\preceq'}(q_ig_i)$. □

Le résultat suivant a déjà été vu et démontré dans le paragraphe 6.3. Il permet de tester l'appartenance d'un élément au radical d'un idéal donné via un calcul de base de Gröbner. Nous le redonnons pour être complets.

**Proposition 4.59.** Soit $I$ un idéal de $\mathbf{k}[X_1,\ldots,X_n]$ et $T$ une nouvelle variable et soit $f\in\mathbf{k}[X_1,\ldots,X_n]$. Alors

$$f\in\sqrt{I}\iff 1\in\mathbf{k}[X_1,\ldots,X_n,T]\cdot I+\mathbf{k}[X_1,\ldots,X_n,T]\cdot(1-Tf).$$

L'élimination de variables en plus d'être liée géométriquement à la notion de projection possède d'autres applications que nous donnons dans la suite.

**Proposition 4.60** (Intersection d'idéaux)**.** Soient $I,J\subset\mathbf{k}[X_1,\ldots,X_n]$ deux idéaux. Soit $T$ une variable supplémentaire alors

$$I\cap J=\Big(T\cdot I+(1-T)\cdot J\Big)\cap\mathbf{k}[X_1,\ldots,X_n].$$

Ainsi, on est réduit à éliminer la variable $T$ d'un idéal de $\mathbf{k}[X_1,\ldots,X_n,T]$. Ici la notation $T\cdot I$ signifie l'idéal engendré par $T\cdot g$ où $g$ parcourt un ensemble de générateurs de $I$. On peut aussi le voir comme le produit des idéaux $\mathbf{k}[X_1,\ldots,X_n,T]\cdot I$ et $\mathbf{k}[X_1,\ldots,X_n,T]\cdot T$.

*Démonstration.* Notons $K$ l'idéal de droite. Soit $f\in I\cap J$. Alors $f=T\cdot f+(1-T)f\cdot f$ et $f$ appartient alors à $K$. Réciproquement, soit $f\in K$. Alors $f$ est indépendant de $T$ d'où $f=f_{|T=0}=f_{|T=1}$ ce qui montre facilement que $f\in I\cap J$ (les détails sont laissés au lecteur). □

Nous avons vu que le quotient de deux idéaux $I:J$ est directement lié à $V(I)\smallsetminus V(J)$. L'élimination nous permet de calculer un tel quotient.

**Proposition 4.61** (Quotients d'idéaux)**.**

1. Soient $I,J_1,\ldots,J_s\subset\mathbf{k}[\underline{X}]$ des idéaux alors

$$I:\big(\sum_{i=1}^s J_i\big)=\bigcap_{i=1}^s(I:J_i).$$

2. Soit $I \subset \mathbf{k}[\underline{X}]$ un idéal et soit $g \in \mathbf{k}[\underline{X}]$. Soient $g_1, \ldots, g_r$ des générateurs de $I \cap \langle g \rangle$. Alors l'ensemble $\{\frac{g_1}{g}, \ldots, \frac{g_r}{g}\}$ est générateur de $I : \langle g \rangle$.

*Démonstration.* Laissée en exercice. □

Cette proposition permet de calculer $I : J$ si on connait des générateurs de $I$ et de $J$. Le point 1 de la proposition permet de réduire le calcul à un quotient du type $I : \langle g \rangle$ où $g$ est un des générateurs donnés de $J$.

# Table des matières