Table des matières

CHAPITRE 1

Extensions algébriques.

On rappelle qu'un corps K est un anneau unitaire avec $1_K \neq 0$, pour des opérations que l'on notera toujours additivement et multiplicativement, dans lequel tout élément non nul est inversible pour la multiplication. Il suit que tous les idéaux de K sont triviaux, i.e. égaux à $\{0\}$ ou à K. Les morphismes de corps $\varphi : K \to L$ sont les morphismes d'anneaux entre deux corps. Il résulte de la nature des idéaux d'un corps qu'un tel morphisme est ou bien nul ($\varphi(x) = 0$ pour tout x de K), ou bien injectif. Dans tout ce cours on suppose que les morphismes de corps $\varphi : K \to L$ sont unitaires, c'est à dire qu'ils envoient l'élément unité de K sur celui de L, par suite *ils seront tous injectifs.*

Sauf mention expresse du contraire, *tous les anneaux et les corps sont supposés commutatifs.*

1. Extensions de corps.

DÉFINITION 1.1. Soit L un corps et K un sous-corps de L. On dit alors que L est une extension de K, et l'on écrit L/K (qui se lit "L sur K"). Soit E/K une extension et L un corps intermédiaire entre E et K (donc $K \subseteq L \subseteq E$ et ces inclusions sont entre corps et sous-corps), on dit alors que L/K et E/L sont des sous-extensions de E/K.

REMARQUE 1.2. On se gardera bien de confondre inclusions et injections, même canoniques. Par exemple, $E = \mathbb{Q}[X]/(X^2 - 2)$ est un corps muni d'une injection canonique $E \hookrightarrow \mathbb{R}$ venant de l'application $\mathbb{Q}[X] \to \mathbb{R}$ qui à X associe $\sqrt{2}$. De même, étant donné une autre indéterminée Y, on a une injection canonique $F = \mathbb{Q}[Y]/(Y^2 - 2) \hookrightarrow \mathbb{R}$. Les corps E et F sont distincts, mais si l'on confond ces injections canoniques avec des inclusions, ils deviennent égaux (il faut bien que le polynôme $X^2 - 2$ n'ait pas plus de deux racines dans $\mathbb{R}$) !

DÉFINITION 1.3. Soient L/K et E/K deux extensions du corps K. Un morphisme de corps : $L \to E$ trivial sur K est appelé un K-homomorphisme ou un K-morphisme. L'ensemble des K-homomorphismes de L dans E est noté $\mathrm{Hom}_K(L, E)$. Lorsque $L = E$ on parle de K-endomorphismes et l'on écrit $\mathrm{End}_K(L)$, ou encore $\mathrm{Aut}_K(L)$ lorsque l'on ne considère que les automorphismes (les K-automorphismes), ce dernier ensemble étant un groupe pour la composition des applications.

DÉFINITION 1.4. Soit L/K une extension, alors les opérations dont L est muni en font un K-espace vectoriel. On dit que l'extension L/K

est finie si L est un K-espace vectoriel de dimension finie. La dimension de L sur K se note $[L : K]$ et s'appelle le degré de L sur K, ou encore le degré de l'extension L/K. Les K-bases de L sont aussi appelées bases de l'extension L/K.

PROPOSITION 1.5. *Soient L/K et E/L deux extensions (donc on a $K \subseteq L \subseteq E$ et ces inclusions sont entre corps et sous-corps), les assertions suivantes sont équivalentes :*
(i) E/K est une extension finie,
(ii) les extensions L/K et E/L sont finies.
Si l'une de ces assertions est vraie, on a de plus la formule suivante

$$[E : K] = [E : L][L : K].$$

DÉMONSTRATION. Si (i) est vraie. Le corps L est un sous-K-espace vectoriel de E et tout système générateur de E sur K l'est à plus forte raison sur L.

Si (ii) est vraie. Soient $\{u_i\}_{1\leq i\leq r}$ une base de L/K et $\{v_i\}_{1\leq i\leq s}$ une base de E/L. Alors

$$\{u_i v_j\}_{1\leq i\leq r, 1\leq j\leq s}$$

est une base de E/K. En effet :
- C'est un système générateur. Soit $x \in L$, alors x s'écrit $x = \sum_{1\leq j\leq s} \lambda_j v_j$ avec les λ_j dans L, qui donc s'écrivent sous la forme $\lambda_j = \sum_{1\leq i\leq r} \mu_{i,j} u_i$ où les $\mu_{i,j}$ sont dans K. On a donc

$$x = \sum_{1\leq i\leq r, 1\leq j\leq s} \mu_{i,j} u_i v_j.$$

- C'est une partie libre. Soit

$$\sum_{1\leq i\leq r, 1\leq j\leq s} \mu_{i,j} u_i v_j = 0 \text{ avec les } \mu_{i,j} \text{ dans } K.$$

Il vient

$$0 = \sum_{1\leq i\leq r, 1\leq j\leq s} \mu_{i,j} u_i v_j = \sum_{1\leq j\leq s} \Big(\sum_{1\leq i\leq r} \mu_{i,j} u_i \Big) v_j,$$

donc, puisque $\{v_i\}_{1\leq i\leq s}$ est libre sur L

$$\sum_{1\leq i\leq r} \mu_{i,j} u_i = 0 \text{ pour } 1 \leq j \leq s,$$

dont on déduit que les $\mu_{i,j}$ sont tous nuls, puisque $\{u_i\}_{1\leq i\leq r}$ est libre sur K. □

Soient L/K une extension et M une partie de L, alors il existe un plus petit sous-corps de L contenant K et M, c'est l'intersection de tous les sous-corps de L contenant K et M.

DÉFINITION 1.6. Soient L/K une extension et M une partie de L. Le plus petit sous-corps de L contenant K et M s'appelle le sous-corps de L engendré sur K par M, ou encore la sous-extension de L/K

engendrée par M. Ce corps se note $K(M)$, ou $K(x_1, \cdots, x_r)$ si M est fini, $M = \{x_1, \cdots, x_r\}$.

PROPOSITION 1.7. *Soient L/K une extension et M une partie de L. Alors $K(M)$ est l'ensemble des expressions de la forme $P(x_1, \cdots, x_n)/Q(x_1, \cdots, x_n)$ où $x_1, \cdots, x_n \in M$, $n \in \mathbb{N}$, $n \leq$ card(M), où $P, Q \in K[X_1, \cdots, X_n]$ sont des polynômes avec $Q(x_1, \cdots, x_n) \neq 0$.*

DÉMONSTRATION. Les lois de corps impliquent que ces éléments sont dans $K(M)$ et il est facile de vérifier que leur ensemble contient K, contient M et forme un corps pour les lois de L. □

REMARQUE 1.8. Soient L/K une extension et M une partie de L. Il ne faut pas confondre $K(M)$ et $K[M]$, le deuxième étant le sous-anneau engendré par K et M. Rappelons que cet anneau $K[M]$ est l'ensemble des expressions polynomiales de la forme $P(x_1, \cdots, x_n)$ où $x_1, \cdots, x_n \in M$, $n \in \mathbb{N}$, $n \leq \text{card}(M)$, où $P \in K[X_1, \cdots, X_n]$ est un polynôme. En général on a $K[M] \neq K(M)$, par exemple si $M = \{X\}$, où X est une indéterminée, l'anneau des polynômes $K[X]$ n'est pas égal au corps des fractions rationnelles $K(X)$. Cependant il y a égalité pour une classe d'extensions de corps, les extensions algébriques, qui sont l'objet d'étude principal ici et qui seront définies au §(3) de ce chapitre. En guise de préliminaire, on pourra montrer par exemple que l'anneau $\mathbb{Q}[\sqrt{2}]$ est égal au corps $\mathbb{Q}(\sqrt{2})$. Une autre remarque intéressante est de constater que le corps des fractions de $K[M]$ est $K(M)$.

PROPOSITION 1.9. *Soit L/K une extension.*
(i) Soit M et N deux parties de L, alors on a

$$K(M \cup N) = K(M)(N) = K(N)(M).$$

(ii) Soit M une partie de L, alors on a

$$K(M) = \bigcup_{F \subset M, F\, fini} K(F).$$

DÉMONSTRATION. Ces assertions sont faciles, par exemple, pour la première : On a K et M dans $K(M \cup N)$, donc $K(M) \subset K(M \cup N)$ et puisque N est aussi dans $K(M \cup N)$, il vient $K(M)(N) \subset K(M \cup N)$. Réciproquement, $M \cup N$ et K sont dans $K(M)(N)$, d'où l'inclusion inverse. Etc. □

Cette dernière proposition permet la définition suivante

DÉFINITION 1.10. Soient K_1 et K_2 deux sous-corps d'un même troisième L. On appelle compositum de K_1 et K_2 le corps $K_1(K_2) = K_2(K_1)$, que l'on note $K_1 \cdot K_2$.

Parler du compositum de deux corps non inclus dans un même troisième n'a pas de sens, pour s'en convaincre, on peut par exemple examiner les deux corps E et F de la remarque 1.2.

DÉFINITION 1.11. Soit L/K une extension. On dit que c'est une extension de type fini s'il existe une partie finie M de L telle que $L = K(M)$.

REMARQUE 1.12. Une extension L/K finie est de type fini, en effet, si $\{u_1, \cdots, u_n\}$ est une K-base de L, on a $L = K(u_1, \cdots, u_n)$. La réciproque est fausse, par exemple, le corps des fractions rationnelles $K(X)$ est une extension de type fini de K mais n'est pas une extension finie de K.

2. Caractéristique d'un corps.

Soient K un corps et $\varphi_K : \mathbb{Z} \to K$ le morphisme qui à l'entier n associe $n1_K \in K$, où 1_K est l'élément unitaire de K. Comme K est intègre, le noyau de φ_K est un idéal premier de $\mathbb{Z}$, c'est à dire que l'on a $\mathrm{Ker}\varphi_K = \{0\}$ ou $\mathrm{Ker}\varphi_K = p\mathbb{Z}$, p étant un nombre premier.

DÉFINITION 2.1. Soient K un corps et $\varphi_K : \mathbb{Z} \to K$ comme précédemment,
- si $\mathrm{Ker}\varphi_K = \{0\}$, on dit que le corps K est de caractéristique 0 (ou parfois infinie) ou d'exposant caractéristique 1,
- si $\mathrm{Ker}\varphi_K = p\mathbb{Z}$, où p est un nombre premier, on dit que K est de caractéristique p ou d'exposant caractéristique p.

Les corps de caractéristiques les nombres premiers sont dits de caractéristiques positives ou finies.

EXEMPLE 2.2. Les corps $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont de caractéristique 0, si p est un nombre premier, le corps $\mathbb{Z}/p\mathbb{Z}$ est de caractéristique p.

Soit K un corps, de caractéristique 0, alors le morphisme $\varphi_K : \mathbb{Z} \to K$ se prolonge en une application

$$\tilde{\varphi}_K : \mathbb{Q} \to K,$$

qui à la fraction a/b associe $\varphi_K(a)/\varphi_K(b) \in K$; on voit facilement que $\tilde{\varphi}_K$ est un morphisme de corps, donc K *contient le sous-corps* $\tilde{\varphi}_K(\mathbb{Q})$ *qui est isomorphe au corps des nombres rationnels* $\mathbb{Q}$.

Soit K un corps de caractéristique $p > 0$. Alors φ_K induit un morphisme

$$\overline{\varphi}_K : \frac{\mathbb{Z}}{\mathrm{Ker}\varphi_K} = \frac{\mathbb{Z}}{p\mathbb{Z}} \to K,$$

par conséquent K *contient le corps* $\overline{\varphi}_K(\mathbb{Z}/p\mathbb{Z})$*, qui a* p *éléments, qui est isomorphe au corps* $\mathbb{Z}/p\mathbb{Z}$ (un corps à p éléments est souvent noté $\mathbb{F}_p$).

DÉFINITION 2.3. Soit K un corps de caractéristique 0 (resp. $p > 0$), alors le sous-corps $\tilde{\varphi}_K(\mathbb{Q})$ (resp. $\overline{\varphi}_K(\mathbb{Z}/p\mathbb{Z})$) s'appelle le sous-corps premier de K, il est isomorphe à $\mathbb{Q}$ (resp. $\mathbb{Z}/p\mathbb{Z}$).

PROPOSITION 2.4. *Soit* $u : K \to L$ *un morphisme de corps, alors* K *et* L *ont même caractéristique.*

DÉMONSTRATION. Comme le diagramme

$$\begin{array}{ccc} K & \xrightarrow{u} & L \\ {\scriptstyle\varphi_K}\uparrow & & \nearrow{\scriptstyle\varphi_L} \\ & \mathbb{Z} & \end{array}$$

est commutatif, on voit que $\mathrm{Ker}\varphi_K = \mathrm{Ker}\varphi_L$. □

3. Extensions algébriques.

DÉFINITION 3.1. Soit L/K une extension. Un élément x de L est dit algébrique sur K s'il existe un polynôme $P \in K[X]$, qui ne soit pas le polynôme nul, tel que $P(x) = 0$. Sinon on dit que x est transcendant sur K. L'extension L/K est dite algébrique (on dit aussi que L est algébrique sur K) si tout élément de L est algébrique sur K.

Soient, comme dans la définition, L/K une extension et x un élément de L. L'ensemble I_x des polynômes $P \in K[X]$ tels que $P(x) = 0$ est un idéal de l'anneau des polynômes $K[X]$, c'est un idéal principal car l'anneau $K[X]$ est principal. On a $I_x = \{0\}$ dans le cas où x est transcendant sur K. Si $I_x \neq 0$, parmi tous ses générateurs, il en existe un qui est un polynôme unitaire, c'est à dire un polynôme dont le coefficient du terme de plus haut degré (appelé aussi coefficient dominant) est égal à 1.

DÉFINITION 3.2. Soient L/K une extension et x un élément de L, algébrique sur K. On désigne par $\mathrm{irr}(x, K; X)$ le générateur unitaire de

$$I_x = \{P \in K[X] \ / \ P(x) = 0\}.$$

Le polynôme $\mathrm{irr}(x, K; X)$ s'appelle le polynôme minimal de x sur K.

THÉORÈME 3.3. *Soit L/K une extension et soit $x \in L$.*
(i) Alors x est algébrique sur K si et seulement si l'extension $K(x)/K$ est finie (donc si et seulement si $[K(x) : K]$ est fini).
(ii) Supposons x algébrique sur K, alors $\mathrm{irr}(x, K; X)$ est un élément irréductible de $K[X]$, $[K(x) : K] = \deg \mathrm{irr}(x, K; X)$ et $K[x] = K(x)$.

DÉMONSTRATION. Supposons que x soit algébrique sur K, soit $\varphi : K[X] \to L$ l'application qui à tout $P \in K[X]$ associe $P(x)$. C'est un morphisme d'anneaux unitaires et, clairement, l'image de φ est le sous-anneau $K[x]$ de L. Le noyau de φ est, par définition, l'idéal $(\mathrm{irr}(x, K; X))$ de $K[X]$. On a donc l'isomorphisme (canonique) d'anneaux

$$\frac{K[X]}{(\mathrm{irr}(x, K; X))} \simeq K[x].$$

Ceci prouve que l'idéal $(\mathrm{irr}(x, K; X))$ est premier (car l'image de φ est intègre), donc que le polynôme $\mathrm{irr}(x, K; X)$ est irréductible, par suite que $K[X]/(\mathrm{irr}(x, K; X))$ est un corps. Par conséquent $K[x]$ est

un corps. Enfin, la division euclidienne montre que pour tout élément P de $K[X]$ il existe un unique $R \in K[X]$ tel que

$$\deg R < \deg \mathrm{irr}(x, K; X) \text{ et } P - R \in (\mathrm{irr}(x, K; X))$$

(on fait la convention $\deg 0 = -\infty$). Soit d le degré de $\mathrm{irr}(x, K; X)$, ce qui précède montre que l'image canonique de $\{1, X, X^2, \cdots, X^{d-1}\}$ dans le quotient $K[X]/(\mathrm{irr}(x, K; X))$ en est une base sur K.

Il reste à prouver la réciproque de (i). Supposons l'extension $K(x)/K$ finie et posons $d = [K(x) : K]$. Alors la famille $\{1, x, \cdots, x^{d-1}, x^d\}$ est liée sur K, puisqu'elle possède $d+1$ éléments distincts, donc il existe $a_0, a_1, \cdots, a_d$ appartenant à K, non tous nuls, tels que

$$\sum_{0 \leq i \leq d} a_i x^i = 0,$$

par conséquent, x est algébrique sur K. □

REMARQUE 3.4. Soient L/K une extension et $x \in L$ algébrique sur K. On a mis en évidence dans cette démonstration le morphisme $\varphi : K[X] \to L$, qui à tout $P \in K[X]$ associe $P(x)$, et l'isomorphisme

$$\frac{K[X]}{(\mathrm{irr}(x, K; X))} \simeq K(x) = K[x]$$

qui s'en déduit. Ils sont intéressants en soi et nous seront utiles d'autres fois. Il résulte aussi de la démonstration que $\{1, x, x^2, \cdots, x^{d-1}\}$ est une K-base de $K(x)$.

Le théorème 3.3 admet plusieurs conséquences, que nous regroupons en le corollaire suivant.

COROLLAIRE 3.5. *Soit L/K une extension de corps.*
(i) Soit M une partie de L formée d'éléments algébriques sur K, alors l'extension $K(M)/K$ est algébrique et l'on a $K[M] = K(M)$; si de plus M est finie, alors $K(M)/K$ est une extension finie.
(ii) Soit E l'ensemble des éléments de L algébriques sur K, alors E est un sous-corps de L (c'est une extension algébrique de K).
(iii) Soit E un corps intermédiaire entre K et L (on a donc les inclusions entre corps et sous-corps $K \subset E \subset L$), alors l'extension L/K est algébrique si et seulement si les deux extensions L/E et E/K le sont.
(iv) Supposons que L/K soit une extension finie, alors c'est une extension algébrique.

DÉMONSTRATION. (i) Soit $x \in K(M)$. Par définition de $K(M)$ (voir aussi la proposition 1.9) il existe des éléments $y_1, \cdots, y_d$ de M, en nombre fini, tels que $x \in K(y_1, \cdots, y_d)$. Alors chaque y_i, $1 \leq i \leq d$, est algébrique sur K, donc à plus forte raison sur $K(y_1, \cdots, y_{i-1})$, $2 \leq i \leq d$. Il vient en itérant 1.5 que l'extension $K(y_1, \cdots, y_d)/K$ est finie, par suite que $K(x)$ est un K -espace vectoriel de dimension finie (car c'est un sous-K espace vectoriel de $K(y_1, \cdots, y_d)$), ce qui prouve que x

algébrique sur K. On a $K[M] = K(M)$, en effet, soit $x \in K[M]$, $x \neq 0$, comme $K[x] = K(x)$ on a $x^{-1} \in K[M]$, donc $K[M]$ est un corps. Enfin, si M est finie, $M = \{y_1, \cdots, y_d\}$, les arguments précédents montrent que $K(M)/K$ est finie.

(ii) D'après (i), $K(E)/K$ est une extension algébrique, donc $K(E) \subset E$, dont il résulte $K(E) = E$.

(iii) Si L/K est algébrique. Alors les éléments de L sont algébriques sur E, puisqu'ils annulent des polynômes non nuls à coefficients dans K, donc dans E. Les éléments de E sont aussi des éléments de L, donc sont algébriques sur K.

Si L/E et E/K sont algébriques. Soit $x \in L$ et soit $\mathrm{irr}(x, E, X) = X^d + a_1 X^{d-1} + \cdots + a_d$, avec donc $a_1, \cdots, a_d$ dans E. Considérons les extensions

$$K \subset K(a_1, \cdots, a_d) \subset K(x, a_1, \cdots, a_d).$$

Comme les a_i sont dans E, ils sont algébriques sur K, donc $K(a_1, \cdots, a_d)/K$ est une extension finie (cf. (i) de ce corollaire). De plus , x est algébrique sur $K(a_1, \cdots, a_d)$, par définition des a_i, donc $K(x, a_1, \cdots, a_d)/K(a_1, \cdots, a_d)$ est aussi une extension finie (cf. le théorème 3.3). Ainsi $K(x, a_1, \cdots, a_d)/K$ est une extension finie, donc $K(x)/K$, qui en est une sous-extension, est finie et on applique encore le théorème.

(iv) Soit $x \in L$. Comme $K(x)$ est un sous-K-espace vectoriel de L, il est de dimension finie. □

4. Corps de ruptures.

L'objet de ce paragraphe est de démontrer le théorème suivant.

THÉORÈME 4.1. *Soient K un corps et $P(X)$ un élément de $K[X]$ n'appartenant pas à K. Alors il existe une extension L de K dans laquelle P admet une racine.*

DÉMONSTRATION. On peut supposer $P(X)$ irréductible dans $K[X]$, quitte à le remplacer par l'un de ses diviseurs. Soit

$$s : K[X] \to E = \frac{K[X]}{(P(X))}$$

la surjection canonique de $K[X]$ sur son quotient E par l'idéal $(P(X))$. Soit σ la restriction de s à K, soit $P^\sigma(T) \in E[T]$ le polynôme obtenu à partir de P par l'action de σ sur ses coefficients [1]. Le polynôme P^σ a une racine dans E car

$$P^\sigma(s(X)) = s(P(X)) = 0,$$

mais $\sigma : K \hookrightarrow E$ n'est pas une inclusion, E n'est pas une extension de K.

[1] On a $\sigma : K \to E$, si $P(X) = \sum_{1 \leq i \leq d} a_i X^i \in K[X]$ alors $P^\sigma(X) = \sum_{1 \leq i \leq d} \sigma(a_i) X^i \in E[X]$. Nous utiliserons plusieurs fois cette notation.

Construisons une extension L de K qui soit isomorphe à E et dans laquelle P a une racine. Selon le lemme suivant, il existe un ensemble F qui est disjoint de K et en bijection avec $E - \sigma(K)$, le complémentaire de $\sigma(K)$ dans E. Soit $\varphi : F \to (E - \sigma(K))$ cette dernière bijection et soit $L = K \cup F$. L'ensemble L est en bijection avec E par l'application ψ ainsi définie : soit $x \in L$, on pose $\psi(x) = \sigma(x)$ si $x \in K$ et $\psi(x) = \varphi(x)$ si $x \in F$. On fait de L un corps, extension de K, par transport de structure, c'est à dire par les lois : pour tous $x, y \in L$

$$x + y = \psi^{-1}(\psi(x) + \psi(y)),$$

$$x \cdot y = \psi^{-1}(\psi(x) \cdot \psi(y)).$$

Alors $\psi^{-1}(s(X))$ est une racine de P dans L. □

LEMME 4.2. *Soient A et B deux ensembles, alors il existe un ensemble C disjoint de A et en bijection avec B.*

DÉMONSTRATION. La démonstration donnée ici nous a été communiquée par notre collègue Anne BAUVAL. Désignons par Z la réunion des ensembles qui sont des éléments de A et soit X l'ensemble des éléments u de Z qui n'admettent pas eux-même comme élément :

$$X = \{u \in Z \ / \ u \notin u\}.$$

Montrons $X \notin Z$. En effet, on a pour tout $u \in Z$

$$u \in X \iff u \notin u,$$

donc si $X \in Z$, on aurait

$$X \in X \iff X \notin X$$

ce qui est faux.

Soit $C = \{\{X, b\} \ / \ b \in B\}$. Il est clair que C est en bijection avec B. Il reste à prouver que $C \cap A = \emptyset$: s'il existe $b \in B$ tel que $\{X, b\} \in A$, alors, par définition de Z, on a $\{X, b\} \subset Z$, donc $X \in Z$, ce qui est faux. □

DÉFINITION 4.3. Soient K un corps et $P(X)$ un élément de $K[X]$ n'appartenant pas à K. Une extension algébrique L de K dans laquelle $P(X)$ possède une racine s'appelle un corps de rupture sur K de $P(X)$.

REMARQUE 4.4. Soient K un corps et $P(X)$ un élément de $K[X]$ n'appartenant pas à K. Le théorème 4.1 prouve donc que $P(X)$ possède toujours un corps de rupture L sur K, la démonstration ainsi que 3.4 montrent, lorsque $P(X)$ est irréductible sur K, que l'on peut choisir ce corps de rupture L et une racine x de $P(X)$ dans L tels que

$$L = K(x) \simeq \frac{K[X]}{(P(X))},$$

l'isomorphisme associant x à la classe de X.

5. Clôtures algébriques.

PROPOSITION 5.1. *Soit K un corps, les assertions suivantes sont équivalentes.*
(i) Tout élément de $K[X]$ qui n'est pas dans K admet une racine dans K.
(ii) Tout élément de $K[X]$ qui n'est pas dans K se décompose en un produit de polynômes du premier degré, autrement dit, les éléments irréductibles de $K[X]$ sont les polynômes du premier degré.
(iii) Le corps K n'admet pas d'extension algébrique non triviale (c'est à dire distincte de lui-même).

DÉMONSTRATION. (i) implique (ii). Soit $P(X) \in K[X]$ un polynôme non constant. Il possède une racine α dans K, donc il s'écrit $P(X) = (X - \alpha)Q(X)$ avec $Q(X) \in K[X]$. On a $\deg Q = \deg P - 1$. Par récurrence sur le degré de $P(X)$ on prouve donc (ii).

(ii) implique (iii). Soient L/K une extension algébrique, $x \in L$ et $P(X) = \mathrm{irr}(x, K; X)$. D'après (ii), $P(X)$ s'écrit dans $K[X]$ sous la forme $K[X] = \prod_{1 \leq i \leq d}(X - x_i)$, avec $x_i \in K$ et $d = \deg P$. Les racines de $P(X)$ dans L sont encore les x_i, $1 \leq i \leq d$, x est l'une de ces racines et est donc dans K. Ceci implique $d = 1$.

(iii) implique (i). Soit $P(X) \in K[X]$ un polynôme non constant. Soit L un corps de rupture de $P(X)$ sur K (cf. 4.1 et 4.3). On a d'après (iii) $L = K$, donc $P(X)$ possède une racine dans K. □

Cette proposition conduit à la définition

DÉFINITION 5.2. Un corps K vérifiant l'une des assertions de la proposition 5.1 est dit algébriquement clos.

EXEMPLE 5.3. Le corps des nombres complexes $\mathbb{C}$ est algébriquement clos. les corps des rationnels $\mathbb{Q}$ et des réels $\mathbb{R}$ ne sont pas algébriquement clos, de même les corps finis (si $\mathbb{F}$ est un corps fini, alors le polynôme $1 + \prod_{\lambda \in \mathbb{F}}(X - \lambda)$ n'a pas de racine dans $\mathbb{F}$).

La suite de ce paragraphe consiste à prouver que pour tout corps K, "il existe un plus petit corps Ω algébriquement clos, le contenant et unique pour ces propriétés". Cette formulation est imprécise, mais l'idée s'énonce rigoureusement comme suit.

DÉFINITION 5.4. Soit K un corps, on appelle clôture algébrique de K tout corps Ω qui est une extension algébrique de K et qui est aussi algébriquement clos.

THÉORÈME 5.5. *Soit K un corps.*
(i) Le corps K possède une clôture algébrique.
(ii) Soit Ω une clôture algébrique de K, alors pour tout morphisme $\sigma : K \to L$, où L est un corps algébriquement clos, il existe un morphisme $\tau : \Omega \to L$ qui prolonge σ.
(iii) Deux clôtures algébriques de K sont K-isomorphes.

La démonstration se fait en plusieurs étapes.

LEMME 5.6. *Soit K un corps, alors il existe une extension L de K dans laquelle tout élément P de $K[X]$, $P \notin K$, possède une racine.*

DÉMONSTRATION. Elle est due à Emil ARTIN. Soit

$$\mathfrak{K} = K[X_P \ / \ P \in K[X] - K],$$

c'est à dire que $\mathfrak{K}$ est l'anneau des polynômes à coefficients dans K et en les indéterminées $\{X_P\}$ indexées sur l'ensemble des P de $K[X]$ non constants, on peut le voir comme une réunion d'anneaux de polynômes à un nombre fini de variables :

$$\mathfrak{K} = \bigcup_{F \subset \{X_P\}_{P \in K[X]-K}, F fini} K[X_P \ / \ P \in F].$$

Soit $\mathfrak{I}$ l'idéal de $\mathfrak{K}$ engendré par $\{P(X_P) \ / P \in K[X] - K\}$.

Montrons $\mathfrak{I} \neq \mathfrak{K}$. Sinon, il existe une relation du type

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

avec les Q_i dans $\mathfrak{K}$. Cette relation ne fait intervenir qu'un nombre fini d'indéterminées que l'on note $T_1, \cdots, T_n$, avec $T_i = X_{P_i}$ pour $1 \leq i \leq r$, elle s'écrit donc dans $K[T_1, \cdots, T_n]$

$$(*) \qquad \sum_{1 \leq i \leq r} Q_i(T_1, \cdots, T_n) P_i(T_i) = 1.$$

Soit E une extension de K dans laquelle chaque P_i a une racine, notée α_i, $1 \leq i \leq r$ (cf. 4.1, c'est à dire que l'on considère une extension E_1 de K dans laquelle P_1 a une racine, puis une extension E_2 de E_1 dans laquelle P_2 a une racine... ; avec ces notations on prend $E = E_r$). Soit $\varphi : K[T_1, \cdots, T_n] \to E$ le morphisme de K-algèbres qui à T_i associe α_i. En appliquant φ à $(*)$ il vient $1 = 0$ dans E, ce qui est faux. Par conséquent $\mathfrak{I} \neq \mathfrak{K}$.

Comme $\mathfrak{I} \neq \mathfrak{K}$, il existe un idéal maximal $\mathfrak{M}$ de $\mathfrak{K}$ contenant $\mathfrak{I}$. Soient $E = \mathfrak{K}/\mathfrak{M}$ et $s : \mathfrak{K} \to E$ la surjection canonique, notons σ la restriction de s à K. Soit P un polynôme non constant à coefficient dans K. On a $0 = s(P(X_P) = P^\sigma(s(X_P))$ (la notation P^σ est expliquée dans la note de bas de page suivant la démonstration de 4.1), donc P^σ a une racine dans le corps E, quel que soit P. Il suffit alors de répéter la fin de la démonstration de 4.1 pour obtenir un corps L (isomorphe à E), extension de K et dans lequel tout élément non constant de $K[X]$ a une racine. □

LEMME 5.7. *Soit K un corps, alors il existe un corps L qui est une extension algébrique de K et un corps algébriquement clos.*

DÉMONSTRATION. Soit L_1 une extension de K dans laquelle tout élément non constant de $K[X]$ a une racine (cf. le lemme précédent), de même soit L_2 une extension de L_1 dans la quelle les polynômes non

constants de $L_1[X]$ ont une racine... On construit ainsi, par récurrence, une suite $(L_n)_{n\in\mathbb{N}}$ de corps tels que $L_0 = K$ et que L_{n+1} soit une extension de L_n dans laquelle tous les éléments non constants de $L_n[X]$ ont une racine. Soit $L_\infty = \cup_{n\in\mathbb{N}} L_n$, c'est une extension de K. Désignons par L l'ensemble des éléments de L_∞ algébriques sur K, c'est une extension algébrique de K (cf. (ii) de 3.5). Montrons que L est algébriquement clos. Soit $P(X) = a_0 + a_1X + \cdots + a_dx^d \in L[X]$ un polynôme non constant (avec donc les a_i dans L). Les a_i sont dans L_∞, donc il existe $n \in \mathbb{N}$ tel que $P(X) \in L_n[X]$, par suite $P(X)$ a une racine dans L_{n+1}, donc dans L_∞, que l'on appelle α. Les deux extensions

$$K \subset K(a_0, a_1, \cdots, a_d) \subset K(\alpha, a_0, a_1, \cdots, a_d)$$

sont algébriques, la première car les a_i sont dans L, la seconde parce que α est racine de $P(X) \in K(a_0, a_1, \cdots, a_d)[X]$, donc α est algébrique sur K (cf. (iii) de 3.5). Par conséquent α est dans L_∞ et est algébrique sur K, il est donc dans L. Ceci prouve que L est algébriquement clos (cf. (i) de 5.1). □

Nous avons donc montré la partie (i) du théorème 5.5, la fin de la démonstration nécessite le résultat important suivant.

PROPOSITION 5.8. *Soient E/K une extension algébrique et $\sigma : K \to L$ un morphisme dans le corps algébriquement clos L. Alors il existe un prolongement $\tau : E \to L$ de σ à E.*

DÉMONSTRATION. Soit $\mathcal{S}$ l'ensemble des couples (F, τ) tels que F soit un corps intermédiaire entre K et E et que τ prolonge σ à F.
- L'ensemble $\mathcal{S}$ est non vide car $(K, \sigma) \in \mathcal{S}$.
- Pour des éléments de $\mathcal{S}$, on écrit $(F, \tau) < (F', \tau')$ si $F \subset F'$ et si τ' prolonge τ à F'. Ceci est un ordre sur $\mathcal{S}$.

Pour cet ordre $\mathcal{S}$ est inductif. En effet, soit $((F_n, \tau_n))_{n\in\mathbb{N}}$ une suite croissante d'éléments de $\mathcal{S}$, alors sa borne supérieure est l'élément $(F_\infty = \cup_{n\in\mathbb{N}} F_n, \tau_\infty)$ de $\mathcal{S}$, où τ_∞ est défini par la relation : pour tout $n \in \mathbb{N}$ la restriction de τ_∞ à F_n est τ_n.

Donc $\mathcal{S}$ est inductif et non vide, par suite, d'après le lemme de ZORN, il possède un élément maximal, que l'on note (F, τ). Il reste à prouver que $F = E$, c'est une conséquence de la maximalité de (F, τ) et du lemme suivant appliqué à l'extension $F(x)/F$, pour un éventuel élément x de $E - F$. □

LEMME 5.9. *Soit $\tau : F \to L$ un morphisme d'un corps F dans un corps algébriquement clos L. Soit E/F une extension et $x \in E$ algébrique sur F. Alors τ admet un prolongement à $F(x)$.*

DÉMONSTRATION. Soit $P(X) = \mathrm{irr}(x, F; X)$ et soit y une racine dans L du polynôme $P^\tau(X)$. Soit

$$\varphi : F[X] \to L$$

le morphisme qui à $Q(X) \in F[X]$ associe $Q^\tau(y)$, son noyau est l'idéal $(P(X))$. Soit

$$\overline{\varphi} : \frac{F[X]}{(P(X))} \to L$$

le morphisme qui s'en déduit, soit aussi

$$\theta : F(x) \simeq \frac{F[X]}{(P(X))}$$

l'isomorphisme de 3.4, alors $\overline{\varphi} \circ \theta$ répond à la question. □

Il ne reste plus qu'à montrer l'assertion (iii) du théorème 5.5. Soient Ω_1 et Ω_2 deux clôtures algébriques de K. D'après (ii) de 5.5 l'inclusion $K \subset \Omega_2$ se prolonge en un K-homomorphisme $\sigma_1 : \Omega_1 \to \Omega_2$, de même $K \subset \Omega_1$ se prolonge en un K-homomorphisme $\sigma_2 : \Omega_2 \to \Omega_1$. le lemme suivant montre que $\sigma_2^{-1} \circ \sigma_1$ est un automorphisme de Ω_1, ce qui permet de conclure.

LEMME 5.10. *Soit L/K une extension algébrique et soit σ un K-endomorphisme de L. Alors σ est un automorphisme.*

DÉMONSTRATION. Il faut montrer que σ est surjectif. Soit $x \in L$ et soit $P(X) = \mathrm{irr}(x, K; X)$. Soit R l'ensemble des racines de P dans L et soit $y \in R$. On a $P(y) = 0$, par suite $P(\sigma(y)) = \sigma(P(y)) = 0$ (la première égalité vient du fait que les coefficients de P sont dans K, donc $P^\sigma = P$). Donc $\sigma(y)$ est une racine de P. Par suite, la restriction de σ à R est une application de R dans lui-même, qui est injective, donc surjective puisque R est fini. Ainsi x est dans l'image de σ. □

La proposition suivante est utile, bien qu'elle ne soit guère plus qu'une remarque.

PROPOSITION 5.11. *Soit L/K une extension, où le corps L est algébriquement clos. Alors L contient une unique clôture algébrique de K, qui est l'ensemble Ω des éléments de L algébriques sur K.*

DÉMONSTRATION. La définition de Ω implique l'unicité. Avec l'assertion (ii) de 3.5 on voit qu'il reste à prouver que Ω est algébriquement clos. Soit $P(X) = a_0 + a_1 X + \cdots + a_d X^d \in \Omega[X]$ un polynôme non constant. Soit α une racine de $P(X)$ dans L. Les deux extensions

$$K \subset K(a_0, a_1, \cdots, a_d) \subset K(\alpha, a_0, a_1, \cdots, a_d)$$

sont algébriques, la première car les a_i sont dans Ω, la seconde parceque α est racine de $P(X) \in K(a_0, a_1, \cdots, a_d)[X]$, donc α est algébrique sur K (cf. (iii) de 3.5), c'est à dire $\alpha \in \Omega$. Ceci prouve que Ω est algébriquement clos (cf. (i) de 5.1). □

EXEMPLE 5.12. Le corps $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$ (nous le démontrerons), c'est un des rares cas aussi explicites. Par exemple, on ne sait pas décrire les clôtures algébriques de $\mathbb{Q}$, même celle contenue dans $\mathbb{C}$.

REMARQUE 5.13. Soient E/K une extension, x un élément de E algébrique sur K et $\sigma : K \to L$ un morphisme dans un corps algébriquement clos. Soit $P(X) = \mathrm{irr}(x, K; X)$. Alors, le nombre de prolongements de σ à $K(x)$ est égal au nombre de racines *distinctes* de P^σ dans L. Plus précisément, un prolongement τ de σ à $K(x)$ est complètement caractérisé par la donnée de $\tau(x)$, qui décrit l'ensemble des racines *distinctes* de P^σ dans L. Ceci se voit dans la démonstration de 5.9, où le choix de y est arbitraire parmi les racines de P^σ dans L. Nous reviendrons plus tard sur ce très important phénomène. Une dernière chose, sur laquelle nous reviendrons aussi, est de remarquer que le nombre de racines distinctes de P^σ dans L peut être strictement plus petit que son degré, bien que P^σ soit irréductible dans $K[X]$. Par exemple, soit p un nombre premier et soit $K = \mathbb{F}_p(T)$ un corps de fractions rationnelles à coefficients dans le corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, alors le polynôme $P(X) = X^p - T \in K[X]$ est irréductible dans $K[X]$ et, dans une clôture algébrique K^{alg} de K, il n'a qu'une seule racine (si $\alpha \in K^{\mathrm{alg}}$ est une racine de P, on a $P(X) = X^p - \alpha^p = (X - \alpha)^p$ dans $K^{\mathrm{alg}}[X]$). Ce phénomène ne se produit pas en caractéristique zéro.

6. Exercices.

EXERCICE 6.1. 1) Montrer que les idéaux d'un corps K sont triviaux, i.e. égaux à $\{0\}$ ou à K.

2) Montrer qu'un morphisme de corps $\varphi : K \to L$ est ou bien nul, ou bien injectif ; dans le deuxième cas, montrer que $\varphi(1_K) = 1_L$.

Solution. 1) Soit I un idéal non nul de K. Alors il existe $x \in I$, $x \neq 0$. Comme K est un corps, x admet un inverse x^{-1}. Il suit que, $\forall y \in K$, on a $y = (xx^{-1})y = x(x^{-1}y) \in I$.

2) La première assertion résulte immédiatement de 1) car $\ker(\varphi)$ est un idéal de K.

Si φ est injectif, $\varphi(1_K) \neq 0$, donc il est inversible dans L. On a $\varphi(1_K) = \varphi(1_K 1_K) = \varphi(1_K)\varphi(1_K)$, donc $\varphi(1_K)^{-1}\varphi(1_K) = \varphi(1_K)$, i.e. $1_L = \varphi(1_K)$.

EXERCICE 6.2. Soit A un anneau. S'il existe un entier $n \in \mathbb{N} \setminus \{0\}$ tel que $\forall a \in A$, $na = 0$, on appelle **la caractéristique de** A le plus petit entier $p > 0$ tel que $\forall a \in A$, $pa = 0$. S'il n'existe pas de tel n, on dit que **la caractéristique de** A est 0. On note $\mathrm{car}(A)$ la caractéristique de A.

Soit A un anneau unitaire.

1) Montrer que $\varphi : \mathbb{Z} \to A$, $n \mapsto n1_A$ est un morphisme d'anneaux.

2) Soit $\ker(\varphi) = p\mathbb{Z}$ (car c'est un idéal de l'anneau $\mathbb{Z}$ d'après 1)), montrer que $\mathrm{car}(A) = p$. En particulier, si $p > 0$, p est le plus petit entier > 0 tel que $p1_A = 0$.

3) Si A n'a pas de diviseurs de zéro (par exemple si A est intègre) et si $\mathrm{car}(A) = p > 0$, alors p est un nombre premier.

4) Quelle est la caractéristique de (i) $\mathbb{Z}$, (ii) $\mathbb{Z}/n\mathbb{Z}$, (iii) $\mathbb{C}$?

Solution. 1) Ceci résulte de $1_A 1_A = 1_A$ et de

$$\varphi(k) = k1_A := \begin{cases} 1_A + \cdots + 1_A \quad (k \text{ fois}), & \text{si } k > 0 \\ 0_A, & \text{si } k = 0 \\ (-1_A) + \cdots + (-1_A) \ (-k \text{ fois}), & \text{si } k < 0 \end{cases}$$

2) Il suffit de remarquer que $n1_A = 0 \Rightarrow \forall a \in A, na = n(1_A a) = (n1_A)a = 0_A a = 0$.

3) Si $p = mn$, alors $0_A = mn1_A = (m1_A)(n1_A)$, donc $m1_A = 0$ ou $n1_A = 0$ (car A n'a pas de diviseur de zéro). D'après 2), on a nécessairement $m = \pm p$ ou $n = \pm p$.

4) On utilise 2). (i) $\mathrm{car}(\mathbb{Z}) = 0$, (ii) $\mathrm{car}(\mathbb{Z}/n\mathbb{Z}) = n$, (iii) $\mathrm{car}(\mathbb{C}) = 0$.

EXERCICE 6.3. Soit K un corps à q éléments et de caractéristique p. Montrer que p est un nombre premier et que q est une puissance de p.

Solution. Avec les notations de l'exercice 6.2 2), on a un morphisme injectif $\mathbb{Z}/p\mathbb{Z} \to K$. Puisque K est fini, on a $p > 0$. Donc p est un nombre premier car $\mathbb{Z}/p\mathbb{Z}$ est intègre (il est isomorphe à un sous-anneau de K) (Remarque : on peut aussi utiliser l'exercice 6.2 3)).

Comme p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps. D'après l'exercice 6.2 2), on a une structure naturelle de $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel sur K définie par $\mathbb{Z}/p\mathbb{Z} \times K \to K$, $(\overline{n}, x) \mapsto nx$. Soit r la dimension, alors $|K| = |\mathbb{Z}/p\mathbb{Z}|^r = p^r$.

EXERCICE 6.4. Soient A un anneau commutatif de caractéristique un nombre premier $p > 0$ et $a, b \in A$.

1) Montrer que $(a + b)^p = a^p + b^p$.

2) Montrer que l'application $F : A \to A$, $a \mapsto a^p$ est un morphisme d'anneaux (appelé **le morphisme de Frobenius**).

Solution. 1) A est commutatif, donc $(a + b)^p = \sum_{0 \le i \le p} C_p^i a^{n-i} b^i$. Puisque p est premier, on a $\mathrm{car}(A) = p \mid C_p^i = \frac{p!}{(p-i)!i!}$ pour tout $1 \le i \le p - 1$ (en effet, $p! = (p-1)!i!C_p^i$ et $p \nmid (p-1)!i!$). On applique ensuite l'exercice 6.2 2).

2) $F(a+b) = (a+b)^p = a^p + b^p = F(a) + F(b)$ d'après 1). $F(ab) = (ab)^p = a^p b^p = F(a)F(b)$ car A est commutatif.

EXERCICE 6.5. Les nombres complexes suivants sont-ils conjugués sur $\mathbb{R}$? sur $\mathbb{Q}$? (a) i et $\sqrt{2}$; (b) $i + \sqrt{2}$ et $i - \sqrt{2}$.

Solution. (a) non ; (b) Sur $\mathbb{R}$: non. Sur $\mathbb{Q}$: oui.

En posant $x = i \pm \sqrt{2}$ et en écrivant $x - i = \pm\sqrt{2}$, on obtient que x est un zéro du polynôme $P(X) = X^4 - 2X^2 + 9$. On peut montrer que $P(X)$ est irréductible dans $\mathbb{Q}[X]$ par deux méthodes différentes (on remarque que le critère d'Eisenstein ne s'applique pas à $P(X)$) :

1) On montre d'abord que $P(X)$ n'a pas de zéro dans $\mathbb{Q}$ en utilisant la propriété suivante : si m/n avec $(m, n) = 1$ est un zéro de $f(X) = a_k X^k + \cdots + a_0 \in \mathbb{Z}$, alors $m|a_0, n|a_k$ (Remarque : cette propriété est encore valable pour un anneaux factoriel au lieu de $\mathbb{Z}$). Ensuite supposons que $P(X) = (X^2 + aX + b)(X^2 + cX + d)$ dans $\mathbb{Q}[X]$, on obtient un système (assez simple) de quatre équations en a, b, c, d. En calculant un peu, on trouve qu'il n'y a pas de solutions dans $\mathbb{Q}$.

2) On a $P(X) = (X - i + \sqrt{2})(X + i + \sqrt{2})(X - i - \sqrt{2})(X + i - \sqrt{2})$. Donc (par le fait que $\mathbb{R}[X]$ est factoriel) $P(X) = (X^2 + 2\sqrt{2}X + 3)(X^2 - 2\sqrt{2}X + 3)$ est l'unique factorisation (non triviale et à constante près) de $P(X)$ dans $\mathbb{R}[X]$. Mais cette dernière n'est pas dans $\mathbb{Q}[X]$, donc $P(X)$ est irréductible dans $\mathbb{Q}[X]$.

EXERCICE 6.6. Soient $x = \sqrt{2}$ et $y = 1 - \sqrt{2}$. Montrer que $\mathbb{Q}(x) = \mathbb{Q}(y)$ et que $\mathrm{irr}(x, \mathbb{Q}) \neq \mathrm{irr}(y, \mathbb{Q})$.

Solution. Facile.

EXERCICE 6.7. Soit F un corps fini à q éléments. Soient K un corps et $f : F \to K$ une application. Montrer que

$$\forall x \in F,\ f(x) = \sum_{a \in F} (f(a)(1 - (x - a)^{q-1})),$$

c'est-à-dire f est polynômiale.

Solution. Si $a \neq x$, $x - a \in F^*$, F^* est un groupe multiplicatif d'ordre $q - 1$, donc $(x - a)^{q-1} = 1$.

EXERCICE 6.8. 1) Soit A un anneau intègre unitaire admettant comme sous-anneau un corps K tel que A soit un K-espace vectoriel de dimension finie. Montrer que A est un corps.

2) Soient L/K une extension algébrique de corps et A un sous-anneau de L contenant K. Montrer que A est un corps. La réciproque ?

Solution. 1) Soit $x \in A$, $x \neq 0$. Alors il existe un entier naturel n minimal tel que $1, x, \ldots, x^n$ soient liés.

Une autre méthode consiste à montrer que l'application $y \mapsto xy$ est K-linéaire et bijective.

2) Soit $x \in A$, $x \neq 0$. On a $K(x) = K[x] \subset A$.

EXERCICE 6.9. Montrer que (i) $[L : K] = 1 \iff L = K$; (ii) Si $[L : K]$ est un nombre premier, alors l'extension L/K n'a pas de sous-extension non triviale.

Solution. Facile.

EXERCICE 6.10. Soient α une racine dans $\mathbb{C}$ de l'équation $x^3+x^2+x+2=0$ et $E=\mathbb{Q}(\alpha)$. Exprimer $(\alpha^2+\alpha+1)(\alpha^2+\alpha)$ et $(\alpha^2-1)^{-1}$ sous la forme $a\alpha^2+b\alpha+c$ avec $a,b,c\in\mathbb{Q}$.

Solution. 1) $\alpha^3=-\alpha^2-\alpha-2$ permet de calculer les polynômials en α.

2) Pour $(\alpha^2-1)^{-1}$, il y a un algorithme :

On montre que $P(X)=X^3+X^2+X+2$ n'a pas zéro dans $\mathbb{Q}$, donc irréductible. On pose $Q(X)=X^2-1$, alors $(P(X),Q(X))=1$. Utilisons la division euclidienne (algorithme d'Euclide) pour trouver $A(X),B(X)$ tels que $A(X)P(X)+B(X)Q(X)=1$, alors $Q(x)^{-1}=B(x)$.

Une autre méthode consiste à chercher par calcul direct a,b,c tels que $(a\alpha^2+b\alpha+c)(\alpha^2-1)=1$.

EXERCICE 6.11. Trouver tous les sous-corps intermédiaires de l'extension $\mathbb{Q}(\sqrt[4]{7})$ de $\mathbb{Q}$. (**Remarque.** On pourra refaire cet exercice avec le théorème fondamental de la théorie de Galois.)

Solution. Soit K un corps intermédiaire non trivial. Puisque $[Q(\sqrt[4]{7}) : \mathbb{Q}]=4$ (critère d'Eisenstein par exemple), on a $[Q(\sqrt[4]{7}) : K]=2$. Donc $P(X)=\mathrm{irr}(\sqrt[4]{7},K;X)$ est un polynôme de degré 2 et divise X^4-7 dans $K[X]\subset\mathbb{R}[X]$, d'où nécessairement $P(X)=X^2-\sqrt{7}$. Ce qui donne $\sqrt{7}\in K$, et finalement $K=\mathbb{Q}(\sqrt{2})$.

Remarque. Une autre méthode consiste à utiliser $[K:\mathbb{Q}]=2$ et la base $\{1,\sqrt[4]{7},(\sqrt[4]{7})^2,(\sqrt[4]{7})^3\}$, mais le calcul est plus long.

EXERCICE 6.12. Soit $X^n-a\in K[X]$ irréductible et u une racine dans une extension de K. Soit $m|n$. Montrer que $[K(u^m) : K]=\frac{n}{m}$. Quel est le polynôme irréductible de u^m sur K ?

Solution. $P(X)=\mathrm{irr}(u^m,K;X)$ divise $X^{\frac{n}{m}}-a$ implique que $\mathrm{irr}(u,K;X)$ divise $P(X^{\frac{n}{m}})$. D'où les égalités en comparant les degrés.

EXERCICE 6.13. 1) Montrer que $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$. En déduire $\mathrm{irr}(\sqrt{2}+\sqrt{3},\mathbb{Q})$.

2) Déterminer $\mathrm{irr}(\sqrt{2}+\sqrt{3},\mathbb{Q})$. En déduire que $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

3) Déterminer l'ensemble des sous-corps intermédiaires de $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$.

4) Déterminer le polynôme irréductible de $\sqrt{2}+\sqrt{3}+\sqrt{5}$ sur $\mathbb{Q}$.

Remarque. On pourra aussi utiliser la notion de degré de séparabilité ou, de manière équivalente, le théorème fondamental de la théorie de Galois ; refaire cette exercice quand vous disposerez de ces notions.

Solution. 1) Il suffit de remarquer que $\sqrt{2}-\sqrt{3}=-\frac{1}{\sqrt{2}+\sqrt{3}}$ pour avoir l'égalité. On en déduit que le polynôme irréductible cherché est de degré 4. Soit $\alpha=\sqrt{2}+\sqrt{3}$, on a $(\alpha-\sqrt{2})^2=3$, on trouve finalement que α est racine de X^4-10X^2+1.

2) Comme dans la deuxième moitié de 1), on trouve le polynôme de degré 4. Ensuite on montre qu'il est irréductible (standard comme dans l'exercice 1.1). L'égalité résulte de degré sur $\mathbb{Q}$

3) (cf. exercice 1.6) On montre que le polynôme irréductible de $\sqrt{2}+\sqrt{3}$ sur un sous-corps intermédiaire K non trivial est un facteur de degré 2 dans $K[X]$. Il est de la forme $(X-a)(X-b)$ avec $a,b\in\{\pm\sqrt{2}\pm\sqrt{3}\}$. On en déduit que $\sqrt{2}\in K$, $\sqrt{3}\in K$, $\sqrt{6}\in K$.

4) Comme dans 1), on calcule un polynôme de degré 8 dont $\sqrt{2}+\sqrt{3}+\sqrt{5}$ est une racine. Il suffit alors de monter que $\sqrt{5}\notin\sqrt{2}+\sqrt{3}$, cela résulte de 3).

Exercice 6.14. Soient $p>2$ un nombre premier et $\xi=e^{\frac{2i\pi}{p}}$.

1) Vérifier que ξ est une racine de $P(X)=X^{p-1}+X^{p-2}+\cdots+1$ et montrer que $P(X)$ est irréductible sur $\mathbb{Q}$. En déduire $[\mathbb{Q}(\xi):\mathbb{Q}]$.

2) On pose $\alpha=\cos\frac{2\pi}{p}$.

a) Vérifier que $\mathbb{Q}(\alpha)\subset\mathbb{Q}(\xi)$ et $\mathbb{Q}(\alpha)\neq\mathbb{Q}(\xi)$.

b) Montrer que ξ est une racine de $X^2-2\alpha X+1$. Déterminer $[\mathbb{Q}(\xi):\mathbb{Q}(\alpha)]$ et $[\mathbb{Q}(\alpha):\mathbb{Q}]$.

3) On pose $p=5$.

a) Calculer $\mathrm{irr}(\alpha,\mathbb{Q})$. En déduire que $\cos\frac{2\pi}{5}=\frac{\sqrt{5}-1}{4}$.

b) Calculer $\mathrm{irr}(\xi,\mathbb{Q}(i))$ et $\mathrm{irr}(\xi,\mathbb{Q}(\sqrt{5}))$.

Solution. 1) $X^p-1=(X-1)(X^{p-1}+X^{p-2}+\cdots+1)$, changement de variable $Y=X-1$, ensuite critère d'Eisenstein.

2)a) $\alpha=\frac{1}{2}(\xi+\overline{\xi})=\frac{1}{2}(\xi+\frac{1}{\xi})$; $\alpha\in\mathbb{R}$, $\xi\notin\mathbb{R}$.

b) $\xi+\overline{\xi}=2\alpha$ et $\xi\overline{\xi}=1$. $\mathbb{Q}[\xi]:\mathbb{Q}(\alpha)]=2$ et $[\mathbb{Q}(\alpha):\mathbb{Q}]=\frac{p-1}{2}$.

3)a) $p=5$. On remarque que $\xi^4=\overline{\xi}$ et $\xi^3=\overline{\xi^2}$, d'où $2\alpha+2(2\alpha^2-1)+1=0$. Avec b), on a $\mathrm{irr}(\alpha,\mathbb{Q};X)=X^2+\frac{1}{2}X-\frac{1}{4}$.

b) Chaque racine de $P(X)=X^4+X^3+X^2+X+1$ dans $\mathbb{C}$ est primitive, donc si $\mathbb{Q}(i)$ contient une racine de $P(X)$, il contient alors ξ, mais $\sqrt{5}\notin\mathbb{Q}(i)$. Donc si $P(X)=(X-\xi)(X-\xi^2)(X-\xi^3)(X-\xi^4)$ est réductible sur $\mathbb{Q}(i)$, il est produit de deux facteurs de degré 2 dans $\mathbb{Q}(i)[X]$. Utiliser la somme ou le produit de deux racines de $P(X)$ pour conclure que $P(X)$ est irréductible dans $\mathbb{Q}(i)[X]$.

Sur $\mathbb{Q}(\sqrt{5})$, on utilise 3)a) et 2)b). On a donc $\mathrm{irr}(\xi, \mathbb{Q}(\sqrt{5}) = X^2 - \frac{\sqrt{5}-1}{2}X + 1$.

EXERCICE 6.15. Soient K une extension d'un corps F et $a \in K$ tel que $[F(a) : F]$ soit impair. Montrer que $F(a) = F(a^2)$. Donner un contre exemple avec $[F(a) : F]$ pair.

Solution. $[F(a) : F] = [F(a) : F(a^2)][F(a^2) : F]$. Contre exemple : $\mathbb{Q}(\sqrt[4]{2})$.

EXERCICE 6.16. Soient α et β deux éléments d'une extension algébrique L d'un corps K. Montrer que si les degrés de $\mathrm{irr}(\alpha, K)$ et de $\mathrm{irr}(\beta, K)$ sont premiers entre eux, $\mathrm{irr}(\alpha, K) = \mathrm{irr}(\alpha, K(\beta))$. En déduire $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]$.

Solution. Voir l'exercice suivant. C'est un cas particulier ici.

EXERCICE 6.17. Soient L/K une extension de corps, E/K et F/K deux extensions intermédiaires de degré fini.

1) Montrer que $E(F)/E$ est finie et que $[E(F) : E] \leq [F : K]$. En déduire que $[E(F) : K] \leq [E : K][F : K]$. Montrer qu'on a égalité si $[E : K]$ et $[F : K]$ sont premiers entre eux.

2) Montrer que si $[E(F) : K] = [E : K][F : K]$, alors $E \cap F = K$.

3) Soient x et y deux racines distinctes de $X^3 - 2$ dans $\mathbb{C}$. Montrer que $[\mathbb{Q}(x, y) : \mathbb{Q}] < [\mathbb{Q}(x) : \mathbb{Q}][\mathbb{Q}(y) : \mathbb{Q}]$ et que $\mathbb{Q}(x) \cap \mathbb{Q}(y) = \mathbb{Q}$.

Solution. 1) Soit $F = Kf_1 \bigoplus \cdots \bigoplus Kf_n$, alors $E(F) = E(f_1, \ldots, f_n) = E[f_1, \ldots, f_n]$. On écrit un élément de $E(F)$ comme une fonction polynômiale en les f_i. On remarque qu'un produit de f_i est dans F, donc $E(F) = Ef_1 \bigoplus \cdots \bigoplus Ef_n$, i.e. $[E(F) : E] \leq [F : K]$. Pour le rest, on utilise $[E(F) : E][E : K] = [F(E) : F][F : K]$.

2)On applique 1) pour $E, F, E \cap F$.

3) $[\mathbb{Q}(x, y) : \mathbb{Q}] = 6 < 9$. Ensuite on montre $\mathbb{Q}(x) \cap \mathbb{Q}(y) = \mathbb{Q}$. Supposons que ce n'est pas vrai, alors $\mathbb{Q}(x) = \mathbb{Q}(x) \cap \mathbb{Q}(y) = \mathbb{Q}(y)$.

EXERCICE 6.18. Soient K un corps, $E = K(X)$, $R = \frac{X^3}{X+1} \in E$ et $F = K(R)$.

1) Montrer que $E = F(X)$ et que $X \notin F$.

2) Montrer que $T^3 - RT - R$ est irréductible dans $F[T]$, en déduire $[E : F]$.

Solution. 1) $\deg(\frac{X^3}{X+1}) = 3 - 1 = 2$, donc un élément de F est de degré pair.

2) Par le critère d'Eisenstein.

EXERCICE 6.19. Montrer que $\mathbb{Q}$ et les corps finis ne sont pas algébriquement clos.

Solution. X^2+1 n'a pas de racine dans $\mathbb{Q}$; Pour un corps fini F, $\prod_{a\in F}(X-a)+1$ n'a pas de racine dans F.

EXERCICE 6.20. (**Théorème de Liouville**) On appelle **nombre algébrique** tout nombre complexe qui est une racine d'un polynôme à coefficients dans $\mathbb{Q}$. Soit α un nombre algébrique réel de degré $n>1$ sur $\mathbb{Q}$. Montrer qu'il existe $c=c(\alpha)>0$ tel que $\mid \alpha-\frac{p}{q}\mid > \frac{c}{q^n}$ pour tout $\frac{p}{q}\in\mathbb{Q}$.
(Indication : Soit $P(\alpha)=0$ avec $\deg(P)=n$ et $P(X)\in\mathbb{Z}[X]$. Utiliser $P(\alpha)-P(\frac{p}{q})=(\alpha-\frac{p}{q})P'(\xi)$.)
Application : On appelle **nombres de Liouville** les nombres de la forme $\alpha=\sum_{k=1}^{\infty}\frac{\alpha_k}{10^{k!}}$ où $\{\alpha_k\}_{k\in\mathbb{N}}$ est une suite de chiffres ne tendant pas vers zéro. Montrer que les nombres de Liouville sont transcendants.

Solution. Avec les notations de l'Indication, on a $\mid \alpha-\frac{p}{q}\mid = \frac{|P(\frac{p}{q})|}{P'(\xi)}$. $P(\frac{p}{q})\neq 0$, donc $P(\frac{p}{q})\geq\frac{1}{q^n}$. Quand $|\alpha-\frac{p}{q}|\leq 1$, on majore $P'(\xi)$ par un $c_1>0$. On pose $c=\min(q^n,c_1)$.

Pour les nombres de Liouville, on montre d'abord $\alpha\notin\mathbb{Q}$ en supposant le contraire et en calculant $\alpha_n=\sum_{k=1}^{n}\frac{\alpha_n}{10^{n!}}$. Ensuite on suppose α algébrique sur $\mathbb{Q}$, et on applique le théorème aux $\dfrac{p_n}{q_n}=\alpha_n=\sum_{k=1}^{n}\dfrac{\alpha_n}{10^{n!}}$

EXERCICE 6.21. Trouver un exemple d'une extension algébrique L/K avec $[L:K]=3$ et pour tout $a\in K$, $L\neq K(\sqrt[3]{a})$ où $\sqrt[3]{a}$ est une racine de X^3-a dans une clôture algébrique de L/K.

Solution. Un exemple : $K=\mathbb{F}_3$, $L=\mathbb{F}_3(x)$ où x est une racine du polynôme irréductible X^3-X+1 de $\mathbb{F}_3[X]$ dans une clôture algébrique de $\mathbb{F}_3$. Il suffit alors de remarquer que $a^3=a$ pour tout $a\in\mathbb{F}_3$.

CHAPITRE 2

Corps de décompositions, extensions normales.

1. Corps de décompositions.

DÉFINITION 1.1. Soient K un corps et $(P_i)_{i\in I}$ une famille d'éléments de $K[X]$. Soit L une extension de K telle que
- pour tout $i \in I$, P_i se décompose dans $L[X]$ en un produit de polynômes du premier degré, c'est à dire

$$P_i(X) = \lambda_i \prod_{1\leq j\leq d_i} (X - a_{i,j})$$

avec $a_{i,j} \in L$ et $\lambda_i \in K$ (ce dernier est le coefficient dominant de P_i),
- le corps L est engendré sur K par les racines des P_i, c'est à dire

$$L = K(\{a_{i,j}\}_{i\in I, 1\leq j\leq d_i}).$$

Alors L s'appelle un corps de décomposition de la famille $(P_i)_{i\in I}$ sur K (lorsqu'il n'y a qu'un seul polynôme P, L est appelé corps de décomposition de P sur K).

REMARQUE 1.2. Soient K un corps et $(P_i)_{i\in I}$ une famille d'éléments de $K[X]$. Dans dans toute extension Ω/K, où Ω est algébriquement clos (en particulier dans toute clôture algébrique de K) il existe un corps de décomposition sur K de la famille $(P_i)_{i\in I}$, c'est le corps engendré sur K par les racines dans Ω des (P_i), $i \in I$. La définition montre ce corps est nécessairement ainsi, par suite qu'il est unique (dans tout corps algébriquement clos Ω, extension de K).

EXERCICE 1.3. Soit K un corps. Montrer qu'une extension L de K est une clôture algébrique de K si et seulement si c'est un corps de décomposition sur K de la famille de tous les éléments non constants de $K[X]$.

La proposition suivante énonce une propriété très forte des corps de décomposition, qui permet de préciser l'unicité énoncée à la remarque 1.2.

PROPOSITION 1.4. *Soient K un corps et $(P_i)_{i\in I}$ une famille d'éléments de $K[X]$.*
(i) Soient L_1 et L_2 deux corps de décomposition de $(P_i)_{i\in I}$ sur K, Ω une extension de L_2 qui est un corps algébriquement clos et $\sigma : L_1 \to \Omega$ un K-homomorphisme. Alors on a $\sigma(L_1) = L_2$, c'est à dire que σ induit un K-isomorphisme entre L_1 et L_2.

(ii) Deux corps de décomposition de $(P_i)_{i\in I}$ sur K sont K-isomorphes.

DÉMONSTRATION. Posons pour $i \in I$

$$P_i(X) = \lambda_i \prod_{1\leq j\leq d_i} (X - a_{i,j})$$

avec $a_{i,j} \in L_1$ et $\lambda_i \in K$. On a dans $\Omega[X]$

$$P_i^\sigma(X) = P_i(X) = \lambda_i \prod_{1\leq j\leq d_i} (X - \sigma(a_{i,j}))$$

et rappelons que L_1 est engendré sur K par les $a_{i,j}$ (cf. 1.1). Ainsi

$$\sigma(L_1) = K(\{\sigma(a_{i,j})\}_{i\in I, 1\leq j\leq d_i},$$

c'est à dire que $\sigma(L_1)$ est engendré sur K par les racines des P_i dans Ω, comme L_2. Ceci prouve (i). L'assertion (ii) en est une conséquence : si L_1 et L_2 sont deux corps de décomposition de $(P_i)_{i\in I}$ sur K, on prend pour Ω une clôture algébrique de L_2 et pour σ un prolongement à L_1 de l'inclusion $K \subset \Omega$ (cf. 5.8). □

Le théorème suivant donne des caractérisations des corps de décomposition.

THÉORÈME 1.5. *Soit L/K une extension algébrique. Les assertions suivantes sont équivalentes.*
- (i) L est un corps de décomposition d'une famille d'éléments de $K[X]$.
- (ii) Pour tout corps Ω algébriquement clos, extension de L, tout K-homomorphisme de L dans Ω induit un K-automorphisme de L.
- (iii) Il existe un corps Ω algébriquement clos, extension de L, tel que tout K-homomorphisme de L dans Ω induise un K-automorphisme de L.
- (vi) Tout polynôme de $K[X]$, irréductible, qui possède une racine dans L, se décompose dans $L[X]$ en un produit de polynômes du premier degré.

DÉMONSTRATION. (i) implique (ii). C'est une conséquence directe de l'assertion (i) de 1.4.

(ii) implique (vi). Soient Ω une clôture algébrique de K contenant L, P un élément irréductible de $K[X]$ et x une racine de P dans L. Soit y une racine de P dans Ω. Des morphismes

$$\frac{K[X]}{(P(X))} \simeq K(x) \text{ et } \frac{K[X]}{(P(X))} \simeq K(y)$$

venant de 3.4, on déduit un K-homomorphisme

$$\sigma : K(x) \simeq K(y) \hookrightarrow \Omega,$$

la seconde application étant une inclusion, et l'on a $\sigma(x) = y$. Soit σ' un prolongement de σ à L. On a d'après (ii) $\sigma(L) = L$, donc $y \in L$. On a montré que toutes les racines de P dans Ω sont en fait dans L. Ceci est (iii).

(vi) implique (i). Pour tout $x \in L$, soit $P_x = \mathrm{irr}(x, K; X)$. Comme chaque P_x a une racine dans L, d'après (iii) il se décompose dans $L[X]$ en un produit de polynômes du premier degré, c'est à dire que si l'on considère une clôture algébrique Ω de K contenant L, toutes les racines des P_x dans Ω sont en fait dans L. De plus il est clair que L est engendré sur K par les racines des P_x, $x \in L$, parce que l'ensemble de ces racines contient tous les éléments de L. Donc L est un corps de décomposition de la famille $(P_x)_{x\in L}$ d'éléments de $K[X]$.

(iii) implique (ii). Soit Ω donné par (ii). Soient Ω' un corps algébriquement clos, extension de L et $\sigma : L \to \Omega'$ un K-homomorphisme. Soient Ω_a et Ω'_a l'ensemble des éléments de Ω et Ω' respectivement algébriques sur L, ce sont des clôtures algébriques de L et de K (cf. 5.11). Soit $\tau : \Omega_a \to \Omega'_a$ un prolongement de σ, c'est un isomorphisme (cf. 5.5). On a $\tau^{-1} \mid L$ qui est un K-homomorphisme de L dans Ω, donc $\tau^{-1}(L) = L$, par suite $\tau(L) = L$, ce qui s'écrit $\sigma(L) = L$. □

2. Extensions normales.

DÉFINITION 2.1. Une extension algébrique L/K satisfaisant l'une des conditions équivalentes du théorème 1.5 est dite normale (ou quasi-galoisienne) On dit aussi que L est normal (ou quasi-galoisien) sur K.

La proposition suivante donne quelques propriétés de ces extensions.

PROPOSITION 2.2. *Soit K un corps.*
(i) Soient L/K et E/L deux extensions (donc $K \subset L \subset E$), alors si le corps E est normal sur K, il est normal sur L.
(ii) Soit E une extension de K. Soit $(L_i)_{i\in I}$ une famille de sous-corps de E, chacun étant une extension normale de K, alors $\bigcap_{i\in I} L_i$ est une extension normale de K.
(iii) Soient L_1 et L_2 deux corps, extensions normales de K, qui sont des sous-corps d'un même troisième corps E, alors le compositum $L_1 \cdot L_2$ est une extension normale de K.

DÉMONSTRATION. (i) Soit Ω un corps algébriquement clos, extension de E et soit $\sigma : E \to \Omega$ un L-homomorphisme, il faut prouver que $\sigma(E) = E$ (cf. (ii) de 1.5), mais ceci est vrai à cause de l'hypothèse, puisque σ est à plus forte raison un K-homomorphisme.

(ii) Posons $F = \bigcap_{i\in I} L_i$. Soit E^{alg} une clôture algébrique de E. Soit P un élément irréductible de $K[X]$ ayant une racine x dans F. Dans $E^{\mathrm{alg}}[X]$ on peut écrire

$$P(X) = \lambda \prod_{1\leq j\leq d} (X - x_i)$$

avec par exemple $x = x_1$. Comme L_i contient x, il contient tous les x_j, $1 \leq j \leq d$ (car L_i/K est normale, cf. (iii) de 1.5). Ceci est vrai pour tout $i \in I$, donc F contient tous les x_i, $1 \leq i \leq d$.

(iii) Soit Ω un corps algébriquement clos, extension de $L_1 \cdot L_2$ et soit $\sigma : L_1 \cdot L_2 \to \Omega$ un K-homomorphisme. Comme L_1/K est normale on a $\sigma(L_1) = L_1$ (cf. (ii) de 1.5), de même pour L_2. Il vient $\sigma(L_1 \cdot L_2) = L_1 \cdot L_2$. □

REMARQUE 2.3. La réciproque de l'assertion (i) de 2.2 est *fausse*, c'est à dire que si l'on a deux extensions

$$K \subset L \subset E$$

avec L/K et E/L normales, alors il peut se faire que E/K ne soit pas normale. Par exemple $\mathbb{Q}(\sqrt{2})$ est une extension normale de $\mathbb{Q}$, car c'est un corps de décomposition sur $\mathbb{Q}$ de $X^2 - 2$, $\mathbb{Q}(\sqrt[4]{2})$ est une extension normale de $\mathbb{Q}(\sqrt{2})$ car c'est un corps de décomposition sur $\mathbb{Q}(\sqrt{2})$ de $X^2 - \sqrt{2}$, mais $\mathbb{Q}(\sqrt[4]{2})$ n'est pas une extension normale de $\mathbb{Q}$.

L'assertion (ii) de 1.5 dit qu'étant donnée une extension normale L/K, tout K- homomorphisme de L dans un corps algébriquement clos le contenant, est en fait un K-automorphisme de L. Cette propriété est au coeur de la théorie de Galois.

DÉFINITION 2.4. Soit L/K une extension normale. Le groupe $\mathrm{End}_K(L)$ (pour la composition des applications) des K-automorphismes de L s'appelle le groupe de Galois de L sur K, on le note $\mathrm{Gal}(L/K)$.

3. Fermetures normales.

PROPOSITION 3.1. *Soit L/K une extension algébrique.*
(i) Soit Ω une extension algébriquement close de K contenant L. Alors il existe un plus petit sous-corps N de Ω contenant L et normal sur K.
(ii) Soient Ω et Ω' deux extensions algébriquement closes de K contenant L, soient N et N' les corps mis en évidence en (i), pour Ω et Ω' respectivement. Alors N et N' sont L-isomorphes.

DÉMONSTRATION. Soit $N = \bigcap E$, où E décrit l'ensemble des sous-corps de Ω tels que $L \subset E$ et E normal sur K. L'ensemble de ces sous-corps est non vide car l'un d'entre eux est la clôture algébrique de K contenue dans Ω (cf. 5.11). D'après l'assertion (ii) de 2.2, l'extension N/K est normale, de plus il est clair que c'est la plus petite contenant L et incluse dans Ω. Ceci prouve (i).

Pour (ii). Soit Ω_a la clôture algébrique de K contenue dans Ω. L'inclusion $L \subset \Omega'$ se prolonge en un L-homomorphisme $\sigma : \Omega_a \to \Omega'$. On vérifie que $\sigma(N)$ est une extension normale de L dans Ω', donc $N' \subset \sigma(N)$, d'autre part $\sigma^{-1}(N')$ est aussi une extension normale de L, dans Ω, donc $N \subset \sigma^{-1}(N')$. □

DÉFINITION 3.2. Soient L/K une extension algébrique et Ω une extension algébriquement close de K contenant L. Le plus petit sous-corps N de Ω contenant L et normal sur K, mis en évidence en 3.1, s'appelle la fermeture normale de L/K dans Ω.

REMARQUE 3.3. Soient K un corps et Ω une extension algébriquement close de K. Un sous-corps de Ω extension de K engendré par *des* racines d'une famille de polynômes irréductibles sur K admet pour fermeture normale dans Ω l'extension de K engendrée par *toutes* les racines de ces polynômes. Cela se dit plus précisément de la manière suivante. Soit $(P_i)_{i\in I}$ une famille d'éléments *irréductibles* de $K[X]$ et désignons par R_i l'ensemble des racines de P_i dans Ω, $i \in I$. Soit A une partie de $\cup_{i\in I} R_i$ rencontrant chacun des R_i et posons $L = K(A)$. Alors la fermeture normale de L/K dans Ω est $N = K(\cup_{i\in I} R_i)$. Cela se voit avec l'assertion (iii) de 1.5 (voir aussi la définition 2.1).

Par exemple, la fermeture normale de l'extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ dans $\mathbb{C}$ est $N = \mathbb{Q}(\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)$.

4. Exercices.

EXERCICE 4.1. Soient K un corps et $P(X) \in K[X]$ de degré $n \geq 1$. Soit L un corps de décomposition de P sur K. Montrer que $[L : K]$ divise $n!$. (**Remarque.** Il est plus facile de montrer que $[L : K] \leq n!$.)

Solution. D'abord pour la remarque : Soit $P(X) = (X-a_1)\cdots(X-a_n)$ avec les a_i dans L (Eventuellement $a_i = a_j$). On note $K_0 = K$, $K_i = K(a_1, \ldots, a_i)$. On a $L = K_n$ et $\mathrm{irr}(a_{i+1}, K_i; X)$ divise $\frac{P(X}{(X-a_1)\cdots(X-a_i)}$.

Pour montrer $[L : K] \mid n!$, on raisonne par récurrence sur le degré n. Il est clair que l'assertion est vraie si $n = 1$. Soit $n \geq 2$. Supposons l'assertion vraie pour les polynômes de degré $\leq n-1$.

1er cas : $P(X)$ est irréductible dans $K[X]$. On a $[K(a_1) : K] = n$, et on applique l'hypoyhèse de récurrence à $\frac{P(X)}{X-a_1} \in K(a_1)[X]$.

2e cas : $P(X) = P_1(X)P_2(X)$ avec $P_1(X), P_2(X) \in K[X]$ de degré respectivement m_1, $m_2 \geq 1$. Soit $E \subset L$ un corps de décomposition de $P_1(X)$. "Hypothèse de récurrence" $\Longrightarrow [E : K] \mid m_1!$ et $[L : E] \mid m_2!$. Enfin, $n = m_1 + m_2$ et $C_n^{m_1} = \frac{n!}{m_1!(n-m_1)!} \in \mathbb{N}$.

EXERCICE 4.2. Montrer qu'une extension de degré deux est normale.

Solution. Soit $[E : K] = 2$. Soit $x \in E, x \notin K$, alors "degré d'extension" $\Longrightarrow E = K(x)$. Soit $\mathrm{irr}(x, K; X) = X^2 + aX + b$. Les deux racines sont x et $-a - x$.

EXERCICE 4.3. On considère le polynôme $P(X) = X^4 - 2X^2 + 9 \in \mathbb{Q}[X]$.

1) Montrer que $P(X)$ est irréductible dans $\mathbb{Q}[X]$.

2) Décomposer $P(X)$ en produit de polynômes de second degré dans $\mathbb{Q}(i)$.

3) Montrer que le corps de décomposition de $P(X)$ dans $\mathbb{C}$ est $K = \mathbb{Q}(i + \sqrt{2})$.

4) On note G le groupe des $\mathbb{Q}$-automorphismes de K.

i) Quel est l'ordre de G ?

ii) Montrer qu'il existe $\varphi \in G \setminus \{id_K\}$ laissant invariant chaque élément de $\mathbb{Q}(i)$. Quel est l'ordre de φ.

iii) Montrer qu'il existe $\psi \in G \setminus \{id_K\}$ laissant invariant chaque élément de $\mathbb{Q}(\sqrt{2})$. Quel est l'ordre de ψ.

iv) Montrer que $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Solution.

EXERCICE 4.4. 1) Soient K un corps, $f \in K[X]$, $p = \deg(f)$ un nombre premier. Supposons que, pour toute extension L de K, si f a une racine dans L, alors f se décompose en produit de facteurs de degré 1 dans $L[X]$. Montrer que f est irréductible dans $K[X]$ ou f a une racine dans K.

2) Montrer que les hypothèses de 1) sont vérifiées dans les cas suivants :

i) $f(X) = X^p - a$, $\mathrm{car}(K) = p$, $a \in K$.

ii) $f(X) = X^p - X - a$, $\mathrm{car}(K) = p$, $a \in K$.

iii) $f(X) = X^p - a$, $\mathrm{car}(K) \neq p$, $a \in K$, et K contient un élément ξ tel que $\xi^p = 1, \xi \neq 1$.

Solution.

EXERCICE 4.5. Soit p un nombre premier. Montrer que $X^p - X + 1$ est un polynôme irréductible sur $\mathbb{F}_p$ et que son corps de décomposition est une extension (séparable) de $\mathbb{F}_p$ de degré p.

Solution.

EXERCICE 4.6. Soit L une extension algébrique d'un corps K.

1) Soit L/K une extension normale. Soient $f \in K[X]$ irréductible et $g, h \in L[X]$ deux facteurs unitaires irréductibles de f. Montrer qu'il existe un K-automorphisme σ de L tel que $\sigma(g) = h$.

2) Donner un contre exemple quand L/K n'est pas normale.

3) Montrer que L est une extension normale de K si et seulement si, pour tout $f \in K[X]$ irréductible, les facteurs irréductibles de f dans $L[X]$ sont de même degré.

Solution.

EXERCICE 4.7. Soit $F = \mathbb{Q}(\sqrt{2}i, \sqrt[4]{2}(1 - i))$.

1) Calculer $[\mathbb{Q}(\sqrt{2}i) : \mathbb{Q}]$ et $[\mathbb{Q}(\sqrt{2}i, \sqrt[4]{2}(1 - i)) : \mathbb{Q}(\sqrt{2}i)]$. Ces extensions sont-elles normales ?

2) On se propose de savoir si $F/\mathbb{Q}$ est normale.

i) Montrer que $P(X) = X^4 + 8$ est irréductible dans $\mathbb{Q}[X]$.

ii) Factoriser $P(X)$ dans $\mathbb{C}[X]$.

iii) En calculant, pour u racine de $P(X)$, $\bar{u}/u$ et $(\bar{u}-u)/2i$, montrer que le corps de décomposition de $P(X)$ dans $\mathbb{C}$ est $E = \mathbb{Q}(\sqrt[4]{2}, i)$.

iv) Calculer $[E : \mathbb{Q}]$ et conclure.

Solution.

EXERCICE 4.8. Pour chacun des polynômes $f \in K[X]$ suivants, on note E un corps de décomposition de f sur K. Déterminer $[E : K]$ et le nombre des K-automorphisme de E.

1) $K = \mathbb{Z}/3\mathbb{Z}$ et $f(X) = X^3 + 2X + 1$.

2) $K = \mathbb{Z}/p\mathbb{Z}$ et $f(X) = X^{p^8} - 1$.

3) $K = \mathrm{Fr}(\mathbb{Z}/3\mathbb{Z}[T])$ et $f(X) = X^3 - T$.

Solution.

EXERCICE 4.9. Soit N la fermeture normale de $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ sur $\mathbb{Q}$ contenue dans $\mathbb{C}$.

1) Déterminer N et calculer $[N : \mathbb{Q}]$.

2) Montrer que $N/\mathbb{Q}(\sqrt{2})$ est normale. Déterminer tous les $\mathbb{Q}(\sqrt{2})$-automorphismes de N ainsi que l'ordre de chacun d'entre eux.

Solution.

CHAPITRE 3

Séparabilité.

1. Le degré de séparabilité.

THÉORÈME 1.1. *Soit L/K une extension algébrique et soient $\sigma : K \to E$, $\tau : K \to F$ des morphismes de K dans deux corps algébriquement clos. Soient S_σ et S_τ l'ensemble des prolongements respectivement de σ et de τ à L. Alors S_σ et S_τ sont en bijection. Il suit que le cardinal de S_σ ne dépend que de l'extension L/K, il ne dépend pas du corps algébriquement clos E choisi pour l'évaluer.*

DÉMONSTRATION. On peut supposer que E (resp. F) est une clôture algébrique de $\sigma(K)$ (resp. $\tau(K)$). En effet, E (resp. F) contient une clôture algébrique de $\sigma(K)$ (resp. $\tau(K)$) et les prolongements de σ (resp. τ) arrivent dans cette clôture algébrique. Soit

$$\sigma(K) \xrightarrow{\sigma^{-1}} K \xrightarrow{\tau} F$$

et soit $u : E \to F$ un prolongement de cette application à E. On a $u(E) = F$ car $u(E)$ est inclus dans F et est algébriquement clos. Ceci permet de définir l'application $S_\sigma \to S_\tau$ qui à α associe $u \circ \alpha$, ainsi que son application réciproque, qui à $\beta \in S_\tau$ associe $u^{-1} \circ \beta$. D'où l'égalité des cardinaux. □

REMARQUE 1.2. Soient L/K une extension algébrique, $\sigma : K \to E$ un morphisme de K dans un corps algébriquement clos E et S_σ l'ensemble des prolongements σ à L, il résulte de 5.8 que S_σ est non vide.

DÉFINITION 1.3. Soit L/K une extension algébrique et soit $\sigma : K \to E$ un morphisme de K dans un corps algébriquement clos. Soit S_σ l'ensemble des prolongements de σ à L. Alors le cardinal de S_σ se note $[L : K]_s$ et s'appelle le degré de séparabilité de L sur K.

PROPOSITION 1.4. *Soient $K \subset L \subset E$ des extensions algébriques, alors $[E : K]_s$ est fini si et seulement si $[E : L]_s$ et $[L : K]_s$ le sont, auquel cas l'on a*

$$[E : K]_s = [E : L]_s [L : K]_s.$$

DÉMONSTRATION. Soit $\sigma : K \to \Omega$ un morphisme de K dans un corps algébriquement clos Ω et soit $S_{L/K,\sigma}$ l'ensemble des prolongement de σ à L. Pour tout τ appartenant à $S_{L/K,\sigma}$, soit $S_{E/L,\tau}$ l'ensemble des

prolongements de τ à E. Soit encore $S_{E/K,\sigma}$ l'ensemble des prolongements de σ à E. On a

$$S_{E/K,\sigma} = \bigcup_{\tau \in S_{L/K,\sigma}} S_{E/L,\tau}$$

et cette réunion est disjointe. Il en résulte la proposition. □

La proposition suivante donne des précisions sur le degré de séparabilité lorsque l'extension L/K est *monogène*, c'est à dire lorsque il existe $x \in L$ tel que $L = K(x)$. Elle est très utile pour les applications.

PROPOSITION 1.5. *Soit $K(x)$ une extension algébrique de K engendrée par un élément.*
(i) Le degré de séparabilité $[K(x) : K]_s$ est égal au nombre de racines distinctes du polynôme $\mathrm{irr}(x, K; X)$ *(racines distinctes dans une clôture algébrique de K).*
(ii) Soit p l'exposant caractéristique de K (cf. §1.2) et soit $n \in \mathbb{N}$ l'entier ainsi défini : si $p = 1$ on a $n = 0$, si $p \geq 2$, alors n est le plus grand entier tel qu'il existe un polynôme $Q(X) \in K[X]$ vérifiant $\mathrm{irr}(x, K; X) = Q(X^{p^n})$. *Alors*

$$[K(x) : K] = p^n [K(x) : K]_s.$$

L'entier p^n ainsi défini s'appelle le degré d'inséparabilité de x sur K.

DÉMONSTRATION. (i) Soit Ω un corps algébriquement clos contenant K et posons $P(X) = \mathrm{irr}(x, K; X)$. Soit $\sigma : K(x) \to \Omega$ un prolongement de l'inclusion $i : K \hookrightarrow \Omega$, alors

$$0 = \sigma(P(x)) = P(\sigma(x)),$$

donc $\sigma(x)$ est une racine de $P(X)$ dans Ω. Inversement, soit $y \in \Omega$ une racine de $P(X)$, alors (cf. 3.4)

$$K(x) \simeq \frac{K[X]}{(P(X))} \simeq K(y) \subset \Omega$$

est un prolongement de $i : K \hookrightarrow \Omega$ à $K(x)$.

La preuve de (ii) nécessite le lemme intermédiaire suivant.

LEMME 1.6. *Soient K un corps de caractéristique p et $P(X)$ un élément irréductible de $K[X]$. Soit Ω un corps algébriquement clos, extension de K.*
(i) Si $p = 0$, alors $P(X)$ n'a que des racines simples dans Ω.
(ii) Si $p \geq 2$, alors $P(X)$ a (au moins) une racine multiple dans Ω si et seulement si son polynôme dérivé est le polynôme nul, auquel cas il existe $Q(X) \in K[X]$ tel que $P(X) = Q(X^p)$.

Montrons le lemme. On vérifie d'abord que $x \in \Omega$ est racine multiple (en fait double) du polynôme P si et seulement si il est racine de P et de P'. En effet si x est racine double, on écrit $P(X) = (X - x)^2 Q(X)$ dans $\Omega[X]$ et il vient $P'(X) = 2(X - x)Q(X) + (X - x)^2 Q'(X)$. Si

$P(X) = (X-x)Q(X)$ dans $\Omega[X]$, on a $P'(X) = Q(X)+(X-x)Q'(X)$, ce qui implique que si x est racine de P', alors il l'est de Q.

Soit x une racine de P dans Ω. Comme P est irréductible, il existe $\lambda \in K^*$ tel que $P(X) = \lambda \mathrm{irr}(x, K; X)$. Supposons que x est racine multiple de P, alors x est racine du polynôme dérivé $\mathrm{irr}(x, K; X)'$, par suite ce dernier est divisible par $\mathrm{irr}(x, K; X)$ (cf. 3.2). Comme

$$\deg \mathrm{irr}(x, K; X) > \deg \mathrm{irr}(x, K; X)',$$

il vient que $\mathrm{irr}(x, K; X)' = 0$. Donc $P' = 0$. Ecrivons $P(X) = \sum_{0\leq i\leq d} a_i X^i$ (avec les a_i dans K), alors la relation $P' = 0$ implique que $ia_i = 0$ pour tout i, donc $a_i = 0$ ou $i = 0$ dans K ($i = 0$ dans K signifie que l'entier i est divisible par la caractéristique p de K). Donc $P(X)$ s'écrit alors $P(X) = \sum_{0\leq i\leq dp^{-1}} a_i X^{pi}$. Inversement, une telle écriture de P montre que sa dérivée est nulle, par suite que toutes ses racines sont aussi des racines de P'.

Le lemme est donc démontré, revenons à la preuve de (ii) de 1.5. Si la caractéristique de K est nulle, le lemme dit que le nombre de racines distinctes de $irr(x, K; X)$ est égal à son degré, d'où, avec (i) : $[K(x) : K] = [K(x) : K]_s$.

Supposons maintenant que la caractéristique de K est $p > 0$, posons $P(X) = \mathrm{irr}(x, K; X)$ et soient n, Q définis dans l'énoncé. Alors $Q' \neq 0$, car grâce au lemme, le contraire contredirait la maximalité de n. De plus, Q est un élément irréductible de $K[X]$, car toute factorisation de Q en donne une de P. Soit Ω un corps algébriquement clos, contenant x et extension de K, on écrit dans $\Omega[X]$

$$Q(X) = \lambda \prod_{1\leq i\leq \delta} (X - x_i)$$

(avec $\lambda \in K$) et, comme Q est irréductible dans K et que son polynôme dérivé est non nul, les x_i sont deux à deux distincts. Pour $1 \leq i \leq \delta$, soit $y_i \in \Omega$ tel que $y_i^{p^n} = x_i$ (on peut remarquer que y_i est unique car dans $\Omega[X]$: $X^{p^n} - x_i = X^{p^n} - y_i^{p^n} = (X - y_i)^{p^n}$). On a

$$P(X) = Q(X^{p^n}) = \lambda \prod_{1\leq i\leq \delta} (X^{p^n}-x_i) = \lambda \prod_{1\leq i\leq \delta} (X^{p^n}-y_i^{p^n}) = \lambda \prod_{1\leq i\leq \delta} (X-y_i)^{p^n}.$$

Ainsi les racines distinctes de P dans Ω sont les $y_1, \cdots, y_\delta$, elles sont au nombre de δ, et l'on a

$$\deg(\mathrm{irr}(x, K; X)) = \deg(P(X)) = p^n\delta = p^n[K(x) : K]_s,$$

la dernière égalité venant de (i). Ceci est la formule cherchée □

Remarque 1.7. Quelques propriétés importantes sont apparues dans la démonstration précédente, nous les rappelons. Soient K un corps d'exposant caractéristique p et P un élément de $K[X]$, irréductible. Soient $n \in \mathbb{N}$ et $Q \in K[X]$ donnés par la proposition 1.5. Alors

$P(X) = Q(X^{p^n})$, le polynôme dérivé de Q étant non nul, ou, ce qui revient au même, le polynôme Q n'ayant dans une (ou dans toute) clôture algébrique K^{alg} de K que des racines simples (on dira, avec la définition suivante, qu'un tel polynôme est *séparable*). De plus si $x_1, \cdots, x_\delta$ sont les racines de Q dans K^{alg}, si $y_1, \cdots, y_\delta$ sont des éléments de K^{alg} tels que $y_i^{p^n} = x_i$, alors les y_i, $1 \leq i \leq \delta$, sont les racines distinctes de P, toutes de même multiplicité p^n (rappelons que P est irréductible dans $K[X]$ et que les notations sont celles de 1.5).

DÉFINITION 1.8. Soient K un corps et P un polynôme à coefficient dans K. On dit que P est séparable si, dans une clôture algébrique de K, P n'a que des racines simples. Il revient au même de dire que P n'a que des racines simples dans toute clôture algébrique de K, ou encore, lorsque P est irréductible dans $K[X]$, que le polynôme dérivé de P est non nul.

EXEMPLE 1.9. (i) Soient K un *corps de caractéristique* 0, il suit de 1.5 que tous les éléments *irréductibles* de $K[X]$ sont des polynômes séparables.
(ii) Soient p un nombre premier, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et $K = \mathbb{F}_p(T)$. Soit $P(X) = X^{p^2} + TX^p + T \in K[X]$. Alors $P(X)$ est irréductible dans $K[X]$ et l'on a $P(X) = Q(X^p)$ où $Q(X) = X^p + TX + T \in K[X]$. On vérifie que $Q'(X) = T \neq 0$.

2. Les extensions séparables.

DÉFINITION 2.1. Soit L/K une extension algébrique.
(i) Soit x appartenant à L. On dit que x est séparable sur K si

$$[K(x) : K] = [K(x) : K]_s.$$

(ii) On dit que L est séparable sur K, ou que l'extension L/K est séparable, si tout élément de L est séparable sur K. Sinon, on dit que L est inséparable sur K, que l'extension L/K est inséparable ou encore qu'elle possède de l'inséparabilité.

REMARQUE 2.2. Soit L/K une extension algébrique et soit x appartenant à L, il résulte de 1.5 (voir aussi 1.7 et 1.8) que x est séparable sur K si et seulement si $\mathrm{irr}(x, K; X)$ est un polynôme séparable. Ceci montre que lorsque K est de *caractéristique* 0, *toutes ses extensions algébriques sont séparables* (cf. (i) de 1.9).

La proposition suivante donne des propriétés importantes des extensions séparables.

PROPOSITION 2.3. *(i) Soit L/K soit une extension algébrique finie et soit p l'exposant caractéristique de K, alors il existe $n \in \mathbb{N}$ tel que*

$$[L : K] = p^n [L : K]_s,$$

avec $n = 0$ si $p = 1$. Cet entier p^n s'appelle le degré d'inséparabilité de L sur K.
(ii) Soit L/K une extension algébrique finie, elle est séparable si et seulement si

$$[L : K] = [L : K]_s.$$

(iii) Soit L/K une extension et soit M une partie de L formée d'éléments algébriques et séparables sur K, alors $K(M)$ est une extension séparable de K.
(iv) Soient $K \subset L \subset E$ des extensions algébriques, alors E/K est séparable si et seulement si il en est de même des deux extensions E/L et L/K.

DÉMONSTRATION. (i) On écrit $L = K(x_1, \cdots, x_r)$. Posons $K_0 = K$ et $K_i = K(x_1, \cdots, x_i)$ pour $1 \leq i \leq r$. L'extension L/K se décompose en la suite d'extensions

$$K_0 \subset K_1 \subset \cdots \subset K_r.$$

Pour $1 \leq i \leq r$ soit p^{n_i} le degré d'inséparabilité de x_i sur K_{i-1} (cf. 1.5), on a

$$[K_{i-1} : K_i] = p^{n_i}[K_{i-1} : K_i]_s.$$

Il suit des deux formules précédentes, de la propriété 1.5 de multiplicité des degrés et de celle 1.4 des degrés de séparabilité, que l'on a

$$[L : K] = p^{n_1+\cdots+n_r}[L : K]_s.$$

(ii) Supposons L/K séparable et reprenons les notations de la preuve de (i). Par hypothèse, l'élément x_i de L est séparable sur K, donc sur K_{i-1}, puisque $\mathrm{irr}(x_i, K_{i-1}; X)$ est un diviseur dans $K_{i-1}[X]$ de $\mathrm{irr}(x_i, K; X)$ (ce dernier n'a que des racines simples dans toute clôture algébrique de K), on a donc $n_i = 1$ pour tout i, par suite $[L : K] = [L : K]_s$.

Supposons $[L : K] = [L : K]_s$, soit $x \in L$. Soient p^m et p^n les degrés d'inséparabilité de L sur $K(x)$ et de $K(x)$ sur K, on a,

$$[L : K]_s = [L : K] = [L : K(x)][K(x) : K]$$
$$= p^n[L : K(x)]_s p^m[K(x) : K]_s = p^{n+m}[L : K]_s,$$

donc $m = 0$, c'est à dire $[K(x) : K] = [K(x) : K]_s$.

(iii) Soit $x \in K(M)$, alors il existe des éléments $x_1, \cdots, x_r$ de M, en nombre fini, tels que $x \in K(x_1, \cdots, x_r)$ (cf. 1.9). Posons $K_0 = K$ et $K_i = K(x_1, \cdots, x_i)$ pour $1 \leq i \leq r$. Montrons que $[K_r : K] = [K_r : K]_s$, il en résultera avec (ii) que x est séparable sur K. Les arguments pour montrer cette égalité sont proches de ceux utilisés lors de la preuve de (ii). Soit p^{n_i} le degré d'inséparabilité de x_i sur K_{i-1}, par hypothèse, x_i est séparable sur K, donc sur K_{i-1}, puisque $\mathrm{irr}(x_i, K_{i-1}; X)$ est un diviseur dans $K_{i-1}[X]$ de $\mathrm{irr}(x_i, K; X)$, il suit $n_i = 0$ pour tout i, donc (propriété de multiplicité des degrés et des degrés de séparabilité) $[K_r : K] = [K_r : K]_s$.

(iv) Supposons E/K séparable. Soit $x \in E$, alors on voit que $\mathrm{irr}(x, L; X)$ est séparable (toujours avec le même argument : puisque x est séparable sur K et que $\mathrm{irr}(x, L; X)$ divise dans $L[X]$ le polynôme $\mathrm{irr}(x, K; X)$, ce dernier étant séparable). Soit $x \in L$, alors x est séparable sur K puisque c'est un élément de E.

Supposons que E/L et L/K sont séparables. Soit $x \in E$, posons

$$P(X) = \mathrm{irr}(x, L; X) = X^d + a_1 X^{d-1} + \cdots + a_d$$

avec donc $a_1, \cdots, a_d$ dans L. Considérons les extensions

$$K \subset K(a_1, \cdots, a_d) \subset K(x, a_1, \cdots, a_d),$$

ce sont des extensions algébriques finies. Comme les a_i sont séparables sur K, il vient avec (iii) que la première extension est séparable. Le polynôme irréductible de x sur $K(a_1, \cdots, a_d)$ divise $P(X)$ (puisque ce dernier est à coefficients dans $K(a_1, \cdots, a_d)$), il est donc séparable et la deuxième extension est aussi séparable. La propriété de multiplicité des degrés et des degrés de séparabilité permet de conclure. □

La remarque suivante est très utile pour les applications concrètes.

REMARQUE 2.4. Soit $K(x)/K$ une extension algébrique monogène (c'est à dire engendrée par un seul élément). Soit p^n le degré d'inséparabilité de x sur K (donc p est la caractéristique de K), on peut écrire

$$\mathrm{irr}(x, K; X) = Q(X^{p^n}),$$

où $Q(X) \in K[X]$ est irréductible et séparable, en particulier

$$Q(X) = \mathrm{irr}(x^{p^n}, K; X).$$

Examinons les extensions

$$K \subset K(x^{p^n}) \subset K(x),$$

La première extension est séparable puisque $Q(X)$ est un polynôme séparable, d'autre part l'examen des degrés montre que

$$\mathrm{irr}(x, K(x^{p^n}); X) = X^{p^n} - x^{p^n},$$

en particulier $[K(x) : K(x^{p^n})]_s = 1$ (l'extension $K(x)/K(x^{p^n})$ est purement inséparable).

Soit L/K une extension algébrique et pour tout $x \in L$ soit p^{n_x} le degré d'inséparabilité de x sur K (donc, ici aussi, p désigne la caractéristique de K). On montre, avec des arguments constitant à compter les homomorphismes, que l'extension

$$L \ / \ K(\{x^{p^{n_x}} \ / \ x \in L\})$$

est de degré de séparabilité 1 (on dit qu'elle est purement inséparable), que l'extension

$$K(\{x^{p^{n_x}} \ / \ x \in L\}) \ / \ K$$

est séparable.

3. Séparabilité et normalité.

Le lemme suivant est presque une évidence, mais le phénomène qu'il précise est suffisamment important pour être mis en exergue.

LEMME 3.1. *Soient L/K une extension finie et normale et $G = \mathrm{Gal}(L/K)$ (cf. 2.4). Alors on a*

$$[L : K]_s = o(G),$$

où $o(G)$ désigne l'ordre de G.

DÉMONSTRATION. En effet, soit Ω un corps algébriquement clos admettant L comme sous-corps, alors tout K-homomorphisme de L dans Ω est un K- automorphisme de L. □

Selon les notations habituelles, étant donné un groupe G agissant sur un corps L, on pose

$$L^G = \{x \in L \ / \ g(x) = x \ \forall g \in G\}.$$

THÉORÈME 3.2. *Soit L/K une extension normale et soit $G = \mathrm{Gal}(L/K)$.*
(i) L'extension L^G/K est purement inséparable, l'extension L/L^G est séparable et normale (à partir du chapitre suivant on appellera "galoisiennes" les extensions séparables et normales), on a

$$\mathrm{Gal}(L/L^G) = G.$$

(ii) Supposons l'extension L/K finie, alors

$$[L : L^G] = [L : K]_s = o(G), \ [L^G : K] = \text{degré d'inséparabilité de } L/K.$$

*(iii) On a (cf. **??**)*

$$L_s \cap L^G = K \quad , \quad L_s \cdot L^G = L,$$

ce dernier étant le compositum de L_s et L^G dans L.

DÉMONSTRATION. (i) Soit Ω un corps algébriquement clos admettant L comme sous-corps, alors tout K-homomorphisme de L^G dans Ω se prolonge en un K-automorphisme de L, donc est l'identité sur L^G. Ceci prouve que $[L^G : K]_s = 1$.

Montrons que L/L^G est séparable. Soit $x \in L$ et, dans L, soient $x = x_1, \cdots, x_d$ les racines *distinctes* de $\mathrm{irr}(x, K; X)$. Les fonctions symétriques des racines (qui permettent d'exprimer les coefficients des polynômes) montrent que

$$Q(X) = \prod_{1 \le i \le d} (X - x_i)$$

à ses coefficients stables sous l'action de G, ils sont donc dans L^G. Ainsi $\mathrm{irr}(x, L^G; X)$ divise $Q(X)$ et ce dernier est séparable, donc x est séparable sur L^G. Par suite L/L^G est séparable, elle est normale en

vertu de l'assertion (i) de 2.2, l'égalité des groupes de Galois vient du fait que tout K-automorphisme de L est trivial sur L^G.

(ii) C'est une conséquence directe de la propriété de multiplicité des degrés et des degrés de séparabilité ainsi que du lemme 3.1.

(iii) L'extension $L_s \cap L^G$ de K est séparable car c'est un sous-extension de L_s/K, purement inséparable car c'est une sous-extension de L^G/K, elle est donc égale à K.

Le corps L est une extension de $L_s \cdot L^G$ qui est d'une part séparable, puisque c'est une sous-extension de L/L^G, d'autre part purement inséparable, car c'est une sous-extension de L/L_s, d'où l'égalité cherchée. □

4. Les corps parfaits.

DÉFINITION 4.1. Un corps est dit parfait si toutes ses extensions algébriques sont séparables.

Les corps algébriquement clos et les corps de caractéristique nulle sont parfaits. Le théorème suivant implique qu'il en est de même des corps finis.

DÉFINITION 4.2. Soit K un corps de caractéristique $p > 0$. On appelle endomorphisme absolu de Frobenius de K l'endomorphisme F de K qui à x associe x^p.

THÉORÈME 4.3. *Soit K un corps de caractéristique $p > 0$, alors K est parfait si et seulement si son endomorphisme absolu de Frobenius est un automorphisme.*

DÉMONSTRATION. Soit F l'endomorphisme absolu de Frobenius de K. Supposons K parfait, il faut prouver que F est surjectif. Soit $x \in K$ et, dans une clôture algébrique K^{alg} de K, soit y une racine du polynôme $X^p - x$. Alors dans $K[X]$ le polynôme $\mathrm{irr}(y, K; X)$ divise $X^p - x$, et ce dernier a une seule racine, qui est y, dans K^{alg}. On voit que y est purement inséparable sur K, donc $y \in K$. Ainsi x possède un antécédant par F.

Supposons que F est un automorphisme. Il suffit de montrer que toute extension finie L/K est séparable. Soient donc L/K une extension finie, x un élément de L et $P(X) = \mathrm{irr}(x, K; X)$; supposons que $P(X)$ s'écrive

$$(*) \quad P(X) = X^{np} + a_1 X^{(n-1)p} + \cdots + a_i X^{(n-i)p} + \cdots + a_0,$$

comme F est surjectif sur K, pour tout i il existe $b_i \in K$ tel que $b_i^p = a_i$, donc

$$P(X) = \left(X^n + b_1 X^{n-1} + \cdots + b_i X^{n-i} + \cdots + b_0\right)^p,$$

ce qui contredit l'irréductibilité de $P(X)$ sur K, ainsi l'hypothèse $(*)$ est fausse et x est séparable sur K, quel que soit $x \in L$. □

COROLLAIRE 4.4. *Les corps finis sont parfaits.*

DÉMONSTRATION. En effet, comme l'endomorphisme F est une application injective d'un ensemble fini dans lui-même, il est aussi surjectif. □

5. Les extensions monogènes.

On a déjà rencontré cette notion, rappelons en la définition.

DÉFINITION 5.1. Soit L/K une extension, on dit qu'elle est monogène s'il existe un élément x de L tel que $L = K(x)$. Un tel x est dit élément primitif de L sur K.

THÉORÈME 5.2. *Soit L/K une extension finie, alors elle est monogène si et seulement si elle ne possède qu'un nombre fini de sous-extensions.*

DÉMONSTRATION. Supposons que K est un corps fini, alors L est aussi un corps fini, donc le groupe multiplicatif L^* est cyclique [1]. Soit x un générateur de L^*, clairement $L = K(x)$. On suppose maintenant que K est infini.

Supposons L/K monogène, $L = K(x)$. Soit E un corps intermédiaire entre K et $K(x)$ (donc $K \subset E \subset K(x)$). Posons

$$\mathrm{irr}(x, E; X) = X^d + a_1 X^{d-1} + \cdots + a_d.$$

On a

$$K(a_1, \cdots, a_d) \subset E \quad , \quad [L : E] = d$$

et aussi

$$[L : K(a_1, \cdots, a_d)] \leq d$$

puisque $\mathrm{irr}(x, E : X)$ est à coefficients dans $K(a_1, \cdots, a_d)$. Il en résulte que

$$E = K(a_1, \cdots, a_d).$$

On voit que E est déterminé par les coefficients de $\mathrm{irr}(x, E; X)$, on peut remarquer que ce dernier est un diviseur de $\mathrm{irr}(x, K; X)$ dans $K(x)[X]$. Les sous-extensions de L/K sont donc déterminées par les coefficients des diviseurs de $\mathrm{irr}(x, K; X)$ dans $K(x)[X]$, ces derniers sont en nombre finis.

Inversement, supposons que les sous-extensions de L/K sont en nombre fini. On pose $L = K(x_1, \cdots, x_r)$, considérons la suite d'extensions

$$K \subset K(x_1) \subset K(x_1, x_2) \subset \cdots \subset K(x_1, \cdots, x_i) \subset \cdots \subset K(x_1, \cdots, x_r).$$

Par récurrence sur i, on voit qu'il suffit de montrer le résultat pour $L = K(x_1, x_2)$, ce que nous faisons. Considérons les corps $K(x_1 + \lambda x_2)$,

[1] Nous supposons ce résultat connu, même si nous allons le redémontrer dans le chapitre sur les corps finis.

pour $\lambda \in K$. Par hypothèse ils sont en nombre fini, donc, puisque K est infini, il existe λ et μ appartenant à K, $\lambda \neq \mu$, tels que

$$K(x_1 + \lambda x_2) = K(x_1 + \mu x_2).$$

On a donc

$$x_1 + \lambda x_2 \ , \ x_1 + \mu x_2 \in K(x_1 + \lambda x_2),$$

par suite

$$(x_1 + \lambda x_2) - (x_1 + \mu x_2) = (\lambda - \mu)x_2 \in K(x_1 + \lambda x_2),$$

dont il résulte que x_2, puis x_1, sont dans $K(x_1 + \lambda x_2)$. On a prouvé

$$K(x_1, x_2) = K(x_1 + \lambda x_2).$$

□

COROLLAIRE 5.3. *(Théorème de l'élément primitif.) Soit L/K une extension séparable finie, alors elle est monogène.*

DÉMONSTRATION. Soit Ω un corps algébriquement clos extension de L, on va montrer que l'application qui à E associe $\mathrm{Hom}_E(L, \Omega)$ est une injection définie sur l'ensemble des corps intermédiaires entre K et L, à valeurs dans l'ensemble des parties de $\mathrm{Hom}_K(L, \Omega)$. Il en résultera que l'ensemble des sous-extensions de L/K est fini, donc, suivant 5.2, que l'extension L/K est monogène.

Soient E_1 et E_2, deux corps intermédiaires entre K et L, tels que

$$(1) \quad \mathrm{Hom}_{E_1}(L, \Omega) = \mathrm{Hom}_{E_2}(L, \Omega).$$

Soit E le compositum dans L de E_1 et E_2. Le fait que L/K soit séparable implique qu'il en est de même pour toutes les extensions intermédiaires, donc

$$(2) \quad [L : E] = \mathrm{card}(\mathrm{Hom}_E(L, \Omega)) \ \leq \ [L : E_1] = \mathrm{card}(\mathrm{Hom}_{E_1}(L, \Omega)),$$

l'inégalité venant de ce que $E_1 \subset E$. Il résulte d'autre part de (1) que

$$(3) \quad \mathrm{Hom}_{E_1}(L, \Omega) \subset \mathrm{Hom}_E(L, \Omega).$$

Les relations (2) et (3) impliquent $E = E_1$, donc $E_1 = E_2$. □

REMARQUE 5.4. Soit $L = K(x_1, x_2)$ une extension séparable finie de K, une méthode concrète pour trouver un générateur de cette extension (c'est à dire trouver $x \in L$ tel que $L = K(x)$) est la suivante. Soit Ω un corps algébriquement clos extension de L. Il s'agit de trouver $\lambda \in K$ tel que pour tout $\sigma \in \mathrm{Hom}_K(L, \Omega)$ on ait

$$\sigma(x_1 + \lambda x_2) \neq x_1 + \lambda x_2.$$

En effet cette relation est équivalente au fait que

$$\mathrm{card}(\{\sigma(x_1 + \lambda x_2) \ / \ \sigma \in \mathrm{Hom}_K(L, \Omega)\}) = [L : K],$$

qui montre que le nombre de racines distinctes de $\mathrm{irr}(x_1 + \lambda x_2, K; X)$ est au moins $[L : K]$, donc que

$$[L : K] \leq [K(x_1 + \lambda x_2) : K]_s = [K(x_1 + \lambda x_2) : K]$$

(cf. 1.5). Comme $K(x_1 + \lambda x_2) \subset L$, il en résulte $K(x_1 + \lambda x_2) = L$.

6. Exercices.

EXERCICE 6.1. Soit $K := \mathbb{Q}(i, \sqrt[4]{2})$ le corps de décomposition sur $\mathbb{Q}$, dans $\mathbb{C}$, du polynôme $X^2 - 2 \in \mathbb{Q}[X]$.

– Construire la table du groupe de Galois $\mathrm{Gal}(K/\mathbb{Q})$.

– Montrer que $K = \mathbb{Q}(i + \sqrt[4]{2})$.

SOLUTION 6.2.

EXERCICE 6.3. Soit p un nombre premier. On considère le corps des fractions rationnelles $K = \mathbb{F}_p(T)$ et Ω une clôture algébrique de K.

1) Soit α une racine dans Ω de $f(X) = X^2 + TX + T$. Déterminer $[K(\alpha) : K]$ et montrer que $K(\alpha)/K$ est une extension normale. Est-elle séparable ?

2) Soit β une racine dans Ω de $h(X) = X^{2p} + TX^p + T$. Déterminer $[K(\beta) : K]$ et montrer que $K(\beta)/K(\alpha)$ est une extension purement inséparable. Déterminer $[K(\beta) : K]_s$.

3) Soit γ une racine de $g(X) = X^p + T$. Factoriser g puis h dans Ω.

SOLUTION 6.4.

EXERCICE 6.5. Soient K un corps séparablement clos, F une extension finie de K. Soit L une extension finie et séparable de F, montrer que $L = F$.

SOLUTION 6.6.

EXERCICE 6.7. Soient K un corps de caractéristique $p > 0$ et $a \in K \setminus K^p$. Montrer que $X^p - a$ est irréductible sur K.

SOLUTION 6.8.

EXERCICE 6.9. Soient K un corps de caractéristique $p > 0$ et L une extension purement inséparable de K avec $[L : K] = p^n$. Montrer que $a^{p^n} \in K$ pour tout $a \in L$.

SOLUTION 6.10.

EXERCICE 6.11. (exemple d'une extension L/K telle que L n'est pas séparable sur la fermeture purement inséparable de K dans L) Soient k un corps de caractéristique 2, $K = k(x, y)$ le corps des fonctions rationnelles, $E = K(u)$ où u est une racine de $T^2 + T + x \in K[T]$ et $L = E(\sqrt{uy})$.

1) Montrer que L/E est purement inséparable et E/K est séparable. Montrer que $[L : E] = 2$ et $[E : K] = 2$.

2) Montrer que si $a \in L$ vérifie $a^2 \in K$, alors $a \in K$. En déduire que K est purement inséparablement clos dans L.

SOLUTION 6.12.

EXERCICE 6.13. Soit K le corps des fonctions rationnelles $k(x)$ sur un corps parfait k de caractéristique $p > 0$. Soient $u \in K, u \notin k$ et $E = k(u)$. Montrer que K/E est séparable si et seulement si $u \notin K^p$.

SOLUTION 6.14.

EXERCICE 6.15. (exemple d'une extension finie ayant une infinité de sous-corps intermédiaire) Soient k un corps de caractéristique $p > 0$, $K = k(x, y)$ le corps des fonctions rationnelles sur k en deux variables et $F = k(x^p, y^p)$.

(a) Montrer que K/F est une extension purement inséparable de degré p^2.

(b) Montrer que $K \neq F(a)$ pour tout $a \in K$.

(c) Exhiber une infinité de sous-corps intermédiaires de l'extension K/F.

SOLUTION 6.16.

CHAPITRE 4

extensions galoisiennes.

1. La correspondance de Galois.

DÉFINITION 1.1. Soit L/K une extension algébrique, on dit qu'elle est galoisienne si elle est normale et séparable.

Rappelons que le groupe de Galois d'une extension normale L sur K est $\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$ (groupe pour la composition des applications), que l'on a ensemblistement $\mathrm{Gal}(L/K) = \mathrm{Hom}_K(L, \Omega)$ où Ω désigne n'importe quel corps algébriquement clos extension de L (cf. 2.1 et 2.4). Rappelons aussi que si H est un sous-groupe de $\mathrm{Gal}(L/K)$, on désigne par L^H le sous-corps des éléments de L invariants sous l'action de H, c'est à dire

$$L^H = \{x \in L \ / \ \sigma(x) = x \ \forall \sigma \in H\}.$$

Rappelons enfin qu'étant donné les propriétés des extensions séparables et des extensions normales, si L/K est une extension galoisienne finie, alors

$$[L : K] = o(\mathrm{Gal}(L/K)).$$

THÉORÈME 1.2. *Soit L/K une extension galoisienne finie. Soient $\mathfrak{L}$ l'ensemble des corps intermédiaires entre K et L, $\mathfrak{G}$ l'ensemble des sous-groupes de* $\mathrm{Gal}(L/K)$*, soient*
- $\varphi : \mathfrak{L} \to \mathfrak{G}$ *l'application qui à $E \in \mathfrak{L}$ associe* $\mathrm{Gal}(L/E)$,
- $\psi : \mathfrak{G} \to \mathfrak{L}$ *l'application qui à $H \in \mathfrak{G}$ associe L^H.*

Alors φ et ψ sont des bijections décroissantes, réciproques l'une de l'autre.

De plus, soit E un élément de $\mathfrak{L}$, alors l'extension E/K est galoisienne si et seulement si $\mathrm{Gal}(L/E)$ *est un sous-groupe normal de* $\mathrm{Gal}(L/K)$ *; dans ce cas, la restriction des éléments de* $\mathrm{Gal}(L/K)$ *à E induit un isomorphisme canonique*

$$\frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/E)} \simeq \mathrm{Gal}(E/K).$$

DÉMONSTRATION. Elle se déroule en plusieurs étapes.
1) On ne suppose pas ici que L/K est finie. Montrons que $\psi \circ \varphi = \mathrm{Id}_{\mathfrak{L}}$. Il faut prouver que pour tout $E \in \mathfrak{L}$ on a

$$E = L^{\mathrm{Gal}(L/E)}.$$

Posons $E' = L^{\mathrm{Gal}(L/E)}$. On a $E \subset E'$. Soit $x \in E'$ et supposons que $x \notin E$. Comme $\mathrm{irr}(x, E; X)$ a une racine dans L, il a une autre racine

dans L (puisque $\deg(\mathrm{irr}(x, E; X)) > 1$ et que L est normal sur K, donc sur E) ; notons y cette deuxième racine. Soit $\sigma : E(x) \to L$ le morphisme trivial sur E et qui envoie x sur y, soient L^{alg} une clôture algébrique de L et $\tau : L \to l^{\mathrm{alg}}$ un prolongement de $E(x) \xrightarrow{\sigma} L \subset L^{\mathrm{alg}}$ à L. comme L est normal sur E, l'image de τ est dans L et τ est un élément de $\mathrm{Gal}(L/E)$, mais τ ne laisse pas fixe $x \in E' = L^{\mathrm{Gal}(L/E)}$. Ceci est une contradiction et montre que x n'existe pas.
2) On suppose de nouveau L/K finie. Montrons que $\varphi \circ \psi = \mathrm{Id}_{\mathfrak{G}}$. Il faut prouver que pour tout $H \in \mathfrak{G}$ on a

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

L'extension L/L^H est séparable et finie, donc il existe $x \in L$ tel que $L = L^H(x)$. Soit

$$P(X) = \prod_{\sigma \in H} (X - \sigma(x)).$$

C'est un élément de $L[X]$ et les fonctions symétriques des racines montrent que ses coefficients sont invariants sous l'action de H, donc $P(X) \in L^H[X]$. Il en résulte que $\mathrm{irr}(x, L^H, X)$ divise $P(X)$, puisque x est racine de $P(X)$. Donc $\deg(P) \geq [L : L^H]$, mais le degré de P est $o(H)$, par suite

$$o(H) \geq [L : L^H] = o(\mathrm{Gal}(L/L^H)),$$

De l'inclusion $H \subset \mathrm{Gal}(L/L^H)$ il vient l'inégalité inverse

$$o(\mathrm{Gal}(L/L^H)) \geq o(H).$$

On a prouvé $o(\mathrm{Gal}(L/L^H)) = o(H)$, donc $\mathrm{Gal}(L/L^H) = H$.
3) Soit H un sous-groupe normal de $\mathrm{Gal}(L/K)$, montrons que l'extension L^H/K est normale (il s'en suivra qu'elle est galoisienne). Soit $\sigma : L^H \to L^{\mathrm{alg}}$ un K-homomorphisme de L^H dans une clôture algébrique de L et soit τ un prolongement de σ à L, donc τ est dans $\mathrm{Gal}(L/K)$. Soit $\nu \in H$. On a $\tau' = \tau^{-1}\nu\tau$ qui est dans H, puisque ce dernier est normal dans $\mathrm{Gal}(L/K)$. Donc, pour tout $x \in L^H$, $\tau'(x) = x$, ce qui donne $\nu(\tau(x)) = \tau(x)$, ou encore $\nu(\sigma(x)) = \sigma(x)$. Donc, quel que soit le K-homomorphisme $\sigma : L^H \to L^{\mathrm{alg}}$ son image est dans L^H. Ceci prouve que L^H/K est normale.

Soit $E \in \mathfrak{L}$, supposons E/K galoisienne. Soit L^{alg} une clôture algébrique de L. Comme L/K et E/K sont normales, la restriction de L à E induit une application surjective

$$\mathrm{Gal}(L/K) = \mathrm{Hom}_K(L, L^{\mathrm{alg}}) \to \mathrm{Hom}_K(E, L^{\mathrm{alg}}) = \mathrm{Gal}(E/K),$$

son noyau est par $\mathrm{Gal}(L/E)$ d'après ce qui est prouvé en 2). Ainsi ce dernier est normal dans $\mathrm{Gal}(L/K)$ et l'on a l'isomorphisme cherché. □

REMARQUE 1.3. les notations sont celles du théorème. Cette correspondance, donnée par φ et ψ, entre $\mathfrak{L}$ et $\mathfrak{G}$, s'appelle la correspondance de Galois.

REMARQUE 1.4. On a vu que le point 1) de la démonstration ne nécessite pas que l'extension galoisienne L/K soit finie. Ce n'est pas du tout le cas au point 2). Lorsque L/K est infinie, la correspondance de Galois se fait avec les sous-groupes fermés de $\mathrm{Gal}(L/K)$, pour une certaine topologie, qui est la topologie triviale lorsque l'extension est finie. Le lecteur curieux pourra consulter par exemple le chapitre V du livre d'algèbre du traité de N. Bourbaki.

2. Compléments.

THÉORÈME 2.1. *Soient L/K et E/K deux extensions. On suppose que L/K est galoisienne finie. On suppose aussi que L et E sont des sous-corps d'un même troisième corps, de sorte que l'on peut définir leur compositum $L.E$. Alors $L.E$ est une extension galoisienne de E, l'application*

$$\mathrm{Gal}(L.E/E) \longrightarrow \mathrm{Gal}(L/K),$$

qui à $\sigma \in \mathrm{Gal}(L.E/E)$ associe sa restriction à L, est bien définie, elle induit un isomorphisme

$$\mathrm{Gal}(L.E/E) \simeq \mathrm{Gal}(L/L \cap E).$$

DÉMONSTRATION. L'extension $L.E/E$ est séparable car $L.E = E(L)$ et L est séparable sur K, donc sur E.

Montrons que $L.E/E$ est normale. Soit un E-homomorphisme $\sigma : L.E \to \Omega$, où Ω est un corps algébriquement clos, extension de L et E. Alors la restriction $\sigma \mid L$ à L est un K-homomorphisme, donc $\sigma(L) = L$, puisque L/K est normale. Il vient $\sigma(L.E) = L.E$.

On a prouvé que l'extension $L.E/E$ est galoisienne, elle est aussi finie.

L'application

$$\varphi : \mathrm{Gal}(L.E/E) \longrightarrow \mathrm{Gal}(L/K),$$

qui à tout élément σ de $\mathrm{Gal}(L.E/E)$ associe sa restriction à L, est bien définie, car $\sigma \mid L$ est l'identité sur $L \cap E$, donc sur K et son image est L puisque L/K est normale ; de plus φ est injective : si l'on a $\sigma \mid L = \mathrm{Id}_L$, comme $\sigma \mid E = \mathrm{Id}_E$, il vient $\sigma \mid L.E = \mathrm{Id}_{L.E}$.

Montrons que l'image de φ est $\mathrm{Gal}(L/L \cap E)$. Puisque $L.E/E$ est galoisienne finie, suivant le théorème 1.2, il faut montrer que

$$L^{\mathrm{Im}\varphi} = E \cap L.$$

Soit $x \in L$ laissé stable par les éléments de $\mathrm{Im}\varphi$, comme φ est injectif, il suit que x, vu comme un élément de $L.E$, est laissé stable par tous les éléments de $\mathrm{Gal}(L.E/E)$, donc (cf. 1.2) $x \in E$. On a prouvé $L^{\mathrm{Im}\varphi} \subset L \cap E$, l'inclusion inverse est évidente et a été remarquée plus haut. □

Le corollaire suivant est utile dans les applications concrètes.

COROLLAIRE 2.2. *Soient L/K et E/K deux extensions. On suppose que L/K est galoisienne et finie. On suppose aussi que L et E sont des sous-corps d'un même troisième corps, de sorte que l'on peut définir leur compositum $L.E$. Alors*
(i) $[L.E : E]$ divise $[L : K]$, plus précisément

$$[L : K] = [L.E : E][L \cap E : K];$$

(ii) si $E \cap L = K$, on a

$$[L.E : E] = [L : K],$$

(iii) si $E \cap L = K$ et E/K est finie, on a de plus

$$[L.E : K] = [L : K][E : K].$$

DÉMONSTRATION. Considérons le diagramme

$$\begin{array}{ccccc} & & E & & \\ & \nearrow & & \searrow & \\ K & & & & L.E \\ & \searrow & & \nearrow & \\ & & L & & \end{array}$$

où les flèches signifient des inclusions, on voit que le corollaire est une conséquence immédiate de l'isomorphisme de 2.1. □

REMARQUE 2.3. Le théorème 2.1 et son corollaire 2.2 sont faux sans l'hypothèse que l' extension L/K est galoisienne. Par exemple, soit

$$\begin{array}{ccccc} & & E = \mathbb{Q}(\sqrt[3]{2}) & & \\ & \nearrow & & \searrow & \\ K = \mathbb{Q} & & & & L.E = \mathbb{Q}(\sqrt[3]{2}, j) \\ & \searrow & & \nearrow & \\ & & L = \mathbb{Q}(j\sqrt[3]{2}) & & \end{array}$$

(j est une racine cubique de l'unité, $j \neq 1$). Les deux extensions L/K et E/K sont engendrées par des racines de $X^3 - 2$, elles sont donc de degré 3, comme E est inclus dans $\mathbb{R}$ on a $j \notin E$, donc $L.E/E$ est de degré 2 et 2 ne divise pas 3 (on a aussi $L.E/L$ de degré 2).

EXERCICE 2.4. Soit $\zeta \in \mathbb{C}$ une racine primitive 5-ième de l'unité, montrer que l'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ est galoisienne de degré 4. En déduire que $\mathbb{Q}(\zeta, \sqrt[3]{2})/\mathbb{Q}(\sqrt[3]{2})$ est aussi galoisienne de degré 4, que le degré de $\mathbb{Q}(\zeta, \sqrt[3]{2})/\mathbb{Q}$ est 12.

3. Exercices.

Une remarque. Soit L/K une extension finie contenu dans un corps algébriquement clos Ω, on a $|\mathrm{Gal}(L/K)| \leq |\mathrm{Hom}_K(L, \Omega)| = [L : K]_s \leq [L : K]$. 1er égalité ssi normale, 2e égalité ssi séparable. Ainsi deux égalités ssi galoisienne.

EXERCICE 3.1. Dans les questions suivantes, soient K un corps de décomposition de $P(X)$ sur F. Déterminer $\mathrm{Gal}(K/F)$ et trouver tous les sous-corps intermédiaires de K/F. Trouver un élément primitif de l'extension K/F.

(a) $F = \mathbb{Q}$ et $P(X) = X^3 - 2$.
(b) $F = \mathbb{Q}$ et $P(X) = X^4 - 7$.
(c) $F = \mathbb{F}_5$ et $P(X) = X^4 - 7$.
(d) $F = \mathbb{Q}$ et $P(X) = X^5 - 2$.
(e) $F = \mathbb{F}_2$ et $P(X) = X^6 + 1$.

SOLUTION 3.2.

EXERCICE 3.3. (a) Soit $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Montrer que $K/\mathbb{Q}$ est une extension galoisienne. Montrer que $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Déterminer les sous-groupes de $\mathrm{Gal}(K/\mathbb{Q})$ et les corps d'invariants associés.

(b) Soient F un corps de caractéristique différente de 2, et K une extension galoisienne de F avec $[K : F] = 4$. Supposons que $\mathrm{Gal}(K/F) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, montrer que $\exists a, b \in F$ tels que $K = F(\sqrt{a}, \sqrt{b})$.

EXERCICE 3.4. Soit L une extension galoisienne de K avec $[L : K] = n$. Si p est un diviseur premier de n, montrer qu'il existe un sous-corps E de L tel que $[L : E] = p$.

EXERCICE 3.5. Donner un exemple d'une extension K/F avec

(a) K/F normale et non galoisienne.
(b) K/F séparable et non galoisienne.

EXERCICE 3.6. Soit K une extension finie normale de F ($K \neq F$) telle qu'il n'y a pas de sous-extensions différentes de K et de F. Montrer que $[K : F]$ est premier. Donner un contre-exemple si K/F n'est pas normale.

EXERCICE 3.7. Soit $E \subset \mathbb{C}$ le corps de décomposition sur $\mathbb{Q}$ du polynôme $X^7 - 8$.

(a) Déterminer E et calculer $[E : \mathbb{Q}]$.
(b) Soit $G = \mathrm{Gal}(E/\mathbb{Q})$. Montrer qu'il existe $\sigma \in G$ d'ordre 7 et $\tau \in G$ d'ordre 6 tels que $G =< \sigma, \tau >$.

EXERCICE 3.8. Soit $F \subset L \subset K$ avec L/F purement inséparable. Soit $a \in K$ séparable sur F. Montrer que $\mathrm{irr}(a, F) = \mathrm{irr}(a, L)$. Supposons maintenant K/L séparable et $[K : F] < \infty$. Soit S la clôture séparable de F dans K. Montrer que $K = SL$ et que $[K : L] = [S : F]$. (Remarque : L'exercice 6.5 est un cas particulier).

EXERCICE 3.9. Soient K/F une extension finie normale et L/F une extension finie algébrique. Si K/F ou L/F est séparable, montrer que $[KL : L] = [K : K \cap L]$.

EXERCICE 3.10. Soit $\mathbb{Q} \subset K \subset \mathbb{C}$ avec $K/\mathbb{Q}$ galoisienne. Soit σ la conjugaison complexe, montrer que $\sigma(K) = K$. Montrer que $K^{<\sigma>} = K \cap \mathbb{R}$ et que $[K : K \cap \mathbb{R}] \leq 2$. Donner deux exemples avec $[K : K \cap \mathbb{R}] = 1$ et $[K : K \cap \mathbb{R}] = 2$ respectivement.

CHAPITRE 5

Exemples d'extensions galoisiennes.

1. Les extensions cyclotomiques.

DÉFINITION 1.1. Soient K un corps et $n > 0$ un entier, on appelle racine n-ème de l'unité de K toute racine dans K du polynôme $X^n - 1$. On note $\mu_n(K)$ l'ensemble des racines n-ème de l'unité de K.

PROPOSITION 1.2. *Soient K un corps et $n > 0$ un entier, posons $n = mp^\alpha$ où p est l'exposant caractéristique de K et m est premier avec p. On a*

$$\mu_n(K) = \mu_m(K),$$

soit $n' > 0$ un diviseur de n , alors

$$\mu_{n'}(K) \subset \mu_n(K),$$

$\mu_n(K)$ est un groupe cyclique d'ordre un diviseur de m, d'ordre m si K est algébriquement clos.

La seule chose à prouver est que $\mu_n(K)$ est cyclique, c'est une conséquence du lemme suivant.

LEMME 1.3. *Soient K un corps et G un sous-groupe fini du groupe multiplicatif K^*, alors G est cyclique.*

DÉMONSTRATION. Posons $n = \circ(G)$. Pour tout diviseur d de n soit G_d l'ensemble des éléments de G d'ordre d. Evaluons le cardinal de G_d. Supposons que G_d soit non vide, soit x l'un de ses éléments, alors

$$< x >= \{1, x, x^2, \cdots, x^{d-1}\}$$

est un ensemble de d racines dans K, distinctes, du polynôme $X^d - 1$, c'est à dire que c'est l'ensemble de toutes les racines (dans K) de ce polynôme. Par suite G_d est l'ensemble des générateurs du groupe cyclique $< x >$. Posons $\varepsilon_d = 1$ si $G_d \neq \emptyset$ et $\varepsilon_d = 0$ sinon, on a prouvé

$$\text{card}(G_d) = \varepsilon_d \varphi(d),$$

où φ désigne l'indicateur d'Euler. Comme G est la réunion disjointe des G_d, pour d divisant n, il vient

$$(1) \qquad n = \sum_{d|n} \varepsilon_d \varphi(d).$$

Le même raisonnement, appliqué à un groupe cyclique connu, par exemple $(\mathbb{Z}/n\mathbb{Z}, +)$, donne (puisqu'alors, si d divise n, l'ensemble des éléments d'ordre d est non vide, de cardinal $\varphi(d)$)

$$n = \sum_{d|n} \varphi(d). \tag{2}$$

La comparaison des formules (1) et (2) montre que l'on a toujours $\varepsilon_d = 1$, en particulier $\varepsilon_n = 1$. □

DÉFINITION 1.4. Soient K un corps et $n > 0$ un entier, un générateur de $\mu_n(K)$ s'appelle une racine primitive n-ème de l'unité de K.

Notons $\mathbb{Q}^{\text{alg}}$ la clôture algébrique de $\mathbb{Q}$ contenue dans $\mathbb{C}$ et pour tout entier $n > 0$ posons $\Phi_n(X) = \prod(X - \zeta)$, où ζ décrit l'ensemble des racines primitives n-ème de l'unité de $\mathbb{Q}^{\text{alg}}$.

DÉFINITION 1.5. Le polynôme $\Phi_n(X)$ s'appelle le n-ème polynôme cyclotomique.

PROPOSITION 1.6. *Soit $n > 0$ un entier, alors*

$$\Phi_n(X) \in \mathbb{Z}[X].$$

DÉMONSTRATION. Soit $G = \text{Gal}(\mathbb{Q}^{\text{alg}}/\mathbb{Q})$, l'action de G sur les racines de $\Phi_n(X)$ ainsi que les fonctions symétriques de ces mêmes racines montrent que $\Phi_n(X) \in (\mathbb{Q}^{\text{alg}})^G[X]$, et il résulte de la première partie de la démonstration de 1.2 que $(\mathbb{Q}^{\text{alg}})^G = \mathbb{Q}$. Ainsi $\Phi_n(X) \in \mathbb{Q}[X]$. La formule (évidente)

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

et **??** montrent alors que les polynômes cyclotomiques sont à coefficients entiers, puisqu'ils sont unitaires. □

Les polynômes cyclotomiques sont aussi irréductibles dans $\mathbb{Z}[X]$, cela résulte de l'étude suivante des extensions obtenues par adjonction de racines de l'unité.

DÉFINITION 1.7. Soient K un corps et $n > 0$ un entier. Lorsque K est de caractéristique non nulle on suppose que celle-ci ne divise pas n. Soient K^{alg} une clôture algébrique de K et ζ une racine primitive n-ème de l'unité dans K^{alg}. Le corps $K(\zeta)$ est appelé extension cyclotomique de K de niveau n.

Cette définition ne dépend pas du choix de la racine primitive, en fait on a avec les notations de la définition $K(\zeta) = K(\mu_n(K^{\text{alg}}))$. Cette formule montre aussi que deux extensions cyclotomiques de K de même niveau sont K-isomorphes (cf. 1.4), mais la proposition suivante en dit plus.

PROPOSITION 1.8. *Soient K un corps et $n > 0$ un entier, premier à la caractéristique de K lorsque celle-ci est non nulle. Soit $\alpha : \mathbb{Z} \to K$ l'application canonique, qui à l'entier z associe $z1_K$, où 1_K est l'élément unitaire de K ; notons $\Phi_n^\alpha(X) \in K[X]$ le polynôme obtenu par l'action de α sur les coefficients de $\Phi_n(X)$ (cf. 1.6). Soit E une extension cyclotomique de K de niveau n.*
(i) L'extension E/K est galoisienne. Soit $\zeta \in E$ une racine primitive de l'unité (donc $E = K(\zeta)$), alors $\mathrm{irr}(\zeta, K; X)$ *divise* $\Phi_n^\alpha(X)$.
(ii) Posons $G = \mathrm{Gal}(E/K)$ et soit $\zeta \in E$ une racine primitive de l'unité. Pour tout $\sigma \in G$ soit m_σ un entier tel que $\sigma(\zeta) = \zeta^{m_\sigma}$, alors l'application

$$\omega \ : \ G \longrightarrow \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*,$$

qui à σ associe la classe de m_σ modulo n, est un morphisme injectif de groupes ; il suit que $[E : K]$ divise $\varphi(n)$.

DÉMONSTRATION. (i) Soit $\zeta \in E$ une racine primitive de l'unité. On a $E = K(\zeta)$ et ζ est racine de $X^n - 1$, ce dernier étant séparable sur K, compte tenu de l'hypothèse faite sur n. Donc E/K est séparable. Cette extension est normale car E est un corps de décomposition de $X^n - 1$ sur K. Montrons que ζ est racine de $\Phi_n^\alpha(X)$: ζ est racine de

$$X^n - 1 = \prod_{d|n} \Phi_d^\alpha(X),$$

si ζ est racine de $\Phi_d^\alpha(X)$ pour $d < n$, puisque ce dernier divise $X^d - 1$ dans $K[X]$, il vient que ζ est racine de $X^d - 1$, ce qui est faux.

(ii) Soit $\sigma \in G$. Comme σ induit un isomorphisme de $\mu_n(E)$, $\sigma(\zeta)$ est aussi une racine primitive de l'unité, donc s'écrit $\sigma(\zeta) = \zeta^{m_\sigma}$ avec m_σ premier à n. Ceci montre que l'application ω est définie ; le fait qu'alors ce soit un morphisme injectif est facile. On a $[E : K]$ qui divise $\varphi(n)$ puisque $\omega(G)$ est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^*$. □

COROLLAIRE 1.9. *Soient $n > 0$ un entier et E une extension cyclotomique de $\mathbb{Q}$ de niveau n. Alors $[E : \mathbb{Q}] = \varphi(n)$, le polynôme cyclotomique $\Phi_n(X)$ est irréductible dans $\mathbb{Q}[X]$ (donc dans $\mathbb{Z}[X]$).*

DÉMONSTRATION. Soient $G = \mathrm{Gal}(E/\mathbb{Q})$ et $\zeta \in E$ une racine primitive n-ème de l'unité. Il faut prouver que le morphisme

$$\omega \ : \ G \longrightarrow \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$$

de 1.8 est surjectif, c'est à dire qu'il faut montrer que pour tout nombre premier l ne divisant pas n, il existe $\sigma \in G$ tel que $\sigma(\zeta) = \zeta^l$. Soient donc l un nombre premier ne divisant pas n, $P(X) = \mathrm{irr}(\zeta, \mathbb{Q}; X)$ et $Q(X) = \mathrm{irr}(\zeta^l, \mathbb{Q}; X)$. Il faut prouver que $P(X) = Q(X)$.

Supposons que $P(X) \neq Q(X)$. Les polynômes $P(X)$ et $Q(X)$ sont dans $\mathbb{Z}[X]$, car ils divisent $X^n - 1$ dans $\mathbb{Q}[X]$ et sont unitaires (cf. **??**). Par le même argument, on peut écrire dans $\mathbb{Z}[X]$

$$X^n - 1 = P(X)Q(X)U(X) \quad \text{et} \quad Q(X^l) = P(X)V(X),$$

avec donc $U(X)$ et $V(X)$ dans $\mathbb{Z}[X]$. Nous allons examiner ces relations en réduisant les coefficients des polynômes modulo l, nous indiquons cette réduction en surlignant les polynômes. Il vient dans $(\mathbb{Z}/l\mathbb{Z})[X]$

$$X^n - \bar{1} = \bar{P}(X)\bar{Q}(X)\bar{U}(X) \quad \text{et} \quad (\bar{Q}(X))^l = \bar{P}(X)\bar{V}(X).$$

Soit $w(X)$ un élément irréductible de $(\mathbb{Z}/l\mathbb{Z})[X]$ divisant $\bar{P}(X)$, la deuxième relation montre que $w(X)$ divise $\bar{Q}(X)$ dans $(\mathbb{Z}/l\mathbb{Z})[X]$, la première relation montre alors que $w(X)^2$ divise $X^n - \bar{1}$ dans $(\mathbb{Z}/l\mathbb{Z})[X]$, mais ceci est impossible car $X^n - \bar{1}$ est séparable. □

REMARQUE 1.10. On reprend les notations et hypothèses de 1.8, il n'est pas fréquent que les polynômes $\Phi_n^\alpha(X)$ soient irréductibles dans $K[X]$, par exemple, on va voir au paragraphe suivant en 2.6, que si $K = \mathbb{F}_q$ est un corps fini à q éléments, si $n > 0$ est un entier non divisible par la caractéristique de $\mathbb{F}_q$, si E est une extension cyclotomique de $\mathbb{F}_q$ de niveau n, alors $[E : \mathbb{F}_q]$ est égal à l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^*$.

2. Les corps finis.

On note généralement $\mathbb{F}$ un corps fini, ou encore $\mathbb{F}_q$, pour rappeler son nombre q d'éléments. La caractéristique d'un corps fini est un nombre premier.

PROPOSITION 2.1. *(i) Soit $\mathbb{F}$ un corps fini de caractéristique p, alors $\mathbb{F}$ est une extension finie de son sous-corps premier $\mathbb{F}_p$. Posons $n = [\mathbb{F} : \mathbb{F}_p]$, on a* $\mathrm{card}(\mathbb{F}) = p^n$.
(ii) Soit $L/\mathbb{F}_q$ une extension finie de degré n, où $\mathbb{F}_q$ est un corps à q éléments, alors $\mathrm{card}(L) = q^n$.

DÉMONSTRATION. Le corps $\mathbb{F}$ est un espace vectoriel sur son sous-corps premier $\mathbb{F}_p$, de dimension finie puisqu'il est fini (lui-même forme un système générateur fini sur $\mathbb{F}_p$). On voit qu'il suffit de prouver (ii). Soit $\{e_1, \cdots, e_n\}$ une base de L sur $\mathbb{F}_q$, on a en tant qu'espaces vectoriels

$$L = \bigoplus_{1 \leq i \leq n} \mathbb{F}_q e_i,$$

dont il résulte la formule sur les cardinaux. □

On a vu que les corps finis sont parfaits (cf. 4.4), le théorème suivant dit que ce sont tous des corps de décompositions.

THÉORÈME 2.2. *Soient p un nombre premier, $\mathbb{F}_p$ un corps à p éléments et $\mathbb{F}_p^{\mathrm{alg}}$ une clôture algébrique de $\mathbb{F}_p$. Alors pour tout entier $n > 0$*

il existe un et un seul sous-corps de $\mathbb{F}_p^{\mathrm{alg}}$ à p^n éléments, c'est le corps de décomposition (dans $\mathbb{F}_p^{\mathrm{alg}}$) du polynôme $X^{p^n} - X$.

DÉMONSTRATION. Soit K un sous-corps de $\mathbb{F}_p^{\mathrm{alg}}$ à p^n éléments. Le groupe multiplicatif K^* a $p^n - 1$ éléments, donc tous ses éléments sont racines de $X^{p^n-1} - 1$, comme K possède p^n éléments, il suit que ses éléments sont les racines dans $\mathbb{F}_p^{\mathrm{alg}}$ du polynôme $X^{p^n} - X$. Ceci prouve l'unicité, l'existence provient du fait que les racines de $X^{p^n} - X$ dans $\mathbb{F}_p^{\mathrm{alg}}$ forment un corps (cela se vérifie par un calcul direct). □

COROLLAIRE 2.3. *(i) Soient p un nombre premier et $n > 0$ un entier, alors deux corps à p^n éléments sont isomorphes.*
(ii) Soient p un nombre premier, $\mathbb{F}_p^{\mathrm{alg}}$ une clôture algébrique d'un corps $\mathbb{F}_p$ à p éléments, $n > 0$ et $m > 0$ deux entiers, $\mathbb{F}_{p^n}$ et $\mathbb{F}_{p^m}$ les sous-corps de $\mathbb{F}_p^{\mathrm{alg}}$ à p^n et p^m éléments respectivement. Alors $\mathbb{F}_{p^n}$ est un sous-corps de $\mathbb{F}_{p^m}$ si et seulement si n divise m.

DÉMONSTRATION. La partie (i) résulte du fait que les corps finis sont des corps de décomposition (cf. (ii) de 1.4). Montrons (ii). Supposons que n divise m et posons $m = nd$. On a $p^{nd} - 1 = (p^n - 1)h$ avec $h = 1 + p^n + \cdots + p^{n(d-1)}$, par suite les racines (dans $\mathbb{F}_p^{\mathrm{alg}}$) de $X^{p^n-1} - 1$ sont aussi racines de $X^{p^m-1} - 1$. Il suit que le sous- corps de $\mathbb{F}_p^{\mathrm{alg}}$ à p^n éléments est contenu dans celui à p^m éléments. Réciproquement, si $\mathbb{F}_{p^n}$ est un sous-corps de $\mathbb{F}_{p^m}$, on a alors $n = [\mathbb{F}_{p^n} : \mathbb{F}_p]$ qui divise $m = [\mathbb{F}_{p^m} : \mathbb{F}_p]$. □

COROLLAIRE 2.4. *Soit $L/\mathbb{F}_q$ une extension algébrique d'un corps fini à q éléments. Alors elle est galoisienne. Si de plus $L/\mathbb{F}_q$ est finie, alors son groupe de Galois est cyclique, engendré par le $\mathbb{F}_q$-automorphisme qui à tout élément x de L associe x^q.*

DÉMONSTRATION. Montrons que $L/\mathbb{F}_q$ est normale. Soit $P(X) \in \mathbb{F}_q[X]$, irréductible et ayant une racine x dans L, il faut montrer que $P(X)$ se décompose dans $L[X]$ en un produit de polynômes du premier degré (cf. 1.5 et 2.1). D'après le théorème 2.2, l'extension $\mathbb{F}_q(x)/\mathbb{F}_q$ est normale, donc comme $P(X)$ a une racine dans $\mathbb{F}_q(x)$, il se décompose en un produit de polynômes du premier degré dans $\mathbb{F}_q(x)[X]$, par suite dans $L[X]$.

Supposons $L/\mathbb{F}_q$ finie, de degré n et soit σ le $\mathbb{F}_q$-automorphisme défini dans l'énoncé. Montrons que $\circ(< \sigma >) = n$ (ceci équivaut à $< \sigma >= \mathrm{Gal}(L/\mathbb{F}_q)$). Soit $d \leq n$ tel que $\sigma^d = \mathrm{Id}_L$, alors pour tout x de L on a

$$x = \sigma^d(x) = x^{p^d},$$

donc tous les éléments de L sont racines du polynôme $X^{p^d} - X$. Ceci impose $d = n$. □

DÉFINITION 2.5. Les notations et hypothèses sont celles du corollaire 2.4. Soit σ le générateur du groupe de Galois $\mathrm{Gal}(L/\mathbb{F}_q)$, qui à x

de L associe x^q, on dit que σ est un automorphisme de Frobenius de L. Si $q = p^n$, où p est la caractéristique de $\mathbb{F}_q$, on a $\sigma = \sigma_0^n$, où σ_0 est l' homomorphisme de Frobenius absolu de L (cf. 4.2).

PROPOSITION 2.6. *Soient $\mathbb{F}_q$ un corps fini à q éléments, $n > 0$ un entier premier avec q et E une extension cyclotomique de $\mathbb{F}_q$ de niveau n. Alors $[E : \mathbb{F}_q]$ est égal à l'ordre de la classe de q dans $(\mathbb{Z}/n\mathbb{Z})^*$.*

DÉMONSTRATION. Soit $G = \mathrm{Gal}(E/\mathbb{F}_q$, considérons le morphisme injectif

$$\omega \ : \ G \longrightarrow \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$$

de 1.8. Le groupe G est engendré par le morphisme de Frobenius σ, qui à tout x de $\mathbb{F}_q$ associe x^q, donc l'image de ω est un groupe cyclique engendré par $\omega(\sigma)$ qui est la classe de q modulo n. □

Nous terminons ce paragraphe en énonçant le seul résultat de ce cours qui ne suppose pas à priori que les corps considérés soient commutatifs.

THÉORÈME 2.7. *(Théorème de Wedderburn) . Les corps finis sont commutatifs.*