Prolongement d'isomorphismes

1 Isomorphisme

Nous rappelons qu'un homomorphisme de corps est un homomorphisme d'anneaux qui conserve l'élément neutre de la multiplication.

Théorème Tout homomorphisme de corps est injectif.

Démonstration Soit $\sigma; K \longrightarrow L$ un homomorphisme de corps. $Ker(\sigma)$ est un idéal de K. $Ker(\sigma) \neq K$ car $\sigma(1) = 1$. Il en résulte $Ker(\sigma) = (0)$ et par suite σ est injectif.

Un homomorphisme injectif de corps $\sigma; K \longrightarrow L$ sera dit un **isomorphisme** de K dans L. Le but de ce chapitre est de répondre à la question suivante :

Question : Ayant un isomorphisme $\sigma; K \longrightarrow K'$, une extension simple E de K et une extension E' de K', est-il possible de prolonger σ en un isomorphisme $\overline{\sigma}$ de E dans E' ?

Définition Soit E et F deux extensions du même corps K. Un isomorphisme $\sigma; E \longrightarrow F$ de E dans F sera appelé un **K-isomorphisme** si, et seulement si, il laisse fixe tout élément de K c.à.d. $\sigma(k) = k$ pour tout $k \in K$.

Exemple L'application $\varphi; \mathbb{C} \longrightarrow \mathbb{C}$ définie par $\varphi(u) = \overline{u}$ (le conjugué de u) est un $\mathbb{R}$-isomorphisme de $\mathbb{C}$ dans $\mathbb{C}$.

Théorème Soit E et F deux extensions du même corps K et $\sigma; E \longrightarrow F$ un K-isomorphisme. σ est une application K-linéaire.

Démonstration Nous avons

$$\sigma(ax) = \sigma(a)\sigma(x) = a\sigma(x) \text{ pour tout } (a,x) \in K \times E.$$

Théorème Soit $\sigma; K \longrightarrow K'$ un isomorphisme de K sur K', E une extension de K, E' une extension de K' et $\overline{\sigma}; E \longrightarrow E'$ un isomorphisme qui prolonge σ. Nous avons $[\overline{\sigma}(E) : K'] = [E : K]$.

Démonstration Soit $b = \{e_1,...,e_n\}$ une base du K-espace vectoriel E et soit $f_i = \overline{\sigma}(e_i)$ pour $i = 1,2,...,n$. La famille $\{f_1,...,f_n\}$ est une base du K'-espace vectoriel $\overline{\sigma}(E)$.

En effet, tout élément $y=\overline{\sigma}(x)\in\overline{\sigma}(E)$ peut s'écrire sous la forme

$$\begin{aligned} y=\overline{\sigma}(x)&=\overline{\sigma}(x_1e_1+\cdots+x_ne_n)\\ &=\overline{\sigma}(x_1)\overline{\sigma}(e_1)+\cdots+\overline{\sigma}(x_n)\overline{\sigma}(e_n)\\ &=\sigma(x_1)\,f_1+\cdots+\sigma(x_n)\,f_n \end{aligned}$$

ce qui prouve que $\{f_1,...,f_n\}$ est une famille génératrice du K'-espace vectoriel $\overline{\sigma}(E)$. Les f_i sont linéairement indépendants : Supposons avoir

$$b_1f_1+\cdots+b_nf_n=0.$$

Comme σ est une application surjective, il existe, pour $i=1,2,...,n$, $a_i\in K$ tel que $b_i=\sigma(a_i)$. Nous obtenons

$$\begin{aligned} &\overline{\sigma}(a_1e_1+\cdots+a_ne_n)=\overline{\sigma}(a_1)\overline{\sigma}(e_1)+\cdots+\overline{\sigma}(a_n)\overline{\sigma}(e_n)\\ &=b_1f_1+\cdots+b_nf_n=0. \end{aligned}$$

Cette relation implique $a_1e_1+\cdots+a_ne_n=0$ et $a_i=0$ pour $i=1,2,..,n$. D'où $b_i=0$ pour $i=1,2,..,n$ ce qui achève la démonstration.

2 Prolongement d'isomorphismes

Soit $\sigma;K\longrightarrow K'$ un isomorphisme de K sur K' , $E=K(a)$ une extension simple de K et E' une extension de K'. Nous allons étudier la question du prolongement de σ en un isomorphisme de E dans E'.

2.1 Cas où a est transcendant sur K

Théorème σ peut être prolongé d'une manière unique en un isomorphime

$$\widehat{\sigma};K[X]\longrightarrow K'[X]$$

qui transforme X en X.

Démonstration Soit $\widehat{\sigma};K[X]\longrightarrow K'[X]$ l'application définie par

$$\widehat{\sigma}(a_0+a_1X+\cdots+a_nX^n)=\sigma(a_0)+\sigma(a_1)X+\cdots+\sigma(a_n)X^n.$$

C'est un simple exercice de prouver que $\widehat{\sigma}$ est un homomorphisme d'anneaux vérifiant $\widehat{\sigma}(X)=X$ et $\widehat{\sigma}(k)=\sigma(k)$ pour tout $k\in K$. $\widehat{\sigma}$ est injective, car si nous avons

$$\widehat{\sigma}(P)=\widehat{\sigma}(a_0+a_1X+\cdots+a_nX^n)=0$$

alors $\sigma(a_i)=0$ pour $i=0,1,...,n$. Il en résulte $a_i=0$ pour $i=0,1,...,n$ et $P=0$. $\widehat{\sigma}$ est l'unique isomorphisme qui vérifie $\widehat{\sigma}(X)=X$ et $\widehat{\sigma}(k)=\sigma(k)$ pour tout $k\in K$ car, si τ est une autre solution, alors nous avons

$$\begin{aligned}\tau(a_0+a_1X+\cdots+a_nX^n) &= \tau(a_0)+\tau(a_1)+\cdots+\tau(a_n)X^n\\ &= \sigma(a_0)+\sigma(a_1)X+\cdots+\sigma(a_n)X^n\\ &= \widehat{\sigma}(P).\end{aligned}$$

pour tout $P\in K[X]$.

Théorème Si E' est une extension de K' qui contient un élément a' transcendant sur K', alors on peut prolonger σ:$K\to K'$ d'une manière unique en un isomorphisme $E\to E'$ qui transforme a en a'.

Démonstration Soit $F'=K'(a')$. F'est une extension de K' isomorphe à $K'(X)$ car a' est transcendant sur K'. On peut prolonger σ en un isomorphisme $\widehat{\sigma};K[X]\longrightarrow K'[X]$ par

$$\widehat{\sigma}(a_0+a_1X+\cdots+a_nX^n)=\sigma(a_0)+\sigma(a_1X)+\cdots+\sigma(a_n)X^n.$$

$\widehat{\sigma}$ est l'unique prolongement de σ qui vérifie $\widehat{\sigma}(X)=X$ et $\widehat{\sigma}(k)=\sigma(k)$ pour tout $k\in K$. Cet isomorphisme $\widehat{\sigma}$ peut être prolongé, d'une manière unique, en un isomorphisme σ' de $K(X)$, corps des fractions de $K[X]$, dans $K'(X)$, corps des fractions de $K'[X]$, tel que $\sigma'(X)=X$ et $\sigma'(k)=\sigma(k)$ pour tout $k\in K$. Finalement, soit u l'unique isomorphisme de $K(a)$ sur $K(X)$ tel que $u(a)=X$ et u' l'unique isomorphisme de $K'(X)$ sur $K'(a')$ tel que $u'(X)=a'$. Nous avons

$$\begin{array}{ccccccc} & & K & \xrightarrow{\sigma} & K' & & \\ & & \downarrow & & \downarrow & & \\ & & K[X] & \xrightarrow{\widehat{\sigma}} & K'[X] & & \\ & & \downarrow & & \downarrow & & \\ K(a) & \xrightarrow{u} & K(X) & \xrightarrow{\sigma'} & K'(X) & \xrightarrow{u'} & K'(a') \end{array}$$

où les flêches verticales sont les injections canoniques. Posons $\overline{\sigma}=u'\circ\sigma'\circ u$. $\overline{\sigma}$ est un isomorphisme et il vérifie

$$\overline{\sigma}(a)=\left(u'\circ\sigma'\circ u\right)(a)=u'\left(\sigma'(u(a))\right)=u'\left(\sigma'(X)\right)=u'(X)=a'$$

et

$$\overline{\sigma}(k)=\left(u'\circ\sigma'\circ u\right)(k)=u'\left(\sigma'(u(k))\right)=u'\left(\sigma'(k)\right)=u'(\sigma(k))=\sigma(k)$$

$\overline{\sigma}$ est unique, car $\widehat{\sigma}$,σ',u et u' sont tous uniques.

Remarque Si $E'=K'(a')$ alors $\overline{\sigma}$ est bijectif.

Théorème Si σ peut être prolongé en un isomorphisme $\overline{\sigma}$, alors $a'=\overline{\sigma}(a)$ est transcendant sur K'.

Démonstration Sinon, il existe des éléments $b'_0,b'_1,...,b'_n$, non tous nuls, tels que

$$b'_0 + b'_1 a' + \cdots + b'_n \left(a'\right)^n = 0.$$

Mais chaque b'_i peut s'écrire sous la forme $b'_i = \sigma(b_i)$, il en résulte

$$\begin{aligned}\overline{\sigma}(b_0 + b_1 a + \cdots + b_n a^n) &= \overline{\sigma}(b_0) + \overline{\sigma}(b_1) a' + \cdots + \overline{\sigma}(b_n) (a^n) \\ &= b'_0 + b'_1 a' + \cdots + b'_n \left(a'\right)^n = 0\end{aligned}$$

qui implique $b_0 + b_1 a + \cdots + b_n a^n = 0$, avec les b_i non tous nuls, qui prouve que a est algébrique sur K en contradiction l'hypothèse que a est transcendant sur K.

Ce qui précède permet d'énoncer :

Théorème σ peut être prolongé en un isomorphisme $\overline{\sigma}$ de $E = K(a)$ dans E' si, et seulement si, E' contient un élément a' transcendant sur K'.

2.2 Cas où a est algébrique sur K

Théorème Si E' contient un élément a' algébrique sur K' tel que

$$\widehat{\sigma}(Irr(a,K)) = Irr\left(a',K'\right),$$

alors on peut prolonger σ d'une manière unique en un isomorphisme qui transforme a en a'..

Démonstration Soit $I(a)$ (resp. $I(a')$) l'idéal de $K[X]$ (resp. de $K'[X]$) engendré par $Irr(a,K)$ (resp. par $Irr(a',K')$), u (resp. u') l'unique isomorphisme de $K(a)$ (resp. $K'[X]/I(a')$) sur $K[X]/I(a)$ (resp. $K'(a')$) tel que $u(a) = \overline{X}$ (resp. $u'\left(\overline{X}\right) = a'$). Comme dans le cas où a est transcendant sur K, σ peut être prolongé en $\widehat{\sigma}$. $\widehat{\sigma}$ peut être prolongé en un isomorphisme σ' de $K[X]/I(a)$ sur $K'[X]/I(a')$ car, nous avons $\widehat{\sigma}(I(a)) \subseteq I(a',K')$ du fait que $\widehat{\sigma}(Irr(a,K)) = Irr(a',K')$. Nous obtenons

$$\begin{array}{ccccccc} & & K & \xrightarrow{\sigma} & K' & & \\ & & \downarrow & & \downarrow & & \\ & & K[X] & \xrightarrow{\widehat{\sigma}} & K'[X] & & \\ & & \downarrow & & \downarrow & & \\ K(a) & \xrightarrow{u} & K[X]/I(a) & \xrightarrow{\sigma'} & K'[X]/I(a') & \xrightarrow{u'} & K'(a') \end{array}$$

où les flêches verticales du premier niveau sont les injections canoniques et celles du second niveau sont les surjections canoniques. Posons $\overline{\sigma} = u' \circ \sigma' \circ u$. $\overline{\sigma}$ est un isomorphisme et il vérifie

$$\overline{\sigma}(a) = \left(u' \circ \sigma' \circ u\right)(a) = u'\left(\sigma'\left(u(a)\right)\right) = u'\left(\sigma'\left(\overline{X}\right)\right) = u'\left(\overline{X}\right) = a'$$

et

$$\overline{\sigma}(k) = \left(u' \circ \sigma' \circ u\right)(k) = u'\left(\sigma'\left(u(k)\right)\right) = u'\left(\sigma'(k)\right) = u'(\sigma(k)) = \sigma(k)$$

$\overline{\sigma}$ est unique car $\widehat{\sigma}$,σ',u et u' sont tous uniques.

Remarque Si $E' = K'(a')$, alors $\overline{\sigma}$ est bijectif.

Théorème Si σ peut être prolongé en un isomorphisme $\overline{\sigma}$, alors $a' = \overline{\sigma}(a)$ est algébrique sur K' et $\widehat{\sigma}(Irr(a,K)) = Irr(a',K')$.

Démonstration Soit $P = b_0 + b_1X + \cdots + X^n$ le polynôme minimal de a sur K. Nous avons

$$b_0 + b_1a + \cdots + b_na^n = 0$$

et

$$0 = \overline{\sigma}(b_0 + b_1a + \cdots + a^n) = \overline{\sigma}(b_0) + \overline{\sigma}(b_1)a' + \cdots + \overline{\sigma}(a')^n$$

qui prouve que a' est algébrique sur K'. Le polynôme

$$P' = b'_0 + b'_1X + \cdots + X^n$$

où $b'_i = \overline{\sigma}(b_i) = \sigma(b_i)$ est irréductible dans $K'[X]$ car $\widehat{\sigma}$ est un isomorphisme et P est irréductible dans $K[X]$. D'où

$$Irr(a',K') = P' = \widehat{\sigma}(P) = \widehat{\sigma}(Irr(a,K)).$$

Ce qui précède nous permet d'énoncer :

Théorème σ peut être prolongé en un isomorphisme $\overline{\sigma}$ de $E = K(a)$ dans E' si, et seulement si, E' contient un élément a' algébrique sur K' tel que $\widehat{\sigma}(Irr(a,K)) = Irr(a',K')$.

Les théorèmes précédents peuvent être résumés en :

Théorème Si $\sigma; K \longrightarrow K'$, $E = K(a)$ est une extension simple de K et $E' = K'(a')$ une extension simple de K', alors il est possible de prolonger σ en un isomorphisme $\overline{\sigma}$ de E dans E' tel que $\overline{\sigma}(a) = a'$ si, et seulement si, une des deux conditions suivantes est vérifiée :

- a est transcendant sur K et a' est transcendant sur K'.
- a est algébrique sur K, a' est algébrique sur K' et

$$\widehat{\sigma}(Irr(a,K)) = Irr(a',K').$$

Théorème Si $E = K(a)$ et $E' = K(a')$ sont deux extensions simples du même corps K, alors il existe un K-isomorphisme $\overline{\sigma}$ de E sur E' tel que $\overline{\sigma}(a) = a'$ si, et seulement si, une des deux conditions suivantes est vérifiée :

- a et a' sont tous les deux transcendants sur K.

– a et a' sont tous les deux algébriques sur K et $Irr(a,K) = Irr(a',K)$.

3 Unicité du corps des racines

Théorème Soit $\sigma; K \longrightarrow K'$ un isomorphisme de corps, $P \in K[X]$, $P' = \widehat{\sigma}(P)$, R un corps des racines pour P sur K et R' un corps des racines pour P' sur K'. R s'écrit $R = K(a_1,...,a_n)$ où $a_1,...,a_n$ sont les racines de P dans R. Nous avons aussi $R' = K'(a'_1,...,a'_n)$ où $a'_1,...,a'_n$ sont les racines de P' dans R'. Soit $R_i = K(a_1,...,a_i)$ pour $i = 1,2,..,n$. Il est possible de prolonger σ en un isomorphisme de R sur R'.

Démonstration Nous allons prouver par récurrence sur i, que σ peut être prolongé en un isomorphisme σ_i de R_i dans R'. Pour $i = 1$, le résultat est vrai. En effet, $Irr(a_1,K)$ est un facteur irréductible de P. Ainsi, le polynôme $\widehat{\sigma}(Irr(a_1,K))$ est un facteur irréductible de P'. Un des éléments $a'_1,...,a'_n$, soit a'_1, est une racine de ce facteur. On peut alors prolonger σ en un isomorphisme σ_1 de R_1 dans R'. Supposons σ prolongé en un isomorphisme σ_i de R_i dans R'. Or $R_{i+1} = R_i(a_i)$. En raisonnant comme avant, on peut prolonger σ_i en un isomorphisme σ_{i+1} de R_{i+1} dans R'. Pour $i = n$, nous avons un isomorphisme σ_n de $R_n = R$ dans R' qui prolonge σ. D'où

$$[R : K] = \left[\sigma_n(R) : K'\right] \leq \left[R' : K'\right].$$

D'une manière similaire, nous avons $\left[R' : K'\right] \leq [R : K]$ et par suite,

$$[R : K] = \left[\sigma_n(R) : K'\right] = \left[R' : K'\right].$$

Ceci prouve $\sigma_n(R) = R'$.

Corollaire Deux corps des racines pour le polynôme $P \in K[X]$ sur K sont K-isomorphes.