

EXERCICE 1. Déterminez les $\mathbb{Q}$ -automorphismes de $\mathbb{Q}[7+3i]$ et de $\mathbb{Q}[a]$ où a est racine de $x^2 + 52$.

Un $\mathbb{Q}$ -automorphisme de $\mathbb{Q}[7+3i]$ est un automorphisme de corps qui laisse invariant les éléments de $\mathbb{Q}$.

On a $\mathbb{Q}[7+3i] = \mathbb{Q}[i]$. C'est donc une extension de degré 2 de $\mathbb{Q}$ puisque $x^2 + 1$ est le polynôme minimal de i . Une base du $\mathbb{Q}$ -espace vectoriel $\mathbb{Q}[i] = \mathbb{Q}[7+3i]$ est donc donnée par $\{1, i\}$. Un $\mathbb{Q}$ -automorphisme vérifie

$$\sigma(1) = 1 \quad \text{et} \quad \sigma(i) \sigma(i) = \sigma(i^2) = \sigma(-1) = -1 \quad \text{donc}$$

$$\sigma(i) = \pm i. \quad \text{Il existe donc 2 } \mathbb{Q}\text{-automorphismes de}$$

$$\mathbb{Q}[7+3i] \text{ définis par } \begin{cases} \sigma_1 = \text{Id} \\ \sigma_2(1) = 1 \text{ et } \sigma_2(i) = -i. \end{cases}$$

On a $\mathbb{Q}[a] = \mathbb{Q}[2i\sqrt{13}] = \mathbb{Q}[i\sqrt{13}]$. C'est une extension de degré 2 de $\mathbb{Q}$ de base $\{1, i\sqrt{13}\}$. Un $\mathbb{Q}$ -automorphisme vérifie $\sigma(1) = 1$ et $\sigma(i\sqrt{13})\sigma(i\sqrt{13}) = \sigma(-13) = -13$ d'où $\sigma(i\sqrt{13}) = \pm i\sqrt{13}$.

On obtient donc deux $\mathbb{Q}$ -automorphismes de $\mathbb{Q}[a]$ définis par $\sigma_1 = \text{Id}$ et $(\sigma_2(1) = 1, \sigma_2(i\sqrt{13}) = -i\sqrt{13})$.

EXERCICE 2 : Soient K un corps, $\mathbb{Q} \subset K \subset \mathbb{C}$,
a un nombre ^{complexe} algébrique sur K de polynôme minimal P_a sur K . Toute racine de P_a dans $\mathbb{C}$ est appelée nombre conjugué de a sur K . Deux racines d'un polynôme irréductible de $K[x]$ sont dites conjuguées sur K .

- 1) Les nombres i et $-i$ sont-ils conjugués sur $\mathbb{Q}$? sur $\mathbb{R}$? sur $\mathbb{C}$?
- 2) Quels sont les conjugués de $\sqrt{2}$ sur $\mathbb{Q}$? sur $\mathbb{Q}[\sqrt{2}]$?
- 3) Quels sont les conjugués de $\sqrt[3]{2}$ sur $\mathbb{Q}$?

- 1) Le polynôme minimal de i sur $\mathbb{Q}$ est $x^2 + 1$. Le nombre $-i$ est donc aussi racine de $x^2 + 1$ et i et $-i$ sont donc conjugués sur $\mathbb{Q}$. Il en est de même sur $\mathbb{R}$. Mais sur $\mathbb{C}$, le polynôme minimal de i est $x - i$ et i n'a donc pas de conjugué sur $\mathbb{C}$.

- 2) Le nombre $\sqrt{2}$ a pour polynôme minimal $X^2 - 2$ sur $\mathbb{Q}$.
 Ce polynôme a pour racines $\sqrt{2}$ et $-\sqrt{2}$ qui sont donc conjugués sur $\mathbb{Q}$. Mais sur $\mathbb{Q}[\sqrt{2}]$ le polynôme minimal de $\sqrt{2}$ est $X - \sqrt{2}$ et $\sqrt{2}$ n'a pas de conjugué sur $\mathbb{Q}[\sqrt{2}]$.
- 3) Le nombre $\sqrt[3]{2}$ a pour polynôme minimal $X^3 - 2$ sur $\mathbb{Q}$ (ce polynôme est bien irréductible sur $\mathbb{Q}$ d'après le critère d'Eisenstein) et on a $[\mathbb{Q}[\sqrt[3]{2}]; \mathbb{Q}] = 3$.
 Les racines de $X^3 - 2$ dans $\mathbb{C}$ sont $\sqrt[3]{2}$, $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$ qui sont donc conjugués sur $\mathbb{Q}$.

EXERCICE 3 : Soient K un corps, a un élément algébrique de degré n de polynôme minimal P sur K .

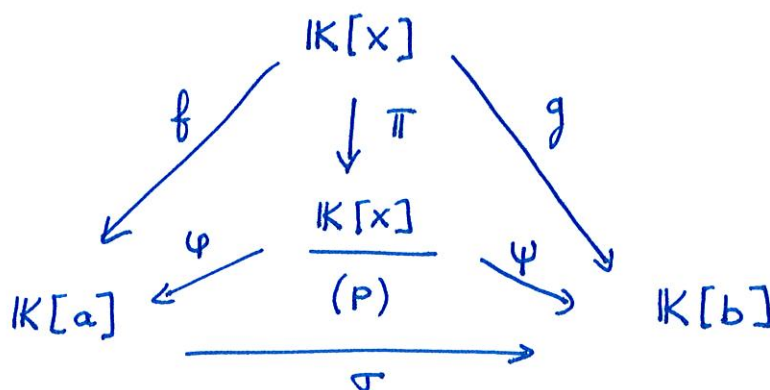
- 1) Si L est une extension de K contenant a et si $\sigma: L \rightarrow \mathbb{C}$ est un K -homomorphisme, alors montrer que $\sigma(a)$ est un conjugué de a sur K .
- 2) Montrer que si b est un conjugué de a sur K , il existe un K -isomorphisme unique $\sigma: K[a] \rightarrow K[b]$ tel que $\sigma(a) = b$.
- 3) Montrer que le nombre de K -homomorphismes distincts de $K[a]$ dans $\mathbb{C}$ est n .

- 1) Soit $P(x) = \sum_{k=0}^n \alpha_k x^k$ le polynôme minimal de a sur K .
 On a $P(a) = 0$. $\alpha_k \in K$.

Si σ est un K -homomorphisme puisque $\alpha_k \in K$ on a $\sigma(\alpha_k) = \alpha_k$
 d'où $P(\sigma(a)) = \sum_{k=0}^n \alpha_k (\sigma(a))^k = \sigma\left(\sum_{k=0}^n \alpha_k a^k\right) = \sigma(P(a)) = 0$

donc $\sigma(a)$ est un conjugué de a sur K .

- 2) Considérons



où π est la surjection canonique
 f l'homomorphisme défini par $f(x) = a$
 g l'homomorphisme défini par $g(x) = b$

ψ et φ sont les factorisations respectives de f et g par π , ce sont des isomorphismes.

Posons $\sigma = \psi\varphi^{-1}$. C'est un isomorphisme de corps :
on a $\sigma f = \psi\varphi^{-1}f = \psi\pi = g$ d'où

$$\sigma(a) = \sigma(f(x)) = g(x) = b,$$

$$\text{et pour tout } \alpha \in K \quad \sigma(\alpha) = \sigma(f(\alpha)) = g(\alpha) = \alpha.$$

On veut de montrer l'existence de σ , montrons l'unicité.

Si σ' vérifie les mêmes propriétés σf et $\sigma' f$ sont l'identité restreinte à K et $\sigma f(x) = b = \sigma' f(x)$. On a alors $\sigma f = \sigma' f$ et puisque f est surjective on en déduit $\sigma = \sigma'$. Ainsi un élément de $K[a]$ de la forme $\sum_{k=0}^n \alpha_k a^k$ a pour image $\sum_{k=0}^n \alpha_k b^k$ par σ .

3) Puisque P est irréductible de degré n , il a n racines distinctes dans $\mathbb{C}$ (toute racine d'un polynôme minimal d'un élément algébrique est simple). Chacune de ces racines permet de construire un unique K -isomorphisme de $K[a]$ sur un sous-corps de $\mathbb{C}$ (vu en 2) et il n'y a pas d'autre manière de construire des K -homomorphismes de $K[a]$ dans $\mathbb{C}$. Il y en a donc n .

Si $a = a_1, a_2, \dots, a_n$ les racines de P dans $\mathbb{C}$

$$\text{Alors} \quad \begin{cases} \sigma_1(a) = a & \sigma_1(1) = 1 \\ \sigma_2(a) = a_2 & \sigma_2(1) = 1 \\ \vdots & \vdots \\ \sigma_n(a) = a_n & \sigma_n(1) = 1 \end{cases} \quad \begin{array}{l} \text{défini les } n \\ K\text{-homomorphismes} \end{array}$$

EXERCICE 4 : Déterminer tous les sous-corps de $\mathbb{C}$ qui sont $\mathbb{Q}$ -isomorphes à $\mathbb{Q}[\sqrt{3}]$, à $\mathbb{Q}[\sqrt[3]{15}]$, à $\mathbb{Q}[\sqrt[5]{3}]$, à $\mathbb{Q}[\sqrt[6]{3}]$.

$\mathbb{Q}[\sqrt{3}]$ est une extension de degré 2 de $\mathbb{Q}$ puisque le polynôme minimal de $\sqrt{3}$ dans $\mathbb{Q}$ est $X^2 - 3$ (irréductible dans $\mathbb{Q}$ d'après Eisenstein). Les deux racines de $X^2 - 3$ dans $\mathbb{C}$ sont $\sqrt{3}$ et $-\sqrt{3}$. On a donc $\mathbb{Q}[\sqrt{3}]$ isomorphe à $\mathbb{Q}[-\sqrt{3}]$ mais en fait $\mathbb{Q}[\sqrt{3}] = \mathbb{Q}[-\sqrt{3}]$.

On a donc 2 $\mathbb{Q}$ -automorphismes de $\mathbb{Q}[\sqrt[3]{15}]$ défini par
 $\sigma_1 = \text{Id}$ et $(\sigma_2(1) = 1, \sigma_2(\sqrt[3]{15}) = -\sqrt[3]{15})$.

Le polynôme minimal de $\sqrt[3]{15}$ sur $\mathbb{Q}$ est $X^3 - 15$. Les 3 racines de ce polynôme sont $\sqrt[3]{15}$, $j\sqrt[3]{15}$ et $j^2\sqrt[3]{15}$ qui sont donc conjugués sur $\mathbb{Q}$. Les corps $\mathbb{Q}[\sqrt[3]{15}]$, $\mathbb{Q}[j\sqrt[3]{15}]$ et $\mathbb{Q}[j^2\sqrt[3]{15}]$ sont donc $\mathbb{Q}$ -isomorphes. De plus ces 3 corps sont bien distincts : le premier est contenu dans $\mathbb{R}$ contrairement aux deux autres. Si $\mathbb{Q}[j\sqrt[3]{15}] = \mathbb{Q}[j^2\sqrt[3]{15}]$ alors $\frac{j^2\sqrt[3]{15}}{j\sqrt[3]{15}}$ appartiendrait aussi à $\mathbb{Q}[j\sqrt[3]{15}]$ donc $j \in \mathbb{Q}[j\sqrt[3]{15}]$

et de même $\frac{j\sqrt[3]{15}}{j^2\sqrt[3]{15}} = \sqrt[3]{15} \in \mathbb{Q}[j\sqrt[3]{15}]$.
 Ainsi on aurait $\mathbb{Q}[j, \sqrt[3]{15}] = \mathbb{Q}[\sqrt[3]{15}][j]$ serait inclus dans $\mathbb{Q}[j\sqrt[3]{15}]$. Or $\mathbb{Q}[j, \sqrt[3]{15}]$ est une extension de degré $2 \times 3 = 6$ alors que $\mathbb{Q}[j\sqrt[3]{15}]$ est une extension de degré 3 sur $\mathbb{Q}$.
 Donc $\mathbb{Q}[j\sqrt[3]{15}] \neq \mathbb{Q}[j^2\sqrt[3]{15}]$.

$\mathbb{Q}[\sqrt[5]{3}]$. $\sqrt[5]{3}$ a pour polynôme minimal $X^5 - 3$ sur $\mathbb{Q}$. Les 5 racines de ce polynôme sont $\sqrt[5]{3}$, $\zeta\sqrt[5]{3}$, $\zeta^2\sqrt[5]{3}$, $\zeta^3\sqrt[5]{3}$ et $\zeta^4\sqrt[5]{3}$ avec $\zeta = e^{\frac{2\pi i}{5}}$. Les corps $\mathbb{Q}[\sqrt[5]{3}]$, $\mathbb{Q}[\zeta\sqrt[5]{3}]$, $\mathbb{Q}[\zeta^2\sqrt[5]{3}]$, $\mathbb{Q}[\zeta^3\sqrt[5]{3}]$ et $\mathbb{Q}[\zeta^4\sqrt[5]{3}]$ sont isomorphes et tous distincts (on le montre par une démonstration analogue à celle faite ci-dessus).

$\mathbb{Q}[\sqrt[6]{3}]$. $\sqrt[6]{3}$ a pour polynôme minimal $X^6 - 3$ sur $\mathbb{Q}$. Les 6 racines sont $\pm\sqrt[6]{3}$, $\pm j\sqrt[6]{3}$ et $\pm j^2\sqrt[6]{3}$. Le corps $\mathbb{Q}[\sqrt[6]{3}]$ est $\mathbb{Q}$ -isomorphe à $\mathbb{Q}[\sqrt[6]{3}]$, $\mathbb{Q}[j\sqrt[6]{3}]$ et $\mathbb{Q}[j^2\sqrt[6]{3}]$ l'isomorphisme étant défini resp. par $\sigma(\sqrt[6]{3}) = \sqrt[6]{3}$, $\sigma(j\sqrt[6]{3}) = j\sqrt[6]{3}$ et $\sigma(j^2\sqrt[6]{3}) = j^2\sqrt[6]{3}$. Les 3 corps sont bien distincts. $\mathbb{Q}[\sqrt[6]{3}] \subset \mathbb{R}$ alors que $\mathbb{Q}[j\sqrt[6]{3}] \not\subset \mathbb{R} \not\subset \mathbb{Q}[j^2\sqrt[6]{3}]$. De plus $\mathbb{Q}[j\sqrt[6]{3}] \neq \mathbb{Q}[j^2\sqrt[6]{3}]$ car $\mathbb{Q}[j\sqrt[6]{3}] = \mathbb{Q}[j^2\sqrt[6]{3}]$ impliquerait que j et $\sqrt[6]{3}$ sont dans $\mathbb{Q}[j\sqrt[6]{3}]$ d'où $\mathbb{Q}[j, \sqrt[6]{3}] \subset \mathbb{Q}[j\sqrt[6]{3}]$ Or $[\mathbb{Q}[j, \sqrt[6]{3}], \mathbb{Q}] = 6$ et $[\mathbb{Q}[j\sqrt[6]{3}], \mathbb{Q}] = 3$. D'où une contradiction et les corps $\mathbb{Q}[j\sqrt[6]{3}]$ et $\mathbb{Q}[j^2\sqrt[6]{3}]$ sont distincts.

EXERCICE 5 : Déterminer les $\mathbb{Q}$ -automorphismes de

1) $\mathbb{Q}[\sqrt{2}]$

2) $\mathbb{Q}[\sqrt[4]{2}]$

1) L'élément $\sqrt{2} \notin \mathbb{Q}$ est de degré 2 sur $\mathbb{Q}$ puisque $X^2 - 2 = P$ est le polynôme minimal de $\sqrt{2}$ sur $\mathbb{Q}$. L'autre racine de P est $-\sqrt{2}$. Les $\mathbb{Q}$ -automorphismes de $\mathbb{Q}[\sqrt{2}]$ sont alors définis par $\sigma_1 = \text{Id}$ et $\begin{cases} \sigma_2(1) = 1 \\ \sigma_2(\sqrt{2}) = -\sqrt{2} \end{cases}$.

2) L'élément $\sqrt[4]{2} \notin \mathbb{Q}$ est de degré 4 sur $\mathbb{Q}$ et admet $P = X^4 - 2$ comme polynôme minimal. Les racines de P sont $\sqrt[4]{2}$, $-\sqrt[4]{2}$, $i\sqrt[4]{2}$ et $i^2\sqrt[4]{2}$. On a 4 $\mathbb{Q}$ -homomorphismes de $\mathbb{Q}[\sqrt[4]{2}]$ sur $\mathbb{C}$ définis par $\sigma_1 = \text{Id}$, $(\sigma_2(1) = 1, \sigma_2(\sqrt[4]{2}) = -\sqrt[4]{2})$, $(\sigma_3(1) = 1, \sigma_3(\sqrt[4]{2}) = i\sqrt[4]{2})$, $(\sigma_4(1) = 1, \sigma_4(\sqrt[4]{2}) = -i\sqrt[4]{2})$. Deux seulement sont des $\mathbb{Q}$ -automorphismes de $\mathbb{Q}[\sqrt[4]{2}]$; ce sont σ_1 et σ_2 . (en effet $\mathbb{Q}[\sqrt[4]{2}] = \mathbb{Q}[-\sqrt[4]{2}]$).

EXERCICE 6 : Déterminer les $\mathbb{Q}$ -homomorphismes de $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ dans $\mathbb{C}$.