L'absence d'une formule pour les racines de polynômes de degré 5

Dorothée Grondin

Université Laval

2024-08-06

Résolubilité par radicaux

Définition

Un polynôme f est `résoluble par radicaux` si les racines de f peuvent être exprimées avec les opérations suivantes: $+ - \times \div \sqrt[n]{}$

Polynôme de degré 2: $ax^2 + bx + x$	$f(x) = x^2 + 8x + 10$
Quand $f(x) = 0 : x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$	$x = \frac{-8 \pm \sqrt{64 - 4(1)(10)}}{2(1)}$

Les polynômes de degré 4 et moins sont toujours résolubles par radicaux.

Il existe une formule pour les polynômes de degré 3 et 4.

$x^5 - 6x + 3$ n'est pas résoluble par radicaux.

La théorie de Galois nous aide à comprendre pourquoi.

Résolubilité par radicaux

Définition

Un polynôme f est **résoluble par radicaux** si les racines de f peuvent être exprimées avec les opérations suivantes: $+ - \times \div \sqrt[n]{}$

Polynôme de degré 2: $ax^2 + bx + x$	$f(x) = x^2 + 8x + 10$
Quand $f(x) = 0 : x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$	$x = \frac{-8 \pm \sqrt{64 - 4(1)(10)}}{2(1)}$

Les polynômes de degré 4 et moins sont toujours résolubles par radicaux.

Il existe une formule pour les polynômes de degré 3 et 4.

$x^5 - 6x + 3$ n'est pas résoluble par radicaux.

La théorie de Galois nous aide à comprendre pourquoi.

Résolubilité par radicaux

Définition

Un polynôme f est **résoluble par radicaux** si les racines de f peuvent être exprimées avec les opérations suivantes: $+ - \times \div \sqrt[n]{\;}$

Polynôme de degré 2: $ax^2 + bx + x$	$f(x) = x^2 + 8x + 10$
Quand $f(x) = 0 : x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$	$x = \frac{-8 \pm \sqrt{64 - 4(1)(10)}}{2(1)}$

Les polynômes de degré 4 et moins sont toujours résolubles par radicaux.

Il existe une formule pour les polynômes de degré 3 et 4.

$x^5 - 6x + 3$ n'est pas résoluble par radicaux.

La théorie de Galois nous aide à comprendre pourquoi.

Résolubilité par radicaux

Définition

Un polynôme f est `résoluble par radicaux` si les racines de f peuvent être exprimées avec les opérations suivantes: $+ - \times \div \sqrt[n]{}$

Polynôme de degré 2: $ax^2 + bx + x$

Quand $f(x) = 0 : x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

$f(x) = x^2 + 8x + 10$

$x = \frac{-8 \pm \sqrt{64 - 4(1)(10)}}{2(1)}$

Les polynômes de degré 4 et moins sont toujours résolubles par radicaux.

Il existe une formule pour les polynômes de degré 3 et 4.

$x^5 - 6x + 3$ n'est pas résoluble par radicaux.

La théorie de Galois nous aide à comprendre pourquoi.

Résolubilité par radicaux

Définition

Un polynôme f est **résoluble par radicaux** si les racines de f peuvent être exprimées avec les opérations suivantes: $+ - \times \div \sqrt[n]{\ }$

Polynôme de degré 2: $ax^2 + bx + x$	$f(x) = x^2 + 8x + 10$
Quand $f(x) = 0 : x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$	$x = \frac{-8 \pm \sqrt{64 - 4(1)(10)}}{2(1)}$

Les polynômes de degré 4 et moins sont toujours résolubles par radicaux.

Il existe une formule pour les polynômes de degré 3 et 4.

$x^5 - 6x + 3$ n'est pas résoluble par radicaux.

La théorie de Galois nous aide à comprendre pourquoi.

Résolubilité par radicaux

Définition

Un polynôme f est **résoluble par radicaux** si les racines de f peuvent être exprimées avec les opérations suivantes: $+ - \times \div \sqrt[n]{\ }$

Polynôme de degré 2: $ax^2 + bx + x$	$f(x) = x^2 + 8x + 10$
Quand $f(x) = 0 : x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$	$x = \frac{-8 \pm \sqrt{64 - 4(1)(10)}}{2(1)}$

Les polynômes de degré 4 et moins sont toujours résolubles par radicaux.

Il existe une formule pour les polynômes de degré 3 et 4.

$x^5 - 6x + 3$ n'est pas résoluble par radicaux.

La théorie de Galois nous aide à comprendre pourquoi.

Résolubilité par radicaux

Définition

Un polynôme f est **résoluble par radicaux** si les racines de f peuvent être exprimées avec les opérations suivantes: $+\ -\ \times\ \div\ \sqrt[n]{\ }$

Polynôme de degré 2: ax^2+bx+x	$f(x)=x^2+8x+10$
Quand $f(x)=0: x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$	$x=\frac{-8\pm\sqrt{64-4(1)(10)}}{2(1)}$

Les polynômes de degré 4 et moins sont toujours résolubles par radicaux.

Il existe une formule pour les polynômes de degré 3 et 4.

x^5-6x+3 n'est pas résoluble par radicaux.

La théorie de Galois nous aide à comprendre pourquoi.

Polynômes irréductibles

Définition

Un polynôme est **irréductible** si il ne peut pas être factorisé. Sinon, on dit qu'un polynôme est **réductible** .

$x^2 - 2x + 1 = (x-1)^2$ est réductible dans $\mathbb{Q}$

$x^2 - 2$ est irréductible dans $\mathbb{Q}$

$x^2 - 2$ est réductible dans $\mathbb{R}$: $x^2 - 2 = (x-\sqrt{2})(x+\sqrt{2})$

Polynômes irréductibles

Définition

Un polynôme est `irréductible` si il ne peut pas être factorisé. Sinon, on dit qu'un polynôme est `réductible` .

$x^2 - 2x + 1 = (x-1)^2$ est réductible dans $\mathbb{Q}$

$x^2 - 2$ est irréductible dans $\mathbb{Q}$

$x^2 - 2$ est réductible dans $\mathbb{R}$: $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$

Polynômes irréductibles

Définition

Un polynôme est irréductible si il ne peut pas être factorisé. Sinon, on dit qu'un polynôme est réductible .

$x^2 - 2x + 1 = (x-1)^2$ est réductible dans $\mathbb{Q}$

$x^2 - 2$ est irréductible dans $\mathbb{Q}$

$x^2 - 2$ est réductible dans $\mathbb{R}$: $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$

Polynômes irréductibles

Définition

Un polynôme est `irréductible` si il ne peut pas être factorisé. Sinon, on dit qu'un polynôme est `réductible` .

$x^2 - 2x + 1 = (x-1)^2$ est réductible dans $\mathbb{Q}$

$x^2 - 2$ est irréductible dans $\mathbb{Q}$

$x^2 - 2$ est réductible dans $\mathbb{R}$: $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$

Polynômes irréductibles

Définition

Un polynôme est `irréductible` si il ne peut pas être factorisé. Sinon, on dit qu'un polynôme est `réductible` .

$x^2 - 2x + 1 = (x-1)^2$ est réductible dans $\mathbb{Q}$

$x^2 - 2$ est irréductible dans $\mathbb{Q}$

$x^2 - 2$ est réductible dans $\mathbb{R}$: $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$

Groupes

Définition

Un groupe est une structure algébrique qui consiste d'un ensemble et d'une opération permettant de combiner les éléments de l'ensemble en respectant certaines propriétés.

Exemple: $\mathbb{Z} = \{... - 1, 0, 1, 2, ...\}$ avec $+$

Ensemble avec opération qui satisfait plusieurs propriétés:

1) $a * b \in G$	$1 + 2 = 3 \in \mathbb{Z}$	(Clos)
2) $(a * b) * c = a * (b * c)$	$(1 + 2) + 3 = 1 + (2 + 3)$	(Associativité)
3) $\exists\ e : e * a = a * e = a$	$0 + 2 = 2 + 0 = 2$	(Élément neutre)
4) $a * a^{-1} = a^{-1} * a = e$	$2 + -2 = -2 + 2 = 0$	(Inverse)

Groupes

Définition

Un groupe est une structure algébrique qui consiste d'un ensemble et d'une opération permettant de combiner les éléments de l'ensemble en respectant certaines propriétés.

Exemple: $\mathbb{Z} = \{... -1, 0, 1, 2, ...\}$ avec $+$

Ensemble avec opération qui satisfait plusieurs propriétés:

1) $a * b \in G$	$1 + 2 = 3 \in \mathbb{Z}$	(Clos)
2) $(a * b) * c = a * (b * c)$	$(1 + 2) + 3 = 1 + (2 + 3)$	(Associativité)
3) $\exists\ e : e * a = a * e = a$	$0 + 2 = 2 + 0 = 2$	(Élément neutre)
4) $a * a^{-1} = a^{-1} * a = e$	$2 + -2 = -2 + 2 = 0$	(Inverse)

Groupes

Définition

Un groupe est une structure algébrique qui consiste d'un ensemble et d'une opération permettant de combiner les éléments de l'ensemble en respectant certaines propriétés.

Exemple: $\mathbb{Z} = \{... -1, 0, 1, 2, ...\}$ avec $+$

Ensemble avec opération qui satisfait plusieurs propriétés:

1) $a * b \in G$	$1 + 2 = 3 \in \mathbb{Z}$	(Clos)
2) $(a * b) * c = a * (b * c)$	$(1 + 2) + 3 = 1 + (2 + 3)$	(Associativité)
3) $\exists\ e : e * a = a * e = a$	$0 + 2 = 2 + 0 = 2$	(Élément neutre)
4) $a * a^{-1} = a^{-1} * a = e$	$2 + -2 = -2 + 2 = 0$	(Inverse)

Groupes

Définition

Un groupe est une structure algébrique qui consiste d'un ensemble et d'une opération permettant de combiner les éléments de l'ensemble en respectant certaines propriétés.

Exemple: $\mathbb{Z} = \{... - 1, 0, 1, 2, ...\}$ avec $+$

Ensemble avec opération qui satisfait plusieurs propriétés:

1) $a * b \in G$	$1 + 2 = 3 \in \mathbb{Z}$	(Clos)
2) $(a * b) * c = a * (b * c)$	$(1 + 2) + 3 = 1 + (2 + 3)$	(Associativité)
3) $\exists\ e : e * a = a * e = a$	$0 + 2 = 2 + 0 = 2$	(Élément neutre)
4) $a * a^{-1} = a^{-1} * a = e$	$2 + -2 = -2 + 2 = 0$	(Inverse)

Groupes

Définition

Un **groupe** est une structure algébrique qui consiste d'un ensemble et d'une opération permettant de combiner les éléments de l'ensemble en respectant certaines propriétés.

Exemple: $\mathbb{Z} = \{... - 1, 0, 1, 2, ...\}$ avec $+$

Ensemble avec opération qui satisfait plusieurs propriétés:

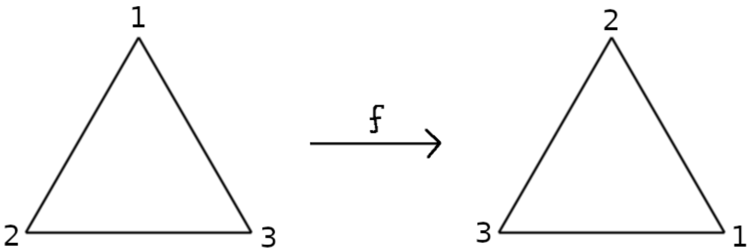
1) $a * b \in G$	$1 + 2 = 3 \in \mathbb{Z}$	(Clos)
2) $(a * b) * c = a * (b * c)$	$(1 + 2) + 3 = 1 + (2 + 3)$	(Associativité)
3) $\exists\ e : e * a = a * e = a$	$0 + 2 = 2 + 0 = 2$	(Élément neutre)
4) $a * a^{-1} = a^{-1} * a = e$	$2 + -2 = -2 + 2 = 0$	(Inverse)

Exemple de groupe

Symmétrie d'un triangle équilatéral

Groupe contenant des fonctions qui effectuent des rotations et des réflexions sur le triangle

Les fonctions de ce groupe font une permutation des sommets du triangle

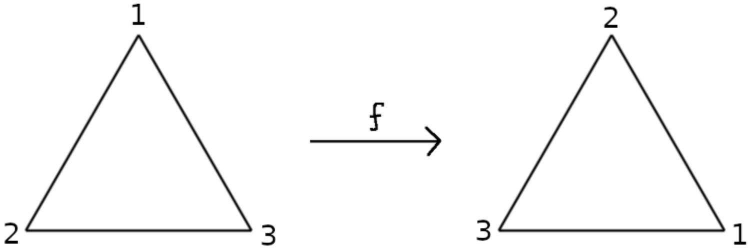


Exemple de groupe

Symmétrie d'un triangle équilatéral

Groupe contenant des fonctions qui effectuent des rotations et des réflexions sur le triangle

Les fonctions de ce groupe font une permutation des sommets du triangle

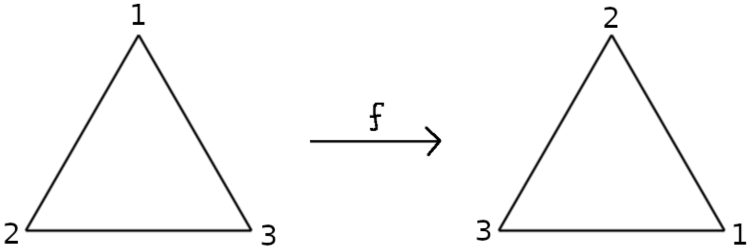


Exemple de groupe

Symmétrie d'un triangle équilatéral

Groupe contenant des fonctions qui effectuent des rotations et des réflexions sur le triangle

Les fonctions de ce groupe font une permutation des sommets du triangle

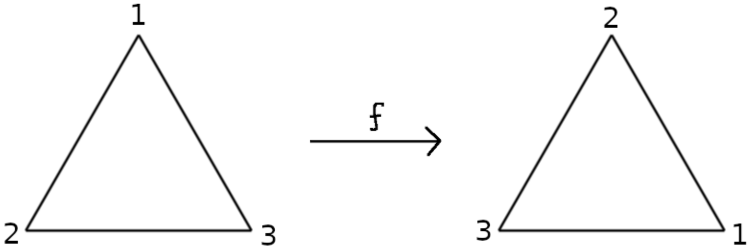


Exemple de groupe

Symmétrie d'un triangle équilatéral

Groupe contenant des fonctions qui effectuent des rotations et des réflexions sur le triangle

Les fonctions de ce groupe font une permutation des sommets du triangle

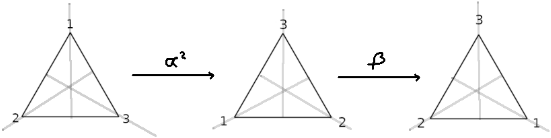


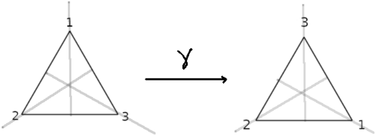
Exemple de groupe

Symétrie d'un triangle équilatéral

Les fonctions qui ne change pas le triangle équilatéral sont:

$\{e, \alpha, \alpha^2, \beta, \gamma, \delta\}$ où e est l'élément neutre, α est la rotation par 120 °, α^2 par 240 °, β la réflexion selon la première ligne, γ selon la deuxième et δ selon la troisième.



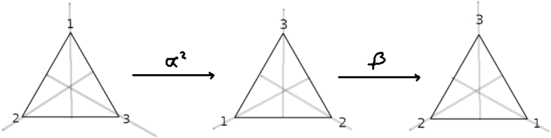


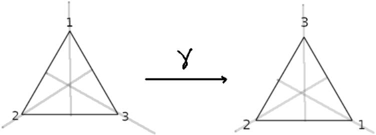
Exemple de groupe

Symmétrie d'un triangle équilatéral

Les fonctions qui ne change pas le triangle équilatéral sont:

$\{e, \alpha, \alpha^2, \beta, \gamma, \delta\}$ où e est l'élément neutre, α est la rotation par 120 °, α^2 par 240 °, β la réflexion selon la première ligne, γ selon la deuxième et δ selon la troisième.



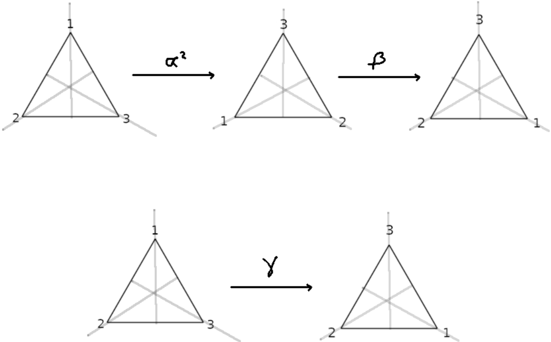


Exemple de groupe

Symétrie d'un triangle équilatéral

Les fonctions qui ne change pas le triangle équilatéral sont:

$\{e, \alpha, \alpha^2, \beta, \gamma, \delta\}$ où e est l'élément neutre, α est la rotation par 120 °, α^2 par 240 °, β la réflexion selon la première ligne, γ selon la deuxième et δ selon la troisième.

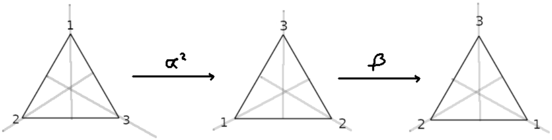


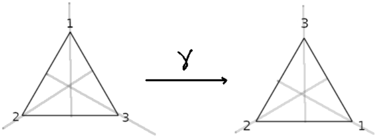
Exemple de groupe

Symmétrie d'un triangle équilatéral

Les fonctions qui ne change pas le triangle équilatéral sont:

$\{e, \alpha, \alpha^2, \beta, \gamma, \delta\}$ où e est l'élément neutre, α est la rotation par 120 °, α^2 par 240 °, β la réflexion selon la première ligne, γ selon la deuxième et δ selon la troisième.





Sous-groupe

Définition

Un **sous-groupe** H est un groupe à l'intérieur d'un groupe G qui satisfait plusieurs propriétés. Si $a, b \in \mathrm{H}$, alors $a * b^{-1} \in \mathrm{H}$.

Si on applique l'opération du groupe G sur deux éléments du sous-groupe H, le résultat doit être dans H

Les nombres paires sont un groupe avec l'addition:

Si on additionne deux nombres pairs, on obtient un autre nombre pair

Les nombres impairs ne sont pas un groupe avec l'addition:

Si on additionne deux nombres impairs, n'obtient pas un nombre impair

Sous-groupe

Définition

Un sous-groupe H est un groupe à l'intérieur d'un groupe G qui satisfait plusieurs propriétés. Si $a, b \in \mathrm{H}$, alors $a * b^{-1} \in \mathrm{H}$.

Si on applique l'opération du groupe G sur deux éléments du sous-groupe H, le résultat doit être dans H

Les nombres paires sont un groupe avec l'addition:

Si on additionne deux nombres pairs, on obtient un autre nombre pair

Les nombres impairs ne sont pas un groupe avec l'addition:

Si on additionne deux nombres impairs, n'obtient pas un nombre impair

Sous-groupe

Définition

Un sous-groupe H est un groupe à l'intérieur d'un groupe G qui satisfait plusieurs propriétés. Si $a, b \in \mathrm{H}$, alors $a * b^{-1} \in \mathrm{H}$.

Si on applique l'opération du groupe G sur deux éléments du sous-groupe H, le résultat doit être dans H

Les nombres paires sont un groupe avec l'addition:

Si on additionne deux nombres pairs, on obtient un autre nombre pair

Les nombres impairs ne sont pas un groupe avec l'addition:

Si on additionne deux nombres impairs, n'obtient pas un nombre impair

Sous-groupe

Définition

Un **sous-groupe** H est un groupe à l'intérieur d'un groupe G qui satisfait plusieurs propriétés. Si $a, b \in \mathrm{H}$, alors $a * b^{-1} \in \mathrm{H}$.

Si on applique l'opération du groupe G sur deux éléments du sous-groupe H, le résultat doit être dans H

Les nombres paires sont un groupe avec l'addition:

Si on additionne deux nombres pairs, on obtient un autre nombre pair

Les nombres impairs ne sont pas un groupe avec l'addition:

Si on additionne deux nombres impairs, n'obtient pas un nombre impair

Sous-groupe

Définition

Un sous-groupe H est un groupe à l'intérieur d'un groupe G qui satisfait plusieurs propriétés. Si $a, b \in \mathrm{H}$, alors $a * b^{-1} \in \mathrm{H}$.

Si on applique l'opération du groupe G sur deux éléments du sous-groupe H, le résultat doit être dans H

Les nombres paires sont un groupe avec l'addition:

Si on additionne deux nombres pairs, on obtient un autre nombre pair

Les nombres impairs ne sont pas un groupe avec l'addition:

Si on additionne deux nombres impairs, n'obtient pas un nombre impair

Sous-groupe

Définition

Un sous-groupe H est un groupe à l'intérieur d'un groupe G qui satisfait plusieurs propriétés. Si $a, b \in \mathrm{H}$, alors $a * b^{-1} \in \mathrm{H}$.

Si on applique l'opération du groupe G sur deux éléments du sous-groupe H, le résultat doit être dans H

Les nombres paires sont un groupe avec l'addition:

Si on additionne deux nombres pairs, on obtient un autre nombre pair

Les nombres impairs ne sont pas un groupe avec l'addition:

Si on additionne deux nombres impairs, n'obtient pas un nombre impair

Sous-groupe

Définition

Un sous-groupe H est un groupe à l'intérieur d'un groupe G qui satisfait plusieurs propriétés. Si $a, b \in \mathrm{H}$, alors $a * b^{-1} \in \mathrm{H}$.

Si on applique l'opération du groupe G sur deux éléments du sous-groupe H, le résultat doit être dans H

Les nombres paires sont un groupe avec l'addition:

Si on additionne deux nombres pairs, on obtient un autre nombre pair

Les nombres impairs ne sont pas un groupe avec l'addition:

Si on additionne deux nombres impairs, n'obtient pas un nombre impair

Corps numérique

Définition

Un `corps numérique` est une structure algébrique qui consiste d'un ensemble de nombres et de deux opérations permettant de combiner les éléments de l'ensemble en respectant certaines propriété.

Exemple: $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}\}$ avec $+$ et $\times$

Satisfait aussi plusieurs propriétés: éléments inverses (pour les deux opérations).

On peut additionner, soustraire, multiplier et diviser dans $\mathbb{Q}$.

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}$$

$$\frac{a}{b} - \frac{c}{d} = \frac{ad-cb}{bd}$$

$$\frac{a}{b} \times \frac{c}{d} = \frac{ab}{bd}$$

$$\frac{a}{b} \div \frac{c}{d} = \frac{ad}{bc}$$

Corps numérique

Définition

Un corps numérique est une structure algébrique qui consiste d'un ensemble de nombres et de deux opérations permettant de combiner les éléments de l'ensemble en respectant certaines propriété.

Exemple: $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}\}$ avec $+$ et $\times$

Satisfait aussi plusieurs propriétés: éléments inverses (pour les deux opérations).

On peut additioner, soustraire, multiplier et diviser dans $\mathbb{Q}$.

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}$$

$$\frac{a}{b} - \frac{c}{d} = \frac{ad-cb}{bd}$$

$$\frac{a}{b} \times \frac{c}{d} = \frac{ab}{bd}$$

$$\frac{a}{b} \div \frac{c}{d} = \frac{ad}{bc}$$

Corps numérique

Définition

Un **corps numérique** est une structure algébrique qui consiste d'un ensemble de nombres et de deux opérations permettant de combiner les éléments de l'ensemble en respectant certaines propriété.

Exemple: $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}\}$ avec $+$ et $\times$

Satisfait aussi plusieurs propriétés: éléments inverses (pour les deux opérations).

On peut additionner, soustraire, multiplier et diviser dans $\mathbb{Q}$.

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}$$

$$\frac{a}{b} - \frac{c}{d} = \frac{ad-cb}{bd}$$

$$\frac{a}{b} \times \frac{c}{d} = \frac{ab}{bd}$$

$$\frac{a}{b} \div \frac{c}{d} = \frac{ad}{bc}$$

Corps numérique

Définition

Un `corps numérique` est une structure algébrique qui consiste d'un ensemble de nombres et de deux opérations permettant de combiner les éléments de l'ensemble en respectant certaines propriété.

Exemple: $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}\}$ avec $+$ et $\times$

Satisfait aussi plusieurs propriétés: éléments inverses (pour les deux opérations).

On peut additioner, soustraire, multiplier et diviser dans $\mathbb{Q}$.

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}$$

$$\frac{a}{b} - \frac{c}{d} = \frac{ad-cb}{bd}$$

$$\frac{a}{b} \times \frac{c}{d} = \frac{ab}{bd}$$

$$\frac{a}{b} \div \frac{c}{d} = \frac{ad}{bc}$$

Corps numérique

Définition

Un corps numérique est une structure algébrique qui consiste d'un ensemble de nombres et de deux opérations permettant de combiner les éléments de l'ensemble en respectant certaines propriété.

Exemple: $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}\}$ avec $+$ et $\times$

Satisfait aussi plusieurs propriétés: éléments inverses (pour les deux opérations).

On peut additioner, soustraire, multiplier et diviser dans $\mathbb{Q}$.

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}$$
$$\frac{a}{b} - \frac{c}{d} = \frac{ad-cb}{bd}$$
$$\frac{a}{b} \times \frac{c}{d} = \frac{ab}{bd}$$
$$\frac{a}{b} \div \frac{c}{d} = \frac{ad}{bc}$$

Extensions de corps

Définition

Une extension de corps M : K (M par rapport à K) est un corps M créé à partir de K en y ajoutant des éléments.

Par exemple, $\mathbb{Q}(\sqrt{2})$ dénote les nombres rationels avec l'élément $\sqrt{2}$ ajouté.

$\mathbb{Q}(\sqrt{2})$ est le plus petit corps ayant $\mathbb{Q}$ et $\sqrt{2}$ comme éléments.

Les éléments $\sqrt{2}+6$, $5\sqrt{2}+17$, $\frac{37\sqrt{2}}{4}$ et $\frac{89}{59}$ sont dans $\mathbb{Q}(\sqrt{2})$

Extensions de corps

Définition

Une **extension de corps** M : K (M par rapport à K) est un corps M créé à partir de K en y ajoutant des éléments.

Par exemple, $\mathbb{Q}(\sqrt{2})$ dénote les nombres rationels avec l'élément $\sqrt{2}$ ajouté.

$\mathbb{Q}(\sqrt{2})$ est le plus petit corps ayant $\mathbb{Q}$ et $\sqrt{2}$ comme éléments.

Les éléments $\sqrt{2}+6$, $5\sqrt{2}+17$, $\frac{37\sqrt{2}}{4}$ et $\frac{89}{59}$ sont dans $\mathbb{Q}(\sqrt{2})$

Extensions de corps

Définition

Une `extension de corps` M : K (M par rapport à K) est un corps M créé à partir de K en y ajoutant des éléments.

Par exemple, $\mathbb{Q}(\sqrt{2})$ dénote les nombres rationels avec l'élément $\sqrt{2}$ ajouté.

$\mathbb{Q}(\sqrt{2})$ est le plus petit corps ayant $\mathbb{Q}$ et $\sqrt{2}$ comme éléments.

Les éléments $\sqrt{2}+6$, $5\sqrt{2}+17$, $\frac{37\sqrt{2}}{4}$ et $\frac{89}{59}$ sont dans $\mathbb{Q}(\sqrt{2})$

Extensions de corps

Définition

Une extension de corps M : K (M par rapport à K) est un corps M créé à partir de K en y ajoutant des éléments.

Par exemple, $\mathbb{Q}(\sqrt{2})$ dénote les nombres rationels avec l'élément $\sqrt{2}$ ajouté.

$\mathbb{Q}(\sqrt{2})$ est le plus petit corps ayant $\mathbb{Q}$ et $\sqrt{2}$ comme éléments.

Les éléments $\sqrt{2}+6$, $5\sqrt{2}+17$, $\frac{37\sqrt{2}}{4}$ et $\frac{89}{59}$ sont dans $\mathbb{Q}(\sqrt{2})$

Extensions de corps

Définition

Une extension de corps M : K (M par rapport à K) est un corps M créé à partir de K en y ajoutant des éléments.

Par exemple, $\mathbb{Q}(\sqrt{2})$ dénote les nombres rationels avec l'élément $\sqrt{2}$ ajouté.

$\mathbb{Q}(\sqrt{2})$ est le plus petit corps ayant $\mathbb{Q}$ et $\sqrt{2}$ comme éléments.

Les éléments $\sqrt{2}+6$, $5\sqrt{2}+17$, $\frac{37\sqrt{2}}{4}$ et $\frac{89}{59}$ sont dans $\mathbb{Q}(\sqrt{2})$

Corps de rupture

Définition

Un corps de rupture d'un polynôme irréductible f, dénoté $\mathbb{SF}_{\mathbb{Q}}(f)$ est le plus petit corps contenant toutes les racines de f.

$f(x) = x^2 - 2$ a pour racines $-\sqrt{2}, \sqrt{2}$.

On ajoute souvent les racines du polynôme étudié au corps $\mathbb{Q}$.

On ajoute $\sqrt{2}$ à $\mathbb{Q}$ et on obtient $\mathbb{Q}(\sqrt{2})$.

On a donc $\mathbb{SF}_{\mathbb{Q}}(x^2 - 2) = \mathbb{Q}(\sqrt{2})$

Corps de rupture

Définition

Un corps de rupture d'un polynôme irréductible f, dénoté $\mathbb{SF}_{\mathbb{Q}}(f)$ est le plus petit corps contenant toutes les racines de f.

$f(x) = x^2 - 2$ a pour racines $-\sqrt{2}, \sqrt{2}$.

On ajoute souvent les racines du polynôme étudié au corps $\mathbb{Q}$.

On ajoute $\sqrt{2}$ à $\mathbb{Q}$ et on obtient $\mathbb{Q}(\sqrt{2})$.

On a donc $\mathbb{SF}_{\mathbb{Q}}(x^2 - 2) = \mathbb{Q}(\sqrt{2})$

Corps de rupture

Définition

Un **corps de rupture** d'un polynôme irréductible f, dénoté $\mathbb{SF}_{\mathbb{Q}}(f)$ est le plus petit corps contenant toutes les racines de f.

$f(x) = x^2 - 2$ a pour racines $-\sqrt{2}, \sqrt{2}$.

On ajoute souvent les racines du polynôme étudié au corps $\mathbb{Q}$.

On ajoute $\sqrt{2}$ à $\mathbb{Q}$ et on obtient $\mathbb{Q}(\sqrt{2})$.

On a donc $\mathbb{SF}_{\mathbb{Q}}(x^2 - 2) = \mathbb{Q}(\sqrt{2})$

Corps de rupture

Définition

Un **corps de rupture** d'un polynôme irréductible f, dénoté $\mathbb{SF}_{\mathbb{Q}}(f)$ est le plus petit corps contenant toutes les racines de f.

$f(x) = x^2 - 2$ a pour racines $-\sqrt{2}, \sqrt{2}$.

On ajoute souvent les racines du polynôme étudié au corps $\mathbb{Q}$.

On ajoute $\sqrt{2}$ à $\mathbb{Q}$ et on obtient $\mathbb{Q}(\sqrt{2})$.

On a donc $\mathbb{SF}_{\mathbb{Q}}(x^2 - 2) = \mathbb{Q}(\sqrt{2})$

Corps de rupture

Définition

Un **corps de rupture** d'un polynôme irréductible f, dénoté $\mathbb{SF}_{\mathbb{Q}}(f)$ est le plus petit corps contenant toutes les racines de f.

$f(x) = x^2 - 2$ a pour racines $-\sqrt{2}, \sqrt{2}$.

On ajoute souvent les racines du polynôme étudié au corps $\mathbb{Q}$.

On ajoute $\sqrt{2}$ à $\mathbb{Q}$ et on obtient $\mathbb{Q}(\sqrt{2})$.

On a donc $\mathbb{SF}_{\mathbb{Q}}(x^2 - 2) = \mathbb{Q}(\sqrt{2})$

Corps de rupture

Définition

Un corps de rupture d'un polynôme irréductible f, dénoté $\mathbb{SF}_{\mathbb{Q}}(f)$ est le plus petit corps contenant toutes les racines de f.

$f(x) = x^2 - 2$ a pour racines $-\sqrt{2}, \sqrt{2}$.

On ajoute souvent les racines du polynôme étudié au corps $\mathbb{Q}$.

On ajoute $\sqrt{2}$ à $\mathbb{Q}$ et on obtient $\mathbb{Q}(\sqrt{2})$.

On a donc $\mathbb{SF}_{\mathbb{Q}}(x^2 - 2) = \mathbb{Q}(\sqrt{2})$

Degré d'une extension de corps

Définition

Le `degré d'une extension de corps` est le nombre de paramètres nécessaires pour représenter n'importe quel éléments de l'extension.

Le degré d'une extension M : K est dénoté [M : K].

$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

Les éléments de $\mathbb{Q}(\sqrt{2})$ peuvent être représentés par 2 paramètres: (a,b)

$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{2^2} : a, b, c \in \mathbb{Q}\}$.

Les éléments de $\mathbb{Q}(\sqrt{2})$ peuvent être représentés par 3 paramètres: (a,b,c)

Nous avons donc $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ et $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Degré d'une extension de corps

Définition

Le `degré d'une extension de corps` est le nombre de paramètres nécessaires pour représenter n'importe quel éléments de l'extension.

Le degré d'une extension M : K est dénoté [M : K].

$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

Les éléments de $\mathbb{Q}(\sqrt{2})$ peuvent être représentés par 2 paramètres: (a,b)

$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{2^2} : a, b, c \in \mathbb{Q}\}$.

Les éléments de $\mathbb{Q}(\sqrt{2})$ peuvent être représentés par 3 paramètres: (a,b,c)

Nous avons donc $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ et $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Degré d'une extension de corps

Définition

Le degré d'une extension de corps est le nombre de paramètres nécessaires pour représenter n'importe quel éléments de l'extension.

Le degré d'une extension M : K est dénoté [M : K].

$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

Les éléments de $\mathbb{Q}(\sqrt{2})$ peuvent être représentés par 2 paramètres: (a,b)

$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{2^2} : a, b, c \in \mathbb{Q}\}$.

Les éléments de $\mathbb{Q}(\sqrt{2})$ peuvent être représentés par 3 paramètres: (a,b,c)

Nous avons donc $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ et $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Degré d'une extension de corps

Définition

Le `degré d'une extension de corps` est le nombre de paramètres nécessaires pour représenter n'importe quel éléments de l'extension.

Le degré d'une extension M : K est dénoté [M : K].

$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

Les éléments de $\mathbb{Q}(\sqrt{2})$ peuvent être représentés par 2 paramètres: (a,b)

$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{2^2} : a, b, c \in \mathbb{Q}\}$.

Les éléments de $\mathbb{Q}(\sqrt{2})$ peuvent être représentés par 3 paramètres: (a,b,c)

Nous avons donc $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ et $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Degré d'une extension de corps

Définition

Le `degré d'une extension de corps` est le nombre de paramètres nécessaires pour représenter n'importe quel éléments de l'extension.

Le degré d'une extension M : K est dénoté [M : K].

$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

Les éléments de $\mathbb{Q}(\sqrt{2})$ peuvent être représentés par 2 paramètres: (a,b)

$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{2^2} : a, b, c \in \mathbb{Q}\}$.

Les éléments de $\mathbb{Q}(\sqrt{2})$ peuvent être représentés par 3 paramètres: (a,b,c)

Nous avons donc $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ et $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Degré d'une extension de corps

Définition

Le `degré d'une extension de corps` est le nombre de paramètres nécessaires pour représenter n'importe quel éléments de l'extension.

Le degré d'une extension M : K est dénoté [M : K].

$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

Les éléments de $\mathbb{Q}(\sqrt{2})$ peuvent être représentés par 2 paramètres: (a,b)

$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{2^2} : a, b, c \in \mathbb{Q}\}$.

Les éléments de $\mathbb{Q}(\sqrt{2})$ peuvent être représentés par 3 paramètres: (a,b,c)

Nous avons donc $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ et $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Degré d'une extension de corps

Définition

Le `degré d'une extension de corps` est le nombre de paramètres nécessaires pour représenter n'importe quel éléments de l'extension.

Le degré d'une extension M : K est dénoté [M : K].

$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

Les éléments de $\mathbb{Q}(\sqrt{2})$ peuvent être représentés par 2 paramètres: (a,b)

$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{2^2} : a, b, c \in \mathbb{Q}\}$.

Les éléments de $\mathbb{Q}(\sqrt{2})$ peuvent être représentés par 3 paramètres: (a,b,c)

Nous avons donc $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ et $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Degré d'une extension de corps

Définition

Le `degré d'une extension de corps` est le nombre de paramètres nécessaires pour représenter n'importe quel éléments de l'extension.

Le degré d'une extension M : K est dénoté [M : K].

$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

Les éléments de $\mathbb{Q}(\sqrt{2})$ peuvent être représentés par 2 paramètres: (a,b)

$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{2^2} : a, b, c \in \mathbb{Q}\}$.

Les éléments de $\mathbb{Q}(\sqrt{2})$ peuvent être représentés par 3 paramètres: (a,b,c)

Nous avons donc $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ et $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Extensions normales

Définition

Une extension de corps est **normale** si quand elle possède une racine d'un polynôme irréductible f, elle possède automatiquement toutes les racines de f.

Les corps de ruptures sont toujours des extensions normales.

$\mathbb{SF}_{\mathbb{Q}}(x^2 - 2) = \mathbb{Q}(\sqrt{2})$ est le corps de rupture de $x^2 - 2$ car il est le plus petit corps contenant $\sqrt{2}$.

Nous avons donc que $\mathbb{SF}_{\mathbb{Q}}(x^2 - 2)$ est une extension normale.

Extensions normales

Définition

Une extension de corps est `normale` si quand elle possède une racine d'un polynôme irréductible f, elle possède automatiquement toutes les racines de f.

Les corps de ruptures sont toujours des extensions normales.

$\mathbb{SF}_{\mathbb{Q}}(x^2-2) = \mathbb{Q}(\sqrt{2})$ est le corps de rupture de x^2-2 car il est le plus petit corps contenant $\sqrt{2}$.

Nous avons donc que $\mathbb{SF}_{\mathbb{Q}}(x^2-2)$ est une extension normale.

Extensions normales

Définition

Une extension de corps est normale si quand elle possède une racine d'un polynôme irréductible f, elle possède automatiquement toutes les racines de f.

Les corps de ruptures sont toujours des extensions normales.

$\mathbb{SF}_{\mathbb{Q}}(x^2-2) = \mathbb{Q}(\sqrt{2})$ est le corps de rupture de x^2-2 car il est le plus petit corps contenant $\sqrt{2}$.

Nous avons donc que $\mathbb{SF}_{\mathbb{Q}}(x^2-2)$ est une extension normale.

Extensions normales

Définition

Une extension de corps est `normale` si quand elle possède une racine d'un polynôme irréductible f, elle possède automatiquement toutes les racines de f.

Les corps de ruptures sont toujours des extensions normales.

$\mathbb{SF}_{\mathbb{Q}}(x^2-2) = \mathbb{Q}(\sqrt{2})$ est le corps de rupture de x^2-2 car il est le plus petit corps contenant $\sqrt{2}$.

Nous avons donc que $\mathbb{SF}_{\mathbb{Q}}(x^2-2)$ est une extension normale.

Extensions normales

Définition

Une extension de corps est `normale` si quand elle possède une racine d'un polynôme irréductible f, elle possède automatiquement toutes les racines de f.

Les corps de ruptures sont toujours des extensions normales.

$\mathbb{SF}_{\mathbb{Q}}(x^2-2) = \mathbb{Q}(\sqrt{2})$ est le corps de rupture de x^2-2 car il est le plus petit corps contenant $\sqrt{2}$.

Nous avons donc que $\mathbb{SF}_{\mathbb{Q}}(x^2-2)$ est une extension normale.

Automorphismes

Définition

Un automorphisme est une fonction θ d'une structure algébrique A à elle-même $\theta : A \to A$ où θ préserve la structure tel que $\theta(a) * \theta(b) = \theta(a * b)$, pour tous les opérations de A.

L'automorphisme trivial e envoie chaque élément $a \in$ A à lui même tel que $e(a) = a$.

Automorphisme d'une extension de corps: $\theta : M : K \to M : K$.

Un automorphisme θ de $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ à lui même appliqué à l'élément $5\sqrt{2} + 17 \in \mathbb{Q}(\sqrt{2})$ devrait donc satisfaire la relation suivante:

$$\theta(5\sqrt{2} + 17) = \theta(5)\theta(\sqrt{2}) + \theta(17)$$

Automorphismes

Définition

Un **automorphisme** est une fonction θ d'une structure algébrique A à elle-même $\theta : A \to A$ où θ préserve la structure tel que $\theta(a) * \theta(b) = \theta(a * b)$, pour tous les opérations de A.

L'automorphisme trivial e envoie chaque élément $a \in$ A à lui même tel que $e(a) = a$.

Automorphisme d'une extension de corps: $\theta : M : K \to M : K$.

Un automorphisme θ de $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ à lui même appliqué à l'élément $5\sqrt{2} + 17 \in \mathbb{Q}(\sqrt{2})$ devrait donc satisfaire la relation suivante:

$$\theta(5\sqrt{2} + 17) = \theta(5)\theta(\sqrt{2}) + \theta(17)$$

Automorphismes

Définition

Un automorphisme est une fonction θ d'une structure algébrique A à elle-même $\theta : A \to A$ où θ préserve la structure tel que $\theta(a) * \theta(b) = \theta(a * b)$, pour tous les opérations de A.

L'automorphisme trivial e envoie chaque élément $a \in$ A à lui même tel que $e(a) = a$.

Automorphisme d'une extension de corps: $\theta : M : K \to M : K$.

Un automorphisme θ de $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ à lui même appliqué à l'élément $5\sqrt{2} + 17 \in \mathbb{Q}(\sqrt{2})$ devrait donc satisfaire la relation suivante:

$$\theta(5\sqrt{2} + 17) = \theta(5)\theta(\sqrt{2}) + \theta(17)$$

Automorphismes

Définition

Un automorphisme est une fonction θ d'une structure algébrique A à elle-même $\theta : A \rightarrow A$ où θ préserve la structure tel que $\theta(a) * \theta(b) = \theta(a * b)$, pour tous les opérations de A.

L'automorphisme trivial e envoie chaque élément $a \in$ A à lui même tel que $e(a) = a$.

Automorphisme d'une extension de corps: $\theta : M : K \rightarrow M : K$.

Un automorphisme θ de $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ à lui même appliqué à l'élément $5\sqrt{2} + 17 \in \mathbb{Q}(\sqrt{2})$ devrait donc satisfaire la relation suivante:

$$\theta(5\sqrt{2} + 17) = \theta(5)\theta(\sqrt{2}) + \theta(17)$$

Automorphismes

Définition

Un automorphisme est une fonction θ d'une structure algébrique A à elle-même $\theta : A \to A$ où θ préserve la structure tel que $\theta(a) * \theta(b) = \theta(a * b)$, pour tous les opérations de A.

L'automorphisme trivial e envoie chaque élément $a \in$ A à lui même tel que $e(a) = a$.

Automorphisme d'une extension de corps: $\theta : M : K \to M : K$.

Un automorphisme θ de $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ à lui même appliqué à l'élément $5\sqrt{2} + 17 \in \mathbb{Q}(\sqrt{2})$ devrait donc satisfaire la relation suivante:

$$\theta(5\sqrt{2} + 17) = \theta(5)\theta(\sqrt{2}) + \theta(17)$$

Automorphismes

Définition

Un automorphisme est une fonction θ d'une structure algébrique A à elle-même $\theta : A \to A$ où θ préserve la structure tel que $\theta(a) * \theta(b) = \theta(a * b)$, pour tous les opérations de A.

L'automorphisme trivial e envoie chaque élément $a \in$ A à lui même tel que $e(a) = a$.

Automorphisme d'une extension de corps: $\theta : M : K \to M : K$.

Un automorphisme θ de $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ à lui même appliqué à l'élément $5\sqrt{2} + 17 \in \mathbb{Q}(\sqrt{2})$ devrait donc satisfaire la relation suivante:

$$\theta(5\sqrt{2} + 17) = \theta(5)\theta(\sqrt{2}) + \theta(17)$$

Exemple d'automorphisme

On considère un automorphisme θ sur l'extension de corps $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ tel que $\theta(a) = a$ pour tous a $\in \mathbb{Q}$ et $\theta(\sqrt{2}) = -\sqrt{2}$

$\theta(52/91) = 52/91$

$\theta(-\sqrt{2}) = \theta(\sqrt{2})\theta(-1) = (-1)(-\sqrt{2}) = \sqrt{2}$

$\theta(23/2 + 4\sqrt{2}) = \theta(23/2) + \theta(4)\theta(\sqrt{2}) = 23/2 + 4(-\sqrt{2}) = 23/2 - 4\sqrt{2}$

Cet automorphisme fixe les éléments de $\mathbb{Q}$ et fait une permutation de $\sqrt{2}$ avec $-\sqrt{2}$

Exemple d'automorphisme

On considère un automorphisme θ sur l'extension de corps $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ tel que $\theta(a) = a$ pour tous a $\in \mathbb{Q}$ et $\theta(\sqrt{2}) = -\sqrt{2}$

$\theta(52/91) = 52/91$

$\theta(-\sqrt{2}) = \theta(\sqrt{2})\theta(-1) = (-1)(-\sqrt{2}) = \sqrt{2}$

$\theta(23/2 + 4\sqrt{2}) = \theta(23/2) + \theta(4)\theta(\sqrt{2}) = 23/2 + 4(-\sqrt{2}) = 23/2 - 4\sqrt{2}$

Cet automorphisme fixe les éléments de $\mathbb{Q}$ et fait une permutation de $\sqrt{2}$ avec $-\sqrt{2}$

Exemple d'automorphisme

On considère un automorphisme θ sur l'extension de corps $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ tel que $\theta(a) = a$ pour tous a $\in \mathbb{Q}$ et $\theta(\sqrt{2}) = -\sqrt{2}$

$\theta(52/91) = 52/91$

$\theta(-\sqrt{2}) = \theta(\sqrt{2})\theta(-1) = (-1)(-\sqrt{2}) = \sqrt{2}$

$\theta(23/2 + 4\sqrt{2}) = \theta(23/2) + \theta(4)\theta(\sqrt{2}) = 23/2 + 4(-\sqrt{2}) = 23/2 - 4\sqrt{2}$

Cet automorphisme fixe les éléments de $\mathbb{Q}$ et fait une permutation de $\sqrt{2}$ avec $-\sqrt{2}$

Exemple d'automorphisme

On considère un automorphisme θ sur l'extension de corps $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ tel que $\theta(a) = a$ pour tous a $\in \mathbb{Q}$ et $\theta(\sqrt{2}) = -\sqrt{2}$

$\theta(52/91) = 52/91$

$\theta(-\sqrt{2}) = \theta(\sqrt{2})\theta(-1) = (-1)(-\sqrt{2}) = \sqrt{2}$

$\theta(23/2 + 4\sqrt{2}) = \theta(23/2) + \theta(4)\theta(\sqrt{2}) = 23/2 + 4(-\sqrt{2}) = 23/2 - 4\sqrt{2}$

Cet automorphisme fixe les éléments de $\mathbb{Q}$ et fait une permutation de $\sqrt{2}$ avec $-\sqrt{2}$

Exemple d'automorphisme

On considère un automorphisme θ sur l'extension de corps $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ tel que $\theta(a) = a$ pour tous a $\in \mathbb{Q}$ et $\theta(\sqrt{2}) = -\sqrt{2}$

$\theta(52/91) = 52/91$

$\theta(-\sqrt{2}) = \theta(\sqrt{2})\theta(-1) = (-1)(-\sqrt{2}) = \sqrt{2}$

$\theta(23/2 + 4\sqrt{2}) = \theta(23/2) + \theta(4)\theta(\sqrt{2}) = 23/2 + 4(-\sqrt{2}) = 23/2 - 4\sqrt{2}$

Cet automorphisme fixe les éléments de $\mathbb{Q}$ et fait une permutation de $\sqrt{2}$ avec $-\sqrt{2}$

Exemple d'automorphisme

On considère un automorphisme θ sur l'extension de corps $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ tel que $\theta(a) = a$ pour tous a $\in \mathbb{Q}$ et $\theta(\sqrt{2}) = -\sqrt{2}$

$\theta(52/91) = 52/91$

$\theta(-\sqrt{2}) = \theta(\sqrt{2})\theta(-1) = (-1)(-\sqrt{2}) = \sqrt{2}$

$\theta(23/2 + 4\sqrt{2}) = \theta(23/2) + \theta(4)\theta(\sqrt{2}) = 23/2 + 4(-\sqrt{2}) = 23/2 - 4\sqrt{2}$

Cet automorphisme fixe les éléments de $\mathbb{Q}$ et fait une permutation de $\sqrt{2}$ avec $-\sqrt{2}$

Groupes de Galois

Définition

Le groupe de Galois $\mathrm{Gal}(\mathrm{M} : \mathrm{K})$ d'une extension de corps $\mathrm{M} : \mathrm{K}$ est un groupe qui contient des automorphismes de l'extension $\mathrm{M} : \mathrm{K}$ qui fixent les éléments de K tel que $\theta(a) = a$ si $a \in \mathrm{K}$.

$\mathrm{Gal}(\mathrm{M} : \mathrm{K})$ est un groupe qui contient des automorphismes $\theta : M : K \to M : K$.

L'opération de ce groupe est la composition d'automorphismes.

Un automorphisme de $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q})$ devrait envoyer un élément $a + b\sqrt{2}$ de la manière suivante puisqu'il préserve la structure:

$$\theta(a + b\sqrt{2}) = \theta(a) + \theta(b)\theta(\sqrt{2})$$

Sachant que les éléments de $\mathbb{Q}$ sont fixés par les automorphismes de $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q})$, on a donc:

$$\theta(a + b\sqrt{2}) = a + b\theta(\sqrt{2})$$

Groupes de Galois

Définition

Le groupe de Galois Gal(M : K) d'une extension de corps M : K est un groupe qui contient des automorphismes de l'extension M : K qui fixent les éléments de K tel que $\theta(a) = a$ si $a \in$ K.

Gal(M : K) est un groupe qui contient des automorphismes $\theta : M : K \to M : K$.

L'opération de ce groupe est la composition d'automorphismes.

Un automorphisme de Gal($\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$) devrait envoyer un élément $a + b\sqrt{2}$ de la manière suivante puisqu'il préserve la structure:

$$\theta(a + b\sqrt{2}) = \theta(a) + \theta(b)\theta(\sqrt{2})$$

Sachant que les éléments de $\mathbb{Q}$ sont fixés par les automorphismes de Gal($\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$), on a donc:

$$\theta(a + b\sqrt{2}) = a + b\theta(\sqrt{2})$$

Groupes de Galois

Définition

Le **groupe de Galois** Gal(M : K) d'une extension de corps M : K est un groupe qui contient des automorphismes de l'extension M : K qui fixent les éléments de K tel que $\theta(a) = a$ si $a \in \mathrm{K}$.

Gal(M : K) est un groupe qui contient des automorphismes $\theta : M : K \to M : K$.

L'opération de ce groupe est la composition d'automorphismes.

Un automorphisme de $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q})$ devrait envoyer un élément $a + b\sqrt{2}$ de la manière suivante puisqu'il préserve la structure:

$$\theta(a + b\sqrt{2}) = \theta(a) + \theta(b)\theta(\sqrt{2})$$

Sachant que les éléments de $\mathbb{Q}$ sont fixés par les automorphismes de $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q})$, on a donc:

$$\theta(a + b\sqrt{2}) = a + b\theta(\sqrt{2})$$

Groupes de Galois

Définition

Le groupe de Galois $\mathrm{Gal}(\mathrm{M} : \mathrm{K})$ d'une extension de corps $\mathrm{M} : \mathrm{K}$ est un groupe qui contient des automorphismes de l'extension $\mathrm{M} : \mathrm{K}$ qui fixent les éléments de K tel que $\theta(a) = a$ si $a \in \mathrm{K}$.

$\mathrm{Gal}(\mathrm{M} : \mathrm{K})$ est un groupe qui contient des automorphismes $\theta : M : K \to M : K$.

L'opération de ce groupe est la composition d'automorphismes.

Un automorphisme de $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q})$ devrait envoyer un élément $a + b\sqrt{2}$ de la manière suivante puisqu'il préserve la structure:

$$\theta(a + b\sqrt{2}) = \theta(a) + \theta(b)\theta(\sqrt{2})$$

Sachant que les éléments de $\mathbb{Q}$ sont fixés par les automorphismes de $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q})$, on a donc:

$$\theta(a + b\sqrt{2}) = a + b\theta(\sqrt{2})$$

Groupes de Galois

Définition

Le `groupe de Galois` Gal(M : K) d'une extension de corps M : K est un groupe qui contient des automorphismes de l'extension M : K qui fixent les éléments de K tel que $\theta(a) = a$ si $a \in$ K.

Gal(M : K) est un groupe qui contient des automorphismes $\theta : M : K \to M : K$.

L'opération de ce groupe est la composition d'automorphismes.

Un automorphisme de $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q})$ devrait envoyer un élément $a + b\sqrt{2}$ de la manière suivante puisqu'il préserve la structure:

$$\theta(a + b\sqrt{2}) = \theta(a) + \theta(b)\theta(\sqrt{2})$$

Sachant que les éléments de $\mathbb{Q}$ sont fixés par les automorphismes de $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q})$, on a donc:

$$\theta(a + b\sqrt{2}) = a + b\theta(\sqrt{2})$$

Groupes de Galois

Définition

Le `groupe de Galois` Gal(M : K) d'une extension de corps M : K est un groupe qui contient des automorphismes de l'extension M : K qui fixent les éléments de K tel que $\theta(a) = a$ si $a \in \mathrm{K}$.

Gal(M : K) est un groupe qui contient des automorphismes $\theta : M : K \to M : K$.

L'opération de ce groupe est la composition d'automorphismes.

Un automorphisme de Gal($\mathbb{Q}(\sqrt{2})$: $\mathbb{Q}$) devrait envoyer un élément $a + b\sqrt{2}$ de la manière suivante puisqu'il préserve la structure:

$$\theta(a + b\sqrt{2}) = \theta(a) + \theta(b)\theta(\sqrt{2})$$

Sachant que les éléments de $\mathbb{Q}$ sont fixés par les automorphismes de Gal($\mathbb{Q}(\sqrt{2})$: $\mathbb{Q}$), on a donc:

$$\theta(a + b\sqrt{2}) = a + b\theta(\sqrt{2})$$

Groupes de Galois

Définition

Le `groupe de Galois` Gal(M : K) d'une extension de corps M : K est un groupe qui contient des automorphismes de l'extension M : K qui fixent les éléments de K tel que $\theta(a) = a$ si $a \in$ K.

Gal(M : K) est un groupe qui contient des automorphismes $\theta : M : K \to M : K$.

L'opération de ce groupe est la composition d'automorphismes.

Un automorphisme de Gal($\mathbb{Q}(\sqrt{2})$: $\mathbb{Q}$) devrait envoyer un élément $a + b\sqrt{2}$ de la manière suivante puisqu'il préserve la structure:

$$\theta(a + b\sqrt{2}) = \theta(a) + \theta(b)\theta(\sqrt{2})$$

Sachant que les éléments de $\mathbb{Q}$ sont fixés par les automorphismes de Gal($\mathbb{Q}(\sqrt{2})$: $\mathbb{Q}$), on a donc:

$$\theta(a + b\sqrt{2}) = a + b\theta(\sqrt{2})$$

Groupes de Galois

Définition

Le `groupe de Galois` Gal(M : K) d'une extension de corps M : K est un groupe qui contient des automorphismes de l'extension M : K qui fixent les éléments de K tel que $\theta(a) = a$ si $a \in$ K.

Gal(M : K) est un groupe qui contient des automorphismes $\theta : M : K \to M : K$.

L'opération de ce groupe est la composition d'automorphismes.

Un automorphisme de Gal($\mathbb{Q}(\sqrt{2})$: $\mathbb{Q}$) devrait envoyer un élément $a + b\sqrt{2}$ de la manière suivante puisqu'il préserve la structure:

$$\theta(a + b\sqrt{2}) = \theta(a) + \theta(b)\theta(\sqrt{2})$$

Sachant que les éléments de $\mathbb{Q}$ sont fixés par les automorphismes de Gal($\mathbb{Q}(\sqrt{2})$: $\mathbb{Q}$), on a donc:

$$\theta(a + b\sqrt{2}) = a + b\theta(\sqrt{2})$$

Exemple de groupe de Galois et permutations de racines

$\sqrt{2}$ et $-\sqrt{2}$ sont les seules éléments qui ne sont pas fixés par les automorphismes de $\mathrm{Gal}(\mathbb{Q})$, les deux seules automorphismes de $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}):\mathbb{Q})$ sont les suivantes:

$$\theta \text{ tel que } \theta(\sqrt{2}) = \sqrt{2} \text{ et } \theta(-\sqrt{2}) = -\sqrt{2} \text{ (élément neutre)}$$

$$\phi \text{ tel que } \theta(-\sqrt{2}) = \sqrt{2} \text{ et } \theta(-\sqrt{2}) = \sqrt{2}$$

On a donc $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}):\mathbb{Q}) = \{\theta, \phi\}$

On peut donc voir les automorphismes d'un groupe de Galois comme des permutations de racines de polynômes.

Exemple de groupe de Galois et permutations de racines

$\sqrt{2}$ et $-\sqrt{2}$ sont les seules éléments qui ne sont pas fixés par les automorphismes de $\mathrm{Gal}(\mathbb{Q})$, les deux seules automorphismes de $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q})$ sont les suivantes:

$$\theta \text{ tel que } \theta(\sqrt{2}) = \sqrt{2} \text{ et } \theta(-\sqrt{2}) = -\sqrt{2} \text{ (élément neutre)}$$

$$\phi \text{ tel que } \theta(-\sqrt{2}) = \sqrt{2} \text{ et } \theta(-\sqrt{2}) = \sqrt{2}$$

On a donc $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q}) = \{\theta, \phi\}$

On peut donc voir les automorphismes d'un groupe de Galois comme des permutations de racines de polynômes.

Exemple de groupe de Galois et permutations de racines

$\sqrt{2}$ et $-\sqrt{2}$ sont les seules éléments qui ne sont pas fixés par les automorphismes de Gal($\mathbb{Q}$), les deux seules automorphismes de Gal($\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$) sont les suivantes:

$$\theta \text{ tel que } \theta(\sqrt{2}) = \sqrt{2} \text{ et } \theta(-\sqrt{2}) = -\sqrt{2} \text{ (élément neutre)}$$

$$\phi \text{ tel que } \theta(-\sqrt{2}) = \sqrt{2} \text{ et } \theta(-\sqrt{2}) = \sqrt{2}$$

On a donc Gal$(\mathbb{Q}(\sqrt{2}) : \mathbb{Q}) = \{\theta, \phi\}$

On peut donc voir les automorphismes d'un groupe de Galois comme des permutations de racines de polynômes.

Exemple de groupe de Galois et permutations de racines

$\sqrt{2}$ et $-\sqrt{2}$ sont les seules éléments qui ne sont pas fixés par les automorphismes de Gal($\mathbb{Q}$), les deux seules automorphismes de $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q})$ sont les suivantes:

$$\theta \text{ tel que } \theta(\sqrt{2}) = \sqrt{2} \text{ et } \theta(-\sqrt{2}) = -\sqrt{2} \text{ (élément neutre)}$$

$$\phi \text{ tel que } \theta(-\sqrt{2}) = \sqrt{2} \text{ et } \theta(-\sqrt{2}) = \sqrt{2}$$

On a donc $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q}) = \{\theta, \phi\}$

On peut donc voir les automorphismes d'un groupe de Galois comme des permutations de racines de polynômes.

Exemple de groupe de Galois et permutations de racines

$\sqrt{2}$ et $-\sqrt{2}$ sont les seules éléments qui ne sont pas fixés par les automorphismes de $\mathrm{Gal}(\mathbb{Q})$, les deux seules automorphismes de $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q})$ sont les suivantes:

$$\theta \text{ tel que } \theta(\sqrt{2}) = \sqrt{2} \text{ et } \theta(-\sqrt{2}) = -\sqrt{2} \text{ (élément neutre)}$$

$$\phi \text{ tel que } \theta(-\sqrt{2}) = \sqrt{2} \text{ et } \theta(-\sqrt{2}) = \sqrt{2}$$

On a donc $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q}) = \{\theta, \phi\}$

On peut donc voir les automorphismes d'un groupe de Galois comme des permutations de racines de polynômes.

Exemple de groupe de Galois et permutations de racines

$\sqrt{2}$ et $-\sqrt{2}$ sont les seules éléments qui ne sont pas fixés par les automorphismes de $\mathrm{Gal}(\mathbb{Q})$, les deux seules automorphismes de $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q})$ sont les suivantes:

$$\theta \text{ tel que } \theta(\sqrt{2}) = \sqrt{2} \text{ et } \theta(-\sqrt{2}) = -\sqrt{2} \text{ (élément neutre)}$$

$$\phi \text{ tel que } \theta(-\sqrt{2}) = \sqrt{2} \text{ et } \theta(-\sqrt{2}) = \sqrt{2}$$

On a donc $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}) : \mathbb{Q}) = \{\theta, \phi\}$

On peut donc voir les automorphismes d'un groupe de Galois comme des permutations de racines de polynômes.

Sous-groupes normaux et groupes quotients

Définition

Un `sous-groupe normal` H de G est un sous-groupe pour lequel $a^{-1}ha \in H$ pour tout $h \in H$ et pour tout $a \in G$.

Les sous-groupes normaux servent à séparer le groupe en sous ensembles nommés classes d'équivalences.

Définition

Un `groupe quotient` $\frac{G}{N}$ est un groupe ayant pour éléments les classes d'équivalences créées avec un sous-groupe normal N.

Sous-groupes normaux et groupes quotients

Définition

Un `sous-groupe normal` H de G est un sous-groupe pour lequel $a^{-1}ha \in H$ pour tout $h \in H$ et pour tout $a \in G$.

Les sous-groupes normaux servent à séparer le groupe en sous ensembles nommés classes d'équivalences.

Définition

Un `groupe quotient` $\frac{G}{N}$ est un groupe ayant pour éléments les classes d'équivalences créées avec un sous-groupe normal N.

Sous-groupes normaux et groupes quotients

Définition

Un sous-groupe normal H de G est un sous-groupe pour lequel $a^{-1}ha \in H$ pour tout $h \in H$ et pour tout $a \in G$.

Les sous-groupes normaux servent à séparer le groupe en sous ensembles nommés classes d'équivalences.

Définition

Un groupe quotient $\frac{G}{N}$ est un groupe ayant pour éléments les classes d'équivalences créées avec un sous-groupe normal N.

Sous-groupes normaux et groupes quotients

Définition

Un `sous-groupe normal` H de G est un sous-groupe pour lequel $a^{-1}ha \in H$ pour tout $h \in H$ et pour tout $a \in G$.

Les sous-groupes normaux servent à séparer le groupe en sous ensembles nommés classes d'équivalences.

Définition

Un `groupe quotient` $\frac{G}{N}$ est un groupe ayant pour éléments les classes d'équivalences créées avec un sous-groupe normal N.

Exemple de sous-groupes normaux et groupes quotients

Les nombres entiers $\mathbb{Z}$ peuvent être séparés en considérant le sous-groupe normal des entiers pairs, dénoté $[0]$:

$$[0] = \{..., -2, 0, 2, 4, ...\} \text{ et } [1] = \{..., -3, -1, 1, 3, 5, ...\}$$

On peut utiliser les deux classes d'équivalences $[0]$ et $[1]$ pour former un nouveau groupe.

Ce nouveau groupe est dénoté $\mathbb{Z}_2$ et contient $[0]$ et $[1]$.$[0]$ représente tous les nombres pairs et $[1]$ représente tous les nombres impairs.

$\mathbb{Z}_2$ est le groupe quotient du groupe $\mathbb{Z}$ et de son sous-groupe normal $[0]$

Exemple de sous-groupes normaux et groupes quotients

Les nombres entiers $\mathbb{Z}$ peuvent être séparés en considérant le sous-groupe normal des entiers pairs, dénoté [0]:

$$[0] = \{..., -2, 0, 2, 4, ...\} \text{ et } [1] = \{..., -3, -1, 1, 3, 5, ...\}$$

On peut utiliser les deux classes d'équivalences [0] et [1] pour former un nouveau groupe.

Ce nouveau groupe est dénoté $\mathbb{Z}_2$ et contient [0] et [1].[0] représente tous les nombres pairs et [1] représente tous les nombres impairs.

$\mathbb{Z}_2$ est le groupe quotient du groupe $\mathbb{Z}$ et de son sous-groupe normal [0]

Exemple de sous-groupes normaux et groupes quotients

Les nombres entiers $\mathbb{Z}$ peuvent être séparés en considérant le sous-groupe normal des entiers pairs, dénoté [0]:

$$[0] = \{..., -2, 0, 2, 4, ...\} \text{ et } [1] = \{..., -3, -1, 1, 3, 5, ...\}$$

On peut utiliser les deux classes d'équivalences [0] et [1] pour former un nouveau groupe.

Ce nouveau groupe est dénoté $\mathbb{Z}_2$ et contient [0] et [1].[0] représente tous les nombres pairs et [1] représente tous les nombres impairs.

$\mathbb{Z}_2$ est le groupe quotient du groupe $\mathbb{Z}$ et de son sous-groupe normal [0]

Exemple de sous-groupes normaux et groupes quotients

Les nombres entiers $\mathbb{Z}$ peuvent être séparés en considérant le sous-groupe normal des entiers pairs, dénoté [0]:

$$[0] = \{..., -2, 0, 2, 4, ...\} \text{ et } [1] = \{..., -3, -1, 1, 3, 5, ...\}$$

On peut utiliser les deux classes d'équivalences [0] et [1] pour former un nouveau groupe.

Ce nouveau groupe est dénoté $\mathbb{Z}_2$ et contient [0] et [1].[0] représente tous les nombres pairs et [1] représente tous les nombres impairs.

$\mathbb{Z}_2$ est le groupe quotient du groupe $\mathbb{Z}$ et de son sous-groupe normal [0]

Exemple de sous-groupes normaux et groupes quotients

Les nombres entiers $\mathbb{Z}$ peuvent être séparés en considérant le sous-groupe normal des entiers pairs, dénoté [0]:

$$[0] = \{..., -2, 0, 2, 4, ...\} \text{ et } [1] = \{..., -3, -1, 1, 3, 5, ...\}$$

On peut utiliser les deux classes d'équivalences [0] et [1] pour former un nouveau groupe.

Ce nouveau groupe est dénoté $\mathbb{Z}_2$ et contient [0] et [1].[0] représente tous les nombres pairs et [1] représente tous les nombres impairs.

$\mathbb{Z}_2$ est le groupe quotient du groupe $\mathbb{Z}$ et de son sous-groupe normal [0]

Exemple de sous-groupes normaux et groupes quotients

Les nombres entiers $\mathbb{Z}$ peuvent être séparés en considérant le sous-groupe normal des entiers pairs, dénoté [0]:

$$[0] = \{..., -2, 0, 2, 4, ...\} \text{ et } [1] = \{..., -3, -1, 1, 3, 5, ...\}$$

On peut utiliser les deux classes d'équivalences [0] et [1] pour former un nouveau groupe.

Ce nouveau groupe est dénoté $\mathbb{Z}_2$ et contient [0] et [1].[0] représente tous les nombres pairs et [1] représente tous les nombres impairs.

$\mathbb{Z}_2$ est le groupe quotient du groupe $\mathbb{Z}$ et de son sous-groupe normal [0]

Extensions résolubles

Définition

Une extension M : K est **résoluble** si il existe une séquence de corps tel que:

$$K = L_0 \subseteq L_1 \subseteq ...L_{n-1} \subseteq L_n = M$$

avec $L_i : L_{i-1}$ normale et $Gal(L_i : L_i - 1)$ commutatif pour tout i $\in \{0, 1, ..., n\}$.

Par exemple, l'extention $\mathbb{Q}(\sqrt{3}, \sqrt{2})$: $\mathbb{Q}$ est résoluble

Exemple d'extensions résolubles

On considère l'extension $\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}$

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

$\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ sont normales car ils ne contiennent pas d'autres racines que celle des polynômes irréductibles $x^2 - 2$ et $x^3 - 3$

Les groupes de Galois $Gal(\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2}))$ et $Gal(\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2}))$ sont commutatifs.

En effet, si on compose deux fonctions ϕ et θ du groupe de Galois $Gal(\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2}))$, on a que $\phi\theta = \theta\phi$

Exemple d'extensions résolubles

On considère l'extension $\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}$

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

$\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ sont normales car ils ne contiennent pas d'autres racines que celle des polynômes irréductibles $x^2 - 2$ et $x^3 - 3$

Les groupes de Galois $Gal(\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2}))$ et $Gal(\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2}))$ sont commutatifs.

En effet, si on compose deux fonctions ϕ et θ du groupe de Galois $Gal(\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2}))$, on a que $\phi\theta = \theta\phi$

Exemple d'extensions résolubles

On considère l'extension $\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}$

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

$\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ sont normales car ils ne contiennent pas d'autres racines que celle des polynômes irréductibles $x^2 - 2$ et $x^3 - 3$

Les groupes de Galois $Gal(\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2}))$ et $Gal(\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2}))$ sont commutatifs.

En effet, si on compose deux fonctions ϕ et θ du groupe de Galois $Gal(\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2}))$, on a que $\phi\theta = \theta\phi$

Exemple d'extensions résolubles

On considère l'extension $\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}$

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

$\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ sont normales car ils ne contiennent pas d'autres racines que celle des polynômes irréductibles $x^2 - 2$ et $x^3 - 3$

Les groupes de Galois $Gal(\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2}))$ et $Gal(\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2}))$ sont commutatifs.

En effet, si on compose deux fonctions ϕ et θ du groupe de Galois $Gal(\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2}))$, on a que $\phi\theta = \theta\phi$

Exemple d'extensions résolubles

On considère l'extension $\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}$

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

$\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ sont normales car ils ne contiennent pas d'autres racines que celle des polynômes irréductibles $x^2 - 2$ et $x^3 - 3$

Les groupes de Galois $Gal(\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2}))$ et $Gal(\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2}))$ sont commutatifs.

En effet, si on compose deux fonctions ϕ et θ du groupe de Galois $Gal(\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2}))$, on a que $\phi\theta = \theta\phi$

Exemple d'extensions résolubles

On considère l'extension $\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}$

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

$\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ sont normales car ils ne contiennent pas d'autres racines que celle des polynômes irréductibles $x^2 - 2$ et $x^3 - 3$

Les groupes de Galois $Gal(\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2}))$ et $Gal(\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2}))$ sont commutatifs.

En effet, si on compose deux fonctions ϕ et θ du groupe de Galois $Gal(\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2}))$, on a que $\phi\theta = \theta\phi$

Groupes résolubles

Définition

Un groupe G est **résoluble** si il existe une séquence de sous-groupes normaux tel que:

$$G = G_0 \trianglerighteq G_1 \trianglerighteq ... \trianglerighteq G_{n-1} \trianglerighteq G_n = \{e\}$$

et $\frac{G_i}{G_i+1}$ commutatif pour tout i $\in \{0, 1, ..., n\}$

Par exemple, l'extention $\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}$ est résoluble

Exemple de groupe résoluble

Par exemple, $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}) = \{id, \theta_1, \theta_2, \theta_3\}$ contient quatres éléments

Ces éléments correspondent à certaines permutations de racines.

Ce groupe est commutatif (contient 4 éléments) donc tous ces sous-groupes sont normaux. $(aha^{-1} \in \mathrm{H})$

Par exemple, $\{id, \theta_1\}$ est un sous-groupe normal de $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q})$. Nous avons donc:

$$Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}) = \{id, \theta_1, \theta_2, \theta_3\} \trianglerighteq \{id, \theta_1\} \trianglerighteq \{id\} = \{e\}$$

Exemple de groupe résoluble

Par exemple, $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}) = \{id, \theta_1, \theta_2, \theta_3\}$ contient quatres éléments

Ces éléments correspondent à certaines permutations de racines.

Ce groupe est commutatif (contient 4 éléments) donc tous ces sous-groupes sont normaux. $(aha^{-1} \in \mathrm{H})$

Par exemple, $\{id, \theta_1\}$ est un sous-groupe normal de $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q})$. Nous avons donc:

$$Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}) = \{id, \theta_1, \theta_2, \theta_3\} \trianglerighteq \{id, \theta_1\} \trianglerighteq \{id\} = \{e\}$$

Exemple de groupe résoluble

Par exemple, $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}) = \{id, \theta_1, \theta_2, \theta_3\}$ contient quatres éléments

Ces éléments correspondent à certaines permutations de racines.

Ce groupe est commutatif (contient 4 éléments) donc tous ces sous-groupes sont normaux. $(aha^{-1} \in \mathrm{H})$

Par exemple, $\{id, \theta_1\}$ est un sous-groupe normal de $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q})$. Nous avons donc:

$$Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}) = \{id, \theta_1, \theta_2, \theta_3\} \trianglerighteq \{id, \theta_1\} \trianglerighteq \{id\} = \{e\}$$

Exemple de groupe résoluble

Par exemple, $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}) = \{id, \theta_1, \theta_2, \theta_3\}$ contient quatres éléments

Ces éléments correspondent à certaines permutations de racines.

Ce groupe est commutatif (contient 4 éléments) donc tous ces sous-groupes sont normaux. ($aha^{-1} \in$ H)

Par exemple, $\{id, \theta_1\}$ est un sous-groupe normal de $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q})$. Nous avons donc:

$$Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}) = \{id, \theta_1, \theta_2, \theta_3\} \trianglerighteq \{id, \theta_1\} \trianglerighteq \{id\} = \{e\}$$

Exemple de groupe résoluble

Par exemple, $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}) = \{id, \theta_1, \theta_2, \theta_3\}$ contient quatres éléments

Ces éléments correspondent à certaines permutations de racines.

Ce groupe est commutatif (contient 4 éléments) donc tous ces sous-groupes sont normaux. $(aha^{-1} \in \mathrm{H})$

Par exemple, $\{id, \theta_1\}$ est un sous-groupe normal de $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q})$. Nous avons donc:

$$Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}) = \{id, \theta_1, \theta_2, \theta_3\} \trianglerighteq \{id, \theta_1\} \trianglerighteq \{id\} = \{e\}$$

Exemple de groupe résoluble

Par exemple, $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}) = \{id, \theta_1, \theta_2, \theta_3\}$ contient quatres éléments

Ces éléments correspondent à certaines permutations de racines.

Ce groupe est commutatif (contient 4 éléments) donc tous ces sous-groupes sont normaux. $(aha^{-1} \in \mathrm{H})$

Par exemple, $\{id, \theta_1\}$ est un sous-groupe normal de $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q})$. Nous avons donc:

$$Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}) = \{id, \theta_1, \theta_2, \theta_3\} \trianglerighteq \{id, \theta_1\} \trianglerighteq \{id\} = \{e\}$$

Polynômes résolubles

Définition

Un polynôme est **résoluble** si ses racines peuvent être exprimées avec les opérations suivantes: $+$ - $\times$ $\div$ $\sqrt[n]{a}$.

Un polynôme de degré n qui ne peut pas être exprimé par radicaux implique qu'il n'existe pas de formule pour les racines de polynômes de degré n utilisant les opérations $+$ - $\times$ $\div$ $\sqrt[n]{a}$.

On prends pour aquis le résultat suivant:

Théorème

Si f est résoluble par radicaux, alors ses racines $\alpha_1, \alpha_2, ..., \alpha_n$ sont tous contenues dans une extension de $\mathbb{Q}$ qui est finie, normale et résoluble.

Polynômes résolubles

Définition

Un polynôme est **résoluble** si ses racines peuvent être exprimées avec les opérations suivantes: $+ \text{ - } \times \div \sqrt[n]{a}$.

Un polynôme de degré n qui ne peut pas être exprimé par radicaux implique qu'il n'existe pas de formule pour les racines de polynômes de degré n utilisant les opérations $+ \text{ - } \times \div \sqrt[n]{a}$.

On prends pour aquis le résultat suivant:

Théorème

Si f est résoluble par radicaux, alors ses racines $\alpha_1, \alpha_2, ..., \alpha_n$ sont tous contenues dans une extension de $\mathbb{Q}$ qui est finie, normale et résoluble.

Polynômes résolubles

Définition

Un polynôme est `résoluble` si ses racines peuvent être exprimées avec les opérations suivantes: + - $\times$ $\div$ $\sqrt[n]{a}$.

Un polynôme de degré n qui ne peut pas être exprimé par radicaux implique qu'il n'existe pas de formule pour les racines de polynômes de degré n utilisant les opérations + - $\times$ $\div$ $\sqrt[n]{a}$.

On prends pour aquis le résultat suivant:

Théorème

Si f est résoluble par radicaux, alors ses racines $\alpha_1, \alpha_2, ..., \alpha_n$ sont tous contenues dans une extension de $\mathbb{Q}$ qui est finie, normale et résoluble.

Polynômes résolubles

Définition

Un polynôme est résoluble si ses racines peuvent être exprimées avec les opérations suivantes: $+$ - $\times$ $\div$ $\sqrt[n]{a}$.

Un polynôme de degré n qui ne peut pas être exprimé par radicaux implique qu'il n'existe pas de formule pour les racines de polynômes de degré n utilisant les opérations $+$ - $\times$ $\div$ $\sqrt[n]{a}$.

On prends pour aquis le résultat suivant:

Théorème

Si f est résoluble par radicaux, alors ses racines $\alpha_1, \alpha_2, ..., \alpha_n$ sont tous contenues dans une extension de $\mathbb{Q}$ qui est finie, normale et résoluble.

Polynômes résolubles

Définition

Un polynôme est `résoluble` si ses racines peuvent être exprimées avec les opérations suivantes: $+$ - $\times$ $\div$ $\sqrt[n]{a}$.

Un polynôme de degré n qui ne peut pas être exprimé par radicaux implique qu'il n'existe pas de formule pour les racines de polynômes de degré n utilisant les opérations $+$ - $\times$ $\div$ $\sqrt[n]{a}$.

On prends pour aquis le résultat suivant:

Théorème

Si f est résoluble par radicaux, alors ses racines $\alpha_1, \alpha_2, ..., \alpha_n$ sont tous contenues dans une extension de $\mathbb{Q}$ qui est finie, normale et résoluble.

Théorème fondamental de la théorie de Galois

Théorème

On considère une extension M : K normale et finie et L un corps tel que M : L : K. Si L : K est une extension normale, alors

$$Gal(M : L) \trianglelefteq Gal(M : K)$$

$$\frac{Gal(M:K)}{Gal(M:L)} \cong Gal(L : K)$$

Si $Gal(M : L)$ est un sous-groupe normal de $Gal(M : K)$, alors il peut être utilisé pour créer le groupe quotient $\frac{Gal(M:K)}{Gal(M:L)}$.

Le symbole $\cong$ signifie que $\frac{Gal(M:K)}{Gal(M:L)}$ et $Gal(L : K)$ on la même structure et sont donc considérés comme étant le même groupe.

Théorème fondamental de la théorie de Galois

Théorème

On considère une extension M : K normale et finie et L un corps tel que M : L : K. Si L : K est une extension normale, alors

$$Gal(M : L) \trianglelefteq Gal(M : K)$$

$$\frac{Gal(M:K)}{Gal(M:L)} \cong Gal(L : K)$$

Si $Gal(M : L)$ est un sous-groupe normal de $Gal(M : K)$, alors il peut être utilisé pour créer le groupe quotient $\frac{Gal(M:K)}{Gal(M:L)}$.

Le symbole $\cong$ signifie que $\frac{Gal(M:K)}{Gal(M:L)}$ et $Gal(L : K)$ on la même structure et sont donc considérés comme étant le même groupe.

Théorème fondamental de la théorie de Galois

Théorème

On considère une extension M : K normale et finie et L un corps tel que M : L : K. Si L : K est une extension normale, alors

$$Gal(M:L) \trianglelefteq Gal(M:K)$$

$$\frac{Gal(M:K)}{Gal(M:L)} \cong Gal(L:K)$$

Si $Gal(M:L)$ est un sous-groupe normal de $Gal(M:K)$, alors il peut être utilisé pour créer le groupe quotient $\frac{Gal(M:K)}{Gal(M:L)}$.

Le symbole $\cong$ signifie que $\frac{Gal(M:K)}{Gal(M:L)}$ et $Gal(L:K)$ on la même structure et sont donc considérés comme étant le même groupe.

Théorème fondamental de la théorie de Galois

Théorème

On considère une extension M : K normale et finie et L un corps tel que M : L : K. Si L : K est une extension normale, alors

$$Gal(M : L) \trianglelefteq Gal(M : K)$$

$$\frac{Gal(M:K)}{Gal(M:L)} \cong Gal(L : K)$$

Si $Gal(M : L)$ est un sous-groupe normal de $Gal(M : K)$, alors il peut être utilisé pour créer le groupe quotient $\frac{Gal(M:K)}{Gal(M:L)}$.

Le symbole $\cong$ signifie que $\frac{Gal(M:K)}{Gal(M:L)}$ et $Gal(L : K)$ on la même structure et sont donc considérés comme étant le même groupe.

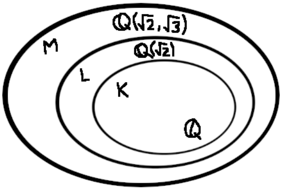
Sous-ensembles

On démontre que $Gal(M : L)$ est un sous-ensemble de $Gal(M : K)$

$Gal(M : L) = \{$automorphismes de M qui fixent les éléments de L$\}$

$Gal(M : K) = \{$automorphismes de M qui fixent les éléments de K$\}$

Puisque M : L : K, nous avons que K $\in$ L $\in$ M



Puisque K $\subseteq$ L, un automorphisme de M qui fixe L doit aussi fixer K.

Donc si $\theta \in Gal(M : L)$ alors $\theta \in Gal(M : K)$.

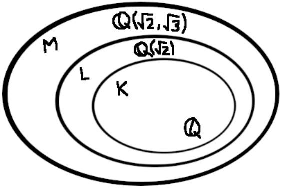
Sous-ensembles

On démontre que $Gal(M : L)$ est un sous-ensemble de $Gal(M : K)$

$Gal(M : L) = \{$automorphismes de M qui fixent les éléments de L$\}$

$Gal(M : K) = \{$automorphismes de M qui fixent les éléments de K$\}$

Puisque M : L : K, nous avons que K $\in$ L $\in$ M



Puisque K $\subseteq$ L, un automorphisme de M qui fixe L doit aussi fixer K.

Donc si $\theta \in Gal(M : L)$ alors $\theta \in Gal(M : K)$.

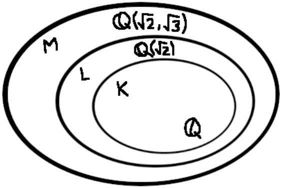
Sous-ensembles

On démontre que $Gal(M : L)$ est un sous-ensemble de $Gal(M : K)$

$Gal(M : L) = \{$automorphismes de M qui fixent les éléments de L$\}$

$Gal(M : K) = \{$automorphismes de M qui fixent les éléments de K$\}$

Puisque M : L : K, nous avons que K $\in$ L $\in$ M



Puisque K $\subseteq$ L, un automorphisme de M qui fixe L doit aussi fixer K.

Donc si $\theta \in Gal(M : L)$ alors $\theta \in Gal(M : K)$.

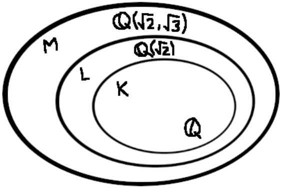
Sous-ensembles

On démontre que $Gal(M : L)$ est un sous-ensemble de $Gal(M : K)$

$Gal(M : L) = \{$automorphismes de M qui fixent les éléments de L$\}$

$Gal(M : K) = \{$automorphismes de M qui fixent les éléments de K$\}$

Puisque M : L : K, nous avons que K $\in$ L $\in$ M



Puisque K $\subseteq$ L, un automorphisme de M qui fixe L doit aussi fixer K.

Donc si $\theta \in Gal(M : L)$ alors $\theta \in Gal(M : K)$.

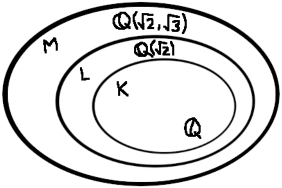
Sous-ensembles

On démontre que $Gal(M : L)$ est un sous-ensemble de $Gal(M : K)$

$Gal(M : L) = \{$automorphismes de M qui fixent les éléments de L$\}$

$Gal(M : K) = \{$automorphismes de M qui fixent les éléments de K$\}$

Puisque M : L : K, nous avons que K $\in$ L $\in$ M



Puisque K $\subseteq$ L, un automorphisme de M qui fixe L doit aussi fixer K.

Donc si $\theta \in Gal(M : L)$ alors $\theta \in Gal(M : K)$.

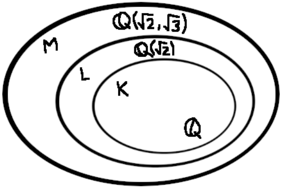
Sous-ensembles

On démontre que $Gal(M : L)$ est un sous-ensemble de $Gal(M : K)$

$Gal(M : L) = \{$automorphismes de M qui fixent les éléments de L$\}$

$Gal(M : K) = \{$automorphismes de M qui fixent les éléments de K$\}$

Puisque M : L : K, nous avons que K $\in$ L $\in$ M



Puisque K $\subseteq$ L, un automorphisme de M qui fixe L doit aussi fixer K.

Donc si $\theta \in Gal(M : L)$ alors $\theta \in Gal(M : K)$.

Sous-groupes

On démontre que $Gal(M : L)$ est un sous-groupe de $Gal(M : K)$

On considère ϕ, $\psi \in Gal(M : L)$

On considère l'élément $\phi\psi^{-1}$. On veut démontrer que $\phi\psi^{-1} \in Gal(M : L)$

ϕ est un automorphisme de M qui fixe L.

ψ est aussi un automorphisme de M qui fixe L ce qui veut dire que son inverse ψ^{-1} doit aussi fixer L.

La composition de deux automorphismes qui fixent L doit aussi fixer L.

On peut en conclure que $\phi\psi^{-1}$ fixe L, et donc $\phi\psi^{-1} \in Gal(M : L)$.

Sous-groupes

On démontre que $Gal(M : L)$ est un sous-groupe de $Gal(M : K)$

On considère ϕ, $\psi \in Gal(M : L)$

On considère l'élément $\phi\psi^{-1}$. On veut démontrer que $\phi\psi^{-1} \in Gal(M : L)$

ϕ est un automorphisme de M qui fixe L.

ψ est aussi un automorphisme de M qui fixe L ce qui veut dire que son inverse ψ^{-1} doit aussi fixer L.

La composition de deux automorphismes qui fixent L doit aussi fixer L.

On peut en conclure que $\phi\psi^{-1}$ fixe L, et donc $\phi\psi^{-1} \in Gal(M : L)$.

Sous-groupes

On démontre que $Gal(M : L)$ est un sous-groupe de $Gal(M : K)$

On considère ϕ, $\psi \in Gal(M : L)$

On considère l'élément $\phi\psi^{-1}$. On veut démontrer que $\phi\psi^{-1} \in Gal(M : L)$

ϕ est un automorphisme de M qui fixe L.

ψ est aussi un automorphisme de M qui fixe L ce qui veut dire que son inverse ψ^{-1} doit aussi fixer L.

La composition de deux automorphismes qui fixent L doit aussi fixer L.

On peut en conclure que $\phi\psi^{-1}$ fixe L, et donc $\phi\psi^{-1} \in Gal(M : L)$.

Sous-groupes

On démontre que $Gal(M : L)$ est un sous-groupe de $Gal(M : K)$

On considère ϕ, $\psi \in Gal(M : L)$

On considère l'élément $\phi\psi^{-1}$. On veut démontrer que $\phi\psi^{-1} \in Gal(M : L)$

ϕ est un automorphisme de M qui fixe L.

ψ est aussi un automorphisme de M qui fixe L ce qui veut dire que son inverse ψ^{-1} doit aussi fixer L.

La composition de deux automorphismes qui fixent L doit aussi fixer L.

On peut en conclure que $\phi\psi^{-1}$ fixe L, et donc $\phi\psi^{-1} \in Gal(M : L)$.

Sous-groupes

On démontre que $Gal(M : L)$ est un sous-groupe de $Gal(M : K)$

On considère ϕ, $\psi \in Gal(M : L)$

On considère l'élément $\phi\psi^{-1}$. On veut démontrer que $\phi\psi^{-1} \in Gal(M : L)$

ϕ est un automorphisme de M qui fixe L.

ψ est aussi un automorphisme de M qui fixe L ce qui veut dire que son inverse ψ^{-1} doit aussi fixer L.

La composition de deux automorphismes qui fixent L doit aussi fixer L.

On peut en conclure que $\phi\psi^{-1}$ fixe L, et donc $\phi\psi^{-1} \in Gal(M : L)$.

Sous-groupes

On démontre que $Gal(M : L)$ est un sous-groupe de $Gal(M : K)$

On considère ϕ, $\psi \in Gal(M : L)$

On considère l'élément $\phi\psi^{-1}$. On veut démontrer que $\phi\psi^{-1} \in Gal(M : L)$

ϕ est un automorphisme de M qui fixe L.

ψ est aussi un automorphisme de M qui fixe L ce qui veut dire que son inverse ψ^{-1} doit aussi fixer L.

La composition de deux automorphismes qui fixent L doit aussi fixer L.

On peut en conclure que $\phi\psi^{-1}$ fixe L, et donc $\phi\psi^{-1} \in Gal(M : L)$.

Sous-groupes

On démontre que $Gal(M : L)$ est un sous-groupe de $Gal(M : K)$

On considère ϕ, $\psi \in Gal(M : L)$

On considère l'élément $\phi\psi^{-1}$. On veut démontrer que $\phi\psi^{-1} \in Gal(M : L)$

ϕ est un automorphisme de M qui fixe L.

ψ est aussi un automorphisme de M qui fixe L ce qui veut dire que son inverse ψ^{-1} doit aussi fixer L.

La composition de deux automorphismes qui fixent L doit aussi fixer L.

On peut en conclure que $\phi\psi^{-1}$ fixe L, et donc $\phi\psi^{-1} \in Gal(M : L)$.

Sous-groupes

On démontre que $Gal(M : L)$ est un sous-groupe de $Gal(M : K)$

On considère ϕ, $\psi \in Gal(M : L)$

On considère l'élément $\phi\psi^{-1}$. On veut démontrer que $\phi\psi^{-1} \in Gal(M : L)$

ϕ est un automorphisme de M qui fixe L.

ψ est aussi un automorphisme de M qui fixe L ce qui veut dire que son inverse ψ^{-1} doit aussi fixer L.

La composition de deux automorphismes qui fixent L doit aussi fixer L.

On peut en conclure que $\phi\psi^{-1}$ fixe L, et donc $\phi\psi^{-1} \in Gal(M : L)$.

Sous-groupes normaux et groupes quotients

On démontre que $Gal(M : L)$ est un sous-groupe normal de $Gal(M : K)$

On utilise le test pour les sous-groupes normales:

Un sous-groupe $Gal(M : L)$ est normal dans $Gal(M : K)$ si pour toutes éléments ϕ de $Gal(M : L)$ et θ de $Gal(M : K)$ alors $\theta^{-1}\phi\theta \in Gal(M : L)$

On considère un élément $a \in$ L. On veut démontrer que $\theta^{-1}\phi\theta$ fixe a c'est à dire que $\theta^{-1}\phi\theta(a) = a$

On veut donc montrer que $\phi\theta(a) = \theta(a)$.

Puisque $\theta(a)$ est une permutation de racines et que L est normal, alors a sera envoyé par θ à une racine qui est aussi dans L.

Sous-groupes normaux et groupes quotients

On démontre que $Gal(M : L)$ est un sous-groupe normal de $Gal(M : K)$

On utilise le test pour les sous-groupes normales:

Un sous-groupe $Gal(M : L)$ est normal dans $Gal(M : K)$ si pour toutes éléments ϕ de $Gal(M : L)$ et θ de $Gal(M : K)$ alors $\theta^{-1}\phi\theta \in Gal(M : L)$

On considère un élément $a \in$ L. On veut démontrer que $\theta^{-1}\phi\theta$ fixe a c'est à dire que $\theta^{-1}\phi\theta(a) = a$

On veut donc montrer que $\phi\theta(a) = \theta(a)$.

Puisque $\theta(a)$ est une permutation de racines et que L est normal, alors a sera envoyé par θ à une racine qui est aussi dans L.

Sous-groupes normaux et groupes quotients

On démontre que $Gal(M : L)$ est un sous-groupe normal de $Gal(M : K)$

On utilise le test pour les sous-groupes normales:

Un sous-groupe $Gal(M : L)$ est normal dans $Gal(M : K)$ si pour toutes éléments ϕ de $Gal(M : L)$ et θ de $Gal(M : K)$ alors $\theta^{-1}\phi\theta \in Gal(M : L)$

On considère un élément $a \in$ L. On veut démontrer que $\theta^{-1}\phi\theta$ fixe a c'est à dire que $\theta^{-1}\phi\theta(a) = a$

On veut donc montrer que $\phi\theta(a) = \theta(a)$.

Puisque $\theta(a)$ est une permutation de racines et que L est normal, alors a sera envoyé par θ à une racine qui est aussi dans L.

Sous-groupes normaux et groupes quotients

On démontre que $Gal(M : L)$ est un sous-groupe normal de $Gal(M : K)$

On utilise le test pour les sous-groupes normales:

Un sous-groupe $Gal(M : L)$ est normal dans $Gal(M : K)$ si pour toutes éléments ϕ de $Gal(M : L)$ et θ de $Gal(M : K)$ alors $\theta^{-1}\phi\theta \in Gal(M : L)$

On considère un élément $a \in$ L. On veut démontrer que $\theta^{-1}\phi\theta$ fixe a c'est à dire que $\theta^{-1}\phi\theta(a) = a$

On veut donc montrer que $\phi\theta(a) = \theta(a)$.

Puisque $\theta(a)$ est une permutation de racines et que L est normal, alors a sera envoyé par θ à une racine qui est aussi dans L.

Sous-groupes normaux et groupes quotients

On démontre que $Gal(M : L)$ est un sous-groupe normal de $Gal(M : K)$

On utilise le test pour les sous-groupes normales:

Un sous-groupe $Gal(M : L)$ est normal dans $Gal(M : K)$ si pour toutes éléments ϕ de $Gal(M : L)$ et θ de $Gal(M : K)$ alors $\theta^{-1}\phi\theta \in Gal(M : L)$

On considère un élément $a \in$ L. On veut démontrer que $\theta^{-1}\phi\theta$ fixe a c'est à dire que $\theta^{-1}\phi\theta(a) = a$

On veut donc montrer que $\phi\theta(a) = \theta(a)$.

Puisque $\theta(a)$ est une permutation de racines et que L est normal, alors a sera envoyé par θ à une racine qui est aussi dans L.

Sous-groupes normaux et groupes quotients

On démontre que $Gal(M : L)$ est un sous-groupe normal de $Gal(M : K)$

On utilise le test pour les sous-groupes normales:

Un sous-groupe $Gal(M : L)$ est normal dans $Gal(M : K)$ si pour toutes éléments ϕ de $Gal(M : L)$ et θ de $Gal(M : K)$ alors $\theta^{-1}\phi\theta \in Gal(M : L)$

On considère un élément $a \in$ L. On veut démontrer que $\theta^{-1}\phi\theta$ fixe a c'est à dire que $\theta^{-1}\phi\theta(a) = a$

On veut donc montrer que $\phi\theta(a) = \theta(a)$.

Puisque $\theta(a)$ est une permutation de racines et que L est normal, alors a sera envoyé par θ à une racine qui est aussi dans L.

Sous-groupes normaux et groupes quotients

On démontre que $Gal(M : L)$ est un sous-groupe normal de $Gal(M : K)$

On utilise le test pour les sous-groupes normales:

Un sous-groupe $Gal(M : L)$ est normal dans $Gal(M : K)$ si pour toutes éléments ϕ de $Gal(M : L)$ et θ de $Gal(M : K)$ alors $\theta^{-1}\phi\theta \in Gal(M : L)$

On considère un élément $a \in$ L. On veut démontrer que $\theta^{-1}\phi\theta$ fixe a c'est à dire que $\theta^{-1}\phi\theta(a) = a$

On veut donc montrer que $\phi\theta(a) = \theta(a)$.

Puisque $\theta(a)$ est une permutation de racines et que L est normal, alors a sera envoyé par θ à une racine qui est aussi dans L.

Sous-groupes normaux et groupes quotients

On a que $\theta(a) \in L$.

Puisque ϕ est un élément de $Gal(M : L)$ qui fixe les éléments de L, on a que l'égalité $\phi\theta(a) = \theta(a)$ est vrai.

$Gal(M : L)$ est donc un sous-groupe normal de $Gal(M : K)$.

Pour prouver $\frac{Gal(M:K)}{Gal(M:L)} \cong Gal(L : K)$, on construit une fonction surjective entre $Gal(M : K)$ et $Gal(L : K)$ (Premier théorème d'isomorphisme)

$$\begin{tikzcd}
Gal(M:K) \arrow[rr, "\phi"] \arrow[dr, "\psi"'] & & Gal(L:K) \\
& \frac{Gal(M:K)}{Gal(M:L)} \arrow[ur, "\bar{\phi}"'] &
\end{tikzcd}$$

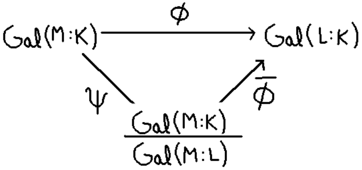
Sous-groupes normaux et groupes quotients

On a que $\theta(a) \in L$.

Puisque ϕ est un élément de $Gal(M : L)$ qui fixe les éléments de L, on a que l'égalité $\phi\theta(a) = \theta(a)$ est vrai.

$Gal(M : L)$ est donc un sous-groupe normal de $Gal(M : K)$.

Pour prouver $\frac{Gal(M:K)}{Gal(M:L)} \cong Gal(L : K)$, on construit une fonction surjective entre $Gal(M : K)$ et $Gal(L : K)$ (Premier théorème d'isomorphisme)



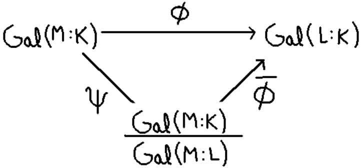
Sous-groupes normaux et groupes quotients

On a que $\theta(a) \in L$.

Puisque ϕ est un élément de $Gal(M : L)$ qui fixe les éléments de L, on a que l'égalité $\phi\theta(a) = \theta(a)$ est vrai.

$Gal(M : L)$ est donc un sous-groupe normal de $Gal(M : K)$.

Pour prouver $\frac{Gal(M:K)}{Gal(M:L)} \cong Gal(L : K)$, on construit une fonction surjective entre $Gal(M : K)$ et $Gal(L : K)$ (Premier théorème d'isomorphisme)



Sous-groupes normaux et groupes quotients

On a que $\theta(a) \in L$.

Puisque ϕ est un élément de $Gal(M : L)$ qui fixe les éléments de L, on a que l'égalité $\phi\theta(a) = \theta(a)$ est vrai.

$Gal(M : L)$ est donc un sous-groupe normal de $Gal(M : K)$.

Pour prouver $\frac{Gal(M:K)}{Gal(M:L)} \cong Gal(L : K)$, on construit une fonction surjective entre $Gal(M : K)$ et $Gal(L : K)$ (Premier théorème d'isomorphisme)

$$\begin{tikzcd}
Gal(M:K) \arrow[rr, "\phi"] \arrow[dr, dash, "\psi"'] & & Gal(L:K) \\
& \frac{Gal(M:K)}{Gal(M:L)} \arrow[ur, "\bar{\phi}"'] &
\end{tikzcd}$$

Sous-groupes normaux et groupes quotients

On a que $\theta(a) \in L$.

Puisque ϕ est un élément de $Gal(M : L)$ qui fixe les éléments de L, on a que l'égalité $\phi\theta(a) = \theta(a)$ est vrai.

$Gal(M : L)$ est donc un sous-groupe normal de $Gal(M : K)$.

Pour prouver $\frac{Gal(M:K)}{Gal(M:L)} \cong Gal(L : K)$, on construit une fonction surjective entre $Gal(M : K)$ et $Gal(L : K)$ (Premier théorème d'isomorphisme)

$$\begin{tikzcd}
Gal(M:K) \arrow[rr, "\phi"] \arrow[dr, "\psi"'] & & Gal(L:K) \\
& \frac{Gal(M:K)}{Gal(M:L)} \arrow[ur, "\bar{\phi}"'] &
\end{tikzcd}$$

Les extensions résolubles ont des groupes de Galois résolubles

Théorème

Si une extension M : K est résoluble, alors son groupe de Galois Gal(M : K) est aussi résoluble.

Une extension M : K est résoluble si il existe une séquence de corps tel que:

$K = L_0 \subseteq L_1 \subseteq ...L_{n-1} \subseteq L_n = M$ avec $L_i : L_{i-1}$ normale et $Gal(L_i : L_{i-1})$ commutatif pour tout i $\in \{0, 1, ..., n\}$

Un groupe G est résoluble si il existe une séquence de sous-groupes normaux tel que:

$G = G_0 \trianglerighteq G_1 \trianglerighteq ... \trianglerighteq G_n - 1 \trianglerighteq G_n = \{e\}$ et $\frac{G_i}{G_i+1}$ commutatif pour tout i $\in \{0, 1, ..., n\}$

Les extensions résolubles ont des groupes de Galois résolubles

Théorème

Si une extension M : K est résoluble, alors son groupe de Galois Gal(M : K) est aussi résoluble.

Une extension M : K est résoluble si il existe une séquence de corps tel que:

$K = L_0 \subseteq L_1 \subseteq ... L_{n-1} \subseteq L_n = M$ avec $L_i : L_{i-1}$ normale et $Gal(L_i : L_{i-1})$ commutatif pour tout i $\in \{0, 1, ..., n\}$

Un groupe G est résoluble si il existe une séquence de sous-groupes normaux tel que:

$G = G_0 \trianglerighteq G_1 \trianglerighteq ... \trianglerighteq G_n - 1 \trianglerighteq G_n = \{e\}$ et $\frac{G_i}{G_i + 1}$ commutatif pour tout i $\in \{0, 1, ..., n\}$

Les extensions résolubles ont des groupes de Galois résolubles

Théorème

Si une extension M : K est résoluble, alors son groupe de Galois Gal(M : K) est aussi résoluble.

Une extension M : K est résoluble si il existe une séquence de corps tel que:

$K = L_0 \subseteq L_1 \subseteq ...L_{n-1} \subseteq L_n = M$ avec $L_i : L_{i-1}$ normale et $Gal(L_i : L_{i-1})$ commutatif pour tout i $\in \{0, 1, ..., n\}$

Un groupe G est résoluble si il existe une séquence de sous-groupes normaux tel que:

$G = G_0 \trianglerighteq G_1 \trianglerighteq ... \trianglerighteq G_n - 1 \trianglerighteq G_n = \{e\}$ et $\frac{G_i}{G_i + 1}$ commutatif pour tout i $\in \{0, 1, ..., n\}$

Les extensions résolubles ont des groupes de Galois résolubles

On considère une extension résoluble M : K tel que

$K = L_0 \subseteq L_1 \subseteq ...L_{n-1} \subseteq L_n = M$ avec $L_i : L_{i-1}$ normale et $Gal(L_i : L_{i-1})$ commutatif pour tout i $\in \{0, 1, ..., n\}$.

Selon le théorème fondamental de la théorie de Galois

Puisque $L_i : L_{i-1}$ est normale, on peut en conclure que $Gal(M : L_i) \trianglelefteq Gal(M : L_{i-1})$

On a aussi que $\frac{Gal(M:L_{i-1})}{Gal(M:L_i)} \cong Gal(L_i : L_{i-1})$

Les extensions résolubles ont des groupes de Galois résolubles

On considère une extension résoluble M : K tel que

$K = L_0 \subseteq L_1 \subseteq ...L_{n-1} \subseteq L_n = M$ avec $L_i : L_{i-1}$ normale et $Gal(L_i : L_{i-1})$ commutatif pour tout i $\in \{0, 1, ..., n\}$.

Selon le théorème fondamental de la théorie de Galois

Puisque $L_i : L_{i-1}$ est normale, on peut en conclure que $Gal(M : L_i) \trianglelefteq Gal(M : L_{i-1})$

On a aussi que $\frac{Gal(M:L_{i-1})}{Gal(M:L_i)} \cong Gal(L_i : L_{i-1})$

Les extensions résolubles ont des groupes de Galois résolubles

On considère une extension résoluble M : K tel que

$K = L_0 \subseteq L_1 \subseteq ...L_{n-1} \subseteq L_n = M$ avec $L_i : L_{i-1}$ normale et $Gal(L_i : L_{i-1})$ commutatif pour tout i $\in \{0, 1, ..., n\}$.

Selon le théorème fondamental de la théorie de Galois

Puisque $L_i : L_{i-1}$ est normale, on peut en conclure que $Gal(M : L_i) \trianglelefteq Gal(M : L_{i-1})$

On a aussi que $\frac{Gal(M:L_{i-1})}{Gal(M:L_i)} \cong Gal(L_i : L_{i-1})$

Les extensions résolubles ont des groupes de Galois résolubles

On considère une extension résoluble M : K tel que

$K = L_0 \subseteq L_1 \subseteq ...L_{n-1} \subseteq L_n = M$ avec $L_i : L_{i-1}$ normale et $Gal(L_i : L_{i-1})$ commutatif pour tout i $\in \{0, 1, ..., n\}$.

Selon le théorème fondamental de la théorie de Galois

Puisque $L_i : L_{i-1}$ est normale, on peut en conclure que $Gal(M : L_i) \trianglelefteq Gal(M : L_{i-1})$

On a aussi que $\frac{Gal(M:L_{i-1})}{Gal(M:L_i)} \cong Gal(L_i : L_{i-1})$

Les extensions résolubles ont des groupes de Galois résolubles

On considère une extension résoluble M : K tel que

$K = L_0 \subseteq L_1 \subseteq ...L_{n-1} \subseteq L_n = M$ avec $L_i : L_{i-1}$ normale et $Gal(L_i : L_{i-1})$ commutatif pour tout i $\in \{0, 1, ..., n\}$.

Selon le théorème fondamental de la théorie de Galois

Puisque $L_i : L_{i-1}$ est normale, on peut en conclure que $Gal(M : L_i) \trianglelefteq Gal(M : L_{i-1})$

On a aussi que $\frac{Gal(M:L_{i-1})}{Gal(M:L_i)} \cong Gal(L_i : L_{i-1})$

Les extensions résolubles ont des groupes de Galois résolubles

$Gal(L_i : L_{i-1})$ est commutatif selon la définition d'une extension résoluble

$\frac{Gal(M:L_{i-1})}{Gal(M:L_i)}$ doit donc aussi être commutatif car les deux groupes partagent la même structure.

On peut en déduire que

$Gal(M : K) = Gal(M : L_0) \trianglerighteq ... \trianglerighteq Gal(M : L_n) = Gal(M : M) = \{e\}$

avec $\frac{Gal(M:L_{i-1})}{Gal(M:L_i)}$ commutatif.

Cela correspond à la définition d'une extension résoluble.

On peut en conclure que si une extension est résoluble, son groupe de Galois est résoluble.

Les extensions résolubles ont des groupes de Galois résolubles

$Gal(L_i : L_{i-1})$ est commutatif selon la définition d'une extension résoluble

$\frac{Gal(M:L_{i-1})}{Gal(M:L_i)}$ doit donc aussi être commutatif car les deux groupes partagent la même structure.

On peut en déduire que

$Gal(M : K) = Gal(M : L_0) \trianglerighteq ... \trianglerighteq Gal(M : L_n) = Gal(M : M) = \{e\}$

avec $\frac{Gal(M:L_{i-1})}{Gal(M:L_i)}$ commutatif.

Cela correspond à la définition d'une extension résoluble.

On peut en conclure que si une extension est résoluble, son groupe de Galois est résoluble.

Les extensions résolubles ont des groupes de Galois résolubles

$Gal(L_i : L_{i-1})$ est commutatif selon la définition d'une extension résoluble

$\frac{Gal(M:L_{i-1})}{Gal(M:L_i)}$ doit donc aussi être commutatif car les deux groupes partagent la même structure.

On peut en déduire que

$$Gal(M : K) = Gal(M : L_0) \trianglerighteq ... \trianglerighteq Gal(M : L_n) = Gal(M : M) = \{e\}$$

avec $\frac{Gal(M:L_{i-1})}{Gal(M:L_i)}$ commutatif.

Cela correspond à la définition d'une extension résoluble.

On peut en conclure que si une extension est résoluble, son groupe de Galois est résoluble.

Les extensions résolubles ont des groupes de Galois résolubles

$Gal(L_i : L_{i-1})$ est commutatif selon la définition d'une extension résoluble

$\frac{Gal(M:L_{i-1})}{Gal(M:L_i)}$ doit donc aussi être commutatif car les deux groupes partagent la même structure.

On peut en déduire que

$$Gal(M : K) = Gal(M : L_0) \trianglerighteq ... \trianglerighteq Gal(M : L_n) = Gal(M : M) = \{e\}$$

avec $\frac{Gal(M:L_{i-1})}{Gal(M:L_i)}$ commutatif.

Cela correspond à la définition d'une extension résoluble.

On peut en conclure que si une extension est résoluble, son groupe de Galois est résoluble.

Les extensions résolubles ont des groupes de Galois résolubles

$Gal(L_i : L_{i-1})$ est commutatif selon la définition d'une extension résoluble

$\frac{Gal(M:L_{i-1})}{Gal(M:L_i)}$ doit donc aussi être commutatif car les deux groupes partagent la même structure.

On peut en déduire que

$$Gal(M : K) = Gal(M : L_0) \trianglerighteq ... \trianglerighteq Gal(M : L_n) = Gal(M : M) = \{e\}$$

avec $\frac{Gal(M:L_{i-1})}{Gal(M:L_i)}$ commutatif.

Cela correspond à la définition d'une extension résoluble.

On peut en conclure que si une extension est résoluble, son groupe de Galois est résoluble.

Les polynômes résolubles ont des groupes de Galois résolubles

Théorème

Si un polynôme irréductible f avec coefficients dans $\mathbb{Q}$ est résoluble par radicaux, alors le groupe de Galois du corps de rupture de ce polynôme est résoluble par radicaux.

Définition

Le `groupe de Galois du corps de rupture` du polynôme f est le groupe de Galois du plus petit corps contenant toutes les racines de f. Le groupe de Galois de $\mathbb{SF}_{\mathbb{Q}}(f)$ est dénoté $Gal(\mathbb{SF}_{\mathbb{Q}}(f) : \mathbb{Q})$ ou $Gal_{\mathbb{Q}}(f)$.

On va prendre pour aquis le résultat suivant:

Théorème

Si f est résoluble par radicaux, alors ses racines $\alpha_1, ..., \alpha_n$ sont toutes contenues dans une extension de $\mathbb{Q}$ qui est finie, normale et résoluble.

Les polynômes résolubles ont des groupes de Galois résolubles

Si f est résoluble, alors ses racines $\alpha_1, ..., \alpha_n$ sont toutes contenues dans une extension de $\mathbb{Q}$ qui est finie, normale et résoluble (théorème pris pour aquis).

Cette extension sera dénotée M.

Puisque $\mathbb{SF}_{\mathbb{Q}}(f)$ est le plus petit corps contenant les racines de f, alors $\mathbb{SF}_{\mathbb{Q}}(f) \subseteq M$.

Nous avons donc M : $\mathbb{SF}_{\mathbb{Q}}(f)$: $\mathbb{Q}$.

Puisque $\mathbb{SF}_{\mathbb{Q}}(f)$ est un corps de rupture, l'extension $\mathbb{SF}_{\mathbb{Q}}(f)$: $\mathbb{Q}$ est normale

Nous pouvons donc appliquer le théorème fondamental de la théorie de Galois.

Les polynômes résolubles ont des groupes de Galois résolubles

Si f est résoluble, alors ses racines $\alpha_1, ..., \alpha_n$ sont toutes contenues dans une extension de $\mathbb{Q}$ qui est finie, normale et résoluble (théorème pris pour aquis).

Cette extension sera dénotée M.

Puisque $\mathbb{SF}_{\mathbb{Q}}(f)$ est le plus petit corps contenant les racines de f, alors $\mathbb{SF}_{\mathbb{Q}}(f) \subseteq M$.

Nous avons donc M : $\mathbb{SF}_{\mathbb{Q}}(f)$: $\mathbb{Q}$.

Puisque $\mathbb{SF}_{\mathbb{Q}}(f)$ est un corps de rupture, l'extension $\mathbb{SF}_{\mathbb{Q}}(f)$: $\mathbb{Q}$ est normale

Nous pouvons donc appliquer le théorème fondamental de la théorie de Galois.

Les polynômes résolubles ont des groupes de Galois résolubles

Si f est résoluble, alors ses racines $\alpha_1, ..., \alpha_n$ sont toutes contenues dans une extension de $\mathbb{Q}$ qui est finie, normale et résoluble (théorème pris pour aquis).

Cette extension sera dénotée M.

Puisque $\mathbb{SF}_{\mathbb{Q}}(f)$ est le plus petit corps contenant les racines de f, alors $\mathbb{SF}_{\mathbb{Q}}(f) \subseteq M$.

Nous avons donc M : $\mathbb{SF}_{\mathbb{Q}}(f)$: $\mathbb{Q}$.

Puisque $\mathbb{SF}_{\mathbb{Q}}(f)$ est un corps de rupture, l'extension $\mathbb{SF}_{\mathbb{Q}}(f)$: $\mathbb{Q}$ est normale

Nous pouvons donc appliquer le théorème fondamental de la théorie de Galois.

Les polynômes résolubles ont des groupes de Galois résolubles

Si f est résoluble, alors ses racines $\alpha_1, ..., \alpha_n$ sont toutes contenues dans une extension de $\mathbb{Q}$ qui est finie, normale et résoluble (théorème pris pour aquis).

Cette extension sera dénotée M.

Puisque $\mathbb{SF}_{\mathbb{Q}}(f)$ est le plus petit corps contenant les racines de f, alors $\mathbb{SF}_{\mathbb{Q}}(f) \subseteq M$.

Nous avons donc M : $\mathbb{SF}_{\mathbb{Q}}(f)$: $\mathbb{Q}$.

Puisque $\mathbb{SF}_{\mathbb{Q}}(f)$ est un corps de rupture, l'extension $\mathbb{SF}_{\mathbb{Q}}(f)$: $\mathbb{Q}$ est normale

Nous pouvons donc appliquer le théorème fondamental de la théorie de Galois.

Les polynômes résolubles ont des groupes de Galois résolubles

Si f est résoluble, alors ses racines $\alpha_1, ..., \alpha_n$ sont toutes contenues dans une extension de $\mathbb{Q}$ qui est finie, normale et résoluble (théorème pris pour aquis).

Cette extension sera dénotée M.

Puisque $\mathbb{SF}_{\mathbb{Q}}(f)$ est le plus petit corps contenant les racines de f, alors $\mathbb{SF}_{\mathbb{Q}}(f) \subseteq M$.

Nous avons donc M : $\mathbb{SF}_{\mathbb{Q}}(f)$: $\mathbb{Q}$.

Puisque $\mathbb{SF}_{\mathbb{Q}}(f)$ est un corps de rupture, l'extension $\mathbb{SF}_{\mathbb{Q}}(f)$: $\mathbb{Q}$ est normale

Nous pouvons donc appliquer le théorème fondamental de la théorie de Galois.

Les polynômes résolubles ont des groupes de Galois résolubles

Si f est résoluble, alors ses racines $\alpha_1, ..., \alpha_n$ sont toutes contenues dans une extension de $\mathbb{Q}$ qui est finie, normale et résoluble (théorème pris pour aquis).

Cette extension sera dénotée M.

Puisque $\mathbb{SF}_{\mathbb{Q}}(f)$ est le plus petit corps contenant les racines de f, alors $\mathbb{SF}_{\mathbb{Q}}(f) \subseteq M$.

Nous avons donc M : $\mathbb{SF}_{\mathbb{Q}}(f)$: $\mathbb{Q}$.

Puisque $\mathbb{SF}_{\mathbb{Q}}(f)$ est un corps de rupture, l'extension $\mathbb{SF}_{\mathbb{Q}}(f)$: $\mathbb{Q}$ est normale

Nous pouvons donc appliquer le théorème fondamental de la théorie de Galois.

Les polynômes résolubles ont des groupes de Galois résolubles

Si f est résoluble, alors ses racines $\alpha_1, \ldots, \alpha_n$ sont toutes contenues dans une extension de $\mathbb{Q}$ qui est finie, normale et résoluble (théorème pris pour aquis).

Cette extension sera dénotée M.

Puisque $\mathbb{SF}_{\mathbb{Q}}(f)$ est le plus petit corps contenant les racines de f, alors $\mathbb{SF}_{\mathbb{Q}}(f) \subseteq M$.

Nous avons donc M : $\mathbb{SF}_{\mathbb{Q}}(f)$: $\mathbb{Q}$.

Puisque $\mathbb{SF}_{\mathbb{Q}}(f)$ est un corps de rupture, l'extension $\mathbb{SF}_{\mathbb{Q}}(f)$: $\mathbb{Q}$ est normale

Nous pouvons donc appliquer le théorème fondamental de la théorie de Galois.

Les polynômes résolubles ont des groupes de Galois résolubles

Nous avons donc que $Gal(M : \mathbb{SF}_{\mathbb{Q}}(f)) \trianglelefteq Gal(M : \mathbb{Q})$ et que $\frac{Gal(M:\mathbb{Q})}{Gal(M:\mathbb{SF}_{\mathbb{Q}}(f)} \cong Gal(\mathbb{SF}_{\mathbb{Q}}(f)) : \mathbb{Q})$.

Puisque $Gal(M : \mathbb{Q})$ est résoluble, son quotient est résoluble (on doit prendre cette étape pour aquis)

Puisque $\frac{Gal(M:\mathbb{Q})}{Gal(M:\mathbb{SF}_{\mathbb{Q}}(f)}$ est résoluble, $Gal(\mathbb{SF}_{\mathbb{Q}}(f)) : \mathbb{Q})$ est aussi résolubles. (les deux groupes partagent la même structure)

On a donc que $Gal(\mathbb{SF}_{\mathbb{Q}}(f)) : \mathbb{Q}) = Gal_{\mathbb{Q}}$(f) est résoluble quand f résoluble.

Les polynômes résolubles ont des groupes de Galois résolubles

Nous avons donc que $Gal(M : \mathbb{SF}_{\mathbb{Q}}(f)) \trianglelefteq Gal(M : \mathbb{Q})$ et que $\frac{Gal(M:\mathbb{Q})}{Gal(M:\mathbb{SF}_{\mathbb{Q}}(f)} \cong Gal(\mathbb{SF}_{\mathbb{Q}}(f)) : \mathbb{Q})$.

Puisque $Gal(M : \mathbb{Q})$ est résoluble, son quotient est résoluble (on doit prendre cette étape pour aquis)

Puisque $\frac{Gal(M:\mathbb{Q})}{Gal(M:\mathbb{SF}_{\mathbb{Q}}(f)}$ est résoluble, $Gal(\mathbb{SF}_{\mathbb{Q}}(f)) : \mathbb{Q})$ est aussi résolubles. (les deux groupes partagent la même structure)

On a donc que $Gal(\mathbb{SF}_{\mathbb{Q}}(f)) : \mathbb{Q}) = Gal_{\mathbb{Q}}(\mathrm{f})$ est résoluble quand f résoluble.

Les polynômes résolubles ont des groupes de Galois résolubles

Nous avons donc que $Gal(M : \mathbb{SF}_{\mathbb{Q}}(f)) \trianglelefteq Gal(M : \mathbb{Q})$ et que $\frac{Gal(M:\mathbb{Q})}{Gal(M:\mathbb{SF}_{\mathbb{Q}}(f)} \cong Gal(\mathbb{SF}_{\mathbb{Q}}(f)) : \mathbb{Q})$.

Puisque $Gal(M : \mathbb{Q})$ est résoluble, son quotient est résoluble (on doit prendre cette étape pour aquis)

Puisque $\frac{Gal(M:\mathbb{Q})}{Gal(M:\mathbb{SF}_{\mathbb{Q}}(f)}$ est résoluble, $Gal(\mathbb{SF}_{\mathbb{Q}}(f)) : \mathbb{Q})$ est aussi résolubles. (les deux groupes partagent la même structure)

On a donc que $Gal(\mathbb{SF}_{\mathbb{Q}}(f)) : \mathbb{Q}) = Gal_{\mathbb{Q}}$(f) est résoluble quand f résoluble.

Les polynômes résolubles ont des groupes de Galois résolubles

Nous avons donc que $Gal(M : \mathbb{SF}_{\mathbb{Q}}(f)) \trianglelefteq Gal(M : \mathbb{Q})$ et que $\frac{Gal(M:\mathbb{Q})}{Gal(M:\mathbb{SF}_{\mathbb{Q}}(f)} \cong Gal(\mathbb{SF}_{\mathbb{Q}}(f)) : \mathbb{Q})$.

Puisque $Gal(M : \mathbb{Q})$ est résoluble, son quotient est résoluble (on doit prendre cette étape pour aquis)

Puisque $\frac{Gal(M:\mathbb{Q})}{Gal(M:\mathbb{SF}_{\mathbb{Q}}(f)}$ est résoluble, $Gal(\mathbb{SF}_{\mathbb{Q}}(f)) : \mathbb{Q})$ est aussi résolubles. (les deux groupes partagent la même structure)

On a donc que $Gal(\mathbb{SF}_{\mathbb{Q}}(f)) : \mathbb{Q}) = Gal_{\mathbb{Q}}(\mathrm{f})$ est résoluble quand f résoluble.

Les polynômes résolubles ont des groupes de Galois résolubles

Nous avons donc que $Gal(M : \mathbb{SF}_{\mathbb{Q}}(f)) \trianglelefteq Gal(M : \mathbb{Q})$ et que $\frac{Gal(M:\mathbb{Q})}{Gal(M:\mathbb{SF}_{\mathbb{Q}}(f)} \cong Gal(\mathbb{SF}_{\mathbb{Q}}(f)) : \mathbb{Q})$.

Puisque $Gal(M : \mathbb{Q})$ est résoluble, son quotient est résoluble (on doit prendre cette étape pour aquis)

Puisque $\frac{Gal(M:\mathbb{Q})}{Gal(M:\mathbb{SF}_{\mathbb{Q}}(f)}$ est résoluble, $Gal(\mathbb{SF}_{\mathbb{Q}}(f)) : \mathbb{Q})$ est aussi résolubles. (les deux groupes partagent la même structure)

On a donc que $Gal(\mathbb{SF}_{\mathbb{Q}}(f)) : \mathbb{Q}) = Gal_{\mathbb{Q}}(\mathrm{f})$ est résoluble quand f résoluble.

Un polynôme non résoluble par radicaux

Théorème d'Abel Ruffini

Il n'existe pas de formule pour les racines de polynôme de degré 5.

Si un polynôme irréductible f a un groupe de Galois non résoluble, cela implique que f n'est pas résoluble par radicaux.

Le polynôme irréductible $x^5 - 6x + 3$ a un groupe de Galois qui a la même structure que le groupe de symmétrie S_5.

Le seule sous-groupe de S_5 est A_5.

A_5 n'a pas d'autre sous-groupe normaux que le groupe contenant seulement l'élément neutre.

Un polynôme non résoluble par radicaux

Théorème d'Abel Ruffini

Il n'existe pas de formule pour les racines de polynôme de degré 5.

Si un polynôme irréductible f a un groupe de Galois non résoluble, cela implique que f n'est pas résoluble par radicaux.

Le polynôme irréductible $x^5 - 6x + 3$ a un groupe de Galois qui a la même structure que le groupe de symmétrie S_5.

Le seule sous-groupe de S_5 est A_5.

A_5 n'a pas d'autre sous-groupe normaux que le groupe contenant seulement l'élément neutre.

Un polynôme non résoluble par radicaux

Théorème d'Abel Ruffini

Il n'existe pas de formule pour les racines de polynôme de degré 5.

Si un polynôme irréductible f a un groupe de Galois non résoluble, cela implique que f n'est pas résoluble par radicaux.

Le polynôme irréductible $x^5 - 6x + 3$ a un groupe de Galois qui a la même structure que le groupe de symétrie S_5.

Le seule sous-groupe de S_5 est A_5.

A_5 n'a pas d'autre sous-groupe normaux que le groupe contenant seulement l'élément neutre.

Un polynôme non résoluble par radicaux

Théorème d'Abel Ruffini

Il n'existe pas de formule pour les racines de polynôme de degré 5.

Si un polynôme irréductible f a un groupe de Galois non résoluble, cela implique que f n'est pas résoluble par radicaux.

Le polynôme irréductible $x^5 - 6x + 3$ a un groupe de Galois qui a la même structure que le groupe de symétrie S_5.

Le seule sous-groupe de S_5 est A_5.

A_5 n'a pas d'autre sous-groupe normaux que le groupe contenant seulement l'élément neutre.

Un polynôme non résoluble par radicaux

Théorème d'Abel Ruffini

Il n'existe pas de formule pour les racines de polynôme de degré 5.

Si un polynôme irréductible f a un groupe de Galois non résoluble, cela implique que f n'est pas résoluble par radicaux.

Le polynôme irréductible $x^5 - 6x + 3$ a un groupe de Galois qui a la même structure que le groupe de symmétrie S_5.

Le seule sous-groupe de S_5 est A_5.

A_5 n'a pas d'autre sous-groupe normaux que le groupe contenant seulement l'élément neutre.

Un polynôme non résoluble par radicaux

On obtient donc la chaine de sous-groupes normaux suivante:

$$S_5 \trianglerighteq A_5 \trianglerighteq \{\mathrm{e}\}$$

Si S_5 est résoluble, alors les quotients $\frac{G_i}{G_i+1}$ devraient être commutatifs.

Par contre, le quotient $\frac{A_5}{\{e\}} \cong A_5$ et A_5 n'est pas commutatif.

S_5 n'est donc pas résoluble ce qui implique que $x^5 - 6x + 3$ n'est pas résoluble par radicaux.

Il n'existe donc pas de formule pour les polynômes de degré 5 et plus car ces polynômes ne sont pas tous résolubles par radicaux.

Un polynôme non résoluble par radicaux

On obtient donc la chaine de sous-groupes normaux suivante:

$$S_5 \trianglerighteq A_5 \trianglerighteq \{\mathrm{e}\}$$

Si S_5 est résoluble, alors les quotients $\frac{G_i}{G_i+1}$ devraient être commutatifs.

Par contre, le quotient $\frac{A_5}{\{e\}} \cong A_5$ et A_5 n'est pas commutatif.

S_5 n'est donc pas résoluble ce qui implique que $x^5 - 6x + 3$ n'est pas résoluble par radicaux.

Il n'existe donc pas de formule pour les polynômes de degré 5 et plus car ces polynômes ne sont pas tous résolubles par radicaux.

Un polynôme non résoluble par radicaux

On obtient donc la chaine de sous-groupes normaux suivante:

$$S_5 \trianglerighteq A_5 \trianglerighteq \{\mathrm{e}\}$$

Si S_5 est résoluble, alors les quotients $\frac{G_i}{G_i+1}$ devraient être commutatifs.

Par contre, le quotient $\frac{A_5}{\{e\}} \cong A_5$ et A_5 n'est pas commutatif.

S_5 n'est donc pas résoluble ce qui implique que $x^5 - 6x + 3$ n'est pas résoluble par radicaux.

Il n'existe donc pas de formule pour les polynômes de degré 5 et plus car ces polynômes ne sont pas tous résolubles par radicaux.

Un polynôme non résoluble par radicaux

On obtient donc la chaine de sous-groupes normaux suivante:

$$S_5 \trianglerighteq A_5 \trianglerighteq \{\mathrm{e}\}$$

Si S_5 est résoluble, alors les quotients $\frac{G_i}{G_i+1}$ devraient être commutatifs.

Par contre, le quotient $\frac{A_5}{\{e\}} \cong A_5$ et A_5 n'est pas commutatif.

S_5 n'est donc pas résoluble ce qui implique que $x^5 - 6x + 3$ n'est pas résoluble par radicaux.

Il n'existe donc pas de formule pour les polynômes de degré 5 et plus car ces polynômes ne sont pas tous résolubles par radicaux.

Un polynôme non résoluble par radicaux

On obtient donc la chaine de sous-groupes normaux suivante:

$$S_5 \trianglerighteq A_5 \trianglerighteq \{\mathrm{e}\}$$

Si S_5 est résoluble, alors les quotients $\frac{G_i}{G_i+1}$ devraient être commutatifs.

Par contre, le quotient $\frac{A_5}{\{e\}} \cong A_5$ et A_5 n'est pas commutatif.

S_5 n'est donc pas résoluble ce qui implique que $x^5 - 6x + 3$ n'est pas résoluble par radicaux.

Il n'existe donc pas de formule pour les polynômes de degré 5 et plus car ces polynômes ne sont pas tous résolubles par radicaux.

Un polynôme non résoluble par radicaux

On obtient donc la chaine de sous-groupes normaux suivante:

$$S_5 \trianglerighteq A_5 \trianglerighteq \{\mathrm{e}\}$$

Si S_5 est résoluble, alors les quotients $\frac{G_i}{G_i+1}$ devraient être commutatifs.

Par contre, le quotient $\frac{A_5}{\{e\}} \cong A_5$ et A_5 n'est pas commutatif.

S_5 n'est donc pas résoluble ce qui implique que $x^5 - 6x + 3$ n'est pas résoluble par radicaux.

Il n'existe donc pas de formule pour les polynômes de degré 5 et plus car ces polynômes ne sont pas tous résolubles par radicaux.

Références

[1] Tom Leinster - Introduction to Galois Theory