Une introduction au problème inverse de Galois

François Legrand

Laboratoire Paul Painlevé, Université Lille 1

25 janvier 2013

Soit k un corps (commutatif).

Soit k un corps (commutatif).

Definition

Soit $P(X) \in k[X] \setminus k$. On dit que $P(X)$ est

Soit k un corps (commutatif).

Definition

Soit $P(X) \in k[X] \setminus k$. On dit que $P(X)$ est

- *irréductible sur k* si pour tout $(A(X), B(X)) \in k[X]^2$ tel que $P(X) = A(X)B(X)$, $A(X)$ est constant ou $B(X)$ est constant,

Soit k un corps (commutatif).

Definition

Soit $P(X) \in k[X] \setminus k$. On dit que $P(X)$ est

- *irréductible sur k* si pour tout $(A(X), B(X)) \in k[X]^2$ tel que $P(X) = A(X)B(X)$, $A(X)$ est constant ou $B(X)$ est constant,
- *séparable sur k* si $P(X)$ n'a que des racines simples.

Soit k un corps (commutatif).

Definition

Soit $P(X) \in k[X] \setminus k$. On dit que $P(X)$ est

- *irréductible sur k* si pour tout $(A(X), B(X)) \in k[X]^2$ tel que $P(X) = A(X)B(X)$, $A(X)$ est constant ou $B(X)$ est constant,
- *séparable sur k* si $P(X)$ n'a que des racines simples.

Remarque

Si $\mathbb{Q} \subset k$, tout polynôme irréductible sur k est séparable sur k.

Soient $P(X) \in k[X]$ un polynôme séparable sur k et n son degré. Notons $x_1, \ldots, x_n \in \overline{k}$ ses racines (distinctes).

Soient $P(X) \in k[X]$ un polynôme séparable sur k et n son degré. Notons $x_1, \ldots, x_n \in \overline{k}$ ses racines (distinctes).

Definition

(1) Le corps $k(x_1, \ldots, x_n)$ est appelé *corps de décomposition de $P(X)$ sur k*.

Soient $P(X) \in k[X]$ un polynôme séparable sur k et n son degré. Notons $x_1, \ldots, x_n \in \overline{k}$ ses racines (distinctes).

Definition

(1) Le corps $k(x_1, \ldots, x_n)$ est appelé *corps de décomposition de $P(X)$ sur k*.
(2) L'ensemble des automorphismes de $k(x_1, \ldots, x_n)$ $f : k(x_1, \ldots, x_n) \to k(x_1, \ldots, x_n)$ tels que $f(x) = x$ pour tout $x \in k$ est un groupe appelé *groupe de Galois de $P(X)$ sur k* et noté $\mathrm{Gal}(P(X)/k)$.

Soient $P(X) \in k[X]$ un polynôme séparable sur k et n son degré. Notons $x_1, \ldots, x_n \in \overline{k}$ ses racines (distinctes).

Definition

(1) Le corps $k(x_1, \ldots, x_n)$ est appelé *corps de décomposition de $P(X)$ sur k*.
(2) L'ensemble des automorphismes de $k(x_1, \ldots, x_n)$ $f : k(x_1, \ldots, x_n) \to k(x_1, \ldots, x_n)$ tels que $f(x) = x$ pour tout $x \in k$ est un groupe appelé *groupe de Galois de $P(X)$ sur k* et noté $\mathrm{Gal}(P(X)/k)$.

Remarque

Tout élément de $\mathrm{Gal}(P(X)/k)$ peut être vu comme permutation de $\{x_1, \ldots, x_n\}$. Ainsi $\mathrm{Gal}(P(X)/k)$ est isomorphe à un sous-groupe de S_n et est en particulier fini.

Inverse Galois Problem

Definition

On dit qu'*un groupe fini G est groupe de Galois sur un corps k* s'il existe un polynôme $P(X)$ irréductible et séparable sur k tel que $\mathrm{Gal}(P(X)/k) = G$.

Inverse Galois Problem

Definition

On dit qu'*un groupe fini G est groupe de Galois sur un corps k* s'il existe un polynôme $P(X)$ irréductible et séparable sur k tel que $\mathrm{Gal}(P(X)/k) = G$.

Le problème inverse de Galois consiste à répondre à la question suivante :
(**IGP**) : Tout groupe fini est-il groupe de Galois sur $\mathbb{Q}$?

La réponse à cette question n'est pas connue. Il y a eu des avancées depuis 40 ans environ. Mais le problème inverse de Galois reste toujours ouvert...

La réponse à cette question n'est pas connue. Il y a eu des avancées depuis 40 ans environ. Mais le problème inverse de Galois reste toujours ouvert...

Plus généralement, étant donné un corps k :

(**IGP**/k) : Tout groupe fini est-il groupe de Galois sur k?

Quels sont les groupes finis dont on sait qu'ils sont groupes de Galois sur $\mathbb{Q}$?

Un premier exemple pas très difficile est donné par la

Proposition

Tout groupe abélien fini est groupe de Galois sur $\mathbb{Q}$.

Un premier exemple pas très difficile est donné par la

Proposition

Tout groupe abélien fini est groupe de Galois sur $\mathbb{Q}$.

Preuve.

Deux ingrédients :

Un premier exemple pas très difficile est donné par la

Proposition

Tout groupe abélien fini est groupe de Galois sur $\mathbb{Q}$.

Preuve.

Deux ingrédients :
- tout groupe abélien fini est isomorphe à un produit direct de groupes cycliques,

Un premier exemple pas très difficile est donné par la

Proposition

Tout groupe abélien fini est groupe de Galois sur $\mathbb{Q}$.

Preuve.

Deux ingrédients :
- tout groupe abélien fini est isomorphe à un produit direct de groupes cycliques,
- une version faible du théorème de Dirichlet : pour tout $n \geq 2$, il existe une infinité de nombres premiers congrus à 1 modulo n. □

Un résultat beaucoup plus profond est donné par le

Theorem (Shafarevitch, 1954)

Tout groupe fini résoluble est groupe de Galois sur $\mathbb{Q}$.

Un résultat beaucoup plus profond est donné par le

Theorem (Shafarevitch, 1954)

Tout groupe fini résoluble est groupe de Galois sur $\mathbb{Q}$.

On peut combiner le théorème de Shafarevitch et le théorème de Feit-Thompson :

Theorem (Feit-Thompson, 1963)

Tout groupe d'ordre impair est résoluble.

Un résultat beaucoup plus profond est donné par le

Theorem (Shafarevitch, 1954)

Tout groupe fini résoluble est groupe de Galois sur $\mathbb{Q}$.

On peut combiner le théorème de Shafarevitch et le théorème de Feit-Thompson :

Theorem (Feit-Thompson, 1963)

Tout groupe d'ordre impair est résoluble.

pour obtenir le

Corollary

Tout groupe d'ordre impair est groupe de Galois sur $\mathbb{Q}$.

Après les groupes résolubles, on peut s'attaquer au cas des groupes simples non abéliens. Dans ce cas, la question est encore ouverte : on ne sait pas si tout groupe simple est groupe de Galois sur $\mathbb{Q}$.

Après les groupes résolubles, on peut s'attaquer au cas des groupes simples non abéliens. Dans ce cas, la question est encore ouverte : on ne sait pas si tout groupe simple est groupe de Galois sur $\mathbb{Q}$.

Un résultat très important des années 70 a été la classification des groupes simples. On y trouve
- les groupes alternés A_n ($n \geq 5$),
- des familles de groupes géométriques sur un corps fini ($\mathrm{PSL}_n(\mathbb{F}_q)$, $\mathrm{PSU}_n(\mathbb{F}_q)$...),
- 26 groupes, dits sporadiques.

Après les groupes résolubles, on peut s'attaquer au cas des groupes simples non abéliens. Dans ce cas, la question est encore ouverte : on ne sait pas si tout groupe simple est groupe de Galois sur $\mathbb{Q}$.

Un résultat très important des années 70 a été la classification des groupes simples. On y trouve
- les groupes alternés A_n ($n \geq 5$),
- des familles de groupes géométriques sur un corps fini ($\mathrm{PSL}_n(\mathbb{F}_q)$, $\mathrm{PSU}_n(\mathbb{F}_q)$...),
- 26 groupes, dits sporadiques.

Un "problème" est que le théorème de Shafarevitch ne s'étend pas aux groupes non résolubles. Cependant, on sait réaliser sur $\mathbb{Q}$ les groupes alternés, certains groupes géométriques et 25 des 26 groupes sporadiques.

La méthode consiste à d'abord montrer qu'un groupe donné est groupe de Galois sur $\mathbb{Q}(T)$, puis à spécialiser convenablement l'indéterminée T (*i.e.* "remplacer" T par $t \in \mathbb{Q}$). Cela repose sur le théorème d'irréductibilité de Hilbert :

La méthode consiste à d'abord montrer qu'un groupe donné est groupe de Galois sur $\mathbb{Q}(T)$, puis à spécialiser convenablement l'indéterminée T (*i.e.* "remplacer" T par $t \in \mathbb{Q}$). Cela repose sur le théorème d'irréductibilité de Hilbert :

Theorem (Hilbert)

Soit $P(T, X) \in \mathbb{Q}(T)[X]$ un polynôme irréductible sur $\mathbb{Q}(T)$ et de groupe de Galois G sur $\mathbb{Q}(T)$.
Alors il existe une infinité de nombres rationnels t tels que $P(t, X)$ $(\in \mathbb{Q}[X])$ soit irréductible sur $\mathbb{Q}$ et admette G comme groupe de Galois sur $\mathbb{Q}$.

Example

Prenons l'exemple $P(T, X) = X^2 - T$. Soit $t \in \mathbb{Q}$.

Example

Prenons l'exemple $P(T, X) = X^2 - T$. Soit $t \in \mathbb{Q}$.
(a) $t = 0$: $P(t, X) = X^2$ est réductible et inséparable sur $\mathbb{Q}$,

Example

Prenons l'exemple $P(T, X) = X^2 - T$. Soit $t \in \mathbb{Q}$.
(a) $t = 0$: $P(t, X) = X^2$ est réductible et inséparable sur $\mathbb{Q}$,
(b) $t = a^2$ pour un certain $a \in \mathbb{Q} \setminus \{0\}$ (par exemple $t = 1$) :
$P(t, X) = X^2 - a^2 = (X - a)(X + a)$ est réductible et séparable sur $\mathbb{Q}$.

Example

Prenons l'exemple $P(T, X) = X^2 - T$. Soit $t \in \mathbb{Q}$.
(a) $t = 0$: $P(t, X) = X^2$ est réductible et inséparable sur $\mathbb{Q}$,
(b) $t = a^2$ pour un certain $a \in \mathbb{Q} \setminus \{0\}$ (par exemple $t = 1$) :
$P(t, X) = X^2 - a^2 = (X - a)(X + a)$ est réductible et séparable sur $\mathbb{Q}$.
(c) t n'est pas un carré non-nul dans $\mathbb{Q}$ (par exemple $t = -1$) :
$P(t, X)$ est irréductible (et donc séparable) sur $\mathbb{Q}$.

Corollary

Tout groupe de Galois sur $\mathbb{Q}(T)$ est groupe de Galois sur $\mathbb{Q}$.

Corollary

Tout groupe de Galois sur $\mathbb{Q}(T)$ est groupe de Galois sur $\mathbb{Q}$.

Example

Par cette méthode, Hilbert a prouvé en 1892 que les groupes symétriques sont groupes de Galois sur $\mathbb{Q}$.

Corollary

Tout groupe de Galois sur $\mathbb{Q}(T)$ est groupe de Galois sur $\mathbb{Q}$.

Example

Par cette méthode, Hilbert a prouvé en 1892 que les groupes symétriques sont groupes de Galois sur $\mathbb{Q}$.

On voit donc qu'une réponse positive à (IGP/$\mathbb{Q}(T)$) impliquerait une réponse positive à (IGP)...

Mais la réponse à (IGP/$\mathbb{Q}(T)$) n'est pas connue...

Mais la réponse à (IGP/$\mathbb{Q}(T)$) n'est pas connue...

Elle l'est cependant si on remplace $\mathbb{Q}$ par $\mathbb{C}$:

Theorem (Théorème d'existence de Riemann)

Tout groupe fini est groupe de Galois sur $\mathbb{C}(T)$.

Theorem (Théorème d'existence de Riemann)

Tout groupe fini est groupe de Galois sur $\mathbb{C}(T)$.

Corollary

Tout groupe fini est groupe de Galois sur $\overline{\mathbb{Q}}(T)$.

Theorem (Théorème d'existence de Riemann)

Tout groupe fini est groupe de Galois sur $\mathbb{C}(T)$.

Corollary

Tout groupe fini est groupe de Galois sur $\overline{\mathbb{Q}}(T)$.

Comment utiliser ces résultats pour étudier (IGP/$\mathbb{Q}(T)$)?

Definition

Soient k un corps, $P(T,X) \in k(T)[X]$ un polynôme séparable sur $k(T)$ et E son corps de décomposition sur $k(T)$. On dit que $P(T,X)$ *est régulier sur* k si $E \cap \overline{k} = k$.

Definition

Soient k un corps, $P(T,X) \in k(T)[X]$ un polynôme séparable sur $k(T)$ et E son corps de décomposition sur $k(T)$. On dit que $P(T,X)$ *est régulier sur* k si $E \cap \overline{k} = k$.

Example

(1) $P(T,X) = X^2 - 2$ n'est pas régulier sur $\mathbb{Q}$ car $E = \mathbb{Q}(T)(\sqrt{2})$.

Definition

Soient k un corps, $P(T,X) \in k(T)[X]$ un polynôme séparable sur $k(T)$ et E son corps de décomposition sur $k(T)$. On dit que $P(T,X)$ *est régulier sur* k si $E \cap \overline{k} = k$.

Example

(1) $P(T,X) = X^2 - 2$ n'est pas régulier sur $\mathbb{Q}$ car $E = \mathbb{Q}(T)(\sqrt{2})$.
(2) $P(T,X) = X^2 - T$ est régulier sur $\mathbb{Q}$ car $E = \mathbb{Q}(T)(\sqrt{T})$.

Definition

Soient k un corps, $P(T,X) \in k(T)[X]$ un polynôme séparable sur $k(T)$ et E son corps de décomposition sur $k(T)$. On dit que $P(T,X)$ *est régulier sur* k si $E \cap \overline{k} = k$.

Example

(1) $P(T,X) = X^2 - 2$ n'est pas régulier sur $\mathbb{Q}$ car $E = \mathbb{Q}(T)(\sqrt{2})$.
(2) $P(T,X) = X^2 - T$ est régulier sur $\mathbb{Q}$ car $E = \mathbb{Q}(T)(\sqrt{T})$.
(3) $P(T,X) = X^3 - T$ n'est pas régulier sur $\mathbb{Q}$ car $e^{2i\pi/3} \in E$.

Soit G un groupe fini. D'après le théorème d'existence de Riemann, il existe un polynôme $P(T,X) \in \overline{\mathbb{Q}}(T)[X]$ tel que son groupe de Galois sur $\overline{\mathbb{Q}}(T)$ soit égal à G. Notons E le corps de décomposition de $P(T,X)$ sur $\overline{\mathbb{Q}}(T)$.

Soit G un groupe fini. D'après le théorème d'existence de Riemann, il existe un polynôme $P(T,X) \in \overline{\mathbb{Q}}(T)[X]$ tel que son groupe de Galois sur $\overline{\mathbb{Q}}(T)$ soit égal à G. Notons E le corps de décomposition de $P(T,X)$ sur $\overline{\mathbb{Q}}(T)$.

Supposons qu'il existe un polynôme $\tilde{P}(T,X) \in \mathbb{Q}(T)[X]$ régulier sur $\mathbb{Q}$ et satisfaisant la propriété suivante :
le corps de décomposition $\tilde{E}$ de $\tilde{P}(T,X)$ sur $\mathbb{Q}(T)$ vérifie $\tilde{E}\overline{\mathbb{Q}} = E$.

Comme $\tilde{P}(T,X)$ *est régulier sur* $\mathbb{Q}$, on a

$$\begin{aligned}\mathrm{Gal}(\tilde{P}(T,X)/\mathbb{Q}(T)) &= \mathrm{Gal}(\tilde{E}/\mathbb{Q}(T)) \\ &= \mathrm{Gal}(\tilde{E}\overline{\mathbb{Q}}/\overline{\mathbb{Q}}(T)) \\ &= \mathrm{Gal}(E/\overline{\mathbb{Q}}(T)) \\ &= \mathrm{Gal}(P(T,X)/\overline{\mathbb{Q}}(T)) \\ &= G\end{aligned}$$

En particulier, G est groupe de Galois sur $\mathbb{Q}(T)$.

Comme $\tilde{P}(T,X)$ *est régulier sur* $\mathbb{Q}$, on a

$$\begin{aligned}\mathrm{Gal}(\tilde{P}(T,X)/\mathbb{Q}(T)) &= \mathrm{Gal}(\tilde{E}/\mathbb{Q}(T)) \\ &= \mathrm{Gal}(\tilde{E}\overline{\mathbb{Q}}/\overline{\mathbb{Q}}(T)) \\ &= \mathrm{Gal}(E/\overline{\mathbb{Q}}(T)) \\ &= \mathrm{Gal}(P(T,X)/\overline{\mathbb{Q}}(T)) \\ &= G\end{aligned}$$

En particulier, G est groupe de Galois sur $\mathbb{Q}(T)$.

On dit que $E/\overline{\mathbb{Q}}(T)$ *est définie sur* $\mathbb{Q}$ *comme G-extension* et que $\tilde{E}/\mathbb{Q}(T)$ *est un* $\mathbb{Q}$*-modèle de* $E/\overline{\mathbb{Q}}(T)$ (comme G-extension).

Mais en général, on ne sait pas s'il existe un polynôme $\tilde{P}(T, X)$ comme précédemment...

Definition

Etant donné un corps k, on dit qu'*un groupe fini G peut être réalisé régulièrement sur $k(T)$* s'il est le groupe de Galois sur $k(T)$ d'un polynôme $P(T,X) \in k(T)[X]$ régulier sur k.

Regular Inverse Galois Problem

La forme régulière du problème inverse de Galois est la question suivante :

(**RIGP**) : Tout groupe fini peut-il être réalisé régulièrement sur $\mathbb{Q}(T)$?

Regular Inverse Galois Problem

La forme régulière du problème inverse de Galois est la question suivante :

(**RIGP**) : Tout groupe fini peut-il être réalisé régulièrement sur $\mathbb{Q}(T)$?

Plus généralement, étant donné un corps k :

(**RIGP**/k) : Tout groupe fini peut-il être réalisé régulièrement sur $k(T)$?

(1) D'après le théorème d'irréductiblité de Hilbert, on a

$$(\mathrm{RIGP}) \Longrightarrow (\mathrm{IGP}/\mathbb{Q}(T)) \Longrightarrow (\mathrm{IGP})$$

(1) D'après le théorème d'irréductiblité de Hilbert, on a

$$(\mathrm{RIGP}) \Longrightarrow (\mathrm{IGP}/\mathbb{Q}(T)) \Longrightarrow (\mathrm{IGP})$$

(2) Si k est un corps contenant $\mathbb{Q}$ (resp. $\mathbb{F}_p$), alors (RIGP) (resp. (RIGP/$\mathbb{F}_p$)) $\Longrightarrow$ (RIGP/k).

(1) D'après le théorème d'irréductiblité de Hilbert, on a

$$(\mathrm{RIGP}) \Longrightarrow (\mathrm{IGP}/\mathbb{Q}(T)) \Longrightarrow (\mathrm{IGP})$$

(2) Si k est un corps contenant $\mathbb{Q}$ (resp. $\mathbb{F}_p$), alors (RIGP) (resp. (RIGP/$\mathbb{F}_p$)) $\Longrightarrow$ (RIGP/k).

(3) On ne connaît pas de corps k tels que la réponse à (RIGP/k) soit négative.

(1) D'après le théorème d'irréductiblité de Hilbert, on a

$$(\mathrm{RIGP}) \Longrightarrow (\mathrm{IGP}/\mathbb{Q}(T)) \Longrightarrow (\mathrm{IGP})$$

(2) Si k est un corps contenant $\mathbb{Q}$ (resp. $\mathbb{F}_p$), alors (RIGP) (resp. (RIGP/$\mathbb{F}_p$)) $\Longrightarrow$ (RIGP/k).

(3) On ne connaît pas de corps k tels que la réponse à (RIGP/k) soit négative.

(4) Les extensions de $\mathbb{Q}(T)$ définies par les corps de décomposition sur $\mathbb{Q}(T)$ des polynômes réguliers sur $\mathbb{Q}$ correspondent aux revêtements galoisiens $f : X \to \mathbb{P}^1$ définis sur $\mathbb{Q}$. Ainsi l'énoncé (RIGP) consiste à étudier l'action de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur les revêtements de $\mathbb{P}^1$.

D'après le théorème d'existence de Riemann, la réponse à (RIGP/$\overline{\mathbb{Q}}$) est positive. Le principal problème consiste à descendre de $\overline{\mathbb{Q}}$ à $\mathbb{Q}$.

D'après le théorème d'existence de Riemann, la réponse à (RIGP/$\overline{\mathbb{Q}}$) est positive. Le principal problème consiste à descendre de $\overline{\mathbb{Q}}$ à $\mathbb{Q}$.
Si l'on se donne une extension finie galoisienne $E/\overline{\mathbb{Q}}(T)$, la difficulté est de contrôler l'action de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur $E/\overline{\mathbb{Q}}(T)$.

D'après le théorème d'existence de Riemann, la réponse à (RIGP/$\overline{\mathbb{Q}}$) est positive. Le principal problème consiste à descendre de $\overline{\mathbb{Q}}$ à $\mathbb{Q}$.
Si l'on se donne une extension finie galoisienne $E/\overline{\mathbb{Q}}(T)$, la difficulté est de contrôler l'action de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur $E/\overline{\mathbb{Q}}(T)$.
On a cependant un bon contrôle sur les invariants de l'extension $E/\overline{\mathbb{Q}}(T)$:
- son degré,
- son groupe de Galois,
- ses points de branchement,
- son invariant canonique de l'inertie.

D'après le théorème d'existence de Riemann, la réponse à (RIGP/$\overline{\mathbb{Q}}$) est positive. Le principal problème consiste à descendre de $\overline{\mathbb{Q}}$ à $\mathbb{Q}$.
Si l'on se donne une extension finie galoisienne $E/\overline{\mathbb{Q}}(T)$, la difficulté est de contrôler l'action de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur $E/\overline{\mathbb{Q}}(T)$.
On a cependant un bon contrôle sur les invariants de l'extension $E/\overline{\mathbb{Q}}(T)$:
- son degré,
- son groupe de Galois,
- ses points de branchement,
- son invariant canonique de l'inertie.

Pour que $E/\overline{\mathbb{Q}}(T)$ soit définie sur $\mathbb{Q}$ (comme G-extension), il est nécessaire que l'action sur les invariants soit triviale. Mais la réciproque n'est pas vraie en général...

En gros, il y a deux méthodes pour essayer de résoudre ce problème :

En gros, il y a deux méthodes pour essayer de résoudre ce problème :

- (théorie des groupes) On fixe un groupe fini et on essaie de le réaliser régulièrement sur $\mathbb{Q}(T)$.

En gros, il y a deux méthodes pour essayer de résoudre ce problème :

- (théorie des groupes) On fixe un groupe fini et on essaie de le réaliser régulièrement sur $\mathbb{Q}(T)$.

- (géométrie arithmétique) On fixe une extension algébrique $k/\mathbb{Q}$ et on essaie de réaliser régulièrement tous les groupes finis sur $k(T)$.

Sous certaines conditions supplémentaires, les conditions nécessaires précédentes sur les invariants permettent d'affirmer qu'une extension finie galoisienne de $\overline{\mathbb{Q}}(T)$ est définie sur $\mathbb{Q}$.

Sous certaines conditions supplémentaires, les conditions nécessaires précédentes sur les invariants permettent d'affirmer qu'une extension finie galoisienne de $\overline{\mathbb{Q}}(T)$ est définie sur $\mathbb{Q}$.
Ces conditions supplémentaires s'appellent *conditions de rigidité*.
Ce sont des conditions de théorie des groupes portant sur le groupe G que l'on souhaite réaliser. Ces conditions ont permis de réaliser sur $\mathbb{Q}$ certains groupes simples :

Sous certaines conditions supplémentaires, les conditions nécessaires précédentes sur les invariants permettent d'affirmer qu'une extension finie galoisienne de $\overline{\mathbb{Q}}(T)$ est définie sur $\mathbb{Q}$.
Ces conditions supplémentaires s'appellent *conditions de rigidité*.
Ce sont des conditions de théorie des groupes portant sur le groupe G que l'on souhaite réaliser. Ces conditions ont permis de réaliser sur $\mathbb{Q}$ certains groupes simples :

Example (Thompson)

Le groupe Monstre (d'ordre $2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$) peut être réalisé régulièrement sur $\mathbb{Q}(T)$ et est donc groupe de Galois sur $\mathbb{Q}$.

Le théorème suivant donne tous les corps k pour lesquels on sait que la réponse à (RIGP/k) est positive :

Theorem (Pop, 1996)

Pour tout corps ample k, la réponse à (RIGP/k) est oui.

Le théorème suivant donne tous les corps k pour lesquels on sait que la réponse à (RIGP/k) est positive :

Theorem (Pop, 1996)

Pour tout corps ample k, la réponse à (RIGP/k) est oui.

Remarque

(1) Ce théorème englobe les cas particuliers $k = \mathbb{C}$ (Riemann), $k = \mathbb{R}$ (Hurwitz, 1890) et d'autres cas établis par Harbater, Fried, Völklein, Pop, Dèbes dans les années 80-90.

Le théorème suivant donne tous les corps k pour lesquels on sait que la réponse à (RIGP/k) est positive :

Theorem (Pop, 1996)

Pour tout corps ample k, la réponse à (RIGP/k) est oui.

Remarque

(1) Ce théorème englobe les cas particuliers $k = \mathbb{C}$ (Riemann), $k = \mathbb{R}$ (Hurwitz, 1890) et d'autres cas établis par Harbater, Fried, Völklein, Pop, Dèbes dans les années 80-90.

(2) On ne connaît pas de corps non amples k tels que la réponse à (RIGP/k) soit positive.

Definition

Un corps k est dit *ample* si, pour tout polynôme $P(T, X) \in k(T)[X]$ irréductible sur $\overline{k}(T)$, l'ensemble $\{(t, x) \in k^2 \,/\, P(t, x) = 0\}$ est vide ou infini.

Definition

Un corps k est dit *ample* si, pour tout polynôme $P(T,X) \in k(T)[X]$ irréductible sur $\overline{k}(T)$, l'ensemble $\{(t,x) \in k^2 \,/\, P(t,x) = 0\}$ est vide ou infini.

Example

(1) Les corps algébriquement clos sont amples.

Definition

Un corps k est dit *ample* si, pour tout polynôme $P(T,X) \in k(T)[X]$ irréductible sur $\overline{k}(T)$, l'ensemble $\{(t,x) \in k^2 \,/\, P(t,x) = 0\}$ est vide ou infini.

Example

(1) Les corps algébriquement clos sont amples.

(2) Les corps valués complets sont amples : $\mathbb{Q}_p$, $\mathbb{R}$, $k((T))$...

Definition

Un corps k est dit *ample* si, pour tout polynôme $P(T,X) \in k(T)[X]$ irréductible sur $\overline{k}(T)$, l'ensemble $\{(t,x) \in k^2 \,/\, P(t,x) = 0\}$ est vide ou infini.

Example

(1) Les corps algébriquement clos sont amples.

(2) Les corps valués complets sont amples : $\mathbb{Q}_p$, $\mathbb{R}$, $k((T))$...

(3) Le corps $\mathbb{Q}^{\mathrm{tr}}$ des nombres algébriques sur $\mathbb{Q}$ totalement réels est ample.

Definition

Un corps k est dit *ample* si, pour tout polynôme $P(T,X) \in k(T)[X]$ irréductible sur $\overline{k}(T)$, l'ensemble $\{(t,x) \in k^2 \,/\, P(t,x) = 0\}$ est vide ou infini.

Example

(1) Les corps algébriquement clos sont amples.

(2) Les corps valués complets sont amples : $\mathbb{Q}_p$, $\mathbb{R}$, $k((T))$...

(3) Le corps $\mathbb{Q}^{\mathrm{tr}}$ des nombres algébriques sur $\mathbb{Q}$ totalement réels est ample.

(4) $\mathbb{Q}$ n'est pas ample.

Bibliographie

- Lior Bary-Soroker et Arno Fehm, *Open problems in the theory of ample fields*.

- Pierre Dèbes, *Arithmétique des revêtements de la droite*.

- Pierre Dèbes, *Autour du problème inverse de Galois*.

- Pierre Dèbes, *Théorie de Galois et géométrie : une introduction*.

- Pierre Dèbes et Bruno Deschamps, *The Regular Inverse Galois Problem over large fields*.