Algèbre II - 2019/2020

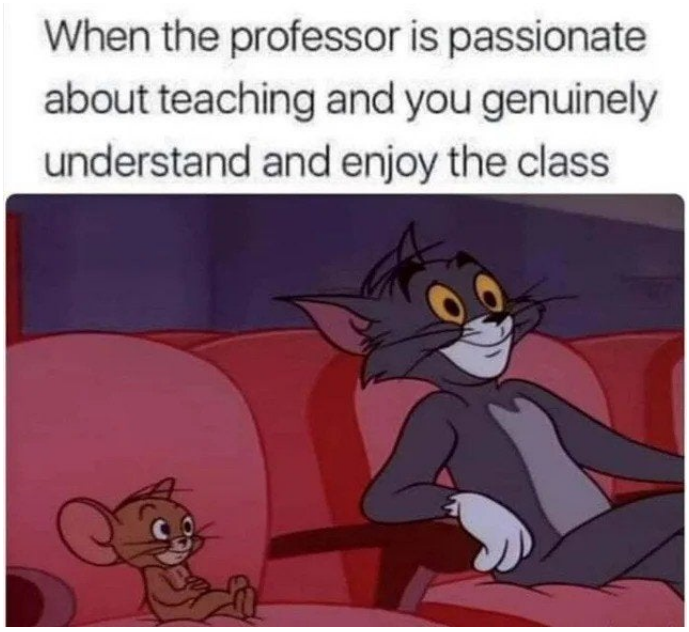
Anders Karlsson

Evariste Galois

Quick Message

Hello hello, je tiens à noter que ce PDF ne représente pas le cours du professeur A. Karlsson officiellement. En particulier, je reformule et remanie souvent le matériel en plus d'y ajouter des fautes d'orthographe. Ne vous étonnez pas de trouver des passages un peu douteux ou des petites blagues par ci par là, il faut bien se détendre un peu pendant la prise de note non ?

J'espère que mes notes serviront de supplément au matériel fourni en cours et pourront aider quelques étudiants. N'oubliez pas, ce PDF ne peut pas répondre à vos questions aussi bien que Mr. Karlsson le ferait en live. Suivez son cours, posez lui plein de questions intéréssantes, amour et bonheur <3



Contents

0 Catégories (≈ 1940s) **1**

1 Groupes **3**
1.1 Monoïdes . . . 3
1.2 Groupes . . . 4
Proposition 1 . . . 5
Théorème (Ore 1951), *pour le fun (pas dans l'exa):* . . . 5
1.3 Groupes résolubles . . . 6
Théorème (Feit-Thompson 1963) . . . 6
Proposition 2 . . . 6
Théorème (Jordan-Holder) . . . 7
1.4 Actions de groupes . . . 8
Proposition 3 . . . 8
Corollaire (Formule d'orbite) . . . 9
Application: Conjugaison . . . 10
Corollaire: La formule des classes . . . 10
1.5 p-groupe . . . 11
Théorème: Cauchy . . . 11
1.6 Sous-groupes de Sylow . . . 13
Théorème: 1er théorème de Sylow . . . 14
Théorème: 2ème théorème de Sylow . . . 14
1.7 Le produit semi-direct . . . 16
1.8 Graphe de Cayley . . . 18
1.9 Groupes libres . . . 19
Rappel: Le monoïde libre (langage) . . . 19
1.10 Présentation d'un groupe . . . 21

2 Théorie de représentation de groupes **23**
2.1 Définitions . . . 23
Exemple important . . . 24
Une construction générale - représentation de permutations . . . 24
2.2 Décomposition . . . 28
Rappel: Le produit scalaire (hermitien) . . . 28
2.3 Lemme de Schur . . . 30
2.4 Caractères . . . 32
2.5 Fonctions centrales . . . 37
2.6 Un exemple "facile" . . . 39

3 Anneaux **40**
3.1 Définitions et exemples . . . 40
3.2 Diviseur de zéro . . . 42
3.3 Anneaux finis . . . 44
Théorème: Wedderburn 1905 . . . 45
3.4 Corps finis . . . 47
3.5 L'analogie entre entiers et polynômes . . . 48
Intro . . . 48
ABC pour polynômes . . . 48
Théorème: Stothers 1981, Mascon 1983 (ABC pour polynômes) . . . 48
Corollaire: Théorème de Fermat pour polynômes, 19ème siècle . . . 48
ABC pour des entiers ?! . . . 50
3.6 Polynômes irréductibles . . . 52
1er Lemme de Gauss . . . 52
2ème Lemme de Gauss . . . 53

Proposition: Critère d'Eisenstein . . . 53
Proposition: Critère de réduction . . . 54
3.7 Polynômes symétriques . . . 55
Définition: Le discriminant . . . 55
Exemple important: Polynômes symétriques élémentaires . . . 55
Théorème fondamental des polynômes symétriques . . . 55

4 Quelques notions algébrique importantes 57
4.1 Algèbre . . . 57
Théorème structure de M type fini, R anneau principal . . . 57
4.2 Le produit tensoriel . . . 58
Définition: Le produit tensoriel . . . 58
4.3 Produit extérieur . . . 59

5 Corps et théorie de Galois 60
5.1 Nombres et équations polynomiales . . . 61
5.2 Géométrie greque classique . . . 62
5.3 Extensions de corps . . . 63
Théorème: Clôture Algébrique . . . 66
5.4 Extension algébriques . . . 67

6 Galois: Application à la géométrie classique 69
6.1 Algébrification . . . 69
6.2 Critère de constructibilité . . . 71
6.3 Application à l'impossibilité de certaines constructions . . . 73
Théorème: Wantzel (1837) . . . 73
Théorème: Quadrature du cercle . . . 75

7 Théorie de Galois: Plongements 79
7.1 Morphismes de corps . . . 79
7.2 Extensions de plongements . . . 81
Proposition: Extension de plongements . . . 81

8 Préparations pour les théorèmes de Galois 83
8.1 Séparabilité . . . 83
8.2 Théorème d'élément primitif . . . 85
Théorème: [Abel/Galois] Élément primitif . . . 85

9 Théorème de Galois 86
9.1 Introduction . . . 86
9.2 Rappel de notions et faits établis . . . 86
Théorème des éléments primitifs . . . 86
9.3 Corps de décomposition . . . 87
Proposition 1 . . . 87
Lemme 1 . . . 87
Proposition 2 . . . 88
9.4 Application: Corps finis . . . 89
9.5 Extensions normales . . . 90
Proposition 1 . . . 90
Proposition 2 . . . 90
9.6 La correspondence de Galois . . . 92
Proposition 3 . . . 92
Théorème: Galois, partie 1 . . . 92
Théorème: Galois, partie 2 . . . 94
9.7 Rappel sur les groupes résolubles . . . 98

9.8 Solutions par radicaux 99
9.9 Un exemple 101

0 Catégories ($\approx$ 1940s)

(Ce chapitre n'es pas strictement inclus dans l'examen)

Voyons grossièrement ce que peuvent être les structures mathématiques:

Définition:

Une catégorie ξ est:

- Une classe ξ d'objects $A, B, C, \ldots$
- Avec ses morphismes $f : A \to B$ dénotés $\mathrm{Mor}(A, B)$

Le plus souvent, les morphismes sont des applications entre ensembles munis de cetaines structures (= objects). Ces applications doivent préserver les structures.

Exemples:

1. $\xi =$ { Groupes }, donc la classe où les groupes sont les objects.
   $\mathrm{Mor}(G, H) =$ tout homomorphisme (de groupe) $f : G \to H$
2. Même chose pour les anneaux, corps...
3. $\xi =$ { Espaces Vectoriels }, avec comme morphismes les applications linéaires.
4. $\xi =$ { Espaces Topologiques }, avec comme morphismes les applications continues.
5. $\xi =$ { Domaines de $\mathbb{C}$ }, nous verrons que les morphismes sont ici les fonctions holomorphes.

Définition:

Un isomorphisme $f : A \to B$ est un morphisme tel qu'il existe un morphisme $g : B \to A$ tel que $f \circ g = id_B$ et $g \circ f = id_A$

Exemple

$\xi =$ { ensembles }, les morphismes sont les applications et les isomorphismes sont les bijections.

Remarque

Les isomorphismes dans chaques catégorie sont toujours comme ça (bijections), mais dans des situations données il est possible que certaines conditions soient automatiques, et donc obligatoirement vérifiée.

Exemple

1. $\xi =$ { Espaces Vectoriels de dimension finie sur $\mathbb{R}$ }, les morphismes sont les applications linéaires $\varphi : E \to F$
   Les isomorphismes sont donc les fonctions φ bijectives et linéaires. Mais φ^{-1} est automatiquement linéaire.
2. C'est la même chose dans la théorie des groupes, si un homomorphisme admet un inverse au niveau des ensembles, cet inverse est automatiquement un homomorphisme (c.f. Algèbre I).
3. $\xi =$ { Espaces Topologiques }, les isomorphismes sont les "Homeomorphismes" (c.f. Topologie Générale), il faudrait ici encore vérifier que l'inverse est bien continue.

Notations:

- ⋆ Les morphismes $f : A \to A$ s'appellent des endomorphismes.
- ⋆ Les isomorphismes $f : A \to A$ s'appellent des automorphismes.
- ⋆ Un foncteur est un morphisme entre catégories (à voir en Algèbre et Géométrie III)
  { Espaces Topologiques } $\mapsto$ { Groupes } qui prend un element topologique "flou" et l'envoie sur un élément de la théorie des groupes qui lui, est précis algébriquement.
  Donc la "théorie des catégories" est utile pour plusieurs raisons:
  - Rendre le langage et les structures plus clairs, et faire en sorte qu'il y aie moins de choses à retenir.
  - Cette idée de considerer non pas seulement les objets mais principalement les applications est l'idée principale des math du 20ème siecle.

1 Groupes

C'est un language pour les symétries, donc ce n'est pas juste un chapitre d'algèbre, en effet chaque structure mathématique possède son groupe de symétrie (d'automorphismes).

1.1 Monoïdes

Définitions:

1. Un monoïde $(G, \cdot)$ est un ensemble G muni d'une opération (loi de composition) $\cdot : G \times G \to G$ qui se doit d'être associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, et G doit posséder un élément neutre pour cette opération. On le note $e \in G$ et $e \cdot a = a \cdot e = a \quad \forall a \in G$

2. Un morphisme de monoïde est une application $\phi : G_1 \to G_2$ telle que:

$$\phi(a \cdot b) = \phi(a) \star \phi(b) \quad \text{et} \quad \phi(e_{G_1}) = e_{G_2}$$

où $(G_1, \cdot)$ et $(G_2, \star)$ sont des monoïdes.

Remarque

Si on n'impose pas l'existence de l'element neutre, on parle d'un demi-groupe (ou semi-groupe)

Exemples

a) $\mathbb{N} \setminus \{0\} = \{1, 2, 3, \dots\}$ muni de l'opération $+$ est un demi groupe.

b) $\mathbb{Z}_{\geq 0} = \{0, 1, 2, \dots\}$ muni de l'addition est un monoïde (et donc un demi-groupe aussi).

c) $(\mathbb{Z}, +)$ est même un groupe car il possède les inverses.

d) $(\mathbb{N}, \cdot)$ est un monoïde avec $e = 1$, mais ce n'est pas un groupe car il manque evidemment les inverses.

Un autre exemple:

Les languages ou codes, Alphabet $= \{a, b, c, \dots z\}$, on pourrait choisir un autre alphabet comme $\{a, b, c\}$ ou encore $\{0, 1\}$.

$G = \{$ mots $\}$ est un monoïde pour l'opération de concatenation $g \cdot h =$ "gh" donc: $abd \cdot ddb = abdddb$. L'opération est trivialement associative et nous pouvons définir l'element neutre e comme étant le "mot vide".

Encore un autre exemple:

En prenant $G = \{0, 1\}$, on peut se placer dans le contexte de la logique avec les opération AND=$\wedge$ et OR=$\vee$ ce qui défini deux monoïdes, $(G, \vee)$ et $(G, \wedge)$

Dans le cas du AND, l'élément neutre est 1, et pour le OR c'est 0 (voir tables de vérité pour les opérations c.f. Logique)

1.2 Groupes

Définition

Un Groupe $(G, \cdot)$ est un ensemble G non-vide muni d'une opération $\cdot : \begin{array}{ccc} G \times G & \longrightarrow & G \\ (g,h) & \longmapsto & g \cdot h \end{array}$ tel que:

1. Associativité: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
2. Element neutre: $\exists e \in G$ tel que $e \cdot g = g \cdot e = g \quad \forall g \in G$
3. Inverse: $\forall g \in G,\ \exists g^{-1} \in G$ tel que $g \cdot g^{-1} = g^{-1} g = e$

Remarques

- Autrement dit, un groupe est un monoïde qui possède des inverses.
- Il est facile de montrer que l'élément neutre et les inverses sont uniques dans un groupe.

Définition

Un homomorphisme (de groupes) est une application $\phi : G \to H$ telle que:

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$$

Il découle de cette définition que:

$$\phi(e_G) = e_H \quad \text{et aussi} \quad \phi(g^{-1}) = \phi(g)^{-1}$$

Exemple

Soit X un ensemble. Alors $(\mathrm{Aut}(X), \circ)$ est un groupe pour la composition de fonction (c.f. Algèbre I).
Nous pouvons dériver de là, pour $X = \{1, 2, 3, \ldots, n\}$, le groupe des symétries:

$$\mathrm{Aut}(X) = \text{ Permutations de } n = S_n$$

Ce qui nous amène à montrer que $|S_n| = n!$

Définitions

- Groupes Abéliens
  On dit qu'un groupe G est abélien (ou commutatif) si $gh = hg \quad \forall h, g \in G$

- Groupes Simples
  Un groupe G est simple si il ne possède pas de sous-groupes normaux non triviaux (e ou G). On peut faire une analogie entre ces groupes et les nombres premiers, ils forment une sorte de base aux autres groupes.

- Sous-groupe engendré par A
  Soit $A \subset G$ un sous-ensemble d'un groupe G, on défini:

  $$< A > \ := \bigcap_{K \supset A} K$$

  comme étant le sous-groupe engendré par A.
  Intuitivement, chaque élément de $< A >$ peut être obtenu en combinant les éléments de A et leur inverse.

Exemple

Pour $[a,b] := aba^{-1}b^{-1}$ un commutateur où $a \in A, b \in B$, on peut définir $[A,B] :=<$ tout les commutateurs $>$ comme étant le sous groupe engendré par tout les commutateurs. Plus formellement:

$$[A,B] :=< \{[a,b] \mid a \in A,\ b \in B\} >$$

Remarque

En général, un produit de deux commutateurs n'est pas un commutateur.

Proposition 1

Si A et B sont normaux dans G alors $[A,B]$ est aussi un sous-groupe normal.

Preuve:
Soit $g \in G$, il suffit de vérifier que pour un commutateur, $g[a,b]g^{-1} \in [A,B]$

- $[a,b]^{-1} = [b,a]$ (facile par calcul)
- $g \cdot s_1 \cdot s_2 \cdot \cdots \cdot s_n \cdot g^{-1} = g \cdot s_1 \cdot g^{-1} \cdot g \cdot s_2 \cdot \cdots \cdot g \cdot s_n \cdot g^{-1}$

Cela nous donne directement que le conjugé d'un commutateur est le commutateur des conjugés:

$$g[a,b]g^{-1} = [gag^{-1}, gbg^{-1}] \in [A,B] \quad \text{car } A \text{ et } B \text{ normaux dans } G$$

□

Remarque

$G/_{[G,G]}$ est abélien.

Définition

Un groupe G est parfait si $[G,G] = G$

Exemple

Un groupe G simple et non-abélien est parfait.

⌜

$[G,G]$ est normal dans G, par simplicité de G, $[G,G] = G \implies G$ est parfait.
Note: $[G,G] \neq \{e\}$ car G est non-abélien.

⌟

Théorème (Ore 1951), *pour le fun (pas dans l'exa):*

Tout élément de A_n, $n \geq 5$ est lui même un commutateur.

Conjecture de Ore

Il conjectura que la même chose devait être vraie pour tout groupe simple et non-abélien.
Cela fut démontré en 2008 mais la preuve passe par la classification des groupes simples. C'est donc malheureusement une preuve par énumération et non "directe".

1.3 Groupes résolubles

Ce chapitre est important pour la théorie de Galois qu'on abordera en printemps.
On montrera qu'une équation est résoluble $\iff$ son groupe de Galois est résoluble.

Définition

Un groupe G est résoluble s'il existe une suite de sous-groupes $G = H_0 \supset H_1 \supset H_2 \supset \cdots \supset H_n = \{e\}$ telle que:

1. $H_i \triangleleft H_{i-1} \quad \forall i$ (H_i est normal dans H_{i-1})
2. H_{i-1}/H_i est abélien.

Remarque

Un groupe abélien est trivialement résoluble.

Non-exemple

Soit G un groupe simple et non-abélien, il ne peut pas être résoluble, en effet:
$G = H_0$, $H_1 \triangleleft G \implies H_1 = G$ ou $H_1 = \{e\}$ mais G est non-abélien, donc $H_1 \neq \{e\}$ et donc $H_1 = G$. Il ne peut donc pas exister de suite de sous-groupes allant vers $\{e\}$.

Donc les groupes résolubles sont une sorte "d'extension" aux groupes abéliens, et une sorte "d'opposé" aux groupes simples.

Le groupe des Symétries S_n

Nous avons vu pendant le cours d'Algèbre I que S_n n'était pas résoluble pour $n \geq 5$ mais l'était pour $n = 1, 2, 3, 4$.

Théorème (Feit-Thompson 1963)

Soit G un groupe fini, avec $|G|$ = impair. Alors G est résoluble.

La démonstration ne fait pas partie du cours, ce théorème se démontre sur plus de 200 pages.

Idée de suite

Proposons une suite de sous-groupe qui pourrait mener à $\{e\}$:
Pour G un groupe, définissons de manière récursive: $G^{(0)} = G$, $G^{(n+1)} = [G^{(n)}, G^{(n)}]$, on obtient ainsi:

$$G = G^{(0)} \triangleright G^{(1)} \triangleright G^{(2)} \triangleright \cdots$$

Proposition 2

G est résoluble si et seulement si il existe n tel que $G^{(n)} = \{e\}$

Définition

Définissons une autre suite: $\begin{cases} G_0 = G \\ G_{n+1} = [G, G_n] \quad n > 0 \end{cases}$
C'est aussi une suite de sous-groupes normaux par Proposition 1.

Définition

On dit que G est nilpotent si $G_n = \{e\}$ pour un certain n.

Exemples

1. G abélien $\implies G_1 = [G,G] = \{e\} \implies G$ nilpotent.
2. Nilpotent $\implies$ résoluble parce que $G_n \supset G^{(n)}$ car $[G,H] \supset [H,H]$

Définition

Une suite de sous-groupe $H_i < G$ est : $G = H_0 > H_1 > \cdots > H_n = \{e\}$ avec $H_{i+1} \triangleleft H_i \quad \forall i$

Définition

Une suite de sous-groupe est de Jordan-Hölder (ou suite de composition) si tout $H_i \big/ H_{i+1}$ sont simples.

Théorème (Jordan-Holder)

Soit G un groupe fini. Alors il existe une suite de Jordan Hölder et chaque telle suite a la même longeur et les même quotients $\left\{ H_i \big/ H_{i+1} \right\}$.
Note: L'ordre n'est pas unique.

Remarques

1. C'est dans ce sens que les goupes simples sont les "premiers", les "atomes" pour les groupes finis.

2. Cela généralise le théorème fondamental de l'arithmétique:

   Prenons le groupe cyclique d'ordre 12, C_{12}:

$$C_{12} \triangleright C_6 \triangleright C_3 \triangleright 1 \quad \rightsquigarrow \quad C_{12}\big/C_6 = C_2,\ C_6\big/C_3 = C_2,\ C_3\big/1 = C_3 \quad \rightsquigarrow \quad 2\cdot 2\cdot 3 = 12$$
$$C_{12} \triangleright C_4 \triangleright C_2 \triangleright 1 \quad \rightsquigarrow \quad C_{12}\big/C_4 = C_3,\ C_4\big/C_2 = C_2,\ C_2\big/1 = C_2 \quad \rightsquigarrow \quad 3\cdot 2\cdot 2 = 12$$
$$C_{12} \triangleright C_6 \triangleright C_2 \triangleright 1 \quad \rightsquigarrow \quad C_{12}\big/C_6 = C_2,\ C_6\big/C_2 = C_3,\ C_2\big/1 = C_2 \quad \rightsquigarrow \quad 2\cdot 3\cdot 2 = 12$$

1.4 Actions de groupes

Définition

Une action d'un groupe H sur un ensemble X est un homomorphisme $\phi : H \to \mathrm{Aut}(X)$.

Cela donne une application : $\begin{array}{ccc} H \times X & \longrightarrow & X \\ (h,x) & \longmapsto & \phi(h)\cdot x =: hx \end{array}$

Exemples

1. H un groupe de $n \times n$ matrices à coefficients dans $\mathbb{R}$. $X = \mathbb{R}^n$, $A \in H, v \in X \implies Av = v' \in X$

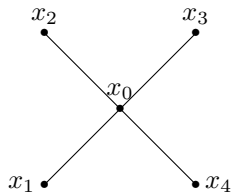
Définition

Une orbite de x sous H est l'ensemble $Hx = \{hx \mid h \in H\} \subset X$

2. $H < G$ un sous-groupe, H agit sur $X := G$ par $(h,g) \mapsto hg$
   Les orbites coïncident avec les classes à droite car les orbites sont $Hg \quad g \in G$.

3. G agit sur lui même par : $\begin{array}{ccc} G & \longrightarrow & \mathrm{Aut}(G) \\ g & \longmapsto & \phi(g) \end{array}$ définie par $\phi(g)h = ghg^{-1} \quad h \in G$ qui est donc la conjugaison.
   Les orbites sont donc les classes de conjugaisons: $C_G(x) =$ tout élément de G conjugé à x.

4. $H = C_4$, le groupe cyclique d'ordre 4. Rappel: $C_4 \cong \left({}^{\mathbb{Z}}\!/_{4\mathbb{Z}} \ , + \right)$. Si $C_4 = \{e, a, a^2, a^3\}$, où a est une rotation de 90°. Ce groupe agit sur X défini par:



   Avec les deux orbites: $\{x_0\}$ et $\{x_1, x_2, x_3, x_4\}$

Proposition 3

L'action de H sur X défini une relation d'équivalence sur X:

$$x \sim y \iff \exists h \quad \text{tel que} \quad hx = y$$

Démonstration:
Il suffit de vérifier les axiomes d'une relation d'équivalence:

i) $x \sim x$, ok car $1x = x$

ii) $x \sim y \implies y \sim x$, car si $hx = y$, alors $x = h^{-1}y$

iii) $x \sim y,\ y \sim z \implies x \sim z$, en effet, $hx = y,\ h_2 y = z \implies h_2 h x = z$

□

Corollaire

X est une union disjointes des orbites. $X = \bigsqcup_{x_i} Hx_i$

Exemple

Cela à déjà été vu/étudié pour les classes à droites/gauches.

Définition

Le stabilisateur de x (ou groupe d'isotropie de x) est le sous-groupe:

$$H_x := \{h \in H \mid hx = x\} \subset H$$

H_x est bien un sous-groupe de H:

i) $e \cdot x = x \implies e \in H_x$

ii) Si $h_1, h_2 \in H_x$ alors $h_1 h_2 x = h_1 x = x \implies h_1 h_2 \in H_x$

iii) $hx = x \implies h^{-1}hx = h^{-1}x \implies h^{-1}x = x \implies h^{-1} \in H$

Exemple

Prenons C_4 avec l'exemple vu précédemment. $Hx_0 = \{x_0\}$, $Hx_1 = \{x_1, x_2, x_3, x_4\}$, alors $X = Hx_0 \sqcup Hx_1$ et $H_{x_0} = H$, $H_{x_1} = \{e\}$

Proposition

Soit H un groupe fini qui agit sur X un ensemble fini. Alors $\forall x \in X$ on a:

$$|H_x| \cdot |Hx| = |H|$$

Démonstration:

Affirmation: la fonction $\overline{f}$: $\begin{array}{ccc} {}^{H}\!/_{H_x} & \longrightarrow & Hx \\ gH_x & \longmapsto & gx \end{array}$ est une bijection.

Vérifions d'abord que $\overline{f}$ est bien définie: si $g' \in gH_x$, alors $g' = gh$ et donc $g'x = ghx = gx$.
Montrons ensuite que c'est bien une bijection:
La surjectivité est claire, $g \in H \implies \{gx\} = Hx$

Pour l'injectivité, supposons que $gx = hx \iff h^{-1}gx = x \iff h^{-1}g \in H_x \iff hH_x = hh^{-1}gH_x = hH_x$

□

Corollaire (Formule d'orbite)

$$|X| = \sum_{\text{orbites}} {}^{|H|}\!/_{|H_x|}$$

On note: ${}^{|H|}\!/_{|H_x|} =: [H : H_x]$ l'index.

Démonstration:

$$X = \bigsqcup_i Hx_i \quad \text{donc:} \quad |X| = \sum_i |Hx_i| = \sum_i {}^{|H|}\!/_{|H_{x_i}|}$$

□

Application: Conjugaison

C'est un cas particulier important:$C : \begin{array}{ccc} G & \longrightarrow & \mathrm{Aut}(G) \\ g & \longmapsto & C_g(\cdot) \end{array}$ où $C_g(h) = ghg^{-1}$ $\forall h \in G$, c'est un homomorphisme avec comme spécifitités:
Orbite $\rightarrow \{gxg^{-1} \mid g \in G\} = \mathrm{Cl}_G(x)$ la classe de conjugaison de x.
Stabilisateur $\rightarrow \{g \in G \mid gxg^{-1} = x \implies gx = xg\} = C_G(x)$ le centralisateur de x.

Le centre $Z(G)$ de G est le sous-groupe (abélien)

$$\big\{h \mid \forall g \in G \quad gh = hg\big\} = \big\{x \mid C_G(x) = G\big\} = \big\{x \mid \mathrm{Cl}_G(x) = \{x\}\big\}$$

Il est facile de montrer que c'est un sous-groupe.

Corollaire: La formule des classes

$$|G| = |Z(G)| + \sum_{i=1}^{m} |\mathrm{Cl}_G(x_i)|$$

où $|\mathrm{Cl}_G(x_i)| \geq 2$ et $|\mathrm{Cl}_G(x_i)| = {}^{|G|}\big/_{|C_g(x_i)|}$

Preuve:
Application imédiate de la formule d'orbites. On va séparer le groupe en deux partie, l'une où on met tout x avec orbite un point (unique, donc x lui même) ensemble, c'est à dire $Z(G)$ et le reste, là où les orbites ont plus d'un point dans la deuxième partie.

□

Exemples

1. Les classes de conjugaison d'un groupe abélien:

$$G = Z(G) \qquad |G| = |Z(G)|$$

2. Les classes de conjugaison dans S_3 ($\longleftrightarrow$ les types de décompositions en cycle)

$$\left.\begin{array}{ll} id & (1) \\ \text{transpo} & (1\ 2), (1\ 3), (2\ 3) \\ \text{3-cycles} & (1\ 2\ 3), (1\ 3\ 2) \end{array}\right\} \text{ 6 éléments car } |S_3| = 3!$$

$Z(S_3) = \{(1)\}$
$\mathrm{Cl}_{S_3}\big((1\ 2)\big) = \big\{(1\ 2), (1\ 3), (2\ 3)\big\} = \mathrm{Cl}_{S_3}\big((1\ 3)\big)$
$\mathrm{Cl}_{S_3}\big((1\ 2\ 3)\big) = \big\{(1\ 2\ 3), (1\ 3\ 2)\big\}$

$$\implies 6 = |S_3| = 1 + (2 + 3)$$

1.5 p-groupe

Soit p un nombre premier.

Définition

Un groupe G, fini ou infini, est un p-groupe si

$$\forall g \in G \qquad o(g) = p^n \qquad 0 \leq n < \infty$$

où $o(g) := | < g > | = \big|\{e, g, g^2, \ldots, g^{n-1}\}\big|$ est l'ordre de g.

Exemple

C_p, C_{p^n} groupes cycliques et $C_p \times C_p$ sont des p-groupes (cf. Théorème de Lagrange)

En général, $|G| = p^k \implies G$ p-groupe

En prenant $G = \mathrm{GL}_n\left(\mathbb{Z}\big/p\mathbb{Z}\right)$, et T le sous groupe de G formé par les matrices triangulaires supérieure où $a_{i,j} = 1 \quad \forall i = j$ (Donc la diagonale est remplie de 1) On arrive à montrer que $|T| = p^{n(n-1)/2}$

Théorème: Cauchy

Soient G un groupe fini et p premier. Si $p \mid |G|$, alors $\exists g \in G$ tel que $o(g) = p$

Démonstration:
Supposons que $p \mid |G|$. Soit $X = \big\{(x_1, \ldots, x_p) \in G^p \mid x_1 x_2 \cdots x_p = 1\big\}$.
Notons que $X \neq \varnothing$ car $(1, 1, \ldots, 1) \in X$. On peut aussi choisir librement les $p-1$ premiers choix $(x_1, x_2, \ldots, x_{p-1})$ (on a donc $|G|^{p-1}$ choix), et le dernier x_p est fixé comme l'inverse du produit $x_1 x_2 \cdots x_{p-1}$. Du coup $|X| = |G|^{p-1}$ $(\geq |G| \quad p \geq 2)$.
En particulier, $p \mid |X|$

On remarque que si $x_1 x_2 \cdots x_p = 1$ on a aussi $x_p x_1 \cdots x_{p-1} = 1$
Donc le groupe cyclique C_p agit sur X

$$C_p =< a >= \{1, a, a^2, \ldots, a^{p-1}\} \quad \text{est une action si} \quad a\big((x_1, x_2, \ldots, x_p)\big) := (x_p, x_1, \ldots, x_{p-1})$$

Les orbites de C_p ont soit 1 éléments, soit p éléments. Vu que $|\operatorname{St}_{C_p}(\overline{x}) \mid |C_p| = p$ par Lagrange $(\overline{x} := (x_1, \ldots, x_p))$

$$|\mathrm{orbit}(\overline{x})| = \frac{|C_p|}{|\operatorname{St}_{C_p}(\overline{x})|} = \quad \text{soit 1 soit } p$$

et quand l'orbite $C_p\overline{x}$ a 1 point $|C_p\overline{x}| = 1$
$\iff \overline{x} = (x, \ldots, x) \in X \iff x^p = 1 \quad x \in G$

Soit $B = \{x \in G \mid x^p = 1\}$, $1 \in B$ donc $|B| \geq 1$, utilisons la formule de l'orbite:

$$|X| = |B| + \sum_1^r p$$

Mais p divise $|X|$, mais il divise tout les éléments de la somme $\displaystyle\sum_1^r p$, et divise donc la somme entière, cela implique forcément que p divise $|B|$. Cela donne donc:

$$\implies |B| \geq p \implies \exists g \neq 1 \quad \text{tel que} \quad g^p = 1 \quad \text{c'est à dire} \quad o(g) = p$$

□

Corollaire

Soit G un groupe fini.
G est un p-groupe $\iff$ $|G| = p^n$ pour un certain $n \geq 0$

Démonstration:
[$\Leftarrow$] : Déjà observé (Lagrange)
[$\Rightarrow$] : G un p-groupe, $|G| = p^k \cdot m$, pgcd$(m, p) = 1$, à voir: $m = 1$, si non, prennons $q \mid m$ premier, $q \neq p$.
Alors $q \mid |G|$ premier et par Cauchy $\implies \exists g \quad o(g) = q \neq p^l$, impossible, donc $|G| = p^k$

□

Théorème

Soit G un p-groupe fini. Alors G est résoluble.

Proposition

Soient G un groupe et $K \triangleleft G$. Si K et G/K sont résolubles alors G est résoluble aussi.

Note: Il me semble qu'on peut démontrer la proposition en notant: $\varphi : G_1 \to G_2$ morphisme surjectif.

$$\varphi(G_1^{(n)}) \subset G_2^{(n)} \rightsquigarrow \pi(G^{(\ell)}) \subset \left(G/K \right)^{(\ell)} = \{e\} \implies G^{(\ell)} \subset K \implies (G^{(\ell)})^{(k)} = G^{(\ell k)} \subset K^{(k)} = \{e\}$$

Démonstration du Théorème
On sait que $|G| = p^n$, avec la formule des classes:

$$|G| = |Z(G) + \sum_i [a : C_G(x_i)] \implies p \mid |Z(G)| \implies |Z(G)| \geq p > 1$$

Par récurrence: $G = 1$ est résoluble
Supposons que pour tout p-groupe G, $|G| \leq p^n$ sont résolubles.
Soit G, $|G| = p^{n+1}$. Remarquons que $|Z| \geq p$ car $|Z| \triangleleft G$, G/Z est un p-groupe $\left| G/Z(G) \right| = p^m \leq p^n$, par hypothèse $G/Z(G)$ est résoluble, $Z(G)$ est abélien et donc résoluble, par la proposition précédente, G est résoluble aussi.

□

Remarque

En fait, on arrive à montrer que G est même nilpotent avec une preuve analogue.

1.6 Sous-groupes de Sylow

Soit G un groupe fini et p un premier. Supposons que $|G| = p^n \cdot m$ avec $\text{pgcd}(p, m) = 1$.

Définition

$H < G$ est un Sylow p sous-groupe de G (noté aussi p-Sylow sous-groupe) si $|H| = p^n$.
C'est à dire un p-groupe maximal dans G.

Notons que si H est p-Sylow, alors gHg^{-1} l'est aussi car $|gHg^{-1}| = |H|$. Donc G agit sur l'ensemble de toute p-Sylow par conjugaison.

Exemples

1. Si $|G| = p^n$ alors G lui même est p-Sylow.

2. Etudions les Sylow pour des groupes cycliques.
   Soit $G = \left({}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \ , + \right)$, $n = p^k \cdot m$ où $\text{pgcd}(p, m) = 1$.
   Bezout nous dit que: $\exists r, s$ tels que $rp^k + sm = 1$.
   Soit donc $x \in \mathbb{Z}$

   $$\begin{aligned} x &= x \cdot 1 = xrp^k + xsm \\ x &\equiv xrp^k \pmod{m} \\ x &\equiv xsm \pmod{p^k} \end{aligned}$$

   Alors

   $${}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \ \cong \ {}^{\mathbb{Z}}\!/_{p^k\mathbb{Z}} \ \times \ {}^{\mathbb{Z}}\!/_{m\mathbb{Z}}$$

3. $T =$ les matrices triangulaires supérieure de diagonale 1 est un p-Sylow de $\text{GL}_n\left({}^{\mathbb{Z}}\!/_{p\mathbb{Z}} \right)$.
   En effet, $\left|\text{GL}_n\left({}^{\mathbb{Z}}\!/_{p\mathbb{Z}} \right)\right| = \#\ {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ -bases de $\left({}^{\mathbb{Z}}\!/_{p\mathbb{Z}} \right)^n = \underbrace{p^{\frac{n(n-1)}{2}}}_{|T|} \ \underbrace{\cdot \prod_{i=1}^{n} (p^i - 1)}_{\text{pas divisible par } p}$

4. $\left({}^{\mathbb{Z}}\!/_{4\mathbb{Z}} \ , + \right)$, Notons que le 2-Sylow est ${}^{\mathbb{Z}}\!/_{4\mathbb{Z}}$.

   $$G = {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \ \times \ {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \ = \{(0,0), (1,0), (0,1), (1,1)\}$$

   Le 2-Sylow est G lui même, $4 \mid |G|$ mais il n'a aucun élément d'ordre 4. Cela implique donc que Cauchy ($p \mid |G| \implies \exists g,\ o(g) = p$) est vrai que pour p premier.

Théorème: 1er théorème de Sylow

Tout groupe fini a un p-Sylow sous-groupe.

Démonstration:
Il en existe plusieurs. Montrons le par récurrence pour $n = |G|$. Si $|G| = p$ ou que $|G| = 1$, l'énnoncé est correct.

Supposons donc que le théorème est démontré pour tous groupes plus petit que G.

Soit p et n tels que $p^n \mid |G|$, $p^{n+1} \nmid |G|$.
Si $H \subsetneqq G$, et $p^n \mid |H|$ alors par récurrence H a un p-Sylow, qui est à la même fois p-Sylow pour G

$$S < H < G \quad \text{et} \quad |S| = p^n$$

Du coup supposons que pour tout sous-groupe $H \subsetneqq G$, $p^n \nmid |H|$, donc $p \mid [G : H] = \dfrac{|G|}{|H|} = \dfrac{p^n m}{p^k m_2} \qquad k < n$ En passant par la formule des classes:

$$|G| = |Z(G)| + \sum_{x_i} [G : C_G(x_i)] \implies p \mid |Z(G)|$$

Par Cauchy: $\exists a \in Z(G) \quad o(a) = p$, donc $< a >= \{e, a, a^2, \ldots, a^{p-1}\} \triangleleft Z(G) \triangleleft G$
Il existe donc un homomorphisme $f : G \to {}^{G}\!/_{< a >}$. $p^n \mid |G| \implies p^{n-1} \mid \left| {}^{G}\!/_{< a >} \right|$
Par récurrence, il existe un p-Sylow K' de ${}^{G}\!/_{< a >}$, soit $K := f^{-1}(K')$, ${}^{K}\!/_{< a >} \cong K'$ donc K a cardinalité de p^n.
Nous avons donc bien $K < G$ est un p-Sylow de G.

□

Théorème: 2ème théorème de Sylow

Soient G fini et $p \mid |G|$ premier. Alors:

i) Si H est un p-sous-groupe alors il existe S un p-Sylow tel que $H < S$.

ii) Tous p-Sylow sont conjugés.

iii) Le nombre de p-Sylow est congruant à $1 \pmod p$

Démonstration:

i) Soit S l'ensemble de tout p-Sylow (p fixé). Comme noté G agit sur S par conjugaison. Soit donc $P \in S$ et soit S_o le G-orbite de P. Notons pour plus tard que $ii) \iff S_o = S$. Soit

$$\mathrm{Stab}_G(P) = \{g \in G \mid gPg^{-1} = P\} < G \quad \text{et} \quad P \leqq \mathrm{Stab}_G(P)$$

Alors $|S_o| = {}^{|G|}\!/_{|\,\mathrm{Stab}_G(P)|}$, $P \leqq \mathrm{Stab}_G(P) \implies |P| = p^n \mid |\,\mathrm{Stab}_G(P)| \implies p \nmid |S_o|$

Soit $H < G$ un p-groupe $|H| \geq p$ (le cas $H = \{1\}$ est trivial). Vu que $H < G$, H agit aussi sur S_o par conjugaison $S_o = G \cdot P(G \text{ agit sur } P) = \{gPg^{-1} \mid g \in G\}$

En passant par la formule des orbites $\implies$:

$$|S_o| = \sum_{P_i \in S_o} [H : \mathrm{Stab}_H(P_i)]$$

Mais $[H : \mathrm{Stab}_G(P_i)] = p^k$ par Lagrange et $|S_o|$ n'est pas divisible par p. Cela implique qu'il existe au moins un i où $[H : \mathrm{Stab}_H(P_i)] = 1$.
Prenons donc un tel P', c'est à dire $hP'h^{-1} = P' \qquad \forall h \in H \iff H = \mathrm{Stab}_H(P')$
On sait que $HP' < G$ est un sous groupe grâce à $hP'h^{-1} = P' \qquad \forall h \in H$ et $P' \triangleleft HP'$. Nous pouvons maintenant utiliser le deuxième théorème d'isomorphismes:

$$HP'\Big/_{P'} \cong H\Big/_{H \cap P'} \overset{\text{Lagrange}}{\Longrightarrow} \left| HP'\Big/_{P'} \right| = p^k$$

Et donc $|HP'| = p^k$ mais P' est p-Sylow, donc p-groupe maximal $\implies HP' = P'$, donc $H \subset P'$

ii) On a juste démontré que chaque H p-groupe est contenu dans un conjugué P' de P. Donc ça s'applique pour H un p-Sylow

$$H \leqq P' - gPg^{-1} \quad \text{Mais donc} \quad H = P' \quad \text{car } H \text{ est maximal.}$$

iii) Soit $H = P$ p-Sylow. Il y a un H-orbite dans $S =$ tout p-Sylow qui est juste un élément $\{P\}$. Soit S' une autre orbite, alors $|S'| > 1$, parce que si nous supposons le contraire:

$$S' = \{P'\},\ H \leqq \{g \mid gP'g^{-1}\}$$

Comme avant par maximalité de H, $H = P'$, donc $P = P'$.

Soit $P' \in S$ tel que $\mathrm{Stab}_H(P') \lneqq H$, donc l'indice $[H : \mathrm{Stab}_H(P')] > 1$ et donc divisible par p. (En vue $|H| = p^k$)
Par la formule d'orbite $\implies$:

$$|S| = 1 + \sum \text{ indices div. par } p \equiv 1 \pmod{p}$$

□

1.7 Le produit semi-direct

Le produit direct de H, K groupes est:

$$G := H \times K = \{(h,k) \mid h \in H,\ k \in K\}$$

Et il difini une structure de groupe sur G pour $\cdot$ défini comme:

$$\cdot : \begin{array}{ccc} G \times G & \longrightarrow & G \\ \Big((h_1,k_1);(h_2,k_2)\Big) & \longmapsto & (h_1h_2, k_1k_2) \end{array}$$

Exemple

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

On peut prendre un analogie géométrique pour expliquer la différence entre produit direct et produit "Tordu".

Prenons un rectangle dans $\mathbb{R}^2$, nous pouvons "étirer" ce rectangle et le relier à lui même dans $\mathbb{R}^3$. Cela revient à recoller le bout d'une bandellette à elle même.

Nous pouvons aussi partir du même rectangle mais avant de le recoller à lui même lui effectuer une demi rotation. Nous obtenons ainsi un ruban de Möebius, c'est une analogie pour le produit "Tordu"

Reprenons donc le cas du produit direct, la caractérisation interne:
Soient G un groupe et $H, K < G$, tels que

i) $H \cup K = \{e\}$

ii) $G = H \cdot K = \{h \cdot k \mid h \in H,\ k \in K\}$

iii) $hk = kh \qquad \forall h \in H,\ k \in K$

Alors $G \cong H \times K$

Définition

Soient H et K deux groupes. Soit $\phi : H \to \mathrm{Aut}(K)$ homomorphisme, c'est à dire H agit sur K.

$G := H \ltimes K$ pour $G = H \times K$ comme ensemble avec $(h_1,k_1) \cdot (h_2,k_2) := (h_1h_2, k_1\phi(h_1)k_2)$
On vérifie que c'est un groupe:
L'élément neutre est donné par: (e_H, e_K)
L'inverse de (h,k) est $(h^{-1}, (\phi(h^{-1})k)^{-1})$

Exemple

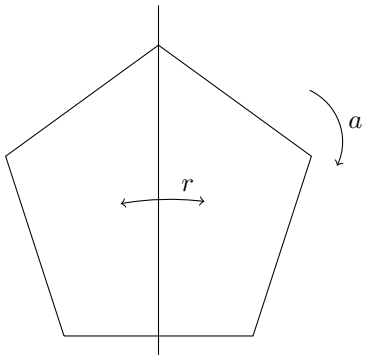
Trivial si $\phi(h) := id_K \quad \forall h \in H$, alors $H \ltimes K = H \times K$
Caractérisation interne:
Soient $H < G,\ K \triangleleft G$ tels que $H \cap K = \{e\},\ H \cdot K = G$.
Alors $G \cong H \ltimes K$ avec $\phi : \begin{array}{ccc} H & \longrightarrow & \mathrm{Aut}(K) \\ h & \longmapsto & \phi(h) \end{array}$ où $\phi(h)k = hkh^{-1}$

Exemple

(Voir exercices) $S_n \cong A_n \rtimes C_2$, $K = A_n$, $H = C_2$.

Exemple

Le groupe diedral:



$$< r >= C_2 \text{ et } C_5 =< a > \text{ car } a^5 = id$$

$$D_{2n} = C_n \rtimes C_2 \quad \text{où } C_2 \text{ sont les rotations et } C_2 \text{ des réflexions}$$

Exemple: (Géométrie I)

$$G = \mathrm{Isom}(\mathbb{R}^n) = \underbrace{\text{rotation}}_{\cong On\mathbb{R}} \ltimes \underbrace{\text{translation}}_{\cong \mathbb{R}^n}$$

Prenons $x \in \mathbb{R}^n$, g_1, g_2 deux isométries:

$$g_1 x = A_1 x + b_1,\ A_1 \in On\mathbb{R},\ b_1 \in \mathbb{R}^n$$
$$g_2 x = A_2 x + b_2,\ A_2 \in On\mathbb{R},\ b_2 \in \mathbb{R}^n$$

Alors

$$\begin{aligned}(g_1 g_2)x = g_1(g_2 x) &= A_1(g_2 x) + b_1 = A_1(A_2 x + b_2) + b_1 \\ &= A_1 A_2 x + A_1 b_2 + b_1\end{aligned}$$

Donc: $(A_1, b_1)(A_2, b_2) = (A_1 A_2, b_1 + A_1 b_2)$

Exemple

$$\mathrm{Affine}(\mathbb{R}^n) = \mathrm{GL}_n\,\mathbb{R} \rtimes \mathbb{R}^n$$

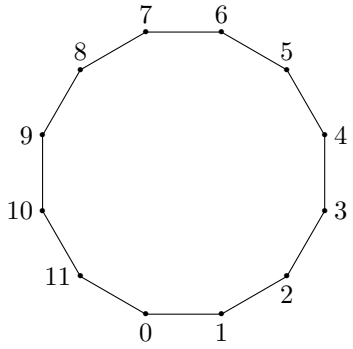
1.8 Graphe de Cayley

Soit G un groupe et $S \subset G$ un ensemble. On peut définir un graphe associé $\mathrm{Cay}(G, S)$, le graphe de Cayley par:

- Les sommets $:= G$
- Les arètes $:= \{(g, gs) \mid g \in G,\ s \in S\}$

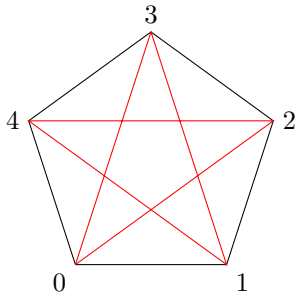
Exemple

$$\left({}^{\mathbb{Z}}\!/_{12\mathbb{Z}}\ , + \right) = \left(\{0, 1, 2, \ldots, 11\}, 1 \pmod{12} \right) \quad \text{et} \quad S = \{1\}$$



Exemple

$$\left({}^{Z}\!/_{5\mathbb{Z}}\ , + \right), \quad S = \{1, 2\}$$



Ces graphes nous donnent un manière de visualiser G ($\Longrightarrow$ Géométrie de groupe). Ils sont aussi une source importante de graphes (symétriques)

1.9 Groupes libres

Rappel: Le monoïde libre (langage)

- Symboles $A = \{a, b, c, \dots\}$, M_A = tout les mots avec A, $e = \varnothing$, le mot vide, l'opération est la juxtaposition (concaténation), par exemple:
$$a^2bc \cdot bc = a^2bcbc = a^2(bc)^2$$
Ce qu'on veut maintenant est un groupe libre, donc on doit avoir des inverses (monoïde + inverse = groupe).

- Alphabet $X = A \cup A^{-1} = \{a, b, \cdots, a^{-1}, b^{-1}, \dots\}$.
- On considère M_X comme un monoïde libre
- On dit que un mot W dans M_X est réduit s'il n'y a aucun $W = Uxx^{-1}v$ ou $Ux^{-1}xv$ (Donc si tout est simplifié)

  Exemple

  $abcc^{-1}dd^{-1}$ n'est pas réduit, alors que: ab et cbc^{-1} sont réduits.

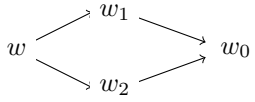
- Une réduction élémentaire est passer de: $\underbrace{\dots}xx^{-1}\underbrace{\dots} \to \underbrace{\dots}\underbrace{\dots}$, par exemple: $uxx^{-1}v \to uv$.
C'est une opération de $M_X \to M_X$.

- La longueur de W, notée $|W|$= le nombre de Symboles.

Lemme

Soit $w \in M_X$ un mot. Soient $w \to w_1$ et $w \to w_2$ deux réduction élémentaires. Alors, il y a:

- Soit deux réductions élémentaires $w_1 \to w_0$, $w_2 \to w_0$
- Soit $w_1 = w_2$



Preuve:
$x, y, z \in X$; $v, w, \cdots \in M_X$

Cas 1

$w = v_1xx^{-1}v_2yy^{-1}v_3 \dots \qquad v_i \in M_X$ et donc:

$$\left.\begin{aligned} w_1 &= v_1v_2yy^{-1}v_3 \\ w_2 &= v_1xx^{-1}v_2v_3 \end{aligned}\right\} \xrightarrow{\text{Rédu. élém.}} v_1v_2v_3 =: w_0$$

Cas 2

$w = v_1xx^{-1}xv_2 \implies w_1 = v_1xv_2 \quad \text{et} \quad w_2 = v_1xv_2$

□

Proposition

Soit w un mot. Le mot réduit $\overline{w}$ de w est unique. (Le mot réduit étant le mot réstant après avoir effectué toutes les réductions possibles)

Exemple

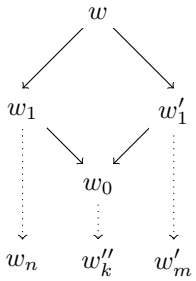
$$abb^{-1}a^{-1}baa^{-1}c \to abb^{-1}a^{-1}bc \to aa^{-1}bc \to bc$$

Preuve:
On doit vérifier que :
$w \to w_1 \to \cdots \to w_n$ réduit
$w \to w'_1 \to \cdots \to w'_m$ réduit sont équivalents.
Montrons donc par récurrence que $w'_m = w_n$.

Induction sur la longueur $|w|$:

$|w| = 0$ c'est à dire $w = \varnothing$, ok. De même pour $|w| = 1$

Supposons l'hypothèse vraie pour tout w tel que $|w| \leq k$, et prenons w tel que $|w| = k + 1$



w_0 existe par le lemme précédent (sinon $w_1 = w'_1$ et on retombe dans la récurrence), et donc par l'hypothèse de récurrence $w_n = w''_k$ et aussi $w'_m = w''_k \implies w_n = w'_m$

□

Notation

w mots, $\overline{w}$ sa forme réduite (unique!)

Théorème

Soit S un ensemble. Les mots réduits dans $S \cup S^{-1}$ avec produit $w_1 \cdot w_2 = \overline{w_1 w_2}$ est un groupe, le groupe libre sur S, noté $F(s)$

Preuve:
e ok, le mot vide, pour l'inverse:
$w = y_1 \cdots y_n$ alors $w^{-1} = y_n^{-1} \cdots y_1^{-1}$ Vérifions:

$$y_1 \cdots y_n y_n^{-1} \cdots y_1^{-1} \to \cdots \to e$$

Le produit est-il associatif ? C'est à dire $\overline{\overline{uv}w} = \overline{u \cdot \overline{vw}}$
Oui car les deux sont des réductions du mot uvw et notre proposition dit que c'est une unique réduction.

□

1.10 Présentation d'un groupe

Souvent, les groupes viennent dans la forme: < Générateurs | relations >, surtout en topologie. Mais il est difficile de les analyser comme ça.

Définition

Le sous-groupe normal N_A engendré par $A \subset G$ est:

$$N_A =< B > \quad \text{où} \quad B := \bigcup_{g \in G} gAg^{-1}$$

Définition

Soit S un ensemble et R un ensemble de mots (en S pour alphabet), on a un groupe

$$G =< S \mid R >:= {}^{F(S)}\Big/_{N_R}$$

On peut voir S comme les générateurs de notre groupe et R les relations, les règles de "grammaires" du groupe.

On dit que $< S \mid R >$ est une présentation de G.

Exemples

1. $$F(S) =< S \mid \varnothing >$$

2. $$< a \mid a^n > \cong {}^{\mathbb{Z}}\Big/_{n\mathbb{Z}}$$

   Pour $n = 5$ on a donc $a^3 \cdot a^4 = a^7 = \underbrace{a^5}_{=1} \cdot a^2 = a^2$

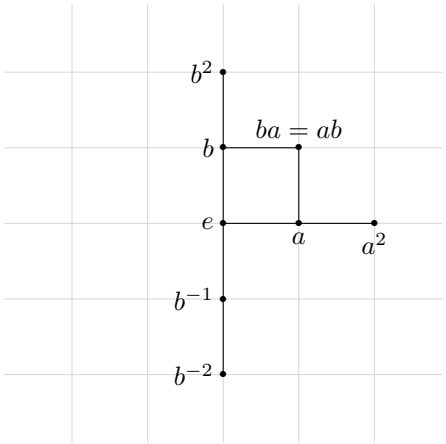
3. $$G =< a, b \mid aba^{-1}b^{-1} > \cong \mathbb{Z}^2$$

   La relation veut que $aba^{-1}b^{-1} = 1 \iff ab = ba$, c'est donc abélien. On justifie donc prenons $g \in G$, par exemple:

   $$g = aba^{-1}b^3a^{-1}baba = aba^{-1}b^3a^{-1}baab = \cdots a^0b^6 = b^6$$

   $\forall g \implies g = a^{k_1}b^{k_2}$ unique avec $k_i \in \mathbb{Z} \implies G \cong \mathbb{Z}^2$ par l'isomorphisme $g \mapsto (k_1, k_2)$.

   On peut donc grapher $\mathrm{Cay}(G, \{a, b\})$:



4. $\mathrm{PSL}_2\mathbb{Z} =< S, T \mid S^2 = 1, (ST)^3 = 1 >$ où $\mathrm{PSL}_2\mathbb{Z} = {}^{\mathrm{SL}_2\,\mathbb{Z}}\Big/_{\pm I}$

5. On peut définir les groupes de tresses:
   Posons $\sigma_i = (i, i+1) \in S_n$ une permutation pour $i = 1, 2, 3$.

$$B_4 =< \sigma_1, \sigma_2, \sigma_3 \mid \begin{array}{c} \sigma_1\sigma_3 = \sigma_3\sigma_1 \\ \sigma_2\sigma_3\sigma_2 = \sigma_3\sigma_2\sigma_3 \\ \sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2 \end{array} >$$

   On voit aussi que l'on a un homomorphisme $\phi : B_n \to S_n$

6. $$G =< a, b \mid aba^{-1}b^{-1},\ a^{-2}b^{-1}ab > \cong \{1\}$$

   On commence avec cet exemple à saisir la difficulté de compréhension lorsqu'on pose nos groupe sous cette forme

7. $$G =< a, b, c \mid a^5 = 1,\ abc = 1,\ b^{-1}c = 1 > \cong ??$$ C'est "impossible" de se représenter ça

2 Théorie de représentation de groupes

Ce sujet est important pour les maths, la physique, la chimie etc...
En math ce sujet est par exemple relié à la théorie des nombres, l'analyse de Fourier, la probabilité. On va voir des actions de groupe sur des espaces vectoriel linéaires comment "représenter le groupe avec des matrices".

2.1 Définitions

Soit V un espace vectoriel sur un corps $\mathbb{C}$.
$\mathrm{GL}(V) := \mathrm{Aut}(V)$ = les automorphismes linéaires de V
$\mathrm{GL}(\mathbb{C}^n) = \mathrm{GL}_n\,\mathbb{C}$ = les $n \times n$ matrices, $\det \neq 0$

Définition

Soit G un groupe fini et V un espace vectoriel sur $\mathbb{C}$ de dimension fini. Une représentation (linéaire) de G sur V est un homomorphisme:

$$\pi : G \to \mathrm{GL}(V) \quad \text{Noté} \quad (\pi, V)$$

Remarque

Autrement dit, c'est une action de G sur V par transformation linéaire.

Le but abstrait: Donné G on va essayer de déterminer toute représentation (π, V) (à isomorphisme près).
La stratégie:

1) Décomposer π dans des irréductibles.

2) Déterminer les irréductibles.

Remarques

1. C'est une stratégie assez standard. En effet pour essayer de comprendre le groupe dans son ensemble, on peut commencer par comprendre comment ses "blocs fondateurs" fonctionnent, c'est le rôle que jouent les irréductibles.

2. On peut faire la comparaison avec les nombres et les premiers. Une autre comparaison est quand nous avions étudié les groupes finis en observant les groupes simples.

Exemples

1. La représentation triviale: $\rho : \begin{array}{ccc} G & \longrightarrow & \mathrm{GL}(V) \\ g & \longmapsto & \rho(g) = id \end{array}$

2. Posons avec la notation vue dans le paragraphe sur la présentation des groupes: $G =< a \mid a^4 >$ Voici une liste non exhaustive de représentation:

   i)
   $$\pi_1 : \begin{array}{ccc} G & \longrightarrow & \mathrm{GL}(\mathbb{C}) = \mathbb{C}^* \\ e & \mapsto & 1 \\ a & \mapsto & i(\text{car } i^4 = 1) \end{array}$$

   ii)
   $$\pi_2(a) = -1 \qquad (-1)^4 = 1 \quad \text{OK}$$

   iii)
   $$\pi_3 : \begin{array}{ccc} G & \longrightarrow & \mathrm{GL}_2(\mathbb{C}) \\ a & \longmapsto & \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \end{array} \quad \text{Car:} \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^4 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}^2 = I$$

iv)

$$\pi_4(a) = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix} \implies \pi_4(a^4) = \begin{pmatrix} i^4 & 0 \\ 0 & i^4 \end{pmatrix} = I$$

3. $G = \mathbb{Z}$, $n \mapsto \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ est une représentation sur $\mathbb{C}^2$

4. $C_3 = \{1, x, x^2\}$ et $\rho(x) = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$ car $\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}^3 = I$

   Pour $V = \mathbb{C}^3$ on peut aussi poser $\tilde{\rho}(x) = \begin{pmatrix} -1 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

Exemple important

Un construction générale (et importante!).
Supposons que G agit sur X un ensemble fini. Considerer:

$$V = \mathrm{Fonc}(X, \mathbb{C}) = \{f : X \to \mathbb{C}\}$$

Notons que $\dim_{\mathbb{C}} V = |X|$ et aussi donc $V \cong \mathbb{C}^{|X|}$

L'action de G sur X induit une représentation linéaire sur V de manière naturelle:

$$\lambda_X : \begin{array}{ccc} G & \longrightarrow & \mathrm{GL}(V) \\ g & \longmapsto & \lambda_X(g) f(x) := f(g^{-1}x) \end{array}$$

On a donc besoin d'un peu de systématique/théorie. Il est difficile de faire cela pour G un groupe infini, mais par contre, pour les groupes finis il y a une belle théorie.

Une construction générale - représentation de permutations

Soit G un groupe fini qui agit sur X un ensemble fini (Par exemple $X = G$). Considérons l'espace vectoriel $V = \mathrm{Fonc}(X, \mathbb{C})$ sur $\mathbb{C}$ avec $\dim(V) = |X|$.
On peut considérer pour $f_i \in \mathbb{C}$, $X = \{1, 2, 3, \ldots, n\}$ le vecteur:

$$f = (f_1, f_2, \ldots, f_n) \quad \text{ou aussi} \quad f : \begin{array}{ccc} X & \longrightarrow & \mathbb{C} \\ i & \longmapsto & f_i \end{array}$$

L'action induit une représentation linéaire sur V

$$\lambda_{\mathcal{X}} : G \to \mathrm{GL}(V) \qquad \big(\lambda_{\mathcal{X}}(g)\ f\big)(x) := f(g^{-1}x)$$

Vérifion que $\lambda := \lambda_{\mathcal{X}}$ est bien un homomorphisme:

$$\begin{aligned} \big(\lambda(gh)\ f\big)(x) &= f\left((gh)^{-1}\ x\right) = f\left(h^{-1}g^{-1}x\right) = \big(\lambda(h)\ f\big)(g^{-1}x) = \lambda(g)\big(\lambda(h)\ f\big)(x) \\ &= \big(\lambda(g)\lambda(h)\ f\big)(x) \end{aligned}$$

Donc $\lambda(gh) = \lambda(g)\lambda(h)$

Sous-exemple général:

$X = G$, G agit sur X par $(g, h) \mapsto gh$
$V = L^2(G, \mathbb{C}) := \mathrm{Fonc}(G, \mathbb{C})$

Cette représentation λ_G est très importante et s'appelle la <u>représentation régulière</u> de G.

Autre sous-exemple:

Soient $G = S_3$ engendré par $s = (1\ 2)$ et $t = (1\ 2\ 3)$. $X = \{1, 2, 3\}$.
$V = \text{Fonc}(X, \mathbb{C}) \cong \mathbb{C}^3$, et avec base e_1, e_2, e_3 où $e_i(x) = \begin{cases} 1 & i = x \\ 0 \end{cases}$

$f \in V\ f(x) = f_1e_1(x) + f_2e_2(x) + f_3e_3(x)$, donc pour $g \in S_3$ on à la représentation:

$$\lambda_{\mathcal{X}}(g)\ e_i = e_{g(i)} \qquad (e_{g(i)}(x) = e_i(g^{-1}x))$$

$$\lambda_{\mathcal{X}}(s) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{car} \quad \lambda_{\mathcal{X}}(s) \begin{pmatrix} f_1 \\ f_2 \\ f_3 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} f_1 \\ f_2 \\ f_3 \end{pmatrix} = \begin{pmatrix} f_2 \\ f_1 \\ f_3 \end{pmatrix}$$

Et de plus

$$\lambda_{\mathcal{X}}(t) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

Notons rapidement que dans l'expression:

$$\big(\lambda_{\mathcal{X}}(g)\big)f(x) = f(g^{-1}x)$$

$\lambda_{\mathcal{X}}(g)$ est une matrice, f un vecteur et x la place du coefficient, $g^{-1}x$ la permutation de place.

Définition

Soit $\pi :\ G \to \text{GL}(V)$

- Le <u>degré</u> ou <u>dimension</u> de π est $\dim V$.
- $W \subset V$ est un sous-espace <u>invariant</u> si $\pi(g)W \subset W$ pour tout $g \in G$.
- Dans ce cas on a une <u>sous-représentation</u> $\pi\ |_W \colon\ G \to \text{GL}(W)$.
- On dit que π est <u>irréductible</u> si les seuls sous-espaces invariants sont $\{0\}$ et V.

Exemple

$G = C_4 =< a \mid a^4 >$, $\rho :\ G \to \text{GL}_3(\mathbb{C})$ où $\rho(a) := \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ (On a bien $\rho(a)^4 = I_3$)

Le degré de $\rho = \dim V = \dim \mathbb{C}^3 = 3$, ρ n'est pas irréductible car $W = \left\{ \begin{pmatrix} \star \\ \star \\ 0 \end{pmatrix} \right\}$ est invariant. Vérifions:

$$\begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ 0 \end{pmatrix} = \begin{pmatrix} x_2 \\ -x_1 \\ 0 \end{pmatrix}$$

Ce qui nous donne:

$$\rho\ |_W\ (a) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad \rho\ |_W \colon\ C_4 \to \text{GL}_2(\mathbb{C})$$

Affirmation: $\rho\,|_W$ est irréductible

Soit $0 \neq E \subset \mathbb{C}^2$, supponsons que E est invariant et montrons ensuite que $E = \mathbb{C}^2$:

Prenons $v \in E$ où $v = (v_1, v_2)$

$$\rho(a)\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} v_2 \\ -v_1 \end{pmatrix} \in E \quad \text{(Par hypothèse)}$$

Mais

$$(v_1, v_2) \cdot (v_2, -v_1) = v_1 v_2 + v_2(-v_1) = 0$$

Donc ils sont orthogonaux !

$$\Longrightarrow < \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}, \begin{pmatrix} v_2 \\ -v_1 \end{pmatrix} > \subset E \quad \text{a dim 2} \quad \Longrightarrow E = \mathbb{C}^2$$

Définition

On dit que (π_1, V_1) et (π_2, V_2) sont équivalents, noté $\pi_1 \approx \pi_2$ si:
$\exists T : V_1 \to V_2$ isomorphisme tel que $\overline{T \circ \pi_1(g) = \pi_2(g) \circ T} \qquad \forall g \in G$
Cela revient à dire: $(\pi_2(g) = T \circ \pi_1(g) \circ T^{-1}$, ils sont conjugués).
Dit autrement:

$$\begin{array}{ccc} V_1 & \xrightarrow{\pi_1(g)} & V_1 \\ \Big\downarrow T & & \Big\downarrow T \\ V_2 & \xrightarrow{\pi_2(g)} & V_2 \end{array}$$

Remarque

- Comme les changements de base vectoriel
- Comparer avec les exemples $\mathrm{SL}_2\,\mathbb{Z}$, s, r

Définition

On dit que π est fidèle si $\pi : G \to \mathrm{GL}_n\,\mathbb{C}$ est injective.

Exemple

λ_G la représentation régulièe est fidèle:

$$e_1(g) = \begin{cases} 1 & g = 1 \\ 0 \end{cases} \qquad \lambda_G(g)\ e_1 = e_g \qquad e_g(h) = \begin{cases} 1 & g = h \\ 0 \end{cases}$$

Donc si $g \neq 1$ $e_g \neq e_1$, et alors $\lambda_G(g) \neq 1$ ce qui montre que λ_G est injective.

2.2 Décomposition

Rappel

Pour $V = W \oplus W'$. Si $W, W' \subset V$ des sous espaces tels que $W + W' = V$ et $W \cap W' = \{0\}$ alors on note $V = W \oplus W'$

De plus quand $\dim V < \infty$:

$$V = W \oplus W' \iff \dim W + \dim W' = \dim V \quad \text{et} \quad W \cap W' = \{0\}$$

Définition

La somme directe de représentation:
Soient $\pi_1 : G \to \mathrm{GL}(V_1)$ et $\pi_2 : G \to \mathrm{GL}(V_2)$ on forme $\pi_1 \oplus \pi_2 : G \to \mathrm{GL}(V_1 \oplus V_2)$ telle que:

$$G \ni g \mapsto \left(\begin{array}{c|c} \pi_1(g) & 0 \\ \hline 0 & \pi_2(g) \end{array}\right)$$

Rappel: Le produit scalaire (hermitien)

C'est donc une fonction $(V \times V) \to \mathbb{C}$ telle que:

- $(v, v) > 0$ si $v \neq 0$
- $(v, w) = \overline{(w, v)}$
- $(av + bw, u) = a(v, u) + b(w, u)$
- $(v, bw + cu) = \overline{b}(v, u) + \overline{c}(v, u)$

Notons que v, u sont orthogonaux $\iff (v, u) = 0$

Proposition

Soit V un espace vectoriel sur $\mathbb{C}$ et $\pi : G \to \mathrm{GL}(V)$ une représentation linéaire de G, groupe fini sur V. Alors:

1) Il existe un produit scalaire invariant, c'est à dire $\big(\pi(g)v_1, \pi(g)v_2\big) = (v_1, v_2) \qquad \forall g \in G$ et $\forall v_1, v_2$
2) Si $W \subset V$ est invariant alors $W^\perp := \{u \mid (u, w) = 0 \quad \forall w \in W\}$ est aussi invariante et $V = W \oplus W^\perp$ et $\pi = \pi_W \oplus \pi_{W^\perp}$

Preuve:

1) (Idée standard, donc à retenir !)

   Prenons un produit scalaire arbitraire $<\cdot, \cdot>$ et définissons:

   $$(v, u) := \frac{1}{|G|} \sum_{g \in G} <\pi(g)v, \pi(g)u>$$

   Cela représente "la moyenne", notons que c'est bon car $|G| < \infty$
   C'est une combinaison linéaire de produits scalires donc $(\cdot, \cdot)$ est un produit scalaire. Mais de plus $(\cdot, \cdot)$ est $\pi(G)$-invariant:

   $$\forall h \in G \qquad \big(\pi(h)v, \pi(h)u\big) = \frac{1}{|G|} \sum_{g \in G} <\underbrace{\pi(g)\pi(h)}_{\pi(g \cdot h)} v, \pi(g)\pi(h)u> \overset{gh =: t}{=} \frac{1}{|G|} \sum_{t \in G} <\pi(t)v, \pi(t)u> = (v, u)$$

2) Avec $(\cdot,\cdot)$ noter que pour $u \in W^\perp$, c'est à dire $(u,w) = 0 \quad \forall w \in W$. A voir: $\pi(g)u \in W^\perp$:

$$\big(\pi(g)u, w\big) = \big(\pi(g^{-1})\pi(g)u, \underbrace{\pi(g^{-1})w}_{=:w' \in W}\big) = (u,w') = 0$$

Donc $W^\perp$ est invariant, et $\pi = \pi\mid_W \oplus \pi\mid_{W^\perp}$

$$\pi(g) = \left(\begin{array}{c|c} \pi\mid_W(g) & 0 \\ \hline 0 & \pi\mid_{W^\perp}(g) \end{array}\right)$$

□

Remarque

Donc avec $(\cdot,\cdot)$ les matrices $A = \pi(g)$ sont unitaires, c'est à dire: $A^{-1} = \overline{A}^t = A^*$

Corollaire

Toute représentation d'un groupe fini est une somme directe des irréductibles.

Preuve:
Soit $\pi : G \to \mathrm{GL}(V)$. Soit $(\cdot,\cdot)$ invariant. Notons que si $\dim V = 0$ ou 1 alors π est irréductible, donc OK.En général, $\dim V < \infty$
Soit (π, V) est irréductible OK
Si ce n'est pas irréductible, c'est à dire $\exists 0 \neq W \subset V$ invariante. Donc par la proposition $W^\perp$ est invariant et $\pi = \pi\mid_W \oplus \pi\mid_{W^\perp}$
En répétant ce processus en se demandant si $\pi\mid_W$ est irréductible ou pas ? De même avec $\pi\mid_{W^\perp}$ jusqu'à ce que ça se termine.

$$\pi = \pi\mid_{V_1} \oplus \cdots \oplus \pi\mid_{V_n}$$

Où tous sont irréductibles.

□

Remarque

Contrairement à des nombres (ex: $36 = 2\cdot 2\cdot 3\cdot 3$), cette décomposition n'est pas unique, par exemple:

$$\pi : \begin{array}{ccc} G & \longrightarrow & \mathrm{GL}(\mathbb{C}^2) \\ g & \longmapsto & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{array}$$

Cela implique donc que tout les sous-espaces de $\mathbb{C}^2$ sont invariant. Choisissons en un, W, $\mathbb{C}^2 = W \oplus W^\perp$ ou un autre V, $\mathbb{C}^2 = V \oplus V^\perp$

2.3 Lemme de Schur

Soient G un groupe et V_1 et V_2 deux espaces vectoriels sur $\mathbb{C}$ de dimension finies. Soient $\rho_1 : G \to \mathrm{GL}(V_1)$ et $\rho_2 : G \to \mathrm{GL}(V_2)$ deux représentations irréductibles. Supposons qu'il y a une transformation linéaire $T : V_1 \to V_2$ telle que:

$$\rho_2(g) \circ T = T \circ \rho_1(g) \qquad \forall g \in G$$

Alors:

1) Soit T est un isomorphisme, soit $T = 0$.
2) Si $V_1 = V_2$ et $\rho_1 = \rho_2$ alors $T = \lambda \cdot I$ pour un certain $\lambda \in \mathbb{C}$.

Démonstration:

1) Soit $W_1 := \mathrm{Ker}\, T \subset V_1$ Notons que pour $w \in W_1$

$$T \circ \rho_1(g)w = \rho_2(g) \circ \underbrace{Tw}_{=0} = 0 \quad \implies \rho_1(g)w \in W_1$$

Donc W_1 est $\rho_1(G)$-invariant, mais ρ_1 est irréductible, cela implique donc que soit $W_1 = V_1$, soit $W_1 = 0$Soit

$W_2 := \mathrm{Im}\, T$, Prenons $w \in W_2$ donc $w = T \cdot y$ pour un cerain $y \in V_1$. Alors

$$\rho_2(g)w = \rho_2(g)Ty = T\rho_1(g)y \quad \implies \rho_2(g)w \in W_2$$

Donc W_2 est $\rho_2(G)$-invariant et ρ_2 est irréductible, donc forcément, soit $W_2 = V_2$ ou $W_2 = 0$

Conclusion, soit T est un isomorphisme, soit $T = 0$.

2) Soient $V = V_2 = V_2 = \mathbb{C}^n$, $\rho = \rho_1 = \rho_2$ Et $T : V \to V$. Soit λ valeur propre (qui existe grace au théorème fondamental de l'Algèbre). Donc $T - \lambda I$ n'est pas inversible ($Tv = \lambda v,\ v \neq 0 \iff (T - \lambda I)v = 0$), définissons $A = T - \lambda I$

$$\rho(g)A = \rho(g)T - \rho(g)\lambda I = T \circ \rho(g) - \lambda I \circ \rho(g) = (T - \lambda I) \circ \rho(g) = A\rho(g)$$

Donc on peut appliquer le point (1)! $\implies$ Soit A est un isomorphisme soit $A = 0$, mais A ne peut pas être un isomorphisme car A n'est pas inversible par définition.

$$A = 0 \iff T - \lambda I = 0 \iff T = \lambda I$$

□

Corollaire

Chaque représentation irréductible sur $\mathbb{C}$ d'un groupe abélien est 1-dimensionnel.

Démonstration:
Fixons $g \in G$ et notons que trivialement:

$$\pi(g)\pi(h) = \pi(gh) = \pi(hg) = \pi(h)\pi(g) \qquad \forall h \in G$$

Donc comme π est irréductible, appliquons le théorème de Schur $\implies T = \pi(g) = \lambda_g \cdot I$.
Mais donc $\forall g \in G$, $\pi(g) = \lambda_g I_n$ (la matrice identitée $n \times n$) avec $n = \dim \pi$.
Mais π irréductible $\iff n = 1$ car $V = \{ \begin{pmatrix} * \\ 0 \\ \vdots \\ 0 \end{pmatrix} \}$ est invariante, $\dim \pi = 1$.

□

Proposition

Soit $h : V_1 \to V_2$ linéaire. Soient (ρ_1, V_1) et (ρ_2, V_2) deux représentation de G, $|G| < \infty$, $\dim V_1$ et $\dim V_2$ finis et complexes. Définissons:

$$h^o = \frac{1}{|G|} \sum_{g \in G} \rho_2(g)^{-1} h \rho_1(g)$$

Alors:

1) Si $\rho_1 \ncong \rho_2$ alors $h^o = 0$

2) Si $V_1 = V_2$, $\rho_1 = \rho_2$ et alors $h^0 = \frac{1}{\dim V} \operatorname{Tr}(h) \cdot I$

Preuve:

1. Affirmation:

$$\rho_2(g) h^o = h^o \rho_1(g) \qquad \forall g \in G$$

   En effet:

$$\rho_2^{-1}(s) h^o \rho_1(s) = \frac{1}{|G|} \sum_g \underbrace{\rho(s)^{-1} \rho_2(g)^{-1}}_{\rho_2(gs)^{-1}} h \underbrace{\rho_1(g)\rho_1(s)}_{\rho_1(gs)} = h^o$$

   h^o vérifie les conditions du lemme de Schur. Donc $h^o = 0$ si les représentation ne sont pas équivalentes.

2. Si elles sont égales $h^o = \lambda Id$

$$\operatorname{Tr}(h^o) = \frac{1}{|G|} \sum_g \operatorname{Tr}\left(\rho(g)^{-1} h \rho(g)\right)$$

   Car $\rho_1 = \rho_2 =: \rho$

$$\begin{aligned} &= \frac{1}{G} \sum_g \operatorname{Tr}(h) = \operatorname{Tr}(h) \\ &\implies \operatorname{Tr}(h) = \operatorname{Tr}(h^o) = \operatorname{Tr}(\lambda Id) = \lambda \dim(V) \\ &\implies \lambda = \frac{\operatorname{Tr}(h)}{\dim V} \end{aligned}$$

□

2.4 Caractères

Le but est de définir un outil nous permettant facilement de vérifier si une représentation est irreductible, de voir si deux représentations sont équivalentes, de décomposer une représentation etc...

Définition

Soit $A = (a_{ij})$ une matrice de taille $n \times n$ à coefficients complexes. On définit la trace de A comme la somme des éléments diagonaux, c'est à dire

$$\mathrm{Tr}(A) := \sum_{i=1}^{n} a_{ii}$$

Proposition

Soient A, B deux matrices de taille $n \times n$, alors $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$

Démonstration:
Si $A = (a_{ij})$ et $B = (b_{ij})$, alors

$$\mathrm{Tr}(AB) = \sum_i (ab)_{ii} = \sum_i \sum_j a_{ij} b_{ji} = \sum_j \sum_i b_{ji} a_{ij} = \sum_j (ba)_{jj} = \mathrm{Tr}(BA)$$

□

Remarque

La trace d'une matrice est invariante par changement de base, en effet $\mathrm{Tr}(ABA^{-1}) = \mathrm{Tr}(AA^{-1}B) = \mathrm{Tr}(B)$
On se rappelle que les représentations peuvent être vue comme des matrices en choisissant une base de l'espace vectoriel.

Définition

Soient G un groupe fini et (ρ, V) une représentation de G. On défini χ_ρ, le caractère associé à ρ comme

$$\chi_\rho : \begin{array}{ccc} G & \longrightarrow & \mathbb{C} \\ g & \longmapsto & \mathrm{Tr}(\rho(g)) \end{array}$$

Exemples

1. Si on regarde la représentation triviale de G dans V, $\chi(g) = \dim(V) = \mathrm{Tr}(\rho(g)) \quad \forall g \in G$
2. On considère $C_2 = \{1, x\}$ le groupe cyclique d'ordre 2. On définit une représentation $(\rho, \mathbb{C}^2)$ via:

$$\rho(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \rho(x) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

   On a donc $\chi_\rho(1) = 2$ et $\chi_\rho(x) = -2$
3. $G = S_3$, $V =$Vect(e_1, e_2, e_3), On a défini une représentation ρ de G sur V

$$\rho((1\ 2)) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \rho((1\ 2\ 3)) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \implies \chi_\rho((1\ 2)) = 1,\ \chi_\rho((1\ 2\ 3)) = 0$$

4. G un groupe agissant sur X un ensemble fini; On peut définir λ_X la représentation permut. On note X^g les éléments de X fixés par g, c'est à dire $X^g = \{x \in X \mid g \cdot x = x\}$

$$\chi_{\lambda_X}(g) = |X^g|$$

Proposition

Soit G un groupe fini, $(\rho, V), (\eta, W)$ deux représentations alors

1) $\chi_\rho(e) = \dim(V)$
2) $\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)} \qquad \forall g \in G$
3) $\chi_\rho(ghg^{-1}) = \chi_\rho(h) \qquad \forall g, h \in G$
4) $\chi_{\rho\oplus\eta} = \chi_\rho(g) + \chi_\eta(g)$

Démo en exercice

Définition

G un groupe fini et χ, η deux caractères associés à des représentations de G. On définit leur produit hermitien comme:

$$<\chi, \eta>= \frac{1}{|G|}\sum_g \chi(g)\overline{\eta(g)} = \frac{1}{|G|}\sum_g \chi(g)\eta(g^{-1})$$

Théorème

Soit G un groupe fini.

1. Soit ρ une représentation de G, alors ρ est irréductible si et seulement si $<\chi_\rho, \chi_\rho>= 1$
2. Si on a ρ_1, ρ_2 deux représentations irréductibles non equivalentes, alors $<\chi_{\rho_1}, \chi_{\rho_2}>= 0$

Proposition

Soient $(\rho_1, V_1), (\rho_2, V_2)$ deux représentation irréductibles d'un groupe fini G, $h : V_1 \to V_2$ une application linéaire. On défini un opérateur moyenne $h^o : V_1 \to V_2$ comme suit:

$$h^o = \frac{1}{|G|}\sum_g \rho_2(g)^{-1} h \rho_1(g)$$

Alors:

1. Si ρ_1 et ρ_2 ne sont pas équivalents alors $h^o = 0$
2. Si $V_1 = V_2$ et $\rho_1 = \rho_2$ alors $h^o = \dfrac{\mathrm{Tr}(h)}{\dim V} Id$

On peut énoncer cette proposition en termes matriciels:

Proposition

Si les applications de la proposition précédentes sont données par des matrices $(a_{ij}), (b_{ij}), (c_{ij})$, on a que

$$h^o_{ij} = \frac{1}{|G|}\sum_{\substack{g\in G\\ k,l}} b_{ik}(g^{-1}) h_{kl} a_{lj}(g)$$

alors

1. Si les représentations ne sont pas équivalentes alors $\dfrac{1}{|G|}\sum_g b_{ik}(g^{-1})a_{lj}(g) = 0 \qquad \forall i, j, k, l$
2. Si c'est les mêmes représentations alors $\dfrac{1}{|G|}\sum_g b_{ij}(g^{-1})a_{kl}(g) = \begin{cases} \dfrac{1}{\dim V} & i = l \\ 0 & \text{sinon} \end{cases}$

Démo en exercice

Démonstration du Théorème

1) $\chi_\rho(g) = \sum_i \rho(g)_{ii}$

$$<\chi_\rho, \chi_\rho> = \frac{1}{|G|}\sum_g \chi_\rho(g)\chi_\rho(g^{-1}) = \frac{1}{|G|}\sum_{\substack{g\in G\\ i,j}} \rho(g)_{ii}\rho(g^{-1})_{jj}$$

$$= \sum_{i,j} \underbrace{\left(\frac{1}{|G|}\sum_g \rho(g)_{ii}\rho(g^{-1})_{jj}\right)}_{(\star)}$$

En appliquant le point 2 de la proposition précédente sur $(\star)$

$$(\star) = \begin{cases} 0 & i \neq j \\ \frac{1}{\dim V} & i = j \end{cases}$$

$$= \sum_{i,j} \frac{1}{\dim V} = 1$$

2) Même raisonnement mais avec $(\star) = 0 \quad \forall i, j$.

□

Théorème

Soit (ρ, V) une décomposition de G, χ_ρ son caractère. Supposons que V se décompose en somme de représentations irréductibles, $V = W_1 \oplus \cdots \oplus W_k$, si on considère (η, W) une représentation (irréductible) de G, alors le nombre de représentatoin équivalente à W se trouvant dans la décomposition de V est donnée par $<\chi_\rho, \chi_\eta>$

Démonstration:
On note χ_i le caractère associé à la représentation de W_i.

$$<\chi_\rho, \chi_\eta> =<\chi_1 + \chi_2 + \cdots + \chi_k, \chi_\eta>=<\chi_1, \chi_\eta> + \cdots + <\chi_k, \chi_\eta>$$

Mais donc:

$$<\chi_i, \chi_\eta> = \begin{cases} 1 & W_i \cong W \\ 0 & \text{sinon} \end{cases}$$

Et alors

$$<\chi_\rho, \chi_\eta> = \#\quad \text{représentations où} \quad W_i \cong W$$

□

Corollaire

Le nombre de fois qu'une représentation irréductible apparait dans la décomposition d'une représentation est indépendant de la décomposition choisie.

Corollaire

Deux représentations avec les mêmes caractères sont équivalentes.

Exemple

$G = S_3$ et $(\pi, \mathbb{C}^2)$ définie comme:

$$\pi(id) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \pi((1\ 2)) = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \quad \pi((1\ 3)) = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$$
$$\pi((2\ 3)) = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix} \quad \pi((1\ 2\ 3)) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \quad \pi((1\ 3\ 2)) = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$$

Le caractère associé est:
$\chi_\pi(id) = 2$, $\chi_\pi((1\ 2)) = \chi_\pi((1\ 3)) = \chi_\pi((2\ 3)) = 0$, $\chi_\pi((1\ 2\ 3)) = \chi_\pi((1\ 3\ 2)) = -1$

$$<\chi_\pi, \chi_\pi> = \frac{1}{6}\left(2^2 + 0 + 0 + 0 + (-1)^2 + (-1)^2\right) = 1 \implies (\pi, \mathbb{C}^2) \quad \text{est irréductible}$$

On avait définit la représentation de S_3 sur $\text{Vect}(e_1, e_2, e_3)$, notée $\lambda_{\{1,2,3\}}$ Le caractère associé:
$\chi_{\lambda_{\{1,2,3\}}}(id_) = 3$, $\chi_{\lambda_{\{1,2,3\}}}((1\ 2)) = \chi_{\lambda_{\{1,2,3\}}}((2\ 3)) = \chi_{\lambda_{\{1,2,3\}}}((1\ 3)) = 1$, $\chi_{\lambda_{\{1,2,3\}}}((1\ 2\ 3)) = \chi_{\lambda_{\{1,2,3\}}}((1\ 3\ 2)) = 0$

$$<\chi_\pi, \chi_{\lambda_{\{1,2,3\}}}> = \frac{1}{6}(2 \cdot 3 + 0 \cdot 1 + 0 \cdot 1 + 0 \cdot 1 + (-1) \cdot 0 + (-1) \cdot 0) = 1$$

Ce qui implique que $(\pi, \mathbb{C}^2)$ apparait $1\times$ dans la décomposition de $(\lambda_{\{1,2,3\}}, V)$

On se permet de noter $V = m_1 W_1 \oplus m_2 W_2 \oplus \cdots \oplus m_k W_k$ (on regroupe les représentations irréductibles et on note leur multiplicité)

$$<\chi_\rho, \chi_\rho> = \sum m_i^2$$

Théorème

Soit χ le caractère d'une représentation, alors $<\chi, \chi>$ est toujours un entier.

Proposition

Si on note r_G le caractère de $(\lambda_G, \mathcal{L}^2(G))$, alors:

1. $r_G(1) = |G|$
2. $r_G(g) = 0$ si $g \neq 1$

Démonstration:

1. $\dim(\mathcal{L}^2(G)) = |G|$
2. $g \neq 1$ alors $\lambda_G(g)$ permute tout les éléments de base

□

Proposition

Toute représentation irréductible W_i de G est contenue dans λ_G un nombre de fois égal à sa dimension

Démonstration:

$$<r_G, \chi_i> = \frac{1}{|G|}\sum_g r_G(g)\chi_i(g^{-1}) = \frac{1}{|G|} r_G(1)\chi_i(1) = \frac{1}{|G|}|G| \dim(W_i)$$

□

Remarque

$$\mathcal{L}^2(G) = (\dim W_1)W_1 \oplus \cdots \oplus (\dim W_k)W_k$$

Corollaire

Soient (ρ_i, W_i) les représentations irréductibles de G, alors ρ_i apparaît dans $\lambda_G \dim W_i$ fois.

Preuve:

$$m_i = <r_R, \chi_i> = \frac{1}{|G|} \sum_{g \in G} r_G(g)\overline{\chi_i(g)} = \frac{1}{|G|} \cdot |G| \cdot \overline{\chi_i(1)} = \dim W_i$$

Car $r_G(g) = 0$ sauf pour $g = 1$.

□

Corollaire 2

1. $|G| = \sum_{i=1}^{k} m_i^2$ où $m_i = \dim W_i$ des irréductibles de G.
2. Si $g \neq 1$, $\sum_i m_i \chi_i(g) = 0$

Preuve:

1. $r_G = \sum m_i \chi_i$, $r_G(1) = |G|$ et $\chi_i(1) = \dim W_i$, OK
2. Pour $g \neq 1$, $0 = r_G(g) = \sum m_i \chi_i(g)$

□

2.5 Fonctions centrales

Soit G un groupe.

Définition

Une fonction $f : G \to \mathbb{C}$ est une fonction centrale si $f\left(sts^{-1}\right) = f(t) \quad \forall s, t \in G$

Exemple

Les caractères χ_ρ car ils sont la trace: $\mathrm{Tr}(ABA^{-1}) = \mathrm{Tr}(B)$

Définition

$\mathrm{Class}(G, \mathbb{C})$ est l'espace vectoriel de toute les fontions centrales.
C'est les fonctions qui sont constantes sur les classes de conjugaison. $\dim \mathrm{Class}(G, \mathbb{C}) = \#$ de classe de conjugaison.

Exemple

G abélien, donc $sts^{-1} = t \quad \forall s, t \in G$ donc: $\mathrm{Class}(G, \mathbb{C}) = L^2(G, \mathbb{C})$

Théorème

L'ensemble $\{\chi_i\}_{i=1}^n$ de tous les caractères irréductibles de G est une base orthonormée de $\mathrm{Class}(G, \mathbb{C})$

On sait déjà que χ_i est un système orthonormé avec $<f, h>= \dfrac{1}{|G|} \displaystyle\sum_{g \in G} f(g)\overline{h(g)}$. Donc il reste à montrer que'il engendre bien $\mathrm{Class}(G, \mathbb{C})$. Avant de montrer le théorème, faisons un peu de préparation.

Soit $f \in \mathrm{Class}(G, \mathbb{C})$ et $\rho : G \to \mathrm{GL}(V)$. Définissons la transformée de Fourier/coeff. de Fourier

$$\hat{f}(\rho) = \sum_{g \in G} f(g)\overline{\rho(g)}$$

Et donc $\hat{f}(\rho) : V \to V$.

Proposition

Si ρ est irréductible de degré n et caractère χ, alors $\hat{f}(\rho) = \lambda I$

$$\lambda = \frac{1}{n} \sum_{g \in G} f(g)\overline{\chi(g)} = \frac{|G|}{n} <f, \chi> \in \mathbb{C}$$

Preuve:
On va montrer que $\hat{f}(\rho)\overline{\rho(s)} = \overline{\rho(s)}\hat{f}(\rho)$

$$\overline{\rho(s)}\hat{f}(\rho)\overline{\rho(s^{-1})} = \sum_g f(g)\overline{\rho(s)\rho(g)\rho(s^{-1})} = \sum_g f(g)\overline{\rho(sgs^{-1})} \overset{sgs^{-1}=:u}{=} \sum_u \in G f(s^{-1}us)\overline{\rho(u)}$$

Comme f est centrale

$$= \sum_u f(u)\overline{\rho(u)} = \hat{f}(\rho)$$

ρ est irréductible, et par le Lemme de Schur: $\hat{f}(\rho) = \lambda \cdot I$.

$$n\lambda = \mathrm{Tr}(\lambda I) = \mathrm{Tr}(\hat{f}(\rho)) = \mathrm{Tr}(\sum f(g)\overline{\rho(g)}) = \sum f(g)\underbrace{\mathrm{Tr}(\overline{\rho(g)})}_{\chi(g)}$$

□

Démonstration du Théorème
Il reste à montrer que $\{\chi_i\}$ engendre Class$(G, \mathbb{C})$. Soit $f : G \to \mathbb{C}$ centrale, supposons que $<f, \chi_i>= 0 \quad \forall i$.
A montrer: $f(g) = 0 \quad \forall g$

Soit ρ une représentation. Si ρ est irréductible la proposition nous dit que:

$$\hat{f}(\rho) = \frac{|G|}{n} <f, \chi_\rho> \cdot I = 0 \qquad (\star)$$

Si ρ n'est pas irréductible, $\rho = \rho_{n_1} \oplus \rho_{n_2} \oplus \cdots \oplus \rho_{n_k}$, et alors:

$$\begin{aligned}\hat{f}(\rho) &= \sum f(g)\overline{\rho(g)} = \sum f(g)(\overline{\rho_{n_1}(g)} \oplus \cdots \oplus \overline{\rho_{n_k}(g)} \\ &= \sum f(g)\overline{\rho_{n_1}(g)} \oplus \cdots \oplus \sum f(g)\overline{\rho_{n_k}(g)} = \hat{f}(\rho_{n_1}) \oplus \cdots \oplus \hat{f}(\rho_{n_k})\end{aligned}$$

Par $(\star)$, on a que comme les ρ_{n_i} sont irréductibles, $\hat{f}(\rho_{n_i}) = 0$

$$\hat{f}(\rho) = 0$$

En particulier $\rho := \lambda_G$ la représentation régulière.

$$0 = \hat{f}(\lambda_G) \implies 0 = \hat{f}(\lambda_G)\delta_1 = \sum_g f(g)\underbrace{\lambda_G(g)\delta_1}_{\delta_g} \implies 0 = \sum_g f(g)\delta_g \implies f(g) = 0 \quad \forall g$$

□

Corollaire 1

1. $\dim \mathrm{Class}(G, \mathbb{C}) = \#$ de classe de conjugaisons $= \#$ de représentations irréductible de $G =: K$
2. $\sum_{k=1}^{K} m_k^2 = |G|$

Preuve:

1. $$K = |G| \iff sgs^{-1} = g \quad \forall g, s \iff \quad G \text{ abélien}$$
2. $[\Rightarrow]$ Déjà vu Schur

   $[\Leftarrow]$
   $$|G| = m_1^2 + \cdot + m_k^2 = 1^2 + \cdots + 1^2 = K$$

□

2.6 Un exemple "facile"

D'abord: Comparaison
Algèbre I, $\{e_i\}_1^n$, base orthonormée, $v = \sum_1^n <v, e_i> e_i$

Analyse II $\mathbb{C}$, $\{e^{inx}\}_{n=-\infty}^{\infty}$, f : $\begin{array}{ccc} [-\pi,\pi] & \longrightarrow & \mathbb{C} \\ x & \longmapsto & \sum_{n=-\infty}^{\infty} \hat{f}(n)e^{inx} \end{array}$

On sait que $\frac{d}{dx}e^{inx} = ine^{inx}$ et donc:

$$\hat{f}(n) = <f, e^{inx}> = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(x)e^{-inx}\,dx$$

Soit $G = \mathbb{Z}/N\mathbb{Z}$ avec l'adition. C'est un groupe abélien, donc toute représentation irréductible est 1-dim et $\chi_K = \mathrm{Tr}(\rho_k) = \rho_k$.

Proposition

$\chi_k(x) = e^{2n\pi ixk/N}$ où $0 \le k \le N-1$ sont les caractères (=rep) irréductibles.

Preuve:

- Bien définie $\pmod N$

$$\chi_k(x+mN) = e^{2\pi i(x+mN)k/N} = e^{2\pi ixk/N}\cdot e^{2\pi imk} = \chi_k(x)$$

- Homomorphisme $\rho_k(x+y) = \rho_k(x)\cdot\rho_k(y)$, simplement par les propriétés de l'exponentielle.
-

$$<\chi_k, \chi_\ell> = \frac{1}{N}\sum_{x=0}^{N-1} e^{\pi 2ixk/N}\cdot e^{-2\pi ix\ell/N} = \frac{1}{N}\sum_{x=0}^{N-1} e^{2\pi ix(k-\ell)/N}$$

Donc si $k=\ell \implies <\chi_k,\chi_k> = \frac{1}{N}\underbrace{(1+\cdots+1)}_{N \text{ fois}} = 1$

Si $k \neq \ell$, alors

$$\frac{1}{N}\sum_{x=0}^{N-1} e^{2\pi ixa/N} = \frac{1}{N}\frac{1-e^{e\pi i\frac{x}{N}\cdot N}}{1-e^{2\pi ia/N}} = \frac{1}{N}\frac{1-1}{1-e^{2\pi ia/N}} = 0$$

$N = |G| =$ # irréductible χ_k $0 \le k \le N-1$

□

Exemple

Théorie de Fourier finie.
Soit $f(x) = \begin{cases} 1 & x = 0 \\ 0 & x \neq 0 \end{cases}$ une fonction f : $\mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$

$f(x) = \sum_{k=0}^{N-1} \hat{f}(k)e^{2\pi ixk/N}$

$$\hat{f}(k) = <f,\chi_k> = \frac{1}{N}\sum_0^{N-1} f(x)e^{-2\pi ixk/N} = \frac{1}{N}1\cdot e^0 = \frac{1}{N} \implies f(x) = \sum_{k=0}^{N-1}\frac{1}{N}e^{2\pi ixk/N}$$

3 Anneaux

Cette partie des Mathématiques a été étudiée, en particulier, par Dedekind, Hilbert, Emmy Noetho au début du 20ème siècle.

3.1 Définitions et exemples

Définition

Un anenau R est un ensemble muni de deux opérations, notées $+$ et $\cdot$, $+, \cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ telle que

1. $(R, +)$ est un groupe abélien.
2. $(R, \cdot)$ est un monoïde:
   a) $\cdot$ est associative
   b) $\exists 1 \in R$ tel que $1 \cdot x = x \cdot 1 = x \quad \forall x \in R$
3. Loies distributives: $\left.\begin{array}{l} x(y+z) = xy + xz \\ (y+z)y = yx + zy \end{array}\right\} \quad \forall x, y, z \in R$

Remarques

- Parfois on n'insiste pas sur le 2b), ce qui nous donnerait un "anneau sans 1"
- R est commutatif si $xy = yx \quad \forall x, y \in R$
- Rappelons la notation: $n \in \mathbb{Z}$

$$na := a + a + \cdots + a \quad \text{ou si } n < 0 \quad na := -a - a - \cdots - a$$

  En ce qui concerne a^n, on le défini pour $n > 0$ (car a^{-1} n'est en général pas défini) par:

$$a^n = a \cdot a \cdots a$$

- Cette notion est une axiomatisation des nombres de beaucoup d'éléments que nous avons déjà étudié:
  - Les nombres, $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$, ou encore $\mathbb{Z}/n\mathbb{Z}$ (Ce sont des corps, c'est à dire: $(R \setminus \{0\}, \cdot)$ est un groupe abélien)
  - Les matrices
  - Les polynômes, à une ou plusieurs variables.

Exemple

Soit S un ensemble. Soit R les fonctions $f : S \to A$ où A est un anneau muni des opérations:

$$\left.\begin{array}{l} (f+g)(t) := f(t) + g(t) \\ (f \cdot g)(t) := f(t) \cdot g(t) \end{array}\right\} \quad \forall t \in S$$

Si A est commutatif, alors R est commutatif.

Non-Exemple

Un espace Vectoriel, en général, n'est pas un anneau car il ne possède pas d'opération de multiplication $\cdot : V \times V \to V$

Exemple

Soit V un espace vectoriel.

$$R = \operatorname{End} V := \{T : V \to V \quad \text{linéaire} \quad \}$$

R forme un anneau (non-commutatif en général)

Exemple

Soit A un anneau commutatif. $R = A[X]$, les polynômes est un anneau commutatif

Exemple

Soient G un groupe (ou un monoïde) et A un anneau commutatif.
L'algèbre de groupe est $A[G] = \{$ toutes combinations linéaires (finies) formels $\}$

$$\sum_{g \in G} a_g \cdot g \quad a_g \in A \quad \text{Avec un nombre fini de } a_g \text{ non-nuls}$$

On peut donc définir les opérations de bases comme:

- Addition: $\sum a_g g + \sum b_g g = \sum (a_g + b_g) g$
- Multiplication: $\left(\sum a_g g\right) \cdot \left(\sum b_g g\right) = \sum_{g,h \in G} a_g b_h g \cdot h$

Et donc si nous prenons $G = (\mathbb{N}, +)$ qui est un monoïde. $A[\mathbb{N}] \cong A[X]$, les polynômes avec variable x.
En effet, $\mathbb{N} \cong \{x^n \mid n \geq 0\}$

Et si on prend cette fois $R = \mathbb{C}$, $G =< a \mid a^5 = 1 >$ le groupe cyclique d'ordre 5. Donc dans $\mathbb{C}[G]$ on obtient des calculs de type:

$$2ia^4 \left(\frac{3}{7}a + \pi a^2\right) + a = \frac{6i}{7}a^5 + 2\pi i a^6 + a = \frac{6i}{7} + (2\pi i + 1)a$$

3.2 Diviseur de zéro

Soit R un anneau.

Définition

$a \in R \setminus \{0\}$ est un diviseur de zéro si $\exists b \neq 0$ tel que $a \cdot b = 0$

Exemples

1. $R := \mathbb{Z}/n\mathbb{Z}$, si on prend n non premier tel que $n = p \cdot q$, alors, $[p], [q] \in \mathbb{Z}/n\mathbb{Z}$ et $[p] \cdot [q] = [n] = [0]$.
2. Par contre, $\mathbb{Z}/p\mathbb{Z}$, avec p premier, n'a pas de diviseurs de zéro car si $a \cdot b \equiv 0 \pmod{p} \iff ab = kp$, et donc soit $a \mid p$, soit $b \mid p$ et comme p est premier on a forcément $a \equiv 0 \pmod{p}$ ou $b \equiv 0 \pmod{p}$
3. Si R est un corps, c'est à dire $(R \setminus \{0\}, \cdot)$ est un groupe commutatif, soit $a \in R \setminus \{0\}$, $\exists a^{-1} \in R$ tel que $a \cdot a^{-1} = a^{-1} \cdot a = 1$. Donc en particulier R ne possède pas de diviseur de zéro:
$$ab = 0 \iff a^{-1}ab = a^{-1}0 = 0 \iff 1b = 0 \iff b = 0$$
4. Prenons $R = \text{Fonc}([0,1], \mathbb{C})$, $f = \begin{cases} 1 & x < \frac{1}{2} \\ 0 & x \geq \frac{1}{2} \end{cases}, g = \begin{cases} 0 & x < \frac{1}{2} \\ 1 & x \geq \frac{1}{2} \end{cases}$ Alors:
$$(f \cdot g)(x) = f(x)g(x) = 0 \quad \text{Mais} \quad f \neq 0,\ g \neq 0$$
5. Soit A commutatif et sans diviseur de zéro. Alors $R = A[X]$ n'a aucun diviseurs de zéro car, $f, g \neq 0$:
$$f(x)g(x) = (a_m x^m + a_{m-1}x^{m-1} + \cdots)(b_n x^n + \cdots) = a_m b_n x^{m+n} + \cdots \neq 0 \quad \text{car } a_m \cdot b_n \neq 0$$
6. Soient G un groupe et $R = \mathbb{C}[G]$. Supposons que $g \in G,\ g \neq 1,\ g^n = 1$. Alors
$$R \ni \underbrace{(1-g)}_{\neq 0}\underbrace{(1+g+g^2+\cdots+g^{n-1})}_{\neq 0} = 1+g+g^2+\cdots+g^{n-1}-g-g^2-\cdots-g^n = 1-g^n = 1-1 = 0$$

   Si on suppose maintenant que $g \neq 1$ a ordre infinis, le problème n'est pas résolu (depuis 1950). Une conjecture dit que $\mathbb{C}[G]$ n'a aucun diviseurs de zéros.

   Un problème plus faible, inconnu est la conjecture des idempotents.
   $p \in R$ est un idempotant si $p^2 = p$ (comme une projection).
   $o(g) = \infty \overset{?}{\implies}$ pas d'idempotent non-trivial ?? (Les solutions triviales sont: $p = 0,\ p = 1$)

Définition

Un anneau $R \neq 0$ est un anneau à division si:

$$\forall a \in R \setminus \{0\} \quad \exists a^{-1} \quad \text{tq} \quad a^{-1}a = aa^{-1} = 1$$

Définition

Un anneau à division $R \neq 0$ commutatif est appelé un corps.

Définition

Un anneau R est intègre si:

- $R \neq 0$
- R commutatif
- R n'a aucun diviseur de zéro.

On obtient donc la chaîne d'inclusion suivante:

$$\text{Corps} \subset \text{Intègre} \subset \text{Anneaux Commutatifs} \subset \text{Anneaux}$$

Exemples

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des anneaux intègre, même des corps.
2. $\mathbb{Z}/p\mathbb{Z}$, avec p premier est un corps aussi.
3. Si A est intègre, alors $A[X]$ l'est aussi.
4. Les fonctions holomorphes sur un ouvert. $R = \text{Hol}(U, \mathbb{C})$ est un anneau commutatif.

3.3 Anneaux finis

Définition

Un anneau fini est un anneau R avec $|R| < \infty$.

Exemples

1. $\left({}^{\mathbb{Z}}\!/_{n\mathbb{Z}} \ , +, \cdot \right)$
2. Un exemple non commutatif: les matrices $d \times d$ avec coefficients dans ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$. Alors $|R| = n^d$ éléments.
3. ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ avec p premier est un corps.
4. Hamilton trouve en 1843 la relation entre ce qu'il appelera les quaternions:

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	h	j	$-i$	-1

Et donc $\mathbb{H} = \{a + ib + jc + kd\},\ a, b, c, d \in \mathbb{R}$ et notons que $\mathbb{C} = \{a + ib\} \subset \mathbb{H}$
On peut aussi noter que $\mathbb{H}$ n'est pas commutatif et qu'il est possible de définir une division, donc $\mathbb{H}$ est un anneau à division:

$$(a + ib + jc + kd)^{-1} = \frac{1}{a^2 + b^2 + c^2 + d^2} \ (a - ib - jc - kd)$$

Un fameux théorème nous dit (pas dans l'examen):

Théorème de Frobenius

Les seuls anneaux à division de dimension finie sur $\mathbb{R}$ sont $\mathbb{R}, \mathbb{C}$, et $\mathbb{H}$.

Lemme

Soit R sans diviseurs de zéro. Alors pour $a \neq 0$:

$$T_a : \begin{array}{ccc} R & \longrightarrow & R \\ x & \longmapsto & ax \end{array} \quad \text{est injective.}$$

Démonstration:
Supposons que $T_a(x) = T_a(y)$, montrons que $x = y$:

$$T_a(x) = T_a(y) \iff ax = ay \iff ax - ay = 0 \iff a(x - y) = 0 \overset{a \neq 0}{\iff} x - y = 0 \iff y = x$$

□

Proposition

Soit R un anneau sans diviseurs de zéro. Supposons que $|R| < \infty$. Alors R est un anneau à division.

Démonstration:
Soit $a \in R \setminus \{0\}$. Il faut montrer que a^{-1} existe. $T_a : R \to R$ est injective (cf Lemme) mais $|R| < \infty \implies T_a$ est surjective. Donc il existe forcément un $x \in R \setminus \{0\}$ tel que $T_a(x) = 1 \implies ax = 1 \implies x = a^{-1}$.

□

Définitions

Soit R un anneau, si pour $a \in R$ a^{-1} existe, alors a est une unité.
On note donc $R^* = \{\text{les unités de } R\}$

Aussi:

$$R^* = R \setminus \{0\} \overset{\text{Déf.}}{\iff} R \quad \text{est un anneau à division}$$

Théorème: Wedderburn 1905

Un anneau fini R sans diviseur de zéro est forcément commutatif, en fait un corps.

Exemple

En reprenant $\mathbb{H}$ on peut voir qu'il n'est pas possible de faire un anneau fini à partir de $\mathbb{H}$

Lemme

Soit:

$$\Phi_n(x) := \prod_{\substack{1 \le k \le n \\ \text{pgcd}(k,n)=1}} \left(x - e^{2\pi i k/n}\right)$$

le n-ème polynôme cyclotomique. Alors

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

Démonstration:

$$x^n - 1 = \prod_{1 \le k \le n} \left(x - e^{2\pi i k/n}\right) = \prod_{b|n} \prod_{\substack{1 \le k \le n \\ \text{pgcd}(k,n)=b}} \left(x - e^{2\pi i k/n}\right) = \prod_{b|n} \prod_{\substack{1 \le k' \le \frac{n}{b} \\ \text{pgcd}(k', \frac{n}{b})=1}} \left(x - e^{2\pi i k'/\frac{n}{b}}\right)$$

$$= \prod_{b|n} \Phi_{\frac{n}{b}}(x) \overset{n/b=:d}{=} \prod_{d|n} \Phi_d(x)$$

□

Si A est un sous-corps d'un anneau R alors on peut regarder R comme un espace vectoriel sur A car:

- $(R, +)$ est un groupe abélien et la multiplication scalaire $\cdot : \begin{array}{ccc} A \times R & \longrightarrow & R \\ (a, v) & \longmapsto & av \end{array}$ tel que:
  1. $1v = v$
  2. $a(bv) = (ab)v$
  3. $(a + b)v = av + bv$

  Et donc si $\dim_A R = n$, alors: $R = \{a_1 e_1 + \cdots + a_n e_n \mid a_i \in A\}$ est une base.

Démonstration: Théorème de Wedderburn
Soit R tel que $R^* = R \setminus \{0\}$ et $|R| < \infty$. Faisons une preuve par récurrence de cardinalité de R.
Cas initial:
$\mathbb{F}_2 = \{0, 1\} = \mathbb{Z}/2\mathbb{Z}$ est un corps.

Rappel: On note $Z(R) = \{x \in R \mid xy = yx \quad \forall y \in R\}$ le centre de R. Evidemment $\{0,1\} \subset Z(R)$. $Z(R)$ est un corps, en effet il est commutatif (par définition) et si x^{-1} existe alors il est dans $Z(R)$ aussi.

Soit $q = |Z(R)| \geq 2$, R est un espace vectoriel sur $Z(R)$.
Posons $n = \dim_{Z(R)} R < \infty$ et alors $|R| = q^n$ et $|R^*| = q^n - 1$. A montrer: $n = 1$, c'est à dire $R = Z(R) \iff R$ est commutatif.

Soit $Z_x(R) := \{z \in R \mid zx = xz\}$ le centralisateur de x. $Z_x(R)$ est un sous-anneau, car

$$(z_1 + z_2)x = z_1x + z_2x = xz_1 + xz_2 = x(z_1 + z_2) \quad \text{et} \quad z_1z_2x = z_1xz_2 = xz_1z_2$$

Nous avons vu que si $x \notin Z(R)$, alors $Z_x(R) \subsetneq R$ et alors par hypothèse de récurence, $Z_x(R)$ est un corps. $Z_x(R)$ est un espace vectoriel sur $Z(R)$.
Donc $|Z_x(R)| = q^d$, $d < n$. En plus, R est une espace vectoriel sur $Z_x(R)$ ($Z_x(R)$ un corps) et alors:

$$q^n = \left(q^d\right)^k = q^{dk} \implies d \mid n,\ d < n$$

Si on regarde R^*, $Z(R)^*$, $Z_x(R)^*$ comme groupes avec la multiplication, la formule de classe nous dit que:

$$|G| = |Z(G)| + \sum_{\substack{\text{Classes de} \\ \text{Conjugaison}}} [G \ : \ Z_{x_i}(G)] \implies q^n - 1 = q - 1 + \sum_i \frac{q^n - 1}{q^{d_i} - 1}$$

En passant par le lemme précédent:

$$\frac{q^n - 1}{q^d - 1} = \frac{\prod_{k|n} \Phi_k(q)}{\prod_{l|d} \Phi_l(q)} \overset{\substack{d|n \\ d \leq n}}{=} \Phi_n(q) \cdot F(q) \quad \text{où} \quad F(q) \text{ est un certain polynôme}$$

$$\implies \Phi_n(q) \quad \text{Divise les termes } q^n - 1 \text{ et chaque } \quad \frac{q^n - 1}{q^d - 1}$$
$$\implies \Phi_n(q) \mid q - 1 \quad \text{et aussi} \quad |\Phi_n(q)| \leq q - 1$$

Affirmation: $|\Phi_n(q)| > q - 1$ si $n > 1$

$$|\Phi_n(q)| = \prod_{(k,n)=1} \left|q - e^{2\pi ik/n}\right| > |q - 1|$$

Ce qui mène donc à une contradiction ! Cela implique que $n = 1$, c'est à dire $R = Z(R)$

□

3.4 Corps finis

Nous savons déjà que $\mathbb{Z}/p\mathbb{Z}$, pour p premier est un corps. Peut-on en trouver d'autres ?Nous avons vu en Algèbre

I que nous pouvons suivre la construction suivante:

$A = \mathbb{Z}/p\mathbb{Z}\left[X\right]/(f(x))$ où f un polynôme irréductible: $f(x) = g_1(x)g_2(x) \implies$ soit g_1 soit g_2 unité.

Nous avons donc que $(f(x))$ est un idéal maximal et donc A est un corps.

Exemple mais avec A infini

$$\mathbb{C} = \mathbb{R}[X]/(x^2+1) = \{a+ib \mid a,b \in \mathbb{R},\ i^2+1=0\}$$

Autre exemple

$$\mathbb{F}_4 = \mathbb{Z}/2\mathbb{Z}\left[X\right]/(x^2+x+1) = \left\{a+b\alpha \mid a,b \in \mathbb{Z}/2\mathbb{Z}\right\} = \{0,1,\alpha,\alpha+1\}$$

Notons que nous sommes dans $\mathbb{Z}/2\mathbb{Z}$, et donc: $\alpha^2+\alpha+1=0 \iff \alpha^2 = -\alpha-1 = \alpha+1$ et alors:

$$\alpha(1+\alpha) = \alpha+\alpha^2 = \alpha+\alpha+1 = 2\alpha+1 = 1$$

Et en tableau:

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

3.5 L'analogie entre entiers et polynômes

Intro

D'une part ($\to$théorie standard, algèbre I), $(\mathbb{Z}, +, \cdot)$, $(\mathbb{C}[t], +, \cdot)$, ce sont des anneaux commutatifs, intègres, factoriels et principaux en plus d'être Euclidien.

Nous avons vu qu'on pouvait écrire tout nombre comme combinaison unique, à ordre près et unité près de premiers. Donc:

$$\mathbb{Z} \ni m = (\pm 1) \prod_{i=1}^{n} p_i^{r_i} \qquad \mathbb{C}[t] \ni f(t) = c \prod_{i=1}^{n} (t - \alpha_i)^{r_i}$$

Avec p_i des premiers distincts, α_i des racines distinctes de multiplicité r_i. On peut introduire une notion de taille en prenant $|m|$ et le $\deg f$ dans le cas des polynômes.
D'autre part, il y a des analogies plus profondes et mysterieuse, par exemple Fermat, ABC, à voir...

ABC pour polynômes

Soit $f \in \mathbb{C}[t]$, $f \neq 0$. On peut écrire $f(t) = c(t - \alpha_1)^{m_1} \cdots (t - \alpha_r)^{m_r}$ où $c \neq 0$ et α_i des racines distinctes.
$\deg f = m_1 + \cdots m_r$, et $n_0(f) = \#$ racines distinctes $= r$
Rappel:

- En prenant $\deg(0) = -\infty$ alors on a l'identité suivante:

$$\deg(f \cdot g) = \deg f + \deg g$$

- $n_0(fg) \leq n_0(f) + n_0(g)$ pour $f, g \neq 0$ avec une égalité si $\operatorname{pgcd}(f, g) = 1$
- $n_0(f) \leq \deg f$ Il est clair que $\deg f$ peut être beaucoup plus grand que $n_0(f)$.

Théorème: Stothers 1981, Mascon 1983 (ABC pour polynômes)

Soient $f, g, h \in \mathbb{C}[t]$ non constants, premiers entre eux tels que $f + g = h$. Alors:

$$\max(\deg f, \deg g, \deg h) \leq n_0(f \cdot g \cdot h) - 1$$

Corollaire: Théorème de Fermat pour polynômes, 19ème siècle

Soit $n \geq 3$ avec $x, y, z \in \mathbb{C}[t]$ non constants, premiers entre eux, alors il n'y a aucunes solutions à:

$$x(t)^n + y(t)^n = z(t)^n$$

Remarques

a) $\deg 0$, alors $a^n + b^n = c^n$ avec $a, b, c \in \mathbb{C}$, facile, par exemple $1^3 + \sqrt[3]{2}^3 = \sqrt[3]{3}^3$

b) $n = 1$, $t + (2t - 1) = 3t - 1$

c) $n = 2$, $(t^2 - a^2)^2 + (2ta)^2 = (t^2 + a^2)^2$

d) char $\mathbb{C} = 0$, où la charactéristique est le Ker de l'homomorphisme d'anneau entre $\mathbb{Z} \to \mathbb{C}$ (cf. Algèbre I)

$$(\text{mod } p): \qquad (x + a)^p \equiv x^p + a^p \pmod{p}$$

Démonstration du corollaire
Soient $f = x^n$, $g = y^n$ et $h = z^n$ avec $f + g = h$, f, g, h non constant et premier entre eux. Par le théorème:

$$\max(\deg x^n, \deg y^n, \deg z^n) \leq n_0(x^n y^n z^n) - 1$$

Notons que:

- $\deg x^n = n \deg x$ etc.
- $n_0(x^n y^n z^n) = n_0(xyz) = n_0(x) + n_0(y) + n_0(z) \leq \deg x + \deg y + \deg z$

  Donc en mettant tout bout à bout:

$$\max(n \deg x, n \deg y, n \deg z) \leq \deg x + \deg y + \deg z - 1$$

En sommant le tout on obtient:

$$n \deg x + n \deg y + n \deg z \leq 3(\deg x + \deg y + \deg z - 1) \implies (n-3) \underbrace{(\deg x + \deg y + \deg z)}_{\geq 0} \leq -3 \implies n \leq 2$$

□

Préparation pour la preuve du Théorème

- La dérivée, si $f = \sum_{n \geq 0} a_n t^n$, alors $Df = f' = \sum_{n \geq 1} n a_n t^{n-1}$, avec la règle $(fg)' = f'g + fg'$
- Dérivée du log $= \dfrac{f'}{f}$
- **Proposition**

  1. $$\frac{(fg)'}{fg} = \frac{f'}{f} + \frac{g'}{g}$$

  2. $$\frac{\left(\frac{f}{g}\right)'}{\frac{f}{g}} = \frac{f'}{f} - \frac{g'}{g}$$

  3. Si $f = c \prod_1^r (t - \alpha_i)^{m_i}$ alors:

$$\frac{f'}{f} = \frac{m_1}{t - \alpha_1} + \cdots + \frac{m_r}{t - \alpha_r}$$

  Démo facile, faire en exo.

Démonstration du Théorème ABC

Soient $f+g=h\ \forall t$, $f=c_1\prod_{i=1}^{r_1}(t-\alpha_i)^{m_i}$, $g=c_2\prod_{i=1}^{r_2}(t-\beta_i)^{n_i}$, $h=c_3\prod_{i=1}^{r_3}(t-\gamma_i)^{l_i}$ avec α_i, β_i, γ_i toutes distinctes car f,g,h sont premiers entre eux.

$$\implies \underbrace{\frac{f}{h}}_{=:R}+\underbrace{\frac{g}{h}}_{=:S}=1 \quad \forall t \implies R'+S'=0 \quad S,R\neq 0 \text{ car } f,g,h \text{ non const.}$$

$$\implies \frac{R'}{R}R+\frac{S'}{S}S=0 \implies \frac{R'}{R}R=-\frac{S'}{S}S \implies \frac{\frac{R'}{R}}{\frac{S'}{S}}=-\frac{S}{R}$$

Nous avons donc:

$$\frac{g}{f}=\frac{\frac{g}{h}}{\frac{f}{h}}=\frac{S}{R}=-\frac{\frac{R'}{R}}{\frac{S'}{S}} \implies \frac{g}{f}=-\frac{\frac{f'}{f}-\frac{h'}{h}}{\frac{g'}{g}-\frac{h'}{h}}=-\frac{\sum\frac{m_i}{t-\alpha_i}-\sum\frac{l_k}{t-\gamma_k}}{\sum\frac{n_j}{t-\beta_j}-\sum\frac{l_k}{t-\gamma_k}}$$

Soit $D(t)=\prod_i(t-\alpha_i)\prod_j(t-\beta_j)\prod_k(t-\gamma_k)$, donc $\deg D(t)=n_0(fgh)$, notons que $\deg\left(\frac{D(t)}{t-\alpha_i}\right)=n_0(fgh)-1$

$$\implies \frac{g}{f}=\frac{\text{Polynôme de degré} \leq n_0(fgh)-1}{\text{Polynôme de degré} \leq n_0(fgh)-1}$$

Et donc g et f sont premier entre eux et $\max(\deg f,\deg g)\leq n_0(fgh)-1$

$$h=f+g \implies \deg h\leq n_0(fgh)-1$$

□

ABC pour des entiers ?!

Peut on trouver des analogues au degré de f, $n_0(f)$, f' etc pour $\mathbb{Z}$? Si on a $m=(\pm1)\prod_{i=1}^{r}p_i^{m_i}$ on pourrait, dans un premier temps, suggerer que le degré de m soit: $\sum_1^r m_i$ et $n_0(m)=r$. Mais cette analogie ne tient pas.

On peut proposer mieux:

$$\log|m|=\sum_{i=1}^{r}m_i\log(p_i) \quad \text{et} \quad n_0(m)=\sum_{i=1}^{r}\log(p_i)$$

Mais l'analogie ne tiens pas pour f' ou $\frac{f'}{f}$ malheureusement.
Maintenant il est clair que $n_0(m)\leq\log(m)$ même beaucoup plus grand:

$$m=2^{1000} \implies \log m=1000\log(2) \quad \text{et} \quad n_0(m)=\log(2)$$

Il existe dessus une conjecture:

Conjecture ABC (Masser-Oesterlé 1986)

$\forall \varepsilon > 0,\ \exists C$ tel que tout $a, b, c \in \mathbb{Z} \setminus \{0\}$ premier entre eux, et $a + b = c$ nous avons alors:

$$\max(\log |a|, \log |b|, \log |b|) \leq (1 + \varepsilon) n_0(abc) + C$$

Remarques

- La raison pour ε est , $a_n = 3^{2^n},\ b_n = -1,\ c_n = 3^{2^n} - 1 \implies a_n + b_n = c_n$
- La liste de conséquences est incroyable, par exemple Fermat $x^n + y^n = z^n$.

3.6 Polynômes irréductibles

Rappel

Soit A un anenau intègre. On défini:
Un élément $a \neq 0$ est irréductible si:

- a n'est pas une unité
- Si $a = b \cdot c$ alors b ou c est une unité.

Exemple

1. $n \in \mathbb{Z} \setminus \{0\}$ est irréductible si et seulement si $n = (\pm 1) \cdot p$ où p est premier.
2. $A = \mathbb{C}[x]$, $p(x)$ est irréductible ssi $p(x) = ax + b$ selon le théorème fondamental de l'algèbre.
3. $A = \mathbb{R}[x]$, $p(x) = 4x^2 + 4$ est irréductible: $p(x) = 4 \cdot (x^2 + 1)$, 4 est une unité car $\frac{1}{4} \in \mathbb{R}$.
   Le même raisonnement s'applique dans $\mathbb{Q}[x]$, par contre pas dans $\mathbb{Z}[x]$ car $\frac{1}{4} \notin \mathbb{Z}$.

Définition

Un polynôme $P \in \mathbb{Z}[t]$ (ou plus généralement $P \in A[t]$, A factoriel) est primitif si tous les coefficients de P sont tous premiers entre eux. ($\text{pgcd}(a_n, \ldots, a_0) = 1$, il n'existe pas de $a \in A$ qui divise tout a_i)

Exemple

$P(t) = 3t^2 + 2t + 1$ est primitif mais $P(t) = 3t^2 + 6t + 3$ ne l'est pas.

Remarques

- Si P n'est pas primitif on peut diviser par le pgcd: $P(t) = 3t^2 + 3 = 3(t^2 + 1)$
- Pour $f \in \mathbb{Z}[t]$ irréductible, alors il est forcément primitif.

1er Lemme de Gauss

Si f et g sont primitifs sur $\mathbb{Z}$, alors $f \cdot g$ l'est aussi.

Preuve:

1. $f(t) = a_n t^n + \cdots + a_0$, $a_n \neq 0$ et $g(t) = b_m t^m + \cdots b_0$, $b_m \neq 0$.
   Posons p un premier et montrons que p ne peut pas diviser tous les coefficients de $f \cdot g$. Soient:
   $$r = \max\{i \mid p \nmid a_i \quad a_i \neq 0\} \geq 0 \quad \text{et} \quad r = \max\{j \mid p \nmid b_j \quad b_j \neq 0\} \geq 0$$
   Considérons le coefficient de t^{r+s} dans $f \cdot g$:
   $$c = \underbrace{a_0 b_{r+s} + a_1 b_{r+s-1} + \cdots}_{\text{divisible par } p} + \underbrace{a_r b_s}_{\text{non divisible par } p} + \underbrace{a_{r+1} b_{s-1} + \cdots + a_{r+s} b_0}_{\text{divisible par} p}$$
   $\implies p \nmid c$, donc top !
2. Supposons que p premier divise tous coefficients de $f \cdot g$.
   Soit $\sigma : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$. Cela définit une réduction $\pmod p$: $\sigma : \mathbb{Z}[t] \to \mathbb{Z}/p\mathbb{Z}\ [t]$ qui est donc un morphisme. Alors $\sigma(f) \neq 0$ car f est primitif, de même $\sigma(g) \neq 0$ car g est primitif. Par hyposèse nous avons $0 = \sigma(f \cdot g) = \sigma(f)\sigma(g)$ Mais nous savons que $\mathbb{Z}/p\mathbb{Z}$ est intègre, donc $\lightning$.

□

2ème Lemme de Gauss

Soit $f \in \mathbb{Z}[t]$ irréductible et non-constant. Alors f est aussi irréductible dans $\mathbb{Q}[t]$.

Preuve:
Supposons que $f(t) = g(t) \cdot h(t),\ g, h \in \mathbb{Q}[t]$ avec degré plus petit que $\deg f$. On peut multiplier avec tous les dénominateurs des coefficients dans $\mathbb{Q}$. Soit n ce grand nombre on a donc:

$$n \cdot f(t) = \tilde{g}(t) \cdot \tilde{h}(t) \quad \text{avec maintenant} \quad \tilde{g}, \tilde{h} \in \mathbb{Z}[t]$$

Le cas $n = 1$ est exclus car f est irréductible. Soit p premier $p \mid n$.

Affirmation: Soit p divise tous coefficients de $\tilde{g}(t)$, soit il divise tous coefficients de $\tilde{h}(t)$. En effet sinon cela implique: Soient: $r := \max\{i \mid p \nmid g_i\} \geq 0$ et $s := \max\{j \mid p \nmid h_j\} \geq 0$. Les coefficients de t^{r+s} dans $\tilde{g}(t) \cdot \tilde{h}(t)$ sont:

$$c = \underbrace{h_0 g_{r+s} + \cdots}_{\text{divisible par } p} + \underbrace{h_s g_r}_{\text{non divisible par } p} + \underbrace{\cdots + h_{r+s} g_0}_{\text{divisible par } p}$$

Pas possible car $p \mid n \cdot f(t)$ mais pas $\tilde{g}(t) \cdot \tilde{h}(t) = n \cdot f(t)$ ↯. Donc l'affirmation est correcte.

Supposons sans perte de généralité que p divise tous coefficients de $\tilde{g}$. Donc on divise les deux côtés par p pour obtenir:

$$n' \cdot f(t) = \tilde{\tilde{g}}(t)\tilde{h}(t) \quad \text{où} \quad \tilde{\tilde{g}}, \tilde{h} \in \mathbb{Z}[t]$$

Cet argument peut être répété jusqu'à ce que $n = 1$ où nous aurions:

$$f(t) = \overline{g}(t) \cdot \overline{h}(t) \quad \text{avec} \quad \overline{g}, \overline{h} \in \mathbb{Z}[t]$$

Ce qui est en contradiction avec f irréductible dans $\mathbb{Z}[t]$.

□

Note: Pour démontrer le Lemme on peut aussi passer par le premier Lemme de Gauss. Je m'explique:
Prenons $f \in \mathbb{Z}[t]$ d'après les hypothèses, supposons que dans $\mathbb{Q}$: $f = \hat{g} \cdot \hat{h} \in \mathbb{Q}[t]$. Il existe $n \in \mathbb{N}^*$ tel que $n \cdot f = \tilde{g}\tilde{h} \in \mathbb{Z}[t]$.
Donc $n \cdot f$ n'est pas primitif, donc en fait $\tilde{g}$ et/ou $\tilde{h}$ ne l'est pas non plus. Supposons que $\tilde{g}$ ne l'est pas, notons $a := \text{pgcd}(\tilde{g})$ le facteur commun tel que $\tilde{g} = a \cdot g$ avec g primitif. $\frac{n}{a} f = g \cdot \tilde{h} \in \mathbb{Z}[t]$. Si $\tilde{h}$ n'est pas primitif, réduisons le de la même manière et alors: $\frac{n}{a \cdot b} f = g \cdot h \in \mathbb{Z}[t]$ avec g et h primitifs par construction. Donc $\frac{n}{ab} f$ est primitif, $ab = n$ et on a trouvé une décomposition de f dans $\mathbb{Z}[t]$ ↯

Proposition: Critère d'Eisenstein

Soit $f(t) = a_n t^n + \cdots + a_1 t + a_0$, $n \geq 1$ et $a_i \in \mathbb{Z}$. Soit p un premier. Supposons que $\forall i < n$:

- $a_n \not\equiv 0 \pmod{p}$
- $a_i \equiv 0 \pmod{p}$
- $a_0 \not\equiv 0 \pmod{p^2}$

Alors f est irréductible sur $\mathbb{Q}$.

Preuve:
Par division, on peut supposer que f est primitif (ne change pas l'irréductibilité dans $\mathbb{Q}$).
Supposons que $f(t) = g(t) \cdot h(t)$ avec: $1 \leq \deg g,\ \deg h < \deg f,\ g, h \in \mathbb{Z}[t]$. (Grâce au 2ème Lemme de Gauss on peut supposer $\mathbb{Z}$ au lieu de $\mathbb{Q}$.)

$$g(t) = g_d t^d + \cdots \quad \text{et} \quad h(t) = h_m t^m + \cdots$$

On a donc que $g_0 \cdot h_0 = a_0$ et $p \mid a_0$ mais $p^2 \nmid a_0 \implies p$ divise exactement un de g_0 et h_0. Sans perte de généralité supposons que $p \nmid g_0$ et $p \mid h_0$.
Notons que $p \nmid a_n = g_d h_m$ donc $p \nmid h_m$.
Soit h_r le coefficient avec r minimal tel que $p \nmid h_r$ et remarquons que: $0 < r \leq m < n$

$$\underbrace{a_r}_{\text{div par } p} = \underbrace{g_0 h_r}_{\text{non div par } p} + \underbrace{g_1 h_{r-1} + \cdots + g_r h_0}_{\text{div par } p}$$

Donc cela mène à une contradiction.

□

Exemples

1. $p(t) = t^2 - 2$ est irréductible sur $\mathbb{Q}$ grâce à Eisenstein avec $p = 2$. Donc si $t^2 - 2$ est irréductible sur $\mathbb{Q}$, il ne peut pas s'écrire comme $\left(t - \frac{a}{b}\right)\left(t - \frac{c}{d}\right)$ avec $a, b, c, d \in \mathbb{Z}$. Cela implique directement que $\sqrt{2} \notin \mathbb{Q}$.

2. Soit $f(t) = \frac{2}{9}t^5 + \frac{5}{3}t^4 + t^3 + \frac{1}{3}$ est-il irréductible sur $\mathbb{Q}$?
   Multiplions par 9, le polynôme résultant ne sera pas le même mais le résultat d'irréductibilité ne varie pas:

   $$\tilde{f}(t) = 2t^5 + 15t^4 + 9t^3 + 3$$

   En prenant Eisenstein avec $p = 3 \implies \tilde{f}$ et donc f aussi est irréductible sur $\mathbb{Q}$.

Proposition: Critère de réduction

Soit $f \in \mathbb{Z}[t]$ primitif, $f(t) = a_n t^n + \cdots + a_0$ avec $a_n \neq 0$ et $p \nmid a_n$ un premier.
Soit $\overline{f}$ la réduction $\pmod p$ de f (c'est à dire: $\overline{f} = \sigma(f(t))$, $\sigma : \mathbb{Z}[t] \to {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\ [t]$) Alors si $\overline{f}$ est irréductible dans ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\ [t]$, f est irréductible dans $\mathbb{Q}[t]$.
La démo est à faire en exercice.

Exemple

Soit $f(t) = t^3 - t - 1$. Soit $p = 3$ alors:

x	$\overline{f}(x)$
0	-1
1	-1
2	2

$\implies$ aucun $(x - \alpha) \mid \overline{f}$. De plus $\deg \overline{f} = 3$ et si $\overline{f} = \overline{g}\overline{h} \implies \deg \overline{g} = 1$ et $\deg \overline{h} = 2$ ce qui n'est pas possible.
On a donc $\overline{f}$ irréductible dans ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\ [t] \implies f(t)$ est irréductible dans $\mathbb{Q}[t]$.

3.7 Polynômes symétriques

Soient A un anneau commutatif et $A[x_1, \ldots, x_n]$ l'anneau des polynômes en variables $x_1, x_2, \ldots, x_n$.
Un élément $\sigma \in S_n := \mathrm{Aut}(\{1, 2, \ldots, n\})$ induit un isomorphisme de $A[x_1, x_2, \ldots, x_n]$ par permutation de variables et en gardant fixe les coefficients: $\sigma(a) = a \quad \forall a \in A$

Exemple

$n = 3$ $\sigma \in S_3$:

$$\sigma(3x_1x_3 + x_1x_2x_3) = \sigma(3)\sigma(x_1)\sigma(x_3) + \sigma(x_1)\sigma(x_2)\sigma(x_3) = 3x_{\sigma(1)}x_{\sigma(3)} + x_{\sigma(1)}x_{\sigma(2)}x_{\sigma(3)} = 3x_{\sigma(1)}x_{\sigma(3)} + x_1x_2x_3$$

Définition

On dit que f est symétrique si:

$$(\sigma f)(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) \qquad \forall \sigma \in S_n$$

Exemple

$$x_1^k + x_2^k + \cdots + x_n^k \qquad k \geq 1 \quad \text{"Somme de Newton"}$$

Non-exemple

$n = 2$, $x_1^2 + x_2$ n'est pas symétrique car en prenant $\sigma = (1\ 2)$:

$$x_{\sigma(1)}^2 + x_{\sigma(2)} = x_2^2 + x_1 \neq x_1^2 + x_2$$

Exemple

$$\triangle = \prod_{1 \leq i < j \leq n} (x_i - x_j)$$

Rappelons que $\sigma\triangle = \mathrm{sgn}(\sigma)\triangle$ avec sgn : $S_n \to {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$ et $A_n := \mathrm{Ker}(\mathrm{sgn})$

Définition: Le discriminant

$D = \triangle^2$ (selon ex précédant) et D est un polynôme symétrique.

Exemple important: Polynômes symétriques élémentaires

$$\prod_{i=1}^{n}(t + x_i) = t^n + s_1(x_1, \ldots, x_n)t^{n-1} + \cdots + s_{n-1}(x_1, \ldots, x_n)t + s_n(x_1, \ldots, x_n)$$

Où $s_0 = 1$, $s_1 = x_1 + x_2 + \cdots + x_n$, $s_2 = \sum_{1 \leq i < j \leq n} x_ix_j \cdots$, $s_n = x_1x_2 \cdots x_n$

Théorème fondamental des polynômes symétriques

Soit $n \in \mathbb{N}$. Les polynômes $s_1, s_2, \ldots, s_n$ engendre l'anneau de tous les polynômes symétriques. Plus précisément:

$$\forall Q(x_1, \ldots, x_n) \quad \text{symétrique} \quad \exists P \in A[T_1, \ldots, T_n] \quad \text{tel que} \quad Q(x_1, \ldots, x_n) = P\big(s_1(x_1, \ldots, x_n), \ldots, s_n(x_1, \ldots, x_n)\big)$$

Exemple

1) $n = 2$, posons $Q = x_1^2 + x_2^2$. Essayons d'écrire Q comme combinaison linéaire de $s_1 = x_1 + x_2$ et $s_2 = x_1 x_2$:

$$Q = x_1^2 + x_2^2 = (x_1 + x_2)^2 - 2x_1 x_2$$

On obtient donc $P(T_1, T_2) = T_1^2 - 2T_2$

2) $x^2 + bx + c = (x - t_1)(x - t_2)$, on sait déjà qu'il faut résoudre $x^2 + bx + c = 0$ par viète: $t_1, t_2 = \dfrac{-b \pm \sqrt{b^2 - 4c}}{2}$
Mais calculons maintenant le discriminant:

$$D = \left(\prod_{i<j} (t_i - t_j) \right)^2 = (t_1 - t_2)^2 = \left(2\frac{\sqrt{b^2 - 4c}}{2} \right)^2 = b^2 - 4c$$

On a alors $b = t_1 + t_2$ et $c = t_1 t_2$

(Chaques expressions symétriques dans les racines peut être exprimée par les coefficients de polynômes.)

3) $x^3 - 2x^2 + x + 5 = 0$ Soient $\alpha_1, \alpha_2, \alpha_3$ les trois solutions complexes, calculer $\alpha_1^2 + \alpha_2^2 + \alpha_3^2 =: Q$
Premièrement observons qu'on peut écrire: $s_1 = \alpha_1 + \alpha_2 + \alpha_3,\ s_2 = \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3,\ s_3 = \alpha_1\alpha_2\alpha_3$ On peut donc remarquer:

$$(\alpha_1 + \alpha_2 + \alpha_3)^2 = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + 2\alpha_1\alpha_2 + 2\alpha_1\alpha_3 + 2\alpha_2\alpha_3 = Q + 2s_2 \iff Q = s_1^2 - 2s_2$$

D'autre part: $x^3 - 2x^2 + x + 5 = \prod_{i=1}^{3} (x - \alpha_i) \implies s_1 = 2,\ s_2 = 1,\ s_3 = -5 \implies Q = 2^2 - 2 \cdot 1 = 2$

4 Quelques notions algébrique importantes

4.1 Algèbre

Rappel

Un espace vectoriel sur un corps K est un groupe commutatif $(+)$ avec une multiplicattion scalaire $\cdot : K \times V \to V$. Si on remplace K par un anneau R on a la notion d'un R-module.

Exemple de Emmy Noether 1920s

$M = C^\infty(\mathbb{R})$, $R = \mathbb{R}[x]$. $(P(x), f(x)) \mapsto P(x) \cdot f(x) \in C^\infty$

Exemples

1) I un idéal (à gauche) $M = I$ est un R-Module.
2) Groupes abéliens $\iff \mathbb{Z}$-modules

Théorème structure de M type fini, R anneau principal

$$M \cong {R}\Big/{(d_1)} \oplus {R}\Big/{(d_2)} \oplus \cdots \oplus {R}\Big/{(d_n)}$$

3) V espace vectoriel sur $\mathbb{R}$ $\dim n \iff V = \mathbb{R} \oplus \cdots \oplus \mathbb{R} = \mathbb{R}^n$
4) $R = \mathbb{Z} \implies$ Classification de groupes abéliens.
5) $M = V$ un espace vectoriel, $R = \mathbb{C}[t]$, $T : V \to V$ linéaire $\implies$ forme de Jordan canonique de T.

Définition

Soient M un A-module avec A un anneau commutatif, M est une algèbre sur A s'il est muni d'un produit bilinéaire $(\cdot, \cdot) : M \times M \to M$. C'est à dire $(a_1x_1 + a_2x_2, y) = a_1(x_1, y) + a_2(x_2, y)$ et $(x, a_1y_1 + a_2y_2) = a_1(x, y_1) + a_2(x, y_2)$

Non-exemple

Le produit scalaire n'en est pas un: $M \times M \to \underline{R}$

Exemples

1) Les anneaux commutatifs
2) Les matrices avec $+, \cdot$ $(A, B) = A \cdot B$ en plus $A(BC) = (AB)C$ donc c'est une algèbre associatif.
3) L'algèbre de Lie qui n'est pas associative !
   Par exemple $M = M_n(\mathbb{R})$ les matrices $n \times n$ avec produit $(A, B) \mapsto AB - BA =: [A, B]$
   Autre sous exemple de l'algèbre de Lie:
   $\mathbb{R}^3$ avec produit vectoriel $\times$: $\begin{array}{ccc} \mathbb{R}^3 \times \mathbb{R}^3 & \longrightarrow & \mathbb{R}^3 \\ (v, w) & \longmapsto & v \times w \end{array}$ n'est pas associatif non plus:

$$(e_1 \times e_2) \times e_2 = -e_1 \neq 0 = e_1 \times (e_2 \times e_2)$$

4) Algèbre d'un groupe sur K

$$M = \left\{ \sum_{\text{fini}} a_g \cdot g \mid g \in G \; a_g \in K \right\}$$

4.2 Le produit tensoriel

Soient E et F deux espaces vectoriels sur un corps K. Soit $V = \text{Free}(E \times F)$ l'espace vectoriel sur K engendré par tout $(e, f) \in E \times F$. C'est à dire $v \in V \iff v = \sum_{\text{fini}} \lambda_i (e_i, f_i) \quad \lambda_i \in K,\ e_i \in E,\ f_i \in F$ (V est énorme, $\dim V = \infty$).
Introduisons la relation d'équivalence $\sim$ définie par:

$$(e, f) + (e', f) \sim (e + e', f) \quad \text{et} \quad (e, f) + (e, f') \sim (e, f + f') \quad \text{et} \quad c(e, f) \sim (ce, f) \quad \text{comme} \quad c(e, f) \sim (e, cf)$$

Définition: Le produit tensoriel

$$E \otimes F := \text{Free}(E \times F) \Big/ \sim$$

Les classes d'équivalences de (e, f) est dénotée $e \otimes f$. On va voir que si $\{e_i\}$ (respectivement $\{f_i\}$) base pour E (resp. F): $e_i \otimes f_j$ est une base pour $E \otimes F$ en particulier $\dim(E \otimes F) = \dim E \cdot \dim F$

Exemple

1)
$$(5e) \otimes f + (e + e') \otimes f - e' \otimes f = 5(e \otimes f) + e \otimes f + e' \otimes f - e' \otimes f = 6(e \otimes f)$$

2)
$$\vec{0} \otimes f = (0 \cdot \vec{0} \otimes f) = 0(\vec{0} \otimes f) = \vec{0} \otimes 0 \cdot f = \vec{0} \otimes \vec{0}$$

3)
$$\vec{0} \otimes \vec{0} + e \otimes f = 0(e \otimes f) + e \otimes f = (0 + 1)e \otimes f = e \otimes f$$

Proposition

Soient E et F des espaces vectoriels sur K de dimension n et m respectivement. Si $\{e_i\}_1^n$ est une base de E et $\{f_j\}_1^m$ est une base de F, alors:

$$\{e_i \otimes f_j\}_{\substack{i=1,\dots,n \\ j=1,\dots,m}} \quad \text{est une base pour} \quad E \otimes F$$

Donc en particulier $\dim(E \otimes F) = m \cdot n$. (Notons que $\dim(E \oplus F) = n + m$)

Nous ne donnerons pas de preuve ici mais on peut donner une piste:
Soient $v \in E$, $w \in F$ on considère $v \otimes w \in E \otimes F$.

$$v = \sum_{i=1}^{n} v_i e_i \quad \text{et} \quad w = \sum_{j=1}^{m} w_j f_j \implies v \otimes w = (v_1 e_1 + \cdots + v_n e_n) \otimes (w_1 f_1 + \cdots + w_m f_m) = \sum_{i,j} v_i w_j (e_i \otimes f_j)$$

4.3 Produit extérieur

$\Lambda^2(V) = {}^{V \otimes V}\big/_{\sim}$ avec $v \otimes v \sim 0 \quad \forall v$.
La classe de $v \otimes w$ est notée $v \wedge w$.

Proposition

$$x \wedge y = -y \wedge x \qquad \forall x, y \in V$$

Preuve:

$$0 = (x+y) \wedge (x+y) = x \wedge x + x \wedge y + y \wedge x + y \wedge y = x \wedge y + y \wedge x \iff x \wedge y = -y \wedge x$$

□

Exemple

$V = \mathbb{R}^2$, avec la base orthonormale e_1, e_2.

$$(5,3) \wedge (-1,2) = (5e_1 + 3e_2) \wedge (-e_1 + 2e_2) = \cdots = 10 e_1 \wedge e_2 - 3 e_2 \wedge e_1 = 13 e_1 \wedge e_2$$

Ce calcul nous montre (en rajoutant une couche de généralisation par dessus) que $\dim(\Lambda^2(\mathbb{R}^2)) = 1$ avec base $e_1 \wedge e_2$.
Si $A : V \to V$ linéaire, $A(v \wedge w) = (Av \wedge Aw)$, alors $A : \Lambda^2(V) \to \Lambda^2(V)$. Par exemple $V = \mathbb{R}^2$:

En prenant $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$$A(e_1 \wedge e_2) = Ae_1 \wedge Ae_2 = (ae_1 + ce_2) \wedge (be_1 + de_2) = \underbrace{(ad - bc)}_{\det A} e_1 \wedge e_2$$

5 Corps et théorie de Galois

Introduction

Ce chapitre devrait représenter environ 40% du cours. Une bonne référence est: *Théorie de Galois - I. Stewart.*

L'étude de solutions des équations polynômiales en utilisant les corps, extensions de corps et la théorie de groupe! On peut créditer l'origine de cette théorie à: *Éveriste Galois (1811-1832).* (Nota Bene: penser à lire une biographie de Galois, ces histoires de duels me semblent des plus intéréssantes)

Cette théorie va clarifier plusieurs points:

- Quand on peut résoudre des équations contenant $+, -, \cdot, \div, \sqrt[n]{}$
- Et aussi des problèmes géométrique datant de 2000 ans.

5.1 Nombres et équations polynomiales

Second degré

On trouva déjà il y à longtemps que la solution à $x^2 + ax + b = 0$:

$$x = -\frac{a}{2} \pm \sqrt{\frac{a^2}{4} - b}$$

Renaissance $\simeq 1500$

Formule de résolution de polynôme de degré 3, outil indispensable lors des fameux duels mathématiques de l'époque. En particulier, Fontana "Tartaglia" 1530:

$$t^3 - at^2 + bt + c = 0 \quad \text{posons} \quad t = y - \frac{a}{3}$$
$$y^3 + \underbrace{(\frac{a^3}{3} - \frac{2a^3}{3} + b)}_{p} y - \underbrace{\frac{a^3}{27} + \frac{a^2}{9} - \frac{ab}{3} + c}_{q} = 0$$

Après une petite après midi de calcul, on obtient la formule de Cardano:

$$y = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

La formule n'est clairement pas triviale et de plus pas facile à manipuler.
Il n'y a pas beaucoup de progrès jusqu'à Lagrange en 1770. Nous pouvons trouver des solutions telles pour des systèmes de degrés 2,3,4 mais les scientifiques ne trouvent rien pour les polynômes de degré 5.
Nous ponvons ici nous poser plusieures questions:

1. Est ce qu'il existe une formule pour les degrés 5,6,7,etc... ?

2. Est-ce que $\mathbb{C}$ est suffisant ? i.e: dans $\mathbb{C}$:

$$\forall P \in \mathbb{C}[t] \quad \text{on a} \quad P(t) = c(t - \alpha_1) \cdots (t - \alpha_n)$$

La première réponse est donnée par Galois (degré 5 par Abel en 1826) pour les solutions d'équations et oui, $\mathbb{C}$ est suffisant grâce au théorème fondamental d'Algèbre par Gauss-d'Alembert.

5.2 Géométrie greque classique

Toute la théorie dévellopée par Euclide dans *"Elements"* (Vu en partie en Géométrie I) On peut entre autre montrer l'impossibilité de ces construction (à la règle et au compas):

- Trisection d'un angle.
- Quadrature du cercle.
- Doubler le volume du cube.

En 1882 Lindemann a montré que π est transendant.

5.3 Extensions de corps

Définition/Rappel

F est un sous-corps de E si F est un sous ensemble de E et F forme un corps avec les mêmes opérations $+$, $\cdot$ que sur E. On pourra noter cela comme E/F (pour E est une extension de F, ce sera une notion très importante dans la suite du cours)

Exemples

1. $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$
2. $\mathbb{F}_p \subset \mathbb{F}_p[x] \Big/ \big(f(x)\big)$, où f est un polynôme irréductible.

Proposition

Tout sous-corps de $\mathbb{C}$ contient $\mathbb{Q}$.

Preuve:
Soit un sous-corps $K \subset \mathbb{C}$ alors $0, 1 \in K$, donc $n = 1 + 1 + \cdots + 1 \in K$ aussi. Nous avons donc $\mathbb{Z} \in K$, mais comme K se doit d'être un corps il faut qu'il contienne les inverses n^{-1}. L'inverse de $k \in \mathbb{Z}$ est $\frac{1}{k}$ et donc $\frac{a}{b} \in K$ ce qui implique $\mathbb{Q} \subset K$.

□

Soit E/F. On peut alors voir E comme un espace vectoriel sur F. Pour plus rentrer en détail:
$(E, +)$ un groupe additif alors prenons la multiplication scalaire comme : $\begin{array}{ccc} F \times E & \longrightarrow & E \\ (f, e) & \longmapsto & f \cdot e \end{array}$. Ces deux opérations respectent bien tous les axiomes d'un espace vectoriel car ils sont les mêmes que pour E un anneau ou un corps.

Définition: Extension finie

On dit que E est une extension finie si $\dim_F E$ est finie.

Remarque: $\dim_F E$ est souvent noté $[E : F]$, le degré de l'extension E sur F.

Exemples

1. $\mathbb{C} \supset \mathbb{R}$, base: $\{1, i\}$ où $i^2 = -1$, $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$. Donc $[\mathbb{C} : \mathbb{R}] = 2$.
2. Par contre on notera que $[\mathbb{R} : \mathbb{Q}] = \infty$

   ⌜

   $\mathbb{Q}$ est dénombrable, donc $\mathbb{Q}^n$ l'est aussi $\forall n$, mais $\mathbb{R}$ n'est pas dénombrable, i.e. on ne peut pas donner une base de $\mathbb{R}$ finie avec des éléments de $\mathbb{Q}$.

   ⌟
3. $\left[\mathbb{F}_p[x] \Big/ \big(f(x)\big) \ : \mathbb{F}_p \right] = \deg f$ avec f irréductible.
4. $$[E : F] = 1 \iff E = F$$

Proposition: La loi multiplicative

Soit $E_2 \supset E_1 \supset F$, alors:

$$[E_2 : F] = [E_2 : E_1] \cdot [E_1 : F]$$

(Démo en exercice).

Définition

Soit un sous-ensemble $S \subset K$ et $F \subset K$ un corps.
Alors $F(s)$ est le corps le plus petit qui contient F et S. Plus formellement il est obtenu comme:

$$F(s) := \bigcap_{\substack{\text{sous-corps } E \\ F,S \subset E \subset K}} E$$

Donc l'intersection de tout les sous corps qui contiennent F et S. Nous avons notamment si $S = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$: $E = F(\alpha_1, \ldots, \alpha_n)$ qu'on appelle le corps engendré par $\alpha_1, \ldots, \alpha_n$ sur F. Ou encore on peut dire que E est l'extension de F par l'ajout de $\alpha_1, \ldots, \alpha_n$.

Exemples

1. $\mathbb{Q}(i) = \{a + ib \mid a, b \in \mathbb{Q}\}$ car $i^2 = -1 \in \mathbb{Q}$.

2. $\mathbb{Q}\left(\sqrt[3]{5}\right) = \left\{a + \sqrt[3]{5} \cdot b + 5^{2/3} \cdot c \mid a, b, c \in \mathbb{Q}\right\}$ car $(\sqrt[3]{5})^2 = 5^{2/3} \notin \mathbb{Q}$ et $(\sqrt[3]{5})^3 = 5 \in \mathbb{Q}$.

3. $\big(\mathbb{Q}(i)\big)(\sqrt{5}) = \mathbb{Q}(i, \sqrt{5})$, en effet nous avons $i^2 = -1$, $\sqrt{5}^2 = 5$, $(i\sqrt{5})^2 = -5$. Nous pouvons donc poser $\{1, i, \sqrt{5}, i\sqrt{5}\}$ comme base. Et donc $[\mathbb{Q}(i, \sqrt{5}) : \mathbb{Q}] = 4$.

4. $\mathbb{Q}(i, -i, \sqrt{5}, -\sqrt{5}) = \mathbb{Q}(i + \sqrt{5})$.

   ⌜

   D'abord, il est clair que $\mathbb{Q}(i, -i, \sqrt{5}, -\sqrt{5}) = \mathbb{Q}(i, \sqrt{5})$ car chaque corps doit contenir son inverse.
   Il semble aussi évident que $\mathbb{Q}(i+\sqrt{5}) \subset \mathbb{Q}(i, \sqrt{5})$, mais est ce que l'autre inclusion est vraie ? Faisons quelques calculs:
   Notons que $(i + \sqrt{5}) \in \mathbb{Q}(i + \sqrt{5}) \implies (i + \sqrt{5})^2 \in \mathbb{Q}(i + \sqrt{5})$ et aussi $(i + \sqrt{5})^3 \in \mathbb{Q}(i + \sqrt{5})$ donc:

   $$\begin{aligned}(i + \sqrt{5})^2 &= -1 + 2i\sqrt{5} + 5 = 4 + 2i\sqrt{5} \in \mathbb{Q}(i + \sqrt{5}) \\ (i + \sqrt{5})^3 &= (i + \sqrt{5})(4 + 2i\sqrt{5}) = 14i + 2\sqrt{5} \in \mathbb{Q}(i + \sqrt{5}) \\ &\implies 14i + 2\sqrt{5} - 2(i + \sqrt{5}) = 12i \in \mathbb{Q}(i + \sqrt{5})\end{aligned}$$

   Et donc $\pm i \in \mathbb{Q}(i + \sqrt{5})$

   Alors on obtient naturellement:

   $$i - (i + \sqrt{5}) = -\sqrt{5} \in \mathbb{Q}(i + \sqrt{5})$$

   ⌟

Définition

Soit E/F. Un element $\alpha \in E$ est algébrique sur F s'il existe un polynôme $f \in F[t]$ tel que $f(\alpha) = 0$.

Définition

Si tout $\alpha \in E$ est algébrique sur F on dit que l'extension E/F est algébrique.

Exemple

$\mathbb{C}$ est algébrique sur $\mathbb{R}$. Soit $\alpha \in \mathbb{C}$, alors:

$$f(t) = (t-\alpha)(t-\overline{\alpha}) = t^2 - (\alpha+\overline{\alpha})t + |\alpha|^2 = t^2 - 2\cdot\Re(\alpha)t + |\alpha|^2 \in \mathbb{R}[t]$$

Définition

Soit $\alpha \in E$. S'il n'existe aucun $P \in F[t]$ tel que $P(\alpha) = 0$, alors on dit que α est transcendant sur F.

Exemples

Algébrique: $\sqrt{2},\ \sqrt[3]{4},\ \sqrt[7]{\sqrt{2}+\sqrt{5}}$ etc...

Transcendants: $\displaystyle\sum_{n=1}^{\infty} 10^{-n!},\ \pi,\ e$ aussi a^b si a est algebrique $\neq 0, 1$ et b algébrique mais pas rationel. Ce sont des preuves difficiles la plupart du temps.

Inconnus: $\pi + e,\ \pi e,\ \pi^\pi,\ \gamma = \lim_{n\to\infty}\left(\sum_{k=1}^{n}\frac{1}{k} - \log n\right)$ et plein plein d'autres exemples.

Proposition

Si $[E : F] < \infty$, alors tous $\alpha \in E$ est algébrique.

Preuve:
Soit $\alpha \in E$.
$\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ ne peut pas être linéairement indépendant si $n > [E : F]$ $(= \dim_F E)$. Donc $\exists a_1, \ldots, a_n$ dans F pas tous nuls tels que:

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

Dit autrement: $P(t) = a_n t^n + \cdots a_1 t + a_0 \in F[t]$ avec $P(\alpha) = 0$ donc α est algébrique.

□

Définition

Soit L/K une extension de corps. On dit que L/K est (une extension) simple si $L = K(\alpha)$ pour un certain $\alpha \in L$.

Exemples

1. $\mathbb{R}/\mathbb{Q}$ n'est pas simple car $\{1, \alpha, \alpha^2, \ldots\}$ engendre un corps dénombrable.
2. $\mathbb{C}/\mathbb{R}$ est simple car $\mathbb{C} = \mathbb{R}(i)$ où $i^2 = -1$
3. On a vu que, en fait, $\mathbb{Q}(i, \sqrt{5})$ est simple car égal à $\mathbb{Q}(i + \sqrt{5})$.

Définition

Un corps K est algébriquement clos si $\forall P \in K[t]$, $\deg P \geq 1$, a une racine dans K. Une formulation équivalente est qu'on peut reécrire tout $P \in K[t]$ comme:

$$P(t) = c \cdot \prod (t - \alpha_i),\ \alpha_i \in K$$

Théorème: Clôture Algébrique

Pour tout corps K, $\exists \overline{K} \supset K$ qui est algébriquement clos (si K' algébrique sur K, il est unique).

Nous ne verrons pas la démonstration dans ce cours. C'est une construction abstraite en général. Par contre il est important de connaître le résultat suivant:
Par le théorème fondamental de l'algèbre, nous avons que $\mathbb{C}$ est algébriquement clos.

5.4 Extension algébriques

Rappel

- α est algébrique sur F si $\exists P \in F[t]$ tel que $F(\alpha) = 0$.
- E/F est algébrique si tout $\alpha \in E$ est algébrique.
- Si $[E : F] < \infty$, alors E est algébrique.

À noter que nous avons montré le résultat suivant:

Corollaire

Si α et β sont algébrique sur F, alors $\alpha\beta$, $\dfrac{\alpha}{\beta}$, $\alpha + \beta$, $\alpha - \beta$ le sont aussi.

Preuve:
$\alpha\beta$, $\dfrac{\alpha}{\beta}$, $\alpha + \beta$, $\alpha - \beta \in F(\alpha, \beta)$.

$$\begin{aligned}[F(\alpha,\beta) : F] &= \underbrace{[F(\alpha,\beta) : F(\beta)]}_{=[(F(\beta))(\alpha):F(\beta)]} \cdot \underbrace{[F(\beta) : F]}_{<\infty} \\ &\leq [F(\alpha) : F] < \infty\end{aligned}$$

Et donc $F(\alpha, \beta)$ est algébrique.

□

Remarque

Soient $\alpha = \sqrt{2}$, $\beta = \sqrt[4]{3}$, il est pas si facile de trouver un polynôme $P \in \mathbb{Q}[t]$ tel que $P(\alpha \cdot \beta) = 0$, mais grâce à ce corollaire nous connaissons son existence et la démonstration fut facile et abstraite.

Proposition

Soit α algébrique sur F. Soit J l'idéal de tout les polynômes qui ont α comme racine, i.e.:

$$J := \{P \in F[t] \mid P(\alpha) = 0\}$$

Soit $p(t)$ tel que $J = (p(t))$, alors p est irréductible. (l'idéal est engendré par un élément générateur car nous travaillons dans un anneau euclidien)

Démonstration:
Supposons que $p = gh$ avec $\deg g < \deg p$, $\deg h < \deg p$. $p(\alpha) = 0$ implique que:
Soit $g(\alpha) = 0$, soit $h(\alpha) = 0$. Sans perte de généralité disons $g(\alpha) = 0$. Mais $\deg g < \deg p$, et $g \in J$. Ce n'est pas possible car $J = (p)$. ↯

□

Définition

Soit α algébrique. Le polynôme P avec degré minimal et unitaire (c'est à dire $P(t) = t^n + a_{n-1}t^{n-1} + \cdots$) tel que $P(\alpha) = 0$ s'apelle le polynôme minimal de α.

Corollaire

$J = (\text{ Poly-minimal })$, donc P est irréductible et unique (grâce à la condition "unitaire").

Preuve:
Prenons le polynôme p de la preuve précédente tel que $J = (p)$. Nous avons donc p de degré minimal et irréductible. Par division par une constante on peut supposer que p est unitaire. Soit p et g polynômes minimaux de α. Alors:

$$f(t) := p(t) - g(t) = t^n + a_{n-1}t^{n-1} + \cdot - (t^n + b_{n-1}t^{n-1} + \cdots) = (a_{n-1} - b_{n-1})t^{n-1} + \cdots$$

En particulier $f(\alpha) = p(\alpha) - g(\alpha) = 0$ et $\deg f \leq n-1$, contradiction avec la minimalité sauf si $p = g$.

□

Rappel important

Soit K un corps et $f \in K[t]$ irréductible. Soit α une racine de f (dans un corps plus grand, par exemple une clôture algébrique). Alors:
$[K(\alpha) : K] = \deg f$ et alors $K(\alpha) \cong {K[x]}/{(f(x))}$ par $\alpha \to$ classe d'équiv de x. Une base de $K(\alpha)/K$ serait $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ où $d = \deg f$.

Exemples

1. $\mathbb{Q}(i)$, $f(x) = x^2 + 1$, possède comme base $\{1, i\}$, car i est racine de f.

2. $\mathbb{C} = \mathbb{R}(i)$, toujours avec $f(x) = x^2 + 1$.

6 Galois: Application à la géométrie classique

Simplement avec les quelques notions que nous avons introduites jusque ici, nous pouvons arriver à des conclusions impressionantes. Des questions qui ont pues rester sans réponses sur des périodes de plus de 1000 ans.

6.1 Algébrification

Nous avons déjà abordé le sujet durant l'introduction, Euclide, Platon et aussi Dante...
Soit P_0 un ensemble fini de points dans $\mathbb{R}^2$. On possède deux opération qui nous semblent naturelles:

La règle: Elle nous permet, de construire la droite passant par deux points.

Le compas: Il permet quant à lui de dessiner le cercle dont le centre est dans P_0 et de rayon $d(p,q)$ où $p,q \in P_0$. Cette construction semble, à priori, plus générale que l'outil classique du compas mais il est en fait équivalent.

Définition

On dit que un point r est constructible dans une étape de P_0 si r est l'intersection de deux droites et cercles avec P_0.

Nous avons plus généralement:

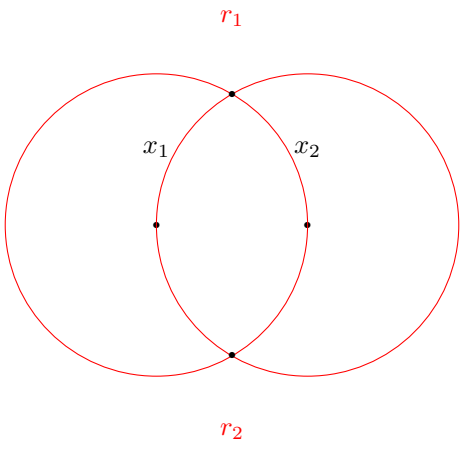
Définition

r est constructible de P_0 si $\exists r_1, r_2, \ldots, r_n = r$ où r_i est constructible d'une étape de $P_0 \cup \{r_1, \ldots, r_{i-1}\}$

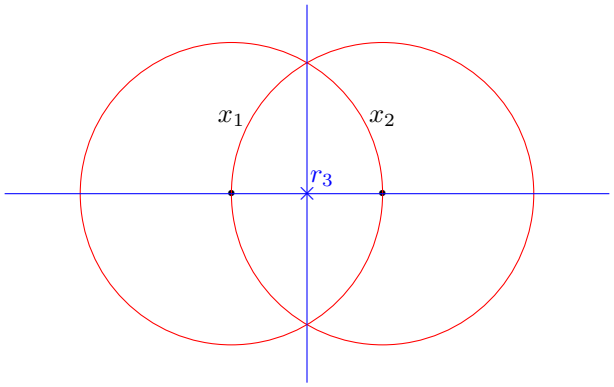
Exemple

Commençons avec 2 points $x_1,\ x_2$.

Traçons à la première étape l'intersection de deux cercles:



On peut ensuite dans une dernière étape tracer les droites passant par (x_1, x_2) et (r_1, r_2):



Voici la version algébrique du problème:
Soit $P_0 = \{p_1, \ldots, p_n\}$ avec les coordonnées $p_i = (x_i, y_i)$. Soit $K_0 = \mathbb{Q}(x_1, y_1, \ldots, x_n, y_n) \subset \mathbb{R}$ Une extension de corps de $\mathbb{Q}$.
Soit encore $K_j = K_{j-1}(z_j, w_j)$, $r_j = (z_j, w_j)$, nous avons donc la chaîne suivante:

$$\mathbb{Q} \subset K_0 \subset K_1 \subset K_2 \subset \cdots \subset \mathbb{R}$$

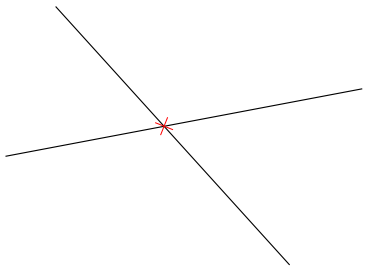
6.2 Critère de constructibilité

Lemme principal

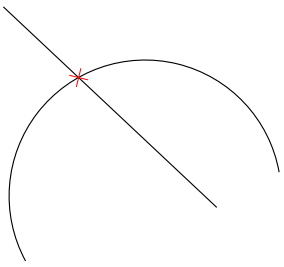
Soit $r_j = (z_j, w_j)$ construit par une étape de $P_0 \cup \{r_1, \ldots, r_{j-1}\}$. Alors z_j et w_j sont des racines dans K_j d'un polynôme quadratique sur K_{j-1}

Preuve:
Nous avons trois cas à considérer:

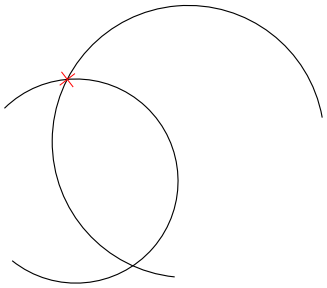
a)



b)



c)



a) Si nous avons une droite reliant (p, q) et (r, s), et un poit (x, y) sur cette droite, alors l'égalité suivante est respectée:

$$\frac{x-p}{r-p} = \frac{y-q}{s-q}$$

Nous pouvons isoler $y = f(x)$ où f est de degré 1. De même pour l'autre droite nous avons une relation similaire et nous pouvons ensuite substituer y:

$$\frac{x-\tilde{p}}{\tilde{r}-\tilde{p}} = \frac{y-\tilde{q}}{\tilde{s}-\tilde{q}} = \frac{\frac{x-p}{r-p}(s-q)+q-\tilde{q}}{s-\tilde{q}}$$

Nous obtenons donc une équation linéaire pour x, il suffit donc de multiplier avec y pour avoir une équation quadratique (même procédé pour y)

OK

b)

$$\begin{cases} \dfrac{x-p}{r-p} = \dfrac{y-q}{s-q} \\ (x-t)^2 + (y-u)^2 = w^2 \end{cases} \implies (x-t)^2 + \left(\frac{(x-p)(s-q)}{(r-p)} + q - u\right)^2 = w^2$$

C'est une équation de degré 2 avec coefficients dans K_{j-1}, même chose pour y

OK

c) Commençons avec les deux équations de cercles:

$$\begin{cases} (x-t)^2 + (y-u)^2 = w^2 & (1) \\ (x-\tilde{t})^2 + (y-\tilde{u})^2 = \tilde{w}^2 & (2) \end{cases}$$

En soustrayant (2) à (1): (1) - (2) $\implies$ $y =$ une expression de degré 1 en x. Il suffit ensuite de substituer dans (1) et cela donne une équation de degré 2 pour x avec coefficients dans K_{j-1}, de même pour y.

OK

□

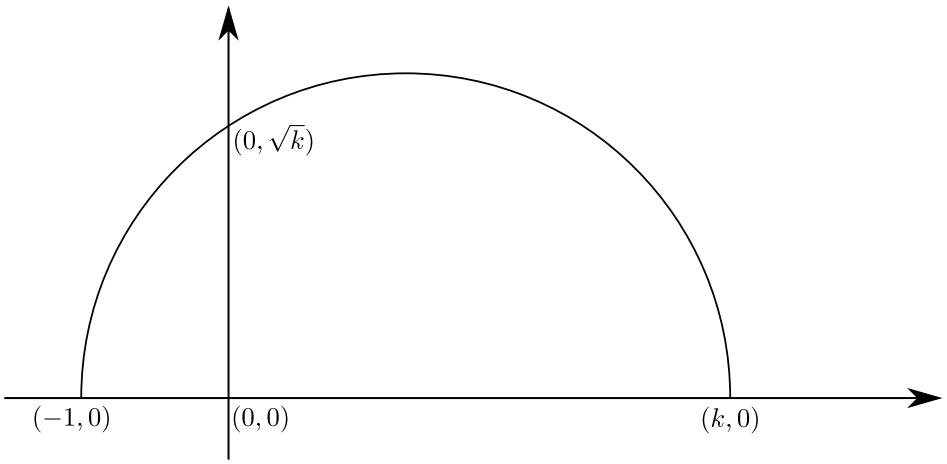
Théorème

Si $r = (x, y)$ est constructible de P_0 et K_0 est le corps engendré par les coordonées de points de P_0. Alors il existe une suite d'extensions de corps:

$$K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n$$

Où toutes extensions sont de degré 2 tel que $x, y \in K_n$. En particulier $[K_0(x) : K_0]$ et $[K_0(y) : K_0]$ sont des puissances de 2.

Remarque La réciproque est aussi vraie, le degré des extensions est de 2 $\implies$ constructible. On ne donnera pas de preuve ici mais on peut penser à la construction géométrique suivante:



$$\left(x - \frac{k-1}{2}\right)^2 + y^2 = \left(\frac{k+1}{2}\right)^2 \quad \text{et} \quad \frac{(k-1)^2}{4} + y^2 = \frac{(k+1)^2}{4}$$

$$\implies y^2 = -\frac{k^2 - 2k + 1}{4} + \frac{k^2 + 2k + 1}{4} = \frac{4k}{4} = k$$

Preuve du théorème

Pour un corps F, α racine de $f(t) \in F[t]$ de degré 2, alors $[F(\alpha) : F] = 1$ ou 2. deg $= 1 \iff \alpha \in F$ donc ce n'est pas une extension, on peut oublier.
Par le Lemme, $[K_{j-1}(x_j) : K_{j-1}] = 1$ ou 2 montre l'existence de la suite $K_0 \subset K_1 \subset \cdots \subset K_n$.
Puis par la loi de multiplication nous avons:

$$2^\ell = [K_n : K_0] = [K_n : K_0(x)][K_0(x) : K_0] \implies [K_0(x) : K_0] = 2^k$$

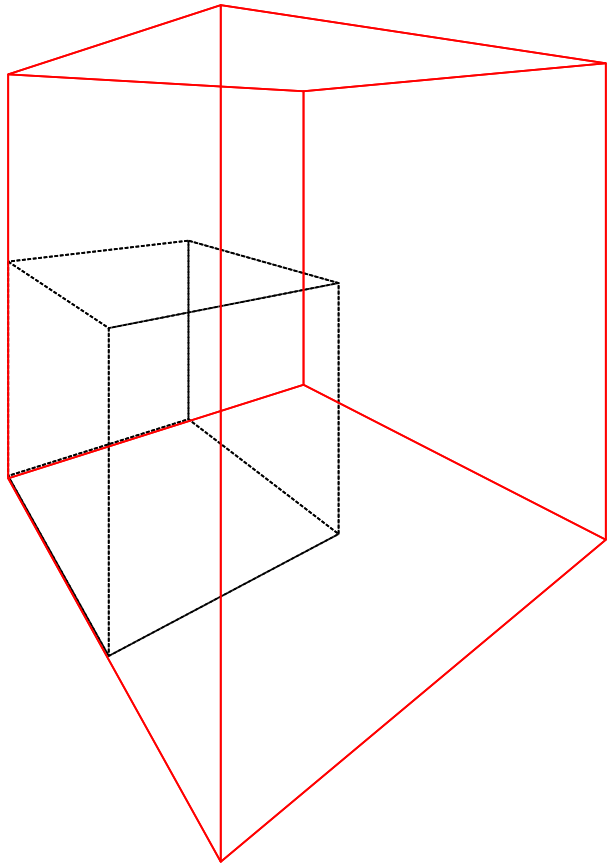
□

6.3 Application à l'impossibilité de certaines constructions

Problème 1

Théorème: Wantzel (1837)

Le cube ne peut pas être dupliqué.
Démonstration:
Considérons l'image:



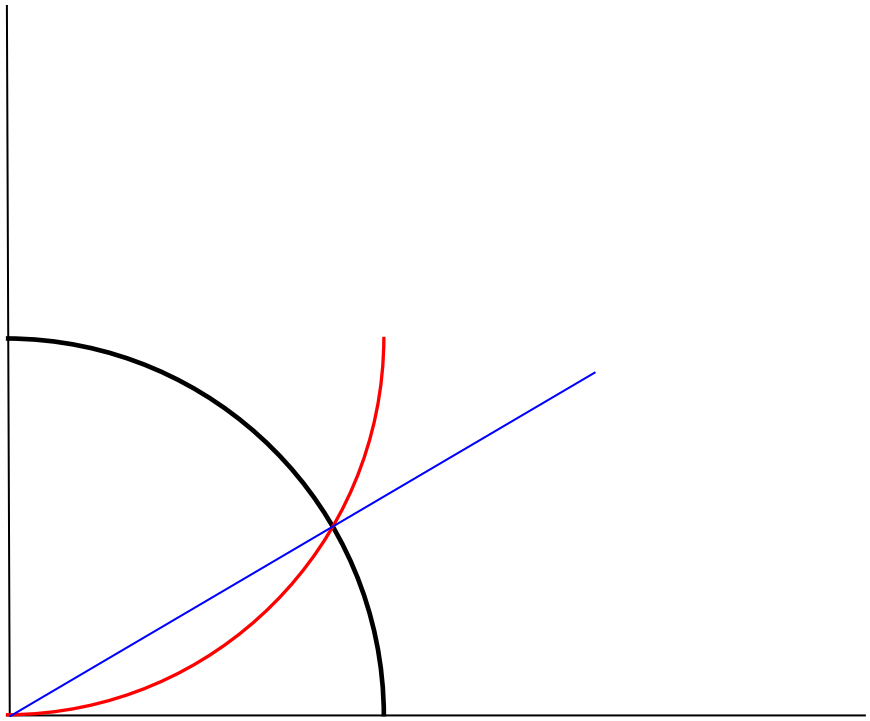
Le cube noir est de volume 1 et son le coin gauche est centré en $(0,0,0)$. Si le cube rouge est de volume double, le coin le plus proche doit être de coordonée $(\sqrt[3]{2},0,0)$, d'où le raisonnement qui suit.

Pour le volume 1, $K_0 = \mathbb{Q}$. Pour doubler le volume nous devons construire le nombre $\sqrt[3]{2}$ car $(\sqrt[3]{2})^3 = 2$.
Mais il n'est pas possible de construire $\sqrt[3]{2}$ car $t^3 - 2$ est irréductible dans $\mathbb{Q}$ (par exemple en utilisant le critère d'Eisenstein avec $p = 2$). C'est donc le polynôme minimal et aussi: $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Donc d'après notre théorème on ne peut pas construire ce nombre.

□

Problème 2: Trisection d'angle

La trisection d'angle est parfois possible, par exemple avec $\theta := \frac{\pi}{2}$:



Théorème: Wantzel

On ne peut pas trisecter l'angle $\frac{\pi}{3}$

Démonstration:

Prenons l'angle $\frac{\pi}{3}$ et l'intersection de la droite de ce même angle avec le cercle trigonométrique. Ce point p aura pour coordonée:
$p = (\cos\frac{\pi}{9}, \sin\frac{\pi}{9})$, notons $\alpha := \cos\frac{\pi}{9}$, peut on le construire ?

Rappel: $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$. Si $\theta = \frac{\pi}{9}$ on a:

$$\frac{1}{2} = 4\cos^3\frac{\pi}{9} - 3\cos\frac{\pi}{9} \implies 8t^3 - 6t - 1 = 0$$
$$\overset{x=2t}{\Longrightarrow} x^3 - 3x - 1 = 0 \overset{x=y+1}{\Longrightarrow} (y+1)^3 - 3(y+1) - 1 = y^3 + 3y^2 + 3y + 1 - 3y - 3 - 1 = y^3 + 3y^2 - 3$$

On à bien que c'est un polynôme irréductible par Eisenstein avec $p = 3 \implies [\mathbb{Q}(\cos\frac{\pi}{9}) : \mathbb{Q}] = 3$, ce qui n'est pas possible par le théorème vu précédemment.

Petit récapitulatif: Les points donné sont $P_0 = \{(0,0),\ (1,0),\ (\cos\frac{\pi}{3})\ \sin\frac{\pi}{3}\}$ Donc, en vue que $\cos\frac{\pi}{3} = \frac{1}{2}$ et $\sin\frac{\pi}{3} = \frac{\sqrt{3}}{2}$, notre corps de départ est

$$K_0 = \mathbb{Q}(\sqrt{3})$$

qui est une extension du corps $\mathbb{Q}$ de degé 2. La preuve montre qu'ajouter $\alpha := \cos\frac{\pi}{9}$ à $\mathbb{Q}$ est une extension de degré 3. Comme 2 et 3 sont premiers entre eux, $\mathbb{Q}(\sqrt{3}, \alpha)$ est forcement une extension de degré 6 à $\mathbb{Q}$ (loi de multiplication de degré) et alors $[K_0(\alpha) : K_0] = 3$. Contradiction au théorème.

□

Remarque

Avec des origamis, on peut trisecter tout les angles. Donc en particulier, les nipons étaient vachement meilleurs que nous autre occidentaux.

Problème 3

Théorème: Quadrature du cercle

La quadrature du cercle est impossible.

Démonstration:
Pour construire un carré de même aire que le cercle unité, il faut construire le nombre $\sqrt{\pi}$, mais Lindeman à montré en 1880s que π est transcendant. Donc en particulier: $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$ et $\mathbb{Q}(\sqrt{\pi}) \supset \mathbb{Q}(\pi)$, pas de chance pour la quadrature.

□

Petit aparté

Pierre Laurent Wantzel: Mini Bio

Pierre Laurent Wantzel (5 June 1814 in Paris – 21 May 1848 in Paris) was a French mathematician who proved that several ancient geometric problems were impossible to solve using only compass and straightedge.

In a paper from 1837, Wantzel proved that the problems of 1 doubling the cube, and 2 trisecting the angle are impossible to solve if one uses only compass and straightedge. In the same paper he also solved the problem of determining which regular polygons are constructible: 1 a regular polygon is constructible if and only if the number of its sides is the product of a power of two and any number of distinct Fermat primes (i.e. that the sufficient conditions given by Carl Friedrich Gauss are also necessary)

> *"Ordinarily he worked evenings, not lying down until late; then he read, and took only a few hours of troubled sleep, making alternately wrong use of coffee and opium, and taking his meals at irregular hours until he was married. He put unlimited trust in his constitution, very strong by nature, which he taunted at pleasure by all sorts of abuse. He brought sadness to those who mourn his premature death."*
>
> —Adhémar Jean Claude Barré de Saint-Venant, on the occasion of Wantzel's death.

Petit moment culture: Dante

Nel mezzo del cammin di nostra vita
mi ritrovai per una selva oscura
ché la diritta via era smarrita.
...
"Qual è 'l geomètra che tutto s'affige
per misurar lo cerchio, e non ritrova,
pensando, quel principio ond' elli indige,
tal era io a quella vista nova:
veder voleva come si convenne
l'imago al cerchio e come vi s'indova;
ma non eran da ciò le proprie penne:
se non che la mia mente fu percossa
da un fulgore in che sua voglia venne.
A l'alta fantasia qui mancò possa;
ma già volgeva il mio disio e 'l velle,
sì come rota ch'igualmente è mossa,
l'amor che move il sole e l'altre stelle."

Dante, Paradiso XXXIII.

C'était à la moitié du trajet de la vie;
Je me trouvais au fond d'un bois sans éclaircie,
Comme le droit chemin était perdu pour moi.
Ah ! que la retracer est un pénible ouvrage,
Cette forêt épaisse, âpre à l'œil et sauvage,
Et dont le seul penser réveille mon effroi !
Tâche amère ! la mort est plus cruelle à peine;
Mais puisque j'y trouvai le bien après la peine,
Je dirai tous les maux dont j'y fus attristé.

Je ne sais plus comment j'entrai dans ce bois sombre,
Tant pesait sur mes yeux le sommeil chargé d'ombre,
Lorsque du vrai chemin je m'étais écarté.
Mais comme j'atteignais le pied d'une colline,
Au point où la vallée obscure se termine,
Qui d'un si grand effroi m'avait poigné le cœur,
...
As the geometer intently seeks
to square the circle, but he cannot reach,
through thought on thought, the principle he needs,
so I searched that strange sight: I wished to see
the way in which our human effigy
suited the circle and found place in it—
and my own wings were far too weak for that.
But then my mind was struck by light that flashed
and, with this light, received what it had asked.
Here force failed my high fantasy; but my
desire and will were moved already—like
a wheel revolving uniformly—by
the Love that moves the sun and the other stars.

7 Théorie de Galois: Plongements

Ce chapitre est un peu abstrait, mais nous avons pu voir avec les constructions géométriques que les bonnes notions au bon moment peuvent s'averer puissantes. L'avis personnel: Les idées que l'on va développer font partie des plus importantes du 20ème siècle mathématique.

7.1 Morphismes de corps

Soit K_1 et K_2 deux corps. Une application $\sigma : K_1 \to K_2$ est un morphisme si elle préserve les opérations, en particulier: $\sigma(0) = 0$, $\sigma(1) = 1$ et $\sigma(x+y) = \sigma(x) + \sigma(y)$, $\sigma(xy) = \sigma(x)\sigma(y)$.
Le noyau, $\operatorname{Ker}\sigma$ est alors un idéal. Nous savons aussi que tout idéal d'un corps est trivial, i.e. $I \subset K$ un idéal alors $I = \{0\}$ ou K. Mais donc nous avons $\sigma(1) = 1 \neq 0$ et alors $\operatorname{Ker}\sigma = 0$, c'est à dire, σ est toujours injectif.
Nous pouvons aussi le prouver directement en posant: $\sigma(x) = \sigma(y) \iff \sigma(x) - \sigma(y) = 0 \iff \sigma(x-y) = 0$ et alors si $x \neq y$ nous avons:

$$1 = \sigma(1) = \sigma((x-y)^{-1} \cdot (x-y)) = \sigma((x-y)^{-1}) \cdot \underbrace{\sigma(x-y)}_{=0} = 0 \quad \lightning$$

C'est pour cette raison que nous appelons σ un plongement de K_1 dans K_2.

Nous avons aussi que σ est un isomorphisme s'il existe un morphisme σ^{-1}. Dans le cas des corps, il est suffisant de vérifier que σ est surjectif. En particulier $\sigma(K_1) \subset K_2$ est un sous-corps isomorphe à K_1.

Rappel

- ${K[t]}/{(p(t))}$ est un corps si et seulement si p est irréductible.
- Soit α une racine de p (avec du coup p le polynôme minimal de α à une constante multiplicative)
  $\sigma : \begin{array}{ccc} K[t] & \longrightarrow & K(\alpha) \\ f(t) & \longmapsto & f(\alpha) \end{array}$, en particulier: $\begin{array}{ccc} t & \to & \alpha \\ k & \to & k \end{array} \quad \forall k \in K.$

  On peut noter que $\operatorname{Ker}\sigma = \{f(t) \mid f(\alpha) = 0\} = (p)$ et donc $\sigma : {K[t]}/{(p)} \to K(\alpha)$ est un isomorphisme.

Observation importante

Soit p irréductible et $\alpha,\ \beta$ deux racines, alors d'après la proposition on obtient:

$$K(\alpha) \cong {K[t]}/{(p(t))} \cong K(\beta)$$

Exemple

$K = \mathbb{Q}$, $p(x) = x^4 - 2$, de racines: $\pm\sqrt[4]{2},\ \pm i\sqrt[4]{2}$, alors $\mathbb{Q}(\sqrt[4]{2}) \cong \mathbb{Q}(i\sqrt[4]{2})$.

Proposition

Soit α transcendant sur K. Alors $K(\alpha) \cong K(t)$ les fonctions rationelles (= corps des fractions de $K[t]$).

Preuve:
Nous avons $\varphi : F(t) \to F(\alpha)$, $\varphi\left(\dfrac{f(t)}{g(t)}\right) = \dfrac{f(\alpha)}{g(\alpha)}$.
Rappelons que $K(t) = \left\{ \dfrac{f(t)}{g(t)} \,\middle|\, f, g \in K[t],\ g \neq 0 \right\}$ où la division dénote les classes d'équivalence modulo la division.

Si $g(t) \neq 0$, c'est à dire pas de polynôme nul, alors $g(\alpha) \neq 0$ car α est transcendant. Donc φ est bien défini et préserve les opération $+, -, \cdot, \div$.

L'application est bien surjective: $k \in K$: $\varphi\left(\frac{k}{1}\right) = \frac{k}{1} = k$

Elle est aussi injective car nous travaillons avec des corps. Et alors φ est un isomorphisme.

□

Exemples

1. $\mathbb{R}[t]\Big/(t^2+1) = \mathbb{R}(i) = \mathbb{C}$.
2. $\mathbb{Q}[t]\Big/(t^2-2) = \mathbb{Q}(\sqrt{2})$
3. Soit $\mathbb{F}_2$ et $p(x) = x^3 + x + 1$, p est irréductible car $p(0) = 0 + 0 + 1 \neq 0$ et $p(1) = 1^3 + 1 + 1 = 1 \neq 0$. Donc $\mathbb{F}_2[x]\Big/(p(t))$ est un corps à 8 éléments. $\mathbb{F}_2(\alpha) = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{F}_2\}$ avec $\alpha^3 = -\alpha - 1$.

Proposition

$[L : K] < \infty$ si et seulemet si L/K est algébrique et $\exists \alpha_1, \ldots, \alpha_s$ tels que $L = K(\alpha_1, \ldots, \alpha_s)$

Preuve:

($\Rightarrow$) Déjà vu: dim $< \infty$ donc $\exists$ un nombre fini de "vecteurs"/éléments linéaires inidépendant. Il suffira d'ajouter $\alpha_1, \alpha_2, \ldots$ si besoin.

($\Leftarrow$) Loi de tours/multiplication de degré, chaque $[K_j(\alpha_{j+1}) : K_j] < \infty$ car α_{j+1} est algébrique sur K.

□

7.2 Extensions de plongements

Une question générale et importante à nous poser est si $\sigma : K \subset E \to L$ un plongement. Existe-t-il un plongement $\tau : E \to L$ tel que $\tau \mid_K = \sigma$?
Prenons par exemple $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \to \mathbb{C}$. Nous avons deux possibilités, prendre la fonction identité ou encore la fonction "conjugaison", c'est à dire $\sqrt{2} \mapsto -\sqrt{2}$.

Commençons par noter que les sous corps caractéristique (Soit $\mathbb{Q}$ soit $\mathbb{F}_p$) sont toujours fixés par automorphismes $K \to K$. Supposons que K est de caractéristique nulle, c'est à dire: $\underbrace{1+1+\cdots+1}_{n} \neq 0 \quad \forall n$. Alors $\mathbb{Z} \subset K$, donc $\mathbb{Q} \subset K$. Soit $\sigma : K \to K$ un automorphisme. Comme $1 \mapsto 1$, alors $n \mapsto n$ et alors $\frac{a}{b} \mapsto \frac{a}{b}$, c'est à dire que $\mathbb{Q}$ est fixé point par point.

Exemple

$K = \mathbb{Q}(\sqrt{2})$, avec base $\{1, \sqrt{2}\}$, $K = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Soit alors $\sigma : K \to K$ un plongement donc:

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

Il nous faut alors trouver $\sigma(\sqrt{2}) =?$. Quelles sont les possibilités qui s'ouvrent à nous ?

$$0 = \sigma(0) = \sigma(\sqrt{2}^2 - 2) = \sigma(\sqrt{2})^2 - 2 \implies \sigma(\sqrt{2}) = \pm\sqrt{2}$$

Nous avons donc ces deux choix, σ sujectif implique σ un automorphisme et alors: $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})) = \{id, \tau\}$ où $\tau(a + b\sqrt{2}) = a - b\sqrt{2}$

Proposition

Soit $\sigma : K \to L$ un plongement. Si $p(t) \in K[t]$ possède une racine α alors $(\sigma p)(t)$ a comme racine $\sigma(\alpha)$

Démonstration:

$$0 = \sigma(p(\alpha)) = \sigma(a_n\alpha^n + \cdots + a_1\alpha + a_0) = \sigma(a_n)\sigma(\alpha)^n + \cdots + \sigma(a_0) = \big(\sigma p\big)(\sigma(\alpha))$$

□

Proposition: Extension de plongements

Soient F, L, $E = F(\alpha)$ des corps avec α algébrique sur F, et $\sigma : F \to L$ un plongement. Soit p le polynôme minimal de α sur F. Si β est une racine de $\sigma(p)$ dans L alors $\exists \tau : F(\alpha) \to L$ plongement, une extension de σ, c'est à dire que $\tau \mid_F = \sigma$ avec $\tau(\alpha) = \beta$.
Le nombre de telles extensions est le nombre de racines distinctes de $\sigma(p)$ dans $L \leq \deg p = [E : F]$.

Démonstration:
Chaque élément y de E peut être écrit comme $y = f(\alpha)$ pour un certain $f \in F[t]$. Définissons $\tau(y) := \sigma(f)(\beta)$ et vérifions qu'elle est bien définie:

- $\tau(a) = \sigma(a) \quad \forall a \in F$
- $\tau(\alpha) = \beta$
- Supposons que $y = g(\alpha)$, alors $(f - g)(\alpha) = (f - g)(\alpha) = 0$

  $$\implies p \mid f - g \quad \text{c'est à dire} \quad f - g = p \cdot h \implies \sigma(f) - \sigma(g) = \sigma(p) \cdot \sigma(h)$$

  Avec $t = \beta$ nous obtenons

  $$\sigma(f)(\beta) - \sigma(g)(\beta) = \underbrace{\sigma(p)(\beta)}_{=0}\sigma(h)(\beta) = 0$$

Et donc $y \mapsto \sigma(f)(\beta)$ est bien défini.

On obtient immédiatement que τ est un plongement et pour chaque racine β on possède une extension différente:

$$\tau_1(\alpha) = \beta_1 \neq \beta_2 = \tau_2(\alpha)$$

De plus $\#\beta \leq \deg \sigma(p) = \deg p = [E : F]$, OK

□

Corollaire

Soient $[E : F] < \infty$ et A un corps algébriquement clos (par exemple $A = \mathbb{C}$). Soit $\sigma : F \to A$ plongement, alors $\exists \tau : E \to A$, $\tau \mid_F = \sigma$. Si A a en plus la propriété que chaque polynôme $\sigma(p)$ avec $p \in F[t]$ irréductible de degré n, a n racines disctinctes, alors le nombre de tels extension est $[E : F]$.

Démonstration:
Soit $E = F(\alpha_1, \cdots, \alpha_r)$. Regardons:

$$F \subset F(\alpha_1) \subset F(\alpha_1,\ \alpha_2) \subset \cdots \subset E$$

Soit p le polynôme minimal de α_1. Grâce au fait que A soit algébriquement clos, $\exists \beta$ tel que $(\sigma\ p)(\beta) = 0$. Donc $\tau_1 : F(\alpha_1) \to F$ existe et $\tau_1 \mid_F = \sigma$.
Si en plus nous avons $\deg(p)$ de β différents (nb de racines distinctes), il y a $[F(\alpha_1) : F]$ nombre d'extensions. Maintenant $[F(\alpha_1,\ \alpha_2) : F(\alpha_1)] = \deg p_2$ où p_2 est le polynôme minimal de α_2. En appliquant la proposition d'extension à celui-ci, on obtient la même chose: Il existe une extension et si A a la propriété des racines distincts on a $\deg p_2$ de ces extensions. On peut donc continuer comme ça et avec la loi de tour/multiplication, le choix des extension est égal à $[E : F]$.

□

Exemple

$p(t) = t^3 - 2$, $F = \mathbb{Q}$ irréductible par Eisenstein. Les racines sont $\alpha = \sqrt[3]{2}$, $\zeta\alpha$ et $\zeta^2\alpha$ où $\zeta = e^{2\pi i/3}$.
Nous avons $\sigma : \mathbb{Q} \to \mathbb{C}$ l'identité et trois extensions: $\mathbb{Q}(\alpha) \to \mathbb{C}$:

$$\tau_1(\alpha) = \alpha\ (\tau_1 = id\ ) \quad \tau_2(\alpha) = \zeta\alpha \quad \tau_3 = \zeta^2\alpha$$

8 Préparations pour les théorèmes de Galois

8.1 Séparabilité

On dit qu'un polynôme $f(t) = c(t-\alpha_1)^{n_1}\cdots(t-\alpha_r)^{n_r}$ a des racines distinctes si $n_1 = n_2 = \cdots = n_r = 1$.

Proposition

Soit K un corps. Soient $f \in K[t]$ de degré ≥ 1, et α une racine de f dans K. Alors la multiplicité de α dans f est ≥ 2 si et seulement si $f'(\alpha) = 0$.

Preuve:
On écrit $f(t) = (t-\alpha)^m g(t)$ avec $g(\alpha) \neq 0$, $m \geq 1$.

$$f'(t) = m(t-\alpha)^{m-1}g(t) + (t-\alpha)^m g'(t)$$
$$f'(\alpha) = m \cdot 0^{m-1}g(\alpha) + 0 \cdot g'(\alpha)$$

Si $m > 1 \implies f'(\alpha) = 0$. Si $m = 1$, $f'(\alpha) = 1 \cdot 1 \cdot g(\alpha) \neq 0$
Et donc $m \geq 2$ si et seulement $f'(\alpha) = 0$

□

Proposition

Soit $F \subset A$, avec A algébriquement clos de charactéristique 0 (par exemple $A = \mathbb{C}$). Soit $f \in F[t]$ irréductible de degré $n \geq 1$. Alors f a n racines distinctes dans A.

Démonstration:
On peut écrire $f(t) = a(t-\alpha_1)\cdots(t-\alpha_n)$ avec $\alpha_i \in A$. Soit α une de ces racines. Alors f (diviser par a) est le polynôme minimal de α. Soit $f'(t)$ la dérivée $\deg f' < \deg f$.
Notons que, comme A est de charastéristique nulle, $f'(t) = \underbrace{n \cdot a}_{\neq 0} t^{n-1} + \cdots$. Alors $f' \not\equiv 0$, $\deg f' \geq 0$ car f a le degré minimal. Donc $f'(\alpha) \neq 0$ et α sont des racines distinctes.

□

Contre-Exemple

En Char $F = p$ n'est pas toujours vrai. Soit $F = \mathbb{F}_p(x)$ fonctions rationnels en variable x. Soit $f \in F[t]$, $f(t) = t^p - x$. Supposons que $f(u) = 0$ pour un certain u dans une certaine extension, c'est à dire: $u^p = x$. Donc $u \notin F$.
Notons que $t^p - x = (t^p - u^p) \overset{\text{char } p}{=} (t-u)^p$. Par unicité de factorisation, chaques facteurs est $(t-u)^m$ mais $u \notin F$ donc f irréductible.
$(t-u)^m = t^m - \underbrace{m \cdot u}_{\in F} t^{m-1} + \cdots$, $m < p \implies m^{-1}$ existe et $u \in f$. ↯.

Définition

α est séparable si son polynôme minimal dans $F[t]$ a des racines distinctes (dans une clôture algébrique de F).

Une extension E/F est séparable si tout $\alpha \in E$ est séparable.

Nous avons démontré que dans une charactéristique nulle, tout E/F sont séparable.
En particulier, $\mathbb{Q} \subset F \subset E \subset \mathbb{C}$, notre situation principale.

Définition

Un corps est parfait si toutes les extensions algébriques sont séparable, c'est à dire tout polynôme irréductible est à racines distinctes.

Théorème

K_1 à charactéristique nulle et K_2 un corps fini sont parfait.

Démonstration:
Nous avons déjà prouvé le théorème pour le corps à charactéristique nulle.

Supposons que $\pi(x) \in K[x]$ est irréductible et inséparable, c'est à dire:
Supposons que π est polynôme minimal de α et $\pi'(\alpha) = 0$ car α est racine multiple de π. Mais $\deg \pi' < \deg \pi$, par minimalité de π, il faut que $\pi'(x) \equiv 0$.
Alors il faut que $\pi(x)$ soit un 0 polynôme dans x^p (? help je sais pas, suis pas sûr de moi ?), c'est à dire:

$$\pi(x) = a_m x^{p_m} + a_{m-1} x^{p_{m-1}} + \cdots + a_1 x^p + a_0$$

Comme ça $\pi'(x) = 0$ car $p = 0$.

Affirmation: Si K est fini de charactéristique p, alors $K^p = K$

L'application $k \mapsto k^p$ est injective, car si $a^p = b^p$ alors $0 = a^p - b^p = (a-b)^p = (a-b)(a-b)\cdots(a-b)$ et donc $a = b$. Injection ok, comme K est fini, l'application est aussi surjective $\implies K^p = K$. OK

Donc $a_j = b_i^p$, $\forall i$ pour certains $b_j \in K$.

$$\implies \pi(x) = b_m^p x^{p_m} + \cdots + b_0^p = (b_m x^m + \cdots + b_1 x + b_0)^p$$

Mais π est irréductible et donc contradiction.

Donc vrai pour tout polynôme irréductible de corps fini a racines distinctes.

□

Exemple

$f = x^4 + x + 1$ irréductible dans $\mathbb{Z}/2\mathbb{Z}\ [x]$?
Il est séparable car $f'(x) = 4x^3 + 1 = 1 \neq 0$, $f(0) = 1$ et $f(1) = 1$, donc il n'y a aucun facteur linéaire.
Ne reste plus que les facteurs de degré 2:

- $x^2 + 1$, $x^2 + x$, x^2 ne peuvent pas être facteurs car possèdent comme racines 1 ou 0.
- $x^2 + x + 1$

On peut donc tenter la division euclidienne de f par $x^2 + x + 1$, nous obtenons au final:

$$x^4 + x + 1 = (x^2 + x + 1)(x^2 - x) + 1 \implies x^4 + x + 1 \quad \text{est irréductible}$$

8.2 Théorème d'élément primitif

Exemple

Soient $\alpha = \sqrt{2}$, $\beta = \sqrt{3}$. Affirmation: $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\gamma)$ pour $\gamma = \alpha + \beta$.
En fait: $\alpha = \dfrac{\gamma^3 - 9\gamma}{2}$, $\beta = \gamma - \alpha$ ce qui se vérifie facilement algébriquement.

Théorème: [Abel/Galois] Élément primitif

Soient $F \subset \mathbb{C}$ un corps et $[E : F] < \infty$. Alors $\exists \gamma \in E$ tel que $E = F(\gamma)$.

Démonstration:
On sait que $E = F(\alpha_1, \cdots, \alpha_m)$, il est alors suffisant de prendre $E = F(\alpha, \beta)$ et ensuite trouver γ tel que $E = F(\gamma)$. Il suffit en effet de répéter la manoeuvre pour atteindre le résultat général.

Soit $n = [E : F]$. Soient $\sigma_1, \sigma_2, \cdots, \sigma_n : E \to \mathbb{C}$ les n plongements distincts sur F, c'est à dire: $\sigma_i \mid_F = id$. Alors $\sigma_i(\alpha) + c\sigma_i(\beta)$ ($= \sigma_i(\alpha + c\beta)$) sont distincts pour $1 \leq i \leq n$. Considérons en effet le polynôme:

$$p(t) = \prod_{i=1}^{n} \prod_{j \neq i} \Big(\sigma_j(\alpha) - \sigma_i(\alpha) + t\big(\sigma_j(\beta) - \sigma_i(\beta)\big) \Big)$$

S'il existe des $i \neq j$ tel que $\sigma_i(\alpha) = \sigma_j(\alpha)$ et $\sigma_i(\beta) = \sigma_j(\beta)$ alors $p(t) = 0$ forcément, mais ce n'est pas possible:

$\deg p \geq 1$ et $\mathbb{Q} \subset F$ donc $|F| = \infty$. Un polynôme de degré plus grand ou égal à 1 possède au plus $\deg p$ racines, du coup $\exists c \in F$ tel que $p(c) \neq 0$, ce qui montre bien que $\sigma_i(\alpha) + c\sigma_i(\beta)$ sont distincts.

Affirmation: $E = F(\gamma)$ avec $\gamma = \alpha + c\beta$
Par construction $\sigma_i(\alpha + c\beta)$ sont tous disctincts, $\sigma_i \mid_F = id_F$ donc nous avons n plongemets différents. Alors $[F(\gamma) : F] = n$. D'autre part $F(\gamma) \subset E$ et donc:

$$\underbrace{[E : F]}_{=n} = [E : F(\gamma)] \cdot \underbrace{[F(\gamma) : F]}_{=n} \implies [E : F(\gamma)] = 1 \implies E = F(\gamma)$$

□

9 Théorème de Galois

9.1 Introduction

Dans cette section du cours nous allons discuter de la découverte exraordinaire de Galois dont l'idée principale est:

On aimerait savoir si

$$f(t) := a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0 = 0$$

est résoluble avec les opérations arithmétiques $+,\ -,\ \cdot,\ \div$, et $\sqrt[n]{}$ appliquées sur les coefficients $a_0,\ a_1, \ldots,\ a_n \in K$.
Le résultat est connu depuis un certain temps pour $n = 2, 3$, et même 4. Mais et alors pour $n \geq 5$?
Prenons $L = K(\alpha_1, \ldots, \alpha_n)$ les racines α_i de f et considérons $G = \mathrm{Gal}(L/K) := \{\sigma :\ L \to L \text{ autom. } :\ \sigma \mid_K = id\}$

Théorème

Les sous-groupes de G coïncident avec les corps intermédiaires $K \subset F \subset L$.
Donc $f(t) = 0$ est "résoluble" $\iff$ G est un groupe résoluble !

On vient donc de transformer une problème d'équation en un problème de groupes. Notons qu'à l'époque de Galois la notion de groupe était encore très floue, voire inéxistante.

9.2 Rappel de notions et faits établis

On sait que pour des sous-corps de $\mathbb{C}$ et des corps finis, les racines d'un polynôme irréductible sont distinctes. (Séparabilité, corps parfait)
Soient $[E : F] < \infty$ et A algébriquement clos. Soit $\sigma :\ F \to A$ un plongement, alors $\exists \tau :\ E \to A$ avec $\tau \mid_F = \sigma$ et si A est tel que pour tout polynôme irréductible possède des racines distinctes alors le nombre de telles extensions est donné par $[E : F]$.

Théorème des éléments primitifs

Soient $F \subset \mathbb{C}$ un corps et $[E : F] < \infty$, alors $\exists \gamma \in E$ tel que $E = F(\gamma)$.

9.3 Corps de décomposition

Soit $[E : F] < \infty$. Soit $\sigma : F \to F$ et $\tau : E \to A$ une extension. Si $\sigma = id_F$ on dit que τ est un plongement de E sur F. On dit alors que $\tau(E)$ est le conjugé de E sur F. Pour un $\alpha \in E$ on parle de $\tau(\alpha)$ comme le conjugué.
Si $F \subset E \subset \mathbb{C}$ nous avons vu que le nombre de conjugués est égal à $[E : F]$.

Exemple

$F = \mathbb{Q}$, $E = \mathbb{Q}(i)$, $\tau(z) = \overline{z} \rightsquigarrow \tau(x + iy) = x - iy$. On vérifie bien $\tau \mid_{\mathbb{Q}} = id_{\mathbb{Q}}$, $[\mathbb{Q}(i) : \mathbb{Q}] = 2 < \infty$.
$\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \{id,\ \tau\}$

Définition

Soit $f(t) \in F[t]$ un polynôme de degré $n \geq 1$.
Un corps de décomposition ("Splitting field" en anglais) K est une extension de F telle que f se décompose en facteurs linéaires:

$$f(t) = c(t - \alpha_1)(t - \alpha_2) \cdots (t - \alpha_n) \quad c \in F, \text{ et } K = F(\alpha_1, \ldots, \alpha_n) \quad \text{(Donc le plus petit corps)}$$

Proposition 1

Soit $f(t)$ dans $F[t]$, de degré au moins 1. Il existe alors un corps de décomposition pour f.

On dit que $f \in F[t]$ se décompose sur L si $f(t) = c(t - \alpha_1) \cdots (t - \alpha_n)$ avec $c \in F$ et $\alpha_i \in L$.

Exemples

1) Tout polynôme dans $\mathbb{R}$ (dans $\mathbb{C}$ aussi) se décompose sur $\mathbb{C}$ par le théorème fondamental de l'algèbre.

2) $f(t) := t^3 - 1 \in \mathbb{Q}[t]$, on peut montrer: $f(t) = (t - 1)(t - w)(t - w^2)$ où $w = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Donc f se décompose sur $L = \mathbb{Q}(i, \sqrt{3})$.

Lemme 1

Soient F un corps et $p \in F[t]$, $\deg f \geq 1$ et irréductible. Alors il existe une extension E de F telle que f a comme racine $\alpha \in E$.

Démonstration:
Cette preuve découle de l'observation que nous avons déjà faite: $E := {F[t]}/{(p)}$ $(\cong F(\alpha))$ est un corps et que $F \subset E$. Le polynôme p possède comme racine $\alpha = t \pmod{p(t)}$ car $p(t) = 0$ dans E.

□

Remarque: Pour F dans $\mathbb{C}$ on le sait déjà plus concrètement.
On peut donner un exemple trivial: $p(t) = t - a$ avec donc a déjà dans F. Alors ${F[t]}/{(p)} = F$.

Démonstration de la proposition 1:
Procédons par récurrence sur le degré de f. Cas $\deg f = 1$ est trivial: $K = F$.
Soit p un facteur irréductible de f. Par le lemme 1 il existe $E_1 = F(\alpha_1)$ avec α_1 une racine de p et donc de f aussi. Soit alors $f(t) = (t - \alpha_1)g(t)$, nous avons $\deg g = \deg f - 1 \implies$ par hypothèse de récurence on peut écrire $g(t) = c(t - \alpha_2) \cdots (t - \alpha_n)$ et donc $E = E_1(\alpha_2, \ldots, \alpha_n)$.

□

Proposition 2

Soit $f \in F[t]$ avec $\deg f \geq 1$. Soient K et L deux corps de décompositions, alors il existe un isomorphisme $\sigma : K \to L$ sur F.

Démonstration:

$f(t) = c\prod_{i=1}^{n}(t-\alpha_i)$ avec $\alpha_i \in K$, aussi $f(t) = c\prod_{j=1}^{n}(t-\beta_j)$ où $\beta_j \in L$, et $c \in F$ dans les deux cas.

Procédons par recurrence, dans le cas où le degré est de 1 il n'y a rien à montrer car $K = L = F$. Nous pouvons aussi supposer que le coefficient principal (a_n) de f est égal à 1 et donc que f est de la forme: $f(t) = t^n + a_{n-1}t^{n-1} + \cdots$

De manière plus précise, pour l'étape de récurrence nous allons montrer:

Soit $\sigma_0 : F \to \sigma_0(F)$ un isomorphisme. Soient $f \in F[t]$ et $K = F(\alpha_1, \ldots, \alpha_n)$ un corps de décomposition de f:

$$f(t) = \prod_{i=1}^{n}(t-\alpha_i)$$

Soit L un corps de décomposition de σf et $L = (\sigma F)(\beta_1, \ldots, \beta_n)$, $\sigma f(t) = \prod_{i=1}^{n}(t-\beta_i)$

Il existe alors un isomorphisme $\tau : K \to L$ sur σ_0 tel que, si necessaire après permutation des β_i, $\tau(\alpha_i) = \beta_i \quad \forall i$.

Soit $p(t)$ un facteur irréductible de f. Nous savons déjà que pour une racine α_1 de p et β_1 de $\sigma(p)$ il existe un isomorphisme $\tau_1 : F(\alpha_1) \to (\sigma F)(\beta_1)$ qui prolonge σ et tel que $\alpha_1 \mapsto \beta_1$. Donc on peut factoriser:

$$f(t) = (t-\alpha_1)g(t) \quad \text{sur} \quad F(\alpha_1)$$
$$\sigma f(t) = (t-\beta_1)(\tau_1 g)(t) \quad \text{sur} \quad \sigma F(\beta_1)$$

Par reurrence on peut faire la même chose pour g, $\tau_1 g$, et τ_1 (au lieu de f, σf, et σ).

Pour récapituler: Nous avons, à priori, deux factorisations dans deux "univers" différents, plus précisement, dans deux extensions de corps différentes. Pour trouver l'isomorphisme, on travaille avec les facteurs irréductibles de f. Pour chaque tel facteur p, nous avons vu que l'on peut faire un prolongement tel que la racine α_1 est envoyée sur β_1. Nous pouvons ensuite, par principe de recurrence continuer jusqu'à ce qu'il ne reste plus de racines.

Nous avons donc montré qu'un corps de décomposition existe et est unique dans le sens qu'il va toujours exister un isomorphisme.

□

Note: La démonstration est pas forcément facile à saisir mais on peut aussi passer par les résultats intermédiaires: $\sigma : F \to F'$ un isomorphisme $\implies$ induit naturellement $\sigma : F[t] \to F'[t]$ isomorphisme et en posant $\alpha \in E/F$ racine de $p \in F[t]$, $\beta \in E'/F'$ racine de σp:

$$F(\alpha) \overset{\phi_1}{\cong} F[t]\Big/_{(p)} \overset{\phi_2}{\cong} F'[t]\Big/_{(\sigma p)} \overset{\phi_3}{\cong} F'(\beta) \quad \text{avec} \quad \phi_1\phi_2\phi_3|_F = \sigma \quad (F \to F')$$

De là montrer que si $\varphi : F \to F'$ iso, $f \in F[t]$, E/F le corps de décomposition de f et E'/F' le corps de décomposition de $\varphi f \in F'[t]$, $\exists \phi : E \to E'$ tel que $\phi|_F = \varphi$. On peut montrer ça en étudiant les facteurs irréductibles des f et φf et exhiber un isomorphisme qui va mapper $\alpha_i \leftrightarrow \beta_j$ par le mini-lemme précédent, puis procéder par récu. Il suffit de poser $\varphi : F \to F$ l'identité pour avoir le résultat voulu après coup.

9.4 Application: Corps finis

Soit $\mathbb{F}_p := \left(\mathbb{Z}/p\mathbb{Z} \ , +, \cdot \right)$ pour p premier.
Pour K un corps fini, on sait qu'il existe p premier, la caractéristique avec $\mathbb{F}_p \subset K$. Donc $K/\mathbb{F}_p$ et $[K : \mathbb{F}_p] = n$ où alors $|K| = p^n$ car:

$$K = \{a_1 w_1 + \cdots + a_n w_n \mid a_i \in F_p\}$$

Rappel (Exemples)

1) $\mathrm{GF}(4) = \mathbb{F}_4$:
   $\mathbb{F}_4 = \mathbb{F}_2[t]/(t^2 + t + 1)$ (car $t^2 + t + 1$ est irréductible dans $\mathbb{F}_2$) $= \{a \cdot 1 + b \cdot \alpha \mid a, b \in \mathbb{F}_2\}$ avec la loi $\alpha^2 = -\alpha - 1 = \alpha + 1$
2) $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3 + x + 1)$

Remarque: Il n'y a donc pas de corps avec cardinalité $6, 10, 12, \ldots$ etc.

Note: Résultat suivant découle de Lagrange: $|G| < \infty$, $g^{|G|} = e$.
Le groupe multiplicatif $K^* = K \setminus \{0\}$ a $p^n - 1$ éléments. Donc $x^{p^n - 1} = 1 \quad \forall x \in K^*$, c'est à dire:

$$x^{p^n - 1} - 1 = 0 \implies f(x) := x^{p^n} - x \quad \text{possède la propriété que} \quad f(x) = 0 \quad \forall x \in K.$$

3) $\mathbb{F}_4$:

$$t^4 - t = t(t^3 - 1) = t(t - 1)(t^2 + t + 1)$$

Notons maintenant, plus généralement, que $f(x) = x^{p^n} - x$ est un polynôme dans $\mathbb{F}_p[x]$ et pour n'importe quel K où $|K| = p^n$ on a:

$$f(x) = x(x - \alpha_1) \cdots (x - \alpha_{p^n - 1}) = \prod_{k \in K} (x - k)$$

Donc K est un corps de décomposition de $f(t)$, mais ils sont tous isomorphe ! Nous venons donc de démontrer:

Théorème

Pour chaque p premier et nombre $n > 0$, il existe un corps unique $\mathrm{GF}(p^n) = \mathbb{F}_{p^n}$ de p^n éléments.
C'est une classification, c'est à dire qu'il n'y a aucun autre corps fini.

9.5 Extensions normales

Définition

Soient K une extension de F avec $[K:F] < \infty$ et $F \subset K \subset A$, où A est algébriquement clos.
On dit que l'extension K/F est normale si pour tout plongement $\sigma : K \to A$ sur F on a $\sigma(K) = K$. Donc $\sigma : K \to K$ est un automorphisme.

Non-exemple: Pour chercher un (non)-exemple pour une application non surjective,il est necessaire d'avoir un degré fini, sinon une application injective est surjective automatiquement (cf. Algèbre Linéaire).

$$\rho : \begin{array}{ccc} \mathbb{Q}(\pi) & \longrightarrow & \mathbb{Q}(\pi) \\ \pi & \longmapsto & \pi^2 \end{array}$$

Proposition 1

Soit $[K:F] < \infty$.
L'extension K/F est normale $\iff$ K est un corps de décomposition pour un polynôme dans $F[t]$.

Démonstration:

$\Longrightarrow$: Supposons que $K = F(\alpha)$. Soit $p(t)$ le polynôme minimal de α. Nous avons déjà vu que $\forall \alpha_i$ racine de p, il existe un unique plongement σ_i de K sur F tel que $\sigma_i(\alpha) = \alpha_i$.
Et en voyant que $\sigma_i(K) = K$, alors $\alpha_i \in K$. Nous obtenons donc $K = F(\alpha) = F(\alpha_1, \ldots, \alpha_n)$ le corps de décomposition de pOK.

Si $\operatorname{car} F = 0$ et $A = \mathbb{C}$, on sait que $K = F(\alpha)$ (théorème de l'élément primitif). Nous avons en général $K = F(\alpha, \beta, \gamma, \ldots, \zeta)$.
Soient alors $p_1, p_2, \ldots, p_n$ leur polynôme minimal. Soit $f(t) = p_1(t) \cdot p_2(t) \cdots p_n(t)$. Avec le même argument et par récursion on obtient bien:

$$K = F(\quad \text{Toutes les racines de } f \quad)$$

$\Longleftarrow$: Supposons ici que K est un corps de décomposition de $f \in F[t]$ (pas forcément irreductible) avec comme racines $\alpha_1, \ldots, \alpha_n$. $K = F(\alpha_1, \ldots, \alpha_n)$
Si $\sigma : K \to A$ est un plongement sur F, c'est à dire si $\sigma \mid_F = id_F$, alors $\sigma(\alpha_i)$ est aussi racine de $\sigma(f) = f$. Donc $\sigma(\alpha_i) \subset K$ et ce pour tout $i \implies \sigma(K) = K$ OK.

□

Proposition 2

Soit l'extension K/F normale. Si $p(t) \in F[t]$ est irréductible sur F et si p a une racine dans K, alors toutes les racines de p sont dans K.

Démonstration:
Soit $\alpha \in K$, $p(\alpha) = 0$. Soit $\beta \in A$, $p(\beta) = 0$. Alors il existe un plongement:

$$\sigma : \begin{array}{ccc} F(\alpha) & \longrightarrow & F(\beta) \\ \alpha & \longmapsto & \beta \end{array} \qquad \sigma \mid_F = id_F$$

Donc il prolonge σ à K, on sait que $\sigma(K) = K$, donc $\beta \in K$.

□

Remarque: On voit souvent comme définition alternative que:
K/F est normale si pour chaque polynôme irréductible p dans $F[t]$ on a que si K contient une racine de p alors il contient toutes les racines de p.

Corollaire

Ces deux définitions sont équivalentes.

Démonstration:
Soit K/F normale selon la première définition. Si p est un polynôme avec $\alpha \in K$ tel que $p(\alpha) = 0$. Soit b une autre racine, alors il existe un plongement $\sigma : K \to A$ tel que $\sigma(\alpha) = \beta$. Mais $\sigma(K) = K$, donc β est dans K, et donc cela vérifie bien la deuxième définition.

Soit K/F normale selon la deuxième définition. Soit $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Soient $p_1, p_2, \ldots, p_n$ leur polynôme minimal. La deuxième définition implique que K contient toutes les racines de $p_1, \ldots, p_n$.
Or nous savons que tout plongements $\sigma : K \to A$ doit envoyer les racines de $p_1, \ldots, p_n$ aux racines de l'image de $p_1, \ldots, p_n$. Comme ils étandent $id : F \to A$ les racines sont égales. Et alors $\sigma(K) = K$, ce qui vérifie notre première définition.

□

Conclusion: Nous avons au final trois notions équivalentes:

1) Condition avec les plongements.

2) Corps de décomposition.

3) Contenir une racine d'un polynôme irréductible implique la même chose de toutes ses racines.

Voyons maintenant quelques exemples concrets.

Exemples

i. Soit $\alpha \in \mathbb{Q}$. $\mathbb{Q}(\sqrt{\alpha}) \supset \mathbb{Q}$ est normal car c'est un corps de décomposition, celui du polynôme: $p(x) := x^2 - \alpha$ qui a pour racines $\pm\sqrt{\alpha} \in \mathbb{Q}(\sqrt{\alpha})$.

ii. Voyons ici un non-exemple.

L'extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ n'est pas normale ! En effet $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ mais les autres racines de $x^3 - 2$ (un polynôme irréductible) sont complexes. On peut alors poser le plongement:

$$\sigma \ : \ a + b\sqrt[3]{2} - c\sqrt[3]{4} \mapsto a + bw\sqrt[3]{2} + cw^2\sqrt[3]{4} \quad \text{où} \quad w := \sqrt[3]{2} \cdot \exp\left(i\frac{2\pi}{3}\right) \implies \sigma\left(\mathbb{Q}(\sqrt[3]{2})\right) \neq \mathbb{Q}(\sqrt[3]{2})$$

Définition

Une extension algébrique est Galois (ou galoisienne) si elle est normale et séparable.

9.6 La correspondence de Galois

Pour simplifier un peu en gardant les idées principales, on va supposer dans ce chapitre que tout nos corps sont des sous corps des nombres complexes $\mathbb{C}$. Comme $\mathbb{C}$ est parfait alors toute extension K/F finie est Galois si et seulement si K/F est normale.

Définition

Soit K/F

$$\mathrm{Gal}(K/F) = \mathrm{Aut}_F(K) = \{\sigma : K \to K \text{ autom. tel que } \sigma|_F = id\}.$$
$$\mathrm{Fix}(H) = \{x \in K \mid hx = x \quad \forall h \in H\}$$

Notons bien que:

- $\mathrm{Gal}(K/F)$ est un groupe, en fait nous avons même:

$$1 \subseteq \mathrm{Gal}(K/F) \subseteq \mathrm{Gal}(K/\text{ss-corps}) = \mathrm{Aut}(K)$$

- $\mathrm{Fix}(H)$ est un sous-corps: $F \subset \mathrm{Fix}(H) \subset K$
  Notons aussi qu'il est évident que $\mathrm{Fix}(\{1\}) = K$, $K \supset \mathrm{Fix}(\mathrm{Gal}(K/F)) \supset F$

Proposition 3

Soit K/F finie et Galois, alors $F = \mathrm{Fix}(\mathrm{Gal}(K/F))$.

Preuve:
Notons $G := \mathrm{Gal}(K/F)$. Par définition nous avons $F \subset \mathrm{Fix}(G)$. Posons alors $\alpha \in \mathrm{Fix}(G)$ et supposons que le polynôme minimal p de α est de dégré ≥ 2, ce qui est vrai si et seulement si $\alpha \notin F$.
Comme K/F est normale (et séparable $\beta \neq \alpha$), $\exists \beta \neq \alpha$ autre racine de p dans K. Nous obtenons alors un plongement $\sigma : K \to K$ sur F défini par $\alpha \mapsto \beta$ où $\sigma \in \mathrm{Aut}(K)$, mais où alors α n'est pas fixé:

$$\sigma(\alpha) = \beta \neq \alpha$$

Cela n'est pas possible et donc $\deg p = 1$, c'est à dire $\alpha \in F$.

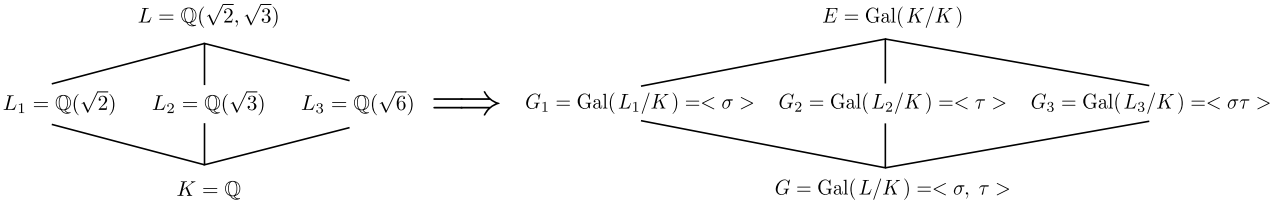
□

Théorème: Galois, partie 1

Soient $F \subset K \subset \mathbb{C}$, K/F finie et Galois. Pour chaque corps E, $F \subset E \subset K$, K/E est Galois.
L'application $E \mapsto \mathrm{Gal}(K/E)$ est une bijection entre les corps intérmédiaires $\mathbb{F} \subset E \subset K$ et les sous-groupes de $G := \mathrm{Gal}(K/F)$.
L'inverse est donnée avec $1 \subseteq H \subseteq G$

$$H \mapsto \mathrm{Fix}(H) =: K^H \quad \text{et} \quad E = \mathrm{Fix}(\mathrm{Gal}(K/E))$$

Exemple:



Démonstration:

i) Tout plongement $\sigma : K \to \mathbb{C}$ sur E est un plongement sur F car $E \supset F$. K/F normale implique que $\sigma(K) = K$ et alors K/E est normale, et donc Galois. OK

ii) Donc par proposition 3 on obtient directement $E = \text{Fix}(\text{Gal}(K/E))$. OK

iii) Affirmation: $E \mapsto \text{Gal}(K/E)$ est injectif. Supposons que $\text{Gal}(K/E) = \text{Gal}(K/E')$, alors par la proposition 3 on obtient:

$$E = \text{Fix}(\text{Gal}(K/E)) = \text{Fix}(\text{Gal}(K/E')) = E'$$

iv) En ce qui concerne la surjectivité:
Prenons $H < G = \text{Gal}(K/F)$. Soit $E := \text{Fix}(H)$ qui est un sous-corps. Il faut montrer que $\text{Gal}(K/E) = H$. Il est à priori clair que $H < \text{Gal}(K/E)$, écrivons alors $H = \{\sigma_1, \ldots, \sigma_r\}$.
Soit $K = F(\alpha)$ (théorème élément primitif). Soit $f(t) = (t - \sigma_1(\alpha)) \cdots (t - \sigma_r(\alpha))$:

$$\forall \sigma \in H \quad H = \{\sigma\sigma_1, \ldots, \sigma\sigma_r\}$$

Ce qui implique alors:

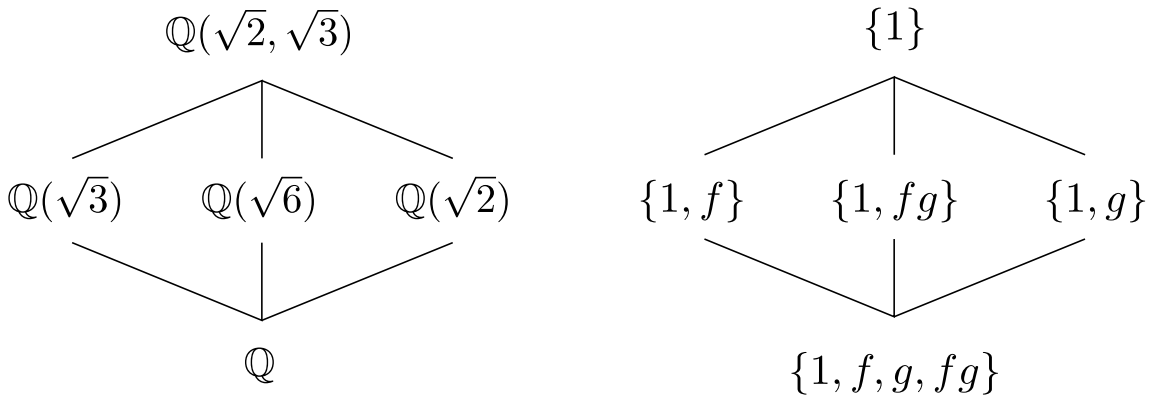
$$(\sigma f)(t) = (t - \sigma\sigma_1(\alpha)) \cdots (t - \sigma\sigma_r(\alpha)) = f(t)$$

Donc $f(t) \in \text{Fix}(H)[t] = E[t]$ Comme pour un certain i nous avons $\sigma_i = id$, on obtient $f(\alpha) = 0$.
Alors, d'une part $K = F(\alpha) \subset E(\alpha)$ car $F \subset E$. Mais d'autre part $E(\alpha) \subset K$.
Alors $K = E(\alpha)$ et logiquement $[K : E] = [E(\alpha) : E] < \deg f = r$. Comme K admet $\geq r$ plongements distincs sur E, en fait $\sigma_1, \sigma_2, \ldots, \sigma_r \in H$.
Ces deux inégalités impliquent que:

$$[K : E] = r \implies \text{Gal}(K/E) = \{\sigma_1, \ldots, \sigma_r\} = H$$

□

Exemple



$K = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3})$. On peut donc écrire $x \in K$ comme $x = (a + b\sqrt{2}) + (c + d\sqrt{2})\sqrt{3}$ pour $a, b, c, d \in \mathbb{Q}$. Nous avons les automorphismes $f(\sqrt{2}) = -\sqrt{2}$, $g(\sqrt{3}) = -\sqrt{3}$, par exemple:

$$f\Big((a + b\sqrt{2}) + (c + d\sqrt{2})\sqrt{3}\Big) = (a - b\sqrt{2}) + (c - d\sqrt{2})\sqrt{3}$$

Ce qui nous donne:

$$G := \text{Gal}(K/\mathbb{Q}) = \{1, f, g, fg\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

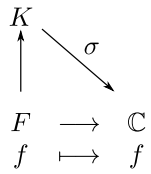
Rappel: Soit K/F une extension finie (donc algébrique) et Galois (normale et séparable).
Prenons par exemple F un sous-corps de $\mathbb{C}$, et K le corps de décomposition d'un polynôme $p(t) \in F[t]$. $K = F(\alpha_1, \ldots, \alpha_m)$ où $p(t) = c(t-\alpha_1)\cdots(t-\alpha_m)$
Nous venons d'étudier les correspondences entres les sous-corps intermédiaires et les sous groupes de Galois. En particulier $\mathrm{Gal}(K/E)$ est le groupe des automorphismes de K qui fixent E point par point. La correspondence de Galois est alors:

$$E \mapsto \mathrm{Gal}(K/E) \quad \text{d'inverse} \quad H \mapsto \mathrm{Fix}(H) = \{x \in K \mid \sigma x = x \ \forall \sigma \in H\}$$

$$E = \mathrm{Fix}(\mathrm{Gal}(K/E)) \quad \text{et} \quad H = \mathrm{Gal}(K/\mathrm{Fix}(H))$$

Remarque

Soit $f \in F[t]$, $F \subset \mathbb{C}$. Alors posons $f(t) = c(t-\alpha_1)^{k_1}\cdots(t-\alpha_n)^{k_n}$, $K = F(\alpha_1, \cdots, \alpha_n)$ le corps de décomposition lié. Soit $\sigma \in \mathrm{Gal}(K/F)$. Nous savons que les $\alpha_i \mapsto \alpha_j$ sont fixés de manière injective. Donc cela détermine une fonction $\phi : \mathrm{Gal}(K/F) \to S_n$, un homomorphisme avec le groupe des permutations. Cet homomorphisme ϕ est injectif mais il n'est pas toujours surjectif.



Nous avons aussi déjà discuté du fait que si $\lambda : K \to \lambda(K)$ est un isomorphisme et K est un corps de décomposition de f, alors $\lambda(K)$ est un corps de décomposition de $\lambda(f)$. De plus:

$$\mathrm{Gal}(\lambda(K)/\lambda(F)) = \lambda\,\mathrm{Gal}(K/F)\lambda^{-1}$$

$$\begin{array}{ccc} K & \xrightarrow{\sigma} & K \\ {\scriptstyle\lambda}\downarrow & & \downarrow{\scriptstyle\lambda} \\ \lambda(K) & \xrightarrow[g:=\lambda\sigma\lambda^{-1}]{} & \lambda(K) \end{array}$$

Exemple

$F \subset E \subset K$, $\lambda : E \to \lambda(E) \subset K$ qui se prolonge sur $\lambda : K \to \lambda(K) = K$ (par exemple si K/F est normale). Alors

$$\mathrm{Gal}(K/\lambda(E)) = \lambda\,\mathrm{Gal}(K/E)\lambda^{-1}$$

Théorème: Galois, partie 2

Soient $F \subset K \subset \mathbb{C}$ Galois, fini et $F \subset E \subset K$. Soit $H = \mathrm{Gal}(K/E)$ et $G := \mathrm{Gal}(K/F)$.
Alors E est Galois (ici $\to$ normale) sur F si et seulement si H est un sous-groupe normal de G.
Dans ce cas la restriction : $\begin{array}{ccc} G & \longrightarrow & \mathrm{Gal}(E/F) \\ \sigma & \longmapsto & \sigma\,|_E \end{array}$ induit un isomorphisme ${}^{G}\!/_{H} \to \mathrm{Gal}(E/F)$. En plus, $|\mathrm{Gal}(E/F)| = [E:F]$

Démonstration:

$\Longleftarrow$: Supposons que $H = \mathrm{Gal}(K/E) \triangleleft G$ normal. Soit $\lambda_0 : E \to \mathbb{C}$ un plongement sur F. On doit montrer que $\lambda_0(E) = E$.
Soit λ un prolongement de λ_0, $\lambda : K \to \mathbb{C}$ comme K Galois sur $F \implies \lambda(K) = K$ et donc $\mathrm{Gal}(K/E) = \lambda\,\mathrm{Gal}(K/E)\lambda^{-1} = \mathrm{Gal}(K/\lambda(E))$. Donc par la première partie du théoème de Galois, et par normalité $\lambda(E) = E$ et donc E/F est normale.

$\Longrightarrow$: Supposons ici que E/F est normale. Alors la restriction : $\begin{array}{ccc} \mathrm{Gal}(K/F) & \longrightarrow & \mathrm{Gal}(E/F) \\ \sigma & \longmapsto & \sigma\mid_E \end{array}$ est un homomorphisme. Le noyau est, par définition:

$$\mathrm{Gal}(K/E) = \{\sigma \in \mathrm{Aut}(K) \mid \sigma\mid_E = id_E\}$$

Donc $\mathrm{Gal}(K/E)$ est normal.

De plus nous avons déjà montré que $|\mathrm{Gal}(E/F)| = [E:F]$. En effet, l'homomorphisme est surjectif car chaque $\sigma_0 : E \to \mathbb{C}$ se prolonge $\sigma : K \to \mathbb{C}$ sur F et $\sigma(K) = K$, $\sigma_0(E) = E$. Donc σ_0 est dans l'image de notre restriction.

□

Exemple

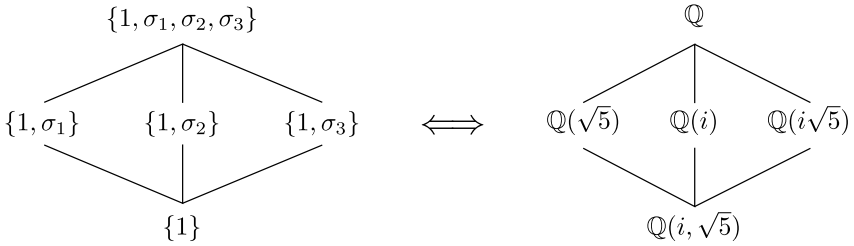
Prenons un exemple de degré 4.
Posons $p(t) := t^4 - 4t^2 - 5 \in \mathbb{Q}[t]$, donc $p(t) = (t^2+1)(t^2-5)$. Les racines de p sont $\pm i,\ \pm\sqrt{5}$ et son corps de décomposition est donc $K = \mathbb{Q}(i, \sqrt{5})$, une extension de degré 4 avec comme base $\{1, i, \sqrt{5}, i\sqrt{5}\}$. La question centrale est donc:

$$G := \mathrm{Gal}(K/\mathbb{Q}) =? < S_4$$

Étudions les éléments de G:

$$\sigma_0 = id \qquad \sigma_1 = \{i \leftrightarrow -i\}$$
$$\sigma_2 = \{\sqrt{5} \leftrightarrow -\sqrt{5}\} \qquad \sigma_3 = \{i \leftrightarrow -i,\ \sqrt{5} \leftrightarrow -\sqrt{5}\}$$

$\sigma_1,\ \sigma_2,\ \sigma_3$ sont d'ordre 2 et on remarque aussi que $\sigma_3 = \sigma_1\sigma_2$ et comme $|G| = 4 \implies G = C_4$ ou $C_2 \times C_2$. Mais comme il n'y a aucun élément d'ordre 4, forcément $G \cong C_2 \times C_2$. On peut alors tracer le graph de correspondance suivant:



De plus comme G est abélien, tout sous-groupe est normal et alors on applique la partie 2 du théorème ce qui nous donne:

$$\mathrm{Gal}(\mathbb{Q}(i,\sqrt{5})\big/\mathbb{Q}) \cong \ C_2 \times C_2\big/_{C_2} \ \cong C_2$$

Exemples de degré 1, 2, et 3

Soit $F \subset \mathbb{C}$ un corps.

Deg 1: $f(t) \in F[t]$, $f(t) = at + b$ avec $a, b \in F$.
$0 = at + b \iff t = -\dfrac{b}{a} \in F$ donc il n'y a pas d'extension, $G = \{1\}$

Deg 2: Soit $f(t) \in F[t]$, $\deg f = 2$ alors $f(t) = t^2 + bt + c$ (on peut diviser par le coefficient dominant pour simplifier le polynôme, ça ne change pas l'irreductibilité de f).
Si f est réductible alors les facteurs sont de degré 1, il n'y a pas d'extension et $G = \{1\}$.
Si f est irréductible, alors son corps de décomposition est $F(\alpha)$ où α est une des deux options:

$$\alpha = \frac{-b + \sqrt{b^2 - 4c}}{2} \quad \text{ou} \quad \frac{-b - \sqrt{b^2 - 4c}}{2}$$

Donc $F(\alpha)/F$ est Galois et $|\operatorname{Gal}(F(\alpha)/F)| = 2$, donc le groupe associé est $G = \{1, \tau\}$ où

$$\tau(\sqrt{b^2-4c}) = -\sqrt{b^2-4c}$$

$F(\alpha) = F(\sqrt{d})$ où $d := b^2 - 4c$, le discriminant, qui est égal à $(\alpha_1 - \alpha_2)^2$. Et $t^2 - d$ est irréductible si et seulement si $d \neq a^2$ pour $a \in F$.

Deg 3: Soit $f \in F[t]$, $\deg f = 3$. Si f est réductible $f(t) = (t-a)g(t)$ où g est de degré 2 et $a \in F$. Soit alors:

$$D := \prod_{i<j}(\alpha_i - \alpha_j) \quad \text{donc} \quad D = \Delta^2$$

Notons que pour $\sigma \in Gal(\,F(\alpha_1, \alpha_2, \alpha_3)/F\,)$, $\sigma(D) = D$ et $\sigma(\Delta) = \pm\Delta$. Si $\sigma(D) = D \implies D \in F$. En fait si $f(x) = x^3 + px + q$ alors $D = -4p^3 - 27q^2$

Proposition

Soit f irréductible sur F de degré 3. Soit K son corps de décomposition et $G := \operatorname{Gal}(K/F)$. Alors

$$G \cong S_3 \iff D \quad \text{n'est pas un carré dans } F \ (\Delta \notin F)$$

Et si $D = a^2$, $a \in F$ alors $[K : F] = 3$ et $G \cong S_3$.

Démonstration:
Supposons que $D = a^2$ avec $a \in F$.
$a = \pm\Delta$ et $\sigma(\Delta) = \Delta \quad \forall \sigma \in G$. Alors $\phi : G \to S_3$ et $\phi(G) \subset A_3$.
En effet $|S_3| = 3! = 6$, $|A_3| = \dfrac{|S_3|}{2} = 3 \implies A_3 = C_3 = \{1, \tau, \tau^2\}$ D'autre part $[K : F] \geq [F(\alpha_1) : F] \overset{\text{irré.}}{=} 3$
Donc $[K : F] = |\operatorname{Gal}(K/F)| = 3$ et $G \cong S_3$ OK

Supposons maintenant que $\sqrt{D} \notin F$, alors $[F(\Delta) : F] = 2$, par irréductibilité $[F(\alpha_1) : F] = 3$, mais alors $[F(\alpha_1, \Delta) : F] = 6 \implies |G| \geq 6$ mais $\phi : G \to S_3$ est une fonction injective, donc $G \cong S_3$

□

Remarque: Cette preuve nous donne que $K = F(\alpha, \sqrt{\Delta})$ où α est une racine.

Exemple

Prenons par exemple $f(t) := t^3 - 3t + 1$, est-il irréductible ?
En étudiant la fonction simplement, $f'(t) = 3t^2 - 3 \implies f'(t) = 0 \iff t = \pm 1$ et $f(-2) < 0 < f(2) \implies$ les 3 racines réelles sont dans $[-2, 2]$ mais on remarque que $f(n) \neq 0$ pour $n = -2, -1, \ldots, 2$ et donc f est irréductible sur $\mathbb{Z}$ et par Gauss aussi sur $\mathbb{Q}$.
Calculons le discriminant:

$$D = -4(-3)^3 - 27 \cdot 1^2 = 3^4 \implies \sqrt{D} = 9 \in \mathbb{Q} \implies K = \mathbb{Q}(\alpha) \quad \text{et} \quad \operatorname{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = C_3$$

Nous venons de trouver un exemple où le groupe de Galois n'est pas le groupe S_n entier.

Définition

On dit que K/F est abélien, cyclique résoluble si $\operatorname{Gal}(K/F)$ est abélien, cyclique résoluble.

Problème inconnu

Donné un groupe G fini, est-ce qu'il existe $K/\mathbb{Q}$ avec $\operatorname{Gal}(K/\mathbb{Q}) = G$?

Problème central

Mieux comprendre le groupe $\mathrm{Gal}(\mathbb{Q}^a/\mathbb{Q})$, en particulier ses représentations linéaires. (Q^a = tout les nombres algébriques)

9.7 Rappel sur les groupes résolubles

Soit G un groupe. On dit que G résoluble s'il existe une suite de sous-groupes H_i tels que:

$$G = H_0 > H_1 > \cdots > H_r = \{e\} \quad \text{où} \quad H_i \triangleleft H_{i-1} \quad \text{et} \quad {}^{H_{i-1}}\Big/_{H_i} \quad \text{est abélien } (\forall i)$$

Pour des groupes G fini, cela équivaut à trouver pour chaque quotient un isomorphisme pour un certain groupe cyclique C_p (p premier). Nous avons aussi vu que les sous-groupes et quotients de groupes résolubles sont aussi résolubles.
De l'autre côté du spectre il y a les groupes simples qui ne possèdent aucun sous-groupe normal (sauf les sous-groupes triviaux). C'est pour cette raison qu'il sont considérés comme l'équivalant des nombres premiers pour les groupes. Il existe d'ailleurs une classification des groupes finis simples. Voyons quelques exemples:

1. Les groupes abéliens sont résolubles.

2. Le groupes cycliques d'ordres premiers sont les seuls groupes simples et résolubles.

3. Les groupes symétriques S_1, S_2, S_3, S_4 sont résolubles, mais S_5 ne l'est plus.

   – $$A_3 \cong C_3 \implies S_3 \underbrace{\triangleright}_{C_2} A_3 \underbrace{\triangleright}_{C_3} 1$$

   – $$S_4 \underbrace{\triangleright}_{C_2} A_4 \underbrace{\triangleright}_{C_3} V \underbrace{\triangleright}_{C_2 \times C_2} 1$$

   – S_5 ne l'est pas car $A_5 \triangleleft S_5$ est simple et non abélien.

4. Les p groupes d'ordre p^k sont résolubles et même nilpotents.

5. Tout groupe d'ordre < 60 est résoluble. Notons que $|A_5| = \dfrac{5!}{2} = 60$.

6. Burnside: Tout groupe d'ordre $p^a \cdot q^b$, p et q premiers, est résoluble. Notons encore que $60 = 2 \cdot 2\dot{3} \cdot 5$ n'est juste pas de cette forme.

7. Le théorème de Feit-Thompson (1963) nous dit que tout groupe fini d'ordre impair est résoluble. La preuve fait 250 pages.

9.8 Solutions par radicaux

Intuition

L'idée intuitive qu'on se fait d'un radical est un nombre qui pourrait, par exemple, s'écrire sous cette forme:

$$\sqrt[3]{11} \cdot \sqrt[5]{\frac{7+\sqrt{3}}{2}} + \sqrt[4]{1+\sqrt[3]{4}}$$

Ce nombre appartient à une extension de $\mathbb{Q}$ par le cheminement:

$$\alpha := \sqrt[3]{11} \rightsquigarrow \beta := \sqrt{3} \rightsquigarrow \gamma := \sqrt[5]{\frac{7+\beta}{2}} \rightsquigarrow \delta := \sqrt[3]{4} \rightsquigarrow \varepsilon := \sqrt[4]{1+\delta}$$

Définitions

1. On dit que L/K dans $\mathbb{C}$ est une extension radical si $L = K(\alpha_1, \ldots, \alpha_m)$ et $\forall j = 1, \ldots, m$, $\exists n_j$ tel que:
$$\alpha_j^{n_j} \in K(\alpha_1, \ldots, \alpha_{j-1})$$

2. Soit $f \in F[t]$, $F \subset \mathbb{C}$. Soit K le corps de décomposition de f. On dit que $f(t) = 0$ est résoluble par radicaux s'il existe une extension $M \supset K$ telle que M/F est radical.

3. Le groupe de Galois du polynôme $f \in F[t]$ est $\mathrm{Gal}(K/F)$ où K est le corps de décomposition de f.

Théorème

Soit $f \in F[t]$, $F \subset \mathbb{C}$. L'équation $f(t) = 0$ est résoluble par radicaux si et seulement si le groupe de Galois de f est résoluble.

Nous utilisons donc tout le pouvoir de la théorie des groupes et de Galois pour résoudre un ancien problème concernant les polynômes, magique n'est ce pas ?

Lemme

Soient $K \subset \mathbb{C}$ et L le corps de décomposition de $t^p - 1$ sur K où p est premier. Alors $\mathrm{Gal}(L/K)$ est abélien, et en fait:

$$\mathrm{Gal}(L/K) \cong C_{p-1}$$

Démonstration:
$f(t) = t^p - 1 = (t-1)(t^{p-1} + t^{p-2} + \cdots + t + 1)$ et $f'(t) = p \cdot t^{p-1} \neq 0$ sauf en $t = 0$ qui n'est pas une racine. Donc f a des racines distinctes. Ce sont les racines p-ème de l'unité: $t_k := \exp\left(2\pi i \cdot \frac{k}{p}\right)$ pour $k = 0, 1, \ldots, p-1$.
Ces racines forment un groupe cyclique, posons $\varepsilon := t_1$ et alors μ_p (les racines p-ème de l'unité) est généré par ε:

$$\mu_p = \{1, \varepsilon, \ldots, \varepsilon^{p-1}\}$$

Donc $L = K(\varepsilon)$. Le polynôme $t^{p-1} + t^{p-2} + \cdots + t + 1$ est irréductible par Eisenstein:

$$t^{p-1} + t^{p-2} + \cdots + t + 1 = \frac{1-t^p}{1-t} = \frac{(u+1)^p - 1}{u} = u^{p-1} + a_{p-2} \cdot u^{p-2} + \cdots + a_1 \cdot u + p \rightsquigarrow \text{Eisenstein avec } p$$

Cela nous montre donc que $|\mathrm{Gal}(K(\varepsilon)/K)| = [K(\varepsilon) : K] = p - 1$.

Donc prenons $\phi \in \mathrm{Gal}(\,L/K\,)$. ϕ est déterminé par $\phi(\varepsilon)$ car:

$$\phi(a + b\varepsilon + \cdots + y\varepsilon^n) = \phi(a) + \phi(b)\phi(\varepsilon) + \cdots + \phi(y)\phi(\varepsilon)^n = a + b\phi(\varepsilon) + \cdots + y\phi(\varepsilon)^n$$

On sait que $0 = \phi(f(\varepsilon)) = f(\phi(\varepsilon))$ car ϕ fixe les coefficients de f. Donc en fait:

$$\phi(\varepsilon) = \varepsilon^k \quad \text{pour un certain } k, \text{ et} \quad \phi(\varepsilon^n) = \phi(\varepsilon)^n = (\varepsilon^k)^n = \varepsilon^{kn}$$

Prenons un autre automorphisme τ où $\tau(\varepsilon) = \varepsilon^\ell$ avec $k \neq \ell$. Alors:

$$\phi\tau(\varepsilon) = \phi(\varepsilon^\ell) = \varepsilon^{\ell k} = (\varepsilon^k)^\ell = \tau\phi(\varepsilon)$$

Les automorphismes commutent et donc le groupe de Galois est abélien.

Nous avons alors un isomorphisme de groupe: $\mathrm{Gal}(\,L/K\,) \longrightarrow \left(\left(\mathbb{Z}/p\mathbb{Z} \right)^*, \cdot \right)$.
Comme $\sigma_k\sigma_\ell \mapsto k \cdot \ell$ l'isomorphisme est défini comme:

$$\begin{array}{ccc} id & \longmapsto & 1 \\ \sigma_1 & \longmapsto & 2 \\ & \vdots & \\ \sigma_k & \longmapsto & k \\ & \vdots & \\ \sigma_{p-1} & \longmapsto & p-1 \end{array}$$

Le groupe $\mathrm{Gal}(\,L/K\,)$ est donc isomorphe au groupe cyclique C_{p-1}.

□

Nous n'allons pas faire la démonstration de l'équivalence entre la résolution par radicaux d'une équation et la résolution de son groupe de Galois. C'est une preuve un poil technique et nous manquons de temps mais voici une idée intuitive:

On peut obtenir les solution de l'équation $f(t) = 0$ par radical si toutes les racines sont contenues dans une extension obtenue par l'ajout de racines d'équations $x^n - a = 0$. Le Lemme précédent indique que ces extensions sont abéliennes.
Par la correspondence de Galois, une suite de sous-corps correspond aux sous-groupes. L'extension par radical correspond dans cette suite à ce que chaque extension soit abélienne (le groupe Galois associé).

9.9 Un exemple

Proposition

Le polynôme $t^5 - 6t + 3 \in \mathbb{Q}[t]$ n'est pas résoluble par radicaux.

Lemme

Soient p premier, $f \in \mathbb{Q}[t]$ irréductible de degré p. Supposons que f possède exactement 2 racines non-réelles. Alors le groupe de Galois sur $\mathbb{Q}$ du polynôme est isomorphe à S_p.

Démonstration:
Soit L le corps de décomposition de f. Donc $\mathbb{Q} \subset L \subset \mathbb{C}$ et posons $G := \mathrm{Gal}(L/\mathbb{Q})$. f irréductible implique que f possède p racines distinctes. Soit α tel que $f(\alpha) = 0$. Considérons alors:

$$L \supset \mathbb{Q}(\alpha) \supset \mathbb{Q} \quad \text{et} \quad [\mathbb{Q}(\alpha) : \mathbb{Q}] = p \quad \text{car } f \text{ irréductible de degré } p$$

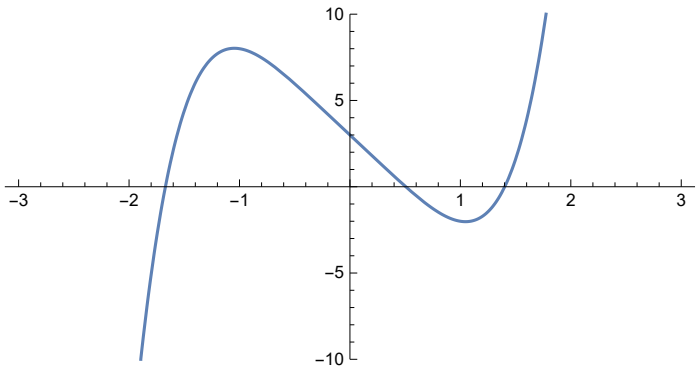
Alors $p \mid |G|$, $G < S_p$. Par Cauchy il existe un élément $\sigma \in G$ d'ordre p. Donc un p-cycle $\sigma = (1, 2, 3, \ldots, p)$. Une $\mathbb{C}$-conjugaison τ fixe $\mathbb{R}$ et permute les deux racines non-réelles $\tau = (1\ \ 2)$ (On va supposer ici que $\sigma\ :\ 1 \longmapsto 2$ car on peut toujours remplacer σ par σ^n s'il le faut. $\sigma^n\ :\ 1 \overset{\sigma}{\mapsto} \cdots \overset{\sigma}{\mapsto} 2$)
On sait que S_n est engendré par σ et τ (un n-cycle et une transposition) et donc $\mathrm{Gal}(L/\mathbb{Q}) \cong S_p$

□

Démonstration de la proposition
On remarque que $f(t) = t^5 - 6t + 3$ est irréductible sur $\mathbb{Q}$ en passant par Eisenstein avec $p = 3$. Le polynôme possède alors 5 racines distinctes, de plus 3 racines sont réelles. On peut pour cela étudier f entre $[-2, 2]$, trouver les maxima en résolvant:

$$0 = f'(t) = 5t^4 - 6 \implies t = \pm\sqrt[4]{\frac{6}{5}} \approx \pm 1$$

On peut, en utilisant les valeurs de $f(n)$ pour $n = -2, \ldots, 2$ et la position des maxima tracer un graph de f. (Même un graph approximatif suffit pour comprendre que f possède 3 racines réelles)



Par le lemme précédent, le groupe de Galois est S_5 entier. S_5 n'est pas résoluble et donc par le théorème, f n'est pas résoluble par radicaux.

□

Cela implique en particulier que l'équation $t^5 - 6t + 3 = 0$ n'a pas de solution "radical", donc qui pourrait ressembler à un nombre du style: $\left(\sqrt[15]{3} - \sqrt[15]{6}\right)^3 - \left(\sqrt[15]{18} + \sqrt[3]{25}\right)^2$. Pour prouver cela on est passé par pleins de chapitres et théorèmes, Théorème fondamental d'algèbre, Théorème de Galois, Théorème de Cauchy et plein d'autres notions encore.