Théorie de Galois

printemps 2017

Université de Neuchâtel

Enseigné par Ana Khukhro
Notes prises par Laurent Hayez

Date de création: 23 février 2017
Dernière modification: 24 février 2017

Table des matières

Chapitre 0

Introduction et histoire

Babylone vers 1600 av. J.-C., solution de l'équation du second degré.

$$ax^2 + bx + c = 0 \iff x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

En ~1540 ap. J.-C., Caradano et Ferrari donnent une solution pour les polynômes de degré jusqu'à 4. La question restait ouverte pour les polynômes de degrés plus grands ou égal à 5. « Résolubles par radicaux » ? Évariste GALOIS (1811-1832) donne la solution.

Si $p(x)$ est un polynôme et E une extension d'un corps K $\begin{smallmatrix} E \\ | \\ K \end{smallmatrix}$, son idée est de construire un groupe à partir de E.

Il y a également des constructions à la règle et au compas (Grèce : Euclide, etc. en 300/400 av. J.-C. environ), par exemple donner l'ensemble des points équidistants à un point A et un point B. Il y a des questions que les grecs n'ont pas réussi à résoudre, par exemple

- la trisection de l'angle (partager un angle en 3) ;
- la quadrature du cercle ;
- la duplication du cube (cube donné, trouver un cube plus grand ayant le double du volume).

Chapitre 1

Rappels et notions basiques

Définition 1.1. Un **anneau** est un ensemble A muni de deux opérations (lois) de composition appelées respectivement addition et multiplication satisfaisant :

- pour l'addition, A est un groupe commutatif ;
- la multiplication est associative et possède un élément neutre (**unité**) ;
- la multiplication est distributive par rapport à l'addition.

Dans le reste du cours, tout anneau sera commutatif !

- A^* est le groupe multiplicatif de A, c'est-à-dire l'ensemble des éléments inversibles par rapport à la multiplication.
- Un **sous-anneau** B de A est une partie de A qui est un sous-groupe additif, qui est stable par multiplication, et contient l'élément neutre. Par exemple, $\mathbb{Z}$ et $\mathbb{Q}$ sont des anneaux, et comme $\mathbb{Z} \subset \mathbb{Q}$, $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$.
- Un **idéal** I de A est un sous-groupe du groupe additif de A tel que pour tout $x \in A$ et $a \in I$, alors $xa \in I$. Par exemple $n\mathbb{Z} \subset \mathbb{Z}$ sont des idéaux de $\mathbb{Z}$ pour tout $n \in \mathbb{N}$.
- L'**idéal principal** engendré par $a \in A$ est $Aa = \{xa \mid x \in A\} =: (a)$.
- Un **anneau principal** est un anneau **intègre** (si $ab = 0$, alors $a = 0$ ou $b = 0$, i.e., pas de diviseur de 0) où tout idéal est principal.
- Un idéal $p \neq A$ de A est dit **premier** si les conditions équivalentes suivantes sont satisfaites :
  - l'anneau A/p est intègre ;
  - pour tous $x, y \in A$ et $xy \in p$, alors $x \in p$ ou $y \in p$.
  - p est le noyau d'un homomorphisme de A dans un corps.
- m est un **idéal maximal** si $m \neq A$ et $m \subset I$ un autre idéal, alors $I = m$.
- Si m est maximal, alors m est premier. La réciproque est vraie dans un anneau principal, un idéal non-nul premier est maximal.
- Chaque $I \neq A$ est contenu dans un idéal maximal.
- Un anneau $K \neq 0$ est un **corps** si tout élément non-nul de K est inversible.
- Soit A un anneau, I un idéal de A. I est premier ssi A/I est intègre et I est maximal ssi A/I est un corps.

- Soit K un corps. $K[X]$ est l'anneau des polynômes à coefficients dans K. $K[X]$ est un anneau principal.
- Les idéaux premiers de $K[X]$ sont
  - (0) (car $K[X]$ est intègre) ;
  - (f) pour $f \in K[X]$ est un polynôme irréductible (un élément $a \in A$, $a \neq 0$, anneau intègre, est **irréductible** si a n'est pas inversible et si $a = bc$, alors b ou c est inversible).
- Un polynôme est irréductible s'il est non-constant et il n'est pas un produit de deux polynômes non-constants de degrés inférieurs.
- Tout idéal premier non-nul de $K[X]$ est maximal.
- Sont équivalentes pour $f \neq 0 \in K[X]$:
  - f est irréductible ;
  - (f) est premier ;
  - $K[X]/(f)$ est intègre ;
  - (f) est maximal ;
  - $K[X]/(f)$ est un corps.

Exemples 1.2.
- $K = \mathbb{R}$, $f(X) = X^2 + 1$. Alors $\mathbb{R}[X]/(f) \simeq \mathbb{C}$.
- $K = \mathbb{F}_2$, $f(X) = X^2 + X + 1$, alors $\mathbb{F}_2[X]/(f) \simeq \mathbb{F}_4$.

★

- Un anneau A est dit **factoriel** si A est intègre et tout élément $a \neq 0 \in A$ s'écrit comme produit
$$a = u \prod_{i \in I} p_i$$
où $u \in A^*$ et $\{p_i \mid i \in I\}$ est un ensemble fini d'éléments irréductibles (unique à multiplication près).
- Tout anneau principal est factoriel ($\mathbb{Z}$, $K[X]$, ...).
- Si A est factoriel, alors $A[X]$ l'est aussi.
- Les éléments irréductibles de $A[X]$ sont les éléments irréductibles de A et les polynômes non-constant avec pgdc des coefficients égal à 1, qui restent irréductibles dans $K[X]$, où K est le corps de fractions de A.
- Dans un anneau factoriel, un élément irréductible p engendre un idéal premier.

1.1 Critères d'irréductibilité

Soit A un anneau factoriel et soit K son corps de fractions.

Critère d'Eisenstein : soit $f(X) = a_nX^n + \cdots + a_0$ un polynôme de degré $n \geq 1$ dans $A[X]$. Soit p un élément irréductible de A. Si $a_n \not\equiv 0 \pmod p$, $a_i \equiv 0 \pmod p$ pour tout $i < n$ et $a_0 \not\equiv 0 \pmod{p^2}$, alors $f(X)$ est irréductible dans $K[X]$.

Exemple 1.3. Soit $f(X) = \frac{2}{9}X^5 + \frac{5}{3}X^4 + X^3 + \frac{1}{3} \in \mathbb{Q}[X]$. En multipliant par 9, on obtient un polynôme dans $\mathbb{Z}[X]$. Ainsi $f(X)$ est irréductible si et seulement si $9f(X) = 2X^5 + 15X^4 + 9X^3 + 3$ est irréductible. Par le critère d'Eisenstein pour $p = 3$, $f(X)$ est irréductible dans $\mathbb{Q}[X]$. ★

Réduction : soit $f(X) = a_nX^n + \cdots + a_0$ monique ($a_n = 1$) et soit $p \in A$ irréductible. Soit $\overline{f}$ l'image de f dans $A/(p)[X]$. Si $\overline{f}$ est irréductible dans $A/(p)[X]$, il l'est aussi dans $A[X]$ (et aussi $K[X]$).

Exemple 1.4. Soit $f(X) = X^3 + 2X^2 + X + 5 \in \mathbb{Q}[X]$. On prend $p = 2$. $\overline{f}(X) = X^3 + X + 1 \in \mathbb{Z}/2\mathbb{Z}[X]$. On remarque que s'il existait une factorisation non triviale de $\overline{f}$, alors l'un des polynôme serait de la forme $(X - \xi)$, i.e., il admettrait une racine. Comme on vérifie facilement qu'il n'en possède pas, $\overline{f}$ est irréductible, et donc f aussi. ★

Dérivation et racines multiples : Soit A un anneau. On définit la dérivation par $D : A[X] \to A[X]$, $a_nX^n + \cdots + a_0 \mapsto na_nX^{n-1} + \cdots + a_1$.

- D est A-linéaire.
- $D(fg) = D(f)g + fD(g)$.
- $D((x-a)^m) = m(x-a)^{m-1}$.

Définition 1.5. Soit K un corps et soit $f \in K[X]$. Soit $a \in K$ une racine de f. On peut écrire $f(X) = (X-a)^m g(X)$ où $g(X)$ est premier avec $(X-a)$, et m est appelée la **multiplicité** de a et on dit que a une **racine multiple** si $m > 1$.

Proposition 1.6. *Un élément $a \in K$ est une racine multiple de f ssi a est une racine de f et $D(f)(a) = 0$.*

Preuve. Exercice. □

1.2 Caractéristique d'un corps

Soit K un corps. On considère l'homomorphisme d'anneau

$$\begin{array}{cccc} \eta & \mathbb{Z} & \to & K \\ & n & \mapsto & \operatorname{sgn}(n) \cdot (\underbrace{1 + 1 + \cdots + 1}_{n \text{ fois}}) \end{array}$$

$\ker(\eta)$ est un idéal premier de $\mathbb{Z}$, car $\mathbb{Z}/\ker(\eta) \simeq \mathrm{Im}(\eta) \subset K$ est un anneau intègre. Il y a deux cas :

- $\ker(\eta) = \{0\}$ et donc η est injective, $\mathbb{Z}$ est un sous-anneau de K, et K contient le corps de fractions de $\mathbb{Z}$. Dans ce cas, on dit que K est de **caractéristique** 0.
- $\ker(\eta) = p\mathbb{Z}$, p premier. p est la **caractéristique** de K. Dans ce cas, $\mathbb{F}_p$ est un sous-corps de K et $\underbrace{1 + 1 + \cdots + 1}_{p \text{ fois}} = 0$ dans K.