Algèbre M1 S2

THOMAS DELZANT

Prologue

Il s'agit d'un cours d'algèbre de master 1. Les étudiants ont déjà rencontré en L3 les notions de base : groupes, anneaux, corps et des exemples importants.

Bibliographie.

Il y a d'abord et avant tout Algebra de van der Waerden (tome 1 et 2). Ce livre écrit dans les années 1930 à partir de deux cours d'E. Artin et d'E. Noether a fixé (devrai-je dire figé?) la façon de présenter le sujet, qui n'a pratiquement pas évolué depuis.

Sinon, pour pour écrire ce cours, j'ai consulté :

Demazure, Michel. Cours d'algèbre. Avec une ouverture sur les applications à la cryptographie
Fulton, William. Algebraic curves. Livre dont j'ai repris a peu près mot à mot le chapitre 1 pour écrire la quatrième partie de ce cours.
Jacobson, Nathan. Basic Algebra, t.1. Un livre de référence.
Perrin, Daniel. Cours d'algèbre. Spécial agrégatif, avec beaucoup d'exercices.
Stewart, Ian. Galois Theory. Facile d'accès, très détaillé, avec de nombreux exemples.
Samuel, Pierre. Théorie Algébrique des nombres. Un peu rapide pour le niveau de ce cours.

Par ailleurs, le livre de Serge Lang (Algebra) est très synthétique et une excellente référence sur la théorie de Galois (je ne le recommanderai pas forcément sur d'autres sujets...). Il contient de nombreux exercices intéressants, pour ceux qui veulent aller plus loin.

Avertissement 1. Ce cours ne contient rien d'original.
Le seul point sur lequel nous avons un point de vue différent de la littérature est la notion de corps de rupture d'un polynôme P de $\mathbb{K}[X]$. Pour nous, il s'agit d'un couple $(\mathbb{L}, x_0)$ composé d'une extension du corps $\mathbb{K}$ et d'un élément de $\mathbb{L}$ dont le polynôme minimal est précisément P.

Les énoncés, les démonstrations, les exercices et les problèmes ont tous (sauf une dizaine) été pris soit dans l'un de ces excellents ouvrages ci-dessus, ou alors dans les listes d'exercices donnés par H. Carayol les années précédentes. Ce cours ne contient donc rien d'original, certaines parties sont même directement *copiées* des ouvrages ci dessus.

La partie « anneaux » (sauf 1.4) reprend beaucoup le cours d'algèbre de Perrin, avec l'aide de Samuel.
La partie 1.4 est prise chez Jacobson.
La partie « corps » reprend le cours d'algèbre de Perrin et celui de Demazure.
La partie Galois est un mix de Jacobson, Stewart et Lang.
La partie « ensembles algébriques » est (presque) recopiée de Fulton.

Remarque 1. Le mot « homomorphisme » est formé à partir du nom grec $\mu o \rho \varphi \eta$ « la forme » et de l'adjectif $o \mu o \sigma$, semblable.

Dire qu'une application est un homomorphisme, c'est dire qu'elle relie deux objets semblables. Depuis quelques années, certains auteurs -surtout français- utilisent le mot « morphisme » au lieu de « homomorphisme », dans le cas des groupes, anneaux ou corps, comme si le préfixe « homo » posait problème à certains. Comme ni Demazure, ni Jacobson, ni Fulton, ni Lang, ni Perrin, ni Stewart ni van der Waerden ne le font, nous ne le ferons pas non plus.

Contenu du programme de Master de Mathématiques Fondamentales de l'Université de Strasbourg

1. Anneaux. Idéaux premiers, idéaux maximaux ; anneaux quotients ; anneaux noethériens et factoriels, exemples (anneaux de polynômes en plusieurs variables).

2. Corps. Extensions de corps, corps de rupture, corps de décomposition, clôtures algébriques ; existence et unicité des corps finis. Extensions cyclotomiques.

3. Théorie de Galois. Automorphismes, groupe de Galois ; extensions galoisiennes, théorème d'Artin ; extensions normales, extensions séparables; correspondance de Galois.

4.Nullstellensatz et premiers exemples de géométrie algébrique.

Seules les parties 1 et 2 sont au programme du concours d'agrégation. Nous y consacrerons donc plus de temps qu'aux parties 3 et 4. Les 50 exercices qui sont proposés pour ces deux parties le sont dans cet objectif.

Table des matières

Chapitre 1

Anneaux

Il s'agit d'un second cours sur ce sujet, et les étudiants connaissent déjà cette notion, ainsi que la notion de corps, et quelques exemples.

Les deux familles d'exemples importants d'anneaux commutatifs sont les anneaux de fonctions d'une part, les exemples provenant de l'arithmétique de l'autre. Les anneaux de polynômes sont à l'interface entre ces deux familles.

Convention 1.1. Tous les anneaux sont commutatifs et unitaire.

Avertissement 1.1. Dans ce chapitre, nous utilisons beaucoup les ouvrages suivants : [Perrin], [Samuel], tant pour le cours que pour les exercices.

1.1. Exemples et rappels de L3.

1.1.1. Définitions.

Définition 1.1. *Un anneau $(A, +, \times)$ est un ensemble A muni de deux lois de composition commutatives telles que $(A, +)$ est un groupe d'élément neutre 0, la loi $\times$ est associative, possède une unité notée 1 (c'est à dire que pour tout élément a de A, $1 \times a = a$), et est distributive par rapport à la loi $+$.*

Exemple 1.1. $(\mathbb{Z}, +, \times)$, $(\mathbb{Z}/p\mathbb{Z}, +, \times)$, $\mathbb{K}[X]$, $\mathbb{Z}[X]$, $\mathbb{R}[X, Y]$, $\mathbb{R}^E$ = fonctions de E à valeurs dans $\mathbb{R}$. On sait ajouter et multiplier les fonctions à valeurs réelles.

Axiome 1.1. *La loi $\times$ est distributive par rapport à la loi $+$ si :*
$\forall a, b, c \in A^3$, *on a* $a \times (b + c) = a \times b + a \times c$

Convention 1.2. Sauf si cela est vraiment utile on oublie de noter la multiplication explicitement c'est à dire que ab désigne le produit $a \times b$.

On a une notion évidente d'homomorphisme d'anneaux.

Définition 1.2. *Soient $(A, +, \times)$ et $(B, +, \times)$ deux anneaux. Une application $f : A \to B$ est un homomorphisme d'anneaux si f conserve multiplication et addition c'est à dire si pour tout couple a, a' d'élément de A, $f(aa') = f(a)\, f(a')$ et $f(a + a') = f(a) + f(a')$*

Un exemple important est l'homomorphisme dit « caractéristique ».

Proposition 1.1. *Si $(A, +, \times)$ et un anneau il existe un unique homomorphisme $\chi : \mathbb{Z} \to A$ tel que $\chi(1) = 1$.*

Démonstration. voir l'exercice 1. Noter qu'il faut utiliser une récurrence pour définir χ. □

On a aussi une notion évidente de sous-anneau.

Définition 1.3. *Si $(B, +, \times)$ est un anneau et A un partie de B, on dit que A est un sous-anneau si A contient l'unité ($1 \in A$), est stable par addition et multiplication.*

Exemple 1.2. Si $f: A \to B$ est un homomorphisme l'image de A est un sous anneau (pourvu que que $f(1) = 1$. En particulier l'image de $\mathbb{Z}$ par 'homomorphisme caractéristique est un sous anneau.

PROPOSITION 1.2. *L'image de l'homomorphisme caractéristique est isomorphe soit à $\mathbb{Z}$ soit à $\mathbb{Z}/n\mathbb{Z}$.*

Démonstration. *Si χ est injectif, c'est un isomorphisme sur son image, sinon son noyau est de la forme $n\mathbb{Z}$ et χ passe au quotient en un homomorphisme injectif $\mathbb{Z}/n\mathbb{Z} \to A$.* □

Comme l'intersection de deux sous anneaux est un sous anneau, on peut fabriquer le plus petit sous anneau contenant une partie donnée.

En effet si $X \subset A$ est une partie, l'intersection $\cap_{X \in B \subset A, \text{sousanneau}} B$ est un anneau, et c'est le plus petit qui contient X. On appelle l'anneau engendré par cette partie X.

DÉFINITION 1.4. *Dans l'anneau A on dit que d divise a et l'on note $d|a$ si il existe b tel que $a = d.b$*

DÉFINITION 1.5. *Un diviseur de 0 dans l'anneau A c'est un élément a non nul tel qu'il existe un b non nul avec $ab = 0$.*

Exemple 1.3. Dans $\mathbb{Z}/ab\mathbb{Z}$ l'image de a est un diviseur de 0 car dans cet anneau $ab = 0$.

DÉFINITION 1.6. *Un anneau est dit intègre si la loi de multiplication n'a pas de diviseur de 0, autrement dit si le produit de deux éléments non nuls est non nul.*
Formellement : $\forall a, b \in A - \{0\}, ab = 0 \Rightarrow a = 0 \quad \text{ou} \quad b = 0$.

Exemple 1.4. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est un nombre premier, comme on l'a vu en licence.

DÉFINITION 1.7. *Dans l'anneau A un élément a est inversible si il existe un élément b tel que $ab = 1$. On note A^* l'ensemble des inversibles de A.*

Remarque 1.1. Un diviseur de 0 n'est jamais inversible.

Question 1. A travailler à la maison. Si $\Omega \subset \mathbb{C}$ l'anneau des fonctions holomorphes sur Ω est intègre si et seulement Ω est connexe.

PROPOSITION 1.3. *Muni de la multiplication, $(A^*, \times)$ est un groupe abélien.*

Exemple 1.5. Si $A = \mathbb{Z}, A^* = \{\pm 1\}$, si $A = \mathbb{K}[X], A^* = \mathbb{K}^*$, si $A = \mathbb{Z}[i] = \mathbb{Z} + i\mathbb{Z} \subset \mathbb{C}, A^* = \{\pm 1, \pm i\}$.

DÉFINITION 1.8. *Un corps est un anneau dans lequel tout élément est inversible.*

THÉORÈME 1.1. *Si A est un anneau intègre, il existe un corps, unique à isomorphisme près qui contient A et dont tout élément s'écrit comme produit d'un élément de A et de l'inverse d'un autre. On l'appelle le corps de fraction de A.*□

Nous ne démontrerons pas ce théorème, mais laissons la démonstration en exercice.

Prendre $\mathbb{K} = A \times \{A - 0\}/\sim$, où $\sim$ est la relation $(a, b) \sim (a', b')$ si $ab' = ba'$. Les éléments de $\mathbb{K}$ sont les fractions $\frac{a}{b}$ où $b \neq 0$. On définit $\frac{a}{b} + \frac{c}{d} = \frac{da + bc}{bd}$, $\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$ et on doit vérifier que dans $\mathbb{K}$ ces nombres ne dépendent pas du choix de a, b et c, d.

Remarque 1.2. Ce théorème devient faux pour les anneaux non commutatifs. Il y a des anneaux non commutatifs mais intègre qui ne sont contenus dans aucun corps.

Exemple 1.6. Si $\mathbb{K}$ est un corps et $A = \mathbb{K}[X]$ l'anneau de polynômes le corps des fractions de A est le corps des fractions rationnelles noté $\mathbb{K}(X)$.

1.1.2. Nombres.

Les ensembles $(\mathbb{Z},+,\times)$,$(\mathbb{Z}/n\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$ sont des anneaux, les trois derniers étant des corps.

En fait les inclusions naturelles $\mathbb{Z}\subset\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C}$ font que $\mathbb{Z}$ est un sous anneau de $\mathbb{Q}$ qui est lui même un sous-anneaux de $\mathbb{R}$ etc etc.

On peut aussi considérer des anneaux plus rigolos comme par exemple $\mathbb{Z}[\sqrt{2}]\subset\mathbb{C}$ qui est le plus petit sous anneau contenant $\mathbb{Z}$ et $\sqrt{2}$, ou alors $\mathbb{Z}[\sqrt{5},i\,]$ qui est le plus petit anneau contenant $\mathbb{Z}, i, \sqrt{5}$, on peut aussi fabriquer des corps $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(i)$, $\mathbb{Q}(j)$, $\mathbb{R}(X)$, $\mathbb{Q}(X,\sqrt{2})\subset\mathbb{C}(X)$ et nous étudierons plus tard ces objets plus en détail.

1.1.3. Fonctions.

Si X est un ensemble et $(A,+,\times)$ un anneau, l'ensemble A^X des fonctions à valeurs dans A est naturellement muni d'une structure d'anneau. On peut ajouter et multiplier les fonctions. Il est fréquent de considérer des sous-anneaux de cet anneau.

1.1.4. Polynômes.

Si A est un anneau, on forme l'anneau des polynômes à coefficients dans A , noté $A[X]$ qui est l'ensemble des combinaisons linéaires formelles $f(X)=a_0+a_1X+\cdots+a_nX^n$, ou n est un entier appelé le degré du polynôme, les a_i sont des éléments de A tels que a_n est non nul, muni de la loi d'addition évidente et de la multiplication est donnée par la formule :

$$(a_0+a_1X+\cdots+a_nX^n)\times(b_0+b_1X+\cdots+b_mX^m)=\Sigma_{k=0}^{m+n}\,(\Sigma_{i+j=k}a_ib_j)X^k$$

Attention si l'anneau n'est pas intègre, il se peut très bien que le terme a_nb_m soit nul, donc dans cette somme on convient d'oublier tous les termes nuls. Ce n'est pas très difficile de vérifier l'associativité de la loi $\times$ et sa distributivité.

Si A est un anneau, on peut considérer l'anneau des *fonctions polynômes* sur A c'est l'image de l'homomorphisme :

$F\colon A[X]\to A^A$ défini par $F(p)(x)=\Sigma_{i=0}^{n}a_i\,x^i$, si $p(X)$est le polynôme $\Sigma_{i=0}^{n}a_i\,X^i$

Autrement dit un polynôme à coefficients dans A défini une fonction sur A.

Proposition 1.4. *Soit $A\subset B$ deux anneaux, et $x\in B$. L'application d'évaluation en x définie par*

$$A[X]\to B$$
$$\Sigma_{i=0}^{n}a_iX^i\to\Sigma_{i=0}^{n}a_ix^i$$

est un homomorphisme d'anneaux dont l'image est le plus petit sous-anneau de B contenant A et x. On le note $A[x]$.

Démonstration. Pour la somme, on laisse ça en exercice, et pour le produit, à gauche on a $(a_0+a_1X+\cdots+a_nX^n)\times(b_0+b_1X+\cdots+b_mX^m)=\Sigma_{k=0}^{m+n}\,(\Sigma_{i+j=k}a_ib_j)X^k$
et à droite on connait la formule :
$(a_0+a_1x+\cdots+a_nx^n)\times(b_0+b_1x+\cdots+b_mx^m)=\Sigma_{k=0}^{m+n}\,(\Sigma_{i+j=k}a_ib_j)x^k$
qui résulte de la formule
$(a_0+....+a_n)(b_0+..+b_m)=\Sigma_{k=0}^{m+n}(\Sigma_{i+j=k}a_ib_j)$
appliquée à a_ix^i et b_jx^j. □

Avertissement 1.2. En général, il n' a aucune raison pour que les anneaux $A[X]$ et $A[x_0]$ soit isomorphes. En effet, il se peut très bien qu'un polynôme s'annule en un point x_0 de A, par exemple le polynôme $X-x_0$, et alors l'application d'évaluation n'est pas injective.

Exemple 1.7. Si d est un entier, l'anneau $\mathbb{Z}[\sqrt{d}] \subset \mathbb{C}$ est l'ensemble des combinaisons $a + b\sqrt{d}$, où $\sqrt{d}$ est l'une des deux racines de cet entier. Si d est un carré $\mathbb{Z}[\sqrt{d}] = \mathbb{Z}$. on voit bien que l'application $\mathbb{Z}[X] \to \mathbb{C}$ définie par l'image de X est $\sqrt{d}$ n'est pas injective, parce que le polynôme $X^2 - d$ est dans le noyau.

DÉFINITION 1.9. *Si $x \in \mathbb{C}$, on dit que x est algébrique si il existe un polynôme à coefficients entiers $f \in \mathbb{Z}[X]$ tel que $f(x) = 0$. Sinon, x est transcendant. Comme $\mathbb{C}$ est non dénombrable, il existe des nombres transcendants.*

NOTATION 1.1. *On note $\bar{\mathbb{Q}} \subset \mathbb{C}$ l'ensemble des nombres algébriques. Cet ensemble est dénombrable.*

En itérant la construction précédente ($A \to A[X]$) on forme l'anneau $A[X_1, ...X_d]$ des polynômes à d indéterminées (ou d variables) à coefficients dans A: $A[X_1, ...X_d] = A[X_1, ...X_{d-1}][X_d]$. Un polynôme étant une expression formelle $\Sigma_{i_1+i_2+\cdots+i_d \leqslant n} a_{i_1 i_2 .... i_d} X_1^{i_1} .... X_d^{i_d}$

On écrit volontiers $\Sigma_{|i| \leqslant d} a_i X^i$, où $i = (i_1, ..., i_n)$ est un multi-indice $\Sigma i_k = |i|$ et X^i désigne par convention $X_1^{i_1} .... X_d^{i_d}$, alors que $a_i = a_{i_1 i_2 .... i_d}$.

PROPOSITION 1.5. *Pour tout anneau A intègre les inversibles de $A[X_1, ...X_n]$ sont les inversibles de A.*

Démonstration. Par récurrence sur l'entier n.

Initialisation : Si on écrit, $(\ a_n X^n + \cdots + a_0) \times (b_m X^m + \cdots + .b_0) = 1$ on se rend compte que $m = n = 0$ et $a_0 b_0 = 1$. le coefficient en X^{n+m} est $a_n b_m \neq 0$.

Induction. On remarque que $\mathbb{P}_n$ n'est autre que la proposition $\mathbb{P}_1$ appliquée à l'anneau $A[X_1, ...X_{n-1}]$. Donc, si $n \geqslant 2$, $\mathbb{P}_{n-1} \Rightarrow \mathbb{P}_n$ □

On considère très souvent l'application de $A[X]$ dans A^A qui a un polynôme associe la fonction polynôme qu'il définit : son image est l'ensemble des fonctions polynômes sur A.

PROPOSITION 1.6. *Si A est intègre et infini, l'application $A[X] \to A^A$ qui a un polynôme associe la fonction polynôme qu'il définit est injective.*

Démonstration.
Comme A est infini, cette proposition résulte du lemme suivant vu en L3.

LEMME 1.1. *Un polynôme non nul de degré d à coefficient dans un corps s'annule en au plus d points.*

Ceci se démontre grâce à la division euclidienne et la récurrence.

On vérifie plutôt que si P s'annule en n points son degré est supérieur ou égal à d.

Initialisation Pour $d = 1$ le résultat est clair car un polynôme non nul et constant ne s'annule nulle part. Pour l'induction on raisonne ainsi : si P s'annule en $(x_1, ...x_n)$ alors P est divisible par $(X - x_n)$ et le quotient Q s'annule en $(x_1, ...x_{n-1})$, donc $\deg(Q) \geqslant n - 1$ et $\deg(P) \geqslant n$.

□

Exemple 1.8. Si, au contraire A est fini, $A = \{a_1, ...a_n\}$ le polynôme $\Pi_{1 \leqslant i \leqslant n}(X - a_i)$ n'est pas nul, mais la fonction qu'il définit l'est.

Par récurrence sur l'entier n, on déduit.

Proposition 1.7. *Si A est intègre et infini, l'application $A[X_1,...X_n] \to (A)^{(A^n)}$ est injective* □.

Sous cette hypothèse, on peut donc confondre polynôme et fonction polynôme .

1.2. Idéaux.

On fixe un anneau A.

1.2.1. Définition, congruence.

Définition 1.10. *Un idéal de A est un sous ensemble I de A qui est un sous-groupe de $(A,+)$ et tel que pour tout a dans A, $aI \subset I$.*

Si $x \in I$ et a est quelconque $ax \in I$.

Exemple 1.9. Si a est dans A, l'ensemble des multiples de a, c'est à dire $A \times a$ est un idéal. On l'appelle idéal *principal* engendré par a. Par exemple $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$.

Si $x \in aA$ il existe y tel que $x = ay$. pour $b\hat{}$quelconque $bx = (by)a$ est bien dans aA.

Exemple 1.10. Si $A = \mathbb{K}$ est un corps, les seuls idéaux de $A = \mathbb{K}$ sont 0 et $\mathbb{K}$. En effet, si I est un idéal et $a \in I$ est non nul $1/a.a$ est dans I donc 1 est dans I donc tout élément $x = x.1$ aussi.

Proposition 1.8. *Réciproquement si A est intègre et si les seuls idéaux de A sont 0 et A alors A est un corps.*

Démonstration. Si $a \neq 0$ aA est un idéal non nul donc il contient 1 il existe b tel que $ab = 1$ □

Théorème 1.2. *Dans $\mathbb{Z}$, ou dans $\mathbb{K}[X]$, où $\mathbb{K}$ est un corps tout idéal est principal.*

Démonstration. La démonstration de ce résultat est tellement importante (algorithme d'Euclide) que nous la laissons au lecteur, nous la reverrons plus tard dans le cas des anneaux euclidiens.

Indication. pour $\mathbb{Z}$ soit $I \subset \mathbb{Z}$ un idéal non réduit à 0 et $n \in I$ le plus petit entier positif de I, alors $I = n\mathbb{Z}$, pour $\mathbb{K}[X]$ soit $I \subset \mathbb{K}[X]$ un idéal non réduit à 0 et $P \in I$ un polynôme non nul de plus petit degré dans I, alors I est l'idéal principal engendré par P □

Proposition 1.9. *L'intersection d'une famille d'idéaux est un idéal.* □

Définition 1.11. *L'idéal engendré par une partie P est l'intersection de tous les idéaux contenant P.*

Proposition 1.10. *L'idéal engendré par la partie P est l'ensemble des combinaisons linéaires $a_1p_1 + \cdots + a_np_n$ des éléments de P à coefficients dans A.* □

Proposition 1.11. *Si $f: A \to B$ est un homomorphisme d'anneaux, son noyau $f^{-1}(0)$ est un idéal de A. Plus généralement, si $J \subset B$ est un idéal, alors $f^{-1}(J)$ est un idéal de A.*

Démonstration. L'image réciproque d'un sous groupe par un homomorphisme est un sous groupe, donc $f^{-1}(J)$ est un sous groupe de$A,+$. montrons qu'il est stable par multiplication externe par un élément a. En effet si $f(x) \in J$ $f(ax) = f(a) \times f(x) = b \times f(x) \in J$. □

Exemple 1.11. Soit $Y \subset X$ un sous ensemble $A^X \to A^Y$ l'homomorphisme de restriction : a une fonction sur X on associe sa restriction à Y. Alors $\ker(f)$ est l'idéal des fonctions nulles sur Y.

Si $I \subset A$ un idéal, on introduit la notion de congruence modulo I

DÉFINITION 1.12. *On dit que x est congru à y modulo I et on note $x \equiv y\,(I)$ si la différence $x-y$ est dans I*

Il s'agit d'une relation d'équivalence qui généralise la congruence modulo un entier dans $\mathbb{Z}$. Mais aussi dans le cas des fonction deux fonctions sur un ensemble X sont égales sur le sous ensemble Y si et seulement si leur différence est dans l'idéal des fonctions nulles sur Y.

Exemple 1.12.
Si $f\colon A \to B$ est un homomorphisme d'anneaux, et $I = f^{-1}(0)$ alors $x \equiv y(I)$ si et seulement si $f(x) = f(y)$.

LEMME 1.2. *Soit I un idéal de A. Si $a \equiv b(I)$ et $a' \equiv b'(I)$ alors $a+a' \equiv b+b'\,(I)$ et $aa' \equiv bb'(I)$.*

THÉORÈME 1.3. *Soit I un idéal de l'anneau A. Il existe une unique structure d'anneau sur l'ensemble quotient de A par la congruence modulo I, noté $A\,/\,I$ telle que la projection canonique $A \to A/I$ soit un homomorphisme d'anneaux, de noyau I.*□

Exemple 1.13. Si $f\colon A \to B$ est un homomorphisme d'anneaux, et $I = f^{-1}(0) = \ker(f)$ alors le quotient A/I est l'image de A par f. Le quotient de A par $\ker(f)$ et l'image de A.

Les exemples venant de l'arithmétique élémentaire sont les anneaux de congruences $\mathbb{Z}/n\mathbb{Z}$, qui ont été largement étudiés en licence.

On peut alors définir la caractéristique d'un anneau.

DÉFINITION 1.13. *Si A est un anneau, il existe un unique homomorphisme $\mathbb{Z} \to A$. Son noyau est un idéal principal de la forme $n\mathbb{Z}$, son image un anneau de congruence $\mathbb{Z}/n\mathbb{Z}$ si $n \neq 0$, ou $\mathbb{Z}$ sinon. L'entier n s'appelle la caractéristique de l'anneau A. Le sous anneau de A engendré par 1 est $\mathbb{Z}/n\mathbb{Z}$.*

PROPOSITION 1.12. *Si A est un corps, sa caractéristique est un nombre premier.*

1.2.2. Opérations sur les idéaux, lemme Chinois.

PROPOSITION 1.13. *Soit I et J deux idéaux de A. L'ensemble des éléments de A qu'on peut écrire comme somme d'un élément de I et d'un élément de J est un idéal de A, noté $I+J$. C'est le plus petit idéal contenant I et J.* □

L'addition des idéaux correspond à la notion de pgcd.

PROPOSITION 1.14. *Dans $\mathbb{Z}$, $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$, en particulier $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$ équivaut à a et b premiers entre eux.*□

Démonstration. On écrit $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Comme $a \in d\mathbb{Z}$ $d|a$, de même $d|b$. Comme $d = an + bm$, tout diviseur commun à a et b divise d. en particulier le plus grand, donc d est bien le plus grand commun diviseur de ces deux nombres. □

Remarque 1.3. Dans ce contexte l'identité de Bézout prend la forme suivante : si I et J sont « premiers entre eux », alors il existe deux éléments a dans I, b dans J dont la somme est 1.

PROPOSITION 1.15. *Soit I et J deux idéaux de A. L'ensemble des éléments de A qu'on peut écrire comme somme $a_1b_1 + \cdots + a_nb_n$ de produits d'éléments de I et de J est un idéal, noté $I.J$. C'est le plus petit idéal contenant les produits des éléments de I et de J.* □

Exemple 1.14. Dans $\mathbb{Z}$ on a $a\mathbb{Z} \times b\mathbb{Z} = (\mathrm{ab})\mathbb{Z}$. Plus généralement si $I = aA$ est l'idéal principal engendré par a et $J = bA$ l'idéal engendré par b, alors IJ est l'idéal principal engendré par ab.

On peut énoncer le célèbre lemme Chinois.

Théorème 1.4. *Soit A un anneau, I, J deux idéaux tels que $I+J=A$. Alors $A/I.J=A/I\times A/J$. Plus précisément si $\varphi: A\to A/I\times A/J$ est l'homomorphisme canonique, φ passe au quotient en un isomorphisme $\theta: A/I.J\to A/I\times A/J$.*

Démonstration. Si deux éléments sont congrus modulo IJ il sont congrus modulo I (et J)puisque $IJ\subset I$. La projection canonique $\varphi: A\to A/I\times A/J$ passe donc au quotient en un homomorphisme $\theta: A/I.J\to A/I\times A/J$. Il faut démontrer que cet homomorphisme est bijectif.

Pour cela on « écrit l'identité de Bézout » : comme $I+J=A$ on peut trouver deux élément u, v dans ces deux idéaux tels que $u+v=1$.

Pour montrer que θ est injective, on considère un élément x du noyau de φ. Celui-ci est dans $I\cap J$. Comme $x=xu+xv$ comme $x\in J$ et $u\in I$ $xu\in IJ$, de même $xv\in IJ$ et donc $x\in IJ$. Ainsi $\ker\varphi\subset IJ$. Par ailleurs si $y\in IJ$, $y\in I\cap J$ donc $y\in\ker\varphi$. Ainsi $\ker\varphi=I.J$ ce qui démontre que θ est injective.

Pour montrer que θ est surjective, il suffit de voir que φ l'est. On se donne un couple (a,b) dans $A\times A$. Comme $a=au+va=va(I)$ et $b=ub\,(J)$. Modulo I $va+ub=_{u\in I}va=a$ et modulo J, $va+ub=_{v\in J}ub=b$. Donc l'image de $va+ub$ est la classe de (a,b) dans $A/I\times A/J$ et φ est surjective. □

1.2.3. Idéaux premiers, et idéaux maximaux

Proposition 1.16. *Si $I\subset A$ est un idéal propre, les propriétés suivantes sont équivalentes.*

i. *le quotient A/I est intègre*

ii. $\forall a,b\in A,\ ab\in I\Rightarrow a\in I$ ou $b\in I$.

iii. $\forall a,b\in A,\ ab\notin I\Longleftarrow a\notin I\quad$ et $b\notin I$

Démonstration. On raisonne par équivalence. Notons que ii et iii sont des propositions contraposée l'une de l'autre. Montrons que la négation de i équivaut à celle de iii. L'anneau A/I n'est intègre si et seulement on peut trouver deux éléments non nuls α,β dont le produit est nul, si et seulement si on peut trouver deux éléments a,b dans A qui ne sont pas dans I, mais dont le produit est dans I. □

Définition 1.14. *Si A/I est intègre, on dit que I est premier. De façon équivalente si le produit de deux éléments est dans I l'un des deux y est.*

Exemple 1.15. Si $A=\mathbb{Z}$; l'idéal $n\mathbb{Z}$ est premier si et seulement si n est premier.

En effet si l'entier n n'est pas premier si il est le produit de deux éléments strictement plus petit, donc l'idéal $n\mathbb{Z}$ n'est pas premier. Réciproquement, si l'entier n et premier et si n divise un produit ab, il divise l'un des deux facteurs (Lemme de Gauss).

Définition 1.15. *Dans un ensemble ordonné, on dit qu'un élément I est maximal si il n'existe pas d'élément J strictement plus grand.*

L'ensemble qui nous intéresse ici, est l'ensemble des idéaux **propres** d'un anneau, la relation d'ordre étant l'inclusion. Propre veut dire $I\neq A$, ou $1\in I$.

On cherche a trouver des idéaux les plus gros possibles. Par exemple dans $\mathbb{Z}$ les idéaux maximaux sont les $p\mathbb{Z}$, pour p premier. Si a n'est pas premier et p un diviseur de $a\mathbb{Z}\subset p\mathbb{Z}$.

PROPOSITION 1.17. *Si $I \subset A$ est un idéal, I est maximal si et seulement si le quotient A/I est un corps.*

Démonstration. Montrons que si I est maximal, A/I est un corps. Si $\bar{x} \in A/I$ est non nul, et si x est un représentant de x, l'idéal engendré par x et I, c'est à dire $Ax + I$ est A tout entier. Donc il contient 1 et l'on peut trouver un élément y dans A tel que $xy + i = 1$, du coup vuksémodulo I $xy = 1$ dan le quotient .Donc $\bar{x}$ est bien inversible.

Réciproquement si A/I est un corps, il ne contient pas d'idéaux propre. Donc si $J \supset I$ l'image de J dans le quotient est soit 0 soit A/I tout entier et $J = I$ ou $J = A$ □

A refaire chez soit pour vérifier que $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier si et seulement si $n\mathbb{Z}$ est un idéal maximal.

Nous allons énoncer un célèbre résultat du à Krull, et qui dépend de l'axiome du choix. Donc nous en donnerons deux démonstrations, l'une dans le cas dénombrable l'autre dans le cas général.

THÉORÈME 1.5. *Tout idéal propre est contenu dans un idéal maximal propre.*

La démonstration de ce résultat n'est pas évidente, elle est basée sur l'axiome du choix. Comme toujours dans ces cas là, on peut en donner une version affaiblie à partir de l'axiome du choix dénombrable. Les deux axiomes AC, ACD sont indécidables dans les axiomatiques classiques (ZF) de la théories des ensembles.

Remarque 1.4. Les chaussettes et les chaussures de Russell : Si on a une infinité dénombrable de paires de chaussettes, il faut ACD pour choisir une chaussette de chaque paire, mais pour les chaussures ce n'est pas la peine. Pourquoi ?

1.2.3.1. Le cas dénombrable.

Démonstration. Nous démontrons donc le cas particulier ou A est **dénombrable**. On écrit $A = (a_i)_{i \in \mathbb{N}}$, en faisant attention à ce que cette numérotation soit surjective. Si $I \subset A$ est un idéal, nous allons construire **par récurrence** une suite croissante d'idéaux I_n dont la réunion sera un idéal maximal propre de A.

On pose $I_1 = I$
On suppose I_n connu. Si I_n est maximal, on pose $I_{n+1} = I_n$. Sinon, on regarde le plus petit entier k_n tel que $I_n + a_{k_n}A$ soit un idéal propre, et on pose $I_{n+1} = I_n + a_{k_n}A$.

Par construction la suite des I_n est croissante, et la réunion est donc un idéal J. Il est propre car sinon, pour un certain entier $1 \in I_n$. Si il n'est pas maximal, alors la suite des idéaux I_n est strictement croissante et la suite des entiers k_n tend vers l'infini. Alors on peut trouver un indice m tel que $J + a_m$ soit encore plus grand. Comme $k_n \to \infty$, on a un entier n tel que $k_n < m < k_{n+1}$, et l'on contredit ainsi que le choix de $a_{k_{n+1}}$. En effet $I_n + a_n A$ est un idéal propre contenant strictement I_n. □

Question 2. Où a-t-on utilisé l'axiome du choix dénombrable ?

1.2.3.2. Le cas général.

Nous allons donner une « démonstration » par la méthode connue sous le joli nom de « zornification », c'est à dire l'application du Lemme de Zorn[1.1] qui est une version utile de l'Axiome du Choix.

1.1. Max Zorn 1906-93, mathématicien allemand. Contraint de quitter l'Allemagne en 1933 car il avait été candidat aune élection sur une liste socialiste.

Dans un ensemble ordonné, une chaine est un sous-ensemble tel que la restriction de l'ordre à ce sous ensemble soit total.

Théorème 1.6. *Lemme de Zorn. Si dans un ensemble ordonné $\mathcal{I}$, toute chaine admet une borne supérieure, alors pour toute chaine C il existe un élément $I \in \mathcal{I}$ qui est maximal*

Admettons ce théorème, et démontrons le théorème de Krull.

Démonstration. Ici, $\mathcal{I} \subset P(A - \{1\})$ est l'ensemble des idéaux de A ne contenant pas 1, ordonné par l'inclusion. Evidemment si C est une famille d'idéaux telle que si I, J sont dedans, alors $I \subset J$ ou $J \subset I$ la réunion $\cup_{i \in C} I$ est un idéal. Donc il existe des idéaux maximaux. □

1.3. Anneaux principaux, anneaux factoriels.

1.3.1. Anneaux principaux.

Rappelons qu'un idéal I de A est *principal* si il existe un élément a tel que $I = aA$.

Définition 1.16. *Un anneau est principal si tout ses idéaux sont principaux.*

Avertissement 1.3. Les ouvrages internationaux font bien la distinction entre Principal Integral Domain (anneau intègre principal) et Principal Ideal *Ring* pas forcément intègre.

Les deux exemples de base sont l'anneau $\mathbb{Z}$ des entiers, et l'anneau $\mathbb{K}[X]$ des polynômes à coefficients dans le corps $\mathbb{K}$. En fait il s'agit d'anneaux **euclidiens**.

Un autre exemple est donné par l'anneau des fonctions sur un ensemble E à valeurs dans $\mathbb{R}$. Si $F \subset E$ est un sous ensemble l'idéal des fonctions nulles sur F est principal et est engendré par la fonction caractéristique du complémentaire de F, notée 1_{F^c}. En effet si $f \in I(E)$, $f = f.1_{F^c}$.On va voir la réciproque dans l'exercice 1.8.

Définition 1.17. *On dit que A est euclidien s'il on s'est donné une application $d\colon A - \{0\} \to \mathbb{N}$ vérifiant la propriété d'Euclide : pour tout couple (a, b) d'élément de $A \times A - \{0\}$ il existe deux éléments q et r dans A tels que $a = bq + r$ avec $r = 0$ ou $d(r) < d(b)$.*

Remarque 1.5. Certains auteurs (on attribue cette définition à Samuel) très lettrés et un peu pédants appellent d un $\sigma\tau\alpha\theta\mu\eta$. Les deux exemples principaux sont : les anneaux de polynômes $A = \mathbb{K}[X]$ et d est le degré, et $A = \mathbb{Z}$ où d est la valeur absolue. L'existence d'une telle fonction rend **algorithmique** le calcul du PGCD de deux nombres, ou si l'on veut le calcul du générateur de l'idéal $I + J$ à partir de ceux de I et de J. D'habitude il faut 3 exemples pour poser une définition, donc nous n'utiliserons pas cette terminologie.

La démonstration qu'un anneau euclidien est principal est laissée en exercice.

1.3.2. Anneaux factoriels

Définition 1.18. *Dans un anneau A un élément p est irréductible si $p = ab$ implique que l'un des deux éléments a ou b est inversible.*

Exemple. Dans $\mathbb{Z}[X]$ le polynôme $2X$ il n'est pas irréductible car c'est le produit de 2 et de X, mais il l'est dans $\mathbb{Q}[X]$, car 2 est inversible dans $\mathbb{Q}$.

Les éléments irréductibles d'un anneau jouent un peu le rôle de nombre premier. Dans $\mathbb{K}[X]$ un polynôme est irréductible si on ne peut l'écrire comme produit de polynômes de degré strictement inférieur. En particulier dans $\mathbb{C}[X]$ les seul polynômes irréductibles sont les polynômes de degré 1.

L'idée d'anneau factoriel est d'essayer de généraliser le fait qu'un nombre entier s'écrit d'une **unique** façon comme produit de nombre premiers, on qu'un polynôme de $\mathbb{C}[X]$ s'écrit d'une unique façon comme produit d'une constante et de polynômes de degré 1.

Exemple 1.16. L'anneau $\mathbb{Z}[i\sqrt{5}]$, dont les seuls éléments inversibles sont $1, -1$ n'est pas factoriel. En effet $9 = 3 \times 3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$

DÉFINITION 1.19. *Un anneau est factoriel si il est intègre et si il satisfait les deux propriétés suivantes (existence et unicité de la décomposition en produit de facteurs irréductibles) :*

1. *Pour tout élément non nul x il existe un entier r un élément inversible u et des éléments irréductibles $p_1, ...p_r$ tels que $x = up_1....p_r$*
2. *L'écriture d'un élément comme produit d'un inversible et d'irréductibles est unique à inversible près et permutation près :*
   si $x = up_1....p_r = vq_1....q_s$, avec $u, v \in A^*$, p_i, q_j irréductibles, alors $r = s$ et il existe une permutation σ de $\{1, ...r\}$ et des inversibles u_i tels que $p_i = u_i q_i$

PROPOSITION 1.18. *Soient $x = up_1...p_r$ et $y = vq_1....q_s$ l'écriture de deux éléments comme produit d'un inversible et d'irréductibles. Alors $xy = (uv)p_1...p_rq_1....q_s$ est une écriture de xy comme produit d'un inversible et d'éléments irréductibles.*

On en déduit :

PROPOSITION 1.19. *Soit A un anneau factoriel, $x = up_1...p_r$ avec p_i irréductibles et u inversible. les diviseurs de x sont les éléments de la forme $vp_{i_1}....p_{i_k}$ ou $\{i_1, ...i_k\}$ est un sous ensemble de $\{1, ...r\}$. En particulier si p est un diviseur irréductible de x , il existe un indice i et un élément inversible u tel que $p = up_i$.*

THÉORÈME 1.7. *L'anneau $\mathbb{K}[X]$ est factoriel.*

Démonstration. Si un polynôme est réductible, il s'écrit comme produit de polynôme de degré strictement inférieur. Un polynôme de degré 1 étant irréductible, en raisonnant par récurrence sur le degré, on en déduit que tout polynôme est produit de polynômes irréductibles. J'utilise juste que le degré du produit est la somme des degrés.

Pour l'unicité, on peut raisonner ainsi. Soit $f = f_1....f_n = g_1....g_m$ une écriture de f comme produit de facteurs irréductibles. Si f est de degré 1, on remarque que $n = m = 1$, et il n'y a rien à démontrer. Supposons que $\deg(f) > 1$. Réduisons modulo f_1. On a $g_1....g_m = 0(f_1)$. Comme l'anneau quotient est intègre, l'un des facteurs -qui est irréductible- doit être divisible par f_1 donc lui être égal (après multiplication par un élément de k.) Quitte à renuméroter on peut supposer que $f_1 = g_1$. On conclu par récurrence sur le degré ou sur l'entier n. □

THÉORÈME 1.8. *Un anneau principal intègre est factoriel.* □

Avertissement 1.4. La démonstration de ce théorème et très facile pour les anneaux euclidiens, mais repose sur la théorie des anneaux noetheriens pour le cas général. Nous la reportons au chapitre 4.

PROPOSITION 1.20. *Soit A un anneau factoriel. Alors :*

1. *Lemme d'Euclide. Si p est irréductible et p divise ab alors il divise a ou b*

2. p est irréductible si et seulement si l'idéal pA est premier

3. Lemme de Gauss. Si a divise bc et a et b sont premier entre eux, alors a divise c.

Démonstration. Résulte de la proposition 1.74. □

Nous allons maintenant définir le PGCD et le PPCM dans un anneau factoriel.

Si p est un élément irréductible, et $x \in A$, on définit l'entier $v_p(x)$ comme le plus grand entier n tel que p^n divise x. Cet entier s'appelle la p valuation de x. Notons que si $p' = up$ est le produit de p par un inversible $v_{p'} = v_p$.

Proposition 1.21. *Si p est un élément irréductible, p divise x si et seulement si $v_p(x) \geqslant 1$*
$v_p(xy) = v_p(x) + v_p(y)$
$v_p(x+y) \geqslant \min v_p(x), v_p(y)$

Ainsi, v_p est un homomorphisme de semi-groupe. $(A - \{0\}, \times) \to (\mathbb{N}, +)$

Si on est malin on en déduit un homomorphisme de groupe

Proposition 1.22. *Soit $\mathbb{K}$ le corps des fractions de A. L'application de $\mathbb{K} - \{0\} \to \mathbb{Z}$ définie par $v_p(x) = v_p(a) - v_p(b)$ si $x = \frac{a}{b}$ est un homomorphisme de groupes* □.

Deux éléments irréductibles p, p' sont dits équivalents si il existe un élément inversible u tel que $p' = up$. On choisit un ensemble $\mathcal{P}$ de représentants des irréductibles, alors on a :

Proposition 1.23. *Tout élément x de A non nul s'écrit d'une unique façon $x = u\Pi_{p\in P} p^{v_p(x)}$, ou u est inversible. Ce produit est fini car il n'y a qu'on nombre fini d'éléments de $\mathcal{P}$ qui divise x.*

On a alors un notion claire de PGCD d'une famille d'éléments de $A - (0)$

Définition 1.20. *Si $(x_i)_{i\in I}$ est une famille d'éléments de A leur PGCD est $\Pi_{p\in P} p^{\mathrm{MIN}_i v_p(i)}$*

Le PGCD semble dépendre de la famille de représentant choisi, mais il n'en dépend pas à un inversible près, comme on le vérifie aisément.

On arrive alors au premier théorème non évident de ce cours, attribué à K.F Gauss, donc autour de 1800.

Théorème 1.9. *Si l'anneau A est factoriel, alors l'anneau de polynômes $A[X]$ l'est aussi.*

Gauss voulait étudier $\mathbb{Z}[X]$.

Remarque 1.6. Par récurrence, on en déduit que $\mathbb{K}[X_1, ...X_n]$ est factoriel.

La démonstration est assez longue, et va utiliser le corps $\mathbb{K}$ des fractions de A (qui est intègre par définition), et le fait que $\mathbb{K}[X]$ est principal (et même euclidien). Le plus difficile va être de comprendre qui sont les irréductibles de cet anneau. Elle se fait en quatre étapes.

Etape 1 : Le contenu.

Définition 1.21. *Si $f(X) = a_0 + a_1 X + \cdots + a_n X^n$ est un polynôme à coefficients dans A, son contenu est $c(P) = \mathrm{PGCD}(a_i)$*

LEMME 1.3. *Le contenu du produit est le produit des contenus, c'est à dire que pour tout couple de polynômes P,Q, il existe un inversible u tel que $c(fg)=uc(f)c(g)$.*

Démonstration. On se ramène évidemment au cas ou $c(f)=c(g)=1$, en écrivant $f=c(f)f_1$, $g=c(g)g_1$. Il s'agit de démontrer qu'alors $c(fg)=1$.

On raisonne par l'absurde et on suppose que ce n'est pas le cas. Il existe un irréductible p qui divise tous les coefficients du produit fg.

Comme p ne divise pas tous les coefficients de f ni ceux de g il existe deux indices i_0, j_0 tels que p divise tous les a_i et les b_j pour $i<i_0$ et $j<j_0$, mais p ne divise ni a_{i_0} ni b_{j_0}. Regardons le coefficient de degré i_0+j_0 du produit

$c_{i_0+j_0}=\Sigma_{i+j=i_0+j_0}\,a_ib_j=a_{i_0}b_{j_0}+\text{termes multiples de } p$

D'après le lemme de Gauss, comme p divise $c_{i_0+j_0}$, il divise a_{i_0} ou b_{j_0}, contradiction. □

LEMME 1.4. *Soit A un anneau factoriel, $\mathbb{K}$ son corps des fractions. Tout polynôme de $\mathbb{K}[X]$ s'écrit $f=\frac{a}{b}\,f_1, a, b$ deux éléments de A premiers entre eux, P_1 un polynôme de $A[X]$ de contenu égal à 1. Cette écriture est unique à inversible près.*

Démonstration. Si on multiplie f par le ppcm b' des dénominateurs de ses coefficients, on obtient un polynôme à coefficients dans A. On met alors son contenu en facteur et $bf=c(bf)\,f_1$, $f=\frac{a'}{b'}\,f_1$, et on met en facteur le pgcd de a',b', pour obtenir $f=\frac{a}{b}\,f_1$.

Pour l'unicité. Si $\frac{a}{b}\,f_1=\frac{a'}{b'}\,f_2$, sont deux écritures de f satisfaisant les hypothèses du lemme, alors $ab'\,f_1=ba'\,f_2$. Comme $c(f_1)=c(f_2)=1$ $ab'=ba'$ et $f_1=f_2$. On applique Gauss 2 fois pour montrer que $a=ua', b=ub'$. □

Exemple 1.17. Une polynôme de $\mathbb{Q}[X]$ s'écrit $\frac{a}{b}\,f(x)$, avec $a,b\in\mathbb{Z}$ premiers entre eux et $f\in\mathbb{Z}[X]$ de contenu 1.

Etape 2 les irréductibles de $A[X]$.

THÉORÈME 1.10. *On suppose A factoriel, et on note $\mathbb{K}$ son corps de fractions. Un élément f de l'anneau $A[X]$ est irréductible si et seulement si :*

1. *Soit $\deg(f)=0$ et $f=p$ est un irréductible de A*
2. *Soit f est irréductible dans $\mathbb{K}[X]$ de contenu égal à 1.*

Démonstration. Si $f=p$, irréductible de A il ne peut être produit de deux polynômes que si ceux ci sont de degré 0 donc des éléments de A, mais si p est irréductible l'un des deux est inversible, donc p est irréductible.

Si $f\in A[X]$ est irréductible dans $\mathbb{K}[X]$ et de contenu 1 et que dans $A[X]=f=f_1f_2$, l'un est de degré 0, disons f_1. D'après le lemme du contenu, f_1 est en fait inversible.

Réciproquement soit f un irréductible de $A[X]$. Si $\deg(f)=0$, f est irréductible dans A. Sinon, son contenu est 1 car le contenu divise f. Montrons qu'il est irréductible dans $\mathbb{K}[X]$. Sinon, on peut l'écrire comme produit de deux polynômes de $\mathbb{K}[X]$ disons $f=gh$.

D'après le lemme précédent écrire $g=\frac{a}{b}\,g_1$, $h=\frac{c}{d}\,h_1$ avec g_1,h_1 dans $A[X]$ de contenu 1, a,b premiers entre eux, ainsi que c,d. On a alors $\frac{ac}{bd}\,(h_1\,g_1)=f$. En calculant le contenu, $ac=bdu$, ou u est inversible. Donc $f=uh_1\,g_1$ est réductible dans $A[X]$. □

Par exemple 2X n'est pas irréductible dans $\mathbb{Z}[X]$, mais l'est dans $\mathbb{Q}[X]$.

Etape 3. Démonstration de l'existence.

Soit $f \in A[X]$, nous allons démontrer que f s'écrit comme produit d'un élément irréductible de A et de polynômes de $A[X]$ de contenu égal à 1.

De fait, on écrit d'abord f comme produit de polynômes irréductibles de $\mathbb{K}[X]$, puis on applique à chacun le lemme 1.87. On voit que $f = \frac{a}{b} f_1 \ldots\ldots f_n$ ou les f_i sont des polynômes de $A[X]$ de contenu 1 et irréductibles dans $\mathbb{K}[X]$. Comme le produit $f_1 \ldots\ldots f_n$ est un polynôme de $A[X]$ de contenu égal à 1 la partie unicité du lemme 1.56 nous dit que b est inversible, $\frac{a}{b} \in A$. On écrit alors $\frac{a}{b}$ comme produit d'irréductibles de A. On a ainsi établi l'existence d'un décomposition de f en élément irréductible. □

Etape 4. Démonstration de l'unicité.

Soit f un polynôme de $A[X]$ nous devons démontrer que son écriture comme produit d'un élément de A et de polynômes irréductibles est essentiellement unique.

Soit $f = a f_1 \ldots\ldots f_n = b g_1 \ldots g_r$ deux telles écritures. En appliquant le lemme 1.56 a $a(f_1 \ldots\ldots f_n) = b(g_1 \ldots g_r)$, on voit que $a = bu$ ou u est inversible. Maintenant, $\mathbb{K}[X]$ est principal donc factoriel. Quitte à renuméroter, nous pouvons donc supposer que $r = n$ et $f_i = \lambda_i g_i$, où $\lambda_i \in \mathbb{K}$, en écrivant $\lambda_i = \frac{a_i}{b_i}$ et en calculant le contenu, on voit que $\lambda_i \in A$ est un inversible de cet anneau. □

1.4. Modules de type fini sur un anneau principal et algèbre linéaire.

Dans ce paragraphe, nous allons étudier un grand classique de l'algèbre élémentaire, qui permet d'étudier aussi bien les groupes abéliens de type fini que le théorème de Jordan sur la forme normale des matrices. Ce second point étant fait un problème. Dans ce paragraphe, nous fixons un anneau principal A. Il se peut que A soit euclidien, et dans ce cas, nous noterons $d: A \to \mathbb{N}$ un structure euclidienne sur A.

1.4.1. Modules libres types finis et leurs sous modules.

Rappelons qu'un module M sur un anneau A est comme un espace vectoriel sur un corps $\mathbb{K}$ sauf que dans l'axiomatique, on remplace le mot corps par le mot espace vectoriel. Par exemple A^n est un module sur A. La grosse différence étant qu'il peut y avoir un élément non nul $x \in M$ et un élément non nul a tel que $ax = 0$: ceci est impossible pour un espace vectoriel car le scalaire a y est inversible et dons $ax = 0 \Rightarrow \frac{1}{a} ax = x = 0$.

L'axiomatique est :
1. $(M, +)$ est un groupe abélien.
2. il y a un e multiplication externe $A \times M \to M$ qui satisfait les identités :
$1.x = x, a(bx) = (ab)x$, $(a+b)x = ax + bx$, $a(x+y) = ax + ay$

Les deux gros exemples, pour nous sont les $\mathbb{Z}$ modules, qui sont exactement les groupes abéliens, et les $\mathbb{K}[X]$ modules qui sont les couples (E, φ), où E est un espace vectoriel et φ un endomorphisme de E. Le premier exemple a été étudié en $L3$, le second fera l'objet d'un problème en fin de chapitre.

L'exemple de A module qui nous intéresse le plus est A/I ou I est un idéal. On peut décliner cet exemple en prenant $A/I_1 \oplus A/I_2 \oplus \cdots \oplus A/I_n \oplus A^r$. Dans le cas ou $A = \mathbb{Z}$, on a par exemple

$M = \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_k\mathbb{Z} \oplus \mathbb{Z}^r$, et nous savons bien que tout groupe abélien de type fini est de cette forme. nous allons vérifier que la démonstration faite de ce résultat important se généralise mot pour mot au cas des modules de type fini sur l'anneau principal A. Il s'agit juste de copier la démonstration.

Toutes la terminologie des espaces vectoriels et des applications linéaires se transpose à ce cadre.

DÉFINITION 1.22. *On dit qu'un A module est de type fini si il est engendré par un nombre fini d'éléments.*

En d'autres termes il existe des éléments $u_1, ..., u_n \in M$ tel que tout élément s'écrit $x = \Sigma_{i=1}^n x_i u_i$.

DÉFINITION 1.23. *Un module libre de rang n est module isomorphe à A^n.*

PROPOSITION 1.24. *Si A^n est isomorphe à A^m, alors $m = n$.*

Démonstration. On choisit un idéal maximal $I \subset A$. Si M est un A module, on peut considérer $IM \subset M$. le sous-module des multiples de I, et M/IM devient évidemment un $\mathbb{K}$ espace vectoriel, pour $\mathbb{K} = A/I$. Clairement si $M = A^n$, $M/iM = \mathbb{K}^n$, et donc $n = \dim_{\mathbb{K}}(M/I.M)$. □

PROPOSITION 1.25. *Soient M,N deux modules libres de rangs m et n.*

La somme $M \oplus N$ est un module libre de rang $m+n$

L'ensemble $\mathrm{Hom}(M, N)$ *est un module libre de rang n.p isomorphe au groupe additifs des matrices (p, n) à coefficients dans A*

En particulier le dual $\mathrm{Hom}(M, A) = M'$ *est aussi un module libre.*

Démonstration. $A^n \oplus A^p = A^{n+p}$, $\mathrm{Hom}(A^n, A^p) = A^p \oplus \cdots \oplus A^p$ (n facteurs), $\mathrm{Hom}(A^n, A) = A \oplus \cdots \oplus A$ (n facteurs). □

DÉFINITION 1.24. *Soit M un module libre. On dira qu'une famille finie de vecteurs $\mathfrak{F} \subset \Lambda$ est libre (sur A) si l'équation $\Sigma_{u \in \mathfrak{F}} a_u u = 0$ implique que tous les coefficients a_u sont nuls.*

DÉFINITION 1.25. *Le sous-module engendré par une famille d'éléments d'un module est l'ensemble des combinaisons linéaires* ***à coefficients dans A*** *de ces éléments.*

Exemple 1.18. Un sous module de l'anneau A est précisément un idéal de A.

DÉFINITION 1.26. *Une base du module libre Λ est une famille de vecteurs libres sur A qui engendre Λ.*

PROPOSITION 1.26. *Soit $\mathfrak{F} = \{u_1, ...u_k\} \subset \Lambda$ un ensemble fini et $\varphi_A = A^k \to \Lambda$ l'homomorphisme $\varphi_A(x_1, ..., x_k) = \Sigma_{i=1}^k x_i u_i$. Alors A est libre si et seulement si φ_A est injectif, et A est génératrice si et seulement si φ_A est surjective.*

Démonstration. Laissée en exercice. □

LEMME 1.5. *Tout sous-module d'un module libre de rang n est libre de type fini, et de rang inférieur ou égal à n*

Démonstration. La démonstration se fait par **récurrence sur l'entier n**. On peut supposer que $\Lambda = A^n$.

Initialisation. Le cas $n=1$ est précisément la définition de principal. On sait qu'un idéal de A est de la forme $a.A$ engendré par un seul élément.

Induction. On pose $e_1=\begin{pmatrix}1\\0\\.\\0\end{pmatrix}$, et considère la suite d'homomorphismes :

$$Ae_1=\ker(\pi) \;\to\; A^n \xrightarrow{\pi} A^{n-1} \;\to\; 0$$

Par définition, l'image du vecteur $\begin{pmatrix}x_1\\x_2\\.\\x_n\end{pmatrix}\in A^n$ par π est $\begin{pmatrix}x_2\\x_3\\.\\x_n\end{pmatrix}\in A^{n-1}$.

Soit Λ un sous-module de A^n. Grâce à la l'hypothèse de récurrence, on sait que son image dans A^{n-1} est un module libre de type fini engendré par $f'_1,....f'_d$, avec $d\leqslant n-1$ Regardons le noyau de la restriction de la projection π à Λ. Si il est réduit à 0, l'homomorphisme π induit un isomorphisme, et on a terminé. Sinon, c'est un sous module de Ae_1, donc (A est principal) engendré par un élément $f_1=ae_1$. Relevons les f'_i en des éléments f_i de Λ. On vérifie que $f_1,....f_d$ est une base de Λ. □

Théorème 1.11. *Soit $\Gamma\subset\Lambda$ un sous-module d'un groupe module libre de rang n. Il existe une base $e_1,....e_n$ de Λ et des éléments $d_1,....d_r$ de A tels que $d_i|d_{i+1}$ et $\Gamma=Ad_1e_1\oplus...Ad_re_r$.*

Démonstration. On va démontrer ce résultat **par récurrence sur l'entier n.**

Initialisation. On sait qu'un sous-groupe Γ de A est de la forme dA.

Induction. Si $\Gamma=0$ il n'y a rien à démontrer. Sinon, on considère l'image par Γ de toutes les formes linéaires sur $\Lambda=A^n$, c'est à dire $\Lambda'(\Gamma)\subset A$. C'est un sous module de A, c'est à dire un idéal donc de la forme d_1A.

Il y a un élément de Γ, disons e'_1 et une forme linéaire φ de Λ' telle que $\varphi(e'_1)=d_1$. Mais, si on fixe une base, toutes les coordonnées de e'_1 sont divisibles par d_1, donc il existe un vecteur e_1 dans Λ tel que $d.e_1=e'_1$

Lemme 1.6. $\Lambda=Ae_1\oplus\ker\varphi$ *et* $\Gamma=d_1.Ae_1\oplus\ker\varphi\cap\Gamma$

Démonstration. Cela résulte de $x=\varphi(x)e_1+(x-\varphi(x)e_1)$

On remarque que cette écriture décompose n'importe quel élément de Λ comme somme d'un vecteur proportionnel à e_1 et d'un vecteur de $\ker(\varphi)$, d'où la première égalité.

Pour la seconde, on remarque que si $x\in\Gamma$ $\varphi(x)\in d_1A$, donc $\varphi(x)e_1\in\Gamma\cap d_1.Ae_1=\mathrm{Ae}'_1$. Et par différence $(x-\varphi(x)e_1)\in\Gamma$ et bien entendu est toujours dans $\ker(\varphi)$ □

Pour terminer l'argument de récurrence, nous remarquons $\ker\varphi$ est libre (lemme1.96) Il est de rang $n-1$ car on sait $\mathrm{rang}(\ker(\varphi))+1=\mathrm{rang}(\Lambda)$. On peut donc appliquer l'hypothèse de récurrence à $\ker\varphi\cap\Gamma<\ker\varphi$, ce qui termine la démonstration.

□

Dans le cas ou on suppose A intègre, on peut affiner la décomposition du A module grâce au lemme chinois. Comme un anneau principal intègre est factoriel, on peut décomposer les d_i en produit de puissance d'élément indécomposables $d_1=p_1^{n_1}....p_m^{d_m}$ et le module A/dA est isomorphe, grâce au lemme chinois à $A/p_1^{n_1}\oplus\cdots\oplus A/p_m^{d_m}$.

1.5. EXERCICES.

Ces exercices sont pour la plupart copiés de [Demazure], [Perrin]

1.5.1. Anneaux

Exercice 1.1. L'anneau $\mathbb{Z}$ ne contient pas de sous anneau distinct de lui même.
Un anneau $(A, +, \times)$ possède un plus petit sous-anneau non nul.
Quels sont ses éléments, et à quoi peut il être isomorphe?

Exercice 1.2. Anneau de Boole.

Si X est un ensemble, l'ensemble $\mathcal{P}(E)$ des parties de E est muni de plusieurs lois de composition interne : la réunion, l'intersection et la différence symétrique Δ définie par $A\Delta B = A \cup B \backslash A \cap B$.
Démontrer que $(\mathcal{P}(E), \Delta, \cap)$ est un anneau. Pour cela on pourra construire une bijection de $\mathcal{P}(E)$ avec $(\mathbb{Z}/2\mathbb{Z})^E$.

Exercice 1.3. Binôme de Newton. Soit A un anneau. Si n est un entier, on note par abus n l'image de l'entier n par l'homomorphisme canonique $\chi : \mathbb{Z} \to A$. C'est l'unique homomorphisme $\mathbb{Z} \to A$ qui a été construit dans l'exo 1.

Si n et k sont deux entiers et $k \leqslant n$, on note $\left(\begin{smallmatrix} n \\ k \end{smallmatrix} \right)$ l'image de l'entier $\frac{n!}{k!(n-k)!}$ dans A. Démonter que dans tout anneau on a $(a+b)^n = \Sigma_{k=0}^n \left(\begin{smallmatrix} n \\ k \end{smallmatrix} \right) a^k b^{n-k}$.

Pourquoi ne peut on pas écrire $\frac{(a+b)^n}{n!} = \Sigma_{k=0}^n \frac{a^k}{k!} \frac{b^{n-k}}{(n-k)!}$

Soit p un nombre premier. On suppose que $p.1 = 0$ dans A. Démontrer que $(a+b)^p = a^p + b^p$

1.5.2. Idéaux

Exercice 1.4. Soit $f : A \to B$ un homomorphisme d'anneaux, et $I \subset B$ un idéal premier. Que peut on dire que $f^{-1}(I)$? Même question si l'on suppose I maximal.

Exercice 1.5. Soit $\mathbb{K}$ un corps fini, $\mathbb{K} = \{a_1, ...a_n\}$. Quel est le noyau de l'application qui à un polynôme associe la fonction qu'il définit? Démontrer qu'il existe un polynôme irréductible sur $\mathbb{K}$. On pourra considérer $P = \Pi_{i=1}^n (X - a_i) + 1$

Exercice 1.6. Calculer le groupe des éléments inversibles des anneaux $\mathbb{Z}, \mathbb{K}[X]$ ou $\mathbb{K}$ est un corps, $A[X]$ ou A est intègre.

* Soit $\mathbb{K}[[X]]$ l'anneau des séries formelles à coefficients dans $\mathbb{K}$. Montrer que la série formelle $\Sigma_0^\infty a_n X^n$ est inversible si et seulement si $a_0 \neq 0$. Montrer que cet anneau n'a qu'un seul idéal maximal/premier.

Exercice 1.7. Si I est un idéal et si I n'est pas premier, il existe deux idéaux distincts I_1, I_2 tels que $I \subset I_1$, $I \subset I_2$ et $I_1.I_2 \subset I$. Quels sont les idéaux de $\mathbb{Z}/n\mathbb{Z}$ et quel sont ses idéaux premiers.

Exercice 1.8. Soit A un anneau intègre qui n'est pas un corps. Montrer que l'anneau $A[X]$ n'est pas principal.

Exercice 1.9. Soit E un ensemble fini et $A = \mathbb{R}^E$ l'anneau des fonctions de E à valeurs dans $\mathbb{R}$.
0. Quels sont les éléments inversibles de A

1. Si $x_0 \in E$ l'ensemble $I(x_0)$ des fonctions qui s'annulent en x_0 est un idéal. Quel est le quotient $A/I(x_0)$

2. Si $F \subset E$ est un sous ensemble, l'ensemble $I(F)$ des fonctions qui s'annulent sur F est un idéal. Quel est le quotient $A/I(F)$

3. Si I est un idéal ne contenant pas d'élément inversible démontrer qu'il existe un point x de E tel que toutes les fonctions de I s'annulent en x.

4*. Quels sont tous les idéaux de A, tous les idéaux maximaux de A.

Exercice 1.10. Dans $\mathbb{Z}$, calculer la somme et le produit des idéaux $n\mathbb{Z}$ et $m\mathbb{Z}$.
Dans $\mathbb{K}[X]$ calculer la somme et le produit des idéaux principaux engendrés par les polynômes unitaires P et Q.

Exercice 1.11. Soit I un idéal de A. montrer que l'ensemble des combinaisons linéaires de carrés d'éléments de I (des somme finie $\Sigma_{i=1}^{n} a_i x_i^2$, ou les x_i sont dans I est un idéal, noté J. Montrer que si l'élément 2 de A est inversible, alors $J = I^2$. Donner un exemple ou cela n'est pas le cas.

Exercice 1.12. Construire un isomorphisme entre $\mathbb{K}[T]$ et $\mathbb{K}[X,Y]/Y - X^2$.
Entre $\mathbb{K}[T,T^{-1}]$ et $\mathbb{K}[X,Y]/XY - 1$. Ici $\mathbb{K}[T,T^{-1}]$ est le sous anneau du corps $\mathbb{K}(T)$ engendré par T et T^{-1}.

Exercice 1.13. * Nilradical d'un anneau.
Un élément a d'un anneau A est dit nilpotent si il existe un entier n tel que $a^n = 0$
1. L'ensemble $\mathrm{Nil}(A)$ des éléments nilpotents est un idéal de A
2. Le quotient $A/\mathrm{Nil}(A)$ n'a pas d'élément nilpotent.
3. Si P est un idéal premier, alors $\mathrm{Nil}(A) \subset P$
4.* Si s n'est pas nilpotent, il existe un idéal premier de A qui ne contient pas s. Indication.
a. On considère l'ensemble E des idéaux qui ne contiennent aucune puissance de s. Il contient un élément maximal P pour l'inclusion. il faut démontrer que cet idéal est premier. Pour cela on considère un produit xy de deux éléments dont le produit est dans P mais ni l'un ni l'autre ne le sont. Montrer qu'il existe deux entiers k,l et deux éléments de A tels que $s^k - ax$ et $s^l - by$ soient dans P. Montrer que s^{k+l} est dans p et obtenir une contradiction.
5. Nil(A) est l'intersection des idéaux premiers de A.

Problème 1.1. Anneau $C(X)$.

On va voir quelques propriétés de l'anneau des fonctions continues à valeurs dans $\mathbb{R}$ définies sur un espace métrique (ou même topologique).

1. Compact.
Soit K un espace métrique compact, et $C(K)$ la $\mathbb{R}-$algèbre des fonctions continues sur $\mathbb{K}$.
Idéaux

1. Si $x_0 \in K$ démontrer que $I_{x_0} = \{f : f(x_0) = 0\}$ est un idéal maximal de $C(K)$.
2. Quels sont les éléments inversibles de $C(K)$
3. Soit $I \subsetneq C(K)$ un idéal propre. Montre que pour toute fonction $f \in I$ il existe un point x de K tel que $f(x) = 0$
4. Si $f \in I$, on pose $Z_f = \{x \,/\, f(x)\} = 0$. Montrer que si l'intersection $\cap_{f\in I} Z(f)$ est vide qu'il existe une famille finie de fonction $f_1, \ldots f_n$ de I telle que $\cap_{i=1}^{n} Z_{f_i}$ soit vide.
5. En considérant $\Sigma_{i=1}^{n} f_i^2$, montrer que si l'intersection $\cap_{f\in I} Z(f)$ est vide, I contient un élément inversible.
6. Montrer que pour tout idéal propre de $C(K)$ il existe un point x_0 tel que $I \subset I_{x_0}$.

2. Idempotents.
Rappelons qu'un élément e d'un anneau est dit idempotent si $e^2 = e$
Etablir que l'espace topologique K est connexe si et seulement si $C(K)$ n'a pas d'idempotents différents de 0 et 1.

1.5.3. Anneaux euclidiens, principaux, factoriels.

Exercice 1.14. Dans $\mathbb{K}[X]$, l'idéal engendré par le polynôme f est premier si et seulement si f est irréductible, c'est à dire n'est pas produit de deux polynômes de degré strictement inférieur.

Si f est quelconque, quels sont les idéaux premiers de $\mathbb{K}[X]/f$.

Exercice 1.15. Soit A un anneau $\delta: A-\{0\}\to\mathbb{N}$ une structure euclidienne sur A. Soit $s\in A$ un élément premier. Dans le corps de fractions k de A on considère $A\left[\frac{1}{s}\right]=\{x\in k/\exists n\in\mathbb{N}\text{ et }xs^n\in A\}$.

Montrer que tout élément de cet anneau s'écrit d'une unique façon $a=b.s^n$ avec $b\in A$, $n\in\mathbb{Z}$ et $\text{pgcd}(b,s)=1$

Montrer que $A\left[\frac{1}{s}\right]$ est un anneau factoriel et même euclidien.

Quels sont les éléments irréductibles de cet anneau. (Indication si a,b sont premier avec s quelle est la division euclidienne de a par b.)

Quels sont les éléments irréductibles=indécomposables de $\mathbb{C}[X,X^{-1}]$, de $\mathbb{R}[X,X^{-1}]$.

Exercice 1.16. L'anneau $\mathbb{Z}[i]$ est euclidien. Plus précisément la fonction $\delta(a+ib)=a^2+b^2$ satisfait la propriété d'Euclide.

Exercice 1.17. Quels sont les polynômes irréductibles de $\mathbb{R}[X]$. Décomposer X^4+X^2+1 dans $\mathbb{R}[X]$.

Exercice 1.18. Un anneau factoriel qui satisfait la propriété de Bézout (l'idéal engendré par deux éléments est principal) est un anneau principal.

Exercice 1.19. Rappeler quels sont les irréductibles de $\mathbb{C}[X,Y]$. Les polynômes suivant de $\mathbb{C}[X,Y]$ sont-ils irréductibles

$Y-X^2, X^2+Y^2+1, X^2+Y^2-1, Y^2-X^3, X^3-Y^2-X, XY^3-X^2Y-Y^2+X$

Exercice 1.20. Montrer que l'anneau $\mathbb{C}[X,Y]/X^3-X-Y^2$ n'est pas factoriel. On pourra essayer d'écrire Y^2 de deux façons comme produit d'irréductibles.

Exercice 1.21. Soit A un anneau factoriel, A^* l'ensemble de ses inversibles $\mathcal{P}$ une famille de représentant des irréductibles; et $\mathbb{K}$ le corps de fractions. Démontrer qu'en tant que groupe $\mathbb{K}^*,+$ est isomorphe à $A^*\oplus_{p\in\mathcal{P}}\mathbb{Z}$

Ici la somme directe infinie veut dire les suites $(n_p)_{p\in\mathcal{P}}$ nulles sauf un nombre fini de termes.

Exercice 1.22. Nous souhaitons démontrer le critère d'Eisenstein.

THÉORÈME 1.12. *Soit A un anneau factoriel et $\mathbb{K}$ son corps des fractions. Soit p un élément irréductible de A (=premier dans un anneau factoriel), et $f(X)=a_nX^n+a_{n-1}X^{n-1}+\cdots++a_0$ un polynôme de $A[X]$. On suppose que : $a_n\not\equiv 0(p)$, pour $0\leqslant i\leqslant a_i=0(p)$ et $a_0\not\equiv 0(p^2)$ alors f est irréductible dans $\mathbb{K}[X]$*

a. Montrer qu'on peut supposer que le contenu de f est 1.

b. En déduire que si f n'est pas irréductible, f est le produit de deux polynôme de $A[X]$ $g(X)=b_dX^d+\cdots+b_0$ $h(X)=c_mX^m+\cdots+c_0$.

c. montrer qu'un seul des deux éléments b_0,c_0 est divisible par p. Supposons $c_0=0(p)$

d. Démontrer que p ne divise pas c_m

e. Soit r le coefficient de h tel que $c_r=0(p)$ et r est maximal pour cette propriété. En développant a_r arriver à une contradiction.

Application. Démontrer que si $a\in\mathbb{Z}$ n'est pas divisible par le carré d'un nombre premier, le polynôme X^n-a est irréductible dans $\mathbb{Q}[X]$

Problème 1.2. * Module de type fini sur un anneau principal et théorème de Jordan.

Soit $\mathbb{K}$ un corps, E un $\mathbb{K}$ espace vectoriel de dimension finie sur $\mathbb{K}$ et $\varphi\in\text{End}(E)$ un endomorphisme. Si $P\in\mathbb{K}[X]$ est un polynôme, comme E est une $\mathbb{K}$ algèbre, on peut considérer $p(\varphi)\in\text{End}(E)$. On obtient ainsi un homomorphisme d'anneau (et même de $\mathbb{K}$ algèbre) $\Phi:\mathbb{K}[X]\to\text{End}(E)$.

0. Vérifier que, même si $\text{End}(E)$ n'est pas un anneau commutatif, l'image de cet homomorphisme est un sous anneau commutatif de $\text{End}(E)$.

Le noyau de Φ est un idéal de $\mathbb{K}[X]$, et il est donc principal, engendré par un certain polynôme unitairep_φ, appelé le polynôme minimal de φ.

1. Montrer l'on peut munir E d'un structure de $\mathbb{K}[X]$ module en posant $p.x=p(\varphi)\,x$.

2. Montrer qu'en tant que $\mathbb{K}[X]$ module E est de type fini.

3. Montrer que si E est engendré -en tant que

$\mathbb{K}[X]$-module par un seul vecteur, alors il est isomorphe à $\mathbb{K}[X]/p$, et en déduire que dans ce cas, il existe une base de E (en tant que $\mathbb{K}$ espace vectoriel) la matrice de φ soit la matrice

$$C_p = \begin{pmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & \\ & 1 & 0 & & \\ & & \ldots & & \\ & & & 1 & 0 & -a_{n-2} \\ & & & & 1 & -a_{n-1} \end{pmatrix}$$

appelé matrice compagnon du polynôme p, qui est la matrice de la multiplication par X dans le $\mathbb{K}$ espace vectoriel $\mathbb{K}[X]/p$

4. Montrer -sans calcul- que le polynôme caractéristique de C_p est $\pm p$ (on pourra utiliser le théorème de Cayley Hamilton).

5. En utilisant le théorème de structure des modules de type fini sur un anneau principal, démontrer qu'en général, il existe des polynômes $p_1, p_2, \ldots . p_k = p$ tels que p_i divise p_{i+1} et tel que, en tant que $\mathbb{K}[X]$ module, E soit isomorphe à $\oplus_{i=1}^{k} \mathbb{K}[X]/p_i$.

6. En déduire que dans une base bien choisie, la matrice de φ est $\begin{pmatrix} C_{p_1} & 0 & \ldots & \\ 0 & C_{p_2} & 0 & \\ & & \ldots & \\ & & & C_{p_n} \end{pmatrix}$, et en déduire que le polynôme minimal de φ est p_n.

7. Démontrer que si le polynôme minimal de φ est X^n il existe une base dans laquelle la matrice de φ est la matrice dite de Jordan

$\begin{pmatrix} J_1 & 0 & \ldots & \\ 0 & J_2 & 0 & \\ & & \ldots & \\ & & & J_k \end{pmatrix}$, où $J_{n_i} = \begin{pmatrix} 0 & & & & 0 \\ 1 & 0 & & & \\ & 1 & 0 & & \\ & & \ldots & & \\ & & & 1 & 0 & 0 \\ & & & & 1 & 0 \end{pmatrix}$ est une matrice de Jordan de taille n_i avec $n_1 \leqslant \cdots \leqslant n_k = n$

8. En déduire que si $p = (X-\lambda)^n$ est scindé sur le corps $\mathbb{K}$, il existe une base dans laquelle la matrice de φ est

$\begin{pmatrix} B_1 & 0 & \ldots & \\ 0 & B_2 & 0 & \\ & & \ldots & \\ & & & B_k \end{pmatrix}$, ou B_i est $\lambda Id + J_{n_i}$ avec $n_1 \leqslant \cdots \leqslant n_k = n$

Supposons que $p = qr$ soit le produit de deux polynômes premiers entre eux. démontrer que $E = E_p \oplus E_q$ ou $E_p = \ker p(\varphi)$, et $E_q = \ker q(\varphi)$

7. En déduire la forme normale de Jordan des matrices dont le polynôme minimal est scindé.

Chapitre 2

Corps

.

Rappelons qu'un corps est un anneau commutatif intègre dans lequel tout élément est inversible. Les premiers exemples que nous avons rencontré sont $\mathbb{Q}, \mathbb{F}_p$ (quotient de $\mathbb{Z}$ par son idéal maximal $p\mathbb{Z}$), $\mathbb{R}, \mathbb{C}$ les corps de nombres comme $\mathbb{Q}(\sqrt{d})$, le corps des fractions rationnelles à une variable $\mathbb{K}(X)$ qui est le corps des fractions de $\mathbb{K}[X]$ ou celui des fractions à plusieurs variables $\mathbb{K}(X_1, X_2, ...X_n)$.

Proposition 2.1. *Soit $\mathbb{K}$ un corps. Soit l'homomorphisme canonique $\varphi: \mathbb{Z} \to K$ tel que $\varphi(1) = 1$ est injectif et $\mathbb{K}$ contient un sous-corps canoniquement isomorphe à $\mathbb{Q}$, soit φ n'est pas injectif et il existe un nombre premier p tel que $\ker \varphi = p\mathbb{Z}$. L'image de $\mathbb{Z}$ est un sous-corps isomorphe à $\mathbb{F}_p$.*

Démonstration. En effet, le noyau de φ est un idéal de la forme $n\mathbb{Z}$. Si φ n'est pas injectif $n \neq 0$, et l'image de φ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Or si $\mathbb{Z}/n\mathbb{Z}$ est intègre, alors n est premier p, et $\mathbb{K} \supset \mathbb{Z}/p\mathbb{Z} = \mathrm{Im}(\varphi)$. Si $n = 0$; $\mathbb{K} \supset \mathbb{Z}$, donc le corps des fractions $\mathbb{Q}$ de cet anneau. □

Définition 2.1. *Le sous corps de $\mathbb{K}$ contenant 1 s'appelle le sous corps premier de $\mathbb{K}$. Nous dirons que la caractéristique de $\mathbb{K}$ est p si c'est $\mathbb{F}_p$, 0 si c'est $\mathbb{Q}$.*

L'un des objets les plus important de la théorie est le groupe de Galois de $\mathbb{K}$.

Définition 2.2. *Soit $\mathbb{K}$ un corps. Le groupe de Galois de $\mathbb{K}$, noté $\mathrm{Gal}(\mathbb{K})$ est le groupe des automorphismes de $\mathbb{K}$.*

Proposition 2.2. *Tout automorphisme de $\mathbb{K}$ induit l'identité sur le corps premier de $\mathbb{K}$.*

Démonstration. Soit $\varphi \in \mathrm{Gal}(\mathbb{K})$. Alors $\varphi(1) = 1$, donc par récurrence sur n, $\varphi(n) = n$. Si $\mathrm{car}(\mathbb{K})$ est finie on a terminé car φ est l'identité sur le corps premier qui est l'image de $\mathbb{N}$ par l'homomorphisme caractéristique. Si $\mathrm{car}(\mathbb{K}) = 0$ on en déduit que $\varphi\left(\frac{n}{m}\right) = \frac{n}{m}$ et que φ induit l'identité sur $\mathbb{Q}$. □

Donc nous essayerons de garder en tête que ce groupe existe et qu'il joue un rôle un peu partout. Un autre concept est celui d'extension d'un corps.

Définition 2.3. *Si $\mathbb{K}$ est un corps, une extension $\mathbb{L}$ de $\mathbb{K}$ est un corps « contenant » $\mathbb{K}$, c'est à dire qu'on s'est donné un homomorphisme (injectif) $\mathbb{K} \to \mathbb{L}$. On note soit $\mathbb{L}: \mathbb{K}$ pour signifier que $\mathbb{L}$ est une extension de $\mathbb{K}$ soit $\mathbb{K} \subset \mathbb{L}$ pour dire la même chose, mais dans l'autre sens, c'est à dire que $\mathbb{K}$ et un sous corps de $\mathbb{L}$.*

Remarque 2.1. Tout homomorphisme de corps $\mathbb{K} \to \mathbb{L}$ est injectif : en effet le noyau est un idéal de $\mathbb{K}$, donc c'est soit 0, soit $\mathbb{K}$. Mais c'est pas $\mathbb{K}$ car $\varphi(1) = 1$.

Par exemple $\mathbb{C}$ est une extension de $\mathbb{R}, \mathbb{F}_p(t)$ une extension de $\mathbb{F}_p$. $\mathbb{Q}(\sqrt{2})$est une extension de $\mathbb{Q}$.

Définition 2.4. *Si $\mathbb{L}: \mathbb{K}$ est une extension, le groupe de Galois de $\mathbb{L}$ sur $\mathbb{K}$, noté $\mathrm{Gal}(\mathbb{L}: \mathbb{K})$ est le sous groupe de $\mathrm{Gal}(\mathbb{L})$ dont la restriction à $\mathbb{K}$ est l'identité*

Remarque 2.2. Un automorphisme φ de $\mathbb{K}$ satisfait $\varphi(1)=1$, donc sa restriction au corps premier de $\mathbb{K}$ est l'identité (cf supra). Ainsi $\mathrm{Gal}(\mathbb{K}) = \mathrm{Gal}(\mathbb{K}\colon \mathbb{Q})$ si $\mathrm{car}(\mathbb{K}) = 0$, $\mathrm{Gal}(\mathbb{K}) = \mathrm{Gal}(\mathbb{K}\colon \mathbb{F}_p)$ si $\mathrm{car}(\mathbb{K}) = \mathbb{F}_p$.

La théorie de Galois va permettre d'expliquer le lien entre les sous groupes de $\mathrm{Gal}(\mathbb{L}\colon\mathbb{K})$ et les corps $\mathbb{M}$ compris entre les deux : $\mathbb{L}\supset\mathbb{M}\supset\mathbb{K}$.

Exemple 2.1. La conjugaison complexe $z\to\bar{z}$ est un automorphisme de $\mathbb{C}$ dont l'ensemble des points fixes est $\mathbb{R}$. Nous allons vérifier que $\mathrm{Gal}(\mathbb{C}\colon\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$.

Soit $\varphi\in\mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Considérons le polynôme X^2+1 dans $\mathbb{C}[X]$. Comme φ conserve 1, et comme ce polynôme est à coefficient réel, si x est une racine de ce polynôme $\varphi(x)$ aussi.

Si $x^2+1=0$, j'applique φ $(x)^2+1=0$

Donc soit $\varphi(i) = i$ auquel cas $\varphi = \mathrm{Id}$, vu que $\varphi|_{\mathbb{R}}$=Id soit $\varphi(i) = -i$ auquel cas φ est la conjugaison complexe.

Plus généralement on a un fait très facile et très important.

PROPOSITION 2.3. *Si P est un polynôme à coefficients dans le corps $\mathbb{K}$ et si $\mathbb{L}\colon\mathbb{K}$ est une extension un automorphisme de $\mathbb{L}$ qui conserve $\mathbb{K}$ permute les racines du polynôme P.*

Démonstration. On écrit $P(X)=a_0+a_1X\ldots+a_nX^n$

Si $x\in\mathbb{L}$ est une racine, on a $a_0+a_1x\ldots+a_nx^n=0$
J'applique φ et on a $a_0+a_1\varphi(x)\ldots+a_n(\varphi(x))^n=0$ □

2.1. DEGRÉ, NOMBRES ALGÉBRIQUES ET TRANSCENDANTS.

Pour étudier les extensions de corps, on va utiliser de façon cruciale les résultats d'algèbre linéaire. Le point de départ est de remarquer que, si $\mathbb{K}\subset\mathbb{L}$, alors $\mathbb{L}$ est un $\mathbb{K}$ espace vectoriel.

2.1.1. Degré d'une extension.

DÉFINITION 2.5. *Soit $\mathbb{K}$ un corps et $\mathbb{L}\colon\mathbb{K}$ une extension. Le degré de l'extension $\mathbb{L}\colon\mathbb{K}$ est la dimension $\dim_{\mathbb{K}}(\mathbb{L})$. On le note $[\mathbb{L}\colon\mathbb{K}]$. On dit que l'extension est finie si cette dimension est finie.*

On a alors le théorème de la base télescopique.

PROPOSITION 2.4. *Soit $\mathbb{K}\subset\mathbb{L}\subset\mathbb{M}$ trois corps. Alors $[\mathbb{M}\colon\mathbb{K}]=[\mathbb{M}\colon\mathbb{L}][\mathbb{L}\colon\mathbb{K}]$. De plus si $(e_i)_{i\in I}$ est une base de $\mathbb{L}$ sur $\mathbb{K}$ et $(f_j)_{j\in J}$ une base de $\mathbb{M}$ sur $\mathbb{L}$, $(e_i f_j)_{i\in I,j\in J}$ est une base de $\mathbb{M}$ sur $\mathbb{K}$.*

Remarque 2.3. Le cas échéant, et si c'est vraiment indispensable, nous pouvons tout à fait accepter que les dimensions soient des cardinaux infinis. Mais les sommes considérées sont toujours finies.

Démonstration. On considère l'application $(\mathbb{K})^{I\times J}\to\mathbb{M}$ définie par $l((x_{i,j}))=\Sigma_{i,j}x_{ij}(e_i f_j)$

Cette application est manifestement linéaire, il faut vérifier son injectivité et sa surjectivité.

Si $l(x) = 0$, alors $\Sigma_j(\Sigma_i\ x_{ij}e_i)f_j = 0$. Par indépendance de la famille des f_j, pour tout j, $\Sigma_i x_{ij}e_i=0$, et par indépendance de la famille e_i $x_{i,j}=0$. Donc $\ker l=0$.

Par ailleurs si $x\in M$ il existe des éléments y_j de $\mathbb{L}$ tels que $x=\Sigma_j y_j f_j$. Pour chacun, on peut trouver des x_{ij} dans $\mathbb{K}$ tels que $y_j=\Sigma x_{ij}e_i$, et on a la surjectivité. □

2.1.2. Nombres algébriques ou transcendants.

Soit $\mathbb{K} \subset \mathbb{L}$ une extension de $\mathbb{K}$, et x un élément de $\mathbb{L}$.

Définition 2.6. *On dit que x est algébrique sur $\mathbb{K}$ si la famille des $(x^i)_{i\in\mathbb{N}}$ est liée (comme famille de vecteurs du $\mathbb{K}$ espace vectoriel $\mathbb{L}$). Autrement dit, si il existe un entier n et des éléments $a_0, ...a_n$ de $\mathbb{K}$ non tous nuls tels que $a_0 + a_1 x + \cdots + a_n x^n = 0$.*

On dit que x est transcendant si il n'est pas algébrique.

Si $x \in \mathbb{L}$ est fixé, on a un unique homomorphisme $\varphi_x : \mathbb{K}[X] \to \mathbb{L}$ tel que l'image de X soit x, c'est l'application $p \to p(x)$. C'est l'homomorphisme d'évaluation en x.

L'élément x est algébrique si et seulement si cet homomorphisme n'est pas injectif. Dans ce cas, son noyau est un idéal maximal de $\mathbb{K}[X]$, dont le générateur est un polynôme irréductible unitaire p_x de $\mathbb{K}[X]$.

Définition 2.7. *Soit x un élément (de $\mathbb{L}$) algébrique sur $\mathbb{K}$. On appelle polynôme minimal de x le polynôme unitaire qui engendre le noyau de l'homomorphisme $\varphi_x : \mathbb{K}[X] \to \mathbb{L}$ tel que $\varphi_x(X) = x$ On note $\mathbb{K}[x]$ l'image de cet homomorphisme.*

Proposition 2.5. *Si x est algébrique et si p son polynôme minimal, le sous-corps de $\mathbb{L}$ qui contient x est isomorphe à $\mathbb{K}[X]/p$, et son degré est le degré de p.*□

Exemple 2.2. $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$ est le plus petit sous corps de $\mathbb{C}$ (ou de $\mathbb{R}$) contenant $\sqrt{2}$. Il est de degré 2 sur $\mathbb{Q}$. Le polynôme minimal de $\sqrt{2}$ est $X^2 - 2$.

Définition 2.8. *Le degré de x est le degré de son polynôme minimal.*

Proposition 2.6. *Si x est transcendant le plus petit sous-corps de $\mathbb{L}$ contenant x est canoniquement isomorphe à $\mathbb{K}(x)$.*

Démonstration. Comme l'application φ_x est injective son noyau est réduit à 0, et on peut définir $\varphi\left(\frac{f}{g}\right) = \frac{f(x)}{g(x)}$. Cet homomorphisme de corps est injectif car tout homomorphisme de corps l'est. □

Définition 2.9. *L'extension $\mathbb{K} \subset \mathbb{L}$ est algébrique si tout élément de $\mathbb{L}$ est algébrique sur $\mathbb{K}$.*

Proposition 2.7. *Une extension finie (de degré fini) d'un corps $\mathbb{K}$ est algébrique. Si elle est engendrée par un élément, elle est isomorphe à $\mathbb{K}[X]/p$, ou p est un polynôme irréductible sur $\mathbb{K}$*

Démonstration. Si la dimension $\dim_{\mathbb{K}}(\mathbb{L})$ est finie, il n'y a pas d'application linéaire injective $\mathbb{K}[X] \to \mathbb{L}$. Donc son noyau est un idéal premier engendré par un polynôme vu que $\mathbb{K}[X]$ est principal. Cet idéal est même maximal vu que dans un anneau principal, un idéal premier est maximal. □

Lemme 2.1. *Soit $\mathbb{K} \subset \mathbb{L}$ une extension, x et y deux éléments de $\mathbb{L}$ algébriques sur $\mathbb{L}$. Le sous-anneau $\mathbb{K}[x, y]$ de $\mathbb{L}$ engendré par x est y est un corps de degré inférieur ou égal au produit des degré de x et de y.*

Démonstration. Soient x, y deux éléments de $\mathbb{L}$. Considérons le sous anneau $\mathbb{K}[x, y] \subset \mathbb{L}$ engendré par x et y. Il contient le sous anneau $\mathbb{K}[x]$ engendré par x qui est un corps. C'est donc $(\mathbb{K}[x])[y]$. Mais y est algébrique sur $\mathbb{K}$ donc aussi sur $\mathbb{K}[x]$. Donc ce sous anneau est un corps. Sa dimension en tant que $\mathbb{K}[x]$ espace vectoriel est finie, donc par composition, sa dimension en tant que $\mathbb{K}$ espace vectoriel aussi (inférieure au produit des degré de x et y). Ainsi $\dim_{\mathbb{K}}(\mathbb{K}[x, y]) \leqslant \text{degré}(x)\text{degré}(y)$. En fait les $(x^i y^j)_{0\leqslant i<\text{degré}(x), 0\leqslant j<\deg(y)}$ engendrent cet espace vectoriel. □

Théorème 2.1. *Soit $\mathbb{K} \subset \mathbb{L}$ une extension. Le sous-ensemble $\mathbb{M}$ de $\mathbb{L}$ formé des éléments algébriques sur $\mathbb{K}$ est un corps.*

Démonstration. Il s'agit de démontrer que la somme et le produit de x et y sont aussi algébriques sur $\mathbb{K}$. Cela résulte du lemme précédent. □

Exemple 2.3. Il existe un polynôme de degré inférieur ou égal à 105 de $\mathbb{Q}[X]$ qui annule $5^{\frac{1}{7}} + 17^{\frac{1}{3}} \times 3^{\frac{1}{5}}$. En effet, La somme d'un élément de degré $1 \leqslant 15$ et d'un élément de degré $\leqslant 7$ est de degré au plus 105.

COROLLAIRE 2.1. *Soit $\mathbb{K} \subset \mathbb{L}$ une extension engendrée par un nombre fini d'éléments algébriques. Alors $\mathbb{L}$ est algébrique.*

Démonstration. C'est un corollaire du lemme 2.10, par récurrence. □

DÉFINITION 2.10. *On dit qu'un corps $\mathbb{K}$ est algébriquement clos si toute extension algébrique de $\mathbb{K}$ est de degré 1.*

PROPOSITION 2.8. *Soit $\mathbb{K}$ un corps. Les propriétés suivantes sont équivalentes.*

1. *Tout polynôme de degré $\geqslant 1$ à coefficients dans $\mathbb{K}$ admet une racine.*
2. *Tout polynôme de degré $\geqslant 1$ est scindé (produit de polynômes de degré 1)*
3. *Les polynômes irréductibles de $\mathbb{K}[X]$ sont les polynômes de degré 1.*
4. *Le corps $\mathbb{K}$ est algébriquement clos.*

Démonstration. On démontre $4 \Rightarrow 3 \Rightarrow 2 \Rightarrow 1 \Rightarrow 4$. Notons que les implication $3 \Rightarrow 2 \Rightarrow 1$ sont immédiates.

$4 \Rightarrow 3$. On suppose que $\mathbb{K}$ est algébriquement clos, et on considère un polynôme irréductible f de $\mathbb{K}$ de degré d. L'anneau $\mathbb{K}[X]/f$ est un corps. Son degré comme extension de $\mathbb{K}$ est d. Comme $\mathbb{K}$ est algébriquement clos $d = 1$.

On note que $3 \Rightarrow 2$, car $\mathbb{K}[X]$ est principal, donc factoriel, et que $2 \Rightarrow 1$ car un polynôme de degré 1 a une racine.

$1 \Rightarrow 4$. Soit $\mathbb{L}$ une extension algébrique de $\mathbb{K}$ et $x \in \mathbb{L}$. Le polynôme unitaire qui engendre l'idéal annulateur de x est irréductible. Comme il admet une racine, il est de degré 1 de la forme $X - \alpha$, avec $\alpha \in \mathbb{K}$. Comme $P(x) = 0,\ x - \alpha = 0$ et $x \in \mathbb{K}$. Donc $\mathbb{K} = \mathbb{L}$. □

La démonstration du théorème suivant nécessite des outils de la topologie (il y a des démonstration très algébriques mais qui cache toutes un peu d'analyse, par exemple reposent sur le fait qu'un polynôme de degré impair à coefficients réels s'annule.

THÉORÈME 2.2. *Dit de d'Alembert Gauss. Le corps $\mathbb{C}$ des nombres complexes est algébriquement clos.* ■

On fera en exercice la démonstration dont l'idée est celle de d'Alembert : si $P \in \mathbb{C}[X]$, un point x_0 où $|P|$ atteint son minimum est une racine de ce polynôme.

Note 2.1. En France on dit théorème de d'Alembert, en Allemagne théorème de Gauss, et ailleurs « The fundamental theorem of algebra ». Son histoire est compliquée. Il a été énoncé par Albert Girard en 1629. Jean Le Rond d'Alembert en a publié 2 démonstrations en 1746 et 1754. Dans sa thèse de doctorat K.-F. Gauss « explique » la preuve de d'Alembert, dit pourquoi il la trouve insuffisante, et donne la sienne. Ces « preuves » sont elles rigoureuses ? Il s'agit plutôt d'arguments convaincants.[2.1]

2.1. Voir l'article de Christopher Baltus, « *D'Alembert's proof of the fundamental theorem of algebra* », *Historia Mathematica*, vol. 31, n° 4, 2004, p. 414-428

Proposition 2.9. *Soit $\mathbb{L}$ un corps algébriquement clos et $\mathbb{K} \subset \mathbb{L}$. Le sous ensemble $\mathbb{M}$ de $\mathbb{L}$ formé des éléments algébriques sur $\mathbb{K}$ est algébriquement clos.*

Démonstration. Soit x un élément algébrique sur $\mathbb{M}$, il est algébrique sur une extension finie de $\mathbb{K}$. En effet il annule un polynôme à coefficient dans $\mathbb{M}$, $a_0 + a_1X + \cdots + a_nX^n$. Donc il est algébrique sur $\mathbb{K}[a_0, ...a_n]$ qui est de degré fini sur $\mathbb{K}$. Donc il est algébrique sur $\mathbb{K}$ c'est à dire qu'il est dans $\mathbb{M}$. □

Corollaire 2.2. *L'ensemble $\bar{\mathbb{Q}} \subset \mathbb{C}$ formé des éléments algébriques est un corps algébriquement clos. Il est dénombrable.*

Un élément de $\bar{\mathbb{Q}}$ est un nombre complexe qui annuel un polynôme à coefficient dans $\mathbb{Q}$ ou dans $\mathbb{Z}$, par exemple $2 - 7X^3 + 9X^{451}$.

Nous verrons que tout corps est contenu dans un corps algébriquement clos.

Définition 2.11. *Un corps de nombre est un sous corps de $\mathbb{C}$ de degré fini sur $\mathbb{Q}$.*

Notation 2.1. *Si les α_i sont des nombres (complexes) on note $\mathbb{Q}[\alpha_1, ...\alpha_n]$ le sous-corps de $\mathbb{C}$ qu'ils engendrent. Si ces nombres sont algébriques, ce corps et un corps de nombre.*

Par exemple $\mathbb{Q}[\sqrt{2}, i^5\sqrt{3}]$

2.2. Corps de décomposition et de rupture.

L'idée de corps de décomposition d'un polynôme est assez subtile et varie au cours des siècles. Si on a un polynôme donné à coefficients rationnels, on peut y penser comme le corps de nombres engendré par les racines complexes de ce polynômes. Pour « le » corps de rupture, on part d'un polynôme irréductible f, c'est l'un des sous corps engendré par une seule des racines du polynômes, disons x_0. En tant qu'ensemble il dépend du choix de cette racine, mais il est toujours isomorphe à $\mathbb{K}[X]/f$ par l'unique isomorphisme qui envoie x_0 sur X.

2.2.1. Corps de rupture d'un polynôme irréductible.

Remarque 2.4. *Le point de vue que nous adoptons n'est pas le point de vue usuel.* Pour nous, **le** corps de rupture d'un polynôme irréductible f est $\mathbb{K}[X]/f$, ou si l'on veut la donnée d'un couple $(\mathbb{K}_f, x_0)$ d'un corps et d'un élément x_0 dans ce corps dont le polynôme minimal est f et qui engendre $\mathbb{K}_f$.

En effet si $\mathbb{K}_f$ est un corps contenant $\mathbb{K}$, x_0 un élément de $\mathbb{K}_f$ dont le polynôme minimal est f et qui engendre $\mathbb{K}_f$ alors il existe un unique isomorphisme de $\mathbb{K}[X]/f$ et $\mathbb{K}_f$ qui envoie X sur x_0.

Avertissement 2.1. L'idée de corps de rupture est une spécialité franco-française. Elle est presque inconnue des traités non français sur ce sujet, mais permet d'avoir une premier exemple de groupe de Galois un peu plus facile à comprendre.

Si $f \in \mathbb{K}[X]$ est un polynôme irréductible, il est facile de construire un corps abstrait dans lequel f a une racine : on prend $\mathbb{K}_f = \mathbb{K}[X]/f$. Par construction, l'image de X dans $\mathbb{K}_f$ est une racine de f dans ce corps.

Ce choix est tout à fait naturel tant qu'on a pas un polynôme concret, par exemple à coefficients dans $\mathbb{Q}$. De fait un tel polynôme a d racines dans $\mathbb{C}$, et pour chacune d'entre elles x_i engendre un sous-corps de $\mathbb{C}$ de degré d et isomorphe à $\mathbb{K}_f$.

Exemple 2.4. Le polynôme $X^3-2 \in \mathbb{Q}[X]$ a 3 racines dans $\mathbb{C}$, $\sqrt[3]{2}$, $j \times^3 \sqrt{2}$, $\bar{j} \times^3 \sqrt{2}$ mais en fait ces corps $\mathbb{Q}[\sqrt[3]{2}]$ et $\mathbb{Q}[j\sqrt[3]{2}]$ ne sont pas du tout égaux le premier est contenu dans $\mathbb{R}$ le second dans $\mathbb{R}j$, et le dernier dans $\mathbb{R}\bar{j}$. Mais ils sont isomorphes au corps de rupture $\mathbb{Q}[X]/X^3-2$.

Cela conduit à poser la définition :

DÉFINITION 2.12. *Soit $f \in \mathbb{K}[X]$ un polynôme irréductible. Un corps de rupture de f est la donnée $(\mathbb{L}, x)$ d'une extension $\mathbb{L}$ de $\mathbb{K}$ et d'une racine de f dans $\mathbb{K}$ qui l'engendre.*

PROPOSITION 2.10. *Tous les corps de rupture $(\mathbb{L}, x)$ d'un polynôme f sont isomorphes, en tant qu'extension de $\mathbb{K}$ avec une racine préférée de f, et sont isomorphes à $(\mathbb{K}[X]/f, X)$.*

Avertissement 2.2. Soit $f \in \mathbb{Q}[X]$, irréductible x et x' deux racines de f dans $\mathbb{C}$. Les deux corps $\mathbb{Q}[x]$ et $\mathbb{Q}[x']$ sont isomorphes, mais il n'y a aucune raison qu'ils soient égaux.

Exemple 2.5. Il y a **deux** corps de rupture du polynôme X^2+1 sur $\mathbb{R}$ contenus dans $\mathbb{C}$: ce sont $(\mathbb{C}, i)$ et $(\mathbb{C}, -i)$.

C'est la première fois que va intervenir le groupe de Galois dans cette aventure.

PROPOSITION 2.11. *Soit f un polynôme irréductible sur $\mathbb{K}$, $\mathbb{K}_f$ un corps de rupture. Il y a une bijection entre les racines de f dans $\mathbb{K}_f$ et les $\mathbb{K}-$automorphismes de $\mathbb{K}_f$, c'est-à-dire* $\mathrm{Gal}(\mathbb{K}_f : \mathbb{K})$ *En particulier, ce groupe a un cardinal inférieur ou égal au degré de f.* □

Si $f = a_0 + a_1 X + \cdots + .a_n X^n$ se donner un isomorphisme entre $\mathbb{K}_f$ et $\mathbb{K}[X]/f$ c'est la même chose que de donner une racine de f dans $\mathbb{K}_f$.

Exemple 2.6. Le groupe de Galois de $\mathbb{Q}[\sqrt[3]{2}]$ est réduit à un élément car X^3-2 n'a qu'une seule racine dans ce corps et que c'est le corps de rupture de ce polynôme.

Quand j'écris $\mathbb{K}[x_0]$ ou $x_0 \in \mathbb{L}$ est un élément d'une extension fini de $\mathbb{K}$, je pense au cours de rupture $\mathbb{K}_f, x_0$ ou f est le polynôme minimal de x_0.

Exemple 2.7. Le groupe de Galois de $\mathbb{C}$ sur $\mathbb{R}$ est $\mathbb{Z}/2\mathbb{Z}$ engendré par la conjugaison complexe : en effet c'est le corps de rupture du polynôme X^2+1.

2.2.2. Corps de décomposition.

La notion de corps de décomposition (« splitting field » an anglais) est très importante.

DÉFINITION 2.13. *Soit $f \in \mathbb{K}[X]$ un polynôme. Un corps de décomposition de f est une extension $\mathbb{L}$ de $\mathbb{K}$ dans laquelle f est scindé, et qui est engendré par les racines de f.*

Exemple 2.8. Si $f \in \mathbb{Q}[X]$, il est scindé sur $\mathbb{C}$ et le sous corps engendré par les racines de f est donc **un** corps de décomposition. On a tendance a l'appeler **le** corps de décomposition, ce qui est un poil abusif, mais c'est plutôt un choix naturel comme corps de décomposition.

Remarque 2.5. Un corps de décomposition est une extension finie puisqu'elle est engendrée par un nombre fini d'éléments algébriques.

Exemple $X^3 - 2$. On a vu que dans $\mathbb{C}$ il a trois corps de rupture différents $\mathbb{Q}[\sqrt[3]{2}]$, $\mathbb{Q}[j\sqrt[3]{2}]\mathbb{Q}j^{23}\sqrt{2}]$. Son corps de décomposition est $\mathbb{Q}[\sqrt[3]{2}, j\sqrt[3]{2}, j^{23}\sqrt{2}] = \mathbb{Q}[\sqrt[3]{2}, j]$ quel est son degré ?

Théorème 2.3. *Tout polynôme de $\mathbb{K}[X]$ admet un corps de décomposition, unique à isomorphisme près.*

Plus précisément soient φ: $\mathbb{K} \to \mathbb{K}'$ un isomorphisme, $f \in \mathbb{K}[X]$ et g son image par φ (le polynôme de $\mathbb{K}'[X]$ dont les coefficients sont les images de ceux de f). Si $\mathbb{L}$ et $\mathbb{L}'$ sont des corps de décomposition de f,g il existe un isomorphisme de $\mathbb{L}$ et $\mathbb{L}'$ qui étend φ.

Avertissement 2.3. Ici « isomorphisme » veut dire isomorphisme d'extensions de $\mathbb{K}, \mathbb{K}'$.

Démonstration.
Existence. On va construire par récurrence une extension finie de corps dans lequel f est scindé. Ensuite, on considérera le sous corps engendré par ces racines.

L'hypothèse de récurrence est
$\mathbb{H}_n$. Pour tout corps $\mathbb{K}$, tout polynôme de degré $\leqslant n$ sur $\mathbb{K}$ admet un corps de décomposition.

Notons que le prédicat $\mathbb{H}_1$ est clair : le corps lui même est un corps de décomposition. Pour l'induction $\mathbb{H}_{n-1} \Rightarrow \mathbb{H}_n$, on considère un polynôme f de degré n, qu'on écrit f comme produit $\Pi_{i=1}^{n}(X - \alpha_i)\Pi_{j=1}^{m} f_i$, ou les f_i sont irréductibles. Si $m = 0$ le polynôme f est scindé et $\mathbb{L} = \mathbb{K}$ convient. Sinon, sur $\mathbb{L} = \mathbb{K}[X]\,/\,f_1$, le polynôme f_1 a au moins une racine et $f = \Pi_{i=1}^{n'}(X - \beta_i)\Pi_{j=1}^{m'} g_j$, avec $n' > m$. Le corps de décomposition de f sur $\mathbb{L}$ est un corps de décomposition de f sur $\mathbb{K}$.

Unicité. On formule une hypothèse de récurrence, c'est-à-dire une suite $(\Pi_n)_{n\geqslant 1}$ de prédicats qu'il va falloir démontrer.

Π_n : Soient φ: $\mathbb{K} \to \mathbb{K}'$ un isomorphisme, $f \in \mathbb{K}[X]$ de degré $\leqslant n$ et g son image par φ (le polynôme de $\mathbb{K}'[X]$ dont les coefficients sont les images de ceux de f.) Si $\mathbb{L}$ et $\mathbb{L}'$ sont des corps de décomposition de f, g il existe un isomorphisme de $\mathbb{L}$ et $\mathbb{L}'$ qui étend φ.

On suppose donc $\deg(f) = m + 1$

On écrit f comme produit $\Pi_{i=1}^{m}(X - \alpha_i)\Pi_{j=1}^{p} f_i$, ou les f_i sont irréductibles La décomposition de g en facteur irréductible est $\Pi_{i=1}^{m}(X - \varphi(\alpha_i))\Pi_{j=1}^{p} g_i$, ou les g_i sont les polynomes dont les coefficients sont les images de ceux des f_i.

Si $m \geqslant 1$, c'est à dire si f a au moins une racine dans $\mathbb{K}$ (et donc g dans $\mathbb{K}'$) on obtient le résultat grâce à l'hypothèse de récurrence en remplaçant f par $\Pi_{j=1}^{p} f_i$ et g par $\Pi_{j=1}^{p} g_i$: ces deux polynômes de degré $\leqslant n$, les corps $\mathbb{K}$ et $\mathbb{K}'$ sont des corps de décomposition, et il existe donc un isomorphisme de $\mathbb{K}$ sur $\mathbb{K}'$

Pour le cas général, on remarque que si α est une racine de f_1 dans $\mathbb{L}$ et β une racine de g_1 dans $\mathbb{L}'$ il existe un isomorphisme φ_1 de $\mathbb{K}_1 = \mathbb{K}[\alpha] \subset \mathbb{L}$ dans $\mathbb{K}_1' = \mathbb{K}'[\beta]$ qui étend φ. Notons que $\mathbb{L}$ est un corps de décomposition de f vu comme polynôme de $\mathbb{K}_1[X]$ et $\mathbb{L}'$ est un corps de décomposition de g vu comme polynôme de $\mathbb{K}_1'[X]$.

Mais dans $\mathbb{K}_1$, le polynôme f a une racine, et donc d'après ce qui précède l'isomorphisme de $\mathbb{K}_1$ sur $\mathbb{K}_1'$ (qui étendait φ) s'étend en un isomorphisme de $\mathbb{L}$ et $\mathbb{L}'$.

□

On a une proposition très importante

THÉORÈME 2.4. *Si $P \in \mathbb{K}[X]$ est irréductible et si α, α' sont deux racines de f dans un corps de décomposition $\mathbb{L}$ de P, il existe un automorphisme de corps qui envoie α sur α'.*

Démonstration. Soit $\mathbb{K}_1 = \mathbb{K}[\alpha] \subset \mathbb{L}$, $\mathbb{K}_2 = \mathbb{K}[\alpha']$. Il existe un (unique) isomorphisme de $\mathbb{K}_1$ sur $\mathbb{K}_2$ qui envoie α sur α'. Mais $\mathbb{L}$ est aussi un corps de décomposition de P sur $\mathbb{K}_i$, donc il existe un isomorphisme de $\mathbb{L}$ qui envoie α sur α'. □

Exemple 2.9. Le corps de décomposition de $(X^2-2)(X^2-5)$ est $\mathbb{Q}[\sqrt{2}, \sqrt{5}]$, on a vu qu'il est de degré 4 et qu'on peut aussi l'écrire $(\mathbb{Q}[\sqrt{2}])[\sqrt{5}]$. En appliquant le théorème 2 fois, on voit qu'il existe des automorphismes de ce corps qui transforment $\sqrt{2}$ en $\pm\sqrt{2}$ et $\sqrt{5}$ en $\pm\sqrt{5}$. Ça fait un groupe à 4 éléments, commutatif, et il n'est pas difficile de se convaincre que c'est $\mathrm{Gal}(\mathbb{Q}[\sqrt{2}, \sqrt{5}])$. En effet ce corps est engendre par $\sqrt{2}, \sqrt{5}$ et si un automorphisme fixe ces deux éléments c'est donc l'identité.

Ainsi si f est irréductible, et $\mathbb{L}$ est le corps de décomposition, l'action de $\mathrm{Gal}(\mathbb{L}:\mathbb{K})$ est transitive sur les racines de f, mais cette action est aussi fidèle car ce corps et engendré par les racines de ce polynôme (par définition). Ainsi, nous avons démontré :

THÉORÈME 2.5. *Soit $P \in \mathbb{K}[X]$ un polynôme irréductible, et $\mathbb{L}$ un corps de décomposition. Alors l'action de* $\mathrm{Gal}(\mathbb{L}:\mathbb{K})$ *sur l'ensemble des racines de P est transitive et fidèle. Ainsi,* $\mathrm{Gal}(\mathbb{L}:\mathbb{K})$ *est un sous groupe du groupe des permutations des racines de P.* □

Il est très facile de construire une clôture algébrique d'un corps dénombrable à partir de ce résultat. Nous énonçons le cas général, et démontrons le cas particulier où $\mathbb{K}$ est **dénombrable**.

THÉORÈME 2.6. *Soit $\mathbb{K}$ un corps. Il existe un corps algébriquement clos $\bar{\mathbb{K}}$ qui est une extension algébrique de $\mathbb{K}$. Ce corps est unique à isomorphisme près.*

Démonstration. On remarque que l'ensemble des polynômes (non constants) à coefficients dans $\mathbb{K}$ est dénombrable (on a supposé que $\mathbb{K}$ l'est). On les énumère $(f_i)_{i\in\mathbb{N}}$. D'après ce qui précède, il existe une suite d'extensions $\mathbb{L}_i \subset \mathbb{L}_{i+1}$ -unique à isomorphisme près- telle que $\mathbb{L}_i$ soit un corps de décomposition du polynôme $q_i = f_1 .... f_i$. $\mathbb{L}_i$ est un corps de décomposition de f_i sur $\mathbb{L}_{i-1}$. La « réunion » $\cup\mathbb{L}_i$ (en fait c'est plutôt une limite directe) est un corps algébriquement clos (Prop. 2.18).

Pour l'unicité, supposons qu'on en ait deux, $\bar{\mathbb{K}}$, $\bar{\mathbb{K}}'$. On note $\mathbb{L}_i \subset \bar{\mathbb{K}}$, $\mathbb{L}'_i \subset \bar{\mathbb{K}}'$ le sous corps engendré par les racines de q_i. En remarquant que $\mathbb{L}_i$ est un corps de décomposition de q_i sur $\mathbb{L}_{i-1}$, on montre par récurrence qu'il existe une suite φ_i d'isomorphismes $\mathbb{L}_i \to \mathbb{L}'_i$ tels que la restriction de φ_i à $\mathbb{L}_{i-1}$ est φ_{i-1}., d'où le résultat.

□

Remarque 2.6. On remarque que cette démonstration dépend de ACD. Pour le cas général elle dépend de AC. Cependant pour un corps fini, ou pour $\mathbb{Q}$ il est facile de construire une énumération explicite des polynômes à coefficients dans $\mathbb{K}$, ce que nous allons faire au prochain paragraphe pour $\mathbb{F}_p$, et donc en fait n'en dépend pas. pour $\mathbb{Q}$ on peut prendre le sous corps de $\mathbb{C}$ formé des nombres algébriques? mais on utilise secrètement le théorème de d'Alembert-Gauss, donc de l'analyse ce qui est en général peu apprécié des algébristes.

COROLLAIRE 2.3. *Tout corps fini admet une clôture algébrique.*

On verra dans le prochain paragraphe comment construire cette clôture sans se fatiguer.

2.3. Corps finis, automorphisme de Frobenius.

Soit $\mathbb{K}$ un corps fini, et p sa caractéristique. Alors $\mathbb{K}$ est un $\mathbb{F}_p$ espace vectoriel de sorte que le cardinal de $\mathbb{K}$ est un puissance de p. Un tel corps a un automorphisme particulier, l'automorphisme de Frobenius.[2.2] On dit aussi «le Frobenius», par affection.

Théorème 2.7. *Si* $\mathrm{Car}(\mathbb{K})=p$ *l'application* $\Phi:\mathbb{K}\to\mathbb{K}$ *définie par* $\Phi(x)=x^p$ *est un automorphisme. L'ensemble de ses points fixes est précisément le corps premier* $\mathbb{F}_p$.

Démonstration. On a $(x+y)^p=x^p+y^p+\Sigma_{i=1}^{p-1}\left(\begin{smallmatrix}p\\ i\end{smallmatrix}\right)x^iy^{p-i}$

Dans $\mathbb{N}$, $\left(\begin{smallmatrix}p\\ i\end{smallmatrix}\right)=\frac{p!}{i!(p-i)!}$. Mais si $0<i<p$ alors $i!$ et $(p-i)!$ sont inversibles dans $\mathbb{F}_p$, donc cette écriture reste vraie dans ce corps et modulo p $\left(\begin{smallmatrix}p\\ i\end{smallmatrix}\right)=\frac{p!}{i!(p-i)!}=0$.

Ainsi $\Phi(x+y)=\Phi(x)+\Phi(y)$, et comme $\Phi(xy)=\Phi(x)\Phi(y)$, Φ est un automorphisme de $\mathbb{K}$.

Notons que si n est un entier, $\Phi(nx)=n\Phi(x)$ donc si $k\in\mathbb{F}_p$, $\Phi(k)=k\Phi(1)=k$.

Par ailleurs Φ est injective puisque c'est un homomorphisme de corps, et donc surjective puisque $\mathbb{K}$ est fini.

Nous connaissons déjà p racines de l'équation $X^p=X$, donc nous les connaissons toutes : les points fixes de Φ sont justement les éléments de $\mathbb{F}_p$.

□

La classification des corps finis est donnée par le résultat suivant.

Théorème 2.8. *Soit* $q=p^n$. *Il existe un corps* $\mathbb{F}_q$ *ayant* q *éléments. Celui-ci est unique à isomorphisme près. Il est isomorphe au corps de décomposition du polynôme* X^q-X *sur* $\mathbb{F}_p$.

Démonstration. Si $\mathbb{K}$ a q éléments, le groupe $\mathbb{K}^*=\mathbb{K}-\{0\}$ a $q-1$ éléments et donc, grâce au théorème de Lagrange, tout élément de ce groupe satisfait $x^{q-1}=1$; soit $x^q-x=0$. Le polynôme X^q-X de $\mathbb{F}_p[X]$ a exactement q racines dans $\mathbb{K}$; et donc $\mathbb{K}$ est un corps de décomposition de ce polynôme.

Si $\mathbb{K}$ est un corps de décomposition de ce polynôme, et si k est l'ensemble des racines de X^q-X, alors k est un corps car c'est l'ensemble des points fixes de l'automorphisme Φ^n. Donc c'est le plus petit sous corps de $\mathbb{K}$ contenant les racines de X^q-X, c'est-à-dire $\mathbb{K}$. pour vérifier que $\mathbb{K}$ a le bon nombre d'éléments notons que X^q-X n'a pas de racine double car son polynôme dérivé est constant $(X^q-X)'=-1$. Or si un polynôme a une racine double celle ci est une racine du polynôme dérivé. □

Une variante de ce théorème permet de décrire les sous-corps de $\mathbb{F}_q$.

Théorème 2.9. *Soit* $q=p^n$, *et* $\mathbb{F}_q$ *un corps un* q *éléments. Si* $k\subset\mathbb{F}_q$ *est un sous corps, il existe un entier* d *qui divise* n *tel que* $|k|=p^d$, *donc* $k\simeq\mathbb{F}_{p^d}$. *Réciproquement si* d *divise* n $\mathbb{F}_q$ *contient un unique sous-corps à* p^d *élément : c'est l'ensemble des points fixes de* Φ^d.

Démonstration. Le premier point résulte du fait que $\mathbb{F}_q$ est alors un k espace vectoriel de dimensionp^d. Donc p^n est une puissance de p^d c'est à dire que d divise. le second qu'un corps de décomposition de X^q-X contient q racines de ce polynômes donc il contient p^d racines du polynômes $X^{p^d}-X$ qui le divise (pourquoi ?). □

2.2. Ferdinand Georg Frobenius 1848-1917.

On a $\frac{p^n-1}{p^d-1}=1+p^d+....p^{d(\frac{n}{d}-1)}=a\in\mathbb{N}$ donc $X^{p^n-1}=\left(X^{p^d-1}\right)^a$

et donc $\frac{X^{p^n-1}-1}{X^{p^d-1}-1}=1+\left(X^{p^d-1}\right)+\cdots+\left(X^{p^d-1}\right)^{a-1}$

Notons que $\mathbb{F}_{p^{nk}}$ est une extension de $\mathbb{F}_{p^n}$ qui est son sous corps des points fixe de Φ^n. on peut alors construire le corps $\mathbb{F}_{p^\infty}$ comme la limite directe du système $\mathbb{F}_{p^{n!}}\hookrightarrow\mathbb{F}_{p^{(n+1)!}}$, ou à chaque étape in choisi une injection.

PROPOSITION 2.12. *La limite directe du système $\mathbb{F}_{p^{n!}}\hookrightarrow\mathbb{F}_{p^{(n+1)!}}$, ou l'on choisi à chaque étape une injection est un corps algébriquement clos.*

2.4. LE GROUPE $\mathbb{K}^*$.

Soit $\mathbb{K}$ un corps. Le groupe $(\mathbb{K}^*,\times)$ est un groupe abélien. Pour l'étudier, on va utiliser le théorème de structure des groupes abéliens de type fini.

Rappel. Un groupe cyclique d'ordre d est isomorphe soit à $\mathbb{Z}/d\mathbb{Z},+$, soit $\mathbb{U}_d,\times$, où $\mathbb{U}_d$ est le groupe des racines $d-$ièmes de l'unité dans $\mathbb{C}$. Ceci dit en général, il n'y a pas d'isomorphisme préféré.

THÉORÈME 2.10. *(Cours de L3) Soit A un groupe abélien fini. Il existe un entiers r et des entiers $d_1|d_2|...|d_{r-1}|d_r$ tels que $d_1>1$ tel que A soit isomorphe à un produit de groupes cycliques d'ordre d_1.*
$A\simeq\mathbb{U}_{d_1}\times\cdots\times\mathbb{U}_{d_r}\simeq\mathbb{Z}/d_1\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/d_r\mathbb{Z}$.

Démonstration. C'est un cas particulier du théorème sur les modules de type fini sur un anneau principal, quand cet anneau est $\mathbb{Z}$. □

COROLLAIRE 2.4. *Si, dans le groupe $(A,\times)$ l'équation $X^{d_1}=1$ à au plus d_1 solutions, alors $r=1$ et A est cyclique.*

THÉORÈME 2.11. *Soit $\mathbb{K}$ un corps, alors tout sous groupe fini de $(\mathbb{K}^*,\times)$ est cyclique. Son ordre est son exposant.*

Démonstration. En effet, l'équation $X^d=1$ a au plus d solutions dans le corps $\mathbb{K}$, donc dans le groupe $\mathbb{K}^*$. □

DÉFINITION 2.14. *Dans un groupe cyclique C, un élément x est dit primitif si il engendre C.*

Si x est un élément primitif de $\mathbb{F}_q$, les éléments $(x^i)_{0\leqslant i<q}$ décrivent tous les éléments de $\mathbb{F}_q-\{0\}$, en particulier, on a la proposition

PROPOSITION 2.13. *Si $x\in\mathbb{F}_q^*$ est primitif, $\mathbb{F}_p[x]=\mathbb{F}_q$.*

Démonstration. En effet, $\mathbb{F}_p[x]$ contient toutes les puissances de x donc toute $\mathbb{F}_q^*$. □

Remarquons que le polynôme minimal de x est alors de degré $n=\log_p q$: en effet c'est la dimension du sous corps engendré par x. Du coup, $\mathbb{F}_q$ devient le corps de rupture de ce polynôme, c'est en même temps le corps de décomposition vu que ce polynôme divise $X^{q-1}-1$ qui est scindé sur $\mathbb{F}_q$.

Il en résulte que son groupe d'automorphisme est de cardinal inférieur à son degré qui est n.

THÉORÈME 2.12. *Le groupe des automorphismes de $\mathbb{F}_q$ (sur $\mathbb{F}_p$) est le groupe cyclique d'ordre n engendré par l'automorphisme de Frobenius $\Phi(x)=x^p$.*

Démonstration. Il suffit de se convaincre que si x est primitif, les éléments x, $\Phi(x)$, $\Phi^2(x)$, $....\Phi^{n-1}(x)$ sont tous distincts. En effet sinon on aurait $\Phi^k(x)=x$ pour un certain $k<n$ et $x\in\mathbb{F}_{p^k}$. □

Il est tout a fait légitime de se demander combien y a t il d'élément primitifs dans $\mathbb{F}_q^*$. Pour cela, on rappelle la définition de l'indicateur d'Euler[2.3].

Définition 2.15. *Si n est un entier, on appelle indicateur d'Euler, et on note $\varphi(n)$ le nombre de générateurs d'un groupe cyclique d'ordre n.*

Proposition 2.14. *$\varphi(n)$ est le nombre des entiers plus petit que n et premier à n. ou si l'on préfère le nombre des éléments inversibles de $(\mathbb{Z}/n\mathbb{Z}^*, \times)$.*

Démonstration. Un entier a est inversible modulo n si et seulement si il est premier à n d'après Bézout. Si modulo n, a est inversible et si b est son inverse, on a $(\omega^a)^b = \omega$, donc ω est un générateur d'un groupe cyclique d'ordre n si et seulement si ω^a l'est. □

Remarque 2.7. Par définition, le nombre d'éléments primitifs de $\mathbb{F}_q^*$ est donc $\varphi(q-1)$

La proposition suivante est très utile.

Lemme 2.2. *1. Si* $\text{pgcd}(m,n) = 1$, $\varphi(mn) = \varphi(m)\varphi(n)$
2. Si p est premier, $\varphi(p^n) = p^n - p^{n-1} = p^n\Big(1 - \frac{1}{p}\Big)$.

Démonstration. 1. En effet, si $\text{pgcd}(m, n) = 1$, alors $\mathbb{U}_{mn} = \mathbb{U}_m \times \mathbb{U}_n$ (lemme chinois) et un élément engendre $\mathbb{U}_m$ si et seulement si ses deux images engendrent $\mathbb{U}_m$ et $\mathbb{U}_n$ respectivement.
2. Un élément de $\mathbb{U}_{p^n}$ qui n'engendre pas ce groupe est d'ordre p^{n-1}. □

Proposition 2.15. *Si $n = p_1^{s_1}....p_r^{s_r}$ est la décomposition de n en facteurs premiers, alors le nombre d'éléments primitifs d'un groupe cyclique d'ordre n est $\varphi(n) = n\Pi_{p|n}\Big(1 - \frac{1}{p}\Big)$.*

2.5. Cyclotomie.

On a vu que, quel que soit le corps, un sous-groupe abélien fini d'ordre n de $\mathbb{K}^*$ est isomorphe à $\mathbb{U}_n = \{z \in \mathbb{C}/z^n = 1\}$.

Nous utiliserons volontiers le fait que ce groupe $(\mathbb{U}_n, \times)$ est cyclique, c'est à dire isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$. Choisir un isomorphisme $\mathbb{Z}/n\mathbb{Z} \to \mathbb{U}_n$ c'est choisir une racine primitive de l'unité.

Il est fréquent que pour démontrer un énoncé sur $\mathbb{U}_n$ (ou sur $\mathbb{Z}/n\mathbb{Z}$) on le traduise grâce à cet isomorphisme. Voici un exemple.

Proposition 2.16. *Soit ω une racine primitive n-ième de l'unité et k un entier. Alors ω^k est une racine primitive n-ième de l'unité si et seulement si k est inversible modulo n, si et seulement* si le pgcd $k \wedge n$ *k et n sont premiers entre eux*

Démonstration. On utilise l'isomorphisme $\mathbb{Z}/n\mathbb{Z} \to \mathbb{U}_n$ donné par ω. L'énoncé devient k est un générateur de $\mathbb{Z}/n\mathbb{Z}$ si et seulement si k est inversible modulo n, si et seulement si $k \wedge n = 1$. En effet le théorème de Bézout nous dit que $k \wedge n = 1$ si et seulement si il existe des entiers u, v tels que $uk + vn = 1$. □

2.3. L'un des tous derniers articles de L. Euler 1707-83, publié en 1784 donc après sa mort. La définition est « *denotet character $\varphi(d)$ multitudinem istam numerorum ipso d minorum, et qui cum nullum habeant divisorem communem* »

Les éléments de ce groupe sont exactement les racines du polynôme $X^n - 1$ qui ne dépend manifestement pas du corps choisi. Nous allons décomposer ce polynôme en facteurs irréductibles, et voir que l'un de ces facteurs est précisément le polynôme dont les racines sont les racines primitives n-ièmes de l'unité.

Nous pouvons écrire $X^n - 1 = \Pi_{k \in \mathbb{Z}/n\mathbb{Z}}(X - \omega^k)$, où ω est une racine primitive n ième de l'unité, par exemple $\omega = e^{i\frac{2\pi}{n}}$.

Remarque 2.8. La notion de « racine primitive de l'unité » n'a pas de sens en soi. Si pour un certain entier n, on a $\omega^n = 1$, l'ensemble des entiers satisfait cette identité est un sous groupe de $\mathbb{Z}$ de la forme $d\mathbb{Z}$, où d est l'ordre de ω. Ainsi ω est un générateur de $\mathbb{U}_d$ autrement dit une racine primitive $d-$ième de l'unité.

2.5.1. Les polynômes cyclotomiques.

Rappelons que si ω est une racine primitive $n$ième de l'unité, c'est à dire un générateur de $\mathbb{U}_n$, les autres sont les ω^k, où k est inversible modulo n.

DÉFINITION 2.16. *Soit $n \in \mathbb{N}$ un entier. On appelle n-ième polynôme cyclotomique* [2.4]*, et l'on note Φ_n le polynôme unitaires dont les racines sont les racines primitives nième de l'unité. On a donc $\Phi_n(X) = \Pi_{k \in \mathbb{Z}/n\mathbb{Z}^*}(X - \omega^k)$*

Exemple 2.10. Si $n = p$ est un nombre premier, tous les éléments de $\mathbb{Z}/n\mathbb{Z}$ sont inversibles, sauf 0. Il en résulte que $(X-1)\Phi_p(X) = X^p - 1$. Ainsi $\Phi_p(X) = 1 + X + X^2 + \cdots + X^n$.

PROPOSITION 2.17. *Le polynôme Φ_n est unitaire, à coefficients entiers, de degré $\varphi(n)$.*
On a de plus : $X^n - 1 = \prod_{d|n} \Phi_d(X)$

Démonstration. Le point 2 résulte de la remarque précédente : toute racine n ième de l'unité d'ordre d est une racine primitive d-ième de l'unité.

Le point 1 en résulte par récurrence sur l'entier n. De fait, Φ_n n'est autre que le quotient du polynôme $X^n - 1$ de $\mathbb{Z}[X]$par $\Pi_{d|n, d<n}\Phi_d$. Comme celui-ci est unitaire, le quotient est bien un polynôme de $\mathbb{Z}[X]$ □

La formule est bien utile pour calculer les polynômes en questions.
par exemple $X^6 - 1 = (X-1)\Phi_2(X)\Phi_3(X)\Phi_6(X) = (1+X)(X^3-1)\Phi_6(X)$
$\Phi_6 = (X^3+1) : (X+1) = X^2 - X + 1$

Parmi les propriétés célèbres de polynômes cyclotomiques, il y en a deux.

PROPOSITION 2.18. *Si $n \not\equiv 0(\mathrm{car}(K))$ les racines de Φ_n sont simples.*

Démonstration. On écrit par l'absurde $X^n - 1 = (X-\alpha)^2 Q$
On dérive $nX^{n-1} = (X-\alpha)(2Q + (X-\alpha)Q')$, d'ou $n\alpha^{n-1} = 0$ et $n \equiv 0(\mathrm{car}(K))$ □

THÉORÈME 2.13. *(Gauss) Les polynômes cyclotomiques sont irréductibles dans $\mathbb{Z}[X]$.*

La démonstration est assez ardue, et se fait en quatre lemmes.

2.4. Cyclotomique est composé du grec $\kappa\upsilon\kappa\lambda o\varsigma$ le cercle, et de $\tau o\mu\acute{\eta}$ découper. Découper les gâteaux en n parts égales, revient à construire une racine primitive n ième de l'unité, peu importe laquelle. Nous reviendrons sur le problème des gâteaux en fin de chapitre.

Lemme 2.3. *Soient f, g deux polynômes de $\mathbb{K}[X]$. on suppose que f est irréductible et que f, g ont une racine commune dans une extension $\mathbb{L}$ de $\mathbb{K}$. Alors f divise g.*

Démonstration. Sinon, il seraient premier entre eux. Donc on peut trouver deux polynômes u, v tels que $uf + vg = 1$ □

Lemme 2.4. *Soient f, g deux polynômes unitaires de $\mathbb{Q}[X]$ si $fg \in \mathbb{Z}[X]$ alors f et g aussi.*

Démonstration. Soit d le ppcm des dénominateurs des coefficients de f et e celui de g. Le contenu de df divise d car le polynôme fg est unitaire, donc le premier coefficient de dfg est d. Or $c(df)c(eg) = dec(fg)$, donc $c(dF).c(eG) = d.e$. Il en résulte que $c(dF) = d$. Donc $F = \frac{dF}{c(dF)} \in \mathbb{Z}[X]$. □

Soit $f \in \mathbb{Q}[X]$ un facteur irréductible de Φ_n, supposé unitaire. Il s'agit de démontrer que toutes les racines primitives $n - i$èmes de 1 sont des racines de f. Soit ω une racine de f, qui est entre parenthèse une racine de Φ_n, donc une racine primitive n-ième de l'unité. Il s'agit de vérifier que pour tout nombre k premier à n , ω^k est aussi racine de f. Par récurrence on doit juste vérifier.

Lemme 2.5. *Si le nombre premier p ne divise pas n, alors ω^p est une racine de F.*

On écrit $X^n - 1 = f(X)g(X)$ dans $\mathbb{Q}[X]$, g unitaire.
Alors f, g sont tous les deux dans $\mathbb{Z}[X]$.
Pour prouver que $f(\omega^p) = 0$, il suffit de vérifier que $g(\omega^p) \neq 0$
Sinon, $g(X^p)$ aurait ω comme racine, et il serait donc divisible par f : $g(X^p) = f(X)h(X)$
avec toujours $h \in \mathbb{Z}[X]$.

On a dans l'anneau $\mathbb{Z}[X]$: $X^n - 1 = f(X)g(X)$ et $g(X^p) = f(X)h(X)$

Alors idée brillante, on réduit le tout modulo p, en nous rappelant que $g(X^p) = g(X)^p\,(p)$

Ainsi, dans $\mathbb{F}_p$ tout facteur irréductible h de f divise g. Alors h^2 divise $X^n - 1$ dans $\mathbb{F}_p$.

Lemme 2.6. *Si $(p, n) = 1$, il n'y a pas de polynôme non constant dont le carré divise $X^n - 1$ dans $\mathbb{F}_p$*

Démonstration. Si $X^n - 1 = h^2 r$, et qu'on dérive, on obtient $nX^{n-1} = h(2h' + hr')$. Donc en fait h divise X^{n-1}, et $h = aX^k$. En spécialisant en 0, on obtient $0 - 1 = 0$. Nous avons divisé par n ce qui est loisible car $(n, p) = 1$. □

2.5.2. Extension cyclotomiques.

Définition 2.17. *Le n-ième corps cyclotomique, $\mathbb{R}_n[\mathbb{Q}]$ est le plus petit corps de $\mathbb{C}$ qui contient toutes les racines nièmes de l'unité.*

Notons que si un corps contient une racine **primitive** n ième de l'unité, il contient toutes les racines, car se sont des puissances de celle-ci. On a donc.

Proposition 2.19. *Si ω est une racine primitive nième de l'unité, $\mathbb{R}_n(\mathbb{Q}) = \mathbb{Q}[\omega]$.*
Le corps $\mathbb{R}_n(\mathbb{Q}), \omega$ est isomorphe au corps de rupture de Φ_n c'est à dire à $\mathbb{Q}[X]/\Phi_n$, X. Sa dimension est $\varphi(n)$
Le corps $\mathbb{R}_n(\mathbb{Q})$ est aussi un corps de décomposition de Φ_n.

Rappelons que l'ensemble des racines primitives n ième de l'unité est en bijection avec l'ensemble $\mathbb{Z}/n\mathbb{Z}^*$ des inversibles de $(\mathbb{Z}/n\mathbb{Z}, \times)$. plus précisément si ω est un racine primitive n ième de l'unité ω^k est primitive si et seulement si k est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

PROPOSITION 2.20. *Soit $G = \mathrm{Gal}(R_n[\mathbb{Q}])$ le groupe des automorphismes de $\mathbb{R}_n[\mathbb{Q}]$; et soit ω une racine primitive $n-$ième de l'unité. L'application $\theta: G \to (\mathbb{Z}/n\mathbb{Z})^*$ définie par $g(\omega) = \omega^{\theta(g)}$ est un isomorphisme de groupes.* □

COROLLAIRE 2.5. *Le groupe $\mathrm{Gal}(R_n[\mathbb{Q}])$ est abélien, isomorphe à $(\mathbb{Z}/n\mathbb{Z})^*$. Il est même cyclique d'ordre $n-1$ si n est un nombre premier.*

2.6. La règle, le compas et les parts de gâteau.

Ce paragraphe est là pour respecter la tradition : on va étudier les résultats de P.-L. Wantzel (*Recherches sur les moyens de reconnaître si un problème de géométrie peut se résoudre avec la règle et le compas* », 1837). Typiquement peut on découper un gâteau en 7 parts égales, pour les gourmands, ou pour les grecs anciens peut-on trisecter (découper en 3) un angle donné, ou résoudre la quadrature du cercle, ou dupliquer un cube.

Dans un article célèbre, P.L. Wantzel ramène tout cela à un problème de théorie des corps, plus précisément, il démontre que si on peut construire un point à la règle et au compas, alors on peut dire quelque chose d'intéressant sur le sous corps de $\mathbb{R}$ engendré par ses coordonnées, ou le sous-corps de $\mathbb{C}$ engendré par l'affixe de ce point.

2.6.1. Le corps des nombres constructibles.

On considère un plan euclidien et dedans un certains nombres de points P supposés connus, (whatever this means).

A cet ensemble P on associe l'ensemble des droites D passant par deux points de P et l'ensemble des cercles C_0 centrés en un point de P et passant par un autre ou centrés en un point et dont le rayon est la distance entre deux autres points de P.

On dit qu'un point est constructible à la règle et au compas en une fois à partir de P si soit il se trouve à l'intersection de deux droites, de deux cercles ou d'un cercle et d'une droite de $D(P)$, $C(P)$.

On dit qu'un point est constructible en n étapes à partir d'un ensemble de points P si il peut l'être en une étape à partir des points constructibles en $(n-1)$-étapes à partir de P.

Dans la tradition on suppose que $P = P_0$ est constitué de 2 points, appelés $(0,0) = 0$ et $(1,0) = 1$. Mais on peut aussi partir d'un ensemble de points plus compliqué, disons P_0 et chercher quels points on peut construire à partir de cet ensemble. Nous supposerons que P_0 contient au moins deux points qu'on appelle 0 et 1.

A partir de ces deux points, il est facile de construire la droite passant par ces deux points, que nous appellerons l'axe des abscisses, qui est affinement une droite réelle. Un nombre réel est dit constructible si c'est un point constructible (à partir de $\{0,1\}$) de cette droite.

On peut s'amuser (si si) à démontrer successivement

PROPOSITION 2.21.
La médiatrice de deux points constructibles est constructible.
La perpendiculaire à une droite donnée passant par un point donné est constructible
La parallèle à une droite donnée passant pas un point donné est constructible

La droite perpendiculaire à l'axe des abscisses (l'axe des ordonnées) est constructible.
Le nombre $-1 \in \mathbb{R}$ *et le point* $i = (0,1)$ *sont constructibles.*
Le point (x,y) *est constructible si et seulement si les réels* x, y *le sont.*
Si x, y *sont deux nombre réels constructibles* $x+y, x-y, xy, \frac{1}{x}$ *le sont aussi.*

Démonstration. Faire quelques jolis dessins. □

Proposition 2.22. *Si* $x \in \mathbb{R}^+$ *est constructible,* $\sqrt{x}$ *aussi.*

Démonstration. On cherche deux nombre r, c tels que l'intersection du cercle $x^2+y^2=r^2$ avec la droite $x=c$ soit les deux points $\pm(0,\sqrt{x})$.

il vient $r^2-c^2=x$, soit $(r-c)(r+c)=x$. On peut prendre $r=\frac{1+x}{2}$ $c=\frac{x-1}{2}$ qui sont tous les deux constructibles. □

Définition 2.18. *On dit que le nombre complexe* z *est constructible si c'est l'affixe d'un point constructible.(à partir de* $\{0,1\}$*)*

On a donc

Proposition 2.23. *L'ensemble des nombres complexes constructibles à partir d'un ensemble est un corps, dans lequel tout élément est un carré.* □

Théorème 2.14.
L'ensemble des nombres complexes constructibles (à partir de $\{0,1\}$*) est un sous corps de* $\mathbb{C}$. *Tout élément* z *de ce corps est algébrique et son degré* $[\mathbb{Q}[z]:\mathbb{Q}]$ *est une puissance de deux.*

Démonstration.
Elle repose sur le

Lemme 2.7. *Soit* $\mathcal{P}$ *sous ensemble de* $\mathbb{C}$, $\mathbb{K} \subset \mathbb{R}$ *le sous corps engendré par les coordonnées des éléments de et* P^* *un points construit en une étape à partir de* $\mathcal{P}$ *et* $\mathbb{L}$ *le sous corps de* $\mathbb{R}$ *engendré par* $\mathbb{K}$ *et les coordonnée de P. Alors* $[\mathbb{L}:\mathbb{K}]$ *vaut 1,2 ou 4*

Si P, Q sont dans $\mathcal{P}$, l'équation du cercle de centre P passant Q est $(x-x_p)^2+(y-y_p)^2 = (x_q-x_p)^2+(y_q-y_p)^2$, soit $x^2+y^2+ax+by=c=0$ à coefficients dans $\mathbb{K}$. L'équation de la droite passant par ces points est $(y_p-y_q)(x-x_p)+(x_q-x_p)(y-y_p)=0$

Ainsi l'abscisse et l'ordonnée de l'intersection d'un cercle et d'une droite, ou de deux cercles, ou de deux droites, s'obtiennent en résolvant une équation de degré 2 ou 1 à coefficients dans $\mathbb{K}$. Donc si (x^*, y^*) sont les coordonnées de P^* $[\mathbb{K}[x^*]:\mathbb{K}] =$ 1 ou 2, et $[\mathbb{K}[y^*]:\mathbb{K}]=1$ ou 2, puis $[\mathbb{L}:\mathbb{K}]$ = 1,2 ou 4.

□

Remarque 2.9. Le fait que l'ensemble des points constructibles est un corps est intéressant en soi, mais n'est pas utile pour démontrer que l'affixe d'un point constructible est un algébrique et que son degré est une puissance de 2.

Proposition 2.24. *Si un point d'affixe* z *est constructible, non seulement son degré est une puissance de 2, mais en fait il existe une suite de corps* $\mathbb{K}_0=\mathbb{Q}, \mathbb{K}_1 \subset \mathbb{K}_2 .... \mathbb{K}_n$ *tels que* $\mathbb{K}_{i+1}=\mathbb{K}_i$ *soit de degré 2.*

Cette proposition permet de démontrer qu'il existe des nombres algébriques de degré 2^n par exemple de degré 4 qui ne sont pas constructibles (voir au paragraphe sur le théorème de Wantzel). Pour s'assurer de la constructibilité, il faudra s'assurer que le degré du corps de décomposition du polynôme minimal soit une puissance de 2.

2.6.2. La duplication du cube, la trisection de l'angle, la quadrature du cercle et les parts de gâteau.

Le premier problème grec que nous étudions est celui de la duplication du cube. D'après notre ami Wiki, qui cite[2.5] « Ce problème a son origine dans une légende rapportée entre autres par Eratosthene (3-ième siècle avant notre ère) dans le *Platonicien* et par Théon de Smyrne (2-ième siècle avant notre ère) dans son *Arithmétique*. Les Déliens, victimes d'une épidémie de peste, demandèrent à l'oracle de Delphes comment faire cesser cette épidémie. La réponse de l'oracle fut qu'il fallait doubler l'autel consacré à Apollon, autel dont la forme était un cube parfait. Les architectes allèrent trouver Platon pour savoir comment faire. Ce dernier leur répondit que le dieu n'avait certainement pas besoin d'un autel double, mais qu'il leur faisait reproche, par l'intermédiaire de l'oracle, de négliger la géométrie ».

Si l'on reformule le problème, étant donné un cube de coté a donné comment en construire un de volume double c'est-à-dire trouver un nombre x tel que $x^3 = 2a^3$, ou $\left(\frac{x}{a}\right)^3 = 2$. Mais le nombre $\sqrt[3]{2}$ n'est pas constructible sinon son degré sur $\mathbb{Q}$ serait une puissance de 2. Il faut donc attendre Wantzel 1838 pour répondre à cette intéressante question.

On dit que l'angle θ est constructible si le point $(\cos\theta, \sin\theta)$, ou le nombre complexe $e^{i\theta}$ est constructible à la règle et au compas. Comme la construction d'une bissectrice à la règle et au compas est facile à faire, on voit que si θ se construit on peut le couper en deux, c'est à dire que $\theta/2$ l'est aussi. Mais peut on le découper en trois parts égales ?

Il s'agit de savoir si on peut construire $(\cos\varphi, \sin\varphi)$ tel que $(\cos 3\varphi, \sin 3\varphi)$ soit donné

On sait que $\cos 3\varphi = 4\cos^3\varphi - 3\cos\varphi$, de sorte que

PROPOSITION 2.25. *On peut trisecter l'angle θ si et seulement si le nombre réel $4x^3 - 3x - \cos(\theta)$ est constructible.*

Démonstration. En effet le nombre réel $\cos\theta$ est constructible si et seulement si le point $(\cos\theta, \sin\theta)$ l'est. □

Remarque 2.10. Le polynôme $4x^3 - 3x - \cos(\theta)$ a **trois** racines réelles. Mais si on en connait une on connait les deux autres, pourquoi ?

Exemple 2.11. Notez que $\exp 2i\pi/6 = \frac{1}{2} + i\frac{\sqrt{3}}{2}$ est constructible vu que c'est l'affixe du point situé à l'intersection du cercle unité centré en 0 et de celui centré en 1. Notez qu'il y a deux points, l'un étant $\exp 2i\pi/6$, l'autre $\exp -2i\pi/6$. L'angle $\pi/6$ est donc constructible, et $\pi/3$ aussi.

Mais nous allons voir $\pi/3$ ne peut pas être trisecté, si tant est que l'on trisectasse, et on ne peut pas donc découper un gâteau en 18 parts égales, ni en 9 pour la même raison.

En effet le polynôme $4x^3 - 3x - \frac{1}{2} = \frac{1}{2}(8x^3 - 6x - 1)$ est irréductible sur $\mathbb{Q}[X]$. En effet si $\frac{p}{q}$ était une racine, alors $8p^3 - 6pq^2 - q^3 = 0$, donc p divise $-1q^3$ donc -1 et q divise $8p^3$ donc 8, ce qui laisse très peu de possibilité dont aucune ne marche.

Un autre problème, plus intéressant le dimanche à midi lors des repas de famille, est de savoir si l'on peut découper un gâteau en n parts égales. On se ramène donc à savoir si les racines $n-i$èmes de l'unité sont des points constructibles du plan. Comme i est de degré 2, on comprend que si $\cos\left(\frac{2\pi}{n}\right)$, $\sin\left(\frac{2\pi}{n}\right)$ sont constructible, alors le degré de $e^{i2\pi/n} = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$ est une puissance de 2, mais on sait que son polynôme minimal sur $\mathbb{Q}$ est le *polynôme cyclotomique*. C'est d'ailleurs pour cela que le polynôme cyclotomique s'appelle ainsi, c'est celui qui permet de découper les cercles en n parts égales..

2.5. Robert Baccou, *Histoire de la science grecque, de Thalès à Socrate*, Paris, Aubier, 1951

Proposition 2.26. *Si on peut découper un gâteau en n parts égales, alors $\varphi(n) = \deg(\Phi_n)$ est une puissance de 2.* □

Par exemple $\Phi_7 = X^6 + \cdots + 1$. On ne peut pas découper un gâteau en 7 parts égales.

Pour continuer, on a besoin d'une définition.

Définition 2.19. *Un nombre premier est dit de Fermat si il est de la forme $2^{2^n}+1$.*[2.6]

Proposition 2.27. *Si un nombre premier est de la forme 2^k+1, il est de Fermat, c'est à dire que k est une puissance de 2.*

Démonstration. On écrit $k = a2^b$. alors $2^k + 1 = (2^{2^b})^a + 1 = (2^{2^b} + 1) \times \Sigma_0^{a-1}(-2^{2^b})^i$, car $x^n + 1 = (x + 1) \times \Sigma_0^{n-1}(-x)^i$. Si le membre de gauche est premier, il doit être égal au premier terme du membre de droite. □

Théorème 2.15. *Wantzel. Si un polygone régulier a n côtés est constructible, alors n est une puissance de 2 ou est le produit d'une puissance de 2 et de nombres premiers de Fermat différents.*

Démonstration. En effet si $n = \Pi_{p\in\mathcal{P}_n} p^{v_p(n)}$ alors le degré du polynôme cyclotomique se calcule à l'aide de l'indicatrice d'Euler : $\varphi(n) = \Pi(p-1)p^{v_p-1}$. Pour que ce nombre soit une puissance de 2, il faut et il suffit que pour chaque $p, (p-1), p^{v_p-1}$ soit une puissance de 2, ce qui implique que $\nu_p - 1 = 0$ pour $p \neq 2$ et $p-1$ est une puissance de 2, disons 2^k. Or si un nombre de la forme 2^k+1 est premier, alors k est une puissance de 2. □

Remarque 2.11. La réciproque du théorème de Wantzel est vraie, mais il faut utiliser un peu de théorie des groupes (tout 2 groupe fini est nilpotent donc résoluble) et de théorie de Galois (si le groupe de Galois est résoluble l'équation l'est aussi), donc on reporte ça plus loin dans le cours.

Le dernier problème, qui est le plus célèbre, est la quadrature du cercle. Il s'agit de savoir si l'on peut construire le nombre $2.\pi$, longueur d'un cercle unité. Or on a un théorème difficile qui dit que c'est impossible.

Théorème 2.16. *Lindenmann. Le nombre π est transcendant.* □

2.7. Exercices du chapitre 2

2.7.1. Paragraphe 2.1, dimensions.

Exercice 2.1. Démontrer que le seul automorphisme de corps de $\mathbb{Q}$ est l'identité. Même question pour $\mathbb{F}_p$.

Démontrer qu'un automorphisme de corps de $\mathbb{R}$ est une fonction croissante, et en déduire que le seul automorphisme de corps de $\mathbb{R}$ est l'identité.

Exercice 2.2. Soit $\mathbb{K}$ un corps fini ou dénombrable, et $\mathbb{L}/\mathbb{K}$ une extension. Démontrer que l'ensemble des éléments de $\mathbb{L}$ algébriques sur $\mathbb{K}$ est dénombrable. En déduire qu'il existe des nombres réels transcendants.

Exercice 2.3. Calculer le degré $[\mathbb{Q}[\sqrt{2},\sqrt{3}]:\mathbb{Q}]$

Exercice 2.4. Trouver les polynômes minimaux sur $\mathbb{Q} \subset \mathbb{C}$ de :

$$\sqrt{2}; \sqrt{3}; \frac{\sqrt{3}}{2}; \frac{2}{\sqrt{3}}; \sqrt{2}+\sqrt{3}; \sqrt{2}+\frac{\sqrt{3}}{2}.$$

Exercice 2.5. Soit $f \in \mathbb{Q}[X]$ un polynôme irréductible de degré impair.

1. Soit x une racine de f dans $\mathbb{C}$. Est ce que $\sqrt{2} \in \mathbb{Q}[x]$?
2. Quel est le degré de l'extension de $\mathbb{Q}$ engendrée par x et $\sqrt{2}$

2.6. En 1640, Fermat émet l'hypothèse que tous les nombres de la forme $F_n = 2^{2^n}+1$ sont premiers. En 1732, Euler, la réfute $2^{2^5}+1 = 42949667297 = 61 \times 6700417$. A l'heure actuelle, les seuls nombres premier de Fermat connus sont les 5 premiers (3,5,17,257,65 597).

3. Montrer que f reste irréductible quand on le voit comme un polynôme à coefficients dans $\mathbb{Q}(\sqrt{2})[X]$.
4. Peut on enlever l'hypothèse « impair » sur le degré de P.

Exercice 2.6. Montrer qu'il n'existe aucun isomorphisme entre les corps $\mathbb{Q}[\sqrt{2}]$ et $\mathbb{Q}[\sqrt{3}]$. Montrer par contre les corps $\mathbb{Q}\Big[\frac{\sqrt[3]{3}}{2}\Big]$ et $\mathbb{Q}\Big[j\frac{3\sqrt{3}}{2}\Big]$ (avec $j=-\frac{1}{2}+i\frac{\sqrt{3}}{2}$) sont isomorphes.

Exercice 2.7. Soient $\alpha=\frac{\sqrt{3}}{7}, \beta=\frac{\sqrt{5}}{10}$ déterminer les degrés des extensions de $\mathbb{Q}$, $\mathbb{Q}[\alpha]$, $\mathbb{Q}[\beta]$, $\mathbb{Q}[\alpha, b]$, $\mathbb{Q}[\alpha+\beta]$.

Exercice 2.8. Soit $\mathbb{K}$ un corps et $\mathbb{L}=\mathbb{L}(T)$ le corps des fractions rationnelles en l'indéterminée T. Montrer que les éléments de $\mathbb{K}$ sont les seuls éléments de $\mathbb{L}$ qui sont algébriques sur $\mathbb{L}$.

Exercice 2.9. Soit $\mathbb{F}$ un corps, $\mathbb{K}_1/\mathbb{F}$ et $\mathbb{K}_2/\mathbb{F}$ deux extensions contenues dans un même corps $\mathbb{E}$ extension de F. On appelle *extension composée* et on note $\mathbb{K}_1\,\mathbb{K}_2$ le plus petit sous-corps de $\mathbb{E}$ qui contient la réunion $\mathbb{K}_1\cup\mathbb{K}_2$ (autrement dit l'intersection de tous les sous-corps qui contiennent $\mathbb{K}_1\cup\mathbb{K}_2$).

Que vaut $\mathbb{K}_1\,\mathbb{K}_2$ si $\mathbb{K}_1=\mathbb{F}(a_1,\dots a_m)$ et si $\mathbb{K}_2=\mathbb{F}(b_1,\dots b_n)$?
Montrer que $\mathbb{K}_1\,\mathbb{K}_2$ est algébrique sur $\mathbb{F}$ si et seulement si $\mathbb{K}_1$ et $\mathbb{K}_2$ le sont.
Montrer que $\mathbb{K}_1\,\mathbb{K}_2$ est de degré fini sur sur F si et seulement si $\mathbb{K}_1$ et $\mathbb{K}_2$ le sont et qu'on a alors l'inégalité :

$$[\mathbb{K}_1\,\mathbb{K}_2\colon\mathbb{F}]\leq[\mathbb{K}_1\colon\mathbb{F}][\mathbb{K}_2\colon\mathbb{F}]$$

Prouver enfin que cette inégalité est une égalité si on suppose que les entiers $[\mathbb{K}_1\colon\mathbb{F}]$ et $[\mathbb{K}_2\colon\mathbb{F}]$ sont premiers entre eux

Exercice 2.10. Soit p un nombre premier.
1. Quelles sont les racines de $X^{p-1}+X^{p-2}+X^{p-3}+\cdots+X^2+X+1$ dans $\mathbb{C}$.

2. On pose $Q(X)=P(X+1)=\frac{(X+1)^p-1}{X}=X^{p-1}+a_{p-2}X^{p-2}+\cdots+a_1X+a_o$
Montrer que $a_i=0(p)$ et que $a_0=p$

3. En déduire que $Q(X)$ est irréductible dans $\mathbb{Z}[X]$. On pourra raisonner par l'absurde et montrer que si $Q=A.B$, alors A et B sont unitaires et tous leurs coefficients sont nuls modulo p, puis regarder a_0b_0. (Méthode d'Eisenstein)

4. En déduire que $Q(x)$ (et donc $P(X)$) est irréductible dans $\mathbb{Q}[X]$

5. Quelles sont les racines primitives $p-$ième de l'unité dans $\mathbb{C}$.

6. Quel est le groupe des $\mathbb{Q}-$automorphismes de $\mathbb{Q}[\omega]$.

Exercice 2.11. On dit que des éléments x_1, ..., x_n d'une extension de corps $\mathbb{L}\colon\mathbb{K}$ sont algébriquement indépendants sur $\mathbb{K}$ si l'application $\mathbb{K}[X_1,\dots X_n]\to\mathbb{K}$ qui à un polynôme associe sa valeur au point x=(x_1,...,x_n) est injective.

Soit $P\in\mathbb{C}[X_1,\dots X_n]$. On pose $V_P=\{z=(z_1,\dots,z_n)\in\mathbb{C}^n\,/\,P(z)=0\}$
En utilisant la formule de Taylor, montrer que si $P\neq 0$ V_P est un fermé d'intérieur vide.
En utilisant le lemme de Baire, montrer qu'il existe des nombres complexes (z_1, ..., z_n) algébriquement indépendants sur $\mathbb{Q}$.

2.7.2. Corps de décomposition.

Exercice 2.12. Soit $a\in\mathbb{Q}$ un rationnel qui n'est pas un carré dans $\mathbb{Q}$, et $\alpha\in\mathbb{C}$ tel que $\alpha^2=a$. Montrer que $\mathbb{Q}[\alpha]$ est de degré 2. Quel est le corps de rupture du polynôme X^2-a.
Montrer que le groupe des automorphismes de ce corps est $\mathbb{Z}/2\mathbb{Z}$.
Généraliser à un polynôme du second degré n'ayant pas de racines dans $\mathbb{Q}$
Réciproquement soit $\mathbb{Q}\subset\mathbb{K}$ une extension de degré 2 démontrer qu'il existe un rationnel Δ tel que $K\approx Q(\sqrt{\Delta})$

Exercice 2.13. Le degré du corps de décomposition d'un polynôme de degré n est inférieur ou égal à $n!$.

Exercice 2.14. Soit $b\in\mathbb{Q}$ un rationnel qui n'est pas un cube dans $\mathbb{Q}$. Soit $\beta\in\boldsymbol{C}$ tel que $\beta^3=b$. Montrer que $Q[\beta]$ est une extension cubique (i.e. de degré 3) de $\mathbb{Q}$. Montrer que cette extension ne contient qu'une seule racine du polynôme X^3-b. (on pourra d'abord supposer que $\beta\in\mathbb{R}$. En déduire que $\mathbb{Q}(\beta)$ n'admet pas d'automorphisme sauf l'identité.
Construire 3 sous-corps de $\mathbb{C}$ qui sont des corps de rupture du polynôme X^3-b.
Quel est le degré du corps de décomposition de ce polynôme?

Exercice 2.15.

a)Vérifier que le polynôme $f = X^3 + X^2 - 2\,X - 1$ admet trois racines réelles qui sont explicitement $x_k = 2\cos\frac{2\,k\,\pi}{7}$ avec $k = 1, 2, 3$. On pourra factoriser le polynôme $Y^7 - 1$, et poser $X = Y + \frac{1}{Y}$.

(b) Montrer que ce polynôme est irréductible sur $\mathbb{Q}$.

c) Démontrer que $\mathbb{K} = \mathbb{Q}[x_1]$ un corps de degré 3 qui contient également x_2 et x_3 (on pourra penser à la formule $\cos(2\alpha) = \cdots =$), et plus précisément il peut être aussi bien engendré par x_2 ou par x_3.

d) Prouver qu'il existe un automorphisme de $\mathbb{K}$ qui envoie x_1 sur x_2.

(e) Le corps $\mathbb{K}$ peut-il être engendré par une racine cubique β d'un élément de $\mathbb{Q}$. Utiliser l'exercice précédent.

Exercice 2.16. Soit f un polynôme de degré n irréductible sur le corps k, et $\mathbb{K}$ une extension de degré d de k. Montrer que si $\text{pgcd}(d, n) = 1$, alors f est encore irréductible sur $\mathbb{K}$. Raisonner par l'absurde et considérer un corps de rupture d'un facteur premier q de f sur $\mathbb{K}$.

Exercice 2.17. Soit $\alpha = e^{i\pi/6}$, de sorte que $\alpha^{12} = 1$. Noter que le polynôme $X^{12} - 1$ est divisible par les polynômes $X^6 - 1$, $X^4 - 1$ et leur ppcm. Montrer que $[\mathbb{Q}[\alpha]\colon \mathbb{Q}] = 4$, et calculer le polynôme minimal de α.

Exercice 2.18. Montrer que le polynôme $f = X^p - T$ est irréductible dans le corps $\mathbb{F}_p(T)$ des fractions rationnelles à coefficient dans $\mathbb{F}_p$ (corps fini à p éléments). Soit $\mathbb{E}$ son corps de décomposition. Montrer que f n'admet qu'une seule racine dans E. Quels sont les $\mathbb{F}$-automorphismes de $\mathbb{E}$?

Exercice 2.19. Théorème de d'Alembert Gauss, méthode de d'Alembert.

Soit $P \in \mathbb{C}[X]$ un polynôme de degré $d \geqslant 1$.

Montrer que $\lim_{|z|\to\infty} |P(z)| = \infty$

Démontrer (utiliser la **compacité** des disques $D_R = \{|z| \leqslant R\}$) que la fonction $|P(z)|$ atteint son minimum en un point z_0.

On suppose que $P(z_0) \neq 0$. En écrivant la formule de Taylor au voisinage de z_0, montrer que suffisamment petit, il existe un entier n, et un nombre complexe non nul α tels que $\frac{P(z)}{P(z_0)} = 1 + \alpha\,(z - z_0)^n + o(z - z_0)^n$

En écrivant $\alpha = r\,e^{i\theta}$, construire un z tel que $\left|\frac{P(z)}{P(z_0)}\right| < 1$.

Conclure.

2.7.3. Corps finis.

Exercice 2.20.

1. Quels sont les polynômes irréductibles de degré inférieur à 4 sur $\mathbb{F}_2$.
2. Quelle est la factorisation sur $\mathbb{F}_4$ d'un polynôme irréductible de $\mathbb{F}_2[X]$ de degré 4.
3. Combien y a t il de polynômes irréductibles de degré 2 sur $\mathbb{F}_4$

Exercice 2.21. Pour $q = 4, 8, 9, 16$, donner une construction de $\mathbb{F}_q$ comme comme de rupture d'un polynôme irréductible. Déterminer l'ordre des éléments inversibles de $\mathbb{F}_q$, leur polynôme minimal sur p, ou p est la caractéristique.

Exercice 2.22. Soit p un nombre premier $\neq 2$. Montrer que 2 est un carré dans $\mathbb{F}_p$ si $p \equiv 1(8)$ (on pourra remarquer que si ω est une racine primitive 8-ième de l'unité, alors $\omega + \frac{1}{\omega}$ est une racine de 2.

Exercice 2.23. Si $\Phi(x) = x^p$ est l'automorphisme de Frobenius de $\mathbb{F}_q$, quel est le plus petit entier tel que $\Phi^d = \text{Id}$

Exercice 2.24. Soit p un nombre premier, et $q = p^d$ une puissance de p. Démontrer que le groupe des automorphismes de $\mathbb{F}_{q^n}$ qui induisent l'identité sur $\mathbb{F}_q$ est cyclique engendré par l'automorphisme de Frobenius $\Phi_q(x) = x^q$

Exercice 2.25.

1. Montrer que $X^2 + X + 1$ est irréductible dans $\mathbb{F}_5$ (indication : Le nombre 2 est il un carré dans $\mathbb{F}_5$.)
2. Soit P un polynôme irréductible de degré 2 de $\mathbb{F}_5[X]$, montrer que P est scindé sur $\mathbb{F}_{25}$.
3. Soit α une racine de P dans $\mathbb{F}_{25}$, montrer que tout élément de $\mathbb{F}_{25}$ s'écrit $a\alpha + b$, avec a, b dans $\mathbb{F}_5$.
4. Soit $P = X^5 - X + 1$, montrer que P ne s'annule pas dans $\mathbb{F}_{25}$. En déduire que P est irréductible sur $\mathbb{F}_5$

Exercice 2.26. A quelle condition un polynôme irréductible de degré 2 sur $\mathbb{F}_p$ est il encore irréductible sur $\mathbb{F}_{p^n}$

Problème 2.1. Formes quadratique sur un corps fini.

Soit $\mathbb{K}$ un corps de caractéristique $\neq 2$, et $\mathbb{E}$ un espace vectoriel de dimension finie n.

Question 1. Rappeler la définition de forme quadratique et de forme bilinéaire associée. Quand dit on qu'une forme quadratique est non dégénérée ? Quand dit on que deux formes quadratiques sont congruentes ?

Question 2. Soit q une forme quadratique sur $\mathbb{E}$.

1. Démontrer qu'il existe une base de $\mathbb{E}$, et des éléments non nuls a_1, $..a_r$ de $\mathbb{K}$ dans laquelle $q(x_1, .., x_n) = \Sigma_{i=1}^{r} a_i x_i^2$.
2. A quelle condition q est elle non dégénérée.

Question 3. On suppose que pour tout couple $(a; b)$ d'éléments non nuls de $\mathbb{K}$ l'équation $ax^2 + by^2 = 1$ admet une solution.

1. Démontrer que si $\dim(\mathbb{E}) = 2$ et q est non dégénérée, il existe un élément α de $\mathbb{K}$ et une base de $\mathbb{E}$ et dans laquelle $q(x, y) = x^2 + \alpha y^2$
2. Démontrer que si $\dim(\mathbb{E}) = n$ et q est non dégénérée, il existe une base de $\mathbb{E}$ dans laquelle $q(x_1, .., x_n) = \Sigma_{i=1}^{n-1} x_i^2 + \alpha x_n^2$

On suppose maintenant que $\mathbb{K} = \mathbb{F}_q$ est un corps **fini** (et q impair).

Question 4.

1. Démontrer qu'il y a exactement $\frac{q+1}{2}$ carrés différents dans $\mathbb{K}$. On pourra étudier l'homomorphisme $\mathbb{F}_q^* \to \mathbb{F}_q^*$ $\varphi(x) = x^2$.
2. En déduire que pour tout couple $(a; b)$ d'éléments non nuls de $\mathbb{K}$ l'équation $ax^2 + by^2 = 1$ admet une solution. Indication on pourra écrire cette équation $ax^2 = by^2 - 1$

Question 5. Soient α, β deux éléments non nuls de $\mathbb{F}_q$. Montrer les formes quadratiques $q(x) = \Sigma_{i=1}^{n-1} x_i^2 + \alpha x_n^2$ et $q'(x) = \Sigma_{i=1}^{n-1} x_i^2 + \alpha' x_n^2$ sont congruentes si et seulement si $\frac{\alpha}{\beta}$ est un carré dans $\mathbb{F}_q^*$.

2.7.4. Racines de l'unité.

Exercice 2.27. Soit $\mathbb{K}$ un corps de caractéristique $\neq 2$. Alors ω est une racine primitive 2^n-ième de l'unité si et seulement si $\omega^{2^{n-1}} = -1$

Exercice 2.28. Soit $\mathbb{K}$ un corps. montrer que les conditions suivantes sont équivalentes :

i. il y a exactement n racines n-ième de l'unité dans $\mathbb{K}$

ii. il y a (au moins) une racine primitive $n-$ ième de l'unité dans $\mathbb{K}$

iii. il y a exactement $\varphi(n)$ racines primitives $n-$ièmes de l'unité dans $\mathbb{K}$

2.7.5. Polynôme cyclotomiques.

Exercice 2.29. Démontrer que $\Phi_{p^k}(X) = \Phi_p(X^{p^{k-1}})$

Exercice 2.30. Exprimer, pour n impair Φ_{2n} en fonction de Φ_n.

Exercice 2.31. Soit $n = p_1^{\alpha_1}....p_k^{\alpha_k}$ la décomposition de n en produit de facteurs premiers distincts. On pose $n' = p_1....p_k$, et $n'' = \frac{n}{n'}$. Démontrer que $\Phi_n(x) = \Phi_{n'}(x^{n''})$.

On établira que les racines primitives n ième de l'unité sont les racines n''ièmes des racines n'ièmes de l'unité, et on en déduira que les deux membres sont des polynômes ayant les mêmes racines.

Exercice 2.32. Fonction de Möbius.

On note $\mu(n)$ la somme des racines primitives n-ièmes de l'unité.

1. Quel est le lien entre $\mu(n)$ et Φ_n.
2. Si p est un nombre premier, $\mu(p) = -1$
3. Si p est un nombre premier, $\mu(p^k) = 0$ (utiliser 2.29)
4. Démontrer que $\mu(1) = 1$ et $\Sigma_{d|n}\mu(d) = 0$ si $n > 1$ (on utilisera $X^n - 1 = \Pi_{d/n}\Phi_d(X)$
5. Si a et b sont premier entre eux $\mu(ab) = \mu(a)\mu(b)$.
6. Si n est divisible par le carré d'un nombre premier, alors $\mu(n) = 0$ (utiliser 3)
7. Si n est le produit d'un nombre pair de nombre premiers distincts, $\mu(n) = 1$
8. Si n est le produit d'un nombre impair de nombre premiers distincts, $\mu(n) = -1$

Exercice 2.33. * Pour chaque entier m on note $R_m[\mathbb{Q}] \subset \mathbb{C}$ le corps cyclotomique qui est le corps de décomposition de $X^m - 1$ sur $\mathbb{Q}$, engendré par une racine primitive n-ième de l'unité. Soient m et n deux entiers, et d (respectivement l) leur PGCD (resp. leur PPCM). Démontrer :

1. Si $m|n$ alors $R_m[\mathbb{Q}] \subset R_n[\mathbb{Q}]$.

2. Le groupe $\mathbb{U}_l$ des racines l-ièmes de l'unité coïncide avec le groupe $\mathbb{U}_m \times \mathbb{U}_n$ et le corps $R_m[\mathbb{Q}]R_n[\mathbb{Q}]$ coïncide avec $R_l[\mathbb{Q}]$

3. L'intersection $R_m[\mathbb{Q}] \cap R_n[\mathbb{Q}]$ coïncide avec $R_d[\mathbb{Q}]$(pour ce dernier point on pourra établir au préalable l'égalité : $\varphi(m)\,\varphi(n) = \varphi(d)\,\varphi - (l)$)

4. Expliquer pourquoi si m est impair on a : $R_{2m} = R_m$. Y a-t-il d'autres cas où on a l'égalité $R_n = R_m$ bien que $m \neq m$?

Chapitre 3

Digression : Fonctions symétriques des racines, résultant et discriminant.

Dans ce chapitre, on fixe un anneau factoriel $\mathbb{A}$, et on note $\mathbb{K}$ son corps des fractions.

3.1. Polynômes symétriques.

Un polynôme $P(x_1,..,x_n)$ de $\mathbb{A}[x_1,..x_n]$ est dit symétrique si, pour toute permutation $\pi \in S_n$, on a $P(x_1,..,x_n) = P(x_{\pi(1)},..,x_{\pi(n)})$.

Exemple 3.1. Les fonctions $\sigma_i(X_1,...,X_n)$ définie par
$\sigma_1(X_1,...X_n) = \Sigma_{1\leqslant i\leqslant n} X_i$
$\sigma_2(X_1,...X_n) = \Sigma_{1\leqslant i_1<i_2\leqslant n} X_{i_1}X_{i_2}$
$\sigma_k(X_1,...X_n) = \Sigma_{1\leqslant i_1<i_2<\cdots<i_k\leqslant n} X_{i_1}X_{i_2}...X_{i_k}$
$\sigma_n(X_1,...X_n) = X_1...X_n$
sont des fonctions symétriques, appelées « polynômes symétriques élémentaires ».

Remarque 3.1. Remarquons qu'il y a $\binom{n}{k}$ termes dans a_k, comme on peut le démontrer en spécialisant $x_1 = \cdots = x_n = 1$

On remarque que le polynôme σ_i dépend non seulement de l'indice i mais aussi de l'indice n. Rigoureusement on devrait écrire un truc du style $\sigma_{i,n}$ mais on oublie toujours cet indice. Ainsi, si $i \geqslant 2$, on voit que

Proposition 3.1. *$\sigma_i(X_1,...,X_{n+1}) = \Sigma_{j=1}^{n+1} \sigma_i(X_1,.,X_{j-1},X_{j+1},...X_{n+1})$, ce qui nous sera fort utile par la suite.*

Les relations coefficients-racines d'un polynôme scindé s'obtiennent grâce aux formules de Viète.

Proposition 3.2. *Dans $\mathbb{K}[T,X_1,...X_n]$ on a*
$\Pi_{i=1}^n (T - X_i) = T^n - \sigma_1 T^{n-1} + \cdots + (-)^k \sigma_k T^{n-k} + \cdots + (-1)^n \sigma_n$ □

Corollaire 3.1. *Soit $f \in A[X]$ un polynôme de degré n scindé dont les racines sont $x_1,..x_n$ alors ses coefficients sont les valeurs des polynômes σ_i calculées en ses racines : $\frac{a_i}{a_0} = (-)^i \sigma_i(x_1,..x_n)$.*

Proposition 3.3. *Soit $f \in \mathbb{K}[Y_1,...Y_n]$. On pose $\sigma(f) \in \mathbb{K}[X_1,...X_n]$ le polynôme définit par $\sigma(f)(X_1,...X_n) = f(\sigma_1(X),...\sigma_n(X))$. L'application σ est un homomorphisme **injectif** d'anneau.*

Démonstration. La seule chose à vérifier est l'injectivité. Si $\mathbb{K}$ n'est pas algébriquement clos, on le remplace par une clôture algébrique ce qui renforce le résultat (la restriction d'une application injective est toujours injective). L'application de $\mathbb{K}^n$ dans lui même définie par $S(x_1,...x_n) = (\sigma_1(x),...\sigma_n(x))$ est surjective puisque $\mathbb{K}$ est algébriquement clos. Donc si $\sigma(f)$ est nul , alors f s'annule sur $\mathbb{K}^n$ donc est nul. □

Le théorème fondamentale de Newton est

Théorème 3.1. *Soit $f \in A[X_1,..X_n]$ un polynôme symétrique en les X_i. Il existe un unique polynôme $g \in \mathbb{A}[y_1,..y_n]$ tel que $f = \sigma(g) = g(\sigma_1,..,\sigma_n)$.*

Compte tenu de la proposition précédente, il s'agit d'établir l'existence.

Démonstration. Soit f un polynôme. Alors f s'écrit d'une unique façon $f = \Sigma_{i=1}^{n} f_i$ ou f est homogène de degré i. Si de plus f est symétrique, alors les f_i le sont aussi à cause justement de l'unicité .

Notons que pour un polynôme homogène de degré p, son degré q par rapport à l'une quelconque des indéterminées ne dépend pas de cette indéterminée.

Pour ne pas tout mélanger, on appelle **poids** d'un polynôme homogène son degré total, et **ordre** son degré partiel. Par exemple $X_1^3X_2^7 + X_1^7X_2^3$ est de poids 10 et d'ordre 7.

Si un polynôme est homogène et si $\lambda\sigma_1^{\alpha_1}...\sigma_n^{\alpha_n}$ est l'un de ses monômes son poids est, $p = \Sigma i\alpha_i$, puis σ_i est homogène de degré i.

Le démonstration du théorème se fait par récurrence sur la somme $p+n$ du poids total et du nombre de variable. Le cas d'une variable étant clair puisque tout polynôme est alors symétrique.

Soit f un polynôme homogène de poids p en n variables, et posons $f_1(X_1, ...X_{n-1}) = f(X_1, ...X_{n-1}, 0)$. Si f_1 est nul, alors f est divisible par X_1, donc par $X_1...X_n = \sigma_n$ et on utilise la récurrence appliquée à $f_1 = f / \sigma_n$, qui est de poids $p - n$, pour conclure. Sinon, f_1 est symétrique en $n-1$ variables et de même poids que f. Il existe donc un polynôme Γ tel que $f_1(X_1, ...X_{n-1}) = \gamma(\sigma'_1, ...\sigma'_{n-1})$ ou les σ'_i sont les fonctions symétriques élémentaires des $n-1$ premières variables. On pose alors $g(X_1, ...X_n) = \gamma(\sigma_1, ...\sigma_n)$. Alors $f - g$ est un polynôme en n variables symétrique et de même poids que f. Maintenant, par construction $(f-g)(X_1, ...X_{n-1}, 0) = 0$. On applique alors le premier argument à $f - g$ pour conclure. □

Remarque 3.2. La démonstration est algorithmique.

3.2. RÉSULTANT.

Le problème que nous allons étudier est connu sous le nom de problème de l'*élimination* : étant donné deux polynômes $P(X) = a_nX^n + a_1X^{n-1} + \cdots + a_0$; $Q(X) = b_mX^m + \cdots + b_0$, trouver une condition nécessaire et suffisante pour que les deux équations $P = 0$, $Q = 0$ aient une solution commune dans une clôture algébrique $\mathbb{K}$ du corps des fractions de A. Nous supposerons que a_n et b_m sont non nuls.

Remarque 3.3. S C'est le cas si et seulement si il existe un ac tel que es deux polynômes soient divisible par $(X - \alpha)$, ou si ils ont un pgcd de degré au moins 1.

Pour résoudre ce problème nous allons étudier le déterminant de Sylvester.

LEMME 3.1. *Les polynômes P et Q ont une racine commune dans une extension du corps des fractions de A si et seulement si il existe deux polynômes non nuls U, V dans $A[X]$ tels que* $\deg(U) < \deg(Q)$, $\deg(V) < \deg(P)$ *et* $UP + VQ = 0$

Démonstration. Sens direct : comme $A[X]$ est factoriel, on écrit $P = P_1D, Q = Q_1D$ de sorte que $Q_1P - P_1Q = 0$

Sens réciproque : on décompose P, Q, U, V en produit d'irréductibles. Pour des questions de degré l'un des facteurs de P est aussi un facteur de Q □

Sous cette hypothèse, le noyau de l'application linéaire $\mathbb{K}_{m-1}[X] \times \mathbb{K}_{n-1}[X] \to \mathbb{K}_{n+m-1}[X]$ $(U, V) \to UQ + VP$ n'est pas injective.

On peut choisir comme base du premier espace les polynômes $(X^{m-1}, 0), (X^{m-2}, 0), .., (1, 0)$, $(0, X^{n-1})$, $(0, X^{n-2})$, ..(0, 1) et comme base du second la base X^{n+m-1}, X^{n+m-2}, ..1 Son déterminant s'appelle le déterminant de Sylvester de P et Q Pour l'instant on le note $S(P, Q)$; Nous donnerons une autres formule un peu plus tard, et il s'appellera alors le résultant de P et Q.

LEMME 3.2. $S(P,Q) =$

$$\begin{vmatrix}
a_n & 0 & & & b_m & & & 0 \\
a_{n-1} & a_n & 0 & & b_{m-1} & b_m & & 0 \\
 & a_{n-1} & & & b_{m-2} & b_{m-1} & b_m & \\
 & & & & & & b_{m-1} & \\
a_0 & a_1 & & a_n & & & & 0 \\
 & a_0 & & a_{n-1} & b_1 & & & \\
0 & 0 & & a_{n-2} & b_0 & b_1 & & \\
 & & & & & b_0 & & \\
 & & & & & & & \\
 & & & a_0 & & & & b_0
\end{vmatrix}$$

On voit que $S(P,Q)$ peut parfaitement être défini comme étant la valeur en $(a_0,..a_n,b_0,..b_m)$ d'un polynôme de $\mathbb{Z}[a_0,a_1,..a_n,b_0,..b_m]$ qui s'appelle le **résultant universel.** Il est de degré m en chacune des variables a_i et n en chacune des variables b_j.

Définition 3.1. *Le résultant universel est le polynôme de $\mathbb{Z}[a_0,\ a_1,\ ..a_n,\ b_0,\ ..b_m]$ défini par le déterminant ci-dessus. Pour tout anneau A et tout couple de polynôme à coefficient dans A, le déterminant de Sylvester $S(P,Q)$ s'obtient en évaluant R sur les coefficients de P et Q.*

Après avoir définit le résultant de cette manière, on définit le polynôme $R\in\mathbb{Z}[a_0,a_1,..a_n,b_0,..b_m]$ grâce au théorème sur les fonctions symétriques élémentaires des racines.

On identifie $\mathbb{Z}[a_0,\ a_1,\ ..a_n,\ b_0,\ ..b_m]$ au sous anneau de $\mathbb{Z}[a_0,\ x_1,\ ..x_n,\ b_0,\ y_1..y_m]$ formé par les polynômes symétriques en les racines grâce au formule de Viète $a_k=a_0.\Sigma_{i_1<i_2<\cdots<i_k}x_{i_1}..x_{i_k}$ et grâce au théorème de Newton.

On pose alors $R(P,Q)=b_m^n\Pi P(y_i)=a_n^m\Pi Q(x_i)=(-)^{n+m}a_n^mb_m^n\Pi(x_i-y_j)$.

On sait déjà que $R\in\mathbb{Z}[a_0,a_1,..a_n,b_0,..b_m]$.

Théorème 3.2. $R(P,Q)=\pm S(P,Q)$

Etape 1. On se ramène tout d'abord au cas ou $a_n=b_m=1$: en effet $S(P,Q)=a_n^mb_m^nS\Big(\frac{P}{a_m},\frac{Q}{b_m}\Big)$ d'une part, et la même propriété est satisfaite pour $R(P,\ Q)$. On pose alors $S_1(a_0,\ ..a_{n-1},\ b_0,\ ..b_{m-1})=S(a_0,..a_{n-1},1,b_0,..b_{m-1},1)$.

Etape 2. On fait un raisonnement abstrait en considérant $\mathbb{Z}[a_0,a_1,..,a_{n-1},b_0,..b_{m-1}]$ comme sous anneau de $\mathbb{Z}[x_1,..x_n,y_1,..y_m]$, qui est un anneau factoriel.

On peut décomposer S_1 dans $\mathbb{Z}[x_1,..x_n,y_1,..y_m]$ comme produit d'irréductibles.

Notons que dans cet anneau factoriel, les éléments x_i-y_j sont irréductibles et non équivalents : en effet, si on écrit $\mathbb{Z}[x_1,..x_n,y_1,.;y_{j-1},y_{j+1},..y_m][y_j]$ ce polynôme est de degré 1 en y_j.

Par ailleurs que polynôme de $\mathbb{Z}[x_1,\ ..x_n,\ y_1,\ ..y_m]$, le polynôme S_1 s'annule pour $y_j=x_i$ il est donc divisible par x_i-y_j.

Comme cet anneau est factoriel, le polynôme T est divisible par $\Pi_{i,j}(x_i-y_j)$.

Ainsi, il existe un polynôme U de $\mathbb{Z}[a_0,a_1,..a_n,b_0,..b_m]$ tel que $S(P,Q)=a_n^mb_m^n\Pi_{i,j}(x_i-y_j).U$

Pour vérifier que $U=\pm1$, notons d'abord que pour chaque variable a_i, le polynôme S est un polynôme de degré $\leqslant m$ (regarder le déterminant) et $a_n^mb_m^n\Pi(x_i-y_j)$ de degré m, donc U est de degré 0 en chaque variable a_i et b_j, de sorte que U est un entier. En réduisant modulo p, on voit que $U=\pm1$, sinon il existe un nombre premier pour lequel la réduction modulo p du membre de droite serait nul, or, en tout degré, il existe deux polynômes de $\overline{\mathbb{F}_p}$ qui n'ont pas de racines communes car $\overline{\mathbb{F}_p}$ est infini. Pour savoir si c'est $+1$ ou -1, on peut se creuser la tête longtemps, mais cela n'a a vrai dire aucune importance.

3.3. Discriminant.

Nous reviendrons sur cette notion importante plus tard dans le cours, mais nous pouvons définir le discriminant « universel », comme nous avions défini le résultant universel. On veut regarder si un polynôme a ou pas une racine double dans une extension du corps.

On considère toujours $\mathbb{Z}[a_0,a_1,..a_n,b_0,..b_m]$ comme sous anneau de $\mathbb{Z}[a_0,x_1,..x_n,b_0,y_1..y_m]$

Proposition 3.4. *Soit $P(x)=a_n\Pi_{i=1}^n(X-x_i)\in\mathbb{Z}[a_0,\ a_1,\ ..a_n,\ b_0,\ ..b_m]\subset\mathbb{Z}[a_0,\ x_1,\ ..x_n,\ b_0,\ y_1..y_m]$. Alors $R(P,P')=a_n^{2n-1}\Pi_{i\neq j}(x_i-x_j)$*

Démonstration. Comme $P(x)=a_n\Pi(x-x_j)$, $P'(x)=\Sigma_ja_n\Pi_{j\neq i}(x_i-x_j)$, $P'(x_j)=a_n\Pi_{j\neq i}(x_i-x_j)$ et donc $R(P,P')=\Pi P'(x_i)=a_n^{2n-1}\Pi_{i\neq j}(x_i-x_j)$ □

Lemme 3.3. *Dans $\mathbb{Z}[a_0,..a_n]$, $R(P,P')$ est divisible par a_n.*

Démonstration. Considérer la première ligne du déterminant de Sylvester. □

DÉFINITION 3.2. *Le discriminant universel et le polynôme de* $\mathbb{Z}[a_0,..a_n]$ *défini par* $\Delta(P)=\frac{1}{a_n}R(P,P')=a_n^{2n-2}\Pi_{i\neq j}(x_i-x_j)$

Remarque 3.4. L'intérêt d'avoir divisé par a_n est que maintenant son exposant est pair, et que l'on peut écrire $D=(a_n^{n-1}\Pi_{i<j}(x_i-x_j))^2$. Evidemment le polynôme $\Pi_{i<j}(x_i-x_j)$ n'est pas symétrique, mais il est invariant par le groupe alterné. Nus reviendrons plus tard sur la question de savoir si D est ou pas un carré ou pas.

Pour tout corps $\mathbb{K}$ et tout polynôme de $\mathbb{K}[X]$, on peut calculer $\Delta(P)$ et on a

PROPOSITION 3.5. *Soit* $P\in\mathbb{K}[X]$ *un polynôme. Alors* P *a une racine double dans une extension de* $\mathbb{K}$ *si et seulement si* $\Delta(P)=0$.

Exemple. Les polynômes de degré 2. $P(X)=c+bX+aX^2, P'(X)=b+2aX$
$\Delta(P)=a^2P\Big(\frac{-b}{2a}\Big)=4a^2\Big(c-\frac{b^2}{2a}+a.\frac{b^2}{4a^2}\Big)=4a\Big(c-\frac{b^2}{4a}\Big)=(4ac-b^2)$
Si, grâce au théorème de Newton, on considère $\mathbb{Z}[a_0,..a_n]$ comme sous anneau de $\mathbb{Z}[x_1,..x_n,a_n]$ grâce aux formules de Viète, on obtient $\Delta(P)=a_n^{n-1}\Pi_{i=1}^nP'(x_i)$.

PROPOSITION 3.6. $R(P,P')=a_n^{2n-1}\Pi_{i\neq j}(x_i-x_j)=a_n^{n-1}\Pi_{i=1}^nP'(x_i)$

Démonstration. Comme $P(x)=a_n\Pi(x-x_j), P'(x)=\Sigma_j a_n\Pi_{j\neq i}(x_i-x_j)$, $P'(x_j)=a_n\Pi_{j\neq i}(x_i-x_j)$ et donc $\Delta(P)=R(P,P')=\Pi P'(x_i)=a_n^{2n-1}\Pi_{i\neq j}(x_i-x_j)$ □

3.4. EXERCICES.

Exercice 3.1. Formules de Newton.

On rappelle que $\sigma_k=\Sigma_{i_1<\cdots<i_k}X_{i_1}..X_{i_k}$ est la k ième fonction symétrique élémentaires des racines du polynôme $F(X)=\Pi_{i=1}^n(X-x_i)$, et on se propose d'évaluer $s_k=\Sigma_{i=1}^n x_i^k$.

1. Démontrer que $\frac{F'}{F}=\frac{n}{X}+\Sigma_{i=1}^{\infty}s_i\,X^{-(i+1)}$
2. En écrivant que
   $nX^{n-1}-(n-1)\sigma_1X^{n-1}+\cdots++(-1)^{n-1}\sigma_{n-1}=F'$, et en utilisant $F'=\frac{F'}{F}\times F$, en déduire que :
   si $j\leqslant n$, on a $s_j-s_{j-1}\sigma_1+s_{j-2}\sigma_{j-2}+\cdots+..(-)^{j-1}s_1\,\sigma_{j-1}+(-1)^j\,j\sigma_j=0$
   si $j>n+1$ $s_j-s_{j-1}\sigma_1+s_{j-2}\sigma_{j-2}+\cdots+..(-)^{j-1}s_1\,s_{j-1}+(-1)^j\,s_j=0$

On considère le polynôme $E_n(x)=x^n+\frac{x^{n-1}}{1!}+\frac{x^{n-2}}{2!}+\cdots+\frac{x}{(n-1)!}+\frac{1}{n!}$
Calculer les sommes s_i, pour $1\leqslant i\leqslant n$.

Exercice 3.2. Formules de Cardan.

On considère le polynôme $P(X)=X^3+pX+q$ dont on cherche les racines. On suppose $o\neq 0$

1. On cherche $x=u+v$ avec $3uv+p=0$, démontrer que l'équation $P(x)=0$ équivaut à une équation du second degré en u^3. En déduire les formules des racines de P.

2. On suppose $p,q\in\mathbb{R}$, de sorte que P a au moins une racine réelle. On rappelle que le discriminant de P est $((x_1-x_2)(x_1-x_3)(x_2-x_3))^2$. Montrer sans le calculer que $\Delta<0$ si et seulement il y a deux racines non réelle.

3. Calculer P' . Quel est le résultant de P?

3. On ne suppose plus que $\mathbb{K}=\mathbb{R}$, mais que Δ est un carré dans $\mathbb{K}$ démontrer que le corps de rupture de P est un corps de décomposition.

Exercice 3.3. Eliminer x entre $x^3-\lambda x^2-q=0$ et $x^3-\lambda x-3=0$

Exercice 3.4.

Un polynôme est dit réciproque si 1 et -1 ne sont pas une racine et si x est racine alors $\frac{1}{x}$ aussi. Montrer que P est réciproque si et seulement si il est de degré pair $2n$ et $a_k=a_{2n-k}$.

Soit P un polynôme réciproque de degré $2n$, démontrer qu'il existe un polynôme de degré n tel que $x^nQ\Big(x+\frac{1}{x}\Big)=P$.

Trouver l'équation dont les racines sont les 6 rapports des racines de $x^3+px+q=0$

Exercice 3.5. Soient $h(x)=\frac{a\,x+b}{c\,x+d}$ une homographie (ops $a\,d-b\,c=1$). Et $P(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$. Trouver le polynôme de même degré dont les racines sont les images des racines de P par h. On pourra écrire $z=h(x)$ sous forme d'un polynôme du premier degré en x, et éliminer x dans le système obtenu.

Chapitre 4

Théorie de Galois

Dans ce chapitre, nous allons étudier plus systématiquement le groupe de Galois d'une extension $[\mathbb{L}:\mathbb{K}]$. Par définition, ce groupe est le groupe des automorphismes de $\mathbb{L}$ qui fixent $\mathbb{K}$. Nous le noterons $\mathrm{Gal}(\mathbb{L}:\mathbb{K})$.

Nous avons déjà vu plusieurs résultats importants.

1. Le groupe de Galois $\mathrm{Gal}(\mathbb{R}_n(\mathbb{Q}):\mathbb{Q}) \sim (\mathbb{Z}/n\mathbb{Z})^*$, dont le cardinal est $\varphi(n)$.

Rappelons l'argument. Le corps $\mathbb{R}_n(\mathbb{Q})$ est le corps de rupture du $n-i$ème polynôme cyclotomique Φ_n qui est irréductible (et c'est aussi son corps de décomposition, car si un corps contient une racine primitive n-ième de l'unité, il les contient toutes). Comme les racines sont en bijection avec les éléments de $(\mathbb{Z}/n\mathbb{Z})^*$, le groupe de Galois opère dessus de façon simplement transitive. Autrement dit si ω, ω' sont deux racines primitives n-ièmes de l'unité, il existe un unique élément g de ce groupe tel que $g(\omega) = \omega'$.

2. Le groupe $\mathrm{Gal}(\mathbb{F}_{p^n}:\mathbb{F}_p)$ est le groupe cyclique d'ordre n engendré par l'automorphisme de Frobenius.

3. Si $P \in \mathbb{K}[X]$ est un polynôme, alors le groupe de Galois du corps de décomposition $\mathbb{L}$ de P est un sous groupe du groupe des permutations des racines de P, plus précisément nous avons vu

Théorème 4.1. *Soit P un polynôme de $\mathbb{K}[X]$, $\mathbb{L}$ un corps de décomposition et R l'ensemble des racines de P dans L. Alors le groupe de Galois $\mathrm{Gal}(\mathbb{L}:\mathbb{K})$ opère fidèlement sur R (autrement dit l'homomorphisme naturel vers le groupe de permutation des racines est injectif). Si de plus P est irréductible cette opération est transitive.*

4.1. Extensions séparables, normales, galoisiennes.

4.1.1. Dérivation.

Soit $\mathbb{K}$ un corps. On rappelle que, si $P(X) = a_0 + a_1X + \cdots + a_nX^n$, son polynôme dérivé est $P'(X) = a_1 + 2a_2X^2 + \cdots + na_nX^{n-1}$

Remarque 4.1. Si $\mathrm{car}(K) \neq 0$, il peut y avoir des trucs bizarres, car il se peut très bien que $P' = 0$ alors que P est compliqué : il suffit pour cela que les seuls coefficients non nuls de P soit les a_i pour $i \equiv 0(p)$.

On peut néanmoins se demander si P a des racines multiples dans « son » corps de décomposition.

THÉORÈME 4.2. *Soit P un polynôme de $\mathbb{K}[X]$. Alors les racines de P dans son corps de décomposition sont simples si et seulement si le pgcd de P et P' est 1.*

Démonstration. Soit $\mathbb{L}$ le corps de décomposition de P. Si dans $\mathbb{L}$, $P=(X-a)^2Q$, alors $P'=(X-a)(2Q+(X-a)Q')$; et $\text{pgcd}(Q,Q')$ est divisible par $(X-a)$ donc est de degré $\geqslant 1$.

Réciproquement, si toutes les racines de P sont simples, alors $P=a_n\Pi(X-a_{i_i})$ est dans L la décomposition de p en facteur irréductibles. Alors $P'(X)=a_n\Sigma_i\Pi_{i\neq j}(X-\alpha_i)$, et

$P'(\alpha_i)=a_n\Pi_{i\neq j}(\alpha_i-\alpha_j)\neq 0$. Donc aucun diviseur irréductible (=premier) de P ne divise P'. □

PROPOSITION 4.1. *On suppose $\mathbb{K}$ de caractéristique nulle. Si P est irréductible alors $(P,P')=1$, et donc ses racines sont simples. Mais en caractéristique $\neq 0$ il se peut que $P'=0$ et ce résultat n'est plus vrai.*□

PROPOSITION 4.2. *On suppose $\mathbb{K}$ de caractéristique $p\neq 0$. Soit P un polynôme. Son polynôme dérivé P' est nul, si et seulement si il existe Q tel que $P(X)=Q(X^p)$.*

Démonstration. Un polynôme est nul si et seulement si tous ses coefficients le sont. Si $P'=0$, alors pour $1\leqslant i\leqslant \deg(P)$, $ia_i=0$. Donc si $i\neq 0(p)$, $a_i=0$, et les seuls coefficients non nuls de P sont les a_{kp}. Dans ce cas, $P(X)=\Sigma_{k=0}^{\deg(P)/p}a_{kp}X^{kp}$. Si on pose $Q(X)=\Sigma_{k=0}^{\deg(P)/p}a_{kp}X^k$, on a le résultat. □

4.1.2. Séparabilité.

Soit $\mathbb{K}$ un corps.

DÉFINITION 4.1. *Un polynôme irréductible à coefficients dans $\mathbb{K}$ est dit séparable si dans toute extension de $\mathbb{K}$ il n'a que des racines simples. Un polynôme est dit séparable si ses facteurs irréductibles le sont.*

PROPOSITION 4.3. *Si $\text{car}(\mathbb{K})=0$ tout polynôme irréductible n'a que des racines simples est séparable.*

Démonstration. Soit P un polynôme irréductible de degré $n\geqslant 1$. Comme $\text{car}(\mathbb{K})=0$ le polynôme P' est non nul et de degré $n-1$. Les polynômes P et P' sont premiers entre eux car P est irréductible et $P'\neq 0$. D'après notre ami Bézout, il existe deux polynômes Y,V tels que $UP+VP'=1$. Donc P n'a pas de racine double. □

LEMME 4.1. *Soit $\text{car}(\mathbb{K})=p\neq 0$, et $a\in\mathbb{K}$. Soit il existe b tel que $a=b^p$, et $X^p-a=(X-b)^p$, soit le polynôme X^p-a est irréductible.*

Démonstration. Supposons X^p-a réductible et écrivons $X^p-a=F(X)G(X)$. Soit $\mathbb{L}$ un corps de décomposition de $F(X)$ et b une racine de $F(X)$ dans ce corps. Alors $b^p=a$, et dans $\mathbb{L}$, on a $X^p-a=(X-b)^p=F(X)G(X)$, de sorte que $F(X)=(X-b)^k$ avec $k<p$. Donc $b^k\in\mathbb{K}$ car c'est le terme constant de F. Comme $b^p=a$ aussi, et comme p est premier, le théorème de Bézout $(up+vk=1)$ montre que $b=(b^p)^u\times(b^k)^v\in\mathbb{K}$ et en fait $P(X)=(X-b)^p$. □

THÉORÈME 4.3. *Soit $\mathbb{K}$ un corps de caractéristique $p\neq 0$. Si pour tout élément a de $\mathbb{K}$, il existe b tel que $a=b^p$, alors tout polynôme irréductible est séparable.*

Démonstration. On raisonne par l'absurde et on considère F un polynôme irréductible F qui n'est pas séparable. Donc F admet une racine multiple dans une certaine extension. Comme F est irréductible, alors $F'=0$, ce qui veut dire que

$$F(X)=a_0+a_pX^p+\cdots+a_{np}X^{np}$$

Comme les a_i sont des puissances $p-$ièmes, on peut écrire $a_i=b_i^p$ et

$F(X) = b_0^p + (b_1X)^p \ldots \dot{+} (b_nX^n)^p = (b_0 + b_1X + \cdots + b_nX^n)^p$
On a une contradiction car F est irréductible. Donc l'un des a_i n'est pas une puissance $p-i$ème, contradiction.

□

Corollaire 4.1. *Si $\mathbb{K}$ est fini, tout polynôme irréductible de $\mathbb{K}[X]$ est séparable.*

Démonstration. En effet l'automorphisme de Frobenius $\Phi\colon \mathbb{K}^* \to \mathbb{K}^*$ donné par $\Phi(x) = x^p$ est injectif (car p ne divise pas $q-1 = p^n - 1$), donc surjectif, vu que que $\mathbb{K}^*$ est fini. □

Remarque 4.2. Ainsi, si l'on se restreint aux corps finis ou aux corps de caractéristique nulle, tout polynôme irréductible est séparable : on dit que ces corps sont **parfaits**. En première lecture, nous pourrons continuer la théorie dans ce cadre.

Remarque 4.3. Il est facile de se convaincre que $\mathbb{F}_p(t)$ n'est pas parfait, car l'équation $t = X^p$ n'a pas de solution dans ce corps. Pourquoi ?

Définition 4.2. *Une extension $\mathbb{L}\colon\mathbb{K}$ finie est dite séparable si le polynôme minimal de tout élément de $\mathbb{L}$ est séparable.*

Exemple 4.1. Si $\mathrm{car}(\mathbb{K}) = 0$ ou si $\mathbb{K}$ est fini, toute extension finie est séparable.

Nous allons voir qu'en fait les extensions séparables sont engendrées par un seul élément.

Théorème 4.4. *Théorème de l'élément primitif. Si l'extension $\mathbb{L}\colon\mathbb{K}$ est séparable, il existe un élément α tel que $\mathbb{L} = \mathbb{K}[\alpha]$.*

Nous démontrons ce résultat si le corps $\mathbb{K}$ est infini. De fait, si $\mathbb{K}$ est fini, $\mathbb{L}^*$ étant cyclique il existe une racine primitive n-ième de l'unité qui fait le job.

Lemme 4.2. *Etant donné deux éléments α_1, β_1 de $\mathbb{L}$ il existe un γ tel que $\mathbb{K}[\alpha_1, \beta_1] = \mathbb{K}[\gamma]$.*

Démonstration. Soient P, Q les polynômes minimaux de α_1, β_1 et soit $\mathbb{M}$ le corps de décomposition du polynôme PQ.

Dans $\mathbb{M}$, on a $P(X) = (X-\alpha_1)\Pi_{i=2}^{d}(X-\alpha_i)$, $Q(X) = (X-\beta_1)\Pi_{i=2}^{e}(X-\beta_j)$
où, par définition tous les α_i, et tous les β_i sont distincts.

On choisi un élément $t \in \mathbb{K}$ tel que pour tout couple (i, j) $t \neq \frac{\alpha_1 - \alpha_i}{\beta_1 - \beta_j}$ ce qui est possible vu que $\mathbb{K}$ est infini.

Pour pose alors $\gamma = \alpha_1 + t\beta_1$, et $\mathbb{K}' = \mathbb{K}[\gamma] \subset \mathbb{M}$. Nous allons vérifier que γ fait le travail.

Soit $F(X) = P(\gamma - tX) \in \mathbb{K}'[X]$.

Calculons les racines de F. Si x est une racine alors il existe i tel que $\gamma - tx = \alpha_i$. Ainsi les racines de F sont les $x_i = \frac{\gamma - \alpha_i}{t} = \frac{\alpha_1 - \alpha_i}{t} + \beta_1$.

Par construction, F et Q ont exactement une racine commune qui est β_1, de sorte que
$\mathrm{PGCD}(F, Q) = (X - \beta_1)$

Il en résulte que $\beta_1 \in \mathbb{K}'$, car $F \in \mathbb{K}'[X]$, $Q \in \mathbb{K}[X] \subset \mathbb{K}'[X]$ et le calcul de ce PGCD se fait dans le corps $\mathbb{K}'$. Alors α_1 aussi est dans $\mathbb{K}'$ vu que $\alpha_1 = \gamma - t\beta_1$.

Ainsi $\mathbb{K}[\alpha_1, \beta_1] = \mathbb{K}' = \mathbb{K}[\gamma]$.

□

La fin de la démonstration est une récurrence routinière. On choisi des éléments $\alpha_1, ...\alpha_n$ qui engendrent $\mathbb{L}:\mathbb{K}$. Par hypothèse de récurrence, il existe un γ_{n-1} tel que $\mathbb{K}[\alpha_1, ..., \alpha_{n-1}] = \mathbb{K}[\gamma_{n-1}]$. On applique alors le lemme à (γ_{n-1}, α_n) pour obtenir le résultat.

4.1.3. Normalité.

Il s'agit là d'un concept tout à fait important.

DÉFINITION 4.3. *L'extension $\mathbb{L}$ de $\mathbb{K}$ est dite normale si tout polynôme irréductible de $\mathbb{K}[X]$ qui a une racine dans $\mathbb{K}$ est scindé dans $\mathbb{L}$.*

Exemple 4.2. L'extension $\mathbb{Q}[\sqrt[3]{2}]$ n'est pas normale. En fait par définition $X^3 - 2$ qui est irréductible sur $\mathbb{Q}$ n'a qu'une seule racine dans $\mathbb{R}$ et $\mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{R}$. Les autres racines sont ailleurs.

THÉORÈME 4.5. *Une extension finie $\mathbb{L}:\mathbb{K}$ est normale si et seulement si $\mathbb{L}$ est un corps de décomposition d'un polynôme de $\mathbb{K}[X]$.*

Démonstration. Il y a un sens « facile ».

Normale $\Rightarrow$ Corps de décomposition.

Si l'extension $\mathbb{L}:\mathbb{K}$ est finie, elle est engendrée par un nombre fini d'éléments $\alpha_1, ..., \alpha_n$ tous algébriques sur $\mathbb{K}$. Soit P_i le polynôme minimal de α_i. Le produit des P_i est un polynôme de $\mathbb{K}$, scindé dans $\mathbb{L}$ par hypothèse, et dont les racines engendrent $\mathbb{L}$. Donc $\mathbb{L}$ est bien un corps de décomposition de P.

La réciproque est plus compliquée.

Si $\mathbb{L}$ est le corps de décomposition d'un polynôme P. Alors $\mathbb{L}:\mathbb{K}$ est finie vu qu'elle est engendrée par les racines de P, qui sont tous algébriques.

On considère un polynôme irréductible $Q \in \mathbb{K}[X]$ qui a un 0 dans $\mathbb{L}$. Il s'agit de démontrer qu'il est scindé.

On note $\mathbb{M} \supset \mathbb{L}$ un corps de décomposition de PQ, de sorte que ce polynôme (et donc Q) y est scindé, et soient α_1, α_2 deux racines de Q dans M.

Nous allons voir que les degré $[\mathbb{L}(\alpha_1):\mathbb{L}]$ et $[\mathbb{L}(\alpha_2):\mathbb{L}]$ sont égaux.

regardons les deux tours de corps
$\mathbb{K} \subset \mathbb{K}(\alpha_1) \subset \mathbb{L}(\alpha_1) \subset \mathbb{M}$
$\mathbb{K} \subset \mathbb{K}(\alpha_2) \subset \mathbb{L}(\alpha_2) \subset \mathbb{M}$

$[\mathbb{L}(\alpha_i):\mathbb{L}].[\mathbb{L}:\mathbb{K}] = [\mathbb{L}(\alpha_i):\mathbb{K}] = [\mathbb{L}(\alpha_i):\mathbb{K}(\alpha_i)][\mathbb{K}(\alpha_i):\mathbb{K}]$

$[\mathbb{K}(\alpha_1):\mathbb{K}] = [\mathbb{K}(\alpha_2):\mathbb{K}]$ est le degré du polynôme Q, donc ne dépend pas de i. Mais $\mathbb{L}(\alpha_i)$ est le corps de décomposition de P sur $\mathbb{K}(\alpha_i)$ et comme $\mathbb{K}(\alpha_1)$ est isomorphe à $\mathbb{K}(\alpha_2)$, la dimension $[\mathbb{L}(\alpha_i):\mathbb{K}(\alpha_i)]$ ne dépend pas de i. Donc $[\mathbb{L}(\alpha_i):\mathbb{L}]$ ne dépend pas de i comme promis.

Mais $\alpha_1 \in \mathbb{L}$ équivaut à $[\mathbb{L}(\alpha_1):\mathbb{L}] = 1$ donc à $\alpha_2 \in \mathbb{L}$.

□

Il et intéressant de reformuler la normalité en oubliant les polynômes.

Théorème 4.6. *L'extension $\mathbb{L}:\mathbb{K}$ est normale si et seulement si pour toute extension $\mathbb{M}:\mathbb{L}$ et tout homomorphisme $\sigma:\mathbb{L}\to\mathbb{M}$ induisant l'identité sur $\mathbb{K}$, $\sigma(\mathbb{L})=\mathbb{L}$.*

Démonstration. Supposons $\mathbb{L}:\mathbb{K}$ normale. Soit $\omega\in\mathbb{L}$, et P son polynôme minimal. Alors P est scindé dans $\mathbb{L}$, c'est à dire que toute ses racines sont dans $\mathbb{L}$. Bien évidemment comme σ induit l'identité sur $\mathbb{K}$, il permute les racines de P, et donc $\sigma(w)$ est une racine de P dans $\mathbb{L}$.Donc $\sigma(\mathbb{L})\subset\mathbb{L}$ et on a l'égalité à cause des dimensions.

Réciproquement soit $\omega\in\mathbb{L}$. Supposons que $\sigma(\omega)\notin\mathbb{L}$. Si P désigne le polynôme minimal de ω, $\sigma(\omega)$ est une racine de P qui n'est pas dans L, et l'extension n'est pas normale. □

Exemple 4.3. Il y a 3 plongements de $\mathbb{Q}[\sqrt[3]{2}]=\mathbb{Q}[X]/X^3-2$ dans $\mathbb{C}$. L'extension $\mathbb{Q}[\sqrt[3]{2}]:\mathbb{Q}$ n'est donc pas normale.

4.1.4. Extension Galoisienne.

Définition 4.4. *L'extension finie $\mathbb{L}:\mathbb{K}$ est galoisienne si elle est normale et séparable.*

Remarque 4.4. Tant que l'on s'intéresse aux corps de caractéristique 0, ou aux corps finis, les extensions galoisiennes sont les extensions normales.

Proposition 4.4. *On suppose le corps $\mathbb{K}$ parfait . Les propositions suivantes sont équivalentes.*

i. L'extension $\mathbb{L}:\mathbb{K}$ est galoisienne

ii. Il existe un élément $\alpha\in\mathbb{L}$ qui engendre $\mathbb{L}$ et dont le polynôme minimal est scindé à racines simples

iii. $\mathbb{L}$ est le corps de décomposition d'un polynôme irréductible à racines simples.

iv. $\mathbb{L}$ est le corps de décomposition d'un polynôme à racines simples.

Démonstration. Le seul point non évident est $iv\Rightarrow i$ et c'est ce qu'on vient de démontrer au théorème 3.18. □

Un critère commode est aussi

Proposition 4.5. *L'extension $\mathbb{L}:\mathbb{K}$ est galoisienne si, et seulement si tout polynôme irréductible de $\mathbb{K}$ qui a une racine dans $\mathbb{L}$ y est scindé à racines simples.*□

Le groupe de Galois d'une extension galoisienne est très sympathique.

Théorème 4.7. *Si $\mathbb{L}:\mathbb{K}$ est galoisienne et soit ω un élément primitif de polynôme minimal $P\in\mathbb{K}[X]$. Ainsi P est un polynôme de $\mathbb{K}[X]$ irréductible, à racines simples dans $\mathbb{L}$, et dont $\mathbb{L}$ est le corps de rupture.*
Alors $\mathrm{Gal}(\mathbb{L}:\mathbb{K})$ opère de façon simplement transitive sur les racines de P.
En particulier $|\mathrm{Gal}(\mathbb{L}:\mathbb{K})|=[\mathbb{L}:\mathbb{K}]$

Remarque 4.5. Transitif veut dire que si ω_1,ω_2 sont deux racines, il existe un élément du groupe de Galois (un automorphisme de $\mathbb{L}$) tel que $g\omega_1=\omega_2$ et simplement veut dire que cet élément est unique autrement dit que l'application d'orbite $\mathrm{Gal}(\mathbb{L}:\mathbb{K})\to\mathbb{L}$ qui a g associe $g\omega$ est une bijection avec les racines. L'important c'est cette bijection entre un groupe et un ensemble sur lequel il opère.

Démonstration. Si $\omega\in L$ est une racine de P, $\mathbb{L},\omega$ est un corps de rupture de P tous ces corps sont isomorphes, et si η est une autre racine il existe donc un automorphisme de $\mathbb{L}$ et un seul qui envoi ω sur η. L'action est donc transitive. Mais elle est aussi simplement transitive car le seul automorphisme qui fixe ω est l'identité, vu qu'il fixe aussi $\omega^2,....\omega^n$. □

Nous allons étudier de façon plus approfondie cette action. Heureusement nous avons déjà deux exemples précieux dans la poche que l'on rappelle.

L'extension cyclotomique $\mathbb{R}_n[\mathbb{Q}] = \mathbb{Q}[e^{2i\pi/n}]$ est galoisienne, son groupe de Galois est abélien, isomorphe au groupe $(\mathbb{Z}/n\mathbb{Z})^*$des éléments inversibles de cet anneau, son ordre est $\varphi(n)$ l'indicateur d'Euler. Si ω est une racine primitive de l'unité ω^a en est une autre si et seulement si $a \wedge n = 1$. C'est aussi le corps de décomposition du polynôme cyclotomique Φ_n.

L'extension $\mathbb{F}_{p^n}\colon \mathbb{F}_p$ est galoisienne, son groupe de Galois est cyclique d'ordre n, engendré par l'automorphisme de Frobenius, d'ordre $n = [\mathbb{F}_{p^n}\colon \mathbb{F}_p]$.

Remarque 4.6. Ces deux exemples ont des groupes de Galois commutatifs, ce qui n'est pas du tout typique.

4.1.5. Un exemple important : les fonctions symétriques élémentaires.

Si $\mathbb{K}$ est un corps, on peut considérer le corps $\mathbb{K}(x_1, ...x_n)$ des fonctions rationnelles à n indéterminées dans $\mathbb{K}$.

Ici, on va voir que le corps en question a beaucoup d'automorphismes et que c'est une extension galoisienne du corps des point fixes.

Le groupe symétrique S_n opère naturellement comme groupe d'automorphismes de $\mathbb{K}(x_1, ...x_n)$ par la formule $\sigma.F\,(x_1, ..., x_n) = F(x_{\sigma^{-1}(1)}, ..., x_{\sigma^{-1}(n)})$.

Une fraction rationnelle est dite symétrique si c'est un point fixe de cette action.

L'exemple typique de fraction rationnelle symétrique est la somme des racines, c'est à dire $s_1(x_1, ..., x_n) = x_1 + x_2 + \cdots + x_n$

Nous aurions pu aussi prendre la $k - i$ème fonction symétrique élémentaire, $s_k(x_1, ..., x_n)$ qui est le coefficient en X^k du polynôme $(X - x_1)...(X - x_n)$: en effet ce polynôme qui est une fonction de $\mathbb{K}(x_1, ...x_n)$ vers $\mathbb{K}(x_1, ...x_n)[X]$ est évidemment invariant, donc ses coefficients le sont.
$s_k(x_1, ...x_n) = \Sigma x_1^{i_1}....x_n^{i_n}$ la somme étant prise sur tout les $i_1 + i_2 + \cdots + i_n = k$

Le polynôme s_k s'appelle la $i - i$ème fonction symétrique élémentaire.

Nous noterons $\mathbb{K}(x_1, ...x_n)^{S_n}$ le sous corps formé des fonctions symétriques. Il contient en son sein le corps $\mathbb{K}(s_1, ..., s_n)$ engendré par les fonctions symétriques élémentaires des racines.

Un théorème célèbre, du à Newton dit qu'en fait ces deux corps sont les mêmes.

THÉORÈME 4.8. $\mathbb{K}(x_1, ...x_n)^S = \mathbb{K}(s_1, ...s_n)$.□

Cet théorème sera (re)-démontré plus tard, dans le cadre de la correspondance de Galois.

Nous allons démontrer

PROPOSITION 4.6. *L'extension* $\mathbb{K}(x_1, ...x_n)\colon \mathbb{K}(s_1, ...s_n)$ *est galoisienne de groupe de Galois égal justement au groupe* S_n.

De loin, cet énoncé à l'air très savant et très compliqué, mais en fait pas du tout, la démonstration tient en 4 lignes.

Démonstration. Considérons le polynôme $P(X) = X^n - s_1X^{n-1} + s_2X^{n-2} + \cdots + (-1)^n s_n \in \mathbb{K}(s_1, ...s_n)[X]$. Par construction dans $\mathbb{K}(x_1, ...x_n)[X]$, il vaut $(X - x_1)...(X - x_n)$ c'est à dire qu'il est scindé à racines simples. Ces racines sont $x_1, ...x_n$ et elles engendrent tout le corps. A peu près par définition toutes les permutations de ces racines sont des automorphismes. □

4.1.6. Un exemple de dimension infinie.

Dans cette histoire, il se peut que le corps $\mathbb{L}$ soit de degré infini sur $\mathbb{K}$, et il n'en reste pas moins qu'étudier $\mathrm{Gal}(\mathbb{L}\colon\mathbb{K})$ peut être intéressant, voire captivant.

Soit $\mathbb{K}$ un corps et $\mathbb{L} = \mathbb{K}(t)$ le corps des fractions rationnelles à une indéterminée sur $\mathbb{K}$. SI $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est une matrice inversible à coefficient dans $\mathbb{K}$ et $h(t) = \frac{az+b}{cz+d}$, alors l'application Φ_h: $\mathbb{K}(t) \to \mathbb{K}(t)$ définie par $\Phi_h(f) = f \circ h^{-1}$ est un automorphisme.

On obtient ainsi un homomorphisme $\mathrm{GL}_2(\mathbb{K}) \to \mathrm{Gal}(\mathbb{L}\colon\mathbb{K})$ de noyau les matrices $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$. En effet $\Phi_{h\circ k}(f) = f \circ (h \circ k)^{-1} = (f \circ k^{-1}) \circ h^{-1} = \Phi_h \circ \Phi_k(f)$. C'est d'ailleurs pour ça qu'on a mis $f \circ h^{-1}$, pas $f \circ h$.

Cet homomorphisme passe au quotient $\mathrm{PGL}(2, \mathbb{K}) \to \mathrm{Gal}(\mathbb{L}\colon\mathbb{K})$

Théorème 4.9. *(Luröth)* $\mathrm{Gal}(\mathbb{K}(t)\colon\mathbb{K}) \simeq \mathrm{PGL}(2, \mathbb{K})$

Démonstration. Nous démontrons ce théorème d'abord dans le cas où $\mathbb{K}$ est algébriquement clos.

Soit $\Phi \in \mathrm{Gal}(\mathbb{K}(t)\,/\,K)$. On considère $\Phi(t)$ qui est donc une fraction rationnelle $r(t) = \frac{a(t)}{b(t)}$ ou a et b sont deux polynômes premiers entre eux.

Rappelons que le degré d'une fraction rationnelle $\frac{a(t)}{b(t)}$ écrite sous forme réduite (gcd=1) est le maximum des degrés de a et b.

Comme $\mathbb{K}$ est algébriquement clos, le degré est donné par $\deg(f) = \#\{x\,/\,f(x) = \alpha\}$ sauf pour un nombre fini de α. On a donc $\deg(f \circ g) = \deg(f) \times \deg(g)$

Maintenant $\Phi(f) = f \circ r$. Donc $\deg(\Phi(f)) = \deg(r).\deg(f)$
SI Φ il doit bien y avoir une fraction rationnelle $\Phi^{-1}(t)$, dont l'image est t. Alors $1 = \deg(r).\deg(s)$, ce qui montre que $\deg(r) = 1$

Si $\mathbb{K}$ n'est pas algébriquement clos, c'est pas très grave, il suffit de vérifier que la formule $\deg(f \circ g) = \deg(f) \times \deg(g)$ reste vraie. Or elle est vraie sur la clôture algébrique de $\mathbb{K}$. Donc elle est vraie. □

Remarque 4.7. Les esprits chafouins me feront remarquer que nous avons utilisé l'axiome du choix pour passer à la clôture algébrique. Je leur répondrai que f, g étant fixées, on peut regarder le sous-corps $\mathbb{K}'$ de $\mathbb{K}$ engendré par les coefficients de ses fractions rationnelles qui est un corps dénombrable. Et pour ce genre de corps, on a déjà construit une clôture algébrique. Il n'y a pas besoin de ACD car on connait une famille de générateurs de $\mathbb{K}'$ donc on peut construire une surjection $\mathbb{N} \to \mathbb{K}'$, puis $\mathbb{N} \to \mathbb{K}'[X]$.

Remarque 4.8. Le groupe de $\mathrm{Gal}(\mathbb{K}(t_1, ...t_n)\colon\mathbb{K})$ s'appelle le groupe de Cremona $\mathrm{Cr}_n(\mathbb{K})$. Il fait l'objet de recherches actuelles très intéressantes.

4.2. Correspondance de Galois.

Jusqu'à présent, nous avons considéré un corps $\mathbb{K}$, une extension $\mathbb{L}:\mathbb{K}$ et regardé le groupe $\mathrm{Gal}(\mathbb{L}:\mathbb{K})$. Maintenant, nous allons regarder les sous-groupes de ce groupe, et voir comment il agit sur l'ensemble des sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$.

4.2.1. Le corps des points fixes.

Soit $G<\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ un sous groupe. Nous noterons $\mathbb{L}^G=\{x\in\mathbb{L}/\forall g\in G,\, g(x)=x\}$ le sous-corps des points fixes de G. Alors $\mathbb{L}$ est une extension de $\mathbb{L}^G$.

Quelques remarques sur les liens entre groupe et corps.

PROPOSITION 4.7. *Si* $G_1\supset G_2$ *alors* $\mathbb{L}^{G_1}\subset\mathbb{L}^{G_2}$
Si $\mathbb{L}\supset\mathbb{K}_2\supset\mathbb{K}_1$ *alors* $\mathrm{Gal}(\mathbb{L}/\mathbb{K}_2)\subset\mathrm{Gal}(\mathbb{L}/K_1)$
$\mathbb{L}^{\mathrm{Gal}(\mathbb{L}/\mathbb{K})}\supset\mathbb{K}$
$\mathrm{Gal}(\mathbb{L}/\mathbb{L}^G)\supset G$

THÉORÈME 4.10. *Lemme d'Artin*[4.1]. *Soit* G *un groupe fini d'automorphismes d'un certain corps* $\mathbb{L}$.
Le degré de l'extension $(\mathbb{L}/\mathbb{L}^G)$ *est inférieur ou égal à l'ordre de* G.

Autrement dit si G n'est pas très gros, le sous corps $\mathbb{L}^G$ est très gros, par exemple si $G=\mathbb{Z}/2\mathbb{Z}$ $\mathbb{L}/\mathbb{L}^G$ est de degré 2 ou 1.

Démonstration. On note $n=|G|$ l'ordre du groupe G. Il 'agit de démontrer que si $m>n$ toute famille de m éléments de $\mathbb{L}$ est liée sur $\mathbb{L}^{\mathbb{G}}$.

Nous allons raisonner par l'absurde et supposer qu'il existe une famille libre de rang $m>n$.

Soient donc $G=\{g_1,\ldots,g_n\}$ et considérons une famille libre d'éléments $u_1,\ldots u_m$ de $\mathbb{L}$, avec $m>n$. Le système suivant, à coefficients dans $\mathbb{L}$, a plus d'inconnues $(x_1,\ldots.x_m)$ que d'équations n (l'ordre de G).

$$\text{Pour tout } g\in G \text{ on a } \Sigma_{j=1}^m x_j\, g(u_j)=0$$

LEMME 4.3. *Ce sytème d'équation est invariant par le groupe* G, *c'est à dire que si* $(x_1,\ldots x_m)$ *est une solution et si* $h\in G$, *alors* $h(x_1),\ldots h(x_m)$ *aussi.*

Démonstration. E effet si pour tout g, on a $\Sigma_{j=1}^m\, x_j\, g(u_j)=0$, on a pour tout g, h. $\Sigma_{j=1}^m x_j\,(h^{-1}g)(u_j)=0$. Appliquons h alors $\Sigma_{j=1}^m h\,(x_j)\,g(u_j)=0$ □

Comme il y a une inconnue de plus que d'équations, il y a une solution non nulle $(x_1,\ldots x_m)$ sur $\mathbb{L}$, et quitte à ré-ordonner le tout, on peut même supposer que $x_1=1$.

Autrement dit, il existe des éléments $1,x_2,\ldots x_{n+1}$ de $\mathbb{L}$ tels que pour tout élément de G on ait $1+\Sigma_{j=2}^{n+1} x_j g(u_j)=0$

Par invariance, si $(1,x_2,\ldots,x_{n+1})$ est une solution, $(1,g\,(x_2),\ldots,g\,(x_{n+1}))$ en est une autre.

En soustrayant; $(x_2-g(x_2))\,u_2+(x_3-g(x_3))u_3+\cdots+(x_{n+1}-g(x_{n+1}))u_{n+1}=0$

Comme la famille $u_2,\ldots u_m$ est libre, $x_i=g(x_i)$, et les x_i sont dans $\mathbb{L}^{\mathbb{G}}$, donc la famille $u_1,\ldots u_m$ est liée sur $\mathbb{K}^{\mathbb{G}}$, car $1.u_1+\Sigma_{i=2}^m x_i u_i=0$ □

4.1. Il s'agit d'Emil Artin [1898-1962], père de Michael [1934-]

4.2.2. Le théorème de Galois.

Le premier résultat important est

Théorème 4.11. *Soit $\mathbb{L}$ une extension d'un corps $\mathbb{K}$. Les conditions suivantes sont équivalentes :*

i. Il existe un polynôme séparable de $\mathbb{K}[X]$ dont $\mathbb{L}$ est le corps de décomposition.

ii. Il existe un sous-groupe fini $G < \mathrm{Aut}(\mathbb{L})$ tel que $\mathbb{K} = \mathbb{L}^G$.

iii. L'extension $\mathbb{L}/\mathbb{K}$ est de degré fini, normale et séparable (c'est à dire galoisienne).

Par ailleurs, sous l'hypothèse ii, $G = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ et $[\mathbb{K}:\mathbb{L}] = |G|$

Démonstration.
D'abord $i \Rightarrow ii$. Soit $G = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ et $\mathbb{K} \subset \mathbb{L}^G \subset \mathbb{L}$ le corps des points fixes de G.
Evidemment $\mathrm{Gal}(\mathbb{L}:\mathbb{K}) = \mathrm{Gal}(\mathbb{L}:\mathbb{K}^G)$

Comme l'extension est spérable, il existe un élment primitif ω. Son polynome minimal est de degré $[\mathbb{L}:\mathbb{K}]$, et comme elle est normale le groupe de Galois a pour ordre $[\mathbb{L}:\mathbb{K}] = |\mathrm{Gal}(\mathbb{L}/\mathbb{K})| = |\mathrm{Gal}(\mathbb{L}:\mathbb{K}^G)|$. D'après le lemme d'Artin $[\mathbb{L}:\mathbb{K}^G] \leqslant |\mathrm{Gal}(\mathbb{L}:\mathbb{K}^G)| = [\mathbb{L}:\mathbb{K}]$, et on a donc bien égalité.

Ensuite $ii \Rightarrow iii$. Grâce au lemme d'Artin $[\mathbb{L}:\mathbb{K}] \leqslant |G|$, de sorte qu'en tant que $\mathbb{K}$ espace vectoriel, $\mathbb{L}$ est de dimension finie. Si $f \in \mathbb{K}[X]$ est un polynôme irréductible qui a une racine ω dans $\mathbb{L}$. Notons $\omega = \omega_1, ...\omega_m$ l'orbite de ω sous l'action de G. Le polynôme f est divisible par $X - \omega_i$, donc par le produit $p(X) = \Pi_{i=1}^m (X - \omega_i)$

Si $g \in G$, on considère l'automorphisme noté g de $\mathbb{L}[X]$ qui envoi X sur lui même et dont la restriction $\mathbb{L}$ est g. On a $g(p)(X) = \Pi_{i=1}^m (X - g.\omega_i) = p(X)$ ce qui veut dire que les coefficients de p sont invariants, ou que $p \in \mathbb{K}[X]$. Mais f est irréductible, donc $f = p$ donc f est un polynôme scindé à racine simples. Et l'extension est bien galoisienne.

Enfin $iii \Rightarrow i$. On choisi un élément primitif (ce qui est possible vu que l'extension est séparable) son polynôme minimal est bien scindé à racine simple vu que l'extension est normale, et comme il est primitif il engendre bien $\mathbb{L}$.

Sous l'hypothèse ii, nous avons vu le lemme d'Artin qui dit que $[\mathbb{L}:\mathbb{K}] \leqslant |G|$. Comme l'extension est galoisienne $|\mathrm{Gal}(\mathbb{L}/\mathbb{K})| = [\mathbb{L}:\mathbb{K}]$ (c'est le degré du polynôme minimal d'un élément primitif). Donc comme $G < \mathrm{Gal}(\mathbb{L}/\mathbb{K})$, on a l'égalité. □

Corollaire 4.2. *Soit $\mathbb{L}$ un corps et G un sous groupe fini de $\mathrm{Aut}(\mathbb{L})$ et soit $\mathbb{K} = \mathbb{L}^G$ Alors $\mathbb{L}:\mathbb{K}$ est galoisienne, de degré $|G|$.*

Démonstration. C'est une reformulation du point ii du théorème précédent. □

4.2.3. La correspondance de Galois

Soit $\mathbb{L}:\mathbb{K}$ une extension galoisienne de groupe de Galois G (et donc de degré $|G|$). Si $H < G$ est un sous groupe, on considère le corps $\mathbb{L}^H$. Le paragraphe précédent montre que l'extension $\mathbb{L}/\mathbb{L}^H$ est galoisienne de groupe de Galois H et donc que le degré de $\mathbb{L}^H/\mathbb{K}$ est $\frac{|G|}{|H|}$. Ainsi à chaque sous groupe de G nous avons associé une extension de $\mathbb{K}$ contenue dans $\mathbb{L}$, l'indice de celui ci se transformant en le degré de celle-là.

Le théorème de Galois nous dit que réciproquement si l'extension $\mathbb{L}:\mathbb{K}$ est galoisienne de groupe G, et si $\mathbb{K}\subset\mathbb{M}\subset\mathbb{L}$, il existe un sous groupe de G tel que $\mathbb{M}=\mathbb{L}^H$. Evidemment si ce sous groupe existe, on a pas le choix, c'est $\mathrm{Aut}(\mathbb{L}:\mathbb{M})$. Le théorème suivant est appelé le théorème fondamental de la théorie de Galois.

THÉORÈME 4.12. *Soit $\mathbb{L}:\mathbb{K}$ une extension galoisienne de groupe de Galois fini G.*
Si $\mathbb{K}\subset\mathbb{M}\subset\mathbb{L}$, et $H=\mathrm{Aut}(\mathbb{L}/\mathbb{M})$, alors $\mathbb{M}=\mathbb{L}^H$
Si $H<G$ et $\mathbb{M}=\mathbb{L}^H$, alors $H=\mathrm{Aut}(\mathbb{L}:\mathbb{M})$

Remarque 4.9. La correspondance entre les sous groupe du groupe de Galois et les sous corps s'appelle la correspondance de Galois.

Démonstration. Démontrons le premier. Comme l'extension $\mathbb{L}:\mathbb{K}$ est séparable, l'extension $\mathbb{L}:\mathbb{M}$ l'est aussi et $\mathbb{L}$ est le corps de décomposition d'un polynôme à racines simples à coefficients dans $\mathbb{M}$. Il est scindé vu que $\mathbb{L}:\mathbb{K}$ est galoisienne. Donc l'extension $\mathbb{L}:\mathbb{M}$ est galoisienne de groupe $\mathrm{Aut}(\mathbb{L}:\mathbb{M})$, et M est l'ensemble des points fixes de ce groupe.
Le second point est simplement le point ii du théorème 3.35 □

Exemple 4.4. Le théorème de Newton. Nous avons vu que le fait que les coefficients d'un polynômes sont des fonctions symétriques élémentaires de racines peu se formuler ainsi.
L'extension $\mathbb{K}(x_1,...x_n):\mathbb{K}(s_1....s_n)$ est galoisienne, ou les s_i sont les fonctions symétriques élémentaires des racines. C'est le corps de décomposition du polynôme séparable $X^n-s_1X^{n-1}+\cdots+s_n$. Son groupe de Galois est le groupe symétrique. Donc $\mathbb{K}(s_1...s_n)$ est exactement égal au groupe des permutations des x_i. Or une fonction symétrique des racines c'est précisément un élément de $\mathbb{K}(x_1,...x_n)^G$. A dire vrai, le théorème de Newton concerne plutôt les fonctions polynômes que les fonctions rationnelles.

Pour aller plus loin dans la correspondance de Galois, il faut comprendre non pas l'extension $\mathbb{L}:\mathbb{L}^H$, mais l'extension $\mathbb{L}^H:\mathbb{K}$, dont le degré est $|G/H|$

THÉORÈME 4.13. *Soit $\mathbb{L}:\mathbb{K}$ une extension galoisienne de groupe de Galois G. Soit $H<G$. les propriétés suivantes sont équivalentes.*

i. L'extension $\mathbb{L}^H:\mathbb{K}$ est normale

ii. le sous groupe H est normal (=distingué) dans G

Sous ces hypothèses, $\mathrm{Gal}(\mathbb{L}^H:\mathbb{K})=G/H$.

Remarque 4.10. C'est pour cela que le mot normal est utilisé dans les deux cas. Certain auteurs français utilisent le mot « distingué » pour les sous-groupes normaux, mais l'usage de cette terminologie tend à disparaitre.

Démonstration. L'extension $\mathbb{L}^H:\mathbb{K}$ est séparable car $\mathbb{L}:\mathbb{K}$ l'est. Si elle est de plus normale, on peut donc choisir un élément primitif ω dont les racines du polynômes minimal sont précisément les images de ω par l'action de $\mathrm{Gal}(\mathbb{L}^H:\mathbb{K})$. Ce polynôme étant à coefficient dans $\mathbb{L}^H$ le groupe G les permute ce qui donne un homomorphisme $G\to\mathrm{Gal}(\mathbb{L}^H:\mathbb{K})$ dont le noyau est précisément le sous groupe qui fixe ω c'est à dire H. Donc $i\Rightarrow ii$ avec le complément en sus.
Réciproquement si $H\lhd G$, le sous corps $\mathbb{L}^H$ est invariant par tout le groupe G en effet soit $m\in\mathbb{L}^H$ $hgm=g\,(g^{-1}hg)m=g.h'm=g.m$. On obtient ainsi un homomorphisme $G\to\mathrm{Aut}(\mathbb{L}^H:\mathbb{K})$ dont le noyau est précisément H. Comme $|G/H|=[\mathbb{L}^H:\mathbb{K}]=|\mathrm{Gal}(\mathbb{L}^H:\mathbb{K})|$, on a l 'égalité. □

Un exemple très utile est le cas des sous groupe d'indice 2 : on sait que tout sous groupe d'indice 2 est normal.

COROLLAIRE 4.3. *Soit $\mathbb{L}:\mathbb{K}$ une extension galoisienne de groupe de Galois G. Soit $H<G$ un sous groupe d'indice 2.*

L'extension $\mathbb{L}^H:\mathbb{K}$ est normale, $\mathrm{Gal}(\mathbb{L}^H:\mathbb{K})=\mathbb{Z}/2\mathbb{Z}$, $\mathrm{Gal}(\mathbb{L}:\mathbb{L}^H)=H$.

4.2.4. Le théorème de Gauss-Wantzel.

En combinant un petit résultat de théorie des groupes et le théorème de la correspondance de Galois, nous allons démontrer le théorème de Wantzel.

Théorème 4.14. *Wantzel. Si un polygone régulier a n côtés, où n est le produit d'une puissance de 2 et de nombres premiers de Fermat différents, alors il est constructible.*

Ici on est en train d'étudier une extension cyclotomique (donc galoisienne) et on sait que son degré est une puissance de 2, son groupe de Galois est donc un groupe fini d'ordre 2^b. c'est ce qu'on appelle un 2-groupe.(Dans la théorie des groupes finis, les 2-groupes jouent un rôle très important, par exemple on sait que 99% des groupes d'ordre $\leqslant 10^{10}$ sont des 2-groupes.)

Nous allons en fait démontrer, par récurrence sur le degré, que si $P[X]$ est un polynôme irréductible de $\mathbb{Q}[X]$, alors ses racines sont constructibles si le degré de son corps de décomposition est une puissance de 2.

Lemme 4.4. *Soit $P(X) = aX^2 + bX + c$ un polynôme de degré 2. On suppose que les nombres complexes a, b, c sont constructibles. Alors les racines de P aussi.*

Démonstration. On pose $\Delta = b^2 - 4ac$. Il s'agit de montrer que les deux racines complexes de Δ sont constructibles. Mais le module $|\Delta|$ s'obtient en intersectant l'axe $(0, 1)$ avec le cercle centré en 0 passant en Δ. Donc $\sqrt{|\Delta|}$ aussi comme on l'a déjà vu. □

L'initialisation de notre récurrence résulte du lemme précédent quand $a, b, c \in \mathbb{Q}$.

Pour l'induction, nous remarquons que sous les hypothèses du théorème, si $\mathbb{L}$ est le corps de décomposition de P alors $\mathbb{L}\colon \mathbb{Q} = |\mathrm{Gal}(\mathbb{L}\colon \mathbb{Q})|$ est une puissance de 2. Or on a le

Lemme 4.5. *Tout groupe d'ordre 2^n contient un élément d'ordre 2 dans son centre (et en fait est nilpotent).*

Démonstration. On fait opérer G sur lui même par conjugaison. Le centre $Z(G)$ de G est l'ensemble des points fixes, et grâce à la formule de Lagrange les autres orbites ont un cardinal pair.

$|G| = \text{Fixes} + \text{Somme des cardianux des orbites non fixes}$

L'orbite d'un point x_0 non fixe a pour cardinal $|G| / |G_{x_0}|$ qui est ici une puissance de 2 donc un nombre pair.

Le nombre de points fixe est congru à $|G|$ modulo 2. Or $1 \in Z(G)$ donc $|Z(G)|$ contient un élément différent de 1, disons g_0. L'ordre de cet élément est une puissance de 2, disons 2^{n_0}. Alors $(g)^{2^{n_0-1}}$ est d'ordre 2. □

Soit g_1 un élément comme construit. Donc $(1, g_1)$ est un sous groupe normal du groupe de Galois et qui est d'ordre 2. D'après ce qui précède $\mathbb{L}^{g_1}$ est une extension normale de $\mathbb{Q}$, de degré 2^{n-1}. C'est le corps de rupture d'un polynôme à coefficients dans $\mathbb{Q}$, et l'hypothèse de récurrence montre que ses racines sont des complexes constructible. Mais l'extension $\mathbb{L}\colon \mathbb{L}^{g_1}$ est de degré 2, donc le polynôme minimal sur $\mathbb{L}^{g_1}$ de l'une des racines de P qui n'est pas dans $\mathbb{L}^{g_1}$ est un polynôme de degré 2 à coefficient dans $\mathbb{L}^{g_1}$. Donc cette racine (et toutes les autres) sont constructibles.

4.2.5. Clôture algébrique

A strictement parler, la clôture algébrique $\bar{\mathbb{K}}\colon \mathbb{K}$ n'est pas une extension normale car elle est de degré infini. Il n'empêche c'est tout comme, puisque par définition tout polynôme y est scindé. En faisant attention de prendre des extensions finies et des sous-groupes d'indice fini, la théorie de Galois fonctionne bien. Tout aussi embêtant, elle n'est pas toujours séparable vu que si $\mathbb{K}$ est infini de caractéristique $p \neq 0$ il existe des extensions qui ne le sont pas.

Nous supposerons donc que nous sommes dans l'un de ces deux cas pour ne pas trop se fatiguer la tête. On dit que le corps est parfait, car pour nous c'est parfait. Autrement dit soit $\mathrm{car}(\mathbb{K}) = 0$ soit $\mathbb{K}$ est fini.

Comme la clôture algébrique contient toutes les extensions finies possibles d'un corps $\mathbb{K}$ supposé parfait (soit fini soit de car 0), nous obtenons la correspondance de Galois

THÉORÈME 4.15. *Soit $\bar{\mathbb{K}}/\mathbb{K}$ une clôture algébrique*
Si $\mathbb{M}\colon \mathbb{K}$ et finie, et $H = \mathrm{Gal}(\bar{\mathbb{K}}/\mathbb{M})$, alors $\mathbb{M} = \bar{\mathbb{K}}^H$
Si $H < \mathrm{Gal}(\bar{\mathbb{K}}/\mathbb{K})$ est un sous groupe d'indice fini, alors $\mathbb{M} = \bar{\mathbb{K}}^H$ et une extension finie et $H = \mathrm{Gal}(\mathbb{L}/\mathbb{M})$

Remarque 4.11. En clair il y a une bijection entre les extensions finies d'un corps parfait et les sous groupes d'indice fini du groupe de Galois de sa clôture algébrique.

THÉORÈME 4.16. *La correspondance de Galois induit une bijection entre les extensions normales de degré fini d'un corps parfait $\mathbb{K}$ et les sous-groupes normaux d'indices fini de $\mathrm{Gal}(\bar{\mathbb{K}}/\mathbb{K})$.*

Dans le cas de $\mathbb{F}_p$ la clôture algébrique $\overline{\mathbb{F}_p}$ est la limite directe $\lim_n \mathbb{F}_{p^n}$, ou l'on voit $\mathbb{F}_{p^n}$ comme sous corps de $\mathbb{F}_{p^{n+1}}$. Alors $\mathbb{F}_{p^n}$ est l'ensemble des points fixes de Φ^n.

4.3. Résolubilité.

Ce paragraphe a essentiellement un intérêt historique. La question de savoir si les équations polynomiales $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ peuvent ou pas être résolues « par radicaux » a beaucoup excité les mathématiciens de la Renaissance (Tartaglia, Cardano, Ferrari), et a finalement été résolue par Ruffini en 1799, puis Abel en 1824. En fait c'est Ruffini qui le premier a l'idée (révolutionnaire, nous sommes dans les années 1790), qu'il est impossible de trouver des formules pour résoudre les équation de degré 5. Sa démonstration consiste à étudier le groupe S_5 (personne ne sait ce qu'est un groupe en particulier pas S_5), mais apparement cette démonstration contient une faute. Mais bon l'idée est bien là…La première démonstration complète est due à Abel. La théorie générale a été faite par Galois (1832), qui en fait démontré que S_5 n'est pas résoluble.

Un peu comme le problème de Fermat, on peut franchement douter de l'intérêt de cette question mais on ne peut que s'émerveiller du fait que d'y réfléchir a fait faire un progrès majeur des mathématiques avec la découverte de la théorie des groupes avec les noms de Newton, Lagrange, Abel, Galois, Gauss, Jordan, Klein. Le mot « groupe » a été inventé par Galois.

4.3.1. L'équation $X^n - a = 0$, et son groupe de Galois.

Nous avons déjà vu que cette équation a des difficulté particulière en caractéristique p, si n est multiple de p, car ce polynôme n'est pas séparable. Pour ne pas nous embarrasser, nous supposons donc que $\mathrm{car}(\mathbb{K}) = 0$, et même que $\mathbb{K} \subset \mathbb{C}$.

Nous savons bien que dans $\mathbb{C}$ ce polynôme devient scindé à racines simples et que ses racines sont $b, \omega b, \omega^2 b, ...\omega^{n-1} b$, ou ω est une racine primitive n ième de l'unité par exemple $e^{\frac{i2\pi}{n}}$, et b une racine préférée de ce polynôme.

Proposition 4.8. *Soit $\mathbb{K}$ un corps de caractéristique nulle sur lequel $X^n - 1$ est scindé (si on préfère il « contient » $R_n[\mathbb{Q}]$), $a \in \mathbb{K}$. Si $\mathbb{L}$ est le corps de décomposition de $X^n - a$, alors* $\mathrm{Gal}(\mathbb{L}\colon \mathbb{K})$ *est cyclique.*

Démonstration. Comme $\mathbb{K}$ contient toutes les racines de l'unité disons $(w_i)_{1 \leqslant i \leqslant n}$; si b est une racine de $X^n - a$, $\mathbb{L}$ contient bw_i : $\mathbb{L}$ est donc engendré par b en tant qu'extension de $\mathbb{K}$. Alors effet si $g \in \mathrm{Gal}(\mathbb{L}\colon \mathbb{K})$ on pose $\varphi(g) \in \mathbb{Z}/n\mathbb{Z}$ défini par $\varphi(g) = \frac{g(b)}{b}$, où b est une racine de $X^n - a$. On obtient ainsi un homomorphisme de $\mathrm{Gal}(\mathbb{L}\colon \mathbb{K})$ vers le groupe des racines de l'unité (qui est cyclique). Cet homomorphisme est injectif car b engendre $\mathbb{L}$, donc $g(b) = b \Rightarrow g = \mathrm{Id}$. Or tout sous -groupe d'un groupe cyclique est cyclique. □

Proposition 4.9. *Une extension de $\mathbb{K}$ sur lequel $X^n - a$ est scindé contient tout les racines de l'unité.*

Démonstration. En effet si b_1, ...b_n sont les racines de $X^n - a$, les rapports $w_i = \frac{b_i}{b_1}$ sont manifestement les racines de l'unité. □

En appliquant le théorème fondamental de la théorie de Galois, on obtient.

Proposition 4.10. *Soit $\mathbb{L}$ le corps de décomposition du polynôme $X^n - a$, et $R_n(\mathbb{K})$ celui de $X^n - 1$, de sorte que $R_n(\mathbb{K}) \subset \mathbb{L}$. Alors le sous groupe* $\mathrm{Gal}(\mathbb{L}\colon R_n(\mathbb{K}))$ *de* $\mathrm{Gal}(\mathbb{L}\colon \mathbb{K})$ *est normal et isomorphe à un sous groupe C de $\mathbb{U}_n$ (le groupe cyclique à n éléments). Le quotient est* $\mathrm{Gal}(\mathbb{R}_n\colon \mathbb{K}) = \mathrm{Aut}(\mathbb{U}_n)$.

Autrement dit la suite de groupe :

$1 \to C \to \mathrm{Gal}(\mathbb{L}/\mathbb{K}) \to \mathrm{Aut}(\mathbb{U}_n) \to 1$ est exacte.

ce qui veut dire que le noyau de la troisième flèche est l'image de la seconde.

Remarque 4.12. Si d divise n, $\mathbb{U}_n$ contient un unique sous groupe d'ordre d, ce qui explique que $\mathrm{Aut}(\mathbb{U}_n)$ agit par automorphisme sur le groupe cyclique C.

4.3.2. Equation résoluble par radicaux.

Soit $P \in \mathbb{K}[X]$ un polynôme. On voudrait savoir si on peut résoudre $P = 0$ en utilisant que des signes +,-, *, $\sqrt[n]{}$, et des éléments de $\mathbb{K}$. Par exemple $\frac{-b + \sqrt{b^2 - 4\mathrm{ca}}}{2a}$,
ou alors $\sqrt[5]{a + \sqrt{b} - 17^{89}\sqrt{ab}} + 1664^{2021}\sqrt{b^5 - 1515.a^2.\sqrt[9]{ab}}$

Si tel est le cas, il existe un entier n, une suite de corps $\mathbb{K} \subset \mathbb{K}_1 \subset \mathbb{K}_2 .... \subset \mathbb{K}_l$ des éléments a_i de $\mathbb{K}_i$ et des entiers $n_1, ...n_l$ tels que d'une part $\mathbb{K}_{i+1}$ soit le corps de décomposition de $X^{n_i} - a_i$ sur $\mathbb{K}_i$, et d'autre part que les racines cherchées sont dans $\mathbb{K}_n$, c'est à dire que le polynôme P soit scindé dans $\mathbb{K}_l$.

Définition 4.5. *L'équation définie par le polynôme P est résoluble par radicaux si il existe une telle suite.*

DÉFINITION 4.6. *Une extension $\mathbb{L}:\mathbb{K}$ est dite radicale, si il existe une suite $\mathbb{K}=\mathbb{K}_0\subset\mathbb{K}_1...\subset\mathbb{K}_n=\mathbb{K}$ telle que pour tout i l'extension $\mathbb{K}_{i+1}:\mathbb{K}_i$ soit obtenue en ajoutant une racine d'un élément de $\mathbb{K}_i$, c'est à dire qu'il existe un élément α_i et un entier n_i telle que $\mathbb{K}_{i+1}$ soit le corps de rupture du polynôme $X^{n_i}-\alpha_i$ sur $\mathbb{K}_i$.*

L'équation définie par le polynôme P est donc résoluble par radicaux si l'une de ses racines est dans une extension radicale.

Remarque 4.13. Dans ce genre de question, on se ramène toujours au cas où le polynôme P est irréductible, donc séparable. Sinon, on cherche les facteurs premiers : comment, me direz vous ? Mystère et boule de gomme. *Le but est de chercher si l'équation est résoluble, pas de la résoudre.* La question de savoir si il existe un algorithme pour la résoudre est évidemment beaucoup plus facile que celle de déterminer les solutions.

La difficulté principale que nous allons rencontrer dans l'étude des extensions radicales, c'est qu'elle ne sont pas normales, en général.

Exemple 4.5. La tour $\mathbb{Q}\subset\mathbb{Q}(\sqrt{2})\subset\mathbb{Q}(\sqrt[4]{2})$ n'est pas normale, car le polynôme X^4-2 n'y est pas scindé. (le corps de décomposition de X^n-a contient toutes les racines n de l'unité, ici aussi i et $-i$. Mais c'est bien une succession de deux extensions par une racine carrée (donc radicales). Pour améliorer la situation, il faut rajouter i à un moment ou à un autre.

La première étape est la suivante.

Soit $\mathbb{K}=\mathbb{K}_0\subset\mathbb{K}_1...\subset\mathbb{K}_n=\mathbb{K}$ une extension radicale : pour tout i, on choisit un élément α_i de $\mathbb{K}_i$ et un entier n_i telle que $\mathbb{K}_{i+1}$ soit le corps de rupture du polynôme $X^{n_i}-\alpha_i$ sur $\mathbb{K}_i$.

Première étape. On pose $n=\text{ppcm}(n_i)$, $\mathbb{K}'_0=\mathbb{K}_0(\xi)$, ou ξ est une racine primitive n-ème de l'unité, $\mathbb{K}'_i=\mathbb{K}'_0[a_1,...a_i]=\mathbb{K}'_{i-1}[a_i]$ ou $a_i\in\mathbb{K}_i<\mathbb{K}'_i$ est une racine de l'équation $X^{n_{i-1}}-\alpha_{i-1}$.

Clairement la suite $\mathbb{K}_0<\mathbb{K}'_0<\cdots<\mathbb{K}'_n$ est encore une extension radicale.
Ce que nous avons gagné ici, c'est que l'extension $\mathbb{K}'_{i+1}:\mathbb{K}'_i$ est galoisienne et son groupe de Galois est cyclique, vu que $\mathbb{K}'_i$ contient déjà *toutes* les racines n_i- ième de l'unité, et que le polynôme minimal de a_i sur $\mathbb{K}$ divise $X^{n_i}-a_i$.

L'exemple précédent montre que nous n'avons toujours pas automatiquement une extension normale. Nous allons donc normaliser tout cela ; le point délicat est de bien expliquer que l'extension normalisée reste radicale.

Pour chaque i on note A_i l'ensemble des conjugués de a_i dans la clôture algébrique de $\mathbb{K}_0$.(les racines du polynômes minimal de a_i). Nous allons démontrer

LEMME 4.6. *L'extension $\mathbb{L}=\mathbb{K}_0[\xi,A_1,....A_n]$ est galoisienne, radicale.*

Par construction $\mathbb{L}:\mathbb{K}$ est le corps de décomposition du polynôme $(X^n-1)\times\Pi P_i$, ou P_i est le polynôme minimal de a_i sur $\mathbb{K}_0$. Mais celui ci est scindé à racine simples vu qu'aucun des a_i n'est une racine de l'unité et que tous les conjugués de tous les a_i sont différents.

Pour vérifier qu'elle est radicale, on raisonne par récurrence et on vérifie que pour tout entier i et pour tout élément a de A_i, $a^{n_i}\in\mathbb{K}[\xi,\cup_{j<i}A_j]$. C'est clair pour a_i

Soit σ un homomorphisme de $\mathbb{K}[a_i]$ dans la clôture algébrique de $\mathbb{K}$ tel que $\sigma(a_i)=a$. On étend σ à $\mathbb{K}[\xi,\cup_{j<i}A_j][a_i]$, et on en déduit que $a^n=\sigma(a_i^{n_i})=\alpha_i\in\mathbb{K}_{i-1}$ et donc l'extension obtenu en ajoutant a est encore radicale.

Proposition 4.11. *Il existe une racine ξ de l'unité dans $\mathbb{C}$, et une suite de corps $\mathbb{K}_0 = \mathbb{K}$, $\mathbb{K}_1 = \mathbb{K}[\xi], \mathbb{K}_2, ...\mathbb{K}_n = \mathbb{L}$ telle que $\mathbb{K}_{i+1} = \mathbb{K}_i[s_i]$ soit une extension cyclique normale de $\mathbb{K}_i$.*

Proposition 4.12. *Le groupe de Galois $\mathrm{Gal}(\mathbb{L}:\mathbb{K})$ contient une suite de sous groupe normaux G_i tels que $G_{i+1}:G_i$ soit cyclique.*□

Ici G_i est juste le sous groupe qui fixe $\mathbb{K}_i$.

4.3.3. Les groupes et les équations résolubles.

Les groupes satisfaisant la propriété que nous venons de voir sont appelés des groupes résolubles.

Définition 4.7. *Un groupe G est résoluble si il existe une suite $G_0 \lhd G_1 \lhd G_2 \lhd ...G_{n-1} \lhd G_n = G$ telle que pour tout i G_i est normal dans G et G_{i+1}/G_i est abélien.*

(En théorie des groupes, on note $H \lhd K$ pour dire que H est un sous groupe normal de K).

Lemme 4.7. *Tout sous groupe et tout quotient d'un groupe résoluble est résoluble.*

Démonstration. Soit $H < G$ un sous groupe de G. Ecrivons $G_0 \lhd G_1 \lhd G_2 \lhd ...G_{n-1} \lhd G_n = G$, de sorte que G_{i+1}/G_i est abélien. Le groupe $H \cap G_i$ est un sous groupe normal de H que l'on note H_i.

Le groupe H_{i+1}/H_i est isomorphe à l'image de H dans G_{i+1}/G_i. Comme tout sous groupe d'un groupe abélien est abélien, on a le résultat.

Soit H un quotient de G, c'est à dire qu'il existe un homomorphisme surjectif $\pi: G \to G$. Alors l'image de G_i dans H est normale (car π est surjectif) et H_{i+1}/H_i est un quotient de G_{i+1}/G_i donc est abélien. □

Notation 4.1. *Le groupe $[G,G] \lhd G$ est le sous groupe dérivé de G, c'est à dire le sous groupe engendré engendré par les commutateurs $aba^{-1}b^{-1}$.*

Proposition 4.13. *Si $\varphi: G \to A$ est un homomorphisme de G vers un groupe abélien,* $\ker\varphi \supset [G,G]$.
Le sous groupe $[G,G]$ est normal (et même invariant) et le quotient $G/[G,G]$ est abélien.

Démonstration. Le premier point est facile. Comme $\varphi(aba^{-1}b^{-1}) = \varphi(a)\varphi(b)\varphi(a)^{-1}\varphi(b)^{-1}$ et comme A est abélien, $\varphi(aba^{-1}b^{-1}) = e$.

Pour voir que $[G,G]$ est normal, on démontre qu'il est invariant par tout automorphisme, donc aussi par tout automorphisme intérieur. Si $\psi \in \mathrm{Aut}(G)$, $\psi(aba^{-1}b^{-1}) = \psi(a)\psi(b)\psi(a)^{-1}\psi(b)^{-1}$, et donc $\psi([G,G]) = [G,G]$, le quotient est abélien, car si α, β son les images de a, b dans ce quotient $\alpha\beta\alpha^{-1}\beta^{-1}$ est l'image de $aba^{-1}b^{-1}$, or cet élément est dans $[G,G]$ donc $\alpha\beta\alpha^{-1}\beta^{-1} = e$. □

Proposition 4.14. *Si G est résoluble $G\,/\,[G,\,G]$ n'est pas réduit à l'élément neutre. En effet Comme G/G_{n-1} est abélien, il est contenu dans $G/[G,G]$.*

Théorème 4.17. *Si $P \in \mathbb{K}[X]$ est un polynôme irréductible et résoluble par radicaux, alors le groupe de Galois de son corps de décomposition est un groupe résoluble.*

Démonstration. Combiner 3.53 avec le fait que tout quotient d'un groupe résoluble. Son corps de décomposition est un sous corps d'une extension normale et radicielle, dont la groupe de Galois est résoluble. En tant que quotient d'un groupe résoluble le groupe de Galois de ce corps de décomposition est donc résoluble. □

Théorème 4.18. *Soit $\mathbb{K} = \mathbb{Q}(a_0, ...a_{n-1})$. Alors l'équation générale $P(X) = X^n + \Sigma_{i=0}^{n} a_i X^i$ n'est pas résoluble par radicaux si $n \geqslant 5$.*

Démonstration. Nous avons vu que son groupe de Galois est S_n et nous allons voir que si $n \geqslant 5$ ce groupe n'est pas résoluble. □

PROPOSITION 4.15. *Pour tout entier n, le groupe A_n est engendré par les $3-$cycles.*
Si $n \geqslant 5$ tout 3-cycle est conjugué dans A_n à son inverse.
Tout quotient abélien de A_n est trivial.
En particulier A_n (et donc S_n) n'est pas résoluble.

Démonstration. On sait que S_n est engendré par les transpositions, donc A_n par les produits de 2-transpositions.
Maintenant $(12)(23) = (123)$ est un trois cycle et
$(12)(34) = (12)(23)(23)(34) = (123)(234)$ est le produit de deux 3-cycles.

Notons que dans A_n le cycle (123) est conjugué à son inverse (123), en effet la permutation (23)(45) qui les conjugue est dans A_n.

Donc $A_n/[A_n, A_n]$ est un groupe abélien engendré par des éléments d'ordre 3 (les images des 3-cycles. Donc tout élément $\neq 1$ de $A_n/[A_n, A_n]$ est d'ordre 3. Mais dans A_n, $n \geqslant 5$, tout 3-cycle est conjugué à un son inverse, son image dans $A_n/[A_n, A_n]$ est égale à son inverse. Ainsi, dans $A_n/[A_n, A_n]$ un trois cycle satisfait $\sigma^3 = 1, \sigma = \sigma^{-1}$. Donc $\sigma = 1$. □

Remarque 4.14. En fait, on peut démontrer que A_n est un groupe simple.

4.4. Exercices

4.4.1. Section 3.1

Séparabilité

Exercice 4.1. Dans le corps $\mathbb{F}_p(t)$, démontrer que t n'est pas une puissance $p-i$ème. En déduire que $X^p - t$ est irréductible. Combien ce polynôme a-t-il de racines distinctes dans son corps de décomposition ?
Quel est le groupe d'automorphismes de ce corps de décomposition ?

Exercice 4.2. Soit $\mathbb{L}\colon\mathbb{K}$ une extension séparable. Démontrer que le degré $[\mathbb{L}\colon\mathbb{K}]$ est le maximum (ou le ppcm) des degrés des polynômes minimaux des éléments de $\mathbb{K}$.

Exercice 4.3. Soit $\mathbb{K}$ un corps de caractéristique $p \neq 0$, et soit f un polynôme irréductible dans $\mathbb{K}[X]$. Démontrer qu'il existe un polynôme G tel que $f(X) = g(X^{p^k})$, ou g est irréductible et **séparable**. En déduire que les multiplicités des racines de f dans un corps de décomposition sont des puissances de p.

Normalité

Exercice 4.4. Quelles extensions sont normales.

$\mathbb{Q}(\sqrt[7]{5})\colon\mathbb{Q}$
$\mathbb{Q}(\sqrt{-5})\colon\mathbb{Q}$
$\mathbb{Q}(\sqrt{5}, \alpha)\colon\mathbb{Q}(\alpha)$, où $\alpha = \sqrt[17]{11}$
$\mathbb{Q}(\sqrt{5}, \alpha)\colon\mathbb{Q}$, où $\alpha = \sqrt[17]{11}$
$\mathbb{R}(\sqrt{-17})\colon\mathbb{R}$

Exercice 4.5. Toute extension de degré 2 est normale.
Si G est un groupe, tout sous-groupe d'indice 2 est normal.
Donner un exemple d'une extension de degré 3 (ou même n) de $\mathbb{Q}$ qui n'est pas normale.

Exercice 4.6. Soit f un polynôme de degré n sur $\mathbb{K}$, et $\mathbb{L}$ un corps de décomposition. Montrer que $[\mathbb{L}\colon\mathbb{K}]$ divise $n!$. On pourra d'abord supposer que f est irréductible, et raisonner par récurrence.

Exercice 4.7. Soit $\mathbb{K}$ un corps de caractéristique $p > 0$. On considère le corps $\mathbb{E} = \mathbb{K}(U, V)$ des fractions rationnelles en les deux indéterminées U et V et le sous-corps $\mathbb{F} = \mathbb{K}(U^p, V^p)$.

Montrer que l'extension $\mathbb{E}/\mathbb{F}$ est de degré p^2 mais que chaque élément $x \in \mathbb{E} \setminus \mathbb{F}$ engendre un corps de degré p. (si $Q(U, V)$ est un polynôme on remarquera que $\frac{1}{Q(U,V)} = \frac{Q^{p-1}(U,V)}{Q_1(U^p, V^p)}$)

Cette extension est-elle monogène?

Si $\mathbb{K}$ est infini montrer qu'il existe une infinité de corps intermédiaires $\mathbb{L}$: $\mathbb{F} \subset \mathbb{L} \subset \mathbb{E}$.

4.4.2. Section 3.2

Exercice 4.8. Soit $f \in \mathbb{K}[X]$ un polynôme séparable irréductible de degré n, et $\mathbb{L}$ son=un corps de décomposition. On note $R = \{x_1, x_2, ..., x_n\}$ l'ensemble des racines de f dans $\mathbb{L}$. Démontrer le groupe $G = \mathrm{Gal}(\mathbb{L}\colon \mathbb{K})$ opère fidèlement et transitivement sur R.

On ne suppose plus f irréductible. Quelles sont les orbites du groupe de Galois.

Exercice 4.9. Soit $\mathbb{L}\colon \mathbb{K}$ le corps de décomposition d'un polynôme de degré 3 séparable irréductible de $\mathbb{K}[X]$, ou bien le degré de l'extension est 3 et le groupe de Galois est cyclique d'ordre 3, ou bien le degré est 6 et le groupe est le groupe de permutation des racines.

Exemple : Soient p et q deux nombres rationnels. On suppose que le polynôme $P(X) = X^3 + p\,X + q$ est irréductible sur $\mathbb{Q}$. Si x_1, x_2, x_3 sont les trois racines complexes, le *discriminant* de P est $\Delta = (x_1 - x_2)^2\,(x_1 - x_3)^2\,(x_2 - x_3)^2$.

Expliquer pourquoi Δ est un rationnel. En utilisant les relations entre coefficients et racines on peut calculer : $\Delta = -4\,p^3 - 27\,q^2$

Montrer que si l'extension est de degré 3 (resp. 6) alors Δ est (resp. n'est pas) le carré d'un élément de $\boldsymbol{Q}$.

Dans le premier cas expliquer pourquoi les trois racines sont nécessairement réelles.

Exercice 4.10. Soit $\mathbb{L}\colon \mathbb{K}$ le corps de décomposition d'un polynôme f de degré n séparable irréductible de $\mathbb{K}[X]$.Alors le groupe de Galois est un sous groupe du groupe de permutation des racines $\{x_1, ...x_n\}$ de f. Soit $\delta = \Pi_{i<j}(x_i - x_j)$.

Montrer que si $g \in \mathrm{Gal}(\mathbb{L}\colon \mathbb{K})$, $g(\delta) = \varepsilon(\sigma)\delta$, où ε est la signature.

Montrer que $\Delta = \Pi_{i\neq j}(x_i - x_j)$ est un élément de $\mathbb{K}$

Montrer que $\mathrm{Gal}(\mathbb{L}\colon \mathbb{K})$ est un sous groupe du groupe A_n si et seulement si Δ est un carré dans $\mathbb{K}$.

Exercice 4.11. Soit $\mathbb{K}$ de caractéristique $\neq 2$ et $\mathbb{L}$ une extension galoisienne de degré 4. Montrer que le groupe de Galois est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ si et seulement si il existe a et b dans $\mathbb{K}$ tels que $\mathbb{L} = \mathbb{K}\big[\sqrt{a}, \sqrt{b}\,\big]$

Donner un exemple où le groupe est au contraire isomorphe à $\mathbb{Z}/4\mathbb{Z}$. Dans les deux cas on déterminera les corps intermédiaires.

Exercice 4.12. Dans chacun des exemples suivants on note $\mathbb{K}$ le corps de décomposition du polynôme $P \in \mathbb{K}[X]$. Déterminer le groupe de Galois de $\mathbb{K}\colon \mathbb{F}$ et trouver tous les corps intermédiaires.

$\mathbb{F} = \mathbb{Q}$ et $P = X^4 - 7$
$\mathbb{F} = \mathbb{F}_5$ et $P = X^4 - 7$
$\mathbb{F} = \mathbb{F}_{11}$ et $P = X^4 - 7$
$\mathbb{F} = \mathbb{Q}$ et $P = X^5 - 2$
$\mathbb{F} = \mathbb{F}_2$ et $P = X^6 + 1$
$\mathbb{F} = \mathbb{Q}$ et $P = X^6 - 1$

Exercice 4.13. Soit $\mathbb{F}$ un corps, $\mathbb{K}\colon \mathbb{F}$ et $\mathbb{L}\colon \mathbb{F}$ deux extensions de degré fini contenues dans un même corps $\mathbb{E}$ extension de $\mathbb{F}$. On suppose que $\mathbb{K}\colon \mathbb{F}$ est normale (resp. séparable, resp. galoisienne). Montrer alors qu'il en est de même de $\mathbb{K}\mathbb{L}\colon \mathbb{L}$ où $\mathbb{K}\mathbb{L}$ désigne le plus petit sous-corps de $\mathbb{E}$ contenant $\mathbb{K}$ et $\mathbb{L}$.

Dans le cas d'une extension galoisienne $\mathbb{K}\colon \mathbb{F}$ définir un homomorphisme du groupe $\mathrm{Gal}(\mathbb{K}\mathbb{L}\colon \mathbb{L})$ vers $\mathrm{Gal}(\mathbb{K}\colon \mathbb{K} \cap \mathbb{L})$. Montrer que cet homomorphisme est injectif puis qu'il est surjectif.

On se place dans l'hypothèse où les deux extensions $\mathbb{K}:\mathbb{F}$ et $\mathbb{K}:\mathbb{F}$ sont galoisiennes. Définir un homomorphisme "naturel" ϕ du groupe de Galois $\mathrm{Gal}(\mathbb{K}\mathbb{L}:\mathbb{F})$ vers le produit $\mathrm{Gal}(\mathbb{K}:\mathbb{F})\times\mathrm{Gal}(\mathbb{K}:\mathbb{F})$. Montrer que ϕ est injectif. Si $\mathbb{K}\cap\mathbb{L}=\mathbb{F}$ montrer (en utilisant les résultats précédents) qu'il est surjectif.

4.4.3. Section 3.3

Exercice 4.14. En faisant opérer le groupe sur lui même par conjugaison, démontrer que le centre d'un groupe d'ordre p^n est non réduit à l'élément neutre e. En déduire que le groupe en question est nilpotent.

Exercice 4.15. Soit G un groupe opérant transitivement sur un ensemble fini E, et $N\lhd G$ un sous groupe normal de G. Montrer que toutes les orbites de N ont même cardinal. En déduire que si $|E|=p$ est un nombre premier, et que l'action de G sur E est fidèle (c'est à dire que si $\forall x, gx=x\Rightarrow g=e$) alors N est aussi transitif sur E. On suppose $G<S_p$ est un sous groupe résoluble qui est transitif sur $\{1,....p\}$. Démontrer qu'en fait G contient un sous groupe normal isomorphe à $(\mathbb{F}_p,+)$ engendré par un p cycle.

Montrer que $\mathrm{Aut}(\mathbb{F}_p,+)\approxeq\mathbb{F}_p^*,\times$

Montrer que si p est premier et S_p est résoluble alors $p=2,3$.

Montrer le groupe symétrique S_n est résoluble si et seulement si $n=2,3,4$.

Exercice 4.16. Soit $P(X)=X^5-14X+7$. Montrer que P est irréductible sur $\mathbb{Q}$ et a 3 racines réelles exactement.

Soit $\mathbb{K}$ le corps de décomposition de P sur $\mathbb{Q}$. montrer que $\mathbb{K}:\mathbb{Q}$ est divisible par 5.

Soit G le groupe de Galois de ce corps. montrer que $|G|$ est divisible par 5

On admet le théorème de Cauchy qui dit qu'alors G contient un élément d'ordre 5

Soit $G\subset S_5$ un sous groupe qui contient un élément d'ordre 2 et un 5 cycle. Montrer que $G=S_5$.

En déduire que le groupe de Galois de ce polynôme est S_5.

Exercice 4.17. Théorème de Cauchy. Si G est un groupe fini d'ordre n et p un nombre premier divise n, alors G contient un élément d'ordre p.

On considère l'ensemble X des p uplets $(a_1,...a_p)$ tels que $a_1....a_p=1$.

1. Montrer que $|X|=|G|^{p-1}$

2. On fait opérer $\mathbb{Z}/p\mathbb{Z}$ sur cet ensemble par permutation cyclique. Démontrer que le nombre de solution de l'équation $x^p=1$ est congru à 0 modulo p et en déduire que G a au moins un élément d'ordre p.

Chapitre 5

Un peu de géométrie algébrique.

Le point de vue des physiciens est que pour comprendre un objet, on l'observe et on regarde le résultat de l'observation. En terme mathématique, une observable est simplement une fonction f, à valeur dans $\mathbb{R}$ ou $\mathbb{C}$, définie à partir d'un ensemble X tout à fait inconnu (l'espace des phases) . L'ensemble des observables est réputé être une algèbre de fonctions car on peut ajouter deux telles fonctions, les multiplier, ou les multiplier par un scalaire, et l'espace X se comprend grâce à cet algèbre de fonction.

Par exemple, en thermodynamique un système particulier est bien déterminé par sa température, son volume, sa pression son entropie sa quantité de chaleur etc etc.

Nous allons voir que les courbes algébriques planes sont aussi des objets qu'on peut étudier grâce à leurs algèbres de fonctions.

Définition 5.1. *Une courbe algébrique plane C est l'ensemble des points du plan $\mathbb{C}^2$ définie par une équation $P(X,Y)=0$ ou $P\in\mathbb{C}[X,Y]$ est un polynôme.*

Exemple 5.1. Le cercle $X^2+Y^2-1=0$
La réunion de deux droites $XY=0$
La courbe elliptique $Y^2-X(X-1)(X-\lambda)=0$
La cubique à point double dite « crunodale » $Y^2-X^2(X+1)=0$
Le cusp $Y^2=X^3$

L'algèbre des fonctions sur une telle courbe est l'algèbre $\mathbb{C}[X,\,Y]$ des fonctions polynômes restreinte à C. Deux fonctions polynômes étant égale sur $\mathbb{C}$ si et seulement si leur différence y est nulle, il est naturel de considérer l'idéal $I_c=\{f\,/\,\forall(X,Y)\in C,\,f(X,Y)=0\}$ et l'anneau quotient $C[X,Y]\,/\,I_C$.

La question qui nous intéresse le plus est :

Quel est le rapport entre l'anneau $C[X,Y]\,/\,I_c$ et la courbe C.

Même si le cas des courbes nous suffit beaucoup de résultats se généralisent en toute dimension, quand on a non pas une mais plusieurs équations.

Définition 5.2. *Un ensemble algébrique affine est un sous ensemble de $\mathbb{C}^n$ qui est défini par une famille d'équations $P_\alpha(X)=0$, ou $X=(X_1...X_n)$ et $P_\alpha(X)\in\mathbb{C}[X_1,....X_n]$*

5.1. Ensemble algébrique affine.

Nous nous limiterons au cas des nombres complexes.

5.1.1. Définition, courbes et surfaces .

Soit $P\in\mathbb{C}[X_1,...X_n]$ un polynôme. L'hypersurface $V(P)$ est $\{X\,/\,P(X)=0\}$

Si $n=2$ $V(P)$ est une courbe algébrique plane, si $n=3$ une surface algébrique affine.

Soit $S \subset K[X_1, ...X_n]$ un sous ensemble. Le sous ensemble défini par par S est $V(S) = \cap_{F\in S}V(P)$, c'est un ensemble algébrique affine.

PROPOSITION 5.1.

1. *Si $I \subset K[X_1, ...X_n]$ est l'idéal engendré par S, $V(S)=V(I)$.*
2. *Si $(I_\alpha)_{\alpha\in A}$ est une famille de sous ensembles, $V(\cup_\alpha I_\alpha)=\cap_\alpha V(I_\alpha)$ donc l'intersection d'une famille d'ensembles algébriques l'est encore.*
3. *Si $I \subset J$ alors $V(J) \subset V(I)$*
4. *Si F, G sont deux polynômes, $V(FG)=V(F)\cup V(G)$*
5. *$V(X_1-a_1, X_2-a_2, ...X_n-a_n)$ est réduit au point $\{a_1, ...a_n\}$*
6. *Tout ensemble fini est algébrique.*

Démonstration. AQT □

5.1.2. Idéaux.

Si $X \subset \mathbb{C}^n$ est un ensemble, on peut former l'idéal $I(X)$ des polynômes qui s'annulent sur X

PROPOSITION 5.2. *Soit $S \subset \mathbb{C}[X_1, ...X_n]$ et $X \subset \mathbb{C}^n$*

1. *Si $X \subset Y$ alors $I(X) \subset I(Y)$*
2. *$I(\varnothing)=\mathbb{C}[X_1, ...X_n]$ et $I(\mathbb{C}^n)=0$*
3. *$I(V(S)) \supset S \quad V(I(X)) \supset X$*
4. *$V(I(V(S)))=V(S)$ et $I(V(I(X)))=I(X)$* □

Remarque 5.1. Si on remplace $\mathbb{C}^n$ par un corps fini, la second proposition devient fausse, pourquoi ?

PROPOSITION 5.3. *Si V est algébrique, alors $V=V(I(V))$. Si I est l'idéal d'un ensemble algébrique $V(I)$ alors $I=I(V(I))$* □

Un propriété intéressante de l'idéal d'un ensemble algébrique est qu'il est radical au sens suivant.

PROPOSITION 5.4. *Si $f^n \in I(X)$ alors $f \in I(X)$.* □

Exemple 5.2. L'idéal principal I^n engendré par X^n n'est pas radical, on a $V(I^n) = \{0\}$ et $I(V(I^n))=I$ l'idéal engendré par X.

5.1.3. Le théorème de la base de Hilbert : Anneaux noetheriens.

THÉORÈME 5.1. *Un ensemble algébrique est défini par un nombre fini d'équations.*

Pour démontrer ce résultat, nous partons d'un ensemble algébrique V défini par un système d'équation $S \subset K[X_1, ...X_n]$. Comme $V=I(X)$ pour démontrer notre résultat il suffit de démontrer que cet idéal est engendré par un nombre fini d'éléments.

DÉFINITION 5.3. *Un idéal est de type fini, si il est engendré par un nombre fini d'éléments.*

Cette définition est un peu moins forte que principal : un idéal est principal si il est engendré par un seul élément.

Proposition 5.5. *Les propositions sont équivalentes.*

i. Tout idéal est de type fini

ii. Toute suite croissante d'idéaux est stationnaire

iii. Tout sous ensemble non vide d'idéaux admet un élément maximal pour l'inclusion.

Démonstration. $i \Rightarrow ii$. Soit I_n une suite croissante d'idéaux. Leur réunion I est un idéal engendré par un nombre fini d'éléments. Tous ces éléments appartiennent à l'un des I_n, donc en fait $i = I_n$ et la suite est stationnaire.

$ii \Rightarrow iii$. On montre la contraposée. Considérons une ensemble d'idéaux qui n'admet pas d'élément maximal. On considère I_1 un idéal de cette famille. Comme il n'est pas maximal, il existe un élément I_2 le contenant strictement qui n'est pas maximal. Par récurrence on construit une suite strictement croissante et infinie d'idéaux.

$iii \Rightarrow i$ Soit I un idéal, pour tout partie fini $F \subset I$ on considère l'idéal I_F engendré. La famille des I_F admet un élément maximal. C'est I, car sinon on pourrait trouver un élément a de I tel que $a \notin I_F$. Alors $I_{F\cup\{a\}}$ serait alors un idéal strictement plus grand que I_F. □

Définition 5.4. *On dit qu'un anneau est noetherien*[5.1] *si il satisfait l'une des propriétés équivalents de la proposition 1.61.*

Exemple 5.3. Evidemment un anneau principal est noetherien, vu que tout idéal est engendré par un seul élément.

Un théorème important concernant les anneaux noetheriens est le théorème du transfert.

Théorème 5.2. *Théorème du transfert de Hilbert.*
Si A est noetherien, $A[X]$ aussi.

Corollaire 5.1. *Toute ensemble algébrique est défini par un nombre fini d'équations*

Remarque 5.2. En première lecture, on peut douter de l'intérêt de ce résultat, vu que les ensemble que nous étudions sont définis par une ou deux équations. Heureusement, il a d'autre applications.

On note $A_n[X]$ l'ensemble des polynômes de degré n.

Soit I un idéal de A. On regarde $I \cap A_n[X]$, et on pose $d_n(I)$ l'ensemble des coefficients de plus haut degré des éléments de $I \cap A_n[X]$. C'est évidemment un idéal de A

Notons que d'une part si $I \subset J$ $d_n(I) \subset d_n(J)$ d'autre part, $d_n(I) \subset d_{n+1}(I)$ car si $P \in A_n[X] \cap I$, $XP \in I \cap A_{n+1}[X]$.

Lemme 5.1. *Soit $I \subset J$. Alors $I = J$ équivaut à $\forall n,\ d_n(I) = d_n(J)$.*

Démonstration. On raisonne par l'absurde, c'est à dire qu'on suppose que $\forall n,\ d_n(I) = d_n(J)$, et on considère un polynôme de plus petit degré, disons d, P qui est dans I pas dans J. Par hypothèse, il existe un polynôme de même degré dans I ayant même coefficient dominant Q. Alors $P - Q$ est un polynôme de degré $<d$ qui est dans J et pas dans I contradiction. □

5.1. En hommage à Emmy Noether [1882-1935], mathématicienne allemande géniale. Inventrice en particulier de la théorie des idéaux, et en physique mathématique du principe d'invariance. Victime d'abord la la misogynie du milieu universitaire, elle n'aura le droit d'enseigner que très tard (1923) à l'université de Göttingen, victime des lois antisémites, elle en sera chassée par les nazis en 1933 à cause de ses origines.

Soit I_n une suite croissante d'idéaux de A. Pour chaque entier k fixé la suite $d_n(I_k)$ est croissante, donc stationnaire. Nous noterons n_k le plus petit entier tel que $d_m(I_k) = d_{n_k}(I_k)$

On a le schéma suivant d'inclusions horizontales et verticales

$$\begin{array}{lllllll}
d_0(I_1) & \to & d_1(I_1) & \ldots & \to & d_{n_1}(I_1) & \text{STOP} \\
 & & & & & \downarrow & \\
d_0(I_2) & & d_1(I_2) & \ldots & & d_{n_1}(I_2) \to & \ldots \quad d_{n_2}(I_2) \quad \text{STOP} \\
 & & & & & & \downarrow \\
 & & & & & & \downarrow \\
d_0(I_k) & & d_1(I_k) & \ldots & & d_{n_k-1}(I_k) & \ldots \quad d_{n_k}(I_k) \to \quad d_{n_k}(I_k) \\
 & & & & & & \text{STOP}
\end{array}$$

Par construction la suite des $d_{n_k}(I_k)$ est donc stationnaire, et il existe un entier k_0 à partir de laquelle elle reste constante. Pour $k \geqslant k_0$ et $i \leqslant k_0$ la suite des $d_i(I_k)$ est stationnaire aussi. Donc il existe un entier k_1 tel que pour $k \geqslant k_1$ la suite des idéaux $d_n(I_k)$ est constante égale à $d_n(I_{k_1})$. D'après lemme précédent la suite des idéaux est aussi constante. □

COROLLAIRE 5.2. *Si A est noetherien, l'anneau $A[X_1, ...X_n]$* est noetherien.

Exemple 5.4. Une variété algébrique affine est définie par un nombre fini d'équations $p_1(x, y) = \cdots = = p_n(x, y) = 0$

5.1.4. Les composantes irréductibles d'un ensemble algébrique.

Rappelons que $I(A \cup B) = I(A) \cap I(B)$.

Ceci est une façon compliquée de dire que si une fonction s'annule sur A et sur B alors elle s'annule sur A et elle s'annule sur B.

D'où la question : peut-on décomposer un ensemble algébrique en plusieurs ensembles et si oui combien.

DÉFINITION 5.5. *Un ensemble algébrique est irréductible si il n'est pas la réunion de deux ensembles algébriques distincts.*

PROPOSITION 5.6. *L'ensemble algébrique V est irréductible si et seulement si l'idéal $I(V)$ est premier.*

Démonstration. Si $I(V)$ n'est pas premier on peut trouver deux polynômes distincts F_1, F_2 qui ne sont pas dans $I(V)$ mais dont le produit y est. posons $V_1 = V \cap \{F_1 = 0\}$ $V_2 = V \cap \{F_2 = 0\}$ ces deux sous ensembles sont strictement inclus dans V sinon, $F_i \in I(V)$, et manifestement leur réunion est V

Si V est réductible $V = V_1 \cup V_2$ soit $F_1 \in I(V_1)$ mais pas à $I(V_2)$ et $F_2 \in I(V_2)$ mais pas à $I(V_1)$. Alors $F_1 F_2$ s'annule sur $V_1 \cup V_2$. □

LEMME 5.2. *Dans un anneau noetherien toute famille d'idéaux admet un élément maximal.*

Démonstration. Soit I_α une famille d'idéaux ne satisfaisant pas cette propreté. On construit par récurrence une suite d'idéaux strictement croissante. Donc l'anneau n'est pas noetherien. □

COROLLAIRE 5.3. *Toute famille d'ensemble algébriques admet un élément minimal pour l'inclusion.*

THÉORÈME 5.3. *Tout ensemble algébrique est réunion fini d'ensembles algébriques irréductibles $V = V_1 \cup \cdots \cup V_k$ tels que V_i n'est jamais contenu dans V_j.*

Démonstration. On raisonne par l'absurde et on considère l'ensemble des ensembles algébriques qui n'ont pas cette propriété. Il admet donc un élément minimal V. Comme V n'est pas irréductible, $V = V_1 \cup V_2$ union stricte. Mais $V_i \notin S$, donc V_i est une réunion d'ensemble irréductibles. Donc V aussi. On enlève le $V_{i,k}$ contenu dans un $V_{j,l}$ pour obtenir le résultat. □

5.1.5. Le cas des courbes planes

Théorème 5.4. *Petit Bézout.*
Soit F, G deux polynômes de $\mathbb{C}[X,Y]$ sans facteur commun. Alors l'ensemble $F=G=0$ est fini.

Démonstration. Le théorème de Bézout montre qu'il existe deux polynômes A, B dans $\mathbb{C}(X)[Y]$ tels que $AF + BG = 1$ En réduisant au même dénominateur P, on trouve des polynômes U, $V \in \mathbb{C}[X, Y]$ et $P \in \mathbb{C}[X]$ tel que que $P(X) = UF + BG$. Donc les abscisses des points de l'intersection sont des racines de P et sont en nombre fini. Par le même raisonnement les ordonnées des points de notre ensemble ne prennent qu'un nombre fini de valeurs. □

Remarque 5.3. Le vrai théorème de Bézout dit que le cardinal de cet ensemble est (au plus) $\deg(F) \times \deg(G)$, où $\deg(F)$ est le degré du théorème de plus haut degré total X^iY^j étant de degré $i + j$. Pour le démontrer, on se appelle que le résultant permet justement de dire des choses à ce sujet.

Théorème 5.5. *Soient F, G deux polynômes sans facteurs commun. Le nombre de points d'intersection des courbes $F=0, G=0$ est majoré par le produit des degrés de F et G.*

Démonstration. On considère les polynômes F, G comme étant des élément de l'anneau factoriel $\mathbb{C}[X][Y]$. On note $p_i = (x_i, y_i)$ leurs points d'intersections, et on suppose que les x_i sont distincts si $i \leqslant D$. (On s'y ramène en changeant de coordonnées, le cas échéant. On calcule le résultant $\rho_Y(F, G)$. C'est un polynôme de degré $d(F) \times d(G)$ en X qui s'annule pour tous les x_i. Comme il n'est pas nul, c'est que $D \leqslant d(F) \times d(G)$. □

Corollaire 5.4. *Si $F \in \mathbb{C}[X,Y]$ est irréductible, alors $I(F=0)) = (F)$.*

Démonstration. En effet si $F(X, Y) = 0$ est infini car $\mathbb{C}$ est algébriquement clos (vérifier en exercice). Si G s'annule sur cet ensemble infini, il est divisible par F. □

Corollaire 5.5. *Si V est un sous ensemble algébrique irréductible qui n'est pas réduit à un point et qui n'est pas tout le plan, alors il existe un polynôme irréductible tel que $V = \{F=0\}$*

Démonstration. En effet $I(V)$ contient un polynôme irréductible F alors $V \subset \{F=0\}$ et toute polynôme de $I(V)$ est divisible par F. □

5.1.6. Le Nullstellensatz de Hilbert

C'est un théorème très célèbre a qui on a donné un joli petit nom très poétique : « Nullstellensatz » ce qui veut dire « théorème sur le lieu des zéros ».

Théorème 5.6. *Soit I un idéal propre de $\mathbb{C}[X_1, ...X_n]$. Alors $V(I) \neq 0$*

C'est une forme forte du théorème de d'Alembert (tout polynôme s'annule quelque part.)

Théorème 5.7. *Mieux si I est un idéal maximal, il existe un point p tel que $I = I(p)$.*

5.1.6.1. Digression sur la clôture intégrale

La démonstration de ce résultat est basée sur le fait que l'anneau de polynôme à coefficient dans un corps est intégralement clos au sens suivant.

Définition 5.6.
Un élément x appartenant au corps k des fractions d'un anneau intègre A est dit entier si il existe un polynôme unitaire à coefficient dans A dont x est racine.

On dit que A est intégralement clos si tout entier de A est un élément de A.

THÉORÈME 5.8. *Soit R un anneau, A un sous anneau intègre et $x \in R$. On a équivalence entre*

i. x est entier sur A

ii. $A[x]$ est de type fini.

iii. Il existe une sous anneau B de R contenant A et x, de type fini sur A.

Démonstration. On a $i \Rightarrow$ ii car si $x^n = \Sigma_{i=0}^{n-i} a_i x^i$, toute les puissance de x sont dans le sous-module de R engendré par $1, ...x^{n-1}$. Pour $ii \Rightarrow iii$, faire $B = A[x]$.

L'implication $iii \Rightarrow i$ mérite d'être expliquée. On note $(y_1, ...y_n)$ des générateurs de B sur A ; ops $y_1 = 1$.

Il existe donc une matrice $A = (a_{ij})$ à coefficients dans A telle que, dans R on ait $x\begin{pmatrix} y_1 \\ \\ y_n \end{pmatrix} = A.\begin{pmatrix} y_1 \\ \\ y_n \end{pmatrix}$

Ou encore $(A - x\,\mathrm{Id})\begin{pmatrix} y_1 \\ \\ y_n \end{pmatrix} = 0$

La matrice $(A - x\,\mathrm{Id})$ a coefficient dans lm'anneau R a donc un noyau non nul (l'un des y_i est non nul). Et donc son déterminant est nul. Autrement dit x annule le polynôme de Cayley Hamilton de A, qui est un polynôme à coefficients entiers. □

PROPOSITION 5.7. *L'ensemble des entiers de A est un sous anneau de k.*

Démonstration. Si x et y sont dans A la sous-algèbre $A[x,\ y]$ est engendrée par les $x^i y^j$ .Comme x et y sont entiers, pour des entiers n, m bien choisi, les x^ket y^l sont des combinaisons linéaires à coefficients dans A des x^i et y^j, $i \leqslant n, j \leqslant m$. Donc cette sous algèbre est en fait engendrée par les $x^i y^j$ pour $i, j \leqslant n, m$, et le théorème précédent s'applique.

□

PROPOSITION 5.8. *Si A et intègre principal, alors A est intégralement clos.*

Démonstration. On raisonne par l'absurde. Sinon, il existe un élément de k et un polynôme unitaire $P = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + X^n$ qui a un zéro $x = \frac{p}{q}$ (écriture irréductible) dans k qui n'est pas dans A. On développe, il vient $a_0 q^n + a_1 q^{n-1} p + \cdots + a_{n-1} q p^{n-1} = -p^n$. Donc q divise p^n et donc q divise p, contradiction. □

5.1.6.2. Démonstration du théorème

Pour se simplifier la vie, nous allons faire le cas $n = 2$. Le quotient $\mathbb{C}[X, Y]/I = \mathbb{K}$ est un corps. C'est une extension de $\mathbb{C}$ engendrée comme anneau par deux éléments x, y.

Deux deux choses l'une, soit y est algébrique soit il est transcendant.

Si il est algébrique, c'est un élément y de $\mathbb{C}$ vu que $\mathbb{C}$ est algébriquement clos. Donc notre corps $\mathbb{K}$ est engendré par un seul élément (l'image de X) comme anneau. Le noyau de $\mathbb{C}[X] \twoheadrightarrow k$ est un idéal premier, donc x est algébrique et $x \in \mathbb{C}$. Il en résulte que le noyau contient les polynômes $X - x$ et $Y - y$. Mais l'idéal engendré par ces deux polynômes est maximal. Donc c'est I et $V(I) = (x, y)$.

Supposons donc l'image y de Y transcendant. Le corps $\mathbb{K}$ contient un sous corps $\mathbb{C}(y)$ isomorphe à $\mathbb{C}(Y)$. On a donc un homomorphisme surjectif de l'anneau $\mathbb{C}(y)[X]$ vers $\mathbb{K}$. Cet homomorphisme n'est pas injectif car $\mathbb{C}(y)[X]$ n'est pas un corps. Il y a donc un polynôme unitaire à coefficients dans $C(y)$ dont x est racine, disons $x^n + r_1 x^{n-1} + \cdots + r_n = 0$ ou $r_n \in \mathbb{C}(y)$. Soit d le produit des dénominateurs de ces fractions rationnelles supposé unitaire. On multiplie par d^n et on obtient $(dx)^n + a_1(dx)^{n-1} + \cdots + a_n = 0$. Ainsi $d(y)x$ appartient à la clôture intégrale de $\mathbb{C}[y]$ dans $\mathbb{K}$.

Soit $z = \Sigma_{i=1}^k p_i(y)x^i$. alors $d^k z = \Sigma_{i=1}^k q_i(y)(dx)^i$ est aussi dans la clôture intégrale de $\mathbb{C}[y]$. On applique ça à $\frac{1}{y} : \frac{d^k}{y}$ est entier sur $\mathbb{C}[y]$. Il existe donc des polynômes $a_1 .... a_n$ tels que $\frac{d^{nk}}{y^k} + a_1 \frac{d^{n(k-1)}}{y^{k-1}} + . + a_n = 0$ dans $\mathbb{C}(y)$, ce qui n'est pas possible vu que cette fraction rationnelle est $\frac{1}{y^k} + \Sigma_{i=-l+1}^j a_l y^l$ manifestement non nulle.

5.2. Exercices.

Exercice 5.1. Un sous ensemble de $\mathbb{C}$ est algébrique si et seulement si il est fini.

Exercice 5.2. soit $\gamma : \mathbb{C} \to \mathbb{C}^3$ la courbe $\gamma(T) = (T, T^2, T^3)$. Démontrer que son image est algébrique.
Le graphe de la fonction exponentielle n'est pas un sous ensemble algébrique de $\mathbb{C}^2$ (utiliser 1).

Exercice 5.3. Soient V, W deux ensembles algébriques. Montrer que $V = W$ équivaut à $I(V) = I(W)$. Ou utilise t on algébrique ?

Exercice 5.4. Soit V un ensemble algébrique, et $P \notin V$. Démontrer qu'il existe un polynôme $F \in I(V)$ tel que $F(P) = 1$ et $F(Q) = 0$ si $Q \in V$ (indication $I(V) \supsetneq I(V \cup P)$. On pourra commencer dans $\mathbb{C}^2$ en supposant $P = (0, 0)$.
Soient $P_1, ...P_m \in \mathbb{C}^n$ démontrer qu'il existe des polynômes F_i tel que $F_j(P_i) = \delta_{i,j}$ ($=0$ si $i \neq j, =1$ si $i = j$)
Soit Soit V un ensemble algébrique et $P_1, P_2 \notin V$. Démontrer qu'il existe $F \in I(V)$ tel que $F(P_i) \neq 0$. On pourra considérer $F_i \in I$ tel que $F_i(P_i) = 1$ et chercher une combinaison de F_1 et F_2.

Exercice 5.5. Soit $p \in \mathbb{C}^n$ un point. L'idéal $I(p) \subset \mathbb{C}[X_1, ...X_n]$ des fonctions qui s'annulent en p est maximal. Quel est le quotient.?
Soit $F \in \mathbb{C}[X_1, ...X_n]$. L'idéal (F) engendré par F n'est pas maximal.
**Soient $F_1, ...F_k \in \mathbb{C}[X_1, ...X_n]$. On suppose $k < n$. L'idéal $(F_1, ...F_k)$ n'est pas maximal.

Exercice 5.6. Soit A l'anneau des fonction entières sur $\mathbb{C}$. En utilisant la fonction $f(z) = e^{2i\pi z} - 1$, construire une suite f_n de fonction qui s'annulent sur $\{z \in \mathbb{N} / z \geqslant k\}$ mais pas sur $\{z \in \mathbb{N}0 \leqslant z < k\}$. En déduire qu'il existe un idéal qui n'est pas de type fini.
Soit $A = \mathbb{K}[X_1, X_2, ...]$ un anneau de polynôme sur une infinité de variable. Construire un idéal qui n'est pas de type fini.

Exercice 5.7. Tout quotient d'un anneau noetherien est noetherien.

Exercice 5.8. La décomposition d'un ensemble algébrique en composantes irréductibles est unique. On pourra raisonner en considérant deux décompositions $V_1 \cup \cdots \cup V_n = W_1 \cup \cdots \cup W_m$ en ensembles irréductibles tels que $V_i \not\subset V_j$ et pareil pour $W_i \not\subset W_j$. Montrer que pour tout i il existe j tel que $V_i \subset W_j$ et conclure.

Exercice 5.9. Démontrer que la parabole $\Pi = \{Y - X^2 = 0\}$ est irréductible, et que $I(\Pi) = (Y - X^2)\mathbb{C}[X, Y]$

Problème 5.1. Le théorème de Pascal.

Dans ce problème on fixe un corps $\mathbb{K}$.

1. Courbes planes.

Question 1. L'espace vectoriel $\mathbb{K}_d[X, Y]$ des polynômes de degré inférieur ou égal à d est un espace de dimension $\frac{(d+1)(d+2)}{2}$.

Si P est un polynôme de degré égal à d, on note $\mathcal{P}$ la courbe plane $\{P(X, Y) = 0\}$. Une conique est une courbe de degré 2. On dit qu'elle est non dégénérée si elle est définie par un polynôme irréductible.

Question 2. Si une conique est dégénérée, c'est la réunion de deux droites (éventuellement confondue).

Question 3. Soit $p_1, ...p_k$ k points du plan. Le sous espace de $\mathbb{K}_d[X,Y]$ formé des polynômes tels que $P(p_i)=0$ est de dimension au moins $\frac{(d+1)(d+2)}{2} - p$

Question 4. Par 5 points passe une conique, par 9 points passe une cubique.

Question 5. Soient P et Q des polynôme de $\mathbb{K}[X,Y]$ degré d et e respectivement. Le théorème de Bézout affirme que si P et Q sont irréductibles et distincts $\mathcal{P} \cap \mathcal{Q}$ a au plus $d.e$ points. En déduire que si P est irréductible et $\mathcal{P} \cap \mathcal{Q}$ a plus que de points, alors P divise Q.

Question 6. Si une conique et une cubique se rencontrent en 7 points, alors la cubique est la réunion de cette conique et d'une droite.

2. Le théorème de Pascal.

Une conique non dégénérée du plan est juste l'ensemble $\mathcal{E} = \{E(X,Y)=0\}$, où E est un polynôme de degré 2 irréductible en ces deux variables.

Soit a, b, c, a', b', c' 6 points sur une conique non dégénérée. On note u, v, w les points d'intersections des droites $u = (bc') \cap (c'b)$, $v = (ac') \cap (a'c)$ $w = (ab') \cap (ba')$. Nus alons démontrer un résultat célèbre :

Théorème de Pascal. L*es points* u, v, w *sont alignés.*

Question 7. Soit P un polynôme de degré 3. Démontrer (utiliser la première partie) que si P n'est pas divisible par E, alors l'intersection de $\{P=0\} \cap \{E=0\}$ au au plus 6 points.

Si x, y sont deux points du plan, on note (xy) un polynôme de degré 1 qui est l'équation de la droite passant par x et y.

Soit $F = (ab')(bc')(ca')$ le polynôme de degré 3 (cubique) qui et le produit de ces trois polynômes de degré 1. Et $G = (a'b)(b'c)(c'a)$ son petit frère.

Question 8. En utilisant le fait que $E=0$ est un ensemble infini, montrer qu'il existe un point de E disons p tel que $F(p) \neq 0$.

Posons alors $\lambda = \frac{G(p)}{F(p)}$ de sorte que $H = G - \lambda F$ est un polynôme de degré 3.

Question 9. Montrer que l'intersection $H=0 \cap E=0$ a au moins 7 points, et en déduire que $\mathcal{H} = \{H=0\}$ est la réunion de $\mathcal{E}$ et d'une droite. Puis démontrer le théorème de Pascal.