THÉORIE DE GALOIS ET RÉDUCTION MODULO p

MERCEDES HAIECH
ENCADRÉE PAR FABRICE ORGOGOZO
CMLS

Table des matières

Introduction 2
1. Préliminaires 2
1.1. Corps et extension de corps 2
1.2. Corps de rupture, de décomposition et clôture algébrique 4
1.3. Extensions normales et séparables 10
1.4. Le groupe de Galois 12
2. Théorème de Dedekind 15
2.1. Le polynôme $s_u(y)$ et quelques propriétés 15
2.2. Le théorème de Dedekind, première démonstration 17
2.3. Le théorème de Dedekind, deuxième démonstration 19
2.4. Théorèmes sur les modules 19
3. Théorème de Van der Waerden 23
3.1. Existence de polynômes irréductibles dans $\mathbf{F}_p[X]$ 23
3.2. Polynômes de groupe de Galois maximal 25
3.3. Théorème de Van der Waerden 26
4. Intermède : fonction zêta de Dedekind 27
4.1. Norme d'un idéal 27
4.2. Fonction zêta de Dedekind 31
5. Théorème de Frobenius 31
5.1. Résultats préliminaires 31
5.2. Théorème de Frobenius 35
Annexe A. Polynômes symétriques et discriminant 38
Références 39

Dans toute la suite du document, les anneaux seront supposés unitaires et commutatifs.

Introduction

Le présent document s'intéresse à divers théorèmes dans le cadre de la théorie de Galois qui traitent des liens entre le groupe de Galois d'un polynôme sur $\mathbf{Q}$, et celui de ce même polynôme sur les différents corps finis $\mathbf{F}_p$.

La partie 1 constitue une introduction aux extensions de corps et à la théorie de Galois. Nous survolerons la théorie assez rapidement, le but étant d'introduire les définitions nécessaires pour la compréhension de la suite du document.

La partie 2 énonce et démontre le théorème de Dedekind. Ce dernier montre que le groupe de Galois d'un polynôme sur le corps fini $\mathbf{F}_p$ est inclus, *en un certain sens*, dans le groupe de Galois de son relèvement sur $\mathbf{Q}$.

La partie 3 traite de l'abondance des polynômes de groupe de Galois maximal, ce qui est essentiellement l'objet du théorème de Van der Waerden.

La partie 4 forme un intermède analytique qui introduit quelques propriétés des fonctions zêta utiles pour démontrer le théorème de la partie 5.

Enfin la partie 5 forme une sorte de réciproque au théorème de Dedekind. Le théorème de Frobenius énonce que l'ensemble des nombres premiers p tels que, étant donné σ dans le groupe de Galois du polynôme f sur $\mathbf{Q}$ le groupe de Galois de f sur $\mathbf{F}_p$ possède un élément de type σ, a une certaine densité analytique.

Une partie annexe regroupe quelques définitions sur la notion de discriminant.

Dans la mesure du possible nous avons essayé de démontrer tous les théorèmes énoncés. Néanmoins, pour ne pas trop alourdir le présent rapport, nous avons simplement donné des références pour certains théorèmes classiques.

Enfin, je me tenais à remercier mon maître de stage Fabrice Orgogozo, ainsi que le CMLS (Centre de mathématiques Laurent Schwartz) situé à l'école Polytechnique, pour m'avoir accueilli pendant plus d'un mois dans un lieu à l'ambiance fort sympathique. Les théorèmes de Van der Waerden (en partie) et de Frobenius (intégralement) sont repris de documents non publiés écrit par M. Orgogozo.

1. Préliminaires

1.1. **Corps et extension de corps.** Rappelons qu'un corps est la donnée d'un ensemble k muni de deux lois de composition interne notées $+$ et $\times$ vérifiant les propriétés suivantes :

- L'ensemble k muni de ses deux lois $+$ et $\times$ est un anneau unitaire commutatif.
- Tous les éléments de k possèdent un inverse pour la loi $\times$.

Définition 1.1.1 (Extension de corps)**.** Soient k et K deux corps, et $\varphi\colon k \to K$ un morphisme d'anneaux. On dit que K est une extension du corps k via φ.

Une telle extension se note en général K/k et on se permettra l'abus de notation consistant à oublier le morphisme φ.

Proposition 1.1.2. *Soit K un corps, A un anneau et $\varphi\colon K \to A$ un morphisme d'anneaux. Alors le morphisme φ est injectif.*

Démonstration. Soit $x \in \mathrm{Ker}(\varphi)$. Raisonnons par l'absurde et supposons que $x \neq 0$. Alors il existe $y \in K$ tel que $xy = 1$. Donc $\varphi(xy) = \varphi(x)\varphi(y) = 1$. Donc $\varphi(x)$ est inversible dans l'anneau A, ce qui est absurde. Donc $x = 0$.

Ainsi, le morphisme φ est injectif. □

Remarque 1. La proposition précédente rend légitime l'identification entre k et son image $\varphi(k) = \{\varphi(a), a \in k\} \subset K$.

Exemple 1.1.3. Le corps $\mathbf{C}$ est une extension de $\mathbf{R}$.

Une extension de corps K/k est naturellement munie d'une structure de k-espace vectoriel. Lorsque cette dimension est finie, on dit que K est une extension finie de k.

Définition 1.1.4. La dimension $\dim_k(K) = [K : k]$ est appelée le **degré de l'extension**.

Proposition 1.1.5 (Tour d'extensions)**.** *Soient K/k et L/K deux extensions finies. Alors l'extension L/k est finie de degré $[L : k] = [L : K][K : k]$.*

Démonstration. Soit $e_1, \ldots, e_n$ une base de K sur k, et $f_1, \ldots, f_m$ une base de L sur K. Un élément x de L s'écrit de manière unique sous la forme $\sum_{j=1}^{m} \lambda_j f_j$, où les λ_j sont dans K. De même, chaque λ_j s'écrit de manière unique sous la forme $\sum v_{i,j} e_i$ où les $v_{i,j}$ sont dans k. Finalement, x s'écrit de façon unique sous la forme $x = \sum_{i,j} v_{i,j} e_i f_j$, comme combinaison linéaire à coefficients dans k des $e_i f_j$, où (i, j) parcourt $\{1, \ldots, n\} \times \{1, \ldots, m\}$. □

Définition 1.1.6 (Extension algébrique)**.** Soit K/k une extension de corps. Un élément $a \in K$ est dit algébrique sur le corps k si l'extension $k(a)/k$ est finie, sinon l'élément a est dit transcendant sur k. Une extension K/k est dite algébrique si tous ses éléments sont algébriques sur k.

Remarque 2. Une définition équivalente revient à considérer le morphisme $\varphi\colon k[X] \to K$ d'évaluation en x. L'élément x est dit transcendant si φ est injectif, et algébrique sinon.

Exemple 1.1.7. Le morphisme $\varphi\colon \mathbf{Q}[X] \to \mathbf{R}$, qui à un polynôme associe sa valeur en $\sqrt{2}$ n'est pas injectif. En effet, son noyau est l'idéal engendré dans $\mathbf{Q}[X]$ par le polynôme $X^2 - 2$. Ainsi le réel $\sqrt{2}$ est algébrique sur $\mathbf{Q}$.

Proposition 1.1.8. *Soit K/k une extension de corps. Un élément $x \in K$ est algébrique sur k si et seulement si il existe un polynôme P non nul, à coefficients dans k, tel que $P(x) = 0$.*

Démonstration. Supposons l'extension $k(x)/k$ finie, notons d son degré. La famille $\{1, x, x^2, \ldots, x^d\}$ est composée de $d+1$ éléments, elle est donc liée. Donc il existe $P \in k[X]$ tel que $P(x) = 0$.

Réciproquement, s'il existe un tel polynôme de degré d. On montre par récurrence que $\mathrm{Vect}(1, x, \ldots, x^n) = \mathrm{Vect}(1, x, \ldots, x^{d-1})$, pour tout $n \geqslant d$. Pour chaque élément $y \in k(x)$, il existe $n \in \mathbf{N}$ tel que $y \in \mathrm{Vect}(x^1, \ldots, x^n) = \mathrm{Vect}(1, x, \ldots, x^{d-1})$. Donc l'extension $k(x)/k$ est finie. □

Proposition 1.1.9. *Soit K/k une extension de degré fini. Alors K/k est une extension algébrique.*

Démonstration. Montrons que tout élément de K est algébrique sur k. Soit $x \in K$, et notons $[K : k] = n$. Alors la famille $\{1, x, \ldots, x^n\}$ est liée, donc il existe un polynôme $P \in k[X]$ tel que $P(x) = 0$. Donc l'élément x est algébrique sur k. Donc K/k est une extension algébrique. □

Proposition 1.1.10. *Soit K/k une extension. L'ensemble des éléments algébriques de K sur k est un sous-corps de K.*

Démonstration. Soient $x, y \in K$ deux éléments algébriques sur k, de sorte que les extensions $k(x)/k$ et $k(x)(y)/k(x)$ soient finies. La deuxième extension est finie, grâce à la proposition 1.1.8, car comme il existe un polynôme à coefficients dans $k[X]$ qui annule y, il en existe *a fortiori* un dans $k(x)[X]$. Par la proposition 1.1.5, l'extension $k(x, y)/k$ est finie, donc $x + y$ et xy sont des éléments algébriques. Par ailleurs si $x \in K$ est un élément algébrique sur k, montrons qu'il en va de même pour son inverse x^{-1}. Soit $P \in k[X]$ un polynôme annulateur de x. Alors le polynôme $Q(X) = X^{\deg(P)} P(1/X) \in k[X]$ est annulateur de x^{-1}. □

Définition 1.1.11. L'ensemble précédent est parfois appelé clôture algébrique de k dans K.

1.2. **Corps de rupture, de décomposition et clôture algébrique.**

1.2.1. *Corps de rupture.* Il existe des corps dans lesquels certains polynômes, à coefficients dans ce corps, n'admettent pas de racines. Nous allons voir qu'il est alors possible de construire des corps plus "grands", en un certain sens, en y adjoignant des racines de polynômes.

Exemple 1.2.1. Soit $f := X^2 + X + 1$ un polynôme de $\mathbf{F}_2[X]$. Le polynôme f ne s'annule en aucun des deux éléments de $\mathbf{F}_2$.

On va maintenant voir une construction qui servira souvent dans la suite. Étant donné un corps k et un polynôme non constant $f \in k[X]$, on construit $k[X]/(f(X))$ l'anneau quotient. Nous noterons k_f cet anneau.

Proposition 1.2.2. *L'anneau quotient $k[X]/(f(X))$ contient une racine du polynôme f.*

Démonstration. On note x l'image de X dans l'anneau quotient, par la surjection canonique : $\varphi_f \colon k[X] \twoheadrightarrow k_f$. Un calcul montre alors que : $f(x) =$

$f(\varphi(X)) = \varphi(f(X)) = 0$, car le polynôme f est envoyé sur l'élément nul dans l'anneau k_f. □

Proposition 1.2.3. *L'anneau quotient k_f se surjecte sur un corps.*

Démonstration. L'anneau k_f étant non nul, il contient, d'après le théorème de Krull, un idéal maximal, noté $\mathfrak{M}$. L'ensemble quotient $k_f/\mathfrak{M}$ est donc un corps sur lequel k_f se surjecte. □

Remarque 3. Le corps $k_f/\mathfrak{M}$ contient aussi une racine du polynôme f.

Proposition 1.2.4. *Soit k un corps, et f un polynôme non constant de $k[X]$. Il existe une extension finie K/k telle que f possède une racine dans K et que K/k soit engendrée par cette racine.*

Démonstration. Quitte à diviser par le coefficient dominant, on peut supposer le polynôme f unitaire. Le morphisme déduit des propositions 1.2.2 et 1.2.3 : $\varphi\colon k \to k[X] \twoheadrightarrow k_f \twoheadrightarrow k_f/\mathfrak{M}$ montre que l'ensemble $(k_f/\mathfrak{M})/k := K$ est une extension du corps k qui contient une racine de f, notée α. Puisque l'anneau k_f vu comme k-algèbre est engendré par x, alors le corps K est engendré par α. □

Définition 1.2.5 (Corps de rupture)**.** Soit k un corps, et f un polynôme non constant à coefficients dans k. Alors un corps K vérifiant la propriété de la proposition 1.2.4 est appelé *corps de rupture* du polynôme f.

Remarque 4. Le degré de l'extension $[K : k]$ est majoré par le degré du polynôme f. En effet, la famille $\{1, \alpha, \ldots, \alpha_{\deg(f)}\}$ est une famille liée dans K, car $f(\alpha) = 0$.

Proposition 1.2.6. *Soit k un corps, et f un polynôme non constant à coefficients dans k. Si le polynôme f est irréductible sur k, alors l'anneau k_f est un corps.*

Démonstration. Le polynôme f étant irréductible, alors l'idéal $(f(X))$ est premier car l'anneau $k[X]$ est factoriel. Comme cet anneau est aussi principal, alors l'idéal $(f(X))$ est maximal. Donc l'ensemble quotient k_f est un corps. □

Exemple 1.2.7. Un corps de rupture du polynôme $X^3 + 1$ est isomorphe à $\mathbf{Q}[\sqrt[3]{2}]$, ou encore $\mathbf{Q}[j\sqrt[3]{2}]$.

1.2.2. *Corps de décomposition.*

Proposition 1.2.8. *Soit k un corps, et f un polynôme unitaire non constant à coefficients dans k.*

(1) Il existe une extension K/k telle que le polynôme f se décompose sous la forme $\prod_{i=1}^{\deg(f)} (X - \alpha_i)$ avec $\alpha_i \in K$. Et telle que K soit engendré par les α_i sur k.

(2) Deux telles extensions sont isomorphes de degré au plus $\deg(f)!$

Définition 1.2.9 (Corps de décomposition)**.** Soit k un corps, et f un polynôme non constant à coefficients dans k. Une extension K/k vérifiant la propriété (1) précédente est appelée *corps de décomposition* de f sur k, noté éventuellement $\mathcal{D}_k(f)$.

Démonstration. Existence. Soit $d = \deg(f)$; on procède par récurrence sur le degré de f. Si le polynôme f est de degré 1, le résultat est immédiat, et $K = k$ convient. Pour un polynôme f de degré $d+1$, on considère le corps de rupture K_0 du polynôme f. D'après la proposition 1.2.4 et la remarque 4, l'extension est de degré au plus $d+1$, et le polynôme f y possède une racine. Dans K_0, le polynôme f se décompose sous la forme $(X-\alpha)g$, où $\alpha \in K_0$ et g est un polynôme de $K_0[X]$ de degré d. On applique l'hypothèse de récurrence à g, il existe donc une extension K/K_0 de degré au plus $d!$ telle que g soit scindé dans K. Donc le polynôme f est scindé sur le corps K. De plus, par la proposition 1.1.5, on a aussi $[K:k] = [K:K_0][K_0:k] \leqslant (d+1) \times d! = (d+1)!$. Enfin, le corps K_0 est engendré par une racine de f sur k, et K est engendré sur K_0 par les racines de g. Donc le corps K est engendré par les racines de f.

Unicité. Se référer au théorème suivant 1.2.10 avec $k_1 = k_2 = k$ et $\varphi = \mathrm{Id}$. □

Afin de démontrer l'unicité, nous allons avoir besoin de nous intéresser à un théorème d'extension des isomorphismes.

Théorème 1.2.10 (Extension des isomorphismes)**.** *Soit k_1, k_2 deux corps, et φ un isomorphisme de k_1 sur k_2. Soit g un polynôme à coefficients dans k_1 de degré supérieur ou égal à 1, et K_1 un corps de décomposition de g sur k_1. Soit K_2 un corps de décomposition de $\varphi(g)$ sur k_2. Alors il existe un isomorphisme de K_1 sur K_2 qui prolonge l'homomorphisme φ.*

Nous utiliserons la notation $\varphi(g) \in k_2[X]$ pour désigner le polynôme g dont les coefficients ont été évalué *via* l'homomorphisme φ.

Démonstration. Nous allons procéder par récurrence sur le degré de l'extension $[K_1 : k_1] = n$. Si $n = 1$, alors $K_1 = k_1$, et comme le polynôme g est alors scindé sur k_1, le polynôme $\varphi(g)$ est aussi scindé sur k_2, d'où $K_2 = k_2$, et le résultat est vrai. Supposons donc $n > 1$. Dans ce cas les racines de g ne sont pas toutes dans K_1, et le polynôme g possède alors un facteur irréductible h de degré d strictement supérieur à 1. Soit α une racine du polynôme h dans K_1. Le polynôme $\varphi(h)$ est aussi irréductible de degré d et l'élément $\beta = \varphi(\alpha)$ est racine de $\varphi(h)$ dans K_2. Nous allons maintenant définir un isomorphisme σ entre $k_1(\alpha)$ et $k_2(\beta)$ qui prolonge φ en posant, pour tous $(a_i)_{0 \leqslant k \leqslant d-1} \in k_1^{d-1}$

$$\sigma\Big(\sum_{0 \leqslant k \leqslant d-1} a_k \alpha^k\Big) = \sum_{0 \leqslant k \leqslant d-1} \varphi(a_k)\beta^k.$$

Montrons que le morphisme σ est bien défini, et supposons que l'on ait

$$\sum_{0\leqslant k\leqslant d-1} a_k\alpha^k = \sum_{0\leqslant k\leqslant d-1} b_k\alpha^k.$$

Alors le polynôme h, puisqu'il est irréductible sur k_1, divise le polynôme $\sum_{0\leqslant k\leqslant d-1}(a_k - b_k)X^k$, puisque ce dernier possède α comme racine. Ce qui implique que $\sigma(h)$ divise $\sigma(\sum_{0\leqslant k\leqslant d-1}(a_k - b_k)X^k) = \sum_{0\leqslant k\leqslant d-1}\varphi(a_k - b_k)X^k$, d'où l'égalité

$$\sum_{0\leqslant k\leqslant d-1}\varphi(a_k - b_k)\beta^k = 0$$

Il est alors immédiat de vérifier que σ est un isomorphisme entre $k_1(\alpha)$ et $k_2(\beta)$ qui prolonge φ, son inverse étant défini, pour tous $b_k \in k_2$, par

$$\sigma^{-1}(\sum_{0\leqslant k\leqslant d-1} b_k\beta^k) = \sum_{0\leqslant k\leqslant d-1}\varphi^{-1}(b_k)\alpha^k$$

Mais on a maintenant $[K_1 : k_1(\alpha)] = n/d < n$. On peut donc appliquer l'hypothèse de récurrence, et il existe un isomorphisme ψ entre K_1 et K_2 qui prolonge σ. En particulier ψ prolonge φ ce qui démontre la proposition.

□

Exemple 1.2.11. Un corps de décomposition du polynôme $X^3 + 1$ est isomorphe à $\mathbf{Q}[\sqrt[3]{2}, j\sqrt[3]{2}]$.

1.2.3. *Clôture algébrique.*

Définition 1.2.12. Soit K un corps. On dit que K est algébriquement clos, si tout polynôme non constant sur $K[X]$ est scindé.

Proposition 1.2.13. *Soit K un corps. Les propositions suivantes sont équivalentes :*

(1) Tout polynôme non constant de $K[X]$ admet une racine dans K

(2) Tout polynôme non constant de $K[X]$ est scindé sur K.

(3) Toute extension algébrique de K est de degré 1.

Démonstration. (2) ⇒ (1) est évident. On suppose (1), et soit f un polynôme non constant de $K[X]$. Procédons par récurrence sur le degré de f. Si f est de degré 1, il admet une racine dans K et il est scindé sur K. On suppose désormais que f est de degré $d + 1 \geqslant 2$. Par hypothèse f admet une racine dans K, donc f se décompose sous la forme $(X - \alpha)\cdot g$, où $\alpha \in K$, et g un polynôme de $K[X]$. Le polynôme g est non constant de degré strictement inférieur à $d + 1$, on lui applique donc l'hypothèse de récurrence, il est donc scindé sur K. Donc f est scindé sur K. Donc (2) ⇔ (1).

On suppose (3). Soit f un polynôme non constant de $K[X]$. Un corps de décomposition de f sur K, noté $\mathcal{D}_K(f)$ est une extension algébrique de k car de degré fini par la proposition 1.1.9. Donc c'est une extension algébrique de

degré 1, ce qui implique $\mathcal{D}_K(f) = K$. Donc le polynôme f est scindé sur K. Ainsi (3) $\Rightarrow$ (2).

Réciproquement, on suppose (2). Soit L une extension algébrique de K. Soit $x \in L$. Comme l'extension L/K est algébrique, il existe un polynôme non constant $f \in K[X]$ tel que $f(x) = 0$. Par hypothèse ce polynôme est scindé dans K. Donc $x \in K$. Donc $L \subset K$. L'extension L/K est donc de degré 1. (3) $\Leftrightarrow$ (2) □

Définition 1.2.14. Soit k un corps. On appelle clôture algébrique de k toute extension algébrique K de k telle que tout polynôme non constant à coefficients dans K admette une racine dans K.

Théorème 1.2.15. *Soit k un corps. Alors k admet une clôture algébrique.*

Démonstration. (Artin) *On va construire dans un premier temps une extension E_1/k telle que tout polynôme non constant de $k[X]$ possède une racine dans E_1.*

À tout polynôme non constant $f \in k[X]$, on lui associe une variable X_f, et on appelle S l'ensemble de ces variables. Ainsi l'ensemble S est en bijection avec l'ensemble des polynômes non constants de $k[X]$. On considère l'anneau de polynômes $k[S]$ [1], ainsi que l'idéal de $k[S]$ engendré par tous les polynômes non constants $f(X_f)$. Ce n'est pas l'idéal unité, car sinon, il existerait une combinaison finie d'éléments dans notre idéal telle que :

$$g_1 f_1(X_{f_1}) + \ldots + g_n f_n(X_{f_n}) = 1$$

avec $g_i \in k[S]$. Pour simplifier la notation, nous noterons X_i pour X_{f_i}. Les polynômes g_i ne, font intervenir qu'un nombre fini de variables, disons $X_1, \ldots, X_N$. On peut supposer $N \geqslant n$. Notre relation devient

$$\sum_{i=1}^{n} g_i(X_1, \ldots, X_N) f_i(X_i) = 1$$

Soit F/k une extension de degré fini dans laquelle chaque polynôme f_i possède une racine, disons α_i. Ce corps F existe, il suffit de considérer le corps de décomposition du produit des f_i, pour $1 \leqslant i \leqslant n$. On pose $\alpha_i = 0$ pour $i > n$. En remplaçant les X_i par les α_i dans notre relation, on obtient $0 = 1$, ce qui est absurde.

D'après le théorème de Krull, il existe donc un idéal maximal, noté $\mathfrak{M}$ contenant l'idéal engendré par tous les polynômes $f(X_f)$ de $k[S]$. Alors l'ensemble quotient $k[S]/\mathfrak{M}$ est un corps, et on a la surjection canonique

$$\sigma \colon k[S] \twoheadrightarrow k[S]/\mathfrak{M}$$

Pour tout polynôme non constant $f \in k[X]$, le polynôme $\sigma(f)$ possède une racine dans $k[S]/\mathfrak{M} := E_1$, qui est une extension de k. Donc E_1 est bien une extension de k dans laquelle tout polynôme non constant de $k[X]$ possède une racine.

1. Cette construction a du sens !

On peut construire par récurrence une suite de corps $E_1 \subset E_2 \subset \ldots \subset E_n \ldots$ telle que chaque polynôme non constant de $E_n[X]$ possède une racine dans E_{n+1}. L'ensemble $E = \bigcup_{i \geqslant 1} E_i$ est naturellement muni d'une structure de corps. En effet, pour $x, y \in E$, il existe $n \geqslant 1$ tel que $x, y \in E_n$. On peut alors sommer ou multiplier x et y dans le corps E_n. De plus, tout polynôme à coefficients dans E est à coefficients dans un certain E_n, donc possède une racine dans E_{n+1} donc dans E. Donc le corps E est une clôture algébrique de k. □

Proposition 1.2.16. *Tout corps algébriquement clos est infini.*

Démonstration. Raisonnons par contraposé. Soit k un corps fini. Alors il existe $n \in \mathbf{N}$ tel que $k = \{a_1, a_2, ..., a_n\}$. Considérons dès lors le polynôme $P(X) = \prod_{i=1}^{n} (X - a_i) + 1_k$. Alors, pour tout $1 \leqslant i \leqslant n$, l'évaluation de P en a_i donne $P(a_i) = 1_k \neq 0_k$. C'est un polynôme non constant qui n'admet pas de racines dans k. Donc k n'est pas algébriquement clos. □

Soit k un corps, K une extension de k et Ω une clôture algébrique de k. Nous avons vu dans la proposition 1.2.10 qu'étant donné un automorphisme de k (par exemple l'identité), il est possible de le prolonger en un automorphisme de K dans un cas particulier où K est le corps de décomposition d'un polynôme sur k. La question est maintenant de savoir combien il existe de tels prolongements dans le cas général.

Théorème 1.2.17 (Dedekind)**.** *Soient $k \subset K \subset \Omega$ comme précédemment. On suppose que l'extension K/k est finie de degré n. Alors il existe au plus n k-automorphismes de K qui laissent fixes tous les éléments du corps k.*

Démonstration. Le corps K dispose d'une structure naturelle de k espace-vectoriel de dimension n. Soit $(x_1, \cdots, x_n)$ une k-base de K. On note V l'ensemble des applications k-linéaires de K dans Ω. L'ensemble V est muni d'une structure d'espace vectoriel sur Ω. Il s'agit même d'un espace vectoriel de dimension finie n sur Ω. En effet, l'application $\varphi \colon V \to \Omega^n$ définie par $\varphi(u) = (u(x_i))$ est Ω-linéaire et est une bijection de V sur Ω^n.

Supposons désormais qu'il existe $N > n$ plongements de K dans Ω égaux à l'identité sur k et deux à deux distincts (il s'agit en particulier de N éléments de V), alors le théorème dû à Dedekind ce dessous 1.2.18, nous assure que ces N éléments sont linéaires indépendants sur Ω. C'est absurde, car V est un espace vectoriel sur Ω de dimension n. Donc il existe bien au plus n automorphismes de K qui laissent fixe tous les éléments du corps k. □

Théorème 1.2.18. *Soient N un entier et $(\sigma_i)_{1 \leqslant i \leqslant N}$ N plongements de K dans Ω égaux à l'identité sur k et deux à deux distincts. Alors ces N plongements sont linéairement indépendants sur Ω.*

Démonstration. Supposons par l'absurde que la famille est liée, et notons r son rang. Quitte à renuméroter les σ_i, on peut supposer que la famille

$(\sigma_i)_{1\leqslant i\leqslant r}$ est libre. Il existe donc une unique famille de $(\lambda_i)_{1\leqslant i\leqslant r} \in \Omega^r$ tel que

$$\sigma_{r+1} = \sum_{1\leqslant i\leqslant r} \lambda_i \sigma_i$$

Par ailleurs, il existe nécessairement un i_0 tel que l'élément λ_{i_0} soit non nul. Soit $y \in K$ non nul, d'après l'égalité précédente, pour tout $x \in K$, on a

$$\sigma_{r+1}(xy) = \sum_{1\leqslant i\leqslant r} \lambda_i \sigma_i(xy)$$

Ce qu'on peut réécrire sous la forme, en prenant en compte le fait que les σ_i sont des morphismes d'anneaux

$$\sigma_{r+1}(x) = \sum_{1\leqslant i\leqslant r} \lambda_i \frac{\sigma_i(y)}{\sigma_{r+1}(y)} \sigma_i(x)$$

Par unicité des λ_i, cela implique que pour tout $1 \leqslant i \leqslant r$

$$\lambda_i = \lambda_i \frac{\sigma_i(y)}{\sigma_{r+1}(y)}$$

En particulier, puisque λ_{i_0} est non nul, cela implique que $\sigma_{r+1}(y) = \sigma_{i_0}(y)$, pour tout y non nul dans K. C'est absurde, puisque les σ_i sont supposés deux à deux distincts. Ce qui conclut. □

Remarque 5. Le théorème 1.2.17 aura une certaine importance lorsque nous introduirons la notion de groupe de Galois. En effet, un corollaire de ce théorème sera que si K/k est une extension finie de degré n, alors le cardinal du groupe de Galois $\mathrm{Gal}(K/k)$ est inférieur ou égal à n.

1.3. **Extensions normales et séparables.**

1.3.1. *Extensions normales.*

Définition 1.3.1. Soit k un corps. Une extension K/k est dite normale si tout polynôme irréductible sur $k[X]$ qui possède une racine dans K est scindé sur K.

Il est notable qu'en général, un corps de rupture d'un polynôme irréductible n'est pas une extension normale.

Exemple 1.3.2. Le corps $\mathbf{Q}[\sqrt[3]{2}]$ est un corps de rupture du polynôme $X^3 - 2$, mais cette extension n'est pas normale. En effet, l'élément $j\sqrt[3]{2}$ (où j est une racine troisième de l'unité), qui est aussi une racine du polynôme n'appartient pas à $\mathbf{Q}[\sqrt[3]{2}]$.

Proposition 1.3.3. *Soit k un corps, et f un polynôme de $k[X]$. Alors un corps de décomposition de f, noté K, est une extension normale de k.*

Démonstration. Soit g un polynôme irréductible de $k[X]$ qui possède une racine dans K, notée α. Soit β une autre racine de g. Montrons dans un premier temps que $K(\alpha)$ est k-isomorphe à $K(\beta)$.

Remarquons dans un premier temps que les corps $k(\alpha)$ et $k(\beta)$ sont k-isomorphes. En effet ils sont tous deux des corps de rupture de g sur k. Par ailleurs, le corps $K(\alpha)$ est un corps de décomposition de f sur $k(\alpha)$ puisque K est un corps de décomposition de f sur k. De même $K(\beta)$ est un corps de décomposition de f sur $k(\beta)$. Comme les corps $k(\alpha)$ et $k(\beta)$ sont isomorphes, nous en déduisons que les extensions $K(\alpha)/k(\alpha)$ et $K(\beta)/k(\beta)$ sont isomorphes par unicité des corps de décomposition à isomorphisme près. Ainsi $[K(\alpha) : k(\alpha)] = [K(\beta) : k(\beta)]$. Par la proposition 1.1.5 nous en déduisons les égalités $[K(\alpha) : K] \times [K : k] = [K(\alpha) : k(\alpha)] \times [k(\alpha) : k]$. De plus $[k(\alpha) : k] = [k(\beta) : k]$. L'on en déduit par substitution dans ces égalités que $[K(\beta) : K] = [K(\alpha) : K] = 1$, puisque $\alpha \in K$. Donc β est aussi un élément de K, ce qui démontre notre proposition. □

Nous allons maintenant voir une forme de réciproque au théorème précédent. Étant donné une extension normale, peut-il s'agir d'un corps de décomposition d'un polynôme donné ?

Proposition 1.3.4. *Soit K/k une extension normale de degré fini n. Alors K est un corps de décomposition sur k d'un polynôme à coefficients dans k.*

Démonstration. Comme le corps K est une extension de degré fini, il existe des éléments $x_1, \cdots, x_n \in K$ tels que $K = k[x_1, \cdots, x_n]$. Pour tout $1 \leqslant i \leqslant n$, notons f_i le polynôme minimal de x_i. Il s'agit alors de montrer que K est le corps de décomposition de $f = \text{ppcm}(f_i)$. Il est clair que pour tout $1 \leqslant i \leqslant n$, l'élément x_i est racine de f (puisque f_i divise f). Notons donc $x'_1, \cdots, x'_m \in K$ les racines de f distinctes des x_i. Ces racines sont bien dans K puisqu'il s'agit d'une extension normale. Par définition un corps de décomposition de f est engendré sur k par les racines de f. Donc $\mathcal{D}_k(f) = k[x_1, \cdots, x_n, x'_1, \cdots, x'_m] = K$. □

En conclusion de ces deux dernières propositions, une extension finie est une extension normale si et seulement si c'est un corps de décomposition d'un polynôme.

1.3.2. *Extensions séparables.*

Définition 1.3.5. Soit k un corps. Un polynôme $f \in k[X]$ est dit séparable s'il n'est pas constant et que ses racines dans un corps de décomposition sont toutes simples.

La proposition suivante utilise la notion de discriminant. Pour plus de précisions se reporter à la définition A.0.5.

Proposition 1.3.6. *Si $f \in k[x]$ est un polynôme unitaire, non constant, alors les propositions suivantes sont équivalentes*

(1) Le polynôme f est séparable

(2) $\Delta(f) \neq 0$

(3) Les polynômes f et f' sont premiers entre eux dans $k[X]$.

Démonstration. On supposera que le polynôme f est non constant pour que le discriminant ait du sens. Le polynôme f est séparable si et seulement s'il est à racines simples, si et seulement si le discriminant de f, qui est un produit de différences de racines de f, est non nul. Donc (1) $\Leftrightarrow$ (2).

Montrons maintenant (1) $\Leftrightarrow$ (3). En effet, les polynômes f et f' ne sont pas premiers entre eux si et seulement si ils ont une racine commune dans une clôture algébrique de K, si et seulement si le polynôme f possède une racine double. □

Définition 1.3.7. Soit $k \subset K$ une extension algébrique.

(1) Un élément $a \in K$ est dit séparable sur k si son polynôme minimal à coefficients dans k est séparable.

(2) L'extension K/k est dite séparable si tout élément a de K est séparable sur k.

Le théorème suivant est un classique, mais il ne sera pas démontré. Nous donnerons seulement une référence.

Théorème 1.3.8 (Théorème de l'élément primitif)**.** *Soit k un corps, et $K = k(\alpha_1, \cdots, \alpha_n)$ une extension de degré fini où chaque élément α_i est séparable sur k. Alors il existe un élément $\alpha \in K$, séparable sur k tel que $K = k[\alpha]$. De plus, si k est infini, alors α peut être choisi de la forme*

$$\alpha = t_1\alpha_1 + \cdots + t_n\alpha_n$$

où $t_1, \cdots, t_n \in k$.

Démonstration. Une preuve de ce théorème se trouve dans la référence [1], à la page 119. □

1.4. **Le groupe de Galois.**

1.4.1. *Le groupe de Galois.*

Définition 1.4.1. Soit $k \subset K$ une extension de degré fini. On définit l'ensemble $\mathrm{Gal}(K/k)$ comme étant

$$\{\sigma \in \mathrm{Aut}_k(K) \mid \forall a \in k, \sigma(a) = a\}$$

où l'ensemble $\mathrm{Aut}_k(K)$ désigne les automorphismes de K.

En d'autre termes, c'est l'ensemble des automorphismes de K qui laissent fixe tout élément de k. Il peut s'agir cependant d'un ensemble plus grand que $\mathrm{Aut}_k(k)$.

Proposition 1.4.2. *L'ensemble* $\mathrm{Gal}(K/k)$ *forme un groupe lorsqu'il est muni de la loi de composition pour les applications.*

Démonstration. On va montrer que $\mathrm{Gal}(K/k)$ *est un sous-groupe du groupe des automorphismes de K.* La loi de composition pour les applications est bien une loi de composition interne. En effet, pour $\sigma, \tau \in \mathrm{Gal}(K/k)$, et pour $a \in k$, on a bien l'égalité $\tau \circ \sigma(a) = \tau(a) = a$.

L'identité est bien un automorphisme de K qui laisse k fixe, et c'est bien l'élément neutre pour cette loi.

Soit $\sigma \in \mathrm{Gal}(K/k)$, comme c'est un automorphisme de K cet élément admet un inverse dans $\mathrm{Aut}(K)$ que l'on note σ^{-1}. En composant par σ^{-1} dans l'égalité $\sigma(a) = a$, pour tout $a \in k$, on obtient $\sigma^{-1}(a) = a$, pour tout $a \in k$. Donc l'inverse de σ est bien un élément de $\mathrm{Gal}(K/k)$, qui forme donc un groupe. □

Remarque 6. Lorsque l'extension K/k est galoisienne, on appelle l'ensemble $\mathrm{Gal}(K/k)$ le **groupe de Galois** de l'extension K/k. La proposition précédente justifie la dénomination de groupe.

Lemme 1.4.3. *Soit $k \subset K$ une extension de degré fini, et soit $\sigma \in \mathrm{Gal}(K/k)$. Alors pour tout $n \in \mathbf{N}^*$, et pour tout $h \in k[x_1, \cdots, x_n]$*

$$\sigma(h(x_1, \cdots, x_n)) = h(\sigma(x_1), \cdots, \sigma(x_n))$$

Démonstration. Soit $h = \sum_{\nu \in \mathbf{N}^n} \alpha_\nu x^\nu$, où $\alpha \in k$. Alors, les propriétés des morphismes permettent d'écrire les égalités suivantes :

$$\begin{aligned}
\sigma(h(x_1, \cdots, x_n)) &= \sigma(\sum_{\nu \in \mathbf{N}^n} \alpha_\nu x^\nu) \\
&= \sum_{\nu \in \mathbf{N}^n} \sigma(\alpha_\nu)\sigma(x)^\nu \\
&= \sum_{\nu \in \mathbf{N}^n} \alpha_\nu \sigma(x)^\nu \qquad \text{car } \sigma(a) = a, \forall a \in k \\
&= h(\sigma(x_1), \cdots, \sigma(x_n))
\end{aligned}$$

□

Proposition 1.4.4. *Soit $k \subset K$ une extension de degré fini, soit $\sigma \in \mathrm{Gal}(K/k)$, et soit $h \in k[X]$ un polynôme non constant. Alors si $\alpha \in K$ est une racine du polynôme f, alors $\sigma(\alpha)$ est aussi une racine du polynôme f.*

Démonstration. Il suffit d'appliquer le lemme 1.4.3. En effet, $f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0$. □

Si on considère l'ensemble des racines de f, numérotées de manière arbitraire de 1 à n, le groupe de Galois peut être vu comme un sous-groupe de $\mathfrak{S}_n$ de par son action sur les racines de f.

Définition 1.4.5. Soit $f \in k[X]$ un polynôme. Le groupe de Galois du polynôme f sur le corps k est défini comme étant $\mathrm{Gal}(K/k)$, où K est un corps de décomposition de f.

Il faut vérifier que cette définition a du sens et ne dépend pas du corps de décomposition choisi. Ce fait découle de la proposition suivante, et du fait que deux corps de décomposition d'un même polynôme sont isomorphes d'après la proposition 1.2.8.

Proposition 1.4.6. *Soit K_1/k et K_2/k deux extensions de corps. On suppose que les corps K_1 et K_2 sont k-isomorphes. Alors les groupes de Galois $\mathrm{Gal}(K_1/k)$ et $\mathrm{Gal}(K_2/k)$ sont isomorphes.*

Démonstration. Soit $\varphi\colon K_1 \to K_2$ un isomorphisme qui fixe tous les éléments de k. Alors

$$\begin{array}{rccc} \varphi^*\colon & \mathrm{Gal}(K_1/k) & \to & \mathrm{Gal}(K_2/k) \\ & \sigma & \mapsto & \varphi \circ \sigma \circ \varphi^{-1} \end{array}$$

est un isomorphisme de groupes. □

Proposition 1.4.7. *Soit K/k une extension normale et séparable. Alors l'ensemble noté K^G défini comme étant $\{a \in K | \forall \sigma \in \mathrm{Gal}(K/k),\ \sigma(a) = a\}$ est égal à k.*

Démonstration. On a l'inclusion évidente $k \subset K^G$. Supposons par l'absurde qu'il existe une élément $\alpha \in K^G$ tel que $\alpha \notin k$. Alors, le polynôme minimal de α, noté f_α est de degré supérieur ou égal à deux. Comme l'extension K/k est séparable, il existe un élément β, différent de α, dans une clôture algébrique de k tel que β soit une racine de f_α. Comme l'extension K/k est normale le polynôme irréductible f_α est scindé sur K, donc l'élément β est aussi dans le corps K. On considère le morphisme $\varphi\colon k[\alpha] \to k[\beta]$ qui à tout élément de la forme $\sum_i a_i\alpha^i$ associe $\sum_i a_i\beta^i$. On remarque que ce morphisme agit comme l'identité sur le corps k. On peut se référer à la démonstration du théorème 1.2.10 pour démontrer que φ est un isomorphisme. D'ailleurs ce même théorème permet de démontrer que cet isomorphisme s'étend en un automorphisme de K qui laisse fixe tout élément de k. Donc $\varphi \in \mathrm{Gal}(K/k)$, mais ne laisse pas fixe α. C'est absurde.

On a donc bien démontré par double inclusion que $K^G = k$. □

Définition 1.4.8. Soit K/k une extension de corps. Si $K^G = k$, alors l'extension K est dite galoisienne.

1.4.2. *Le morphisme de Frobenius.* Nous allons maintenant étudier rapidement un morphisme très important dans les extensions de $\mathbf{F}_p$, le morphisme de Frobenius.

Définition 1.4.9. Soit k un corps de caractéristique p. On appelle **morphisme de Frobenius**, le morphisme noté Frob, qui à tout élément $x \in k$ associe x^p.

Il est élémentaire de vérifier que le morphisme précédemment défini est bien un morphisme d'anneaux.

Proposition 1.4.10. *Soit p un nombre premier, et $m \in \mathbf{N}\backslash\{0\}$. Alors le morphisme d'anneaux* $\mathrm{Frob}\colon \mathbf{F}_{p^m} \to \mathbf{F}_{p^m}$ *est un automorphisme qui laisse fixe tout élément de $\mathbf{F}_p$.*

En d'autres termes, le morphisme de Frobenius est un élément du groupe de Galois de l'extension $\mathbf{F}_{p^m}/\mathbf{F}_p$.

Démonstration. Nous savons que éléments de $\mathbf{F}_{p^m}$ sont exactement les racines du polynôme $X^{p^m} - X$, donc pour tout $x \in \mathbf{F}_{p^m}$, nous avons l'égalité suivante

$$\mathrm{Frob}^m(x) = x^{p^m} = x$$

L'inverse du morphisme de Frobenius est donc le morphisme Frob^{m-1}. C'est donc un automorphisme.

Par ailleurs, tout élément $x \in \mathbf{F}_p$, est racine du polynôme $X^p - X$, on a donc bien $\text{Frob}(x) = x^p = x$. Ce qui finit de démontrer que le morphisme de Frobenius est un élément du groupe de Galois $\text{Gal}(\mathbf{F}_{p^m}/\mathbf{F}_p)$. □

Proposition 1.4.11. *Soit p un nombre premier, et $m \in \mathbf{N}\backslash\{0\}$. Alors l'automorphisme d'anneaux* $\text{Frob}\colon \mathbf{F}_{p^m} \to \mathbf{F}_{p^m}$ *est un élément d'ordre m du groupe de Galois* $\text{Gal}(\mathbf{F}_{p^m}/\mathbf{F}_p)$.

Démonstration. Nous avons vu dans la démonstration de la proposition précédente 1.4.10 que $\text{Frob}^m = \text{Id}$. Supposons que le morphisme de Frobenius soit d'ordre n strictement inférieur m. Alors $\text{Frob}^n = \text{Id}$, ce qui implique que $x^{p^n} = x$ pour tout $x \in \mathbf{F}_{p^m}$. Nous en déduisons que tous les éléments de $\mathbf{F}_{p^m}$ sont racines du polynôme $X^{p^n} - X$. Or ce polynôme possède au plus p^n racines (puisque $\mathbf{F}_{p^m}$ est un corps). Ce qui impliquerait que $\text{Card}(\mathbf{F}_{p^m}) \leqslant p^n$, ce qui est absurde puisque $n < m$. Donc le morphisme de Frobenius est d'ordre exactement m. □

Proposition 1.4.12. *Soit p un nombre premier, et $m \in \mathbf{N}\backslash\{0\}$. Le morphisme de Frobenius engendre le groupe de Galois* $\text{Gal}(\mathbf{F}_{p^m}/\mathbf{F}_p)$.

Démonstration. Comme nous l'avons signalé dans la remarque 5, le groupe de Galois $\text{Gal}(\mathbf{F}_{p^m}/\mathbf{F}_p)$ est de cardinal fini inférieur ou égal au degré de l'extension, à savoir m. Par ailleurs, nous avons vu dans la proposition 1.4.11 que le morphisme de Frobenius est d'ordre exaxtement m. Ceci implique qu'il y a au moins m éléments dans le groupe de Galois $\text{Gal}(\mathbf{F}_{p^m}/\mathbf{F}_p)$. Les deux inégalités nous assurent donc qu'il y a m éléments dans le groupe de Galois $\text{Gal}(\mathbf{F}_{p^m}/\mathbf{F}_p)$, et qu'ils sont tous des puissances du morphisme de Frobenius. □

2. Théorème de Dedekind

La motivation de ce paragraphe est de savoir si, étant donné un polynôme à coefficients dans $\mathbf{Z}$, on peut tirer de l'information sur son groupe de Galois sur $\mathbf{Q}$ à partir des groupes de Galois de ce polynôme sur les différents $\mathbf{F}_p$.

2.1. Le polynôme $s_u(y)$ et quelques propriétés.

Soit k un corps, et f un polynôme séparable de $k[X]$ de degré n. On note $\alpha_1, \ldots, \alpha_n$ ses racines dans un corps de décomposition, noté K.

Définition 2.1.1. On définit le polynôme suivant

$$s_u(y) := \prod_{\sigma \in \mathfrak{S}_n} (y - (u_1\alpha_{\sigma(1)} + \cdots + u_n\alpha_{\sigma(n)})) \in K[u_1, \ldots u_n, y]$$

Lemme 2.1.2. *Le polynôme $s_u(y)$* a priori *dans $K[u_1, \ldots u_n, y]$ est un élément de $k[u_1, \ldots u_n, y]$.*

Démonstration. Le polynôme est stable sous l'action des éléments du groupe de Galois de f, ce qui conclut d'après la proposition 1.4.7. □

Lemme 2.1.3. *La décomposition du polynôme $s_u(y)$ sous la forme $\prod_{\sigma\in\mathfrak{S}_n}(y-(u_1\alpha_{\sigma(1)}+\cdots+u_n\alpha_{\sigma(n)}))$ est une décomposition en polynômes irréductibles.*

Démonstration. Via le morphisme d'évaluation $\varphi\colon K[u_1,\dots u_n,y]\to K[y]$, qui envoie les variables u_i sur 0, et y sur y, le facteur $y-(u_1\alpha_{\sigma(1)}+\cdots+u_n\alpha_{\sigma(n)})$ est envoyé sur y, qui est irréductible dans $K[y]$. De plus ce morphisme ne modifie pas le degré du polynôme par rapport à la variable y. Donc le polynôme $y-(u_1\alpha_{\sigma(1)}+\cdots+u_n\alpha_{\sigma(n)})$ est irréductible dans $K[u_1,\dots u_n,y]$. □

Considérons un corps k et un polynôme f de degré n à coefficients dans ce corps. Notons K un corps de décomposition de f. Le groupe de Galois $\mathrm{Gal}(K/k)$ peut-être vu comme un sous-groupe de $\mathfrak{S}_n$, par son action sur les racines de f.

En effet, notons $R_f=\{x_1,x_2,\cdots,x_n\}$ l'ensemble des n racines de f, on a vu dans la proposition 1.4.4 que si $\sigma\in\mathrm{Gal}(K/k)$, alors $\sigma(x_i)\in R_f$, pour tout $1\leqslant i\leqslant n$.

Ainsi pour $\tau\in\mathfrak{S}_n$, $\tau(f)(X)=\prod_{i=1}^{n}(X-x_{\tau(i)})$.

Proposition 2.1.4. *Soit k un corps, et soit $f\in k[X]$ un polynôme unitaire, séparable, de degré n. Soit $h\in k[u_1,\dots u_n,y]$ un facteur irréductible de $s_u(y)\in k[u_1,\dots u_n,y]$, défini en 2.1.1. Alors le groupe de Galois de f, noté $G_f\subset\mathfrak{S}_n$, vu comme un sous-groupe du groupe des permutations est conjugué au sous-groupe $G:=\{\tau\in\mathfrak{S}_n,\tau.h=h\}$.*

Démonstration. Le polynôme h est un diviseur de $s_u(y)$, donc le lemme 2.1.3 nous assure qu'il existe $\sigma\in\mathfrak{S}_n$, de telle sorte que $y-(u_1\alpha_{\sigma(1)}+\cdots+u_n\alpha_{\sigma(n)})$ soit un facteur de h dans $K[u_1,\dots u_n,y]$. On définit

$$\begin{aligned}\tilde{h} &= \prod_{\gamma\in\mathrm{Gal}(K/k)}(y-(u_1\gamma(\alpha_{\sigma(1)})+\cdots+u_n\gamma(\alpha_{\sigma(n)})))\\ &= \prod_{\mu\in G_f}(y-(u_1\alpha_{\mu\sigma(1)}+\cdots+u_n\alpha_{\mu\sigma(n)}))\end{aligned}$$

On remarque que $\tilde{h}$ est invariant sous l'action du groupe de Galois, il est donc à coefficients dans le corps k d'après la proposition 1.4.7. De plus $y-(u_1\alpha_{\sigma(1)}+\cdots+u_n\alpha_{\sigma(n)})$ est un facteur de h, donc pour tout $\gamma\in\mathrm{Gal}(K/k)$, le polynôme $\gamma(y-(u_1\alpha_{\sigma(1)}+\cdots+u_n\alpha_{\sigma(n)}))$ est un facteur irréductible de $\gamma.h=h$. Comme tous les $y-(u_1\alpha_{\sigma(1)}+\cdots+u_n\alpha_{\sigma(n)})$ sont distincts -et donc premiers entre eux- car le polynôme f est séparable, alors $\tilde{h}$ divise h. Or le polynôme h est irréductible dans $k[u_1,\dots u_n,y]$, donc $h=\tilde{h}$.

Si $\tau\in\mathfrak{S}_n$ satisfait $\tau.h=h$, alors $\tau(y-(u_1\alpha_{\sigma(1)}+\cdots+u_n\alpha_{\sigma(n)}))$ est un facteur de h dans $K[u_1,\dots u_n,y]$. Alors il existe $\mu\in G_f$ tel que

$$y-(u_{\tau(1)}\alpha_{\sigma(1)}+\cdots+u_{\tau(n)}\alpha_{\sigma(n)})=y-(u_1\alpha_{\mu\sigma(1)}+\cdots+u_n\alpha_{\mu\sigma(n)})$$

Comme les variables $u_1,\cdots,u_n$ sont distinctes l'égalité $\tau(i)=j$ implique $\alpha_{\sigma(i)}=\alpha_{\mu\sigma(j)}$, ou encore $\alpha_{\sigma\tau^{-1}(i)}=\alpha_{\mu\sigma(j)}$. Les racines α_i étant distinctes,

on en déduit que $\sigma\tau^{-1} = \mu\sigma$, c'est-à-dire $\tau = \sigma^{-1}\mu^{-1}\sigma \in \sigma^{-1}G_f\sigma$. Donc $G \subset \sigma^{-1}G_f\sigma$.

Réciproquement si $\tau \in \sigma^{-1}G_f\sigma$, alors il existe un élément $\lambda \in G_f$ tel que $\tau = \sigma^{-1}\lambda\sigma$. Démontrons la stabilité de h sous l'action de τ.

$$\begin{aligned}
\tau.h &= \prod_{\mu\in G_f} (y - (u_{\tau(1)}\alpha_{\mu\sigma(1)} + \cdots + u_{\tau(n)}\alpha_{\mu\sigma(n)})) \\
&= \prod_{\mu\in G_f} (y - (u_1\alpha_{\mu\sigma\tau^{-1}(1)} + \cdots + u_{\tau(n)}\alpha_{\mu\sigma\tau^{-1}(n)})) \\
&= \prod_{\mu\in G_f} (y - (u_1\alpha_{\mu\sigma\sigma^{-1}\lambda^{-1}\sigma(1)} + \cdots + u_{\tau(n)}\alpha_{\mu\sigma\sigma^{-1}\lambda^{-1}\sigma(n)})) \\
&= \prod_{\mu\in G_f} (y - (u_1\alpha_{\mu\lambda^{-1}\sigma(1)} + \cdots + u_{\tau(n)}\alpha_{\mu\lambda^{-1}\sigma(n)}))
\end{aligned}$$

Faire varier $\mu \in G_f$ revient à faire varier $\mu\lambda^{-1} \in G_f$, donc $\tau \cdot h = h$. Par double inclusion on en déduit bien l'égalité $G = \sigma^{-1}G_f\sigma$. □

2.2. **Le théorème de Dedekind, première démonstration.**

Théorème 2.2.1 (Théorème de Dedekind)**.** *Soit $f \in \mathbf{Z}[X]$ un polynôme unitaire et séparable de degré n. Étant donné un nombre premier p qui ne divise pas le discriminant du polynôme f ; on décompose $f \bmod p$, noté $\bar{f}$, comme produit d'irréductibles*

$$\bar{f} = f_1 f_2 \dots f_r$$

On note $d_i = \deg(f_i)$. Alors

(1) Le groupe de Galois de $\bar{f}$ sur $\mathbf{F}_p$ est cyclique d'ordre $\mathrm{ppcm}(d_1, \dots, d_r)$

(2) Le groupe de Galois de f sur $\mathbf{Q}$ contient un élément qui agit sur les racines de f comme un produit de cycles disjoints de la forme

$$\underbrace{(\dots)}_{d_1\text{-cycle}} \cdots \underbrace{(\dots)}_{d_r\text{-cycle}}$$

En particulier le groupe de Galois du polynôme f contient un élément d'ordre $\mathrm{ppcm}(d_1, \dots, d_r)$.

Démonstration. La première partie de la proposition est prouvée par les équivalences suivantes : f est scindé sur $\mathbf{F}_{p^m}$ si et seulement si pour tout $1 \leqslant i \leqslant r$ le polynôme f_i est scindé sur $\mathbf{F}_{p^m}$. Comme les racines du polynôme $X^{p^m} - X$ sont exactement les éléments de $\mathbf{F}_{p^m}$, dire que f_i est scindé sur $\mathbf{F}_{p^m}$ est équivalent à dire que f_i divise $X^{p^m} - X$, pour tout $1 \leqslant i \leqslant r$. La proposition 3.1.4 démontrée plus bas nous assure que le polynôme f_i, qui est irréductible dans $\mathbf{F}_p$, divise $X^{p^m} - X$, si et seulement si son degré d_i divise m. Ce qui est équivalent à dire que le $\mathrm{ppcm}(d_1, \dots, d_r)$ divise m. On note désormais $d = \mathrm{ppcm}(d_1, \dots, d_r)$.

On résume la suite d'équivalence précédente de la manière suivante : f est scindé sur $\mathbf{F}_{p^m}$

$$\begin{aligned}
&\Leftrightarrow \quad f_i | X^{p^m} - X, \forall i \\
&\Leftrightarrow \quad d_i | m, \forall i \\
&\Leftrightarrow \quad \mathrm{ppcm}(d_1, \dots, d_r) | m
\end{aligned}$$

Le groupe de Galois $\mathrm{Gal}(\mathbf{F}_{p^d}/\mathbf{F}_p)$ est engendré par le morphisme de Frobenius d'après la proposition 1.4.12. Soit a une racine de f dans $\mathbf{F}_{p^d}$, et $l \in \mathbf{N}^*$ le plus petit entier tel que $\mathrm{Frob}^{l+1}(a) = a$, qui existe car $l = d-1$ convient. Alors tous les éléments $a, \mathrm{Frob}(a), \cdots, \mathrm{Frob}^l(a)$ sont distincts. En effet, supposons par l'absurde qu'il existe $l \geqslant i > j$ tels que $\mathrm{Frob}^j(a) = \mathrm{Frob}^i(a)$. Alors en composant par le Frobenius $l-i$ fois, on obtient $\mathrm{Frob}^{l-i+j}(a) = a$. Ce qui est absurde, car l a été choisi comme le plus petit élément vérifiant cette égalité. Donc les éléments $a, \mathrm{Frob}(a), \cdots, \mathrm{Frob}^l(a)$ sont tous distincts. Par ailleurs, il existe un élément i dans $\{1, \cdots, r\}$ tel que a soit racine de f_i. De plus pour tout $1 \leqslant j \leqslant l$, l'élément $\mathrm{Frob}^j(a)$ est racine f_i. Donc le polynôme $\tilde{f}_i = \prod_{j=0}^{l} (X - \mathrm{Frob}^j(a))$ divise f_i. Or le polynôme $\tilde{f}_i$ est stable sous l'action du morphisme de Frobenius, donc sous l'action du groupe de Galois $\mathrm{Gal}(\mathbf{F}_{p^d}/\mathbf{F}_p)$ qu'il engendre. Dans la mesure où l'extension $\mathbf{F}_{p^d}/\mathbf{F}_p$ est normale et séparable, la proposition 1.4.7 assure que le polynôme $\tilde{f}_i$ est à coefficients dans $\mathbf{F}_p$. Or par irréductibilité de f_i dans $\mathbf{F}_p$, on en déduit que $f_i = \tilde{f}_i$. Donc $l = d_i - 1$ et les racines du polynôme f_i sont exactement $a, \mathrm{Frob}(a), \cdots, \mathrm{Frob}^{d_i-1}(a)$. Donc le Frobenius agit sur les racines de f_i comme un d_i-cycle. Le polynôme f étant séparable, les polynômes f_i n'ont pas de racine commune, donc le Frobenius agit sur f comme un produit de cycles disjoints $d_1, \cdots, d_r$.

Considérons une version généralisée de $s_u(y)$ défini en 2.1.1.

$$S_u(y) := \prod_{\sigma \in \mathfrak{S}_n} (y - (u_1 x_{\sigma(1)} + \cdots + u_n x_{\sigma(n)})) \in \mathbf{Z}[x_1, \ldots, x_n, u_1, \ldots, u_n, y]$$

Ce polynôme est symétrique en les x_i, donc d'après un résultat sur les polynômes symétriques A.0.2, $S_u(y) \in \mathbf{Z}[\sigma_1, \ldots, \sigma_n, u_1, \ldots, u_n, y]$, où les σ_i désignent les polynômes symétriques en les x_i. Écrivons le polynôme f sous la forme $f = x^n - c_1 x^{n-1} + \cdots + (-1)^n c_n$. Par réduction modulo p, on a aussi l'expression $\bar{f} = x^n - \bar{c_1} x^{n-1} + \cdots + (-1)^n \bar{c_n}$. En évaluant respectivement les σ_i en c_i puis en $\bar{c_i}$, on obtient deux polynômes

$$s_u(y) \in \mathbf{Z}[u_1, \cdots, u_n, y] \text{ et } \bar{s_u}(y) \in \mathbf{F}_p[u_1, \cdots, u_n, y]$$

De plus, le polynôme $\bar{s_u}(y)$ est la réduction modulo p de $s_u(y)$. On va alors relier les polynômes $\bar{s_u}(y)$ et $s_u(y)$ aux groupes de Galois de f et $\bar{f}$, comme dans la proposition 2.1.4. On note toujours $G_f \subset \mathfrak{S}_n$ le groupe de Galois du polynôme f, vu comme un sous-groupe de $\mathfrak{S}_n$ de part son action sur les racines de f. Soit h un facteur irréductible de $s_u(y)$ sur $\mathbf{Q}$. D'après la proposition 2.1.4, le groupe G_f est conjugué à

$$G = \{\sigma \in \mathfrak{S}_n, \sigma \cdot h = h\}$$

Quitte à multiplier par le plus grand diviseur commun des dénominateurs des coefficients, on peut supposer que $h \in \mathbf{Z}[u_1, \cdots, u_n, y]$. On considère alors la réduction de h modulo p, notée $\bar{h}$, et soit $\bar{g}$ un facteur irréductible de $\bar{h}$. C'est alors aussi un facteur irréductible de $\bar{s_u}(y)$, et par toujours par

la proposition 2.1.4, le groupe de Galois de $\bar{f}$ sur $\mathbf{F}_p$ donne un sous-groupe de $\mathfrak{S}_n$ conjugué à

$$\bar{G} = \{\sigma \in \mathfrak{S}_n; \sigma \cdot \bar{g} = \bar{g}\}$$

Montrons que $\bar{G} \subset G$. Procédons par l'absurde, et supposons qu'il existe $\sigma \in \bar{G}$ tel que $\sigma \cdot \bar{g} = \bar{g}$, mais $\sigma \cdot h = h_1 \neq h$. Alors l'égalié $\sigma \cdot s_u(y) = s_u(y)$ implique que h_1 est aussi un facteur irréductible de $s_u(y)$. Comme l'anneau $\mathbf{Z}[u_1, \cdots, u_n, y]$ est factoriel, il existe $q \in \mathbf{Z}[u_1, \cdots, u_n, y]$ tel que

$$s_u(y) = hh_1q$$

La réduction modulo p donne $\bar{s_u}(y) = \bar{h}\bar{h_1}\bar{q} \in \mathbf{F}_p[u_1, \cdots, u_n, y]$. Par ailleurs, comme l'action de $\mathfrak{S}_n$ sur les racines est compatible avec la réduction modulo p, l'égalité $\sigma \cdot h = h_1$ implique $\sigma\bar{h} = \bar{h_1}$. Comme $\bar{g}$ divise $\bar{h}$, alors $\sigma \cdot \bar{g} = \bar{g}$ divise $\sigma \cdot \bar{h} = \bar{h_1}$. L'égalité précédente, nous montre donc que $\bar{g}^2$ divise $\bar{s_u}(y)$. Or, sur un corps de décomposition le polynôme $\bar{s_u}(y)$ est produit de facteurs irréductibles distincts. Donc le polynôme $\bar{g}^2$ ne peut pas diviser $\bar{s_u}(y)$. Ce qui est absurde. Ainsi pour tout $\sigma \in \bar{G}$ tel que $\sigma \cdot \bar{g} = \bar{g}$ on a aussi $\sigma \cdot h = h$, et donc $\bar{G} \subset G$. Ce qui démontre la deuxième partie du théorème. □

2.3. **Le théorème de Dedekind, deuxième démonstration.** Nous allons maintenant nous lancer dans une deuxième démonstration un peu plus abstraite du théorème de Dedekind. L'énoncé mettra en avant les propriétés des morphismes entre les différents groupes.

2.4. **Théorèmes sur les modules.** Commençons par quelques théorèmes sur les modules qui nous serons utiles.

Théorème 2.4.1. *Soit A un anneau principal, M un A-module de rang fini n, et M' un sous-module de M. Alors :*

(1) Le A-module M' est libre de rang inférieur ou égal à n ;

(2) Il existe une base $(e_1, \cdots, e_n)$ de M, un entier $q \leqslant n$, et des éléments non nuls $a_1, \cdots, a_q$ tels que $(a_1e_1, \cdots, a_qe_q)$ soit une base de M' et que a_i divise a_{i+1} pour $1 \leqslant i \leqslant q-1$.

De plus les idéaux Aa_i sont uniquement déterminés par la donnée de M et M'.

Démonstration. Une preuve de ce théorème se trouve dans la référence [5] chap. I §5, th. 1. □

Théorème 2.4.2 (Théorème de structure des modules de type fini)**.** *Soit A un anneau principal et M un A-module de type fini. Alors il existe un entier p et une famille $(a_1, \cdots, a_q)$ d'éléments de A non nuls tels que a_i divise a_{i+1} pour tout $1 \leqslant i \leqslant q-1$ tels que*

$$M \simeq A^p \times A/(a_1) \times \cdots \times A/(a_q)$$

L'entier p et les idéaux $(a_1), \cdots, (a_q)$ sont uniques.

Démonstration. Ce théorème sera démontré comme corollaire du théorème précédent 2.4.1. Par hypothèse le A-module M est de type fini. Il existe donc $n \in \mathbf{N}\backslash\{0\}$, tel que la famille $(x_1, \cdots, x_n)$ soit génératrice de M. Alors l'homomorphisme $\varphi\colon A^n \to M$ qui à $e_i = (0, \cdots, 0, 1, 0, \cdots)$ (un 1 en i ème position) associe x_i est surjectif. Donc le A-module M est isomorphe au quotient $A^n/\mathrm{Ker}(\varphi)$. Cependant $\mathrm{Ker}(\varphi)$ est un sous A-module de A^n, il existe donc, d'après le théorème précédent, des éléments non nuls $a_1, \cdots, a_q$ tels que $(a_1e_1, \cdots, a_qe_q)$ soit une base de $\mathrm{Ker}(\varphi)$ et que a_i divise a_{i+1} pour $1 \leqslant i \leqslant q-1$. On pose $a_i = 0$ pour $n \geqslant i > q$.

Donc le quotient $A^n/\mathrm{Ker}(\varphi)$ est isomorphe au produit des Ae_i/Aa_ie_i. On a bien $M \simeq A^p \times A/(a_1) \times \cdots \times A/(a_q)$. □

Soit f un polynôme unitaire à coefficients dans $\mathbf{Z}$ de degré d. On note K un corps de décomposition de f et R_f l'ensemble des racines de f dans K.

Proposition 2.4.3. *Le sous-anneau $A = \mathbf{Z}[R_f]$ est un $\mathbf{Z}$-module libre de type fini, stable sous l'action de G_f.*

Démonstration. Tout élément $r \in R_f$ est annulé par f. Une récurrence montre alors que pour tout entier $m \in N\backslash\{0\}$, on a $r^m \in \mathrm{Vect}\{1, r, \cdots, r^{d-1}\}$. Donc tout élément de A est une combinaison linéaire à coefficients dans $\mathbf{Z}$ de monônes en les $r \in R_f$ dont les exposants sont strictement inférieurs à d. En conséquence A est un $\mathbf{Z}$-module de type fini. Par ailleurs, l'anneau $\mathbf{Z}$ est principal. Le théorème de structure des modules de type fini 2.4.2 donne l'existence de $m, l \in \mathbf{N}$, et de $d_i \in Z$ avec pour tout $1 \leqslant i \leqslant l-1$ on ait $d_i | d_{i+1}$ tels qu'on ait l'isomorphisme

$$A \simeq \mathbf{Z}^r \times \mathbf{Z}/(d_1) \times \cdots \times \mathbf{Z}/(d_l)$$

Comme le corps K est sans torsion, alors A aussi (car $A \subset K$), ce qui nous assure que $l = 0$, et donc $A \simeq \mathbf{Z}^r$. Ainsi A est un $\mathbf{Z}$-module libre de type fini.

L'anneau est stable sous l'action de G_f, car pour tout $r \in R_f$ et $g \in G_f$, l'élément $g(r)$ est aussi une racine de f. □

Corollaire 2.4.4. *L'intersection entre A et $\mathbf{Q}$ vaut $\mathbf{Z}$.*

Démonstration. Soit $a \in A \cap \mathbf{Q}$. L'endomorphisme de A $\varphi_a\colon x \mapsto ax$, est tel que son déterminant est un élément de $\mathbf{Z}$. Cela vient du fait que A est un $\mathbf{Z}$-module libre, et que la théorie matricielle a alors du sens. Par ailleurs, ce déterminant coïncide avec le déterminant de la même application φ_a, vu comme un endomorphisme de $\mathbf{Q}(R_f)$. Dans ce cas, $\det(\varphi_a) = a^n$, où n désigne la dimension de $\mathbf{Q}(R_f)$ vu comme $\mathbf{Q}$-espace vectoriel. Donc $a^n \in \mathbf{Z}$. On en déduit donc que $a \in \mathbf{Z}$, ce qui conclut la preuve. □

Corollaire 2.4.5. *Pour tout nombre premier p, il existe un idéal premier $\mathfrak{m}$ de A le contenant.*

Démonstration. Montrons dans un premier temps que $A/pA \neq 0$. On a vu dans la démonstration précédente que $A \simeq \mathbf{Z}^r$. Montrer $A/pA \neq 0$ revient

alors à montrer $\mathbf{Z}^r/p\mathbf{Z}^r \neq 0$, à cause de l'isomorphisme $A/pA \simeq \mathbf{Z}^r/p\mathbf{Z}^r$. Or on a bien $\mathbf{Z}^r \neq p\mathbf{Z}^r$ car l'élément $(1, 0, \ldots, 0) \in \mathbf{Z}^r$, n'est pas dans $p\mathbf{Z}^r$. D'après le lemme de Krull tout idéal strict est contenu dans un idéal maximal, donc il existe bien un idéal premier $\mathfrak{m}$ de A contenant p. □

Soit p un nombre premier et $\mathfrak{m}$ un idéal maximal de A le contenant. Considérons les ensembles $D_\mathfrak{m} := \{g \in G_f, g(\mathfrak{m}) \subset \mathfrak{m}\}$ et $\kappa(\mathfrak{m}) := A/\mathfrak{m}$.

Proposition 2.4.6. *L'ensemble $D_\mathfrak{m}$ est un sous-groupe de G_f, appellé* ***sous-groupe de décomposition****.*

Démonstration. Le morphisme identité est un élément de $D_\mathfrak{m}$ qui est donc non vide et contient l'élément neutre. Soit $g_1, g_2 \in D_\mathfrak{m}$, alors $g_1 \circ g_2(\mathfrak{m}) \subset g_1(\mathfrak{m}) \subset \mathfrak{m}$.

Soit maintenant $g \in D_\mathfrak{m}$, montrons que son inverse $g^{-1} \in D_\mathfrak{m}$. Sachant que $g(\mathfrak{m}) \subset \mathfrak{m}$, on en déduit par composition par g^{-1} que $g^{-1} \circ g(\mathfrak{m}) \subset g^{-1}(\mathfrak{m})$, d'où $\mathfrak{m} \subset g^{-1}(\mathfrak{m})$. L'ensemble $g^{-1}(\mathfrak{m})$ est un idéal de A contenant l'idéal maximal $\mathfrak{m}$. Donc $g^{-1}(\mathfrak{m}) = \mathfrak{m}$ ou $g^{-1}(\mathfrak{m}) = A$. La deuxième supposition est absurde, car elle contredirait l'injectivité de g^{-1}. En effet, soit $u \in A\backslash\mathfrak{m} \neq \varnothing$, alors $g^{-1}(u) \in A$. Si $g^{-1}(\mathfrak{m}) = A$, alors il existe $x \in \mathfrak{m}$ tel que $g^{-1}(x) = g^{-1}(u)$. Par injectivité du morphisme g^{-1}, on aurait alors $x = u$, ce qui est absurde. Donc $g^{-1}(\mathfrak{m}) = \mathfrak{m}$, ce qui implique bien que $g^{-1} \in D_\mathfrak{m}$. □

Remarque 7. La démonstration précédente nous montre que l'inclusion *a priori* est une égalité.

$$D_\mathfrak{m} = \{g \in G_f, g(\mathfrak{m}) = \mathfrak{m}\}$$

Proposition 2.4.7. *L'ensemble $\kappa(\mathfrak{m})$ est une extension finie du corps $\mathbf{F}_p$. C'est un corps de décomposition du polynôme f_p obtenu par réduction de f modulo p.*

Démonstration. On considère le morphisme $\varphi\colon \mathbf{Z} \to A \twoheadrightarrow A/\mathfrak{m} = \kappa(\mathfrak{m})$, où la première flèche désigne le morphisme structural qui munit A de sa structure de $\mathbf{Z}$-module. Dans la mesure où p est un élément de $\mathfrak{m}$, le noyau de φ contient l'idéal (p) de $\mathbf{Z}$. Donc par le lemme de factorisation, le morphisme φ se factorise en un morphisme $\bar{\varphi}\colon \mathbf{F}_p \to \kappa(\mathfrak{m})$. Donc l'ensemble $\kappa(\mathfrak{m})$ est une extension du corps $\mathbf{F}_p$. Par ailleurs, comme A est engendré par les racines de f sur $\mathbf{Z}$, alors le corps $\kappa(\mathfrak{m})$ est engendré par la réduction modulo $\mathfrak{m}$ des racines de f sur $\mathbf{F}_p$, qui sont les racines de f_p, la réduction de f modulo p. C'est un corps de décomposition du polynôme f_p et donc une extension finie de $\mathbf{F}_p$. □

Notons R_{f_p} l'ensemble des racines de f_p dans $\kappa(\mathfrak{m})$.

Théorème 2.4.8 (Théorème de Dedekind)**.**

(1) L'application

$$\begin{array}{ccc} D_\mathfrak{m} & \to & \mathrm{Gal}(\kappa(\mathfrak{m})/\mathbf{F}_p) = G_{f_p}, \\ g & \mapsto & \bar{g}\colon (a \bmod \mathfrak{m} \mapsto g(a) \bmod \mathfrak{m}) \end{array}$$

est une surjection

(2) Supposons que f_p est séparable

- *(a) L'application $A \to \kappa(\mathfrak{m})$ de réduction moodulo $\mathfrak{m}$ induit une bijection $R_f \tilde{\to} R_{f_p}$*
- *(b) Le morphisme $D_\mathfrak{m} \to G_{f_p}$ est un isomorphsime.*
- *(c) Les applications composées $D_\mathfrak{m} \hookrightarrow G_f \hookrightarrow \mathfrak{S}_{R_f}$ et $D_\mathfrak{m} \tilde{\to} G_{f_p} \hookrightarrow \mathfrak{S}_{R_{f_p}}$, où les morphsimes $G_P \to G_{R_P}$ sont les morphismes de restriction à l'action sur les racines, coïncident modulo l'identification du (a).*

Démonstration. (1) Soit $\alpha \in \kappa(\mathfrak{m})$ un élément primitif, qui existe en vertu du théorème de l'élément primitif 1.3.8. Montrons dans un premier temps qu'il existe un relèvement $a \in A$ de α tel que pour tout $g \in G_f \backslash D_\mathfrak{m}$, $a \in g(\mathfrak{m})$. Comme l'ensemble G_f est fini, alors l'ensemble $\{g(\mathfrak{m}); g \in G_f \backslash D_\mathfrak{m}\}$ est fini. Notons $\mathfrak{n}_1, \cdots, \mathfrak{n}_s$ les éléments de cet ensemble. Tous ces idéaux sont maximaux car chacun des morphismes g induit un isomorphisme $A/\mathfrak{m} \to A/g(\mathfrak{m})$. D'après le théorème chinois, l'application

$$A \to a/\mathfrak{m} \times (A/\mathfrak{n}_1 \times \cdots \times A/\mathfrak{n}_s)$$

est surjective. Choisissons un relèvement a de $(\alpha, 0, \cdots, 0)$. Un tel relèvement convient, car pour tout $1 \leqslant i \leqslant s$, l'élément $a \in \mathfrak{n}_i$. Définissons le polynôme $P = \prod_{g \in G_f} (X - g(a))$. C'est un polynôme à coefficients dans A, mais aussi dans le corps laissé fixe sous l'action de G_f, à savoir $\mathbf{Q}$. Donc $P \in A \cap \mathbf{Q}[X] = \mathbf{Z}[X]$, d'après le corollaire 2.4.4. Notons $P_p \in \mathbf{F}_p[X]$ sa réduction modulo p. L'égalité $P(a) = 0$ entraîne par réduction $P_p(\alpha) = 0$. Le polynôme minimal de α dans $\mathbf{F}_p$ divise donc P_p. Il en résulte que les conjugués de α dans $\kappa(\mathfrak{m})$ font partie des racines du polynôme P_p.

Montrons que les racines non nulles de P_p sont les $\bar{\sigma}(\alpha)$ pour $\sigma \in D_\mathfrak{m}$. Il est clair que les racines de P_p sont exactement les $\bar{\sigma}(\alpha)$. Maintenant, si $\sigma \in D_\mathfrak{m}$, montrons $\sigma(a) \notin \mathfrak{m}$. C'est bien le cas, car on a vu que $\sigma(\mathfrak{m}) = \mathfrak{m}$, or $a \notin \mathfrak{m}$. Par ailleurs, si $\sigma \in G_f \backslash D_\mathfrak{m}$, alors $\sigma^{-1} \in G_f \backslash D_\mathfrak{m}$, en effet si ce n'était pas le cas et que $\sigma^{-1} \in D_\mathfrak{m}$, alors la structure de groupe de $D_\mathfrak{m}$ impliquerait que $\sigma \in D_\mathfrak{m}$. Par hypothèse sur a, $a \in \sigma^{-1}(\mathfrak{m})$, donc $\sigma(a) \in \mathfrak{m}$. Donc $\bar{\sigma}(\alpha) = 0$ pour $\sigma \in G_f \backslash D_\mathfrak{m}$. Ce qui démontre bien que les racines non nulles de P_p sont les $\bar{\sigma}(\alpha)$ pour $\sigma \in D_\mathfrak{m}$.

Un élément de $\mathrm{Gal}(\kappa(\mathfrak{m})/\mathbf{F}_p)$ est caractérisé par son action sur l'élément primitif α, qui est nécessairement envoyé sur un de ses conjugués. Or pour chacun des conjugués de α, il existe un élément $\sigma \in D_\mathfrak{m}$ qui envoie α sur ce conjugué. La surjectivité du morphisme $D_\mathfrak{m} \to \mathrm{Gal}(\kappa(\mathfrak{m})/\mathbf{F}_p)$ est donc acquise.

(2) (a) Le polynôme f_p étant séparable, l'ensemble R_{f_p} est de cardinal d, de sorte que la surjection naturelle $R_f \to R_{f_p}$ est une bijection. (b) Montrons que le morphisme défini en (1) est injectif. Soit g un élément du noyau du morphisme $D_\mathfrak{m} \to \mathrm{Gal}(\kappa(\mathfrak{m})/\mathbf{F}_p)$. Alors g agit trivialement sur les racines de f_p. Soit r une racine de f, on a alors $g(r) \in R_f$, et $g(r) - r \in \mathfrak{m}$. La

bijection $R_f \to R_{f_p}$ implique alors que $g(r) = r$, et ce pour tout $r \in R_f$. Comme les éléments de R_f engendrent $\mathbf{Q}[R_f]$, on a alors $g = \mathrm{Id}$. Donc le morpshisme $D_{\mathfrak{m}} \to \mathrm{Gal}(\kappa(\mathfrak{m})/\mathbf{F}_p)$ est un isomorphisme. (c) Ce point découle de la définition de ces morphismes. □

3. Théorème de Van der Waerden

Ce paragraphe a pour but d'estimer l'abondance des polynômes de groupe de Galois maximal.

Sauf mention du contraire, l'élément noté p sera un nombre premier supérieur ou égal à 3.

3.1. Existence de polynômes irréductibles dans $\mathbf{F}_p[X]$.

3.1.1. *Quelques propositions.*

Lemme 3.1.1. *Soit $r, d \in \mathbf{N}\backslash\{0\}$. Alors r est un diviseur de d si et seulement si le polynôme $X^{p^r} - X$ divise le polynôme $X^{p^d} - X$.*

Démonstration. Supposons que r divise d. Les racines de $X^{p^r} - X$ sont exactement les éléments de $\mathbf{F}_{p^r}$. Montrons donc que tout élément de F_{p^r} est racine de $X^{p^d} - X$. Prenons $a \in \mathbf{F}_{p^r}$, et $q \in \mathbf{N}$ tel que $d = qr$. Sachant que $\mathrm{Frob}^r(a) = a$, une récurence sur q nous montre que $\mathrm{Frob}^d(a) = \mathrm{Frob}^{rq}(a) = a$. L'on en déduit que a est une racine de $X^{p^d} - X$, ce qui montre que $X^{p^r} - X | X^{p^d} - X$. Réciproquement si le polynôme $X^{p^r} - X$ divise le polynôme $X^{p^d} - X$, alors tout élément de $\mathbf{F}_{p^r}$ peut être identifié à un élément de $\mathbf{F}_{p^d}$. Par le théorème 1.1.5 des tours d'extensions, on a alors

$$[\mathbf{F}_{p^d} : \mathbf{F}_{p^r}][\mathbf{F}_{p^r} : \mathbf{F}_p] = [\mathbf{F}_{p^d} : \mathbf{F}_p]$$

Donc r divise d. □

Lemme 3.1.2. *Soit p un nombre premier et $d \in \mathbf{N}\backslash\{0\}$. Soit Q un facteur irréductible de $X^{p^d} - X$, alors il existe un morphisme d'inclusion de $\mathbf{F}_p[X]/(Q)$ dans $\mathbf{F}_{p^d}$.*

Remarque 8. On dit aussi que le corps $\mathbf{F}_p[X]/(Q)$ se plonge dans $\mathbf{F}_{p^d}$.

Démonstration. Notons $\bar{x}$ l'image de X par la projection canonique $\mathbf{F}_p[X] \to \mathbf{F}_p[X]/(Q)$, c'est une racine de Q dans $\mathbf{F}_p[X]/(Q)$. La relation de divisibilité entre les polynômes $X^{p^d} - X$ et Q nous montre que $\bar{x}$ est aussi une racine du polynôme $X^{p^d} - X$. Or $\bar{x}$ engendre la $\mathbf{F}_p$-algèbre $\mathbf{F}_p[X]/(Q)$, or la $\mathbf{F}_p$-algèbre engendrée par x est incluse dans $\mathbf{F}_{p^d}$, puisque $x \in \mathbf{F}_{p^d}$. Donc le corps $\mathbf{F}_p[X]/(Q)$ se plonge dans $\mathbf{F}_{p^d}$. □

Proposition 3.1.3. *Soit p un nombre premier et $m \in \mathbf{N}\backslash\{0\}$. Soit Q un facteur irréductible dans $\mathbf{F}_p$ de degré $d \geqslant 1$ de $X^{p^m} - X$, alors d divise m.*

Démonstration. Comme le polynôme Q est irréductible dans $\mathbf{F}_p$, le corps de rupture $\mathbf{F}_p[X]/(Q)$ est isomorphe au corps $\mathbf{F}_{p^d}$. Le lemme 3.1.2 nous assure donc l'existence d'un morphisme d'inclusion de $\mathbf{F}_{p^d}$ dans $\mathbf{F}_{p^m}$. La proposition 1.1.5 sur les tours d'extensions nous permet d'écrire l'égalité suivante

$$[\mathbf{F}_{p^m} : \mathbf{F}_p] = [\mathbf{F}_{p^m} : \mathbf{F}_{p^d}] \times [\mathbf{F}_{p^d} : \mathbf{F}_p]$$

D'où d divise m, ce qui conclut la preuve. □

3.1.2. *Polynômes irréductibles.*

Proposition 3.1.4 (Caractérisation des polynômes irréductibles de degré $r|d$)**.** *Soit $d \geqslant 2$ un entier. Alors l'ensemble des facteurs irréductibles de $X^{p^d} - X$ est égal à l'ensemble des polynômes irréductibles de $\mathbf{F}_p$ dont le degré r divise d.*

Démonstration. Soit $Q \in \mathbf{F}_p[X]$ un facteur irréductible de $X^{p^d} - X$. Alors la proposition 3.1.3 nous assure que r divise d.

Réciproquement soit Q est un polynôme irréductible de $\mathbf{F}_p$ dont le degré r divise d. Par unicité du corps à p^r éléments, on a $\mathbf{F}_p[X]/(Q) \simeq \mathbf{F}_{p^r}$. Donc Q et $X^{p^r} - X$ ont une racine commune dans $\mathbf{F}_{p^r}$, et comme le polynôme Q est irréductible dans $\mathbf{F}_p[X]$, alors $Q|X^{p^r} - X$. Par ailleurs, comme r divise d, alors par le lemme 3.1.1 $X^{p^r} - X|X^{p^d} - X$. Donc $Q|X^{p^d} - X$, ce qui montre que Q est un facteur irréductible du polynôme $X^{p^d} - X$. □

On note désormais, pour $r \geqslant 2$, N_r le nombre de polynômes irréductibles de degré r dans $\mathbf{F}_p[X]$.

Lemme 3.1.5. *Soit $d \geqslant 2$, on a l'inégalité suivante*

$$dN_d \leqslant p^d$$

Démonstration. En vertu de la proposition 3.1.4, on sait que $X^{p^d} - X$ est le produit des polynômes irréductibles de $\mathbf{F}_p[X]$ dont le degré divise d. On obtient alors une égalité entre les degrés, donnée par $p^d = \sum_{r|d} rN_r$.

$$dN_d = p^d - \sum_{\substack{r|d \\ r \neq d}} rN_r \leqslant p^d$$

□

Proposition 3.1.6. *Soit $d \geqslant 2$. Alors on a l'inégalité suivante*

$$N_d \geqslant \frac{p^d}{d} \frac{2p-1}{2p}$$

Démonstration.

$$\begin{aligned} dN_d &= p^d - \sum_{\substack{r|d \\ r\neq d}} rN_r \\ &\geqslant p^d - \sum_{\substack{r|d \\ r\neq d}} p^r \qquad \text{par le lemme 3.1.5} \\ &\geqslant p^d - \sum_{r=0}^{\lfloor \frac{d}{2} \rfloor} p^r \\ &\geqslant p^d - \frac{p^{\lfloor \frac{d}{2} \rfloor}-1}{p-1} \\ &\geqslant p^d(1 - \frac{p^{\lfloor \frac{d}{2} \rfloor - d}-p^{-d}}{p-1}) \end{aligned}$$

Or $p^{\lfloor \frac{d}{2} \rfloor - d} - p^{-d} \leqslant \frac{1}{p}$, en effet

$$\begin{aligned} p^{\lfloor \frac{d}{2} \rfloor - d} - p^{-d} &\leqslant p^{\lfloor \frac{d}{2} \rfloor - d} \\ &\leqslant \frac{1}{p} \qquad \text{car } \lfloor \tfrac{d}{2} \rfloor - d \geqslant 1 \end{aligned}$$

De plus $\frac{1}{p-1} \leqslant \frac{1}{2}$, car $p \geqslant 3$, donc $-\frac{p^{\lfloor \frac{d}{2} \rfloor - d}-p^{-d}}{p-1} \geqslant -\frac{1}{2p}$. On en déduit bien l'inégalité

$$N_d \geqslant \frac{p^d}{d}\frac{2p-1}{2p}$$

□

Remarque 9. On peut adapter la démonstration si $p = 2$. On a alors l'ínégalité $N_d \geqslant \frac{p^d}{d}\frac{p-1}{p} = \frac{p^d}{2d}$

Remarque 10. En pratique, on retiendra le plus souvent l'ínégalité $N_d \geqslant \frac{p^d}{2d}$, valable pour tout nombre p premier, et tout entier $d \geqslant 2$.

Corollaire 3.1.7. *Pour tout nombre premier $p \geqslant 2$, et tout entier $d \geqslant 2$, il existe au moins un polynôme irréductible de degré d.*

Démonstration. C'est un corollaire immédiat de l'inégalité 3.1.6. □

3.2. **Polynômes de groupe de Galois maximal.**

Lemme 3.2.1. *Soit d un entier supérieur ou égal à deux, et p un nombre premier supérieur ou égal à $d-2$, mais différent de 2 ou 3. Alors il existe un polynôme $f \in \mathbf{Z}[X]$ tel que*

- *La réduction de f modulo 2 soit irréductible dans $\mathbf{F}_2[X]$*
- *La réduction modulo 3 de f soit de la forme $XQ(X)$, où $Q(X) \in \mathbf{F}_3[X]$ est irréductible.*
- *La réduction de f modulo p ait un facteur irréductible de degré 2 et $d-2$ racines distinctes*

Démonstration. On considère la projection

$$\pi \colon \mathbf{Z}[X] \to \mathbf{F}_2[X] \times \mathbf{F}_3[X] \times \mathbf{F}_p[X]$$

Dans la mesure où les nombres $2, 3$ et p sont premiers entre eux, le lemme chinois nous assure la surjectivité de π. Démontrer le lemme revient donc à démontrer l'existence de trois éléments, respectivement dans $\mathbf{F}_2[X]$, $\mathbf{F}_3[X]$, et $\mathbf{F}_p[X]$ qui satisfont aux conditions de l'énoncé. Or d'après le corollaire 3.1.7, il existe un polynôme f_2 de degré d, irréductible dans $\mathbf{F}_2[X]$, un polynôme Q de degré $d-1$ irréductible dans $\mathbf{F}_3[X]$ et l'on note $f_3 = Q(X)X$, et il existe un polynôme irréductible de degré 2 dans $\mathbf{F}_p[X]$, on note f_p la multiplication entre ce polynôme et $d-2$ polynôme de degré 1 distincts. Comme l'application π est surjective, il existe un polynôme $f \in \mathbf{Z}[X]$ qui relève les polynômes f_2, f_3 et f_p. □

Proposition 3.2.2. *Soit d un entier supérieur ou égal à deux. Alors il existe un polynôme $f \in \mathbf{Z}[X]$ de dégré d, tel que son groupe de Galois soit isomorphe à $\mathfrak{S}_d$.*

Démonstration. Soit un polynôme $f \in \mathbf{Z}[X]$, tel que décrit dans le lemme 3.2.1. D'après le théorème de Dedekind, le groupe de Galois de f sur $\mathbf{Q}$ contient une transposition, un $d-1$ cycle, et un d-cycle, de par les décomposition de f sur $\mathbf{F}_2[X]$, $\mathbf{F}_3[X]$ et $\mathbf{F}_p[X]$. Quitte à numéroter les racines de f dans un certain ordre, on peut supposer que le $d-1$ cycle est $(1, 2, \ldots, d-1)$, et quitte à conjuguer la transposition par le d-cycle, on peut supposer que la transposition est de la forme (i, d) avec $1 \leqslant i \leqslant d-1$. Or ces deux permutations engendrent $\mathfrak{S}_d$, en effet les conjugués de (i, d) par la permutation $(1, 2, \ldots, d-1)$, donnent toutes les permutations (j, d) avec $1 \leqslant j \leqslant d-1$, dont il est connu qu'elles engendrent $\mathfrak{S}_d$. □

3.3. **Théorème de Van der Waerden.**

Théorème 3.3.1 (Van der Waerden)**.** *Soit $d \geqslant 1$ un entier. Parmi les polynônes $f \in \mathbf{Z}[X]$ unitaires de degré d à coefficients dans un intervalle $[-N, N]$, la proportion de ceux qui sont irréductibles et dont le groupe de Galois est isomorphe à $\mathfrak{S}_d$ tend vers 1 lorsque N tend vers $+\infty$.*

Démonstration. Pour simplifier la preuve, on suppose $d \geqslant 4$. D'après l'inégalité de la proposition 3.1.6 pour chaque nombre premier $p \geqslant 2$ la proportion des polynômes unitaires de degré d qui sont :

- ▻ Type 1 : Irréductibles est au moins égale à $\frac{1}{2d}$
- ▻ Type 2 : Produit d'un facteur linéaire et d'un facteur irréductible est au moins $\frac{1}{2(d-1)}$
- ▻ Type 3 : Produit d'un facteur quadratique irréductible et un ou deux facteurs irréductibles disctints de degré impair est au moins $\frac{1}{8(d-3)}$. En effet, si d est impair (*resp.* pair) la partition $d = 2 + (d-2)$ (*resp.* $d = 1 + (d-3) + 2$) montre que la proportion de polynôme de cette forme est au moins $\frac{1}{2\times 2}\frac{1}{2(d-2)}$ (*resp.* $\frac{1}{2\times 2}\frac{1}{2(d-3)}\frac{1}{1}$).

La preuve de la proposition 3.2.2 nous montre que s'il existe trois nombres premiers p_1, p_2, p_3 distincts, tels que la réduction de f modulo p_i soit de type i, alors le polynôme f possède un groupe de Galois isomorphe à $\mathfrak{S}_d$.

La probabilité que le polynôme f mod p soit de l'un de ces trois types est supérieure à la probabilité d'un type en particulier, donc il existe un réel $0 < \delta < 1$, indépendant de p, tel que la proportion de polynômes modulo p ayant un des trois types de décomposition précédent est supérieure ou égale à δ. Notons que tout polynôme (unitaire de degré d) à coefficients entiers ayant ces trois types de décomposition modulo trois nombres premiers distincts a comme groupe de Galois $\mathfrak{S}_d$ (*cf* la démonstration de la proposition 3.2.2), il faut simplement éventuellement élever le produit de cycle issu du type 3 à une puissance impaire pour obtenir une transposition.

Soit $P = p_1 \dots p_r \leqslant N$ un produit de nombres premiers distincts. Le lemme chinois nous assure un isomorphisme d'anneau entre $(\mathbf{Z}/P\mathbf{Z})[X]$ et $\prod_i (\mathbf{Z}/p_i\mathbf{Z})[X]$, donc la proportion de polynômes unitaires de degré d de $(\mathbf{Z}/P\mathbf{Z})[X]$ dont aucune réduction modulo $p_1, \dots, p_r$ n'est de l'un des trois types ci-dessus est au plus $(1-\delta)^r$. En conséquence, la proportion de polynômes f tels qu'il existe un type $t \in \{1,2,3\}$ tels que pour tout p_{i_t} divisant P, la réduction de f modulo p_{i_t} ne soit pas de type t est, au plus, $3(1-\delta)^r$. Par ailleurs, un polynôme de $(\mathbf{Z}/P\mathbf{Z})[X]$ admet au plus $(\frac{2N+1}{P}+1)^d$ antécédents par l'application qui à un polynôme unitaire de degré d lui associe sa réduction modulo P. En notant Nb_d le nombre de polynômes unitaires de degré d à coefficients dans $[-N, N]$ dont les réalisations modulo $p_1, \dots, p_r$ réalisent les trois types considérés, on obient l'inégalité suivante (en calculant le nombre de polynômes qui ne satisfont pas à la condition demandée, où $(2N+1)^d$ représente le nombre de polynôme unitaires de degré d à coefficients dans $[-N, N]$) :

$$\begin{aligned}(2N+1)^d - \mathrm{Nb}_d &\leqslant 3(1-\delta)^r P^d (\tfrac{2N+1}{P}+1)^d \\ &\leqslant 3(1-\delta)^r (2N+1+P)^d \\ &\leqslant 3(1-\delta)^r 2^d (2N+1)^d \qquad \text{car } P \leqslant 2N+1\end{aligned}$$

L'on en déduit :

$$\tfrac{\mathrm{Nb}_d}{(2N+1)^d} \geqslant 1 - 3 \times 2^d (1-\delta)^r$$

Pour tout $\epsilon > 0$, il existe r assez grand tel que la proportion de polynômes unitaires de degré d à coefficients dans $\mathbf{Z}$ ayant un groupe de Galois isomorphe à $\mathfrak{S}_d$ soit supérieure à $1-\epsilon$. Ce qui conclut la preuve.

□

4. Intermède : fonction zêta de Dedekind

Comme précisé dans l'introduction, ce chapitre a pour but d'introduire des notions qui seront utiles dans la démonstration du théorème de Frobenius.

4.1. **Norme d'un idéal.**

4.1.1. *Corps de nombres.* On appelle **corps de nombres** toute extension finie du corps $\mathbf{Q}$ des nombres rationnels.

Exemple 4.1.1. L'extension $\mathbf{Q}[\sqrt{2}]$ est un corps de nombres. C'est une extension de degré 2 du corps $\mathbf{Q}$.

Soit K un corps de nombres. Tout élément $x \in K$ est racine d'un polynôme non nul dans $\mathbf{Q}[X]$. Quitte à multiplier par le pgcd des dénominateurs (s'il y en a), on peut supposer que ce polynôme est dans $\mathbf{Z}[X]$.

Définition 4.1.2. On appelle **entier algébrique** sur K tout élément $x \in K$, tel que x soit racine d'un polynôme non constant *unitaire* à coefficients dans $\mathbf{Z}$. On note O_K l'ensemble des entiers algébriques sur K.

Exemple 4.1.3. Les entiers algébriques sur $\mathbf{Q}$ sont les éléments de $\mathbf{Z}$. En effet si $\frac{p}{q} \in \mathbf{Q}$ est racine d'un polynôme P à coefficients dans $\mathbf{Z}$, alors q divise le coefficient dominant du polynôme unitaire P. Donc $q \in \{\pm 1\}$.

Proposition 4.1.4. *Soit $a \in \mathbf{C}$, alors les propositions suivantes sont équivalentes*

(1) L'élément a est un entier algébrique

(2) Le $\mathbf{Z}$-module $\mathbf{Z}[a]$ est engendré par un nombre fini d'éléments

(3) Il existe B un $\mathbf{Z}$-module de type fini tel que $\mathbf{Z}[a] \subset B$

Démonstration. On suppose (1), dans ce cas il existe un polynôme unitaire P de degré $d \geqslant 1$, tel que a soit racine de P. Montrons que la famille $\{1, a, \cdots, a^{d-1}\}$ génère $\mathbf{Z}[a]$. Pour cela, montrons par récurrence que pour tout $n \in \mathbf{N}$, l'élément a^n est dans l'ensemble engendré par la famille $\{1, a, \cdots, a^{d-1}\}$ dans $\mathbf{Z}$. Le résultat est clair pour $n = 0$, et supposons le acquis pour un entier n fixé. Alors il existe des entiers $(u_i)_{0 \leqslant i \leqslant d-1}$ tels que $a^n = \sum_{i=0}^{d-1} u_i a^i$. Par multiplication par a, on a l'égalité $a^{n+1} = \sum_{i=0}^{d-1} u_i a^{i+1}$. Or, comme a est racine du polynôme P unitaire, on peut exprimer l'élément a^d comme combinaison linéaire à coefficients dans $\mathbf{Z}$ des $\{1, a, \cdots, a^{d-1}\}$. Ce qui prouve donc que a^{n+1} est engendré par la famille $\{1, a, \cdots, a^{d-1}\}$ et termine la récurrence.

L'implication (2) $\Rightarrow$ (3) est montrée en prenant $B = \mathbf{Z}[a]$.

On suppose (3), alors il existe n tel que la famille $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ engendre B. Comme pour tout $1 \leqslant i \leqslant n$ l'élément $a\alpha_i$ est dans B, alors il existe une matrice M de taille $n \times n$ à coefficients dans $\mathbf{Z}$ telle que

$$a \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = M \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

Donc

$$(aI_n - M) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = 0$$

Ce qui signifie que a est un zéro du polynôme caractéristique de la matrice M, qui est un polynôme unitaire à coefficients dans $\mathbf{Z}$. Donc a est un entier algébrique. □

Théorème 4.1.5. *Soit K un corps de nombre. L'ensemble O_K des entiers algébriques sur K muni des lois d'addition et de multiplication déduites de $\mathbf{C}$ est un anneau.*

Démonstration. Pour démontrer ce théorème, il s'agit de montrer que pour des entiers algébriques a et b donnés, les éléments $a+b$ et ab sont algébriques. Comme les entiers a et b sont algébriques, il existe des éléments $\alpha_1, \cdots, \alpha_n$ et $\beta_1, \cdots, \beta_m$ qui génèrent respectivement $\mathbf{Z}[a]$ et $\mathbf{Z}[b]$. Ainsi les éléments $\alpha_i\beta_j$ avec $1 \leqslant i \leqslant n$ et $1 \leqslant j \leqslant m$ génèrent le $\mathbf{Z}$-module $\mathbf{Z}[a,b]$. D'après la proposition 4.1.4, les éléments $a+b \in \mathbf{Z}[a,b]$, et $ab \in \mathbf{Z}[a,b]$ sont algébriques. □

Lemme 4.1.6. *Soit K un corps de nombres. Alors pour tout $x \in K$, il existe $m \in \mathbf{N}\backslash\{0\}$ tel que $mx \in O_K$*

Démonstration. Soit $x \in K$. Comme K est de dimension finie comme $\mathbf{Q}$-espace vectoriel, il existe des éléments $\alpha_0, \cdots, \alpha_{n-1} \in \mathbf{Q}$ tels que $P(x) = x^n + \sum_{i=0}^{n-1} \alpha_i x^i = 0$. Pour tout $0 \leqslant i \leqslant n-1$, posons $\alpha_i = a_i/b_i$, où les couples (a_i, b_i) sont dans $\mathbf{Z} \times \mathbf{Z}\backslash\{0\}$. Notons m le ppcm des b_i et considérons le polynôme $Q(X) = x^n + \sum_{i=0}^{n-1} \alpha_i m^{n-i} x^i \in \mathbf{Z}[X]$. L'élément mx est alors racine de Q, en effet $Q(mx) = m^n P(x) = 0$. Donc mx est un entier algébrique. □

Il est possible formuler la remarque suivante. Si $\alpha_1, \cdots, \alpha_n$ sont des éléments de K tels que $K = \mathbf{Q}[\alpha_1, \cdots, \alpha_n]$, alors pour tout n-uplet d'entiers $(m_1, \cdots, m_n) \in (\mathbf{Z}\backslash\{0\})^n$, on a $K = \mathbf{Q}[m_1\alpha_1, \cdots, m_n\alpha_n]$.

Proposition 4.1.7. *Il existe des bases de K sur $\mathbf{Q}$ composées uniquement d'entiers algébriques.*

Démonstration. Cette proposition résulte du couplage du lemme et de la remarque précédente. □

4.1.2. *Norme.* Soit B un anneau et A un sous-anneau de B de telle sorte que B soit un A-module libre de rang fini, noté n. Pour $x \in B$, la multiplication par x, notée m_x, est un endomorphisme du A-module B.

Définition 4.1.8. On appelle norme (*resp.* trace) de $x \in B$ relativement à B et A, et on note $\mathrm{N}_{B/A}(x)$ (*resp.* $\mathrm{Tr}_{B/A}(x)$), le déterminant (*resp.* la trace) de l'endomorphisme m_x de multiplication par x.

Lorsque les notations ne prêteront pas à confusion, on se permettra l'abus de notation $\mathrm{N}(x)$ pour $\mathrm{N}_{B/A}(x)$ (*resp.* $\mathrm{Tr}(x)$ pour $\mathrm{Tr}_{B/A}(x)$).

Remarque 11. Soit K un corps de nombres de degré n. Étant fixé $x \in K$, on note s_x le morphisme de K dans $\mathbf{Q}$, qui à y associe $\mathrm{Tr}_{K/\mathbf{Q}}(xy)$. Dans ce contexte, on se place dans le cadre de la théorie des espaces vectoriels de dimension finie.

Considérons alors le morphisme $\varphi\colon K \to \mathrm{Hom}(K, \mathbf{Q})$ qui à x associe s_x. C'est une injection de K dans $\mathrm{Hom}(K, \mathbf{Q})$. En effet, si $x \in K$ est non nul,

alors il admet un inverse noté x^{-1}. Alors $\mathrm{Tr}(xx^{-1}) = \mathrm{Tr}(1) \neq 0$, donc le morphisme s_x est non nul. Enfin, comme les deux espaces sont de même dimension finie, alors le morphisme φ est une bijection. L'existence de *bases duales* sur un espace vectoriel montre alors que pour toute famille $(x_1, \cdots, x_n)$, il existe une famille $(y_1, \cdots, y_n)$, telle que $\mathrm{Tr}(x_i y_j) = \delta_{ij}$, pour $1 \leqslant i, j \leqslant n$.

Proposition 4.1.9. *Soit K un corps de nombres de degré n. L'anneau des entiers algébriques O_K est un $\mathbf{Z}$-module libre de rang fini n.*

Démonstration. On va commencer par montrer que O_K est un sous-module d'un A-module libre de rang fini. Soit $(x_1, \cdots, x_n)$ une base d'entiers algébriques de K sur $\mathbf{Q}$. Il existe d'après la proposition 4.1.7. Par la remarque 11, il existe une autre base $(y_1, \cdots, y_n)$ de K sur $\mathbf{Q}$ telle que $\mathrm{Tr}(x_i y_j) = \delta_{ij}$. Soit alors $z \in O_K$, comme $(y_1, \cdots, y_n)$ est une base de K sur $\mathbf{Q}$, il existe $b_i \in \mathbf{Q}$ tels que $z = \sum_{i=1}^{n} b_i y_i$. Par ailleurs $z x_i \in O_K$ pour tout $1 \leqslant i \leqslant n$. Donc $\mathrm{Tr}(z x_i) = \mathrm{Tr}(b_i x_i y_i) = b_i \in \mathbf{Z}$. Donc O_K est inclus dans le $\mathbf{Z}$-module libre $\sum_{j=1}^{n} \mathbf{Z} y_j$.

Comme l'anneau $\mathbf{Z}$ est principal, le théorème 2.4.1 nous assure que O_K est un module libre de rang inférieur ou égal à n. De plus comme O_K contient une base de K par la proposition 4.1.7, c'est donc un module libre de rang n. □

Proposition 4.1.10. *Soit K un corps de nombres de degré n. Soit x un élément non nul de O_K. Alors $|\mathrm{N}(x)| = \mathrm{Card}(O_K / x O_K)$*

Démonstration. Montrons déjà que l'ensemble O_K/xO_K est fini. L'anneau des entiers algébriques O_K est un $\mathbf{Z}$-module libre de rang n. Et xO_K est un sous-module de O_K. Il est aussi de rang n, car la multiplication par x est une bijection $O_K \to xO_K$. D'après le théorème 2.4.1, il existe une base $(e_1, \cdots, e_n)$ du Z-module O_K et des éléments $c_i \in \mathbf{N}\backslash\{0\}$ tels que la famille $(c_1 x_1, \cdots, c_n x_n)$ soit une base du sous-module xO_K. Alors O_K/xO_K est isomorphe au $\mathbf{Z}$-module $\prod_{i=0}^{n} \mathbf{Z}/c_i\mathbf{Z}$, donc est de cardinal fini $c_1 c_2 \cdots c_n$.

Notons u l'application $\mathbf{Z}$-linéaire de O_K sur xO_K définie par $u(e_i) = c_i e_i$ pour $i \in \{1, \cdots, n\}$. Par ailleurs, $\det(u) = c_1 c_2 \cdots c_n$ D'autre part la famille $(xe_1, \cdots, xe_n)$ est aussi une base de xO_K, il existe donc un automorphisme v du $\mathbf{Z}$-module O_K, tel que $v(c_i e_i) = x e_i$. Alors le déterminant de v est inversible dans $\mathbf{Z}$, d'où $\det(v) = \pm 1$. Mais alors, le morphisme $v \circ u$ est la multiplication par x, et son déterminant est par définition $\mathrm{N}(x)$. D'où $\mathrm{N}(x) = \det(v \circ u) = \det(v) \cdot \det(u)$. On en déduit donc l'égalité voulue : $\mathrm{N}(x) = |\mathrm{Card}(O_K/xO_K)|$. □

Lemme 4.1.11. *Soit K un corps de nombres. Soit $\mathfrak{a}$ un idéal de O_K. Alors l'ensemble quotient $O_K/\mathfrak{a}$ est fini.*

Démonstration. Soit a un élément non nul de $\mathfrak{a}$. Alors l'idéal $aO_K \subset \mathfrak{a}$. Ce qui signifie que l'anneau $O_K/\mathfrak{a}$ s'identifie à un quotient de l'anneau O_K/aO_K.

D'où $\mathrm{Card}(O_K/\mathfrak{a}) \leqslant \mathrm{Card}(O_K/aO_K)$. Or, on a vu dans la proposition précédente que cet ensemble est fini. □

Définition 4.1.12. Étant donné un corps de nombres K, et un idéal $\mathfrak{a}$ de O_K, on appelle norme de $\mathfrak{a}$ et on note $\mathrm{N}_{K/\mathbf{Q}}(\mathfrak{a})$, l'entier $\mathrm{Card}(O_K/\mathfrak{a}O_K)$.

4.2. **Fonction zêta de Dedekind.** Avant d'aborder la définition de la fonction zêta de Dedekind, rappelons quelques point sur son analogue, la fonction zêta de Riemann. Elle est définie en deux temps. D'abord comme somme de série pour les complexes de partie réelle strictement supérieure à 1. Elle peut ensuite être prolongée de manière analytique à tout le plan complexe, bien que nous ne détaillerons pas ce point.

Définition 4.2.1. On apelle **fonction zêta de Riemann**, et on note $\zeta(s)$ pour $s > 1$, la fonction définie par

$$\zeta(s) = \sum_{n>0} \frac{1}{n^s}$$

Définition 4.2.2. Soit K un corps de nombres. On note $\mathfrak{I}$ l'ensemble des idéaux non nuls de l'anneau des entiers algébriques O_K. La **fonction zêta de Dedekind** est définie pour $s > 1$ comme

$$\zeta_K(s) = \sum_{I \in \mathfrak{I}} \frac{1}{\mathrm{N}_{K/\mathbf{Q}}(I)^s}$$

Proposition 4.2.3. *Soit K un corps de nombre. Alors il existe une constante non nulle $C^\times \in K$ telle que*

$$(s-1)\zeta_K(s) \underset{s \to 1+}{\to} C^\times$$

Démonstration. Une démonstration de ce théorème pourra se trouver dans [2], chapitre VIII, théorème 5 (page 161). □

5. Théorème de Frobenius

5.1. **Résultats préliminaires.** Notons $\mathcal{P}$ l'ensemble des nombres premiers.

Proposition 5.1.1. *Soit $F \in \mathbf{Z}[X]$. Notons $n_p(F)$ le nombre de racines de F modulo p comptées avec multiplicités, et l le nombre de facteurs irréductibles de F dans $\mathbf{Q}[X]$. Alors pour $s > 1$,*

$$\sum_{p \in \mathcal{P}} n_p(F) p^{-s} = l \times \log(\frac{1}{s-1}) + \mathrm{O}(1)$$

Démonstration. Montrons que l'on peut se réduire au cas où F est irréductible. Supposons que $F = F_1 F_2$ où $F_i \in \mathbf{Z}[X]$ pour $i \in \{1, 2\}$. Alors le nombre de racine de F modulo p est le nombre de racines de F_1 additionné au nombre de racines de F_2. Et le nombre de facteurs irréductibles de F est le nombre de facteurs irréductibles de F_1 auquel on ajoute le nombre de facteurs irréductibles de F_2. Donc les termes de gauche et de droite sont additifs vis-à-vis

d'une décomposition de F en produit. On peut donc supposer le polynôme F irréductible.

Montrons que l'on peut supposer que le polynôme F est unitaire. Notons $a \in \mathbf{Z}$ le coefficient dominant de F et d le degré du polynôme. Décomposons a en facteurs premiers, $a = \prod p_i^{\alpha_i}$. Multiplions F par $n = \prod p_i^{\max(\alpha_j)d-\alpha_i}$. On peut alors effectuer le changement de variable $Y = \prod p_i^{\max(\alpha_j)} X$. En effet pour tout $1 \leqslant k \leqslant n$, on a $Y^{d-k} = \prod p_i^{(d-k)\max(\alpha_j)} X^{d-k}$, et on remarque que $\prod p_i^{(d-k)\max(\alpha_j)}$ divise n, ce qui nous autorise ce changement de variable en restant à coefficients dans $\mathbf{Z}$. De plus, ce changement de variable ne change pas la valeur de $n_p(F)$ sauf pour un nombre fini de p (les premiers p tels que $p|n$).

Posons $A_F = \mathbf{Z}[X]/(F)$ et $K = \mathrm{Frac}(A_F)$. On considère le morphisme $\varphi\colon \mathbf{Z} \hookrightarrow \mathbf{Z}[X] \twoheadrightarrow A_F$.

Lemme 5.1.2. *Ce morphisme induit un morphisme sur le spectre de ces anneaux $\psi\colon \mathrm{Spec}(A_F) \to \mathrm{Spec}(\mathbf{Z})$ qui à un idéal premier P associe l'idéal $\varphi^{-1}(P)$. De plus, ce morphisme envoie un idéal maximal sur un idéal maximal, et le cardinal de ses fibres est au plus d.*

Démonstration. Vérifions dans un premier temps que ce morphisme est bien défini. Soit donc P un idéal premier de A_F. Considérons le morphisme $\phi\colon \mathbf{Z} \xrightarrow{\varphi} A_F \xrightarrow{\pi} A_F/P$. Le noyau de ce morphisme est

$$\mathrm{Ker}(\phi) = \varphi^{-1} \circ \pi^{-1}(\{0\}) = \varphi^{-1}(P)$$

Par lemme de factorisation, on en déduit donc un morphisme injectif

$$\tilde{\psi}\colon \mathbf{Z}/\varphi^{-1}(P) \hookrightarrow A_F/P$$

Comme $\mathbf{Z}/\varphi^{-1}(P)$ s'injecte dans un anneau intègre A_F/P (en effet P est un idéal premier de A_F), alors l'anneau quotient $\mathbf{Z}/\varphi^{-1}(P)$ est intègre. Donc $\varphi^{-1}(P) \in \mathrm{Spec}(\mathbf{Z})$.

Par ailleurs, montrons que l'image d'un idéal maximal est maximal. Pour cela il suffit de montrer que si P est maximal, alors $\varphi^{-1}(P)$ n'est pas l'idéal nul. En effet, tout idéal premier non nul de $\mathbf{Z}$ est maximal. Comme P est un idéal maximal de A_F il n'est pas l'idéal nul. Soit $x \in P$ un élément non nul. Comme A_F est un $\mathbf{Z}$-module de rang fini, il existe $n \in \mathbf{N}$ et des éléments $a_i \in \mathbf{Z}$ tels que

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

Quitte à mettre x en facteur et à simplifier l'expression, on peut supposer que $a_0 \neq 0$. Or $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x \in P$ puisque $x \in P$, et $-a_0 \in \mathbf{Z}$, donc $a_0 \in P \cap \mathbf{Z} = \varphi^{-1}(P) \neq (0)$. Ce qui démontre bien que si P est un idéal maximal de A_F alors $\varphi^{-1}(P)$ est un idéal maximal de $\mathbf{Z}$.

Démontrons maintenant l'inégalité sur le cardinal des fibres. Soit (p) un idéal maximal de $\mathbf{Z}$, où p est un nombre premier. Cherchons les idéaux premiers $P \in \mathrm{Spec}(A_F)$ tels que $\varphi^{-1}(P) = (p)$. La traduction de cette égalité signifie $\{x \in \mathbf{Z}; \varphi(x) \in P\} = (p)$. De part la nature du morphisme φ on peut

se permettre l'abus de notation $(p) \subset P$ dans l'anneau A_F. Or l'ensemble des idéaux premiers P de A_F tels que $(p) \subset P$ est en bijection avec les idéaux premiers de l'anneau quotient $A_F/(p) = \mathbf{F}_p[X]/(F \bmod p)$. *Reste à dénombrer les idéaux premiers de cet anneau quotient.* On décompose alors $F \bmod p$ en produit de facteurs irréductibles $\prod_i f_i^{m_i}$, où les f_i sont tous distincts deux à deux. Le lemme chinois assure l'existence d'un isomorphisme entre $\mathbf{F}_p[X]/(F \bmod p)$ et $\prod_i \mathbf{F}_p[X]/(f_i^{m_i})$. Le nombre d'idéaux premier du second terme est majoré par d. Ce qui conclut la preuve. □

Si $(p) = P \cap \mathbf{Z}$, on dit que p divise P, et on le note $p|P$.

Par ailleurs les racines de F modulo p sont en bijection avec les morphismes $A_F \twoheadrightarrow \mathbf{F}_p$. En effet, si α est une racine de F, l'application $\psi\colon A_F \to \mathbf{F}_p$ telle que $\sum a_i x^i \mapsto \sum \bar{a_i}\alpha^i$, où $a_i \in \mathbf{Z}$, et x est l'image de X dans A_F, définit un morphisme. Réciproquement si $\psi\colon A_F \to \mathbf{F}_p$ est un morphisme, alors $\psi(x)$ est une racine de F dans $\mathbf{F}_p$.

Les morphismes $A_F \twoheadrightarrow \mathbf{F}_p$ correspondent aussi aux idéaux maximaux P de A_F tel que $\mathrm{N}(P)$ soit un nombre premier p, où $\mathrm{N}(P) = \mathrm{Card}(A_F/P)$. Ce cardinal est fini, car A_F/P est une extension de corps de $\mathbf{F}_p$. De tels idéaux maximaux sont dit "de degré 1" car en général A_F/P est une extension finie de $\mathbf{F}_p$ (de degré inférieur ou égal à d). Ainsi,

$$Z_F(s) = \sum_p n_p(F) p^{-s} = \sum_p \mathrm{Card}\{P \in \mathrm{Specmax}(A_F); p|P \text{ et } \mathrm{N}(P) = p\} p^{-s}$$

Cette série est convergente pour $s > 1$; comme $n_p(F) \leqslant d$ elle est majorée par $d \cdot \zeta_{\mathbf{Z}}(s)$, où $\zeta_{\mathbf{Z}} = \zeta$ est la fonction d'Euler-Riemann qui converge pour $s > 1$. De plus, comme $\zeta(2s)$ est bornée au voisinage de 1, on a

$$Z_F(s) = \sum_{P \in \mathrm{Specmax}(A_F)} \frac{1}{\mathrm{N}(P)^s} + \mathrm{O}(1)$$

En effet, les idéaux premiers de degré $\geqslant 2$ contribuent au maximum à hauteur de $d \cdot \zeta(2s)$. En particulier le produit

$$\zeta_{A_F}(s) = \prod_{(0) \neq P \in \mathrm{Spec}(A_F)} \frac{1}{1 - N(P)^{-s}} = \prod_P (1 + N(P)^{-s} + N(P)^{-2s} + \cdots)$$

est également convergeant pour $s > 1$, et l'on a, par développement limité :

$$\log \zeta_{A_F}(s) = Z_F(s) + \mathrm{O}(1)$$

Soit O_K l'ensemble des éléments de K entiers sur $\mathbf{Z}$; c'est un $\mathbf{Z}$-module libre de rang fini (*cf* proposition 4.1.9). L'inclusion $A_F \hookrightarrow O_K$ induit un isomorphisme de K sur K par tensorisation par $\mathbf{Q}$ sur $\mathbf{Z}$. Ainsi, à un nombre fini de facteurs près, ζ_{A_F} coïncide avec $\zeta_{O_K}(s) = \zeta_K(s)$, la fonction zêta de Dedekind. En particulier

$$\log \zeta_{O_K} = \log \zeta_{A_F} + \mathrm{O}(1)$$

La conclusion résulte alors du fait que les fonctions zêta de Dedekind ont un pôle simple en 1 (*cf.* la proposition 4.2.3).

$$\sum_{p\in\mathcal{P}} n_p(F)p^{-s} = \log(\frac{1}{s-1}) + \mathrm{O}(1)$$

□

Lemme 5.1.3. *Soit $f = X^d + b_{d-1}X^{d-1} + \cdots + b_0$ un polynôme irréductible de degré $d \geqslant 2$ à coefficients dans $\mathbf{Z}$. Choisissons un ordre sur ses racines $R_f = \{a_1, \cdots, a_d\}$; on pose $\underline{a} = (a_1, \cdots, a_d) \in \bar{\mathbf{Q}}^d$, où $\bar{\mathbf{Q}}$ désigne une clôture algébrique de $\mathbf{Q}$. Pour tout sous-groupe $S \leqslant \mathfrak{S}_d$, il existe un polynôme $\Psi_S \in \mathbf{Z}[X_1, \cdots, X_d]$ satisfaisant les conditions suivantes*

(1) Pour $s \in \mathfrak{S}_d$, on a l'égalité $s\Psi_S = \Psi_S$ si et seulement si $s \in S$

(2) Si $sS \neq s'S$ alors $s\Psi(\underline{a}) \neq s'\Psi(\underline{a})$

Démonstration. Cherchons le polynôme Ψ_S de la forme

$$\Psi_S(X_1, \cdots, X_d) = \prod_{s\in S}(u_0 + u_1X_{s(1)} + \cdots + u_dX_{s(d)})$$

où les variables u_i seront choisies plus tard dans $\mathbf{Z}$. Un tel polynôme est bien S-invariant. Le second point entraine donc le premier. En effet si $u \notin S$, alors $uS \neq S$ ce qui implique d'après (2) que $u\Psi(\underline{a}) \neq \Psi(\underline{a})$. En particulier, $u\Psi_S \neq \Psi_S$. Montrons donc le deuxième point.

Lemme 5.1.4. *Si $sS \neq s'S$, le polynôme $(s\Psi_S)(\underline{a}) - (s'\Psi_S)(\underline{a})$, vu comme élément de $\bar{\mathbf{Q}}[u_0, \cdots, u_d]$ est non nul.*

Démonstration. L'anneau $\bar{\mathbf{Q}}[u_0, \cdots, u_d]$ est factoriel et les polynômes $u_0 + u_1X_{s(1)} + \cdots + u_dX_{s(d)}$ sont irréductibles pour tout $s \in S$. En effet, le morphisme d'évaluation de $\bar{\mathbf{Q}}[u_0, \cdots, u_d]$ vers $\bar{\mathbf{Q}}[u_0]$ qui envoie u_0 sur u_0 et toutes les autres variables sur 0, ne change pas le degré du polynôme en u_0. De plus par ce morphisme, l'image du polynôme $u_0 + u_1X_{s(1)} + \cdots + u_dX_{s(d)}$ est u_0 qui est irréductible sur $\bar{\mathbf{Q}}[u_0]$. On en déduit bien que le polynôme $u_0 + u_1X_{s(1)} + \cdots + u_dX_{s(d)}$ est irréductible sur $\bar{\mathbf{Q}}[u_0, \cdots, u_d]$.

L'égalité $s\Psi(\underline{a}) = s'\Psi(\underline{a})$ entraînerait $u_0 + u_1a_{s(1)} + \cdots + u_da_{s(d)} = u_0 + u_1a_{s'\sigma(1)} + \cdots + u_da_{s'\sigma(d)}$ pour un certain $\sigma \in S$. Comme les racines sont toutes distinctes car le polynôme f est irréductible et séparable sur $\mathbf{Z}$, cela force l'égalité $s = s'\sigma$ c'est-à-dire $sS = s'S$. □

Les polynômes en les variables $(u_1, \cdots, u_d)$, à savoir $(s\Psi_S)(\underline{a}) - (s'\Psi_S(\underline{a})$ étant non nuls pour tout $sS \neq s'S$ et en nombre fini, il existe un d-uplet $(u_1, \cdots, u_d)$ tel que le polynôme Ψ_S correspondant satisfasse la seconde condition du lemme.

□

5.2. **Théorème de Frobenius.** Soit $f \in \mathbf{Z}[X]$ un polynôme de degré d, et on note R_f l'ensemble de ses racines dans une clôture algébrique de $\mathbf{Q}$.

Théorème 5.2.1 (Frobenius, 1880)**.** *Soit $f = X^d + a_{d-1}X^{d-1} + \cdots + a_0$ un polynôme de $\mathbf{Z}[X]$ irréductible de degré $d \geqslant 2$. Soit $G_f = \mathrm{Gal}(\mathbf{Q}(R_f)/\mathbf{Q}) \leqslant \mathfrak{S}_d$ son groupe de Galois. Soit λ une classe de conjugaison de $\mathfrak{S}_d$, c'est-à-dire une partition de d. Alors pour $s > 1$ tendant vers 1,*

$$\sum_{\substack{p \text{ tel que } f \bmod p \\ \text{soit de type } \lambda}} p^{-s} = \frac{g_\lambda}{g_f} \log(\frac{1}{s-1}) + \mathrm{O}(1)$$

où $g_f = \#G_f$ et g_λ est le nombre d'éléments de G_f de type λ.

Démonstration. Pour chaque $S \leqslant \mathfrak{S}_d$, choisissons un Ψ_S comme dans le lemme 5.1.3 et posons

$$f_S := \prod_{\sigma \in \mathfrak{S}_d} (X - (\sigma\Psi_S(\underline{a}))) \in \mathbf{Z}[X]$$

C'est un polynôme de degré $d!$ qui est la puissance $\#S$-ième de $\tilde{f}_S$ défini par le même produit mais restreint aux σ parcourant les représentants de $\mathfrak{S}_d/S$ (classes à gauche). Soient $\Delta = \mathrm{Disc}(f)$ et $\Delta_S = \mathrm{Disc}(\tilde{f}_S)$ leurs discriminants respectifs. Ils appartiennent tous les deux à $\mathbf{Z}\backslash\{0\}$. En effet, les polynômes sont chacun à racine simples. Les polynômes f et $\tilde{f}_S$ sont irréductibles et séparables sur $\mathbf{Z}[X]$. Soit Σ_S l'ensemble des nombres premiers divisant $\Delta\Delta_S$.

Soit $p \notin \Sigma_S$, alors les polynômes $f \bmod p$ et $\tilde{f}_s \bmod p$ sont à racines simples dans $\bar{\mathbf{F}}_p$. Choisissons un morphisme $\mathbf{Z}[X_f] \to \bar{\mathbf{F}}_p$ et notons $\{a_{1,p}, \cdots, a_{d,p}\}$ les images des racines de f par ce morphisme ; ce sont les racines de $f \bmod p$; les racines de $\tilde{f}_s \bmod p$ sont alors les $\{\sigma\Psi_S(\underline{a}_p)\}$, pour $\sigma \in \mathfrak{S}_d/S$. Le morphisme de Frobenius $\mathrm{Frob}_p \in \mathrm{Gal}(\bar{\mathbf{F}}_p/\mathbf{F}_p)$ agit sur les racines des deux polynômes par $a_{i,p} \mapsto a_{i,p}^p$ et correspond à une permutation des indices. On peut donc voir le morphisme de Frobenius comme un élément $F_p \in \mathfrak{S}_d$. Une racine du polynôme $f_S \bmod p$ est dans $\mathbf{F}_p$ si et seulement si elle est fixée par l'action de Frob_p, ce que l'on écrit :

$$\begin{aligned}(\sigma\Psi_S)(\underline{a}_p) \in \mathbf{F}_p &\Leftrightarrow \mathrm{Frob}_p(\sigma\Psi_S)(\underline{a}_p) = (\sigma\Psi_S)(\underline{a}_p) \\ &\Leftrightarrow (F_p\sigma)\Psi(\underline{a}_p) = \sigma\Psi_S(\underline{a}_p) \\ &\Leftrightarrow \sigma^{-1}F_p\sigma \in S\end{aligned}$$

On en tire :

$$n_p(f_S) = \mathrm{Card}(\{\sigma \in \mathfrak{S}_d, \sigma^{-1}F_p\sigma \in S\})$$

Remarquons que ce n'est pas le cardinal de {classe de conjugaison de $F_p\} \cap S$. Rappelons également que f_S n'est pas séparable si $S \neq \{1\}$ et que les racines ci-dessus sont comptées avec multiplicités. Notons λ le type de la permutation F_p, s_λ le nombre d'éléments de type λ dans S, $d!_\lambda$ le nombre de tels éléments dans $\mathfrak{S}_d$, et enfin $s = \mathrm{Card}(S)$.

Lemme 5.2.2. *Le cardinal de l'ensemble $\{\sigma \in \mathfrak{S}_d, \sigma^{-1}F_p\sigma \in S\}$ est égal à $s_\lambda \frac{d!}{d!_\lambda}$.*

Démonstration. Il y a s_λ éléments dans S de type λ. Pour connaître le cardinal de l'ensemble, il suffit de compter combien de fois chaque élément de type λ sera atteint. Sous l'action du groupe $\mathfrak{S}_d$ sur l'ensemble $\{F_p\}$ par $\sigma \mapsto \sigma^{-1}F_p\sigma$, on dénombre $d!_\lambda$ orbites dans $\mathfrak{S}_d$. En effet, pour tout $\sigma \in \mathfrak{S}_d$, l'élément $\sigma^{-1}F_p\sigma$ est de type λ. Par ailleurs, pour tout élément μ de type λ de $\mathfrak{S}_d$, il existe un élément σ tel que $\sigma^{-1}F_p\sigma = \mu$. Pour le démontrer, on utilise le fait que si F_p s'écrit comme produit de cycle sous la forme $(a_1 \cdots a_{r_1}) \cdots (a_{r_{n-1}} \cdots a_{r_n})$, alors $\sigma^{-1}F_p\sigma$ s'écrit de la manière suivante : $(\sigma(a_1) \cdots \sigma(a_{r_1})) \cdots (\sigma(a_{r_{n-1}}) \cdots \sigma(a_{r_n}))$.

Par ailleurs, par cette action, toutes les orbites sont de même cardinal, à savoir, $\frac{d!}{d!_\lambda}$. Donc pour chacun des s_λ éléments $s \in S$ de type λ, il existe $\frac{d!}{d!_\lambda}$ éléments $\sigma_{i,s}\mathfrak{S}_d$ tel que $\sigma_{i,s}^{-1}F_p\sigma_{i,s} = s$. □

Avec ces notations et le lemme précédent, l'égalité précédente se réécrit :

$$(\star)\ n_p(f_S) = s_\lambda \frac{d!}{d!_\lambda}$$

Soit g_f le cardinal du groupe de Galois G_f de $\mathbf{Q}(\underline{a})/\mathbf{Q}$. Comme l'extension $\mathbf{Q}(\underline{a})/\mathbf{Q}$ est normale et séparable, g_f est aussi le degré de cette extension. Pour tout $S \leqslant \mathfrak{S}_d$, on a la tour d'extension suivante $\mathbf{Q} \subset \mathbf{Q}(\Psi_S(\underline{a})) \subset \mathbf{Q}(\underline{a})$. En effet, $\Psi_S(\underline{a}) \in \mathbf{Q}(\underline{a})$. Notons maintenant c_S le degré de l'extension $\mathbf{Q}(\Psi_S(\underline{a}))/\mathbf{Q}$, et c'_S le degré de l'extension $\mathbf{Q}(\underline{a})/\mathbf{Q}(\Psi_S(\underline{a}))$. Comme $\mathbf{Q}(\underline{a})$ est un corps de décomposition de f_S sur $\mathbf{Q}(\Psi_S(\underline{a}))$, et que l'extension est séparable, son degré est égal au cardinal du groupe de Galois de cette extension. Ce cardinal est $\mathrm{Card}(G_f \cap S)(= c'_S)$. En effet, un l'élément $g \in G_f$ fixe les $\Psi_S(\underline{a})$ si et seulement si il appartient à S. Ainsi, par le théorème de la tour d'extension, le degré de l'extension $\mathbf{Q}(\Psi_S(\underline{a}))/\mathbf{Q}$ est

$$c_S := \frac{g_f}{\mathrm{Card}(G_f \cap S)}$$

Pour un sous-groupe S donné, les conjugués (sur $\mathbf{Q}$) de $\Psi_S(\underline{a})$ sont donc au nombre de c_S ; ce sont des racines de f_S : $\sigma_1\Psi_S(\underline{a}), \cdots, \sigma_{c_S}\Psi_S(\underline{a})$, pour des $\sigma_i \in \mathfrak{S}_d$ convenables. Pour chaque $\sigma \in \mathfrak{S}_d$, la fonction polynomiale $\sigma\Psi_S$ satisfait aux conditions du lemme 5.1.3, pour le sous-groupe $S_\sigma := \sigma S\sigma^{-1}$ de $\mathfrak{S}$. Notons

$$g_{\sigma,S} = \mathrm{Card}(G_f \cap S_\sigma)$$

le cardinal de cette intersection. En vertu de la formule précédente, les $\sigma_i\Psi_S(\underline{a})$ sont de degré $\frac{g_f}{g_{\sigma_i,S}}$ sur $\mathbf{Q}$ (en appelant degré d'un élément, le degré de son polynôme minimal). Comme ils sont tous conjugués, on a $\frac{g_f}{g_{\sigma_i,S}} = c_S = \frac{g_f}{g_{e,S}}$. Finalement,

$$g_f = c_S g_{e,S} = \sum_{i=1}^{c_S} g_{\sigma_i,S}$$

En effet, pour la dernière égalité

$$\sum_{i=1}^{c_S} g_{\sigma_i,S} = \sum_{i=1}^{c_S} \frac{g_f}{c_S} = g_f$$

Si l'on somme sur tous les $\sigma \in \mathfrak{S}_d$ cette égalité, on obtient

$$\sum_{\sigma\in\mathfrak{S}_d} g_{\sigma,S} = m_S g_f$$

où m_S est le nombre de facteurs irréductibles de f_S. En effet, le raisonnement précédent montre que la somme des $g_{\sigma_i,S}$ (avec σ_i tels que les $\sigma_i\Psi_S(\underline{a})$ sont exactement les racines d'un facteur irréductible) vaut g_f. Par ailleurs les ensembles $\{\sigma_i \ ; \ \sigma_i\Psi_S(\underline{a})$ soit une racine de $f_j\}_j$, où f_j est un facteur irréductible de f_S, forment une partition de $\mathfrak{S}_d$.

Enfin, en regroupant par type :

$$\sum_{\lambda} \underbrace{\sum_{\sigma\in\mathfrak{S}_d} (\text{nombre d'élément de } S_\sigma \cap G_f \text{ de type } \lambda)}_{=s_\lambda g_\lambda \frac{d!}{d!_\lambda}}$$

où l'égalité sous l'accolade résulte du fait que, si $s_1, \cdots, s_{s_\lambda}$ sont des éléments de S de type λ et $g_1, \cdots, g_{g_\lambda}$ des éléments de type λ de G_f, pour chaque $\sigma \in \mathfrak{S}_d$, les $\sigma s_i \sigma^{-1}$ sont les éléments de type λ dans S_σ et $\mathrm{Card}(\{\sigma, \ \sigma s_i\sigma^{-1} = g_j\}) = \frac{d!}{d!_\lambda}$

Les égalités précédentes se combinent pour donner

$$(\star\star) \ m_S = \frac{d!}{g_f} \sum_{\lambda} \frac{s_\lambda g_\lambda}{d!_\lambda}$$

On a alors les égalités utilisant la proposition 5.1.1 :

$$\begin{array}{ccc} \sum\limits_{p\notin\Sigma_S} n_p(f_S)p^{-s} & \overset{(\star)}{=} & \sum\limits_{\lambda} s_\lambda \frac{d!}{d!_\lambda}(\sum\limits_{p} p_\lambda^{-s}) \\ & \overset{\zeta(1)=\infty \text{ et } (\star\star)}{=} & \frac{d!}{g_f}(\sum\limits_{\lambda} \frac{s_\lambda g_\lambda}{d!_\lambda}) \log(\frac{1}{s-1}) + \mathrm{O}_S(1) \end{array}$$

où $\sum\limits_{p} p_\lambda^{-s}$ est la somme sur les p tel que $f \bmod p$ soit de type λ. Posons : $\sum\limits_{p} p_\lambda^{-s} = \frac{g_\lambda}{g_f}\log(\frac{1}{s-1}) + \mathrm{R}_\lambda(s)$ On veut montrer que $\mathrm{R}_\lambda = \mathrm{O}(1)$, c'est-à-dire que $\mathrm{R}_\lambda(s)$ reste bornée quand $s \to 1+$. Avec ces notions les égalités précédentes deviennent :

$$(\star\star\star) \sum_{\lambda} \frac{s_\lambda}{d!_\lambda} \mathrm{R}_\lambda = \mathrm{O}_S(1)$$

Jusqu'à présent, le sous-groupe S était fixe. On va utiliser des groupes variables pour démontrer $\mathrm{R}_\lambda = \mathrm{O}(1)$ par récurrence. Introduisons l'ordre partiel suivant les types d'éléments de $\mathfrak{S}_d$. On dira que $\lambda' < \lambda$ si et seulement si les nombres d'orbites correspondants vérifient l'inégalité opposée.

Par exemple, l'élément minimal est le type de l'identité et l'élément maximal est le type d'un d-cycle. Soient $s \in \mathfrak{S}_d$ un élément de type λ et $S = \langle s \rangle$ le sous-groupe engendré. Compte tenu du fait que S n'a aucun élément de type $\lambda' > \lambda$ (le nombre d'orbite augmente en élevant à une puissance), l'égalité $(\star\star\star)$ devient :

$$\frac{s_\lambda}{d!_\lambda}\mathrm{R}_\lambda + \sum_{\lambda'<\lambda} \frac{s_{\lambda'}}{d!_{\lambda'}}\mathrm{R}_{\lambda'} = \mathrm{O}_S(1)$$

Ainsi, grâce à l'hypothèse de récurrence, R_λ est une combinaison linéaire de fonctions bornées au voisinages de $1+$. Il ne reste plus qu'à remarquer que, pour λ_0 le type de l'identité, $\mathrm{R}_{\lambda_0} = \mathrm{O}_e(1)$; la récurrence est donc amorcée. Cela achève la démonstration du théorème de Frobenius.

□

Annexe A. Polynômes symétriques et discriminant

Soit k un anneau, et $n \in \mathbf{N}$. Étant donné un polynôme $f = \prod_{i=1}^n (X - x_i) \in k[x_1, \cdots, x_n, X]$, on définit les fonctions symétriques des racines, notées $\sigma_i \in k[x_1, \cdots, x_n]$, de telle sorte qu'on puisse écrire le polynôme f sous la forme,

$$f = \sum_{i=0}^{n} (-1)^i \sigma_i X^i$$

Définition A.0.1. Soit $g \in k[x_1, \cdots, x_n, X]$ un polynôme. On dit que le polynôme g est symétrique (en les x_i) si pour tout $\tau \in \mathfrak{S}_n$, on a l'égalité suivante :

$$g(x_1, \cdots, x_n, X) = g(x_{\tau(1)}, \cdots, x_{\tau(n)}, X)$$

Théorème A.0.2. *Soit $g \in k[x_1, \cdots, x_n, X]$ un polynôme symétrique. Alors il existe un polynôme $h \in k[\sigma_1, \cdots, \sigma_n, X]$ tel que :*

$$g(x_1, \cdots, x_n, X) = h(\sigma_1, \cdots, \sigma_n, X)$$

Démonstration. On peut trouver une preuve de ce théorème dans [1], à la page 30, bien que la formulation soit quelque peut différente, il s'agit bien du même théorème. □

Définition A.0.3. Soit $n \geqslant 2$ variables $x_1, \cdots, x_n$ sur un corps k. On définit le discriminant comme étant le polynôme :

$$\Delta(x_1, \cdots, x_n) := \prod_{i<j} (x_i - x_j)^2$$

Le nombre de facteur dans ce produit est $\binom{n}{2}$. De plus, on constate l'égalité $(x_i - x_j)^2 = -(x_i - x_j)(x_j - x_i)$, d'où

$$\Delta = (-1)^{\frac{1}{2}n(n-1)} \prod_{i \neq j} (x_i - x_j)$$

Proposition A.0.4. *Le discriminant Δ est un élément de $k[\sigma_1, \cdots, \sigma_n]$*

Démonstration. Le polynôme Δ est clairement symétrique, la proposition est un corollaire immédiat du théorème A.0.2. □

Soit $f \in k[X]$ un polynôme de degré $n \geqslant 1$. On note Ω une clôture algébrique de k. Dans l'extension de corps Ω, le polynôme f est scindé, il existe donc $\alpha_1, \cdots, \alpha_n \in \Omega$, non nécéssairement distincts, tels que $f = (X - \alpha_1) \cdots (X - \alpha_n)$.

Définition A.0.5. Le discriminant du polynôme f est défini comme étant

$$\Delta(f) := \Delta(\alpha_1, \cdots, \alpha_n)$$

Remarque 12. Par convention, si f est un polynôme de degré 1, on posera $\Delta(f) = 1$.

Proposition A.0.6. *L'élément* $\Delta(f)$, a priori *élément de* Ω *est un élément de* k.

Démonstration. Par la proposition A.0.4,

$$\Delta(f) \in k[\sigma_1(\alpha_1, \cdots, \alpha_n), \cdots, \sigma_n(\alpha_1, \cdots, \alpha_n)] = k$$

□

Références

1. David A. Cox, *Galois theory*, 1 ed., Wiley-Blackwell, 2004.
2. Serge Lang, *Algebraic number theory*, Springer-Verlag, 1986.
3. ———, *Algebra*, 3 ed., Springer-Verlag, 2002.
4. Daniel A. Marcus, *Number fields*, Springer, 1977.
5. Pierre Samuel, *Théorie algébrique des nombres*, Hermann Paris, 1967.
6. P. Stevenhagen and H.W Lenstra, Jr, *Chebotarev and his density theorem*, The Mathematical Intelligencer **18** (2002), no. 2.
7. Ian Stewart, *Galois theory*, Chapman and Hall, 1973.