David Hernandez et Yves Laszlo

INTRODUCTION À LA THÉORIE DE GALOIS

David Hernandez et Yves Laszlo

David Hernandez : Université Paris-Cité, Institut de Mathématiques de Jussieu-Paris Rive Gauche, B Sophie Germain, Case 7012, 75205 Paris Cedex 13, France.

E-mail : david.hernandez@imj-prg.fr

Yves Laszlo : Université Paris-Saclay, Département de Mathématiques, 91405 Orsay Cedex, France.

E-mail : yves.laszlo@math.u-psud.fr

February 14, 2023

INTRODUCTION À LA THÉORIE DE GALOIS

David Hernandez et Yves Laszlo

La théorie de Galois est née au XIX ème siècle pour étudier l'existence de formules pour les solutions d'une équation polynomiale (en fonction des coefficients de l'équation). Cette théorie, à la fois puissante et élégante, fut à l'origine d'un pan entier de l'algèbre moderne, et a depuis connu un développement considérable. Elle demeure un sujet de recherche extrêmement actif.
L'objet de ce cours est dans un premier temps d'introduire les bases et outils d'algèbre générale (groupes, anneaux, algèbres, quotients, extensions de corps...) qui permettront dans un deuxième temps de développer la théorie de Galois, ainsi que certaines de ses applications les plus remarquables.
Au delà de l'intérêt propre du sujet, le cours se veut être une bonne introduction à l'algèbre et à ses diverses applications, tant en mathématiques que dans d'autres disciplines (informatique avec les corps finis, physique ou chimie avec la théorie des groupes par exemple). Ainsi, aucun prérequis n'est nécessaire.

Galois theory appeared in the XIXth century to study the existence of formulas for solutions of polynomial equations (in terms of the coefficients of the equation). This extremely powerful and efficient theory gave birth to an extensive part of modern algebra theory. Nowadays it is a very active research area.
We will first introduce basics of Algebra (groups, rings, algebras, quotients, field extensions...) so that we can explain and prove fundamental results of Galois theory, as well as some of its most striking applications.
Beyond the importance of the subject, the course is a good introduction to Algebra and its applications in various domains, certainly in mathematics, but also in Computer Science (finite fields), Physics or Chemistry (group theory) for instance.
No prerequisite is necessary.

FIGURE 1. Évariste Galois

Dans la nuit du 29 Mai 1832 , Évariste Galois [1] sait sa mort proche. Il écrit une lettre-testament [2] adressée à son ami Auguste Chevalier dont voici un fac-similé.

1. 1811-1832
2. Voir [**Ga**].

Je ferai voir en outre que l'on peut toujours transformer une intégrale simple en une autre dans laquelle la période de la première soit devenue égale à un nombre entier p, et les $2n-1$ autres restent les mêmes.

Je vous dirai donc à propos que des intégrales où les périodes soient les mêmes à part et d'autre, et telles proportionnelles que n terme de l'une s'exprimant dans l'autre, l'équation qu'une telle dépendra au moyen de cette de Galois et réciproquement. Ici nous ne savons rien.

Je dois, mon cher Auguste, que ces sujets ne sont pas les seuls que j'ai explorés. Mes principales méditations depuis quelque temps étaient dirigées sur l'application à l'analyse transcendante de la théorie de l'ambiguité. Il s'agissait de voir à priori dans une relation entre des quantités ou quantités fonctions transcendantes quelles échanges on pouvait faire, quelles quantités on pouvait substituer aux quantités données sans que la relation fût cesse d'avoir lieu. Cela fait reconnaître d'avance l'impossibilité de beaucoup d'expressions que l'on pourrait chercher. Mais je n'ai pas le temps et mes idées ne sont pas encore bien développées sur ce terrain qui est immense.

Je ferai imprimer cette lettre dans la revue Encyclopédique.

Je me dis souvent dans ma vie Barrande à avancer des propositions dont je n'étais pas sûr. Mais tout ce que j'ai écrit là est depuis bientôt un an dans ma tête, et il est trop d'un intérêt de ne pas me tromper pour que je ne sois longuement assuré des théorèmes dont je vous parle sans en donner la démonstration complète.

Vous ~~pourrez~~ ferez publiquement Jacobi ou Jacobi de donner leur avis sur la vérité, mais sur l'importance des théorèmes.

Après cela il se trouvera, j'espère, des gens qui trouveront leur profit à déchiffrer tout ce gâchis.

Je t'embrasse avec affection. E. Galois Le 29 Mai 1832.

Voici la transcription de la fin. *[...]Je me suis souvent hasardé dans ma vie à avancer des propositions dont je n'étais pas sûr. Mais tout ce que j'ai écrit là est depuis bientôt un an dans ma tête, et il est trop de mon intérêt de ne pas me tromper pour qu'on me soupçonne d'avoir énoncé des théorèmes dont je n'aurais pas la démonstration complète. Tu prieras publiquement Jacobi et Gauss de donner leur avis, non sur la vérité, mais sur l'importance des théorèmes. Je t'embrasse avec effusion.*

Le premier feuillet de la lettre précitée commence comme suit. Même si le style paraît un peu abscons, le lecteur reconnaîtra d'abord la définition d'un sous-groupe distingué (1.2.1) puis le théorème de résolubilité 7.4.2 des équations algébriques.

I

LETTRE A AUGUSTE CHEVALIER

Paris, le 29 Mai 1832.

Mon cher Ami,

8 a J'ai fait en analyse plusieurs choses nouvelles.

Les une concernent la théorie des Équations, les autres les fonctions Intégrales.

Dans la théorie des équations, j'ai recherché dans quels cas les équations étaient résolubles par des radicaux : ce qui m'a donné occasion d'approfondir cette théorie, et de décrire toutes les transformations possibles sur une équation lors même qu'elle n'est pas soluble par radicaux.

* On pourra faire avec tout cela trois mémoires.

Le premier est écrit, et malgré ce qu'en a dit Poisson, je le maintiens avec les corrections que j'y ai faites.

* Le second contient des applications assez curieuses de la théorie des équations. * Voici le résumé des choses les plus importantes :

1° D'après les propositions II et III du 1er Mémoire, on voit une grande différence entre adjoindre à une équation une des racines d'une équation auxiliaire, ou les adjoindre toutes.

Dans les deux cas le groupe de l'équation se partage par l'adjonction en groupes tels que l'on passe de l'un à l'autre par une même substitution. Mais la condition que * ces groupes aient les mêmes substitutions n'a lieu certainement que dans le second cas. * Cela s'appelle la décomposition propre.

En d'autres termes, quand un groupe ⌜G⌝ en contient un autre H le groupe G peut se partager en groupes * que l'on obtient chacun

en opérant sur les permutations de H une même substitution, en sorte $G = H + HS + HS' + \ldots$ et aussi il peut se décomposer en groupes qui ont tous les mêmes substitutions en sorte que $G = H + TH + T'H + \ldots$.

Ces deux ⌜genres de⌝ décompositions ne coïncident pas ordinairement. Quand elles coïncident, la décomposition est dite propre.

Il est aisé de voir que quand ⌜le groupe d'⌝ une équation n'est susceptible d'aucune décomposition propre, on aura beau transformer cette équation, les groupes des équations transformées auront toujours le même nombre de permutations.

Au contraire quand * le groupe d'une équation est susceptible d'une décomposition propre en sorte qu'il se partage en M groupes **8 b** de N permutations, on pourra résoudre l'équation donnée au moyen de deux équations : l'une aura un groupe de M permutations, l'autre un de N permutations.

Lors donc qu'on aura épuisé * sur le groupe ⌜d'une équation⌝ tout ce qu'il y a de décompositions propres possibles sur ce groupe, on arrive à des groupes qu'on pourra transformer, mais dont les permutations seront toujours en même nombre.

Si ces groupes ont chacun un nombre premier de permutations l'équation * sera soluble par radicaux. Sinon, non.

Le plus petit nombre de permutations que puisse avoir un groupe * indécomposable quand ce nombre ⌜n'est pas⌝ premier est 5.4.3.

2° Les * décompositions les plus simples sont celles qui ont lieu par la Méthode de M. Gauss.

* Comme ces décompositions sont évidentes même dans la forme actuelle du groupe de l'équation, il est inutile de s'arrêter longtemps sur cet objet.

Quelles décompositions sont praticables sur une équation qui ne se * simplifie pas par la méthode de M. Gauss ?

J'ai appelé primitives les équations qui * ne peuvent pas se simplifier par la méthode de M. Gauss : non que ces équations soient réellement indécomposables, puisqu'elles peuvent même se résoudre par radicaux.

Comme lemme à la théorie des équations primitives solubles par radicaux, j'ai * mis en juin 1830 dans le bulletin férussac, une analyse sur les imaginaires de la théorie des nombres.

INTRODUCTION

L'objet de ce cours est de montrer à quel point des domaines qui *a priori* sont sans grand rapport, la théorie des groupes et celle des extensions de corps, sont intimement liés. Ce lien profond mis en lumière au XIXème siècle par Galois [3] permet de donner des résultats importants en arithmétique [4]. Même si, faute de temps, on n'a guère pu présenter de résultats modernes, la théorie de Galois et ses extensions tiennent actuellement une place centrale en Mathématiques. La compréhension des groupes de Galois des corps de nombres est très partielle, même si des progrès spectaculaires ont été réalisés ces cinquante dernières années. On a préféré dans ce cours sacrifier à la tradition en ne donnant que les grandes lignes des solutions de problèmes classiques et séculaires qu'apportent la théorie de Galois (constructibilité à la règle et au compas par exemple), pour aller plus avant dans l'exposition de méthodes algébriques puissantes (introduction à la réduction modulo p des groupes de Galois (8)) ou de résultats récents (quelques résultats de théorie de Galois inverse (9.6)). On n'a pas non plus cherché à développer des méthodes sophistiquées de calcul algorithmique de groupes de Galois, qui existent, mais qui constituent, à notre sens, plutôt des problèmes "d'experts". On n'a pas abordé non plus la théorie des résolvantes. On a disséminé des exercices tout au long du texte, qui, la plupart du temps, sont très simples mais permettront de "se faire la main" ainsi que de vérifier si les notions sont assimilées. On invite le lecteur à ne consulter les indications de preuve qu'en dernière extrémité.

3. On pourra trouver dans [**Eh**] une présentation historique récente.
4. La "reine des sciences" comme disait Gauss.

FIGURE 2. Alexandre Grothendieck

Les extensions de la théorie sont très nombreuses. Par exemple, on ne saurait trop conseiller au lecteur d'étudier la théorie des revêtements ramifiés finis des surfaces de Riemann S. Il verra alors que cette étude est équivalente à l'étude des groupes de Galois des extensions finies du corps des fonctions méromorphes de S ! Concernant la bibliographique, on pourra se reporter aux beaux livres d'A. Chambert-Loir [**CL**] ou de R. Elkik [**El**]. Pour aller plus loin, en particulier dans l'étude de la séparabilité, [**B2**] est un classique.

Ce cours, qui se veut assez élémentaire, souffre encore de l'absence du produit tensoriel qui à lui seul aurait rendu bien des preuves nettement plus naturelles. Hélas, le temps manque. Plus généralement, la théorie de Galois a été largement généralisée et n'est en fait qu'un cas particulier de la vaste théorie de la descente fidèlement plate de Grothendieck exposée dans [**Gr**], qui, en un sens, est plus simple et plus géométrique.

Si cet ouvrage n'est guère accessible à ce stade, ce point de vue très géométrique a été exposé pour la théorie de Galois dans le très joli livre de R. et A. Douady [**D**], ouvrage dont la lecture ne saurait trop être conseillée. Il explique l'analogie entre corps de nombres et surfaces de Riemann et le dictionnaire galoisien entre extensions de corps et revêtements étales. Il aborde la très riche et largement ouverte théorie des *dessins d'enfants* de Grothendieck [5], qui fait le pont entre la théorie des surfaces de Riemann et l'arithmétique via l'étude du groupe de Galois de $\bar{\mathbf{Q}}$ sur $\mathbf{Q}$.

Ce cours se veut donc une invitation au voyage plus qu'un exposé exhaustif qui aurait nécessité plus de place.

D'un point de vue technique, nous nous sommes en particulier limités aux corps parfaits ce qui a permis d'éviter les discussions sur les extensions séparables. Il nous a paru ne

5. 1928-

pas nuire à la compréhension des méthodes, ce d'autant que ce cadre recouvre de très nombreux problèmes actuels. On ne s'est pas restreint aux corps de caractéristique nulle pour avoir une théorie englobant le cas des corps finis qui, on le verra (8), est de toute manière utile pour calculer les groupes de Galois intervenant en caractéristique nulle.
Les passages en petits caractères peuvent être parcourus rapidement en première lecture. Il s'agit en général d'approfondissements intéressants.
On a volontairement cherché à aller au plus court dans les preuves tant que celles-ci restaient "naturelles", sans chercher à les généraliser inutilement (cf. par exemple les discussions sur les entiers algébriques).

Puissent la beauté et la puissance de cette merveilleuse théorie toucher le lecteur.

INVITATION À LA THÉORIE DE GALOIS

Nous allons esquisser, de manière assez informelle, deux succès historiquement importants de la théorie de Galois. Dans cette invitation, on n'utilisera que le fait bien connu que la donnée d'un sous-corps k d'un corps K munit K d'une structure de k-espace vectoriel. La dimension, finie ou non, se note $[\mathrm{K} : k]$ et s'appelle aussi le degré de *l'extension* K/k.
Le début du cours proprement dit commence au Chapitre 1.

0.1. Construction à la règle et au compas

On identifie le plan euclidien (orienté) à $\mathbf{C}$ muni de la norme usuelle $||z||=|z|$.
Pour deux points A, B distincts de $\mathbf{C}$, l'unique droite passant par A et B est notée $\langle \mathrm{A}, \mathrm{B} \rangle$.
Pour A un point de $\mathbf{C}$ et R un nombre réel positif, le cercle de centre A et de rayon R est noté $\mathrm{C}(\mathrm{A}, \mathrm{R})$. Un lieu géométrique qui est une droite ou un cercle est appelé un "cercle-droite".

Définition 0.1.1. — *On dira qu'un point* $\mathrm{P} \in \mathbf{C}$ *est* constructible *s'il existe une suite finie de points* $\mathrm{P}_0, \cdots, \mathrm{P}_\mathrm{N} = \mathrm{P}$ *telle que* $\mathrm{P}_0 = 0$, $\mathrm{P}_1 = 1$ *et pour tout* $n < \mathrm{N}$ *le point* P_{n+1} *est dans l'intersection de deux cercle-droites différents de type* $\langle \mathrm{P}_\alpha, \mathrm{P}_\beta \rangle$ *avec* $0 \leq \alpha < \beta \leq n$ *ou de type* $\mathrm{C}(\mathrm{P}_\gamma, |\mathrm{P}_\alpha - \mathrm{P}_\beta|)$ *avec* $0 \leq \alpha, \beta, \gamma \leq n$.

Notons que les deux cercle-droites différents dont on considère l'intersection peuvent être du même type.
Explicitons la définition : on décide d'abord que 0 et 1 sont constructibles. Puis, récursivement, étant donnée une famille de points constructibles, on construit les droites passant par deux points constructibles distincts, ou bien un cercle centré sur un de ces points, de

rayon une distance entre deux points constructibles : ceci définit les cercle-droites admissibles. Les points constructibles au rang $n+1$ sont les points constructibles au rang n, ainsi que les intersections finies entre deux cercle-droites admissibles.
Par exemple, le nombre complexe i est constructible.
Le lecteur se souviendra des théorèmes de Thales et Pythagore et montrera les propriétés

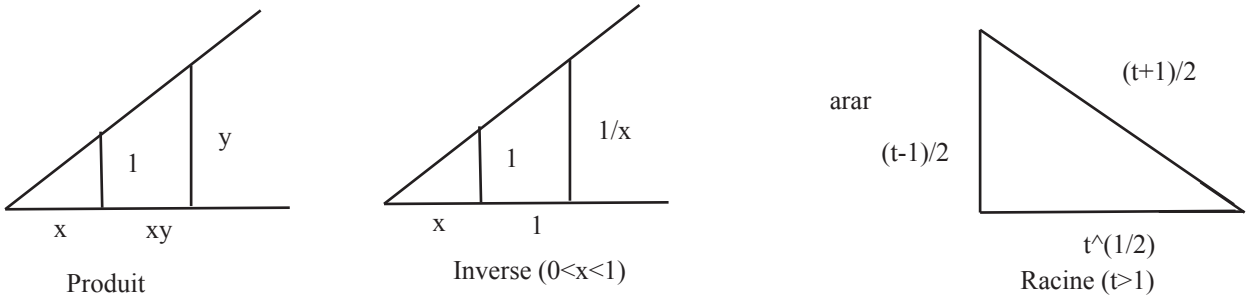


FIGURE 3. Constructions utiles

de l'exercice suivant.

Exercice 0.1.2. — *L'ensemble des nombres réels constructibles est un sous-corps de* $\mathbf{R}$ *(en particulier il contient les nombres rationnels). Un nombre réel positif est constructible si et seulement si sa racine carrée l'est. Le nombre complexe z est constructible si et seulement ses parties réelles et imaginaires le sont, de sorte que les nombres complexes constructibles forment un sous-corps de* $\mathbf{C}$.

Nous montrerons (6.5.1) le résultat suivant.

Théorème 0.1.3 **(Wantzel [6])**. — *Un nombre complexe z est constructible si et seulement si il existe une suite finie de corps $\mathrm{L}_0 = \mathbf{Q} \subset \mathrm{L}_1 \cdots \subset \mathrm{L}_n$ tels que pour chaque i, $[\mathrm{L}_{i+1} : \mathrm{L}_i] = 2$ et $z \in \mathrm{L}_n$.*

Lorsque cette condition est vérifiée, on a en particulier que $[\mathbf{Q}[z] : \mathbf{Q}]$ est finie et est une puissance de 2.

6. 1814-1848

Par exemple, π étant transcendant (9.3), on en conclut l'impossibilité de la quadrature du cercle : on ne peut pas construire à la règle et au compas un carré de même aire que le disque unité.

On peut aussi en déduire par exemple que l'on ne peut pas construire à la règle et au compas un heptagone régulier. En effet, sinon, la dimension de $\mathbf{Q}[\exp(\frac{2i\pi}{7})]$ sur $\mathbf{Q}$ serait une puissance de 2. Or, nous montrerons le résultat suivant (6.3.8).

Proposition 0.1.4 **(Gauss [7])**. — *On a* $[\mathbf{Q}[\exp(\frac{2i\pi}{n})], \mathbf{Q}] = \varphi(n)$ *où* φ *est l'indicateur d'Euler [8] et* $\mathbf{Q}[\exp(\frac{2i\pi}{n})]$ *est le corps engendré par* $\exp(\frac{2i\pi}{n})$*, qui est aussi l'ensemble des polynômes en* $\exp(\frac{2i\pi}{n})$ *à coefficients rationnels.*

La formule $\varphi(7) = 7 - 1 = 6$ implique le résultat.

Généralement donc, si le polygone régulier à n côtés est constructible, alors $\varphi(n)$ est une puissance de 2. On verra qu'alors n est le produit d'une puissance de 2 par un nombre fini de nombres premiers de Fermat F_m. On rappelle ici que le nombre de Fermat F_m est $\mathrm{F}_m = 2^{2^m} + 1$. Ce résultat est dû à Gauss.

Ces résultats *ne font pas* intervenir la théorie de Galois [9]. Cette dernière est par contre cruciale pour la réciproque, qui avait été conjecturée semble-t-il par Gauss.

FIGURE 4. Karl Friedrich Gauss

FIGURE 5. Leonhard Euler

Il avait deviné juste :

Théorème 0.1.5 **(Gauss-Wantzel)**. — *La réciproque est vraie : si* n *est un produit d'une puissance de* 2 *et d'un nombre fini de nombre premiers de Fermat distincts, alors le polygone régulier à* n *côtés est constructible.*

8. 1777-1855
8. 1707-1783
9. 1811-1832

En fait la preuve donne presque un algorithme pour construire un polygone régulier à n côtés (lorsque c'est possible !) : on doit décomposer n en facteurs premiers *et* trouver un générateur du groupe cyclique $(\mathbf{Z}/p\mathbf{Z})^*$. Notons qu'on a $\mathrm{F}_0 = 3, \mathrm{F}_1 = 5, \mathrm{F}_2 = 17, \mathrm{F}_3 = 257, \mathrm{F}_4 = 65537$ et qu'ils sont tous premiers. Si les constructions des triangles équilatéraux, carrés, et pentagones réguliers sont élémentaires, celle du polygone régulier à 17 côtés est moins évidente [10]...

Rappelons d'abord la construction (connue de Ptolémée [11], premier siècle de notre ère) du pentagone régulier, simple conséquence de la formule élémentaire

$$\cos\left(\frac{2\pi}{5}\right) = \frac{\sqrt{5}-1}{4}.$$

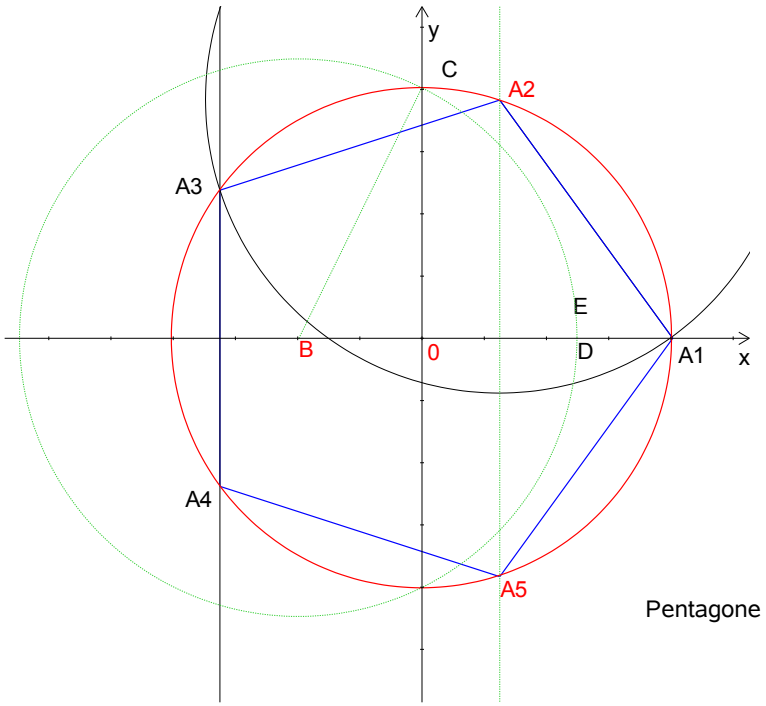


FIGURE 6. Construction du pentagone régulier

10. Cf. http://pagesperso-orange.fr/debart/geoplan/polygone_regulier.html, dont les constructions explicites suivantes sont tirées.

11. ∼90-168

FIGURE 7. Claudius Ptolémée

Gauss, encore lui, a donné une construction du polygone à 17 côtés ; voici une construction :

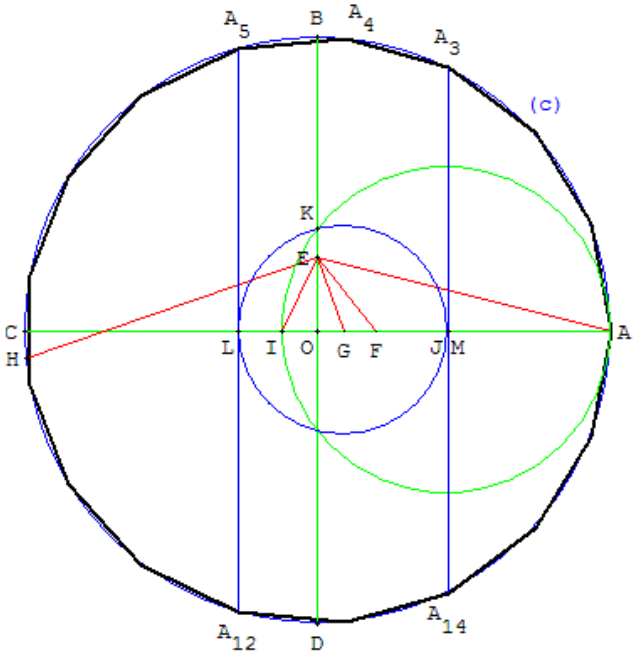


FIGURE 8. Construction de l'heptadécagone régulier

On a ici déjà une formule assez compliquée

$$16\cos\left(\frac{2\pi}{17}\right) = -1+\sqrt{17}+\sqrt{34-2\sqrt{17}}+\sqrt{68+12\sqrt{17}-4\sqrt{34-2\sqrt{17}}-8\sqrt{34+2\sqrt{17}}},$$

formule qui se déduit d'ailleurs de la théorie de Galois et qui permet de donner effectivement une construction.

En revanche, F_5 est divisible par 641 (Euler). On ne sait pas si F_{33} est premier, alors qu'on sait que $F_{2478782}$ ne l'est pas : peu de choses sont connues sur la primalité des nombres de Fermat.

La réciproque, elle, fait intervenir la théorie de Galois : c'est une conséquence du calcul du groupe de Galois $\mathrm{Gal}(\mathbf{Q}[\exp(\frac{2i\pi}{n})], \mathbf{Q})$ (cf. 6.3.10).

0.2. Résolution d'équations

Les solutions $x = \pm\sqrt{a}$ de l'équation quadratique $x^2 - a = 0$, $a \in \mathbf{C}$, sont bien connues. En général, pour l'équation de degré n, une habile translation de la variable annule le terme de degré $n-1$. En degré 3, on a donc affaire à l'équation $x^3 + ax + b = 0$ dont les solutions ont été achetées au 16ème siècle par Cardan [12] au mathématicien Tartaglia [13] (mais étaient sans doute connues de del Ferro [14]). Elles s'écrivent

$$\begin{aligned}
x_1 &= \sqrt[3]{-\frac{b}{2} + \sqrt{(\frac{a}{3})^3 + (\frac{b}{2})^2}} + \sqrt[3]{-\frac{b}{2} - \sqrt{(\frac{a}{3})^3 + (\frac{b}{2})^2}} \\
x_2 &= j\sqrt[3]{-\frac{b}{2} + \sqrt{(\frac{a}{3})^3 + (\frac{b}{2})^2}} + j^2\sqrt[3]{-\frac{b}{2} - \sqrt{(\frac{a}{3})^3 + (\frac{b}{2})^2}} \\
x_3 &= \bar{j}\sqrt[3]{-\frac{b}{2} + \sqrt{(\frac{a}{3})^3 + (\frac{b}{2})^2}} + \bar{j}^2\sqrt[3]{-\frac{b}{2} - \sqrt{(\frac{a}{3})^3 + (\frac{b}{2})^2}}
\end{aligned}$$

avec $j = \exp(\frac{2i\pi}{3})$, les racines cubiques étant normalisées par

$$\sqrt[3]{-\frac{b}{2} + \sqrt{(\frac{a}{3})^3 + (\frac{b}{2})^2}}\sqrt[3]{-\frac{b}{2} - \sqrt{(\frac{a}{3})^3 + (\frac{b}{2})^2}} = -\frac{a}{3}.$$

12. 1501-1576
13. 1499-1557
14. 1465-1526

Un élève de Cardan, Ferrari [15], a découvert comment ramener les équations de degré 4 à celles de degré 3. On part de l'équation

$$x^4 = ax^2 + bx + c$$

qui équivaut, y étant un paramètre, à l'équation

$$x^4 + 2yx^2 + y^2 = (a + 2y)x^2 + bx + (c + y^2).$$

On cherche y tel que $(a+2y)x^2 + bx + (c+y^2)$ soit un carré $(\mathrm{A}x + \mathrm{B})^2$, autrement dit on résout l'équation

$$b^2 - 4(a + 2y)(c + y^2) = 0$$

qui est de degré 3 en y. Une fois qu'on a un tel y, il ne nous reste qu'à résoudre l'équation $x^4 + 2yx^2 + y^2 = (\mathrm{A}x + \mathrm{B})^2$ qui n'est autre que

$$(x^2 + y - \mathrm{A}x - \mathrm{B})(x^2 + y + \mathrm{A}x + \mathrm{B}) = 0,$$

soit deux équations de degré 2 !

FIGURE 9. Gerolamo Cardano

FIGURE 10. Niccolo Fontana dit Tartaglia

Dans tous ces cas de petit degré, les racines complexes de l'équation générale initiale s'obtiennent à l'aide de polynômes en ses coefficients ainsi que des racines de tels polynômes : on dit qu'elles s'expriment par radicaux. C'est impossible pour $n \geq 5$: c'est une conséquence du théorème des fonctions symétriques et de la théorie de Galois (cf. 7.4). C'est le succès le plus connu de la théorie de Galois. On a des résultats très précis. Par exemple, on peut montrer avec les méthodes développées ici que les racines de l'équation $\mathrm{X}^5 - \mathrm{X} - 1$ ne s'expriment pas par radicaux de nombres rationnels !

Pour finir cette invitation, insistons sur le fait que la théorie de Galois ne se limite pas, loin s'en faut, à ces applications à l'intérêt désormais historique. Elle a de multiples

15. 1522-1565

facettes, très profondes, gouvernant de vastes aspects tant de l'algèbre que de la théorie des nombres et de la géométrie. C'est l'étude fine des représentations linéaires du groupe de Galois "absolu"de $\bar{\mathbf{Q}}/\mathbf{Q}$ -au travers notamment d'un cas particulier des conjectures de Langlands- qui a permis à Wiles de prouver le théorème de Fermat : pour n nombre entier strictement supérieur à 2, il n'existe pas de nombres entiers non nuls x, y et z tels que $x^n + y^n = z^n$.

Ce cours n'est que le *début* d'une longue histoire, bien loin d'être terminée.

CHAPITRE 1

COMPLÉMENTS DE THÉORIE DES GROUPES

Dans ce chapitre on rappelle des éléments importants de théorie des groupes qui seront utiles par la suite.

1.1. Groupes

Définition 1.1.1. — *Un groupe est un ensemble* G *muni d'une loi de composition interne, c'est-à-dire d'une application* $* : \mathrm{G} \times \mathrm{G} \to \mathrm{G}$*, telle que*

- $*$ *est associative :* $(a * b) * c = a * (b * c)$ *pour tous* $a, b, c \in \mathrm{G}$,
- $*$ *est munie d'un élément neutre* e *:* $a * e = e * a = a$ *pour tout* $a \in \mathrm{G}$,
- $*$ *est munie du passage à l'inverse : pour tout* $a \in \mathrm{G}$*, il existe* $a^{-1} \in \mathrm{G}$ *tel que* $a * a^{-1} = a^{-1} * a = e$.

Par exemple, l'ensemble des entiers relatifs $\mathbf{Z}$ muni de la somme est un groupe.
On dit que $*$ est la loi du groupe.
La loi $*$ est dite commutative si $x * y = y * x$ pour tout x, y dans le groupe. On dit alors que le groupe est abélien.

Définition 1.1.2. — *Un sous-groupe* G' *d'un groupe* G *est une partie non-vide stable par la loi du groupe et le passage à l'inverse, c'est-à-dire telle que* $x * y \in \mathrm{G}'$ *et* $x^{-1} \in \mathrm{G}'$ *pour tous* $x, y \in \mathrm{G}'$.

Par exemple, les sous-groupes de $\mathbf{Z}$ sont les $n\mathbf{Z}$ avec $n \geq 0$. L'intersection de sous-groupes est encore un sous-groupe.
Pour A une partie d'un groupe G, le sous-groupe $< \mathrm{A} >$ de G engendré par A est défini comme le plus petit sous-groupe de G contenant A, c'est-à-dire l'intersection de tous les sous-groupes de G contenant A. On dit que A engendre G si $< \mathrm{A} >= \mathrm{G}$. Un groupe est

dit cyclique si il est engendré par un ensemble à un élément. Par exemple, le groupe $\mathbf{Z}$ et ses sous-groupes $n\mathbf{Z}$ sont cycliques.

Un morphisme de groupe est une application $\phi : \mathrm{G} \to \mathrm{G}'$, avec G et G′ groupes, telle que $\phi(x * y) = \phi(x) * \phi(y)$ et $\phi(x^{-1}) = (\phi(x))^{-1}$ pour tous $x, y \in \mathrm{G}$. Noter qu'alors, automatiquement, le neutre de G est envoyé sur le neutre de G′.

Le noyau $\mathrm{Ker}(\phi) = \{x \in \mathrm{G} | \phi(x) = e'\}$ du morphisme de groupe $\phi : \mathrm{G} \to \mathrm{G}'$ est l'image inverse du neutre e' de G′ par ϕ. C'est un sous-groupe de G (avec la propriété supplémentaire d'être "distingué", comme on va le voir). De plus l'image $\mathrm{Im}(\phi) = \{\phi(x) | x \in \mathrm{G}\}$ de ϕ est un sous-groupe de G′.

Un isomorphisme de groupe est un morphisme de groupe qui est une bijection. Alors, automatiquement, la bijection réciproque est aussi un morphisme de groupe. Par exemple, l'application $\phi : \mathbf{Z} \to n\mathbf{Z}$ définie par $\phi(m) = nm$ est un isomorphisme de groupe.

1.2. Groupes quotients

Soit H un sous-groupe de G. On définit l'ensemble des translatés à droite de H

$$\mathrm{G/H} = \{g\mathrm{H}, g \in \mathrm{G}\}.$$

Le cardinal |G/H| de G/H, fini ou non, s'appelle l'indice de H dans G.

Pour $g, g' \in \mathrm{G}$, si $g' \in g\mathrm{H}$, alors $g'\mathrm{H} = g\mathrm{H}$. Ceci implique que G/H est une partition de G, c'est-à-dire que G est l'union disjointe des translatés à droite. Notons enfin que l'application $h \mapsto gh$ définit une bijection entre H et gH.

En conséquence, si G est fini, tous les translatés à droite ont le même cardinal |H|. On a ainsi montré que

$$|\mathrm{G}| = |\mathrm{G/H}||\mathrm{H}|.$$

En particulier, le cardinal de H divise celui de G : c'est le théorème de Lagrange. On obtient aussi que |G/H| est fini égal à |G|/|H|. Il peut arriver que G/H est fini alors que ni G, ni H ne le sont (on verra des exemples plus loin).

Revenons au cas général G non nécessairement fini. On a la surjection canonique

$$\pi : \mathrm{G} \to \mathrm{G/H}$$

qui envoie g sur gH.

On voudrait mettre **une structure de groupe** sur G/H de sorte que la surjection canonique π soit un morphisme de groupe. On doit donc avoir

$$g_1 g_2 \mathrm{H} = g_1 \mathrm{H} g_2 \mathrm{H} \text{ pour tout } g_1, g_2 \in \mathrm{G}.$$

En particulier, pour $g_1 g_2 = e$, on obtient que nécessairement

$$\mathrm{H} = g_1 \mathrm{H} g_1^{-1}.$$

Définition 1.2.1. — *Un sous-groupe* H *de* G *est dit distingué si* $g\mathrm{H}g^{-1} = \mathrm{H}$ *pour tout* $g \in \mathrm{G}$. *On note* $\mathrm{H} \triangleleft \mathrm{G}$.

Par exemple, si G est abélien, tout sous-groupe de G est distingué. Mais, par exemple :

Exercice 1.2.2. — *Montrer que* $\mathbf{GL}_n(\mathbf{R})$ *n'est pas distingué dans* $\mathbf{GL}_n(\mathbf{C})$.

Pour les groupes symétriques (voir les rappels dans la section suivante), le sous-groupe S_3 de S_4 n'est pas distingué.
De manière générale, on a

Lemme 1.2.3. — *Le noyau de tout morphisme de groupes est distingué.*

Démonstration. — Soit $\phi : \mathrm{G} \to \mathrm{G}'$ un morphisme de groupes. Si $\phi(g) = e'$ est le neutre de G′, alors pour $h \in \mathrm{G}$, on a $\phi(hgh^{-1}) = \phi(h)\phi(g)\phi(h)^{-1} = \phi(h)\phi(h)^{-1} = e'$ et donc $hgh^{-1} \in \mathrm{Ker}(\phi)$. □

Une autre manière d'exprimer la propriété $\mathrm{H} \triangleleft \mathrm{G}$ est de dire $g\mathrm{H} = \mathrm{H}g$ pour tout $g \in \mathrm{G}$. On a alors

$$g_1 g_2 \mathrm{H} = (g_1 \mathrm{H})(g_2 \mathrm{H}) \text{ pour tout } g_1, g_2.$$

Ceci permet de définir, de manière unique, une structure de groupe, dit *groupe quotient*, sur G/H faisant de π un morphisme : pour $g_1\mathrm{H}$ et $g_2\mathrm{H}$ dans G/H, on pose

$$(g_1 \mathrm{H}) * (g_2 \mathrm{H}) = (g_1 g_2)\mathrm{H}.$$

D'après ce qui précède, cette définition ne dépend pas du choix de g_1 et g_2 dans leur classe, mais seulement des classes $g_1\mathrm{H}$ et $g_2\mathrm{H}$ elles-mêmes. On vérifie facilement qu'on obtient bien un groupe [1], de neutre $\mathrm{H} \in \mathrm{G/H}$ et de loi inverse $(g\mathrm{H})^{-1} = g^{-1}\mathrm{H}$.

1. Le groupe G/H peut aussi être caractérisé par une propriété universelle. On verra plus loin, dans le cas des anneaux quotients, un exemple de propriété universelle.

Notons que comme H est le noyau de la surjection canonique $G \to G/H$, tout sous-groupe distingué est le noyau d'un morphisme de groupe, ce qui est une réciproque du lemme 1.2.3.

Exemple 1.2.4. — *Soit $\mathbf{Z}/n\mathbf{Z}$ le groupe des entiers modulo $n \in \mathbf{Z}$. C'est bien le quotient du groupe $\mathbf{Z}$ par le sous-groupe distingué $n\mathbf{Z}$, ce qui justifie la notation. Pour tout $n \in \mathbf{Z}$, le groupe $\mathbf{Z}/n\mathbf{Z}$ est cyclique. Notons que si $n \neq 0$, $\mathbf{Z}$ et $n\mathbf{Z}$ sont infinis, alors que $\mathbf{Z}/n\mathbf{Z}$ est fini d'ordre n. Dans ce dernier cas, les autres générateurs de $\mathbf{Z}/n\mathbf{Z}$ sont les images dans $\mathbf{Z}/n\mathbf{Z}$ des $m \in \{1, \cdots, n-1\}$ qui sont premiers avec n.*

Revenons donc au cas général d'un morphisme de groupe arbitraire.

Proposition 1.2.5. — *Soit $f : G \to G'$ un morphisme de groupe. Alors $Im(f)$ est isomorphe au groupe quotient $G/Ker(f)$.*

Démonstration. — On a vu que $\mathrm{Ker}(f)$ est distingué dans G, donc $G/\mathrm{Ker}(f)$ est bien un groupe. Pour $g, g' \in G$ tels que $g' \in g\mathrm{Ker}(f)$, on a bien $f(g') = f(g)$. Donc f induit une application $\overline{f} : (G/\mathrm{Ker}(f)) \to \mathrm{Im}(f)$. C'est clairement une application surjective qui est un morphisme de groupe. De plus, si $(g\mathrm{Ker}(f)) \in \mathrm{Ker}(\overline{f})$, alors $f(g) = 1$, et donc $g\mathrm{Ker}(f) = \mathrm{Ker}(f)$. Donc $\overline{f}$ est injective et est un isomorphisme de groupe. □

1.3. Suites exactes

Soient G_1, G_2, G_3 trois groupes et

$$f_1 : G_1 \to G_2 \ , \ f_2 : G_2 \to G_3$$

deux morphismes de groupes.

Définition 1.3.1. — *On dit que la suite*

$$G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3$$

est exacte si $\mathrm{Im}(f_1) = \mathrm{Ker}(f_2)$.

Lorsque G_1 (resp. G_3) est réduit au groupe trivial $\{1\}$, l'exactitude signifie que f_2 est injective (resp. f_1 est surjective).

Considérons une suite de morphismes de groupes plus longue, c'est-à-dire $G_1, \cdots, G_n$ des groupes et $f_i : G_i \to G_{i+1}$ des morphismes de groupe :

$$G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \xrightarrow{f_3} \cdots G_{n-1} \xrightarrow{f_{n-1}} G_n.$$

Définition 1.3.2. — *On dit qu'une telle suite est exacte si toutes les sous-suites à trois termes consécutifs*

$$G_{i-1} \xrightarrow{f_{i-1}} G_i \xrightarrow{f_i} G_{i+1}$$

sont exactes.

Soient G_1, G_2, G_3 trois groupes. On a les morphismes de groupe canoniques $\{1\} \to G_1$ et $G_3 \to \{1\}$. Soient $G_1 \xrightarrow{f_1} G_2$ et $G_2 \xrightarrow{f_2} G_3$ deux morphismes de groupes.

Proposition 1.3.3. — *La suite*

$$\{1\} \to G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \to \{1\}$$

est exacte si et seulement si

(i) f_1 est injective,

(ii) f_2 est surjective,

(iii) $Im(f_1) = Ker(f_2)$.

Dans ce cas, $Im(f_1) \simeq G_1$ est un sous-groupe distingué de G_2 et G_3 est isomorphe au groupe quotient $G_2/Im(f_1)$.

Démonstration. — L'exactitude des trois sous-suites à trois termes de la grande suite est équivalente aux propriétés (i), (ii) et (iii). Le premier point est donc clair. Maintenant, supposons que la suite est effectivement exacte. Comme f_1 est injective, on a bien $\mathrm{Im}(f_1) \simeq G_1$. Comme f_2 est surjective, on a (1.2.3)

$$G_3 \simeq G_2/(\mathrm{Ker}(f_2)) \simeq G_2/\mathrm{Im}(f_1).$$

□

Reprenons l'exemple d'un morphisme de groupes arbitraire $f : G \to G'$ comme dans la section précédente. On a alors une suite exacte canoniquement associée

$$\{1\} \to \mathrm{Ker}(f) \xrightarrow{i} G \xrightarrow{f} \mathrm{Im}(f) \to \{1\} \tag{3.a}$$

où $i : \mathrm{Ker}(f) \to G$ est l'inclusion.

De manière générale, pour H un sous-groupe distingué d'un groupe G, on a une suite exacte canoniquement associée

$$\{1\} \to H \xrightarrow{i} G \xrightarrow{\pi} G/H \to \{1\}.$$

Une "suite exacte à 3 termes"

$$\{1\} \to \mathrm{G}_1 \xrightarrow{f_1} \mathrm{G}_2 \xrightarrow{f_2} \mathrm{G}_3 \to \{1\}$$

est dite *suite exacte courte* ; on dit alors que G_2 est une *extension* de G_3 par G_1.

Exemple 1.3.4. — *Soit* D_n *le groupe des isométries planes laissant invariant un polygone régulier à* n *côtés de centre* 0 *(*D_n *est appelé groupe diédral).* D_n *contient le groupe des rotations laissant invariant ce polygone. Ce sous-groupe est cyclique, engendré par la rotation d'angle* $2\pi/n$*, et donc est isomorphe à* $\mathbf{Z}/n\mathbf{Z}$*. Comme une isométrie conserve les distances, un élément de* D_n *est déterminé par l'image de deux sommets consécutifs. Donc* D_n *a au plus* $2n$ *éléments et est engendré par les rotations et une symétrie orthogonale par rapport à une droite. On obtient donc une suite exacte courte*

$$\{1\} \to \mathbf{Z}/n\mathbf{Z} \to \mathrm{D}_n \to \mathbf{Z}/2\mathbf{Z} \to \{1\},$$

et D_n *est une extension non abélienne de* $\mathbf{Z}/2\mathbf{Z}$ *par* $\mathbf{Z}/n\mathbf{Z}$*.*

Exercice 1.3.5. — *Montrer que le groupe*

$$\mathbf{GL}_n(\mathbf{C})/\mathbf{SL}_n(\mathbf{C})$$

est isomorphe à $\mathbf{C}^*$*.*

1.4. Actions de groupes

Une des motivations principales pour étudier la notion de groupe est que les groupes peuvent agir sur des ensembles.

Soit E un ensemble et Bij(E) l'ensemble des bijections de E. Alors Bij(E) est un groupe pour la loi de composition, l'élément neutre étant l'identité de E et l'inverse d'une bijection sa bijection réciproque. Il est appelé groupe des permutations de E.

Définition 1.4.1. — *Soit* E *un ensemble et* G *un groupe. Une action de* G *sur* E *est la donnée d'un morphisme de groupe* $\phi : \mathrm{G} \to \mathrm{Bij(E)}$*.*

Par exemple, le morphisme identité de Bij(E) définit une action de Bij(E) sur E. Le groupe des isomorphismes linéaires GL(V) d'un espace vectoriel V agit naturellement sur cet espace V, mais aussi sur l'ensemble P(V) des droites vectorielles de V, ou sur l'ensemble des sous-espaces vectoriels de V de dimension fixée. L'application $\phi : \{1, -1\} \to \mathrm{Bij}(\mathbf{C})$

telle que $\phi(1)$ est l'identité et $\phi(-1)$ est la conjugaison complexe définit une action du groupe à deux éléments $\{1,-1\}$ sur $\mathbf{C}$. L'application qui à $\theta \in \mathbf{R}$ associe la rotation du plan R_θ d'angle θ définit une action de $\mathbf{R}$ sur le cercle unité du plan. Il existe bien d'autres actions de groupe, nous en verrons plus loin de nombreux exemples. Voici notamment un exemple qui sera particulièrement utile dans la suite.

Exemple 1.4.2. — *Soit* G *un groupe. L'application* $\phi_g : \mathrm{G} \to \mathrm{G}$ *définie par* $\phi_g(h) = ghg^{-1}$ *est un morphisme de groupe. De plus* $\phi : \mathrm{G} \to \mathrm{Bij(G)}$ *est également un morphisme de groupe. On obtient ainsi l'action par conjugaison de* G *sur lui-même. Notons que pour* H *un sous-groupe de* G, $\phi_g(\mathrm{H})$ *est également un sous-groupe de* G. *Ainsi* G *agit par conjugaison sur l'ensemble de ses sous-groupes.*

Dans la suite de cette section, E est un ensemble muni d'une action $\phi : \mathrm{G} \to \mathrm{Bij(E)}$ d'un groupe G. Pour $g \in \mathrm{G}$ et $x \in \mathrm{E}$, l'élément $(\phi(g))(x)$ sera simplement noté $g.x$.

Définition 1.4.3. — *Soit* $x \in \mathrm{E}$.
L'orbite de x *sous l'action de* G *est l'ensemble* $\{g.x | g \in \mathrm{G}\} \subset \mathrm{E}$.
Le stabilisateur de x *dans* G *est l'ensemble* $\{g \in \mathrm{G} | g.x = x\} \subset \mathrm{G}$.

Notons que l'ensemble des orbites est une partition de E car il est clair que pour $x, y \in \mathrm{E}$, x est dans l'orbite de y si et seulement si y est dans l'orbite de x.
Notons aussi que le stabilisateur de x est clairement un sous-groupe de G.
Un sous-groupe H d'un groupe G est distingué dans G si et seulement si son orbite sous l'action de G par conjugaison est $\{\mathrm{H}\}$.

Définition 1.4.4. — *Un point fixe (ou élément invariant) de* E *sous l'action de* G *est un élément* $x \in \mathrm{E}$ *dont le stabilisateur est* G.
Pour H *un sous-groupe de* G, *l'ensemble* E^{H} *des élément invariants sous* H *est*

$$\mathrm{E}^{\mathrm{H}} = \{x \in \mathrm{E} | \forall h \in \mathrm{H}, h.x = x\} \subset \mathrm{E}.$$

Dire qu'un point x est fixe sous l'action de G revient à dire que l'orbite de x sous l'action de G est réduite à $\{x\}$, ou bien que $g.x = x$ pour tout $g \in \mathrm{G}$.
L'ensemble E^{H} n'est autre que l'ensemble des points fixes de E sous l'action de H induite par celle de G.

Définition 1.4.5. — *L'action de* G *sur* E *est dite fidèle si* ϕ *est injective.*
L'action de G *sur* E *est dite transitive si* E *n'est formé que d'une seule orbite.*

Dire que l'action est transitive revient à dire que pour tous $x, y \in \mathrm{E}$, il existe $g \in \mathrm{G}$ tel que $g.x = y$.

Exercice 1.4.6. — *Soit* V *un espace vectoriel de dimension finie* n *sur un corps* k. *Pour* $0 \leq d \leq n$, *montrer que l'action de* $\mathrm{GL(V)}$ *sur l'ensemble des sous-espaces vectoriels de* V *de dimension* d *est transitive.*

Définition 1.4.7. — *Un sous-ensemble* $\mathrm{F} \subset \mathrm{E}$ *est dit globalement invariant sous l'action de* G *si pour tout* $g \in \mathrm{G}$, *on a* $g(\mathrm{F}) \subset \mathrm{F}$.

Un sous-ensemble formé d'éléments invariants est globalement invariant, mais la réciproque est fausse en général.

1.5. Groupes symétriques

Soit un entier $n \geq 2$.

Définition 1.5.1. — *Le groupe symétrique est* $\mathrm{S}_n = \mathrm{Bij(X)}$ *où* $\mathrm{X} = \{1, \cdots, n\}$.

Le groupe symétrique S_n agit naturellement sur X. Il est de cardinal $n!$. Le groupe S_1 étant le groupe trivial, on suppose dans la suite que $n \geq 2$.
Si $\sigma \in \mathrm{S}_n$, on définit une relation d'équivalence en disant que deux éléments $x, y \in \mathrm{X}$ sont équivalents si et seulement si il existe $j \in \mathbf{Z}$ tel que $y = \sigma^j(x)$. Une classe d'équivalence s'appelle aussi une σ-orbite [2]. Comme pour toute relation d'équivalence, X est réunion disjointes de σ-orbites $\mathrm{O}_i(\sigma)$. Soit

$$n_1 \geq n_2 \geq \cdots \geq n_{\mathrm{N}}$$

la suite (éventuellement vide) ordonnée des cardinaux des orbites non réduites à un élément. On a donc $\mathrm{N} = 0$ si et seulement si $\sigma = \mathrm{Id}$.

Définition 1.5.2. — *Le type de* σ *est le* N*-uple* $\bar{n} = (n_1, \cdots, n_{\mathrm{N}})$.

On dit que σ *est un cycle (de longueur* $d = n_1$*) si* $\mathrm{N} = 1$ *: on parle alors de* d*-cycle. Le support d'un cycle est son unique orbite non réduite à un élément.*

2. Il s'agit d'une orbite sous l'action du sous-groupe de S_n engendré par σ.

La longueur d'un cycle est le cardinal de son support. Un cycle de longueur 2 est une transposition.
On note un cycle de longueur $d > 1$ sous la forme

$$\sigma = (x, \sigma(x), \cdots, \sigma^{d-1}(x))$$

où x est un élément arbitraire dans l'orbite non triviale de σ (cette notation n'est pas unique). Par exemple, le cycle de longueur 3 noté $(3, 7, 5)$ fixe tout élément distinct de $3, 7, 5$ et permute circulairement les autres éléments comme sur le dessin

$$3 \to 7 \to 5 \to 3.$$

Deux cycles commutent si et seulement si leurs supports sont disjoints. Le produit de tels cycles est donc bien défini, l'ordre n'intervenant pas. On a alors la propriété suivante.

Proposition 1.5.3. — *Toute permutation s'écrit de façon unique comme produit (éventuellement vide) de cycles à supports disjoints.*

Les cycles de longueur 2 s'appellent les transpositions. Elles engendrent le groupe S_n.
Pour un cycle $(a_1, \cdots, a_m) \in \mathrm{S}_n$ $(m \leq n)$ et $\sigma \in \mathrm{S}_n$, on a la formule

$$\sigma \circ (a_1, \cdots, a_m) \circ \sigma^{-1} = (\sigma(a_1), \cdots, \sigma(a_m)). \tag{5.a}$$

Elle assure que le conjugué d'un cycle est un cycle de même longueur et que de plus deux cycles sont conjugués si et seulement si ils ont la même longueur. Plus généralement, on a la caractérisation suivante, corollaire immédiat de cette remarque et de la proposition précédente.

Proposition 1.5.4. — *Deux permutations sont conjuguées si et seulement si elles ont même type.*

On ne saurait trop conseiller au lecteur de faire l'exercice suivant.

Exercice 1.5.5. — *Montrer que les transpositions $(i, i+1), 1 \leq i \leq n-1$ engendrent S_n. En déduire que $(1, \cdots, n)$, et $(1, 2)$ engendrent S_n. Montrer que S_n est engendré par n'importe quel triplé (a, b, c) avec a, b, c cycles de longueur $n, n-1$ et 2 respectivement.*

On définit la signature

$$\epsilon : \mathrm{S}_n \to \{1, -1\}$$

par la formule

$$\epsilon(\sigma) = (-1)^{\sum_{i=1}^{\mathrm{N}} (n_i - 1)}$$

où σ est de type $(n_1, \cdots, n_{\mathrm{N}})$.
On vérifie que la signature est aussi $(-1)^i$ où

$$i = \mathrm{card}\{(x, y) \in \mathrm{X}^2 \text{ tels que } x > y \text{ et } \sigma(x) < \sigma(y)\}$$

est le *nombre d'inversions* de σ.
On a le résultat fondamental suivant.

Proposition 1.5.6. — *La signature ϵ est l'unique morphisme surjectif de groupes de $\mathrm{S}_n \to \{1, -1\}$.*

Démonstration. — En utilisant la formule avec le nombre d'inversions, on obtient bien que la signature est un morphisme de groupe. La signature d'une transposition étant égale à -1, la signature est surjective. Maintenant, les transpositions engendrent S_n. Un morphisme de groupe $\phi : \mathrm{S}_n \to \{1, -1\}$ est donc déterminé de manière unique par sa valeur sur les transpositions. Toutes les transpositions étant conjuguées, ϕ prend la même valeur sur toutes les transpositions. Si cette valeur est -1, ϕ est la signature. Sinon, ϕ est le morphisme trivial, non surjectif. □

Le noyau A_n de la signature est donc un sous-groupe distingué, de cardinal $n!/2$: il s'appelle le groupe alterné. On a une suite exacte

$$\{1\} \to \mathrm{A}_n \to \mathrm{S}_n \to \{1, -1\} \to \{1\}.$$

Les transpositions sont de signature -1. On déduit que la signature d'une permutation σ est aussi $(-1)^{\mathrm{N}}$ où N est le nombre de transpositions intervenant dans *une* décomposition de σ en produit de transpositions.

Exercice 1.5.7. — *Montrer que A_n est engendré par les 3-cycles dès que $n \geq 3$.*

Exercice 1.5.8. — *Soit* H *un sous-groupe d'indice fini dans* G. *Montrer que si l'indice de* H *dans* G *est* 2, *alors* H *est distingué dans* G *et le quotient* G/H *est canoniquement isomorphe à $\{\pm 1\}$. Soit n un entier ≥ 2. Montrer que le groupe alterné A_n est l'unique sous-groupe de S_n d'indice* 2.

1.6. Groupes résolubles

La classe des groupes commutatifs n'est pas stable par suite exacte courte. Il faut une classe plus vaste : celle des groupes résolubles.

Définition 1.6.1. — *Un groupe* G *est dit résoluble s'il possède une suite croissante de sous-groupes*

$$\{1\} = \mathrm{G}_n \subset \cdots \subset \mathrm{G}_0 = \mathrm{G}$$

telle que pour $0 \leq i \leq n-1$, *le groupe* $\mathrm{G}_{i+1} \subsetneq \mathrm{G}_i$ *est distingué dans* G_i *et le groupe quotient* $\mathrm{G}_i/\mathrm{G}_{i+1}$ *est commutatif.*

On dira simplement que "les quotients successifs sont commutatifs".
Notons qu'un groupe commutatif est résoluble, il suffit de poser $\mathrm{G}_1 = \{1\}$. Notons aussi qu'un groupe résoluble non commutatif contient toujours un sous-groupe distingué non trivial, le sous-groupe G_1.

Exercice 1.6.2. — *Montrer que le groupe des matrices complexes de taille* $n \geq 2$ *de déterminant* 1 *n'est pas résoluble.*

Définition 1.6.3. — *Le sous-groupe dérivé* DG *d'un groupe* G *est le sous-groupe de* G *engendré par tous les commutateurs* $[a,b] = aba^{-1}b^{-1}$ *avec* $a, b \in \mathrm{G}$.

Notons qu'en général DG n'est pas égal au sous-ensemble $\{[a,b] | a, b \in \mathrm{G}\}$, qui n'est d'ailleurs pas un sous-groupe en général.

Lemme 1.6.4. — DG *est un sous-groupe distingué de* G, *et le groupe quotient* G/DG *est commutatif.*

Démonstration. — Soit $g \in \mathrm{G}$. L'application ϕ_g de (1.4.2) est un morphisme de groupe. En conséquence, pour $a, b \in \mathrm{G}$, on obtient $\phi_g([a,b]) = [\phi_g(a), \phi_g(b)] \in \mathrm{DG}$. Donc DG est distingué. Le groupe quotient est commutatif par construction. □

On définit alors par récurrence sur n la suite de sous-groupes $(\mathrm{D}^n\mathrm{G})_{n\geq 0}$

$$\mathrm{D}^0\mathrm{G} = \mathrm{G} \text{ et } \mathrm{D}^{n+1}\mathrm{G} = \mathrm{D}\mathrm{D}^n\mathrm{G} \text{ si } \ n \geq 0.$$

Lemme 1.6.5. — G *est résoluble si et seulement si* $\mathrm{D}^n\mathrm{G}$ *est trivial pour* n *assez grand.*

Démonstration. — Si G est résoluble et G_i est comme dans la définition, l'image d'un commutateur dans le groupe abélien $\mathrm{G}_0/\mathrm{G}_1$ est triviale de sorte que $\mathrm{D}^1\mathrm{G}$ est contenu dans G_1. Par récurrence, on montre $\mathrm{D}^i\mathrm{G}$ contenu dans G_i et donc $\mathrm{D}^n\mathrm{G}$ est trivial. Inversement, si $\mathrm{D}^n\mathrm{G}$ est trivial, on pose $\mathrm{G}_i = \mathrm{D}^i\mathrm{G}$ qui convient. □

Proposition 1.6.6. — *Si*

$$1 \to \mathrm{G}_1 \to \mathrm{G}_2 \to \mathrm{G}_3 \to 1$$

est exacte, alors G_2 *résoluble si et seulement si* G_1 *et* G_3 *résolubles.*

Démonstration. — On a d'une part $\mathrm{D}^n\mathrm{G}_2 \to \mathrm{D}^n\mathrm{G}_3$ surjectif et $\mathrm{D}^n\mathrm{G}_1 \to \mathrm{D}^n\mathrm{G}_2$ injectif de sorte que G_2 résoluble entraîne G_1 et G_3 résoluble. Inversement, si $\mathrm{D}^n\mathrm{G}_3$ est trivial, l'image de $\mathrm{D}^n\mathrm{G}_2$ dans G_3 est nul et donc $\mathrm{D}^n\mathrm{G}_2$ est contenu dans G_1. Si maintenant on a de plus $\mathrm{D}^m\mathrm{G}_1 = 1$, on en déduit $\mathrm{D}^{m+n}\mathrm{G}_2 \subset \mathrm{D}^m\mathrm{G}_1 = 1$, d'où la réciproque. □

En fait, on a mieux : la classe des groupes résolubles est stable par extension, ce qui compte tenu de ce qui précède, s'écrit

Corollaire 1.6.7. — *Si* G *possède une suite croissante de sous-groupes*

$$1 = \mathrm{G}_0 \subset \cdots \subset \mathrm{G}_n = \mathrm{G}$$

avec G_i *distingué dans* G_{i+1} *et* $\mathrm{G}_{i+1}/\mathrm{G}_i$ *résoluble, alors* G *est résoluble.*

Exercice 1.6.8. — *On se propose de montrer que le groupe* B *des matrices de* $\mathbf{GL}_n(k)$ *qui sont triangulaires supérieures est résoluble (*k *est un corps). Soit* U *le sous-groupe de* B *des matrices dont toutes les valeurs propres sont égales à* 1 *(matrices unipotentes).*
1) Montrer qu'on a une suite exacte de groupes

$$1 \to \mathrm{U} \to \mathrm{B} \to (k^*)^n \to 1.$$

En déduire que B *est résoluble si et seulement si* U *est résoluble.*
Soit (e_i) *la base canonique de* k^n. *Pour* $i \leq n$, *soit* F_i *le sous-espace vectoriel de* k^n *engendré par* $e_1, \cdots, e_i$. *On a donc* $\mathrm{F}_i = (0)$ *si* $i \leq 0$ *et* $\mathrm{F}_n = k_n$. *Pour tout* $f \in \mathrm{U}$, *on note* $\ln(f)$ *la matrice* $f - \mathrm{Id}$. *Pour tout* $j = 0, \cdots, n$, *soit* U_j *le sous ensemble de* U *des matrices* f *telles que* $\ln(f)(\mathrm{F}_i) \subset \mathrm{F}_{i-j}$ *pour* $i \leq n$.
2) Vérifier qu'on a

$$(1) = \mathrm{U}_n \subset \mathrm{U}_{n-1} \cdots \subset \mathrm{U}_1 = \mathrm{U}.$$

Montrer que U_i *est un sous-groupe distingué de* U *pour tout* $i \leq n$ *et donc également de* U_{i-1}.
3) Soit $f \in \mathrm{U}_j$. *Montrer que pour tout* $i \leq n$, *la restriction* $\ln(f)_{i,j}$ *de* $\ln(f)$ *à* F_i *induit une application linéaire de* $\mathrm{F}_i/\mathrm{F}_{i-j-1}$ *qui est nulle si et seulement si* $\ln(f)(\mathrm{F}_i) \subset \mathrm{F}_{i-j-1}$.

4) Montrer que l'application

$$\ln_j : \begin{cases} \mathrm{U}_i & \to & \prod_i \mathrm{End}(\mathrm{F}_i/\mathrm{F}_{i-j}) \\ f & \mapsto & (\ln(f)_{i,j}) \end{cases}$$

est un morphisme de groupes et calculer son noyau.
5) En déduire que U *est résoluble. Conclure.*

Lemme 1.6.9. — *Les groupes* S_3 *et* S_4 *sont résolubles non commutatifs.*

Démonstration. — Pour montrer que S_3 et S_4 ne sont pas commutatifs, il suffit de considérer deux transpositions qui n'ont pas le même support. Maintenant, pour $n \geq 2$, la suite exacte

$$1 \to \mathrm{A}_n \to \mathrm{S}_n \to \{\pm 1\} \to 1$$

et (1.6.6) assurent que S_n est résoluble si et seulement si A_n l'est. Comme A_3 est cyclique d'ordre 3, il est résoluble. Pour A_4, on peut observer que

$$\mathrm{K} = \{\mathrm{Id}, (12)(34), (13)(24), (14)(23)\}$$

est un sous-groupe distingué de A_4 (et de S_4 d'ailleurs; il est appelé groupe de Klein). Comme A_4 est de cardinal 12, le quotient est de cardinal 3, et donc est cyclique comme tout groupe d'ordre premier. On conclut encore grâce à (1.6.6). □

Le résultat suivant est fondamental pour la suite.

Proposition 1.6.10. — *Si* $n \geq 5$, *on a* $\mathrm{D}(\mathrm{A}_n) = \mathrm{A}_n$ *et donc* S_n *n'est pas résoluble.*

Démonstration. — $n \geq 3$, donc A_n est engendré par les 3-cycles (cf. 1.5.5). Soit $\gamma = (a, b, c)$ un 3-cycle. On a $\gamma^2 = (a, c, b)$. Soit $\sigma \in \mathrm{S}_n$ envoyant le triplet (a, b, c) sur (a, c, b), c'est-à-dire tel que $\sigma(a, b, c)\sigma^{-1} = (a, c, b)$. Soient d, e distincts de a, b, c (c'est possible car $n \geq 5$). On a également $\sigma \circ (d, e)(a, b, c) = (a, c, b)$ et donc on peut supposer, quitte à changer σ en $\sigma \circ (d, e)$, que σ est dans A_n. Or, $\sigma \circ \gamma \circ \sigma^{-1} = \gamma^2$ et donc $\gamma \in \mathrm{D}(\mathrm{A}_n)$.
On conclut pour le dernier point en remarquant que $\mathrm{D}(\mathrm{S}_n) \subset \mathrm{A}_n$. □

Exercice 1.6.11. — *Soit*

$$\mathrm{X} = \{(1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$$

l'ensemble des permutations de S_4 *de type* $(2,2)$. *Montrer que* S_4 *agit sur* X *par conjugaison. En déduire qu'il existe un morphisme* $\pi : \mathrm{S}_4 \to \mathrm{S}_3$ *et calculer son noyau. Montrer que* π *est surjectif et en déduire que* S_4 *est résoluble. On retrouve ainsi un résultat de 1.6.2.*

Exercice 1.6.12 **(Difficile)**. — *Soit* G *un groupe de cardinal* p^n *avec* p *premier*[3]. *On se propose de montrer par récurrence sur* n *l'existence d'une suite croissante de sous-groupes* $\mathrm{G}_i, i = 1 \cdots n$ *de* G *de cardinal* p^i *avec* G_i *distingué dans* G_{i+1}. *Ceci montre en particulier que* G *est résoluble.*

a) Soit H *un sous-groupe distingué de* G. *Montrer que si l'énoncé est vrai pour* H *et* G/H *il est vrai pour* G.

b) Traiter le cas commutatif.

c) En faisant opérer G *sur lui même par conjugaison, montrer que le centre de* G *est non réduit à* 1. *Conclure.*

3. L'intérêt de ces groupes résulte en partie du fait que si p^n est la puissance maximale de p divisant le cardinal d'un groupe G fini, alors G admet un sous-groupe d'ordre p^n (dit p-Sylow) et que tous ces sous-groupes sont conjugués (voir par exemple [**B1**]).

CHAPITRE 2

COMPLÉMENTS DE THÉORIE DES ANNEAUX

Comme dans le chapitre précédent, nous rappellons ici des éléments importants de théorie des anneaux.

2.1. Anneaux

Rappelons quelques définitions fondamentales.

Définition 2.1.1. — *Un anneau est un ensemble* A *muni de deux applications*

$$+ : \mathrm{A} \times \mathrm{A} \to \mathrm{A} \text{ et } \times : \mathrm{A} \times \mathrm{A} \to \mathrm{A}$$

commutatives telles que $(\mathrm{A}, +)$ *est un groupe,* $\times$ *est associative, munie d'un élément neutre, distributive sur* $+$ *:*

$$x \times (y + z) = x \times y + x \times z \text{ pour tous } x, y, z \in \mathrm{A}.$$

Autrement dit, un anneau est un ensemble muni d'une addition et d'une multiplication permettant de calculer comme sur les entiers ou les réels par exemple, mis à part qu'on ne peut en général diviser par un élément non nul. Parfois on notera simplement $x.y$ ou xy pour $x \times y$. Le neutre de $+$ est noté 0, et le neutre de $\times$ est noté 1.

On notera que, à la vue de notre définition ci-dessus, on dira dans ce livre anneau pour anneau commutatif unitaire.

Les éléments d'un anneau A qui sont inversibles pour $\times$, c'est-à-dire admettant un inverse pour $\times$, forment un groupe noté A^* et appelé groupe des inversibles de A.

Définition 2.1.2. — *Un corps est un anneau non nul dans lequel tout élément non nul admet un inverse pour* $\times$*.*

Exemple 2.1.3. — *L'ensemble des entiers relatifs* $\mathbf{Z}$*, des entiers modulo* n *(noté* $\mathbf{Z}/n\mathbf{Z}$*), les fonctions d'un ensemble à valeurs réelles, les séries entières convergentes (munis des lois usuelles) sont des exemples d'anneaux, mais pas des corps en général. L'ensemble* $\mathbf{Z}/p\mathbf{Z}$ *des entiers modulo* p *premier est un corps, comme les ensembles* $\mathbf{Q}$ *des nombres rationnels,* $\mathbf{R}, \mathbf{C}$ *des nombres réels, complexes (munis des lois usuelles).*

En général, si on ne précise pas et que le contexte est clair, la lettre A désignera un anneau tandis que k désignera un corps.

Définition 2.1.4. — *Un morphisme d'anneaux* $f : \mathrm{A} \to \mathrm{B}$ *est une application telle que* $f(1) = 1$ *et qui vérifie*

$$f(a+b) = f(a) + f(b) \text{ et } f(ab) = f(a)f(b)$$

pour tous $a, b \in \mathrm{A}$*. Son noyau* $\mathrm{Ker}(f) \subset \mathrm{A}$ *est l'ensemble des éléments annulés par* f*. L'ensemble de ces morphismes est noté* $\mathrm{Hom}(\mathrm{A}, \mathrm{B})$

Notons que nécessairement $f(0) = 0$ (unicité du neutre dans un groupe) et $f(-a) = -f(a)$ pour tout $a \in \mathrm{A}$.

Définition 2.1.5. — *Un idéal* I *d'un anneau* A *est un sous-groupe de* A *pour* $+$ *tel que* $xy \in \mathrm{I}$ *pour tous* $x \in \mathrm{A}$*,* $y \in \mathrm{I}$*.*

Cette notion est différente de la notion de sous-anneau, pour laquelle la dernière condition est remplacée par la stabilité pour $\times$.
Tout idéal I de $\mathbf{Z}$ est engendré par un élément, c'est-à-dire que I est de la forme $\mathrm{I} = n\mathbf{Z}$ avec $n \in \mathbf{Z}$. C'est une conséquence bien connue de la division euclidienne dans $\mathbf{Z}$. Comme nous allons le voir dans la section suivante, c'est aussi le cas pour l'anneau polynômes sur un corps.
Le noyau d'un morphisme d'anneau est toujours un idéal.

Exercice 2.1.6. — *Montrer que l'image réciproque d'un sous-groupe de* $\mathbf{Z}/n\mathbf{Z}$ *par la projection canonique est un sous-groupe de* $\mathbf{Z}$ *contenant* $n\mathbf{Z}$*. En déduire qu'un sous-groupe de* $\mathbf{Z}/n\mathbf{Z}$ *est cyclique de cardinal* $d|n$*, engendré par la classe de* $\frac{n}{d}$*. En particulier, l'application qui à un sous-groupe de* $\mathbf{Z}/n\mathbf{Z}$ *associe son cardinal est une bijection sur l'ensemble des diviseurs (positifs) de* n*.*

2.2. Anneau des polynômes

Soit A un anneau. Alors considérons l'ensemble A[X] des polynômes à une variable à coefficients dans A. Muni de l'addition et la multiplication des polynômes, A[X] a une structure naturelle d'anneau.
Lorsque $A = k$ est un corps, on dispose de la division euclidienne dans k[X] : pour tous $A, B \in k[X]$ avec $B \neq 0$, il existe un unique couple (Q, R) de polynômes tels que

$$A = QB + R \text{ et } \deg(R) < \deg(B).$$

Comme conséquence, on obtient comme pour l'anneau des entiers que tous les idéaux de k[X] sont engendrés par un seul élément, c'est-à-dire qu'ils sont de la forme $I = P(X)k[X]$ avec $P(X) \in k[X]$. Un tel idéal est alors noté (P).
Ceci permet de définir le PGCD (resp. le PPCM) de deux polynômes non nuls $P, Q \in k[X]$ comme générateur de l'idéal $(P)+(Q)$ (resp. $(P)\cap(Q)$). Notons que le PGCD et le PPCM sont définis à une constant multiplicative dans k^* près.
Lorsque deux polynômes non nuls P et Q sont premiers entre eux, c'est-à-dire de PGCD égal à 1, alors on a l'identité de Bézout, c'est-à-dire qu'il existe $A, B \in k[X]$ tels que

$$PA + QB = 1.$$

L'algorithme d'Euclide permet de calculer le PGCD de deux polynômes $P, Q \in k$. Cet algorithme ne dépend que des coefficients de P et de Q, et pas du corps k. En particulier, si L est un corps contenant k, les polynômes P et Q, vus dans L[X], ont le même PGCD que lorsqu'ils sont vus dans k[X]. On dit que le PGCD est invariant par changement de corps.

2.3. Morphisme de corps

Notons qu'un idéal I d'un anneau A est égal à A si et seulement si il contient 1. Ceci est équivalent au fait que I contienne un élément inversible de A (c'est-à-dire un élément de A qui possède un inverse pour $\times$). En conséquence :

Proposition 2.3.1. — *Le seul idéal non nul d'un corps est le corps lui-même.*

Un morphisme de corps est un morphisme d'anneaux entre deux corps. En particulier, comme un morphisme de corps envoie 1 sur 1 (non nul car un corps est non nul), le noyau d'un morphisme de corps est toujours nul. Ainsi, on a le résultat remarquable suivant.

Proposition 2.3.2. — *Un morphisme de corps est toujours injectif.*

Ainsi, un morphisme de corps $\sigma : k \to k'$ permet d'identifier le sous-corps $\sigma(k)$ de k' à k (ils sont isomorphes). On dit aussi que σ définit un plongement de k dans k'. Remarquons que k' est une extension de $\sigma(k)$, dans le sens suivant :

Définition 2.3.3. — *Une extension d'un corps* K *est un corps* K′ *contenant* K.

Ainsi, pour un morphisme de corps $\sigma : k \to k'$, k' peut être vu comme une extension de k.

Lorsqu'on a trois corps $\mathrm{K} \subset \mathrm{K}' \subset \mathrm{K}''$, on dit que l'extension K'/K est une sous-extension de l'extension K''/K.

2.4. Anneaux quotients

Rappelons la construction du quotient $\bar{\mathrm{A}} = \mathrm{A}/\mathrm{I}$ d'un anneau A par un idéal I et surtout ses propriétés [1]. L'idée est de fabriquer un nouvel anneau $\bar{\mathrm{A}}$ dans lequel on a "tué" les éléments de I. On adapte simplement la construction de $\mathbf{Z}/n\mathbf{Z}$, qui sera un cas particulier de la construction générale pour $\mathrm{A} = \mathbf{Z}$ et $\mathrm{I} = n\mathbf{Z}$.

Pour $a \in \mathrm{A}$, le translaté de a est l'ensemble

$$\overline{a} = a + \mathrm{I} \overset{\text{déf}}{=} \{a + i, i \in \mathrm{I}\} \subset \mathrm{A}.$$

Notons que deux tels translatés $(a + \mathrm{I})$ et $(a' + \mathrm{I})$ sont égaux si et seulement si $a - a' \in \mathrm{I}$. L'ensemble quotient A/I est l'ensemble des translatés. Le groupe $(\mathrm{A}, +)$ étant abélien, I est distingué dans A. On a vu qu'alors A/I est muni d'une structure de groupe telle que

$$(a + \mathrm{I}) + (a' + \mathrm{I}) \overset{\text{déf}}{=} (a + \mathrm{I} + a' + \mathrm{I}) = (a + a') + \mathrm{I}$$

On observe que A/I est un groupe commutatif d'élément neutre $\bar{0}$.

1. Comme souvent en mathématiques, la construction n'est pas la plus importante ; les propriétés importent beaucoup plus. Par exemple, on sait très bien travailler sur les réels en connaissant les propriétés de son ordre sans pour autant se souvenir voire connaître une quelconque de ses constructions !

De même, A/I est muni d'un produit défini par

$$(a+\mathrm{I}).(b+\mathrm{I}) \overset{\text{déf}}{=} (a+\mathrm{I})(b+\mathrm{I})+\mathrm{I} = ab+a\mathrm{I}+b\mathrm{I}+\mathrm{I}^2+\mathrm{I} = ab+\mathrm{I}.$$

Le lecteur vérifiera aisément le résultat suivant.

Proposition 2.4.1. — A/I *muni des lois* $+$ *et* $\times$ *est un anneau. Le neutre de* $+$ *est* $\overline{0}$ *et le neutre de* $\times$ *est* $\overline{1}$.

Définissons la **surjection canonique**

$$\pi : \ \mathrm{A} \twoheadrightarrow \mathrm{A/I}$$

par $a \mapsto \overline{a}$ (le symbole $\twoheadrightarrow$ signifie que l'application est surjective). On voit $\bar{a} = \pi(a)$ comme la classe A modulo I, exactement comme en arithmétique usuelle.

Proposition 2.4.2. — π *est un morphisme surjectif d'anneaux de noyau* $Ker(\pi) = \mathrm{I}$.

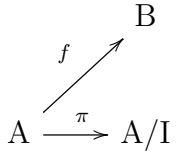
Démonstration. — On a pour $a, a' \in \mathrm{A}$

$$\pi(1) = \overline{1},\ \overline{a}.\overline{a'} = \overline{a.a'},\ \overline{a+a'} = \overline{a}+\overline{a'}$$

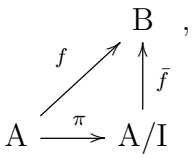
donc π est un morphisme d'anneaux. Il est clairement surjectif. Pour $a \in \mathrm{Ker}(\pi)$, on a $\overline{a} = \overline{0}$, c'est-à-dire $a \in \mathrm{I}$. Réciproquement, chaque $a \in \mathrm{I}$ vérifie $\overline{a} = \mathrm{I}$. □

Exemple 2.4.3. — *Pour* k *un corps, on a l'anneau* $k[\mathrm{X}]/(\mathrm{P})$ *où* (P) *est l'idéal* $\mathrm{P}k[\mathrm{X}]$ *de* $k[\mathrm{X}]$ *engendré par un polynôme* $\mathrm{P} \in k[\mathrm{X}]$.

L'énoncé suivant, dit de *propriété universelle du quotient*, est maintenant clair, et... fondamental.
Partons d'un diagramme



avec f morphisme d'anneaux tel que $f(\mathrm{I}) = 0$. Alors il existe un unique morphisme d'anneaux $\bar{f}$ faisant *commuter* le diagramme



c'est-à-dire tel que $f = \bar{f} \circ \pi$. On dit aussi que f se *factorise* à travers π.
En termes ensemblistes, ceci équivaut au théorème suivant, dit de propriété universelle du quotient.
Soient A, B deux anneaux et I un idéal de A. On définit

$$\pi^* : \mathrm{Hom}(\mathrm{A}/\mathrm{I}, \mathrm{B}) \to \{f \in \mathrm{Hom}(\mathrm{A}, \mathrm{B}) \text{ tels que } f(\mathrm{I}) = 0\}$$

par $\pi^*(g) = g \circ \pi$.

***Théorème 2.4.4* (Propriété universelle du quotient).** — *L'application π^* est une bijection.*

On identifiera sans plus de précaution ces deux espaces.

Démonstration. — Soient ϕ, ϕ' tels que $\phi \circ \pi = \phi' \circ \pi$, c'est-à-dire $(\phi - \phi') \circ \pi = 0$. Comme π est surjective, $\phi - \phi'$ est nulle sur $\pi(\mathrm{A}) = \mathrm{A}/\mathrm{I}$ donc est nulle, d'où l'injectivité.
Passons à la surjectivité. Soit donc $f \in \mathrm{Hom}(\mathrm{A}, \mathrm{M})$ annulant I et cherchons un antécédent ϕ. Soit $t \in \mathrm{A}/\mathrm{I}$: c'est la classe d'un élément a, bien déterminé à addition d'un élément $i \in \mathrm{I}$ quelconque près. Comme $f(\mathrm{I}) = 0$, les images par f de tous les éléments a représentant t sont un seul et même élément qu'on baptise $\phi(t)$. Par construction, $\phi \circ \pi = f$ et ϕ est évidemment un morphisme (par exemple, si $t = \pi(a), t' = \pi(a')$ avec $a, a' \in \mathrm{A}$, on a

$$\phi(tt') = \phi(\pi(a)\pi(a')) = \phi(\pi(aa')) = f(aa') = f(a)f(a') = \phi(\pi(a))\phi(\pi(a')) = \phi(t)\phi(t')$$

ce qui prouve la multiplicativité puisque ϕ est surjective; l'additivité se traite de la même manière). □

Remarque 2.4.5. — *Si $f : \mathrm{A} \to \mathrm{B}$ est un morphisme d'anneaux, on a donc une factorisation canonique $\bar{f} : \mathrm{A}/\mathrm{Ker}(f) \to \mathrm{B}$ de f à travers $\mathrm{A} \to \mathrm{A}/\mathrm{Ker}(f)$ puisque $f(\mathrm{Ker}(f)) = \{0\}$. Comme on a précisément "tué" le noyau de f, celui de $\bar{f}$ est nul de sorte que $\bar{f}$ est* injective. *Si f est supposée surjective, on a donc un isomorphisme canonique $\bar{f} : \mathrm{A}/\mathrm{Ker}(f) \xrightarrow{\sim} \mathrm{B}$.*

Montrons un lemme, facile, mais très utile.

Lemme 2.4.6. — *L'application qui à un idéal* $\bar{\mathrm{J}}$ *de* $\mathrm{A/I}$ *associe son image inverse* $\mathrm{J} = \pi^{-1}(\bar{\mathrm{J}})$ *identifie les idéaux de* $\mathrm{A/I}$ *aux idéaux de* A *contenant* I. *De plus, le morphisme* $\mathrm{A} \to \bar{\mathrm{A}} \to \bar{\mathrm{A}}/\bar{\mathrm{J}}$ *passe au quotient et induit un isomorphisme* $\mathrm{A/J} \xrightarrow{\sim} \bar{\mathrm{A}}/\bar{\mathrm{J}}$.

Démonstration. — Comme I contient 0, l'idéal $\pi^{-1}(\mathrm{I})$ contient $\mathrm{I} = \pi^{-1}(0)$. Inversement, si J est un idéal de A contenant I, on vérifie que $\pi(\mathrm{J})$ est un idéal de $\mathrm{A/I}$. Les deux constructions sont clairement inverses l'une de l'autre. Par ailleurs, le noyau de la surjection $\mathrm{A} \to \bar{\mathrm{A}}/\bar{\mathrm{J}}$ est l'ensemble des $a \in \mathrm{A}$ tels que $\pi(a) \in \bar{\mathrm{J}}$, c'est-à-dire J. Par propriété universelle du quotient, on a une factorisation $\mathrm{A/J} \to \bar{\mathrm{A}}/\bar{\mathrm{J}}$ qui reste évidemment surjective, mais qui en plus est injective d'après la remarque précédente. □

2.5. Caractéristique

Rappelons le résultat suivant :

Lemme 2.5.1. — *Soit* A *un anneau. Il existe un unique morphisme d'anneaux* $\gamma : \mathbf{Z} \to \mathrm{A}$.

Démonstration. — Un tel morphisme γ vérifie pour $n \geq 0$, $\gamma(n) = 1 + \cdots + 1$ n fois, et pour $n \leq 0$, $\gamma(n) = -1 - 1 - \cdots - 1$ $(-n)$ fois. Il est donc unique. De plus ces formules définissent un morphisme d'anneaux. □

Le noyau de γ est un idéal de $\mathbf{Z}$. Il existe donc un unique entier $n \geq 0$ tel que $\mathrm{Ker}(\gamma) = n\mathbf{Z}$.

Définition 2.5.2. — *L'unique entier* $n \geq 0$ *tel que* $Ker(\gamma) = n\mathbf{Z}$ *est appelé caractéristique de* A.

Par exemple, la caractéristique de $\mathbf{Z}$ est nulle, la caractéristique de $\mathbf{Z}/n\mathbf{Z}$ est n.

Proposition 2.5.3. — *La caractéristique d'un corps* k *est nulle ou est un nombre premier.*

Démonstration. — Supposons que la caractéristique n de k se factorise $n = pq$ avec p, q entiers positifs plus grands que 2. On a alors $\gamma(p)\gamma(q) = 0$ dans k. Comme k est un corps, ceci implique $\gamma(p) = 0$ ou $\gamma(q) = 0$. Contradiction car $2 \leq p, q < n$ donc p et q ne sont pas dans $\mathrm{Ker}(\gamma) = n\mathbf{Z}$. □

Par exemple, $\mathbf{Q}$ est de caractéristique nulle tandis que $\mathbf{Z}/p\mathbf{Z}$ est de caractéristique p (p premier).

Proposition 2.5.4. — *Soit k un corps. Si la caractéristique de k est nulle, alors k est infini et contient un sous-corps isomorphe à $\mathbf{Q}$. Si la caractéristique de k est un nombre premier p, alors k contient un sous-corps isomorphe à $\mathbf{Z}/p\mathbf{Z}$ appelé sous-corps premier de k.*

Démonstration. — Considérons $\gamma : \mathbf{Z} \to k$ l'unique morphisme d'anneaux. Alors γ se factorise à travers son noyau $n\mathbf{Z}$ pour définir une injection canonique $\mathbf{Z}/n\mathbf{Z} \hookrightarrow k$. Si $n = 0$, alors k contient $\mathrm{Im}(\gamma) \simeq \mathbf{Z}$. Le sous-corps de k est engendré par $\mathrm{Im}(\gamma)$ est alors isomorphe à $\mathbf{Q}$. De plus k est infini car il contient $\mathrm{Im}(\gamma)$ infini. Si $n = p$ nombre premier, alors k contient $\mathrm{Im}(\gamma) \simeq \mathbf{Z}/p\mathbf{Z}$. □

2.6. Anneaux intègres, propriétés des idéaux

Définition 2.6.1. — *On dit qu'un anneau* A *est intègre si il est non nul et si le produit de deux éléments non nuls de* A *est non nul.*

Exemple 2.6.2. — *L'anneau $\mathbf{Z}$ est intègre. Un corps k est un anneau intègre. De plus $k[\mathrm{X}]$ est alors également intègre. En effet, le produit de deux polynômes non nuls $\mathrm{P}_1(\mathrm{X}) = a_n\mathrm{X}^n + \cdots + a_0$ et $\mathrm{P}_2(\mathrm{X}) = b_m\mathrm{X}^m + \cdots + b_0$ est non nul car il est de degré $n + m$ de coefficient dominant $a_n b_m \neq 0$.*

Un anneau intègre A peut être plongé dans un corps K, dans le sens qu'il existe un morphisme d'anneau injectif de A vers K. Un exemple important est le corps *corps des fractions* de A. Sa construction est calquée sur la construction de $\mathbf{Q}$ qui est le corps des fractions de $\mathbf{Z}$: on considère l'ensemble Frac(A) des classes d'équivalences de $\mathrm{A} \times \mathrm{A}^*$ pour la relation ((a, b) équivalent à (c, d) si $ad = bc$) : ici (a, b) et (c, d) représentent respectivement les fractions a/b et c/d. En utilisant les règles habituelles d'addition et multiplications des fractions, on munit alors Frac(A) d'une structure de corps.
On notera $(a_s, s \in \mathrm{S})$ l'idéal engendré par la famille des $a_s, s \in \mathrm{S}$. Si I, J sont des idéaux, on note IJ l'idéal engendré par les produits $ij, i \in \mathrm{I}, j \in \mathrm{J}$. On parle alors, abusivement, d'*idéal produit* de I et J.

Définition 2.6.3. — *Soit* I *un idéal d'un anneau* A. *On suppose* $\mathrm{I} \neq \mathrm{A}$.

- *On dit que* I *est premier si* A/I *est intègre.*
- *On dit que* I *est maximal si* A/I *est un corps.*

En particulier, un corps étant intègre, un idéal maximal est nécessairement premier. Notons que l'idéal A n'est ni premier ni maximal.

Lemme 2.6.4. — *L'image inverse d'un idéal premier par un morphisme d'anneaux est un idéal premier.*

Démonstration. — Si $\mathfrak{p}$ est premier dans A et $f : \mathrm{B} \to \mathrm{A}$ est un morphisme d'anneaux, f induit un morphisme $\mathrm{B}/f^{-1}(\mathfrak{p}) \to \mathrm{A}/\mathfrak{p}$ (2.4.4), injectif par construction. Ceci assure que $\mathrm{B}/f^{-1}(\mathfrak{p})$ est intègre comme sous-anneau d'un anneau intègre et donc que $f^{-1}(\mathfrak{p})$ est premier. □

En général l'image inverse d'un idéal maximal n'est pas un idéal maximal. Par exemple, l'image inverse de l'idéal maximal (0) de $\mathbf{Q}$ par l'injection $\mathbf{Z} \to \mathbf{Q}$ est nulle. Or (0) n'est pas maximal dans $\mathbf{Z}$ car $\mathbf{Z}/(0) = \mathbf{Z}$ n'est pas un corps.
L'ensemble des idéaux premiers de A se note Spec(A) et est appelé spectre de A. C'est l'un des objets fondamentaux de l'une des branches des mathématiques appelée géométrie algébrique.

Définition 2.6.5. — *Un élément a d'un anneau intègre est dit* irréductible *s'il n'est ni nul ni inversible et si ses diviseurs sont ou bien inversibles ou bien multiples de a.*

Par exemple, les éléments irréductibles de $\mathbf{Z}$ sont, au signe près, les nombres premiers. Les irréductibles de $k[\mathrm{X}]$ sont les polynômes irréductibles au sens usuel du terme.
Un idéal d'un anneau A est dit propre si il est non égal à A.

Proposition 2.6.6. — *Un idéal propre d'un anneau* A *est maximal si et seulement si le seul idéal qui le contient strictement est* A.

Démonstration. — Soit I un idéal propre de A maximal. Supposons que J est un idéal de A qui contient I strictement. Il existe alors $a \in \mathrm{J} \setminus \mathrm{I}$. Comme A/I est un corps, il existe $b \in \mathrm{A}$ tel que $ab \in 1 + \mathrm{I}$. Alors $1 \in \mathrm{J}$ et $\mathrm{J} = \mathrm{A}$. Réciproquement, supposons que le seul idéal qui contient I strictement est A. Soit $a \in \mathrm{A} \setminus \mathrm{I}$. Alors l'idéal $\mathrm{I} + \mathrm{A}a$ engendré par I et a est A, donc il existe $b \in \mathrm{A}$ tel que $1 = ba + i$ avec $i \in \mathrm{I}$. Alors on a dans A/I, $\overline{1} = \overline{b}\overline{a}$ et donc $\overline{a}$ est inversible dans A/I. Donc A/I est un corps et I est maximal. □

Exemple 2.6.7. — *Soit k un corps et $\mathrm{P} \in k[\mathrm{X}]$. Alors l'anneau $k[\mathrm{X}]/(\mathrm{P})$ est un corps si et seulement si* P *est un polynôme non nul irréductible. Par exemple, pour $k = \mathbf{R}$ et*

$\mathrm{P}(\mathrm{X}) = \mathrm{X}^2 + 1$ *irréductible dans* $\mathbf{R}[\mathrm{X}]$*, on obtient le corps*

$$\mathbf{R}[\mathrm{X}]/(\mathrm{X}^2 + 1) \simeq \mathbf{C}$$

des nombres complexes.

Définition 2.6.8. — *Un anneau intègre* A *tel que tout idéal de* A *est engendré par un élément est dit principal.*

On a vu ci-dessus que $\mathbf{Z}$ est principal et que pour k un corps, l'anneau $k[\mathrm{X}]$ est principal.

Lemme 2.6.9. — *Soit* A *un anneau principal et* a *un élément non nul de* A*. Les 3 propriétés suivantes sont équivalentes :*
(1) a *est irréductible;*
(2) $(a) = a\mathrm{A}$ *est premier ;*
(3) $(a) = a\mathrm{A}$ *est maximal.*

Démonstration. — Montrons l'équivalence des propriétés. L'implication (3) $\Rightarrow$ (2) est déjà connue. Supposons (2). Alors écrivons a comme un produit bc. On alors $\overline{b}\overline{c} = \overline{0}$ dans $\mathrm{A}/(a)$. Comme $\mathrm{A}/(a)$ est intègre, on a $\overline{b} = \overline{0}$ ou $\overline{c} = \overline{0}$, c'est-à-dire $b \in (a)$ ou $c \in (a)$. On obtient donc (1). Enfin supposons que (1) est vérifiée. Soit J un idéal de A qui contient (a) strictement. Comme A est principal, on a $\mathrm{J} = (b)$ pour un certain $b \in \mathrm{A}$. Alors b divise a, et comme $b \notin (a)$, b est inversible et $(b) = \mathrm{I}$. Ceci implique (3). □

Par exemple, comme $\mathbf{Z}$ est principal, on obtient alors immédiatement :

Proposition 2.6.10. — *Soit* $n > 0$ *un entier. Alors l'anneau* $\mathbf{Z}/n\mathbf{Z}$ *est un corps si et seulement si* n *est premier. Ceci équivaut aussi à* $\mathbf{Z}/n\mathbf{Z}$ *intègre.*

Exercice 2.6.11. — *Soit* I *un idéal de* A *tel que pour tout* $i \in \mathrm{I}$*, il existe un entier* $n \geq 1$ *tel que* $i^n = 0$*. Montrer que la surjection canonique* $\mathrm{A} \to \mathrm{A}/\mathrm{I}$ *induit une surjection au niveau du groupe des inversibles. Montrer que c'est faux sans condition sur* I*.*

2.7. Rang d'un module libre de type fini

Soit A un anneau non nul. Un A-module V est un groupe abélien $(\mathrm{V}, +)$ muni d'une loi $\mathrm{A} \times \mathrm{V} \to \mathrm{V}$ vérifiant les axiomes des espaces vectoriels (en particulier, si A est un corps, un A-module est simplement un espace vectoriel sur k). On définit de même la notion

d'isomorphisme entre A-modules, de partie libre, de partie génératrice. Un A-module de type fini est un module qui admet une partie génératrice finie.
Un A-module libre (de type fini) est un module isomorphe à A^n avec $n \geq 0$ entier. La question est de savoir si le n en question est unique. Autrement dit, l'existence d'un isomorphisme $\mathrm{A}^n \xrightarrow{\sim} \mathrm{A}^m$ entraîne-t-elle $n = m$? [2] Voyons une preuve "élémentaire".
Supposons qu'un tel isomorphisme $\mathrm{A}^n \to \mathrm{A}^m$ existe. Il est alors défini par une matrice $\mathrm{M} \in \mathrm{M}_{m,n}(\mathrm{A})$. L'isomorphisme inverse a une matrice $\mathrm{N} \in \mathrm{M}_{n,m}(\mathrm{A})$. Ces deux matrices vérifient

$$\mathrm{MN} = \mathrm{Id}_{m,\mathrm{A}} \text{ et } \mathrm{NM} = \mathrm{Id}_{n,\mathrm{A}}.$$

Soit alors $\mathfrak{m}$ un idéal maximal de A (qui est non nul !) et notons $k = \mathrm{A}/\mathfrak{m}$ le corps résiduel (pour l'existence de $\mathfrak{m}$, voir (9.1.4) dans l'annexe). Réduisant ces identités matricielles mod $\mathfrak{m}$, on déduit l'existence de matrices dans k vérifiant

$$\bar{\mathrm{M}}\bar{\mathrm{N}} = \mathrm{Id}_{m,k} \text{ et } \bar{\mathrm{N}}\bar{\mathrm{M}} = \mathrm{Id}_{n,k}.$$

La matrice $\bar{\mathrm{M}}$ définit donc un isomorphisme de k-espaces vectoriels $k^n \xrightarrow{\sim} k^m$. La théorie de la dimension assure alors $n = m$. Cet entier n s'appelle **le rang** du module libre A^n.
Cette propriété est complètement fausse si on ne suppose plus l'anneau commutatif.

2.8. Le lemme Chinois

On sait que les anneaux $\mathbf{Z}/nm\mathbf{Z}$ et $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$ sont isomorphes si n et m sont premiers entre eux. Cette dernière condition peut s'écrire aussi $(n) + (m) = \mathbf{Z}$ d'après l'identité de Bézout.
Plus généralement, supposons qu'on ait des idéaux $\mathrm{I}_1, \cdots, \mathrm{I}_n$ d'un anneau A, deux à deux étrangers, *ie* tels que $\mathrm{I}_i + \mathrm{I}_j = \mathrm{A}$ pour $i \neq j$.

2. Le lecteur familier avec l'algèbre extérieure trouvera l'énoncé évident.

Lemme 2.8.1 **(Lemme Chinois).** — *Sous ces conditions, l'application canonique* $\mathrm{A} \to \prod_{1\leq j\leq n} \mathrm{A}/\mathrm{I}_j$ *se factorise à travers* $\bigcap_{1\leq j\leq n} \mathrm{I}_j$ *pour donner un isomorphisme*

$$\mathrm{A}/\left(\mathrm{I}_1 \cap \cdots \cap \mathrm{I}_n\right) \xrightarrow{\sim} \prod_{1\leq j\leq n} \mathrm{A}/\mathrm{I}_j.$$

De plus, on a

$$\mathrm{I}_1 \cap \cdots \cap \mathrm{I}_n = \mathrm{I}_1.\cdots.\mathrm{I}_n.$$

Remarque 2.8.2. — *Le lemme chinois (pour les entiers) est attribué au mathématicien et astronome chinois Sunzi (écriture pinyin) (ou Sun Tzu*[3]*). Il semble que son traité de mathématiques ait été écrit autour de l'an 400 (c'est du moins ce qu'écrivait en 1963 l'historien des sciences reconnu Qian Baocong), même si certains pensent qu'il vivait autour de 300. Ce qui est certain est que la première version écrite se trouve dans le livre de Qin Jiushao*[4]*,* Traité mathématique en 9 sections*, daté de 1247.*

Démonstration. — Bien entendu, le noyau de

$$\mathrm{A} \to \mathrm{A}/\mathrm{I}_1 \times \cdots \times \mathrm{A}/\mathrm{I}_n$$

est l'intersection $\mathrm{I}_1 \cap \cdots \cap \mathrm{I}_n$. Par propriété universelle du quotient, on a donc une application

$$\mathrm{A}/\mathrm{I}_1 \cap \cdots \cap \mathrm{I}_n \to \prod_{1\leq j\leq n} \mathrm{A}/\mathrm{I}_j$$

qui est injective (on a "tué" le noyau de la flèche initiale !). Vérifions la surjectivité. Si on note $\mathrm{I}(-j)$ l'idéal

$$\mathrm{I}(-j) = \mathrm{I}_1 \cdots \widehat{\mathrm{I}_j} \cdots \mathrm{I}_n = \prod_{1\leq k\leq n, k\neq j} \mathrm{I}_k$$

produit des idéaux I_i distincts de I_j (*ie* engendré par les produits d'éléments des I_i distincts de I_j), observons qu'on a

$$\sum_{1\leq j\leq n} \mathrm{I}(-j) = \mathrm{A}.$$

3. Contrairement à ce qu'on peut parfois lire sur la toile, il n'a rien à voir avec l'auteur de *L'art de la guerre.*

4. 1202–1261

En effet, on peut faire une récurrence sur n. Si $n = 2$, c'est l'hypothèse $\mathrm{I}_2 + \mathrm{I}_1 = \mathrm{A}$. Sinon, on applique l'hypothèse de récurrence à $\mathrm{I}_1, \cdots, \mathrm{I}_{n-1}$. On obtient alors que la somme des $n-1$ idéaux $\mathrm{I}_1 \cdots \widehat{\mathrm{I}_j} \cdots \mathrm{I}_{n-1}$ est A, de sorte que, multipliant par I_n, on a

$$\sum_{1 \leq j < n} \mathrm{I}(-j) = \mathrm{I}_n$$

et la somme $\sum_j \mathrm{I}(-j)$ contient I_n. En appliquant le même procédé à $\mathrm{I}_2, \cdots, \mathrm{I}_n$, on obtient que la somme contient I_1. Comme $\mathrm{I}_1 + \mathrm{I}_n = \mathrm{A}$, la somme vaut A.
On écrit alors $1 = \sum_{1 \leq j \leq n} a_j$ avec $a_j \in \mathrm{I}(-j)$. Soit alors $\bar{b}_j \in \mathrm{A}/\mathrm{I}_j$ des classes quelconques. Posons

$$b = \sum_{1 \leq j \leq n} a_j b_j.$$

Observons alors

$$a_j \equiv \begin{cases} 0 \mod \mathrm{I}_i \text{ si } i \neq j, \\ 1 \mod \mathrm{I}_i \text{ si } i = j, \end{cases}$$

de sorte que $b \equiv b_j a_j \equiv b_j \mod \mathrm{I}_j$ pour tout j.
Reste à se convaincre que le produit des I_i, clairement dans l'intersection des I_i, lui est égale. Soit donc a dans cette intersection. On a $a = \sum_i a a_i$. Comme $a \in \mathrm{I}_i$, on a $a \in \mathrm{I}_i \mathrm{I}(-i) = \mathrm{I}_1 \cdots \mathrm{I}_n$ pour tout i, ce qu'on voulait. □

Exercice 2.8.3. — *Soit d un diviseur de $n > 0$. Montrer que le morphisme d'anneaux canonique*

$$\mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/d\mathbf{Z}$$

induit une surjection au niveau des groupes des inversibles (utiliser le lemme chinois et 2.6.11).

2.9. Le morphisme de Frobenius

Soit p un nombre premier et A un anneau de caractéristique p. Montrons que A admet toujours un endomorphisme non trivial. Ceci est non banal. En effet l'anneau $\mathbf{R}$ par exemple n'a pas d'endomorphisme non trivial :

Exercice 2.9.1. — *Soit f un endomorphisme d'anneau de $\mathbf{R}$. Montrer que la restriction de f à $\mathbf{Q}$ est l'identité. Montrer que f préserve $\mathbf{R}^+$ (étudier l'image d'un carré). En déduire que f est croissante puis que f est l'identité.*

Précisément, montrons le théorème à la fois facile et important suivant.

Théorème 2.9.2 (**Morphisme de Frobenius** [5]). — *Soit p un nombre premier et* A *un anneau de caractéristique p. Alors l'application* $\mathrm{F} : a \mapsto a^p$ *définit un endomorphisme de l'anneau* A.

Démonstration. — Visiblement, F respecte le produit et $\mathrm{F}(1) = 1$. Montrons que F respecte la somme. D'après la formule du binôme de Newton, on a

$$\mathrm{F}(a+b) = \sum_{n=0}^{p} \binom{p}{n} a^n b^{p-n} = \mathrm{F}(a) + \sum_{n=1}^{p-1} \binom{p}{n} a^n b^{p-n} + \mathrm{F}(b).$$

Comme A est de caractéristique p, si $m \in \mathbf{Z}$ est multiple de p, on a $m\mathrm{A} = 0$. Il suffit donc de prouver le lemme bien connu ci-dessous. □

Lemme 2.9.3. — *Soit n tel que $0 < n < p$. Alors, le coefficient binomial $\binom{p}{n}$ est divisible par p.*

Démonstration. — On a

$$n!\binom{p}{n} = p(p-1)\cdots(p-n+1)$$

(il y a n facteurs). Donc p divise le produit $n!\binom{p}{n}$. Comme $n! = n(n-1)\cdots 1$ est produit d'entiers distincts de p premier (car $n < p$), il est premier à p. Donc le nombre premier p divise nécessairement $\binom{p}{n}$ (c'est le lemme de Gauss pour les entiers). □

5. 1848-1917

FIGURE 1. Georg Ferdinand Frobenius

CHAPITRE 3

ALGÈBRES

Les algèbres et extensions de corps jouent un rôle crucial en théorie de Galois. Dans ce chapitre nous étudions les définitions et propriétés générales de ces structures.

3.1. Algèbres et morphismes d'algèbres

Il est bien connu que $\mathbf{C}$ est à la fois un corps et un $\mathbf{R}$-espace vectoriel. De plus, la structure de multiplication externe par les réels est compatible avec la structure de produit de $\mathbf{C}$ au sens où $x.z$ (multiplication externe du complexe z par le réel x) est aussi le produit des complexes $x.1$ et z (et de façon analogue pour la somme). On dit que $\mathbf{C}$ est une $\mathbf{R}$-algèbre. Plus généralement, si k est un sous-corps du corps K, alors K est naturellement un k-espace vectoriel et la structure de k-espaces vectoriels sur K est compatible avec la structure de corps sur K. Plus généralement, donnons la définitions suivante.

Définition 3.1.1. — *Soient un corps k et un anneau* B. *On dit que* B *est une k-algèbre si* B *est de plus muni d'une multiplication externe $k \times \mathrm{B} \to \mathrm{B}$ qui en fait un k-espace vectoriel et qui vérifie*

$$1.b = b \text{ et } a.(bb') = (a.b)b' \text{ pour tous } a \in k,\ b, b' \in \mathrm{B}.$$

Cette dernière condition est la condition de compatibilité entre les structures d'anneaux et d'espace vectoriel. Il revient au même de se donner un morphisme d'anneaux $f : k \to \mathrm{B}$ car on définit alors la structure d'espace vectoriel par $a.b = f(a)b$ pour $a \in k,\ b \in \mathrm{B}$.

Exemple 3.1.2. — *L'anneau des polynôme k[X] à coefficients dans k a une structure naturelle de k-algèbre.*

Définition 3.1.3. — *Soit* B *une algèbre sur un corps* k. *Si l'anneau* B *est un corps, on dit que* B *est une* extension *de* k.

Cette extension est alors notée B/k. Cette définition est compatible avec la définition de la partie 2.3, comme discuté dans cette même partie.

Définition 3.1.4. — *Une morphisme* $f : \mathrm{B} \to \mathrm{B}'$ *de* k*-algèbres* B, B' *est un morphisme d'anneaux qui est de plus* k*-linéaire. On note* $\mathrm{Hom}_k(\mathrm{A}, \mathrm{A}')$ *l'ensemble des morphismes de* k*-algèbres.*

Deux extensions K/k et L/k de k sont dites isomorphes (ou k-isomorphes) si il existe un morphisme de k-algèbres $f : \mathrm{K} \to \mathrm{L}$ qui est un isomorphisme k-linéaire. On note alors $\mathrm{K} \simeq \mathrm{L}$ et on dit que f est un isomorphismes de k-algèbres.

Lorsqu'un morphisme de k-algèbre $f : \mathrm{A} \to \mathrm{B}$ est injectif, on dit que c'est un (k-)plongement. On note alors $f : \mathrm{A} \hookrightarrow \mathrm{B}$.

Exemple 3.1.5. — *Si* B *est une* k*-algèbre, se donner un morphisme d'algèbres* f *de* $k[\mathrm{X}]$ *dans* B *revient à se donner l'image* $b \in \mathrm{B}$ *de* X. *En effet on aura alors*

$$f(\sum a_i \mathrm{X}^i) = \sum a_i b^i$$

où $a_i \in k$ *et qu'inversement une telle formule définit bien un morphisme d'algèbre. Ainsi,*

$$\mathrm{Hom}_k(k[\mathrm{X}], \mathrm{B})$$

s'identifie canoniquement à B.

Plus généralement, on montre de la même manière le résultat suivant;

Proposition 3.1.6. — *Soient* $b_1, \cdots, b_n$ *des éléments d'une* k*-algèbre* B. *Il existe un unique morphisme de* k*-algèbre* $\phi : k[\mathrm{X}_1, \cdots, \mathrm{X}_n] \to \mathrm{B}$ *tel que pour chaque* i, $\phi(\mathrm{X}_i) = b_i$.

Si ϕ est surjectif, on dit que B est *engendré* par les b_i et on écrit $\mathrm{B} = k[b_1, \cdots, b_n]$.

Notons que si A est une k-algèbre et I un idéal de A, l'anneau quotient A/I est aussi un k-espace vectoriel (car A et I sont des k-espaces vectoriels). On vérifie facilement qu'on obtient ainsi une structure de k-algèbre sur A/I. Les résultats pour les anneaux quotients s'adaptent littéralement au cas des k-algèbres. C'est le cas notamment du lemme chinois 2.8.1.

Exemple 3.1.7. — *Le quotient* $\mathrm{K} = \mathbf{R}[\mathrm{X}]/(\mathrm{X}^2 + 1)$ *est isomorphe en tant que* $\mathbf{R}$*-algèbre à* $\mathbf{C}$. *Soit* $\overline{\mathrm{X}}$ *la classe de* X *dans le quotient* K. *On a deux isomorphismes de* $\mathbf{R}$*-algèbres* $\sigma, \overline{\sigma} : \mathrm{K} \to \mathbf{C}$ *caractérisés par* $\sigma(\overline{\mathrm{X}}) = i$ *et* $\overline{\sigma}(\overline{\mathrm{X}}) = -i$.

Exercice 3.1.8. — *Décrire un isomorphisme de* $\mathbf{R}$*-algèbres entre* $\mathbf{R}[X]/(X^2+X+1)$ *et* $\mathbf{C}$ *d'une part et entre* $\mathbf{R}[X]/(X(X+1))$ *et* $\mathbf{R}^2$ *d'autre part (utiliser le lemme chinois 2.8.1).*

3.2. Degré d'une algèbre

Définition 3.2.1. — *Soit* A *une* k*-algèbre. Sa dimension se note* $[A : k]$ *(finie ou non) et est appelée degré de* A *sur* k*.*

Le degré est donc un entier positif ou $+\infty$. Dans le cas où A est un corps K, on parle de degré de l'extension K/k.

Exemple 3.2.2. — *Le degré de* $\mathbf{C}$ *sur* $\mathbf{R}$ *est* 2*, alors que le degré de* $\mathbf{R}$ *sur* $\mathbf{Q}$ *est* $+\infty$*. Pour* k *un corps et* $P \in k[X]$*, on a la formule*

$$[k[X]/(P) : k] = deg(P).$$

En effet, les images de 1, X, ..., $X^{deg(P)-1}$ *dans* $k[X]/(P)$ *en forment une base.*

Définition 3.2.3. — *Une extension est dite finie si elle est de degré fini.*

Le théorème donne une relation importante entre les degrés d'extensions.

***Théorème 3.2.4* (Base télescopique).** — *Soit* L *une* K*-algèbre où* K *est un corps contenant* k *de sorte qu'on a des inclusions* $k \subset K \subset L$*. Soit* $(\lambda_i)_{i\in I}$ *et* $(\kappa_j)_{j\in J}$ *des bases de* L/K *et* K/k *respectivement. Alors,* $(\lambda_i\kappa_j)_{(i,j)\in I\times J}$ *est une base de* L/k*. En particulier, on a*

$$[L : k] = [L : K][K : k].$$

Démonstration. — Si on a

$$\sum_{i\in I, j\in J} a_{i,j}\lambda_i\kappa_j = \sum_{i\in I}(\sum_{j\in J} a_{i,j}\kappa_j)\lambda_i = 0$$

avec $a_{i,j} \in k$ on a $\sum_{j\in J} a_{i,j}\kappa_j = 0$ pour tout $i \in I$ (liberté des λ_i sur K) et donc $a_{i,j} = 0$ (liberté de κ_j sur k). Par ailleurs, tout $l \in L$ s'écrit

$$\sum_{i\in I} b_i\lambda_i \text{ avec } b_i \in K$$

(λ_i générateur sur K) et chaque b_i s'écrit

$$\sum_{j\in J} a_{i,j}\kappa_j \text{ avec } a_{i,j} \in k$$

(κ_j générateur sur k) de sorte que

$$l = \sum_{i\in \mathrm{I}, j\in \mathrm{J}} a_{i,j}\lambda_i\kappa_j.$$

□

3.3. Corps de rupture

Soit P un polynôme de $k[\mathrm{X}]$, qu'on suppose *irréductible* (au sens des anneaux défini précédemment, ce qui correspond à la notion usuelle de polynôme irréductible). Comme $k[\mathrm{X}]$ est principal, (P) est maximal (2.6.6) et la k-algèbre quotient $\mathrm{K} = k[\mathrm{X}]/(\mathrm{P})$ est un corps.

Le polynôme P peut être considéré comme à coefficients dans K. Par construction, $\mathrm{P}(\bar{\mathrm{X}})$ est la classe de P dans $\mathrm{K}[\mathrm{X}]/(\mathrm{P})$, et donc est nul.

Définition 3.3.1. — *On dit que* $\mathrm{K} = k[\mathrm{X}]/(\mathrm{P})$ *est le* corps de rupture *de* P.

Exemple 3.3.2. — *Le corps de rupture de* $\mathrm{X}^2 + 1$ *sur* $\mathbf{R}$ *est* $\mathbf{C}$.

Si x désigne l'image de X dans K, on a évidemment $\mathrm{K} = k[x]$.

On a donc construit une extension de corps K/k engendrée par une racine $x \in \mathrm{K}$ de P.

C'est "la plus petite" au sens suivant :

Proposition 3.3.3. — *Soit* L *une extension de* k *dans laquelle* $\mathrm{P} \in k[\mathrm{X}]$ *a une racine* ξ. *Alors le corps de rupture* K *de* P *se plonge dans* L *(comme* k*-algèbre). De plus, si* L *est engendré par* ξ, *les extensions* K/k *et* L/k *sont isomorphes.*

Démonstration. — Soit $\phi : k[\mathrm{X}] \to \mathrm{L}$ le morphisme de k-algèbre tel que $\phi(\mathrm{X}) = \xi$. Alors comme $\mathrm{P}(\xi) = 0$, on a l'idéal $(\mathrm{P}) \subset \mathrm{Ker}(\phi)$ et donc ϕ induit un morphisme $\overline{\phi} : \mathrm{K} \to \mathrm{L}$. Comme K est un corps, ce morphisme est injectif. Si L est engendré, le morphisme $\overline{\phi}$ est aussi surjectif, c'est donc un isomorphisme. □

On a alors le lemme fondamental suivant.

Lemme 3.3.4. — *Soit* L *une extension de* k *et* $\mathrm{K} = k[x]$ *le corps de rupture de* $\mathrm{P} \in k[\mathrm{X}]$ *irréductible. Alors, l'application de* $\mathrm{Hom}_k(\mathrm{K}, \mathrm{L})$ *dans* L *qui à* ϕ *associe* $\phi(x)$ *définit une bijection de* $\mathrm{Hom}_k(\mathrm{K}, \mathrm{L})$ *sur les racines de* P *dans* L.

Autrement dit, on peut identifier $\mathrm{Hom}_k(\mathrm{K}, \mathrm{L})$ et l'ensemble des racines de P dans L.

Démonstration. — Se donner $\sigma \in \mathrm{Hom}_k(k[x], \mathrm{L}) = \mathrm{Hom}_k(k[\mathrm{X}]/(\mathrm{P}), \mathrm{L})$ c'est se donner $\sigma \in \mathrm{Hom}_k(k[\mathrm{X}], \mathrm{L})$ qui annule P par propriété universelle du quotient (2.4.5). Autrement dit c'est se donner $y = \sigma(\mathrm{X})$ tel que $\sigma(\mathrm{P}(\mathrm{X})) = \mathrm{P}(y)$ est nul (3.1.5). □

3.4. Éléments algébriques, transcendants

Soit k un sous-corps d'un corps K, c'est-à-dire une extension K/k.

Définition 3.4.1. — *Un élément $x \in \mathrm{K}$ est dit* ***algébrique*** *sur k si il existe $\mathrm{P} \in k[\mathrm{X}]$ non nul annulant x. Sinon, il est dit* ***transcendant*** *(sur k). Une extension K/k est dite* ***algébrique*** *si tous les éléments de K sont algébriques (sur k).*

Dans le cas $k = \mathbf{Q}$, on a le résultat suivant.

Proposition 3.4.2. — *L'ensemble des nombres complexes qui sont algébriques sur $\mathbf{Q}$ est dénombrable.*

Démonstration. — Le corps $\mathbf{Q}$ étant dénombrable, l'ensemble des polynômes de $\mathbf{Q}[\mathrm{X}]$ de degré $n \geq 0$ fixé est dénombrable. L'ensemble X_n de toutes leurs racines dans K est donc dénombrable, car chacun de ces polynômes a au plus n racines. L'ensemble des racines $\bigcup_{n\geq 0} \mathrm{X}_n$ de tous les polynômes non nuls de $\mathbf{Q}[\mathrm{X}]$ est donc dénombrable comme union dénombrable d'ensembles dénombrables. Cette union est exactement l'ensemble des éléments de K algébriques sur $\mathbf{Q}$. □

Par exemple, le réel $\sum_{n\geq 0} 10^{-n!}$ est transcendant sur $\mathbf{Q}$: c'est le premier exemple explicite de nombre transcendant (dû à Liouville en 1844). Il est bien connu que les nombres e (Hermite [1], 1872) et π (Lindemann [2], 1882) sont transcendants sur $\mathbf{Q}$, mais c'est beaucoup plus difficile.

Rappelons que la transcendance de π assure qu'un problème vieux de plus 3 millénaires est insoluble, la quadrature du cercle, car sinon $\sqrt{\pi}$ donc également π seraient algébriques sur $\mathbf{Q}$. Une preuve de la transcendance de e et π, présentation de la simplification des preuves originales due à Hilbert largement inspirée de [**CL**], sera donnée plus bas dans la partie (9.3).

1. 1822-1901
2. 1852-1935

FIGURE 1. Charles Hermite

FIGURE 2. Ferdinand Lindemann

3.5. Degré de transcendance

Soit K/k une extension d'un corps K. Définissons l'analogue algébrique de la notion de famille linéairement libre dans un espace vectoriel.

Définition 3.5.1. — *Une famille* $\mathcal{F} = (x_i)_{i\in \mathrm{I}}$ *d'éléments de* K *est dite algébriquement indépendante (sur* k*) si pour tout* $\mathrm{N} \geq 0$*, toute sous-famille finie* $\{x_{i_1}, \cdots, x_{i_\mathrm{N}}\} \subset \mathcal{F}$ *(les* i_j *sont distincts) et tout polynôme de* N *variables* $\mathrm{P}(\mathrm{X}_1, \cdots, \mathrm{X}_\mathrm{N}) \in k[\mathrm{X}_1, \cdots, \mathrm{X}_n]$ *non trivial, on a* $\mathrm{P}(x_1, \cdots, x_\mathrm{N}) \neq 0$*.*

Autrement dit, il n'y a pas de relation algébrique non triviale entre les x_i. Par analogie avec la notion de dimension pour un espace vectoriel, définissons la notion de degré de transcendance de la manière suivante.

Définition 3.5.2. — *Supposons qu'il existe* $\mathrm{N} \geq 0$ *tel qu'il n'existe pas de famille algébriquement libre de* K *de cardinal* $\mathrm{N}+1$ *et qu'il existe une famille algébriquement libre de* K *de cardinal* N*. On dit alors que* K/k *est de degré de transcendance* N*.*

Sinon, on dit que le degré de transcendance de K/k *est infini.*

Par exemple, le corps des fractions à n-indéterminées

$$\mathrm{Frac}(k[\mathrm{X}_1, \cdots, \mathrm{X}_n]) = k(\mathrm{X}_1, \cdots, \mathrm{X}_n)$$

est un corps de degré de transcendance n sur k. C'est loin d'être immédiat (cf. corollaire 2 de [**B2**, V.14.3]).

Proposition 3.5.3. — *L'extension* K/k *est de degré de transcendance* 0 *si et seulement si* K/k *est algébrique.*

Démonstration. — Si l'extension est de degré de transcendance 0, alors toute famille avec un élément $\{x\}$ n'est pas algébriquement indépendante. Ceci signifie qu'on a un polynôme

$\mathrm{P}(\mathrm{X}) \in k[\mathrm{X}]$ tel que $\mathrm{P}(x) = 0$, c'est-à-dire que x est algébrique sur k. Réciproquement, si K/k est algébrique, pour la même raison, aucune famille non vide n'est algébriquement indépendante. □

Le corps des réels est de degré de transcendance infini sur le corps des rationnels.

3.6. Critère d'algébricité

La caractérisation suivante est aussi élémentaire que fondamentale.

Proposition 3.6.1. — *Les propositions suivantes sont équivalentes.*

- *(i) x est algébrique sur k ;*
- *(ii) l'algèbre $k[x]$ est de dimension finie sur k ;*
- *(iii) l'algèbre $k[x]$ engendrée par x est un corps.*

Démonstration. — $(i) \Rightarrow (ii)$: si x est algébrique sur k, il est annulé par un polynôme de degré $d > 0$ et $1, \cdots, x^{d-1}$ engendre $k[x]$.
$(ii) \Rightarrow (iii)$: l'implication provient du fait qu'une algèbre A intègre de dimension finie sur un corps K est un corps. En effet, soit a non nul dans une telle algèbre A. On définit $\phi : \mathrm{A} \to \mathrm{A}$ par $\phi(x) = ax$. Alors ϕ est k-linéaire et, comme A est intègre, ϕ est injective. Donc ϕ est un isomorphisme et $1 \in \mathrm{Im}(\phi)$. Le résultat en découle.
$(iii) \Rightarrow (i)$: si $k[x]$ est un corps, ou bien x est nul, et $x = 0$ est certainement algébrique, ou bien $x^{-1} = \mathrm{P}(x) \in k[x]$ et l'équation

$$x\mathrm{P}(x) - 1 = 0$$

est une relation de liaison entre les $x^i, i \leq \deg(\mathrm{P}) + 1$ prouvant que $k[x]$ est de dimension finie sur k. □

Un polynôme non nul $\mathrm{P} \in k[\mathrm{X}]$ est dit *unitaire* si son coefficient dominant est égal à 1.

Proposition 3.6.2. — *Soit* I *un idéal non nul de* $k[\mathrm{X}]$. *Alors il existe un unique polynôme unitaire* $\mathrm{P} \in k[\mathrm{X}]$ *tel que* $\mathrm{I} = (\mathrm{P})$.

Démonstration. — On a déjà vu l'existence de $\mathrm{P} \in k[\mathrm{X}]$ tel que $\mathrm{I} = (\mathrm{P})$. Si un autre polynôme Q engendre I, alors P divise Q et Q divise P, donc il existe $\lambda \in k$ non nul tel que $\mathrm{Q} = \lambda\mathrm{P}$. Réciproquement, un tel polynôme $\lambda\mathrm{P}$ engendre I. Donc l'ensemble des polynômes qui engendrent I est exactement l'ensemble des $\lambda\mathrm{P}$ avec $\lambda \in k$ non nul. Dans

ces ensemble, il y a un seul polynôme unitaire, obtenu pour λ égal à l'inverse du coefficient dominant de P. □

Définition 3.6.3. — *Soit x algébrique sur k;*

On appelle polynôme minimal de x le générateur unitaire de l'idéal des polynômes de $k[\mathrm{X}]$ annulant x (idéal des polynômes annulateurs de x).

On appelle degré $\deg_k(x)$ de x sur k la dimension $[k[x] : k]$.

Proposition 3.6.4. — *Soit* P *le polynôme minimal de $x \in \mathrm{K}$ algébrique sur k. Alors,*

— P *est irréductible dans $k[x]$;*

— *le corps $k[x]$ est (canoniquement) k-isomorphe à $k[\mathrm{X}]/(\mathrm{P})$;*

— *on a $\deg_k(x) = \deg(\mathrm{P})$.*

Démonstration. — Par définition, le morphisme d'algèbre $k[\mathrm{X}] \to \mathrm{K}$ qui envoie X sur x (3.1.5) a pour image $k[x]$ et pour noyau l'idéal (P). On a donc (2.4.5) un isomorphisme $k[\mathrm{X}]/(\mathrm{P}) \xrightarrow{\sim} k[x]$ d'où la formule $\deg_k(x) = \deg(\mathrm{P})$ puisque les images des monômes $\mathrm{X}^n, 0 \leq n < \deg(\mathrm{P})$ forment une base de $k[\mathrm{X}]/(\mathrm{P})$. Si maintenant $\mathrm{P} = \mathrm{QR}$ avec Q, R unitaires, on a $\mathrm{Q}(x)\mathrm{R}(x) = 0$. Comme K est intègre, on a $\mathrm{Q}(x) = 0$ et donc $\mathrm{P}|\mathrm{Q}$. Comme $\deg(\mathrm{Q}) \leq \deg(\mathrm{P})$, on a $\mathrm{P} = \mathrm{Q}$ et P irréductible (on peut aussi invoquer (2.6.6) si on veut). □

Définition 3.6.5. — *Soient x algébrique sur k de polynôme minimal* P *et* L *une extension de k. Les racines de* P *dans* L *s'appellent les k-conjugués de x dans* L *(ou conjugués dans* L *lorsque le corps de base k est clair dans le contexte).*

Soit L une extension de k et x algébrique sur k. Alors, $\mathrm{Hom}_k(k[x], \mathrm{L})$ s'identifie aux conjugués de x dans L. Précisément, tenant compte de 3.6.4 et 3.3.4, on obtient le résultat suivant.

Proposition 3.6.6. — *L'application qui à $\sigma \in \mathrm{Hom}_k(k[x], \mathrm{L})$ associe $\sigma(x)$ est une bijection entre l'ensemble des k-plongements de $k[x]$ dans* L *et les conjugués de x dans* L.

Proposition 3.6.7. — *Le sous-ensemble* A *de* K *des éléments algébriques sur k est un sous-corps de* K.

Démonstration. — A et $\mathrm{A} - 0$ sont non vides. Vérifions que la différence et le produit de deux algébriques x, y est algébrique. Par hypothèse, les x^i $(0 \leq i \leq \deg_k(x))$, y^j $(0 \leq \deg_k(y))$ engendrent $k[x]$ et $k[y]$ respectivement. On en déduit que les monômes $x^i y^j$ avec $0 \leq i \leq \deg_k(x)$, $0 \leq j \leq \deg_k(y)$ engendrent $k[x, y]$ qui est donc de dimension finie

sur k. Mais $k[x-y]$ et $k[xy]$ sont contenus dans $k[x,y] = k[x][y]$, donc sont eux-mêmes de dimension finie. Si x non nul est algébrique annulé par P, alors $1/x$ est annulé par $\mathrm{X}^{\deg(\mathrm{P})}\mathrm{P}(1/\mathrm{X})$ qui est un polynôme non nul. □

Bien entendu, le degré d'une extension de corps est plus grand que le degré de tous ses éléments.

Comme conséquence du Théorème 3.2.4, on a le résultat suivant.

Corollaire 3.6.8. — *Si $x_1, \cdots, x_n$ sont algébriques, alors l'algèbre $k[x_1, \cdots, x_n]$ des polynômes en les x_i est un corps de dimension sur k inférieure ou égale à $\prod_{1\leq i\leq n} \deg_k(x_i)$.*

On en déduit le résultat suivant.

Corollaire 3.6.9. — *Une extension d'un corps k est finie si et seulement si elle est algébrique et engendrée par un nombre fini d'éléments.*

Démonstration. — Une extension algébrique engendrée par un nombre fini d'éléments est finie d'après le résultat précédent. La réciproque se démontre par récurrence sur le degré $[\mathrm{K} : k]$ d'une telle extension K/k. Pour $[\mathrm{K} : k] = 1$ c'est clair. En général, on considère x dans K qui n'est pas dans k. Alors $[\mathrm{K} : k[x]] < [\mathrm{K} : k]$. Il suffit alors d'appliquer l'hypothèse de récurrence à l'extension $\mathrm{K}/k[x]$. On obtient alors $x_1, \cdots, x_\mathrm{N}$ tels que $\mathrm{K} = (k[x])[x_1, \cdots, x_\mathrm{N}] = k[x, x_1, \cdots, x_\mathrm{N}]$. □

Notons que le terme "engendrée" dans le Corollaire peut signifier "engendrée comme k-algèbre" ou bien "engendrée comme espace vectoriel sur k" (l'énoncé est vrai dans les deux cas).

Remarque 3.6.10. — *Réciproquement, on peut prouver, mais c'est plus difficile et surtout beaucoup plus profond, que $k[x_1, \cdots, x_n]$ est un corps si et seulement il est de dimension finie sur k. C'est le théorème des zéros de Hilbert*[3].

3.7. Notion de clôture algébrique

Un polynôme $\mathrm{P} \in \mathrm{K}[\mathrm{X}]$ est dit *scindé* si toutes ses racines sont dans K, c'est-à-dire si P se factorise sous la forme $\mathrm{P}(\mathrm{X}) = \lambda(\mathrm{X} - x_1)\cdots(\mathrm{X} - x_n)$ avec $\lambda, x_1, \cdots, x_n \in \mathrm{K}$.

Définition 3.7.1. — *On dit qu'un corps* K *est algébriquement clos si tout polynôme non constant de* $\mathrm{K}[\mathrm{X}]$ *est scindé sur* K.

3. 1862-1943

FIGURE 3. David Hilbert

L'exemple fondamental est le corps $\mathbf{C}$ qui est algébriquement clos. Ceci peut être obtenu comme conséquence du théorème de Liouville [4] :

***Théorème 3.7.2* (Liouville).** — *Soit $f : \mathbf{C} \to \mathbf{C}$ une fonction holomorphe. Si f est bornée alors f est constante.*

FIGURE 4. Joseph Liouville

On en déduit :

Corollaire 3.7.3. — *Le corps $\mathbf{C}$ est algébriquement clos.*

Démonstration. — Soit $\mathrm{P} \in \mathbf{C}[\mathrm{X}]$ non constant unitaire de degré $n > 0$. Supposons $\mathrm{P}(z)$ non nul pour tout $z \in \mathbf{C}$. Alors, $1/\mathrm{P}$ est holomorphe comme quotient de fonctions holomorphes à dénominateur qui ne s'annule pas. Soit $a \geq 0$ le maximum des modules des coefficients de P de degré strictement plus petit que n. On a pour $|z| > 1$ l'inégalité $|\mathrm{P}(z)|/|z|^n \geq 1 - a/|z|$ et donc $\lim_{|z|\to\infty} |1/\mathrm{P}(z)| = 0$. Par continuité, on déduit que $1/\mathrm{P}$ est bornée sur $\mathbf{C}$, donc constante d'après le théorème de Liouville, contradiction. □

4. 1809-1882

Exercice 3.7.4. — *Soit* P *un polynôme irréductible de* $k[X]$ *et soit* L *un sur-corps de* k *qui contient une racine de* P. *Montrer qu'on peut trouver un* k*-morphisme (injectif) du corps de rupture de* P *dans* L. *Si* P *est quelconque, non constant, montrer par récurrence sur* $\deg(P)$ *qu'il existe une extension* L/k *tel que* P *soit scindé dans* L. *Généraliser au cas d'une famille* $P_1, \cdots, P_n$ *de polynômes non constants.*

Définition 3.7.5. — *On dit qu'un corps* K *est une clôture algébrique du sous-corps* k *si* K *est algébrique sur* k *et si tout polynôme de* $k[X]$ *est scindé dans* K.

Avec cette définition, si Ω est algébriquement clos et contient k, l'ensemble des éléments de Ω qui sont algébriques sur k est d'une part un corps (3.6.7) et d'autre part est une clôture algébrique de k.

Avant de montrer qu'une clôture algébrique existe toujours, montrons le lemme "rassurant" suivant.

Lemme 3.7.6. — *Une clôture algébrique* $\bar{k}$ *de* k *est algébriquement close.*

Démonstration. — Soit $P \in \bar{k}[X]$ non constant. Il suffit de montrer qu'il a une racine dans $\bar{k}$. Le corps L engendré par les coefficients de P est de dimension finie sur k, puisque les coefficients de P sont algébriques sur k. Ainsi, la k-algèbre $A = L[X]/(P)$ est de dimension finie sur k, à savoir $\deg(P)\dim_k(L)$ (base télescopique). Considérons le morphisme $k[T] \to A$ d'évaluation en la classe x de X dans A (c'est-à-dire qui à P associe $P(x)$). Ce morphisme n'est donc pas injectif puisque $\dim_k(k[T]) = \infty$. Soit donc $Q \in k[T] - 0$ annulant x, autrement dit $P|Q$ et en particulier Q non constant (car $\deg(P) > 0$). Mais Q étant à coefficients dans k, Q est scindé sur $\bar{k}$. Il en est donc de même de P qui le divise. □

Exemple 3.7.7. — *Le sous-corps* $\bar{\mathbf{Q}}$ *de* $\mathbf{C}$ *des éléments de* $\mathbf{C}$ *algébriques sur* $\mathbf{Q}$ *est donc algébriquement clos. Mais* $\bar{\mathbf{Q}}$ *n'est pas égal à* $\mathbf{C}$ *! En effet, nous avons vu que* $\bar{\mathbf{Q}}$ *est dénombrable, alors que* $\mathbf{C}$ *ne l'est pas.*

Théorème 3.7.8 (**Steinitz**[5]). — *Tout corps* k *admet une clôture algébrique, unique à* k*-isomorphisme près.*

Notons que l'isomorphisme dont le théorème affirme l'existence est loin d'être unique comme on le verra : on peut même prouver qu'un corps algébriquement clos admet une

5. 1871-1928

FIGURE 5. Ernst Steinitz

infinité d'automorphismes. On va prouver d'abord l'existence, puis l'unicité qui découle du fondamental théorème de prolongement des morphismes. On invite le lecteur à passer cette preuve d'existence à la première lecture.

3.8. Preuve de l'existence de la clôture algébrique

Une fois encore, on va quotienter. Construisons tout d'abord une grande algèbre A dans laquelle tout polynôme a une racine. On note $c(\mathrm{P})$ le coefficient dominant de tout polynôme non nul. Le plus simple est de considérer l'algèbre de polynômes à "beaucoup d'indéterminées"

$$\mathrm{A} = k[\mathrm{X}_{\mathrm{P},i}]_{\mathrm{P}\in k[\mathrm{X}]\setminus\{0\},1\leq i\leq \deg(\mathrm{P})}.$$

Pour $\mathrm{P} \in k[\mathrm{X}]$ non nul et $0 \leq i \leq \deg(\mathrm{P})$, on note alors $\gamma(i,\mathrm{P})$ les coefficients du polynôme en X

$$\mathrm{P}(\mathrm{X}) - c(\mathrm{P}) \prod_{i=1}^{\deg(\mathrm{P})} (\mathrm{X} - \mathrm{X}_{\mathrm{P},i}).$$

Soit I l'idéal engendré par les $\gamma(i,\mathrm{P})$ où P décrit $k[\mathrm{X}] \setminus \{0\}$ et $0 \leq i \leq \deg(\mathrm{P})$. Notons que si P est constant, on a $\gamma(0,\mathrm{P}) = 0$.
On a alors $\mathrm{I} \neq \mathrm{A}$. Sinon, on aurait une écriture

$$\sum_{j,\mathrm{P}} \mathrm{Q}_{\mathrm{P},i_j}\gamma(i_j,\mathrm{P}) = 1 \text{ avec } \mathrm{Q}_{\mathrm{P},i_j} \in \mathrm{A}.$$

Les coefficients $\gamma(0,\mathrm{P})$ des polynômes constants étant nuls, seuls contribuent dans cette somme des polynômes de degré strictement positif. Choisissons une extension de corps K/k telle que ces polynômes P (qui sont en nombre fini) soient scindés de racines $(x_{\mathrm{P},i})_{1\leq i\leq \deg(\mathrm{P})}$

dans cette extension K (3.7.4). Soit $\phi : \mathrm{A} \to \mathrm{K}$ le morphisme de k-algèbres envoyant les $\mathrm{X}_{\mathrm{P},i}$ correspondants sur $x_{\mathrm{P},i}$ et les autres indéterminées sur 0. Alors ϕ induit un morphisme $\mathrm{A}[\mathrm{X}] \to \mathrm{K}[\mathrm{X}]$ qui envoie les polynômes correspondants

$$\mathrm{P}(\mathrm{X}) - c(\mathrm{P}) \prod_{i=1}^{\deg(\mathrm{P})} (\mathrm{X} - \mathrm{X}_{\mathrm{P},i})$$

sur

$$\mathrm{P}(\mathrm{X}) - c(\mathrm{P}) \prod_{i=1}^{\deg(\mathrm{P})} (\mathrm{X} - x_{\mathrm{P},i}) = 0$$

par construction de sorte que

$$\phi(\gamma(i, \mathrm{P})) = 0 \text{ pour tout } i.$$

On en déduit que $0 = 1$ dans K, ce qui n'est pas. L'idéal I est propre.
Soit alors J un idéal maximal de A contenant I et L le corps A/J (pour l'existence de J, voir (9.1.4) dans l'annexe). Par construction, tout polynôme $\mathrm{P} \in k[\mathrm{X}]$ non constant est scindé dans L, ses racines étant les images de $\mathrm{X}_{\mathrm{P},i}$. Toutes ces racines sont algébriques sur k. Or elles engendrent L comme k-algèbre. On a donc bien L algébrique sur k.

3.9. Preuve de l'unicité de la clôture algébrique

Pour l'unicité, montrons l'énoncé suivant.

Théorème 3.9.1 **(Prolongement des morphismes).** — *Soient* K, Ω *deux extensions de* k*. Supposons* K/k *algébrique et* Ω *algébriquement clos. Alors, il existe un plongement (de* k*-algèbres)* $\mathrm{K} \hookrightarrow \Omega$*.*

Démonstration. — Soit E l'ensemble (non vide) des couples (L, σ) où L est un sous-corps de K contenant k et σ un k-plongement

$$\sigma : \mathrm{L} \hookrightarrow \Omega.$$

Chaque σ fait de Ω une L-algèbre. Le prolongement de tels plongements définit une relation d'ordre sur E qui en fait visiblement un ensemble inductif (voir l'Annexe (9.1)). Soit alors (L, σ) un élément maximal (Lemme de Zorn, voir l'Annexe (9.1)). Montrons $\mathrm{L} = \mathrm{K}$. Soit $x \in \mathrm{K}$. Comme x est algébrique sur k il l'est sur L. Soit $\mathrm{P}(\mathrm{X}) = \sum a_i \mathrm{X}^i$ le polynôme minimal de x sur L. On a un isomorphisme naturel de L-algèbre entre $\mathrm{L}[\mathrm{X}]/(\mathrm{P})$ et $\mathrm{L}[x]$. Soit y une racine de $\mathrm{P}^\sigma(\mathrm{X}) = \sum \sigma(a_i)\mathrm{X}^i$ dans Ω. Il existe un unique morphisme

de L-algèbres $L[X]/P \to \Omega$ tel que l'image de X est y. En effet, l'image de P dans Ω est par définition $P^\sigma(y) = 0$ (3.6.6). On obtient donc maintenant l'existence d'un morphisme de k-algèbres $L[x] \to \Omega$ prolongeant σ. Par maximalité de L, on déduit $x \in L$. □

Remarque 3.9.2. — *σ permet d'identifier* L *à σ(L). Dorénavant, on le fera directement, sans distinguer entre* L *et σ(L) (cf. 2.3). Notons également que si* K *est une extension finie, alors la notion de dimension permet de montrer l'existence de* L *sans recours au lemme de Zorn.*

Une autre manière d'exprimer l'énoncé du théorème de prolongement, que nous utiliserons souvent, est la suivante.

Corollaire 3.9.3. — *Soit K/k algébrique et Ω/k algébriquement clos. Soit $\sigma : K \to \Omega$ un morphisme de k-algèbres et Ω'/k une clôture algébrique de k contenant* K. *Alors σ peut être prolongé en un morphisme de k-algèbres $\tilde{\sigma} : \Omega' \to \Omega$.*

Démonstration. — Le corps Ω' est une K-algèbre qui est algébrique sur K. De plus σ fait de Ω une K-algèbre qui est algébriquement close sur K. Donc d'après le théorème de prolongement, on a $\Psi : \Omega' \to \Omega$ un plongement qui est un morphisme de K-algèbres. Mais alors comme $k \subset K$, Ψ est aussi un morphisme de k-algèbres. De plus, pour $x \in K$, on a $\Psi(x.1) = \sigma(x)\Psi(1)$ donc $\Psi = \sigma$ sur K. Ainsi Ψ prolonge bien σ. □

Nous avons maintenant les conséquences importantes suivantes.

Corollaire 3.9.4. — *Deux clôtures algébriques K_1, K_2 de k sont k-isomorphes.*

Démonstration. — Considérant K_1 comme algébrique et K_2 comme algébriquement clos, le théorème de prolongement 3.9.1 assure qu'il existe un plongement de K_1 dans K_2. Avec les notations précédentes, le choix d'un tel plongement de K_1 dans K_2 permet de voir K_1 comme un sous-corps de K_2. Faisant alors jouer les rôles de (k, K, Ω) à (K_1, K_2, K_1), on déduit l'existence de $\tau \in \mathrm{Hom}_{K_1}(K_2, K_1)$, autrement dit d'un diagramme commutatif

$$\begin{array}{ccc} K_2 & \xrightarrow{\tau} & K_1 \\ {\scriptstyle\sigma}\uparrow & \nearrow & \\ K_1 & & \end{array} .$$

(le terme "diagramme commutatif" signifie que les deux sens du diagramme donnent la même application, c'est-à-dire ici que $\tau \circ \sigma = \mathrm{Id}$). Comme τ est un morphisme de corps, τ est injectif. L'égalité $\tau \circ \sigma = \mathrm{Id}$ assure sa surjectivité, τ et σ sont inverses l'un de l'autre. □

Corollaire 3.9.5. — *Soient* K/k, Ω/k *deux extensions de* k *avec* K/k *algébrique et* Ω *algébriquement clos. Alors, les conjugués dans* Ω *de* $x \in \mathrm{K}$ *sont les* $\sigma(x), \sigma \in \mathrm{Hom}_k(\mathrm{K}, \Omega)$.

Démonstration. — Si $y \in \Omega$ est un conjugué de x, il existe $\sigma \in \mathrm{Hom}_k(k[x], \Omega)$ tel que $\sigma(x) = y$ (3.6.6). Reste à prolonger σ à K tout entier, ce qui est possible (3.9.1). Inversement, $\sigma \in \mathrm{Hom}_k(\mathrm{K}, \Omega)$ laisse invariant le polynôme minimal de x sur k (c'est-à-dire que σ laisse invariant tous ses coefficients). Il permute donc ses racines, qui sont les conjugués de x par définition (3.6.6). □

3.10. Corps des racines d'un polynôme

Soit k un sous-corps de Ω algébriquement clos. Soit P un polynôme de $k[\mathrm{X}]$, non nécessairement irréductible.

Définition 3.10.1. — *Le corps des racines (ou de décomposition) de* P *est le sous-corps de* Ω *engendré par les racines de* P *dans* Ω.

C'est le plus petit sous-corps de Ω dans lequel P est scindé. Bien sûr, il est contenu dans la clôture algébrique de k dans Ω, sous-ensemble des algébriques sur k. On en déduit qu'il ne dépend pas de Ω, à isomorphisme non unique près (3.9.4). Ceci justifie l'article "le" dans l'expression **le corps des racines de** P (on peut dire aussi **le corps de décomposition de** P). Dans la suite, on fixera ainsi une clôture algébrique dans laquelle on travaillera. Ceci permet de parler du corps des racines. Par exemple, on s'intéressera aux sous-corps de $\mathbf{C}$ algébriques sur $\mathbf{Q}$.

CHAPITRE 4

CORPS FINIS, CORPS PARFAITS

Le cadre choisi dans ce livre est celui des corps parfaits, que nous étudions dans ce chapitre. Nous introduisons d'abord les corps finis qui sont des exemples fondamentaux de corps parfaits.

4.1. Existence et unicité des corps finis

Soit k un corps fini (c'est-à-dire de cardinal fini en tant qu'ensemble). On a vu (Proposition 2.5.4) que la caractéristique de k est alors nécessairement un nombre premier $p > 0$ et qu'il contient le corps $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. Étudions le cardinal de k.

Lemme 4.1.1. — *Le cardinal d'un corps fini k est de la forme $q = p^n$ où p est la caractéristique de k.*

Démonstration. — Comme k est fini, il est de dimension finie n comme espace vectoriel sur $\mathbf{F}_p$. Le choix d'une base définit un $\mathbf{F}_p$-isomorphisme d'espaces vectoriels $\mathbf{F}_p^n \xrightarrow{\sim} k$. Comme $\mathbf{F}_p^n$ est de cardinal p^n, le lemme est prouvé. □

Soit Ω une clôture algébrique de $\mathbf{F}_p$. Comme k est de cardinal fini, il est algébrique sur $\mathbf{F}_p$. D'après 3.9.1, k se plonge dans Ω. On peut donc supposer que k est contenu dans Ω.

Lemme 4.1.2. — *k est l'ensemble des racines dans Ω du polynôme $\mathrm{X}^q - \mathrm{X}$.*

Démonstration. — Comme k^* est d'ordre $q-1$, on a $x^{q-1} = 1$ pour tout $x \neq 0$ d'après le théorème de Lagrange. Donc $x^q = x$ pour tout $x \in k$. Comme le polynôme $\mathrm{X}^q - \mathrm{X}$ admet au plus $\mathrm{card}(k) = q$ racines, on déduit que k est nécessairement l'ensemble des racines de $\mathrm{X}^q - \mathrm{X}$. □

Le lemme implique en particulier l'unicité d'un corps de cardinal $q = p^n$, au sens où tout sous-corps de Ω de cardinal q est égal à k.

Lemme 4.1.3. — *Deux corps finis sont isomorphes si et seulement si ils ont même cardinal.*

Démonstration. — Soient k, k' de même cardinal $q = p^n$. Choisissons Ω algébriquement clos de caractéristique p (donc contenant $\mathbf{F}_p$). L'identité de $\mathbf{F}_p$ se prolonge en des plongements s, s' de k, k' dans Ω. Mais comme Ω a un unique sous-corps de cardinal q, on a $s(k) = s'(k')$ de sorte que $s^{-1}s'$ est bien défini et est l'isomorphisme cherché. □

Maintenant montrons l'existence.
Considérons donc $\mathbf{F}_q$ l'*ensemble* des racines dans Ω de $\mathrm{X}^q - \mathrm{X}$.

Lemme 4.1.4. — $\mathbf{F}_q$ *est un sous-corps de* Ω *à* q *éléments (et c'est le seul).*

Démonstration. — Notons F le morphisme de Frobenius (2.9.2) $\mathrm{F} : \ x \mapsto x^p$ de Ω.
Rappelons que c'est un morphisme d'anneaux, et donc l'itéré F^n également. On a donc

$$(x+y)^q = \mathrm{F}^n(x+y) = \mathrm{F}^n(x) + \mathrm{F}^n(y) = x^q + y^q,$$

ce qui prouve la stabilité par somme de $\mathbf{F}_q$. La stabilité par produit, inverse et opposé est évidente. Ainsi, $\mathbf{F}_q$ est un sous-corps. Reste le cardinal. Il faut voir que les racines sont simples. Si l'une d'elles était double au moins, elle annulerait $(\mathrm{X}^q - \mathrm{X})' = -1$, ce qui n'est pas. L'unicité a été vue dans la discussion au début de cette partie : un tel corps est nécessairement l'ensemble des racines de $\mathrm{X}^q - \mathrm{X}$. □

Lemme 4.1.5. — $\mathbf{F}_{p^n}$ *est contenu dans* $\mathbf{F}_{p^m}$ *si et seulement si* $n|m$. *De plus, pour* $q = p^n$, *la clôture algébrique* $\bar{\mathbf{F}}_q$ *de* $\mathbf{F}_q$ *dans* Ω *est la réunion croissante* $\bigcup_{\mathrm{N}\geq 1} \mathbf{F}_{q^{\mathrm{N}!}}$.

Démonstration. — Si $n|m$, toute racine de $\mathrm{X}^{p^n} - \mathrm{X}$ est racine de $\mathrm{X}^{p^m} - \mathrm{X}$ d'où l'inclusion $\mathbf{F}_{p^n} \subset \mathbf{F}_{p^m}$. Inversement, si $\mathbf{F}_{p^n} \subset \mathbf{F}_{p^m}$, on a $\mathbf{F}_{p^n}^* \subset \mathbf{F}_{p^m}^*$ et donc $(p^n - 1)|(p^m - 1)$ d'après le théorème de Lagrange. Écrivons la division euclidienne $m = an + r, 0 \leq r < n$. On a alors

$$p^m - 1 = p^{an}p^r - 1 = (p^{an} - 1)p^r + p^r - 1.$$

Mais, d'après la formule des sommes partielles d'une série géométrique, $(p^n-1)|(p^{an}-1)$. Ainsi $p^n-1|p^r-1<p^n-1$, ce qui n'est possible que si $r=0$. On obtient le résultat voulu.

Soit à présent $q=p^n$. Pour $\mathrm{N}\geq 1$, les éléments de $\mathbf{F}_{q^{\mathrm{N}!}}$ sont algébriques sur $\mathbf{F}_q$ et donc $\mathbf{F}_{q^{\mathrm{N}!}}\subset\bar{\mathbf{F}}_q$.

Soit maintenant $x\in\bar{\mathbf{F}}_q$. Alors on a un polynôme non trivial $\mathrm{P}(\mathrm{X})\in\mathbf{F}_q[\mathrm{X}]$ tel que $\mathrm{P}(x)=0$. En appliquant les itérés de F^n (le morphisme de Frobenius à la puissance n), on obtient $\mathrm{P}(\mathrm{F}^{rn}(x))=0$ pour tout $r\geq 0$. Donc $(\mathrm{F}^{rn}(x))_{r\geq 0}$ est inclus dans l'ensemble des racines de P, qui est fini. Donc il existe $r'>r\geq 0$ tel que $\mathrm{F}^{r'n}(x)=\mathrm{F}^{rn}(x)$. Ceci implique $\mathrm{F}^{(r'-r)n}(x)=x$ et donc $x\in\mathbf{F}_{q^{r'-r}}$. □

Notons que, pour $n|m$, si d est la dimension de $\mathbf{F}_{p^m}$ sur $\mathbf{F}_{p^n}$, on a, en tant qu'espace vectoriel, $\mathbf{F}_{p^m}\xrightarrow{\sim}(\mathbf{F}_{p^n})^d$. En comptant les cardinaux, on obtient $p^m=(p^n)^d$, d'où $d=m/n$.

Notons aussi qu'*a fortiori*, $\mathbf{F}_q$ est le corps de décomposition de $\mathrm{X}^q-\mathrm{X}$ sur $\mathbf{F}_p$ (dans Ω). On parlera donc du corps fini $\mathbf{F}_q$ (on sous-entend en général qu'un corps algébriquement clos de caractéristique p a été choisi).

4.2. Automorphismes des corps finis

On va utiliser le résultat classique suivant.

Proposition 4.2.1. — *Soit k un corps. Tout sous-groupe fini de k^* est cyclique.*

Démonstration. — Soit $\mathrm{G}\subset k^*$ un sous-groupe fini d'ordre $n=|\mathrm{G}|$. Alors, d'après le théorème de Lagrange, on a $x^n=1$ pour tout $x\in\mathrm{G}$. Donc X^n-1 est scindé dans $k[\mathrm{X}]$ à racines distinctes, ses racines étant exactement les n éléments de G. Maintenant pour d un entier qui divise n, X^d-1 divise le polynôme X^n-1. Donc X^d-1 est scindé à racines distinctes. Par exemple, soit p un nombre premier qui divise n et $r\geq 1$ maximal tel que $d=p^r$ divise n. Alors X^d-1 a d racines distinctes dans k. Les racines d'ordre différent de d sont des racines de $\mathrm{X}^{p^{r-1}}-1$, donc il y en a au plus p^{r-1}. Comme $p^r>p^{r-1}$, il y a au moins un $x\in k$ racine de X^d-1 qui n'est pas racine de $\mathrm{X}^{p^{r-1}}-1$, et donc x est d'ordre p^r. Maintenant soient $x_1,\cdots,x_{\mathrm{N}}$ obtenus ainsi pour chaque nombre premier qui divise n. Soit $y=x_1\cdots x_{\mathrm{N}}$. Comme G est commutatif et que pour $i\neq j$ l'ordre de x_i est premier

avec celui de x_j, l'ordre de y est le produit des ordres de x_1, ..., x_n, c'est-à-dire n. Donc G est cyclique. □

Par exemple, pour p un nombre premier, $(\mathbf{Z}/p\mathbf{Z})^*$ est un groupe cyclique d'ordre $p-1$.

Remarque 4.2.2. — *Si on connaît la structure des groupes abéliens finis, ce résultat est évident. En effet, on sait alors que k^* est isomorphe à un produit*

$$\Pi = \prod_{i=1}^{d} \mathbf{Z}/n_i\mathbf{Z}$$

avec $1 < n_1 | \cdots | n_d$ (attention, la loi sur k^* est multiplicative, alors qu'à droite la loi est additive de neutre 0). Or, dans un corps, le nombre de solutions de $\mathrm{X}^{n_1} = 1$ est au plus n_1. Dans Π, elles correspondent aux solutions de l'équation $n_1\pi = 0$. Si $d > 1$, il y en a au moins $2n_1$, à savoir les éléments de $\mathbf{Z}/n_1\mathbf{Z}$ et ceux de $n_2/n_1\mathbf{Z}/n_2\mathbf{Z} \xrightarrow{\sim} \mathbf{Z}/n_1\mathbf{Z}$, une contradiction.

Soit $q = p^n$ la puissance d'un nombre premier et m un entier > 0. On note

$$\mathrm{F}_q : \mathbf{F}_{q^m} \to \mathbf{F}_{q^m}$$

l'itéré F^n du morphisme de Frobenius : $\mathrm{F}_q(x) = x^q$ pour $x \in \mathbf{F}_{q^n}$. C'est un morphisme de corps, qui vaut l'identité sur $\mathbf{F}_q$ (ensemble des racines de $\mathrm{X}^q - \mathrm{X}$).

Théorème 4.2.3. — *Le groupe $\mathrm{Aut}_{\mathbf{F}_q}(\mathbf{F}_{q^m})$ est cyclique d'ordre m engendré par F_q.*

Démonstration. — Soit x un générateur du groupe cyclique $\mathbf{F}_{q^m}^*$. Comme $[\mathbf{F}_{q^m} : \mathbf{F}_q] = [\mathbf{F}_q[x] : \mathbf{F}_q] = m$, le polynôme minimal P de x sur $\mathbf{F}_q$ est degré m. Un morphisme $\sigma \in \mathrm{G} = \mathrm{Aut}_{\mathbf{F}_q}(\mathbf{F}_{q^m})$ laisse invariant P de sorte que $\sigma(x)$ est une racine de P, qui en a au plus m dans k. Comme x engendre $\mathbf{F}_{q^m}^*$, le morphisme σ est déterminé par $\sigma(x)$ de sorte que $\mathrm{card}(\mathrm{G}) \leq m$. Par ailleurs, F_q est d'ordre m. Sinon, il existerait $0 < d < m$ tel que $\mathrm{F}^d = \mathrm{Id}$, et donc $x^{q^d} = x$ contredisant que x d'ordre $q^m - 1$. Or, F_q est bien automorphisme, puisque c'est une application injective (comme tout morphisme de corps) entre ensembles finis de même cardinal. □

Exercice 4.2.4 **(Difficile)**. — *Soit $\mathrm{M} \in \mathbf{GL}_n(\mathbf{F}_q)$, vu comme une bijection de $(\mathbf{F}_q)^n$. Quelle est sa signature [Distinguer le cas q pair ou impair]? Montrer que le polynôme minimal de F_q vu comme endomorphisme du $\mathbf{F}_q$-espace vectoriel $\mathbf{F}_{q^n}$ est $\mathrm{X}^n - 1$ [Prouver*

que des homomorphismes distincts d'un groupe G *dans le groupe multiplicatif* k^* *d'un corps* k *sont linéairement indépendants, vus comme fonctions de* G *dans* k*]. Quelle est sa signature ?*

Exercice 4.2.5. — *Montrer qu'il existe des polynômes irréductibles sur* $\mathbf{F}_q$ *de tout degré non nul. Montrer qu'un tel polynôme* P *divise* $\mathrm{X}^{q^n} - \mathrm{X}$*. Montrer que le corps de rupture de* P *est son corps de décomposition.*

4.3. Une application du lemme chinois : l'algorithme de Berlekamp

Nous allons donner un algorithme, que l'on peut utiliser avec un ordinateur, permettant de factoriser un polynôme $\mathrm{P} \in \mathbf{F}_p[\mathrm{X}]$ en facteurs irréductibles, ou au moins de déterminer s'il est irréductible ou pas.

On se donne donc p premier et $\mathrm{P} \in \mathbf{F}_p[\mathrm{X}]$ non constant, unitaire. Rappelons (petit théorème de Fermat ou théorème de Lagrange) que si p ne divise pas $n \in \mathbf{Z}$, on a la congruence $n^{p-1} \equiv 1 \mod p$. On déduit l'égalité

$$x^p = x \text{ pour tout } x \in \mathbf{F}_p.$$

FIGURE 1. Pierre de Fermat

4.3.1. Où l'on se ramène à P **sans facteur carré.** — Si P est divisible par un carré Q^2 de degré > 0, le degré de $\mathrm{S} = \mathrm{PGCD}(\mathrm{P}, \mathrm{P}')$ est au moins $\deg(\mathrm{Q})$ et donc est strictement positif.

Si $\deg(S) = \deg(P)$, alors P' est nul puisque $S|P'$, autrement dit P s'écrit $\sum_i a_{ip}^p X^{ip} = R$ avec $R = (\sum_i a_{ip} X^i)^p \in \mathbf{F}_p[X]$, (cf. la preuve de 4.5.3 *infra*). On applique à nouveau l'algorithme à R.
Sinon, $S = \mathrm{PGCD}(P, P')$ est un diviseur non trivial de P et on applique l'algorithme à S et P/S qui sont de degré plus petits.

On peut supposer, ce qu'on fait désormais, que P **est sans facteur carré.**

4.3.2. Points fixes du morphisme de Frobenius. — Écrivons

$$P = \prod_{i=1}^{m} P_i$$

avec $n_i > 0$ et P_i unitaires irréductibles deux à deux distincts. Comme P_i et P_j sont premiers entre eux pour $i \neq j$, la somme des idéaux qu'ils engendrent est tout $\mathbf{F}_p[X]$. Le lemme chinois (2.8.1) assure que le morphisme de $\mathbf{F}_p$-algèbres canonique

$$\gamma : \ A = \mathbf{F}_p[X]/(P) \to \oplus_i \mathbf{F}_p[X]/(P_i)$$

est un isomorphisme d'algèbres.
Soit F le morphisme de Frobenius de A (on note de même celui de $A_i = \mathbf{F}_p[X]/(P_i)$). Comme $\mathbf{F}_p[X]$ est principal et P_i irréductible, chaque A_i est un corps fini (2.6.6) de sorte qu'on a $A_i^F = \mathrm{Ker}(F - Id_{A_i}) = \mathbf{F}_p$ (4.1.4). La formule

$$\gamma(a^p) = \gamma(a)^p = (a_i^p \mod P_i)$$

assure que l'image de $A^F = \mathrm{Ker}(F - \mathrm{Id}_A)$ par γ est égale à $\mathbf{F}_p^m = \oplus_i \mathbf{F}_p$. En particulier, on a

$$\dim_{\mathbf{F}_p} A^F = m.$$

Ainsi, P est irréductible si et seulement si $A^F = \mathbf{F}_p$. Notons que le calcul de cette dimension est parfaitement **algorithmique** : on calcule la matrice de F dans la base des classes des $X^i, i = 0, \cdots, d-1$ (ce qui se fait en divisant X^{ip} par P) puis on calcule le rang de $F - \mathrm{Id}$ par pivot de Gauss.
On a donc un critère algorithmique pour déterminer si P est irréductible, qu'on peut résumer de la façon suivante : P **sans facteur carré est irréductible si et seulement si la matrice de** $F - \mathrm{Id}$ **est de rang** $\deg(P) - 1$, rang qu'on calcule avec le pivot de Gauss par exemple.

4.3.3. Factorisation de P. — Allons plus loin, dans de le cas $\dim \mathrm{A}^{\mathrm{F}} > 1$. Dans ce cas, il existe $a \in \mathrm{A}$ qui n'est pas dans notre droite vectorielle $\mathbf{F}_p \subset \mathbf{F}_p[\mathrm{X}]$ des polynômes constants. Autrement dit, il existe Q de degré $0 < \deg(\mathrm{Q}) < \deg(\mathrm{P})$ tel que $\bar{\mathrm{Q}} \in \mathrm{A}^{\mathrm{F}}$, *ie* $\mathrm{P}|\mathrm{F}(\mathrm{Q}) - \mathrm{Q} = \mathrm{Q}^p - \mathrm{Q}$. De la factorisation

$$\mathrm{X}^p - \mathrm{X} = \prod_{i \in \mathbf{F}_p} (\mathrm{X} - i),$$

on tire

$$\mathrm{Q}^p - \mathrm{Q} = \prod_{i \in \mathbf{F}_p} (\mathrm{Q} - i)$$

et donc

$$\mathrm{P}| \prod_{i \in \mathbf{F}_p} (\mathrm{Q} - i).$$

Notons que si $i \neq j$ dans $\mathbf{F}_p$, l'identité

$$1/(j-i)((\mathrm{Q} - i) - (\mathrm{Q} - j)) = 1$$

assure $\mathrm{PGCD}(\mathrm{Q} - i, \mathrm{Q} - j) = 1$.

Ainsi, chaque facteur P_j de P divise **exactement un** des facteurs $\mathrm{Q} - i$ de sorte que

$$\mathrm{P} = \prod_{i \in \mathbf{F}_p} \mathrm{PGCD}((\mathrm{Q} - i), \mathrm{P}).$$

Maintenant, chaque polynôme $\mathrm{PGCD}((\mathrm{Q} - i), \mathrm{P})$ (qui se calcule grâce à l'algorithme de Bézout) est de degré strictement inférieur à $\deg(\mathrm{P})$ par construction et on recommence le processus pour chaque polynôme $\mathrm{PGCD}((\mathrm{Q} - i), \mathrm{P})$. Ce processus s'arrête en un nombre fini d'étapes.

Ce processus est algorithmique, mais pas très efficace. En effet, imaginons par exemple que P soit de degré 1000 et p de l'ordre de 10^6. La probabilité que $\mathrm{PGCD}((\mathrm{Q} - i), \mathrm{P})$ soit différent de 1 est de l'ordre de $1/1000$ et on voit donc que ce produit à 10^6 termes a très peu de facteurs non triviaux. En fait, dans la pratique, on adapte cet algorithme qui devient probabiliste.

Un exercice est de programmer cet algorithme avec un logiciel de calcul formel. Un autre exercice est d'évaluer le nombre d'opérations nécessaire : en effet, comme le nombre de polynômes de degré donné dans $\mathbf{F}_p[\mathrm{X}]$ est fini, on aurait pu effectuer tous les produits de deux polynômes et comparer avec P, ce qui donne un algorithme de factorisation.

Mais, dès que le degré est grand, le nombre d'opérations est énorme et fait exploser n'importe quelle machine. En revanche, pour les petits p, d, il est efficace. Quoi qu'il en soit, l'algorithme de Berlekamp, relativement efficace en général, est théoriquement intéressant.

Remarque 4.3.1. — *Le lecteur généralisera l'algorithme en remplaçant* $\mathbf{F}_p$ *par* $\mathbf{F}_{p^n}$ *simplement en remplaçant* F *par le composé* $\mathrm{F}_{p^n} = \mathrm{F}^n$.

4.4. Extensions de corps parfaits

On a vu dans la preuve de 4.2.3 que le morphisme de Frobenius d'un corps fini $k = \mathbf{F}_q$ ($q = p^n$) est surjectif, autrement dit, tout élément de $\mathbf{F}_q$ est une puissance p-ième. Ce n'est cependant pas le cas pour tous les corps de caractéristique positive. Par exemple, soit $k = \mathrm{Frac}(\mathbf{F}_p[t])$ le corps des fractions de $\mathbf{F}_p[t]$. Alors, pour des raisons claires de degré, l'élément t n'est pas une puissance p-ième.

Définition 4.4.1. — *On dit qu'un corps k est parfait si sa caractéristique est nulle ou s'il est de caractéristique $p > 0$ et son morphisme de Frobenius est surjectif.*

Remarquons que le morphisme de Frobenius étant toujours injectif, la condition en caractéristique $p > 0$ revient à dire que le morphisme de Frobenius est un isomorphisme.
On a l'exemple fondamental suivant :

Lemme 4.4.2. — *Un corps algébriquement clos est parfait.*

Démonstration. — Soit Ω un tel corps. Si sa caractéristique est nulle, c'est clair. Sinon, sa caractéristique est $p > 0$. Mais alors pour tout $x \in \Omega$, le polynôme $\mathrm{X}^p - x$ a au moins une racine dans Ω, donc x est une racine p-ième. Donc Ω est parfait. □

Il n'est pas vrai qu'un sous-corps d'un corps parfait est parfait. En effet la clôture algébrique d'un corps non parfait (par exemple $\mathrm{Frac}(\mathbf{F}_p[t])$) est un corps parfait contenant un sous-corps qui ne l'est pas. Il n'est pas vrai non plus qu'une extension d'un corps parfait est parfaite. Par exemple le corps parfait $\mathbf{F}_p$ admet pour extension $\mathrm{Frac}(\mathbf{F}_p[t])$ qui n'est pas un corps parfait. En revanche, on a l'énoncé important suivant.

Proposition 4.4.3. — *Soit* K/k *une extension finie. Alors si k est parfait,* K *l'est aussi.*

Démonstration. — La question ne pose problème qu'en caractéristique $p > 0$. Soit F le morphisme de Frobenius de K, qui est bijectif sur k par hypothèse (k est parfait). On a donc un inverse $\mathrm{F}^{-1} : k \to k$. Alors, F(K) est visiblement un $\mathrm{F}(k)$-sous-espace vectoriel de K, donc un k-sous-espace vectoriel, puisque $\mathrm{F}(k) = k$. De même, si les $x_i \in \mathrm{K}$ sont libres sur k, les $\mathrm{F}(x_i)$ sont libres sur k dans F(K). En effet, si $\sum a_i \mathrm{F}(x_i) = 0$ avec les $a_i \in k$, alors $\mathrm{F}(\sum \mathrm{F}^{-1}(a_i)x_i) = 0$ et donc $\sum \mathrm{F}^{-1}(a_i)x_i = 0$. La famille des x_i étant libre, ceci entraîne $\mathrm{F}^{-1}(a_i) = 0$ pour tout i, et donc $a_i = 0$. On déduit, en prenant une base, l'inégalité $[\mathrm{K} : k] \leq [\mathrm{F}(\mathrm{K}) : k]$, puis l'inégalité inverse car $\mathrm{F}(\mathrm{K}) \subset \mathrm{K}$. Donc $\mathrm{K} = \mathrm{F}(\mathrm{K})$. □

La réciproque est vraie (même si moins utile). Pour la démontrer, commençons par un lemme. Soit k un sous-corps d'un corps Ω algébriquement clos de caractéristique $p > 0$. Comme le morphisme de Frobenius de Ω est bijectif (Ω est parfait), la racine p-ième $x^{1/p} = \mathrm{F}^{-1}(x)$ de tout élément de Ω est bien définie. C'est vrai de la même manière pour les racines p^n-ièmes.

Lemme 4.4.4. — *Soit $t \in k$ qui n'a pas de racine p-ième dans k. Alors, pour tout $n \geq 1$, le polynôme $\mathrm{X}^{p^n} - t$ est irréductible dans $k[\mathrm{X}]$.*

Autrement dit, on a $\deg_k(t^{1/p^n}) = p^n$.

Démonstration. — Soit τ racine p^n-ième de t. On sait que $\tau \notin k$ puisque par hypothèse $t^{1/p} = \tau^{p^{n-1}} \notin k$. Soit P le polynôme minimal de τ sur k : c'est un polynôme irréductible (3.6.4) de $k[\mathrm{X}]$ qui divise $\mathrm{Q} = \mathrm{X}^{p^n} - t$ puisque $\mathrm{Q}(\tau) = 0$. En utilisant une décomposition de Q en facteurs irréductibles dans $k[\mathrm{X}]$, on peut écrire :

$$\mathrm{Q} = \mathrm{P}^m \mathrm{R} \text{ avec } \mathrm{R} \in k[\mathrm{X}] \text{ et } \mathrm{PGCD}(\mathrm{P}, \mathrm{R}) = 1.$$

L'identité de Bézout s'écrit $\mathrm{PA} + \mathrm{RB} = 1$ avec $\mathrm{A}, \mathrm{B} \in k[\mathrm{X}]$. En conséquence, P et R n'ont pas de racine commune dans Ω. Or, dans $\Omega[\mathrm{X}]$, on a $\mathrm{Q}(\mathrm{X}) = (\mathrm{X} - \tau)^{p^n}$ de sorte que R n'a pas de racine du tout et donc $\mathrm{Q} = \mathrm{P}^m$. En comparant les degrés, on obtient $m = p^\nu, 0 \leq \nu \leq n$. En évaluant en 0, on a alors

$$\mathrm{Q}(0) = -t = (\mathrm{P}(0))^{p^\nu}.$$

Comme t n'est pas une puissance p-ième dans k, on a donc $\nu = 0$. Ainsi $\mathrm{Q} = \mathrm{P}$ est irréductible. □

On obtient alors la réciproque de 4.4.3.

Corollaire 4.4.5. — *Soit* K/k *une extension finie. Si* K *est parfait, alors* k *est parfait.*

Démonstration. — En effet, si $t \in k$ n'est pas une puissance p-ième, $t^{p^{-n}} \in \mathrm{K}$ est de degré p^n sur k qui tend vers l'infini avec n. Contradiction, car K/k étant une extension finie, le degré des éléments de K sur k est majoré par $[\mathrm{K} : k]$. □

4.5. Polynômes séparables et corps parfaits

L'intérêt des corps parfaits vient du théorème 4.5.3 fondamental suivant. Soit k un corps et Ω un corps algébriquement clos le contenant.

Définition 4.5.1. — *Un polynôme unitaire est dit séparable si ses racines dans* Ω *sont simples.*

Rappelons le lemme bien connu.

Lemme 4.5.2. — *Un polynôme est séparable si et seulement si il est premier avec sa dérivée.*

Démonstration. — Supposons P séparable. Écrivons

$$\mathrm{P} = a\prod_{i\in \mathrm{I}}(\mathrm{X} - z_i), a \in k^*, z_i \in \Omega$$

où les z_i sont distincts deux à deux. On déduit donc

$$\mathrm{PGCD}(\mathrm{P}, \mathrm{P}') = \prod_{i\in \mathrm{I}'}(\mathrm{X} - z_i) \text{ où } \mathrm{I}' \subset \mathrm{I}.$$

Supposons $\mathrm{I}' \neq \varnothing$ et choisissons $i' \in \mathrm{I}'$. On a donc $\mathrm{P}(z_{i'}) = 0$. Or,

$$\mathrm{P}' = a\sum_{i\in \mathrm{I}}\prod_{j\neq i}(\mathrm{X} - z_j)$$

de sorte que

$$\prod_{j\neq i'}(z_{i'} - z_j) = 0$$

ce qui est absurde car les z_i sont distincts deux à deux.

Inversement, si P, P' sont premiers entre eux, l'identité de Bézout $\mathrm{AP} + \mathrm{BP}' = 1$ avec A, B polynômes assure que P, P' n'ont pas de racines communes dans Ω et donc que les racines de P dans Ω sont simples. □

Théorème 4.5.3. — *Un corps k est parfait si et seulement tout polynôme irréductible de $k[\mathrm{X}]$ est séparable.*

Démonstration. — Supposons k parfait et soit P un polynôme irréductible de $k[\mathrm{X}]$ (en particulier non constant). Montrons que P est premier avec P′. Comme P est irréductible, le PGCD de P et P′ est 1 ou P. Montrons par l'absurde que c'est 1. Si c'est P, pour des raisons de degré, c'est que P′ est le polynôme nul. Ceci impose déjà que la caractéristique de k est $p > 0$. En écrivant

$$\mathrm{P} = \sum a_n \mathrm{X}^n \text{ et } \mathrm{P}' = \sum n a_n \mathrm{X}^{n-1}$$

on en déduit que $na_n = 0$ pour tout n et donc $a_n = 0$ si p ne divise pas n. Ainsi, on a

$$\mathrm{P} = \sum_n a_{np} \mathrm{X}^{np}.$$

Comme k est parfait, le morphisme de Frobenius F est bijectif et on a donc

$$\mathrm{P} = \sum_n \mathrm{F}^{-1}(a_{np}^p)\mathrm{X}^{np} = (\sum_n \mathrm{F}^{-1}(a_{np})\mathrm{X}^n)^p$$

puisque $pk[\mathrm{X}] = 0$. Ceci est absurde car P est irréductible.

Inversement, supposons que tout polynôme irréductible de $k[\mathrm{X}]$ est séparable. On peut supposer k de caractéristique $p > 0$ et montrons que tout élément t a une racine p-ième. En effet, dans le cas contraire, soit $t \in k$ qui n'en a pas. Soit alors $t^{1/p}$ une racine p-ième de t dans Ω et P son polynôme minimal k. Alors P est irréductible (3.6.4), il divise $\mathrm{X}^p - t$ et $\deg(\mathrm{P}) > 1$ car par hypothèse $t^{1/p} \notin k$ (notons que d'après la section précédente, $\mathrm{X}^p - t$ est irréductible dans $k[\mathrm{X}]$). Dans $\Omega[\mathrm{X}]$, $\mathrm{X}^p - t$ s'écrit $(\mathrm{X} - t^{1/p})^p$ et donc n'a qu'une seule racine (de multiplicité p). Ainsi $\mathrm{P} = (\mathrm{X} - t^{1/p})^i$ avec $2 \leq i \leq p$. On en déduit que P n'est pas séparable, contradiction. □

4.6. Le théorème de l'élément primitif

Soit k un corps parfait.

Définition 4.6.1. — *On dit qu'une extension de corps K/k est monogène si elle peut-être engendrée par un seul élément, c'est-à-dire si il existe $x \in \mathrm{K}$ tel que $\mathrm{K} = k[x]$. Un tel générateur x de l'extension est appelé un élément primitif.*

On a alors le théorème fondamental suivant.

***Théorème 4.6.2* (Élément primitif).** — *Toute extension finie* K/k *est monogène.*

Démonstration. — Si k est fini, K l'est aussi et K^* est cyclique (4.2.1), engendré par x disons. On a alors $\mathrm{K} = k[x]$. Supposons donc k infini. Par récurrence, on se ramène immédiatement à prouver que si x, y sont des éléments de K, il existe $z \in \mathrm{K}$ tel que

$$k[z] = k[x, y].$$

On cherche z sous la forme $z = x + ty, t \in k^*$. Posons $\mathrm{L} = k[z]$. Il suffit de prouver $x \in \mathrm{L}$, car alors $y = (z - x)/t \in \mathrm{L}$. Soient $\mathrm{P}_x, \mathrm{P}_y \in k[\mathrm{X}]$ les polynômes minimaux de x, y sur k. Le polynôme

$$\mathrm{Q}(\mathrm{X}) = \mathrm{P}_y((z - \mathrm{X})/t)$$

est à coefficients dans L et annule x par construction. Soit

$$\mathrm{R} = \mathrm{PGCD}(\mathrm{Q}, \mathrm{P}_x) \in \mathrm{L}[\mathrm{X}].$$

Comme nous l'avons rappelé, l'algorithme d'Euclide prouve que le calcul de PGCD des polynômes est invariant par changement de corps. On peut ainsi faire par exemple ce calcul dans Ω. Comme P_x est à racines simples, on a

$$\mathrm{R}(\mathrm{X}) = \prod_{\substack{x' \text{ tels que} \\ \mathrm{Q}(x')=\mathrm{P}_x(x')=0}} (\mathrm{X} - x').$$

Si on écrit $\mathrm{P}_y = \prod(\mathrm{X} - y')$, les racines de Q s'écrivent

$$z - ty' = x + t(y - y').$$

Choisissons $t \neq 0$ en dehors du nombre fini de t tels qu'il existe $y' \neq y$ et x' vérifiant

$$x' = x + t(y - y') \ \textit{ie}\ t = \frac{x' - x}{y - y'}.$$

Alors l'ensemble

$$\{x' | \mathrm{Q}(x') = \mathrm{P}_x(x') = 0\}$$

est réduit à x.

On en déduit qu'un tel t étant choisi on a $\mathrm{R}(\mathrm{X}) = \mathrm{X} - x$. Comme $\mathrm{R} \in \mathrm{L}[\mathrm{X}]$, on a $x \in \mathrm{L}$. □

Par exemple, considérons l'extension $\mathrm{K} = \mathbf{Q}(\sqrt{2}, \sqrt{3})$ de $\mathbf{Q}$. Montrons que $\sqrt{2} + \sqrt{3}$ est primitif alors que $\sqrt{2}, \sqrt{3}$ ne le sont pas.
Comme $\sqrt{(2)}, \sqrt{3} \notin \mathbf{Q}$, on a $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = [\mathbf{Q}(\sqrt{3}) : \mathbf{Q}] = 2$ et donc $[\mathrm{K} : \mathbf{Q}] = 2$ ou 4. Si le degré est 2, c'est que $\mathrm{K} = \mathbf{Q}(\sqrt{2})$. Alors $\sqrt{3} = a\sqrt{2} + b$ avec $a, b \in \mathbf{Q}$, ce qui implique $3 - 2a^2 - b^2 = 2ab\sqrt{2}$. Donc $a = 0$ ou $b = 0$ et comme $\sqrt{3} \notin \mathbf{Q}$, $b = 0$. Donc $\sqrt{3/2} \in \mathbf{Q}$, contradiction. Donc $[\mathrm{K} : \mathbf{Q}] = 4$ et $\sqrt{2}, \sqrt{3}$ ne sont pas primitifs. Par contre $x = \sqrt{2} + \sqrt{3}$ est primitif. En effet, soit $\mathrm{L} = \mathbf{Q}[x] \subset \mathrm{K}$. Alors $x^{-1} = \sqrt{3} - \sqrt{2} \in \mathrm{L}$. On en déduit $\sqrt{3}, \sqrt{2} \in \mathrm{L}$ et donc $\mathrm{L} = \mathrm{K}$.
Voici un autre exemple important.

Lemme 4.6.3. — *Pour $n \geq 1$ entier, on note $\zeta_n = \exp(\frac{2i\pi}{n})$. Alors pour $n, m \geq 1$ entiers, on a $\mathbf{Q}(\zeta_n, \zeta_m) = \mathbf{Q}(\zeta_{\mathrm{PPCM}(n,m)})$.*

Démonstration. — Soit $\varpi = \mathrm{PPCM}(n, m)$. Comme $\zeta_\varpi^{\varpi/n} = \zeta_n$, on a $\zeta_n \in \mathbf{Q}(\zeta_\varpi)$ et donc $\mathbf{Q}(\zeta_n, \zeta_m) \subset \mathbf{Q}(\zeta_\varpi)$. Inversement, $\varpi/n, \varpi/m$ sont premiers entre eux de sorte que d'après l'identité de Bézout, il existe des entiers u, v avec

$$u\varpi/n + v\varpi/m = 1.$$

En multipliant par $2i\pi/\varpi$ et en prenant l'exponentielle, on trouve $\zeta_\varpi = \zeta_n^u \zeta_m^v$, prouvant l'inclusion inverse. □

En général, un élément "pris au hasard" d'une extension finie est primitif (le lecteur pourra essayer de donner un sens précis à cette assertion).

Exercice 4.6.4. — *Si k n'est pas supposé parfait, le théorème de l'élément primitif peut tomber en défaut. Par exemple, soit $\mathrm{L} = \mathbf{F}_p(\mathrm{X}, \mathrm{Y})$ le corps des fractions de l'anneau de polynômes $\mathbf{F}_p[\mathrm{X}, \mathrm{Y}]$. Montrer que l'extension $\mathrm{L}(\mathrm{X}^{1/p}, \mathrm{Y}^{1/p})$ est finie, mais n'est pas monogène.*

On obtient la généralisation fondamentale suivante de 3.6.6.

Corollaire 4.6.5. — *Soit K une extension finie de k. Alors, on a $\mathrm{card}\,(\mathrm{Hom}_k(\mathrm{K}, \Omega)) = [\mathrm{K} : k]$.*

Démonstration. — On écrit $\mathrm{K} = k[x]$ pour x primitif et on invoque 3.6.6. □

Remarque 4.6.6. — *Si k n'est pas parfait, l'égalité est fausse en général : elle n'est vraie que pour les extensions dites "séparables" de la théorie de Galois générale. Lorsque que k est parfait, toutes les extensions algébriques sont séparables de sorte que nous ne serons pas ennuyés par cette complication.*

CHAPITRE 5

LA CORRESPONDANCE DE GALOIS

Nous démontrons dans ce chapitre le théorème principal de la correspondance de Galois.

On fixe un corps *parfait* k et un corps Ω algébriquement clos le contenant.
On a en tête l'exemple $\mathbf{Q} \subset \mathbf{C}$, mais aussi $\mathbf{F}_q \subset \bar{\mathbf{F}}_p$. On se rappellera que tout polynôme irréductible P de k[X] est séparable (et donc a deg(P) racines distinctes dans Ω) et que toute extension finie de k est parfaite (4.4.3).
Si $x \in \Omega$ est algébrique sur k, on dira simplement "conjugués de x" pour "k-conjugués de x dans Ω", c'est-à-dire que les conjugués de x sont par définition les racines dans Ω du polynôme minimal P de x sur k (3.6.6). Comme P est irréductible, ses racines sont simples. Mais on sait également que l'application $\sigma \mapsto \sigma(x)$ identifie $\mathrm{Hom}_k(k[x], \Omega)$ et l'ensemble des conjugués de x. On a donc la formule clef

Lemme 5.0.1. — *Le polynôme minimal* P *d'un élément $x \in \Omega$ algébrique sur k vaut*

$$\mathrm{P(X)} = \prod_{\sigma \in \mathrm{Hom}_k(k[x],\Omega)} (\mathrm{X} - \sigma(x)).$$

On s'intéresse aux extensions algébriques K/k, et en fait aux extensions finies. D'après le théorème de prolongement des morphismes (3.9.1), on sait que K se plonge comme k-algèbre dans Ω, de sorte qu'il suffit de considérer les extensions algébriques de k contenues dans Ω.

5.1. Extensions galoisiennes

Définition 5.1.1. — *L'extension* K/k *est dite galoisienne si elle est algébrique et si les conjugués d'un élément arbitraire de* K *sont dans* K.

Lemme 5.1.2. — *Soit* K/k *une extension algébrique de la forme* $\mathrm{K} = k[x_1, \cdots, x_n]$ *avec les* $x_i \in \mathrm{K}$. *Alors* K/k *est galoisienne si et seulement si les conjugués de tous les* x_i *sur* k *sont dans* K.

Autrement dit, il suffit de vérifier que les conjugués sont dans K pour une famille qui engendre l'extension.

Démonstration. — L'implication "seulement si" étant évidente, montrons l'autre. Soit $x \in \mathrm{K}$. Alors les conjugués de x sur k sont de la forme $\sigma(x)$ avec $\sigma \in \mathrm{Hom}_k(\mathrm{K}, \Omega)$ où Ω est un clôture algébrique de K. Mais x est de la forme $x = \mathrm{P}(x_1, \cdots, x_n)$ avec $\mathrm{P} \in k[\mathrm{X}_1, \cdots, \mathrm{X}_n]$ un polynôme à n variables. On a alors $\sigma(x) = \mathrm{P}(\sigma(x_1), \cdots, \sigma(x_n))$. Mais par hypothèse les $\sigma(x_i) \in \mathrm{K}$, et donc $\sigma(x) \in \mathrm{K}$. □

Par exemple, soit $k = \mathbf{Q}$ et $\mathrm{K} = \mathbf{Q}[2^{1/3}, j]$. Comme $\mathrm{X}^2 + \mathrm{X} + 1$ (resp. $\mathrm{X}^3 - 2$) annule j (resp. $2^{1/3}$), les conjugués de j sont dans $\{j, j^2\}$ (resp. $\{2^{1/3}, j2^{1/3}, j^2 2^{1/3}\}$). Comme ces ensembles sont inclus dans K, le résultat précédent implique que K/k est galoisienne.
On a la proposition facile mais importante suivante.

Proposition 5.1.3. — *Soit* E/k *une sous-extension de* K/k *galoisienne et supposons* E *parfait*[1]. *Alors,* K/E *est galoisienne.*

Démonstration. — En effet, le polynôme minimal de $x \in \mathrm{K}$ sur k est a fortiori à coefficients dans E donc x est aussi algébrique sur E. Son polynôme minimal sur k divisible par le polynôme minimal de x sur E. Donc, tous les E-conjugués de x sont aussi des k-conjugués, donc sont dans K par hypothèse. □

En général cependant, avec les mêmes hypothèses, E/k n'est pas forcément galoisienne (on verra plus bas (5.5.1) une condition nécessaire et suffisante assurant que E/k est galoisienne).
Par exemple, posons $k = \mathbf{Q}$, $\mathrm{K} = \mathbf{Q}[2^{1/3}, j]$ et $\mathrm{E} = \mathbf{Q}[2^{1/3}]$. On a vu que K/k est galoisienne et, d'après le résultat précédent, K/E est galoisienne. Vérifions cependant que

1. Cette condition est automatique dès lors que E est finie sur k (4.4.3). Elle n'est ici que parce qu'on a défini la notion d'extension galoisienne que dans le cas où le corps est parfait. Elle disparaît dans le cadre général de la théorie de Galois.

E/k n'est pas galoisienne. En effet, le polynôme minimal de $2^{1/3}$ sur k est $\mathrm{X}^3 - 2$ (ce polynôme de degré 3 est irréductible sur $\mathbf{Q}$, car on peut montrer immédiatement qu'il n'a pas de racine dasn $\mathbf{Q}$). Donc les conjugués de $2^{1/3}$ sur $\mathbf{Q}$ sont $2^{1/3}$, $2^{1/3}j$ et $2^{1/3}j^2$. Or $2^{1/3}j \notin \mathrm{E}$ car $\mathrm{E} \subset \mathbf{R}$.
Rappelons (3.9.5) que les conjugués de $x \in \mathrm{K}$ sont aussi les $\sigma(x)$ avec $\sigma \in \mathrm{Hom}_k(\mathrm{K}, \Omega)$. Notons $j : \mathrm{K} \hookrightarrow \Omega$ l'inclusion de K dans Ω. On a une application injective canonique

$$j^* : \mathrm{Aut}_k(\mathrm{K}) \hookrightarrow \mathrm{Hom}_k(\mathrm{K}, \Omega)$$

qui à un automorphisme $\bar{\sigma} \in \mathrm{Aut}_k(\mathrm{K}, \Omega)$ associe

$$\sigma = j \circ \bar{\sigma} : \mathrm{K} \xrightarrow{\sigma} \mathrm{K} \xhookrightarrow{j} \Omega$$

qui permet d'identifier σ et $\bar{\sigma}$ (et donc $\mathrm{Aut}_k(\mathrm{K})$ à un sous-ensemble de $\mathrm{Hom}_k(\mathrm{K}, \Omega)$).

Lemme 5.1.4. — *Soit* K/k *une extension algébrique et* $\sigma \in \mathrm{Hom}_k(\mathrm{K}, \Omega)$. *Alors,* $\sigma \in \mathrm{Aut}_k(\mathrm{K})$, *ie* $\sigma(\mathrm{K}) = \mathrm{K}$, *si et seulement si* σ *laisse* K *globalement invariant, ie* $\sigma(\mathrm{K}) \subset \mathrm{K}$.

Démonstration. — En effet, supposons $\sigma(\mathrm{K}) \subset \mathrm{K}$. Soient $x_1, \cdots, x_n$ les n conjugués de $x_1 \in \mathrm{K}$, qui sont dans K par hypothèse. Alors, σ laisse $\mathrm{X} = \{x_1, \cdots, x_n\}$ globalement invariant par hypothèse (puisque $\sigma(x_i)$ est un conjugué de x_i (3.9.5), donc de x_1 car x_i et x_1 ont même polynôme minimal). Étant injective comme restriction d'un morphisme de corps toujours injectif, elle induit une bijection de X (puisque X est fini) de sorte qu'il existe $x_i \in \mathrm{X}$ tel que $x_1 = \sigma(x_i)$. Comme $x_i \in \mathrm{K}$ par hypothèse, σ est surjective. □

On obtient alors le résultat important suivant.

Corollaire 5.1.5. — *L'inclusion* $\mathrm{Aut}_k(\mathrm{K}) \hookrightarrow \mathrm{Hom}_k(\mathrm{K}, \Omega)$ *est bijective si et seulement si* K/k *est galoisienne.*

Démonstration. — Supposons $\mathrm{Aut}_k(\mathrm{K}) = \mathrm{Hom}_k(\mathrm{K}, \Omega)$. D'après 3.9.5, tout conjugué de $x \in \mathrm{K}$ s'écrit $\sigma(x)$ pour $\sigma \in \mathrm{Hom}_k(\mathrm{K}, \Omega)$. Mais $\sigma \in \mathrm{Aut}_k(\mathrm{K})$ donc $\sigma(x) \in \mathrm{K}$ prouvant que K/k est galoisienne. Inversement, supposons K/k galoisienne. Soit $\sigma \in \mathrm{Hom}_k(\mathrm{K}, \Omega)$ et $x \in \mathrm{K}$. Alors, $\sigma(x)$ est un conjugué de x (3.9.5), donc est dans K. Comme x est arbitraire, on a $\sigma(\mathrm{K}) \subset \mathrm{K}$ et donc $\sigma \in \mathrm{Aut}_k(\mathrm{K})$ (5.1.4). □

Remarque 5.1.6. — *Cette caractérisation a l'avantage qu'elle ne dépend en fait que de* K/k *et non pas de* Ω *: en effet, les conjugués d'un élément algébrique vivent dans la clôture algébrique de* k *dans* Ω, *qui est unique à isomorphisme près.*

Définition 5.1.7. — *On appelle groupe de Galois d'une extension galoisienne* K/k *le groupe* $\mathrm{Gal}(\mathrm{K}/k) = \mathrm{Aut}_k(\mathrm{K}) \overset{5.1.5}{=} \mathrm{Hom}_k(\mathrm{K}, \Omega)$.

Remarque 5.1.8. — *Comme les conjugués de* $x \in \mathrm{K}$ *sont les* $\sigma(x), \sigma \in \mathrm{Hom}_k(\mathrm{K}, \Omega)$ *(3.9.5), si* K/k *est galoisienne de groupe de Galois* G, *les conjugués de* x *sont les* $g(x), g \in \mathrm{G}$.

On a l'exemple simple suivant.

Lemme 5.1.9. — *L'extension* $\mathbf{C}/\mathbf{R}$ *est galoisienne de groupe de galois* $\mathrm{Gal}(\mathbf{C}/\mathbf{R}) \simeq \mathbf{Z}/2\mathbf{Z}$ *engendré par la conjugaison complexe.*

Démonstration. — On a $\mathbf{C} = \mathbf{R}[i]$ et les conjugués de i étant i et $-i$, l'extension est galoisienne. Un élément de $\mathrm{G} = \mathrm{Gal}(\mathbf{C}/\mathbf{R})$ est uniquement déterminé par sa valeur en i, qui ne peut-être que i ou $-i$. Donc son ordre $|\mathrm{G}|$ est 1 ou 2. Or la conjugaison complexe est bien dans G et satisfait $\bar{i} = -i$, ce qui implique le résultat. □

Le point suivant est aisé, mais important.

Proposition 5.1.10. — *Soit* E/k *une sous-extension de l'extension* galoisienne K/k *avec* E *parfait. Alors,*

i) $\mathrm{Gal}(\mathrm{K}/\mathrm{E})$ *est un sous-groupe de* $\mathrm{Gal}(\mathrm{K}/k)$ *;*

ii) Si E/k *est* galoisienne, *la restriction des morphismes de* K *à* E *induit (5.1.5) un morphisme*

$$\mathrm{Gal}(\mathrm{K}/k) \to \mathrm{Gal}(\mathrm{E}/k)$$

qui est surjectif. Son noyau est $\mathrm{Gal}(\mathrm{K}/\mathrm{E})$. *Autrement dit, on a la suite exacte*

$$\{1\} \to \mathrm{Gal}(\mathrm{K}/\mathrm{E}) \to \mathrm{Gal}(\mathrm{K}/k) \to \mathrm{Gal}(\mathrm{E}/k) \to \{1\}.$$

Démonstration. — On sait (5.1.3) que K/E est galoisienne. Les éléments de $\mathrm{Gal}(\mathrm{K}/\mathrm{E})$ sont les automorphismes de K qui sont E-linéaires tandis que ceux de $\mathrm{Gal}(\mathrm{K}/k)$ sont les automorphismes de K qui sont k-linéaires. Comme E contient k, on déduit une inclusion évidente $\mathrm{Gal}(\mathrm{K}/\mathrm{E}) \to \mathrm{Gal}(\mathrm{K}/k)$ respectant la composition (et l'identité), d'où le premier point.

D'après 5.1.5, l'application de restriction

$$\mathrm{Hom}_k(\mathrm{K}, \Omega) \to \mathrm{Hom}_k(\mathrm{E}, \Omega)$$

s'identifie à une application

$$\mathrm{Gal}(\mathrm{K}/k) \to \mathrm{Gal}(\mathrm{E}/k)$$

dont on vérifie que c'est un morphisme. La surjectivité découle immédiatement du théorème de prolongement des homomorphismes (3.9.1). Les éléments du noyau sont par définition les automorphismes de K fixant E, donc les éléments de Gal(K/E). L'exactitude de la suite dans la proposition n'est que la reformulation de ce qui précède d'après la proposition 1.3.3. □

On précisera ceci dans la correspondance de Galois (5.5.1) pour le cas des extensions galoisiennes finies.

5.2. Caractérisations des extensions galoisiennes

Théorème 5.2.1. — *Soit* K/k *une extension finie. Alors* K/k *est galoisienne si et seulement si l'action de* $\mathrm{Aut}_k(\mathrm{K})$ *sur les conjugués de tout élément de* K *est transitive.*

Démonstration. — Supposons K/k galoisienne et soit $x \in \mathrm{K}$. D'après 3.9.5, un conjugué y de x s'écrit $\sigma(x)$ pour $\sigma \in \mathrm{Hom}_k(\mathrm{K}, \Omega)$; comme $\mathrm{Aut}_k(\mathrm{K}) = \mathrm{Hom}_k(\mathrm{K}, \Omega)$ (5.1.5), l'action de $\mathrm{Aut}_k(\mathrm{K})$sur les conjugués de x est bien transitive. Inversement, soit x primitif de K/k (4.6.2), donc de degré $[\mathrm{K} : k]$. Il a donc $\deg_k(x) = [\mathrm{K} : k]$ conjugués et donc (transitivité), $\mathrm{card}\,\mathrm{Aut}_k(\mathrm{K}) \geq [\mathrm{K} : k]$. On invoque alors à nouveau 5.1.5. □

La définition du corps des racines d'un polynôme a été donnée en (3.10).

Théorème 5.2.2. — *Les extensions galoisiennes finies de* k *sont exactement les corps des racines de polynômes.*

Démonstration. — Supposons K/k galoisienne. D'après le théorème de l'élément primitif (4.6.2), il existe x engendrant K. Soient x_i ses conjugués, à savoir les racines de son polynôme minimal P, qui, par hypothèse sont dans K. On a donc

$$\mathrm{K} = k[x] \subset k[x_i] \subset \mathrm{K}$$

et donc, $\mathrm{K} = k[x_i]$ est le corps des racines de P, ce qu'on voulait.
Inversement, si $\mathrm{K} = k[x_i]$ où les x_i sont les racines d'un polynôme P. Un homomorphisme $\sigma \in \mathrm{Hom}_k(\mathrm{K}, \Omega)$ permute les x_i puisque $\mathrm{P} = \mathrm{P}^\sigma$. On en déduit qu'il envoie $\mathrm{K} = k[x_i]$ sur lui même de sorte que $\sigma \in \mathrm{Aut}_k(\mathrm{K})$. On invoque alors 5.1.4. □

5.3. Groupe de Galois des corps finis

Soit q la puissance d'un nombre premier. Rappelons les résultats de 4.2, traduits dans ce nouveau vocabulaire :

Proposition 5.3.1. — *L'extension* $\mathbf{F}_{q^n}/\mathbf{F}_q$ *est galoisienne, de groupe de Galois cyclique d'ordre* n *engendré par*

$$\mathrm{F}_q : x \mapsto x^q.$$

Les sous-corps de $\mathbf{F}_{q^n}$ *contenant* $\mathbf{F}_q$ *sont les* $\mathbf{F}_{q^m}$ *avec* $m|n$.

En particulier, on constate que l'ensemble des sous-extensions de $\mathbf{F}_{q^n}/\mathbf{F}_q$, c'est-à-dire

$$\{\mathbf{F}_{q^m}/\mathbf{F}_q| \text{ avec } m|n\}$$

est en bijection avec l'ensemble des sous-groupe de $\mathrm{Gal}(\mathbf{F}_{q^n}/\mathbf{F}_q) \xrightarrow{\sim} \mathbf{Z}/n\mathbf{Z}$, c'est-à-dire

$$\{((n/m)\mathbf{Z}/n\mathbf{Z}) \simeq \mathbf{Z}/m\mathbf{Z}| \text{ avec } m|n\}.$$

Plus précisément, $\mathbf{F}_{q^m}$ est le corps des éléments de $\mathbf{F}_{q^n}$ fixés par $\mathrm{H} =< \mathrm{F}_q^{m/n} > \xrightarrow{\sim} \mathbf{Z}/m\mathbf{Z}$. Ce phénomène est général : c'est ce que nous allons expliquer maintenant.

5.4. Points fixes

Jusqu'à la fin de la section 5, K/k désigne une extension finie (avec comme toujours $\mathrm{K} \subset \Omega$ et Ω algébriquement clos).

Notons que $\mathrm{Aut}_k(\mathrm{K})$ est un groupe qui agit sur K.

Proposition 5.4.1. — *Soit* K/k *galoisienne de groupe Galois* G. *Alors,* G *est de cardinal* $[\mathrm{K} : k]$ *et l'espace des points fixes* K^{G} *de* K *sous l'action de* G *est réduit à* k.

Démonstration. — Le premier point est prouvé dans 5.1.5. Pour le second, soit x fixe sous l'action de G. Ses conjugués sont de la forme $\sigma(x)$ avec $\sigma \in \mathrm{G}$ d'après 5.2.1, et donc sont égaux à x. Comme le polynôme minimal $\mathrm{P} \in k[\mathrm{X}]$ de x est séparable car irréductible, il est donc égal à $\mathrm{X} - x$. Ainsi $x = -\mathrm{P}(0) \in k$. □

Inversement, prouvons l'énoncé fondamental suivant.

***Théorème 5.4.2* (Lemme d'Artin [2]).** — *Soit* $\mathbf{K}$ *un corps parfait et* G *un sous-groupe fini du groupe des automorphismes de corps de* $\mathbf{K}$. *Alors,* $\mathbf{K}^{\mathrm{G}}$ *est parfait et l'extension* $\mathbf{K}/\mathbf{K}^{\mathrm{G}}$ *est finie de groupe de Galois* G.

Démonstration. — Vérifions que $\mathbf{K}^{\mathrm{G}}$ est parfait. Le problème ne se pose qu'en caractéristique $p > 0$. Soit $x \in \mathbf{K}^{\mathrm{G}}$. Comme $\mathbf{K}$ est parfait, il a une racine p-ième $\xi \in \mathbf{K}$. Comme $x = \xi^p$ est invariant sous l'action de G, on a $\xi^p = g(\xi^p) = g(\xi)^p$ pour tout $g \in \mathrm{G}$. Comme le morphisme de Frobenius est injectif, on en déduit que ξ est fixe par G et donc $\xi \in \mathbf{K}^{\mathrm{G}}$ de sorte que $\mathbf{k} = \mathbf{K}^{\mathrm{G}}$ est parfait.
On a bien entendu $\mathrm{G} \subset \mathrm{Aut}_{\mathbf{k}}(\mathbf{K})$. Observons que tout élément x de $\mathbf{K}$ est algébrique de degré $\deg_{\mathbf{k}}(x) \leq \mathrm{card}(\mathrm{G}x)$ et donc de degré $\leq \mathrm{card}\,\mathrm{G}$. En effet, le polynôme

$$\mathrm{P}_x = \prod_{\xi \in \mathrm{G}x} (\mathrm{X} - \xi)$$

est invariant sous l'action de G (c'est-à-dire que tous ses coefficients le sont). Donc P_x est dans $\mathbf{k}[\mathrm{X}]$ par définition de $\mathbf{k} = \mathbf{K}^{\mathrm{G}}$. Soit alors $x \in \mathbf{K}$ un élément de degré sur $\mathbf{k}$ maximal. On a alors $\mathbf{K} = \mathbf{k}[x]$. En effet, sinon, soit $y \in \mathbf{K} - \mathbf{k}[x]$. L'extension $\mathbf{k}[x, y]$ est monogène (théorème de l'élément primitif, 4.6.2) engendrée par un élément z de degré $> \deg_{\mathbf{k}}(x)$, contradiction. On déduit que

$$[\mathbf{K} : \mathbf{k}] = \deg_{\mathbf{k}}(x) \leq \mathrm{card}\,\mathrm{G}.$$

Soit Ω algébriquement clos contenant $\mathbf{K}$. On a alors d'après (5.1.5)

$$\mathrm{card}\,\mathrm{G} \leq \mathrm{card}\,(\mathrm{Aut}_{\mathbf{k}}(\mathbf{K})) \leq \mathrm{card}\,(\mathrm{Hom}_{\mathbf{k}}(\mathbf{K}, \Omega)) = [\mathbf{K} : \mathbf{k}] \leq \mathrm{card}\,\mathrm{G}.$$

On conclut grâce à (5.1.5). □

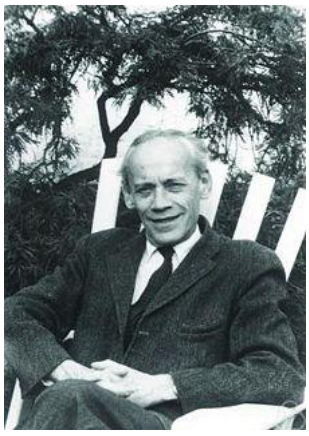


FIGURE 1. Emil Artin

2. 1898-1962

5.5. Énoncé et preuve de la correspondance de Galois

On est en mesure de prouver le théorème principal de la théorie de Galois.
Soit K/k une **extension finie et galoisienne** (contenue dans Ω) de groupe de Galois G. On rappelle (5.1.5) qu'on a alors

$$\mathrm{G} = \mathrm{Hom}_k(\mathrm{K}, \Omega).$$

Soit $\mathcal{F}$ la famille des sous-corps L de K contenant k, ordonnée par l'inclusion. Soit $\mathcal{G}$ la famille de sous-groupes de G, ordonnée par l'inclusion. Bien entendu (5.1.3), l'extension K/L est galoisienne. On peut énoncer le théorème principal.

Théorème 5.5.1 **(Correspondance de Galois)**

i) L'application

$$f : \begin{cases} \mathcal{F} & \to & \mathcal{G} \\ \mathrm{L} & \mapsto & \mathrm{Gal(K/L)} \end{cases}$$

est bijective, strictement décroissante, d'inverse

$$g : \begin{cases} \mathcal{G} & \to & \mathcal{F} \\ \mathrm{H} & \mapsto & \mathrm{K}^{\mathrm{H}} \end{cases}$$

Soit maintenant $\mathrm{H} \in \mathcal{G}$.

ii) L'extension $\mathrm{K/K}^{\mathrm{H}}$ *est galoisienne de groupe de Galois* H.

iii) L'application de restriction

$$r_{\mathrm{H}} : \ \mathrm{G} = \mathrm{Hom}_k(\mathrm{K}, \Omega) \to \mathrm{Hom}_k(\mathrm{K}^{\mathrm{H}}, \Omega)$$

identifie l'ensemble quotient $\mathrm{G/H}$ *à* $\mathrm{Hom}_k(\mathrm{K}^{\mathrm{H}}, \Omega)$.

iv) L'extension $\mathrm{K}^{\mathrm{H}}/k$ *est galoisienne si et seulement si* H *est un sous-groupe distingué de* K. *Dans ce cas, l'identification précédente induit un isomorphisme*

$$\mathrm{G/H} \xrightarrow{\sim} \mathrm{Gal}(\mathrm{K}^{\mathrm{H}}/k).$$

v) En particulier, si L/k *est galoisienne, on a une suite exacte canonique*

$$\{1\} \to \mathrm{Gal(K/L)} \to \mathrm{Gal}(\mathrm{K}/k) \to \mathrm{Gal}(\mathrm{L}/k) \to \{1\}. \tag{5.a}$$

Démonstration. — On doit d'abord vérifier qu'on a bien

$$g(f(\mathrm{L})) = g(\mathrm{Gal}(\mathrm{K}/\mathrm{L})) = \mathrm{K}^{\mathrm{Gal}(\mathrm{K}/\mathrm{L})} = \mathrm{L}.$$

Mais comme K est galoisienne sur L de groupe de Galois $\mathrm{H} = \mathrm{Gal}(\mathrm{L}/\mathrm{K})$, on a bien $\mathrm{K}^{\mathrm{H}} = \mathrm{L}$ d'après 5.4.1.

Ensuite, on a

$$fg(\mathrm{H}) = \mathrm{Gal}(\mathrm{K}/\mathrm{K}^{\mathrm{H}}) \overset{5.4.2}{=} \mathrm{H}.$$

Les deux applications f et g sont bien inverses l'une de l'autre, et en particulier sont bijectives.

La décroissance est claire, son caractère strict découlant de la bijectivité : on a prouvé *i*). Le point *ii*) est le lemme d'Artin (5.4.2).

Prouvons le point *iii*). Soit H un sous-groupe de G et prouvons la surjectivité de r_{H}. Tout k-morphisme $\sigma_{\mathrm{H}} \in \mathrm{Hom}_k(\mathrm{K}^{\mathrm{H}}, \Omega)$ se prolonge en $\sigma \in \mathrm{Hom}_k(\mathrm{K}, \Omega)$ d'après le théorème de prolongement des homomorphismes (3.9.1). Comme K/k est galoisienne, on a $\sigma(\mathrm{K}) = \mathrm{K}$ (5.1.4) *ie* $\sigma \in \mathrm{G}$ de sorte que $r_{\mathrm{H}}(\sigma) = \sigma_{\mathrm{H}}$: l'application de restriction r_{H} est surjective. Bien entendu, g et gh ont même image si $h \in \mathrm{H}$ de sorte qu'on a une surjection

$$\rho_{\mathrm{H}} : \mathrm{G}/\mathrm{H} \twoheadrightarrow \mathrm{Hom}_k(\mathrm{K}^{\mathrm{H}}, \Omega).$$

On a alors

$$\mathrm{card}\,\mathrm{Hom}_k(\mathrm{K}^{\mathrm{H}}, \Omega) \overset{4.6.5}{=} [\mathrm{K}^{\mathrm{H}} : k] = [\mathrm{K} : k]/[\mathrm{K} : \mathrm{K}^{\mathrm{H}}] = \mathrm{card}\,\mathrm{G}/\,\mathrm{card}\,\mathrm{H} = \mathrm{card}(\mathrm{G}/\mathrm{H})$$

de sorte que ρ_{H} est bijective.

Prouvons le point *iv*). Soit H un sous-groupe de G. Bien entendu $g \in \mathrm{G}$ envoie K^{H} dans $\mathrm{K}^{g\mathrm{H}g^{-1}}$ et donc g^{-1} envoie $\mathrm{K}^{g\mathrm{H}g^{-1}}$ dans K^{H} prouvant

$$g(\mathrm{K}^{\mathrm{H}}) = \mathrm{K}^{g\mathrm{H}g^{-1}}.$$

Supposons $\mathrm{K}^{\mathrm{H}}/k$ galoisienne. On a alors

$$\mathrm{K}^{\mathrm{H}} = g(\mathrm{K}^{\mathrm{H}}) = \mathrm{K}^{g\mathrm{H}g^{-1}}$$

et donc $\mathrm{H} = g\mathrm{H}g^{-1}$ par injectivité de la correspondance de Galois et donc $\mathrm{H} \lhd \mathrm{G}$.

Inversement, si $\mathrm{H} \lhd \mathrm{G}$, on a

$$g(\mathrm{K}^{\mathrm{H}}) = \mathrm{K}^{g\mathrm{H}g^{-1}} = \mathrm{K}^{\mathrm{H}}$$

et $\mathrm{K}/\mathrm{K}^{\mathrm{H}}$ est galoisienne.

L'isomorphisme de groupes est celui de 5.1.10. Maintenant v) découle clairement des autres points. □

Exercice 5.5.2. — *Soit* K/k *galoisienne de groupes* G *et* $\mathrm{K}_i/k, i = 1, 2$ *deux sous extensions définies par des sous-groupes* $\mathrm{G}_1, \mathrm{G}_2$ *de sous-groupes de* G. *Montrer que* $\mathrm{K}_1\mathrm{K}_2$ *correspond à* $\mathrm{G}_1 \cap \mathrm{G}_2$ *tandis que* $\mathrm{K}_1 \cap \mathrm{K}_2$ *correspond au sous-groupe de* G *engendré par* G_1 *et* G_2 *[Écrire ces extensions comme des* $\min, \max$ *et utiliser que la correspondance de Galois est bijective strictement décroissante]. Montrer que le stabilisateur* G_x *de* $x \in \mathrm{K}$ *dans* G *correspond au corps* $k[x]$ *engendré par* x.

CHAPITRE 6

CYCLOTOMIE ET CONSTRUCTIBILITÉ

Nous appliquons dans ce chapitre la théorie de Galois au problème de constructibilité des polygones réguliers. Pour ce faire, nous étudions d'abord les extensions cyclotomiques.

6.1. Extensions cyclotomiques

Soit k un corps parfait de caractéristique p et Ω une clôture algébrique de k.
Soit un entier $n \geq 1$. On suppose de plus que n et p sont premiers entre eux si $p > 0$. Ceci assure que $X^n - 1$ et sa dérivée nX^{n-1} n'ont pas de zéro commun dans Ω et donc que $X^n - 1$ est un polynôme séparable (4.5.2). L'ensemble $\mu_n(\Omega)$ de ses racines dans Ω est ainsi un sous-groupe de Ω^* de cardinal fini n. Le groupe $\mu_n(\Omega)$ est donc d'après (4.2.1) un sous-groupe cyclique de Ω^*, isomorphe à $\mathbf{Z}/n\mathbf{Z}$.
On rappelle que, par définition, une racine primitive n-ième de 1 est un générateur du groupe cyclique $\mu_n(\Omega)$. Choisissons ζ_n un tel générateur. Les autres racines primitives n-ièmes sont les ζ_n^m où m est premier avec n, c'est-à-dire les

$$\zeta_n^m, m \in (\mathbf{Z}/n\mathbf{Z})^*$$

où $(\mathbf{Z}/n\mathbf{Z})^*$ est le groupe multiplicatif des éléments inversibles de l'anneau $\mathbf{Z}/n\mathbf{Z}$ [1].
En conséquence, l'extension $k[\zeta_n]$ ne dépend pas du choix de la racine primitive ζ_n.

Définition 6.1.1. — *Une extension de la forme $k[\zeta_n]/k$ est appelée extension cyclotomique.*

Proposition 6.1.2. — *Une extension cyclotomique est galoisienne.*

1. Rappelons que les inversibles de l'anneau $\mathbf{Z}/n\mathbf{Z}$ sont les classes des entiers premiers à n (utiliser l'identité de Bézout pour le voir).

Démonstration. — Comme $\mu_n(\Omega)$ est engendré par ζ_n, le corps de décomposition de X^n-1 est simplement $k[\zeta_n]$. Ainsi l'extension $k[\zeta_n]/k$ est galoisienne (5.2.2). □

Notons

$$G_n = \mathrm{Gal}(k[\zeta_n]/k)$$

le groupe de Galois de l'extension $k[\zeta_n]/k$. Comme $X^n - 1$ est de degré n, le cardinal de G_n est inférieur ou égal à n. Nous allons démontrer dans cette partie un résultat plus précis (le théorème 6.3.10).

6.2. Sur le groupe de Galois de l'extension cyclotomique générale

Définissons d'abord le caractère cyclotomique χ.

Proposition 6.2.1. — *Il existe une unique application*

$$\chi : G_n \to (\mathbf{Z}/n\mathbf{Z})^*$$

telle que pour tout $g \in G_n$ et $\zeta \in \mu_n(k)$, on a

$$g(\zeta) = \zeta^{\chi(g)}.$$

Démonstration. — L'image de ζ_n par un élément du groupe de Galois $g \in G_n$ s'écrit de manière unique

$$g(\zeta_n) = \zeta_n^{\chi(g)} \text{ avec } \chi(g) \in \mathbf{Z}/n\mathbf{Z}.$$

Comme $g(\zeta_n)$ est une racine primitive, $\chi(g)$ est inversible dans $\mathbf{Z}/n\mathbf{Z}$ (*ie* est la classe d'un entier premier à n).

Maintenant, pour $\zeta \in \mu_n(k)$, il existe $m \in \mathbf{Z}/n\mathbf{Z}$ tel que $\zeta = \zeta_n^m$. On a alors

$$g(\zeta) = g(\zeta_n^m) = (g(\zeta_n))^m = (\zeta_n^{\chi(g)})^m = (\zeta_n^m)^{\chi(g)} = \zeta^{\chi(g)},$$

ce qui prouve l'existence. Supposons maintenant il existe un second morphisme

$$\chi' : G_n \to (\mathbf{Z}/n\mathbf{Z})^*$$

telle que pour tout $g \in G_n$ et $\zeta \in \mu_n(k)$, on a

$$g(\zeta) = \zeta^{\chi'(g)}.$$

On a alors la formule

$$1 = \zeta^{\chi(g)-\chi'(g)}$$

pour tout $g \in \mathrm{G}_n$ et $\zeta \in \mu_n(k)$. En l'appliquant à $\zeta = \zeta_n$, on déduit que $\chi(g) - \chi'(g)$ est divisible par l'ordre de ζ_n dans μ_n, donc par n, de sorte que $\chi(g) - \chi'(g) = 0$. □

On obtient alors :

Proposition 6.2.2. — *Le caractère cyclotomique χ définit un isomorphisme entre le groupe G_n et le sous-groupe $\chi(\mathrm{G}_n)$ de $(\mathbf{Z}/n\mathbf{Z})^*$. En particulier, G_n est commutatif.*

Démonstration. — Montrons d'abord que le caractère cyclotomique χ est un morphisme de groupe. Pour $g, g' \in \mathrm{G}_n$ et $\zeta \in \mathrm{G}_n$, on a

$$(gg')(\zeta) = g(\zeta^{\chi(g')}) = \zeta^{\chi(g)\chi(g')}$$

et donc $\chi(gg') = \chi(g)\chi(g')$. Maintenant on a aussi $(gg^{-1})(\zeta) = \zeta = \zeta^{\chi(g)\chi(g^{-1})}$ et donc $\chi(g^{-1}) = (\chi(g))^{-1}$. Comme ζ_n engendre $k[\zeta_n]$, χ est injectif de sorte que χ est un isomorphisme sur son image. □

Dans la suite, on identifiera le groupe G_n et son image $\chi(\mathrm{G}_n)$.

6.3. Irréductibilité du polynôme cyclotomique sur Q

Dorénavant, dans la suite de ce chapitre, $k = \mathbf{Q}$ et $\Omega = \mathbf{C}$.

On peut prendre ici $\zeta_n = \exp(\frac{2i\pi}{n})$ de sorte que les racines primitives n-ièmes de l'unité (dans $\mathbf{C}$) sont les nombres complexes de la forme $\zeta_n^m = \exp(\frac{2i\pi m}{n})$ où $m \in (\mathbf{Z}/n\mathbf{Z})^*$.

Définition 6.3.1. — *On définit le n-ième polynôme cyclotomique*

$$\Phi_n(\mathrm{X}) = \prod_{m \in (\mathbf{Z}/n\mathbf{Z})^*} \left(\mathrm{X} - \exp\left(\frac{2i\pi m}{n}\right)\right).$$

Un élément de G_n, étant injectif, envoie un générateur de $\mu_n(\mathbf{C})$ sur un autre générateur, et donc permute les racines primitives de l'unité. Les coefficients du polynôme cyclotomique sont ainsi dans $\mathbf{Q}[\zeta_n]^{\mathrm{G}_n}$ et donc dans $\mathbf{Q}$ d'après le lemme 5.4.1. On déduit donc que $\Phi_n(\mathrm{X})$ est un polynôme annulateur (unitaire) de degré

$$\varphi(n) = \mathrm{card}(\mathbf{Z}/n\mathbf{Z})^*$$

de ζ_n dans $\mathbf{Q}[\mathrm{X}]$.

En fait, nous allons montrer que Φ_n est irréductible et à coefficients entiers.

Commençons par énoncer un lemme élémentaire.

***Lemme 6.3.2* (Gauss).** — *Soient* P, Q *deux polynômes à coefficients entiers avec* Q *unitaire. Alors, le quotient et le reste de la division euclidienne de* P *par* Q *sont à coefficients entiers.*

Démonstration. — Il suffit de poser la division euclidienne. □

On en déduit :

Corollaire 6.3.3. — *On a* $\Phi_n(\mathrm{X}) \in \mathbf{Z}[\mathrm{X}]$.

Démonstration. — Toute racine n-ième de l'unité a un ordre $d|n$: c'est une racine primitive d-ième de 1. Inversement, si ζ est une racine primitive d-ième de 1 avec $d|n$, c'est une racine n-ième de 1. On déduit que l'ensemble des racines n-ièmes de 1 est l'union disjointe paramétrée par les diviseurs d de n des racines primitives d-ièmes. Comme

$$\mathrm{X}^n - 1 = \prod_{\zeta \in \mu_n} (\mathrm{X} - \zeta),$$

on déduit la formule

$$\mathrm{X}^n - 1 = \prod_{d|n} \Phi_d(\mathrm{X}). \tag{3.a}$$

Partant de $\Phi_1(\mathrm{X}) = \mathrm{X} - 1 \in \mathbf{Z}[\mathrm{X}]$, on obtient par récurrence sur d que Φ_d est à coefficients entiers d'après 6.3.2 i) pour tout $d|n$. C'est donc aussi vrai pour $d = n$. □

Le lemme suivant est dû à Gauss.

***Lemme 6.3.4* (Gauss).** — *Soit* $\mathrm{P} \in \mathbf{Z}[\mathrm{X}]$ *un polynôme non constant.*

i) Si P *est irréductible dans* $\mathbf{Z}[\mathrm{X}]$*, il est irréductible dans* $\mathbf{Q}[\mathrm{X}]$.

ii) Si P *est unitaire, alors les facteurs unitaires irréductibles de la factorisation de* P *dans* $\mathbf{Q}[\mathrm{X}]$ *sont à coefficients entiers.*

Démonstration. — Supposons P irréductible sur $\mathbf{Z}$ et supposons $\mathrm{P} = \mathrm{P}_1\mathrm{P}_2$ avec $\mathrm{P}_1, \mathrm{P}_2 \in \mathbf{Q}[\mathrm{X}]$ et $\deg(\mathrm{P}_1) > 0$. En éliminant les dénominateurs de $\mathrm{P}_1, \mathrm{P}_2$, on obtient une identité

$$n\mathrm{P} = \bar{\mathrm{P}}_1\bar{\mathrm{P}}_2$$

avec $n \in \mathbf{Z}$ et $\bar{\mathrm{P}}_1, \bar{\mathrm{P}}_2 \in \mathbf{Z}[\mathrm{X}]$ égaux à $\mathrm{P}_1, \mathrm{P}_2$ à multiplication scalaire près par un élément de $\mathbf{N}^*$.

Si $n = 1$, on déduit que $\bar{\mathrm{P}}_2$ est constant (irréductibilité sur $\mathbf{Z}$ de P) et donc $\deg(\mathrm{P}_2) = 0$.

Sinon, soit p un nombre premier divisant n. Réduisons modulo p la relation. On obtient l'identité dans $\mathbf{F}_p[\mathrm{X}]$

$$0 = (\bar{\mathrm{P}}_1 \mod p)(\bar{\mathrm{P}}_2 \mod p).$$

Comme $\mathbf{F}_p[\mathrm{X}]$ est intègre, on déduit qu'un des deux polynômes est nul, donc que $\bar{\mathrm{P}}_1$ ou $\bar{\mathrm{P}}_2$ a tous ses coefficients divisibles par p. Par exemple, on a $\bar{\mathrm{P}}_1 = p\tilde{\mathrm{P}}_1$ avec $\tilde{\mathrm{P}}_1 \in \mathbf{Z}[\mathrm{X}]$. En comparant les coefficients dominants, on a

$$n'\mathrm{P} = \tilde{\mathrm{P}}_1\bar{\mathrm{P}}_2 \text{ avec } n' = \frac{n}{p} \in \mathbf{Z} \text{ et } 1 \leq n' < n.$$

De proche en proche, on arrive à une écriture

$$\mathrm{P} = \mathrm{P}_1^*\mathrm{P}_2^*, \text{ avec } \mathrm{P}_1^*, \mathrm{P}_2^* \in \mathbf{Z}[\mathrm{X}]$$

et on s'est ramené au cas $n = 1$.

La preuve du second point est analogue. Écrivons $\mathrm{P} = \mathrm{P}_1\mathrm{P}_2$ avec donc $\mathrm{P}_1, \mathrm{P}_2$ unitaires à coefficients rationnels. Soient n_1, n_2 les plus petits entiers > 0 tels que $\bar{\mathrm{P}}_i = n_i\mathrm{P}_i \in \mathbf{Z}[\mathrm{X}], i = 1, 2$. Si $n_1, n_2 = 1$, c'est terminé. Sinon, soit p premier divisant n_1n_2. Comme pour le point i), p divise tous les coefficients d'un des deux polynômes $\bar{\mathrm{P}}_i$, disons $\bar{\mathrm{P}}_1$, et donc aussi son coefficient dominant, à savoir n_1. On déduit qu'on a

$$\frac{n_1}{p}\mathrm{P}_1 \in \mathbf{Z}[\mathrm{X}],$$

contredisant la minimalité de n_1. □

Définition 6.3.5. — *Un nombre complexe est dit entier algébrique s'il est racine d'un polynôme unitaire à coefficients entiers.*

Lorsque le contexte est clair, on dira simplement "entier" à la place d'entier algébrique. Pour éviter les confusions, on dira que les éléments de $\mathbf{Z}$ sont les *entiers relatifs*.

Par exemple, ζ_n est entier, mais $1/2$ ne l'est pas (cf. exercice 6.3.6). On reviendra sur cette notion importante (8.3).

La cohérence de la terminologie est assurée par le résultat suivant.

Exercice 6.3.6. — *Montrer que $x \in \mathbf{Q}$ est entier sur $\mathbf{Z}$ si et seulement si c'est un entier relatif.*

Le lemme de Gauss 6.3.4 donne immédiatement le résultat suivant.

Corollaire 6.3.7. — *Le polynôme minimal d'un élément entier est à coefficients entiers.*

Alors :

Théorème 6.3.8. — *Le polynôme cyclotomique Φ_n est irréductible sur $\mathbf{Q}$.*

La preuve, due à Gauss, est très astucieuse.

Démonstration. — Soit P le polynôme minimal de ζ_n. Il suffit de prouver $\Phi_n|\mathrm{P}$, ou encore que toutes les racines primitives de l'unité annulent P.
Soit p premier ne divisant pas n et ζ une racine de P. Alors ζ est nécessairement primitive car $\mathrm{P}|\Phi_n$. La clef est le lemme suivant.

Lemme 6.3.9. — *ζ^p est une racine de* P.

Démonstration. — Supposons le contraire. Écrivons

$$\mathrm{X}^n - 1 = \mathrm{P}(\mathrm{X})\mathrm{S}(\mathrm{X})$$

avec $\mathrm{S}(\mathrm{X}) \in \mathbf{Q}[\mathrm{X}]$. Comme ζ_n est entier, on a $\mathrm{P}(\mathrm{X}) \in \mathbf{Z}[\mathrm{X}]$ d'après le corollaire 6.3.7. P(X) étant de plus unitaire, $\mathrm{S}(\mathrm{X}) \in \mathbf{Z}[\mathrm{X}]$. Comme $\mathrm{P}(\zeta^p)$ est supposé non nul, on a $\mathrm{S}(\zeta^p) = 0$. Ainsi, P(X) et $\mathrm{Q}(\mathrm{X}) = \mathrm{S}(\mathrm{X}^p)$ ont une racine complexe commune. Leur PGCD (calculé sur $\mathbf{Q}$) est donc non constant, de sorte que P divise Q dans $\mathbf{Q}[\mathrm{X}]$ (irréductibilité de P) donc également dans $\mathbf{Z}[\mathrm{X}]$ puisque P est de plus unitaire. Réduisons modulo p. On obtient

$$\bar{\mathrm{Q}}(\mathrm{X}) = \bar{\mathrm{S}}(\mathrm{X}^p) = (\bar{\mathrm{S}}(\mathrm{X}))^p$$

en utilisant le morphisme de Frobenius. Comme par hypothèse $n \neq 0$ dans $\mathbf{F}_p$, $\mathrm{X}^n - 1$ et sa dérivée $n\mathrm{X}^{n-1}$ n'ont pas de racine commune dans $\bar{\mathbf{F}}_p$ de sorte que ni $\mathrm{X}^n - 1$ ni $\bar{\mathrm{P}}$ n'ont de facteur commun dans $\mathbf{F}_p[\mathrm{X}]$. Soit Π un facteur irréductible de $\bar{\mathrm{P}}$. Divisant $\bar{\mathrm{S}}^p$, il divise $\bar{\mathrm{S}}$ de sorte que $\Pi^2|\mathrm{X}^n - 1$ dans $\mathbf{F}_p[\mathrm{X}]$. On obtient une contradiction puisque $\bar{\mathrm{P}}$ est séparable. □

On peut maintenant terminer la preuve du théorème 6.3.8.
Soit alors ζ une racine de P et ζ' une racine quelconque de Φ_n. On écrit $\zeta' = \zeta^m$ avec $\mathrm{PGCD}(m, n) = 1$ (car ζ' est primitive). En décomposant m en facteurs premiers, une application répétée du lemme donne ζ' racine de P et donc $\Phi_n|\mathrm{P}$. □

Ainsi,

$$\mathrm{card}(\mathrm{G}_n) = [\mathbf{Q}[\zeta_n] : \mathbf{Q}] = \varphi(n)$$

de sorte que χ est un morphisme injectif (6.2.2) entre groupes de même cardinal. On a démontré le résultat suivant.

Théorème 6.3.10. — *Le caractère cyclotomique*

$$\chi : \mathrm{Gal}(\mathbf{Q}[\zeta_n]/\mathbf{Q}) \to (\mathbf{Z}/n\mathbf{Z})^*$$

est un isomorphisme de groupe.

Exercice 6.3.11. — *Soit $n \geq 1$ et p premier ne divisant pas n. Montrer que si $\Phi_n \mod (p)$ a une racine $x \in \mathbf{F}_p$, alors x est d'ordre exactement n dans $\mathbf{F}_p^*$. En déduire qu'on a la congruence $p \equiv 1 \mod (n)$ puis qu'il existe une infinité de nombres premiers congrus à 1 modulo n (forme faible du théorème de la progression arithmétique de Dirichlet).*

6.4. Intersections de corps cyclotomiques

Soit d divisant n de sorte que $\mathbf{Q}[\zeta_n]$ contient $\mathbf{Q}[\zeta_d]$. La correspondance de Galois prédit que $\mathbf{Q}[\zeta_d]$ correspond à un sous-groupe de $\mathrm{Gal}(\mathbf{Q}[\zeta_n]/\mathbf{Q})$ de cardinal $\varphi(n)/\varphi(d)$, qui doit être le noyau de la surjection

$$\mathrm{Gal}(\mathbf{Q}[\zeta_n]/\mathbf{Q}) \to \mathrm{Gal}(\mathbf{Q}[\zeta_d]/\mathbf{Q}).$$

En tenant compte du théorème 6.3.10, cette surjection n'est autre que le morphisme canonique

$$(\mathbf{Z}/n\mathbf{Z})^* \to (\mathbf{Z}/d\mathbf{Z})^*.$$

On retrouve au passage l'énoncé de l'exercice 2.8.3.

Maintenant, montrons le résultat suivant.

Proposition 6.4.1. — *Pour n, m entiers, on a*

$$\mathbf{Q}[\zeta_n, \zeta_m] = \mathbf{Q}[\zeta_{\mathrm{PPCM}(n,m)}]$$

et

$$\mathbf{Q}[\zeta_n] \cap \mathbf{Q}[\zeta_m] = \mathbf{Q}[\zeta_{\mathrm{PGCD}(n,m)}].$$

Démonstration. — On pose

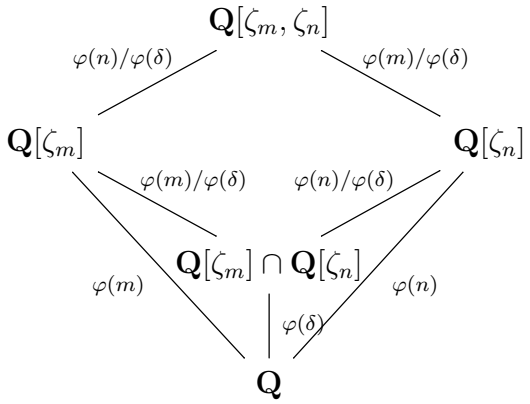
$$\mathrm{PPCM}(n,m) = \pi, \mathrm{PGCD}(n,m) = \delta, \mathrm{K} = \mathbf{Q}[\zeta_\pi]$$

et

$$\Gamma_d = \mathrm{Ker}((\mathbf{Z}/\pi\mathbf{Z})^* \to (\mathbf{Z}/d\mathbf{Z})^*)$$

pour tout d divisant π. On a deux sous-corps $\mathrm{K}_i = \mathbf{Q}[\zeta_i]$, $i = n, m$ de K, définis (correspondance de Galois) d'après ce qui précède par les sous-groupes Γ_i, $i = n, m$. D'après 5.5.2, on doit simplement montrer $\Gamma_n \cap \Gamma_m = \{1\}$ (qui prouve $\mathrm{K}_n\mathrm{K}_m = \mathbf{Q}[\zeta_n, \zeta_m] = \mathbf{Q}[\zeta_\pi]$) et que le groupe engendré par Γ_n et Γ_m est Γ_δ (prouvant $\mathrm{K}_n \cap \mathrm{K}_m = \mathbf{Q}[\zeta_\delta]$).
Le premier point est clair : dire que $g \mod \pi \in (\mathbf{Z}/\pi\mathbf{Z})^*$ est dans l'intersection $\Gamma_n \cap \Gamma_m$, c'est dire que n et m divisent $g-1$, autrement dit $\pi|(g-1)$.
Pour le second énoncé, grâce au lemme chinois, on peut supposer que n, m sont des puissances de p, de la forme p^ν, p^μ avec par exemple $0 \leq \nu \leq \mu$ de sorte que $\delta = p^\nu$. Le cas où ν ou μ est nul est trivial. Supposons donc $\nu, \mu > 0$. On a alors $\Gamma_i = 1+p^i\mathbf{Z}/p^\mu\mathbf{Z}$, $i = \nu, \mu$. Donc le groupe engendré est $\Gamma_\nu = \Gamma_\delta$. □

Les diverses extensions sont résumées comme suit :



6.5. Constructibilité à la règle et au compas

Le but de cette partie est l'application de la théorie de Galois aux problèmes de constructibilité à la règle et au compas. Nous démontrons dans cette partie les résultats de la partie 0.1. D'abord :

Théorème 6.5.1 **(Wantzel [2]).** — *Un nombre complexe z est constructible si et seulement si il existe une suite finie de corps $\mathrm{L}_0 = \mathbf{Q} \subset \mathrm{L}_1 \cdots \subset \mathrm{L}_n$ telle que pour $0 \leq i \leq n-1$, $[\mathrm{L}_{i+1} : \mathrm{L}_i] = 2$ et $z \in \mathrm{L}_n$.*

Démonstration. — Soit k un sous-corps de $\mathbf{R}$.

D'abord, notons qu'une droite $\mathrm{D} \subset \mathbf{R}^2$ contenant deux points de k^2 admet une équation de la forme

$$ax + by + c = 0 \text{ avec } a,\ b,\ c \text{ dans } k.$$

En effet, si D a une équation de la forme $y = \mathrm{A}x + \mathrm{B}$ avec $\mathrm{A}, \mathrm{B} \in \mathbf{R}$, on a par hypothèse $x_1 \neq x_2 \in k$ tels que $\mathrm{A}x_1 + \mathrm{B}, \mathrm{A}x_2 + \mathrm{B} \in k$. Donc $\mathrm{A}, \mathrm{B} \in k$. Sinon D a une équation de la forme $x = \mathrm{A}$. Comme la droite contient un point de k^2, on obtient $\mathrm{A} \in k$. On dit alors que la droite est définie sur k.
Ensuite, montrons qu'un cercle C de $\mathbf{R}^2$ dont le centre est dans k^2 et qui contient un point de k^2 admet une équation de la forme

$$x^2 + y^2 + ax + by + c = 0 \text{ avec } a,\ b,\ c \text{ dans } k.$$

En effet, C a une équation $(x - x_0)^2 + (y - y_0)^2 = \mathrm{R}^2$ avec $(x_0, y_0) \in k^2$ les coordonnées du centre. Comme C contient un point de k^2, on obtient $\mathrm{R}^2 \in k$, d'où le résultat. On dit alors que le cercle est défini sur k.
On en déduit maintenant que si un point $(x, y) \in \mathbf{R}^2$ est dans l'intersection de deux droites, d'un cercle et d'une droite, ou bien de deux cercles distincts, définis sur k, alors $[k[x] : k] \leq 2$ et $[k[y] : k] \leq 2$. Par exemple, dans le cas d'un cercle et d'une droite, on écrit une équation de la droite

$$a\mathrm{X} + b\mathrm{Y} + c = 0$$

et du cercle

$$\mathrm{X}^2 + \mathrm{Y}^2 + d\mathrm{X} + e\mathrm{Y} + f = 0$$

avec $a, b, c, d, e, f \in k$. Si $b \neq 0$, on écrit $y = -c/b - ax/b$ et on substitue y dans l'équation du cercle. On obtient une équation de degré au plus 2 et $[k[x] : k] \leq 2$. Comme $y \in k[x]$, on a aussi $[k[y] : k] \leq 2$. Le raisonnement est analogue si $a \neq 0$. Dans le cas de deux cercles, le raisonnement est analogue en commençant par soustraire les deux équations de cercle pour obtenir une relation du type

$$(d - d')x + (e - e')y + (f - f') = 0.$$

Montrons maintenant le résultat du théorème. Si un point est constructible à la règle et au compas, on obtient la suite de corps $\mathrm{L}_0, \cdots, \mathrm{L}_n$ en appliquant successivement les résultats précédents aux points $\mathrm{P}_1, \mathrm{P}_2, \cdots$.

Réciproquement, si $[\mathrm{L}_i : \mathrm{L}_{i-1}] = 2$, on peut compléter $\{1\}$ en une base $\{1, z\}$ de L_i sur L_{i-1}. Alors il existe $\lambda, \mu \in \mathrm{L}_{i-1}$ tels que

$$z^2 = \lambda z + \mu.$$

Ceci s'écrit

$$(z - \frac{\lambda}{2})^2 = \mu + \frac{\lambda^2}{4}.$$

On pose $x = z - \frac{\lambda}{2}$. Alors par construction $x^2 \in \mathrm{L}_{i-1}^*$. De plus comme $z \notin \mathrm{L}_{i-1}$, on a $x \notin \mathrm{L}_{i-1}$ et $\mathrm{L}_i = \mathrm{L}_{i-1}[x]$. D'après la partie 0.1, x est constructible si les éléments de L_{i-1} le sont. On peut donc conclure par récurrence sur n. □

On alors d'après le théorème 3.2.4)

$$[\mathrm{L} : \mathbf{Q}] = \prod [\mathrm{L}_{i+1} : \mathrm{L}_i] = 2^m.$$

Comme $\mathbf{Q}[z] \subset \mathrm{L}_n$, $[\mathbf{Q}[z] : \mathbf{Q}]$ est une puissance de 2.

Proposition 6.5.2. — *Soit $z \in \mathbf{C}$ et K le corps des racines du polynôme minimal de z sur $\mathbf{Q}$. z est constructible à la règle et au compas si et seulement si $[\mathrm{K} : \mathbf{Q}]$ est une puissance de 2.*

Démonstration. — Supposons que z est constructible et soit $\mathrm{L}_0 = \mathbf{Q} \subset \cdots \subset \mathrm{L}_n$ une suite de corps associée. Soit x_i un élément tel que $\mathrm{L}_i = \mathrm{L}_{i-1}[x_i]$, pour $1 \leq i \leq n$. On définit par récurrence $\mathrm{K}_0 = \mathbf{Q}$ et $\mathrm{K}_i = \mathrm{K}_{i-1}[x_{i,1}, \ldots, x_{i,r_i}]$, où $x_{i,1}, \ldots, x_{i,r_i}$ sont les conjugués de x_i sur $\mathbf{Q}$ pour $1 \leq i \leq n$.

On montre par récurrence que l'extension $\mathrm{K}_i/\mathbf{Q}$ est galoisienne, de degré une puissance de 2 pour tout $0 \leq i \leq n$. Le résultat est bien sûr vrai pour $i = 0$. Supposons qu'il est vrai pour l'entier $i - 1$, avec $i \geq 1$. Soit $y \in \mathrm{K}_i$, et $\sigma \in \mathrm{Hom}_{\mathbf{Q}}(\overline{\mathbf{Q}}, \overline{\mathbf{Q}})$. Il existe $\mathrm{P} \in \mathrm{K}_{i-1}[\mathrm{X}_1, \ldots, \mathrm{X}_{r_i}]$ tel que $y = \mathrm{P}(x_{i,1}, \ldots, x_{i,r_i})$. Alors $\sigma(y) = \mathrm{P}^\sigma(\sigma(x_{i,1}), \ldots, \sigma(x_{i,r_i}))$, où P^σ est le polynôme obtenu en appliquant σ aux coefficients de P. Psuique $\mathrm{K}_{i-1}/\mathbf{Q}$ est galoisienne par hypothèse de récurrence, P^σ est à coefficients dans K_{i-1}. Par construction, tous les $\sigma(x_{i,j})$ sont dans K_i, pour $1 \leq j \leq r_i$. On en déduit que $\sigma(y) \in \mathrm{K}_i$, et donc que l'extension $\mathrm{K}_i/\mathbf{Q}$ est galoisienne. De plus, on a des extensions successives

$$\mathrm{K}_{i-1} \subset \mathrm{K}_{i-1}[x_{i,1}] \subset \mathrm{K}_{i-1}[x_{i,1}, x_{i,2}] \subset \cdots \subset \mathrm{K}_{i-1}[x_{i,1}, \ldots, x_{i,r_i}] = \mathrm{K}_i$$

Or x_i est de degré 2 sur L_{i-1}, donc de degré 1 ou 2 sur K_{i-1}. Chacun des conjugués $x_{i,j}$ est donc de degré 1 ou 2 sur K_{i-1}. On en déduit que le degré $[\mathrm{K}_i : \mathrm{K}_{i-1}]$ est une puissance

de 2, ce qui conclut la preuve par récurrence.

Puisque K est un sous-corps de K_n, le résultat en découle.

Réciproquement, supposons que $[K : \mathbf{Q}]$ est une puissance de 2. On peut appliquer la correspondance de Galois avec l'extension galoisienne $K/\mathbf{Q}$ dont le groupe de Galois a un cardinal qui est une puissance de 2. Le résultat (1.6.12) permet de conclure. □

***Théorème 6.5.3* (Gauss-Wantzel).** — *Le polygone régulier à n côtés est constructible à la règle et au compas si et seulement si n est un produit d'une puissance de 2 et de nombres premiers de Fermat distincts.*

Démonstration. — Le polygone régulier à n côtés est constructible à la règle et au compas si et seulement si $\exp\left(\frac{2i\pi}{n}\right)$ est constructible.

Or, on a vu dans le théorème 6.3.10 que

$$\mathrm{Gal}\left(\mathbf{Q}\left[\exp\left(\frac{2i\pi}{n}\right)\right], \mathbf{Q}\right) \simeq (\mathbf{Z}/n\mathbf{Z})^*.$$

Comme $\mathbf{Q}[\exp\left(\frac{2i\pi}{n}\right)]/\mathbf{Q}$ est galoisienne, on a

$$\left[\mathbf{Q}\left[\exp\left(\frac{2i\pi}{n}\right)\right] : \mathbf{Q}\right] = \phi(n)$$

et d'après la Proposition 6.5.2, $\exp\left(\frac{2i\pi}{n}\right)$ est constructible si et seulement si $\varphi(n)$ est une puissance de 2.

Si $\varphi(n)$ est une puissance de 2, écrivons la décomposition en nombres premiers

$$n = 2^{\mathrm{N}} \prod_{1 \leq i \leq \mathrm{N}} p_i^{\mathrm{N}_i}$$

avec les p_i nombres premiers impairs. Alors

$$\varphi(n) = 2^{\mathrm{N}-1} \prod_{1 \leq i \leq \mathrm{N}} (p_i - 1) p_i^{\mathrm{N}_i - 1}.$$

En conséquence, tous les $\mathrm{N}_i = 1$ et les p_i sont de la forme $p_i = 1 + 2^{\mathrm{M}_i}$. On a $\mathrm{M}_i = \alpha\beta$ avec α impair et β puissance de 2. On obtient alors que $1 + 2^\beta$ divise p_i. Le nombre p_i étant premier, on obtient $1 + 2^\beta = p_i$ et donc $\mathrm{M}_i = \beta$.

Pour la réciproque, si n est de la forme souhaitée, il est clair que $\phi(n)$ est une puissance de 2. □

CHAPITRE 7

RÉSOLUBILITÉ PAR RADICAUX

Dans ce chapitre nous étudions la deuxième application historique de la théorie de Galois : le critère de résolubilité par radicaux des équations polynômiales.

Soit k un corps parfait et Ω une clôture algébrique de k.

7.1. Groupe de Galois d'un polynôme

Soit P un polynôme non constant à coefficients dans k et de racines (distinctes) $x_1, \cdots, x_n$ dans Ω. On peut supposer que P est unitaire. Les racines de P peuvent avoir éventuellement des multiplicités.

Définition 7.1.1. — *On appelle groupe de Galois de* P *sur* k *le groupe de Galois* $\mathrm{Gal}(\mathrm{P}, k) = \mathrm{Gal}(\mathrm{K}/k)$ *de son corps de racines* $\mathrm{K} = k[x_1, \cdots, x_n]$ *(5.2.2).*

Lemme 7.1.2. — *Le polynôme* $\mathrm{Q} = \prod_{1 \leq i \leq n}(\mathrm{X} - x_i)$ *est à coefficients dans* k.

Le résultat est faux si on ne suppose pas que k est parfait.

Démonstration. — Écrivons $\mathrm{P} = \prod_j \mathrm{P}_j^{n_j}$ où les P_j sont des polynômes de $k[\mathrm{X}]$ irréductibles unitaires distincts deux à deux. Le corps k étant parfait, chaque P_j est à racines simples (4.5.3). Comme Q et $\prod_j \mathrm{P}_j$ ont les mêmes racines et sont unitaires à racines simples, on a $\mathrm{Q} \in k[x]$. □

Remarque 7.1.3. — *En considérant* $\mathrm{PGCD}(\mathrm{P}, \mathrm{P}')$*, le lecteur trouvera un algorithme efficace pour calculer* Q *sans le décomposer en facteurs irréductibles.*

Quitte à remplacer P par Q, on peut donc supposer P **séparable**.

Le groupe de Galois G de P ne dépend essentiellement que de P, et non pas du choix de la clôture algébrique Ω (cf. 3.9.1 par exemple).
Rappelons que, G laissant k invariant, on a la formule

$$0 = g(\mathrm{P}(x_i)) = \mathrm{P}(g(x_i)) \text{ pour } 1 \leq i \leq n. \tag{1.a}$$

Comme P est à racine simple, il existe un unique indice $\sigma_g(i)$ tel que $x_{\sigma_g(i)} = g(x_i)$. Comme g est injective, σ_g l'est aussi et donc $\sigma_g \in \mathrm{S}_n$.
L'application $g \mapsto \sigma_g$ définit une action de G sur $\{x_1, \cdots, x_n\}$, c'est-à-dire un morphisme de groupe

$$\mathrm{G} \to \mathrm{S}_n \text{ où } n = \deg(\mathrm{P}).$$

Lemme 7.1.4. — *L'action de* G *sur les racines de* P *est fidèle.*

Démonstration. — Il s'agit de montrer que le morphisme de groupe est *injectif*

$$\mathrm{G} \hookrightarrow \mathrm{S}_n.$$

C'est une conséquence directe du fait que les racines engendrent le corps de décomposition $\mathrm{K} = k[x_1, \cdots, x_n]$. □

C'est le point de vue fondateur de Galois et d'Abel [1] qui voyaient les groupes de Galois comme des sous-groupes de S_n.

FIGURE 1. Niels Abel

1. 1802-1829

Remarque 7.1.5. — *Le lecteur se convaincra aisément que si on change de numérotation, on conjugue simplement l'action par l'élément de* S_n *décrivant le changement de numérotation. Donc, plus que la permutation, c'est sa classe de conjugaison qui est bien définie, donc son type (1.5.2).*

Proposition 7.1.6. — *Le polynôme* P *est* irréductible *si et seulement si l'action de* G *sur les racines de* P *est* transitive.

Démonstration. — Supposons P irréductible. Les x_i s'identifient aux k-homomorphismes de $k[x_1] = k[\mathrm{X}]/(\mathrm{P})$ dans Ω (3.9.5), qui s'identifient comme on l'a vu aux éléments de G. L'action est donc transitive dans ce cas (5.2.1). Inversement, supposons l'action transitive et supposons $\mathrm{P} = \mathrm{QR}, \mathrm{Q}, \mathrm{R} \in k[\mathrm{X}]$ avec $\deg(\mathrm{Q}) > 0$. La formule (1.a) appliquée à Q assure que G laisse globalement invariant l'ensemble non vide des racines de Q. Comme l'action de G sur les racines de P est transitive, toutes les racines de P sont racines de Q et $\mathrm{Q} = \mathrm{P}$ (les polynômes P et Q étant séparables). □

Cette discussion explique l'importance du groupe symétrique et de ses classes de conjugaison dans la théorie. On a l'exemple fondamental suivant.

Lemme 7.1.7. — *Soit* $\mathrm{P} \in \mathbf{F}_p[\mathrm{X}]$ *de degré* $n > 0$ *irréductible. Soit* $\mathrm{G} = \mathrm{Gal}(\mathrm{P}, \mathbf{F}_p)$ *et* $\mathrm{F} \in \mathrm{G}$ *le morphisme de Frobenius. Alors* G *est un sous-groupe cyclique de* S_d, F *est un cycle de longueur* d *et* $\mathrm{card}(\mathrm{G}) = d$.

Démonstration. — Comme P est irréductible et $\mathbf{F}_p$ parfait, le polynôme P est séparable. Soient donc $(z_j)_{1 \leq j \leq d}$ les racines de P dans $\bar{\mathrm{F}}_p$. Comme G agit sur $(z_j)_{1 \leq j \leq d}$, on peut plonger G dans S_d où l'on identifie S_d à $\mathrm{Bij}(z_1, \cdots, z_d)$. Comme P est un polynôme irréductible, P est le polynôme minimal de z_1 sur $\mathbf{F}_p$ et ses racines sont les conjugués de z_1. Le corps $\mathbf{F}_p$ et le corps de décomposition de P étant finis, G est cyclique engendré par F (4.2.3). Les conjugués de z_1 sont donc exactement les $\mathrm{F}^n(z_1), n = 0, \cdots, d-1$. L'image de F dans S_d est ainsi le cycle $(z_1, \mathrm{F}(z_1), \cdots, \mathrm{F}^{d-1}(z_1))$. C'est un cycle de longueur d, ce qui permet de conclure. □

7.2. Discriminant

Soit $\mathrm{G} \subset \mathrm{S}_n$ le groupe de Galois d'un polynôme $\mathrm{P} \in k[\mathrm{X}]$. Voyons une condition simple permettant de décider si on a $\mathrm{G} \subset \mathrm{A}_n$.

Proposition 7.2.1. — *L'élément*

$$\mathrm{disc}(\mathrm{P}) = (-1)^{\frac{n(n-1)}{2}} \prod_{\substack{x \neq y \\ \mathrm{P}(x)=\mathrm{P}(y)=0}} (x-y)$$

est un élément de k^*.

Dans le cas où k est de caractéristique différente de 2, $\mathrm{disc}(\mathrm{P})$ *est un carré de k^* si et seulement si* $\mathrm{G} \subset \mathrm{A}_n$.

On dit que $\mathrm{disc}(\mathrm{P})$ est le discriminant de P. C'est un cas particulier de la notion de *résolvante*.

Démonstration. — Visiblement $\mathrm{disc}(\mathrm{P})$ est non nul et invariant par G, donc (5.4.1) est dans k^*. Choisissons un ordre sur les racines de P qu'on écrit $x_1, \cdots, x_n$. On a alors

$$\mathrm{disc}(\mathrm{P}) = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (x_i - x_j).$$

Posons

$$\sqrt{d} = \prod_{i<j} (x_i - x_j) \in \Omega.$$

On a

$$\sqrt{d}^2 = \mathrm{disc}(\mathrm{P}).$$

Faisons opérer S_n sur les indices $\{1, \cdots, n\}$. On a alors pour $\sigma \in \mathrm{S}_n$

$$\sigma(\sqrt{d}) = \prod_{i<j} (x_{\sigma(i)} - x_{\sigma(j)}).$$

Les couples $(\sigma(i), \sigma(j))$ sont de deux sortes : soit $\sigma(i) < \sigma(j)$, et on retrouve un facteur du produit initial, soit $\sigma(i) > \sigma(j)$ et on retrouve l'opposé d'un facteur du produit initial. On a donc

$$\sigma(\sqrt{d}) = (-1)^{|\sigma|} \prod_{i<j} (x_i - x_j)$$

où

$$|\sigma| = \mathrm{card}\{(i,j) \text{ tels que } i<j \text{ et } \sigma(i) > \sigma(j)\}.$$

On se souvient alors de la formule (1.5)

$$\epsilon(\sigma) = (-1)^{|\sigma|}$$

de sorte que

$$\sigma(\sqrt{d}) = \epsilon(\sigma)\sqrt{d}.$$

Donc, si $\mathrm{G} \subset \mathrm{A}_n$, on a certainement $\sqrt{d} \in k$, quelque soit la caractéristique de k. Inversement, si $\sqrt{d} \in k^*$, on a

$$\sqrt{d} = \epsilon(\sigma_g)\sqrt{d}.$$

Donc $\epsilon(\sigma_g) = 1$ dans k, ce qui signifie $\epsilon(\sigma_g) = 1$ dans $\mathbf{Z}$ si la caractéristique de k ne divise pas $1 + \epsilon(g) = 2$. D'où le lemme. □

Exercice 7.2.2. — *Montrer que le groupe de Galois d'un polynôme de degré* 2 *est trivial ou isomorphe à* $\mathbf{Z}/2\mathbf{Z}$. *Montrer qu'en degré* 3, *caractéristique différente de* 2, *le groupe de Galois est isomorphe à* $\mathbf{Z}/3\mathbf{Z}$ *ou* S_3. *Montrer que ce dernier cas ne se produit que si* $\mathrm{disc}(\mathrm{P})$ *n'est pas un carré à moins que* P *n'ait une racine dans* k. *En déduire que le groupe de Galois de* $\mathrm{X}^3 - 2$ *sur* $\mathbf{Q}$ *est* $\mathrm{S}_3 \xrightarrow{\sim} \mathrm{D}_6$.

Exercice 7.2.3. — *Soit* k *un corps parfait de caractéristique* $p \geq 0$. *Calculer le discriminant de* $\mathrm{P} = \mathrm{X}^n - 1$. *Montrer que* P *est séparable si et seulement* p *ne divise pas* n, *ce qu'on suppose désormais. Soit* K *le corps des racines de* P *(dans une clôture algébrique* $\bar{k}$ *de* k*). Donner une condition nécessaire et suffisante sur* n *pour que l'action de* $\mathrm{Gal}(\mathrm{K}/k)$ *sur* $\mu_n(\bar{k})$ *soit dans* A_n, *au moins si* $p \neq 2$.

Exercice 7.2.4. — *Soit* P *un polynôme séparable à coefficients dans* k *de caractéristique* 2. *On note* x_i *ses racines dans* $\bar{k}$ *et* G *le groupe de Galois de* $k[x_i]/k$, *qui agit donc sur les* x_i, *et ainsi se plonge dans* S_n. *Montrer que* $x_i + x_j$ *et* $x_i^2 + x_j^2$ *sont non nuls si* $i < j$. *Montrer que* $a = \sum_{i<j} \frac{x_i x_j}{x_i^2 + x_j^2}$ *est un élément de* k. *Soit* $b = \sum_{i<j} \frac{x_i}{x_i + x_j} \in \bar{k}$. *Montrer qu'on a d'une part* $b^2 + b = a$ *et, d'autre part,* $g(b) = b$ *ou* $b + 1$ *suivant que* $g \in \mathrm{A}_n$ *ou* $g \notin \mathrm{A}_n$. *En déduire qu'on a* $\mathrm{G} \subset \mathrm{A}_n$ *si et seulement si* a *s'écrit* $x^2 + x$ *avec* $x \in k$.

7.3. Extensions cycliques

Dans ce paragraphe, n **désigne un entier supérieur ou égal à** 2. k **est un corps parfait tel que** $\mu_n(k)$ **est de cardinal** n**.**

On dit alors abusivement que "k contient les racines n-ièmes de l'unité". En particulier, la caractéristique de k ne divise pas n (mais ce n'est évidemment pas suffisant en général). Comme tout sous groupe fini de k^* est cyclique, on sait alors que le groupe $\mu_n(k)$ est isomorphe à $\mathbf{Z}/n\mathbf{Z}$ (non canoniquement en général). Ainsi existent dans k les racines primitives (d'ordre n) de 1 (au nombre de $\varphi(n)$).

Définition 7.3.1. — *Une extension cyclique est une extension* K/k *avec* K *corps de rupture d'un polynôme de la forme* $\mathrm{P}(\mathrm{X}) = \mathrm{X}^n - a$ *avec* $a \in k \setminus \{0\}$.

Notons qu'alors $\mathrm{K} = k[\alpha]$ avec $\alpha = a^{1/n}$ racine de P.

Lemme 7.3.2. — *Une extension cyclique est galoisienne.*

Démonstration. — Les racines de $\mathrm{X}^n - a$ sont les multiples de α par les racines n-ièmes de l'unité. Par hypothèse ces dernières sont dans k. Ainsi, K est le corps des racines de $\mathrm{X}^n - a$, et donc est galoisienne sur k. □

Soit $\mathrm{G} = \mathrm{Gal}(\mathrm{K}/k)$ le groupe de Galois de l'extension K/k.

Lemme 7.3.3. — *Il existe un unique morphisme de groupe*

$$\kappa : \mathrm{G} \to \mu_n(k)$$

tel que $\kappa(g) = g(\alpha)/\alpha$ *pour* $g \in \mathrm{G}$.

Démonstration. — Si $g \in \mathrm{G}$, l'élément $g(\alpha)$ est une racine de P donc de la forme $\zeta\alpha$ pour $\zeta \in \mu_n(k)$. L'application κ est donc bien définie. Maintenant, on a $g(\alpha) = \kappa(g)\alpha$. En composant par g^{-1} on obtient $\alpha = g^{-1}(\kappa(g))g^{-1}(\alpha)$. Or $\kappa(g) \in \mu_n(k) \subset k$ donc $g^{-1}(\kappa(g)) = \kappa(g)$. Ainsi $\alpha(\kappa(g))^{-1} = g^{-1}(\alpha)$ et $\kappa(g^{-1}) = (\kappa(g))^{-1}$. Soit maintenant $h \in \mathrm{G}$. On a de même $g(\kappa(h)) = \kappa(h)$ et

$$(gh)(\alpha) = g(\kappa(h)\alpha) = g(\kappa(h))g(\alpha) = \kappa(h)\kappa(g)\alpha.$$

On obtient ainsi $\kappa(gh) = \kappa(g)\kappa(h)$. On a montré que κ est un morphisme de groupes. □

Lemme 7.3.4. — κ *est injective et* G *est cyclique de cardinal* d *divisant* n. *De plus, les assertions suivantes sont équivalentes :*
(i) P *irréductible,*
(ii) a *n'est pas une puissance* d*-ième dans* k *pour tout diviseur* d *de* n *distinct de* 1,
(iii) $\mathrm{G} = \mu_n(k)$.

Démonstration. — L'injectivité de κ est claire. Comme $\mu_n(k)$ est cyclique de cardinal n, l'ordre de G est un diviseur δ de n. Dire que P est irréductible c'est dire que $[\mathrm{K} : k] = n$ et donc que κ surjective. Supposons que P est irréductible, et donc que $\mathrm{G} = \mu_n(k)$. Soit $\zeta = \kappa(g)$ primitive dans $\mu_n(k)$ et $d|n$ tel que $\alpha^d \in k$ (c'est-à-dire $a \in k^{\frac{n}{d}}$). On a $g(\alpha^d) = \zeta^d\alpha^d$ mais aussi $g(\alpha^d) = \alpha^d$ car $\alpha^d \in k$. On a donc $\zeta^d = 1$ et donc $n|d$ puis $d = n$.

Inversement, si P non irréductible, on a G de cardinal δ qui divise strictement n. Pour tout $g \in \mathrm{G}$, on a $g(\alpha)/\alpha \in \mu_\delta(k)$ et donc $g(\alpha^\delta) = \alpha^\delta$. Donc $\alpha^\delta \in k$. □

La réciproque est, en un sens, assez surprenante.
On rappelle que le cardinal de $\mu_n(k)$ est n (sinon le théorème suivant n'est pas valable).

***Théorème 7.3.5* (Kummer [2]).** — *Soit* K/k *une extension galoisienne de groupe de Galois* $\mathrm{G} = \mathrm{Gal}(\mathrm{K}/k)$ *cyclique d'ordre* n*. Alors, l'extension* K/k *est cyclique.*

Démonstration. — Soit g un générateur de Galois : il vérifie $g^n = \mathrm{Id}$ vu dans $\mathrm{End}_k(\mathrm{K})$. On sait que K est un espace vectoriel de degré n sur k (5.4.1). Par hypothèse, $\mathrm{X}^n - 1$ est scindé sur k à racines simples, donc g est diagonalisable. La formule $g(xy^{-1}) = g(x)g(y)^{-1}$ assure que l'ensemble des valeurs propres de G est un sous-groupe de $\mu_n(k)$ et donc est cyclique d'ordre d. Si on avait $d < n$, on aurait $g^d = \mathrm{Id}$, ce qui n'est pas le cas car g est un générateur et donc il existe une valeur propre de g qui est une racine primitive n-ième ζ de 1. Soit x un vecteur propre non nul. Par construction, x a au moins n conjugués. Ceux sont les $(\zeta^i x)_{1 \leq i \leq n}$ qui sont distincts et nécessairement dans K. L'extension K/k est galoisienne de sorte que $\mathrm{K} = k[x]$. Ainsi, les $(\zeta^i x)_{1 \leq i \leq n}$ sont tous les conjugués de x, et donc le polynôme minimal de x est

$$\prod_{1 \leq i \leq n} (\mathrm{X} - \zeta^i x) = \mathrm{X}^n - a$$

avec $a \in k$. □

FIGURE 2. Ernst Kummer

2. 1810-1893

Remarque 7.3.6. — *Si on lit la preuve précédente attentivement, le phénomène qui se passe est le suivant. Notons* K_a *l'espace propre* $\mathrm{Ker}(g - a\mathrm{Id})$. *On a alors*

$$\mathrm{K} = \oplus_{1 \leq i \leq n} \mathrm{K}_i \text{ avec } \mathrm{K}_i = kx^i \tag{3.a}$$

où x *est non nul dans* K_1.

Exercice 7.3.7. — *Supposons* n *premier à la caractéristique de* k. *Soit* $a \in k$. *Montrer que* $\mathrm{P} = \mathrm{X}^n - a$ *est séparable et que son groupe de Galois* G *est extension de deux groupes abéliens, autrement dit qu'on a une suite exacte* $1 \to \mathrm{G}_1 \to \mathrm{G} \to \mathrm{G}_2 \to 1$ *avec* $\mathrm{G}_1, \mathrm{G}_2$ *abéliens (et même* G_1 *cyclique). Donner un exemple où* G *n'est pas commutatif.*

Bien entendu, toute sous-extension d'une extension cyclotomique $\mathbf{Q}[\zeta_n]$ a un groupe de Galois abélien. Un théorème difficile, dit de Kronecker [3]-Weber [4], assure que la réciproque est vraie ! C'est une conséquence de la vaste théorie du corps de classes, qui débouche naturellement sur la visionnaire théorie de Langlands [5], sujet très difficile et actif à l'heure qu'il est.

FIGURE 3. Leopold Kronecker

FIGURE 4. Heinrich Martin Weber

7.4. Applications aux équations

On suppose dans ce paragraphe que k est de caractéristique nulle.

3. 1823-1891
4. 1842-1913
5. 1936-

FIGURE 5. Robert Langlands

Définition 7.4.1. — *On dit qu'une extension de corps* K/k *est radicale si il existe une suite de corps* $\mathrm{K}_i, i = 0 \cdots, n$ *telle que*

$$k = \mathrm{K}_0 \subset \cdots \subset \mathrm{K}_n = \mathrm{K}$$

et $\mathrm{K}_{i+1} = \mathrm{K}_i[x_i]$ *et une puissance convenable de* x_i *est dans* K_i.

On dit que K/k *est résoluble si il existe une extension finie* L/K *contenant* K *tel que* L/k *radicale.*

On dit aussi que K/k est "résoluble par radicaux" lorsqu'elle est résoluble.

Ainsi, si K/k est résoluble, tout élément $x \in \mathrm{K}$ s'exprime à l'aide de fractions rationnelles et d'extractions successives de radicaux à partir d'éléments de k.

Donc, dire que le corps des racines de $\mathrm{P} \in k[\mathrm{X}]$ est résoluble (sur k), c'est dire que ses racines s'expriment rationnellement à partir d'extractions successives d'éléments de k : c'est la notion intuitive de résolubilité par radicaux !

Théorème 7.4.2 **(Galois)**. — *Soit* K/k *galoisienne. Si* K/k *est résoluble, alors* $\mathrm{G} = \mathrm{Gal}(\mathrm{K}/k)$ *est résoluble.*

En fait, la réciproque du théorème est aussi vraie [6]. Passons à la preuve du théorème.

Démonstration. — Par hypothèse, K est contenu dans L avec L/k radical. On a donc une suite de corps emboîtés

$$k = \bar{\mathrm{L}}_0 \subset \bar{\mathrm{L}}_1 \cdots \subset \bar{\mathrm{L}}_n = \mathrm{L}$$

tels que $\bar{\mathrm{L}}_{i+1} = \bar{\mathrm{L}}_i[x_i]$ et $x_i^{n_i} \in \bar{\mathrm{L}}_i$.

6. Ce n'est pas difficile à démontrer en connaissant la théorie de Kummer.

Le problème est que les $\bar{\mathrm{L}}_i$ n'ont aucune raison d'être galoisiennes sur k. Remédions à cela. On veut utiliser le théorème de Kummer. Soit donc n un multiple de tous les n_i et X_i l'ensemble des conjugués (sur k) des $x_j, 0 \leq j \leq i$.
On pose alors

$$\mathrm{L}_{i+1} = k[\zeta_n, \mathrm{X}_i], i = 0, \cdots, n-1,$$

qui par construction est galoisienne sur k (comme précédemment, ζ_n désigne une racine primitive $n$ième de l'unité dans Ω). On pose $\mathrm{L}_{-1} = k, \mathrm{X}_{-1} = \{\zeta_n\}$ de sorte qu'on a

$$\mathrm{L}_{i+1} = \mathrm{L}_i[\mathrm{X}_i] \text{ pour } i \geq -1$$

avec L_i galoisienne sur $\mathrm{L}_{-1} = k$ pour tout i donc *a fortiori* sur $\mathrm{L}_j, -1 \leq j \leq i$.
Comme $\mathrm{Gal}(\mathrm{K}/k)$ est un quotient (5.5.1) de $\mathrm{Gal}(\mathrm{L}_n/\mathrm{L}_{-1})$, il suffit de montrer que ce dernier est résoluble (1.6.6). Montrons par récurrence sur i que $\mathrm{Gal}(\mathrm{L}_i/\mathrm{L}_{-1})$ est résoluble.

Lemme 7.4.3. — *Chaque groupe* $\mathrm{Gal}(\mathrm{L}_{i+1}/\mathrm{L}_i), i \geq -1$ *est résoluble.*

Démonstration. — Comme $\mathrm{Gal}(\mathrm{L}_0/\mathrm{L}_{-1})$ est commutatif (6.2.2), on peut supposer $i \geq 0$. Si $i \geq 0$, L_{i+1} est obtenu en adjoignant à L_i les conjugués $(y_j)_{1 \leq j \leq \deg_k(x_i)}$ de x_i sur k. On a donc une tour d'extension

$$\mathrm{M}_0 = \mathrm{L}_i \subset \mathrm{M}_1 = \mathrm{L}_i[y_1] \subset \cdots \subset \mathrm{M}_d = \mathrm{L}_i[y_1, \cdots, y_d] = \mathrm{L}_{i+1}.$$

Comme $y_j^n \in \mathrm{L}_i$ et $\zeta_n \subset \mathrm{L}_i$, tous les L_i-conjugués de $y_j, j \leq \delta$ sont dans M_δ qui est donc galoisienne sur M_0, donc aussi sur les $\mathrm{M}_{\delta'}, \delta' \leq \delta$. Comme de plus, $\mathrm{M}_{\delta+1} = \mathrm{M}_\delta[y_{\delta+1}]$, chaque extension élémentaire intermédiaire $\mathrm{M}_{\delta+1}/\mathrm{M}_\delta$ est cyclique, donc galoisienne de groupe de Galois cyclique. Or, on a

$$1 = \mathrm{G}_0 = \mathrm{Gal}(\mathrm{M}_d/\mathrm{M}_d) \subset \mathrm{G}_2 = \mathrm{Gal}(\mathrm{M}_d/\mathrm{M}_{d-1}) \subset \cdots \subset \mathrm{G}_d = \mathrm{Gal}(\mathrm{M}_d/\mathrm{M}_0).$$

On a de plus

$$\mathrm{G}_{\delta+1}/\mathrm{G}_\delta \xrightarrow{\sim} \mathrm{Gal}(\mathrm{M}_{\delta+1}/\mathrm{M}_\delta)$$

(grâce à la suite exacte fondamentale (5.a)) et donc $\mathrm{G}_{\delta+1}/\mathrm{G}_\delta$ est abélien. La proposition 1.6.6 assure que G_d est résoluble. □

La théorie de Galois (5.a) nous donne des suites exactes

$$1 \to \mathrm{Gal}(\mathrm{L}_{i+1}/\mathrm{L}_i) \to \mathrm{Gal}(\mathrm{L}_{i+1}/\mathrm{L}_{-1}) \to \mathrm{Gal}(\mathrm{L}_i/\mathrm{L}_{-1}) \to 1.$$

On conclut grâce au lemme et grâce à la proposition 1.6.6. □

Passons à l'application aux équations : peut-on résoudre par radicaux une équation polynomiale, c'est-à-dire peut-on exprimer ses racines en fonction de ses coefficients ? Ceci revient à montrer que l'extension engendrée par les racines est résoluble sur le corps engendré par les coefficients.

Soit donc $L = \mathrm{Frac}(\mathbf{C}[X_1, \cdots, X_n])$ le corps des fractions de $\mathbf{C}[X_1, \cdots, X_n]$ où les X_i sont des indéterminées. Le groupe symétrique S_n agit sur L par permutation des indices. Soit $K = L^{S_n}$: l'extension L/K est galoisienne de groupe de Galois S_n d'après le lemme d'Artin. On sait d'autre part (Annexe (9.5)) qu'on a

$$K = \mathrm{Frac}(\mathbf{C}[\sigma_1, \cdots, \sigma_n])$$

où les σ_i sont les polynômes symétriques élémentaires en les X_i définis par l'identité suivante (voir l'Annexe (9.5) pour plus de détails) :

$$\prod_{i=1}^{n}(X - X_i) = X^n + \sum_{i=1}^{n}(-1)^i \sigma_i X^{n-i}. \tag{4.a}$$

Remarque 7.4.4. — *On peut aussi invoquer le lemme d'Artin et la majoration triviale* $[L : \mathrm{Frac}(\mathbf{C}[\sigma_1, \cdots, \sigma_n])] \leq n!$ *pour prouver que* $K = \mathrm{Frac}(\mathbf{C}[\sigma_1, \cdots, \sigma_n])$.

La formule 4.a prouve au passage que L est le corps de décomposition sur K de $P(X) = X^n + \sum_{i=1}^{n-1}(-1)^i \sigma_i X^{n-i}$.

Or l'équation polynomiale générale à coefficients dans K s'écrit précisément

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

Dire que cette équation est résoluble par radicaux signifie donc que L/K est résoluble.

Ce n'est pas le cas si $n \geq 5$:

Théorème 7.4.5 **(Abel,Galois)**. — L/K *n'est pas résoluble dès que* $n \geq 5$.

Démonstration. — Il suffit d'utiliser le Théorème 7.4.2 et la Proposition 1.6.10. □

CHAPITRE 8

RÉDUCTION MODULO p

Dans cette partie, nous allons donner des méthodes permettant d'étudier des groupes de Galois de polynômes P unitaires à coefficients entiers par réduction modulo p (p nombre premier), c'est-à-dire en utilisant le polynôme $\bar{\mathrm{P}} \in \mathbf{F}_p[\mathrm{X}]$ obtenu par réduction modulo p des coefficients de P. Ceci va permettre de se ramener à la situation sur $\mathbf{F}_p$ qui est, au moins théoriquement, plus simple : on sait par exemple factoriser les polynômes en polynômes irréductibles (voir (4.3) l'algorithme de Berlekamp [1]), les extensions sont toujours galoisiennes de groupes de Galois cycliques, avec en prime un générateur canonique, le morphisme de Frobenius.

FIGURE 1. Elwyn Berlekamp

On se donne donc un nombre premier p. Dans le cas où $\bar{\mathrm{P}}$ est séparable, on va comparer le groupe de Galois $\mathrm{Gal}(\mathrm{P}, \mathbf{Q})$ de P (*ie* celui de son corps des racines (7.1)) et celui $\mathrm{Gal}(\bar{\mathrm{P}}, \mathbf{F}_p)$ de $\bar{\mathrm{P}}$.

1. 1940-

Le résultat principal pour nous est que, **sous ces conditions, il existe un élément de** $\mathrm{Gal}(\mathrm{P}, \mathbf{Q})$**, unique à conjugaison près, dont la classe de conjugaison dans** $\mathrm{S}_{\mathbf{deg}(\mathrm{P})}$ **est la même que celle du morphisme de Frobenius dans** $\mathrm{Gal}(\bar{\mathrm{P}}, \mathbf{F}_p)$ (pour les plongements canoniques des groupes de Galois dans les groupes symétriques).
Commençons par expliciter le résultat sous une forme que nous utiliserons le plus dans la pratique.

8.1. Théorème de la réduction modulo p

On rappelle que le groupe de Galois d'un polynôme admet un plongement canonique dans le groupe des permutations des racines de ce polynôme. On a vu que si ce polynôme est séparable de degré n, son groupe de Galois se plonge donc dans S_n.
Soit P un polynôme *unitaire* séparable à coefficients entiers de degré n. Soit p un nombre premier et $\overline{\mathrm{P}}$ l'image de P dans $\mathbf{F}_p[\mathrm{X}]$. Comme P est unitaire, le degré de $\overline{\mathrm{P}}$ est n.

Théorème 8.1.1. — **(De la réduction modulo** p**.)** *Supposons que* $\bar{\mathrm{P}}$ *est séparable. Alors* $\mathrm{Gal}(\mathrm{P}, \mathbf{Q})$ *admet un sous-groupe isomorphe à* $\mathrm{Gal}(\bar{\mathrm{P}}, \mathbf{F}_p)$*. Pour toute permutation dans* $\mathrm{Gal}(\bar{\mathrm{P}}, \mathbf{F}_p) \subset \mathrm{S}_n$*, il existe une permutation dans* $\mathrm{Gal}(\mathrm{P}, \mathbf{Q}) \subset \mathrm{S}_n$ *de même type. En particulier, si* $\bar{\mathrm{P}}$ *est irréductible, il existe un cycle de longueur* n *dans* $\mathrm{Gal}(\mathrm{P}, \mathbf{Q}) \subset \mathrm{S}_n$*.*

Le lecteur peut se contenter dans un premier temps de ce résultat et laisser les preuves pour une seconde lecture (bien qu'elles ne soient pas difficiles).

8.2. Spécialisation du groupe de Galois

Soit P un polynôme *unitaire* séparable à coefficients entiers [2]. Notons

$$\mathrm{A} = \mathbf{Z}[z_1, \cdots, z_n]$$

le sous-anneau de $\mathbf{C}$ engendré par les racines complexes $z_1, \cdots, z_n$ de P. Par construction, tous les z_i sont entiers (6.3.5).

Lemme 8.2.1. — *Le corps des fractions* K *de* A *est le corps de décomposition de* P *dans* $\mathbf{C}$.

2. Le lecteur pourra adapter la preuve au cas où l'anneau de coefficients $\mathbf{Z}$ est remplacé par un anneau factoriel, voire intégralement clos.

Démonstration. — En effet, A est contenu dans le corps de décomposition L de P car $z_i \in \mathrm{L}$ pour tout $i \in \{1, \cdots, n\}$, et donc K est contenu dans L. Par ailleurs, P étant scindé sur K, on a bien $\mathrm{K} = \mathrm{L}$ par minimalité de L. □

L'observation fondamentale est que tous les éléments de A sont entiers. Pour démontrer cela, on va donner une caractérisation des entiers en tout point analogue à celle des nombres algébriques (3.6.1).

8.3. Somme, produits d'entiers

Soit C un anneau (en général C n'est pas **C** !).

Définition 8.3.1. — *Soit* B *une* C*-algèbre. On dit que* $b \in \mathrm{B}$ *est entier sur* C *si* b *annule un polynôme* unitaire *à coefficients dans* C.

Lorsque B est un sous-anneau de **C** vu comme algèbre sur $\mathrm{C} = \mathbf{Z}$, on retrouve la notion d'entier algébrique (6.3.5). On généralise (3.6.1) dans la proposition suivante. On peut se reporter à la section 2.7 pour les définitions des modules sur un anneau.

Proposition 8.3.2. — *Soit* B *une* C*-algèbre et* $b \in \mathrm{B}$. *Alors,* b *est entier sur* C *si et seulement si* b *est contenu dans un sous-anneau* B' *de* B *qui est un* C-module *de type fini.*

On rappelle (2.7) que dire B' *est un* C*-module de type fini* signifie qu'il existe une famille finie b_i d'éléments de B' telle que tout élément de B' est combinaison linéaire des b_i à coefficients dans C.

Démonstration. — La partie directe est claire : si b a un polynôme annulateur unitaire de degré d, alors $\mathrm{C} = \mathrm{C}[b]$ est engendré par $1, \cdots, b^{d-1}$. Inversement, supposons $b \in \mathrm{B}'$ de type fini sur C, engendré par $b_1, \cdots, b_n$. Il existe $c_{i,j} \in \mathrm{C}$ tels que $bb_j = \sum_i c_{i,j} b_i$ ($\alpha = (c_{i,j})$ est *une* matrice de l'homothétie $h_b \in \mathrm{End}_{\mathrm{C}}(\mathrm{B}')$ de rapport b dans C). Soit $\mathrm{P} = \det(\mathrm{X}\mathrm{Id} - \alpha)$ le polynôme caractéristique de α : c'est un polynôme unitaire de C[X] qui annule α (théorème de Cayley-Hamilton) et donc *a fortiori* h_b. Mais, on a $0 = \mathrm{P}(h_b).1 = \mathrm{P}(b)$, ce qu'on voulait. □

Comme en (3.6.7), on en déduit

Corollaire 8.3.3. — *L'ensemble des éléments de* B *qui sont entiers sur* C *est un sous-anneau de* B.

Démonstration. — En effet, si $x, y \in \mathrm{B}$ sont entiers sur C, disons annulés par des polynômes unitaires à coefficients dans C de degré n, m, tant $x-y$ que xy sont contenus dans $\mathrm{C}[x,y]$. Or $\mathrm{C}[x,y]$ est engendré par les monômes $x^i y^j, 0 \leq i \leq n, 0 \leq j \leq m-1$ et donc est de type fini sur C. □

Corollaire 8.3.4. — *L'ensemble des entiers algébriques est un sous-anneau de* $\mathbf{C}$.

En particulier, tous les éléments de A sont des entiers.

Exercice 8.3.5 **(Lemme de Kronecker).** — *Soit z un nombre complexe qui est entier sur $\mathbf{Q}$ et soient $(z_i)_i$ ses conjugués. Montrer que les z_i sont entiers. Montrer que tous les polynômes $\prod_i (\mathrm{X} - z_i^n)$ où $n \in \mathbf{N}$ sont à coefficients entiers. En déduire que si $|z_i| \leq 1$ pour tout i, alors ou bien $z = 0$, ou bien les z_i sont des racines de l'unité.*

8.4. Norme des éléments de A

Pour tout nombre complexe algébrique z sur $\mathbf{Q}$, on définit sa norme $\mathrm{N}(z)$ comme le produit de ses conjugués complexes. Si P est le polynôme minimal de z, on a évidemment la formule

$$\mathrm{N}(z) = (-1)^{\deg(\mathrm{P})}\mathrm{P}(0)$$

de sorte que

$$\mathrm{N}(z) \in \mathbf{Q}.$$

Par exemple, $\mathrm{N}(z) = z$ si $z \in \mathbf{Q}$ alors que $\mathrm{N}(\sqrt{2}) = -2$. Si z est entier, on a donc $\mathrm{N}(z) \in \mathbf{Z}$ puisque $\mathrm{P} \in \mathbf{Z}[\mathrm{X}]$ (6.3.7).

Lemme 8.4.1. — *L'anneau $\bar{\mathrm{A}} = \mathrm{A}/p\mathrm{A}$ est non nul.*

Démonstration. — Supposons le contraire. On aurait alors une écriture $1 = pa, a \in \mathrm{A}$. Or, les $d = \mathrm{card}(\mathrm{Hom}_{\mathbf{Q}}(\mathbf{Q}[a], \mathbf{C}))$ conjugués distincts de a sont les nombres complexes $\sigma(a)$ avec $\sigma \in \mathrm{Hom}_{\mathbf{Q}}(\mathbf{Q}[a], \mathbf{C})$. Comme $\mathbf{Q}[a] = \mathbf{Q}[pa]$, le nombre complexe pa a d conjugués distincts qui sont les $p\sigma(a)$ avec $\sigma \in \mathrm{Hom}_{\mathbf{Q}}(\mathbf{Q}[a], \mathbf{C})$. On en déduit la formule

$$\mathrm{N}(pa) = p^{\deg_{\mathbf{Q}}(a)}\mathrm{N}(a)$$

d'une part, et, d'autre part,

$$\mathrm{N}(pa) = \mathrm{N}(1) = 1.$$

Ceci est absurde car $\mathrm{N}(z) \in \mathbf{Z}$, a étant un nombre entier algébrique d'après 8.3.4. □

8.5. Groupe de décomposition

Soit alors $\bar{\mathfrak{p}}$ un idéal maximal de l'anneau (non nul !) $\bar{\mathrm{A}}$.[3] Alors $k = \bar{\mathrm{A}}/\bar{\mathfrak{p}}$ est un corps. Soit $\mathfrak{p}$ l'image inverse de $\bar{\mathfrak{p}}$ dans A, autrement dit le noyau de la surjection canonique

$$\mathrm{A} \twoheadrightarrow \bar{\mathrm{A}} \twoheadrightarrow k.$$

Comme p est nul dans $\bar{\mathrm{A}} = \mathrm{A}/p\mathrm{A}$, le corps k est de caractéristique p.

Remarque 8.5.1. — *Il est utile d'observer qu'on a* $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$. *En effet,* $\mathfrak{p} \cap \mathbf{Z}/p\mathbf{Z}$ *est le noyau du morphisme* $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z} \to \mathrm{A}/\mathfrak{p}$. *Ce morphisme est injectif, comme tout morphisme de corps.*

Comme $\bar{\mathrm{A}}$ est de dimension finie sur $\mathbf{F}_p$, l'extension $k/\mathbf{F}_p$ est finie, et galoisienne comme toute extension finie de corps finis. De même que A est engendré par les polynômes en les z_i à coefficients des $\mathbf{Z}$, k est engendré par les polynômes en les $x_i = z_i \mod \mathfrak{p}$ à coefficients dans $\mathbf{F}_p$. Autrement dit, on obtient :

Lemme 8.5.2. — *k est le corps de décomposition de* $\bar{\mathrm{P}}$ *sur* $\mathbf{F}_p$.

Ceci, au passage, prouve à nouveau que k est de dimension finie sur $\mathbf{F}_p$.
Maintenant, le groupe de Galois $\mathrm{G} = \mathrm{Gal}(\mathrm{K}/\mathbf{Q})$ permute les z_i et donc laisse stable A.

Définition 8.5.3. — *On appelle groupe de décomposition de* $\mathfrak{p}$ *le sous-groupe* $\mathrm{D} = \mathrm{D}_{\mathfrak{p}}$ *de* G *fixant* $\mathfrak{p}$.

Comme l'action de D sur A laisse $\mathfrak{p}$ globalement invariant, elle définit une action sur le quotient $k = \mathrm{A}/\mathfrak{p}$. On a un donc un morphisme de groupe $\phi : \mathrm{D} \to \mathrm{Gal}(k/\mathbf{F}_p)$.

Théorème 8.5.4. — *Le morphisme ϕ est surjectif.*

Démonstration. — Un élément $\sigma_0 \in \mathrm{Gal}(k/\mathbf{F}_p)$ est déterminé par l'image $y = \sigma_0(x)$ d'un générateur $x \neq 0$ de l'extension $k/\mathbf{F}_p$.

3. On pourra remarquer que son existence est tout à fait indépendante de l'axiome du choix (utiliser par exemple que A est de type fini sur $\mathbf{Z}$).

Les idéaux $g^{-1}(\mathfrak{p})$ sont égaux à $\mathfrak{p}$ si et seulement si $g \in \mathrm{D}$. Par ailleurs, la projection $\mathrm{A} \xrightarrow{g} \mathrm{A} \to \mathrm{A}/\mathfrak{p}$ est surjective car g est bijectif et admet $g^{-1}(\mathfrak{p})$ comme noyau. Ainsi, on a un isomorphisme

$$\mathrm{A}/g^{-1}(\mathfrak{p}) \xrightarrow{\sim} \mathrm{A}/\mathfrak{p}$$

assurant que $g^{-1}(\mathfrak{p})$ est maximal puisque le quotient correspondant est le corps $\mathrm{A}/\mathfrak{p}$.[4] Notons $\mathfrak{q}_1, \cdots, \mathfrak{q}_r$ les idéaux (distincts) de la forme $g^{-1}(\mathfrak{p}), g \notin \mathrm{D}$. Comme $\mathfrak{q}_0 = \mathfrak{p}, \mathfrak{q}_1, \cdots, \mathfrak{q}_r$ sont distinct deux à deux et maximaux, on a $\mathfrak{q}_i + \mathfrak{q}_j = \mathrm{A}$ si $i \neq j$. D'après le lemme chinois (2.8.1), on peut trouver $z \in \mathrm{A}$ tel que

$$z \equiv x \mod \mathfrak{q}_0 \text{ et } z \equiv 0 \mod \mathfrak{q}_i \text{ si } i > 0,$$

et donc

$$z \equiv x \mod \mathfrak{p} \text{ et } z \equiv 0 \mod g^{-1}(\mathfrak{p}) \text{ si } g \notin \mathrm{D}.$$

On a alors $g(z) \in \mathfrak{p}$ si $g \notin \mathrm{D}$. Le polynôme

$$\prod_{g \in \mathrm{G}} (\mathrm{X} - g(z))$$

est à coefficients entiers, ses coefficients étant invariants sous l'action de G et entiers sur $\mathbf{Z}$. Par construction, son image dans $k[\mathrm{X}] = \mathrm{A}/\mathfrak{p}[\mathrm{X}]$ s'écrit

$$\prod_{g \in \mathrm{D}} (\mathrm{X} - \overline{g(z)}) \prod_{g \notin \mathrm{D}} \mathrm{X}$$

et annule $\bar{z} = x$. Comme x est non nul, on déduit que le polynôme de $\mathbf{F}_p[\mathrm{X}]$

$$\prod_{g \in \mathrm{D}} (\mathrm{X} - \overline{g(z)})$$

est divisible par le polynôme minimal

$$\prod_{\sigma \in \mathrm{Gal}(k/\mathbf{F}_p)} (\mathrm{X} - \sigma(x))$$

de x sur k, et que donc il existe $g \in \mathrm{D}$ tel que $\sigma_0(x) = \overline{g(z)}$, ce qu'on voulait. □

Notons $x_1, \cdots, x_n$ les réductions modulo $\mathfrak{p}$ des racines $z_1, \cdots, z_n$ de P.

4. En fait, il n'est pas difficile de prouver que les idéaux premiers non nuls de A sont maximaux, mais on n'en aura pas besoin.

Théorème 8.5.5. — *Supposons que* $\bar{\mathrm{P}}$ *est à racines simples (dans* $\bar{\mathbf{F}}_p$*). Alors,* ϕ *est un isomorphisme du sous-groupe* D *de* $\mathrm{Gal}(\mathrm{P}, \mathbf{Q})$ *sur le groupe* $\mathrm{Gal}(\bar{\mathrm{P}}, \mathbf{F}_p)$*. De plus* ϕ *est compatible avec les plongements des groupes de Galois dans le groupe symétrique* S_n *(cf. 5.a) définis par la numérotation* $\{z_i\}_{1\leq i\leq n}$ *des racines de* P *et* $\{x_i\}_{1\leq i\leq n}$ *des racines de* $\bar{\mathrm{P}}$*.*

Démonstration. — Par hypothèse, les x_i sont distincts. Autrement dit, l'application $z_i \mapsto x_i$ est bijective et induit une identification des groupes de permutations

$$\mathrm{Bij}(\{z_i\}_{1\leq i\leq n}) = \mathrm{Bij}(\{x_i\}_{1\leq i\leq n}).$$

On a un diagramme

(5.a)
$$\begin{array}{ccccc} \mathrm{D} & \longrightarrow & \mathrm{Gal}(k/\mathbf{F}_p) & \hookrightarrow & \mathrm{Bij}(\{x_i\}_{1\leq i\leq n}) \\ \downarrow & & & \nearrow & \\ \mathrm{G} & \hookrightarrow & \mathrm{Bij}(\{z_i\}_{1\leq i\leq n}) & & \end{array}$$

qui commute, c'est-à-dire les deux applications composées à partir de D sont les mêmes. Ceci prouve l'injectivité de ϕ. De plus, on sait déjà que ϕ est surjective. □

Remarque 8.5.6. — *La preuve du lemme donne un peu plus, lorsque les hypothèses sont vérifiées. Si on a une permutation des racines de* $\bar{\mathrm{P}}$*, il existe une permutation des racines de* P *du même type. En particulier, si* $\bar{\mathrm{P}}$ *est irréductible, il existe un cycle de longueur* n *dans* G *d'après le Lemme 7.1.7.*

Voyons enfin que, malgré les apparences, le sous-groupe $\mathrm{D} = \mathrm{D}_{\mathfrak{p}}$ ne dépend que très peu de $\mathfrak{p}$ mais plutôt de p. Donnons nous donc deux idéaux maximaux $\mathfrak{p}$, $\mathfrak{q}$ de A tels que $\mathrm{A}/\mathfrak{p} \xrightarrow{\sim} \mathrm{A}/\mathfrak{q} \xrightarrow{\sim} \mathbf{F}_p$.

Proposition 8.5.7. — *Il existe* $g \in \mathrm{G}$ *tel que* $\mathfrak{p} = g(\mathfrak{q})$*. On a alors* $\mathrm{D}_{\mathfrak{p}} = g\mathrm{D}_{\mathfrak{q}}g^{-1}$*.*

Démonstration. — Pour le premier point, imaginons qu'on ait $\mathfrak{p} \not\subset g(\mathfrak{q})$ pour tout $g \in \mathrm{G}$. On a alors $\mathfrak{p} + g(\mathfrak{q}) = \mathrm{A}$ pour tout g car $\mathfrak{p}$ est maximal. Le lemme chinois (2.8.1) permet de construire alors $x \in \mathrm{A}$ tel que $x \equiv 1 \mod g(\mathfrak{q})$ pour tout g et $x \equiv 0 \mod \mathfrak{p}$. Alors $\mathrm{N} = \prod_{g\in\mathrm{G}} g(x)$ est dans $p\mathbf{Z} = \mathfrak{p} \cap \mathbf{Z} = \mathfrak{q} \cap \mathbf{Z}$. Donc $\mathrm{N} \in \mathfrak{q}$ et donc un des facteurs $g(x)$ est dans $\mathfrak{q}$. Autrement dit $x \equiv 0 \mod g^{-1}(\mathfrak{q})$, contradiction. Le second point s'en déduit aisément. □

En particulier, $D_{\mathfrak{p}}$ et $D_{\mathfrak{q}}$ sont isomorphes (via l'automorphisme intérieur $h \mapsto ghg^{-1}$), et même égaux si G est abélien. Ainsi, le morphisme de Frobenius définit un élément de G unique à conjugaison près, et unique tout court si G est abélien ! C'est le début de la théorie du corps de classes...

Le théorème 8.5.5 permet bien souvent de calculer le groupe de Galois d'un polynôme. On va voir notamment dans la section 8.6 une application à la cyclotomie, et on pourra se reporter à l'Annexe (9.4) pour une application au groupe de Galois d'un polynôme à coefficients entiers.

Tout ceci n'est pas un hasard : on va voir dans le dernier paragraphe (8.7) pourquoi la méthode de réduction modulo p est si efficace.

8.6. Cyclotomie et réduction modulo p

On va montrer ici comment la théorie de la réduction modulo p des groupes de Galois permet de calculer le groupe de Galois de l'extension cyclotomique sur $\mathbf{Q}$ (Chapitre 6) et de redémontrer ainsi l'irréductibilité sur $\mathbf{Q}$ du polynôme cyclotomique.

Soit donc $n \geq 1$ un entier et $\zeta \in \mu_n(\mathbf{C})$ une racine primitive de l'unité (par exemple $\zeta = \exp(\frac{2i\pi}{n})$). Soit $K = \mathbf{Q}[\zeta]$ le corps cyclotomique : c'est le corps des racines de $X^n - 1$. On sait (début du chapitre 6) que K est galoisienne sur $\mathbf{Q}$ et qu'il existe (Section 6.2) un morphisme injectif canonique (le caractère cyclotomique sur $\mathbf{Q}$)

$$\chi_{\mathbf{Q}} : \ G := \mathrm{Gal}(K/\mathbf{Q}) \hookrightarrow (\mathbf{Z}/n\mathbf{Z})^*$$

caractérisé par

$$\forall g \in G, \ g(\zeta) = \zeta^{\chi_{\mathbf{Q}}(g)}. \tag{6.a}$$

On va donc montrer

Théorème 8.6.1. — *$\chi_{\mathbf{Q}}$ est un isomorphisme.*

Démonstration. — Il suffit de montrer que $\chi_{\mathbf{Q}}$ est surjectif. Rappelons que $(\mathbf{Z}/n\mathbf{Z})^*$ est le groupe multiplicatif des classes $\bar{m}$ avec $m \in \mathbf{Z}$ tel que $(m, n) = 1$. En décomposant m en facteurs premiers, on s'aperçoit que le théorème revient à prouver que si p est premier et ne divise pas n, alors $p \in \mathrm{Im}(\chi_{\mathbf{Q}})$.

Soit donc p un nombre premier ne divisant pas n. Soit A le sous-anneau

$$\mathrm{A} = \mathbf{Z}[\zeta]$$

de $\mathbf{C}$. Choisissons $\mathfrak{p}$ un idéal maximal dans A tel que $p \in \mathfrak{p}$ comme dans la section précédente. Comme n est premier à p, le polynôme dérivé de $\mathrm{X}^n - 1$ est un multiple non nul de X^n dans $\mathbf{F}_p[\mathrm{X}]$ de sorte que $\mathrm{X}^n - 1$ est séparable. On peut appliquer la théorie de la réduction des groupes de Galois, et le théorème 8.5.5. On obtient que

$$\mathrm{A} \to k(\mathfrak{p}) := \mathrm{A}/\mathfrak{p}$$

induit un isomorphisme $g \mapsto \bar{g}$ du groupe de décomposition

$$\mathrm{G} \supset \mathrm{D}_\mathfrak{p} \xrightarrow{\sim} \mathrm{Gal}(k(\mathfrak{p})/\mathbf{F}_p)$$

et que $k(\mathfrak{p})$ est le corps des racines de $\mathrm{X}^n - 1$. L'isomorphisme est caractérisé par la relation pour tous $a \in \mathrm{A}$ et $g \in \mathrm{D}_\mathfrak{p}$:

$$g(a \mod \mathfrak{p}) = g(a) \mod \mathfrak{p}. \tag{6.b}$$

Il existe donc un unique élément $\mathrm{F}_\mathfrak{p} \in \mathrm{D}_p$ tel que

$$\overline{\mathrm{F}_\mathfrak{p}} = \mathrm{F} \tag{6.c}$$

où F est le morphisme de Frobenius de $k(\mathfrak{p})$. On a dans $\mathbf{C}[\mathrm{X}]$ la décomposition

$$\mathrm{X}^n - 1 = \prod_{\xi \in \mu_n(\mathbf{C})} (\mathrm{X} - \xi)$$

qui est une égalité dans $\mathrm{A}[\mathrm{X}]$. En la réduisant modulo p, on obtient la décomposition

$$\mathrm{X}^n - 1 = \prod_{\xi \in \mu_n(\mathbf{C})} (\mathrm{X} - \bar{\xi})$$

qui est une égalité dans $k(\mathfrak{p})[\mathrm{X}]$. Comme $\mathrm{X}^n - 1$ est séparable sur $\mathbf{F}_p$, on déduit que le morphisme de réduction modulo $\mathfrak{p}$

$$\begin{cases} \mu_n(\mathbf{C}) & \to & \mu_n(k(\mathfrak{p})) \\ \xi & \mapsto & \bar{\xi} \end{cases}$$

est injectif donc bijectif pour des raisons de cardinal. L'image d'un générateur est donc un générateur de sorte que $\bar{\zeta}$ est une racine primitive $n^{\text{ème}}$ de l'unité dans $k(\mathfrak{p})$. La théorie de

la cyclotomie sur $\mathbf{F}_p$ (Chapitre 6) assure alors qu'il existe un morphisme injectif canonique (le caractère cyclotomique sur $\mathbf{F}_p$)

$$\chi_p : \ \mathrm{D}_\mathfrak{p} = \mathrm{Gal}(k(\mathfrak{p})/\mathbf{F}_p) \hookrightarrow (\mathbf{Z}/n\mathbf{Z})^*$$

caractérisé par

$$\forall \gamma \in \mathrm{D}_\mathfrak{p},\ \gamma(\bar{\zeta}) = \zeta^{\chi_p(\zeta)}. \tag{6.d}$$

En comparant les formules 6.a et 6.d avec 6.c et 6.b, on obtient la formule de compatibilité

$$\forall g \in \mathrm{D}_\mathfrak{p},\ \chi_\mathbf{Q}(g) = \chi_p(\bar{g}).$$

Comme $\mathrm{F}(\bar{a}) = a^p$ pour tout $a \in \mathrm{A}$, on a par définition

$$\chi_p(\mathrm{F}) = p$$

de sorte que $\chi_\mathbf{Q}(\mathrm{F}_\mathfrak{p}) = p$. □

8.7. Le théorème de Cebotarev

Terminons ce voyage par un paragraphe sans preuve, expliquant pourquoi la méthode de réduction modulo p est si efficace.

Soit P un polynôme séparable à coefficients entiers. Soit K le corps des racines de P. C'est une extension galoisienne de $\mathbf{Q}$. Si p est un nombre premier est assez grand (ne divisant ni le coefficient dominant de P ni son discriminant), disons $p > n(\mathrm{P})$, la réduction modulo p $\bar{\mathrm{P}}$ de P est à racines simples. On dispose donc d'un groupe de décomposition $\mathrm{D}_\mathfrak{p} = \mathrm{Gal}(k/\mathbf{F}_p)$ cyclique, engendré par le morphisme de Frobenius, bien défini à conjugaison près. Notons C_p l'ensemble des éléments de $\mathrm{Gal}(\mathrm{P}, \mathbf{Q})$ conjugués à un tel élément (qui ne dépend que de p et pas de $\mathfrak{p}$). Soit alors C une classe de conjugaison d'un élément de G. On peut se demander si C provient de la caractéristique p, autrement dit si $\mathrm{C} = \mathrm{C}_p$. C'est vrai, avec "probabilité" $\operatorname{card}\mathrm{C}/\operatorname{card}\mathrm{G}$ au sens suivant.

Théorème 8.7.1 **(Cebotarev).** — *La limite de la suite*

$$n \mapsto \frac{\operatorname{card}\{p \text{ premiers tels que } \mathrm{C} = \mathrm{C}_p \text{ et } \ n(\mathrm{P}) < p \leq n\}}{\operatorname{card}\{p \text{ premiers tels que } p \leq n\}}$$

existe et vaut $\operatorname{card}\mathrm{C}/\operatorname{card}\mathrm{G}$.

La preuve serait au niveau d'un tel cours, mais utilise des techniques plus fines que celles développées ici.

Par exemple, si $C = \{1\}$, cette "probabilité"[5] vaut $1/\operatorname{card} G$. On s'aperçoit sans peine que la condition C_p trivial signifie $\bar{P}$ scindé. En particulier, ce théorème dit qu'il existe une infinité de p tel que $\bar{P}$ est scindé sur $\mathbf{F}_p$, ce qu'on peut démontrer de manière élémentaire, mais astucieuse. Ce sont "les mauvais nombres premiers p"du point de vue du calcul du groupe de Galois.

FIGURE 2. Nicolas Gregorievich Cebotarev

Exercice 8.7.2. — *Montrer que si un nombre entier est un carré modulo p pour tout nombre premier p assez grand, alors c'est un carré. Montrer un résultat analogue avec des puissances l-ièmes où l est un nombre premier (difficile).*

5. Plus précisément, c'est une densité.

CHAPITRE 9

ANNEXES

9.1. Annexe A - Lemme de Zorn et application

Soit E un ensemble (partiellement) ordonné. On pense par exemple à l'ensemble des parties d'un ensemble donné ordonné par l'inclusion. Mais il y a bien d'autres exemples.

Définition 9.1.1. — *On dit que* E *est inductif si toute partie non vide totalement ordonnée de* E *admet un majorant dans* E.

Exemple 9.1.2. — $\mathbf{R}$ *muni de la relation d'ordre usuelle n'est pas inductif. De même l'ensembles des intervalles* $[0, x[, x \in \mathbf{R}$ *ordonné par l'inclusion n'est pas inductif. En revanche, l'ensemble des parties d'un ensemble ordonné par l'inclusion est inductif.*

Lemme 9.1.3 **(lemme de Zorn)**. — *Tout ensemble non vide inductif admet un élément maximal.*

Ce lemme peut-être vu comme un axiome de la théorie des ensembles, en fait équivalent à l'axiome du choix : si (E_i) est une famille d'ensembles non vide, alors $\prod \mathrm{E}_i$ est non vide. On le considérera comme tel.

Corollaire 9.1.4. — *Tout anneau non nul admet un idéal maximal. Plus généralement, tout idéal propre d'un anneau est contenu dans un idéal maximal.*

FIGURE 1. Max Zorn

Démonstration. — Soit E la famille des idéaux propres de A. Comme A est non nul, $\{0\}$ est dans E qui est non nul. Visiblement, E est inductif : la réunion d'une famille totalement ordonnée d'idéaux propres est encore un idéal propre, qui est un majorant. Le lemme de Zorn termine le travail. En considérant A/I, on obtient que tout idéal propre I est contenu dans un idéal maximal (simplement car les idéaux (resp. idéaux maximaux) de A/I s'identifient aux idéaux (resp. idéaux maximaux) de A contenant I d'après 2.4.6). □

9.2. Annexe B - Groupe de Galois des extensions composées

Dans l'étude des extensions cyclotomiques, on a rencontré le problème de l'étude d'une extension composée KL/k en fonction de K/k et L/k (lorsque ces deux dernières sont des extensions cyclotomiques sur $\mathbf{Q}$). On peut le faire en général (on pourrait d'ailleurs en déduire de cette manière le calcul de $\mathbf{Q}[\zeta_n] \cap \mathbf{Q}[\zeta_m]$ effectué en (6.4.1)).
On suppose que toutes les extensions considérées sont contenues dans une extension algébriquement close Ω d'un corps k.
Si x_i est une famille d'éléments de Ω, l'intersection des sous-corps de Ω contenant les x_i est le plus petit sous-corps de Ω contenant les x_i. Si K, L sont deux extensions de k, le plus petit corps contenant K, L se note KL et s'appelle l'extension composée de K et L.

Lemme 9.2.1. — *Soit* K *un extension finie de* k. *Il existe un unique sous-corps de* Ω *contenant* K *qui est galoisien sur* k *: on l'appelle la clôture galoisienne de* K/k.

Démonstration. — L'intersection de deux extensions galoisiennes de k est visiblement encore galoisienne. L'unicité en découle. Pour l'existence, choisissons un élément primitif x de K/k (rappelons que k est parfait). Le corps des racines du polynôme minimal de x sur k est l'extension cherchée. □

Théorème 9.2.2. — *Soient* K, L *deux extensions finies de* k *et supposons* K/k *galoisienne.*

i) Alors, KL/L *est galoisienne et le morphisme de restriction* $r : \mathrm{Gal}(\mathrm{KL}/\mathrm{L}) \to \mathrm{Gal}(\mathrm{K}/\mathrm{K} \cap \mathrm{L})$ *est un isomorphisme.*

ii) Si de plus L/k *est galoisienne, alors* KL/k *et* $\mathrm{K} \cap \mathrm{L}/k$ *le sont également.*

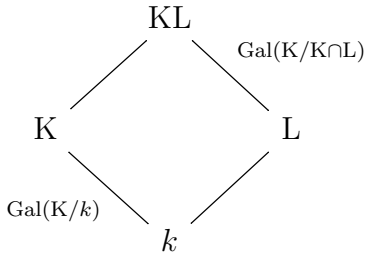
Démonstration. — i). Soit x un élément primitif de K/k de polynôme minimal $\mathrm{P} \in k[\mathrm{X}]$. Visiblement, $\mathrm{KL} = \mathrm{L}[x]$ et le polynôme minimal Q de x sur L divise P de sorte que ses racines sont dans K (comme celles de P) et *a fortiori* dans KL. Comme P est à racines simples, ceci prouve que KL/L est galoisienne. Plus précisément, on a $\mathrm{Q} = \prod(\mathrm{X} - x_i)$ où $x_i \in \mathrm{K}$ sont certains conjugués de x. Donc Q est aussi dans $\mathrm{K}[\mathrm{X}]$ ce qui prouve qu'on a $\mathrm{Q} \in (\mathrm{K} \cap \mathrm{L})[\mathrm{X}]$.
Prouvons la surjectivité de r. Soit alors $g \in \mathrm{Gal}(\mathrm{K}/\mathrm{K} \cap \mathrm{L})$. On a $g(\mathrm{Q}(x)) = \mathrm{Q}(g(x))$ car Q est à coefficients dans $\mathrm{K} \cap \mathrm{L}$. Par propriété universelle du quotient, il existe un

unique L-endomorphisme de KL = L[X]/Q qui envoie $x = (\mathrm{X} \mod \mathrm{Q})$ sur $g(x)$: c'est l'antécédent cherché.

Prouvons l'injectivité de r. Soit alors $g \in \mathrm{Gal}(\mathrm{KL}/\mathrm{L})$ dans le noyau, c'est-à-dire trivial sur K. Comme g est trivial sur L et que K, L engendrent KL, il est trivial sur KL, ce qu'on voulait.

ii). Supposons de plus L galoisienne. Alors, L est le corps des racines d'un polynôme séparable $\mathrm{P}_1 \in k[\mathrm{X}]$ et KL est le corps des racines du polynôme séparable $\mathrm{PPCM}(\mathrm{P}, \mathrm{P}_1)$, prouvant que KL/k est galoisienne. Pour le dernier point, soit $\sigma \in \mathrm{Hom}_k(\mathrm{K} \cap \mathrm{L}, \Omega)$ qu'on prolonge à KL tout entier. Comme K, L sont galoisiennes sur k, on a $\sigma(\mathrm{K}) \subset \mathrm{K}$ et $\sigma(\mathrm{L}) \subset \mathrm{L}$ et donc $\sigma(\mathrm{K} \cap \mathrm{L}) \subset \mathrm{K} \cap \mathrm{L}$ d'où l'égalité (car $\mathrm{K} \cap \mathrm{L}$ est de dimension finie sur k). □

Le point i) du théorème peut être représenté graphiquement :



Corollaire 9.2.3. — *Sous les hypothèses du théorème, on a*

$$[\mathrm{KL} : \mathrm{L}] = [\mathrm{K} : \mathrm{K} \cap \mathrm{L}] \text{ et } [\mathrm{KL} : k] = [\mathrm{K} : k][\mathrm{L} : k]/[\mathrm{K} \cap \mathrm{L} : k].$$

Par suite, $[\mathrm{KL} : k] = [\mathrm{K} : k][\mathrm{L} : k]$ *si et seulement si* $k = \mathrm{K} \cap \mathrm{L}$.

Démonstration. — Le premier point découle du point *ii*) précédent. Pour le second, on écrit alors

$$[\mathrm{KL} : k] = [\mathrm{KL} : \mathrm{L}][\mathrm{L} : k] = [\mathrm{K} : \mathrm{K} \cap \mathrm{L}][\mathrm{L} : k] = ([\mathrm{K} : k]/[\mathrm{K} \cap \mathrm{L} : k])[\mathrm{L} : k].$$

Le troisième en découle. □

Notons $i : \mathrm{Gal}(\mathrm{KL}/k) \to \mathrm{Gal}(\mathrm{K}/k) \times \mathrm{Gal}(\mathrm{L}/k)$ le morphisme de restriction, qui est visiblement injectif. Les morphismes de restriction

$$\mathrm{Gal}(\mathrm{K}/k) \to \mathrm{Gal}(\mathrm{K} \cap \mathrm{L}/k) \text{ et } \mathrm{Gal}(\mathrm{L}/k) \to \mathrm{Gal}(\mathrm{K} \cap \mathrm{L}/k)$$

définissent un morphisme

$$(j_1, j_2) : \mathrm{Gal}(\mathrm{K}/k) \times \mathrm{Gal}(\mathrm{L}/k) \to \mathrm{Gal}(\mathrm{L} \cap \mathrm{K}/k) \times \mathrm{Gal}(\mathrm{L} \cap \mathrm{K}/k).$$

Bien entendu, $j_1 \circ i$ et $j_2 \circ i$ coïncident avec le morphisme de restriction naturel

$$\mathrm{Gal}(\mathrm{KL}/k) \to \mathrm{Gal}(\mathrm{K} \cap \mathrm{L}/k).$$

Proposition 9.2.4. — *Supposons* K/k *et* L/k *galoisiennes. Le morphisme (injectif)* i *induit un isomorphisme de* $\mathrm{Gal}(\mathrm{KL}/k)$ *sur le sous-groupe*

$$\mathrm{Gal}(\mathrm{K}/k) \times_{\mathrm{Gal}(\mathrm{K}\cap\mathrm{L}/k)} \mathrm{Gal}(\mathrm{L}/k)$$

de $\mathrm{Gal}(\mathrm{K}/k) \times \mathrm{Gal}(\mathrm{L}/k)$ *constitué des couples* (u, v) *tels que* $j_1(u) = j_2(v)$ *(ce sous-groupe est appelé produit amalgamé).*

Démonstration. — Il suffit de montrer que les cardinaux des deux groupes en question sont égaux. On note $\mathrm{G_L}, \mathrm{G_K} \cdots$ les groupes de Galois sur k. On a une suite exacte

$$1 \to \mathrm{N} \to \mathrm{G_K} \times \mathrm{G_L} \overset{(j_1,j_2)}{\to} \mathrm{G_{K\cap L}} \times \mathrm{G_{K\cap L}} \to 1$$

(noter que j_1, et *a fortiori* (j_1, j_2), est surjectif). Par construction, notre produit amalgamé G est l'image inverse par (j_1, j_2) du sous groupe diagonal

$$\mathrm{G_{K\cap L}} = \{(g, g), g \in \mathrm{G_{K\cap L}}\} \subset \mathrm{G_{K\cap L}} \times \mathrm{G_{K\cap L}}.$$

On a donc une suite exacte

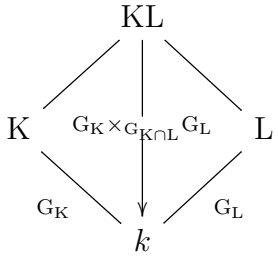
$$1 \to \mathrm{N} \to \mathrm{G} \to \mathrm{G_{K\cap L}} \to 1.$$

Comparant les cardinaux, on en déduit

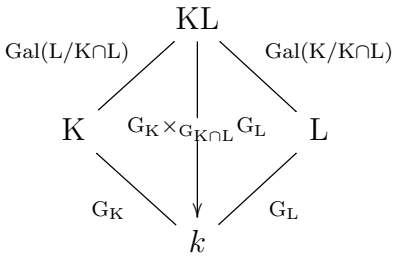
$$\mathrm{card}\, \mathrm{G} = [\mathrm{K} : k][\mathrm{L} : k]/[\mathrm{K} \cap \mathrm{L} : k]$$

et on conclut grâce à 9.2.3. □

Cet énoncé est très agréable lorsque de plus $\mathrm{K} \cap \mathrm{L} = k$, de sorte que le produit amalgamé n'est autre que le produit usuel.
Le théorème peut être représenté graphiquement comme suit



qu'on peut compléter d'après ce qui précède en



9.3. Annexe C - Transcendance de e et π

Les méthodes de preuve de la transcendance de e et π sont analogues.
Soit P un polynôme de degré m à coefficients réels et $\tilde{\mathrm{P}}$ le polynôme déduit de P en remplaçant ses coefficients par leur valeur absolue. Posons alors

$$\mathrm{I}(t) = \int_0^t \mathrm{e}^{t-u}\mathrm{P}(u)\mathrm{d}u.$$

On a (intégrations par parties)

$$\mathrm{I}(t) = \mathrm{e}^t \sum_{j=0}^{m} \mathrm{P}^{(j)}(0) - \sum_{j=0}^{m} \mathrm{P}^{(j)}(|t|) \tag{3.a}$$

et

$$|\mathrm{I}(t)| \leq |t|\mathrm{e}^{|t|}\tilde{\mathrm{P}}(|t|). \tag{3.b}$$

9.3.1. Transcendance de e. — Supposons que e est algébrique. On a alors

$$\sum_{i=0}^{n} a_i \mathrm{e}^i = 0 \tag{3.1.a}$$

avec $n, a_0 > 0$ et les a_i entiers. Posons

$$\mathrm{J} = \sum_{k=0}^{n} a_k \mathrm{I}(k).$$

Avec les notations précédentes, les formules (3.a) et (3.1.a) donnent immédiatement

$$\mathrm{J} = -\sum_{j=0}^{m}\sum_{k=0}^{n} a_k \mathrm{P}^{(j)}(k)$$

ce qui assure déjà que J est entier.
On choisit $p > na_0$ premier et on définit

$$\mathrm{P}(\mathrm{X}) = \mathrm{X}^{p-1}(\mathrm{X}-1)^p \cdots (\mathrm{X}-n)^p$$

et donc $m = (n+1)p - 1$.
Par construction, on a
$\mathrm{P}^{(j)}(k) = 0$ si $j < p$ et $k > 0$,
$\mathrm{P}^{(j)}(0) = 0$ si $j < p-1$.

Ainsi

$$\mathrm{J} = -a_0\mathrm{P}^{(p-1)}(0) - \sum_{j=p}^{m}\sum_{k=p}^{n} a_k\mathrm{P}^{(j)}(k).$$

Or, $j!|\mathrm{P}^{(j)}(k)$ pour tous les entiers j, k (formule de Taylor par exemple) de sorte que

$$(p-1)!|\mathrm{J} \text{ et } \mathrm{J} \equiv -a_0\mathrm{P}^{(p)}(0) \mod (p!).$$

Un calcul direct donne de plus

$$a_0\mathrm{P}^{(p-1)}(0)/(p-1)! = \pm a_0(n!)^p.$$

Comme $p > na_0$, il ne divise pas l'entier $a_0\mathrm{P}^{(p-1)}(0)/(p-1)!$ qui est donc non nul, donc ≥ 1. On a donc l'inégalité

$$|\mathrm{J}| \geq (p-1)!$$

Un calcul direct montre d'autre part qu'on a

$$\tilde{\mathrm{P}}(k) \leq (2n)^m$$

pour $0 \leq k \leq n$. En remplaçant dans (3.b), on déduit l'existence de c ne dépendant que des a_i et de n (et pas de p) tel que

$$|\mathrm{J}| \leq c^p$$

pour tout p premier assez grand, ce qui contredit $|\mathrm{J}| \geq (p-1)!$.

9.3.2. Transcendance de π. — Supposons que π est algébrique sur $\mathbf{Q}$, donc $i\pi$ également. Soient $\alpha_1, \cdots, \alpha_d$ les conjugués de $i\pi$ et G le groupe de Galois sur $\mathbf{Q}$ du corps qu'ils engendrent. Si $\mathrm{N} > 0$ est un dénominateur commun des coefficients du polynôme minimal de $i\pi$, les $\mathrm{N}\alpha_j$ sont des entiers algébriques. Pour tout $\epsilon = (\epsilon_i) \in \{0,1\}^d$, posons

$$\alpha_\epsilon = \sum_j \epsilon_j\alpha_j.$$

On a

$$0 = \prod_j (1+\exp(\alpha_j)) = \sum_\epsilon \exp(\alpha_\epsilon) = q + \sum_{\epsilon\in\mathrm{A}} \exp(\alpha_\epsilon) \tag{3.2.a}$$

où $\mathrm{A} = \{\epsilon | \alpha_\epsilon \neq 0\}$ et $q = 2^d - \mathrm{card}(\mathrm{A}) = 2^d - n > 0$. Notons $a_1, \cdots, a_n$ les n éléments de A.

Lemme 9.3.1. — *Soit* $\mathrm{S} \in \mathbf{Z}[\mathrm{X}_1, \cdots, \mathrm{X}_n]$ *un polynôme symétrique en les* X_i. *Alors,* $s = \mathrm{S}(\mathrm{N}a_1, \cdots, \mathrm{N}a_n) \in \mathbf{Z}$.

Démonstration. — Comme G permute les α_j, il permute aussi les éléments de A. Ceci entraîne que s est fixé par G donc est rationnel (5.4.1). Mais S est aussi un entier algébrique, donc est dans $\mathbf{Z}$ (8.3). □

On procède comme plus haut avec

$$\mathrm{P}(\mathrm{X}) = \mathrm{N}^{np}\mathrm{X}^{p-1}(x - a_1)^p \cdots (\mathrm{X} - a_n)^p$$

où p est un nombre premier qui a vocation à devenir grand et $m = (n+1)p+1$. Grâce à (3.a) et (3.2.a), on a

$$\mathrm{J} := \mathrm{I}(a_1) + \cdots + \mathrm{I}(a_n) = -q\sum_{j=0}^{m} \mathrm{P}^{(j)}(0) - \sum_{j=0}^{m}\sum_{k=1}^{n} \mathrm{P}^{(j)}(a_k).$$

On procède exactement comme plus haut en constatant que 0 et β_i sont des racines d'ordre supérieur ou égal à $p-1$, ce qui, grâce au lemme 9.3.1, assure

$$(p-1)!|\mathrm{J}.$$

Comme plus haut, on doit montrer que p ne divise pas l'entier relatif (9.3.1)

$$q\mathrm{P}^{(p-1)}(0)/(p-1)! = \pm q\mathrm{N}^{np-n}(\mathrm{N}a_1 \cdots \mathrm{N}a_n)$$

ce qui est le cas si p est assez grand. Ainsi, $|\mathrm{J}/(p-1)!|$ est entier et non nul donc ≥ 1. De même que plus haut, on obtient grâce à (3.b) l'existence d'une constante c indépendante de p telle $|\mathrm{J}| \leq c^p$ ce qui contredit $|\mathrm{J}| \geq (p-1)!$ pour p assez grand.

9.4. Annexe D - Groupe de Galois sur Q d'un polynôme à coefficients entiers

Le but de cette partie est d'étudier le groupe de Galois sur $\mathbf{Q}$ de polynômes à coefficients entiers.
D'abord, montrons le lemme suivant, généralisation du Lemme 7.1.7.

Lemme 9.4.1. — *Soient* $\mathrm{P}_1, \cdots, \mathrm{P}_r \in \mathbf{F}_p[\mathrm{X}]$ *de degré respectifs* $d_1, \cdots, d_r > 0$, *irréductibles, premiers entre eux deux à deux. Soit* K *le corps de décomposition de* $\prod_{1 \leq i \leq r} \mathrm{P}_i$, $\mathrm{G} = \mathrm{Gal}(\mathrm{K}, \mathbf{F}_p)$ *et* $\mathrm{F} \in \mathrm{G}$ *le morphisme de Frobenius de* K. *Alors* G *est canoniquement un sous-groupe du groupe produit* $\mathrm{S}_{d_1} \times \cdots \times \mathrm{S}_{d_r}$, F *est un produit de cycles disjoints de longueur* d_i *et* $\mathrm{card}(\mathrm{G}) = \mathrm{PPCM}_{1 \leq i \leq r}(d_i)$.

Démonstration. — Comme P_i est irréductible et $\mathbf{F}_p$ est parfait, P_i est séparable. Pour $1 \leq i \leq r$, soit $(z_{i,j})_{1 \leq j \leq d_i}$ les racines de P_i dans $\bar{\mathrm{F}}_p$. Les polynômes étant premiers entre eux, les $z_{i,j}$ sont tous distincts. Comme G agit sur chaque ensemble $(z_{i,j})_{1 \leq j \leq d_i}$, on peut plonger G dans le groupe produit $\mathrm{S}_{d_1} \times \cdots \times \mathrm{S}_{d_r}$ où l'on identifie $\mathrm{S}_{d_i} = \mathrm{Bij}(z_{i,1}, \cdots, z_{i,d_i})$. Comme P_i est un polynôme irréductible, P_i est le polynôme minimal de $z_{i,1}$ sur $\mathbf{F}_p$ et ses racines sont les conjugués de $z_{i,1}$. Le corps $\mathbf{F}_p$ étant fini, G est engendré par le Frobenius F (4.2.3). Les conjugués de $z_{i,1}$ sont donc exactement les $\mathrm{F}^n(z_{i,1}), n = 0, \cdots, d_i - 1$. Soit γ_i le cycle $(z_{i,1}, \mathrm{F}(z_{i,1}), \cdots, \mathrm{F}^{d_i - 1}(z_{i,1}))$ dans $\mathrm{S}_{d_i} = \mathrm{Bij}(z_{i,1}, \cdots, z_{i,d_i})$. On a par construction $\mathrm{F} = \gamma_1 \times \cdots \times \gamma_r$ vu dans $\mathrm{S}_{d_1} \times \cdots \times \mathrm{S}_{d_r}$. Comme les γ_i commutent deux à deux (ils sont à supports disjoints), on a $\mathrm{F}^n = \prod_{1 \leq i \leq r} \gamma_i^n$ pour tout $n \geq 0$. Ceci assure que F est d'ordre le PPCM des d_i. Comme F engendre G, on en déduit que $\mathrm{card}(\mathrm{G}) = \mathrm{PPCM}_{1 \leq j \leq r}(d_i)$. □

Soit maintenant P un polynôme à coefficients entiers de degré $n \geq 3$. On suppose qu'il existe 3 nombres premiers p_0, p_1, p_2 tels que pour $0 \leq i \leq 2$, la réduction de P modulo p_i a un unique facteur irréductible de degré inférieur ou égal à d_i, avec $d_0 = n$, $d_1 = n - 1$ et $d_2 = 2$.

Proposition 9.4.2. — *Le groupe de Galois de* P *sur* $\mathbf{Q}$ *est* S_n.

Démonstration. — Le Théorème 8.5.5 et le Lemme 9.4.1 assurent que le groupe de Galois $\mathrm{G} \subset \mathrm{S}_n$ contient un n-cycle, un $n - 1$ cycle et une transposition. On conclut grâce à 1.5.5. □

En fait, en raffinant (à peine) la preuve précédente, on peut montrer, qu'en un sens convenable, la probabilité [1] pour qu'un polynôme à coefficients entiers de degré n donné ait pour groupe de Galois sur $\mathbf{Q}$ le groupe S_n est 1 (voir [**B2**, Exercice V.12.13]) !

1. On devrait plutôt parler de *densité*.

9.5. Annexe E - Polynômes symétriques

Le groupe symétrique S_n agit par permutation des indices sur l'anneau $\mathbf{C}[\mathrm{X}_1, \cdots, \mathrm{X}_n]$ des polynômes à n inderterminées $\mathrm{X}_1, \cdots, \mathrm{X}_n$. Un polynôme symétrique est un polynôme dans $\mathbf{C}[\mathrm{X}_1, \cdots, \mathrm{X}_n]$ fixe pour l'action de S_n. L'anneau des polynômes symétriques est ainsi l'ensemble des points fixe pour l'action de S_n, c'est-à-dire $(\mathbf{C}[\mathrm{X}_1, \cdots, \mathrm{X}_n])^{\mathrm{S}_n}$ (on vérifie immédiatement que c'est bien un sous-anneau).

Par exemple, les polynômes symétriques élémentaires σ_i définis par la formule (4.a) sont bien dans $(\mathbf{C}[\mathrm{X}_1, \cdots, \mathrm{X}_n))^{\mathrm{S}_n}$, car le produit $\prod_{i=1}^{n}(\mathrm{X} - \mathrm{X}_i)$ est clairement fixé par l'action de S_n sur ses coefficients. Notons que $\sigma_n = \mathrm{X}_1\mathrm{X}_2 \cdots \mathrm{X}_n$ et $\sigma_1 = \mathrm{X}_1 + \mathrm{X}_2 + \cdots + \mathrm{X}_n$.

Théorème 9.5.1 **(Théorème des polynômes symétriques)**

L'anneau des polynômes symétriques est engendré par les polynômes symétriques élémentaires :

$$(\mathbf{C}[\mathrm{X}_1, \cdots, \mathrm{X}_n])^{\mathrm{S}_n} = \mathbf{C}[\sigma_1, \cdots, \sigma_n].$$

Démonstration. — Le degré d'un polynôme symétrique est le degré maximal d des monômes $\mathrm{X}_1^{d_1} \cdots \mathrm{X}_n^{d_n}$ qui le composent avec $d = d_1 + \cdots d_n$. On peut alors démontrer le résultat par récurrence sur n et sur d comme dans [**L**, IV, 6]. Le résultat pour $n = 1$ est trivial. Soit $\mathrm{P}(\mathrm{X}_1, \cdots, \mathrm{X}_n)$ symétrique de degré d. Alors $\mathrm{P}(\mathrm{X}_1, \cdots, \mathrm{X}_{n-1}, 0)$ est symétrique en les $\mathrm{X}_1, \cdots, \mathrm{X}_{n-1}$. D'après l'hypothèse de récurrence sur n, on a donc $\mathrm{P}(\mathrm{X}_1, \cdots, \mathrm{X}_{n-1}, 0) = \mathrm{Q}(\sigma'_1, \cdots, \sigma'_{n-1})$ avec Q polynôme de $n-1$ variables et $\sigma'_1, \cdots, \sigma'_{n-1}$ les polynôme symétriques élémentaires en les $\mathrm{X}_1, \cdots, \mathrm{X}_{n-1}$. Notons que σ'_i est obtenu à partir de σ_i en posant $\mathrm{X}_n = 0$. Maintenant considérons

$$\tilde{\mathrm{P}}(\mathrm{X}_1, \cdots, \mathrm{X}_n) = \mathrm{P}(\mathrm{X}_1, \cdots, \mathrm{X}_n) - \mathrm{Q}(\sigma_1, \cdots, \sigma_{n-1}).$$

C'est un polynôme symétrique tel que $\tilde{\mathrm{P}}(\mathrm{X}_1, \cdots, \mathrm{X}_{n-1}, 0) = 0$. Il est donc divisible par X_n, et donc par $\sigma_n = \mathrm{X}_1 \cdots \mathrm{X}_n$ par symétrie, c'est-à-dire $\tilde{\mathrm{P}}(\mathrm{X}_1, \cdots, \mathrm{X}_n) = \sigma_n \tilde{\mathrm{Q}}(\mathrm{X}_1, \cdots, \mathrm{X}_n)$ avec $\tilde{\mathrm{Q}}$ symétrique de degré strictement inférieur à celui de $\tilde{\mathrm{P}}$. L'hypothèse de récurrence sur le degré d permet de conclure. □

Une fraction est invariante par l'action de S_n si et seulement si son numérateur et son dénominateur le sont. En termes de corps des fractions, on a donc

$$(\mathrm{Frac}(\mathbf{C}[\mathrm{X}_1, \cdots, \mathrm{X}_n]))^{\mathrm{S}_n} = \mathrm{Frac}((\mathbf{C}[\mathrm{X}_1, \cdots, \mathrm{X}_n])^{\mathrm{S}_n}) = \mathrm{Frac}(\mathbf{C}[\sigma_1, \cdots, \sigma_n]).$$

9.6. Annexe F - Quelques mots de théorie de Galois inverse

Soit $\bar{\mathbf{Q}}$ la clôture algébrique de $\mathbf{Q}$ dans $\mathbf{C}$. La connaissance du groupe de galois *absolu*

$$\mathrm{G} = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$$

a de profondes conséquences arithmétiques.
C'est par exemple en étudiant les propriétés subtiles de certaines représentations linéaires de G dans un $\mathbf{Q}_p$-espace vectoriel V de dimension 2 [2] que Wiles [3] a pu résoudre la fameuse énigme vieille de plus de 350 ans, à savoir donner, entre autres choses, une preuve du théorème de Fermat : si

$$x^n + y^n = z^n \text{ avec } n \geq 3 \text{ et } x, y, z \in \mathbf{Z}, \text{ alors } xyz = 0.$$

FIGURE 2. Andrew Wiles

Il n'est pas question de donner un aperçu de la preuve ici qui dépasse, et de loin, le niveau de ce cours. Pour tenter de comprendre G, on peut déjà se demander quels sont ses quotients finis. C'est ce qu'on appelle la théorie de Galois inverse. C'est un sujet de recherche actif. Donnons-en pour finir ce cours un aperçu. On utilisera sans plus de précaution le principe suivant, déduit immédiatement de la remarque 5.1.10 :

Proposition 9.6.1. — *Tout quotient du groupe de Galois d'une extension galoisienne de* $\mathbf{Q}$ *est isomorphe à un quotient de* G.

9.6.1. Le cas abélien fini. — Nous allons prouver l'énoncé suivant.

Proposition 9.6.2. — *Tout groupe abélien fini est isomorphe à un quotient de* G.

2. C'est-à-dire des morphismes de groupe de G vers GL(V).
3. 1953-

Démonstration. — Le groupe de Galois G_n de l'extension cyclotomique est $(\mathbf{Z}/n\mathbf{Z})^*$. Pour montrer que tout groupe abélien fini est quotient de G, il suffit de prouver que tout groupe abélien est quotient de $H = (\mathbf{Z}/n\mathbf{Z})^*$ pour n convenable.
Supposons que $n = p_1 \cdots p_m$ est un produit de nombres premiers distincts. D'après le lemme chinois et 4.2.1, H est isomorphe au groupe produit

$$(\mathbf{Z}/(p_1 - 1)\mathbf{Z}) \times \cdots \times (\mathbf{Z}/(p_m - 1)\mathbf{Z}).$$

Si N_i est un entier divisant $p_i - 1$, le morphisme de réduction $\bmod N_i$ réalise $\mathbf{Z}/N_i\mathbf{Z}$ comme un quotient de $\mathbf{Z}/(p_i - 1)\mathbf{Z}$. Ainsi, si $N_1, \cdots, N_m$ sont des entiers divisant respectivement $p_1 - 1, \cdots, p_m - 1$, on déduit que $\Pi = \prod_i \mathbf{Z}/N_i\mathbf{Z}$ est un quotient de H.
Maintenant, donnons nous $N_1, \cdots, N_m$ des entiers strictement positifs. Le théorème de la progression arithmétique de Dirichlet (cf. Exercice 6.3.11) assure qu'on peut trouver des nombres premiers arbitrairement grands dans chacune des progressions arithmétiques $1 + \lambda N_i, \lambda \in \mathbf{N}$. On peut donc choisir $p_1, \cdots, p_m$ distincts tels que $N_i | p_i - 1$ pour tout i, assurant que Π est bien un quotient de H, donc de G.
Or, il n'est pas très difficile de montrer que tout groupe abélien fini est produit de groupes cycliques. □

9.6.2. Le premier cas non abélien non trivial. — Le seul groupe non abélien d'ordre ≤ 7 est $S_3 = D_6$ qui est le groupe de Galois de $X^3 - 2$ (7.2.2), donc est quotient de G (voir (1.3.4) pour la définition de D_n). Il y a 5 groupes d'ordre 8. Trois sont abéliens, à savoir

$$\mathbf{Z}/8\mathbf{Z}, \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}, \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z},$$

et deux ne le sont pas, à savoir

$$D_8, H_8.$$

Le groupe H_8, dit des quaternions, est le groupe ayant huit éléments

$$1, i, j, k, t, ti, tj, tk,$$

où t est central [4] et

$$t^2 = 1, \text{ et } i^2 = j^2 = k^2 = ijk = t.$$

4. t commute avec tous les éléments du groupe.

On a vu que D_8 est le groupe de Galois de $X^4 - 2$, de sorte que D_8 est quotient de G. Pour les distinguer, il suffit de constater que D_8 a 5 éléments d'ordre 2 tandis que H_8 n'en a qu'un, qui engendre son centre (le sous-groupe des éléments centraux).
On a alors l'exercice suivant.

Exercice 9.6.3. — *On se propose de montrer que l'extension de corps*

$$\mathbf{Q}(\sqrt{(2+\sqrt{2})(3+\sqrt{6})})/\mathbf{Q}$$

est galoisienne avec pour groupe de Galois le groupe H_8.
(1) Posons $a = (2+\sqrt{2})(3+\sqrt{6})$, *et soit* $K = \mathbf{Q}(a)$ *: expliquer pourquoi l'extension* $\mathbf{Q}$ *est galoisienne de groupe de Galois produit de deux groupes cycliques d'ordre 2. On notera*

$$si, sj, sk \in \mathrm{Gal}(K/\mathbf{Q})$$

les trois éléments non triviaux.
(2) Montrer que pour chaque $\sigma = \sigma_i, \sigma_j, \sigma_k$ *la quantité* $\sigma(a)/a$ *est le carré d'un élément K que l'on précisera.*
(3) Soit $d = \sqrt{a}$ *et* $L = \mathbf{Q}(d)$. *Montrer que* $d \notin K$ *(on pourra utiliser la question précédente). Quel est le groupe de Galois de* L/K *? On note* τ *son générateur, qu'on considérera comme un élément de* $\mathrm{Gal}(L/\mathbf{Q})$ *(dont* $\mathrm{Gal}(L/K)$ *est un sous-groupe).*
(4) Définir des automorphismes $\tilde{\sigma}_i$ *et* $\tilde{\sigma}_j$ *de* L *qui prolongent* σ_i *et* σ_j *respectivement. On posera* $\tilde{\sigma}_k = \tilde{\sigma}_i\tilde{\sigma}_j$.
(5) Calculer la loi de groupe et conclure.

9.6.3. Le cas réductif fini. — La suite exacte fondamentale (5.a) de la théorie de Galois pourrait laisser croire qu'on déduit du cas abélien que tout groupe résoluble est isomorphe au groupe de Galois d'une extension de $\mathbf{Q}$. En fait, il n'en est rien (c'est très délicat).

Théorème 9.6.4 **(Shafarevich** [5]**).** — *Tout groupe fini résoluble est quotient de* G.

5. 1923-

FIGURE 3. Igor Rostilavovich Shafarevich

Il existe de nombreux groupes résolubles non abéliens, comme les groupes diédraux (1.3.4). Les mathématiciens Feit [6] et Thompson [7] ont montré le résultat (très difficile) suivant, qui donne notamment un moyen simple de repérer si certains groupes sont résolubles... Les experts conjecturent qu'en fait tout groupe fini est quotient de G.

***Théorème 9.6.5* (Feit-Thompson).** — *Tout groupe d'ordre impair est résoluble.*

FIGURE 4. Walter Feit

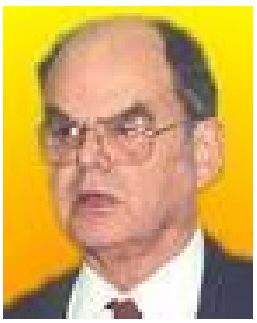


FIGURE 5. John Griggs Thompson

9.6.4. Quelques quotients de G. — Parmi les groupes résolubles on trouve A_n, S_n pour $n \leq 4$. On a vu que S_n est quotient de G (9.4.2). La question de savoir si A_n est quotient de G est très difficile et a été résolue par Hilbert qui a introduit une méthode très puissante pour construire des quotients de G provenant de la géométrie.

***Théorème 9.6.6* (Hilbert).** — *Les groupes alternés sont quotients de* G.

6. 1930-2004
7. 1932-

Il est connu que A_n ($n \geq 5$) est simple, autrement dit qu'il n'a pas de quotient non trivial. Les groupes simples finis sont classifiés. Outre les groupes alternés, on trouve une liste infinie provenant des groupes matriciels à coefficients dans les corps finis, comme par exemple les groupes

$$\mathbf{PSL}_n(\mathbf{F}_q) = \mathbf{SL}_n(\mathbf{F}_q)/\mathbf{F}_q^*$$

et une liste finie de 26 groupes dits sporadiques. Parmi ceux-là, le plus gros d'entre eux, découvert en 1973, s'appelle le "monstre" et a pour cardinal

808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000.

Tous les groupes sporadiques sont quotients de G mis à part une exception : on ne sait pas en janvier 2009 si le groupe de Mathieu [8] M_23, pourtant relativement petit, est quotient de G, même si son cardinal "n'est que" 10 200 960 (comparer à celui du monstre !). En fait, on ne sait même pas en toute généralité, loin s'en faut, si les groupes $\mathbf{GL}_n(\mathbf{F}_q)$, leurs avatars $\mathbf{PSL}_n(\mathbf{F}_q)$, sont quotients de G, même si de nombreux cas sont connus (voir [**V**] pour des résultats dans ce cas, et J.-P. Serre [9] [**S**] pour le problème général). Il semblerait que les experts du sujet ne sachent pas par exemple si les groupes

$$\mathbf{PSL}_2(\mathbf{F}_{5^3}) \text{ ou } \mathbf{GL}_4(\mathbf{F}_{2^2})$$

sont quotients de G.

FIGURE 6. Jean-Pierre Serre

8. 1835-1890
9. 1926-

CHAPITRE 10

CORRECTIONS SOMMAIRES D'EXERCICES

Correction sommaire de l'exercice 1.3.5

Le morphisme surjectif det : $\mathbf{GL}_n(\mathbf{C}) \to \mathbf{C}^*$ envoie $\mathbf{SL}_n(\mathbf{C})$ sur $\{1\}$ et donc induit une surjection $\delta : \mathbf{GL}_n(\mathbf{C})/\mathbf{SL}_n(\mathbf{C}) \twoheadrightarrow \mathbf{C}^*$. Dire $\delta(\mathrm{M} \mod \mathbf{SL}_n(\mathbf{C})) = 1$, c'est dire $\delta(\mathrm{M}) = 1$, prouvant que δ est injectif, donc que δ est un isomorphisme puisqu'on sait qu'il est surjectif.

Correction sommaire de l'exercice 1.5.5

Si $x = \sigma(a_i)$, on a

$$\sigma(a_1, \cdots, a_k)\sigma^{-1}(x) = \sigma(a_1, \cdots, a_k)(a_i) = \sigma(a_{i+1})$$

pour $i \in \mathbf{Z}/k\mathbf{Z}$.

Soit S le groupe engendré par les $(i, i+1)$. On déduit la formule

$$(i+1, j)(i, i+1)(i+1, j) = (i, j)$$

pour tout $j \neq i, i+1$ qui montre (par récurrence) $(i, j) \in \mathrm{S}$ pour tout j et donc $\mathrm{S} = \mathrm{S}_n$ puisque les transpositions engendrent S_n.

De même, la formule $(1, \cdots, n)^j(1, 2)(1, \cdots, n)^j = (j, j+1)$ prouve que $(1, 2)$ et $(1, \cdots, n)$ engendrent S_n d'après ce qui précède.

Enfin, supposons qu'un sous-groupe S contienne un n-cycle, une transposition et un $(n-1)$-cycle. Quitte à renuméroter, on peut supposer $c = (1, \cdots, n) \in \mathrm{S}$. Soit $t = (i, j), i < j$ une transposition dans S. Quitte à conjuguer par c, on peut supposer $t = (1, j)$. Soit γ un $(n-1)$-cycle de S et soit a l'unique point fixé par γ. Quitte à conjuguer par c^{n-a+1}, on peut supposer $a = 1$. Il existe alors $d \in \mathbf{Z}$ tel que $\gamma^d(j) = 2$ puisque γ induit un

$(n-1)$-cycle de $\mathrm{S}_{n-1} = \mathrm{Bij}(\{2, \cdots, n\})$. Mais $\gamma^d(1,j)\gamma^{-d} = (1,2)$ de sorte que $(1,2) \in \mathrm{S}$ et on conclut avec le point précédent.

Correction sommaire de l'exercice 1.5.8

Supposons H d'indice 2. Soit $g \in \mathrm{G}$. On doit montrer $g\mathrm{H} = \mathrm{H}g$. Si $g \in \mathrm{H}$, c'est clair. Sinon, $g\mathrm{H} \neq \mathrm{H}$ et $\mathrm{H}g \neq \mathrm{H}$. Mais G/H est de cardinal 2, donc égal à $\{\mathrm{H}, g\mathrm{H}\}$. Comme G est réunion disjointe de ses classes à droites, on a $g\mathrm{H} = \mathrm{G} - \mathrm{H}$. De même, $\mathrm{H}g = \mathrm{G} - \mathrm{H}$, et donc $g\mathrm{H} = \mathrm{H}g$. Soit alors γ l'unique élément non neutre du groupe G/H. Il existe un unique isomorphisme $\mathrm{G/H} \xrightarrow{\sim} \{\pm 1\}$: il envoie γ sur -1. Si $\mathrm{G} = \mathrm{S}_n$, comme les transpositions sont conjuguées, leurs images dans le groupe *abélien* $\{\pm 1\} = \mathrm{G/H}$ est soit toujours 1 soit toujours -1. Comme les transpositions engendrent $\mathrm{G} = \mathrm{S}_n$, ce ne peut être 1 car sinon le morphisme quotient ne serait pas surjectif. L'image est donc -1 et donc le morphisme quotient est la signature. Son noyau H est donc A_n, ce qu'on voulait.

Correction sommaire de l'exercice 1.6.2

Il est bien connu (utiliser le pivot de Gauss) que $\mathbf{SL}_n(\mathbf{C})$ est engendré par les transvections $\mathrm{T}_{i,j}(\lambda) = \mathrm{I} + \lambda \mathrm{E}_{i,j}, i \neq j, \lambda \neq 0$ et que deux transvections sont conjuguées dans $\mathbf{SL}_n(\mathbf{C})$. Donc, il existe $\mathrm{P} \in \mathbf{SL}_n(\mathbf{C})$ tel que

$$(\mathrm{T}_{i,j}(\lambda))^2 = \mathrm{T}_{i,j}(2\lambda) = \mathrm{P}\mathrm{T}_{i,j}(\lambda)\mathrm{P}^{-1}$$

de sorte que $\mathrm{T}_{i,j}(2\lambda)$ est le commutateur $[\mathrm{P}, \mathrm{T}_{i,j}(\lambda)]$. Comme les transvections engendrent $\mathbf{SL}_n(\mathbf{C})$, on a $\mathrm{D}(\mathbf{SL}_n(\mathbf{C})) = \mathbf{SL}_n(\mathbf{C})$. Notons au passage que l'argument vaut en remplaçant $\mathbf{C}$ par n'importe quel corps de caractéristique différente de 2.

Correction sommaire de l'exercice 1.6.8

1) Il suffit d'associer à une matrice triangulaire inversible la suite de ses coefficients diagonaux pour trouver la suite exacte cherchée. On invoque alors (1.6.6).

2) Le premier point est clair. Soit $f \in \mathrm{U}_j$ et $g \in \mathrm{U}$ (voire $g \in \mathrm{B}$ si on veut). Supposons que $\mathrm{Id} + u, \mathrm{Id} + v \in \mathrm{U}_j$. On a

$$\ln((\mathrm{Id} + u)(\mathrm{Id} + v))(\mathrm{F}_i) = (u + v + uv)(\mathrm{F}_i) \subset \mathrm{F}_{i-j} + uv(\mathrm{F}_i).$$

Comme

$$uv(\mathrm{F}_i) \subset \mathrm{F}_{i-2j} \subset \mathrm{F}_{i-j},$$

on a bien $(\mathrm{Id}+u)(\mathrm{Id}+v) \in \mathrm{U}_j$. Comme Id est dans U_j, ce dernier est bien un sous-groupe de U.
Comme $g(\mathrm{F}_i) \subset \mathrm{F}_i$ et $g^{-1}(\mathrm{F}_i) \subset \mathrm{F}_i$ pour tout i, on a

$$gfg^{-1}(\mathrm{F}_i) \subset gf(\mathrm{F}_i) \subset g(\mathrm{F}_{i-j}) \subset \mathrm{F}_{i-j}.$$

Ainsi $\mathrm{U}_i \lhd \mathrm{U}$.
3) Soit $j \geq 1$. Comme $\ln(f)$ laisse stable F_i et F_{i-j-1}, il induit bien une application linéaire $\ln(f)_{i,j}$ du quotient $\mathrm{F}_i/\mathrm{F}_{i-j-1}$. Dire que $\ln(f)_{i,j}$ est nulle, c'est exactement dire $\ln(f)(\mathrm{F}_i) \subset \mathrm{F}_{i-j-1}$.
4) Si, comme plus haut, $\mathrm{Id}+u, \mathrm{Id}+v \in \mathrm{U}_j$, on a

$$uv(\mathrm{F}_i) \subset \mathrm{F}_{i-2j} \subset \mathrm{F}_{i-j-1}$$

et donc est nul en tant qu'endomorphisme de $\mathrm{F}_i/\mathrm{F}_{i-j-1}$. Ceci assure que $f \mapsto \ln(f)_{i,j}$ est un morphisme de U_i dans le groupe additif commutatif $\mathrm{End}(\mathrm{F}_i/\mathrm{F}_{i-j-1})$. D'après 3), le noyau de $\ln_j$ est U_{j-1}.
5) On applique la définition 1.6.1 pour conclure que U est résoluble et donc que B est résoluble d'après 1).

Correction sommaire de l'exercice 1.6.11

Le fait que S_4 opère sur X résulte de la formule (1.5.4) ou de 5.a comme on veut. Si on numérote les éléments de X en décidant que la transposition $(1, i+1)$ apparaît dans x_i, l'opération $\mathrm{S}_4 \to \mathrm{Aut}(\mathrm{X})$ s'identifie à un morphisme $\mathrm{S}_4 \to \mathrm{S}_3$. L'image de $(1,2)$ est $(2,3)$. On en déduit que π est surjective. Comme le groupe $\mathrm{K} = \{\mathrm{Id}\} \cup \mathrm{X} = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ engendré par X est abélien, il est dans le noyau. Pour des raisons de cardinaux, c'est le noyau. On a donc $\mathrm{Ker}(\pi)$ résoluble car abélien et $\mathrm{S}_4/\mathrm{Ker}(\pi) = \mathrm{S}_3$ résoluble de sorte que S_4 est résoluble (1.6.6).

Correction sommaire de l'exercice 2.6.11

Soit $a \in \mathrm{A}$ dont l'image dans A/I est inversible. Par définition, il existe donc $b \in \mathrm{A}, i \in \mathrm{I}$ tels que $ab = 1 + i$. Mais l'inverse de $1+i$ est $\sum_{k=0}^{n-1}(-i)^k$ grâce à la formule de la progression géométrique. Ainsi, a est inversible d'inverse $b/(1+i)$.

Correction sommaire de l'exercice 2.8.3

Décomposons n, d en facteurs premiers :

$$n = \prod p^{n_p},\ d = \prod p^{m_p}, m_p \leq n_p.$$

D'après le lemme chinois, le morphisme

$$(\mathbf{Z}/n\mathbf{Z})^* \to (\mathbf{Z}/d\mathbf{Z})^*$$

est surjectif si et seulement si chaque morphisme

$$(\mathbf{Z}/p^{n_p}\mathbf{Z})^* \to (\mathbf{Z}/p^{m_p}\mathbf{Z})^*$$

l'est. On peut donc supposer $n = p^{n_p}$. Mais alors, $\mathbf{Z}/p^{m_p}\mathbf{Z}$ s'identifie au quotient de $\mathbf{Z}/p^{n_p}\mathbf{Z}$ par l'idéal I engendré par p^{m_p}. Comme $\mathrm{I}^{n_p - m_p} = (0)$, on invoque l'exercice 2.6.11.

Correction sommaire de l'exercice 3.1.8

D'après la propriété universelle du quotient (2.4.4), les morphismes de $\mathbf{R}$-algèbre de $\mathbf{R}[\mathrm{X}]/(\mathrm{P}(\mathrm{X}))$ dans une algèbre A s'identifient aux racines de P dans A. Soit donc $j = \exp(\frac{2i\pi}{3})$. Le morphisme $\mathbf{R}[\mathrm{X}] \to \mathbf{C}$ défini par $\mathrm{X} \mapsto j$ passe au quotient pour donner un morphisme $\mathbf{R}$-linéaire $\mathrm{K} = \mathbf{R}[\mathrm{X}]/(\mathrm{X}^2+\mathrm{X}+1) \to \mathbf{C}$, visiblement surjectif. Il est injectif pour des raisons de dimension par exemple (ou bien comme tout morphisme de corps). De même, on dispose de deux morphismes de $\mathbf{R}$-algèbres $\mathbf{R}[\mathrm{X}]/(\mathrm{X}(\mathrm{X}+1)) \to \mathbf{R}$ qui envoient X sur 0 et -1 respectivement. Le morphisme correspondant $\mathbf{R}[\mathrm{X}]/(\mathrm{X}(\mathrm{X}+1)) \to \mathbf{R}^2$ est visiblement surjectif, et injectif pour des raisons de dimension.

Correction sommaire de l'exercice 3.7.4

Si $\mathrm{P}(l) = 0, l \in \mathrm{L}$, il existe un unique morphisme de k-algèbre de $k[\mathrm{X}]/(\mathrm{P})$ dans L qui envoie X sur l (2.4.4), d'où le premier point. Si P est non constant arbitraire, montrons par récurrence sur n que pour tout polynôme de degré $\leq n$ il existe un sur-corps K de k de degré $\leq n!$ dans lequel P est scindé. Si $n = 0$, c'est clair. Supposons $n > 0$ et l'énoncé vrai pour $n-1$. Écrivons $\mathrm{P} = \mathrm{P}_1\mathrm{P}_2$ avec P_1 irréductible. Soit l une racine de P_1 dans le corps de rupture L de P_1 qui est de degré $\deg(\mathrm{P}_1) \leq n$. On écrit $\mathrm{P}_1 = (\mathrm{X} - l)\mathrm{P}_3$ avec $\mathrm{P}_3 \in \mathrm{L}[\mathrm{X}]$. On a $\deg(\mathrm{P}_2\mathrm{P}_3) \leq n-1$. Par récurrence, il existe un sur-corps K de L de degré $\leq (n-1)!$ tel que $\mathrm{P}_2\mathrm{P}_3$ est scindé dans K. On a $[\mathrm{K} : k] \leq n!$ (3.2.4) et K convient.

Correction sommaire de l'exercice 4.2.5

Soit $n > 0$ et μ_x le polynôme minimal, nécessairement irréductible, d'un générateur x du groupe multiplicatif de $\mathbf{F}_{q^n}^*$. Comme $\mathbf{F}_{q^n} = \mathbf{F}_q[x]$, on a $\deg(\mu_x) = n$, ce qu'on voulait. Si P est irréductible de degré n, le corps de rupture est de degré n sur $\mathbf{F}_q$. Si x est une racine de P dans $\bar{\mathbf{F}}_p$, il s'identifie (3.7.4) à $\mathbf{F}_q[x]$ qui est $\mathbf{F}_{q^n}$ pour des raisons de dimension. Il est indépendant de la racine x de sorte que toutes les racines de P sont dans $\mathbf{F}_q^n$. Ainsi, P est scindé dans son corps de rupture $\mathbf{F}_{q^n}$ qui est donc aussi son corps de décomposition. Comme les racines de P sont simples et dans $\mathbf{F}_{q^n}$, ensemble des racines de $\mathrm{X}^{p^n} - \mathrm{X}$, on a $\mathrm{P}|(\mathrm{X}^{q^n} - \mathrm{X})$.

Correction sommaire de l'exercice 4.6.4

Les éléments $\mathrm{X}^{1/p}, \mathrm{Y}^{1/p}$ sont algébriques de degré p ($\mathrm{T}^p - \mathrm{X}$ est irréductible dans $\mathbf{F}_p(\mathrm{X},\mathrm{Y})[\mathrm{T}]$ d'après 4.4.4). L'extension $k[\mathrm{X}^{1/p}, \mathrm{Y}^{1/p}]/k$ est en particulier finie. La formule

$$\mathrm{P}(\mathrm{X}^{1/p}, \mathrm{Y}^{1/p})^p = \mathrm{P}_p(\mathrm{X},\mathrm{Y})$$

où $\mathrm{P}_p(\mathrm{U},\mathrm{V}) = \sum_{i,j} a_{i,j}^p \mathrm{U}^i\mathrm{V}^j$ avec

$$\mathrm{P}(\mathrm{U},\mathrm{V}) = \sum_{i,j} a_{i,j}\mathrm{U}^i\mathrm{V}^j \in k[\mathrm{U},\mathrm{V}]$$

assure que tout élément de $k(\mathrm{X}^{1/p}, \mathrm{Y}^{1/p})$ est de degré au plus p. Si l'extension en question était monogène, elle serait de degré p de sorte qu'on aurait $k[\mathrm{X}^{1/p}] = k[\mathrm{Y}^{1/p}]$ pour des raisons de dimension. On aurait donc une écriture $\mathrm{X} = \sum a_i(\mathrm{X}^p, \mathrm{Y}^p)\mathrm{Y}^i$ où les a_i sont des fractions rationnelles. En dérivant par rapport à X, on obtient $1 = 0$, une contradiction.

Correction sommaire de l'exercice 6.3.6

Écrivons $x = p/q$ avec p, q premiers entre eux et $q \geq 1$. Alors, x annule un polynôme du type $\mathrm{P}(\mathrm{X}) = \mathrm{X}^n + \sum_{i<n} a_i\mathrm{X}^i, n \geq 1$ avec $a_i \in \mathbf{Z}$. On a donc

$$q^n\mathrm{P}(p/q) = p^n + q\sum_{i<n} a_i p^i q^{n-1-i} = 0,$$

de sorte que $q|p^n$. Comme $\mathrm{PGCD}(p,q) = 1$, ceci force $q = 1$ et donc $x = p \in \mathbf{Z}$.

Correction sommaire de l'exercice 7.2.2

Tout d'abord, le groupe de Galois G d'un polynôme séparable de degré d est contenu dans S_d et n'est trivial que si P est scindé dans k (puisque le degré du corps des racines de P

est le cardinal du groupe de Galois). Ceci règle le degré 2. En degré 3, on peut supposer P sans racine dans k (sinon on a un groupe trivial ou $\mathbf{Z}/2\mathbf{Z}$ d'après ce qui précède), donc irréductible ici. Le cardinal du groupe de Galois est donc divisible 3, et donc est par 3 ou 6. Or, S_3 a un unique sous-groupe de cardinal $3!/2 = 3$ (1.5.8), le groupe alterné $\mathrm{A}_3 = \mathbf{Z}/3\mathbf{Z}$. Si k est de caractéristique impaire, ceci se produit exactement si disc(P) est un carré dans k (7.2.1).

Correction sommaire de l'exercice 7.2.3

La dérivée de $\mathrm{X}^n - 1$ est $n\mathrm{X}^{n-1}$ qui n'a une racine non nulle que si $p|n$. On en déduit immédiatement que P est séparable si et seulement si p et n sont premiers entre eux.
En général, si $\mathrm{P} \in k[\mathrm{X}]$ est unitaire de degré n de racines $x_1, \cdots, x_n$ dans $\bar{k}$, on a

$$\mathrm{disc}(\mathrm{P}) = (-1)^{\frac{n(n-1)}{2}} \prod_i \prod_{j \neq i} (x_i - x_j) = (-1)^{\frac{n(n-1)}{2}} \prod_i \mathrm{P}'(x_i).$$

Si $\mathrm{P} = \mathrm{X}^n - 1$, on a donc

$$\mathrm{disc}(\mathrm{P}) = (-1)^{\frac{n(n-1)}{2}} n^n \prod_i x_i^{n-1} = (-1)^{\frac{n(n-1)}{2}} n^n (\prod_i x_i)^{-1}.$$

Le produit des racines de $\mathrm{X}^n - 1$ est $(-1)^{n-1}$, de sorte que

$$\mathrm{disc}(\mathrm{X}^n - 1) = (-1)^{\frac{n(n+1)}{2}} n^n.$$

Supposons $\mathrm{PGCD}(p, n) = 1$ et $p \neq 2$. L'action de $\mathrm{Gal}(\mathrm{K}/k)$ sur l'ensemble $\mu_n(\bar{k})$ "est dans A_n" si et seulement si $(-1)^{\frac{n(n+1)}{2}} n^n$ n'est pas un carré dans k (7.2.1).

Correction sommaire de l'exercice 7.2.4

Comme k est de caractéristique 2, on a

$$x_i^2 + x_j^2 = (x_i - x_j)^2 \neq 0$$

pour tout $i \neq j$.
Soit $\mathcal{P}$ l'ensemble des *paires* $\pi = \{x, y\}$ où x, y sont deux racines distinctes de P. Le groupe de Galois G de P permute les paires par action sur les racines. On note π_1, π_2 les éléments xy et $x^2 + y^2$ respectivement. On a $a = \sum_{\pi \in \mathcal{P}} \frac{\pi_1}{\pi_2}$ qui est visiblement invariant par g donc est un élément de k.

On a

$$b^2+b=\sum_{i<j}\left(\frac{x_i^2}{x_i^2+x_j^2}+\frac{x_i(x_i+x_j)}{x_i^2+x_j^2}\right)=\sum_{i<j}\frac{x_ix_j}{x_i^2+x_j^2}=a.$$

La somme des racines de $\mathrm{X}^2+\mathrm{X}+a$ est 1 de sorte que ses racines sont b ou $b+1$. Comme $\mathrm{X}^2+\mathrm{X}+a\in k[\mathrm{X}]$, le groupe G permute ses racines de sorte que $g(b)=b$ ou $b+1$. Si g agit sur les x_i par la permutation σ des indices, on a

$$g\left(\frac{x_i}{x_i+x_j}\right)=\frac{x_{\sigma(i)}}{x_{\sigma(i)}+x_{\sigma(j)}}=1+\frac{x_{\sigma(j)}}{x_{\sigma(i)}+x_{\sigma(j)}}.$$

On en déduit la formule

$$g(b)=\sum_{\substack{i<j\\ \sigma(i)<\sigma(j)}}\frac{x_{\sigma(i)}}{x_{\sigma(i)}+x_{\sigma(j)}}+\sum_{\substack{i<j\\ \sigma(i)>\sigma(j)}}\left(1+\frac{x_{\sigma(j)}}{x_{\sigma(i)}+x_{\sigma(j)}}\right).$$

Comme

$$(-1)^{\mathrm{card}\{(i,j)|i<j \text{ et } \sigma(i)>\sigma(j)\}}=\epsilon(\sigma),$$

on obtient $g(b)=b$ si et seulement si $\epsilon(\sigma)=1$, ce qu'on voulait.

Correction sommaire de l'exercice 7.3.7

Comme n est premier à la caractéristique de k, le cardinal de $\mu_n(\bar{k})$ est n et P est séparable sur k. On sait par ailleurs que c'est un groupe cyclique : choisissons un générateur ζ_n. Soit $\mathrm{K}=k(\zeta_n),\mathrm{L}=\mathrm{K}(\sqrt[n]{a})$. Notons que L ne dépend pas du choix de $\sqrt[n]{a}$. C'est le corps de décomposition de P. Comme P et X^n-1 sont séparables sur k, les corps L et K sont galoisiens sur k. On a alors la suite exacte fondamentale (5.5.1,*iv)*)

$$1\to\mathrm{Gal}(\mathrm{L}/\mathrm{K})\to\mathrm{Gal}(\mathrm{L}/k)\to\mathrm{Gal}(\mathrm{K}/k)\to 1.$$

Mais Gal(L/K) est cyclique grâce à la théorie de Kummer (7.3.4) tandis que Gal(K/k) est un sous-groupe de $(\mathbf{Z}/n\mathbf{Z})^*$ (6.2.2), donc est abélien.

Correction sommaire de l'exercice 8.3.5

Soit P est un polynôme annulateur unitaire à coefficients entiers de z. On peut supposer $z\neq 0$. Observons déjà qu'alors tous les z_i sont non nuls puisqu'ils sont conjugués de z sous l'action du groupe de Galois. Alors, les $z_i, i=1,\cdots,d$ sont des racines de P comme d'habitude, et donc sont des entiers. Soit G le groupe de Galois de $\mathbf{Q}(z_i)$ sur $\mathbf{Q}$. Comme $\pi_n=\prod(\mathrm{X}-z_i^n)$ est fixe par G, il est à coefficients dans $\mathbf{Q}$. Mais ses coefficients sont des polynômes à coefficients entiers en les z_i, donc sont entiers sur $\mathbf{Z}$, donc sont

entiers (6.3.6). Précisément, ces coefficients $a_j(n) \in \mathbf{Z}$ sont des fonctions symétriques élémentaires, somme de $\binom{d}{j}$ produits $z_{i_1}^n \cdots z_{i_j}^n$. On déduit l'inégalité $|a_j(n)| \leq \binom{d}{j}$: on a donc un nombre fini de coefficients. Il existe donc un nombre fini de polynômes π_n et donc un nombre fini de d-uples (z_i^n). Soit donc $n < m$ tel que $(z_i^n) = (z_i^m)$. Alors $z_i^{m-n} = 1$.

Correction sommaire de l'exercice 8.7.2

Voir examen 2007.

CHAPITRE 11

LISTE DES PRINCIPAUX RÉSULTATS

INDEX

BIBLIOGRAPHIE

[B1] **N. Bourbaki**, *Éléments de mathématique, Algèbre, Chap. 1-3*, Masson, 1981

[B2] **N. Bourbaki**, *Éléments de mathématique, Algèbre, Chap. 4-7*, Masson, 1981

[CL] **A. Chambert-Loir**, *Algèbre corporelle*, Ed. de l'Ecole Polytechnique, 2004

[D] **R. et A. Douady**, *Algèbre et théories galoisiennes*, Cassini, 2005

[Eh] **C. Ehrhardt**, *Le bicenteraire d'Evariste Galois (1811-1832)*, Gaz. Math. No. **129** (2011), 71–73

[El] **R. Elkik**, *Cours d'Algèbre*, Ellipses Marketing Col.: Mathématiques Université, 2002

[Ga] **E. Galois**, *Écrits et mémoires mathématiques d'Évariste Galois*, Gauthiers-Villars, 1962

[Gr] **A. Grothendieck**, *Séminaire de Géométrie Algébrique du Bois Marie - 1960-61 - Revêtements étales et groupe fondamental (SGA 1)*, Springer-Verlag, 1971

[HL] **D. Hernandez et Y. Laszlo**, *Introduction à la théorie de Galois*, Ed de l'Ecole Polytechnique, 2012

[L] **S. Lang**, *Algebra*, Graduate Texts in Mathematics, **211**. Springer-Verlag, 2002

[S] **J.-P. Serre**, "Groupes de Galois sur **Q**", *Séminaire Bourbaki*, **30** (1987-1988), Exposé No. 689

[V] **H. Völklein**, "$\mathbf{GL}_n(q)$ as Galois group over the rationals", *Mathematische Annalen* (1992), vol. **293**, no. 1, 163–176

TABLE DES MATIÈRES