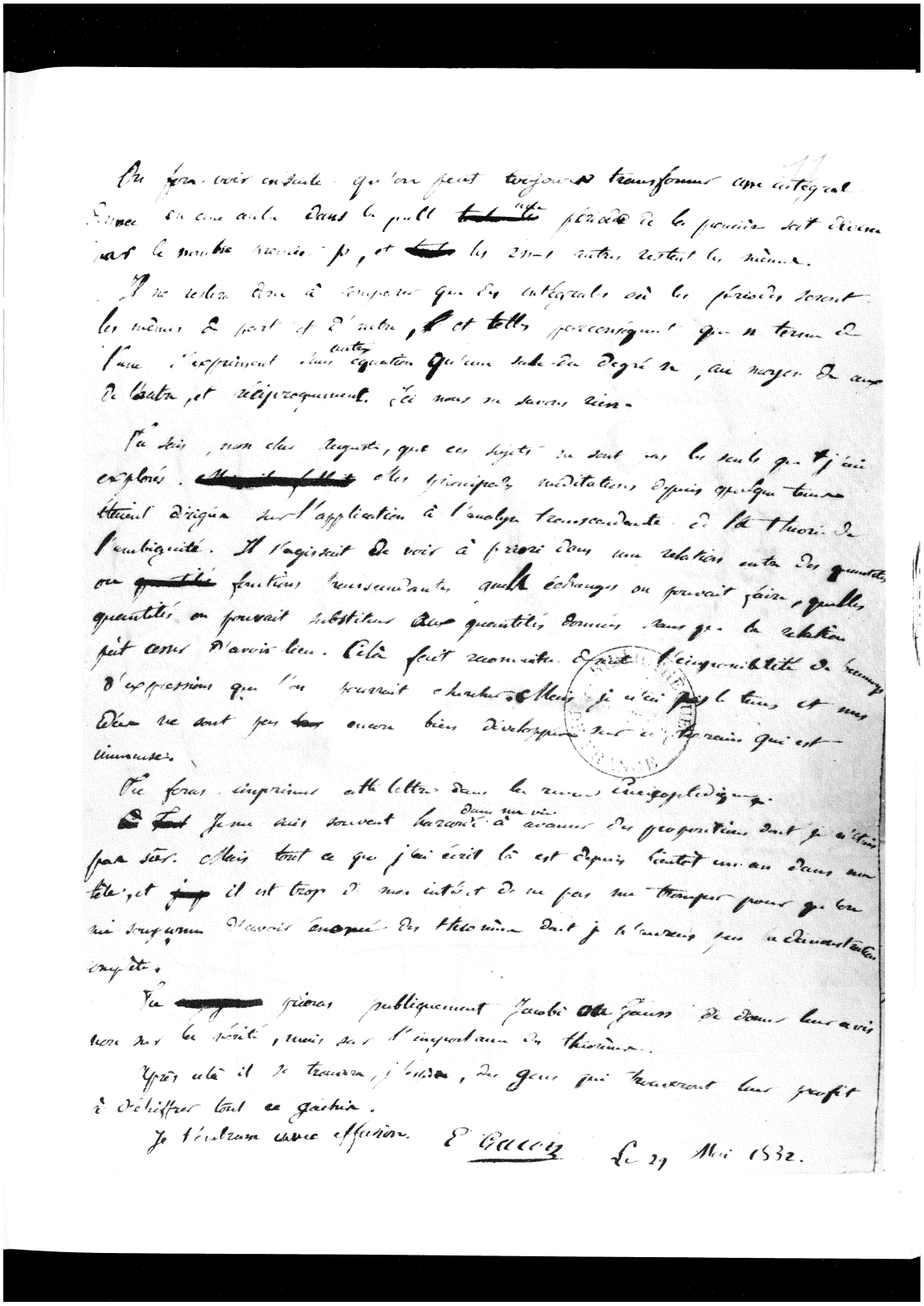
INTRODUCTION À LA THÉORIE DE GALOIS

par

Yves Laszlo

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 *Écrits et mémoires mathématiques d'Évariste Galois*, Gauthiers-Villars (1962).

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*

Pour aller dans le sens de la mode des indicateurs bibliométriques, on constatera avec intérêt que parmi les prépublications disponibles depuis le 1er janvier 2008, près d'un millier mentionnent dans le résumé le mot « Galois » . Ceci donne une idée de l'importance de la théorie de Galois, mais aussi de sa modernité et de la quantité considérable de points restant à découvrir. 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 (cf. chapitre 0 du polycopié de tronc commun ou (6.6.1)) puis le théorème de résolubilité 9.4.1 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′ +... et aussi il peut se décomposer en groupes qui ont tous les mêmes substitutions en sorte que G = H + TH + T′H +....

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.

1. 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 par Galois permet de donner des résultats profonds en arithmétique, la « reine des sciences » comme disait Gauss. Même si, faute de temps, on n'a guère pu présenter de résultats modernes, la théorie de Galois et ses extensions tient actuellement une place centrale en Mathématiques. La compréhension des groupes de Galois des corps de nombres est très lacunaire, même si des progrès spectaculaires ont été réalisés ces cinquante dernières années. On a préféré dans cette exposition 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 mod p des groupes de Galois (10)) ou de résultats récents (quelques résultats de théorie de Galois inverse (12)). On n'a pas non plus cherché à développer des méthodes sophistiquées de calcul algorithmiques de groupes de Galois, qui existent, mais qui sont à mon 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 en fin de poly qu'en dernière extrémité.

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 ! D'un point de vue bibliographique, on pourra se reporter aux jolis livres d'Antoine Chambert-Loir (*Algèbre corporelle*, publication Polytechnique, 2004) ou de Renée Elkik (*Cours d'Algèbre*, Ellipses Marketing Collection : Mathématiques Université, 2002). Pour aller plus loin, en particulier dans l'étude de la séparabilité, le chapitre V de l'*Algèbre* de Bourbaki est un classique.

Maintenant, cette exposition élémentaire souffre 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 d'une vaste théorie, en un sens plus simple et plus géométrique, la théorie de la descente fidèlement plate de Grothendieck exposée dans SGA 1 (*Revêtements étales et groupe fondamental*, Documents Mathématiques 3, 2003).

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 Douady A. et R. (*Algèbre et théories galoisiennes*, Cassini, 2005), 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

Alexandre Grothendieck

revêtements étales. Il aborde la très riche et largement ouverte théorie des *dessins d'enfants* de Grothendieck [3], 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 que cela ne nuisait pas 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, comme on le verra (10) est de toutes manières utiles pour calculer les groupes de Galois intervenant en caractéristique zéro.

Les passages en petit caractère peuvent être passés en première lecture. Leur étude approfondie ne sera pas nécessaire pour l'examen (on rappelerait si besoin des résultats y étant utilisés). La typographie signale en général des approfondissements ou généralisation intéressantes, voire des preuves peu éclairantes pour la compréhension de l'ensemble, plus qu'une difficulté plus importante par rapport au cœur du texte.

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). Le lecteur intéressé par la théorie de Galois générale pourra par exemple consulter l'ancien polycopié (http ://www.math.polytechnique.fr/ laszlo/galois0.pdf).

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

3. 1928-

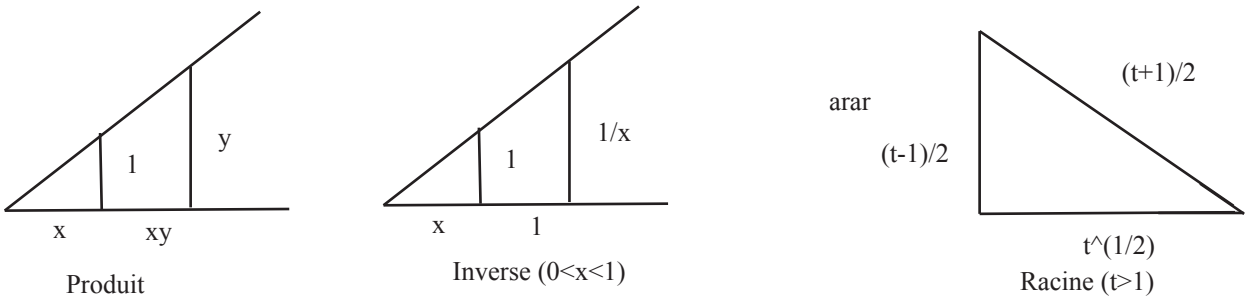
2. Invitation

Nous allons esquisser 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 de 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.

2.1. Construction à la règle et au compas. — On identifie le plan euclidien (orienté) à $\mathbf{C}$ muni de la norme usuelle $||z||=|z|$.

Définition 2.1.1. — *On dira que* $\mathrm{P} \in \mathbf{C}$ *est* constructible *s'il existe une suite finie de points distincts* $\mathrm{P}_0, \cdots, \mathrm{P}_\mathrm{N} = \mathrm{P}$ *de points tel que* $\mathrm{P}_0 \in \{0, 1\}$ *et pour tout* $n < \mathrm{N}$ *le point* P_{n+1} *est un des points d'une intersection finie de deux « droite ou cercle » de type* $(\langle \mathrm{P}_\alpha, \mathrm{P}_\beta \rangle, 0 \leq \alpha < \beta \leq n$ *ou* $\mathrm{C}(\mathrm{P}_\gamma, |\mathrm{P}_\alpha - \mathrm{P}_\beta|), \rangle, 0 \leq \alpha < \beta \leq n, \gamma \leq n$.

En d'autres termes, on décide que $0, 1$ 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 (droite ou cercle)s admissibles. Les constructibles au cran $n + 1$ sont les au cran n, ainsi que les intersections finies entre deux (droite ou cercle)s admissibles.
Par exemple, i est constructible.
Le lecteur se souviendra des théorèmes de Thalès et Pythagore (cf. figure)



Constructions utiles

et montrera les propriétés suivantes.

Exercice 2.1.2. — *L'ensemble des réels constructibles est un sous-corps de* $\mathbf{R}$ *(en particulier contient les rationnels). Un réel positif est constructible si et seulement si sa racine carrée l'est. Le complexe* z *est constructible si et seulement ses parties réelles et imaginaires le sont, de sorte que les complexes constructibles forment un sous-corps de* $\mathbf{C}$.

Soit alors L_n le sous-corps de $\mathbf{C}$ engendré par i et les coordonnées des $P_\alpha, \alpha \leq n$. Les coordonnées des points d'intersection z d'une « droite ou cercle » et d'une droite construite sur les $P_\alpha, \alpha \leq n$ sont solutions d'un équation de degré 2 à coefficients dans L_n de sorte que

$$L_n[z] = \{a + bz, a, b \in L_n\}$$

est un corps de degré ≤ 2 sur L_n. Le cas de l'intersection de deux cercles est analogue.
La réciproque est facile et laissée au lecteur en exercice (montrer que si $K[z]$ est un sous-corps de $\mathbf{C}$ avec $[K[z] : K] = 2$, alors z est solution d'une équation de degré 2 à coefficients dans K).

Théorème 2.1.3 **(Wantzel [4])**. — *Le complexe z est constructible si et seulement si il existe une suite finie de corps $L_0 = \mathbf{Q} \subset L_1 \cdots \subset L_n$ et $[L_{i+1} : L_i] \leq 2$ avec $z \in L_n$.*

Comme on le verra (3.12.8), on a alors

$$[L : \mathbf{Q}] = \prod [L_{i+1} : L_i] = 2^m$$

avec $m \leq n$ et donc $[\mathbf{Q}[z] : \mathbf{Q}]$ est une puissance de 2 (cf. 3.12.8), car $\mathbf{Q}[z] \subset L_n$. En particulier, cette dimension est finie. Si on sait (Lindeman, 1882) que π est transcendant (11), on en conclut l'impossibilité de la quadrature du cercle : construire un carré de même aire que le disque unité.
On peut 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, on a (7.2.8).

Proposition 2.1.4 **(Gauss [5])**. — *On a $[\mathbf{Q}[\exp \frac{2i\pi}{n}], \mathbf{Q}] = \varphi(n)$ où φ est l'indicateur d'Euler [6] 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 à coefficients rationnels en $\exp \frac{2i\pi}{n}$.*

Comme $\varphi(7) = 7 - 1 = 6$...
Généralement donc, si le polygone régulier à n côtés est constructible, $\varphi(n)$ est une puissance de 2, ce qui impose (exercice) que n est un produit d'une puissance de 2 et d'un nombre de Fermat $F_m = 2^{2^m} + 1$ qui est *premier*. Ce résultat est dû à Gauss. Ces résultats *ne font pas* intervenir la théorie de Galois [7]. La réciproque était conjecturée semble-t-il par Gauss.
Comme toujours, il avait deviné juste :

Théorème 2.1.5 **(Gauss-Wantzel)**. — *La réciproque est vraie : si n est un produit d'une puissance de 2 et d'un nombre de Fermat $F_m = 2^{2^m} + 1$ qui est* premier*, alors le polygone régulier à n côtés est constructible.*

En fait la preuve donne presque un algorithme pour construire un polygone régulier à n côtés (lorsque c'est possible !) : on doit pour en avoir un décomposer n en facteurs premiers *et* trouver un générateur du groupe cyclique $(\mathbf{Z}/p\mathbf{Z})^*$ (cf. PC). Notons qu'on a $F_0 = 3, F_1 = 5, F_2 = 17, F_3 =$

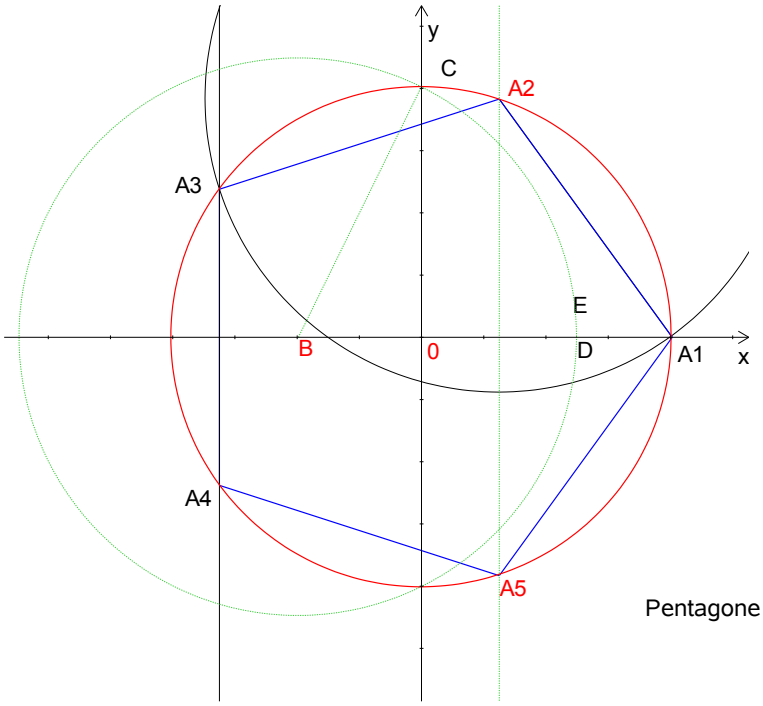
4. 1814-1848, Chargé de cours à Polytechnique.
6. 1777-1855
6. 1707-1783
7. 1811-1832

Karl Friedrich Gauss

Leonhard Euler

$257, \mathrm{F}_4 = 65537$ et sont tous premiers. Si les constructions des triangles équilatéraux, carrés, et pentagones réguliers sont élémentaires, celle du polygone régulier à 17 côté est moins évidente [8]... Rappelons d'abord la construction (connue de Ptolémée [9], premier siècle de notre ère) du pentagone régulier, simple conséquence de la formule élémentaire

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



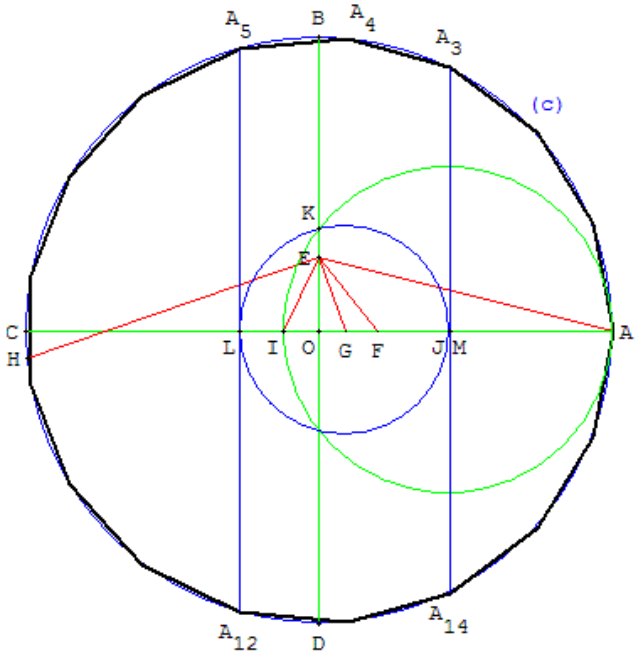
Construction du pentagone régulier

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

9. ∼90-168

Claudius Ptolémée

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



Heptadécagone

Construction de l'heptadécagone régulier

(pour une animation, voir par exemple http ://www.ac-poitiers.fr/math/prof/resso/ima/sar1/index.htm).
On a ici déjà une formule assez compliquée

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

formule qui se déduit d'ailleurs de la théorie de Galois, formule 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 (7.3.3) : c'est une conséquence presque immédiate du calcul du groupe de Galois $\mathrm{Gal}(\mathbf{Q}[\exp\frac{2i\pi}{n}],\mathbf{Q})$ (cf. 7.2.10).

2.2. Résolution d'équations. — Tout le monde connaît les solutions de l'équation quadratique $x^2+a=0, b\in\mathbf{C}$, à savoir $x=\pm\sqrt{a}$. En général, pour l'équation de degré n, une habile translation de la variable tue le terme de degré $n-1$. En degré 3, on a donc affaire avec l'équation $x^3+ax+b=0$ dont les solutions ont été achetées au 16ème siècle par Cardan [10] au mathématicien Tartaglia [11] (mais étaient sans doute connues de del Ferro [12]). 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

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

Un élève de Cardan, Ferrari [13], 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'a 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 !

10. 1501-1576
11. 1499-1557
12. 1465-1526
13. 1522-1565

Gerolamo Cardano

Niccolò 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 facile du théorème des fonctions symétriques et de la théorie de Galois (cf. 9.4). 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 $X^5 - X - 1$ ne s'expriment pas par radicaux de rationnels !

Pour finir cet échauffement, 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 facettes, très profondes, gouvernant de vastes aspects tant de l'algèbre que de la théorie des nombres et de la géométrie (cf. le cours de Jean Lannes de revêtements et celui de Jacques Tilouine de courbes elliptiques). C'est l'étude fine des représentations linéaires (cf. le cours de Majeure « Représentations de groupes ») du groupe de Galois de $\bar{\mathbf{Q}}/\mathbf{Q}$ -au travers notamment d'un cas très particulier des conjectures de Langlands- qui a permis à Wiles de prouver le théorème de Fermat. En bref, ce cours n'est que le *début* d'une longue histoire, bien loin d'être terminée.

3. Généralités sur les algèbres et les corps

Dans tout ce qui suit, on dira anneau pour anneau commutatif unitaire. 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.

3.1. Quelques rappels sur les anneaux. — Rappelons (cf. chapitre 0 du polycopié de tronc commun ou le cours de classe préparatoire) qu'un anneau A est un ensemble A 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 à moins que A ne soit un corps, à savoir un anneau non nul dans lequel tous les éléments non nuls sont inversibles pour la multiplication.

Exemple 3.1.1. — *L'ensemble des entiers relatifs, des entiers modulo n, les fonctions d'une 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).*

Définition 3.1.2. — *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 tout $a, b \in \mathrm{A}$. Le noyau $\mathrm{Ker}(f)$ 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 $a \in \mathrm{A}$. Le noyau d'un morphisme d'anneau est un *idéal* (on rappelle que les idéaux de A sont les sous-groupes additifs I de A tels que $a\mathrm{I} \subset \mathrm{I}$ pour tout $a \in \mathrm{A}$). On sait que si $\mathrm{A} = \mathbf{Z}$ ou $k[\mathrm{X}]$ par exemple, tout idéal est engendré par un élément.

Exercice 3.1.3. — *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 que les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$ sont cycliques 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.*

3.2. Morphisme de corps. — Notons qu'un idéal de I est l'anneau A si et seulement si il contient 1, ou, ce qui revient au même, un inversible de A. En particulier, le seul idéal non nul d'un corps est le corps lui-même. Comme un morphisme de corps [14] envoie 1 sur 1 et qu'un corps est non réduit à zéro, le noyau d'un morphisme de corps est toujours nul :

un morphisme de corps est toujours injectif !

14. A savoir un morphisme d'anneaux entre corps.

Ceci nous permet de penser à un morphisme de corps $\sigma : k \to k'$ comme au sous-corps $\sigma(k)$ de k' identifié à k' via l'isomorphisme $\sigma : k \xrightarrow{\sim} \sigma(k)$. On parlera de plongement de k dans k'. On dira aussi que k' est une extension de k, considérant k comme un sous-corps de k'.

3.3. 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 [15] (cf. chapitre 0 du polycopié de tronc commun). 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 $\mathrm{A} = n\mathbf{Z}$ et $\mathrm{I} = \mathbf{Z}$.

En général, l'ensemble quotient A/I est l'ensemble des **translatés** [16]

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

Notons que deux tels translatés $(a + \mathrm{I})$ et $(a' + \mathrm{I})$ sont égaux si et seulement si $a - a' \in \mathrm{I}$.

On définit la somme de deux translatés

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

qui est bien un translaté de I. Ceci reflète le caractère *distingué* (6.6.1) du sous-groupe I de A (qui est abélien !). On observe que A/I muni de cette addition est un groupe commutatif de groupe $\bar{0}$. De même, A/I est muni d'un produit défini par

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

La **surjection canonique**

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

définie par $a \to a + \mathrm{I}$ est un **morphisme** de groupes additifs (autrement dit respecte l'addition). On voit donc $\bar{a} = \pi(a)$ comme la classe A modulo I, exactement comme en arithmétique usuelle.

Proposition 3.3.1. — *Il existe une unique structure d'anneau sur* A/I *telle que* π *est un morphisme. Le noyau de* π *est* I.

Démonstration. — Laissée au lecteur. □

Autrement dit, on a

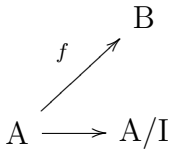
$$\overline{a}.\overline{a'} = \overline{a.a'}, \ \overline{a + a'} = \overline{a} + \overline{a'}$$

et $\overline{1}$ neutre de A/I pour le produit. L'énoncé suivant, dit de *propriété universelle du quotient*, est facile, et... fondamental.

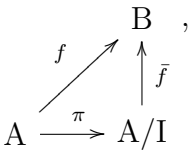
15. Comme souvent en mathématiques, la construction n'a guère d'importance ; seules les propriétés importent. Par exemple, on sait très bien travailler sur les réels en connaissant les propriétés de son ordre sans pour autant se souvenir voire connaître une quelconque de ses constructions !

16. C'est la vision concrète des classes d'équivalence pour la relation d'équivalence de congruence modulo I du polycopié de tronc commun.

Partant d'un diagramme



tel que $f(\mathrm{I}) = 0$, il existe un unique morphisme $\bar{f}$ 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 :

***Théorème 3.3.2* (Propriété universelle du quotient).** — *Soit* B *un anneau. L'application* π^* *de composition par la surjection canonique* $\mathrm{A} \twoheadrightarrow \mathrm{A/I}$ *définit un isomorphisme*

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

On identifiera sans plus de précaution ces deux espaces.

Démonstration. — Observons que π^* est additive. Soit alors ϕ dans le noyau *ie* $\phi \circ \pi = 0$. Comme π est surjective, ϕ est nulle sur $\pi(\mathrm{A}) = \mathrm{A/I}$ 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 $t \in \mathrm{A/I}$: 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 et de même pour l'addition). □

Remarque 3.3.3. — *Si* $f : \mathrm{A} \to \mathrm{B}$ *est un morphisme d'anneaux, on a donc une factorisation canonique* $\bar{f} : \mathrm{A/Ker}(f) \to \mathrm{B}$ *de* f *à travers* $\mathrm{A} \to \mathrm{A/Ker}(f)$ *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 surjective, on a donc un isomorphisme canonique* $\bar{f} : \mathrm{A/Ker}(f) \xrightarrow{\sim} \mathrm{B}$.

Montrons un lemme, facile, mais très utile.

Lemme 3.3.4. — *L'application qui à un idéal* $\bar{\mathrm{J}}$ *de* A/I *associe son image inverse* $\mathrm{J} = \pi^{-1}(\bar{\mathrm{J}})$ *identifie les idéaux de* 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 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 $\mathrm{A}/\mathrm{J} \to \bar{\mathrm{A}}/\bar{\mathrm{J}}$ qui reste évidemment surjective, mais qui en plus est injective d'après la remarque précédente. □

3.4. Caractéristique d'un corps. — Rappelons le résultat suivant :

Exercice 3.4.1. — *Soit* A *un anneau. Il existe un unique morphisme d'anneaux* $\gamma : \mathbf{Z} \to \mathrm{A}$. *Si* A *est un corps, montrer que* $\ker(\gamma) = n\mathbf{Z}$ *avec* $n = 0$ *ou* n *premier.*

On pose alors

Définition 3.4.2. — *Soit* k *un corps. La caractéristique de* k *est l'unique entier* ≥ 0 *engendrant* $\ker(\gamma)$.

La caractéristique d'un corps est donc (3.4.1) nulle ou un nombre premier. Par exemple, $\mathbf{Q}$ est de caractéristique nulle tandis que $\mathbf{Z}/p\mathbf{Z}$ est de caractéristique p (p premier).

Remarque 3.4.3. — *L'unique morphisme d'anneau morphisme* $\gamma : \mathbf{Z} \to \mathrm{A}$ *(3.4.1) se factorise à travers son noyau* $n\mathbf{Z}$ *pour définir une injection canonique* $\mathbf{Z}/n\mathbf{Z} \hookrightarrow \mathrm{A}$. *En particulier, un corps de caractéristique nulle est infini puisqu'il contient* $\mathbf{Z}$, *et même* $\mathbf{Q}$ *en fait comme le prouve l'exercice suivant.*

Exercice 3.4.4. — *Montrer qu'un corps contient un unique sous-corps isomorphe à* $\mathbf{Q}$ *ou* $\mathbf{Z}/p\mathbf{Z}$ *suivant que la caractéristique de* k *est nulle ou* p.

3.5. Propriétés des idéaux. — On notera $(a_s, s \in \mathrm{S})$ l'idéal engendré par la famille $(a_s), s \in \mathrm{S}$. 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 3.5.1. — *Soit* I *un idéal d'un anneau* A.

- *On dit que* A *est intègre si* A *est non nul et si le produit de deux éléments non nuls de* A *est non nul.*
- *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 (l'anneau nul n'est pas intègre),

Exercice 3.5.2. — *Montrer que l'image inverse d'un idéal premier par un morphisme d'anneaux est un idéal premier. En déduire que la caractéristique d'un corps est un nombre premier ou bien est nulle. Montrer qu'en général l'image inverse d'un idéal maximal n'est pas maximal (considérer par exemple l'inclusion de* $\mathbf{Z}$ *dans* $\mathbf{Q}$*).*

L'ensemble des idéaux premiers de A se note Spec(A) : le spectre de A (rien à voir avec Hamlet, ou James Bond!!!).

Rappelons qu'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 irréductibles de $\mathbf{Z}$ sont, au signe près, les nombres premiers. La terminologie est alors justifiée par l'exercice suivant (cf. PC) :

Exercice 3.5.3. — *Montrer qu'un idéal propre de* A *est maximal si et seulement si le seul idéal qui le contient strictement est* A. *Supposons de plus* A *principal, ie intègre tel que tout idéal est engendré par un élément, et soit a un élément non nul. Montrer que les 3 propriétés suivantes sont équivalentes : 1) a est irréductible ; 2)* $(a) = a\mathrm{A}$ *est premier ; 3)* $(a) = a\mathrm{A}$ *est maximal.*

Exercice 3.5.4. — *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* $\mathrm{A} \to \mathrm{A/I}$ *induit une surjection au niveau du groupe des inversibles. Montrer que c'est faux sans condition sur* I.

3.6. 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 3.6.1. — *On dit que* E *est inductif si toute partie non vide totalement ordonnée admet un majorant dans* E.

Exemple 3.6.2. — $\mathbf{R}$ *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 3.6.3 **(lemme de Zorn** [17]**)**. — *Tout ensemble non vide inductif admet un élément maximal.*

Max Zorn

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 3.6.4. — *Tout anneau non nul admet un idéal maximal.*

Démonstration. — Soit E la famille des idéaux propres de A. Comme A est non nul, $\{0\}$ est dans E qui est non vide. 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 (observer que les idéaux de A/I s'identifient aux idéaux de A contenant I).

17. 1906-1993

3.7. Une application : Rang d'un module libre de type fini. — Un A-module libre est, rappelons le, un module (cf. chapitre 0 du polycopié de tronc commun) isomorphe à A^n. Supposons ici que A est non nul. 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-il $n = m$? Le lecteur familier avec l'algèbre extérieure trouvera l'énoncé évident. Voyons une preuve « élémentaire ». Un tel isomorphisme est défini par une matrice $\mathrm{M} \in \mathrm{M}_{m,n}(\mathrm{A})$. L'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. 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.

Remarque 3.7.1. — *De même, si* $\mathrm{A}^{(\mathrm{I})} \xrightarrow{\sim} \mathrm{A}^{(\mathrm{J})}$*, alors* I *et* J *sont en bijection : on se ramène comme plus haut à l'énoncé analogue sur les espaces vectoriels, qu'il reste à prouver !*

Cette propriété est complètement fausse si on ne suppose plus l'anneau commutatif.

3.8. 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.

Remarque 3.8.1. — *Le lemme chinois (pour les entiers) est attribué au mathématicien et astronome chinois Sunzi (écriture pinyin) (ou Sun Tzu*[18]*). 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*[19]*,* Traité mathématique en 9 sections*, daté de 1247.*

Plus généralement, supposons qu'on ait des idéaux $\mathrm{I}_1, \cdots, \mathrm{I}_n, n \geq 2$ d'un anneau A, deux à deux étrangers, *ie* tels que $\mathrm{I}_i + \mathrm{I}_j = \mathrm{A}$ pour $i \neq j$.

Lemme 3.8.2 **(Lemme Chinois)**. — *Sous ces conditions, l'application canonique* $\mathrm{A} \to \prod \mathrm{A}/\mathrm{I}_j$ *se factorise à travers* $\cap \mathrm{I}_j$ *pour donner un isomorphisme*

$$\mathrm{A}/\mathrm{I}_1 \cap \cdots \cap \mathrm{I}_n \xrightarrow{\sim} \prod \mathrm{A}/\mathrm{I}_j.$$

De plus, on a

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

18. 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*.
19. 12021261

Démonstration. — le lecteur est invité à passer cette preuve, qu'il a déjà vu dans le cas où A est $\mathbf{Z}$ ou bien $k[X]$, ou, mieux, à la faire lui-même. Bien entendu, le noyau de

$$A \to A/I_1 \times \cdots \times A/I_n$$

est l'intersection $I_1 \cap \cdots \cap I_n$. Par propriété universelle du quotient, on a donc une application

$$A/I_1 \cap \cdots \cap I_n \to \prod A/I_j$$

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

$$I(-j) = I_1 \cdots \widehat{I_j} \cdots I_n$$

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

$$\sum_j I(-j) = A.$$

En effet, on peut faire une récurrence sur n. Si $n = 2$, c'est l'hypothèse $I_2 + I_1 = A$. Sinon, on applique l'hypothèse de récurrence à $I_1, \cdots, I_{n-1}$. On obtient alors que la somme des $n-1$ idéaux $I_1 \cdots \widehat{I_j} \cdots I_{n-1}$ est A, de sorte que, multipliant par I_n, on a

$$\sum_{j<n} I(-j) = I_n$$

et la somme $\sum_j I(-j)$ contient I_n. En appliquant le même procédé à $I_2, \cdots, I_n$, on obtient que la somme contient I_1. Comme $I_1 + I_n = A$, la somme vaut A.
On écrit alors $1 = \sum_j a_j, a_j \in I(-j)$. Soit alors $\bar{b}_j \in A/I_j$ des classes quelconques. Posons

$$b = \sum_j a_j b_j.$$

Observons alors

$$a_j \equiv 0 \mod I_i \text{ si } i \neq j \text{ et } a_j \equiv 1 \mod I_j$$

de sorte que $b \equiv b_j a_j \equiv b_j \mod I_j$ 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 $a \in I_i$, on a $a \in I_i I(-i) = I_1 \cdots I_n$ pour tout i, ce qu'on voulait. □

Exercice 3.8.3. — *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 inversibles (utiliser le lemme chinois et 3.5.4).

3.9. Algèbres. — On a remarqué en classes préparatoires que $\mathbf{C}$ était 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 nous un corps k et un anneau B. On dit que B est une k-algèbre (unitaire) si B est de plus muni d'une multiplication externe $k \times \mathrm{B} \to \mathrm{B}$ faisant de lui un k-espace vectoriel tel que

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

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 $a \in k,\ b \in \mathrm{B}$. Dans le cas où B est un corps, on dit aussi que B (ou B/k) est une *extension* de k.

Définition 3.9.1. — *Un morphisme $f \in \mathrm{Hom}(\mathrm{B}, \mathrm{B}')$ 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 d'algèbres. Deux extensions K, L de k sont isomorphes si il existe un isomorphisme d'algèbres $\mathrm{K} \xrightarrow{\sim} \mathrm{L}$.*

Exemple 3.9.2. — *Par exemple, 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 *car 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, si $b_1, \cdots, b_n$ sont des éléments de* B, *il existe un unique morphisme d'algèbre $k[\mathrm{X}_1, \cdots, \mathrm{X}_n] \to \mathrm{B}$ envoyant chaque X_i sur* B. *S'il est surjectif, on dit que* B *est* engendré *par les b_i et on écrit $\mathrm{B} = k[x_1, \cdots, x_n]$.*

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) et donc A/I est une k-algèbre canoniquement). On laisse au lecteur le soin de vérifier que les constructions d'anneaux quotients passent *mutatis mutandis* au cas des algèbres. De même, il énoncera une version « algèbre » du lemme chinois 3.8.2 (et vérifiera que la preuve s'adapte également *mutatis mutandis*).

Exercice 3.9.3. — *Décrire un isomorphisme de $\mathbf{R}$-algèbres entre $\mathbf{R}[\mathrm{X}]/(\mathrm{X}^2 + \mathrm{X} + 1)$ et $\mathbf{C}$ d'une part et entre $\mathbf{R}[\mathrm{X}]/(\mathrm{X}(\mathrm{X}+1))$ et $\mathbf{R}^2$ d'autre part (utiliser le lemme chinois 3.8.2).*

3.10. Corps de rupture. — Soit P un polynôme de $k[X]$, qu'on suppose *irréductible*. Comme $k[X]$ est principal, (P) est maximal (3.5.3) et la k-algèbre quotient $K = k[X]/(P)$ est un corps.
Le polynôme P peut être considéré comme à coefficients dans K. Par construction, $P(\bar{X})$ est la classe de P dans $K[X]/(P)$, et donc est nul. On dit que $K = k[X]/(P)$ est le *corps de rupture* de P. Si x désigne l'image de X dans k, on a évidemment $K = k[x]$.

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

D'une certaine manière, c'est la plus petite :

Exercice 3.10.1. — *Soit* L *une extension de* k *dans laquelle* P *a une racine* ξ. *Montrer que* K *se plonge dans* L *(comme* k*-algèbre). Montrer de plus que si* L *est engendré par* ξ, *les extensions* K/k *et* L/k *sont isomorphes.*

Le lemme suivant est facile mais fondamental.

Lemme 3.10.2. — *Soit* K *une extension de* k. *Alors,* $\mathrm{Hom}_k(k[x], K)$ *s'identifie aux racines de* P *dans* K.

Démonstration. — Se donner $\sigma \in \mathrm{Hom}_k(k[x], K) = \mathrm{Hom}_k(k[X]/(P), K)$ c'est se donner $\sigma \in \mathrm{Hom}_k(k[X], K)$ qui annule P par propriété universelle du quotient (3.3.3). Autrement dit c'est se donner $y = \sigma(X)$ tel que $\sigma(P(X)) = P(y)$ est nul (3.9.2). □

3.11. Éléments algébriques, transcendants. — Soit k un sous-corps d'un corps K (on dit qu'on a une extension K/k). On notera $[K : k]$ la dimension du k-espace vectoriel K, qu'elle soit finie ou non.

Définition 3.11.1. — *Un élément* $x \in K$ *est dit* ***algébrique*** *sur* k *si il existe* $P \in k[X]$ *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*).*

Exercice 3.11.2. — *Montrer que l'ensemble des complexes qui sont algébriques sur* $\mathbf{Q}$ *est dénombrable.*

Par exemple, on montrera en PC (et c'est facile) que 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 e (Hermite [20], 1872) et π (Lindemann [21], 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, simplification des preuves originales due à Hilbert, sera donnée plus bas (11). Le lecteur est invité à passer ce paragraphe 11 en première lecture, non pas car les preuves sont difficiles à lire, mais car elles sont un peu « magiques », pas très intuitives.

20. 1822-1901, ancien élève de l'X
21. 1852-1935

Charles Hermite

Ferdinand Lindemann

3.12. Critère d'algébricité. — La caractérisation suivante est aussi élémentaire que fondamentale.

Proposition 3.12.1. — *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. — Si x est algébrique sur k, il est annulé par un polynôme de degré $d > 0$ et $1, \cdots, x^{d-1}$ engendre $k[x]$, prouvant $i) \Rightarrow ii)$. Une algèbre intègre de dimension finie sur un corps est un corps (exercice classique de taupe) ce qui prouve $ii) \Rightarrow iii)$. Si $k[x]$ est un corps, soit x est nul, et $x = 0$ est certainement algébrique, soit $x^{-1} = \mathrm{P}(x) \in k[x]$ 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, de sorte que $iii) \Rightarrow i)$. □

Définition 3.12.2. — *On appelle polynôme minimal de x algébrique sur k le générateur unitaire de l'idéal des polynômes de $k[\mathrm{X}]$ annulant x. Le degré $\deg_k(x)$ est la dimension $\dim_k k[x]$.*

Proposition 3.12.3. — *Soit P le polynôme minimal de $x \in \mathrm{K}$ est algébrique sur k. Alors,*
– *P est irréductible ;*
– *le corps $k[x]$ est canoniquement k-isomorphe à $k[\mathrm{X}]/(\mathrm{P})$ et $\deg_k(x) = \deg(\mathrm{P})$.*

Démonstration. — Par définition, le morphisme d'algèbre $k[\mathrm{X}] \to \mathrm{K}$ qui envoie X sur x (3.9.2) a pour image $k[x]$ et pour noyau l'idéal (P). On a donc (3.3.3) un isomorphisme $k[\mathrm{X}]/(\mathrm{P}) \xrightarrow{\sim} k[x]$ d'où la formule $\deg_k(x) = \deg(\mathrm{P})$ puisque les 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 disons 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 (3.5.3) si on veut). □

Définition 3.12.4. — *Soient x algébrique sur k de 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).*

Tenant compte de 3.12.3 et 3.10.2, on obtient le résultat suivant.

Proposition 3.12.5. — *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, 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 3.12.6. — *Le sous-ensemble* A *de* K *des algébriques sur* k *est un sous-corps de* K.

Démonstration. — A et A − 0 sont non vides. Vérifions que la différence et le produit de deux algébriques x, y est algébrique. Par hypothèse, $x^i, i \leq \deg_k(x), y^j \leq \deg_k(y)$ engendrent $k[x]$ et $k[y]$ respectivement. On en déduit que les monômes $x^i y^j, i \leq \deg_k(x), j \leq \deg_k(y)$ 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 est annulé par P, alors $1/x$ est annulé par le polynôme aux inverses $\mathrm{X}^{\deg(\mathrm{P})}\mathrm{P}(1/\mathrm{X})$. □

Définition 3.12.7. — *Soit* A *une* k*-algèbre. Sa dimension se note* $[\mathrm{A} : k]$ *et s'appelle aussi son degré. Une extension de* k *est dite finie si elle est de dimension finie sur* k.

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

Théorème 3.12.8 **(Base télescopique)**. — *Soit* L *une* K*-algèbre où* K *est un corps contenant* k *de sorte qu'on a des inclusions* $k \subset \mathrm{K} \subset \mathrm{L}$. *Soit* $\lambda_i, i \in \mathrm{I}$ *et* $\kappa_j, j \in \mathrm{J}$ *des bases de* L/K *et* K/k *respectivement. Alors,* $\lambda_i \kappa_j, (i, j) \in \mathrm{I} \times \mathrm{J}$ *est une base de* L/k. *En particulier, on a*

$$[\mathrm{L} : k] = [\mathrm{L} : \mathrm{K}][\mathrm{K} : k],$$

(encore une relation de Chasles !).

Démonstration. — Si on a

$$\sum_{i,j} a_{i,j}\lambda_i\kappa_j = \sum_i (\sum_j a_{i,j}\kappa_j)\lambda_i = 0$$

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

$$\sum_i b_i\lambda_i \text{ avec } b_i \in \mathrm{K}$$

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

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

(κ_j générateur sur k) de sorte que

$$l = \sum a_{i,j}\lambda_i\kappa_j.$$

□

Corollaire 3.12.9. — *Si $x_1, \cdots, x_n$ sont algébriques, alors l'algèbre $k[x_1, \cdots, x_n]$ des polynômes en les x_i est en fait un corps et est de dimension $\leq \prod \deg_k(x_i)$.*

On déduit immédiatement en utilisant le corollaire

Une extension de k est finie si et seulement si elle est algébrique et engendrée (comme algèbre ou comme espace vectoriel sur k comme on veut) par un nombre fini d'éléments.

Exercice 3.12.10. — *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* $\mathrm{P}_1, \cdots, \mathrm{P}_n$ *de polynômes non constants.*

Remarque 3.12.11. — *Réciproquement, on peut prouver (cf. examen 2006), 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*[22].

David Hilbert

3.13. Notion de clôture algébrique. —

Définition 3.13.1. — *On dit qu'un corps* K *est algébriquement clos si tout polynôme non constant de* K[X] *est scindé sur* K.

Exercice 3.13.2. — *Soit* $\mathrm{P} \in \mathbf{C}[\mathrm{X}]$ *non constant. Supposons* $\mathrm{P}(z)$ *non nul pour tout* $z \in \mathbf{C}$. *Montrer que* $1/\mathrm{P}$ *est borné sur* $\mathbf{C}$. *En utilisant le théorème de Liouville*[23] *sur les fonctions holomorphes, conclure que* $\mathbf{C}$ *est algébriquement clos.*

Définition 3.13.3. — *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 (3.12.6) et d'autre part est une clôture algébrique de k.

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

22. 1862-1943
23. 1809-1882, ancien élève de l'X

Joseph Liouville

Lemme 3.13.4. — *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, puisqu'il 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). Le morphisme $k[T] \to A$ d'évaluation en la classe x de X dans A 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, est scindé sur $\bar{k}$, et il en est de même de P qui le divise. □

Exemple 3.13.5. — *Le sous-corps $\bar{\mathbf{Q}}$ de $\mathbf{C}$ des éléments algébriques sur $\mathbf{Q}$ est donc algébriquement clos. Mais $\bar{\mathbf{Q}}$ n'est pas égal à $\mathbf{C}$ (exercice) !*

Théorème 3.13.6 **(Steinitz [24])**. — *Tout corps k admet une clôture algébrique, unique à k-isomorphisme près.*

Ernst Steinitz

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 infinité d'automorphismes. On va prouver d'abord l'existence, puis l'unicité qui découle du fondamental théorème

24. 1871-1928

de prolongement des morphismes. On invite d'ailleurs le lecteur à passer cette preuve d'existence non pas car elle est difficile mais car elle n'apporte pas grand-chose.

3.14. Preuve de l'existence de la clôture algébrique. — Une fois encore, on va quotienter ! Construisons déjà une gigantesque 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

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

On note alors $\gamma(i, \mathrm{P}), i = 0, \cdots, \deg(\mathrm{P})$ les coefficients du polynôme en X

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

et I l'idéal engendré par les $\gamma(i, \mathrm{P}), i = 0, \cdots, \deg(\mathrm{P})$ où P décrit $k[\mathrm{X}] - k$.
Notons que si P est constant (non nul), on a $\gamma(0, \mathrm{P}) = 0$.
Je dis qu'on a $\mathrm{I} \neq \mathrm{A}$. 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 > 0. Choisissons une extension de corps K/k tels que le nombre fini de ces polynômes P non constants soient scindés de racines $x_{\mathrm{P},i}, i = 1, \cdots, \deg(\mathrm{P})$ (3.12.10). 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 par exemple. Bien entendu 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.

Soit alors J un idéal maximal de A contenant I et L le corps A/J. Par construction, tout polynôme P non constant est scindé dans L, ses racines étant les images de $\mathrm{X}_{\mathrm{P},i}$. En particulier, toutes ses racines sont algébriques sur k. Comme elles engendrent L comme k-algèbre, on a bien L algébrique sur k.

3.15. Preuve de l'unicité de la clôture algébrique. — Pour l'unicité, montrons l'énoncé suivant.

***Théorème 3.15.1* (Prolongement des morphismes).** — *Soient* K, Ω *deux extensions de* k *et supposons* 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

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

faisant de Ω une L-algèbre. Le prolongement des plongements définit une relation d'ordre sur E qui en fait visiblement un ensemble inductif. Soit alors (L, σ) un élément maximal. Montrons $\mathrm{L} = \mathrm{K}$.

Soit $x \in \mathrm{K}$. Comme x algébrique sur k il l'est sur L. Soit $\mathrm{P}(\mathrm{X}) = \sum a_i \mathrm{X}^i$ le minimal de x sur L de sorte que l'évaluation en x identifie $\mathrm{L}[\mathrm{X}]/(\mathrm{P})$ 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 L-morphisme $\mathrm{L}[\mathrm{X}]/\mathrm{P} \to \Omega$ qui envoie X sur y car l'image de P dans Ω est par définition $\mathrm{P}^\sigma(y) = 0$ (3.12.5), d'où un k-morphisme $\mathrm{L}[x] \to \Omega$ prolongeant σ. Par maximalité de L, on déduit $x \in \mathrm{L}$. □

Remarque 3.15.2. — *σ permet d'identifier* L *à* $\sigma(\mathrm{L})$. *Dorénavant, on le fera directement, sans distinguer entre* L *et* $\sigma(\mathrm{L})$ *(cf. 3.2). 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.*

Corollaire 3.15.3. — *Deux clôtures algébriques* $\mathrm{K}_1, \mathrm{K}_2$ *de k sont k-isomorphes.*

Démonstration. — Considérant K_1 comme algébrique et K_2 comme algébriquement clos, le théorème de prolongement 3.15.1 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 $(\mathrm{K}_1, \mathrm{K}_2, \mathrm{K}_1)$ (ce qui est possible !), on déduit l'existence de $\tau \in \mathrm{Hom}_{\mathrm{K}_1}(\mathrm{K}_2, \mathrm{K}_1)$, autrement dit d'un diagramme commutatif

$$\begin{array}{ccc} \mathrm{K}_2 & \xrightarrow{\tau} & \mathrm{K}_1 \\ {\scriptstyle\sigma}\uparrow & \nearrow & \\ \mathrm{K}_1 & & \end{array}$$

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 3.15.4. — *Soit* $\mathrm{K}/k, \Omega/k$ *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 $\sigma(x) = y$ (3.12.5). Reste à prolonger σ à K tout entier, ce qui est possible (3.15.1). Inversement, $\sigma \in \mathrm{Hom}_k(\mathrm{K}, \Omega)$ laisse invariant le minimal de x sur k. Il permute donc ses racines, qui sont les conjugués de x par définition (3.12.5). □

3.16. Corps des racines (ou de décomposition). — Soit k un sous-corps de Ω algébriquement clos. Soit P un polynôme de $k[\mathrm{X}]$, non nécessairement irréductible. Le corps des racines 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 (3.15.3). On l'appelle **le corps des racines ou de décomposition** de P. La philosophie est qu'on fixe une clôture algébrique dans laquelle on travaille. Ceci permet de parler du corps des racines. Par exemple, on s'intéressera aux sous-corps de $\mathbf{C}$ algébriques sur $\mathbf{Q}$.

3.17. Le morphisme de Frobenius. — Soit p un nombre premier et A un anneau annulé par p, à savoir $pa = 0$ pour tout $a \in \mathrm{A}$.
Montrons que A admet toujours un endomorphisme non trivial. Ceci est non banal :

Exercice 3.17.1. — *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 3.17.2 **(Morphisme de Frobenius** [25]**)**. — *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 suivant.

Lemme 3.17.3. — *Soit n tel que $0 < n < p$. Alors, le coefficient binomial $\binom{p}{n}$ est divisible par p.*

Démonstration. — Comme $n! = n(n-1)\cdots 1$ est produit d'entiers distincts de p premier (car $n < p$), il est premier à p. D'après le lemme de Gauss, il suffit de prouver que

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

(n facteurs) est divisible par p, ce qui est visiblement le cas car $n > 0$. □

□

Georg Ferdinand Frobenius

25. 1848-1917

4. Corps finis

Soit k un corps fini. Il est nécessairement de caractéristique $p > 0$ car sinon il contiendrait $\mathbf{Q}$ qui est infini. Il contient donc $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ (3.4.4).

4.1. Existence et unicité des corps finis. — . Étudions le cardinal de k.

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

Démonstration. — Comme k est fini, il certainement 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 un corps algébriquement clos contenant $\mathbf{F}_p$ (3.13.6). Comme k est fini, il est algébrique sur $\mathbf{F}_p$. D'après 3.15.1, k se plonge dans Ω. On suppose donc désormais que k est contenu dans Ω. Comme k^* est d'ordre $q-1$, on a $x^{q-1} = 1$ pour tout $x \neq 0$ d'après le théorème de Lagrange (Annexe D du cours de tronc commun) et donc $x^q = x$ pour tout $x \in k$. Comme le polynôme $\mathrm{X}^q - \mathrm{X}$ admet au plus $\operatorname{card} k = q$ racines, on déduit que k est nécessairement l'ensemble des racines de $\mathrm{X}^q - \mathrm{X}$. Ceci motive la construction suivante.

Lemme 4.1.2. — *On note $\mathbf{F}_q$ l'*ensemble *des racines dans Ω de $\mathrm{X}^q - \mathrm{X}$. Alors $\mathbf{F}_q$ est l'unique sous-corps de Ω à q éléments.*

Démonstration. — Notons F le Frobenius $x \mapsto x^p$ de Ω. Rappelons que c'est un morphisme d'anneaux, et donc l'itéré F^n également. On a donc $(x+y)^q = \mathrm{F}^n(x+y) = \mathrm{F}^n(x) + \mathrm{F}^n(y) = x^q + y^q$ qui prouve la stabilité par somme de $\mathbf{F}_q$. La stabilité par produits, 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 au début de la discussion au début de 4 : un tel corps est *l'ensemble* des racines de $\mathrm{X}^q - \mathrm{X}$ nécessairement. □

Exercice 4.1.3. — *Montrer que $\mathbf{F}_{p^n}$ est contenu dans $\mathbf{F}_{p^m}$ si et seulement si $n|m$. Montrer dans ce cas que la dimension du gros sur le petit est m/n. En déduire que la clôture algébrique $\bar{\mathbf{F}}_p$ de $\mathbf{F}_p$ dans Ω est la réunion croissante des $\mathbf{F}_{p^{n!}}$.*

Notons 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).

Exercice 4.1.4. — *Montrer que deux corps finis sont isomorphes si et seulement si ils ont même cardinal.*

4.2. Automorphismes des corps finis. — On utilisera sans plus de précaution le résultat classique suivant (cf. PC)

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

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, 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 $n_2/n_1\mathbf{Z}/n_2\mathbf{Z} \xrightarrow{\sim} \mathbf{Z}/n_1\mathbf{Z}$. Évidemment, on écrase ainsi une mouche avec un marteau-pilon.

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 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 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 > 0. Montrer qu'un tel P divise $\mathrm{X}^{q^n} - \mathrm{X}$. Montrer que le corps de rupture de P est son corps de décomposition.*

Les sections suivantes -celles en petit caractère-, sont intéressantes mais inutiles formellement pour la suite.

4.3. Une application du lemme chinois : l'algorithme de Berlekamp. — Nous allons donner un algorithme, qu'on peut implanter sur un ordinateur, permettant de factoriser un polynôme P de $\mathbf{F}_p[\mathrm{X}]$ en facteurs irréductibles (on note $\mathbf{F}_p$ le corps $\mathbf{Z}/p\mathbf{Z}$), ou au moins de reconnaître 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 [26] ou théorème de Lagrange [27] 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

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

Pierre de Fermat

a) Où l'on se ramène à P *sans facteur carré.* — Si P est divisible par un carré Q^2 de degré > 0, le degré du $\mathrm{PGCD}(\mathrm{P}, \mathrm{P}')$ est au moins $\deg(\mathrm{Q})$ et donc est strictement positif. Si c'est $\deg(\mathrm{P})$, c'est que P' est nul, autrement dit P s'écrit $\sum a_{ip}^p \mathrm{X}^{ip} = \mathrm{R}$ avec $\mathrm{R} = (\sum a_{ip}\mathrm{X}^i)^p \in \mathbf{F}_p[\mathrm{X}]$, (cf. la preuve de 5.1.5 *infra*). On applique à nouveau l'algorithme à R. Sinon, $\mathrm{S} = \mathrm{PGCD}(\mathrm{P}, \mathrm{P}')$ 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.**

b) Points fixes du Frobenius. — Écrivons

$$\mathrm{P} = \prod_{i=1}^{m} \mathrm{P}_i$$

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 $\mathbf{F}_p[\mathrm{X}]$. Le lemme Chinois assure que le morphisme d'algèbres (de caractéristique p) canonique

$$\gamma : \ \mathrm{A} = \mathbf{F}_p[\mathrm{X}]/(\mathrm{P}) \to \oplus \mathbf{F}_p[\mathrm{X}]/(\mathrm{P}_i)$$

est un isomorphisme d'algèbres.
Soit F le morphisme de Frobenius de A (on note de même celui de $\mathrm{A}_i = \mathbf{F}_p[\mathrm{X}]/(\mathrm{P}_i)$). Comme $\mathbf{F}_p[\mathrm{X}]$ est principal et P_i irréductible, chaque A_i est un corps fini (3.5.3) de sorte qu'on a $\mathrm{A}_i^{\mathrm{F}} = \mathbf{F}_p$ (4.1.2). La formule

$$\gamma(a^p) = \gamma(a)^p = (a_i^p \mod \mathrm{P}_i)$$

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

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

26.
27. 1601 (?)-1655

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

c) 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 $\mathbf{F}_p$ 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* $\mathrm{P} | \mathrm{Q}^p - \mathrm{Q} = \mathrm{F}(\mathrm{Q}) - \mathrm{Q}$. De la factorisation

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

on tire

$$\mathrm{Q}^p - \mathrm{Q} = \prod_{i=0}^{p-1} (\mathrm{Q} - i)$$

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 $< \deg(\mathrm{P})$ 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 (cf. le cours de Mestre pour ceux que ça intéresse).
Un excellent exercice est de programmer cet algorithme avec un logiciel de calcul formel. Un autre excellent 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* $\mathrm{F}_{p^n} = \mathrm{F}^n$.

5. Corps parfaits

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

5.1. Extensions de corps parfaits. — Commençons par définir la notion.

Définition 5.1.1. — *On dit qu'un corps k est parfait si sa caractéristique est nulle ou s'il est de caractéristique $p > 0$ et son Frobenius est surjectif (donc un isomorphisme).*

Par exemple, tout corps algébriquement clos de caractéristique positive est parfait. Il n'est pas vrai qu'un sous-corps d'un corps parfait soit parfait (penser à la clôture algébrique d'un corps imparfait par exemple) ni qu'une extension d'un corps parfait soit parfait (penser à $\mathrm{Frac}(\mathbf{F}_p[t]) \subset \overline{\mathrm{Frac}(\mathbf{F}_p[t])}$). En revanche, on a l'énoncé important suivant.

Proposition 5.1.2. — *Soit K/k une extension finie. Alors si k est parfait, K l'est aussi*[28].

Démonstration. — La question ne pose problème qu'en caractéristique $p > 0$. Soit F le Frobenius de K, qui est bijectif sur k par hypothèse (k est parfait) et donc y admet un inverse F^{-1}. Alors, $\mathrm{F}(\mathrm{K})$ 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 $\mathrm{F}(\mathrm{K})$ (si $\sum a_i \mathrm{F}(x_i) = 0$ avec $a_i \in k$ alors $\mathrm{F}(\sum \mathrm{F}^{-1}(a_i)x_i) = 0$ et donc $\sum \mathrm{F}^{-1}(a_i)x_i = 0$ ce qui entraîne $\mathrm{F}^{-1}(a_i) = 0$ pour tout i (la famille x_i est libre) 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 $\mathrm{F}(\mathrm{K}) \subset \mathrm{K}$ d'où $\mathrm{K} = \mathrm{F}(\mathrm{K})$. □

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

Définition 5.1.3. — *Un polynôme unitaire est dit séparable si ses racines dans Ω sont simples.*

Rappelons le lemme bien connu.

Lemme 5.1.4. — *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

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

28. La réciproque est vraie, même si moins utile : voir la section suivante.

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 assure que P, P' n'ont pas de racines communes dans Ω et donc que les racines de P ,dans Ω sont simples. □

Théorème 5.1.5. — *Un corps k est parfait si et seulement tout polynôme irréductible de k[X] est séparable.*

Démonstration. — Supposons k parfait et soit P un polynôme irréductible de k[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 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 k[X] est tué par p, ce qui est absurde car P est irréductible.

Inversement, supposons que tout polynôme irréductible de k[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, le polynôme minimal P sur k d'une racine p-ième $t^{1/p}$ de t dans Ω est irréductible (3.12.3) de degré > 1 ($t^{1/p} \notin k$ par hypothèse) et divise $\mathrm{X}^p - t$. Dans Ω[X], ce polynôme s'écrit $(\mathrm{X} - t^{1/p})^p$ et donc n'a qu'une racine (de multiplicité p) de sorte que $\mathrm{P} = (\mathrm{X} - t^{1/p})^i$ avec $2 \leq i \leq p$. On en déduit que P n'est pas séparable, une contradiction (voir la section suivante pour l'irréductibilité de $\mathrm{X}^p - t$). □

5.2. Racines p-ièmes. — Soit k un sous corps de Ω, algébriquement clos de caractéristique $p > 0$. Comme le Frobenius de Ω est bijectif puisque Ω est parfait, la racine p-ième $x^{1/p} = \mathrm{F}^{-1}(x)$ de tout élément de Ω est bien définie et de même pour les racines p^n-ièmes.

Lemme 5.2.1. — *Soit $t \in k$ qui n'est pas une racine p-ième dans k. alors, pour tout $n \geq 1$, le polynôme $\mathrm{X}^{p^n} - t$ est irréductible dans k[X]. Autrement dit, on a $\deg_k(x^{1/p^n}) = p^n$.*

Démonstration. — Soit τ la racine p^{-n}-ième de t. On sait que $\tau \notin k$ puisqque par hypothèse $t^{1/p} = \tau^{p^{n-1}} \notin k$. Soit P le minimal de τ sur k : c'est un polynôme irréductible (3.12.3) de $k[\mathrm{X}]$ qui divise $\mathrm{Q} = \mathrm{X}^{p^n} - t$ puisque $\mathrm{Q}(\tau) = 0$. Utilisant une décomposition de Q en facteurs irréductibles dans $k[\mathrm{X}]$, on peut-écrire :

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

D'après l'identité de Bézout, 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 $\mathrm{Q} = \mathrm{P}^m$. 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 $\nu = 0$ et donc $\mathrm{Q} = \mathrm{P}$ est irréductible. □

On obtient alors la réciproque de 5.1.2.

Corollaire 5.2.2. — *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. □

6. La correspondance de Galois (pour les corps parfaits)

On fixe dans cette partie 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 $k[\mathrm{X}]$ est séparable (et donc a $\deg(\mathrm{P})$ racines distinctes dans Ω) et que toute extension finie de k est parfaite (5.1.2).

Si $x \in \Omega$ est algébrique sur k, on dira simplement conjugués de x pour conjugués de x dans Ω, c'est-à-dire que les conjugués de x sont par définition les racines dans Ω du minimal P de x sur k. 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

$$\mathrm{P} = \prod_{\sigma \in \mathrm{Hom}_k(k[x],\Omega)} (\mathrm{X} - \sigma(x)). \tag{6.a}$$

On s'intéresse aux extensions algébriques K/k, et en fait aux extensions finies. D'après le théorème de prolongements des morphismes (3.15.1), on sait que K se plonge (au dessus de k) dans Ω, de sorte qu'il suffit de considérer les extensions algébriques de k contenues dans Ω ce qu'on pourra toujours supposer sans dommage.

6.1. Le théorème de l'élément primitif. — On dit qu'une extension de corps est monogène si elle peut-être engendrée par un seul élément.

***Théorème 6.1.1* (Élément primitif).** — *Toute extension finie* K/k *est monogène.*

Un générateur de l'extension s'appelle un élément primitif.

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

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

L'algorithme d'Euclide prouve que le calcul de PGCD est invariant par changement de corps. On peut 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

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

L'ensemble

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

est donc réduit à x dès qu'on a choisi $t \neq 0$ en dehors du nombre fini de t tels qu'il existe $y' \neq y$ et x' vérifiant

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

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

Exercice 6.1.2. — *Si k n'était pas supposé parfait, le résultat 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.*

Par exemple, on se convainc facilement que $\sqrt{2} + \sqrt{3}$ est un élément primitif de $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ alors que $\sqrt{2}$ ne l'est pas. 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 non mathématique).

Exercice 6.1.3. — *On note $\zeta_n = \exp(\frac{2i\pi}{n})$. Montrer qu'on a $\mathbf{Q}(\zeta_n, \zeta_m) = \mathbf{Q}(\zeta_{\mathrm{PPCM}(n,m)})$. Voir la section 7 pour des résultats plus précis.*

On obtient la généralisation fondamentale suivante de 3.12.5.

Corollaire 6.1.4. — *Soit* K *une extension finie de k. Alors, on a* $\mathrm{card}_k \mathrm{Hom}(\mathrm{K}, \Omega) = [\mathrm{K}, k]$.

Démonstration. — On écrit $\mathrm{K} = k[x]$ pour x convenable et on invoque 3.12.5. □

Remarque 6.1.5. — *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 sont séparables de sorte que nous ne serons pas ennuyés par cette complication.*

6.2. Extensions galoisiennes. — Soit K/k une extension algébrique contenue dans Ω. Rappelons (3.12.5) que les *conjugués* de $x \in \mathrm{K}$ sont les racines (dans Ω) du polynôme minimal de x sur k.

Définition 6.2.1. — *L'extension* K/k *est dite galoisienne si elle est algébrique et si les conjugués d'un élément arbitraire de* K *sont encore dans* K.

On a la proposition facile mais importante suivante.

Proposition 6.2.2. — *Soit* E/k *une sous-extension de* K/k *galoisienne et supposons* E *parfait*[29]. *Alors,* K/E *est galoisienne.*

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

Exercice 6.2.3. — *Avec les notations précédentes, montrer qu'en général* K/k *n'est pas galoisienne [Regarder attentivement l'exemple* $\mathbf{Q} \subset \mathbf{Q}[2^{1/3}] \subset \mathbf{Q}[2^{1/3}, j]$ *(cf. PC)].*

On verra plus bas (6.7.1) une condition nécessaire et suffisante assurant que E/k est galoisienne. Rappelons (3.15.4) que les conjugués de $x \in \mathrm{K}$ sont aussi les $\sigma(x), \sigma \in \mathrm{Hom}_k(\mathrm{K}, \Omega)$. 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 6.2.4. — *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 (3.15.4), 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 6.2.5. — *L'inclusion* $\mathrm{Aut}_k(\mathrm{K}) \hookrightarrow \mathrm{Hom}_k(\mathrm{K}, \Omega)$ *est bijective si et seulement si* K/k *galoisienne.*

29. Cette condition est automatique dès lors que E est finie sur k (5.1.2). 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.

Démonstration. — Supposons $\mathrm{Aut}_k(\mathrm{K}) = \mathrm{Hom}_k(\mathrm{K}, \Omega)$. D'après 3.15.4, 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 K/k 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 (3.15.4), donc est dans K. Comme x est arbitraire, on a $\sigma(x) \in \mathrm{K}$. Ainsi $\sigma(\mathrm{K}) \subset \mathrm{K}$ et donc $\sigma \in \mathrm{Aut}_k(\mathrm{K})$ (6.2.4). □

Remarque 6.2.6. — *Cette définition ne dépend en fait que de* K/k *et 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 6.2.7. — *On appelle groupe de Galois d'une extension galoisienne* K/k *le groupe* $\mathrm{Gal}(\mathrm{K}/k) = \mathrm{Aut}_k(\mathrm{K}) \overset{6.2.5}{=} \mathrm{Hom}_k(\mathrm{K}, \Omega)$.

Remarque 6.2.8. — *Comme les conjugués de* $x \in \mathrm{K}$ *sont les* $\sigma(x), \sigma \in \mathrm{Hom}_k(\mathrm{K}, \Omega)$ *(3.15.4), si* K/k *est galoisienne de groupe* G*, les conjugués de* x *sont les* $g(x), g \in \mathrm{G}$.

Le point suivant est aisé, mais important.

Proposition 6.2.9. — *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 (6.2.5) un morphisme*

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

qui est surjectif. Son noyau est $\mathrm{Gal}(\mathrm{K}/\mathrm{E})$.

Démonstration. — On sait (6.2.2) 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 6.2.5, 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 (3.15.1). Les éléments du noyau sont par définition les automorphismes de K fixant E, donc les éléments de $\mathrm{Gal}(\mathrm{E}/k)$. □

On précisera ceci dans la correspondance de Galois (6.7.1) pour le cas des extensions galoisiennes finies.

6.3. Caractérisations des extensions galoisiennes. —

Théorème 6.3.1. — *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 3.15.4, un conjugué y de x s'écrit $\sigma(x)$ pour $\sigma \in \mathrm{Hom}_k(\mathrm{K}, \Omega)$; comme $\mathrm{Aut}_k(\mathrm{K}) = \mathrm{Hom}_k(\mathrm{K}, \Omega)$ (6.2.5), l'action de $\mathrm{Aut}_k(\mathrm{K})$sur les conjugués de x est bien transitive. Inversement, soit x primitif de K/k, 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 6.2.5. □

Théorème 6.3.2. — *Les extensions galoisiennes finies de* k *sont exactement les corps des racines (3.16) de polynômes.*

Démonstration. — Supposons K/k galoisienne. D'après le théorème de l'élément primitif, 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 6.2.4. □

Exercice 6.3.3. — *Montrer qu'on* $\mathrm{Gal}(\mathbf{C}/\mathbf{R}) = \mathbf{Z}/2\mathbf{Z}$ *engendré par la conjugaison.*

6.4. 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 6.4.1. — *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 les sous-extensions $\mathbf{F}_{q^m}/\mathbf{F}_q, m|n$ de $\mathbf{F}_{q^n}/\mathbf{F}_q$ sont en bijection avec les sous-groupes $\mathrm{H} =< \mathrm{F}_q^{m/n} > \xrightarrow{\sim} \mathbf{Z}/m\mathbf{Z}$ de $\mathrm{Gal}(\mathbf{F}_{q^n}/\mathbf{F}_q) \xrightarrow{\sim} \mathbf{Z}/n\mathbf{Z}$ et que, plus précisément, $\mathbf{F}_{q^m}$ est le corps des éléments fixés par H. Ce phénomène est général : c'est ce que nous allons expliquer maintenant.

6.5. Points fixes. — Jusqu'à la fin de la section 6, K/k désigne une extension finie (avec comme toujours $\mathrm{K} \subset \Omega$ et Ω algébriquement clos).

Proposition 6.5.1. — *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* G *est réduit à* k.

Démonstration. — le premier point est prouvé dans 6.2.5. Pour le second, soit x fixe sous G. Ses conjugués sont de la forme $\sigma(x)$ avec $\sigma \in \mathrm{G}$ d'après 6.3.1, et donc sont égaux à x. Comme le minimal $\mathrm{P} \in k[\mathrm{X}]$ de x est séparable car irréductible, il est donc égal à $\mathrm{X} - x$ et donc $x = -\mathrm{P}(0) \in k$. □

Inversement, prouvons l'énoncé fondamental suivant.

***Théorème 6.5.2* (Lemme d'Artin [30]).** — *Soit* $\mathbf{K}$ *un corps parfait et* G *un sous-groupe fini d'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 par G, on a $\xi^p = g(\xi^p) = g(\xi)^p$ pour tout $g \in \mathrm{G}$. Comme 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 $\leq \mathrm{card}\,\mathrm{G}x$ 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 G donc 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. Je dis qu'on a $\mathbf{K} = \mathbf{k}[x]$. Sinon, soit $y \in \mathbf{K} - \mathbf{k}[x]$. L'extension $\mathbf{k}[x, y]$ est monogène (élément primitif) engendrée par un élément z de degré $> \deg_{\mathbf{k}}(x)$, une contradiction. On déduit que le degré $[\mathbf{K} : \mathbf{k}] = \deg_{\mathbf{k}}(x)$ de $\mathbf{K}$ est de degré $\leq \mathrm{card}\,\mathrm{G}$ sur $\mathbf{k}$. Soit Ω algébriquement clos contenant $\mathbf{K}$. On a alors (6.2.5)

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

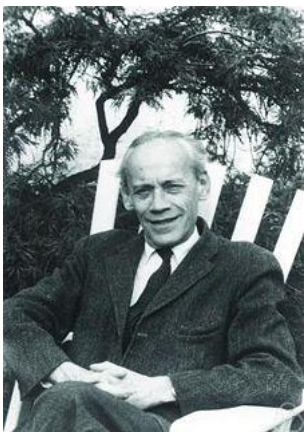
On conclut grâce à 6.2.5. □

6.6. Parenthèse sur les groupes quotients. — On pourra se reporter au chapitre 0 du polycopié du cours de tronc commun. Soit H un sous-groupe de G. On voudrait mettre **une structure de groupe** sur l'ensemble

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

des translatés à droites [31] de H de sorte que la surjection canonique $\pi : \mathrm{G} \to \mathrm{G}/\mathrm{H}$ qui envoie g sur $g\mathrm{H}$ soit un morphisme de groupes, exactement comme dans le cas d'un idéal dans un anneau [32].

30. 1898-1962
31. L'ensemble des translatés à gauche $\mathrm{H}g, g \in \mathrm{G}$ se note $\mathrm{H} \setminus \mathrm{G}$.
32. Le cardinal de G/H, fini ou non, s'appelle l'indice de H dans G.



Emil Artin

On doit donc avoir

$$g_1g_2\mathrm{H} = g_1\mathrm{H}g_2\mathrm{H} \text{ pour tout } g_1, g_2.$$

En particulier, pour $g_1g_2 = 1$, on obtient que nécessairement

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

Définition 6.6.1. — *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 est distingué, le noyau de tout morphisme de groupes est distingué. Mais, par exemple, le sous-groupe S_3 de S_4 n'est pas distingué (exercice) pas plus que $\mathbf{GL}_n(\mathbf{R})$ dans $\mathbf{GL}_n(\mathbf{C})$.

Une autre manière d'exprimer la propriété $\mathrm{H} \triangleleft \mathrm{G}$ est de dire $g\mathrm{H} = \mathrm{H}g$ pour tout g (et donc en particulier $\mathrm{G}/\mathrm{H} = \mathrm{H} \setminus \mathrm{G}$ (31)). On a alors

$$g_1g_2\mathrm{H} = g_1\mathrm{H}g_2\mathrm{H} \text{ pour tout } g_1, g_2.$$

Ceci permet de définir, de manière unique, une structure de groupe sur G/H **faisant de** π **un morphisme.** On laisse au lecteur le soin d'énoncer et de prouver la propriété universelle du quotient analogue à 3.3.2..

Définition 6.6.2. — *Soient* $f_i : \mathrm{G}_i \to \mathrm{G}_{i+1}, i = 1, 2$ *deux morphismes de groupes. On dit que la suite*

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

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

Le lecteur vérifiera que dire que l'exactitude signifie $f_2 \circ f_1 = 1$ et $\mathrm{Ker}(f_2) \subset \mathrm{Im}(f_1)$. De plus, lorsque G_1, (resp. G_3) est réduit au groupe trivial $\{1\}$), l'exactitude signifie que f_1 est injective (resp. f_2 surjective).

Lorsqu'on a une suite plus longue, l'exactitude de la suite signifie que les sous-suites à trois termes consécutifs sont exactes.

Exercice 6.6.3. — *Montrer que la suite*

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

si et seulement si f_3 *identifie* G_3 *au quotient de* G_2 *par* $\mathrm{G}_1 \xrightarrow{\sim} f_1(\mathrm{G}_1)$.

Exercice 6.6.4. — *Montrer que le noyau de* π *est* H. *Montrer par exemple que le groupe*

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

est isomorphe à $\mathbf{C}^*$.

6.7. 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 (6.2.5) 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 (6.2.2), l'extension K/L est galoisienne. On peut énoncer le théorème principal.

Théorème 6.7.1 **(Correspondance de Galois)**

i) L'application

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

est bijective, strictement décroissante, d'inverse

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

ii) L'extension $\mathrm{K}/\mathrm{K}^{\mathrm{H}}$ *est toujours 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 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 l'isomorphisme*

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

de 6.2.9.

v) En particulier, si L/k *est galoisienne, on a une suite exacte (cf. 6.6.2) canonique*

$$\{1\} \to \mathrm{Gal}(\mathrm{K}/\mathrm{L}) \to \mathrm{Gal}(\mathrm{K}/k) \to \mathrm{Gal}(\mathrm{L}/k) \to \{1\}. \tag{6.7.a}$$

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 6.5.1.
Ensuite, on a

$$fg(\mathrm{H}) = \mathrm{Gal}(\mathrm{K}/\mathrm{K}^{\mathrm{H}}) \overset{6.5.2}{=} \mathrm{H}.$$

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 (6.5.2).
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 (3.15.1). Comme K/k est galoisienne, on a $\sigma(\mathrm{K}) = \mathrm{K}$ (6.2.4) *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

$$\mathrm{card}\,\mathrm{Hom}_k(\mathrm{K}^{\mathrm{H}}, \Omega) \overset{6.1.4}{=} [\mathrm{K}^{\mathrm{H}} : k] = [\mathrm{K} : k]/[\mathrm{K} : \mathrm{K}^{\mathrm{H}}] = \mathrm{card}\,\mathrm{G}/\,\mathrm{card}\,\mathrm{H} = \mathrm{card}\,\mathrm{G}/\mathrm{H}$$

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 $\mathrm{K}^{\mathrm{H}}/\mathrm{K}$ galoisienne. □

Exercice 6.7.2. — *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.

6.8. Groupe de Galois d'un polynôme. — Soit P un polynôme (non constant) à coefficients de k de racines $x_1, \cdots, x_n$ (dans Ω, que l'on peut supposer unitaire).

Définition 6.8.1. — *On appelle groupe de Galois de* P *le groupe de Galois de son corps de racines* $\mathrm{K} = k[x_1, \cdots, x_n]$ *(6.3.2).*

On a le lemme suivant, faux si k n'est pas parfait.

Lemme 6.8.2. — *Le polynôme* $\mathrm{Q} = \prod(\mathrm{X} - x_i)$ *est encore à coefficients dans* k.

Démonstration. — Écrivons $\mathrm{P} = \prod \mathrm{P}_j^{n_j}$ où les P_i sont irréductibles unitaires distincts deux à deux. Comme chaque P_i est à racines simples (5.1.5), on a $\mathrm{Q} = \prod \mathrm{P}_j$. □

Remarque 6.8.3. — *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**. Ce groupe G ne dépend essentiellement que de P et pas de Ω (cf. 3.15.1 par exemple).

Rappelons que, G laissant k invariant, on a la formule

$$0 = g(\mathrm{P}(x_i)) = \mathrm{P}(g(x_i)). \tag{6.8.a}$$

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 $\sigma_g \in \mathrm{S}_n$. Trivialement, l'application $g \mapsto \sigma_g$ définit un morphisme de groupes *injectif*

$$\mathrm{G} \hookrightarrow \mathrm{S}_n,$$

où $n = \deg(\mathrm{P})$ (injectif simplement car les racines engendrent le corps de décomposition). En termes d'actions de groupes (Annexe D du polycopié de tronc commun), G agit fidèlement sur les racines de P.

C'est le point de vue fondateur de Galois et d'Abel [33] qui voyaient les groupes de Galois comme des sous-groupes de S_n.

Remarque 6.8.4. — *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.*

Proposition 6.8.5. — *Le polynôme* P *est* irréductible *si et seulement si l'action est* transitive.

33. 1802-1829

Niels Abel

Démonstration. — Supposons P irréductible. Les x_i s'identifient aux k-homomorphismes de $k[x_1] = k[\mathrm{X}]/(\mathrm{P})$ dans Ω (3.15.4), qui s'identifient comme on l'a vu aux éléments de G. L'action est donc **transitive** dans ce cas (6.3.1). 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 (6.8.a) appliquée à Q, R assure que G laissent 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 $\mathrm{Q} = \mathrm{P}$ (on aurait aussi pu utiliser la formule de l'exercice 6.a). □

Cette discussion explique l'importance du groupe symétrique et de ses classes de conjugaison dans la théorie. Rappelons sans démonstration quelques points connus.

6.9. Parenthèse sur le groupe symétrique. — Soit n un entier ≥ 2 (le cas $n = 1$ n'a pas d'intérêt). Le groupe symétrique $\mathrm{S}_n = \mathrm{Bijections}(\mathrm{X})$ agit à gauche sur $\mathrm{X} = \{1, \cdots, n\}$. 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 il existe $j \in \mathbf{Z}$ tel que $y = \sigma^j(x)$. Une classe d'équivalence s'appelle aussi une σ-orbite. Comme pour toute relation d'équivalence, X est réunion disjointes d'orbites $\mathrm{O}_i(\sigma)$. Soit

$$n_1 \geq n_2 \geq \cdots \geq n_d$$

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

Définition 6.9.1. — *Le type de σ est le d-uple $\bar{n} = (n_1, \cdots, n_d)$. On dit que σ est un cycle (de longueur n_1) si $d = 1$: on parle alors de d-cycle. Le support d'un cycle est son unique orbite non réduite à un élément dont le cardinal est appelé longueur du cycle.*

On note, non uniquement, 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 x. 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 6.9.2. — *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 S_n.

On définit la signature

$$\epsilon : \mathrm{S}_n \to \{\pm 1\}$$

par la formule

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

où σ est de type $(n_1, \cdots, n_d)$. On a le résultat fondamental suivant.

Proposition 6.9.3. — *La signature ϵ est l'unique morphisme surjectif de groupes de $\mathrm{S}_n \to \{\pm 1\}$.*

Le noyau A_n de la signature est donc un sous-groupe distingué, de cardinal $n!/2$: il s'appelle le groupe alterné. Les transpositions sont donc 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.

D'autre part, 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 la formule (vérifier !)

$$\sigma \circ (a_1, \cdots, a_m) \circ \sigma^{-1} = (\sigma(a_1), \cdots, \sigma(a_m)). \tag{6.9.a}$$

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 6.9.4. — *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 6.9.5. — *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. Montrer que A_n est engendré par les 3-cycles dès que $n \geq 3$.*

6.10. Discriminant. — Voyons une condition simple permettant de décider si on a $\mathrm{G} \subset \mathrm{A}_n$. C'est un cas particulier de la notion de *résolvante*.

Proposition 6.10.1. — *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^*. Si k est de caractéristique différente de 2, c'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.

Démonstration. — Visiblement $\mathrm{disc}(\mathrm{P})$ est non nul et invariant par G, donc 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.

On a

$$\sqrt{d}^\sigma = \prod_{i<j} (x_{\sigma(i)} - x_{\sigma(j)}).$$

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

$$\sqrt{d}^\sigma = (-1)^{|\sigma|} \prod_{i<j} (x_i - x_j)$$

où

$$|\sigma| = \mathrm{card}\{(i,j) \text{ tels que } i<j \text{ et } \sigma(i) > \sigma(j)\}.$$

On se souvient alors de la formule (6.9)

$$\epsilon(\sigma) = (-1)^{|\sigma|}$$

de sorte que

$$\sqrt{d}^\sigma = \epsilon(\sigma)\sqrt{d}.$$

Donc, si $\mathrm{G} \subset \mathrm{A}_n$, on a certainement $\sqrt{d} \in k$, indépendamment de la caractéristique de k. Inversement, si $\sqrt{d} \in k^*$, on a

$$\sqrt{d} = \epsilon(g)\sqrt{d}$$

autrement $\epsilon(g) = 1$ dans k ce qui signifie $\epsilon(g) = 1$ dans $\mathbf{Z}$ si k est de caractéristique nulle, ou bien $\mathrm{car}(k)|(1 - \epsilon(g))$ en caractéristique positive, d'où le lemme. □

Exercice 6.10.2. — *Soient* $\mathrm{P}_1, \cdots, \mathrm{P}_r$ *des polynômes de degrés* $d_i > 0$ *séparables à coefficients dans* $\mathbf{F}_p$ *et premiers entre eux deux à deux. Montrer que le Frobenius du corps de décomposition des* P_i *est un produit de cycles disjoints de longueur* d_i*. En déduire que son groupe de Galois sur* $\mathbf{F}_p$ *est d'ordre le* PPCM *des* d_i*.*

Exercice 6.10.3. — *Soit* H *un sous-groupe d'indice* G*. Montrer que les ensembles* G/H *et* H G *ont même cardinal. 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*.*

Exercice 6.10.4. — *Montrer que le groupe de Galois d'un polynôme de degré* 2 *est trivial ou* $\mathbf{Z}/2\mathbf{Z}$*. Montrer qu'en degré* 3*, caractéristique différente de* 2*, c'est* $\mathbf{Z}/3\mathbf{Z}$ *ou bien* S_3*, ce dernier cas ne se produisant 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 6.10.5. — *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 6.10.6. — *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. Cyclotomie

Soit n un entier ≥ 1, premier à la caractéristique de k. 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 (5.1.4). L'ensemble $\mu_n(\Omega)$ de ses racines dans Ω a donc pour cardinal n et est un sous-groupe (fini) Ω^*, donc est cyclique (4.2.1), 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, ou, de façon un peu abusive, 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 $\mathbf{Z}/n\mathbf{Z}$ [34].

Comme $\mu_n(\Omega)$ est engendré par ζ_n, le corps de décomposition de $X^n - 1$ est simplement $k[\zeta_n]$ qui est donc galoisien sur k : notons G_n son groupe de Galois. Comme $X^n - 1$ est de degré n, le cardinal de G_n est $\leq n$. On a mieux.

7.1. Sur le groupe de Galois de l'extension cyclotomique générale. — L'image de ζ_n par un élément du groupe de Galois $g \in G_n = \mathrm{Gal}(\mathbf{Q}[\zeta_n]/\mathbf{Q})$ s'écrit de façon 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, on a même $\chi(g)$ inversible (*ie* est la classe d'un entier premier à n). On définit ainsi une application

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

qui est visiblement un morphisme de groupes.

Remarque 7.1.1. — *Si on avait, pour définir χ, choisi une autre racine primitive n-ième de l'unité, on aurait trouvé le même homomorphisme de groupes, dit* caractère cyclotomique. *En effet, il est caractérisé par $g(\zeta) = \zeta^{\chi(g)}$ pour tout $\zeta \in \mu_n(\mathbf{C})$.*

Bien entendu, χ est *injectif* (car ζ_n engendre $\mathbf{Q}[\zeta_n]$). On a donc montré.

Proposition 7.1.2. — *χ identifie G_n à un sous-groupe de $(\mathbf{Z}/n\mathbf{Z})^*$. En particulier, il est commutatif.*

Dorénavant, dans cette section, $k = \mathbf{Q}$ et, par exemple, $\Omega = \mathbf{C}$.

34. 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).

7.2. Irréductibilité du polynôme cyclotomique sur Q. — 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 complexes de la forme $\zeta_n^m = \exp(\frac{2i\pi m}{n})$ où $m \in (\mathbf{Z}/n\mathbf{Z})^*$.

Définition 7.2.1. — *On définit le n-ième polynôme cyclotomique par la formule*

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

Un élément de G_n, étant injectif, envoie un générateur de $\mu_n(\mathbf{C})$ sur un autre générateur, donc permute les racines primitives de l'unité. Les coefficients du polynôme cyclotomiques sont dans $\mathbf{Q}[\zeta_n]^{\mathrm{G}_n}$ et donc dans $\mathbf{Q}$ d'après le lemme 6.5.1. On déduit donc que $\Phi_n(\mathrm{X})$ est un annulateur (unitaire) de degré

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

de ζ_n dans $\mathbf{Q}[\mathrm{X}]$.

En fait, Φ_n est irréductible et à coefficients entiers. Commençons par prouver un lemme élémentaire.

***Lemme 7.2.2* (Gauss)**. — *Soient P, Q deux polynômes à coefficients entiers avec Q unitaire. Alors, les quotient, reste de la division euclidienne de P par Q sont à coefficients entiers.*

Démonstration. — Clair (poser la division !). □

Corollaire 7.2.3. — *On a $\Phi_n(\mathrm{X}) \in \mathbf{Z}[\mathrm{X}]$.*

Démonstration. — Toute racine n-ième 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 disjointes paramétrée par les diviseurs d de n des racines primitives d-ièmes. Comme $\mathrm{X}^n - 1 = \prod(\mathrm{X} - \zeta)$, le produit étant étendu aux racines n-ièmes de 1, on déduit la formule

$$\mathrm{X}^n - 1 = \prod_{d|n} \Phi_d(\mathrm{X}). \tag{7.2.a}$$

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 7.2.2 i) pour tout $d|n$, donc aussi pour $d = n$. □

Le lemme suivant est dû à Gauss.

***Lemme 7.2.4* (Gauss)**. — *Soit P un polynôme non constant de $\mathbf{Z}[\mathrm{X}]$.*

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

ii) Si P est unitaire, tous ses facteurs unitaires à coefficients dans $\mathbf{Q}$ sont en fait 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 chassant les dénominateurs de $\mathrm{P}_1, \mathrm{P}_2$, on a une identité du type

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

avec $\bar{\mathrm{P}}_1, \bar{\mathrm{P}}_2 \in \mathbf{Z}[\mathrm{X}]$ 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 $\deg(\mathrm{P}_2) = 0$ et on a fini.

Sinon, 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 trouve que p divise n et 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 $n = \pm 1$.

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 $\tilde{\mathrm{P}}_i$, 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 7.2.5. — *Un complexe est dit entier algébrique (ou entier*[35] *lorsque le contexte est clair) s'il est racine d'un polynôme unitaire à coefficients entiers.*

Par exemple, ζ_n est entier, mais $1/2$ ne l'est pas (cf. exercice 7.2.6). On reviendra sur cette notion importante (10.2).

Exercice 7.2.6. — *Montrer que $x \in \mathbf{Q}$ est entier sur $\mathbf{Z}$ si et seulement si il c'est un... entier relatif.*

Le lemme de Gauss 7.2.4 donne immédiatement le résultat suivant.

Corollaire 7.2.7. — *Le polynôme minimal d'un élément entier est à coefficients entiers.*

Théorème 7.2.8. — *Le polynôme cyclotomique sur $\mathbf{Q}$ est irréductible sur $\mathbf{Q}$.*

Démonstration. — La preuve, due à Gauss, est très astucieuse. Soit P le minimal de ζ_n. Il suffit de prouver $\Phi_n|\mathrm{P}$, ou encore que toutes les racines primitives annulent P.

Soit p premier ne divisant pas n et ζ une racine de P (le minimal de ζ_n), certainement primitive car $\mathrm{P}|\Phi_n$. La clef est le lemme suivant.

35. Pour éviter les confusions, on dira que les éléments de $\mathbf{Z}$ sont les *entiers relatifs*.

Lemme 7.2.9. — *ζ^p est une racine de* P.

Démonstration. — supposons le contraire. Écrivons

$$\mathrm{X}^n - 1 = \mathrm{P}(\mathrm{X})\mathrm{S}(\mathrm{X}).$$

Comme ζ_n est entier, on a $\mathrm{P}(\mathrm{X}) \in \mathbf{Z}[\mathrm{X}]$ d'après 7.2.7, et, 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|Q dans $\mathbf{Q}[\mathrm{X}]$ (irréductibilité de P) donc dans $\mathbf{Z}[\mathrm{X}]$ puisque P est de plus unitaire. Réduisons modulo p. On a

$$\bar{\mathrm{Q}} = \bar{\mathrm{S}}^p$$

(encore le Frobenius !). Comme $n \neq 0$ dans $\mathbf{F}_p$ par hypothèse, $\mathrm{X}^n - 1$ 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 multiple 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 $\mathbf{F}_p[\mathrm{X}]$, une contradiction puisque $\bar{\mathrm{P}}$ est séparable. □

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' primitive). En décomposant m en facteurs premiers, une application répétée du lemme donne ζ' racine de P et donc $\Phi_n | \mathrm{P}$. □

Ainsi,

$$\operatorname{card} \mathrm{G}_n = [\mathbf{Q}[\zeta_n] : \mathbf{Q}] = \varphi(n)$$

de sorte que χ est un morphisme injectif (7.1.2) entre groupes de même cardinal :

Théorème 7.2.10. — *Le morphisme $\chi : \mathrm{Gal}(\mathbf{Q}[\zeta_n]/\mathbf{Q}) \to (\mathbf{Z}/n\mathbf{Z})^*$ est un isomorphisme.*

Exercice 7.2.11. — *Soit $n \geq 1$ et p premier ne divisant pas n. Montrer que si $\Phi_n \mod (p)$ a une racine dans $x \in \mathbf{F}_p$, alors x est d'ordre exactement n dans $\mathbf{F}_p^*$. En déduire qu'on a $p \equiv 1 \mod (n)$ puis qu'il existe une infinité de nombres premiers congrus à 1 modulo n (forme faible du théorème de la progression aritmétique de Dirichlet).*

7.3. 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 de 7.2.10, cette surjection n'est autre que le morphisme canonique

$$(\mathbf{Z}/n\mathbf{Z})^* \to (\mathbf{Z}/d\mathbf{Z})^*.$$

On retrouve au passage 3.8.3.

Proposition 7.3.1. — *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 $\mathrm{K}_i = \mathbf{Q}[\zeta_n],\ i = n, m$ de K, définis (correspondance de Galois) d'après ce qui précède par les sous-groupes $\Gamma_i,\ i = n, m$. D'après 6.7.2, on doit simplement montrer $\Gamma_n \cap \Gamma_m = \{1\}$ (qui prouve $\mathrm{K}_n\mathrm{K}_m = \mathbf{Q}[\zeta_\pi]$) 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 de $\Gamma_n \cap \Gamma_m$, 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 n, m 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 $\Gamma_i = 1 + p^i\mathbf{Z}/p^\mu\mathbf{Z},\ i = \nu, \mu$ et donc le groupe engendré est $\Gamma_\nu = \Gamma_\delta$. □

Remarque 7.3.2. — *Donnons une autre preuve, moins galoisienne. On pose* $\mathrm{PPCM}(n,m) = \varpi$ *et* $\mathrm{PGCD}(n,m) = \delta$. *Le premier point est élémentaire. Posons* $\varpi = n\nu, \varpi = m\mu$ *où* ν *et* μ *sont premiers entre eux. On a alors,*

$$\zeta_n = \zeta_\varpi^\nu \text{ et } \zeta_m = \zeta_\varpi^\mu$$

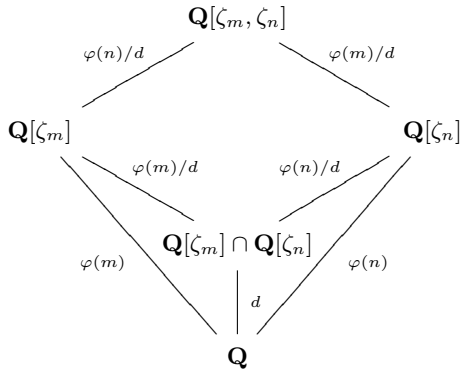
prouvant

$$\mathbf{Q}[\zeta_n, \zeta_m] \subset \mathbf{Q}[\zeta_\varpi].$$

Inversement, choisissons a, b *entiers tels que* $a\mu + b\nu = 1$. *On a alors* $\zeta_\varpi = \zeta_m^a\zeta_n^b$ *prouvant l'inclusion réciproque.*
La deuxième égalité est plus subtile. Posons maintenant $n = \delta\nu, m = \delta\mu$ *où* ν *et* μ *sont premiers entre eux. On a* $\zeta_\delta = \zeta_n^\nu = \zeta_m^\mu$ *prouvant l'inclusion*

$$\mathbf{Q}[\zeta_\delta] \subset \mathbf{Q}[\zeta_n] \cap \mathbf{Q}[\zeta_m]$$

Inversement, les extensions cyclotomiques $\mathbf{Q}[\zeta_n]/\mathbf{Q}$ *étant galoisiennes, on connaît les degrés des diverses extensions grâce à 8.1.2, qui sont résumés comme suit.*



Se souvenant de la formule élémentaire $\delta\varpi = nm$*, l'égalité* $\phi(\varpi) = [\mathbf{Q}[\zeta_n,\zeta_m]:\mathbf{Q}]$ *devient alors*

$$\varphi(n)\varphi(m) = d\varphi(nm/\delta).$$

Comme

$$\varphi(\delta)\varphi(nm/\delta) = \varphi(n)\varphi(m),$$

on a (exercice de PC -décomposer n, m *en facteurs premiers par exemple-)* $d = \varphi(\delta)$ *et la proposition en découle.*

Exercice 7.3.3. — *Soit* $z \in \mathbf{C}$ *et* K *le corps des racines du minimal de* z*. Montrer que* z *est constructible (2.1.1) à la règle et au compas si et seulement si tous ses conjugués le sont. En déduire que* z *est constructible si et seulement si* $[\mathrm{K}:\mathbf{Q}]$ *est une puissance de* 2*. Donner alors une preuve de (2.1.5) en utilisant le résultat (9.3.8) infra.*

8. Appendice : 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 (7.3.1). Cet appendice n'est pas essentiel pour la suite et peut être ignoré en première lecture.
On suppose que toutes les extensions considérées sont contenues dans une extension algébriquement close Ω d'un corps k.

8.1. Extensions composées, clôture galoisienne. — 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.

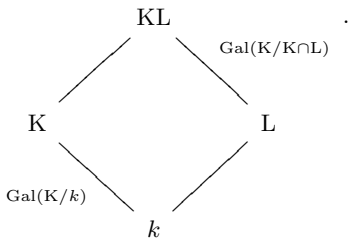
Lemme 8.1.1. — *Soit* K *un extension finie de* k. *Il existe un unique sous-corps de* Ω *contenant* K *qui est galoisien sur* k : *on l'appelle la clôture galoisienne de* K/k.

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). On laisse au lecteur le soin de vérifier que le corps des racines du minimal de x sur k est l'extension cherchée. □

Théorème 8.1.2. — *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,* KL/k *et* $\mathrm{K} \cap \mathrm{L}/k$ *le sont également.*

Démonstration. — Prouvons i). Soit x un élément primitif de K/k de minimal $\mathrm{P} \in k[\mathrm{X}]$. Visiblement, $\mathrm{KL} = \mathrm{L}[x]$ et le 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, et donc 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 $\mathrm{KL} = \mathrm{L}[\mathrm{X}]/\mathrm{Q}$ 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.
Prouvons 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 et on conclut comme d'habitude). □

Le point i) du théorème se retient bien graphiquement.



Corollaire 8.1.3. — *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 (exercice). Les morphismes de restrictions

$$\mathrm{Gal}(\mathrm{K}/k) \to \mathrm{Gal}(\mathrm{K} \cap \mathrm{L}/k) \text{ et } \mathrm{Gal}(\mathrm{L}/k) \to \mathrm{Gal}(\mathrm{K} \cap \mathrm{L}/k)$$

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, on a $j_1 \circ i$ 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 8.1.4. — *Supposons* K/k *et* L/k *galoisiennes. Le morphisme (injectif)* i *induit un isomorphisme de* $\mathrm{Gal}(\mathrm{KL}/k)$ *sur le sous-groupe de* $\mathrm{Gal}(\mathrm{K}/k) \times \mathrm{Gal}(\mathrm{L}/k)$*, appelé produit amalgamé,*

$$\mathrm{Gal}(\mathrm{K}/k) \times_{\mathrm{Gal}(\mathrm{K} \cap \mathrm{L}/k)} \mathrm{Gal}(\mathrm{L}/k),$$

constitué des couples (u, v) *tels que* $j_1(u) = j_2(v)$*.*

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

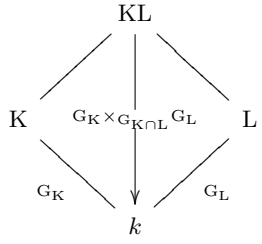
$$1 \to \mathrm{N} \to \mathrm{G} \to \mathrm{G_{K \cap L}} \to 1.$$

Comparant les cardinaux, on déduit

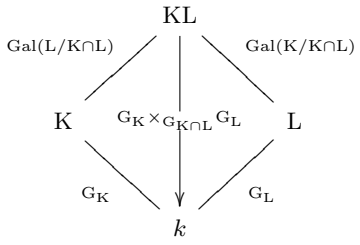
$$\mathrm{card}\, \mathrm{G} = [\mathrm{K} : k][\mathrm{L} : k]/[\mathrm{K} \cap \mathrm{L} : k]$$

et on conclut grâce à 8.1.3. □

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 se retient graphiquement comme suit.



qu'on peut compléter d'après ce qui précède en


KL
Gal(L/K∩L)
Gal(K/K∩L)
K
$G_K \times_{G_{K\cap L}} G_L$
L
G_K
G_L
k

9. Résolubilité par radicaux

9.1. Extensions cycliques. — Dans ce paragraphe, n désigne un entier ≥ 2 et k 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.

On sait alors (tout sous groupe fini de k^* est cyclique) que $\mu_n(k)$ est, non canoniquement en général, isomorphe à $\mathbf{Z}/n\mathbf{Z}$ de sorte qu'existent dans k les racines primitives (d'ordre n) de 1 (au nombre de $\varphi(n)$).

Soit a un élément de $k-0$ et $\mathrm{K}=k[\alpha], \alpha=a^{1/n}$ le corps de rupture de $\mathrm{P}(\mathrm{X})=\mathrm{X}^n-a$. Comme les racines de X^n-a sont les multiples de a par les racines n-ièmes de l'unité, qui sont dans k par hypothèse, K est aussi le corps des racines de X^n-a et donc est galoisienne sur k. Soit G son groupe de Galois. On a une application

$$\kappa : \mathrm{G} \to \mu_n(k)$$

définie comme suit. Si $g \in \mathrm{G}$, l'élément $g(\alpha)$ est une racine de P donc de la forme $\zeta\alpha$ pour $\zeta \in \mu_n(k)$. On pose alors $\kappa(g)=g(\alpha)/\alpha$. C'est un morphisme de groupes.

Lemme 9.1.1. — *κ est injective et* G *est cyclique de cardinal d divisant n. De plus,* P *irréductible si et seulement si a n'est pas une puissance d-ième dans k pour tout diviseur d de n distinct de* 1*, ou, de façon équivalente, si* $\mathrm{G}=\mu_n(k)$.

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 $[\mathrm{K}:k]=n$ et donc κ surjective. Supposons P irréductible, et donc $\mathrm{G}=\mu_n(k)$. Soit $\zeta=\kappa(g)$ primitive dans $\mu_n(k)$ et $d|n$ tel que $\alpha^d \in k$. 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 $\delta|n$ strictement. 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.

Théorème 9.1.2 **(Kummer [36])**. — *Soit* K/k *une extension galoisienne (k contenant les racines de l'unité). On suppose que le groupe de Galois* $\mathrm{G}=\mathrm{Gal}(\mathrm{K}/k)$ *est cyclique d'ordre n. Alors, il existe $a \in \mathrm{K}$ tel que* K *soit le corps des racines de* X^n-a.

Démonstration. — C'est de l'algèbre linéaire. Soit g un générateur de Galois : il vérifie $g^n=\mathrm{Id}$ vu dans $\mathrm{End}_k(\mathrm{K})$. Par hypothèse, X^n-1 est scindé sur k à racines simples, donc est diagonalisable. La formule $g(xy^{-1})=g(x)g(y)^{-1}$ assure que l'ensemble des valeurs propres de G est 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 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, les $\zeta^i x$,

distincts, qui sont nécessairement dans K qui est galoisien de sorte que $\mathrm{K} = k[x]$. Ainsi, ce sont tous les conjugués de x, et donc le minimal de x est

$$\prod_{1\leq i\leq n}(\mathrm{X}-\zeta^i x) = \mathrm{X}^n - a$$

avec $a \in \mathrm{K}$. □

Ernst Kummer

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

$$\mathrm{K} = \oplus_{a\in\mu_n}\mathrm{K}_a \text{ avec } \mathrm{K}_{\zeta^i} = kx^i \tag{9.1.a}$$

où x est non nul dans K_ζ.

Exercice 9.1.3. — *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_2 cyclique. Donner un exemple où G n'est pas commutatif.*

9.2. Commentaire. — 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 [37]-Weber [38], assure que la réciproque est vraie ! C'est une conséquence de la théorie du corps de classes, vaste sujet qui débouche naturellement sur la visionnaire théorie de Langlands [39] sujet très difficile et actif à l'heure qu'il est.

9.3. Intermède sur les 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.

36. 1810-1893
37. 1823-1891
38. 1842-1913
39. 1936-

Leopold Kronecker

Heinrich Martin Weber

Robert Langlands

Définition 9.3.1. — *Un groupe* G *est dit résoluble s'il possède filtration croissante par des sous-groupes*

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

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

On dira simplement que les quotients successifs sont commutatifs.

Exercice 9.3.2. — *Vérifier que* $\mathrm{S}_3, \mathrm{S}_4$ *sont résolubles. Montrer que le groupe des matrices complexes de taille* $n \geq 2$ *de déterminant* 1 *ne l'est pas.*

Exercice 9.3.3. — *On se propose de montre 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 *de* $\ln(f)$ *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

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

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

On rappelle que le groupe dérivé DG de G est le groupe engendré par les commutateurs $aba^{-1}b^{-1}$. C'est un sous-groupe distingué de G, et G/DG est commutatif : on a tout fait pour. On définit alors par récurrence

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

Lemme 9.3.4. — 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 9.3.5. — *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 9.3.6. — *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 *résoluble.*

Exercice 9.3.7. — *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 *opère 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 9.3.2.*

Exercice 9.3.8 **(Difficile)**. — *Soit* G *un groupe de cardinal* p^n *avec* p *premier. 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 *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.*

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

9.4. Applications aux équations. — On suppose k de **caractéristique nulle**. On dira 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. Elle est dite *résoluble* (par radicaux) si il existe une extension finie L/K contenant K tel que L/k radicale. 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, *ie* la notion intuitive de résolubilité par radicaux !

Théorème 9.4.1 **(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 vraie (ce n'est pas difficile, connaissant la théorie de Kummer) ; elle sera détaillée en PC. 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

$$k = \bar{L}_0 \subset \bar{L}_1 \cdots \subset \bar{L}_n = L$$

tels que $\bar{L}_{i+1} = \bar{L}_i[x_i]$ et $x_i^{n_i} \in \bar{L}_i$.
Le problème est que les $\bar{L}_i$ n'ont aucune raison d'être galoisiens sur k. Remédions à cela. On veut utiliser la théorie 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

$$L_{i+1} = k[\zeta_n, X_i], i = 0, \cdots, n-1,$$

qui par construction est galoisienne sur k (comme d'habitude, ζ_n désigne une racine primitive $n$ième de l'unité dans Ω). On pose $L_{-1} = k, X_{-1} = \{\zeta_n\}$ de sorte qu'on a

$$L_{i+1} = L_i[X_i] \text{ pour } i \geq -1$$

avec L_i galoisienne sur $L_{-1} = k$ pour tout i donc *a fortiori* sur $L_j, -1 \leq j \leq i$.
Comme $\mathrm{Gal}(K/k)$ est un quotient (6.7.1) de $\mathrm{Gal}(L_n/L_{-1})$, il suffit de montrer que ce dernier est résoluble (9.3.5). Montrons par récurrence sur i que $\mathrm{Gal}(L_i/L_{-1})$ est résoluble.

Lemme 9.4.2. — *Chaque groupe* $\mathrm{Gal}(L_{i+1}/L_i), i \geq -1$ *est résoluble.*

Démonstration. — Comme $\mathrm{Gal}(L_0/L_{-1})$ est commutatif (7.1.2), on peut supposer $i \geq 0$.
Si $i \geq 0$, L_{i+1} est obtenu en adjoignant à L_i les conjugués $y_j, j = 1, \cdots, \deg_{L_i}(x_i)$ de x_i sur L_i. On a donc une tour d'extension

$$M_0 = L_i \subset M_1 = L_i[y_1] \subset \cdots \subset M_d = L_i[y_1, \cdots, y_d] = L_{i+1}.$$

Comme $y_j^n \in L_i$ et $\zeta_n \subset L_i$, 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 $M_{\delta'}, \delta' \leq \delta$. Comme de plus, $M_{\delta+1} = M_\delta[y_{\delta+1}]$, chaque extension élémentaire intermédiaire $M_{\delta+1}/M_\delta$ est de Kummer, donc galoisienne de groupe cyclique (c'est la partie facile de la théorie de Kummer). Or, on a une filtration

$$1 = G_0 = \mathrm{Gal}(M_d/M_d) \subset G_2 = \mathrm{Gal}(M_d/M_{d-1}) \cdots \subset G_d = \mathrm{Gal}(M_d/M_0).$$

Or, on a

$$G_{\delta+1}/G_\delta \xrightarrow{\sim} \mathrm{Gal}(M_{\delta+1}/M_\delta)$$

(grâce à la suite exacte fondamentale (6.7.a)) et donc est abélien. La proposition 9.3.5 assure que G_d est résoluble. □

La théorie de Galois (6.7.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 9.3.5. □

Soit L le corps des fractions de $\mathbf{C}[\mathrm{X}_1, \cdots, \mathrm{X}_n]$ où les X_i sont des indéterminées. Le groupe symétrique S_n agit sur L par permutation des indices. Soit $\mathrm{K} = \mathrm{L}^{\mathrm{S}_n}$: l'extension L/K est galoisienne de groupe de Galois S_n d'après le lemme d'Artin. On sait d'autre part (théorème des fonctions symétriques) qu'on a

$$\mathrm{K} = \mathrm{Frac}(\mathbf{C}[\sigma_1, \cdots, \sigma_n])$$

où les σ_i sont les fonctions symétriques élémentaires des X_i définies par l'identité

$$\prod(\mathrm{X} - \mathrm{X}_i) = \mathrm{X}^n + \sum_{i=1}^{n-1}(-1)^i \sigma_i \mathrm{X}^{n-i}. \tag{9.4.a}$$

Remarque 9.4.3. — *On peut aussi invoquer le lemme d'Artin et la majoration triviale* $[\mathrm{L} : \mathrm{Frac}(\mathbf{C}[\sigma_1, \cdots, \sigma_n])] \leq n!$ *pour prouver* $\mathrm{K} = \mathrm{Frac}(\mathbf{C}[\sigma_1, \cdots, \sigma_n])$.

La formule 9.4.a prouve au passage que L est le corps de décomposition sur K de $\mathrm{P}(\mathrm{X}) = \mathrm{X}^n + \sum_{i=1}^{n-1}(-1)^i \sigma_i \mathrm{X}^{n-i}$.

Je dis que l'équation générale à coefficients dans K

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

n'est pas résoluble par radicaux pour $n \geq 5$, ce qui se traduit d'après la discussion précédente par le résultat suivant.

Théorème 9.4.4 **(Abel,Galois)**. — L/K *n'est pas résoluble dès que* $n \geq 5$.

Démonstration. — Comme $\mathrm{D}(\mathrm{S}_n) \subset \mathrm{A}_n$ (la signature d'un commutateur vaut 1), il suffit de prouver le lemme suivant.

Lemme 9.4.5. — *Si* $n \geq 5$, *on a* $\mathrm{D}(\mathrm{A}_n) = \mathrm{A}_n$.

Démonstration. — $n \geq 3$, donc A_n engendré par les 3-cycles (6.9.5). 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). Soit d, e distincts de a, b, c (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 $\gamma \in \mathrm{D}(\mathrm{A}_n)$. □

□

10. Réduction modulo p

Dans cette partie, nous allons donner des méthodes permettant d'étudier des groupes de Galois de polynômes unitaires à coefficients entiers par réduction modulo p. Bien entendu, la situation sur $\mathbf{F}_p$ est, au moins théoriquement, très simple : on sait par exemple factoriser les polynômes (Berlekamp [40]), les extensions sont toujours galoisiennes et de groupes Galois cyclique, avec en prime un générateur canonique, le Frobenius.

Elwyn Berlekamp

On se donne un nombre premier p. On va comparer les groupes de Galois de P, *ie* celui de son corps des racines (6.8) et du corps des racines lorsque de plus $\bar{\mathrm{P}}$ est séparable. L'intérêt est que les groupes de Galois des extensions de corps finis sont très simples, cycliques, engendrés par le Frobenius. Le résultat principal pour nous est que, **sous ces conditions, il existe un élément de** $\mathrm{Gal}(\mathrm{P}/\mathbf{Q})$**, bien défini à conjugaison près, dont la classe de conjugaison dans** S_n **est la même que celle du Frobenius** (pour les plongements canoniques des groupes de Galois).
Le lecteur peut se contenter dans un premier temps de ce résultat (cf. l'énoncé du théorème fondamental 10.4.4) et laisser les preuves pour une seconde lecture (bien qu'elles ne soient pas difficiles).

10.1. Spécialisation du groupe de Galois. — Soit P un polynôme *unitaire* séparable à coefficients entiers [41]. 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 (7.2.5).

Lemme 10.1.1. — *Le corps des fractions* K *de* A *est le corps de décomposition de* P *dans* $\mathbf{C}$.

Démonstration. — En effet, A est contenu dans le corps de décomposition L de P car $z_i \in \mathrm{L}$ pour tout i, 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 cela, on va donner un caractérisation des entiers en tout point analogue celle des algébriques (3.12.1).

40. 1940-

41. le lecteur savant adaptera la preuve au cas où l'anneau de coefficients $\mathbf{Z}$ est remplacé par un anneau factoriel, voire intégralement clos

10.2. Somme, produits d'entiers. —

Définition 10.2.1. — *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 $\mathbf{C}$ vu comme $\mathbf{Z}$-algèbre, on retrouve la notion d'entier algébrique(7.2.5). On généralise (3.12.1) ainsi :

Proposition 10.2.2. — *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*[42].

Démonstration. — La partie directe est claire : si b a un 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'homotéthie $h_b \in \mathrm{End}_{\mathrm{C}}(\mathrm{B}')$ de rapport b dans C). Soit $\mathrm{P} = \det(\mathrm{XId} - \alpha)$ le polynôme caractéristique de α : c'est un polynôme unitaire de C[X] qui annule α (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 (3.12.6), on déduit

Corollaire 10.2.3. — *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 $\mathrm{C} = \mathrm{C}[x, y]$ qui 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 10.2.4. — *L'ensemble des entiers algébriques est un sous-anneau de* $\mathbf{C}$. *En particulier, tous les éléments de* A *sont des entiers.*

Exercice 10.2.5 **(Lemme de Kronecker)**. — *Soit* z *un nombre complexe qui est entier sur* $\mathbf{Q}$ *et* z_i *ses conjugués. Montrer que les* z_i *sont entiers. Montrer que tous les polynômes* $\prod(\mathrm{X} - z_i^n)$ *où* $n \in \mathbf{N}$ *sont à coefficients entiers. En déduire que si* $|z_i| \leq 1$ *pour tout* i, *alors où bien* $z = 0$ *ou bien les* z_i *sont des racines de l'unité.*

10.3. Norme des éléments de A. — Pour tout complexe algébrique z sur $\mathbf{Q}$, on définit sa norme $\mathrm{N}(z)$ comme le produit des 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 $\mathrm{P} \in \mathbf{Z}[\mathrm{X}]$ (7.2.7).

Lemme 10.3.1. — *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 complexes $\sigma(a), \sigma \in \mathrm{Hom}_{\mathbf{Q}}(\mathbf{Q}[a], \mathbf{C})$. Comme $\mathbf{Q}[a] = \mathbf{Q}[pa]$, le complexe pa a d conjugués distincts qui sont $p\sigma(a), \sigma \in \mathrm{Hom}_{\mathbf{Q}}(\mathbf{Q}[a], \mathbf{C})$. On déduit la formule

$$\mathrm{N}(pa) = p^{\deg_{\mathbf{Q}}(a)}\mathrm{N}(a)$$

d'une part, et, d'autre part,

$$\mathrm{N}(pa) = \mathrm{N}(1) = 1$$

ce qui est absurde car $\mathrm{N}(z) \in \mathbf{Z}$ car a est un entier algébrique d'après 10.2.4. □

42. Autrement dit, tel 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.

10.4. Groupe de décomposition. — Soit alors $\bar{\mathfrak{p}}$ un idéal maximal de l'anneau (non nul !) $\bar{\mathrm{A}}$. On pourra remarquer que son existence est tout à fait indépendante de l'axiome du choix (utiliser par exemple que $\bar{\mathrm{A}}$ est un espace vectoriel de dimension finie sur k, puisque A est de type fini sur $\mathbf{Z}$). Soit $\mathfrak{p}$ son image inverse dans A, autrement dit le noyau de la surjection canonique

$$\mathrm{A} \twoheadrightarrow \bar{\mathrm{A}} \twoheadrightarrow \bar{\mathrm{A}}/\bar{\mathfrak{p}} = k.$$

Comme p est nul dans $\bar{\mathrm{A}} = \mathrm{A}/p\mathrm{A}$, le corps k est de caractéristique p.

Remarque 10.4.1. — *Il est utile d'observer qu'on a* $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$*, simplement car* $\mathfrak{p} \cap \mathbf{Z}/p\mathbf{Z}$ *est le noyau du morphisme* $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z} \to \mathrm{A}/\mathfrak{p}$ *qui 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 de corps finis. De même que A est engendré par les monômes en les z_i à coefficients des $\mathbf{Z}$, de même k est engendré par les monômes en les $x_i = z_i \mod \mathfrak{p}$ à coefficients dans $\mathbf{F}_p$. **Autrement dit,** k **est le corps de décomposition de** $\bar{\mathrm{P}}$ **sur** $\mathbf{F}_p$**,** ce qui, au passage, prouve à nouveau qu'il est de dimension finie sur $\mathbf{F}_p$.
Le groupe de Galois $\mathrm{G} = \mathrm{Gal}(\mathrm{K}/\mathbf{Q})$ permute les z_i et donc laisse stable A.

Définition 10.4.2. — *On appelle groupe de décomposition de* $\mathfrak{p}$ *le sous-groupe* $\mathrm{D} = \mathrm{D}_{\mathfrak{p}}$ *de* G *fixant* $\mathfrak{p}$*.*

Théorème 10.4.3. — *L'action de* G *sur* A *induit une action de* D *sur* k*. Le morphisme induit* $\mathrm{D} \mapsto \mathrm{Gal}(k/\mathbf{F}_p)$ *est surjectif.*

Démonstration. — Comme l'action de D sur A laisse $\mathfrak{p}$ globalement invariant, elle définit une action sur le quotient $k = \mathrm{A}/\mathfrak{p}$. 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 $k/\mathbf{F}_p$.
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 $\mathrm{A}/\mathfrak{p}$. 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.
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, on peut donc 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 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

$$\prod_{\sigma \in \mathrm{G}al(k/\mathbf{F}_p)} (\mathrm{X} - \sigma(x))$$

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.

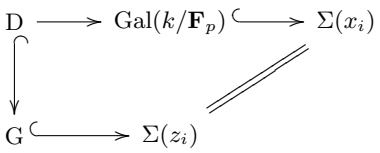
Théorème 10.4.4. — *Supposons que* $\bar{\mathrm{P}}$ *soit à racines simples (dans* $\bar{\mathbf{F}}_p$*). Alors, la flèche* $\mathrm{D} \twoheadrightarrow \mathrm{Gal}(k/\mathbf{F}_p)$ *est un isomorphisme du sous-groupe* D *de* $\mathrm{Gal}(\mathrm{P}/\mathbf{Q})$ *sur le groupe* $\mathrm{Gal}(\bar{\mathrm{P}}/\mathbf{F}_p)$ *et est compatible aux plongements dans le groupe symétrique (cf. 10.4.a) des groupes de Galois définis par les racines* z_i *de* P *et* $z_i \mod \mathfrak{p}$ *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

$$\Sigma(z_i) = \Sigma(x_i).$$

On a un diagramme visiblement

(10.4.a)



qui prouve l'injectivité de $\mathrm{D} \to \mathrm{Gal}(k/\mathbf{F}_p)$. Mais on savait déjà que la flèche était surjective ! □

Remarque 10.4.5. — *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.

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 de A tels que $\mathrm{A}/\mathfrak{p} \xrightarrow{\sim} \mathrm{A}/\mathfrak{q} \xrightarrow{\sim} \mathbf{F}_p$.

Proposition 10.4.6. — *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. — le second point est laissé en exercice. Pour le premier, 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 permet de construire alors $x \in \mathrm{A}$ tel que $x \equiv 1 \mod g(\mathfrak{q})$ pour tout g et $x \equiv 0 \mod \mathfrak{p}$. La norme $\prod_{g\in\mathrm{G}} g(x)$ de x est d'une part dans $p\mathbf{Z} = \mathfrak{p} \cap \mathbf{Z} = \mathfrak{q} \cap \mathbf{Z}$. Elle est donc également dans $\mathfrak{q}$ et donc un des facteurs $g(x)$ est dans $\mathfrak{q}$, autrement dit $x \equiv 0 \mod g^{-1}(\mathfrak{q})$, une contradiction. □

En particulier, $\mathrm{D}_\mathfrak{p}$ et $\mathrm{D}_\mathfrak{q}$ sont isomorphes (via l'automorphisme intérieur $h \mapsto ghg^{-1}$, et même égaux si G est abélien). En particulier, l'élément de Frobenius définit un élément de G bien défini à conjugaison près et bien définit tout court si G est abélien ! C'est le début de la théorie du corps de classes...

Exercice 10.4.7. — *Soit* 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 les réductions* $\mathrm{P} \mod p_i$ *aient un unique facteur irréductible de degré* $\geq d_i$ *avec* $d_0 = n, d_1 = n-1$ *et* $d_2 = 2$*. Montrer que le groupe de Galois de* P *sur* $\mathbf{Q}$ *est* S_n *(utiliser 6.9.5). Montrer l'existence d'un tel polynôme pour tout* $n \geq 3$.

En fait, en raffinant (à peine) l'exercice précédent, on peut montrer, qu'en un sens convenable, la « probabilité »-on devrait plutôt parler de *densité*- 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 Bourbaki, N., *Algèbre*, Chapitre 4 à 7, Masson, (1981), exercice V.12.13) ! ! !

Comme on le verra en PC, le théorème 10.4.4 permet bien souvent de calculer le groupe de Galois d'un polynôme. Ce n'est pas un hasard : terminons ce voyage par un paragraphe sans preuve, expliquant pourquoi la méthode de réduction mod p est si efficace.

10.5. Le théorème de Cebotarev. — Soit K une extension galoisienne de $\mathbf{Q}$, corps des racines de P séparable, à coefficients entiers disons. Si p premier est assez grand (ne divisant ni le terme dominant de P ni son discriminant), disons $p > n(\mathrm{P})$, la réduction $\bmod p$ de $\bar{\mathrm{P}}$ 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 Frobenius, bien défini à conjugaison près. Notons C_p l'ensemble des éléments de G conjugués à un tel élément, qui elle 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 10.5.1* (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 ici développées d'algèbre et de fonctions holomorphes.

Par exemple, si $\mathrm{C} = \{1\}$, cette « probabilité », plus précisément c'est une densité, vaut $1/\operatorname{card}\mathrm{G}$. Si on y réfléchit, on s'aperçoit sans peine que la condition C_p trivial signifie $\bar{\mathrm{P}}$ scindé. En particulier, ce théorème dit qu'il existe une infinité de p tel que $\bar{\mathrm{P}}$ est scindé sur $\mathbf{F}_p$, ce qu'on peut démontrer de manière élémentaire, mais astucieuse. Ce sont les mauvais p du point de vue du calcul du groupe de Galois...

Nicolas Gregorievich Cebotarev

Exercice 10.5.2. — *Montrer que si un entier est un carré modulo p pour tout p est assez grand alors c'est un carré. Montrer que le résultat analogue subsiste avec des puissances l-ièmes où l est premier (difficile).*

11. Appendice : 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

$$\mathrm{I}(t) = \int_0^t \mathrm{e}^{t-u} f(u)\mathrm{d}u.$$

On a (intégrations par parties)

$$\mathrm{I}(t) = \mathrm{e}^t \sum_{j=0}^{m} \mathrm{P}^{(j)}(0) - \sum_{j=0}^{m} \mathrm{P}^{(j)}(|t|) \tag{11.a}$$

et

$$|\mathrm{I}(t)| \leq |t|\mathrm{e}^{|t|}\tilde{\mathrm{P}}(|t|). \tag{11.b}$$

a) Transcendance de e. —

Supposons qu'on ait

$$\sum_{i=0}^{n} a_i \mathrm{e}^i = 0 \tag{11.c}$$

avec $n, a_0 > 0$ et a_i entiers. Posons

$$\mathrm{J} = \sum_{k=0}^{n} a_k \mathrm{I}(k).$$

Avec les notations précédentes, les formules (11.a) et (11.c) 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 premier $> na_0$ 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

$$\mathrm{P}^{(j)}(k) = 0 \text{ si } j < p \text{ et } k > 0 \text{ et } \mathrm{P}^{(j)}(0) = 0 \text{ si } j < p-1$$

de sorte que

$$\mathrm{J} = -a_0\mathrm{P}^{(p-1)}(0) - \sum_{j=p}^{m}\sum_{k=p}^{n} a_k \mathrm{P}^{(j)}(k).$$

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 (11.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 $|\mathrm{J}| \geq (p-1)!$.

b) Transcendance de π. — La preuve est du même type. 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 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

$$0 = \prod_j (1 + \exp(\alpha_j)) = \sum_\epsilon \exp(\alpha_\epsilon) = q + \sum_{\epsilon \in \mathrm{A}} \exp(\alpha_\epsilon) \tag{11.d}$$

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 11.0.3. — *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 (6.5.1). Mais S est aussi un entier algébrique, donc est dans $\mathbf{Z}$ (10.2). □

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 premier qui a vocation à devenir grand et $m = (n+1)p + 1$. Grâce à (11.a) et (11.d), 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 zéros d'ordre $\geq p-1$ ce qui, grâce au lemme 11.0.3, assure

$$(p-1)! | \mathrm{J}.$$

Comme plus haut, on doit montrer que p ne divise pas l'entier relatif (11.0.3)

$$q\mathrm{P}^{(p-1)}(0)/(p-1)! = \pm q\mathrm{N}^{np-n}(\mathrm{N}a_1 \cdots \mathrm{N}a_n)$$

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 (11.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.

12. 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 de dimension 2 que Wiles [43] 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

$$x^n + y^n = z^n \text{ avec } n \geq 3, x, y, z \in \mathbf{Z}, \text{ alors } xyz = 0.$$

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 6.2.9 :

Proposition 12.0.4. — *Tout quotient du groupe de Galois d'une extension galoisienne de* $\mathbf{Q}$ *est quotient de* G.

12.1. Le cas abélien fini. — Nous allons prouver l'énoncé suivant.

Proposition 12.1.1. — *Tout groupe abélien fini est quotient de* G.

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 $\mathrm{H} = (\mathbf{Z}/n\mathbf{Z})^*$ 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 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 $\mod \mathrm{N}_i$ réalise $\mathbf{Z}/\mathrm{N}_i\mathbf{Z}$ comme un quotient de $\mathbf{Z}/(p_i - 1)\mathbf{Z}$. Ainsi, si $\mathrm{N}_i, \cdots, \mathrm{N}_m$ sont des entiers divisant respectivement $p_1 - 1, \cdots, p_m - 1$, on déduit que $\Pi = \prod \mathbf{Z}/\mathrm{N}_i\mathbf{Z}$ est un quotient de H.
Inversement, donnons nous $\mathrm{N}_1, \cdots, \mathrm{N}_m$ des entiers ≥ 1. Le théorème de la progression arithmétique de Dirichlet (cf. polycopié de tronc commun ou mieux l'exercice 7.2.11) assure qu'on peut trouver des nombres premiers arbitrairement grands dans chacune des progressions arithmétiques $1 + \lambda\mathrm{N}_i, \lambda \in \mathbf{N}$. On peut donc choisir $p_1, \cdots, p_m$ distincts tels que $\mathrm{N}_i | p_i - 1$ 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 groupe cycliques (cf. polycopié de cours de tronc commun). □

43. 1953-

12.2. 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 $X^3 - 2$ (6.10.4), donc est quotient de G. Il y a 5 groupes d'ordre 8 (cf. devoir). 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

$$D_8, H_8.$$

Rappelons que le groupe H_8, dit des quaternions, est le groupe ayant huit éléments

$$1, i, j, k, t, ti, tj, tk,$$

où t et central et

$$t^2 = 1, \text{ et } i^2 = j^2 = k^2 = ijk = t.$$

On a vu (PC) que D_8 est le groupe de Galois de $X^4 - 2$, de sorte que D_8 est quotient de G. Pour distinguer 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.
On a alors l'exercice suivant (emprunté à David Madore, qui l'attribue à Dirichlet).

Exercice 12.2.1. — *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.*

12.3. Le cas réductif fini. — La suite exacte fondamentale (6.7.a) de la théorie de Galois pourrait laisser croire qu'on déduit du cas abélien que tout groupe résoluble est groupe de Galois sur $\mathbf{Q}$. En fait, il n'en est rien, c'est très délicat. Mais c'est vrai.

Théorème 12.3.1 **(Shafarevich [44])**. — *Tout groupe fini résoluble est quotient de* G.

Igor Rostilavovich Shafarevich

44. 1923-

Nous avons rencontré en PC notamment de nombreux groupes résolubles non abéliens, comme les groupes diédraux (groupes des isométries planes d'un polygone régulier à n côtés). Les mathématiciens Feit [45] et Thompson [46] ont montré le très difficile et résultat suivant, qui donne un moyen simple de repérer si certains groupes sont résolubles en particulier...
Les experts conjecturent qu'en fait tout groupe fini est quotient de G.

***Théorème 12.3.2* (Feit-Tomaison).** — *Tout groupe d'ordre impair est résoluble.*

Walter Feit

John Griggs Thompson

12.4. Quelques quotients de G. — Parmi les groupes résolubles on trouve $\mathrm{A}_n, \mathrm{S}_n, n\ leq 4$. On a vu que S_n est quotient de G (10.4.7). 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 12.4.1* (Hilbert).** — *Les groupes alternés sont quotients de* G.

Le lecteur cultivé sait que $\mathrm{A}_n, n \geq 5$ est simple, autrement dit 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 [47] 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 H. Völklein, ≪ $\mathbf{GL}_n(q)$ as Galois group over the rationals ≫, Mathematische Annalen (1992), vol. 293, n°1, 163-176 pour des résultats dans ce cas, et J.-P. Serre [48], ≪ Groupes de Galois sur $\mathbf{Q}$ ≫, Séminaire Bourbaki, 30 (1987-1988), Exposé No. 689 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.

45. 1930-2004
46. 1932-
47. 1835-1890
48. 1926-

Jean-Pierre Serre

13. Corrections sommaires d'exercices

Correction sommaire de l'exercice 3.5.2

Si $\mathfrak{p}$ est premier dans A et $f : \mathrm{B} \to \mathrm{A}$ est un morphisme d'anneaux, f induit un morphisme $\mathrm{B}/f^{-1}(\mathfrak{p}) \to \mathrm{A}/\mathfrak{p}$ (3.3.2), 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 particulier, l'image réciproque de l'idéal premier (0) de l'anneau intègre A par l'unique morphisme $\mathbf{Z} \to \mathrm{A}$ est premier. Comme $\mathbf{Z}$ est principal, il est donc de la forme $p\mathbf{Z}$ avec p nul ou premier.

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.

Correction sommaire de l'exercice 3.5.4

Soit $a \in \mathrm{A}$ dont l'image dans A/I est inversible. Par définition, il existe donc $b \in \mathrm{A}, i \in \mathrm{I}$ tel 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 3.9.3

D'après la propriété universelle du quotient (3.3.2), 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 3.8.3

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,

$$(\mathbf{Z}/n\mathbf{Z})^* \to (\mathbf{Z}/d\mathbf{Z})^*$$

est surjectif si et seulement si

$$(\mathbf{Z}/p^{n_p}\mathbf{Z})^* \to (\mathbf{Z}/p^{m_p}\mathbf{Z})^*$$

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 3.5.4.

Correction sommaire de l'exercice 3.11.2

Si x est algébrique sur k de minimal P, le k-morphisme de corps $k[\mathrm{X}]/(\mathrm{P}) \to k[x]$ est visiblement bijectif. L'ensemble des complexes algébriques s'écrit $\cup_{\mathrm{P}\in\mathbf{Q}[\mathrm{X}]-0}\mathrm{P}^{-1}(0)$ et donc est réunion dénombrable d'ensembles finis, donc au plus dénombrable. Comme il contient $\mathbf{Q}$, il est infini dénombrable.

Correction sommaire de l'exercice 3.12.10

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 (3.3.2), d'où le premier point. Si P est non constant arbitraire, montrons par récurrence sur n que pour tout polynôme de degré $\leq n$ qu'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 '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 surcoupes K de L de degré $\leq (n-1)!$ tel que $\mathrm{P}_2\mathrm{P}_3$ est scindé dans K. On a $[\mathrm{K} : k] \leq n!$ (3.12.8) et K convient.

Correction sommaire de l'exercice 3.13.2

Soit $\mathrm{P} \in \mathbf{C}[\mathrm{X}]$ ne s'annulant jamais, unitaire de degré $n > 0$ disons. Alors, $1/\mathrm{P}$ est holomorphe comme quotient de fonctions holomorphes à dénominateur qui ne s'annule pas. Si a est le maximum des modules des coefficients de degré $< n$ de P, 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 : une contradiction.

Correction sommaire de l'exercice 3.17.2

Notons c le coefficient binomial $\binom{p}{k}$ avec $0 < k < p$. On a $p|p! = c.k!.(p-k)!$. Comme p est premier, il est premier avec tout produit d'entiers strictement compris entre 0 et p, notamment avec $k!(p-k)!$. Le lemme de Gauss assure alors $p|c$. Si maintenant $a, b \in \mathrm{A}$, on a

$$(a+b)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k} + b^p = a^p + b^p,$$

ce qu'on voulait.

Correction sommaire de l'exercice 4.1.3

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 $(p^n - 1)|(p^m - 1)$. Écrivons la division euclidienne $m = an + r, 0 \leq r < n$. On écrit

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

Mais (formule de la progression géométrique), $(p^n - 1)|(p^{an} - 1)$ de sorte que $p^n - 1|p^r - 1 < p^n - 1$ qui n'est possible que si $r = 0$, ce qu'on voulait.

Mais alors, 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 contant les cardinaux, on a $p^m = (p^n)^d$, d'où $d = m/n$.

Correction sommaire de l'exercice 4.1.4

On doit montrer que deux corps k, k' de même cardinal $q = p^n$ sont isomorphes. Choisissons Ω algébriquement clos de caractéristique p (donc contenant $\mathbf{F}_p$). On sait que 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.

Correction sommaire de l'exercice 4.2.4

Sujet de réflexion !

Correction sommaire de l'exercice 4.2.5

Soit $n > 0$ et μ_x le 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 (3.12.10) 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 6.1.2

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 5.2.1). L'extension

$$k(\mathrm{X}^{1/p}, \mathrm{Y}^{1/p})/k = k[\mathrm{X}^{1/p}, \mathrm{Y}^{1/p}]/k$$

est en particulier finie. La formule

$$\mathrm{P}(\mathrm{X}^{1/p}, \mathrm{Y}^{1/p})^p = \mathrm{P}_p(\mathrm{X}, \mathrm{Y})$$

o $\mathrm{P}_p(\mathrm{U}, \mathrm{V}) = \sum_{i,j} a_{i,j}^p \mathrm{U}^i \mathrm{V}^j$ 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 $\mathrm{X} = \sum a_i(\mathrm{X}^p, \mathrm{Y}^p)\mathrm{Y}^i$ o les a_i sont des fractions rationnelles. En dérivant par rapport à X, on obtient $1 = 0$, une contradiction.

Correction sommaire de l'exercice 6.1.3

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 qu'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.

Correction sommaire de l'exercice 6.2.3

Une extension finie de k est galoisienne si c'est le corps des racines d'un polynôme P (6.3.2). Or, si F est engendrée sur k par les racines de P, elle est engendrée *a fortiori* par les racines de P sur E (qui contient k !). Dans l'exemple $k = \mathbf{Q} \subset \mathrm{E} = \mathbf{Q}[2^{1/3}] \subset \mathrm{F} = \mathbf{Q}[2^{1/3}, i]$, on remarque que F est le corps des racines du polynôme $\mathrm{X}^3 - 2$ et donc est galoisienne sur k. Mais, $\mathrm{X}^3 - 2$ est irréductible sur k de sorte que $j2^{1/3}$ est un conjugué de $2^{1/3}$ (3.12.5) qui n'est pas dans E, ce qui empêche E/k d'être galoisienne (6.2.1).

Correction sommaire de l'exercice 6.3.3

Le corps fixe de la conjugaison complexe est $\mathbf{R}$. Le lemme d'Artin (6.5.2) assure alors que $\mathbf{C}/\mathbf{R}$ est galoisienne de groupe de Galois $\mathrm{Gal}(\mathbf{C}/\mathbf{R}) = \mathbf{Z}/2\mathbf{Z}$ engendré par la conjugaison. Évidemment, on peut démontrer ça « à la main ».

Correction sommaire de l'exercice 6.6.4

Dire $g \in \mathrm{Ker}(\pi)$, c'est dire $\pi(g) = (1 \mod \mathrm{H})$, *ie* $1 \in \mathrm{H}$. Supposons qu'on ait un morphisme $f : \mathrm{G} \to \mathrm{G}'$ qui tue H. Soit $x \in \mathrm{G/H}$ et $g, g' \in x$. Il existe $h \in \mathrm{H}$ tel que $g = g'h$ de sorte que $f(g) = f(g'h) = h(g')f(h) = f(g')$. Ainsi, f est constante sur x et on définit $\bar{f}(x)$ comme étant cette valeur constante. Vérifier que $\bar{f}$ est un morphisme et que $\bar{f}$ est l'unique morphisme $\mathrm{G/H} \to \mathrm{G}'$ tel que $f = \bar{f} \circ \pi$ est de pure routine. Le morphisme surjectif det : $\mathbf{GL}_n(\mathbf{C}) \to \mathbf{C}^*$ tue $\mathbf{SL}_n(\mathbf{C})$ 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 $\delta(\mathrm{M}) = 1$ *ie* $(\mathrm{M} \mod \mathbf{SL}_n(\mathbf{C})) = \mathrm{Id}$ prouvant que δ est injective, donc un isomorphisme puisqu'on sait qu'elle est surjective.

Correction sommaire de l'exercice 6.7.2

Soit $f : \mathrm{X} \to \mathrm{Y}$ une bijection strictement décroissante entre deux ensembles ordonnés et $x, x' \in \mathrm{X}$. Alors, on a

$$f(\max_{\xi \leq x, x'} \xi) = \min_{\eta \geq f(x), f(x')} \eta,$$

et de même pour le max... En appliquant à la correspondance de Galois $f : \mathcal{F} \to \mathcal{G}$ ($\mathcal{F}, \mathcal{G}$ ordonnés par l'inclusion) (6.7.1), on obtient

$$f(\mathrm{K}^{\mathrm{G}_1}\mathrm{K}^{\mathrm{G}_2}) = f(\min_{\mathrm{L} \supset \mathrm{K}^{\mathrm{G}_1}, \mathrm{K}^{\mathrm{G}_2}} \mathrm{L}) = \max_{\mathrm{H} \subset \mathrm{G}_1, \mathrm{G}_2} \mathrm{H} = \mathrm{G}_1 \cap \mathrm{G}_2.$$

De même,

$$f(\mathrm{K}^{\mathrm{G}_1} \cap \mathrm{K}^{\mathrm{G}_2}) = f(\max_{\mathrm{L} \subset \mathrm{K}^{\mathrm{G}_1}, \mathrm{K}^{\mathrm{G}_2}} \mathrm{L}) = \min_{\mathrm{H} \supset \mathrm{G}_1, \mathrm{G}_2} \mathrm{H} = \langle \mathrm{G}_1\mathrm{G}_2 \rangle.$$

Soit maintenant $x \in \mathrm{K}$. On a

$$f(k[x]) = \mathrm{Aut}_{k[x]}(\mathrm{K}) = \{g \in \mathrm{G} \text{ tels que } g(y) = y \text{ pour tout } y \in k[x]\} = \mathrm{G}_x$$

la dernière égalité venant du fait que tous les éléments de x sont k-linéaires.

Correction sommaire de l'exercice 6.9.5

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 $i \in \mathbf{Z}/k\mathrm{ZZ}$.

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 (récurrence) $(i, j) \in \mathrm{S}$ pour tout j et donc $\mathrm{S} = \mathrm{S}_n$ puisque les transpositions engendrent.

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 une $(n-1)$-cycle de $\mathrm{S}_{n-1} = \mathrm{S}\{2, \cdots, n\}$. Mais $\gamma^d(1, j)\gamma^{-d} = (1, 2)$ de sorte que $(1, 2) \in \mathrm{S}$ et on conclut par le point précédent.

Correction sommaire de l'exercice 6.10.2

Soit $z_{i,j}, j = 1, \cdots, d_i$ les racines de P_i dans $\bar{\mathrm{F}}_p$. On plonge comme d'habitude le groupe de Galois G du corps de décomposition $\mathbf{F}$ de $\prod \mathrm{P}_i$ dans le groupe symétrique des bijections des racines de $\prod \mathrm{P}_i$. Comme P_i est irréductible, P_i est le minimal de z_i sur $\mathbf{F}_p$ et ses racines sont les conjugués sous Galois. Comme G est engendré par le Frobenius F puisque $\mathbf{F}$ est fini (4.2.3), ce sont exactement les $\mathrm{F}^n(z_1), n = 0, \cdots, d_i - 1$. Soit γ_i le cycle $(z_1, \cdots, \mathrm{F}(z_1), \cdots, \mathrm{F}^{d_i-1}(z_1))$. On a par construction $\mathrm{F} = \prod \gamma_i$. Comme les γ_i commutent deux à deux puisqu'ils sont à supports disjoints, on a $\mathrm{F}^n = \prod \gamma_i^n$ ce qui assure visiblement que F est d'ordre le PPCM des d_i. Comme F engendre G, on déduit $\mathrm{card}(\mathrm{G}) = \mathrm{PPCM}(d_i)$. **Correction sommaire de l'exercice 6.10.3**

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* $\{pm1\} = \mathrm{G/H}$ 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 6.10.4

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 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 3 ou 6. Or, S_3 a un unique sous-groupe de cardinal $3!/2 = 2$ (6.10.3), 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 (6.10.1).

Correction sommaire de l'exercice 6.10.5

La dérivée de $\mathrm{X}^n - 1$ est $n\mathrm{X}^{n-1}$ qui n'a de racines 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 (6.10.1).

Correction sommaire de l'exercice 6.10.6

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

$$b^2 + b = \sum_{i<j} \left(\frac{x_i^2}{x_i^2 + x_j^2} + \frac{x_i(x_i + x_j)}{x_i^2 + x_j^2}\right) = \sum_{i<j} \frac{x_i x_j}{x_i^2 + x_j^2} = a.$$

La somme des racines de $X^2 + X + a = 0$ est 1 de sorte que ses racines sont b ou $b+1$. Comme $X^2 + X + a \in k[X]$, 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

$$g(\frac{x_i}{x_i + x_j}) = \frac{x_{\sigma(i)}}{x_{\sigma(i)} + x_{\sigma(j)}} = 1 + \frac{x_{\sigma(j)}}{x_{\sigma(i)} + x_{\sigma(j)}}.$$

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 7.2.6

C'est très classique. Écrivons $x = p/q$ avec p, q premiers entre eux et $q \geq 1$. Alors, x annule un polynôme du type $P(X) = X^n + \sum_{i<n} a_i X^i, n \geq 1$ avec $a_i \in \mathbf{Z}$. On a donc

$$q^n P(p/Q) = p^n + q \sum_{i<n} a_i p^i q^{n-1-i} = 0,$$

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 7.3.3

Conséquence immédiate de la théorie de Galois et de (2.1.3).

Correction sommaire de l'exercice 9.1.3

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 (PC), que c'est un groupe cyclique : choisissons un générateur ζ_n. Soit $K = k(\zeta_n), L = K(\sqrt[n]{a})$. 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 (6.7.1,*iv)*)

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

Mais $\mathrm{Gal}(L/K)$ est cyclique grâce à la théorie de Kummer (9.1.1) tandis que $\mathrm{Gal}(K/k)$ est un sous-groupe de $(\mathbf{Z}/n\mathbf{Z})^*$ (7.1.2), donc est abélien.

Correction sommaire de l'exercice 9.3.2

La suite exacte

$$1 \to A_n \to S_n \to \{\pm 1\} \to 1$$

et (9.3.5) 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

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

est, assez miraculeusement un sous-groupe distingué de A_3 (et de S_3 d'ailleurs). Comme A_3 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 (9.3.5).

Il est bien connu (et facile -utiliser le pivot de Gauss-) que $\mathbf{SL}_n(\mathbf{C})$ est engendré par les transvections $T_{i,j}(\lambda) = I + \lambda E_{i,j}, i \neq j, \lambda \neq 0$ et que deux transvections sont conjuguées dans $\mathbf{SL}_n(\mathbf{C})$. Donc, il existe $P \in \mathbf{SL}_n(\mathbf{C})$ tel que

$$(T_{i,j}(\lambda))^2 = T_{i,j}(2\lambda) = PT_{i,j}(\lambda)P^{-1}$$

de sorte que $T_{i,j}(\lambda)$ est le commutateur $[P, T_{i,j}(\lambda)]$. Comme les transvections engendrent, on a $D(\mathbf{SL}_n(\mathbf{C})) = \mathbf{SL}_n(\mathbf{C})$. 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 9.3.3

1) Il suffit d'associer à une matrice triangulaire inversible la suite des ses coefficients diagonaux pour trouver la suite exacte cherchée. On invoque alors (9.3.5).

2) Le premier point est clair. Soit $f \in U_j$ et $g \in U$ (voire $g \in B$ si on veut). Supposons que $Id + u, Id + v \in U_j$. On a

$$\ln((Id + u)(Id + v))(F_i) = (u + v + uv)(F_i) \subset F_{i-j} + uv(F_i).$$

Comme

$$uv(F_i) \subset F_{i-2j} \subset F_{i-j},$$

on a bien $(Id + u)(Id + v) \in U_j$. Comme Id est dans U_j, ce dernier est bien un sous-groupe de U. Comme $g(F_i) \subset F_i$ et $g^{-1}(F_i) \subset F_i$ pour tout i, on a

$$gfg^{-1}(F_i) \subset gf(F_i) \subset g(F_{i-j}) \subset F_{i-j}.$$

Ainsi $U_i \lhd U$.

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 F_i/F_{i-j-1}. Dire que $\ln(f)_{i,j}$ est nulle, c'est exactement dire $\ln(f)(F_i) \subset F_{i-j-1}$.

4) Si, comme plus haut, $Id + u, Id + v \in U_j$, on a

$$uv(F_i) \subset F_{i-2j} \subset F_{i-j-1}$$

et donc est nul en tant qu'endomorphisme de F_i/F_{i-j-1}. Ceci assure que $f \mapsto \ln(f)_{i,j}$ est un morphisme de U_i dans le groupe additif commutatif $End(F_i/F_{i-j-1})$. D'après 3), le noyau de $\ln_j$ est U_{j-1}.

5) On applique la définition 9.3.1 pour conclure que U est résoluble et donc que B est résoluble d'après 1).

Correction sommaire de l'exercice 9.3.7

Le fait que S_4 opère sur X résulte de la formule (6.9.4) ou de 6.9.a comme on veut. Si on numérote les éléments de X en décideant que la transposition $(1, i+1)$ apparaît dans x_i, l'opération $S_4 \to \mathrm{Aut}(X)$ s'identifie à un morphisme $S_4 \to S_3$. Li'mage de $(1,2)$ est $(2,3)$. On déduit que π est surjective. Comme le groupe engendré par X est $K = \{\mathrm{Id}\} \cup X = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ 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 $S_4/\mathrm{Ker}(\pi) = S_3$ résoluble de sorte que S_4 est résoluble (9.3.5).

Correction sommaire de l'exercice 9.3.8

Sujet de réflexion, assez classique par ailleurs !

Correction sommaire de l'exercice 10.4.7

Le théorème 10.4.4 et l'exercice 6.10.2 assure que le groupe de Galois $G \subset S_n$ contient un n-cycle, un $n-1$ cycle et une transposition. On conclut grâce à 6.9.5.

Correction sommaire de l'exercice 10.5.2

Voir examen de juin 2007.

Correction sommaire de l'exercice 10.2.5

Soit P est un 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 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 $\pi_n = \prod(X - z_i^n)$ 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 (7.2.6). 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 $(z_i^n) = (z_i^m)$ et donc $z_i^{m-n} = 1$.

Index

Table des matières

Yves Laszlo

15 mars 2010

Yves Laszlo, École poytechnique, CMLS, 91128 Palaiseau Cedex, France
E-mail : laszlo@math.polytechnique.fr