Théorème de Galois

February 18, 2019

Le but de ce projet est de se plonger dans la théorie des groupes, et d'arriver à comprendre et à intuiter la démonstration du théorème de Galois ainsi que son application à la constructibilité des polygones régulier. Un rapport devra être rendu avec la solution des questions et une présentation pédagogique de la théorie sera exigée. L'essentiel du travail consiste donc à comprendre et assimiler la théorie, pour être en mesure de l'expliquer à des personnes ayant un bagage mathématique sans pour autant connaître en détail la théorie des groupes. Les exercices sont simplement là pour aider à la compréhension, ainsi la solution importe moins que la démarche de recherche.

Le théorème que nous allons démontrer est le suivant :

Théorème (Gauss-Wantzel)**.** *P_n est constructible si et seulement si $n = 2^N F_1 \cdots F_m$ où les $F_1, \ldots, F_m$ sont des nombres premier de Fermat.*

Ce résultat peut sembler étonnant, voire impossible à montrer. Il n'y a pas besoin de connaître la théorie de Galois pour le comprendre, mais elle va s'avérer essentielle pour les montrer, et ne serait-ce qu'exprimer mathématiquement le sens de "constructible". Ce théorème est en fait une conséquence du théorème de correspondance de Galois qui s'énonce comme suit :

Théorème (Galois)**.** *Soit ${}^K/_k$ une extension finie, Ω la cloture algébrique de k avec $k \subset K \subset \Omega$ et G le groupe de Galois de ${}^K/_k$. On pose $\mathcal{G} = S(G)$ l'ensemble des sous-groupes de G et $\mathcal{F}$ l'ensemble des corps compris entre k et K. D'où $\mathcal{G} = \{G' | G' \text{ sous-groupe de } G\}$ et $\mathcal{F} = \{L \text{ corps} | k \subset L \subset K\}$. Alors on a*

(i) L'application $f : \begin{cases} \mathcal{F} & \to \mathcal{G} \\ L & \to Gal({}^K/_L) \end{cases}$ est une bijection strictement décroissante de bijection réciproque $f^{-1} : \begin{cases} \mathcal{G} & \to \mathcal{F} \\ H & \to K^H \end{cases}$.

(ii) Pour $H \in \mathcal{G}$, ${}^K/_{K^H}$ est galoisienne et $Gal({}^K/_{K^H}) = H$.

(iii) Pour $H \in \mathcal{G}$, L'application de restriction $r_H : \begin{cases} G & \to Hom_k(K^H, \Omega) \\ \sigma & \to \sigma_{|K^H} \end{cases}$ est surjective et $r_H^{-1}(\{Id\}) = H$.

(iv) Pour $H \in \mathcal{G}$, ${}^{K^H}/_k$ est galoisienne si et seulement si H est distingué dans G. Alors ${}^G/_H = Gal({}^{K^H}/_k)$.

(v) Pour $L \in \mathcal{F}$ tel que ${}^L/_k$ est galoisienne, alors on a la suite exacte : $\{e\} \to Gal({}^K/_L) \to Gal({}^K/_k) \to Gal({}^L/_k) \to \{e\}$

Ce théorème met en jeu beaucoup de notions, qu'il va falloir comprendre au fil des sections de ce projet. Encore plus que les définitions et les propriétés, les méthodes de raisonnement et de démonstration sont capitales, il convient d'essayer de les assimiler comme le reste. La première partie sera consacré à introduire toutes les définitions et propriétés des concepts de base, et la deuxième partie à la démonstration du théorème.

Part I
Concepts de base

1 Théorie des groupes

1.1 Rappel de bases

Un *groupe* G est un ensemble muni d'une loi de composition interne $*_G : G \times G \to G$ associative, muni d'un élément neutre e_G et du passage à l'inverse noté $^{-1}$. Pour $g_1, g_2 \in G$, on notera $g_1 *_G g_2$ simplement $g_1 * g_2$ ou $g_1 g_2$ quand il n'y a pas d'ambiguité. De meme, on notera e_G parfois simplement e. Un groupe est dit *abélien* ou *commutatif* si sa loi de composition interne est commutative. Un ensemble G' est un *sous-groupe* de G si il est non vide, inclu dans G et stable par $*$ et le passage à l'inverse. On notera $S(G)$ l'ensemble des sous-groupes de G. Si G est fini, on notera $|G|$ le *cardinal* de G.

1. Ecrire toute les définitions précédentes en langage mathématique.

   Solution: Laissé au lecteur.

2. Montrer qu'un sous-groupe est un groupe.

   Solution: Laissé au lecteur.

3. Montrer que $(\mathbb{R}, +)$, $(\mathbb{R}^*, \times)$ et $(\mathbb{Q}^*, \times)$. Pour $n \in \mathbb{N}$, on définit $\mathbb{Z}/n\mathbb{Z}$ comme l'ensemble des entiers $[\![0, n-1]\!]$ muni de l'addition et la multiplication modulo n (nous verrons un peu plus tard l'explication de la notation). Montrer que $(\mathbb{Z}/5\mathbb{Z}, +)$ et $\left((\mathbb{Z}/5\mathbb{Z})^*, \times\right)$ sont des groupes. Est-ce que $\left((\mathbb{Z}/6\mathbb{Z})^*, \times\right)$ est un groupe ?

   Solution: Laissé au lecteur.

4. Soit E un ensemble quelconque. Montrer que $Bij(E) \coloneqq \{f : E \to E | f \text{ est bijective}\}$ est un groupe pour la composition.

   Solution: Laissé au lecteur.

Un *morphisme de groupe* d'un groupe G vers un groupe H est une application $\phi : G \to H$ vérifiant $\forall g_1, g_2 \in G, \phi(g_1 *_G g_2) = \phi(g_1) *_H \phi(g_2)$ et $\phi(g_1^{-1}) = \phi(g_1)^{-1}$. On notera $Ker(\phi) \subset G$ et $Im(\phi) \subset H$ le noyau et l'image de ϕ, définis par $Ker(\phi) = \{g \in G | \phi(g) = e_H\} = \phi^{-1}(\{e_H\})$ et $Im(\phi) = \{h \in H | \exists g \in G; \phi(g) = h\} = \phi(G)$. Un morphisme bijectif est appelé un *isomorphisme*. Deux groupes G et H sont dit *isomorphes* si il existe un isomorphisme entre les deux, et l'on notera $G \approx H$.

5. Montrer que si $\phi : G \to H$ est un morphisme de groupe, alors $\phi(e_G) = e_H$, $Ker(\phi)$ est un sous-groupe de G et $Im(\phi)$ est un sous-groupe de H.

Solution: Soit $g \in G$, On a $\phi(e_G) = \phi(g *_G g^{-1}) = \phi(g) *_H \phi(g)^{-1} = e_H$. Pour $g_1, g_2 \in Ker(\phi)$, on a $\phi(g_1 g_2) = \phi(g_1)\phi(g_2) = e_H$ et $\phi(g_1^{-1}) = \phi(g_1)^{-1} = e_H$ d'où $g_1 g_2 \in Ker(\phi)$ et $g_1^{-1} \in Ker(\phi)$, donc $Ker(\phi)$ est un sous-groupe. De même, soit $h_1 = \phi(g_1), h_2 = \phi(g_2) \in Im(\phi)$. Alors $h_1 h_2 = \phi(g_1 g_2) \in Im(\phi)$ et $h_1^{-1} = \phi(g_1^{-1}) \in Im(\phi)$. Donc $Im(\phi)$ est un sous-groupe.

6. Montrer que $\phi : G \to H$ est un morphisme de groupe si et seulement si $g_1, g_2 \in G, \phi(g_1 *_G g_2^{-1}) = \phi(g_1) *_H \phi(g_2)^{-1}$.

Solution: $\implies$ trivial.

$\impliedby$ On suppose ϕ vérifie $\forall g_1, g_2 \in G, \phi(g_1 * g_2^{-1}) = \phi(g_1) * \phi(g_2)^{-1}$.

Pour $g_1 = g_2$, on a $\phi(e_G) = \phi(e_H)$. Pour $g_1 = e_G, g_2 = g \in G$, on a $\phi(g^{-1}) = \phi(g)^{-1}$ et pour $g = g_2^{-1}$, $\phi(g_1 * g) = \phi(g_1) * \phi(g)$.

1.2 Sous-groupes distingués

On dit qu'un sous-groupe H d'un groupe G est *distingué* si $\forall h \in H, \forall g \in G, g * h * g^{-1} \in H$.

7. Soit $\phi : G \to H$ un morphisme de groupe. Montrer que $Ker(\phi)$ est un sous-groupe distingué.

Solution: On sait que $Ker(\phi)$ est un sous-groupe. Soit $h \in Ker(\phi), g \in G$. On a $\phi(ghg^{-1}) = \phi(g)e_G\phi(g)^{-1} = e_G$. Donc $ghg^{-1} \in Ker(\phi)$. Donc $Ker(\phi)$ est distingué dans G.

On fixe G un groupe et $H \subset G$ un sous-groupe de G. Pour $g \in G$, on définit $gH = \{g * h | h \in H\}$ et pour $H' \subset G$ sous-groupe de G, $H' * H = \{h'h | h' \in H', h \in H\} = \bigcup_{h' \in H} h'H$.

8. Montrer que si H est dinstingué, alors pour $g_1, g_2 \in G$, on a $(g_1 H) * (g_2 H) = g_1 g_2 H$.

Solution: On procède par double inclusion. Soit $x \in g_1 g_2 H$. Alors $x = g_1 g_2 h$, pour un $h \in H$. Alors $x = g_1 \left(g_2 h g_2^{-1}\right) g_2 = (g_1 h') * (g_2 e_G)$ et $h' \in H$ car H est distingué et $e_G \in H$ car H est un sous-groupe. Donc $x \in (g_1 H) * (g_2 H)$.

Réciproquement, soit $x \in (g_1 H) * (g_2 H)$, on a $x = g_1 h_1 g_2 h_2 = g_1 g_2 \left(g_2^{-1} h_1 g_2\right) h_2 = g_1 g_2 h'$ avec $h' = \left(\left(g_2^{-1}\right) h_1 \left(g_2^{-1}\right)^{-1}\right) h_2 \in H$ car H est un sous-groupe distingué. Donc $x \in g_1 g_2 H$.

On suppose que H est distingué. On définit le *groupe quotient* de G par H, noté ${}^G/_H$ par ${}^G/_H = \{gH | g \in G\}$, et l'application $\pi : G \to {}^G/_H$ telle que $\forall g \in G, \pi(g) = gH$ est appelé la *surjection canonique* de ${}^G/_H$.

9. Montrer que ${}^G/_H$ est un groupe pour une loi bien choisie.

Solution: On définit $*_{G/H}$ par $(g_1 H) *_{G/H} (g_2 H) = (g_1 *_G g_2) H$. $*_{G/H}$ est bien définie par l'exercice ??, associative, a $H = e_G H$ comme élément neutre et possède un passage à l'inverse. Donc $({}^G/_H, *_{G/H})$ est un groupe.

10. Soit $n \in \mathbb{N}$. Montrer que $(n\mathbb{Z}, +)$ est un groupe. Expliquer la notation $\mathbb{Z}/n\mathbb{Z}$.

Solution: On vérifie que $n\mathbb{Z}$ est bien un sous-groupe de $\mathbb{Z}$, et il est distingué car $\mathbb{Z}$ est commutatif. $\mathbb{Z}/n\mathbb{Z}$ correspond donc au quotient de $\mathbb{Z}$ par l'ensemble des éléments divisible par n, ce qui donne les classes de congruence modulo n.

11. Montrer que la surjection canonique est un morphisme de groupe surjectif, et déterminer son noyau.

Solution: Soient $g_1, g_2 \in G$, alors $\pi(g_1 g_2^{-1}) = \left(g_1 g_2^{-1}\right) H = (g_1 H) * (g_2 H)^{-1} = \pi(g_1) * \pi(g_2)^{-1}$ donc π est un morphisme de groupe. En outre, pour $gH \in G/H$, on a $gH = \pi(g)$ donc π est surjectif. Enfin, $\pi(g) = e \iff gH = e \iff \exists h \in H; gh = e \iff g \in H$. Donc $Ker(\pi) = H$.

12. Montrer que tout sous-groupe distingué s'ecrit comme le noyau d'un morphisme de groupe.

Solution: Il suffit de prendre ϕ la surjection canonique de G/H.

13. Soit $\phi : G \to G'$ un morphisme de groupe. Montrer que $G/Ker(\phi)$ est isomorphe à $Im(\phi)$.

Solution: On sait que $Ker(\phi)$ est un sous-groupe distingué, donc $G/Ker(\phi)$ est bien défini. On pose $H = Ker(\phi)$ et $i : G/H \to Im(\phi)$ tel que $i(gH) = \phi(g)$. i est évidemment un morphisme de groupe et on a pour $gH \in Ker(i)$, on a $i(gH) = \phi(g) = e_{G'}$, d'où $g \in H = Ker(\phi)$ donc $gH = H$. Donc $Ker(i) = \{H\} = \{e_{G/H}\}$, donc i est injective, et i est évidemment surjective. Donc $G/Ker(\phi) \approx Im(\phi)$.

14. Montrer que la relation $\sim$ définie par $g_1 \sim g_2 \iff g_1 H = g_2 H$ est une relation d'equivalence.

Solution: L'égalité ensembliste est elle-même réflexive, symétrique et transitive.

15. Montrer le théorème de Lagrange, qui dit que si G est fini et H un sous-groupe distingué, on a $|G| = |G/H| \times |H|$. En déduire que si G est fini et $\phi : G \to G$ un morphisme de groupe, alors $|G| = |Ker(\phi)| \times |Im(\phi)|$.

Solution: A Chaque classe de $\sim$correspond un élément de G/H, donc $|G| = \sum_{x \in G/H} |x|$ et chaque classe d'équivalence possède exactement $|H|$éléments car$\forall g \in G$, $\begin{cases} H & \to gH \\ h & \to gh \end{cases}$ est bijective. Donc $|G| = |G/H| \times |H|$. Pour ϕ un morphisme, on a $Ker(\phi)$ sous-groupe dinstingué et $|G/Ker(\phi)| = |Im(\phi)|$, donc on a $|G| = |Im(\phi)| \times |Ker(\phi)|$.

16. Passage au quotient :

(a) Soient G et G' deux groupes isopmorphes par ϕ et $H \in G$ et $H' \in G'$ deux sous-groupes distingués de G et G' tels que ϕ induise une isomorphisme de H dans H'. Montrer que ϕ induit un isomorphisme de G/H dans G'/H'.

Solution: On pose $\psi : \begin{cases} G/H & \to G'/H' \\ gH & \to \phi(g)H' \end{cases}$, ψ est bien définie, car si $g = g'h$, alors $\psi(g) = \phi(g)H' = \phi(g')\phi(h)H' = \phi(g')H'$, l'image ne dépend donc pas du représentant. On vérifie facilement que ψ est un isomorphisme.

(b) Soit $H \subset G$ un sous-groupe distingué de G et $\phi : G \to G'$ un morphisme tel que $Ker(\phi) = H$. Montrer que ϕ induit un morphisme de $G/H \to G'$.

Solution: On pose $\psi : \begin{cases} G/H & \to G' \\ gH & \to \phi(g) \end{cases}$ et de même, l'image ne dépend pas du représentant de la classe.

1.3 Suites exactes

Soient G_1, G_2, G_3 trois groupes et $f_1 : G_1 \to G_2, f_2 : G_2 \to G_3$ deux morphismes de groupes. La suite $\{e\} \to G_1 \to^{f_1} G_2 \to^{f_2} G_3 \to \{e\}$ est dite *exacte* si f_1 est injective, f_2 surjective et $Im(f_1) = Ker(f_2)$.

17. Soit $\phi : G \to H$ un morphisme de groupe. Montrer que $\{e\} \to Ker(\phi) \to^i G \to^f Im(\phi) \to \{e\}$ est exacte pour i et f bien choisis.

Solution: On pose $i : \begin{cases} Ker(\phi) & \to G \\ g & \to g \end{cases}$ l'injection canonique et $f : \begin{cases} G & \to Im(\phi) \\ g & \to \phi(g) \end{cases}$. On a donc i injective et f surjective et $Im(i) = Ker(\phi) = Ker(f)$.

18. On suppose que les groupes G_1, G_2 et G_3 sont finis et que l'on a une suite exacte $\{e\} \to G_1 \to^{f_1} G_2 \to^{f_2} G_3 \to \{e\}$. Montrer que $|G_2| = |G_1| \times |G_3|$.

Solution: On a $Im(f_1) = Ker(f_2)$. Alors $|Im(f_1)| = |G_1|$ car $f_1$injective et $|Ker(f_2)| = \frac{|G_2|}{|Im(f_2)|} = \frac{|G_2|}{|G_3|}$ car $f_2$surjective. D'où l'égalité.

1.4 Action de groupe

On se donne E un ensemble quelconque et G un groupe. Une *action* de G sur E est un morphisme de groupe $\phi : G \to Bij(E)$ de G vers $Bij(E)$. On dit alors que G agit sur E. Dans ce cas, on note $g.x = (\phi(g))(x)$. Pour $x \in E$, on définit *l'orbite de* x par $G.x = \{g.x | g \in G\} \subset E$ et le *stabilisateur de* x par $Stab(x) = \{g \in G | g.x = x\}$. Pour $H \in S(G)$, on note $E^H = \{x \in E | \forall h \in H, h.x = x\}$ l'ensemble des éléments de E stabilisés par H. Enfin, on dit qu'une action de groupe est *fidèle* si ϕ est injective, et *transitive* si elle n'a qu'une seule orbite.

19. Donner une action de groupe de $\mathbb{R}$ sur le cercle unité.

Solution: Le groupe $(\mathbb{R}, +)$ agit sur le cercle unité $\mathcal{C}$ par les rotations. $r : \begin{cases} \mathbb{R} & \to Bij(\mathcal{C}) \\ \theta & \to r_\theta \end{cases}$.

20. Montrer que pour $x \in E$, $Stab(x)$ est un sous-groupe de G.

Solution: Soient $g_1, g_2 \in Stab(x)$, alors $g_1^{-1}.x = \phi(g_1)^{-1}[x] = x$ car $\phi(g_1)[x] = x$, et $g_1 g_2.x = g_1.x = x$, donc $Stab(x)$ est un sous-groupe de G.

1.5 Groupes résolubles

Un groupe G est *résoluble* si il existe une suite finie de sous-groupe $\{e\} = G_n \subset G_{n-1} \subset \cdots \subset G_1 \subset G_0 = G$ telle que $\forall i \in [\![1, n]\!], G_i$ est distingué dans G_{i-1} et ${}^{G_{i-1}}/_{G_i}$est commutatif.

21. Montrer qu'un groupe abélien est résoluble.

Solution: Soit G un groupe abélien. On pose $G_1 = \{e\}$. Alors $G_1 \subset G_0$ et G_1 est distingué dans G_0 et ${}^{G_0}/_{G_1} = G$ est commutatif.

Pour $g_1, g_2 \in G$, on définit le *commutateur* de $g_1$et g_2 par $[g_1, g_2] = g_1 g_2 g_1^{-1} g_2^{-1}$. Le *sous-groupe dérivé* de G, noté $D(G)$, est le sous-groupe **engendré** par les commutateurs de G, i.e. $D(G)$ est le plus petit sous-groupe contenant $\{[a, b] | a, b \in G\}$. On appelle *centre* de G l'ensemble de ses éléments qui commutent avec tout élément, i.e. $Z(G) = \{z \in G | \forall g \in G, zg = gz\}$.

22. Montrer que $Z(G)$ est un sous-groupe distingué et expliciter $Z(G)$ et $D(G)$ dans le cas où G est abélien.

Solution: Soient $z_1, z_2 \in Z(G)$, alors pour $g \in G$, $z_1 z_2^{-1} g = g z_1 z_2^{-1}$ donc $z_1 z_2^{-1} \in Z(G)$ donc $Z(G)$ est un sous-groupe. En outre, pour $g \in G$ et $z \in Z(G)$, on a $gzg^{-1} = z \in Z$, donc $Z(G)$ est distingué. Si G est abélien, on a $Z(G) = G$ et $D(G) = \{e\}$.

23. Montrer que $D(G)$ est distingué dans G et que ${}^{G}/_{D(G)}$ est commutatif.

Solution: Soit $g \in G$, et $\phi_g : \begin{cases} G & \to G \\ h & \to ghg^{-1} \end{cases}$. Pour montrer que $D(G)$ est distingué, il faut montrer que $D(G)$ est stable par ϕ_g pour tout $g \in G$, ce qui équivaut à montrer que pour tout $a, b, g \in G$,$[a, b]$ est stable par ϕ_g car $D(G)$ est engendré par les commutateurs. Or, pour tout morphisme de groupe ϕ, on $\phi([a, b]) = \phi(a)\phi(b)\phi(a)^{-1}\phi(b)^{-1} = [\phi(a), \phi(b)]$, donc $D(G)$ est distinguée.

Soient π la surjection canonique de G dans ${}^{G}/_{D(G)}$. Pour $a, b \in G$, on a $[\pi(a), \pi(b)] = \pi([a, b]) = e_{G/D(G)}$. Donc $\pi(a)$ et $\pi(b)$ commutent et π est sujective, d'où le résultat.

On définit la *suite dérivé* $(D^n(G))_{n \in \mathbb{N}}$ de G par $D^0(G) = G$ et $\forall n \in \mathbb{N}, D^{n+1}(G) = D(D^n(G))$.

24. Montrer que G est résoluble si et seulement si la *suite dérivé* de G est constante égale à $\{e_G\}$ à partir d'un certain rang.

Solution: $\Longrightarrow$ On suppose G résoluble, on a donc une suite $\{e\} = G_n \subset \cdots \subset G_0 = G$ vérifiant pour tout $i \in [\![1, n]\!]$, G_i distingué dans G_{i-1} et ${}^{G_{i-1}}/_{G_i}$ commutatif. On montre par récurrence sur i que $\forall i \in [\![0, n]\!], D^i G \subset G_i$. On a bien $D^0 G = G \subset G_0 = G$. On suppose le résultat pour un certain $i \geq 0$, alors on a $D^i(G) \subset G_i$ donc $D^{i+1}(G) \subset D(G_i)$. Montrons que $D(G_i) \subset G_{i+1} \subset G_i$. Soit π la surjection canonique de G_i dans ${}^{G_i}/_{G_{i+1}}$. Alors on a, pour $g_1, g_2 \in G_i$, $[\pi(g_1), \pi(g_2)] = \pi([g_1, g_2]) = e$ car ${}^{G_i}/_{G_{i+1}}$ commutatif. Donc $[g_1, g_2] \in G_{i+1} = Ker(\pi)$ donc $D(G_i) \subset G_{i+1}$ ce qui conclut la récurrence. Donc $D^n G \subset G_n = \{e\}$ d'où l'implication directe.

$\Longleftarrow$ On suppose que $\exists n; D^n(G) = \{e_G\}$, alors la suite $D^n(G) = \{e_G\} \subset D^{n-1}(G) \subset \cdots \subset D^0(G) = G$ montre la résolubilité de G.

25. Soit $\{e\} \to G_1 \to^{f_1} G_2 \to^{f_2} G_3 \to \{e\}$ une suite exacte. Montrer que G_2 est résoluble si et seulement si G_1 et G_3 sont résolubles.

Solution: $\Longrightarrow$ On suppose G_2 résoluble. On a donc n tel que $D^n(G_2) = \{e_{G_2}\}$. Pour $a, b \in G_1$, $[f_1(a), f_1(b)] = f_1([a, b])$, donc $f_1(D(G_1)) \subset D(G_2)$ et par récurrence $f_1(D^n(G_1)) \subset D^n(G_2) = \{e_{G_2}\}$ donc G_1 est résoluble car f_1 injective. De même, pour $x, y \in G_3$, par surjectivité de f_2 on a $g_1, g_2 \in G_2$ tels que $x = f_2(g_1)$ et $y = f_2(g_2)$, donc $[x, y] = f_2([g_1, g_2])$. Donc $D(G_3) = f_2(D(G_2))$, et donc de même par récurrence, $D^n(G_3) = f_2(D^n(G_2)) = \{e_{G_3}\}$. Donc G_3 est résoluble.

$\Longleftarrow$ On suppose G_1 et G_3 résolubles. On a donc $n, m \in \mathbb{N}$ tel que $D^n(G_1) = \{e\}$ et $D^m(G_3) = \{e\}$. On a montré que $D^m(G_3) = f_2(D^m(G_2))$. Donc $f_2(D^m(G_2)) = \{e\}$ donc $D^m(G_2) \subset Ker(f_2) = Im(f_1)$. Donc $D^{n+m}(G_2) \subset D^n(Im(f_1)) = f_1(D^n(G_1)) = \{e\}$. D'où G_2 résoluble.

1.6 Suites de Jordan-Hölder

Un groupe est dit *simple* si il ne possède pas de sous-groupe distingué non trivial, i.e. autre que $\{1\}$ et lui-même.

26. Montrer que tout groupe simple abélien fini a pour cardinal un nombre premier.

Solution: Soit G un groupe simple abélien fini. Soit $g \in G \backslash \{e_G\}$. Alors $< g >$ est un sous-groupe distingué de G, et donc $< g >= G$ car G est simple. Donc si $|G| = m \times n$, alors $< g^n >$ est un sous-groupe distingué non trivial de G, ce qui est absurde. Donc $|G|$ est un nombre premier.

Une *suite de Jordan-Hölder* d'un groupe G est une suite finie de sous-groupe $\{e\} = G_n \subset G_{n-1} \subset \cdots \subset G_1 \subset G_0 = G$ telle que $\forall i \in [\![1, n]\!], G_i$ est distingué dans G_{i-1} et ${}^{G_{i-1}}/_{G_i}$ est *simple*, i.e. ne possède pas de sous-groupe distingué autre que le groupe trivial et lui-même.

27. Montrer que tout groupe fini possède une suite de Jordan-Hölder.

Solution: On fait par récurrence, l'initialisation est simple. Si G est un groupe fini non simple, on considère N un sous-groupe distingué d'ordre maximal. Alors G/N est simple. Sinon, pour H un sous-groupe distingué, l'ensemble $\{hn \in G; hN \in H \text{ et } n \in N\}$ serait un sous-groupe distingué d'ordre strictement supérieur, et non égal à G. Donc par récurrence, N possède une suite de Jordan-Hölder, et G également.

1.7 Groupes cycliques

Un *générateur* d'un groupe G est un élément a du groupe tel que $G =< a >$, où $< a >= \{a^k | k \in \mathbb{N}\}$ est le sous-groupe engendré par a. Un groupe est dit *cyclique* ou *monogène* si il possède un générateur. Pour $g \in G$, *l'ordre* de g est le cardinal de $< g >$, i.e. le plus petit entier d tel que $g^d = e$ ou $+\infty$.

28. Montrer que pour $n \in \mathbb{N}$, $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique.

Solution: 1 est générateur.

29. Soit G un groupe cyclique d'ordre n, et x un générateur de G.
    (a) Montrer que l'ordre de tout élément de G divise n.

    Solution: Soit $g \in G$, alors $< g >$ sous-groupe de G, et l'ordre de g vaut $| < g > |$ et donc divise n par le théorème de Lagrange.

    (b) Soit d un diviseur de n. Montrer que G possède un unique sous-groupe d'ordre d

    Solution: On pose x un générateur du groupe et $d' = \frac{n}{d}$, $d' \in \mathbb{N}$, et $H =< x^{d'} >$. Alors H est un sous-groupe d'ordre d. Soit $H' \subset G$ un sous-groupe d'ordre d, et $h \in H'$. Alors $< h >$ est un sous-groupe de H, donc l'ordre de h divise d, et donc $h^d = e$. En outre, comme G est monogène, il existe $a \in \mathbb{N}$ tel que $h = x^a$, et donc $h^d = e = x^{ad}$. Donc $n|ad$ et donc il existe $k \in \mathbb{N}$ tel que $ad = nk$ et donc $a = d'k$ et donc $h \in H$.

    (c) Montrer que les générateurs de G sont les éléments de la forme x^d, avec d premier avec n.

    Solution: Soit x^k un générateur de G, alors on a $x^{kn} = e$ et $x \in G$ et donc il existe $u \in \mathbb{N}$, tel que $x^{ku} = x$ et donc on a $x^{ku} = x$ et donc il existe $v \in \mathbb{Z}$ tel que $ku + vn = 1$, donc k premier avec n. Reciproquement si k premier avec n, par bezout, on a $u, v \in \mathbb{Z}$ tel que $uk + vn = 1$ et donc pour $x^i \in G$, on a $\left(x^k\right)^{iu} = x^{i-vni} = x^i$ donc x générateur.

1.8 Exercie de synthèse : Formule des classes et Lemme de Cauchy

Soit G un groupe fini agissant sur E un ensemble fini. On définit la relation $\sim$ sur E par $x \sim y \iff \exists g \in G; y = g.x$.

30. Montrer que $\sim$ est une relation d'équivalence. On note Θ un ensemble de représentant de classes d'equivalence. Montrer que $|E| = \sum_{x \in \Theta} |G.x|$.

Solution: On a évidemment $x = e_G.x$ donc $x \sim x$. Soient $x, y, z \in E$. $x \sim y \implies \exists g \in G, y = g.x \implies \exists g \in G, x = g^{-1}.y \implies y \sim x$. En outre, on suppose que $x \sim y$ et $y \sim z$. Alors on a g_1, g_2 tels que $z = g_2.y$ et $y = g_1.x$, d'où $z = g_2 g_1.x$. Donc $\sim$ est une relation d'équivalence. Pour $x \in \Theta$, la classe d'équivalence de x est l'orbite de x :$G.x$. Donc $|E| = \sum_{x \in \Theta} |G.x|$.

31. Montrer que $\forall x \in E, |G| = |G.x|.|Stab(x)|$ et en déduire la formule des classes : $|E| = \sum_{x \in \Theta} \frac{|G|}{|Stab(x)|}$.

Solution: Soit $x \in E$. On pose $\approx$ la relation sur G définie par $g_1 \approx g_2 \iff g_1.x = g_2.x \iff g_2^{-1} g_1 \in Stab(x)$. $\approx$ est bien une relation d'équivalence et chaque classe d'équivalence de $\approx$possède $|Stab(x)|$ éléments, et il y a $|G.x|$ classes d'équivalence, d'où $|G| = |Stab(x)| \times |G.x|$. La formule des classes s'obtient directement.

32. En déduire que si $|G|$ est une puissance d'un nombre premier, alors $|X| \equiv |X^G| [\mod p]$.

Solution: On pose p premier et $n \in \mathbb{N}$ tels que $|G| = p^n$. On sait que $Stab(x)$ est un sous-groupe de G, donc son cardinal divise celui de p et on a $|Stab(x)| = p^n \iff x \in E^G$ et dans ce cas, l'orbite $G.x$ est reduite à $\{x\}$. Sinon, on a donc $\frac{|G|}{|Stab(x)|} = p^{n_x}$ avec $n_x > 0$. Donc $|E| = \sum_{x \in E^G} 1 + p \times \sum_{x \in \Theta \setminus E^G} p^{n_x - 1}$, d'où $|E| = |E^G| [\mod p]$.

On se donne maintenant p un nombre premier divisant $|G|$. On se propose de montrer le théorème de Cauchy : G contient un élément d'ordre p.

33. On considère $X = \{(x_1, \ldots, x_p) \in G^p | x_1 \cdots x_p = 1\}$. Calculer $|X|$.

Solution: Pour choisir un éléments de X, on peut fixer arbitrairement $p-1$ premières coordonnées, et prendre la dernière comme l'inverse du produit des autres. On a donc $|X| = |G|^{p-1}$.

34. Montrer que $\phi : \begin{cases} \mathbb{Z}/p\mathbb{Z} & \to Bij(X) \\ i & \to [(x_j) \to (x_{j+i})] \end{cases}$ définit une action de groupe de $\mathbb{Z}/p\mathbb{Z}$ sur X.

Solution: On vérifie que ϕ est bien un morphisme.

35. Conclure.

Solution: On utilise le résultat plus haut. On a donc $|X| = |X^{\mathbb{Z}/p\mathbb{Z}}| [\mod p]$. Or les éléments de X stabilisés par l'action ϕ sont les éléments possédant la même valeur à toute les coordonnées. D'où $|X^{\mathbb{Z}/p\mathbb{Z}}| = |\{g \in G | g^p = 1\}| = 0 [\mod p]$. Or $e_G \in \{g \in G | g^p = 1\} \neq \emptyset$, donc G possède un élément d'ordre p.

Applications :

36. Montrer que tout groupe d'ordre p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Solution: On groupe d'ordre p possède donc un élément x d'ordre p, et on $Fr : \begin{cases} \mathbb{Z}/p\mathbb{Z} & \to G \\ i & \to x^i \end{cases}$ est un isomorphisme.

On considère l'action de groupe G sur lui-même par conjugaison : $g \to \left[h \to ghg^{-1}\right]$. On suppose que $|G| = p^n$ avec p premier.

37. Montrer que $Z(G)$ est non trivial.

Solution: G agit sur lui-même par conjugaison. Donc $|G| = |G^G|[\mod p]$. Or $G^G = \{g \in G | \forall g' \in G, g'gg'^{-1} = g\} = Z(G)$. Donc $|Z(G)| = 0[\mod p]$ et $|Z(G)| \geq 1$ donc $Z(G)$ est non-trivial.

38. En déduire que tout groupe d'ordre p^2 est abélien.

Solution: On suppose que $|Z(G)| = p$. Alors $|G/Z(G)| = \frac{|G|}{|Z(G)|} = p$ par le théorème de lagragne. Donc $|G/Z(G)|$ est isomorophe à $\mathbb{Z}/p\mathbb{Z}$ et donc est abélien. Donc pour $g \in G$, on peut écrire $g = zx^n$ avec $z \in Z(G)$ et x générateur de $G/Z(G)$. Donc $g \in Z(G)$ absurde. Donc $|Z(G)| = p^2$ et G est abélien.

39. Soit G un groupe d'ordre une puissance de 2. Montrer que G possède une suite $G_0, \ldots, G_n$ de Jordan-Hölder vérifiant $\forall i \in [\![0, n-1]\!], |G_{i+1}/G_i| = 2$.

Solution: On sait que G possède une suite de Jordan-Hölder $G_0, \ldots, G_n$ vérifiant pour tout $i \leq n-1$, G_{i+1}/G_i simple. Soit $i \leq n-1$. Si G_{i+1}/G_i est abélien, alors, par la question 26, $|G_{i+1}/G_i| = 2$. Sinon, par la question 36, G_{i+1}/G_i n'est pas simple car son centre est non trivial. Donc $|G_{i+1}/G_i| = 2$.

2 Anneaux, corps, algèbre

2.1 Rappel de base

Un *anneau* $(A, +, \times)$ est un ensemble muni de deux opérations tel que $(A, +)$ est un groupe commutatif, et tel que l'opération $\times$ est associative, possède un élément neutre, et est distributive par rapport à l'addition, i.e. $\forall a, b, c \in A, (a+b)\times c = a\times b + a\times c$ et $c\times(a+b) = c\times a + c\times b$. L'élément neutre pour l'addition est noté 0_A et l'élément neutre pour la multiplication est noté 1_A. Un anneau est dit *commutatif* si l'opération $\times$ est commutative et *intègre* si il est commutatif et sans diviseur de 0, i.e. $\forall a, b \in A, ab = 0 \implies a = 0$ ou $b = 0$. On ne considèrera dans ce projet que des anneaux commutatifs.

40. Montrer que $\mathbb{R}[X]$ est un anneau intègre. Montrer que $\mathbb{Z}/6\mathbb{Z}$ est un anneau. Est-il commutatif ? Intègre ?

Solution: $\mathbb{Z}/6\mathbb{Z}$ est commutatif mais pas intègre, car $3 \times 2 = 0$.

Un *morphisme d'anneau* $\phi : A \to B$ est un morphisme de groupe entre $(A, +)$ et $(B, +)$ vérifiant $\phi(1_A) = \phi(1_B)$ et $\forall (a_1, a_2) \in A, \phi(a_1 \times_A a_2) = \phi(a_1) \times_B \phi(a_2)$.

Un *corps* $\mathbb{K}$ est un anneau dont tout les éléments non nuls sont inversibles, i.e. $(\mathbb{K}^*, \times)$ est un groupe. Un *idéal* I d'un anneau A est un ensemble vérifiant $(I, +)$ est un sous-groupe de $(A, +)$ et $\forall x \in I, \forall a \in A, ax \in I$.

41. Montrer que $(\mathbb{R}, +, \times)$, $(\mathbb{Z}/5\mathbb{Z}, +, \times)$ sont des corps.

> **Solution:** Laissé au lecteur.

42. Montrer qu'un anneau intègre fini est un corps.

> **Solution:** On considère $x \in A$ non nul et l'application $\psi : \begin{cases} A & \to A \\ a & \to ax \end{cases}$. On a alors $\psi(a) = \psi(a') \iff (a - a')x = 0 \iff a = a'$ car A est intègre. Donc ψ est injective, et donc surjective car A est fini. Donc x est inversible et $x^{-1} = \psi^{-1}(1)$. Donc A est un corps.

43. Soit A un anneau et $a \in A$. Montrer que aA est un idéal de A, appelé *idéal engendré* par a et noté (a).

> **Solution:** On sait que aA est un sous-groupe et soit $ax \in aA, a' \in A$, on a $axa' = a(xa') \in aA$. Donc aA est un idéal.

44. Soit ϕ un morphisme d'anneau. Montrer que $Ker(\phi)$ est un idéal.

> **Solution:** On sait que $Ker(\phi)$ est un sous-groupe et soit $x \in Ker(\phi), a \in A$, on a alors $\phi(xa) = \phi(x)\phi(a) = 0$.

45. Soit $\mathbb{K}$ un corps. Expliciter les idéaux de $\mathbb{Z}$, de $\mathbb{K}$ et de $\mathbb{K}[X]$. Soit $\phi : \mathbb{K} \to A$ un morphisme d'anneau. Montrer que ϕ est injective.

> **Solution:** Soit $I \subset \mathbb{Z}$ un idéal et $n = \min I \cap \mathbb{N}$. Montrons que $I = n\mathbb{Z}$. On a évidemment $n\mathbb{Z} \subset I$. Soit $x \in I$ tel que $n \nmid x$. Alors soit q, r le quotient et le reste de la division euclidienne de x par n. On a donc $r = x - n \times q \in I$ et $0 < r < n$ ce qui contredit la définition de n. Donc $I = n\mathbb{Z}$.
>
> Soit $I \subset \mathbb{K}$ un idéal. On suppose $I \neq \{0\}$. Soit $a \in I \backslash \{0\}$ et $x \in \mathbb{K}$. Alors $a \times (a^{-1}x) = x \in I$. Donc $I = \mathbb{K}$ ou $I = \{0\}$.
>
> Soit $I \subset \mathbb{K}[X]$, et $P \in \arg\min_{Q \in I \text{ unitaire}} deg(Q)$. De même que pour $\mathbb{Z}$, on a $(P) \subset \mathbb{K}[X]$. Soit $Q \in I$, on considere R le reste de la division euclidienne de Q par P. On a $R \in I$ et $0 \leq deg(R) < deg(P)$, donc $R = 0$ sinon cela contredit la définition de P, donc $I = (P)$.
>
> $Ker(\phi)$ est un idéal de $\mathbb{K}$ donc $Ker(\phi) = \{0\}$ ou $Ker(\phi) = \mathbb{K}$, donc ϕ injective car $\phi \neq 0$ car $\phi(1) = 1$.

On fixe pour la suite A un anneau commutatif et $I \subset A$ un idéal de A.

46. Soit π la surjection canonique de ${}^{A}/_{I}$. Montrer que ${}^{A}/_{I}$ a une structure d'anneaux telle que π soit un morphisme d'anneaux. On appelle cet anneau *l'anneau quotient*. Montrer que π définit une bijection entre les idéaux de ${}^{A}/_{I}$ et ceux de A contenant I.

Solution: On pose l'opération $\times_{{}^{A}/_{I}}$ par pour $x+I, y+I \in {}^{A}/_{I}$, $(x+I)\times_{{}^{A}/_{I}}(y+I) = ((x\times y)+I) \in {}^{A}/_{I}$. C'est bien défini car si $x = x' + i$ et $y = y' + i'$, on a $xy = x'y' + (x'i' + y'i + ii')$ par commutativité, d'où $((x\times y)+I) = ((x'\times y')+I)$, cela ne dépend donc pas du choix des représentant. On vérifie que c'est bien un anneau. Soit $x+I, y+I, z+I \in {}^{A}/_{I}$, $(x+I+y+I)\times(z+I) = ((x+y)\times z)+I = (xz+I)+(yz+I)$. L'élément neutre pour $\times_{{}^{A}/_{I}}$ est $1+I$.

Soit $I \subset J \subset A$ un idéal contenant I. Alors soit $j \in J$, $x+I \in {}^{A}/_{I}$ et $\pi(j) \in \pi(J)$. Comme π est sujrective, il existe $a \in A$ tel que $x+I = \pi(a)$, d'où $(x+I)+\pi(j) = \pi(a+j) \in \pi(J)$. Donc $\pi(J)$ est un idéal. Reciproquement, soit J un idéal de ${}^{A}/_{I}$, on considère l'ensemble $\pi^{-1}(J)$. Pour $a \in A$ et $k \in \pi^{-1}(J)$, on a $\pi(k+a) = \pi(k)+\pi(a) \in J$ donc $k+a \in \pi^{-1}(J)$ donc $\pi^{-1}(J)$ est un idéal de A et $\pi(I) = 0_{{}^{A}/_{I}}$ donc $I \subset \pi^{-1}(J)$ d'où le résultat.

47. Montrer que ${}^{A}/_{I}$ est un corps si et seulement si I est un idéal maximal, i.e. il n'existe pas d'idéal J tel que $I \subsetneq J \subsetneq A$.

Solution: $\Longrightarrow$ On suppose que ${}^{A}/_{I}$ est un corps. Alors il ne possède que les idéaux triviaux et donc A ne contient que deux idéaux contenant I, I et A par la propriété précédente. On peut voir cette implication directement : Soit J un idéal tel que $I \subsetneq J$. Soit $j \in J\backslash I$. Alors $j+I \neq I$ donc $j+I$ inversible dans ${}^{A}/_{I}$, d'où $x \in A$ tel que $(j+I)\times(x+I) = 1+I$. Donc il existe $i \in I$ tel que $jx = 1+i$, donc $1+i \in J$ car J est un idéal et donc $1 \in J$ car $I \subset J$. Donc $J = A$.

$\Longleftarrow$ On suppose que I idéal maximal. Donc ${}^{A}/_{I}$ ne possède que des idéaux triviaux. Soit $x \in {}^{A}/_{I}\backslash\{0\}$, (x) est un idéal non réduit à $\{0\}$, donc $(x) = {}^{A}/_{I}$ et donc x est inversible. Donc ${}^{A}/_{I}$ est un corps.

48. En déduire que ${}^{\mathbb{Z}}/_{p\mathbb{Z}}$ est un corps si et seulement si p est premier. On notera ${}^{\mathbb{Z}}/_{p\mathbb{Z}}$ également $\mathbb{F}_p$.

Solution: On suppose p premier, alors soit $n\mathbb{Z}$ un idéal de $\mathbb{Z}$ conentant $p\mathbb{Z}$, on donc $p \in n\mathbb{Z}$, donc $p = k\times n$, avec $k \in \mathbb{Z}$, donc $n|p$ donc $n = 1$ ou $n = p$, donc $n\mathbb{Z} = \mathbb{Z}$ ou $p\mathbb{Z}$. Donc ${}^{\mathbb{Z}}/_{p\mathbb{Z}}$ est un corps. Reciproquement, si ${}^{\mathbb{Z}}/_{p\mathbb{Z}}$ est un corps, alors tout idéal contenant $p\mathbb{Z}$ est soit $\mathbb{Z}$, soit $p\mathbb{Z}$, donc p ne possède aucun diviseur, donc p est premier.

2.2 Caractéristique

Soit $\phi : \mathbb{Z} \to A$ le morphisme d'anneau tel que $\forall n \in \mathbb{Z}, \phi(n) = n.1_A = \underbrace{1_A + \ldots + 1_A}_{n \text{ fois}}$. Alors $Ker(\phi)$ est un idéal de $\mathbb{Z}$, donc il existe un unique entier n tel que $Ker(\phi) = n\mathbb{Z}$. Cet entier est appelé la *caractéristique* de A, que l'on note $car(A)$.

49. Donner les caractéristique de $\mathbb{Z}$, $\mathbb{R}$ et${}^{\mathbb{Z}}/_{n\mathbb{Z}}$. Donner un exemple de corps infini de caractéristique finie.

Solution: Les caractéristiques de $\mathbb{Z}$, $\mathbb{R}$ et$\mathbb{Z}/n\mathbb{Z}$ sont 0,0 et n. $\mathbb{F}_p(X)$ est un corps infini de caractéristique finie.

50. Montrer que si A est un corps, alors $car(A) = 0$ ou $car(A) = p$ avec p premier et il existe un morphisme d'anneau injectif $\tilde{\phi} : \mathbb{Z}/car(A)\mathbb{Z} \to A$. Montrer que si $car(A) = 0$, alors A est infini.

Solution: On suppose $car(A) \neq 0$. Alors $car(A).1_A = 0$. Si $d|car(A)$, alors $d.1_A \times \frac{car(A)}{d}.1_A = 0$ et donc par intégrité d'un corps, on aurait $d = car(A)$ ou $\frac{car(A)}{d} = car(A)$ donc $car(A)$ est premier. On pose $\tilde{\phi} : \begin{cases} \mathbb{Z}/car(A)\mathbb{Z} & \to A \\ k & \to k.1_A \end{cases}$. $\tilde{\phi}$ est evidemment un morphisme d'anneau et $Ker(\phi) = \{0\}$.

Si $car(A) = 0$, alors par injectivité de $\tilde{\phi}$, A possède $\tilde{\phi}(\mathbb{N})$ un ensemble dénombrable d'éléments distincts, donc A est inifini.

51. On suppose que A est un anneau commutatif de caractéristique $p > 0$. Montrer que l'application $Fr : \begin{cases} A & \to A \\ a & \to a^p \end{cases}$ est un morphisme d'anneau injectif. On l'appelle le *morphisme de Frobenius*. Montrer qu'il est injectif si A est intègre.

Solution: Fr est bien définie et pour $a, b \in A$, on a $Fr(a + b) = (a + b)^p = \sum_{n=0}^{p} a^n \times b^{p-n} \times \left(\begin{pmatrix} p \\ n \end{pmatrix} .1_A \right)$ par la formule de Newton. Or, $\forall n \in [\![1, p-1]\!], p| \begin{pmatrix} p \\ n \end{pmatrix}$ donc $\begin{pmatrix} p \\ n \end{pmatrix} .1_A = 0$. D'où $Fr(a+b) = a^p + b^p = Fr(a) + Fr(b)$. On a également si $p > 2$, p est impair donc $Fr(-a) = -Fr(a)$ et sinon $Fr(a) = Fr(a) + Fr(a) - Fr(a) = Fr(a) \times 2.1_A - Fr(a) = -Fr(a)$ et $Fr(a \times b) = Fr(a) \times Fr(b)$ et $Fr(1) = 1$. Donc Fr est un morphisme d'anneau. Enfin on a $Ker(Fr) = \{0\}$ si l'anneau est intègre.

2.3 Algèbres

Une $\mathbb{K}$-*algèbre* $(A, +, \times, .)$ est un anneau $(A, +, \times)$ muni d'une multiplication externe . telle que $(A, +, .)$ est un $\mathbb{K}$-espace vectoriel et compatible avec la multiplication, i.e. $\forall \lambda \in \mathbb{K}, a, b \in A, (\lambda a)b = a(\lambda b) = \lambda(ab)$. Un *morphisme de* $\mathbb{K}$-*algèbre* est un morphisme d'anneau $\mathbb{K}$-linéaire. Pour A, A' deux $\mathbb{K}$-algèbre, on note $Hom_{\mathbb{K}}(A, A')$ l'ensemble des morphisme de $\mathbb{K}$-algèbre de A dans A'.

On se fixe pour la suite un corps k et une k-algèbre A. On définit *le degré de* A par k, noté $[A : k]$ par la dimension de A vu comme k-espace vectoriel. On a donc $[A : k] \in \mathbb{N} \cup \{+\infty\}$. On dit que A est une *extension* de k si A est un corps, et on note dans ce cas A/k. Une extension K/k est dite *finie* si $[K : k] < +\infty$. Pour K/k une extension et $x \in K$, on définit $k[x] = \{P(x) | P \in k[X]\}$.

52. Soit K/k une extension et L une K-algèbre. Montrer que $[L : k] = [L : K] \times [K : k]$.

Solution: Soit $(\alpha_i)_{i \in I}$ une base de L comme K-espace vectoriel et $(\beta_j)_{j \in J}$ une base de K comme k-espace vectoriel. Alors pour $x \in L$, $x = \sum_{i \in I} \lambda_i \alpha_i$ avec $(\lambda_i)_{i \in I} \in K^I$ et donc $x = \sum_{i \in I} \sum_{j \in J} \mu_{i,j} \alpha_i \beta_j$, avec $(\mu_{i,j})_{(i,j) \in I \times J} \in K^{I \times J}$. Donc la famille $(\alpha_i \beta_j)_{(i,j) \in I \times J}$ est génératrice de L comme k-espace

vectoriel, et elle est libre car $\sum_{i\in I}\sum_{j\in J}\mu_{i,j}\alpha_i\beta_j = 0 \iff \forall i \in I \sum_j \mu_{i,j}\beta_i = 0 \iff \forall (i,j) \in I\times J, \mu_{i,j} = 0$. D'où le résultat.

53. Soit $P \in k[X]$ un polynôme et ϕ un morphisme d'algèbre sur k. Montrer que $\forall x \in k, \phi(P(x)) = P(\phi(x))$.

Solution: Soit $x \in k$. On a $\phi(x^n) = \underbrace{\phi(x)\times\cdots\times\phi(x)}_{n \text{ fois}} = \phi(x)^n$. Donc pour $P = \sum_i a_i X^i \in k[X]$, on a $\phi(P(x)) = \phi(\sum_i a_i x^i) = \sum_i a_i \phi(x)^i = P(\phi(x))$.

54. Soit B une k-algèbre et $\psi : \begin{cases} Hom_k(k[X], B) & \to B \\ \phi & \to \phi(X) \end{cases}$. Montrer que ψ est bijective.

Solution: Soit $b \in B$, on pose $\phi : \begin{cases} k[X] & \to B \\ P & \to P(b) \end{cases}$, alors on a $\psi(\phi) = \phi(X) = b$. Donc ψ est surjective. En outre, si $\psi(\phi_1) = \psi(\phi_2)$, alors $\phi_1(X) = \phi_2(X)$ et donc $\forall P \in k[X], \phi_1(P(X)) = \phi_2(P(X))$ car ϕ_1 et ϕ_2 sont des morphismes de k-algèbre. Donc $\phi_1 = \phi_2$, donc ψ est bijective.

2.4 Corps de rupture

Soit $P \in k[X]$ un polynome irréductible.

55. Montrer que ${}^{k[X]}/_{(P)}$ est un corps.

Solution: Soit J un idéal de $k[X]$ contenant (P). Alors on sait que il existe $Q \in k[X]$ tel que $J = (Q)$. On a donc $P \in J$, donc $P = Q \times A$ avec $A \in k[X]$. Donc $Q|P$ donc $Q = 1$ ou $Q = P$ car P est irréductible. Donc ${}^{k[X]}/_{(P)}$ est un corps. On peut montrer que réciproquement, si ${}^{k[X]}/_{(P)}$ est un corps alors P est irréductible.

56. Montrer que $[{}^{k[X]}/_{(P)} : k] = deg(P)$ et donner une racine de P dans ${}^{k[X]}/_{(P)}$.

Solution: On considère la surjection canonique $\pi : k[X] \to {}^{k[X]}/_{(P)}$ et la famille $\mathcal{X} = \left(\pi(X^i)\right)_{i\in[\![0,deg(P)-1]\!]}$. Alors π est un morphisme de k-algèbre et pour $(\lambda_i)_{i\in[\![0,deg(P)-1]\!]}$, on a $\sum_i \lambda_i \pi(X^i) = 0 \iff \pi(\sum_i \lambda_i X^i) = 0 \iff P|\sum_i \lambda_i X^i \iff \sum_i \lambda_i X^i = 0$. Donc la famille $\mathcal{X}$ est libre. En outre, pour $Y \in {}^{k[X]}/_{(P)}$, on a $Q \in k[X]$ tel que $Y = \pi(Q)$ et donc en prenant R le reste de la division euclidienne de Q par P, on a $Y = \pi(R)$ car $\pi(P) = 0$ et donc Y s'ecrit comme combinaison linéaire de la famille $\mathcal{X}$, et $|\mathcal{X}| = deg(P)$ donc $[{}^{k[X]}/_{(P)} : k] = deg(P)$. Enfin, on a $P(\pi(X)) = \pi(P) = 0$, donc $\pi(X)$ est une racine de P dans ${}^{k[X]}/_{(P)}$.

Le corps ainsi construit est appelé le *corps de rupture* de P.

57. Construire $\mathbb{C}$ comme un corps de rupture.

Solution: Soit $P = X^2 + 1 \in \mathbb{R}[X]$. Alors P est irréductible dans $\mathbb{R}$ et en notant $i = \pi(X)$ la racine de P dans $\mathbb{C} = {}^{\mathbb{R}[X]}/_{(P)}$, on a bien $P(i) = 0$ donc $i^2 = -1$, et $\mathbb{C} = vect\{1_{\mathbb{C}}, i\}$.

2.5 Algèbricité

On fixe pour la suite ${}^{K}/_{k}$ une extension. On dit que $x \in K$ est *algébrique* sur k si $\exists P \in k[X]\backslash\{0\}$ tel que $P(x) = 0$. Si x n'est pas algébrique, on dit que x est *transcendant* sur k. Par exemple, 1 et $\sqrt{2}$ sont algébriques sur $\mathbb{R}$ et on peut montrer que π et e sont transcendant sur $\mathbb{R}$, mais cela sort du cadre de ce projet. Une extension ${}^{K}/_{k}$ est dite *algébrique* si tout élément de K est algébrique sur k.

Soit $x \in K$ algébrique sur k, et $I_x = \{P \in k[X] | P(x) = 0\}$ l'idéal des polynômes annulateurs de x. Comme x est algébrique, $I_x \neq \{0\}$, et donc il existe un polynôme unitaire $\pi_{x,k} \in k[X]$ tel que $I_x = (\pi_{x,k})$ appelé *polynôme annulateur minimal de x sur k.*

58. Montrer que $\pi_{x,k}$ est irréductible dans $k[X]$.

Solution: Supposons $\pi_{x,k} = P \times Q$ avec $P, Q \in k[X]$. Alors $P(x) \times Q(x) = 0$, d'où par intégrité de k, $P(x) = 0$ ou $Q(x) = 0$, ce qui montre par définition de $\pi_{x,k}$ que $P = 1$ ou $Q = 1$, donc $\pi_{x,k}$ est irréductible dans k.

59. Montrer que ${}^{k[X]}/_{\pi_{x,k}}$ isomorphe à $k[x]$. En déduire que $k[x]$ est un corps.

Solution: On considère l'application $\psi : \begin{cases} k[X] & \to k[x] \\ P & \to P(x) \end{cases}$. Alors ψ est un morphisme de k-algèbre surjectif par définition de $k[x]$, donc $Im(\psi) = k[x]$, et on a $Ker(\psi) = (\pi_{x,k})$ par définition de $\pi_{x,k}$. Donc ${}^{k[X]}/_{Ker(\psi)} \approx Im(\psi)$, d'où le résultat. En outre, $\pi_{x,k}$ est irréductible, donc $(\pi_{x,k})$ est maximal, donc $k[x]$ est un corps.

60. Montrer que$[k[x] : k] = deg(\pi_{x,k})$.

Solution: $k[x]$ est isomorphe au corps de rupture de $\pi_{x,k}$, donc $[k[x] : k] = [{}^{k[X]}/_{(\pi_{x,k})} : k] = deg(\pi_{x,k})$.

61. Montrer les équivalences suivantes : [x algébrique sur k] $\iff$ [$[k[x] : k] < \infty$] $\iff$ [$k[x]$ est un corps].

Solution: On a déjà montré que x algébrique $\implies [k[x] : k] < \infty$, et x algébrique $\implies k[x]$ est un corps.

Supposons que $k[x]$ est un corps. Alors x a un inverse $P(x)$, d'où $Q = P \times X - 1 \in k[X]$ est un polynôme anulateur de x, donc x algébrique.

Supposons que $[k[x] : k] < \infty$, alors on pose un famille génératrice$(P_i(x))_{i \in I}$ avec I fini. On a donc $x = \sum_i \lambda_i P_i(x)$, d'où $Q = \sum_i \lambda_i P_i(x) - x$ annulateur de x.

62. Montrer que l'ensemble des nombres algébriques sur un corps est un corps.

Solution: Soient x, y deux nombres algébriques et $P_x, P_y \in k[X]$ annulant x et y. On a $k \subset k[x] \subset k[x,y]$, d'où $[k[x,y] : k] = [k[x,y] : k[x]] \times [k[x] : k]$. Or y est algébrique sur $k[x]$ car $P_y \in k[X] \subset (k[x])[X]$ et $k[x,y] = (k[x])[y]$, d'où $[k[x,y] : k[x]] < \infty$ et $[k[x] : k] < \infty$, donc $[k[x,y] : k] < \infty$. Et on a $k[x+y] \subset k[x,y]$ et $k[xy] \subset k[x,y]$, donc $[k[-x] : k] < \infty$,$[k[x+y] : k] < \infty$ et $[k[xy] : k] < \infty$ et donc $x+y$ et xy sont algébriques sur k. Et si $x \neq 0$, alors comme $x^{-1} \in k[x]$, $[k[x^{-1}] : k] < \infty$ ce qui donne l'algébricité de x^{-1}. Donc l'ensemble des nombres algébriques sur k est un sous-corps de K.

Soit $x \in K$ algébrique sur k. On définit l'ensemble des *conjugués* de x sur k, noté $Conj_{k,K}(x)$, comme l'ensemble des racines sur K du polynôme annulateur minimal de x sur k.

63. Montrer que $\psi : \begin{cases} Hom_k(k[x], K) & \to Conj_{k,K}(x) \\ \sigma & \to \sigma(x) \end{cases}$ est une bijection.

Solution: Pour $\sigma \in Hom_k(k[x], K)$ et $P \in k[X]$, on a $\sigma(P(x)) = P(\sigma(x))$. Soit $\pi_{x,k}$ le polynôme annulateur de x minimal sur k. Alors $\sigma(\pi_{x,k}) = \pi_{x,k}(x) = 0 = \pi_{x,k}(\sigma(x))$, donc $\sigma(x) \in Conj_{k,K}(x)$, et donc ψ est bien définie. On a $\psi(\sigma) = \psi(\sigma') \implies \forall P \in k[x], \sigma(P(x)) = \sigma'(P(x))$ car x engendre $k[x] \implies \sigma = \sigma'$ donc ψ est injective. En outre, pour $y \in Conj_{k,K}(x)$, on pose $\sigma_y \in Hom_k(k[X], K)$ vérifiant $\sigma_y(P) = P(y)$. On a bien $Ker(\sigma_y) = (\pi_{y,k}) = (\pi_{x,k})$ car y est un conjugué de x et $\pi_{x,k}$ irréductible. Donc $\sigma : \begin{cases} {}^{k[X]}/_{(\pi_{y,k})} \approx k[x] & \to K \\ P + (\pi_{y,k}) & \to P(y) \end{cases}$ est bien définie et est un morphisme de k-algèbre et donc on a bien $\psi(\sigma) = \sigma(x) = y$.

On admettra le théorème de prolongement des morphismes, qui dit que si l'on a $k \subset K \subset \Omega$ des extensions algébriques et $\phi : k \to \Omega$ un morphisme de k-algèbre, on peut prolonger ϕ sur K en un morphisme de k-algèbre coïncidant avec ϕ sur k.

64. Montrer que $\forall y \in Conj_{k,\Omega}(x)$, il existe $\sigma \in Hom_k(K, \Omega)$ tel que $\sigma(x) = y$.

Solution: D'après la question 63, il existe $\sigma \in Hom_k(k[x], \Omega)$ tel que $\sigma(x) = y$, que l'on prolonge par le théorème du prolongement.

2.6 Corps de décomposition

Soit k un corps et $P \in k[X]$. On appelle *corps de décomposition* de P un corps K vérifiant :

- P est scindé dans K.
- K est engendré par les racines $x_1, \ldots, x_n$ de P dans K, soit $K = k[x_1, \ldots, x_n]$.

65. Montrer par récurrence l'existence d'un corps de décomposition.

Solution: On montre cela par récurrence sur le degré de P. Pour $n = 1$, on a $P = aX + b = a\left(X + ba^{-1}\right)$, donc P est scindé sur k et k engendré par $-ba^{-1}$, donc k est un corps de décomposition de P. Supposons le résultat pour $n \geq 2$. Soit S un facteur irréductible de P. Alors on pose k' le corps de rupture de S. On a donc $k' = k[x]$ pour $x \in k'$ une racine de S dans k'. D'où $P = (X-x)Q$ avec $Q \in k'[X]$ et donc par hypothèse de récurrence, Q possède un corps de décomposition dans k', d'où un corps K et $x_2, \ldots, x_n \in K$ vérifiant $K = k'[x_2, \ldots, x_n]$ et donc on a $K = k[x, x_2, \ldots, x_n]$ et P scindé dans K avec pour racines $x, x_2, \ldots, x_n$. D'où l'existence.

66. On veut montrer l'unicité du corps de décomposition. Soient k et k' deux corps et $\tau : k \to k'$ un isomorphisme de corps.

    (a) Montrer que pour tout $P \in k[X]$ irréductible, τ induit un isomorphisme d'anneau de $k[X]$ dans $k'[X]$ et de ${}^{k[X]}/_{(P)}$ dans ${}^{k'[X]}/_{(\tau(P))}$ préservant τ.

    Solution: On pose $\phi_\tau : \begin{cases} k[X] & \to k'[X] \\ \sum_i a_i X^i & \to \sum_i \tau(a_i) X^i \end{cases}$. ϕ_τ est bien un morphisme de k-algèbre (k' a une structure de k-algèbre induite par τ), et on a $\phi_\tau \circ \phi_{\tau^{-1}} = Id$, c'est donc un isomorphisme. Pour $P \in k[X]$, ϕ_τ et $\phi_{\tau^{-1}}$ sont des bijections réciproques entre (P) et $(\tau(P))$, donc induisent des bijections reciproques entre ${}^{k[X]}/_{(P)}$ et ${}^{k[X]}/_{(\tau(P))}$ par passage au quotient.

    (b) Soit $P \in k[X]$, K un corps de décomposition de P sur k et K' un corps de décomposition de $\tau(P)$ sur k'. Montrer que K et K' sont isomorphes.

    Indication On pourra raisonner par récurrence forte sur le nombre de racine de P sur $K\backslash k$, et essayer d'appliquer l'hypothèse de récurrence à une extension de la forme ${}^{K}/_{k'}$, avec k' bien choisi.

    Solution: On montre par récurrence forte sur le nombre m de racine dans K mais pas dans k. Pour $m = 0$, on a $P = (X - \lambda_1) \cdots (X - \lambda_n)$ avec $\lambda_1, \ldots, \lambda_n \in k$. Donc $K = k$ et on a $\tau(P) = (X - \tau(\lambda_1)) \cdots (X - \tau(\lambda_n))$ donc $K' = k'$ ce qui assure le cas $m = 0$. Supposons le résultat pour tout $m' < m$, avec $m > 0$. Soit P ayant m racines dans $K\backslash k$, $P = P_1 \cdots P_r \in k[X]$ sa décomposition en facteur irréductible dans $k[X]$. Comme $m > 0$, au moins l'un des facteur est de degré 2, et l'on supposera sans perte de généralisté que c'est la cas de P_1, qui est par ailleurs scindé dans K. Soit α une racine de P_1 dans $K\backslash k$. On a alors un isomorphisme de k-algèbre ψ de ${}^{k[X]}/_{(P_1)}$ dans $k[\alpha]$, et de même, on a un isomorphisme de k'-algèbre $\phi : {}^{k'[X]}/_{(\tau(P_1)} \to k[\beta]$ avec β une racine de $\tau(P_1)$ dans K' ($\tau(P_1)$) irréductible dans k', sinon P_1 ne le serait pas dans $k[X]$). D'après le lemme, on a un isomorphisme de ${}^{k[X]}/_{(P_1)} \to {}^{k'[X]}/_{(\tau(P_1)}$ qui prolonge τ. Si on pose $k_1 = k[\alpha]$ et $k_1' = k'[\beta]$, alors on a $\tau_1 = \phi \circ \tau \circ \psi^{-1}$ un isomorphisme de k_1 dans k_1' qui prolonge τ. Ainsi K et K' sont des corps de décomposition de P dans k_1 et k_1', donc par hypothèse de récurrence, on a un isomorphisme de K dans K' qui préserve τ_1 et donc τ.

2.7 Cloture algébrique

Un corps K est dit *algébriquement clos* si tout polynôme non constant de $K[X]$ est scindé dans K. Une extention algébrique ${}^{K}/_{k}$ est une *cloture algébrique* de k si tout polynôme non constant de $k[X]$ est scindé dans $K[X]$.

67. Montrer que $\mathbb{C}$ est une cloture algébrique de $\mathbb{R}$. Est-ce que $\mathbb{C}$ est une cloture algébrique de $\mathbb{Q}$?

Solution: Théorème de d'Alembert nous dit que tout polynôme de $\mathbb{R}[X]$ est scindé dans $\mathbb{C}$ est $\mathbb{C}$ est algébrique sur $\mathbb{R}$. Par contre $\mathbb{C}$ n'est pas une cloture algébrique de $\mathbb{Q}$ car $\mathbb{C}/\mathbb{Q}$ n'est pas algébrique, car il existe des réels transcendants.

68. On veut montrer ici que tout cloture algébrique est algébriquement close.

(a) On considère k un corps et K une cloture algébrique de k. Soit $P \in K[X]$, et L la k-algèbre engendrée par les coefficients de P. Montrer que $A = {}^{L[X]}/_{(P)}$ est une extension finie de k.

Solution: Soit k un corps et K une cloture algébrique de k. Soit $P \in K[X]$. Alors on considère L la k-algèbre engendrée par les coefficients de P. Alors L est une extension fini de k car les coefficients de P sont algébrique dans k, donc obtenus à partir d'un nombre fini d'éléments de K. D'où $[L : k] < \infty$.

(b) On note $\bar{X}$ l'image de $X \in L[X]$ dans A. Montrer que $\phi : \begin{cases} k[X] & \to A \\ P(X) & \to P(\bar{X}) \end{cases}$ n'est pas injective.

Solution:
On pose $A = {}^{L[X]}/_{(P)}$. Alors par ce qui précède, on a $[A : k] = [A : L] \times [L : k] < \infty$. On considère $\phi : \begin{cases} k[T] & \to A \\ P(T) & \to P(\bar{X}) \end{cases}$ où $\bar{X}$ est l'image de X dans A. ϕ est un morphisme de k-algèbre, donc k-linéaire et non injective car $\dim_k(k[X]) = +\infty$ et $\dim_k(A) < \infty$. Donc ϕ n'est pas injective.

(c) Conclure.

Solution: ϕ n'est pas injective, donc il existe $Q \in Ker(\phi)\backslash\{0\}$. On a alors $Q(\bar{X}) = 0$, donc $P|Q$ et $Q \in k[T]$, donc Q est scindé dans K et donc P est scindé dans K. Donc K est algébriquement clos.

On admettra le théorème de Steinitz (dont la démonstration fait appel à l'axiome du choix), qui dit que tout corps admet une cloture algébrique. On admet aussi le théorème de prolongement des morphismes qui dit que pour K, Ω extension d'un corps k, avec ${}^{K}/_{k}$ algébrique et Ω algébriquement clos. Alors il existe $\sigma : K \to \Omega$ un morphisme de k-algèbre injectif.

69. Montrer que toute cloture algébrique est unique à isomorphisme de k-algèbre près.

Solution: Soient K_1, K_2 deux clotures algébriques de k. On applique le théorème du prolongement. On a K_1 extension de k et K_2 algébriquement clos. Donc on a $\sigma : K_1 \to K_2$ morphisme de k-algèbre injectif. On pose $K_1' = \sigma(K_1)$. On a donc K_2 extension de K_1' et K_1' algébriquement clos. Donc il existe $\tau : K_2 \to K_1'$ un morphisme de K_1'-algèbre injective. On a donc, pour $x \in K_1'$, $\tau(x) = x$ donc τ est surjective, ce qui donne $K_2 \approx^{\tau} K_1' \approx^{\sigma} K_1$.

2.8 Corps finis

Un *corps fini* est un corps de cardinal fini. On fixe pour la suite un corps k fini.

70. Montrer que $car(k)$ est un nombre premier, et que $|k| = car(k)^{[k:\mathbb{F}_p]}$.

> **Solution:** On suppose $car(k) = a \times b$, avec $a, b \in \mathbb{N}$. Alors on a $car(k).1_k = (a.1_k) \times (b.1_k) = 0$ et donc par intégrité, on a $a = car(k)$ ou $b = car(k)$ et donc $car(k)$ est premier. On pose alors $k' = \{n.1_k | n \in \mathbb{N}\}$, et on a $k' \approx \mathbb{F}_{car(k)}$. D'où k est un k'-espace vectoriel de dimension finie car k est fini et donc $|k| = car(k)^{[k:\mathbb{F}_p]}$.

On pose $q = |k|$, et on a montré que $q = p^n$ avec p premier et $n \in \mathbb{N}$.

71. Montrer que $(k^*, \times)$ est un groupe fini d'ordre $q-1$. En déduire, en utilisant le théorème de Lagrange, que $\forall x \in k^*, x^{q-1} = 1$.

> **Solution:** On a bien k un corps donc $(k^*, \times)$ est un groupe. Soit $x \in k^*$, on a $X = \{x^n | n \in \mathbb{N}\}$ est un sous-groupe de k^*, donc $card(X) | q-1$ par le théorème de Lagrange et donc il existe $d | q-1$ tel que $x^d = 1$ et donc $x^{q-1} = 1$.

On note $\overline{\mathbb{F}_p}$ la cloture algébrique de $\mathbb{F}_p$, et on pose $\mathbb{F}_q = \{x \in \overline{\mathbb{F}_p} | x^q = x\}$. On a donc $\mathbb{F}_p \subset \mathbb{F}_q \subset \overline{\mathbb{F}_p}$.

72. Montrer que $\mathbb{F}_q$ est un sous-corps de $\overline{\mathbb{F}_p}$ de cardinal q et que $Fq : \begin{cases} k & \to k \\ x & \to x^q \end{cases}$ est un morphisme de corps. En déduire que k est isomorphe à $\mathbb{F}_q$.

> **Solution:** Pour $x, y \in \mathbb{F}_q$, on a $(xy)^q = xy$ et $(x+y)^q = F_q(x+y) = F_p(\cdots(F_p(x+y))) = F_q(x) + F_q(y) = x^q + y^q = x + y$ car $F_q = Fr^n$ et $\left(x^{-1}\right)^q = (x^q)^{-1} = x^{-1}$, ce qui montre au passage que F_q est un morphisme de corps, et $\mathbb{F}_q$ est de cardinal q comme l'ensemble des racines du polynôme $X^q - X$, scindé dans $\overline{\mathbb{F}_p}$ et à racine simple car $q.X^{q-1} - 1 = -1 \neq 0$ (la dérivé ne s'annule jamais). Et donc $\mathbb{F}_q$ est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$, et de même, k est le corps de décomposition de $X^q - X$ sur son sous-corps preimer, isomorphe à $\mathbb{F}_p$ et donc par unicité du corps de décomposition, $\mathbb{F}_q \approx k$.

On a donc montré que les corps fini sont unique à isomorphisme près !

73. Montrer que le morphisme de Frobenius est un automorphisme de $\mathbb{F}_p$-algèbre, i.e. $F_r \in Aut_{\mathbb{F}_p}(\mathbb{F}_q) = \{f : \mathbb{F}_q \to \mathbb{F}_q | f \text{ morphisme de } \mathbb{F}_p\text{-algèbre}\}$.

> **Solution:** Fr est un morphisme de corps. Soit $x \in \mathbb{F}_p$, on a $x = n.1$ avec $n \in \mathbb{N}$, d'où$Fr(x) = n.Fr(1) = n.1 = x$. Donc Fr est un morphisme de $\mathbb{F}_p$ algèbre. En outre, pour $x, x' \in \mathbb{F}_q$, tel que $Fr(x) = Fr(x')$, on a $x^p = x'^p$ et donc $x^q = x'^q$ car $p | q$ et donc $x = x'$. Donc Fr est injectif et donc surjectif.
>
> **Remarque :** On voit que le fait que $\mathbb{F}_q$ soit fini joue un rôle important dans la démonstration de cette propriété, et elle est fausse dans le cas général. Cela motivera la notion de corps parfait.

74. Montrer que $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m} \iff n | m$

Solution: On suppose $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$. $\mathbb{F}_{p^m}$ est un $\mathbb{F}_{p^n}$ espace vectoriel de dimension fini N, d'où $p^m = (p^n)^N$ donc $n|m$.
Reciproquement, si $n \times d = m$, pour $x \in \mathbb{F}_{p^n}$, on a $\left(x^{p^m}\right) = F_{p^n}^d(x) = x$, donc $x \in \mathbb{F}_{p^m}$.

75. (a) Pour $n \in \mathbb{N}$, on note $\phi(n)$ l'indicatrice d'Euler de n, le nombre d'entier inférieur à n et premier avec n. Montrer que $\sum_{d|n} \phi(d) = n$.

Solution: Tout élément de $\mathbb{Z}/n\mathbb{Z}$ a un ordre d diviseur de n, et il y a exactement $\phi(d)$ éléments d'ordre d car ils engendrent l'unique sous-groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$. Donc $card(\mathbb{Z}/n\mathbb{Z}) = n = \sum_{d|n} \phi(d)$.

(b) On considère d un diviseur de $q-1$ et H_d l'ensemble des éléments d'ordre d. Montrer que $card(H_d) = 0$ ou $\phi(d)$.

Solution: Si $H_d \neq \emptyset$, on pose $a \in H_d$. Alors $card(< a >) = d$ et donc $card(H_d) \geq \phi(d)$. Supposons $card(H_d) > \phi(d)$, alors $H_d \backslash (< a >) \neq \emptyset$, et donc pour $b \in H_d \backslash (< a >)$, on a $< a, b >> d$ et $card(< a, b >) \leq d$ car il s'agit des racines de $X^d - X$ de degré d, ce qui est absurde. Donc $card(H_d) = \phi(d)$ ou 0.

(c) Montrer que $(\mathbb{F}_q^*, \times)$ est cyclique et isomorphe à $(\mathbb{Z}/(q-1)\mathbb{Z}, +)$.
Indication On pourra utiliser la question (a).

Solution: On a $card(\mathbb{F}_q^*) = q-1 = \sum_{d|q-1} card(H_d)$ car tout élément a un ordre divisant $q-1$ et donc $\forall d|q-1, card(H_d) = d$ d'après (a). En particulier, $card(H_{q-1}) = \phi(q-1)$ et donc il existe un élément d'ordre $q-1$.

76. On veut montrer que $Aut_{\mathbb{F}_q}(\mathbb{F}_{q^n})$ est cyclique d'ordre n engendré par F_q.

(a) Montrer que $F_q \in Aut_{\mathbb{F}_q}(\mathbb{F}_{q^n})$. En déduire que $card(Aut_{\mathbb{F}_q}(\mathbb{F}_{q^n})) \geq n$.

Solution: On a $F_q \in Aut_{\mathbb{F}_q}(\mathbb{F}_{q^n})$ car pour $y \in \mathbb{F}_q, y^q = y$. Soit $0 < d < n$, on a $x^{q^d} \neq x$ et donc $F_q^d \neq Id$, donc F_q est d'ordre au moins n,

(b) Montrer que $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$.

Solution: On pose x un générateur de $\mathbb{F}_{\shortparallel^{\ltimes}}{}^*$. On a $\mathbb{F}_q[x] = \mathbb{F}_{q^n}$ et on sait que $\mathbb{F}_{q^n}$ est un $\mathbb{F}_q$-espace vectoriel de dimension n (on a forcement $q^{dim(\mathbb{F}_{q^n})} = q^n$). Donc $[\mathbb{F}_q[x] : \mathbb{F}_q] = n$.

(c) En déduire que $card(Aut_{\mathbb{F}_q}(\mathbb{F}_{q^n})) \leq n$ et conclure.

Solution: On a donc $\deg(\pi_{x,\mathbb{F}_q}) = n$. Soit $\sigma \in Aut_{\mathbb{F}_q}(\mathbb{F}_{q^n})$, on a $\sigma(\pi_{x,\mathbb{F}_q}(x)) = 0 = \pi_{x,\mathbb{F}_q}(\sigma(x))$ donc $\sigma(x)$ est une racine de $\pi_{x,\mathbb{F}_q}$ et $\sigma(x)$ détermine σ car x générateur. Donc $card(Aut_{\mathbb{F}_q}(\mathbb{F}_{q^n})) \leq n$.
On a donc bien, par cardinalité, $Aut_{\mathbb{F}_q}(\mathbb{F}_{q^n}) =< F_q >$.

2.9 Corps parfait

Un corps k est dit *parfait* si $car(k) = 0$ ou si $\big[car(k) = p > 0$ et $F_r \in Aut_{\mathbb{F}_p}(k)\big]$. Un polynôme unitaire est dit *séparable* si ses racines dans Ω sont distincts. On admettra que P est séparable si et seulement si $P \wedge P' = 1$.

77. Montrer que tout corps fini est parfait. Donner un exemple de corps non parfait.

> **Solution:** La quesion 73 donne le résultat. $\mathbb{F}_2(X)$ est un corps et on a $X \notin Fr(\mathbb{F}_2(X))$.
>
> **Remarque :** On a vu que le morphisme de Frobenius est injectif pour un corps fini, et en général dès que l'anneau est intègre. C'est la surjectivité qui est difficile à obtenir, et qui donne le caractère parfait au corps.

78. Soit K/k une extension finie avec k parfait. Montrer que K est parfait.

> **Solution:** Si $car(k) = 0$, alors $car(K) = 0$. On suppose $car(k) = p$ et $Fr \in Aut_{\mathbb{F}_p}(k)$. On pose $n = [K : k]$. On a $car(K) = p$ et on a une extension finie, donc il existe $(x_i)_{i\in[\![1,n]\!]}$ une base de K vu comme k-espace vectoriel. On sait que Fr est un morphisme de $\mathbb{F}_p$-algèbre injectif. Montrons qu'il est surjectif. On a $Fr(K) \subset K$ est un k-espace vectoriel de dimension au plus $[K : k]$. Soit $(\lambda_i)_{i\in[\![1,n]\!]}$ tels que $\sum_{i=1}^{n} \lambda_i Fr(x_i) = 0$. Alors $Fr(\sum_i Fr^{-1}(\lambda_i)x_i = 0)$, donc par injectivité, $\sum_i Fr^{-1}(\lambda_i)x_i = 0$ et donc $\forall i \in [\![1, n]\!], \lambda_i = 0$ car (x_i) est libre. Donc $Fr(K)$ est de dimension n, et donc $Fr(K) = K$.

79. Soit k un corps. Montrer que k est parfait si et seulement si les polynôme irréductibles de $k[X]$ sont séparables.

> **Solution:** On suppose k parfait. Soit $P \in k[X]$ irréductible. On a $P \wedge P' | P$ donc $P \wedge P' = 1$ ou P. Si $car(k) = 0$, alors $deg(P') = deg(P) - 1$ et donc $P' = 1$ ou $P = 1$ et donc P est séparable. Supposons $car(k) = p$ et $P' = 0$. On pose $P = \sum_i a_i X^i$. On a donc $P' = \sum_i i.a_i X^{i-1} = 0$ et donc $\forall i; p \nmid i, a_i = 0$. D'où $P = \sum_k a_{pk} X^{pk} = (\sum_k Fr^{-1}(a_{pk})X^k)^p$ absurde car P irréductible.
>
> On suppose que tout polynôme irréductible de $k[X]$ est séparable, et que $car(k) = p > 0$. Il faut montrer que Fr est surjectif. Soit $x \in k$ et $P = X^p - x$. On pose r une racine de P dans Ω, on a donc $r^p = x$ et donc $P = (X - r)^p$. On a donc$\pi_{r,k}$ irréductible donc séparable et $\pi_{r,k} | P$ dans $k[x]$ donc dans $\Omega[x]$, donc $\pi_{r,k} = X - r$ et donc $r \in k$.

Une extension K/k est dite *monogène* si il existe $x \in K$ tel que $K = k[x]$.

On admettra le théorème de l'élément primitif : Soit k un corps parfait et K/k une extension finie. Alors K/k est monogène.

80. Soit k un corps parfait, K une extension finie et Ω la cloture algébrique de k. Montrer que $|Hom_k(K, \Omega)| = [K : k]$.

> **Solution:** On a $K = k[x]$ pour un certain $x \in K$. On a donc $[K : k] = [k[x] : k] = deg(\pi_{x,k})$ avec $\pi_{x,k}$ irréductible, donc séprable. Donc $|Conj_{k,K}(x)| = [K : k] = |Hom_k(K, K)|$ par l'exercice ??. Et on a $Hom_k(k[x], \Omega) = Hom_k(K, K)$ car $Conj_{k,K}(x) \subset K$.

Part II
Théorèmes

3 Théorème de Galois

3.1 Définitions

On considère pour la suite un corps k parfait, une extension ${}^{K}/_{k}$ algébrique et Ω la cloture algébrique de k, avec $k \subset K \subset \Omega$. L'extension ${}^{K}/_{k}$ est dite *galoisienne* si elle est algébrique et si pour tout $x \in K$, on a $Conj_{k,\Omega}(x) \subset K$.

81. On suppose que ${}^{K}/_{k}$ est galoisienne. Soit ${}^{E}/_{k}$ une sous-extension, avec $k \subset E \subset K$. Montrer que ${}^{K}/_{E}$ est galoisienne.

> **Solution:** Soit $x \in K$. On a alors $Conj_{k,\Omega} \subset K$. Soit π_k et π_E les polynômes minimaux annulateur de x dans k et E. On a $pi_k \in k[X] \subset E[X]$, d'où $\pi_E | \pi_k$. Donc $Conj_{E,\Omega} \subset Conj_{k,\Omega} \subset K$

82. Montrer que ${}^{K}/_{k}$ est galoisienne si et seulement si $Aut_k(K) = Hom_k(K, \Omega)$.

> **Solution:** $\implies$ Soit $\sigma \in Hom_k(K, \Omega)$, $x \in K$, alors $\sigma(x) \in Conj_{k,\Omega}(x) \subset K$. Donc $Im(\sigma) \subset K$. Montrons que $Im(\sigma) = K$. Soit $x \in K$, on note $X = \{x_1, \ldots, x_n\}$ ses conjugués sur k dans K. On a alors $\sigma(X) \subset X$. Or X fini et σ injective. D'où $\sigma(X) = X$ et donc $x \in Im(\sigma)$.
>
> $\impliedby$ Soit $x \in K$, $g \in Conj_{k,\Omega}(x)$. D'après la question 64, il existe $\sigma \in Hom_k(K, \Omega)$ tel que $\sigma(x) = g$ et $Im(\sigma) \subset K$, d'où $g \in K$.

On définit ainsi le *groupe de Galois* d'une extension galoisienne ${}^{K}/_{k}$ par $Gal({}^{K}/_{k}) = Aut_k(K) = Hom_k(K, \Omega)$.

83. Calculer le groupe de Galois de ${}^{\mathbb{F}_{p^n}}/_{\mathbb{F}_p}$.

> **Solution:** Soit $x \in \mathbb{F}_{p^n}$. On a $\pi_{x,\mathbb{F}_p} | X^{p^n} - X$ et $Conj_{\mathbb{F},\Omega}(x) = \{\text{racines de } X^{p^n} - X\} = \mathbb{F}_{p^n}$. Donc ${}^{\mathbb{F}_{p^n}}/_{\mathbb{F}_p}$ est galoisienne.
>
> D'après question 76, on a $Gal({}^{\mathbb{F}_{p^n}}/_{\mathbb{F}_p}) =< F_p >$.

84. On suppose que ${}^{K}/_{k}$ est galoisienne et on pose $x \in K$. Montrer que $Conj_{k,\Omega}(x) = \{\sigma(x) | \sigma \in Gal({}^{K}/_{k})\}$.

> **Solution:** Immédiat.

85. Montrer que ${}^{K}/_{k}$ galoisienne si et seulement si $\forall x \in K, Aut_k(K).x = Conj_{k,\Omega}(x)$.

Solution: $\Rightarrow$ On a $Aut_k(K).x \subset Conj_{k,\Omega}(x)$. Réciproquement, pour tout $y \in Conj_{k,\Omega}(x)$, il existe σ tel que $\sigma(x) = y$, d'où le résultat.
$\Leftarrow$ On a alors $Conj_{k,\Omega}(x) = Aut_k(K) \subset K$.

86. On suppose que ${}^K/_k$ est galoisienne et on pose ${}^E/_k$ une sous-extension. Montrer que $Gal({}^K/_E) \subset Gal({}^K/_k)$. Montrer que si l'on suppose ${}^E/_k$ galoisienne, alors on a une suite exacte : $\{e\} \to Gal({}^K/_E) \to Gal({}^K/_k) \to Gal({}^E/_k) \to \{e\}$.

Solution: On a $Aut_E(K) \subset Aut_k(K)$, d'où l'inclusion.
On pose $\phi : \begin{cases} Gal({}^K/_k) & \to Gal({}^E/_\Omega) \\ \sigma & \to \sigma_{|E} \end{cases}$. On a bien ϕ surjectif. En outre, $Ker(\phi) = \{\sigma \in Aut_k(K); \sigma_{|E} = Id\} = Aut_E(K, K) = Gal({}^K/_E) = Im(Id_{Gal({}^K/_E)})$, ce qui donne bien la suite exacte.

3.2 Groupe de galois d'un polynome

On se donne $P \in k[X]$, k corps parfait de racines $x_1, \ldots, x_n$ dans Ω, la cloture algébrique de k.

87. Montrer que le corps de décomposition de P définit une extension galoisienne de k

Solution: Simple application de la définition.

On appelle *groupe de Galois* de P le groupe $Gal(P, k) = Gal\left({}^{k[x_1,\ldots,x_n]}/_k\right)$.

88. Montrer que $Q(X) = \prod_{i=1}^n (X - x_i) \in k[X]$.

Solution: On factorise P en facteurs irréductibles, on a $P = \prod P_i^{n_i}$, avec $P_i \in k[X]$ irréductibles. Comme k est parfait, les P_i sont séparables, donc $Q(X) = \prod_i P_i = \prod_i (X - x_i) \in k[X]$.

89. En déduire que l'on peut supposer P séparable, et que l'on a une action fidèle de $Gal(P, k)$ sur les racines de P.

Solution: P et Q ont les mêmes racines, ils ont donc le même groupe de Galois. On peut donc supposer P séparable. On a donc comme action $\phi : \begin{cases} Gal(P, k) & \to Bij(\{x_1, \ldots, x_n\} \\ \sigma & \to \sigma_{|\{x_1,\ldots,x_n\}} \end{cases}$. On a bien ϕ injective car $x_1, \ldots, x_n$ engendre $k[x_1, \ldots, x_n]$.

90. Montrer que P est irréductible si et seulement si cette action agit transitivement sur les racines de P.

Solution: $\Rightarrow$ Soit $i \in [\![1, n]\!]$. On a alors $P = \pi_{x_i,k}$, et donc pour tout $j \leq n$, il existe $\sigma \in Hom_k(k[x_i], \Omega)$ tel que $\sigma(x_i) = x_j$. Le théorème de prolongement permet d'étendre en un élément de $Gal(P, k)$.

$\Leftarrow$ Si $P = QR$, alors Q et R ont des racines distinctes par séparabilité de P. Pour x_q racine de Q et x_r racine de R, on a $\{\sigma.x_q; \sigma \in Gal(P, k)\} = \{\sigma.x_r; \sigma \in Gal(P, k)\}$ par transitivité. Donc il existe σ tel que $x_q = \sigma(x_r)$ et donc $R(x_q) = 0$, ce qui est absurde.

3.3 Théorèmes

91. On suppose que ${}^K/_k$ est finie. Montrer que ${}^K/_k$ est galoisienne si et seulement si il existe $P \in k[X]$ irréductible tel que $K = k[x_1, \ldots, x_n]$ avec $x_1, \ldots, x_n$ les racines de P dans Ω.

Solution: $\Rightarrow$ On utilise le théorème de l'élément primitif. Il existe x tel que que $K = k[x]$. On note $x_1, \ldots, x_n$ conjugués de x dans Ω. Alors, comme ${}^K/_k$ est galoisienne, on a $x_1, \ldots, x_n \in K$ et donc $K = k[x_1, \ldots, x_n]$ corps de décomposition de $P = \pi_{x,k}$.

$\Leftarrow$ Soit $\sigma \in Hom_k(K, \Omega)$. On a $\sigma(\{x_1, \ldots, x_n\}) \subset \{x_1, \ldots, x_n\}$, donc $\sigma(K) \subset K$ et donc ${}^K/_k$ galoisienne.

92. On suppose que ${}^K/_k$ est galoisienne et finie et on pose $G = Gal({}^K/_k)$. Montrer que $|G| = [K : k]$ et que $K^G = k$.

Solution: On a $K = k[x]$. Et $|G| = |Hom_k(K, \Omega)| = [K : k]$ d'après question 80. On a $K^G = \{x \in K; \forall \sigma \in G, \sigma(x) = x\}$, d'où $k \subset K^G$. Soit $x \in K^G$. On a $Conj_{k,\Omega}(x) = \{\sigma(x), \sigma \in G\} = \{x\}$. En outre, $\pi_{x,k}$ est séparable car k parfait, donc $\pi_{x,k} = X - x \in k[X]$, d'où $x \in k$.

On montrer maintenant le Lemme d'Artin, qui s'énonce comme suit :

Lemme d'Artin : Si K est un corps parfait et G un sous-groupe fini de $Aut(K)$. Alors K^G est un corps parfait et ${}^K/_{K^G}$ est galoisienne finie de groupe de galois G.

93. (a) Montrer que K^G est parfait.

Solution: On suppose $car(K^G) = p > 0$. On a $K^G = \{x \in K; \forall g \in G, g(x) = x\}$. Soit $y \in K^G$, comme K est parfait, il existe $x \in K$ tel que $y = x^p$. Alors $g(y) = y = g(x)^p = x^p$, donc par injectivité de F_r, $x \in K^G$, donc F_r est surjectif, donc K^G est parfait.

(b) Montrer que ${}^K/_{K^G}$ est galoisienne.
Indication Pour $x \in K$, on pourra considérer le polynôme $P_x(X) = \prod_{g \in G}(X - g(x))$.

Solution: Soit $x \in K$. On considère $P_x(X) = \prod_{g \in G}(X - g(x))$. On a donc $\forall g \in G, g(P) = P$, donc $P \in K^G[X]$, et donc x algébrique sur K^G car $P_x(x) = 0$. En outre, $\pi_{x,K^G} | P_x$, on a donc $Conj_{K^G,\Omega}(x) \subset \{g(x), g \in G\} \subset K$, donc ${}^K/_{K^G}$ est galoisienne.

(c) Montrer que $Gal(K/K^G) = G$

Indication On pourra utiliser le théorème de l'élément primitif.

> **Solution:** On a $G \subset Aut_{K^G}(K)$. En outre, $\forall x \in K, [K^G[x] : K^G] < +\infty$. Soit $x \in K$ tel que $[K^G[x] : K^G]$ soit maximal. Supposons que $K^G[x] \neq K$. Alors il existe $y \in K$ tel que $[K^G[x, y] : K^G] > [K^G[x] : K]$. Par le théorème de l'élément primitif, $K^G[x, y]$ est monogène ce qui est absurde. D'où $[K : K^G] < +\infty$ et donc le lemme par la question 92.

Théorème. *(Galois) Soit K/k une extension finie, Ω la clôture algébrique de k avec k parfait et $k \subset K \subset \Omega$ et G le groupe de Galois de K/k. On pose $\mathcal{G} = S(G)$ l'ensemble des sous-groupes de G et $\mathcal{F}$ l'ensemble des corps compris entre k et K. D'où $\mathcal{G} = \{G' | G'$ sous-groupe de $G\}$ et $\mathcal{F} = \{L$ corps$|k \subset L \subset K\}$. Alors on a*

(i) L'application $f : \begin{cases} \mathcal{F} & \to \mathcal{G} \\ L & \to Gal(K/L) \end{cases}$ est une bijection strictement décroissante (pour l'inclusion) de bijection réciproque $f^{-1} : \begin{cases} \mathcal{G} & \to \mathcal{F} \\ H & \to K^H \end{cases}$.

(ii) Pour $H \in \mathcal{G}$, K/K^H est galoisienne et $Gal(K/K^H) = H$.

(iii) Pour $H \in \mathcal{G}$, L'application de restriction $r_H : \begin{cases} G & \to Hom_k(K^H, \Omega) \\ g & \to g_{|K^H} \end{cases}$ est surjective et $r_H^{-1}(\{Id\}) = H$.

(iv) Pour $H \in \mathcal{G}$, K^H/k est galoisienne si et seulement si H est distingué dans G. Alors $G/H = Gal(K^H/k)$.

(v) Pour $L \in \mathcal{F}$ tel que L/k est galoisienne, alors on a la suite exacte : $\{e\} \to Gal(K/L) \to Gal(K/k) \to Gal(L/k) \to \{e\}$

94. Démontrer le théorème de Galois en utilisant le lemme d'Artin.

Indication Pour la (iv), on pourra montrer que K^H/k est galoisienne si et seulement si $g(K^H) = K^H$.

> **Solution:**
>
> (i) On a $f^{-1}(f(L)) = K^{Gal(K/L)} = L$ car K/L est galoisienne et finie. Réciproquement, $f(f^{-1})(H) = Gal(K/K^H)$. Or K est parfait et H est fini car K/k est finie, d'où par le lemme d'Artin, $f(f^{-1})(H) = Gal(K/K^H) = H$. Enfin, $H \subset H' \Rightarrow K^{H'} \subset K^H$.
>
> (ii) Lemme d'Artin
>
> (iii) Théorème de prolongement des morphismes pour la surjectivité. $r_H^{-1}(\{Id\}) = \{g \in G; g_{|K^H} = Id\}$. On a $H \subset r_H^{-1}(\{Id\})$ par définition de K^H, et pour $g \in r_H^{-1}(\{Id\})$, on a $\forall x \in K^H, g(x) = x$, donc $g \in Gal(K/K^H) = H$.
>
> (iv) On suppose K^H/k galoisienne. Soit $g \in G$. On a K^H/k galoisienne, donc $g_{|K^H} \in Hom_k(K^H, \Omega) = Gal(K^H/k) = Aut_k(K^H)$, d'où $g(K^H) = K^H$. Et $K^{g^{-1}Hg} = \{x \in K; \forall h \in H, g^{-1}hg(x) = x\} = g(K^H)$. D'où $f^{-1}(H) = f^{-1}(g^{-1}Hg)$, donc H distingué car f bijective. Réciproquement, si H est distingué dans G, alors pour $g \in G$, $K^H = K^{g^{-1}Hg} = g(K^H)$, donc K^H/k galoisienne.
>
> (v) cf question 86

95. Donner les détails du théorème appliqué à $\mathbb{F}_{q^n}/\mathbb{F}_q$ pour $q = p^n$ avec p premier.

Solution: On a $K = \mathbb{F}_{q^n}$, $k = \mathbb{F}_q$ et $\Omega = \bar{\mathbb{F}}_p$.

On a alors $G = Aut_{\mathbb{F}_q}(\mathbb{F}_{q^n}) =< F_q >\simeq \mathbb{Z}/n\mathbb{Z}$, et $\mathcal{G} = \{\mathbb{Z}/d\mathbb{Z}; d|n\}$. On a aussi $\mathcal{F} = \{L \text{ corps }; \mathbb{F}_q \subset L \subset \mathbb{F}_{q^n}\} = \{\mathbb{F}_{q^r}, r|n\}$.

D'où $f : \begin{cases} \mathcal{F} & \to \mathcal{G} \\ \mathbb{F}_{q^r} & \to < F_{q^r} >\simeq r\mathbb{Z}/n\mathbb{Z} \end{cases}$ et $f^{-1} : \begin{cases} \mathcal{G} & \to \mathcal{F} \\ \mathbb{Z}/d\mathbb{Z} & \to \mathbb{F}_{q^{n/d}} \end{cases}$.

Enfin, on a $1 \to Gal(\mathbb{F}_{q^n}/\mathbb{F}_{q^r}) \to Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) \to Gal(\mathbb{F}_{q^r}/\mathbb{F}_q) \to 1$.

4 Cyclotomie

Soit k un corps parfait, et Ω sa clôture algébrique. On se fixe p un nombre premier, n un entier non nul non multiple de p. On suppose que $car(k) = p$.

96. Montrer que $X^n - 1$ est séparable.

Solution: On a alors nX^{n-1} et $X^n - 1$ premier entre eux car $car(k) = 0$.

On pose $\mu_n(\Omega)$ l'ensemble des racines de $X^n - 1$ dans Ω.

97. Montrer que μ_n est un sous-groupe de $\Omega^\times$ fini d'ordre n. On appelle *racine primitive n-ième* un générateur de ce groupe.

Solution: Pour $\mu_1, \mu_2 \in \mu_n(\Omega)$, on a $\mu_1 \times \mu_2^{-1} \in \mu_n(\Omega)$.

98. Soit $j_n \in \mu_n(\Omega)$ un racine primitive n-ième. Montrer que l'extension $k[j_n]/k$ est galoisienne et qu'elle ne dépend pas du choix de la racine primitive.

Solution: Soit j_n^m une autre racine primitive. On a $k[j_n^m] \subset k[j_n]$. De même, on a $k[j_n] \subset k[j_n^m]$, d'où l'égalité.

En outre, $X^n - 1$ annule j_n, donc $Conj_{k,\Omega}(j_n) \subset \mu_n(\Omega) \subset k[j_n]$, donc $k[j_n]/k$ est galoisienne.

L'extension $k[j_n]/k$ est appelé *n-ième extension cyclotomique* de k. On note $O_n = Gal(k[j_n]/k) = Gal(X^n - 1, k)$.

99. Montrer qu'il existe un unique morphisme de groupe $\chi : O_n \to (\mathbb{Z}/n\mathbb{Z})^\times$ tel que $\forall g \in O_n, g(j_n) = j_n^{\chi(g)}$.

Solution: Pour $g \in O_n$, on a $g(j_n)$ est une racine primitive car g est un automorphisme. Donc il existe $\chi(g) \in \mathbb{Z}/n\mathbb{Z}^\times$ tel que $g(j_n) = j_n^{\chi(g)}$. On vérifie que χ est bien un morphisme de groupe. On a $g \circ g'(j_n) = j_n^{\chi(g \circ g')} = g(j_n)^{\chi(g')} = j_n^{\chi(g)\chi(g')}$ et $g \circ g^{-1}(j_n) = j_n^1 = j_n^{\chi(g)\chi(g)^{-1}}$. Donc χ est bien un morphisme de groupe.

100. Montrer que χ est injectif et que O_n est commutatif.

Solution: χ est injective car $g \in O_n$ est déterminé par la donnée de $g(j_n) = j_n^{\chi(g)}$. On a donc $\chi(gg') = \chi(g')\chi(g) = \chi(g'g)$, ce qui donne la commutativité de O_n par injectivité de χ.

χ est appelé *caractère cyclotomique.* **On supposera par la suite que** $k = \mathbb{Q}$. On appelle n-ième polynôme cyclotomique $\phi_n(X) = \prod_{m \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - j_n^m) = \prod_{m \in (\mathbb{Z}/n\mathbb{Z})^\times} \left(X - \exp\left(\frac{2i\pi m}{n}\right)\right) \in \mathbb{C}[X]$.

101. Donner ϕ_1, ϕ_2, ϕ_3 et ϕ_4.

Solution:

- $\phi_1 = 1$
- $\phi_2 = X + 1$
- $\phi_3 = (X - exp(\frac{2i\pi}{3})(X - exp(\frac{4i\pi}{3}) = X^2 + X + 1$
- $\phi_4 = (X - exp(\frac{2i\pi}{4})(X - exp(\frac{6i\pi}{4}) = X^2 + 1$

On admettra par la suite le lemme de Gauss :

Lemme de Gauss : Soient $P, Q \in \mathbb{Z}[X]$ avec Q unitaire. Si Q divise P dans $\mathbb{Q}[X]$ alors Q divise P dans $\mathbb{Z}[X]$.

102. On veut montrer que $\phi_n \in \mathbb{Z}[X]$.

(a) Montrer que $k[j_n]^{O_n} = \mathbb{Q}$

Solution: Simple application du lemme d'Artin.

(b) Montrer que $X^n - 1 = \prod_{d|n} \phi_d(X)$.

Solution: On a $\mu_n(\Omega) = \bigcup_{d|n} \{j; j \text{ racine primitive } d\text{-ième de } 1\}$. D'où $X^n - 1 = \prod_{d|n} \phi_d(X)$.

(c) Montrer que $\phi_n \in \mathbb{Q}[X]$.

Solution: On a $\phi_n(X) \in (k[j_n])[X]$. Pour $g \in O_n$, g induit une permutation des racines de $\phi_n(X)$. Donc $g(\phi_n)(X) = \phi_n(X)$, et donc les coefficients de $\phi_n(X)$ sont dans $k[j_n]^{O_n} = \mathbb{Q}$.

(d) Conclure par récurrence.

Solution: L'initialisation est faite. On suppose le résultat pour tout $d < n$. On a alors $X^n - 1 = \left(\prod_{d|n, d \neq n} \phi_d(X)\right) \times \phi_n(X) = Q(X) \times \phi_n(X)$, avec $Q \in \mathbb{Z}[X]$ par hypothèse de récurrence. En outre, Q est unitaire car $\forall d, \phi_d$ est unitaire, et $Q | X^n - 1$ dans $\mathbb{Q}[X]$ car $\phi_n \in \mathbb{Q}[X]$. Donc, par le lemme de Gauss, Q divise $X^n - 1$ dans $\mathbb{Z}[X]$ et donc $\phi_n \in \mathbb{Z}[X]$.

103. On cherche à montrer que ϕ_n est irréductible dans $\mathbb{Q}[X]$.

(a) Soit $P = \pi_{e^{\frac{2i\pi}{n}},\mathbb{Q}}$, j une racine de P et p premier ne divisant pas n. Montrer que $X^{\bar{n}} - 1$ est séparable, où $X^{\bar{n}} - 1$ est la réduction modulo p de $X^n - 1$.

Solution: $X^n - 1 \wedge nX^{n-1} = 1$

(b) Montrer que j^p est une racine de P.
Indication On pourra considérer une racines de $S(X^p)$ avec S tel que, puis réduire modulo p.

Solution: On sait que $P|\phi_n|X^n - 1$. On écrit $X^n - 1 = P \times S$. On sait que j est une racine de $X^n - 1$, donc j^p aussi. Supposons que j^p ne soit pas une racine de P. Alors, par le théorème de Gauss, $S(j^p) = 0$. D'où j racine de $S(X^p)$. Donc $P(X) \wedge S(X^p) \neq 1$ et comme P est irréductible, on a $P|S(X^p)$.
On réduit modulo p. Ce qui donne $\bar{P}|\bar{S}(X^p) = (\bar{S}(X))^p$ car $F_r = Id$ sur $\mathbb{Z}/p\mathbb{Z}$. Soit π un facteur irréductible de $\bar{P}$. On a $\pi|\bar{P}|\bar{S}^p$, donc $\pi|\bar{S}$ et donc $\pi^2|\bar{P}\bar{S}|X^{\bar{n}} - 1$. Or comme $p \wedge n = 1$, $X^{\bar{n}} - 1$ est séparable. C'est donc absurde. D'où j^p racine de P.

(c) En déduire que ϕ_n est irréductible dans $\mathbb{Q}[X]$.

Solution: Soit $m = \prod_i p_i^{\alpha_i}$ premier avec n et $j = e^{\frac{2i\pi}{n}}$. On a donc pour tout i, p_i premier avec n. Donc $j^{p_1^{\alpha_1}}$ racine de P et par récurrence $j^{\prod_i p_i^{\alpha_i}} = j^m$ racine de P. Donc $\phi_n|P$, et donc ϕ_n est irréductible.

104. Montrer que χ est un isomorphisme.

Solution: On a donc $\phi_n = \pi_{e^{\frac{2i\pi}{n}},\mathbb{Q}}$, et que $[\mathbb{Q}[j_n] : \mathbb{Q}] = deg(\phi_n) = |\mathbb{Z}/n\mathbb{Z}^\times|$, avec ϕ l'indicatrice d'Euler. On sait que χ est injectif, et on a $|O_n| = [\mathbb{Q}[j_n] : \mathbb{Q}]$, d'où le résultat.

5 Constructibilité des polygones réguliers

Soit F un sous-corps de $\mathbb{R}$ et $E = F \times F$ l'ensemble des coordonnées dans F. On note :

- $\mathcal{D}$: l'ensemble des droites passant par deux points de E.
- $\mathcal{S}$: l'ensemble des cercles centré en un point de E, et ayant pour rayon la distance entre deux points de E.

Un point est dit *construit avec une règle et un compas* à partir d'un ensemble de point E si il est obtenu comme intersection entre soit :

(i) Deux droites de $\mathcal{D}$.
(ii) Une droite de $\mathcal{D}$ et un cercle de $\mathcal{S}$.
(iii) Deux cercles de $\mathcal{S}$.

On associe le plan cartésien à $\mathbb{C}$, que l'on identifiera à $\mathbb{R}^2$. On dit qu'un complexe $c \in \mathbb{C}$ est *constructible à la règle et au compas* (ou *constructible*) si on peut le construire à l'aide d'une règle et d'un compas à partir des points 1 et 0. On appelle $\mathcal{C}$ l'ensemble des points constructible.

105. Montrer que $\mathbb{Q}^2 \subset \mathcal{C}$ et que $\mathcal{C}$ est stable par racine carré, addition, multiplication et inverse.

Solution: On a évidement $\mathbb{Z}^2 \subset \mathcal{C}$. On peut alors obtenir tout rationnel par le théorème de Thales. La stabilité par inverse également, addition et multiplication. Pour $(x, x) \in \mathcal{C}$, on construit un carré de côté $\frac{x}{2}$, la diagonale mesure $\sqrt{x}$. Pour $c \in \mathcal{C}$, $\sqrt{c}$ vaut $re^{i\theta}$ où $r = \sqrt{|c|}$ et θ est la bissectrice de l'argument de c.

Ainsi, il est clair que le polygone régulier à n côtés est constructible si et seulement si $e^{\frac{2i\pi}{n}}$ est constructible. Pour faire le lien avec la théorie de Galois, il s'agit de montrer le résultat suivant :

Lemme : $c \in \mathbb{C}$ est constructible si et seulement si il existe $L_0 \subset L_1 \subset \cdots \subset L_n$ des corps tels que $c \in L_n$, $L_0 = \mathbb{Q}$ et $\forall i \in [\![1, n]\!], [L_i : L_{i-1}] = 2$.

106. (a) Montrer que si $d \in \mathcal{D}$, alors d a une équation à coefficients dans F polynomiale de degré 1, et que si $s \in \mathcal{S}$, alors s a une équation à coefficient dans F polynomiale de degré 2.

Solution: Il suffit d'écrire les relations.

(b) Soient $d, d' \in \mathcal{D}$ sécantes en M. Montrer que $M \in E$.

Solution: Il suffit d'écrire la résolution du système linéaire, qui utilise que des additions, multiplications et inverse.

(c) Montrer que si M est un point construit à la règle et au compas à partir de E, alors $M \in E$ ou il existe une extension quadratique G de F tel que $M \in G^2$.

Solution: Si $M = (x, y)$ est l'intersection d'un cercle et d'un cercle/d'une droite, en écrivant les equations, on trouve $P \in F[X]$ de degré 2 tel que $P(X) = 0$ et $Q \in F[X]$ tel que $y = Q(x)$.
Si P est irréductible, P est le polynôme minimal de x sur F et donc $G = F[x]$ convient.
Si P n'est pas irréductible, alors $x \in F$ et donc y aussi.

(d) En déduire le lemme.

Solution: Par une récurrence immédiate et la question (c), on a le résultat.

Le lien avec la théorie de Galois est maintenant effectué, on va pouvoir utiliser les puissants résultats démontrés précédemment, ce qui va nous conduire au théorème suivant.

Théorème (Wantzel) : Soit $c \in \mathbb{C}$ et K le corps de décomposition dans $\mathbb{C}$ de $\pi_{c,\mathbb{Q}}$. Alors c est constructible si et seulement si $[K : \mathbb{Q}]$ est une puissance de 2.

107. (a) Montrer que $[\mathbb{Q}[g] : \mathbb{Q}]$ est une puissance de 2.

Solution: On montre par récurrence sur On a donc une suite $\mathbb{Q} = L_0 \subset \cdots \subset L_n$ avec $g \in L_n$, et $[L_{i+1} : L_i] = 2$. Donc $[\mathbb{Q}[g] : \mathbb{Q}]$ est une puissance de 2.

(b) On pose $g_1, \ldots, g_n$ les conjugués de g dans $\bar{\mathbb{Q}}$ avec $g_1 = g$. Montrer par récurrence que pour tout $i \leq n$, $[\mathbb{Q}[g_1, \ldots, g_i] : \mathbb{Q}]$ est une puissance de 2. En déduire le sens direct.

Solution: On suppose la propriété pour $i - 1$. Alors soit $\sigma \in Hom_{\mathbb{Q}}(\bar{\mathbb{Q}}, \bar{\mathbb{Q}})$ tel que $g_i = \sigma(g)$. Alors on a $\mathbb{Q} = \sigma(L_0) \subset \cdots \subset \sigma(L_n)$ et $g_i \in \sigma(L_n)$. On a donc $\mathbb{Q} \subset \mathbb{Q}[g_1, \ldots, g_{i-1}] \subset \sigma(L_1)[g_1, \ldots, g_{i-1}] \subset \cdots \subset \sigma(L_n)[g_1, \ldots, g_{i-1}]$, d'où $[\mathbb{Q}[g_1, \ldots, g_i : \mathbb{Q}]$ est une puissance de 2.

(c) Montrer le sens réciproque.

Solution: On a ${}^{K}/_{\mathbb{Q}}$ galoisienne et finie car K est un corps de décomposition, et $[K:\mathbb{Q}] = 2^N$, avec $N \in \mathbb{N}$. Donc $|Gal({}^{K}/_{\mathbb{Q}})| = 2^N$. On a par la question 39, on a une suite de Jordan-Hölder $1 = G_0 \subset \cdots \subset G_m = Gal({}^{K}/_{\mathbb{Q}})$ avec G_i distingué dans G_{i+1} et $|{}^{G_{i+1}}/_{G_i}| = 2$. On obtient donc la suite de corps par la correspondance du théorème de Galois.

108. Soit p un nombre premier s'écrivant $p = 1+2^a$ avec $a \in \mathbb{N}$. Montrer qu'il existe $b \in \mathbb{N}$ tel que $p = 1+2^{2^b}$.
Indication On pourra utiliser le fait que, si λ est un entier impair, alors $1 + X|1 + X^\lambda$.

Solution: On écrit $a = \lambda 2^b$, avec $b \in \mathbb{N}$ et λ impair. On a alors $p = 1 + (2^{(2^b)})^\lambda$. En outre, comme λ est impair, on a $1 + X|1 + X^\lambda$, et donc $1 + 2^{2^b}|1 + (2^{2^b})^\lambda = p$. Comme p est premier, $\lambda = 1$ et donc $p = 1 + 2^{2^b}$.

On va enfin montrer le théorème de Gauss-Wantzel :

Théorème (Gauss-Wantzel) : Le polynome régulier à n côté est constructible à la règle et au compas si et seulement si $n = 2^N F_1 \cdots F_m$ avec $N \in \mathbb{N}$ et $F_1, \ldots, F_m$ des nombres premier de Fermat.

109. On rappelle qu'un nombre premier de Fermat est un nombre premier qui s'écrit de la forme $1 + 2^{2^a}$, $a \in \mathbb{N}$.

(a) Montrer le théorème Chinois : si $n_1, \ldots, n_m$ sont premiers entre eux, et $n = \prod_i n_i$, alors l'application

$$\psi : \begin{cases} {}^{\mathbb{Z}}/_{n\mathbb{Z}} & \to {}^{\mathbb{Z}}/_{n_1\mathbb{Z}} \times \cdots \times {}^{\mathbb{Z}}/_{n_m\mathbb{Z}} \\ k & \to (k \mod n_1, \ldots, k \mod n_m) \end{cases}$$

est un isomorphisme.

Solution: ψ est évidemment un morphisme. Soit $k \in Ker(\psi)$. Alors $\forall i, k \mod n_i = 0$, donc k est un multiple de n_i, donc k est un multiple de $\mathrm{PPCM}(n_1, \ldots, n_m) = n$ car les n_i sont premiers entre eux. Donc ψ est injective. En outre, ${}^{\mathbb{Z}}/_{n\mathbb{Z}}$ et ${}^{\mathbb{Z}}/_{n_1\mathbb{Z}} \times \cdots \times {}^{\mathbb{Z}}/_{n_i\mathbb{Z}}$ ont le même nombre d'éléments, donc ψ est un isomorphisme.

(b) On note ϕ l'indicatrice d'Euler. Montrer que si a et b sont premiers entre eux, alors $\phi(ab) = \phi(a)\phi(b)$.

Solution: On pose ψ de ${}^{\mathbb{Z}}/_{ab\mathbb{Z}}$ dans ${}^{\mathbb{Z}}/_{a\mathbb{Z}} \times {}^{\mathbb{Z}}/_{b\mathbb{Z}}$ l'isomorphisme donné par le théorème chinois. Si k est premier avec ab, alors k est premier avec a et b et donc $k \mod a \wedge a = 1$ et $k \mod b \wedge b = 1$. Réciproquement, si k_a et k_b sont premiers avec respectivement a et b, alors $k_a \times k_b = \psi^{-1}((k_a, k_b))$ est premier avec ab. Donc, en notant E l'ensemble des nombres premiers avec ab et inférieur à ab, et X l'ensemble des couples (k_a, k_b) avec k_a premier avec a et k_b premier avec b, on a $\psi(E) = X$ et donc $|E| = \phi(ab) = |X| = \phi(a)\phi(b)$.

(c) Soit $n \in \mathbb{N}$. On décompose n en facteurs premier, $n = \prod_i p_i^{\alpha_i}$, avec p_i premier. Montrer que

$$\phi(n) = \prod_i (p_i - 1) p_i^{\alpha_i - 1}$$

Solution: Soit p un nombre premier, calculons p^α. Les diviseurs de ϕ^α sont exactement tout les multiples de p inférieurs à p^α, soit les nombres de la forme $kp^\alpha + q$, où $0 \leq k \leq p-1$ et q est un diviseur de $p^{\alpha-1}$, et il y a 1 diviseur de p. Par récurrence immédiate, il y en a donc $p^{\alpha-1}$, d'où $\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = (p-1)p^{\alpha-1}$. Ce qui donne le résultat en appliquant la question (b).

(d) Montrer le théorème.

Solution: Le polygone régulier est constructible si et seulement si $e^{\frac{2i\pi}{n}}$ est constructible. Donc si et seulement si $\phi(n)$ est une puissance de 2. On considère la décomposition en facteur premier de n, elle vérifie donc $\prod_i (p_i - 1)p_i^{\alpha_i - 1} = 2^N$. Donc si $p_i \neq 2$, alors $\alpha_i = 1$ et $p_i - 1$ est une puissance de 2. Donc p_i est soit une puissance de 2, soit un nombre premier de Fermat par la question 108.