Chapitre 8

Théorie de Galois

Notation : On note $(L : K)$ l'extension $K \subset L$.

8.1 Extensions normales

Définition 8.1.1. Une extension $f : K \to L$ est normale si et seulement si tout polynôme irréductible de $K[X]$ qui admet une racine dans L est scindé dans L.

Théorème 8.1.2. *Soit $f : K \to L$ une extension. Il y a équivalence entre :*
a) l'extension est normale et de degré fini ;
b) L est corps de décomposition d'un polynôme unitaire de $K[X]$.

Définition 8.1.3. Une clôture normale d'une extension de degré fini : $f : K \to L$ est une extension $g : L \to L'$ telle que
a) l'extension $g \circ f : K \to L'$ est normale, et
b) l'extension $g : L \to L'$ est minimale pour la propriété a).

Proposition 8.1.4. *Toute extension admet une clôture normale, unique à isomorphisme près.*

8.2 Groupe de Galois

Définition 8.2.1. a) Un automorphisme du corps K est un homomorphisme bijectif de K dans lui-même.
b) Un automorphisme d'une extension $(L : K)$ est un automorphisme de L qui fixe les éléments de K (dont la restriction à K est l'identité).

Proposition 8.2.2. *Les automorphismes d'un corps K forment un groupe :* $\mathrm{Aut}(K)$*. Les automorphismes d'un extension* $(L:K)$ *forment un groupe qu'on appelle groupe de Galois de l'extension :* $\mathrm{Gal}(L,K)$ *ou* $\mathrm{Gal}(L:K)$*.*

Remarque 8.2.3. Lorsque K est le sous-corps premier de L, $\mathrm{Gal}(L:K)=\mathrm{Aut}(L)$.

Proposition 8.2.4. *Soit H un sous-groupe d'un groupe de Galois* $\mathrm{Gal}(L:K)$*, alors l'ensemble L^H des éléments fixés par tous les éléments de H est un sous-corps de L qui contient K : le corps fixe de H.*

8.3 Correspondance de Galois

Théorème 8.3.1. *Soit $K \to L$ une extension de degré fini, alors il y a équivalence entre :*
a) l'extension est normale et séparable,
b) $|\mathrm{Gal}(L:K)|=[L:K]$*,*
c) L est corps de décomposition d'un polynôme séparable sur K.

Définition 8.3.2. Une extension $K \to L$ est galoisienne si et seulement si elle est de degré fini et vérifie les conditions équivalentes du théorème précédent.

Théorème 8.3.3 (Galois)**.** *Soit* $(L:K)$ *une extension de degré fini galoisienne, alors :*
i) l' application : $H \mapsto L^H$, établit une bijection entre les sous-groupes H de $\mathrm{Gal}(L:K)$*, et les corps E intermédiaires : $K \subset E \subset L$; la bijection réciproque étant* $E \mapsto \mathrm{Gal}(L:E)$ *.*
ii) L'extension $(L^H:K)$ est galoisienne si et seulement si H est un sous-groupe distingué de $\mathrm{Gal}(L:K)$*. Dans ce cas le groupe de Galois,* $\mathrm{Gal}(E:K)$ *est isomorphe au quotient :* $\mathrm{Gal}(L:K)/H$*.*

6/12/2010

Le théorème suivant est le point clé dans la preuve du théorème de Galois.

Théorème 8.3.4. *Soit H un groupe fini d'automorphisme du corps L et L^H le corps fixe associé. Alors l'extension $(L:L^H)$ est galoisienne, de groupe de Galois H.*

Démonstration. Démontrons le théorème. Posons $n=[L:L^H]$, $m'=|\mathrm{Gal}(L:L^H)|$ et $m=|H|=[L:K]$. Notons que : $H\subset \mathrm{Gal}(L:L^H)$, donc : $m\leq m'$. L'extension $(L:K)$ étant de degré fini, on a : $\mathrm{Gal}(L:K)=\mathrm{Hom}_{K-\mathrm{alg}}(L,L)$. On a vu au chapitre précédent la majoration du nombre de morphismes par le degré : $m'\leq n$. Donc : $m\leq m'\leq n$.

Supposons que $m < n$. On fixe une partie libre de L sur L^H de cardinal $m+1$: $x_1, \ldots, x_{m+1}$. La matrice formée par les $\sigma(x_j)$, $\sigma \in H$, $1 \leq j \leq m+1$, a m lignes et $m+1$ colonnes : ses colonnes sont dépendantes. Quitte à réordonner, on suppose que les r premières colonnes forment une partie liée minimale (rang $r-1$). On a une relation de dépendance avec tous les coefficients $y_j \in L$ non nuls :

$$\forall \sigma \in H \ \sum_{j=1}^{r} \sigma(x_j) y_j = 0 \ .$$

On peut trouver une telle relation avec $y_1 = 1$, ce que nous supposons désormais.

$$\forall \tau \in H \ \forall \sigma \in H \ \sum_{j=1}^{r} \tau(\sigma(x_j) y_j) = 0 \ .$$

En posant $\tau\sigma = \gamma$:

$$\forall \tau \in H \ \forall \gamma \in H \ \sum_{j=1}^{r} \gamma(x_j) \tau(y_j) = 0 \ .$$

Pour chaque τ on obtient une nouvelle relation. En utilisant que le rang est égal à r, et que $\tau(y_1) = y_1 = 1$, on obtient pout tout j, $\tau(y_j) = y_j$. Chaque y_j est fixé par tous les élements de H : $y_j \in L^H$. Reprenons la relation de dépendance qui est maintenant à coefficients dans L^H :

$$\forall \gamma \in H \ \sum_{j=1}^{r} \gamma(x_j) y_j = 0 \ .$$

Avec $\gamma = \mathrm{Id}$, on a une relation de dépendance entre les x_j, ce qui donne une contradiction. On conclut : $n = m = m'$, et $H = \mathrm{Gal}(L : L^H)$. □

Corollaire 8.3.5. *Une extension de degré fini* $(L : K)$ *est galoisienne si et seulement si* $K = L^{\mathrm{Gal}(L,K)}$.

La preuve du b) dans le théorème de Galois utilise les lemmes suivants :

Lemme 8.3.6. *Soient* $(L : K)$ *une extension galoisienne, et* E *un corps intermédiaire associé au sous-groupe* $H \subset \mathrm{Gal}(L : K)$*, alors pour tout* $\sigma \in \mathrm{Gal}(L : K)$*, on a* $\mathrm{Gal}(L : \sigma(E)) = \sigma H \sigma^{-1}$ *(*$N(H)$ *est le normalisateur de* H*, i.e ; le stabilisateur pour l'action de conjugaison sur les sous-groupes.*

Lemme 8.3.7. *Soient* $(L : K)$ *une extension galoisienne, et* E *un corps intermédiaire associé au sous-groupe* $H \subset \mathrm{Gal}(L : K)$*, alors la restriction définit un morphisme surjectif* $N(H) \to \mathrm{Gal}(E, K)$ *de noyau* $\mathrm{Gal}(L : E)$.

9/12/2010

Exercice 8.3.8. Etudier les extensions $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ et $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}, j)$ ($j = e^{i\frac{2\pi}{3}}$). Sont-elles galoisiennes ? Calculer le groupe de Galois. Déterminer les corps intermédiaires.

8.4 Exemples

Un exemple élémentaire

Soit $L \subset \mathbb{C}$ le corps de décomposition (sur $\mathbb{Q}$) de X^4-2. C'est une extension galoisienne, comme corps de décomposition d'un polynôme séparable (en caractéristique zéro tout polynôme est séparable). Les racines de X^4-2 sont $\pm\sqrt[4]{2}$, $\pm i\sqrt[4]{2}$. Le polynôme X^4-2 étant irréductible sur $\mathbb{Q}$ (justifier), l'extension $(\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q})$ est de degré 4. L'extension $(L : \mathbb{Q}(\sqrt[4]{2}))$ est de degré 2 : elle est engendrée par i qui n'est pas dans $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$. On a donc : $[L : \mathbb{Q}] = 8$. Le groupe de Galois $G = \mathrm{Gal}(L : \mathbb{Q})$ est de cardinal 8. Pour $\rho \in G$, $\rho(i) = \pm i$ et $\rho(\sqrt[4]{2}) \in \{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$. L'application

$$\begin{array}{rccl} r: & G & \to & \{\pm i\} \times \{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\} \\ & \rho & \mapsto & (\rho(i), \rho(\sqrt[4]{2})) \end{array}$$

est injective, car i et $\sqrt[4]{2}$ engendrent l'extension. C'est une application entre ensembles finis de mêmes cardinaux : elle est bijective. Les éléments $\tau = r^{-1}(-i, \sqrt[4]{2})$, $\sigma = r^{-1}(i, i\sqrt[4]{2})$ engendrent le groupe G, avec les relations :

$$\tau^2 = \sigma^4 = id \ , \ \sigma\tau = \tau\sigma^{-1} \ .$$

On reconnaît le groupe diédral D_4 (groupe des isométries du carré). Il y a 5 éléments d'ordre 2 et un élément d'ordre 4 qui engendrent des sous-groupes cycliques, et il y a deux sous-groupes de cardinal 4 non cycliques. Voir les corps correspondants dans la figure 8.1.

Corps cyclotomiques

Définition 8.4.1. On appelle corps cyclotomique une extension $(\mathbb{Q}(\zeta_n) : \mathbb{Q})$, où ζ_n est une racine primitive n-ième de l'unité.

Proposition 8.4.2. *L'extension cyclotomique* $(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ *est galoisienne, de groupe de Galois isomorphe à* $(\mathbb{Z}/n\mathbb{Z})^\times$*.*

Démonstration. Le corps cyclotomique $\mathbb{Q}(\zeta_n)$ est le corps de décomposition sur $\mathbb{Q}$ du polynôme $X^n - 1$: c'est une extension galoisienne. Le polynôme minimal de ζ_n est le polynôme cyclotomique Φ_n dont les racines sont les ζ_n^k, $k \in (\mathbb{Z}/n\mathbb{Z})^\times$. Notons $\tau_k \in \mathrm{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ l'automorphisme correspondant à ζ_n^k. On a : $\tau_k\tau'_k = \tau_{kk'}$. Les groupes $\mathrm{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ et $(\mathbb{Z}/n\mathbb{Z})^\times$ sont isomorphes. $\square$

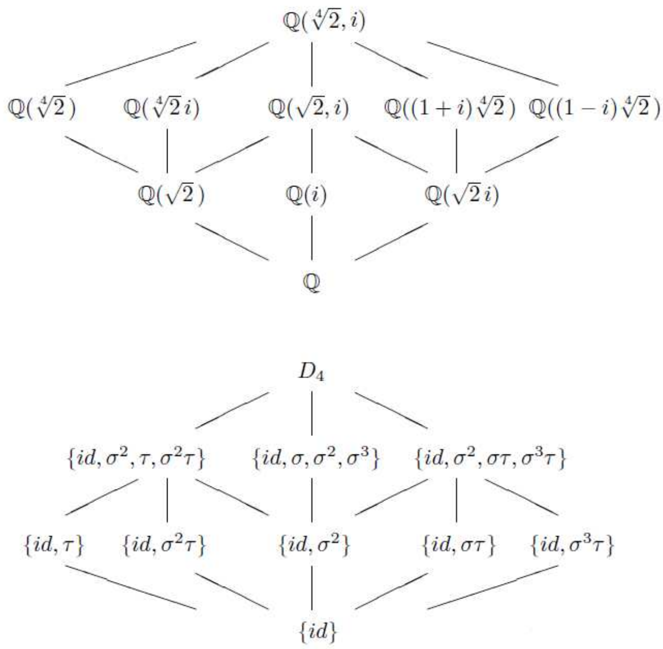

FIGURE 8.1 – Correspondance de Galois pour $X^4 - 2$

Remarque 8.4.3. La structure du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ découle du théorème chinois et des résultats suivants (voir par exemple le cours d'arithmétique de Bernhard Keller, section 19, `http://www.math.jussieu.fr/~keller/mt282/arith.pdf` :

1. Pour p premier impair et $\alpha > 0$, $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique.
2. Pour $\alpha \geq 3$, $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ est isomorphe au produit de $\mathbb{Z}/2$ par un groupe cyclique.

On peut en déduire les sous-groupes et donc les sous-corps de $\mathbb{Q}(\zeta_n)$.

Exercice 8.4.4. Etudier les sous-corps de $\mathbb{Q}(\zeta_{12})$.

Corps finis

Proposition 8.4.5. *Pour $q = p^m$, l'extension $(\mathbb{F}_q : \mathbb{F}_p)$ est galoisienne. Le groupe de Galois est cyclique, engendré par l'automorphisme de Frobenius.*

Démonstration. Pour un corps fini, le morphisme de Frobenius $F : x \mapsto x^p$ est un automorphisme : $F \in \mathrm{Gal}(\mathbb{F}_q : \mathbb{F}_p)$. On va montrer qu'il est d'ordre $m = [\mathbb{F}_q : \mathbb{F}_p]$. Cela justifie que l'extension est galoisienne : $\mathrm{Gal}(\mathbb{F}_q : \mathbb{F}_p) = [\mathbb{F}_q : \mathbb{F}_p]$, et que F engendre le groupe de Galois.

Le groupe multiplicatif $\mathbb{F}_q^*$ est cyclique de cardinal $q-1$. Notons α un générateur : α engendre l'extension. On a $\frac{F^\nu(\alpha)}{\alpha} = \alpha^{p^\nu - 1}$, d'où :

$$F^m = Id \text{ et } F^\nu \neq Id \text{ pour } 0 < \nu < m \ .$$

□

Remarque 8.4.6. La correspondance de Galois redonne que les sous-corps de $\mathbb{F}_q$ sont en bijection avec les diviseurs de m.

8.5 Groupe de Galois d'un polynôme séparable

Définition 8.5.1. Le groupe de Galois d'un polynôme séparable est celui de l'extension qui réalise le corps de décomposition : pour $P \in K[X]$, $\mathrm{Gal}(P) = \mathrm{Gal}(L : K)$, où L est le corps de décomposition de P.

Remarque 8.5.2. Le groupe de Galois agit sur les racines de P, et cette action est fidèle.

Théorème 8.5.3. *Le polynôme générique*

$$P = X^n - \sigma_1 X^{n-1} + \cdots + (-1)^n \sigma_n \ ,$$

est séparable et son groupe de Galois est isomorphe au groupe symétrique $\mathcal{S}_n$.

Démonstration.
Il s'agit d'étudier l'extension $(K(X_1, \ldots, X_n) : K(\sigma_1, \ldots, \sigma_n))$. Toute permutation des variables s'étend en un automorphisme du corps $K(X_1, \ldots, X_n)$ qui est l'identité sur $K(\sigma_1, \ldots, \sigma_n)$. L'action $\mathrm{Gal}(P) \to \mathcal{B}(\{X_1, \ldots, X_n\}) \simeq \mathcal{S}_n$ est un isomorphisme. □

On note $\mathcal{A}_n$ le groupe alterné (formé des permutations paires).

Proposition 8.5.4. *Pour un polynôme séparable $P \in K[X]$, on a :* $\mathrm{Gal}(P) \subset \mathcal{A}_n$ *si et seulement si le discriminant de P est un carré dans K.*

Démonstration. Le discriminant de $P = \prod_{i=1}^n (X - x_i)$ est $D = d^2$, avec $d = \prod_{1 \leq i < j \leq n} (x_i - x_j)$. C'est un carré dans le corps K si et seulement si d est fixe par tous les élements du groupe de Galois. Pour une permutation σ des racines de P, $\sigma.d = \epsilon_\sigma d$, où ϵ_σ est la signature : le discriminant de P est un carré dans K si et seulement si tout élément du groupe de Galois induit une permutation paire. □

Polynômes de petit degré ...

8.6 Résolubilité par radicaux

Définition 8.6.1. Une extension $(L : K)$ est cyclique (resp. abélienne) si et seulement si elle est galoisienne et son groupe de Galois est cyclique (resp. commutatif).

Proposition 8.6.2. *Soit K un corps, de caractéristique nulle ou première avec n, qui contient les racines n-ièmes de l'unité. Pour $a \in K$ l'extension $K(b)$ où b est racine n-ième de a (dans le corps de décomposition de $X^n - a$) est cyclique de degré d diviseur de n.*

Démonstration. Les racines de $X^n - a$ sont les ζb, avec ζ racine n-ième de l'unité : elle sont dans $K(b)$, qui est donc le corps de décomposition sur K du polynôme $X^n - a$. La caractéristique étant nulle ou première avec n, ce polynôme est séparable. On obtient une extension galoisienne. Le polynôme minimal P_b divise $X^n - a$. Notons U_n le groupe des racines de l'unité ; il est cyclique d'ordre n car $X^n - 1$ est séparable. L'application :

$$\begin{array}{rccc} \phi : & \mathrm{Gal}(K(b) : K) & \to & U_n \\ & \tau & \mapsto & \frac{\tau(b)}{b} \end{array}$$

est un morphisme injectif. Le goupe de Galois $\mathrm{Gal}(K(b) : K)$ est isomorphe à un sous-groupe du groupe cyclique U_n. C'est un groupe cyclique dont l'ordre d divise n. □

Proposition 8.6.3. *Soit $(L : K)$ une extension cyclique de degré n sur un corps, de caractéristique nulle ou première avec n, qui contient les racines n-ièmes de l'unité, alors $L = K(b)$ avec b de polynôme minimal $X^n - a$.*

Démonstration. Soit τ un générateur du groupe de Galois. C'est un automorphisme K-linéaire de $K(b)$ qui vérifie $\tau^n = Id$. Le polynôme minimal de τ divise $X^n - 1$ qui est séparable, donc τ est diagonalisable. Ses valeurs propres sont des racines de l'unité. Notons que :$\tau(a) = \alpha a$ et $\tau(b) = \beta b$ entraîne $\tau(\frac{a}{b}) = \frac{\alpha}{\beta}\frac{a}{b}$: l'ensemble des valeurs propres forme un sous-groupe du groupe U_n des racines de l'unité, donc est un groupe cyclique d'ordre d. Si on avait $d < n$, on aurait $\tau^d = Id$, ce qui est exclu. Donc l'ensemble des valeurs propres de τ est égal à U_n. Soit b un vecteur propre non nul pour un générateur ζ de U_n. Tous les $\tau^k(b) = \zeta^k b$ sont des racines du polynôme minimal P_b. On obtient (on a autant de racines que le degré) :

$$P_b = \prod_{k=0}^{n-1}(X - \zeta^k b) = X^n - b^n = X^n - a\ .$$

Notons que a est dans K. □

Définition 8.6.4. a) Une extension radicale d'un corps K est un corps obtenu par une suite d'extensions, chacune étant engendrée par une racine :

$$K = K_0 \subset K_1 \subset \dots K_m = L \ ,$$

avec $K_i = K_{i-1}(\sqrt[n_i]{a_i})$, $a_i \in K_{i-1}$.
b) Un polynôme à coefficients dans un corps de caractéristique nulle est résoluble par radicaux si et seulement s'il existe une extension radicale qui contient toutes ses racines.

Théorème 8.6.5. *Un polynôme P à coefficient dans un corps de caractéristique nulle est résoluble par radicaux si et seulement si son groupe de Galois G est résoluble, c'est à dire qu'il existe une suite :*

$$\{e\} = G_0 \subset G_1 \subset \cdots \subset G_m = G \ ,$$

avec, pour tout $i < m$, G_i sous-groupe distingué de G_{i+1}, et G_{i+1}/G_i abélien.

Démonstration. Soit P un polynôme à coefficients dans K.
Supposons que P est résoluble par radicaux : le corps de décomposition L de P sur K est contenu dans une extension K_m telle que :

$$K = K_0 \subset K_1 \subset \cdots \subset K_m \ ,$$

avec $K_i = K_{i-1}(\sqrt[n_i]{a_i})$. Pour $n = PPCM(n_1, \dots, n_m)$, notons $K' = K(\zeta_n)$ l'extension cyclotomique de K obtenu en adjoignant la racine n-ième de l'unité ζ_n et $K'_i = K_i(\zeta_n) = K'_{i-1}(\sqrt[n_i]{a_i})$. L'extensions $(K' : K)$ est abélienne. Comme n_i divise n, $K'i$ contient les racines n_i-ièmes de l'unité, et les extensions $(K'_i : K'_{i-1})$ sont cycliques pour $1 \leq i \leq m$.
On obtient une tour d'extension galoisiennes :

$$K'_{-1} = K \subset K'_0 = K' \subset K'_1 \subset \cdots \subset K'_m \ .$$

La correspondance de Galois nous donne une suite de groupes :

$$G'_{-1} \supset G'_0 \supset \cdots \supset G'_m = \{id\} \ .$$

avec pour tout $0 \leq i \leq m$, G'_i distingué dans G'_{i-1} et G'_{i-1}/G'_i abélien. Le groupe $G'_{-1} = \mathrm{Gal}(K'_m, K)$ est donc résoluble. On a une tour d'extensions galoisiennes :

$$K \subset L \subset K'_m.$$

Le groupe de Galois $\mathrm{Gal}(L, K) = \mathrm{Gal}(K'_m, K)/\mathrm{Gal}(K'_m, L)$ est quotient d'un groupe résoluble. C'est un groupe résoluble.

Supposons que le groupe de Galois du polynôme P, $\mathrm{Gal}(P) = \mathrm{Gal}(L, K)$ est résoluble (L est corps de décomposition de P) :

$$\{e\} = G_0 \subset G_1 \subset \cdots \subset G_m = G \ ,$$

avec, pour tout $i < m$, G_i sous-groupe distingué de G_{i+1}, et G_{i+1}/G_i cyclique (voir l'exercice 8.6.7). On considère les corps fixes $K_i = L^{G_{m-i}}$. On obtient une tour d'extensions :

$$K = K_0 \subset K_1 \subset \cdots \subset K_m = L \ .$$

Les extensions $(L : K_i)$ sont galoisiennes, et $\mathrm{Gal}(L, K_i) = G_{m-i}$ est un sous-groupe distingué de $\mathrm{Gal}(L, K_{i-1}) = G_{m-i+1}$. Les extensions $(K_i : K_{i-1})$ sont donc galoisiennes de groupe de Galois cyclique G_{m-i+1}/G_{m-i}. Elles sont donc primitives : $K_i = K_{i-1}(x_i)$. On adjoint à chaque corps K_i une racine de l'unité ζ_n d'ordre $n = [L : K]$: $K'_i = K_i(\zeta_n) = K_i(\zeta_n, x_i) = K'_i(x_i)$. Le groupe de Galois $\mathrm{Gal}(K'_i, K'_{i-1})$ est isomorphe au sous-groupe de $\mathrm{Gal}(K_i, K_{i-1})$ correspondant aux racines du polynôme minimal de x_i sur K_{i-1} qui sont aussi racines du polynôme minimal de x_i sur K'_{i-1}. C'est un sous-groupe d'un groupe cyclique, donc un groupe cyclique. Le degré n_i de l'extension (K'_i, K'_{i-1}) divise n, donc les racines n_i-ièmes de l'unité sont dans K'_i. L'extension $(K'_i : K'_{i-1})$ est donc de la forme $K'_{i-1}(\sqrt[n_i]{a_i})$. On obtient que L est inclus dans une extension radicale. □

Exercice 8.6.6. Montrer qu'un groupe fini G est résoluble si et seulement s'il existe une suite :

$$\{e\} = G_0 \subset G_1 \subset \cdots \subset G_m = G \ ,$$

avec, pour tout $i < m$, G_i sous-groupe distingué de G_{i+1}, et G_{i+1}/G_i cyclique

Exercice 8.6.7. Montrer qu'un quotient d'un groupe résoluble est résoluble.

Théorème 8.6.8. *Pour $n \geq 5$, le polynôme générique de degré n n'est pas résoluble par radicaux.*

C'est une conséquence du fait que pour $n \geq 5$ le groupe alterné $\mathcal{A}_n$ est simple (pas de sous-groupe distingué autre que le trivial et lui-même).

Exercice 8.6.9. Décrire les classes de conjugaison dans $\mathcal{A}_5$, et déduire une preuve de la simplicité de $\mathcal{A}_5$.

8.7 Théorème de d'Alembert-Gauss par la théorie de Galois

On se propose de démontrer que $\mathbb{C}$ est algébriquement clos. On obtient, sans utiliser le théorème de d'Alembert-Gauss les lemmes suivants (démontrer) :

Lemme 8.7.1. *Le corps* $\mathbb{C}$ *n'a pas d'extension de degré* 2.

Lemme 8.7.2. *Le corps* $\mathbb{C}$ *n'a pas d'extension non triviale de degré impair.*

Théorème 8.7.3 (d'Alembert-Gauss)**.** *Le corps* $\mathbb{C}$ *est algébriquement clos.*

Démonstration. Soit P un polynôme à coefficients complexes, et K son corps de décomposition. On écrit le degré de l'extension sous la forme $[K : \mathbb{C}] = 2^\alpha m$, avec m impair. Le théorème de Sylow nous donne un sous-groupe $H \subset \mathrm{Gal}(K : \mathbb{C})$ de cardinal 2^α. Le corps fixe K^H est une extension de degré m impair : elle est triviale, $m = 1$. Il reste un groupe de Galois G de cardinal 2^α. L'exercice ci-dessous montre que si G, de cardinal 2^α est non trivial, alors il a un sous-groupe d'indice 2. Le corps fixe pour ce sous-groupe ferait une extension de degré 2, ce qui est exclu par le lemme précédent. Finalement $K = \mathbb{C}$. □

Exercice 8.7.4. Soit G un groupe fini de cardinal p^α.

1. Montrer que le centre de G est non trivial.
2. Montrer qu'il existe une suite emboitée de sous-groupes distingués de G :
$$\{e\} = G_0 \subset G_1 \subset \cdots \subset G_\alpha = G \ ,$$
telle que pour tout i, G_i est d'ordre p^i.
3. Déduire qu'un p-groupe fini est résoluble.

13/12/2010