Développement : Théorème de Burnside (Groupes simples)

Thomas W.

7 juillet 2023

Leçons concernées :

- 101 : Groupe opérant sur un ensemble. Exemples et applications. *****
- 102 : Groupe des nombres complexes de module 1. Racines de l'unité. Applications. *****
- 103 : Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications. *****
- 104 : Groupes finis. Exemples et applications. *****
- 121 : Nombres premiers. Exemples et applications. *****
- 125 : Extensions de corps. Exemples et applications. ***
- 144 : Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications. ****

Références :

- 131 Développements pour l'oral, D.Lesevre, P.Montagnon, P.Le Barbenchon, T.Pierron
- Nouvelles histoires hédonistes de groupes et de géométries, tome 2, P. Caldero et J.Germoni
- Théorie de Galois, I. Gozard

Commentaires sur le développement :
Le gros du développement se trouve dans le livre "131 développements pour l'oral", sous le nom de **théorème p^aq^b de Burnside**, mais j'ai modifié quelques petits détails pour qu'il soit plus à mon goût. On peut aussi suivre le fil de ce livre. Je rajoute aussi dans ce document les preuves de quelques points (laissés sous forme de question dans le livre) qui m'ont posé des problèmes, en espérant aider quelques personnes. Je trouve ce développement difficile sous bien des aspects : les pré-requis sont très vastes, il faut bien connaître la théorie des représentations de groupes finis, quelques résultats de théorie de Galois, les théorèmes de Sylow et la notion d'entiers algébriques. Cela dit, ces pré-requis peuvent être réinvestis dans beaucoup

d'autres leçons, surtout la théorie des représentations. Il n'est donc pas inutile, à mon avis, de les travailler. Ensuite, il y a quelques passages qui sont assez techniques, ce qui impose de le répéter plusieurs fois dans l'année. Enfin, ce développement est vraiment très long et il est impossible de tout faire en 15 minutes. Mais c'est là aussi sa force : on peut le présenter en fonction de la leçon dans laquelle on veut le mettre, ce qui le rend très recasable. Il est cependant nécessaire d'être capable de le mener jusqu'au bout en cas de question du jury. C'était je pense le développement le plus sophistiqué que j'ai appris pendant mon année de préparation à l'agrégation. Rappelons quand même qu'il n'est pas nécessaire de présenter des très grandes choses pour prétendre à une bonne note à l'oral. J'ai passé beaucoup de temps sur ce développement et j'ai terminé l'année avec des impasses dans d'autres leçons (trop à mon goût). Il était peut-être un peu trop au-dessus de mon niveau. En plus, je n'ai même pas pu le présenter le jour J.

Théorème (p^aq^b de Burnside)
Soient p, q deux nombres premiers et $a, b \in \mathbf{N}$ deux entiers naturels. Alors, tout groupe d'ordre p^aq^b n'est pas simple.

On démontre d'abord deux lemmes préliminaires :

Lemme
Soient G un groupe fini d'ordre n et χ un caractère de G. L'élément neutre de G sera noté 1. Alors :

1. $(\forall g \in G), 0 \leq |\frac{\chi(g)}{\chi(1)}| \leq 1$
2. *Si $g \in G$ est tel que $0 < |\frac{\chi(g)}{\chi(1)}| < 1$, alors $\frac{\chi(g)}{\chi(1)}$ n'est pas un entier algébrique.*
3. *Si χ est un caractère irréductible de G, le nombre complexe $\frac{|G|\chi(g)}{|Stab_G(g)|\chi(1)}$ est un entier algébrique.*

Démonstration

1. *La preuve de ce point est très classique. Elle peut-être omise ou présentée rapidement à l'oral si la leçon concernée n'est pas la 102. Les arguments utilisés peuvent apparaître dans d'autres leçons : diagonalisation, polynômes d'endomorphismes, sous-espaces stables... Par exemple, le théorème de co-diagonalisation d'endomorphismes diagonalisables qui commutent et le fait que les $\rho(g)$ soient diagonalisables permet de montrer que les caractères irréductibles d'un groupe abélien fini sont de degré 1. Pour la réciproque, diagonaliser la régulière, qui est fidèle (il est bon d'avoir en tête que la régulière est fidèle). Je n'ai pas de référence qui prouve ce point sans passer par le fait que le nombre de caractère de degré 1 est égal au nombre de classes de conjugaisons. C'est un de mes professeurs qui m'a montré ça.*

G est un groupe fini d'ordre n, donc, d'après le théorème de Lagrange, on a $g^n = 1$ pour tout $g \in G$. χ est le caractère d'une certaine représentation ρ (biensûr, pas unique ! deux représentations (complexes) sont isomorphes au sens des réprésentations ssi elles ont même caractère) à valeurs dans $GL(V)$, V étant un $\mathbf{C}$-espace vectoriel de dimension finie. On a donc $\rho(g^n) = \rho(g)^n = id_V$ car ρ est un morphisme de groupes. Ainsi, le polynôme $P(X) = X^n - 1$ est annulateur de $\rho(g)$ et ce polynôme a pour racines les racines $n-$ièmes de l'unité.(Au passage, P est scindé à racines simples donc $\rho(g)$ est diagonalisable pour tout g). Les valeurs propres de $\rho(g)$ sont donc des racines n-ièmes de l'unité, on les notes $\lambda_1, \ldots, \lambda_s$, répétées avec multiplicités, avec $s = dim(V)$. Ce qui donne :

$$\left|\frac{\chi(g)}{\chi(1)}\right| = \left|\frac{\lambda_1 + \ldots + \lambda_s}{s}\right| \leq 1$$

par inégalité triangulaire, car les λ_i sont de module 1.

2. *Raisonnons par l'absurde et supposons que $\frac{\chi(g)}{\chi(1)}$ est un entier algébrique. Son polynôme minimal est donc un polynôme à coefficient dans $\mathbf{Z}$ (attention, ce n'est pas évident. Je rappelle la démonstration, ainsi que celles d'autres résultats, à la fin du document). Soit $P(X) = X^d + a_{d-1}X^{d-1} + \ldots + a_0$ ce polynôme minimal. Les $\mathbf{Q}$-conjugués de $\frac{\chi(g)}{\chi(1)}$, c'est-à-dire les autres racines de P dans $\mathbf{C}$, sont alors de la forme $\frac{\chi(g)^*}{\chi(1)}$, où $\chi(g)^*$ désigne un $\mathbf{Q}$-conjugué de $\chi(g)$ quelconque (c'est un abus de notation). En effet, P étant irréductible sur $\mathbf{Q}$, son groupe de Galois agit de façon transitive sur l'ensemble de ses racines dans $\mathbf{C}$. Ainsi, pour tout $\mathbf{Q}$-conjugué x de $\frac{\chi(g)}{\chi(1)}$, il existe un élément σ du groupe de Galois de P tel que $\sigma(\frac{\chi(g)}{\chi(1)}) = x$. σ étant un morphisme de corps qui fixe $\mathbf{Q}$, on a $\sigma(\frac{\chi(g)}{\chi(1)}) = \frac{\sigma(\chi(g))}{\chi(1)} = \frac{\sigma(\lambda_1)+\ldots+\sigma(\lambda_s)}{\chi(1)}$. Or, les λ_i étant des racines n-ièmes de l'unité, les $\sigma(\lambda_i)$ sont aussi des racines n-ièmes de l'unité. (Il suffit de mettre à la puissance n, ou alors, pour utiliser un raisonnement qu'on retrouve souvent en théorie de Galois, dire que le polynôme minimal d'une racine n-ième de l'unité λ est le d-ième polynôme cyclotomique Φ_d où d est l'ordre de λ dans le groupe des racines n-ième de l'unité et que l'on a $\Phi_d(\sigma(\lambda)) = \sigma(\Phi_d(\lambda)) = 0$ et donc $\sigma(\lambda)$ est encore une racine de Φ_d, donc une racine d-ième de l'unité). En utilisant le même raisonnement que dans la question 1), on en déduit que $|x| \leq 1$, pour tout $\mathbf{Q}$-conjugué de $\frac{\chi(g)}{\chi(1)}$. Notons alors $z_1, \ldots, z_d$ les racines complexes de P, distinctes deux à deux car P est irréductible, avec $z_1 = \frac{\chi(g)}{\chi(1)}$. P se factorise dans $\mathbf{C}$: $P(X) = (X - z_1)\ldots(X - z_d)$ et donc $|a_0| = |z_1 \ldots z_d| < 1$. Mais a_0 est un entier relatif, ce qui implique $a_0 = 0$. Il s'en suit que X divise P et, comme P est irréductible, $X = P$, ce qui est absurde car $\chi(g)$ n'est pas nul.*

3. *Soit C la classe de conjugaison de g. On définit $\pi = \sum_{h\in C} \rho(h)$, qui est un endomorphisme de V. C'est aussi un morphisme de représentation de (V,ρ) dans lui-même. En effet, pour tout $s \in G$, on a :*

$$\rho(s) \circ \pi \circ \rho(s^{-1}) = \sum_{h\in C} \rho(shs^{-1}) = \pi$$

Comme ρ est irréductible, d'après le lemme de Schur, π est une homothétie. On note λ son rapport. On a alors, en prenant la trace,

$$Tr(\pi) = \chi(1)\lambda = \sum_{h\in C} \chi(h) = Card(C)\chi(g) = \frac{|G|\chi(g)}{|Stab_G(g)|}$$

Donc

$$\lambda = \frac{|G|\chi(g)}{|Stab_G(g)|\chi(1)}$$

Il s'agit alors de montrer que λ possède un polynôme annulateur à coefficients dans $\mathbf{Z}$. Pour cela, on écrit $G = \{h_1, \ldots, h_n\}$.

Remarque : *On peut indexer par les éléments de G directement comme c'est fait dans NH2G2 exercice E.37.*

Pour tout i compris entre 1 et n, il existe donc des éléments $a_{i,j}$ dans $\{0,1\}$ tels que

$$\rho(h_i) \circ \pi = \sum_{j=1}^{n} a_{i,j}\rho(h_j)$$

En effet, en développant $\rho(h_i)\circ\pi$, on obtient une somme de $\rho(h)$ pour certains éléments h de G. Ce que dit le point précédent c'est qu'on les fait tous apparaître dans cette somme, quitte à mettre un 0 devant. Mais $\rho(h_i)\circ\pi = \lambda\rho(h_i)$, donc les égalités précédentes se réécrivent :

$$\forall i \in \{1,\ldots,n\}, \sum_{j=1}^{n}(a_{i,j}\rho(h_j) - \lambda\delta_{i,j}\rho(h_j)) = \sum_{j=1}^{n}(a_{i,j} - \lambda\delta_{i,j})\rho(h_j) = 0$$

Si on note $A = (a_{i,j})_{1\leq i,j\leq n}$, la matrice A est à coefficients dans $\mathbf{Z}$ et les égalités précédentes se résument en

$$(A - \lambda I_n)R = 0$$

où R est le vecteur colonne des $\rho(h_i)$. En multipliant à gauche par la transposée de la comatrice de $A - \lambda I_n$, on trouve $Det(A - \lambda I_n) = 0$. Ainsi, λ est une racine du polynôme caractéristique de A, qui est un polynôme à coefficients dans $\mathbf{Z}$ car A est elle-même à coefficients dans $\mathbf{Z}$. D'où λ est un entier algébrique.

Remarque : Avec ce résultat, il ne faut plus grand chose pour montrer que le degré d'une représentation irréductible d'un groupe G divise l'ordre de ce groupe. On démontrera ceci à la fin du document. Voir encore l'exercice $E.37$ de NH2G2.

Lemme

Supposons que dans le groupe G il existe un élément g dont la classe de conjugaison C est de cardinal p^a, où p est premier et $a \in \mathbf{N}$ non nul. Notons $\chi_1, \ldots, \chi_r$ les caractères irréductibles de G, où χ_1 est le caractère associé à la représentation irréductible triviale. Alors :

1. *Il existe un caractère irréductible χ de G tel que p ne divise pas $\chi(1)$ et $\chi(g) \neq 0$.*
2. *Pour ce caractère χ, on a $\left|\frac{\chi(g)}{\chi(1)}\right| = 1$.*
3. *G n'est pas simple*

Démonstration

1. *Raisonnons par l'absurde et supposons que, pour tout caractère irréductible χ de G, on a p divise $\chi(1)$ dès que $\chi(g) = 0$. On sait que les caractères irréductibles de G forment une base orthonormée de l'espace vectoriel des fonctions centrales sur G. En décomposant la fonction indicatrice de C dans cette base, on obtient la formule suivante :*

$$\forall s \in G, \sum_{i=1}^{s} \chi_i(g)\overline{\chi_i(s)} = \begin{cases} 0 & \text{si } s \text{ et } g \text{ ne sont pas conjugués} \\ \frac{|G|}{|C|} & \text{si } s \text{ et } g \text{ sont conjugués} \end{cases}$$

Comme la classe de conjugaison de g n'est pas réduite à un élément, g est différent de 1 et, en particulier, 1 et g ne sont pas conjugués. Appliquant la formule ci-dessus, on obtient :

$$\begin{aligned} &\sum_{i=1}^{s} \chi_i(g)\overline{\chi_i(1)} = 0 \\ \iff &1 + \sum_{i=2}^{s} \chi_i(g)\overline{\chi_i(1)} = 0 \\ \iff &\sum_{i=2}^{s} \chi_i(g)\frac{\chi_i(1)}{p} = \frac{-1}{p} \end{aligned}$$

Par hypothèse, on a que p divise $\chi_i(1)$ dès que $\chi_i(g) \neq 0$. Donc, pour chacun de ces entiers i, $\frac{\chi_i(1)}{p}$ est un entier. Or, $\chi_i(g)$ étant une somme de racines de l'unité, c'est un entier algébrique car l'ensemble des entiers algébriques est un anneau et que les racines de l'unité sont des entiers algébriques. Par suite, $\frac{-1}{p}$ est un entier algébrique, et c'est un rationnel, et on sait qu'un nombre qui est à la fois rationnel et entier algébrique est un entier. Ce qui est absurde car $p \neq 1$.

2. *Raisonnons par l'absurde. On a alors, d'après le premier point du lemme 1, pour ce caractère χ, $0 < |\frac{\chi(g)}{\chi(1)}| < 1$. Comme p ne divise pas $\chi(1)$, p^a et $\chi(1)$ sont premiers entre eux et on a une relation de Bezout :*

$$up^a + v\chi(1) = 1$$

avec $u, v \in \mathbf{Z}$. Comme $p^a = Card(C) = \frac{|G|}{|Stab_G(g)|}$, en multipliant par $\frac{\chi(g)}{\chi(1)}$, on obtient

$$u\frac{|G|\chi(g)}{|stag_G(g)|\chi(1)} + v\chi(g) = \frac{\chi(g)}{\chi(1)}$$

D'après le premier lemme, et comme l'ensemble des entiers algébrique est un anneau, on en déduit que $\frac{\chi(g)}{\chi(1)}$ est un entier algébrique, ce qui est absurde de nouveau par le premier lemme.

3. *On prends χ le caractère précédent. On montre que le noyau du morphisme ρ associé est alors un sous-groupe strict de G. Tout d'abord, en analysant la preuve du premier point du deuxième lemme, on voit que ρ n'est pas la représentation triviale, donc $Ker(\rho) \neq G$. Supposons par l'absurde (décidément !) que $Ker(\rho) = \{1\}$. ρ est alors injectif, i.e. la représentation est fidèle. On a, d'après ce qui précède, $\left|\frac{\chi(g)}{\chi(1)}\right| = 1 \iff |\chi(g)| = \chi(1)$. On en déduit que $\rho(g)$ est une homothétie (classique, voir NH2G2 exercice E.25 question 1). Par conséquent, $\rho(g)$ commute avec tous les $\rho(s)$ pour $s \in G$. On a donc :*

$$\forall s \in G, \rho(g) \circ \rho(s) = \rho(s) \circ \rho(g) \iff \forall s \in G, \rho(gs) = \rho(sg)$$

Et, comme la représentation est fidèle, on a $\forall s \in G$, $gs = sg$ i.e. g est un élément central. Mais, si c'était le cas, la classe de conjugaison de g serait réduite à un élément, ce qui est absurde.

On a donc établi le résultat suivant :
Si G est un groupe fini qui possède une classe de conjugaison de cardinal une puissance d'un nombre premier, G n'est pas simple.
On démontre alors le théorème de Burnside avec ce résultat.

Théorème (p^aq^b de Burnside)
Soient p, q deux nombres premiers et $a, b \in \mathbf{N}$ deux entiers naturels. Alors, tout groupe d'ordre p^aq^b n'est pas simple.

Démonstration
Tout d'abord, si a ou b est nul, alors il est connu que G n'est pas simple (pourquoi ?). Supposons alors a et b non nuls. Soit H un q-Sylow. H étant un q-groupe, il possède un élément central g. Ainsi, dans l'action par conjugaison de G sur lui-même, H est inclu dans le stabilisateur de g. Il existe

donc un entier α tel que $|Conj(g)| = \frac{|G|}{|stab_G(g)} = \frac{p^a q^b}{p^\alpha q^b} = p^{a-\alpha}$. Si $a \neq \alpha$, alors la classe de conjugaison de g est de cardinal une puissance non nulle d'un nombre premier et G n'est pas simple d'après ce qui précède. Si $a = \alpha$, alors g est un élément central et donc le centre de G n'est pas réduit au neutre. Si G est égal à son centre, il est abélien donc non simple. Sinon, le centre de G est un sous-groupe distingué strict et G n'est pas simple.

Corollaire
Il n'existe aucun groupe simple non trivial (i.e. d'ordre premier) d'ordre strictement inférieur à 60.

Démonstration
En effet, un l'ordre d'un groupe doit donc avoir au moins trois diviseurs premiers pour que ce groupe ait une chance d'être simple. Le plus petit est donc éventuellement d'ordre 30. *Les théorèmes de Sylow permettent de montrer qu'un tel groupe n'est pas simple. Ensuite, on tombe sur 42. De même, les théorèmes de Sylow permettent de conclure rapidement. Arrive alors 60. Pour 60, on sait que A_5 est simple, et que c'est même le seul à isomorphisme près.*

On peut continuer comme ça et traiter les cas douteux uns à uns, mais parfois c'est difficile.
On peut aussi montrer qu'un groupe d'ordre $p^a q^b$ est résoluble. C'est fait dans les commentaires du livre 131 développements pour l'oral.

Quelques résultats supplémentaires utilisés dans la démonstration

Comme promis, on démontre certaines de ces propriétés. Je mettrai une référence à chaque fois si j'en connais une.

Proposition
Référence : *Je n'ai pas de livre comme référence, mais le sujet Maths A X-ENS 2019 traîte ces questions là. On prouve également dans ce sujet l'irréductibilité des polynômes cyclotomiques avec la méthode de Schur. Une autre méthode connue est celle qu'on trouve dans le Perrin. On peut aussi montrer l'irréductibilité des polynômes cyclotomiques d'ordre premier avec le critère d'Eisenstein.*

1. *Soit $r \in \mathbf{Q}$ un rationnel. Si r est un entier algébrique, alors $r \in \mathbf{Z}$.*
2. *Soit $z \in \mathbf{C}$. On dit que z est algébrique sur $\mathbf{Q}$ si z est racine d'un polynôme à coefficients dans $\mathbf{Q}$. On dit que z est un entier algébrique si z est racine d'un polynôme unitaire à coefficients dans $\mathbf{Z}$. Soit z un nombre complexe algébrique sur $\mathbf{Q}$.*

Alors, z est un entier algébrique $\iff$ son polynôme minimal $\Pi_{z,\mathbf{Q}}$ est à coefficients dans $\mathbf{Z}$.

Démonstration

1. *On note $r = \frac{p}{q}$ avec $p \in \mathbf{N}^*$ et $q \in \mathbf{Z}$, p et q premiers entre eux. Soit $P(X) = X^d + a_{d-1}X^{d-1} + \ldots + a_0$ dans $\mathbf{Z}[X]$ qui annule r. On a alors :*

$$\begin{aligned} P(r) = 0 &\iff \frac{p^d}{q^d} + a_{d-1}\frac{p^{d-1}}{q^{d-1}} + \ldots + a_0 = 0 \\ &\iff p^d + a_{d-1}qp^{d-1} + \ldots + a_0q^d = 0 \\ &\iff p^d = q(a_{d-1}p^{d-1} + \ldots + a_0q^{d-1}) \end{aligned}$$

   Ainsi, q divise p^d mais des applications successives du lemme de Gauss, p et q étant premiers entre eux, montrent que q divise p. Ceci impose que $q = 1$ ou $p = 0$. Dans les deux cas, on trouve $r \in \mathbf{Z}$.

2. *Le sens " $\Longleftarrow$ " est évident.*
   Montrons " $\Longrightarrow$ ". Notons $z = z_1, \ldots, z_d$ les racines de $\Pi_{z,\mathbf{Q}}$ dans $\mathbf{C}$. Alors les z_i sont des entiers algébriques, car annulés par le même polynôme à coefficients dans $\mathbf{Z}$ que z. Les relations coefficients/racines montrent que les coefficients de $\Pi_{z,\mathbf{Q}}$ s'expriment comme sommes de produits des z_i. Comme l'ensemble des entiers algébriques est un anneau, on en déduit que les coefficients de $\Pi_{z,\mathbf{Q}}$ sont à la fois des rationnels et des entiers algébriques, donc sont dans $\mathbf{Z}$ d'après le point précédent.

Remarque : Pour une démonstration du fait que l'ensemble des entiers algébriques est un anneau, voir le chapitre sur le résultant du livre de Rombaldi : *Mathématiques pour l'agrégation, Algèbre et géométrie*. Un développement possible pour la leçon sur le déterminant consiste à montrer ce résultat avec le résultant, puis de démontrer le résultat suivant :

Proposition
Référence : *NH2H2 tome 2 Exercice E.27.*
Soit G est un groupe fini et χ un caractère irréductible de G. Soit $g \in G$. Alors :

1. *Le nombre complexe $\frac{|G|\chi(g)}{|Stab_G(g)|\chi(1)}$ est un entier algébrique.*
2. *Le degré de χ divise l'ordre de G.*

Le premier point n'est autre que le troisième point du premier lemme de ce document. Ainsi, on peut récupérer ce point pour en faire un nouveau développement, quasi-gratuitement !

Démonstration

1. *Déjà fait.*

2. *Notons $C_1, \dots, C_s$ les différentes classes de conjugaisons de G, et $g_1, \dots, g_s$ des représentants de ces classes. D'après le premier point, on a que tous les $\frac{|G|\chi(g_i)}{|Stab_G(g_i)|\chi(1)}$ sont des entiers algébriques. Comme χ est un caractère irréductible, on a :*

$$1 = (\chi, \chi) = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\chi(g)} = \frac{1}{|G|} \sum_{i=1}^{s} |C_i| \chi(g_i)\overline{\chi(g_i)}$$

Donc

$$|G| = \sum_{i=1}^{s} \frac{|G|\chi(g_i)}{|stab_G(g_i)|} \overline{\chi(g_i)}$$

En divisant par $\chi(1)$ (qui, au passage, est égal au degré de χ), on obtient :

$$\frac{|G|}{\chi(1)} = \sum_{i=1}^{s} \frac{|G|\chi(g_i)}{|stab_G(g_i)|\chi(1)} \overline{\chi(g_i)}$$

On en déduit, en utilisant encore que l'ensemble des entiers algébriques est un anneau et le premier point, que $\frac{|G|}{\chi(1)}$ est un entier algébrique. Comme c'est aussi un rationnel, on en déduit que c'est un entier et donc que le degré de χ divise l'ordre de G.

Passons au résultat sur les conjugués. Petit commentaire personnel sur ce point là : j'ai mis le recasage dans les leçons 125 et 144 à cause de cet argument. Cependant, pour parler de groupe de Galois, il faut être à l'aise avec la théorie de Galois au cas où le jury ait envie de creuser un peu. C'est un investissement de travail non négligeable, surtout que c'est hors-programme. Personnellement, je n'aurais pas présenté ce développement dans la 125 ni dans la 144 mais si vous le sentez bien alors pourquoi pas. Si on présente ce développement dans les autres leçons, on peut passer sur ce point à l'oral en étant capable de démontrer le résultat que je vais énoncer juste après. Il vaut mieux aussi connaître un peu la correspondance de Galois, mais à mon avis pas les démonstrations en détail... il y a déjà assez de boulot comme ça. Enfin, si vous comptez présenter le théorème de Gauss-Wantzel en développement dans d'autres leçons, il n'est pas inutile de connaître la correspondance de Galois car on peut assez facilement construire la tour d'extensions quadratiques grâce à la correspondance de Galois. Encore une fois, je pense qu'il vaut mieux le faire sans, mais savoir que c'est faisable avec si jamais le jury demande.

Proposition
Soit $\mathbf{K}$ un corps commutatif et $P \in \mathbf{K}[X]$ un polynôme irréductible. Alors, $Gal(P/\mathbf{K})$ agit transitivement sur l'ensemble des racines de P dans son corps de décomposition.

On utilise pour cela les proposition 3.29 et lemme 5.20 du Gozard.

Proposition
Soit K un corps. Soit $P \in K[X]$ un polynôme irréductible. Soient α et β deux racines de P dans un corps de décomposition $D_K(P)$ de P sur K. Alors :

1. *Il existe un K-isomorphisme $\sigma : K(\alpha) \longrightarrow K(\beta)$ qui envoie α sur β.*
2. *Il existe un isomorphisme $\tilde{\sigma} : D_K(P) \longrightarrow D_K(P)$ qui prolonge σ.*

On en déduit biensûr le résultat voulu.

Démonstration

1. *Faîtes un diagramme. P étant irréductible, on a que $\frac{K[X]}{(P)}$ est un corps. α et β étant deux racines de P (supposons distinctes, sinon c'est évident), on a deux isomorphismes de corps :*

$$\frac{K[X]}{(P)} \longrightarrow K(\alpha) \text{ et } \frac{K[X]}{(P)} \longrightarrow K(\beta)$$

   qui consistent à évaluer en α et β. On en déduit un isomorphisme de $K(\alpha)$ dans $K(\beta)$ qui envoie α et β : On pose $\sigma = ev_\beta \circ (ev_\alpha)^{-1}$.
2. *On a $\sigma(P) = P$ car σ fixe $\mathbf{K}$. On voit facilement que $D_{\mathbf{K}}(P)$ est encore un corps de décomposition de P sur $\mathbf{K}(\alpha)$ et $\mathbf{K}(\beta)$. Le lemme 5.20 du Gozard permet de conclure.*