Feuille TD 4 – Algèbre – Corps et théorie de Galois

► *Cette feuille de TD nous occupera trois semaines.*

Exercices fondamentaux de la semaine 1

Exercice 1 — Corps parfaits. Soit K un corps. Soit $\sigma : K \to K$ un automorphisme de K. Soit L un K-espace vectoriel.

1. Montrer que $(L, +)$, muni de la loi externe $(\alpha, x) \mapsto \sigma(\alpha) \cdot x$ est aussi un K-espace vectoriel, que l'on notera L'.
2. Montrer que si L est de dimension finie d, alors L' est aussi de dimension d.
3. En déduire que si K est un corps parfait de caractéristique $p > 0$, toute extension finie de K est un corps parfait.
4. Le résultat de **3.** reste-t-il vrai pour une extension algébrique (pas forcément finie) ?

Solution.

1. Posons $\alpha \bullet x = \sigma(\alpha) \cdot x$. Comme σ est un morphisme de corps, on vérifie alors immédiatement les quatre axiomes requis :
   $1 \bullet x = x$ pour tout $x \in L$.
   $\alpha \bullet (\beta \bullet x) = (\alpha\beta) \bullet x$ pour tous $\alpha, \beta \in K$ et tout $x \in L$.
   $\alpha \bullet (x + y) = \alpha \bullet x + \alpha \bullet y$ pour tout $\alpha \in K$ et tous $x, y \in L$.
   $(\alpha + \beta) \bullet x = \alpha \bullet x + \beta \bullet x$ pour tous $\alpha, \beta \in K$ et tout $x \in L$.
2. Soit $(e_1, \dots, e_d)$ une base du K-espace vectoriel L, montrons que c'est aussi une base de L'. Si $\lambda_1, \dots, \lambda_d$ dans K vérifient
   $$\sum_{i=1}^{d} \lambda_i \bullet e_i = 0,$$
   alors
   $$\sum_{i=1}^{d} \sigma(\lambda_i) \cdot e_i = 0$$
   d'où $\sigma(\lambda_i) = 0$, puis $\lambda_i = 0$ pour tout $i \in \{1, \dots, d\}$ puisque σ est injectif. Ainsi $(e_1, \dots, e_d)$ est libre dans L'. Si maintenant $x \in L'$, on écrit $x = \sum_{i=1}^{d} \mu_i \cdot e_i$ dans L avec $\mu_i \in K$ pour tout $i \in \{1, \dots, d\}$, d'où $x = \sum_{i=1}^{d} \sigma^{-1}(\mu_i) \bullet e_i$ dans L', ce qui montre que la famille $(e_1, \dots, e_d)$ est également génératrice dans L'.
3. Par hypothèse, le morphisme de corps σ défini par $\sigma(x) = x^p$ est un automorphisme de K. Soit L une extension finie de K, qu'on peut voir comme un K-espace vectoriel, notons L' le K-espace vectoriel défini comme en **1.** Alors l'application $u : x \mapsto x^p$ est un morphisme du K-ev L dans le K-ev L' : en effet $u(x + y) = u(x) + u(y)$ résulte de ce qu'on est en caractéristique p et si $\alpha \in K$ et $x \in L$, on a
   $$u(\alpha \cdot x) = \alpha^p x^p = \sigma(\alpha) \cdot u(x) = \alpha \bullet x.$$
   Comme il est immédiat que $\ker(u) = 0$, u est injective et elle est donc bijective car $\dim L = \dim L'$ est finie. Ceci signifie exactement que $x \mapsto x^p$ est bijective de L dans L, et donc que L est parfait.
4. Mais oui ! Si F est une extension algébrique de K et si $x \in F$, alors $L := K[x]$ est une extension finie de K puisque x est algébrique sur K. Appliquant alors **3.** à L, on obtient qu'il existe $y \in L \subset F$ tel que $y^p = x$. Ainsi, F est parfait.

   Une autre méthode ou une conséquence (vue en cours) consiste à observer qu'un corps K est parfait si et seulement si toute extension finie de K est séparable, propriété qui se conserve quand on fait une extension finie (ou algébrique) de K.

Exercice 2 — Corps algébriquement clos. Soit L/K une extension de corps. Soit M le sous-corps de L constitué des éléments algébriques sur K. On suppose que tout polynôme irréductible de $K[X]$ est scindé sur L.

1. Montrer que tout polynôme de $K[X]$ est scindé sur M.
2. Soit F une extension finie de M. Montrer que tout $x \in F$ est algébrique sur K.
3. En déduire que M est un corps algébriquement clos.

Solution.

1. Il suffit de montrer que si $P \in K[X]$ est irréductible, alors il est scindé sur M. Or par hypothèse P est scindé sur L, et par ailleurs toute racine α de P dans L est par définition algébrique sur K, donc $\alpha \in M$; d'où le résultat.
2. Si $x \in F$, alors x est algébrique sur M, donc il annule un polynôme unitaire de $M[X]$. Si $a_0, \dots, a_r$ sont les coefficients de ce polynôme, alors x est algébrique sur $K(a_0, \dots, a_r)$, qui est de dimension finie sur K puisque tous les a_i (qui sont dans M) sont algébriques sur K. En particulier $K(a_0, \dots, a_r)[x]$ est de dimension finie sur $K(a_0, \dots, a_r)$ et aussi sur K (par multiplicativité des degrés), ce qui implique que $K[x]$ est de dimension finie sur K. Finalement, x est algébrique sur K.

3. Avec les notations de **2.**, x annule un polynôme irréductible π de $K[X]$ (son polynôme minimal sur K), et π est scindé sur M d'après **1.** Finalement $x \in M$, ce qui montre que la seule extension finie de M est M, et donc que M est algébriquement clos (sinon il y aurait un polynôme irréductible Q de degré au moins 2 dans $M[X]$, et $M[X]/(Q)$ serait une extension finie de M de degré $\geqslant 2$).

Exercice 3 — Théorème de Steinitz. Soit K un corps. On note $\mathcal{I}$ l'ensemble des polynômes irréductibles unitaires de $K[X]$. On forme l'anneau de polynômes $A := K[(T_{P,i})_{P\in\mathcal{I},1\leqslant i\leqslant \deg P}]$ et pour tout $P \in \mathcal{I}$, on écrit dans $A[X]$:

$$P - \prod_{i=1}^{\deg P}(X - T_{P,i}) = \sum_{j=0}^{\deg P-1} a_{P,j}X^j,$$

où les $a_{P,j}$ sont dans A. On suppose par l'absurde que l'idéal I de A engendré par les $a_{P,j}$ est A et on va montrer qu'on aboutit à une contradiction.

1. Montrer qu'il existe une partie finie $\mathcal{I}_1$ de $\mathcal{I}$ tels que l'idéal engendré par les $a_{P,j}$ avec $P \in \mathcal{I}_1$ soit égal à A.

2. Soit $Q = \prod_{P\in\mathcal{I}_1} P \in K[X]$ et soit L un corps de décomposition de Q sur K. Pour $P \in \mathcal{I}_1$, on pose

$$P = \prod_{i=1}^{\deg P}(X - \alpha_{P,i}), \quad \alpha_{P,i} \in L.$$

Soit $A_1 \subset A$ l'anneau $K[(T_{P,i})_{P\in\mathcal{I}_1,1\leqslant i\leqslant \deg P}]$. Montrer qu'il existe un morphisme de K-algèbres φ de A_1 dans L qui envoie chaque $T_{P,i}$ sur $\alpha_{P,i}$ pour tout $P \in \mathcal{I}_1$ et tout i avec $1 \leqslant i \leqslant \deg P$.

3. Montrer que le morphisme $\tilde{\varphi} : A_1[X] \to L[X]$ induit par φ envoie $P - \prod_{i=1}^{\deg P}(X - T_{P,i})$ sur 0 (pour tout $P \in \mathcal{I}_1$), et aboutir à une contradiction.

Soit maintenant J un idéal maximal de A contenant I (qui existe d'après ce qui précède), on note Ω le corps A/J, qui est une extension de K.

4. Montrer que tout polynôme irréductible de $K[X]$ est scindé sur Ω.

5. En utilisant l'exercice 2, montrer que K admet une clôture algébrique (*théorème de Steinitz*).

6. Montrer que si F et F' sont deux clôtures algébriques de K, elles sont isomorphes (on appliquera le lemme de Zorn aux K-morphismes de E dans F', où E est une extension intermédiaire entre K et F).

Solution.

1. Comme l'idéal engendré par tous les $a_{P,j}$ est A, on peut écrire 1 comme combinaison linéaire à coefficients dans A d'un nombre fini de ces $a_{P,j}$, correspondant à des P dans une partie finie $\mathcal{I}_1$ de $\mathcal{I}$. L'idéal engendré par les $a_{P,j}$ pour $P \in \mathcal{I}_1$ (et toujours $0 \leqslant j < \deg P$) contient alors 1, donc est égal à A.

2. En dépit des notations effrayantes, il s'agit tout simplement de la propriété universelle d'un anneau de polynômes !

3. Comme $P \in K[X]$, on a $\tilde{\varphi}(P) = P$. Par ailleurs

$$\tilde{\varphi}(\prod_{i=1}^{\deg P}(X - T_{P,i})) = \prod_{i=1}^{\deg P}(X - \alpha_{P,i}) = P.$$

Ainsi, $\tilde{\varphi}$ envoie $P - \prod_{i=1}^{\deg P}(X - T_{P,i})$ sur 0. Par définition des $a_{P,j}$, cela donne $\varphi(a_{P,j}) = 0$ pour tout $P \in \mathcal{I}_1$ (et tout $j \in \{0, \dots, \deg P - 1\}$). Comme ces $a_{P,j}$ engendrent l'idéal A de A, on obtient $\varphi(A) = 0$, ce qui n'est pas possible puisque $\varphi(1) = 1$.

4. Si P est un polynôme irréductible de K (qu'on peut supposer unitaire), alors comme dans A/J l'image de tous les $a_{P,j}$ est nulle (puisque J contient I), on obtient

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

où u_i est l'image de $T_{P,i}$ dans $\Omega = A/J$. Ceci montre que P est scindé sur Ω.

5. On vient de trouver une extension Ω de K telle que tout polynôme irréductible de $K[X]$ soit scindé sur Ω. D'après l'exercice 2, l'ensemble $\overline{K}$ des éléments de Ω algébriques sur K est un corps algébriquement clos, et comme c'est une extension algébrique de K, c'est une clôture algébrique de K.

6. On considère l'ensemble S des paires (E, i), où $K \subseteq E \subseteq F$ et $i : E \to F'$ est un morphisme de corps fixant K. On ordonne S par $(E_1, i_1) \leq (E_2, i_2)$ si $E_1 \subset E_2$ et i_2 prolonge i_1. Il est alors immédiat que toute famille non vide totalement ordonnée de S admet un majorant (si (E_j, i_j) est une telle famille, on prend pour majorant (E, i) où E est la réunion des E_j et i le morphisme qui coïncide avec i_j sur chaque E_j). D'après le lemme de Zorn, S possède donc un élément maximal (E_0, i_0). Montrons que $E_0 = F$. Si on avait un $x \in F \setminus E_0$, alors le polynôme minimal de x (qui est algébrique sur K) aurait une racine x' dans F' (qui est algébriquement clos et contient K), ce qui permettrait de prolonger i_0 en un K-morphisme de corps de $E_0[x]$ dans F' en envoyant x sur x', ce qui contredit la maximalité [1]. On obtient donc finalement un morphisme de corps $i_0 : F \to F'$. Mais alors, comme tout élément de F' est algébrique sur K, donc sur F, le fait que F soit algébriquement clos implique que i_0 est un isomorphisme.

Exercice 4 — Caractérisation des extensions simples d'Artin. Soit K un corps infini. Soit L un surcorps de K, on suppose qu'il n'existe qu'un nombre finis de corps M avec $K \subseteq M \subseteq L$. On veut montrer qu'il existe $a \in L$ tel que $L = K(a)$.

1. Montrer que l'extension L/K est finie.

2. On suppose que $L = K(\alpha_1, \alpha_2)$ avec $\alpha_1, \alpha_2 \in L$. En considérant les corps $K(\alpha_1 + \beta\alpha_2)$ avec $\beta \in K$, montrer que l'un de ces corps est égal à L.

3. En déduire le résultat annoncé.

4. Soit réciproquement $L = K(\alpha)$ une extension de K engendrée par un élément algébrique α. Soit M une extension intermédiaire entre K et L. On note P le polynôme minimal de α sur K et P_M son polynôme minimal sur M. Montrer que P_M divise P dans $L[T]$ et que l'application $M \mapsto P_M$ est injective.

5. En déduire qu'il n'y a qu'un nombre fini de telles extensions intermédiaires M.

6. Montrer que $\mathbf{F}_p(X, Y)$ admet une extension finie qui n'est pas engendrée par un élément (autrement dit le théorème de l'élément primitif tombe en défaut sur ce corps imparfait).

Solution.

1. Commençons par établir que L est algébrique. S'il existe un élément transcendant $x \in L$ alors les $K(x^{2^n})$ pour $n \in \mathbf{N}$ forment une suite infinie décroissante de sous-corps distincts deux à deux ce qui est absurde [2]. Ainsi tous les éléments de L sont algébriques sur K et on a $K(a_1, \ldots, a_r)$ (par exemple prendre pour les a_i les vecteurs d'une K-base) de dimension finie sur K pour tous $a_1, \ldots, a_r$ de L. Si L est de dimension infinie sur K, cela permet de construire une suite infinie strictement croissante

$$K(a_1) \subseteq K(a_1, a_2) \subseteq \cdots \subseteq K(a_1, a_2, \ldots, a_n) \subseteq \cdots$$

de corps intermédiaires entre K et L, ce qui contredit l'hypothèse.

2. Comme K est infini et le nombre d'extensions intermédiaires est fini, il existe $\beta \neq \beta'$ dans K tels que $K(\alpha_1 + \beta\alpha_2) = K(\alpha_1 + \beta'\alpha_2)$. Posons $M = K(\alpha_1 + \beta\alpha_2)$, alors

$$(\alpha_1 + \beta'\alpha_2) - (\alpha_1 + \beta\alpha_2) \in M$$

d'où $\alpha_2 \in M$ (vu que $(\beta - \beta') \in K^*$) et

$$\alpha_1 = \alpha_1 + \beta\alpha_2 - \beta\alpha_2 \in M$$

. On en déduit que $M = L$.

3. Comme L est de dimension finie sur K, on peut trouver $\alpha_1, \ldots, \alpha_n$ dans L tels que $L = K(\alpha_1, \ldots, \alpha_n)$. La question **2.** donne alors par récurrence sur n que L s'écrit $K(\alpha)$ avec $\alpha \in L$.

4. Comme $P \in M[X]$ et $P(\alpha) = 0$, on obtient par définition du polynôme minimal que P_M divise P dans $M[T]$, donc aussi dans $L[T]$. Soient maintenant M et N des extensions intermédiaires telles que $P_M = P_N$. Supposons d'abord que $N \subset M$, alors comme $L = M[\alpha]$ et P_M est le polynôme minimal de α sur M, on a $\deg P_M = [L : M]$ et de même pour N, ce qui implique $[L : M] = [L : N]$, puis $[M : K] = [L : K]$ par multiplicativité des degrés. D'où $M = N$ dans ce cas puisque $N \subset M$ et ces deux K-espaces vectoriels ont même dimension. On se ramène au cas où $N \subset M$ en considérant $N' = N \cap M$, qui vérifie encore l'hypothèse que $P_{N'} = P_M$, puisque $P_M \in N'[X]$ annule α et est le minimal de α sur M, donc a fortiori sur N'.
Méthode alternative : soit $K \subseteq E \subseteq L = K[\alpha]$ et F le corps engendré sur K par les coefficients de P_E. Par définition, $P_E \in F[X]$ et $P_E(\alpha) = 0$ si bien que $P_F \mid P_E$. D'où,

$$1 \leqslant [E : F] = \frac{[L : F]}{[L : E]} \leqslant 1$$

ce qui montre que E est entièrement déterminée par P_E et par conséquent l'injectivité ! Noter qu'on a en réalité, $[L : F] = \deg(P_F)$ car $L = K(\alpha) = F(\alpha)$ et $[L : E] = \deg(P_E)$ car $L = K(\alpha) = E(\alpha)$ mais que par choix de F, il vient que $[L : E] = [L : F]$ car on a également que $F \subseteq E$ et donc P_F annule α à coefficients dans F (donc dans E) de sorte que $P_E \mid P_F$.

1. Pour cela, il suffit de voir que x est algébrique sur K et donc sur E_0 et considérer μ_{E_0} son polynôme minimal sur E_0. On a alors $E_0[x] = E_0[X]/(\mu_{E_0})$ et on peut définir une application $f : E_0[X] \to F$ définie par f_0 sur E_0 et envoyant X sur x' où l'on a pu trouvé une racine x' du polynôme $f_0(\mu_{E_0})$ dans F car ce dernier est algébriquement clos. Alors, par définition, on aura que le noyau de f contient (μ_{E_0}) et le prolongement cherché est obtenu au quotient.

2. Noter que puisque x est transcendant, un élément de $K(x^{2^n})$ s'écrit comme une **fraction rationnelle** en x^{2^n}.

5. C'est une conséquence de **4.**, vu que P n'a qu'un nombre fini de diviseurs unitaires dans $L[T]$ (décomposer P en produit de facteurs irréductibles unitaires).

6. Posons $K = \mathbf{F}_p(X, Y)$ et prenons pour L le corps de décomposition du polynôme $(T^p - X)(T^p - Y)$ sur K. Ainsi $L = K(a, b)$ avec $a^p = X$ et $b^p = Y$. On constate alors que pour tout $m \in \mathbf{N}$, l'extension $M_m := K(a + X^m b)$ est intermédiaire entre K et L. Or, pour $m < n$, les extensions M_m et M_n sont distinctes, sinon M_m contiendrait $(X^n - X^m)b$, donc aussi b puisque $(X^n - X^m) \in K^\times$. Alors M_m contiendrait aussi $a = a + X^m b - X^m b$, et on aurait finalement $M_m = L$. Mais ceci n'est pas possible car $a + X^m b$ annule le polynôme $Q = T^p - (X + YX^{mp})$ qui est de degré p, donc $M_m = K(a + X^m b)$ est de degré au plus[3] p sur K, tandis que L est de degré[4] p^2 sur K. Finalement, il y a une infinité d'extensions intermédiaires entre K et L, et on conclut avec **5.**

On pouvait aussi raisonner directement par l'absurde en supposant que $L = K(\theta)$ auquel cas

$$\theta = \frac{P(a,b)}{Q(a,b)} \quad \text{et} \quad \theta^p = \frac{P(X,Y)}{Q(X,Y)} \in K$$

ce qui implique que le degré de θ est inférieur à p, ce qui est absurde.

Exercice complémentaire de la semaine 1

Exercice 5 — Un exemple classique. Montrer que le polynôme $X^4 + 1$ est irréductible sur $\mathbf{Q}$. Soit L un corps de rupture pour ce polynôme. Comment $X^4 + 1$ se factorise-t-il sur L ?

Solution. Plusieurs méthodes ici : soit on remarque que $X^4 + 1 = \Phi_8$, soit on procède par identification, soit on remarque que

$$(Y + 1)^4 + 1 = Y^4 + 4Y^3 + 6Y^2 + 4Y + 2$$

et on applique Eisenstein avec[5] $p = 2$.
Les racines sont clairement $\xi_1 = e^{\frac{i\pi}{4}}, \xi_2 = e^{\frac{3i\pi}{4}} = i\xi_1, \xi_3 = e^{\frac{5i\pi}{4}} = -\xi_1$ et $\xi_4 = e^{\frac{7i\pi}{4}} = -i\xi_1$. On a alors clairement que tout corps de rupture est donné par $\mathbf{Q}(i, \sqrt{2})$ sur lequel $X^4 + 1$ est scindé.
Une autre façon de voir les choses : Un corps de rupture de P est $\mathbf{Q}(\omega)$ où $\omega = e^{i\frac{\pi}{4}}$; comme les autres racines de P sont ω^3, ω^5 et ω^7 qui appartiennent évidement à $\mathbf{Q}(\omega)$, P se décompose sur le corps de rupture $\mathbf{Q}(\omega)$ qui est alors aussi son corps de décomposition. On a $P = (X - \omega)(X - \omega^3)(X - \omega^5)(X - \omega^7)$ dans $\mathbf{Q}(\omega)$.
Voir le Perrin page 78 Proposition 3.11 ou le polycopié de cours pour le fait que ce polynôme, bien qu'irréductible sur $\mathbf{Q}$ est réductible modulo p pour tout p premier.

Exercice 6 — Quelques exemples explicites.

1. Montrer que pour tous nombres rationnels a et b, $\mathbf{Q}(\sqrt{a}, \sqrt{b}) = \mathbf{Q}(\sqrt{a} + \sqrt{b})$. Est-ce que $\sqrt{15} \in \mathbf{Q}(\sqrt{10}, \sqrt{42})$?

2. A-t-on que $\mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) = \mathbf{Q}(\sqrt{2} + \sqrt{3} + \sqrt{5})$?

3. Calculer le degré de $\sqrt{2} + \sqrt[3]{3}$.

4. Montrer que pour $a_1, \ldots, a_\ell \in \mathbf{N}$ et $d_1, \ldots, d_\ell \in \mathbf{N}$, on a

$$\mathbf{Q}\left(\sqrt[d_1]{a_1}, \ldots, \sqrt[d_\ell]{a_\ell}\right) = \mathbf{Q}\left(\sqrt[d_1]{a_1} + \cdots + \sqrt[d_\ell]{a_\ell}\right).$$

Solution.

3. Et en fait exactement p car cette extension est distincte de K puisque $K(a, b)$ est de degré p^2.

4. En effet, par Eisenstein avec $p = X$, le polynôme $T^p - X$ est irréductible sur K et $[K(a) : K] = p$. Reste à voir que $T^p - Y$ est irréductible sur $K(a) = \mathbf{F}_p(X^{1/p}, Y)$ et on peut réappliquer Eisenstein pour cela. Une autre façon de faire est de voir que sur un corps de décomposition, on va avoir $T^p - X = T^p - a^p = (T - a)^p$ et donc si $T^p - X$ n'est pas irréductible dans K, il admet un facteur dans K nécessairement de la forme $(T - a)^i$ avec $1 \leqslant i \leqslant p - 1$. On a donc $a^i, a^p \in K$ et i et p sont premiers entre eux. Une relation de Bézout fournit alors que $a \in K$ ce qui est absurde car cela impliquerait que X^p est une fraction rationnelle en X et Y, contredisant le fait qu'ils sont algébriquement indépendants ! On peut alors procéder de même avec $T^p - Y$ sur $K(a)$ et voir que ce polynôme est irréductible sauf si $b \in K(a)$. Mais une telle relation

$$b = \sum_{i=0}^{p-1} \frac{P_i(X,Y)}{P(X,Y)} a^i$$

fournirait à la puissance p que

$$YP(X^p, Y^p) = \sum_{i=0}^{p-1} P_i(X^p, Y^p) X^i$$

qui aboutit à une contradiction lorsque l'on regarde les degré en Y.

5. Ce polynôme est intéressant (voir Perrin) car il ne reste irréductible modulo aucun nombre premier p.

1. On a clairement que $\mathbf{Q}(\sqrt{a}+\sqrt{b}) \subseteq \mathbf{Q}(\sqrt{a},\sqrt{b})$. Réciproquement, on a en posant $x=\sqrt{a}+\sqrt{b}$

$$(x-\sqrt{a})^2 = b \iff 2x\sqrt{a} = a-b+x^2 \iff \sqrt{a} = \frac{a-b+x^2}{2x} \in \mathbf{Q}(x)$$

et de même $\sqrt{b} \in \mathbf{Q}(x)$, ce qui fournit l'égalité.

On a alors facilement que si $\frac{a}{b} \neq \square$ alors $K = \mathbf{Q}(\sqrt{a},\sqrt{b})$ est galoisienne de groupe de Galois[6] $(\mathbf{Z}/2\mathbf{Z})^2$ et si $\frac{a}{b} = \square$, K est galoisienne de groupe de Galois $\mathbf{Z}/2\mathbf{Z}$.
Calculons le degré de l'extension $\mathbf{Q}(\sqrt{a},\sqrt{b})/\mathbf{Q}$. On doit distinguer trois cas :

(a) Si a et b sont des carrés dans $\mathbf{Q}^\times$ alors $\mathbf{Q}(\sqrt{a}) = \mathbf{Q}(\sqrt{b}) = \mathbf{Q}(\sqrt{a},\sqrt{b}) = \mathbf{Q}(\sqrt{a},\sqrt{b}) = \mathbf{Q}$.

(b) Si a n'est pas un carré dans $\mathbf{Q}^\times$ mais b est un carré dans $\mathbf{Q}^\times$, alors $[\mathbf{Q}(\sqrt{a},\mathbf{Q}] = 2$ et $\sqrt{a}+\sqrt{b} \in \mathbf{Q}(\sqrt{a}) = \mathbf{Q}(\sqrt{b})(\sqrt{a})$, donc $\mathbf{Q}(\sqrt{a}+\sqrt{b})$ est une sous-extension de $\mathbf{Q}(\sqrt{a})$ qui n'est pas de degré 1 car $\sqrt{a} \notin \mathbf{Q}$, donc elle est de degré 2 et $\mathbf{Q}(\sqrt{a},\sqrt{b}) = \mathbf{Q}(\sqrt{a}+\sqrt{b})$. C'est pareil si on inverse les rôles de a et b.

(c) Supposons que ni a ni b soient des carrés dans $\mathbf{Q}$ de sorte que $[\mathbf{Q}(\sqrt{a},\mathbf{Q}] = [\mathbf{Q}(\sqrt{b}),\mathbf{Q}] = 2$. Regardons l'extension $\mathbf{Q}(\sqrt{b})(\sqrt{a})$ de $\mathbf{Q}(\sqrt{b})$. Le polynôme X^2-a est irréductible sur $\mathbf{Q}(\sqrt{b})$ si et seulement si a n'est pas un carré dans $\mathbf{Q}(\sqrt{b})$. Or,

$$\begin{aligned} a \in (\mathbf{Q}^\times)^2 &\iff \exists p,q \in \mathbf{Q} \,|\, (p+q\sqrt{b})^2 = a \\ &\iff \exists p,q \in \mathbf{Q} \,|\, p^2+2pq\sqrt{b}+q^2b = a \\ &\iff \exists p,q \in \mathbf{Q} \,|\, p^2+q^2 = a \text{ et } 2pq = 0 \\ &\iff \exists p \in \mathbf{Q} \,|\, p^2 = a \text{ ou } \exists q \in \mathbf{Q}, q^2 = \frac{a}{b} \end{aligned}$$

On a alors que $\frac{a}{b}$ est un carré si est seulement si $\mathbf{Q}$, $[\mathbf{Q}(\sqrt{b})(\sqrt{a}) : \mathbf{Q}(\sqrt{b})] = 1$ et $[\mathbf{Q}(\sqrt{b},\sqrt{a}) : \mathbf{Q}] = 2$. Dans ce cas, soit $\lambda \in \mathbf{Q}$ tel que $a = \lambda^2 b$. Alors $\sqrt{a}+\sqrt{b} = (1+\frac{1}{\lambda})\sqrt{a}$ et $\mathbf{Q}(\sqrt{a}+\sqrt{b}) = \mathbf{Q}(\sqrt{a}) = \mathbf{Q}(\sqrt{a},\sqrt{b})$.
Supposons maintenant que ni a ni b ni $\frac{a}{b}$ sont des carrés dans $\mathbf{Q}$. Alors a n'est pas un carré dans $\mathbf{Q}(\sqrt{b})$, $\mathbf{Q}(\sqrt{a}) \neq \mathbf{Q}(\sqrt{b})$ et donc X^2-a est irréductible sur $\mathbf{Q}(\sqrt{b})[X]$, donc $[\mathbf{Q}(\sqrt{b},\sqrt{a}) : \mathbf{Q}(\sqrt{b})] = 2$ et $\{1,\sqrt{a}\}$ est une $\mathbf{Q}(\sqrt{b})$-base de $\mathbf{Q}(\sqrt{a},\sqrt{b})$. De même, si $\frac{a}{b}$ n'est pas un carré dans $\mathbf{Q}$, $\frac{b}{a}$ non plus, donc $[\mathbf{Q}(\sqrt{a},\sqrt{b}) : \mathbf{Q}(\sqrt{a})] = 2$ et $\{1,\sqrt{b}\}$ est une $\mathbf{Q}(\sqrt{a})$-base de $\mathbf{Q}(\sqrt{a},\sqrt{b})$. Par le Théorème de la base télescopique on a $[\mathbf{Q}(\sqrt{b},\sqrt{a}) : \mathbf{Q}] = 4$ et $\{1,\sqrt{a},\sqrt{b},\sqrt{ab}\}$ est une $\mathbf{Q}$-base de $\mathbf{Q}(\sqrt{a},\sqrt{b})$.

Comme $\sqrt{a}+\sqrt{b} \in \mathbf{Q}(\sqrt{a},\sqrt{b})$, $\sqrt{a}+\sqrt{b}$ est algébrique sur $\mathbf{Q}$ de degré divisant 4. En regardant les coordonnées de 1, $\sqrt{a}+\sqrt{b}$ et $(\sqrt{a}+\sqrt{b})^2$ dans la base $\{1,\sqrt{a},\sqrt{b},\sqrt{ab}\}$, on voit que $\{2,\sqrt{a}+\sqrt{b},(\sqrt{a}+\sqrt{b})^2\}$ est une famille $\mathbf{Q}$-libre et donc le degré de $\sqrt{a}+\sqrt{b}$ est strictement plus grand que 2; c'est donc 4 et donc $\mathbf{Q}(\sqrt{a}+\sqrt{b}) = \mathbf{Q}(\sqrt{a},\sqrt{b})$.
En calculant $(\sqrt{a}+\sqrt{b})^2$ on trouve que $\sqrt{a}+\sqrt{b}$ est racine de $P(X) = X^4-2(a+b)X^2+(a-b)^2$ qui est alors son polynôme minimal.

2. On a clairement que $\mathbf{Q}(\sqrt{2}+\sqrt{3}+\sqrt{5}) \subseteq \mathbf{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$. Réciproquement, on a en posant $x=\sqrt{2}+\sqrt{3}+\sqrt{5}$

$$(x-\sqrt{2})^2 = 8+2\sqrt{15} \iff \Big((x-\sqrt{2})^2-8\Big)^2 = 60 \iff \sqrt{2} = \frac{a^4-4a^2-24}{4a^3-24a} \in \mathbf{Q}(x)$$

et de même $\sqrt{3},\sqrt{5} \in \mathbf{Q}(x)$, ce qui fournit l'égalité.

On voit alors facilement (comme en question précédente) que $\mathbf{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ est galoisienne de groupe de Galois $(\mathbf{Z}/2\mathbf{Z})^3$ (par exemple en montrant que tout élément est d'ordre 2 et que $[\mathbf{Q}(\sqrt{2},\sqrt{3},\sqrt{5}) : \mathbf{Q}] = 8$).

3. Posons $\alpha = \sqrt{2}+\sqrt[3]{3}$. Le polynôme minimal de $\sqrt[3]{3}$ sur $\mathbf{Q}$ est X^3-3. On peut voir X^3-3 comme polynôme sur $\mathbf{Z}[\sqrt{2}]$ et par Eisenstein avec $p=3$ qui y est irréductible[7], il y est irréductible, c'est donc le polynôme minimal de $\sqrt[3]{3}$ sur $\mathbf{Q}(\sqrt{2})$. Ceci implique que $P(X) = (X-\sqrt{2})^3-3$ est encore irréductible sur $\mathbf{Z}[\sqrt{2}]$ et c'est le polynôme minimal de $\alpha = \sqrt{2}+\sqrt[3]{3}$ sur $\mathbf{Z}[\sqrt{2}]$. On a alors les inclusions $\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{2}) \subseteq \mathbf{Q}(\sqrt{2})(\sqrt[3]{3}) = \mathbf{Q}(\sqrt{2},\sqrt[3]{3})$ et les degrés : $[\mathbf{Q}(\sqrt{2},\sqrt[3]{3}) : \mathbf{Q}] = [\mathbf{Q}(\sqrt{2},\sqrt[3]{3}) : \mathbf{Q}(\sqrt{2})][\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 3 \times 2 = 6$. Or, on a $\mathbf{Q}(\sqrt{2},\sqrt[3]{3}) = \mathbf{Q}(\alpha)$.
On a clairement $\mathbf{Q}(\alpha) \subset \mathbf{Q}(\sqrt{2},\sqrt[3]{3})$. Montrons l'inclusion inverse en montrant que $a=\sqrt{2}$ et $b=\sqrt[3]{3}$ sont des fonctions rationnelles sur α. On a $(\alpha-a)^3 = (\sqrt{2}+\sqrt[3]{3}-\sqrt{2})^3 = 3$ donc $\alpha^3-3a\alpha^2+12\alpha-2a = 3$ donc $a = \frac{3-c^3-12c}{(-3c^2-2)}$ et $a \in \mathbf{Q}(\alpha)$. De plus, $a+b=\alpha$ donc $b=\alpha-a$ et donc $b \in \mathbf{Q}(\alpha)$. Ceci montre aussi que le degré de $\mathbf{Q}(\alpha)$ est égal à 6.

6. Je rappelle que si L est une extension galoisienne de $\mathbf{Q}$ et que $x \in L$ vérifie que $P(x)=0$ avec $P \in \mathbf{Q}[X]$ son polynôme minimal, alors pour tout $\sigma \in \mathrm{Gal}(L/\mathbf{Q})$, on a $P(\sigma(x))=0$. Ici, on calcule aisément les degrés et on vérifie qu'à la lumière de la remarque ci-dessus, tout élément du groupe de Galois est déterminé par l'image de $\sqrt{a}$ et de $\sqrt{b}$ qui annulent respectivement X^2-a et X^2-b de sorte que $\sigma(\sqrt{a}) = \pm\sqrt{a}$ et $\sigma(\sqrt{b}) = \pm\sqrt{b}$ et tout élément du groupe de Galois est d'ordre 2. On sait alors qu'un tel groupe est abélien et isomorphe à un produit direct de plusieurs $\mathbf{Z}/2\mathbf{Z}$.

7. On peut montrer que $\mathbf{Z}[\sqrt{2}]$ est euclidien de stathme $|a^2-2b^2|$ comme dans le cas de $\mathbf{Z}[i]$. Noter qu'Eisenstein ne s'applique que dans des anneaux factoriels.

4. Montrons que pour $a_1, \dots, a_\ell \in \mathbf{N}$ et $d_1, \dots, d_\ell \in \mathbf{N}$, on a

$$\mathbf{Q}\left(\sqrt[d_1]{a_1}, \dots, \sqrt[d_\ell]{a_\ell}\right) = \mathbf{Q}\left(\sqrt[d_1]{a_1} + \cdots + \sqrt[d_\ell]{a_\ell}\right).$$

On utilise le résultat suivant : si L est une extension galoisienne de $\mathbf{Q}$ et si $\alpha, \beta \in L$ sont deux éléments tels que [8]

$$\forall \sigma \in \mathsf{Gal}(L/\mathbf{Q}), \quad \sigma(\alpha) = \alpha \quad \Longrightarrow \quad \sigma(\beta) = \beta$$

alors $\beta \in \mathbf{Q}(\alpha)$.

On pose alors $\alpha = \sqrt[d_1]{a_1} + \cdots + \sqrt[d_\ell]{a_\ell}$ et on considère L une extension galoisienne [9] L contenant tous les $\beta_i = \sqrt[d_i]{a_i}$ et $\sigma \in \mathsf{Gal}(L/\mathbf{Q})$ fixant α. On doit avoir $\sigma(\beta_i) = \xi_i \beta_i$ avec ξ_i une racine d_i-ème de l'unité. L'hypothèse que $\sigma(\alpha) = \alpha$ implique alors que

$$\sum_{i=1}^{\ell} \xi_i \beta_i = \sum_{i=1}^{\ell} \beta_i.$$

On a alors

$$\left|\sum_{i=1}^{\ell} \beta_i\right| = \left|\sum_{i=1}^{\ell} \xi_i \beta_i\right| \leqslant \sum_{i=1}^{\ell} |\beta_i| = \sum_{i=1}^{\ell} \beta_i.$$

Le cas d'égalité de l'inégalité triangulaire fournit alors que tous les ξ_i sont égaux et cela entraîne que $\xi_i = 1$ pour tout i soit $\sigma(\beta_i) = \beta_i$ et donc $\beta_i = \sqrt[d_i]{a_i} \in \mathbf{Q}(\sqrt[d_1]{a_1} + \cdots + \sqrt[d_\ell]{a_\ell})$.

Exercice 7 — Extensions linéairement disjointes. Soit K un corps. Soient K_1, K_2 deux extensions algébriques de K. On dit que K_1 et K_2 sont *linéairement disjointes* sur K si la K-algèbre $K_1 \otimes_K K_2$ est un anneau intègre.

1. On suppose que $K_1 = K(\theta)$ pour θ un élément algébrique. Donner une condition nécessaire et suffisante sur P pour que K_1 et K_2 soient linéairement disjointes.
2. Montrer que si K_1 ou K_2 est algébrique, la condition est équivalente au fait que $K_1 \otimes_K K_2$ soit un corps.
3. Les extensions $\mathbf{Q}(i)$ et $\mathbf{Q}(\sqrt{2})$ sont-elles linéairement disjointes sur $\mathbf{Q}$? Même question pour $\mathbf{Q}(\sqrt[3]{2})$ et $\mathbf{Q}(j\sqrt[3]{2})$.
4. On note K_1K_2 l'extension de K engendrée par K_1 et K_2. On appelle K_1K_2 le *compositum* de K_1 et K_2. On suppose dans cette question que K_1 et K_2 sont deux extensions galoisiennes. Montrer alors que la condition d'être linéairement disjointes est équivalente au fait que $K_1 \cap K_2 = K$.
5. Sous les mêmes hypothèses que la question précédente, montrer qu'on a un isomorphisme entre $\mathsf{Gal}(K_1K_2/K)$ et le produit direct de $\mathsf{Gal}(K_1/K)$ et $\mathsf{Gal}(K_2/K)$.

Solution. Je vous renvoie à la section du polycopié de David Harari pour la structure d'anneau et de K-algèbre de $K_1 \otimes_K K_2$ (page 19 ici).

1. Soit P le polynôme minimal de θ sur K de sorte que $K_1 \cong K[X]/(P)$. Comme on l'a vu en cours, $K[X]/(P) \otimes_K K_2$ est isomorphe à $K_2[X]/(P)$. La condition est donc que P (qui est irréductible dans K puisque K_1 est un corps) reste irréductible dans K_2. Noter qu'on a alors mieux que l'intégrité mais une structure de corps.
2. On peut en effet supposer que K_1 est finie puisque tout élément x non nul de $K_1 \otimes_K K_2$ est de la forme

$$x = \sum_{i=1}^{r} \lambda_i \otimes \mu_i, \quad \text{avec} \quad \lambda_i \in K_1,\ \mu_i \in K_2.$$

On a alors que $K_1' = K(\lambda_1, \dots, \lambda_r)$ est une sous-extension finie de K_1 contenant K. On a alors que [10] $x \in K_1' \otimes_K K_2 \subseteq K_1 \otimes_K K_2$. La question précédente permet alors de conclure. On peut alors se donner une base $(e_1, \dots, e_n)$ de K_1' sur K et on sait que $(e_1 \otimes 1, \dots, e_n \otimes 1)$ est une base de l'anneau intègre $K_1' \otimes_K K_2$ (si l'on suppose K_1 et K_2 linéairement disjointes) qui est par conséquent de dimension finie sur K_2. Cela implique que pour tout $x \in K_1' \otimes_K K_2$ non nul, l'application linéaire injective (par intégrité) entre deux espaces vectoriels de même dimension $K_1' \otimes_K K_2 \to K_1' \otimes_K K_2$ donnée par $y \mapsto yx$ est un isomorphisme et $K_1' \otimes_K K_2$ est bien un corps si bien que x est inversible et $K_1 \otimes_K K_2$ est un corps.
3. D'après **1.**, $\mathbf{Q}(i)$ et $\mathbf{Q}(\sqrt{2})$ sont linéairement disjointes sur $\mathbf{Q}$, en prenant $P = X^2 + 1$, qui est bien irréductible sur $\mathbf{Q}(\sqrt{2})$. Ce n'est pas le cas de $\mathbf{Q}(\sqrt[3]{2})$ et $\mathbf{Q}(j\sqrt[3]{2})$, le polynôme $X^3 - 2$ n'étant pas irréductible dans $\mathbf{Q}(j\sqrt[3]{2})$ (il a une racine dans ce corps).
4. Il est clair que si les extensions sont liéairement disjointes, puisque sous ces hypothèses, $K_1 \otimes_K K_2$ est un corps et $f : K_1 \otimes_K K_2 \to K_1K_2$ donnée par $x \otimes y \mapsto yx$ est un morphisme de corps, il est en particulier injectif. Or, s'il existe $x \in K_1 \cap K_2 \smallsetminus K$, alors on peut compléter $(1, x)$ en une K-base de K_1 et en une K-base de K_2 de sorte que $1 \otimes x$ et $x \otimes 1$ sont deux éléments d'une K-base de $K_1 \otimes_K K_2$, donc distincts mais qui pourtant ont la même image par l'application f. On a donc bien $K_1 \cap K_2 = K$. Reste à démontrer que si $K_1 \cap K_2 = K$ et que les deux extensions sont galoisiennes, alors K_1 et K_2 sont linéairement disjointes. Pour ce faire, on écrit par le théorème de l'élément primitif [11] que $K_1 = K(\theta)$ et on note P le polynôme minimal de θ sur K. Si P admet un facteur

8. Noter que cela impose que pour tout $\sigma \in H := \mathsf{Gal}(L/\mathbf{Q}(\alpha))$, alors $\beta \in L^H$. La correspondance de Galois fournit alors que $\beta \in L^H = \mathbf{Q}(\alpha)$.
9. Possible en considérant une clôture galoisienne.
10. Attention que le fait que $K_1' \subseteq K_1$ implique $K_1' \otimes_K K_2 \subseteq K_1 \otimes_K K_2$ n'est vraie que parce qu'on travaille avec des espaces vectoriels! Pour le voir, il suffit de compléter une base de K_1' en une base de K_1 et alors on obtient une base de $K_1 \otimes_K K_2$ qui commence par une base de $K_1' \otimes_K K_2$. Mais en général, c'es faux comme on le voit avec l'inclusion $\mathbf{Z} \subseteq \mathbf{Q}$ et en prenant le produit tensoriel par $\mathbf{Z}/n\mathbf{Z}$ puisque $\mathbf{Z} \otimes_{\mathbf{Z}} (\mathbf{Z}/n\mathbf{Z}) = \mathbf{Z}$ et $\mathbf{Q} \otimes_{\mathbf{Z}} (\mathbf{Z}/n\mathbf{Z}) = \{0\}$ puisque $\mathbf{Q}$ est divisible!
11. L'extension est séparable finie.

irréductible unitaire $Q \in K_2[X]$, alors $Q \in K_1[X]$ (car P est le polynôme minimal de θ et K_1 est galoisienne donc P est scindé sur K_1) si bien que $Q \in K[X]$, ce qui contredit l'irreductibilité de P sur K. On a donc que P est irréductible sur K_2 et par conséquent que K_1 et K_2 sont linéairement disjointes!

5. Lorsque les deux extensions sont galoisiennes, il est clair que K_1K_2 l'est (c'est un corps de décomposition du produit des polynômes dont K_1 et K_2 sont des corps de décomposition). On a par ailleurs une bijection $K_1 \otimes_K K_2$ avec K_1K_2 donnée par $K_1 \otimes K_2 \to K_1K_2$ et $x_1 \otimes x_2 \mapsto x_1x_2$ de sorte que $[K_1K_2 : K] = [K_1 : K][K_2 : K]$. Il est alors aisé de voir que le morphisme bien défini est injectif et un isomorphisme par cardinalité

$$\begin{array}{ccc} \mathsf{Gal}(K_1K_2/K) & \longrightarrow & \mathsf{Gal}(K_1/K) \times \mathsf{Gal}(K_2/K) \\ \sigma & \longmapsto & (\sigma_{|_{K_1}}, \sigma_{|_{K_2}}). \end{array}$$

Exercices fondamentaux de la semaine 2

Exercice 8. On considère l'extension $\mathbf{Q}(i, \sqrt[4]{2})$ de $\mathbf{Q}$.

1. Montrer que le groupe de Galois de cette extension est égal au produit semi-direct $\langle\alpha\rangle \rtimes \{1, \tau\}$, où τ est la conjugaison complexe et où $\alpha(\sqrt[4]{2}) = i\sqrt[4]{2}$ et $\alpha(i) = i$.
2. Montrer que cette extension est galoisienne.
3. Donner le treillis des sous-groupes de $\mathsf{Gal}(\mathbf{Q}(i, \sqrt[4]{2})/\mathbf{Q})$.
4. Donner le treillis des extensions de $\mathbf{Q}$ contenues dans $\mathbf{Q}(i, \sqrt[4]{2})$.

Solution. L'extension est galoisienne comme corps de décomposition de $X^4 - 2$ (irréductible par Eisenstein par exemple). Par ailleurs, on voit aisément que[12] $[K : \mathbf{Q}] = 8$. D'après le cours, on a alors que $G = \mathsf{Gal}(K/\mathbf{Q})$ peut être vu comme un sous-groupe transitif de $\mathfrak{S}_4$ et utiliser le treillis de $\mathfrak{S}_4$ ou la classification des groupes d'ordre 8.

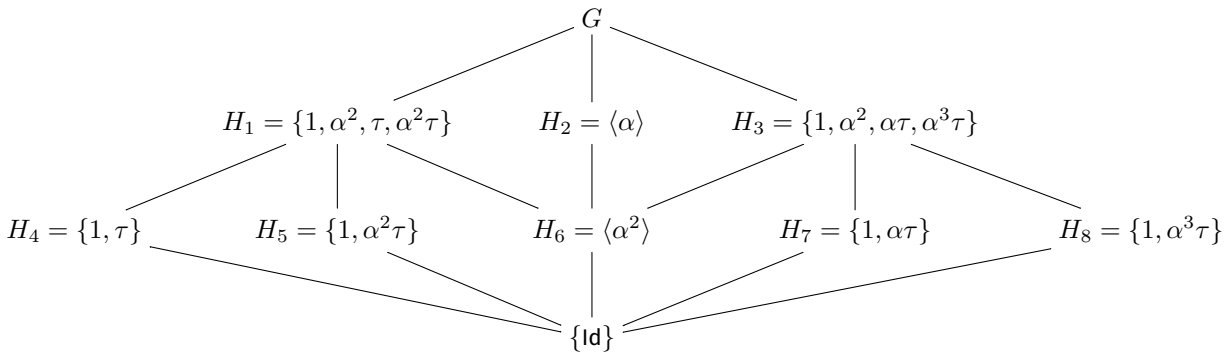
Ou on sait que $\mathsf{Gal}(\mathbf{Q}(i)/\mathbf{Q}) \cong \mathbf{Z}/2\mathbf{Z}$ si bien que $H = \mathsf{Gal}(K/\mathbf{Q}(i)) \lhd G$ de cardinal 4. Par ailleurs, on a que pour tout $\sigma \in H$, $\sigma(\sqrt[4]{2}) = e^{\frac{f(\sigma)i\pi}{2}}\sqrt[4]{2}$ avec $f(\sigma) \in \mathbf{Z}/4\mathbf{Z}$. Puisque $K = \mathbf{Q}(i, \sqrt[4]{2})$, f est injective et donc une bijection par cardinalité. C'est également un morphisme car

$$\sigma \circ \sigma'(\sqrt[4]{2}) = e^{\frac{f(\sigma)i\pi}{2}}\sigma(\sqrt[4]{2}) = e^{\frac{(f(\sigma)+f(\sigma'))i\pi}{2}}.$$

On obtient donc que $H \cong \mathbf{Z}/4\mathbf{Z}$ est engendré par α qui vérifie $\alpha(\sqrt[4]{2}) = i\sqrt[4]{2}$ et $\alpha(i) = i$. On a donc une suite exacte $0 \to \mathbf{Z}/4\mathbf{Z} \to G \to \mathbf{Z}/2\mathbf{Z} \to 0$ dont la conjugaison complexe définit une section[13]. On a donc $G = H \rtimes \langle\tau\rangle$ et $H = \langle\alpha\rangle$ avec $\alpha(\sqrt[4]{2}) = i\sqrt[4]{2}$ et $\alpha(i) = i$ tandis que τ est la conjugaison complexe. Une autre façon de dire les choses est que α et τ engendrent G car si $\sigma \in G$, soit $\sigma \in H$ et on a gagné soit, $\sigma \notin H$ et par définition, $\sigma(i) \neq i$ mais alors on n'a pas le choix, $\sigma(i) = -i$ et $\tau \circ \sigma(i) = i$ et $\tau \circ \sigma \in H$. On a donc bien que $G = \langle\alpha, \tau\rangle$. On calcule alors

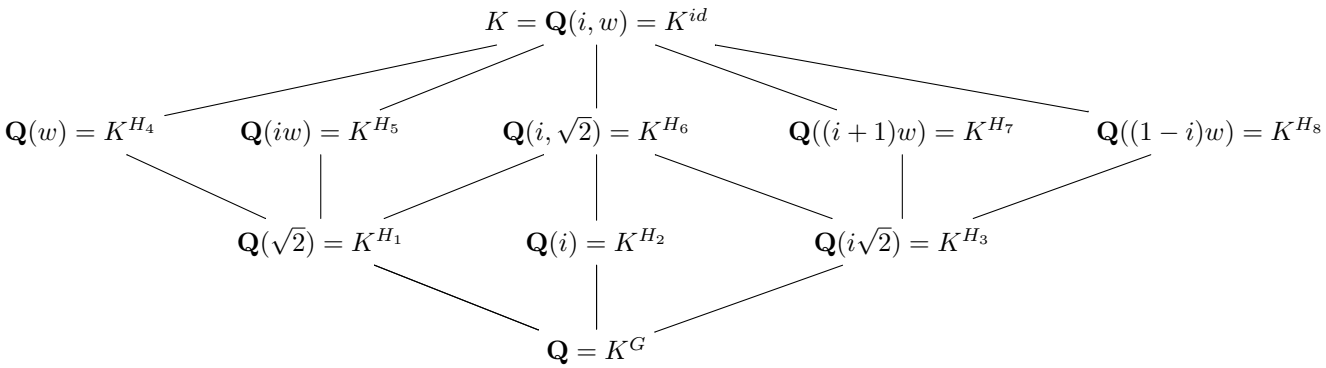
$$\tau \circ \alpha \circ \tau(i) = \tau \circ \alpha(-i) = \tau(-i) = i \quad \text{et} \quad \tau \circ \alpha \circ \tau(\sqrt[4]{2}) = \tau \circ \alpha(\sqrt[4]{2}) = \tau(i\sqrt[4]{2}) = -i\sqrt[4]{2}$$

si bien que $\sigma \circ \alpha \circ \sigma = \alpha^{-1}$ et on reconnaît le groupe diédral $\mathbf{D}_4$. Soit en utilisant le fait que l'on sait par le cours que dans ce cas l'action a lieu par conjugaison soit en utilisant que G n'est pas abélien et qu'il n'existe qu'un seul produit semi-direct non trivial $\mathbf{Z}/4\mathbf{Z} \rtimes \mathbf{Z}/2\mathbf{Z}$ soit en exhibant un isomorphisme explicite.
Le treillis des sous-groupes de G s'écrit alors :



Par correspondance de Galois le treillis des sous-extensions de $\mathbf{Q}(i, w)$ avec $w = \sqrt[4]{2}$ est :

12. Car $\mathbf{Q}(\sqrt[4]{2})$ est un corps de rupture du polynôme irréductible $X^4 - 2$ donc de degré 4 puis $X^2 + 1$ est irréductible sur $\mathbf{Q}(\sqrt[4]{2})$ car ce dernier est inclus dans $\mathbf{R}$ et donc $X^2 + 1$ ne saurait y avoir de racines. Ainsi, $[\mathbf{Q}(\sqrt[4]{2}, i) : \mathbf{Q}(\sqrt[4]{2})] = 2$ et par multiplicativité des degrés, $[K : \mathbf{Q}] = 8$.
13. En effet, le morphisme $G \to \mathbf{Z}/2\mathbf{Z}$ est clairement donné par $\sigma \mapsto 0$ si $\sigma(i) = i$ (soit $\sigma \in H$ et $\sigma \mapsto 1$ sinon.



Pour trouver le treillis des sous-extensions on doit trouver les sous-corps de K suivants : $K^{H_i} = \{x \in K \mid \sigma(x) = x,\ \forall \sigma \in H_i\}$ pour tout $i = 1,2,3,4,5,6,7,8$. Pour simplifier les notations posons $r_0 = id$, $r_1 = \alpha$, $r_2 = \alpha^2$, $r_3 = \alpha^3$, $u_1 = \tau$, $d_1 = \alpha\tau$, $u_2 = \alpha^2\tau$, $d_2 = \alpha^3\tau$ les éléments de G.

- K^{H_2} (ce sont les éléments fixes par $\langle\alpha\rangle$ est une extension de degré 2 car H_2 est un sous-groupe d'ordre 4 et donc d'indice 2 (il est distingué dans G. Comme $\alpha^n(i) = i$ pour $n = 0,1,2,3$ on conclut que $K^{H_2} = \mathbf{Q}(i)$.
- Comme H_4 est un groupe d'indice 4, K^{H_4} est une extension de degré 4 sur $\mathbf{Q}$. Comme $\tau(w) = w$ alors $\mathbf{Q}(w)$ est fixée par τ et id et que $[\mathbf{Q}(w) : \mathbf{Q}] = 4$, le Théorème de Galois dit que c'est la seule, donc $K^{H_4} = \mathbf{Q}(w)$.
- On sait que K^{H_7} est un extension de degré 4 sur $\mathbf{Q}$ car $H_7 = \{id, \alpha\tau\}$ est un groupe d'ordre 2. Si on calcule l'action de $\alpha\tau$ sur les éléments de $\{1, w, w^2, w^3, i, iw, iw^2, iw^3\}$ qui est une $\mathbf{Q}$-base de K on a $\{1, iw, -w^2, -iw^3, -i, , w, iw^2, -w\}$ et on voit que les éléments w et iw sont permutés par $\alpha\tau$. Ceci implique que $\alpha\tau(w + iw) = iw + w$ *i.e.* $w + iw$ est stable par $\alpha\tau$ et donc $\mathbf{Q}(w + iw) \subset K^{H_7}$. Mais $[\mathbf{Q}(w + iw) : \mathbf{Q}] = 4$: en effet, on aimerait trouver le polynôme minimal S de $\gamma = w + iw$ pour avoir le degré de cette extension. Pour tout conjugué γ' de γ sur $\mathbf{Q}$ il existe un élément $\sigma \in G$ tel que $\sigma(\gamma) = \gamma'$, donc pour trouver les racines de S on calcule $\sigma(\gamma)$, pour tout $\sigma \in G$; il suffit de calculer $\sigma(\gamma)$ pour σ dans un ensemble de représentants du quotient $G/H_7 = \{\overline{r_0}, \overline{r_1}, \overline{r_2}, \overline{r_3}\}$. On trouve alors que les conjugués de γ sont : $-w + iw$, $iw - w$, $-w - iw$ et $-iw + w$ et donc que $S = X^4 + 8$.

Une méthode (systématique) pour trouver les sous-extensions associées à des sous-groupes. On sait que pour $H \leqslant G$, $\sum_{\sigma\in H} \sigma(a) \in K^H$ pour tout $a \in K$ (et en fait on peut montrer que ces éléments engendrent[14] K^H). Dans le cas de $H = \langle\alpha\tau\rangle$ et $a = \sqrt[4]{2}$, on a

$$\sum_{\sigma\in H} \sigma(a) \in K^H = (1+i)\sqrt[4]{2}$$

et de même si $H = \langle\alpha^3\tau\rangle$ et $a = \sqrt[4]{2}$, on a

$$\sum_{\sigma\in H} \sigma(a) \in K^H = (1-i)\sqrt[4]{2}.$$

Une autre méthode (plus à la main) : Soit $P = X^4 - 2$ vu comme polynôme dans $\mathbf{Q}[X]$ et soit K un corps de décomposition de P. P est irréductible sur $\mathbf{Q}$ par Eisenstein et $w = \sqrt[4]{2}$ est une racine positive réelle de P. Les zéros de P dans $\mathbf{C}$ sont : w,$-w$,iw et $-iw$. Comme $\frac{iw}{w} = i$ on a $i \in K$. Comme $\mathbf{Q}(w,i)$ contient tous les zéros de P on a que $K = \mathbf{Q}(w,i)$ et comme P est séparable, on a que K est bien galoisienne. Calculons le degré de K comme extension de $\mathbf{Q}$. Soit $E = \mathbf{Q}(w)$. Comme P est irréductible sur $\mathbf{Q}$, $[\mathbf{Q}(w) : \mathbf{Q}] = 4$ et $\{1, w, w^2, w^3\}$ est une $\mathbb{Q}$-base de E. Le polynôme minimal de i sur E est $X^2 + 1$ car $E \subset \mathbf{R}$ et $\{1, i\}$ est une $\mathbf{Q}(w)$-base de $\mathbf{Q}(w,i)$. On a alors que $[K : E] = 2$ et donc par le Théorème de la base télescopique $[K : \mathbf{Q}] = 8$. Une base de K sur $\mathbf{Q}$ est $\{1, w, w^2, w^3, i, iw, iw^2, iw^3\}$. Comme K est galoisienne : le groupe de Galois de $K/\mathbf{Q}$ est un groupe d'ordre 8. Notons G ce groupe de Galois. Tout élément σ de G est complètement déterminé par son action sur les éléments de la base $\{1, w, w^2, w^3, i, iw, iw^2, iw^3\}$ et donc ses valeurs sont déterminées par $\sigma(w)$ et $\sigma(i)$ car σ est un automorphisme. Le polynôme minimal de i sur $\mathbf{Q}(w)$ étant $X^2 + 1$, on a que σ doit envoyer i sur i ou sur $-i$. Posons $\alpha(w) = iw$ et $\tau(i) = -i$ (τ est un élément de G d'ordre 2). On peut donc écrire le tableau suivant qui donne l'action des éléments de G sur w et i :

σ	id	α	α^2	α^3	τ	$\alpha\tau$	$\alpha^2\tau$	$\alpha^3\tau$
$\sigma(w)$	w	iw	-w	-iw	w	iw	-w	-iw
$\sigma(i)$	i	i	i	i	$-i$	$-i$	$-i$	$-i$

14. Car tout $x \in K^H$ est de la forme

$$\frac{1}{\#H}\sum_{\sigma\in H}\sigma(x) = \sum_{\sigma\in H}\sigma\left(\frac{x}{\#H}\right).$$

Pour identifier G, on voit d'abord qu'il n'est pas abélien : par exemple $\tau\alpha(w) = \tau(iw) = -iw$ alors que $\alpha\tau(w) = \alpha(w) = iw$. De même, on voit facilement que α est d'ordre 4 et que τ est d'ordre 2 (τ est la conjugaison complexe) et que la relation suivante est vérifiée : $\alpha\tau = \tau\alpha^3$. On a donc que $G = \langle\alpha\rangle \rtimes \{\tau\} = \{\alpha, \tau \,|\, \alpha^4 = 1, \tau^2 = 1, \alpha\tau = \tau\alpha^3\}$.

Exercice 9 — Calculs de groupes de Galois. Déterminer le groupe de Galois de chacune des extensions de corps ou chacun des polynômes suivants.

1. $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ sur $\mathbf{Q}$.
2. $X^3 - 10$ sur $\mathbf{Q}$, puis sur $\mathbf{Q}(\sqrt{2})$.
3. $X^3 - X - 1$ sur $\mathbf{Q}$.
4. $X^n - t$ sur $\mathbf{C}(t)$, puis sur $\mathbf{R}(t)$.
5. $X^5 - pqX + p$ sur $\mathbf{Q}$, où p est un nombre premier et $q \geqslant 2$ est un entier.
6. $X^6 + 3$ sur $\mathbf{Q}$.
7. $32X^5 + 16X^4 - 32X^3 - 12X^2 + 6X + 1 = 32\prod_{k=1}^{5}\left(X - \cos\left(\frac{2k\pi}{11}\right)\right)$ sur $\mathbf{Q}$.

Remarque : Le livre *Algebra* de Serge Lang contient des dizaines d'exercices de ce type.

Solution.

1. Une façon de faire est comme en section 4.4 du polycopié de D. Harari ici. Le corps $K = \mathbf{Q}(\sqrt{2}, \sqrt{3})$ est un extension galoisienne sur $\mathbf{Q}$ de degré 4 sur $\mathbf{Q}$ (c'est le corps de décomposition de $(X^2 - 2)(X^2 - 3)$) et $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ est une $\mathbf{Q}$-base de [15] K. Le groupe de Galois G de K est un groupe dont tout élément vérifie $g^2 = \mathrm{Id}$ comme dans l'exercice 10 et on voit alors par cardinalité que G est isomorphe à $\mathbf{Z}/2\mathbf{2} \times \mathbf{Z}/2\mathbf{2}$.
2. On a déjà (de même que $X^3 - 2$) que $\mathrm{Gal}(K, \mathbf{Q}) \cong \mathfrak{S}_3$. De même sur $\mathbf{Q}(\sqrt{2})$. En revanche, sur $L = \mathbf{Q}(j)$, on voit que $j \in \mathbf{Q}(j)$ si bien que le corps de décomposition devient $L(\sqrt[3]{10})$ de groupe de Galois $\mathbf{Z}/3\mathbf{Z}$. Voir section 4.4 du polycopié de D. Harari ici. On peut aussi raisonner comme dans l'exercice précédent.

   On a $P = X^3 - 10 = (X - \sqrt[3]{10})(X - \xi\sqrt[3]{10})(X - \xi^2\sqrt[3]{10})$ où ξ est une racine 3-ième de l'unité non triviale. Le corps de décomposition de P est $\mathbf{Q}(\sqrt[3]{10}, \xi)$. L'extension $\mathbf{Q}(\xi)/\mathbf{Q}$ est cyclotomique donc galoisienne de degré 2 (le polynôme minimal de ξ est $X^2 + X + 1$) et le groupe de Galois de $\mathbf{Q}(\xi)/\mathbf{Q}$ est $\{1, \tau\}$ où τ est la conjugaison. L'extension $\mathbf{Q}(\xi)(\sqrt[3]{10})/\mathbf{Q}(\xi)$ est de Kummer de degré 3, son groupe de Galois est $\{1, \alpha, \alpha^2\}$ où $\alpha(\sqrt[3]{10}) = \xi\sqrt[3]{10}$. On conclut alors que le groupe de Galois de P sur $\mathbf{Q}$ est $\{1, \alpha, \alpha^2, \tau, \tau\alpha, \tau\alpha^2\}$ qui est isomorphe à $\mathfrak{S}_3 = \mathbf{Z}/3\mathbf{Z} \rtimes \mathbf{Z}/2\mathbf{Z}$. Pour calculer le groupe de Galois sur $\mathbf{Q}(\sqrt{2})$ on considère la tour d'extensions $\mathbf{Q}(\sqrt{2}) \to \mathbf{Q}(\sqrt{2}\xi) \to \mathbf{Q}(\sqrt{2}, \xi, \sqrt[3]{10})$ et le même raisonnement permet de dire que le groupe de Galois sur $\mathbf{Q}(\sqrt{2})$ est aussi $\{1, \alpha, \alpha^2, \tau, \tau\alpha, \tau\alpha^2\}$.
   On pouvait aussi raisonner exactement comme dans l'exercice 9. On a ici deux générateurs qui sont chacun responsable d'un $\mathbf{Z}/3\mathbf{Z}$ et d'un $\mathbf{Z}/2\mathbf{Z}$ mais comme ces deux générateurs proviennent des racines d'un même polynôme irréductible, ils ne sont pas indépendants et on obtient un produit semi-direct (autrement dit les extensions $\mathbf{Q}(\xi)$ et $\mathbf{Q}(\sqrt[3]{10})$ ne sont pas linéairement disjointes).
3. Ici, plus difficile de construire les racines de P, même si c'est possible par les méthodes de Cardan

$$\frac{1}{3}\left(j^k\sqrt[3]{\frac{27 + 3\sqrt{69}}{2}} + j^{2k}\sqrt[3]{\frac{27 - 3\sqrt{69}}{2}}\right), \quad k \in \{0, 1, 2\}$$

   En revanche, on a plusieurs autres méthodes. Le polynôme $X^3 - X + 1$ est irréductible sur $\mathbf{Q}$ et n'a qu'une seule racine réelle (en effet, $P'(X) = 3X^2 - 1$ s'annule en $\pm\frac{1}{\sqrt{3}}$), son groupe de Galois G est alors isomorphe à $\mathfrak{S}_3$. En effet, la conjugaison complexe $\tau : i \mapsto -i$ est un élément de non trivial de G d'ordre 2. Comme le degré de P est égal à 3, si $\alpha \in K$ est une racine de P (où on note K un corps de décomposition de P), l'extension $\mathbf{Q}(\alpha)$ est de degré 3, or $[K : \mathbf{Q}] = [K = [K : \mathbf{Q}(\alpha)][\mathbf{Q}(\alpha) : \mathbf{Q}]$ donc 3 divise $[K : \mathbf{Q}]$ qui est l'ordre de G. Par le lemme de Cauchy, il existe un élément $\sigma \in G$ d'ordre 3. En considérant le morphisme de groupes qui a τ l'envoie sur une transposition quelconque de $\mathfrak{S}_3$ et σ sur un 3-cycle, on a que G est bien isomorphe à $\mathfrak{S}_3$ (se souvenir que G peut être vu comme un sous-groupe transitif de $\mathfrak{S}_3$ car irréductible de degré 3) car ce dernier est engendré par une transposition et un 3-cycle.

   Ou on a que $X^3 - X - 1$ est irréductible sur $\mathbf{Q}$ (car sans racine). Ainsi, son corps de décomposition K est galoisien et contient une sous-extension de degré 3 (un corps de rupture). On peut donc identifier $G = \mathrm{Gal}(K/\mathbf{Q})$ à $\mathfrak{A}_3$ ou $\mathfrak{S}_3$. Par l'exerice 11, on peut montrer qu'on obtient $\mathfrak{A}_3$ si, et seulement si, $\mathrm{disc}(X^3 - X - 1)$ est un carré et $\mathfrak{S}_3$ sinon. On rappelle que $\mathrm{disc}(X^3 + pX + q) = -4p^3 - 27q^2$. On obtient ici -23.

15. Ou alors $\mathbf{Q}(\sqrt{2})$ est de degré 2 sur $\mathbf{Q}$ et K est de degré 2 sur $\mathbf{Q}(\sqrt{2})$ car $X^2 - 3$ n'y a pas de racine (sinon $\sqrt{3} \in \mathbf{Q}(\sqrt{2})$ et $\sqrt{2}$ serait rationnel.

4. On voit par Eisenstein que $X^n - t$ est irréductible et que le corps de décomposition n'est autre que $\mathbf{C}(t)(\alpha)$ avec $\alpha^n = t$. On a alors

$$X^n - t = X^n - \alpha^n = \prod_{i=1}^{n}(X - \xi_n^i \alpha)$$

avec ξ une racine primitive n-ème de l'unité et K est de degré n. On a également que pour $\sigma \in G = \mathrm{Gal}(K/\mathbf{C}(t))$, $\sigma(\alpha) = \xi^{f(\sigma)}\alpha$ pour $f(\sigma) \in \mathbf{Z}/n\mathbf{Z}$. On vérifie alors que f est un morphisme injectif pour conclure que $G \cong \mathbf{Z}/n\mathbf{Z}$.
Sur $\mathbf{R}(t)$, on n'a pas les racines de l'unité et un corps de décomposition est $\mathbf{R}(t)(i, \alpha)$ et le groupe de Galois est le groupe de Galois de K sur $\mathbf{C}(t)$ produit semi-direct $\{1, \tau\}$, où τ est la conjugaison complexe.

5. On montre que $X^5 - pqX + p$ est irréductible de degré premier avec deux racines complexes et 3 racines réelles.

Le polynôme $P = X^5 - pqX + q$ est irréductible sur $\mathbf{Q}$ par Eisenstein ; notons K un corps de décomposition de P et $r_1, r_2, r_3, r_4, r_5 \in K$ les racines de P (elles sont toutes distinctes car $\mathbf{Q}$ est parfait). Le groupe de Galois G de P est isomorphe à un sous-groupe transitif de $\mathfrak{S}_5$. En considérant $\mathbf{Q}(r_i)$ pour $r_i \in K$ une des racines de P, on voit que 5 divise l'ordre de G, il existe donc un élément de G qui est envoyé sur un 5-cycle dans $\mathfrak{S}_5$. En calculant la dérivée de P on voit que P' a deux racines réelles : $\pm\sqrt[4]{\frac{pq}{5}}$, donc P a au plus 3 racines réelles (si elle en avait 5, sa dérivée s'annulerait 4 fois sur $\mathbf{R}$ et non 2). Comme $P(X)$ tend vers $-\infty$ quand X tend vers $-\infty$, $P(-1) > 0$ et $P(1) < 0$ on a que P a au moins trois racines réelles ce qui implique qu'il en a exactement 3. Il a donc 2 racines complexes et $\tau : i \mapsto -i$, la conjugaison complexe, est un automorphisme de G d'ordre 2. Le groupe G a alors un élément d'ordre[16] 2 qui est une transposition (la conjugaison complexe fixe les trois racines réelles et échange les deux racines complexes conjuguées) et un élément d'ordre 5, il est donc isomorphe[17] à $\mathfrak{S}_5$. On a donc ici un exemple de famille de polynômes non résolubles par radicaux car $\mathfrak{S}_5$ n'est pas résoluble !

6. Ce polynôme est irréductible sur $\mathbf{Q}$ via Eisenstein avec $p = 3$. L'extension est donc galoisienne (car il est séparable en caractéristique nulle) et le groupe de Galois G s'identifie à un sous-groupe transitif de $\mathfrak{S}_6$. Déterminons le corps de décomposition explicitement. On note $\alpha = i\sqrt[6]{3}$ une racine de $P = X^6 + 3$. On a alors que toutes les racines sont données par $\zeta^k\alpha$ pour $k \in \{0, \dots, 5\}$ et $\zeta = e^{\frac{2i\pi}{6}} = e^{\frac{i\pi}{3}} = \frac{1+i\sqrt{3}}{2}$. On constate alors que dans $\mathbf{Q}(\alpha)$, on a $\alpha^3 = -i\sqrt{3}$ de sorte que $\zeta = \frac{1-\alpha^3}{2} \in \mathbf{Q}(\alpha)$. On en déduit que le corps de décomposition de P est donné par $\mathbf{Q}(\alpha)$ (un corps de rupture de P). On en déduit que le groupe de Galois G est d'ordre 6. On sait donc que ce groupe est isomorphe à $\mathbf{Z}/6\mathbf{Z}$ si G est abélien et $\mathfrak{S}_3$ sinon. Or, on constate que $\alpha^2 = -\sqrt[3]{3}$ est dans $K = \mathbf{Q}(\alpha)$ mais que cette extension de $\mathbf{Q}$ n'est pas galoisienne (car le polynôme $X^3 - 3$ y admet une racine sans y être scindé). Cela implique que le groupe de Galois est non abélien et par conséquent que le groupe de Galois est isomorphe à $\mathfrak{S}_3$. On pouvait aussi raisonner "à la main" ici. Un élément d'ordre 2 est donné par la conjugaison complexe et un élément d'ordre 3 par un générateur de $H = \mathrm{Gal}(K/\mathbf{Q}(\zeta))$ avec $\mathbf{Q}(\zeta)$ d'ordre $\varphi(6) = 2$. Noter que l'action d'un tel élément $\sigma \in H$ doit vérifier que $\sigma(\alpha) = \zeta^k\alpha$ pour $k \in \{0, \dots, 5\}$ mais comme $\alpha^3 \in \mathbf{Q}(\zeta)$, on a $\sigma(\alpha^3) = \alpha^3$ ce qui laisse uniquement trois valeurs possibles pour $k \in \{0, 2, 4\}$.

7. Vérifions que le polynôme est irréductible. Pour ce faire, on calcule[18]

$$-1024X^5 + 2816X^4 - 2816X^3 + 1232X^2 - 220X + 11$$

et on obtient l'irréductibilité via Eisenstein avec $p = 11$. Le polynôme est ainsi irréductible et séparable sur $\mathbf{Q}$. Par ailleurs, les formules de duplication[19] permettent de voir que le corps de décomposition est donné par $K = \mathbf{Q}(x)$ pour $x = \cos\left(\frac{2\pi}{11}\right)$ et galoisien d'ordre 5. On constate alors que si on note ζ une racine 11-ème primitive de l'unité, on a $x = \frac{\zeta+\zeta^{-1}}{2}$ de sorte que $K \subseteq \mathbf{Q}(\zeta)$. Or, on sait que $\mathbf{Q}(\zeta)$ est une extension galoisienne de groupe de Galois isomorphe à $(\mathbf{Z}/11\mathbf{Z})^\times \cong \mathbf{Z}/10\mathbf{Z}$. On a donc que le groupe de Galois de K est isomorphe au quotient de $\mathbf{Z}/10\mathbf{Z}$ par son unique (car le groupe est cyclique) sous-groupe d'indice 5. On a donc que le groupe de Galois de K est isomorphe à $\mathbf{Z}/5\mathbf{Z}$.

Exercice 10. Soient n un entier naturel non nul et $p_1, \dots, p_n$ des nombres premiers 2 à 2 distincts. On pose $K = \mathbf{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$.

1. Montrer que l'extension $K/\mathbf{Q}$ est galoisienne. On notera G son groupe de Galois.

2. Montrer que tout élément de G est d'ordre 2 et en déduire que $G \cong (\mathbf{Z}/2\mathbf{Z})^r$ pour un certain entier r.

3. Exprimer le nombre de sous-extensions de $\mathbf{Q}$ de K de degré 2 sur $\mathbf{Q}$.

4. Montrer que $G \cong (\mathbf{Z}/2\mathbf{Z})^n$.

Solution.

16. On aurait obtenu une double transposition si on avait eu quatre racines complexes conjuguées deux à deux. Cela n'aurait pas permis de conclure puisque $\mathfrak{S}_5$ contient une copie du groupe diédral $\mathbf{D}_{10}$ engendré par un 5-cycle et une double transposition ou parce que ces éléments sont contenus dans $\mathfrak{A}_5$.

17. Noter que si n est premier, alors $\mathfrak{S}_n$ est engendré par n'importe quelle transposition et n'importe quel n-cycle (voir `https://kconrad.math.uconn.edu/blurbs/grouptheory/genset.pdf`) mais que ce résultat est faux pour n quelconque. En revanche, par exemple, pour tout n, $\mathfrak{S}_n$ est engendré par (12) et $(12\cdots n)$ (voir par exemple le Perrin pour cela).

18. Voir ici pour une intuition concernant les polynômes minimaux de $\cos\left(\frac{2\pi}{p}\right)$ et $\sin\left(\frac{2\pi}{p}\right)$.

19. Du type $\cos(2\theta) = 2\cos^2(\theta) - 1$.

1. Il s'agit du corps de décomposition du polynôme (séparable car en caractéristique nulle) $(X^2-p_1)\cdots(X^2-p_n)$. L'extension est donc galoisienne.
2. Soit $g \in G$. On a que $\sqrt{p_i}$ annule X^2-p_i de sorte que $g(\sqrt{p_i}) = \pm\sqrt{p_i}$ et donc $g^2 = \mathrm{Id}$ puisque $\sqrt{p_1},\dots,\sqrt{p_n}$ engendrent K. On a vu dans le TD 1 que cela impliquait que G est abélien et qu'il existe un entier m tel que $G = (\mathbf{Z}/2\mathbf{Z})^m$. Noter que puisque $g(\sqrt{p_i}) = \pm\sqrt{p_i}$ pour tout $i \in \{1,\dots,n\}$, on a au plus 2^n automorphismes et donc $m \leqslant n$.
3. Une sous-extension de degré 2 correspond par correspondance de Galois à un sous-groupe d'indice 2, soit aux noyaux de morphismes de groupes surjectifs $G \cong (\mathbf{Z}/2\mathbf{Z})^m \to \mathbf{Z}/2\mathbf{Z}$. Ces morphismes correspondent aux formes $\mathbf{F}_2$-linéaires non nulles, et on en a 2^m-1.
4. Soit I une partie non vide de $\{1,\dots,n\}$ (noter qu'on en a 2^n-1). Montrons alors que si l'on note
$$p_I = \prod_{i\in I} p_i$$
alors les $\mathbf{Q}(\sqrt{p_I})$ constituent des sous-extensions de degré 2 distinctes. Il s'ensuivra que $2^n-1 \leqslant 2^m-1$ et $n \leqslant m$ soit $n=m$. Mais si l'on avait $\sqrt{p_I} = x + y\sqrt{p_J}$ avec $x=a/c$ et $y=b/c$ deux rationnels. On a donc $p_Ic^2 = a^2 + 2ab\sqrt{p_J} + b^2p_J$ mais on ne peut pas avoir $b=0$ sinon $\sqrt{p_I}$ est rationnel. On a donc $2ab=0$ (puisque $(1,\sqrt{p_J})$ est $\mathbf{Q}$-libre) qui implique que $a=0$ et $p_Ic^2 = b^2p_J$. Par unicité de la décomposition en produit de facteurs premiers, il vient $I=J$. On a donc le résultat.
On peut alors traiter la question de savoir si $\sqrt{15} \in \mathbf{Q}(\sqrt{10},\sqrt{42})$ qui est de degré 4 de groupe de Galois $(\mathbf{Z}/2\mathbf{Z})^2$. Elle possède 3 sous-extensions de degré 2 données par $\mathbf{Q}(\sqrt{10})$, $\mathbf{Q}(\sqrt{42})$ et $\mathbf{Q}(\sqrt{420})$. On montre alors comme ci-dessus que $\sqrt{15}$ n'appartient à aucune de ces dernières si bien que $\mathbf{Q}(\sqrt{15})$ n'est pas une sous-extension de $\mathbf{Q}(\sqrt{10},\sqrt{42})$ et $\sqrt{15} \notin \mathbf{Q}(\sqrt{10},\sqrt{42})$.

Exercice 11 — Groupes de Galois en petit degré. Soit k un corps de caractéristique différente de 2, et soit $P \in k[X]$ un polynôme irréductible séparable de degré n. Soit L un corps de décomposition de P sur k, et soient $r_1,\dots,r_n$ les racines de P dans L. On rappelle que le discriminant de P est un élément de k qui peut être défini par
$$\Delta_P = \prod_{i<j}(r_i-r_j)^2.$$
On notera $G = \mathrm{Gal}_k(P) = \mathrm{Gal}(L/k)$ le groupe de Galois de P. On rappelle que pour tous $a,b \in \mathbf{Z}$, on a $\Delta_{X^3+aX+b} = -4a^3-27b^2$.

1. Rappeler pourquoi on peut voir G comme un sous-groupe transitif de $\mathfrak{S}_n$ et traiter le cas $n=2$.
2. Soit $d = \prod_{i<j}(r_i-r_j) \in L$. Montrer que l'extension $k(d)/k$ est galoisienne de degré 1 ou 2.
3. Montrer qu'un élément σ de $\mathrm{Gal}_k(P)$ fixe d si, et seulement si, $\sigma \in \mathrm{Gal}_k(P) \cap \mathfrak{A}_n$. En déduire que $k(d)$ est l'extension de k correspondant au sous-groupe $\mathrm{Gal}_k(P)\cap\mathfrak{A}_n$ de $\mathrm{Gal}_k(P)$.
4. Soit k un entier et $a = k^2+k+7$. Montrer que X^3-aX+a est irréductible sur $\mathbf{Q}$ et déterminer son groupe de Galois.
5. Montrer que si P est irréductible séparable de degré 3, alors si r est racine de P, alors $L = k(r,\sqrt{\Delta_P})$. Conclure le cas $n=3$.

À présent, on suppose que P est irréductible séparable unitaire de degré $n=4$.

6. Lister les sous-groupes transitifs de $\mathfrak{S}_4$.
7. On introduit la résolvante cubique $R_3(X)$ de $P(X) = X^4+aX^3+bX^2+cX+d$, définie par
$$R_3(X) = (X-(r_1r_2+r_3r_4))(X-(r_1r_3+r_2r_4))(X-(r_1r_4+r_2r_3)) = X^3-bX^2+(ac-4d)X-(a^2d+c^2-4bd).$$
Montrer que $\Delta_P = \Delta_{R_3}$ et que R_3 est séparable. Décrire G dans les cas suivants :
   - Δ_P n'est pas un carré et R_3 est irréductible ;
   - Δ_P n'est pas un carré et R_3 est scindé ;
   - Δ_P n'est pas un carré et R_3 est réductible non scindé ;
   - Δ_P est un carré et R_3 est irréductible ;
   - Δ_P est un carré et R_3 est réductible.
8. Dans le cas de $\mathbf{Q}$, montrer que si G est isomorphe à $\mathbf{Z}/4\mathbf{Z}$, alors $\Delta_P > 0$ tandis que si le groupe de Galois est isomorphe à $\mathbf{D}_4$, alors $\Delta_P < 0$.
9. On suppose ici que Δ_P n'est pas un carré dans k et que R_3 est réductible sur k. Montrer que le groupe G est isomorphe à $\mathbf{Z}/4\mathbf{Z}$ si, et seulement si, P est irréductible sur $k(\sqrt{\Delta_P})$ et diédral si, et seulement si, P est réductible sur $k(\sqrt{\Delta_P})$.
10. Étudier les cas particuliers de X^4+bX^2+d avec b,d entiers et $k=\mathbf{Q}$ ainsi que X^4-X-1.

Solution. Je vous renvoie au corrigé du problème 2 du sujet de DM disponible sur la page web du cours !

Exercices complémentaires de la semaine 2

Exercice 12 — Problème de Galois inverse.

1. Soit G un groupe fini. Montrer qu'on peut trouver une extension de corps galoisienne L/K telle que $\mathrm{Gal}(L/K) \cong G$.

Soient p un nombre premier impair et m un entier naturel non nul. Soit $(n_1, \dots, n_{p-2})$ un $p-2$-uplet d'entiers relatifs distincts. On pose alors

$$f(X) = (X^2 + m) \prod_{i=1}^{p-2} (X - n_i).$$

2. Montrer que pour tout réel ε de valeur absolue assez petite, $f(X) + \varepsilon \in \mathbf{R}[X]$ admet $p-2$ racines réelles simples et deux racines complexes conjuguées.
3. Pour tout nombre premier ℓ, on considère le polynôme

$$P_\ell = \ell^p f\left(\frac{X}{\ell}\right) + \ell.$$

Montrer que pour ℓ assez grand, $P_\ell \in \mathbf{Q}[X]$ est irréductible et admet $p-2$ racines réelles simples et deux racines complexes conjuguées. Préciser le groupe de Galois de P_ℓ.

4. Soit G un groupe fini. Montrer qu'il existe une extension finie galoisienne K/L telle que $\mathrm{Gal}(L/K) \cong G$ avec K une extension finie de $\mathbf{Q}$.
5. En considérant une extension cyclotomique et en admettant le fait que pour tout n, il existe un nombre premier $p \equiv 1 \pmod{n}$, montrer que si G est abélien fini, alors il existe une extension galoisienne de $\mathbf{Q}$ de groupe de Galois G.

Solution.

1. On pose $n = \#G$. On sait, par le théorème de Cayley, que G s'identifie à un sous-groupe de $\mathfrak{S}_n$. On a alors que G agit par permutation des variables sur le corps $\mathbf{C}(X_1, \dots, X_n)$. D'après le théorème d'Artin (voir ici, Proposiiton 4.23) que l'extension

$$\mathbf{C}(X_1, \dots, X_n)/\mathbf{C}(X_1, \dots, X_n)^G$$

est galoisienne de groupe de Galois G.
On peut en fait montrer qu'il existe une extension finie K de $\mathbf{Q}$ et L une extension finie de K galoisienne sur K telle que le groupe de Galois de L sur K soit isomorphe à G. Il suffit pour cela de réaliser $\mathfrak{S}_n$ comme groupe de Galois sur $\mathbf{Q}$ et d'utiliser la correspondance de Galois. Or, on peut montrer (voir ici) que $x^n - x - 1$ est irréductible et admet comme groupe de Galois $\mathfrak{S}_n$.

2. Supposons que $n_1 < \cdots < n_{p-2}$ sont les racines réelles de f ordonnées par ordre croissant. On sait alors que si $\varepsilon < \sup_{[n_i, n_{i+1}]} |f|$ pour tout $i \in \{1, \dots, p-1\}$, alors $\varepsilon > 0$. Par ailleurs, puisque f tend vers $-\infty$ en $-\infty$ (caf f est de degré p impair), il vient que $f + \varepsilon$ s'annule sur $]-\infty, n_1[$ par le théorème des valeurs intermédiaires. De même, on obtient deux racines sur $]n_2, n_3[$. De proche en proche, on obtient $p-2$ racines réelles. Pour traiter les racines complexes non réelles, on peut par exemple faire appel au théorème de Rouché (qui découle du théorème des résidus). Soit z une racine de f complexe non réelle et on fixe une boule centrée en z de rayon ε assez petit pour qu'elle n'intersecte pas l'axe réel. On sait alors par le théorème de Rouché que le nombre de zéros de f et de $f + \varepsilon$ dans cette boule sont les même, autrement dit $f + \varepsilon$ admet aussi une racine complexe non réelle dans cette boule. Cela implique bien l'existence de deux racines complexes conjuguées et on a la résultat.
3. Pour tout nombre premier ℓ, le polynôme P_ℓ est irréductible par Eisenstein. Par ailleurs, par la question précédente, pour ℓ assez grand, $f(X) + \frac{1}{\ell^{p-1}} = P_\ell(\ell X)/\ell^p$ a $p-2$ racines réelles simples et deux racines complexes conjuguées. Il en est donc de même pour P_ℓ. On obtient alors une transposition dans le groupe de Galois vu comme sous-groupe transitif de $\mathfrak{S}_p$ et un p-cycle de sorte que ce groupe de Galois est isomorphe à $\mathfrak{S}_p$ (on raisonne comme dans l'exercice 9, question **5.**).
4. On identifie G à un sous-groupe de $\mathfrak{S}_n$ avec $n = \#G$ et on plonge $\mathfrak{S}_n$ dans $\mathfrak{S}_p$ avec $p \geqslant n$ premier et on conclut par correspondance de Galois.
5. Soit G abélien fini. Par le théorème de structure, on sait que

$$G \cong \prod_{i=1}^{r} \mathbf{Z}/n_i\mathbf{Z}, \quad \text{avec} \quad n_1 \mid n_2 \mid \cdots \mid n_r.$$

Par Dirichlet faible (voir l'exercice 19), il existe des premiers $p_i \equiv 1 \pmod{n_i}$ deux à deux distincts. Posons alors $m = \prod_{i=1}^{r} p_i$ et considérons ζ une racine primitive m-ème de l'unité dans $\mathbf{C}$. L'extension cyclotomique $\mathbf{Q}(\zeta)/\mathbf{Q}$ est galoisienne de groupe de Galois isomorphe à

$$(\mathbf{Z}/m\mathbf{Z})^\times \cong \prod_{i=1}^{r} \mathbf{Z}/(p_i - 1)\mathbf{Z}.$$

Il suffit alors de considérer le sous-groupe H donné par

$$\prod_{i=1}^{r} n_i\mathbf{Z}/(p_i-1)\mathbf{Z}$$

et le corps $K=\mathbf{Q}(\zeta)^H$ qui est une extension galoisienne (car le groupe de Galois est ici abélien) de $\mathbf{Q}$ de groupe de Galois isomorphe à

$$(\mathbf{Z}/m\mathbf{Z})^\times/H \cong \prod_{i=1}^{r}\mathbf{Z}/n_i\mathbf{Z} \cong G.$$

Exercice 13. Soient $\mathbf{C}(t)$ le corps des fractions rationnelles à coefficients dans $\mathbf{C}$, et $K=\mathbf{C}(t)[u]/(u^2+t^2-1)$.

1. Montrer que K est un corps, que l'on notera $\mathbf{C}(t,u)$.
2. Montrer que l'extension $\mathbf{C}(t,u)$ de $\mathbf{C}(t^n,u^n)$ est galoisienne, et calculer son groupe de Galois.
3. Montrer que l'élément $u_n=\frac{1}{2}((t+iu)^n+(t-iu)^n)$ est dans $\mathbf{C}(t^n,u^n)$, pour tout entier strictement positif n.
4. Utiliser les questions précédentes pour montrer que $\cos(nx)$ s'exprime comme fonction rationnelle de $\cos^n(x)$ et $\sin^n(x)$.

Solution.

1. Le polynôme $P(u)=u^2+t^2-1$ est irréductible dans $\mathbf{C}(t)[u]$ car t^2-1 n'est pas un carré dans $\mathbf{C}(t)$ (ou par Eisenstein avec $p=t-1$). Donc l'idéal engendré par P dans $\mathbf{C}(t)[u]$ est maximal et donc K est un corps.
2. L'extension est galoisienne car $\mathbf{C}(t,u)$ est un corps de décomposition de $(X^n-t^n)(X^n-u^n)\in\mathbf{C}(t^n,u^n)[X]$. Calculons son groupe de Galois que nous notons G. Tout élément σ de G fixe $\mathbf{C}(t^n,u^n)$ donc $\sigma(t^n)=t^n$ et $\sigma(u^n)=u^n$. Ceci implique qu'il existe deux racines n-ièmes de l'unité ξ et μ telles que $\sigma(t)=\xi t$ et $\sigma(u)=\mu u$. Or $t^2+u^2=1$ donc $\sigma(1)=(\sigma(t))^2+(\sigma(u))^2=\xi^2t^2+\mu^2-\mu^2t^2=1$ (car σ est un automorphisme de $\mathbf{C}(t,u)$. On a alors
$$(\xi^2-\mu^2)t^2+\mu^2=1;$$
comme t est transcendant sur $\mathbf{C}$, ceci implique que $\xi^2=\mu^2$ et $\mu^2=1$. Comme ξ et μ sont des racines n-ièmes de l'unité, on distingue deux cas :
   - si n est impair alors $\xi^2=\mu=1$ implique $\xi=1$ et $\mu=1$, donc $\sigma(t)=t$ et $\sigma(\mu)=\mu$ donc $\sigma=id$. Dans ce cas $G=\{1\}$ et $\mathbf{C}(t,u)=\mathbf{C}(t^n,u^n)$.
   - si n est pair alors $\xi^2=\mu=1$ implique $\xi=\pm1$ et $\mu=\pm1$. Donc on a quatre choix possibles pour l'action de σ et donc l'ordre de G est inférieur ou égal à 4. De plus, on a la tour d'extension suivante :
   $$\mathbf{C}(t^n,u^n)\to\mathbf{C}(t^2,u^2)=\mathbf{C}(t^2)\to\mathbf{C}(t)\to\mathbf{C}(t,u)$$
   car $u^2=1-t^2$; on a aussi $[\mathbf{C}(t,u):\mathbf{C}(t)]=2$ car $\mathbf{C}(t,u)=\mathbf{C}(t)(u)$ et $u^2+(1-t^2)=0$ et le polynôme minimal de u dans $\mathbf{C}(t)$ est $X^2+(1-t^2)$. Donc [20],
   $$[\mathbf{C}(t,u):\mathbf{C}(t^n,u^n)]=[\mathbf{C}(t,u):\mathbf{C}(t)][\mathbf{C}(t):\mathbf{C}(t^2)][\mathbf{C}(t^2,u^2):\mathbf{C}(t^n,u^n)]\geqslant 4$$
   donc l'ordre de G est égal à 4 et $G=\{1,\alpha,\beta,\alpha\beta\}$ où $\alpha(t)=-t$, $\alpha(u)=u$, $\beta(t)=t$ et $\beta(u)=-u$.
3. On a $[\mathbf{C}(t,u):\mathbf{C}(t^n,u^n)]$ est égal à 1 ou 4 en fonction de la parité de n. Si n est impair, ce degré est égal à 1 donc $u_n\in\mathbf{C}(t^n,u^n)=\mathbf{C}(t,u)$. Si n est pair, montrons que $\sigma(u_n)=u_n$ pour tout $\sigma\in G$. Il suffit de montrer qu'il est fixé par α et β. Or, $\alpha(u_n)=\frac{1}{2}((-t+iu)^n+(-t-iu)^n)=u_n$ et $\beta(u_n)=\frac{1}{2}((t-iu)^n+(t+iu)^n)=u_n$.
4. Fixons $(z_1,z_2)\in\mathbf{C}^2$ tels que $z_1^2+z_2^2=1$. On vérifie alors que le morphisme d'évaluation $\mathbf{C}(t)[u]\to\mathbf{C}$ donné par $P\mapsto P(z_1,z_2)$ contient (t^2+u^2-1) et donc lui est égal car cet idéal est maximal. Il s'ensuit une injection $\mathbf{C}(t)[u]/(u^2+t^2-1)\to\mathbf{C}$ qui permet d'évaluer un élément de $\mathbf{C}(t)[u]/(u^2+t^2-1)$. La question précédente fournit qu'on a une égalité du type [21]
   $$u_nQ(t^n,u^n)=P(t^n,u^n)\quad\text{avec}\quad P,Q\in\mathbf{C}(X)[Y]\quad\text{premiers entre eux.}$$
   On a aussi que $Q(t^n,u^n)\neq0$ et donc si on avait $Q(\cos(x)^n,\sin(x)^n)=0$, alors par injectivité de notre morphisme d'évaluation, on obtiendrait $Q(t^n,u^n)=0$ ce qui est exclu. On a donc le résultat. A priori, la fraction rationnelle est à coefficients dans $\mathbf{C}$ mais on peut se ramener à $\mathbf{R}$ en prenant une partie réelle.
   Noter qu'on sait que $\cos(nx)$ est un polynôme en $\cos(x)$ et $\sin(x)$ mais ici la différence est que l'on s'autorise uniquement les puissances n-ièmes. Noter également que $\cos(x)$ n'est jamais transcendant sur $\mathbf{C}$ (où par définition tout élément est algébrique)!

Exercice 14 — Artin-Schreier. Soit K un corps de caractéristique $p\neq0$.

20. Car $\mathbf{C}(t^2)$ est strictement inférieure à $\mathbf{C}(t)$ car t est transcendant.
21. On est obligé d'en passer par là pour éviter des problèmes d'évaluation en des points où les fractions rationnelles ne sont pas définies.

1. Soit a un élément de K qui ne peut pas s'écrire comme $b^p - b$, avec $b \in K$. Trouver le groupe de Galois du polynôme $X^p - X - a$.
2. Soient L/K une extension galoisienne de degré p et σ un générateur de $\mathrm{Gal}(L/K)$. Montrer qu'il existe $x \in L$ tel que $\sigma(x) - x = 1$. En déduire qu'il existe $a \in K^\times$ tel que L soit le corps de décomposition de $X^p - X - a$.

Solution.

1. Soit a un élément de K qui ne peut pas s'écrire comme $b^p - b$, avec $b \in K$. L'hypothèse garantit que le polynôme $X^p - X - a$ n'admet pas de racine sur K. On a alors qu'il est irréductible. En effet, si L est un corps de décomposition et $\alpha \in L$ une racine, alors $\alpha + i$ est encore une racine pour tout $i \in \{0, \dots, p-1\}$ car on est en caractéristique p et car $i^p - i = 0$. Si P était réductible, on aurait alors $P = QR$ avec Q, R de degré $< p$. On aurait alors dans K

$$Q = \prod_{k=1}^{d} (X - \alpha - i_k).$$

Le coefficient en X^{d-1} vaut $-(d\alpha + i_1 + \cdots + i_d) \in K$ et on aurait $\alpha \in K$ car $d < p$. On montre alors sans peine que le groupe de Galois est donné par $\mathbf{Z}/p\mathbf{Z}$ puisque tout $\sigma \in \mathrm{Gal}(L/K)$ (qui est bien galoisienne comme corps de décomposition d'un polynôme séparable [22]) vérifie $\sigma(\alpha) = \alpha + i_\sigma$ avec $i_\sigma \in \mathbf{F}_p$.

2. On a $\mathrm{Ker}(\sigma - \mathrm{Id}) = K$ et en tant qu'application K-linéaire, $\sigma - \mathrm{Id}$ est donc de rang $p-1$. Par ailleurs, σ est d'ordre p donc $(\mathrm{Id} + \sigma + \cdots + \sigma^{p-1}) \circ (\sigma - \mathrm{Id}) = 0$ d'où $\mathrm{Im}(\sigma - \mathrm{Id}) \subseteq \mathrm{Ker}(\mathrm{Id} + \sigma + \cdots + \sigma^{p-1})$. Par indépendance linéaire des caractères (voir par exemple la question 7 du problème 2 du DM II), on a que $\mathrm{Id} + \sigma + \cdots + \sigma^{p-1}$ est non identiquement nulle sur L et donc $\mathrm{Im}(\sigma - \mathrm{Id}) = \mathrm{Ker}(\mathrm{Id} + \sigma + \cdots + \sigma^{p-1})$ et $K \subseteq \mathrm{Ker}(\mathrm{Id} + \sigma + \cdots + \sigma^{p-1})$ ce qui permet de conclure.
On considère alors $x \in L$ tel que $\sigma(x) - x = 1$. Le polynôme minimal de x sur K est alors

$$\prod_{i=0}^{p-1} (X - \sigma^i(x)) = \prod_{i=0}^{p-1} (X - x - i) = X^p - X - (x^p - x)$$

et $a = x^p - x$ convient. Noter que la dernière égalité vient du fait que

$$\prod_{i=0}^{p-1} (X - x - i) \quad \text{et} \quad (X - x)^p - (X - x)$$

sont deux polynômes unitaires de même degré ayant les mêmes racines.

Exercices fondamentaux de la semaine 3

Exercice 15 — Quaternions. Soient $\alpha = (2 + \sqrt{2})(3 + \sqrt{6})$ et $K = \mathbf{Q}(\alpha)$ ainsi que $\delta = \sqrt{\alpha}$ et $L = \mathbf{Q}(\delta)$.

1. Montrer que l'extension $K/\mathbf{Q}$ est galoisienne de groupe de Galois $(\mathbf{Z}/2\mathbf{Z})^2$. On notera $\sigma_i, \sigma_j, \sigma_k$ les éléments distincts de l'identité.
2. Montrer que pour tout $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$, le quotient $\frac{\sigma(\alpha)}{\alpha}$ est un carré dans K.
3. Montrer que $\delta \notin K$ et en déduire $\mathrm{Gal}(L/K)$. On en note τ un générateur, que l'on considérera aussi comme un élément de $\mathrm{Gal}(L/\mathbf{Q})$.
4. Définir des automorphismes $\tilde{\sigma}_i$ et $\tilde{\sigma}_j$ de L sur $\mathbf{Q}$ qui prolongent σ_i et σ_j respectivement. On pose alors $\tilde{\sigma_k} = \tilde{\sigma}_i \tilde{\sigma}_j$.
5. Montrer que le groupe de Galois de $L/\mathbf{Q}$ est isomorphe au groupe des quaternions. Combien le corps L possède-t-il de sous-corps quadratiques ?

Solution.

1. Soit $M = \mathbf{Q}(\sqrt{2}, \sqrt{3})$ qui est galoisienne de degré 4 et de groupe de Galois isomorphe à $(\mathbf{Z}/2\mathbf{Z})^2$ d'éléments distincts de l'identité $\sigma_i, \sigma_j, \sigma_k$ définis par

$$\sigma_i : \begin{cases} \sqrt{2} & \mapsto & -\sqrt{2} \\ \sqrt{3} & \mapsto & \sqrt{3} \end{cases}, \quad \sigma_j : \begin{cases} \sqrt{2} & \mapsto & \sqrt{2} \\ \sqrt{3} & \mapsto & -\sqrt{3} \end{cases}, \quad \sigma_k : \begin{cases} \sqrt{2} & \mapsto & -\sqrt{2} \\ \sqrt{3} & \mapsto & -\sqrt{3}. \end{cases}$$

On vérifie alors que $\sigma_i(\alpha) \neq \alpha$, $\sigma_j(\alpha) \neq \alpha$ et $\sigma_k(\alpha) \neq \alpha$ ce qui montre que $K = M$ et fournit le résultat.

2. On calcule avec les notations de la question précédente

$$\frac{\sigma_k(\alpha)}{\alpha} = \left(\sqrt{2} - 1\right)^2, \quad \frac{\sigma_j(\alpha)}{\alpha} = \left(\sqrt{3} - \sqrt{2}\right)^2, \quad \frac{\sigma_i(\alpha)}{\alpha} = \left(2 - \sqrt{2} - \sqrt{3} + \sqrt{6}\right)^2.$$

22. Ici on a toutes les racines et elles sont bien simples ! On ne peut pas faire appel à la caractéristique nulle.

3. Supposons que $\delta \in K$. Alors σ_k est bien défini sur $L = K$ et on a $\frac{\sigma_k(\delta)}{\delta} = \pm(\sqrt{2}-1)$. Par ailleurs,

$$1 = \frac{\sigma_k^2(\delta)}{\sigma_k(\delta)} \frac{\sigma_k(\delta)}{\delta}$$

puisque δ_k est d'ordre 2. On a par ailleurs, par définition de δ_k que

$$\frac{\sigma_k^2(\delta)}{\sigma_k(\delta)} \frac{\sigma_k(\delta)}{\delta} = (-\sqrt{2}-1)(\sqrt{2}-1) = -1$$

ce qui est une contradiction !

4. On pose simplement

$$\tilde{\sigma}_i(\delta) = (-2+\sqrt{2}-\sqrt{3}+\sqrt{6})\delta, \quad \tilde{\sigma}_j(\delta) = (\sqrt{3}-\sqrt{2})\delta.$$

Ces morphismes sont bien définis puisque le polynôme minimal de δ sur K est $X^2 - \alpha$ et on a besoin (et cela suffit) que $\tilde{\sigma}_i(\delta)$ soit un zéro de $X^2 - \sigma_j(\alpha)$ soit de $X^2 - (\sqrt{3}-\sqrt{2})^2\alpha$.

5. Il suffit de vérifier les relations entre $\tilde{\sigma}_i$, $\tilde{\sigma}_j$ et $\tilde{\sigma}_k$ en δ pour conclure. Par exemple, on a

$$\tilde{\sigma}_i^2(\delta) = -\delta = \tau(\delta) = \tilde{\sigma}_j^2(\delta) = \tilde{\sigma}_k^2(\delta).$$

On a autant de sous-extensions quadratiques que de sous-groupes d'ordre 4 des quaternions, autrement dit on en a 3 (voir le TD 1 pour une étude plus détaillée du groupe des quaternions) ! Il s'agit bien évidemment de $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{3})$ et $\mathbf{Q}(\sqrt{6})$.

Exercice 16 — $\mathbf{C}$ est algébriquement clos.

1. Rappeler pourquoi tout polynôme de $\mathbf{R}[X]$ de degré impair admet une racine réelle.

Soit K une extension finie de $\mathbf{R}(i)$.

2. Montrer que K est contenue dans une extension L, galoisienne sur $\mathbf{R}$. On note G le groupe de Galois de $L/\mathbf{R}$, S un 2-Sylow de G et $F = L^S$.
3. Montrer que F est de degré impair et de la forme $\mathbf{R}(\alpha)$ avec α racine d'un polynôme de $\mathbf{R}[X]$ de degré impair irréductible. En déduire que $G = S$.
4. On pose $G_1 = \mathrm{Gal}(L/\mathbf{R}(i))$ et on suppose que G_1 n'est pas trivial. Justifier que G_1 admet alors un sous-groupe H_1 d'indice 2. En considérant, $M = L^{H_1}$, aboutir à une contradiction. Conclure que $K = \mathbf{R}(i)$ puis que $\mathbf{C}$ est algébriquement clos.

Solution.

1. Il s'agit d'une application immédiate du théorème des valeurs intermédiaires.
2. On a que $K = \mathbf{R}(\alpha_1, \ldots, \alpha_n)$ avec les α_i algébriques. Il suffit alors de prendre un corps de décomposition du ppcm des polynômes minimaux.
3. Le degré de F est l'indice de S dans G, qui est impair par définition d'un 2-Sylow. Par le théorème de l'élément primitif, on a $\mathbf{R}(\alpha)$ avec α racine d'un polynôme de $\mathbf{R}[X]$ de degré impair irréductible (le polynôme minimal de α). On a vu qu'un tel polynôme admet une racine réelle et ne peut donc pas être irréductible sauf s'il est de degré 1. On a donc $[F = \mathbf{R}(\alpha) : \mathbf{R}] = 1$ et par correspondance de Galois, $G = S$ est un 2-groupe.
4. On a que $G_1 = \mathrm{Gal}(L/\mathbf{R}(i))$ est un 2-groupe non trivial. Par le TD 1, il admet alors un sous-groupe H_1 d'indice 2 (un p-groupe admet des sous-groupes distingués de tout ordre). L'extension $M = L^{H_1}$ est alors une extension quadratique de $\mathbf{R}(i)$. Mais, tout polynôme de degré 2 est scindé sur $\mathbf{R}(i)$ et donc $\mathbf{R}(i)$ n'admet aucune extension de degré 2 (une telle extension est nécessairement le corps de rupture ou de décomposition d'un polynôme irréductible de degré 2). On en déduit que G_1 est trivial soit que $L = K = \mathbf{R}(i)$. Soit P un polynôme irréductible de $\mathbb{C} = \mathbf{R}(i)$. Si P était de degré au moins 2, on aurait en prenant un corps de rupture une extension finie de $\mathbb{R}(i)$ de degré au moins 2 ce qui est absurde. On en déduit que P est de degré 1 et donc que $\mathbb{C} = \mathbb{R}(i)$ est algébriquement clos.

Exercice 17 — Cyclotomie. Pour tout entier naturel n non nul, on note Φ_n le n-ème polynôme cyclotomique défini par

$$\Phi_n(X) = \prod_{\zeta} (X - \zeta)$$

où le produit porte sur les racines primitives n-ème de l'unité. On notera également $\zeta_n = e^{\frac{2i\pi}{n}}$ ainsi que φ la fonction indicatrice d'Euler.

1. Soit ζ une racine primitive n-ème de l'unité. Montrer que $\mathbf{Q}(\zeta)/\mathbf{Q}$ est une extension galoisienne de degré $\varphi(n)$ et montrer que son groupe de Galois est isomorphe au groupe des inversibles de l'anneau $\mathbf{Z}/n\mathbf{Z}$.
2. Montrer que pour m et n premier entre eux, $\mathbf{Q}(\zeta_n, \zeta_m) = \mathbf{Q}(\zeta_{mn})$ et que $\mathbf{Q}(\zeta_n) \cap \mathbf{Q}(\zeta_m) = \mathbf{Q}$.
3. Montrer que Φ_n est irréductible sur $\mathbf{Q}$ et sur $\mathbf{Q}(\zeta_m)$.

4. Pour n un entier non nul, préciser combien d'extensions quadratiques de $\mathbf{Q}$ sont contenues dans $\mathbf{Q}(\zeta_n)$. Vérifier qu'on en obtient 7 pour $n = 60$.
5. Soit p un nombre premier impair. Calculer le discriminant de Φ_p et en déduire que l'unique extension quadratique de $\mathbf{Q}$ contenue dans $\mathbf{Q}(\zeta_p)$ est $\mathbf{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right)$.
6. Préciser les extensions quadratiques de $\mathbf{Q}$ qui sont contenues dans $\mathbf{Q}(\zeta_8)$ puis en déduire la liste de celles contenues dans $\mathbf{Q}(\zeta_{60})$.
7. Montrer que toute extension quadratique de $\mathbf{Q}$ est contenue dans une extension cyclotomique de $\mathbf{Q}$.

Solution.

1. Je vous renvoie pour cela ici, exemple 4.31.
2. Puisque m et n sont premiers entre eux, on a deux entiers u et v tels que $mu + nv = 1$. On a alors $\zeta_{mn}^n = \zeta_m$ et $\zeta_{mn}^m = \zeta_n$ de sorte que $\mathbf{Q}(\zeta_n, \zeta_m) \subseteq \mathbf{Q}(\zeta_{mn})$. Réciproquement, on a
$$\zeta_{mn} = e^{\frac{2i\pi}{mn}} = e^{\frac{2i\pi(mu+nv)}{mn}} = \zeta_n^u \zeta_m^v$$
ce qui montre bien l'égalité.
3. On a alors
$$\varphi(mn) = [\mathbf{Q}(\zeta_{mn}) : \mathbf{Q}] = [\mathbf{Q}(\zeta_m)(\zeta_n) : \mathbf{Q}(\zeta_m)][\mathbf{Q}(\zeta_m) : \mathbf{Q}] = \varphi(m)[\mathbf{Q}(\zeta_m)(\zeta_n) : \mathbf{Q}(\zeta_m)].$$
Or, comme m et n sont premiers entre eux, $\varphi(mn) = \varphi(m)\varphi(n)$ de sorte que $[\mathbf{Q}(\zeta_m)(\zeta_n) : \mathbf{Q}(\zeta_m)] = \varphi(n)$. Il s'ensuit que Φ_n annule ζ_n sur $\mathbf{Q}$ et donc sur $\mathbf{Q}(\zeta_m)$ et est unitaire de degré $\varphi(n)$. Il est donc nécessairement irréductible et le polynôme minimal de ζ_n sur $\mathbf{Q}(\zeta_m)$ et donc sur $\mathbf{Q}$.
4. De telles extensions correspondent aux sous-groupes d'indice 2 de $(\mathbf{Z}/n\mathbf{Z})^\times$ soit aux morphismes non triviaux de $(\mathbf{Z}/n\mathbf{Z})^\times$ dans $\mathbf{Z}/2\mathbf{Z}$. Supposons que $n = 2^\alpha p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. On a alors
$$(\mathbf{Z}/n\mathbf{Z})^\times \cong H \times \prod_{i=1}^{r} \mathbf{Z}/p_i^{\alpha_i - 1}(p_i - 1)\mathbf{Z}$$
avec $H = \{0\}$ si $\alpha = 0, 1$, $H = \mathbf{Z}/2\mathbf{Z}$ si $\alpha = 2$ et $H = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{\alpha-2}\mathbf{Z}$ sinon. Un morphisme non trivial de $(\mathbf{Z}/n\mathbf{Z})^\times$ dans $\mathbf{Z}/2\mathbf{Z}$ correspond au choix de l'image du générateur de chaque facteur (dont l'ordre est toujours divisible par 2). On obtient donc $2^r - 1$ si $\alpha = 0, 1$, $2^{r+1} - 1$ si $\alpha = 2$ et $2^{r+2} - 1$ sinon.
On a $60 = 2^2 \times 3 \times 5$ et donc on obtient bien $2^{2+1} - 1 = 7$.
5. On rappelle que le discriminant de Φ_p est donné par
$$\Delta = \prod_{1 \leqslant i < j \leqslant p-1} (\zeta_p^i - \zeta_p^j).$$
On a
$$\Delta = (-1)^{\frac{p-1}{2}} \prod_{1 \leqslant i \neq j \leqslant p-1} (\zeta_p^i - \zeta_p^j).$$
Mais, de
$$\Phi_p(X) = \prod_{i=1}^{p-1} (X - \zeta_p^i)$$
il vient
$$\Phi_p'(\zeta_p^i) = \prod_{\substack{j=1 \\ j \neq i}}^{p-1} (\zeta_p^i - \zeta_p^j)$$
et
$$\prod_{i=1}^{p-1} \Phi_p'(\zeta_p^i) = \prod_{1 \leqslant i \neq j \leqslant p-1} (\zeta_p^i - \zeta_p^j).$$
Or, comme $\Phi_p(X) = \frac{X^p - 1}{X - 1}$, on a $\Phi_p'(X) = \frac{pX^{p-1}}{X-1} - \frac{X^p - 1}{(X-1)^2}$ si bien que
$$\Phi_p'(\zeta_p^i) = \frac{p\zeta_p^{i(p-1)}}{\zeta_p^i - 1}.$$

Le produit des racines de Φ_p vaut son coefficient constant, à savoir 1 et par ailleurs le polynôme minimal des $\zeta_p^i - 1$ est $\Phi_p(X+1)$ de coefficient constant p de sorte que

$$\prod_{i=1}^{p-1}(\zeta_p^i - 1) = p.$$

Il vient finalement $\Delta = (-1)^{\frac{p-1}{2}}p^{p-2}$.
Il est alors clair que $\mathbf{Q}(\sqrt{\Delta})$ est un sous-corps quadratique de $\mathbf{Q}(\zeta_p)$ et comme le groupe de Galois de cette dernière extension est cyclique, il possède un unique sous-groupe de tout cardinal et cette extension quadratique est par conséquent unique. Le résultat découle alors du fait que $p-3$ est pair.

6. On a que $\mathbf{Q}(\zeta_8) = \mathbf{Q}(i, \sqrt{2})$ est galoisienne d'ordre 4 et de groupe de Galois $(\mathbf{Z}/2\mathbf{Z})^2$. Les sous-extensions quadratiques sont $\mathbf{Q}(i), \mathbf{Q}(\sqrt{2})$ et $\mathbf{Q}(i\sqrt{2})$.
On a vu que $\mathbf{Q}(\zeta_{60}) = \mathbf{Q}(\zeta_4, \zeta_3, \zeta_5)$. On a donc les sous-extensions quadratiques $Q_1 = \mathbf{Q}(\sqrt{3})$, $Q_2 = \mathbf{Q}(\sqrt{5})$ et $Q_3 = \mathbf{Q}(\zeta_4) = \mathbf{Q}(i)$. On obtient alors nécssairement $Q_4 = \mathbf{Q}(i\sqrt{3})$, $Q_5 = \mathbf{Q}(i\sqrt{5})$, $Q_6 = \mathbf{Q}(\sqrt{15})$ et $Q_7 = \mathbf{Q}(i\sqrt{15})$. On a obtenu 7 extensions quadratiques distinctes et donc on les a toutes !

7. Soit K une extension quadratique. On a alors $K = \mathbf{Q}(\sqrt{n})$ avec n sans facteur carré de la forme $n = s2^\varepsilon p_1 \cdots p_r$ avec $s, \varepsilon \in \{\pm 1\}$ et p_i des nombres premiers impairs. Il est clair que $\mathbf{Q}(i) = \mathbf{Q}(\zeta_4)$. On a alors que $\mathbf{Q}(\sqrt{p_i})$ ou $\mathbf{Q}(i\sqrt{p_i})$ est une sous-extension quadratique de $\mathbf{Q}(\zeta_{p_i})$. Il s'ensuit que $\mathbf{Q}(\sqrt{p_i})$ est une sous-extension quadratique de $\mathbf{Q}(\zeta_4, \zeta_{p_1}, \ldots, \zeta_{p_r}) = \mathbf{Q}(\zeta_{4p_1\ldots p_r})$. Si maintenant $\varepsilon = 1$, il suffit de remplacer $\mathbf{Q}(\zeta_4)$ par $\mathbf{Q}(\zeta_8)$ pour avoir en plus de $\mathbf{Q}(i)$, l'extension $\mathbf{Q}(\sqrt{2})$. En conclusion, $K = \mathbf{Q}(\sqrt{n})$ est une sous-extension de $\mathbf{Q}(\zeta_{2^{2+\varepsilon}p_1\ldots p_r})$.
On peut en fait montrer (mais c'est plus difficile) que tout extension galoisienne de groupe de Galois abélien est une sous-extension d'une extension cyclotomique. Il s'agit du théorème de Kronecker-Weber.

Exercice 18 — Extensions de Kummer. Soient K un corps et $P = X^n - a \in K[X]$ avec n un entier naturel non nul et $a \in K^\times$.

1. Vérifier que P est résoluble par radicaux sur K.

2. Soit L un corps de décomposition de P. Montrer que $\mathrm{Gal}(L/K)$ s'identifie à un sous-groupe du groupe affine

$$\mathrm{Aff}\,(\mathbf{Z}/n\mathbf{Z}) = \left\{ \begin{pmatrix} u & b \\ 0 & 1 \end{pmatrix} \,:\, u \in (\mathbf{Z}/n\mathbf{Z})^\times,\, b \in \mathbf{Z}/n\mathbf{Z} \right\}.$$

3. On suppose que $K = \mathbf{Q}$, que $n = p$ est premier et que $a \notin (\mathbf{Q}^\times)^p$. Calculer $\mathrm{Gal}(L/K)$.

Solution.

1. C'est immédiat par définition.

2. Soient $\sigma \in \mathrm{Gal}(L/K)$ et ζ_n une racine primitive n-ème de l'unité. Soient $u \in (\mathbf{Z}/n\mathbf{Z})^\times$ et $b \in \mathbf{Z}/n\mathbf{Z}$ tels que $\sigma(\zeta_n) = \zeta_n^u$ et $\sigma(\sqrt[n]{a}) = \zeta_n^b(\sqrt[n]{a}$. Posons

$$f(\sigma) = \begin{pmatrix} u & b \\ 0 & 1 \end{pmatrix}.$$

On vérifie que $f : \mathrm{Gal}(L/K) \to \mathrm{Aff}\,(\mathbf{Z}/n\mathbf{Z})$ est un morphisme de groupes injectif.

3. On a

$$[L : \mathbf{Q}] = [L : \mathbf{Q}(\zeta_p)][\mathbf{Q}(\zeta_p) : \mathbf{Q}] = (p-1)[L : \mathbf{Q}(\zeta_p)].$$

On a alors que $L = \mathbf{Q}(\zeta_p)(\sqrt[p]{a})$. Or $X^p - a$ annule $\sqrt[p]{a}$ sur $\mathbf{Q}$ donc sur $\mathbf{Q}(\zeta_p)$. Montrons que ce polynôme y reste irréductible. Sinon, il existe

$$Q = \prod_{i=0}^{k}(X - \zeta_p^{i_k}\sqrt[p]{a}) \in \mathbf{Q}(\zeta_p)[X].$$

Le coefficient devant X^{k-1} fournit que $\sqrt[p]{a} \in \mathbf{Q}(\zeta_p)$ soit que a est une puissance p-ème dans $\mathbf{Q}(\zeta_p)$. Mais si c'était le cas

$$\prod_{\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})} \sigma(a) = a^{p-1}$$

serait une puissance p-ème dans $\mathbf{Q}$ ce qui est exclu. On en déduit que $[L : \mathbf{Q}] = p(p-1) = \#\mathrm{Aff}\,(\mathbf{Z}/p\mathbf{Z})$ et le morphisme injectif de la question précédente est donc un isomorphisme !

Exercices complémentaires de la semaine 3

Exercice 19 — Théorème de Dirichlet faible. Soit n un entier naturel non nul. Le but de l'exercice est d'établir qu'il existe une infinité de nombres premiers p congrus à 1 modulo n.

1. Soit $P \in \mathbf{Z}[X] \smallsetminus \mathbf{Z}$. Montrer que l'ensemble $\{d \in \mathbf{N} \,:\, \exists n \in \mathbf{N},\, d \mid P(n)\}$ est infini.
2. Soit $P = \dfrac{X^n - 1}{\Phi_n} \in \mathbf{Z}[X]$. Montrer qu'il existe un nombre premier p et un entier x tels que $p \mid \Phi_n(x)$ mais $p \nmid P(x)$.
3. Calculer l'ordre de x modulo p et en déduire que $p \equiv 1 \pmod{n}$.
4. Conclure.

Solution.

1. Supposons cet ensemble $S = \{m_1, \dots, m_r\}$ fini. En particulier, le coefficient constant c de P est non nul puisque sinon on aurait $n \mid P(n)$ pour tout n. Dès lors, $P(m_1 m_2 \cdots m_r | c | n)$ s'écrit sous la forme $|c|Q$ avec $Q \in \mathbf{Z}[X]$ non constant à coefficient constant valant ± 1. On a également $Q(n) = \pm 1$ modulo m_k pour tout $k \in \{1, \dots, r\}$. En prenant n_0 entier assez grand, on a $|Q(n_0)| \geqslant 1$ (sinon Q serait constant égal à 0 ou ± 1) et l'existence d'un diviseur premier p de $Q(n_0)$ contredit la finitude de S.
2. On a $X^a - 1 = \Phi_a P$ avec $P \in \mathbf{Z}[X]$. Par l'identité de Bézout (on utilise ici l'irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}$) dans $\mathbf{Q}[X]$ (bien se souvenir que cette identité est valable dans les anneaux principaux et que $\mathbf{Z}[X]$ ne l'est pas !), il existe $U, V \in \mathbf{Q}[X]$ tels que $1 = \Phi_a U + PV = 1$. En chassant les dénominateurs, on obtient un entier m et des polynômes U_0, V_0 à coefficients entiers tels que $m = \Phi_a U_0 + P V_0$. Par la question précédente, il existe x entier et p diviseur premier de $\Phi_a(x)$ ne divisant pas m. Cela implique que $p \nmid P(x)$.
3. On déduit de la question précédente que $x^a - 1 = 0$ dans $\mathbf{F}_p$ mais $x^d - 1 \neq 0$ pour tout $d \mid a$, $d \neq a$. En effet, on a
$$P = \prod_{\substack{d \mid a \\ d \neq a}} \Phi_d.$$
Il s'ensuit que l'ordre de x dans $\mathbf{F}_p^\times$ est a. Comme ce groupe est d'ordre $p-1$, on a donc bien $a \cong 1 \pmod{p}$.
4. On suppose l'ensemble des nombres premiers p congrus à 1 modulo a fini. On le note $\{p_1, \dots, p_r\}$. On applique alors la démarche précédente avec $ap_1 \cdots p_r$ à la place de a ce qui permet de trouver un nombre premier $p_{r+1} \equiv 1 \pmod{ap_1 \dots p_r}$ soit congrus à 1 modulo p mais distinct de $p_1, \dots, p_r$, ce qui est absurde !

Exercice 20 — Examen 2020. Soient K un corps et L une extension finie et galoisienne de K. On pose $G = \mathrm{Gal}(L/K)$. Soient F_1, F_2 deux extensions de K avec $K \subseteq F_i \subseteq L$ pour $i \in \{1, 2\}$. On pose $G_i = \mathrm{Gal}(L/F_i)$ pour $i \in \{1, 2\}$ de sorte que G_1, G_2 soient deux sous-groupes de G.

1. On suppose que $F_1 \cap F_2 = K$. Montrer que la partie $G_1 \cup G_2$ engendre le groupe G.
2. Montrer réciproquement que si $G_1 \cup G_2$ engendre le groupe G, alors $F_1 \cap F_2 = K$.

   Dans toute la suite, on note F le sous-corps de L engendré par $F_1 \cap F_2$.
3. Montrer que $F = L$ si, et seulement si, $G_1 \cap G_2 = \{\mathrm{Id}\}$.
4. On suppose que F_1, F_2 sont des extensions galoisiennes de K qui vérifient $F_1 \cap F_2 = K$ et $F = L$. Montrer que le groupe G est isomorphe au produit direct $G_1 \times G_2$.
5. Montrer que le résultat de la question précédente ne vaut plus forcément si F_1 et F_2 ne sont pas supposées galoisiennes sur K.
6. On revient au cas général où F_1, F_2 sont des extensions intermédiaires quelconques entre K et L. Montrer qu'il existe un morphisme surjectif de K-algèbres de $F_1 \otimes_K F_2$ dans F, mais que ces deux K-algèbres peuvent ne pas être isomorphes.

Solution. Voir la page web de D. Harari ici.

Exercice 21 — Examen 2021. Soit K un corps. On considère une extension galoisienne L de K et on pose $G = \mathrm{Gal}(L/K)$. Soit p un nombre premier. On suppose que $|G| = p^m a$ avec $m \in \mathbf{N}$ et a un entier non divisible par p.

1. Montrer qu'il existe une extension F de K telle que $[F : K] = a$.
2. Soient F, F' deux extensions de degré a de K avec $F, F' \subseteq L$. Montrer qu'il existe $\sigma \in G$ tel que $\sigma(F) = F'$.
3. On suppose G abélien. On note e l'exposent de G. Soit d un diviseur de e. Montrer qu'il existe une extension galoisienne $E \subseteq L$ de K telle que $\mathrm{Gal}(L/E) \cong \mathbf{Z}/d\mathbf{Z}$.
4. Le résultat de la question précédente vaut-il encore si G n'est plus supposé abélien ?

Solution. Voir la page web de D. Harari ici.

Exercice 22 — Examen 2022.

1. Soit K un corps et n un nombre premier. Montrer que si le polynôme $X^n - 1$ est scindé sur une extension L de K de degré n, il est scindé sur K.
2. Montrer que le résultat précédent tombe en défaut pour $n = 4$.
3. Soit L une extension galoisienne finie d'un corps K, de groupe de Galois $G = \mathrm{Gal}(L/K)$. On considère $\mathcal{E}$ l'ensemble des extensions intermédiaires M, c'est-à-dire des corps M vérifiant $K \subseteq M \subseteq L$. Montrer qu'il existe $M_1 \in \mathcal{E}$ tel que M_1 soit une extension galoisienne de K avec $\mathrm{Gal}(M_1/K)$ abélien et tel que tout $M \in \mathcal{E}$ qui a la même propriété soit contenu dans M_1.
4. On prend $K = \mathbf{Q}$ et $L = \mathbf{Q}\left(j, \sqrt[3]{2}\right)$, où j est une racine primitive cubique de l'unité. Quelle est l'extension M_1 de la question précédente ?
5. On reprend les notations de **3.** mais on suppose seulement que L est séparable (pas nécessairement galoisienne) sur K. Montrer que le résultat de **3.** vaut encore.

Solution. Voir la page web de D. Harari ici.

Exercice 23 — Théorème de Wedderburn. Tout anneau à division fini est commutatif. Un *anneau à division* est un anneau (non nécessairement commutatif) dont tous les éléments non nuls admettent un inverse. Soit A un anneau à division fini et soit $Z(A)$ son centre (c'est un corps). Soit n la dimension de A sur $Z(A)$, et soit q l'ordre de $Z(A)$.

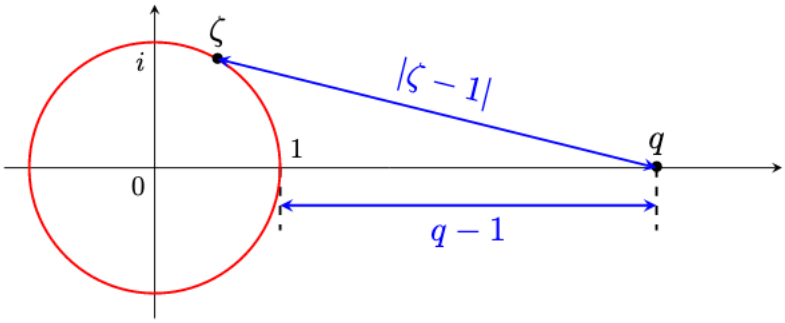
1. En utilisant l'équation des classes, montrer que
$$q^n - 1 = q - 1 + \sum \frac{q^n - 1}{q^d - 1},$$
où la somme est prise sur les représentants d'éléments non dans $Z(A)^\times$, et d est la dimension du centralisateur de cet élément sur $Z(A)$.
2. Montrer qu'alors $\Phi_n(q)$ divise $q - 1$.
3. Montrer que si $n > 1$, alors $\Phi_n(q) > q - 1$.
Indication : utiliser la décomposition de $\Phi_n(X)$ en facteurs linéaires dans $\mathbf{C}[X]$.
4. Conclure que $A = Z(A)$ et que A est un corps.

Solution.
Noter que $Z(A)$ est un corps commutatif fini donc de cardinal q et A est alors un espace vectoriel de dimension finie sur ce corps dont on note n la dimension.

1. $A^\times$ est un groupe multiplicatif qui agit sur lui même par conjugaison. L'équation aux classes s'écrit alors : $|A^\times| = |Z(A^\times)| + \sum_{\text{orbites de taille } \geq 2} |\text{orbites}|$ ce qui est équivalent à $q^n - 1 = q - 1 + \sum_{d|n,\, d\neq n} \frac{q^n-1}{q^d-1}$ car on a $q-1$ orbites de cardinal 1 qui correspondent aux éléments non nuls de $Z(A)$ et lorsque l'orbite n'est pas réduite à un élément, on sait que son cardinal est $\frac{q^n-1}{\#\mathrm{Stab}(x)}$. Or, on a que
$$\mathrm{Stab}(x) = \{y \in A^\times \ : \ xy = yx\}$$
et $\mathrm{Stab}(x) \cup \{0\}$ est un $Z(A)$-espace vectoriel de dimension finie donc de cardinal q^d pour un certain entier d. On a alors par hypothèse que $\mathrm{Stab}(x)$ (de cardinal $q^d - 1$) est un sous-groupe de $Z(A) \smallsetminus \{0\}$ si bien que $q^d - 1 \mid q^n - 1$ ce qui entraîne[23] que $d \mid n$ et le résultat.
2. $\Phi_n(X)$ divise $X^n - 1$ et aussi $\frac{X^n-1}{X^d-1}$ pour tout d diviseur de n, $d \neq n$. Donc $\Phi_n(q)$ divise $q^n - 1$ et $\Phi_n(q)$ divise $\sum_{\substack{d|n,\\ d\neq n}} \frac{q^n-1}{q^d-1}$ donc $\Phi_n(q)$ divise $q - 1$.
3. Dans $\mathbf{C}[X]$, $\Phi_n(X) = \prod_{\xi \text{ racine } n\text{-ième de l'unité primitive}} (X - \xi)$ donc[24] $|\Phi_n(q)| = \prod |q - \xi| \geq \prod ||q| - |\xi|| = \prod |q - 1| > q - 1$.

23. Par division euclidienne, $n = da + r$ avec $0 \leqslant r < d$, on a que
$$q^n - 1 = q^r(q^{da} - 1) + (q^r - 1)$$
de sorte que $q^d - 1 \mid q^r - 1$ mais $q^r - 1 < q^d - 1$ donc cela n'est possible que si $r = 0$ et $d \mid n$.

24. On utilise ici le fait que l'inégalité triangulaire est stricte car $\xi \notin \mathbf{R}^+$.



4. Si $n > 1$, on a que $\Phi_n(q)$ divise $q-1$ et $\Phi_n(q) > q-1$ ce qui n'est pas possible donc $n = 1$. Dans ce cas $Z(A) = A$ et A est alors un corps commutatif.