TD7 : Extensions séparables, normales, galoisiennes

Diego Izquierdo

Les exercices 1, 2, 3, 10, 15, 16 et 19 ont été traités pendant la séance. Vu que certains ont trouvé que j'allais trop vite sur l'exercice 19, j'ai mis un corrigé pour cet exercice.

Exercice 1 (à préparer) : Une infinité d'extensions intermédiaires
Trouver une infinité d'extensions intermédiaires entre $\mathbb{F}_p(X^p, Y^p)$ et $\mathbb{F}_p(X, Y)$. Existe-t'il $\alpha \in \mathbb{F}_p(X, Y)$ tel que $\mathbb{F}_p(X, Y) = \mathbb{F}_p(X^p, Y^p)(\alpha)$?

> **Indications :** On peut prendre les $\mathbb{F}_p(X^p, Y^p)(X + X^{p^k}Y)$ pour $k \geq 1$. Ces derniers sont de dimension p sur $\mathbb{F}_p(X^p, Y^p)$ puisque l'on a $X + X^{p^k}Y \notin \mathbb{F}_p(X^p, Y^p)$ et $(X + X^{p^k}Y)^p \in \mathbb{F}_p(X^p, Y^p)$. Aussi, deux tels sous-corps ne sont pas égaux puisque si $i \neq j$, $X + X^{p^i}Y$ et $X + X^{p^j}Y$ engendrent $\mathbb{F}_p(X, Y)$ sur $\mathbb{F}_p(X^p, Y^p)$: on a $Y = (X^{p^i} - X^{p^j})^{-1}((X + X^{p^i}Y) - (X + X^{p^j}Y))$.

Exercice 2 (à préparer) : Une extension inséparable en caractéristique 2
Soient $K = \mathbb{F}_2(X, Y)$, $L = K(\alpha)$ avec $\alpha^2 + X\alpha + Y = 0$, et $M = K(\beta)$ avec $\beta^2 = \alpha$.

1. Montrer que $[M : K] = 4$.
2. Montrer que $[M : K]_s = 2$ et que $M_s = L$.
3. Montrer qu'un élément $\gamma \in M$ vérifie $\gamma^2 \in K$ si, et seulement si, $\gamma \in K$.
4. Montrer qu'il n'existe pas de corps intermédiaire $K \subsetneq F \subseteq M$ purement inséparable sur K.

Exercice 3 (à préparer) : Extensions séparables et degré
Soit L/K une extension finie de corps de caractéristique $p > 0$ de degré premier à p. Montrer qu'elle est séparable.

Exercice 4 : Une caractérisation des extensions séparables
Soit $F \subseteq E$ une extension finie de corps de caractéristique $p > 0$.

1. Montrer qu'un élément $x \in E$ est séparable si et seulement si on a $F(x) = F(x^p)$.

Indications : Supposons x séparable sur F. Le polynôme $P = X^p - x^p \in F(x^p)[T]$ est soit scindé, soit irréductible. Comme il n'est pas séparable, s'il était irréductible, alors x ne serait pas séparable sur $F(x)$: absurde ! Donc P est scindé et $x \in F(x^p)$. Cela montre que $F(x) = F(x^p)$.
Supposons $F(x) = F(x^p)$. Alors il existe $Q \in F[T]$ tel que $x = Q(x^p)$. Donc x est racine de $Q(T) - T$, qui est un polynôme séparable. On en déduit que x est séparable sur F.

2. Montrer l'équivalence des assertions suivantes :

(i) il existe une base $(x_1, \ldots, x_n)$ de E sur F telle que $(x_1^p, \ldots, x_n^p)$ est aussi une F-base de E ;

(ii) pour toute base $(y_1, \ldots, y_n)$ de E sur F, $(y_1^p, \ldots, y_n^p)$ est aussi une F-base de E.

Indications : Supposons (i). Soit $(y_1, ..., y_n)$ une F-base de E. Il existe des matrices $A, B \in GL_n(F)$ telles que :

$$A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_1^p \\ \vdots \\ x_n^p \end{pmatrix}, \quad B \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

Soit Fr le Frobenius sur E. On a alors :

$$\begin{pmatrix} y_1^p \\ \vdots \\ y_n^p \end{pmatrix} = Fr \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = Fr(B)Fr \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = Fr(B)A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Comme $Fr(B)A \in GL_n(F)$, on en déduit que $(y_1^p, ..., y_n^p)$ est une F-base de E.

3. Montrer que (i) est vraie si et seulement si l'extension $F \subseteq E$ est séparable.

Indications : Supposons (i). Alors on a (ii). Soit $x \in E$. Soit $n = [F(x) : F]$. Il existe une base de E de la forme $(x^i \omega_j)_{1 \leq i \leq n, 1 \leq j \leq \frac{[E:F]}{n}}$ avec $\omega_1 = 1$. Par (ii), on sait que $(x^{pi} \omega_j^p)_{1 \leq i \leq n, 1 \leq j \leq \frac{[E:F]}{n}}$ est une F-base de E. On en déduit que $(1, x^p, x^{2p}, ..., x^{(n-1)p})$ est une famille F-libre de $F(x)$: c'est donc une base et on a $F(x) = F(x^p)$. La question 1 permet alors de conclure que x est séparable sur F.
Réciproquement, supposons que E/F est séparable. Alors il existe $x \in E$ tel que $E = F(x)$, d'après le théorème de l'élément primitif. Une F-base de E est alors donnée par $(1, x, x^2, ..., x^{[E:F]-1})$. Mais d'après la question 1, $E = F(x) = F(x^p)$. Donc $(1, x^p, x^{2p}, ..., x^{p[E:F]-p})$ est aussi une F-base de E. Donc (i) est vérifiée.

Exercice 5 : Éléments primitifs

1. Soit $K = \mathbb{Q}(\sqrt[3]{2}, \rho)$. Pour quelles valeurs de $t \in \mathbb{Q}$ l'élément $\sqrt[3]{2} + t\rho$ est-il un élément primitif de l'extension $K/\mathbb{Q}$? Et $\sqrt[3]{2} + t\rho\sqrt[3]{2}$?

Indications : D'après la démonstration du théorème de l'élément primitif, les valeurs de $t \in \mathbb{Q}$ telles que l'élément $\sqrt[3]{2}+tj$ est un élément primitif de l'extension $K/\mathbb{Q}$ sont celles qui vérifient $t(j-j^2) = y - \sqrt[3]{2}$ pour $y \in \{\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}\}$: on peut donc choisir t dans $\mathbb{Q} \setminus \{0\}$.
Les valeurs de $t \in \mathbb{Q}$ telles que l'élément $\sqrt[3]{2} + tj\sqrt[3]{2}$ est un élément primitif de l'extension $K/\mathbb{Q}$ sont celles qui vérifient $t(j-x) = y - 1$ pour $x \in \{1, j^2\}$ et $y \in \{j, j^2\}$: ce sont donc les rationnels autres que 1.

2. Donner un élément primitif de l'extension $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}$.

Indications : Soient $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ et $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}$. Comme dans la question 1, on vérifie que $\sqrt{2} + \sqrt{3}$ est un élément primitif de K, puis que $\sqrt{2} + \sqrt{3} + \sqrt{5}$ est un élément primitif de L.

Exercice 6 : p-dimension

Soit $F \subseteq E$ une extension finie de corps de caractéristique $p > 0$. On suppose l'inclusion $E^{\times p} \subseteq F^\times$, de sorte que $F \subseteq E$ est purement inséparable. Appelons famille génératrice de E toute famille d'éléments $(x_1, ..., x_n)$ de E telle que $E = F(x_1, ..., x_n)$. Montrer que les familles génératrices minimales de E sont toutes de même cardinal (on pourra calculer le degré de $[E : F]$). On appelle ce cardinal la p-dimension de E/F.

Indications : Soit $(x_1, ..., x_n)$ une famille génératrice minimale. Pour $0 \leq j \leq n$, on note $E_j = F(x_1, ..., x_j)$. Pour $j \leq n-1$, on remarque que $x_{j+1} \notin E_j$ puisque $(x_1, ..., x_n)$ est une famille génératrice minimale. De plus, on a $x_{j+1}^p \in F$. On en déduit que le polynôme $X^p - x_{j+1}^p \in E_j$ est irréductible. Donc $[E_{j+1} : E_j] = p$. Par conséquent, $[F : E] = p^n$. On en déduit que les familles génératrices minimales de E sont toutes de même cardinal.

Exercice 7 : Extensions purement inséparables

Soient K un corps de caractéristique $p > 0$, $\overline{K}$ une clôture algébrique de K et K^s la clôture séparable de K dans $\overline{K}$.

1. Rappeler pourquoi K^s est bien définie.

Indications : Pour pouvoir considérer K^s agréablement, il s'agit de vérifier que la composée de deux extensions séparables L et M de K est séparable. Or tout élément x de M annule un polynôme séparable de $K[X]$, et le polynôme minimal de x sur L est aussi séparable. Ceci assure que $L \subseteq LM$ est séparable. Une extension $K \subseteq L$ étant séparable si et seulement si on a $[L : K] = |\mathrm{Hom}_K(L, \overline{K})|$, l'extension $K \subseteq L \subseteq LM$ est séparable.

Soit $P \in K[X]$ un polynôme unitaire irréductible.

2. Montrer que P a une unique racine dans $\overline{K}$ si et seulement si il existe $r \in \mathbb{N}$ et $a \in K$ tels que $P = X^{p^r} - a$.

Indications : Si P est de la forme $X^{p^r} - a$, et si α est une racine de P dans $\overline{K}$, alors on a sur $\overline{K}$: $P = (X - \alpha)^{p^r}$.
Réciproquement, si P a une unique racine α dans $\overline{K}$, alors P est de la forme $(X-\alpha)^k$. Si l'on a $\alpha \in K$, par irréductibilité de P, on a $k = 1$. Sinon, comme P est irréductible et non séparable, on a $P \in K[X^p]$, et donc $k = pk_1$ pour un entier $k_1 \geq 1$. On a alors $P = (X^p - \alpha^p)^{k_1}$. Mais alors $P_1 = (X - \alpha^p)^{k_1}$ est un polynôme irréductible avec une unique racine dans $\overline{K}$, et par récurrence on obtient $k = p^r$.

Soit $K \subseteq L$ une extension algébrique.

3. Montrer que $K \subseteq L$ est purement inséparable si et seulement si il n'existe qu'un homomorphisme de K-algèbres de L dans $\overline{K}$.

Indications : Supposons que $K \subseteq L$ est purement inséparable et qu'il existe deux morphismes de K-algèbres distincts de L dans $\overline{K}$. Alors il existe $x \in L$ tel que leurs valeurs en x diffèrent. Comme x est algébrique et purement inséparable sur K, son polynôme minimal P divise un certain $X^{p^{r_0}} - a_0$. Mais alors P est irréductible et a une unique racine dans $\overline{K}$: par (a), c'est que l'on a $P = X^{p^r} - a$. De ce fait on a un unique morphisme de K-algèbres de $K(x)$ dans $\overline{K}$, ce qui contredit l'hypothèse initiale. On vient de montrer que si $K \subseteq L$ est purement inséparable, alors on a $\mathrm{Hom}_K(L, \overline{K}) = \{1\}$.
Réciproquement, s'il n'y a qu'un seul morphisme $L \to \overline{K}$, pour tout $x \in L$, il n'y a aussi qu'un seul morphisme de K-algèbres $K(x) \to \overline{K}$. Cela veut dire que le polynôme minimal de x sur K a une unique racine dans $\overline{K}$ et on conclut par (a).

4. Montrer que L est une extension purement inséparable de $K^s \cap L$.

Indications : Par définition, $K^s \cap L$ est la plus grande sous-extension séparable de L. En particulier, on a $\mathrm{Hom}_K(L, \overline{K}) = \mathrm{Hom}_K(K^s \cap L, \overline{K})$, ce qui veut aussi dire qu'il n'y a qu'un unique $(K^s \cap L)$-homomorphisme de L dans $\overline{K}$. En effet, on a l'application de restriction $\mathrm{Hom}_K(L, \overline{K}) \to \mathrm{Hom}_K(K^s \cap L, \overline{K})$, qui est surjective (parce qu'il existe des prolongements de morphismes). Supposons qu'elle n'est pas injective : il existe alors un $x \notin K^s \cap L$ et deux morphismes $L \to \overline{K}$ qui envoient x sur des images distinctes. On peut supposer x de degré minimal sur $K^s \cap L$, ce que l'on va faire. On considère alors le polynôme $P := \prod_\varphi (X - \varphi(x))$ où φ parcourt les morphismes $L \to \overline{K}$ ayant des valeurs distinctes en x (il y en a un nombre fini du fait que x est algébrique). Les coefficients de P sont dans un sous-corps strict M de $(K^s \cap L)(x)$ (puisque les φ ne diffèrent pas sur M). On a alors l'alternative suivante : ou bien $M = K^s \cap L$ et x est alors séparable, ce qui est absurde ; ou bien $M \supsetneq K^s \cap L$ est séparable puisque x a été choisi de degré minimal parmi les non séparables, et c'est aussi absurde. Par (c), $K^s \cap L \subseteq L$ est purement inséparable.

On note L^{rad} le sous-corps de L constitué de tous les éléments $x \in L$ tels qu'il existe $r \in \mathbb{N}$ avec $x^{p^r} \in K$.

5. Montrer que $\overline{K}$ est une extension séparable de $\overline{K}^{\mathrm{rad}}$.

Indications : Comme $x \mapsto x^p$ est surjectif sur $\overline{K}^{\mathrm{rad}}$, tout polynôme irréductible non séparable serait de la forme $P = a_n X^{np} + a_{n-1} X^{(n-1)p} + \cdots + a_0$; et en prenant $b_i^p = a_i$, on a $P = (b_n X^n + b_{n-1} X^{n-1} + \cdots + b_0)^p$, qui n'est donc pas irréductible. C'est que toute extension finie de $\overline{K}^{\mathrm{rad}}$ est séparable. Comme $\overline{K}^{\mathrm{rad}} \subseteq \overline{K}$ est algébrique, elle est ainsi séparable.

6. Est-ce vrai pour $L \subsetneq \overline{K}$ et L^{rad} ?

Indications : Supposons $p > 2$ et considérons

$$K = \overline{\mathbb{F}_p}(t) \subseteq M = D_K(X^2 - X + t) \subseteq L = D_M(X^p - \alpha) \subseteq \overline{K},$$

où $\alpha \in M$ est une racine de $X^2 - X + t$. Parce que l'on a $\Delta = 1 - 4t \notin K^{\times 2} \cup \{0\}$, M est une extension de degré 2 de K et $L = D_M(X^p - \alpha)$ est de degré p ($X^p - \alpha$ est irréductible car une racine n'est pas dans M car non dans L, et est de degré un diviseur de p). L'extension $K \subseteq L$ est visiblement non séparable et il y a deux morphismes dans $\text{Hom}_K(L, \overline{K})$: Id et $\sigma : x \mapsto \dfrac{t^{1/p}}{x}$ où x est zéro de $X^{2p} - X^p + t$. A cause du (c), ces morphismes sont aussi dans $\text{Hom}_{L^{\text{rad}}}(L, \overline{K}) = \text{Aut}_{L^{\text{rad}}} L$. En particulier, on a $L^{\text{rad}} \subseteq L^\sigma = K\left(x + \dfrac{t^{1/p}}{x}\right)$. Or $x + \dfrac{t^{1/p}}{x}$ vérifie $\left(x + \dfrac{t^{1/p}}{x}\right)^p = x^p + \dfrac{t}{x^p} = 1$, et donc on a $x + \dfrac{t^{1/p}}{x} = 1$, de sorte que L^{rad} est K. De ce fait, L n'est pas une extension séparable de L^{rad}.
On remarquera a posteriori que cet exemple repose crucialement sur le fait que $K \subseteq L$ n'est pas normale.

Exercice 8 : Plus grand sous-corps parfait
Soient n un entier naturel et q une puissance d'un nombre premier. Quel est le plus grand sous-corps parfait de $\mathbb{F}_q(X_1, ..., X_n)$?

Indications : Soit K un sous-corps parfait de $L = \mathbb{F}_q(X_1, ..., X_n)$. Soient p un nombre premier et $n > 0$ tels que $q = p^n$. On sait que K est de caractéristique $p > 0$, et que $K^p = K$. On en déduit que K est contenu dans $\bigcap_{r \geq 0} L^{p^r} \subseteq \mathbb{F}_q[X_1, ..., X_n]^\times \cup \{0\} = \mathbb{F}_q$. Comme les corps finis sont parfaits, le plus grand sous-corps parfait de $\mathbb{F}_q(X_1, ..., X_n)$ est $\mathbb{F}_q$.

Exercice 9 : Un exemple de corps parfait
Donner un exemple de corps parfait infini de caractéristique positive non séparablement clos.

Indications : Prendre par exemple $K = \mathbb{F}_3(X, X^{1/3}, X^{1/3^2}, ...)$. C'est un corps de caractéristique 3, parfait car $K^3 = K$, non séparablement clos car le polynôme séparable $T^2 - X$ est irréductible sur K.

Exercice 10 : Sous-corps d'un corps parfait
Soit L/K une extension de corps telle que L est parfait. Montrer que, si $[L : K] < \infty$, alors K est parfait. Que dire si $[L : K] = \infty$?

Exercice 11 : Extensions de type fini d'un corps parfait
Soit L une extension de type fini d'un corps parfait K de caractéristique $p > 0$. Montrer que $[L : L^p] < \infty$.

Indications : En procédant par récurrence, il faut montrer que, si K est un corps de caractéristique $p > 0$ tel que $[K : K^p] < \infty$ et si L est une extension de K pour laquelle il existe $x \in L$ tel que $L = K(x)$, alors $[L : L^p] < \infty$. On a :

$$[K(x) : K(x)^p] = [K(x) : K(x^p)][K(x^p) : K^p(x^p)] \leq [K(x) : K(x^p)][K : K^p] < \infty.$$

Exercice 12 : Partiel 2012

Le résultat de cet exercice est important, mais il n'est pas essentiel d'en connaître la preuve. Soit L/K une extension algébrique de corps. On suppose que tout polynôme de $K[X]$ a une racine dans L. On veut montrer que L est une clôture algébrique de K.

1. Montrer la conclusion si on suppose de plus que tout polynôme de $K[X]$ est scindé dans L.
2. Montrer la conclusion si on suppose de plus que K est parfait.
3. On suppose à partir de maintenant que la caractéristique de K est $p > 0$. Montrer que $M = \{x \in L | \exists n \in \mathbb{N}^*, x^{p^n} \in K\}$ est un sous-corps parfait de L.
4. En déduire que L est un corps parfait.
5. Montrer que tout polynôme de $M[X]$ a une racine dans L. Conclure.

Indications : Voir le corrigé du partiel 2012.

Exercice 13 : Produits tensoriels de corps

1. Exhiber un isomorphisme d'anneaux $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \to \mathbb{C} \times \mathbb{C}$.

   Indications : Considérer $f : \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \to \mathbb{C} \times \mathbb{C}, x \otimes y \mapsto (xy, x\overline{y})$.

2. Soit K une extension finie de $\mathbb{Q}$. Calculer $K \otimes_{\mathbb{Q}} \mathbb{R}$ et $K \otimes_{\mathbb{Q}} \mathbb{C}$.

   Indications : Comme $\mathbb{Q}$ est de caractéristique nulle, K est une extension séparable de $\mathbb{Q}$. D'après le théorème de l'élément primitif, on en déduit qu'il existe un polynôme irréductible unitaire $P \in \mathbb{Q}[X]$ tel que $K \cong K[X]/(P)$. On écrit la décomposition de P est produit de polynômes irréductibles :
   - dans $\mathbb{R}[X]$: $P = R_1 ... R_n T_1 ... T_m$, avec $\deg R_i = 1$ et $\deg T_1 = 2$.
   - dans $\mathbb{C}[X]$: $P = Q_1 ... Q_s$.

   Avec le lemme chinois, on a alors :

   $$K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}[X]/(P) \cong \prod_{i=1}^{n} \mathbb{R}[X]/(R_i) \times \prod_{j=1}^{m} \mathbb{R}[X]/(T_j) \cong \mathbb{R}^n \times \mathbb{C}^m,$$

   $$K \otimes_{\mathbb{Q}} \mathbb{C} \cong \mathbb{C}[X]/(P) \cong \prod_{i=1}^{s} \mathbb{C}[X]/(Q_i) \cong \mathbb{C}^s.$$

3. Calculer $\mathbb{F}_p(t^{1/p}) \otimes_{\mathbb{F}_p(t)} \mathbb{F}_p(t^{1/p})$.

   Indications : On a :

   $$\begin{aligned} \mathbb{F}_p(t^{1/p}) \otimes_{\mathbb{F}_p(t)} \mathbb{F}_p(t^{1/p}) &\cong \mathbb{F}_p(t)[X]/(X^p - t) \otimes_{\mathbb{F}_p} \mathbb{F}_p(t)[X]/(X^p - t) \\ &\cong \mathbb{F}_p(t)[X, Y]/(X^p - t, Y^p - t) \cong \mathbb{F}_{p^p}[Z]/(Z^p). \end{aligned}$$

Exercice 14 : Algèbres étales
Soient K un corps et A une K-algèbre (commutative) de dimension finie sur K. Pour $a \in A$, on note $\mathrm{Tr}_{A/K}(a)$ la trace de l'application K-linéaire $A \to A, x \mapsto ax$. Montrer que les assertions suivantes sont équivalentes :

(i) A est isomorphe à un produit fini d'extensions finies séparables de K ;
(ii) l'anneau $A \otimes_K \overline{K}$ est isomorphe à un produit fini de copies de $\overline{K}$;
(iii) l'anneau $A \otimes_K \overline{K}$ est réduit ;
(iv) la forme bilinéaire $A \times A \to K, (a,b) \mapsto \mathrm{Tr}_{A/K}(ab)$ est non dégénérée.

On dit alors que A est une K-algèbre étale.

Exercice 15 : Calcul de discriminant, le retour
Soient K un corps, $a, b \in K$ et $n > s \geq 1$. Quel est le discriminant de $X^n + aX^s + b \in K[X]$?

Exercice 16 : Extensions normales
Soient $K = \mathbb{Q}(\sqrt{5})$ et $L = \mathbb{Q}(\sqrt{1+\sqrt{5}})$. Montrer que les extensions $\mathbb{Q} \subseteq K$ et $K \subseteq L$ sont normales, mais que $\mathbb{Q} \subseteq L$ ne l'est pas. Quelle est sa clôture normale dans $\overline{\mathbb{Q}}$?

Exercice 17 : Partiel 2011
Soient K et K' deux sous-corps d'un corps L tels que l'extension $L/K \cap K'$ est algébrique. On suppose que L/K et L/K' sont normales. Montrer que $L/K \cap K'$ est normale.

Indications : Voir le corrigé du partiel 2011.

Exercice 18 : Irréductibilité de polynômes

1. Soit L/K une extension finie galoisienne. Soit $f \in L[X]$ un polynôme unitaire. Montrer que le polynôme $g = \prod_{\sigma \in \mathbf{Gal}(L/K)} \sigma f \in L[x]$ est en fait à coefficients dans K, puis que si g est irréductible dans $K[X]$, alors f est irréductible dans $L[X]$.

Indications : Pour chaque $\sigma \in \mathrm{Gal}(L/K)$, on a $\sigma \cdot g = g$. Comme L/K est galoisienne, cela montre que $g \in K[X]$. Si $P \in L[X]$ et $Q \in L[x]$ sont tels que $f = PQ$ et $\deg P > 0$ et $\deg Q > 0$, on a $g = \prod_{\sigma \in \mathbf{Gal}(L/K)} \sigma P \times \prod_{\sigma \in \mathbf{Gal}(L/K)} \sigma Q$, et $\prod_{\sigma \in \mathbf{Gal}(L/K)} \sigma P$ et $\prod_{\sigma \in \mathbf{Gal}(L/K)} \sigma Q$ sont à coefficients dans K, et donc g n'est pas irréductible.

2. Montrer que, pour tout entier naturel n, les polynômes $X^n + 2 + \sqrt{10} \in \mathbb{Q}(\sqrt{10})[X]$ et $X^n + 1 + \sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2})[X]$ sont irréductibles.

Indications : Le polynôme $(X^n+2+\sqrt{10})(X^n+2-\sqrt{10}) = X^{2n}+4X^n-6$ est irréductible dans $\mathbb{Q}[X]$ d'après le critère d'Eisenstein. Donc $X^n+2+\sqrt{10} \in \mathbb{Q}(\sqrt{10})[X]$ est irréductible.
Le polynôme $\prod_{\sigma\in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\rho)/\mathbb{Q}(\rho))} \sigma\cdot(X^n+1+\sqrt[3]{2}) = (X^n+1+\sqrt[3]{2})(X^n+1+\rho\sqrt[3]{2})(X^n+1+\rho^2\sqrt[3]{2}) = (X^n+1)^3+2$ est irréductible dans $\mathbb{Q}[X]$ d'après le critère d'Eisenstein. Comme $\mathbb{Q}(\sqrt[3]{2},\rho)^{\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2},\rho)/\mathbb{Q}(\rho))} = \mathbb{Q}(\rho)$ et $\mathbb{Q}(\rho)\cap\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}$, en procédant comme dans la question 1., on montre que $X^n+1+\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2})[X]$ est irréductible.

Exercice 19 : Automorphismes de corps
Déterminer les groupes d'automorphismes suivants :

$$\mathrm{Aut}(\mathbb{C}/\mathbb{R}),\ \mathrm{Aut}(\mathbb{Q}(\sqrt{3},\sqrt{5})/\mathbb{Q}),\ \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{3})/\mathbb{Q}),\ \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{3},j)/\mathbb{Q}),$$

$$\mathrm{Aut}(\mathbb{Q}(\sqrt{2},\sqrt[3]{3})/\mathbb{Q}),\ \mathrm{Aut}(\mathbb{Q}(\sqrt{2},\sqrt[3]{3},j)/\mathbb{Q}),\ \mathrm{Aut}(\mathbb{R}/\mathbb{Q}); \mathrm{Aut}(\mathbb{F}_{p^k}/\mathbb{F}_p).$$

Indications :

- Un élément de $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$ envoie i sur i ou $-i$. S'il envoie i sur i, c'est l'identité. Sinon, c'est la conjugaison complexe. On obtient donc $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$.
- Un élément de $\mathrm{Aut}(\mathbb{Q}(\sqrt{3},\sqrt{5})/\mathbb{Q})$ envoie $\sqrt{3}$ sur $\pm\sqrt{3}$ et $\sqrt{5}$ sur $\pm\sqrt{5}$. De plus, comme $\mathbb{Q}(\sqrt{3},\sqrt{5})/\mathbb{Q}$ est galoisienne, $\mathrm{Aut}(\mathbb{Q}(\sqrt{3},\sqrt{5})/\mathbb{Q})$ est d'ordre $[\mathbb{Q}(\sqrt{3},\sqrt{5}) : \mathbb{Q}] = 4$ (car $\sqrt{5}$ n'est pas dans $\mathbb{Q}(\sqrt{3})$). On en déduit que le morphisme de groupes :

$$\mathrm{Aut}(\mathbb{Q}(\sqrt{3},\sqrt{5})/\mathbb{Q}) \to \{\pm 1\}^2, \sigma \mapsto (\frac{\sigma(\sqrt{3})}{\sqrt{3}}, \frac{\sigma(\sqrt{5})}{\sqrt{5}})$$

  est un isomorphisme.
- Un élément de $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{3})/\mathbb{Q})$ envoie $\sqrt[3]{3}$ sur $\sqrt[3]{3}$: le groupe d'automorphismes est donc trivial.
- L'extension $\mathbb{Q}(\sqrt[3]{3}, j)/\mathbb{Q}$ est galoisienne (c'est le corps de décomposition de $X^3 - 3$). Elle est de degré 6 car $\mathbb{Q}(\sqrt[3]{3})/\mathbb{Q}$ est de degré 3 (par irréductibilité de $X^3 - 3$) et $\mathbb{Q}(\sqrt[3]{3}, j)/\mathbb{Q}(\sqrt[3]{3})$ est de degré 2 car j n'est pas dans $\mathbb{Q}(\sqrt[3]{3})$. Donc $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{3}, j)/\mathbb{Q})$ est d'ordre 6. C'est de plus un sous-groupe de S_3. Donc :

$$\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{3}, j)/\mathbb{Q}) \cong S_3.$$

- Un élément de $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})/\mathbb{Q})$ envoie $\sqrt{2}$ sur $\pm\sqrt{2}$ et fixe $\sqrt[3]{3}$. Donc $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})/\mathbb{Q})$ est d'ordre au plus 2. Mais $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})/\mathbb{Q}(\sqrt[3]{3}))$ en est un sous-groupe d'ordre 2 (car $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})/\mathbb{Q}(\sqrt[3]{3})$ est galoisienne de degré 2). On en déduit que $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$.
- L'extension $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}, j)/\mathbb{Q}$ est galoisienne (en tant que corps de décomposition de $(X^2 - 2)(X^3 - 3)$). Elle est de degré 12 car $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})/\mathbb{Q}$ est de degré 6 (en effet, le degré est au plus 6 et est multiple de $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ et de $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$) et $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}, j)/\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$ est de degré 2 (puisque j n'est pas dans $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$). Donc $\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}, j)/\mathbb{Q})$ est d'ordre 12. Le morphisme :

$$\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}, j)/\mathbb{Q}) \to \{\pm 1\} \times \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{3}, j)/\mathbb{Q}), \sigma \mapsto (\frac{\sigma(\sqrt{2})}{\sqrt{2}}, \sigma|_{\mathbb{Q}(\sqrt[3]{3}, j)})$$

  est surjectif, donc, par cardinalité, c'est un isomorphisme. On en déduit que

$$\mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt[3]{3}, j)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times S_3.$$

- Soit $\sigma \in \mathrm{Aut}(\mathbb{R}/\mathbb{Q})$. Soit $x, y \in \mathbb{R}$ tels que $x \geq y$. On remarque alors que :

$$\sigma(x) - \sigma(y) = \sigma(x - y) = \sigma(\sqrt{x - y})^2 \geq 0.$$

  Donc σ est croissante. De plus, $\sigma|_{\mathbb{Q}} = Id$. Donc $\sigma = Id$ et $\mathrm{Aut}(\mathbb{R}/\mathbb{Q})$ est trivial.
- L'extension $\mathbb{F}_{p^k}/\mathbb{F}_p$ est séparable car un corps fini est parfait et normale car c'est le corps de décomposition de $X^{p^k} - X$. Elle donc galoisienne de degré k, et $\mathrm{Aut}(\mathbb{F}_{p^k}/\mathbb{F}_p)$ est d'ordre k. Ce groupe contient le Frobenius Fr. Soit r l'ordre de Fr. On sait que $Fr^k = Id$ sur $\mathbb{F}_{p^k}$, donc r divise k. Si $r < k$, on a $\mathbb{F}_{p^k} = (\mathbb{F}_{p^k})^{Fr^r} = \mathbb{F}_{p^r}$: absurde! Donc $r = k$, et $\mathrm{Aut}(\mathbb{F}_{p^k}/\mathbb{F}_p)$ est cyclique d'ordre k, engendré par Fr.

Exercice 20 : Partiel 2013
Quel est le groupe de Galois d'un corps de décomposition du polynôme $X^3 - 10$ sur $\mathbb{Q}$? Et sur $\mathbb{Q}(i\sqrt{3})$?

> **Indications :** Voir le corrigé du partiel 2013.

Exercice 21 : Automorphismes et degré séparable
Soit L/K une extension finie. Montrer que $|\mathrm{Aut}_K(L)|$ divise $[L : K]_s$.

> **Indications :** Voir le cours (proposition 6.13.4).

Exercice 22 : Théorème de Lüroth
Soit K un corps.

1. Soit $F \in K(X)\backslash K$. Soient P et Q deux polynômes dans $K[X]$ premiers entre eux tels que $F = P/Q$. Montrer que l'extension $K(X)/K(F)$ est finie. Quel est son degré ?
   > **Indications :** Voir le lemme 6.7 du polycopié d'Algèbre 2 d'Olivier Debarre (`http://www.math.ens.fr/~debarre/`).
2. Montrer qu'il existe un isomorphisme entre $\mathrm{Gal}(K(X)/K)$ et $PGL_2(K)$.
   > **Indications :** Voir le théorème 6.8 du polycopié d'Algèbre 2 d'Olivier Debarre (`http://www.math.ens.fr/~debarre/`).

Soit maintenant L une extension de K contenue dans $K(X)$. On suppose que $K \neq L$.

3. Montrer que X est algébrique sur L.
4. On note $P = T^n + F_{n-1}T^{n-1} + ... + F_0 \in L[T]$ le polynôme minimal de X sur L. Montrer qu'il existe i tel que $F_i \notin K$.
5. *(Difficile)* Montrer que $L = K(F_i)$.
   > **Indications :** Les questions 3, 4, 5 sont le théorème 6.9 du polycopié d'Algèbre 2 d'Olivier Debarre (`http://www.math.ens.fr/~debarre/`).
6. Quelles sont les fractions rationnelles $F \in K(X)$ telles que $F \circ F \circ ... \circ F = X$?
   > **Indications :** Soit $F \in K(X)$ telles que $F \circ F \circ ... \circ F = X$. On a alors $K(F) = K(X)$. Par conséquent, $F = \frac{aX+b}{cX+d}$ pour certains $a, b, c, d \in K$. La relation $F^n = F \circ F \circ ... \circ F = X$ signifie alors que :
   >
   > $$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^n = Id$$
   >
   > dans $PGL_2(K)$.

Exercice 23 : Non fonctorialité de la clôture algébrique
On va considérer les sous-corps suivants de $\mathbb{C}$: $K = \mathbb{Q}(i)$, $L = K(\sqrt{2})$, $M = K(2^{1/4})$ et $\overline{\mathbb{Q}}$ le corps des nombres algébriques sur $\mathbb{Q}$. Soit $f \in \mathrm{Aut}_K(L)$

l'automorphisme qui envoie $\sqrt{2}$ sur son opposé.

1. Montrer qu'il existe un automorphisme de M qui prolonge f, mais qu'il n'existe pas d'automorphisme involutif de M qui prolonge f.

2. Montrer que tout automorphisme de $\overline{\mathbb{Q}}$ laisse M stable.

3. En déduire qu'il n'existe pas d'automorphisme involutif de $\overline{\mathbb{Q}}$ qui prolonge f.

4. Montrer qu'il n'existe pas d'application $\bar{\cdot}$ vérifiant :

(i) à tout corps k est associé un corps $\overline{k}$, algébriquement clos et extension algébrique de k, et un morphisme de corps $k \to \overline{k}$;

(ii) à tout morphisme de corps $f : k \to k'$ est associé un morphisme $\overline{f} : \overline{k} \to \overline{k'}$ tel que le diagramme

$$\begin{array}{ccc} \overline{k} & \xrightarrow{\overline{f}} & \overline{k'} \\ \uparrow & & \uparrow \\ k & \xrightarrow{f} & k' \end{array}$$

commute et tel que, pour tous f, g on ait $\overline{f \circ g} = \overline{f} \circ \overline{g}$.

On dira qu'il n'existe pas de foncteur « clôture algébrique ».