# TD15 : Théorie de Galois II

Diego Izquierdo

*Je vous dirai plus tard quels exercices seront à préparer et quels exercices nous traiterons.*

**Exercice 0 : TD14**
Faire les questions (xiii) et (xvi) de l'exercice 7 du TD14.

**Exercice 1 : Sous-corps d'un corps cyclotomique**
Faire la liste des sous-corps de $\mathbb{Q}(\zeta_{20})$.

**Exercice 2 : Sous-extensions de degré 3 d'extensions cyclotomiques**

1. Déterminer l'entier positif minimal $n$ tel que l'extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ contient une sous-extension $E$ de degré 3. Montrer que cette sous-extension est unique.

   **Indications :** Le groupe de Galois de $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est $(\mathbb{Z}/n\mathbb{Z})^\times$. Ce groupe possède un sous-groupe d'indice 3 si, et seulement si, $9|n$ ou $n$ possède possède un diviseur premier congru à 1 modulo 3. En invoquant la théorie de Galois, on déduit que l'entier $n$ recherché est 7. Comme $\mathbb{Z}/6\mathbb{Z}$ possède un unique sous-groupe d'indice 3, la sous-extension $E$ est unique.

2. Montrer que $E/\mathbb{Q}$ est galoisienne et exhiber un polynôme unitaire irréductible à coefficients entiers dont c'est le corps de décomposition.

   **Indications :** Le sous-groupe d'indice 3 de $\mathbb{Z}/6\mathbb{Z}$ est distingué. La théorie de Galois montre donc que $E/\mathbb{Q}$ est galoisienne de degré 3. Par ailleurs, on remarque que $E = \mathbb{Q}(\zeta_7) \cap \mathbb{R}$, puisque $E$ est le sous-corps de $\mathbb{Q}(\zeta_7)$ fixé par la conjugaison complexe. On vérifie immédiatement que $E = \mathbb{Q}(\beta)$ où $\beta = \zeta_7 + \zeta_7^{-1}$. Le polynôme minimal de $\beta$ sur $\mathbb{Q}$ est $X^3 + X^2 - 2X - 1$. Donc $E$ est le corps de décomposition du polynôme irréductible $X^3 + X^2 - 2X - 1$.

**Exercice 3 : Irréductibilité des polynômes cyclotomiques**
Soient $m$ et $n$ deux entiers naturels premiers entre eux. Montrer que $\Phi_n$ est irréductible dans $\mathbb{Q}(\zeta_m)$.

**Indications :** Comme $m$ et $n$ sont premiers entre eux, on remarque que $\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{mn})$. On a alors :

$$\begin{aligned}\varphi(mn) &= [\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_m)(\zeta_n) : \mathbb{Q}(\zeta_m)][\mathbb{Q}(\zeta_m) : \mathbb{Q}] \\ &= \varphi(m)[\mathbb{Q}(\zeta_m)(\zeta_n) : \mathbb{Q}(\zeta_m)].\end{aligned}$$

Comme $m$ et $n$ sont premiers entre eux, $\varphi(mn) = \varphi(m)\varphi(n)$, et donc $[\mathbb{Q}(\zeta_m)(\zeta_n) : \mathbb{Q}(\zeta_m)] = \varphi(n)$. On en déduit que $\Phi_n$ est irréductible dans $\mathbb{Q}(\zeta_m)$.

**Exercice 4 : Examen 2014**
Soit $n > 2$. Soient $K_n = \mathbb{Q}(\zeta_{2^n})$ et $K_n^{\pm} = \mathbb{Q}(\zeta_{2^n} \pm \zeta_{2^n}^{-1})$.

**1.** Identifier les groupes $\mathrm{Gal}(K_n/\mathbb{Q})$ et $\mathrm{Gal}(K_n^{\pm}/\mathbb{Q})$.

**Indications :** On a $\mathrm{Gal}(K_n/\mathbb{Q}) \cong (\mathbb{Z}/2^n\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$, le deuxième isomorphisme étant donné par :

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z} \to (\mathbb{Z}/2^n\mathbb{Z})^\times, (a,b) \mapsto (-1)^a 5^b.$$

Par cet isomorphisme, $K_n^+$ est le sous-corps fixé par $(1,0)$ et $K_n^-$ est le sous-corps fixé par $(1, 2^{n-3})$. On a donc :

$$\mathrm{Gal}(K_n^+/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z})/(\mathbb{Z}/2\mathbb{Z} \times \{0\}) \cong \mathbb{Z}/2^{n-2}\mathbb{Z}$$

et

$$\mathrm{Gal}(K_n^-/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z})/\langle (1, 2^{n-3}) \rangle \cong \mathbb{Z}/2^{n-2}\mathbb{Z}.$$

**2.** Montrer que l'on a, pour chaque choix de $n-3$ signes :

$$K_n^+ = \mathbb{Q}\left(\sqrt{2 \pm \sqrt{2 \pm \sqrt{\ldots \pm \sqrt{2 \pm \sqrt{2}}}}}\right),$$

$$K_n^- = \mathbb{Q}\left(i\sqrt{2 \pm \sqrt{2 \pm \sqrt{\ldots \pm \sqrt{2 \pm \sqrt{2}}}}}\right).$$

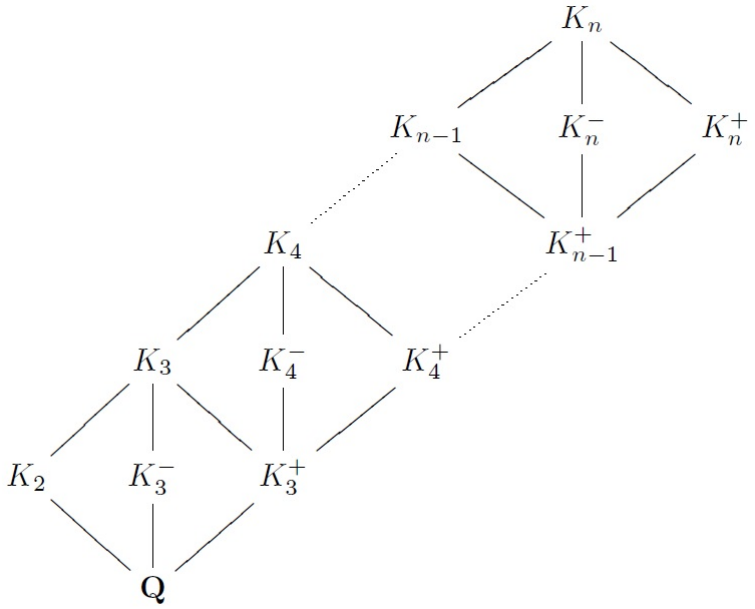
**Indications :** Faisons-le pour $K_n^+$. Pour chaque $k \in (\mathbb{Z}/2^n\mathbb{Z})^\times$, on a $K_n^+ = \mathbb{Q}(\zeta_{2^n}^k + \zeta_{2^n}^{-k})$ et $K_n^- = \mathbb{Q}(\zeta_{2^n}^k - \zeta_{2^n}^{-k})$. Il suffit donc de montrer que, quel que soit le choix de signes, il existe $k \in (\mathbb{Z}/2^n\mathbb{Z})^\times$ tel que

$$\sqrt{2 \pm \sqrt{2 \pm \sqrt{\ldots \pm \sqrt{2 \pm \sqrt{2}}}}} = \zeta_{2^n}^k + \zeta_{2^n}^{-k}.$$

Cela se prouve aisément par récurrence sur $n$.

**3.** Faire un diagramme représentant les sous-corps de $K_n$.

**Indications :** Les sous-groupes de $\mathrm{Gal}(K_n/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2^{n-2}\mathbb{Z}$ sont les $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2^k\mathbb{Z}$ pour $1 \leq k \leq n-2$, $0 \times \mathbb{Z}/2^k\mathbb{Z}$ pour $0 \leq k \leq n-2$ et $\langle(1, 2^k)\rangle$ pour $0 \leq k \leq n-2$. La théorie de Galois permet alors d'affirmer que le treillis des sous-corps de $K_n$ est :




**Exercice 5 : Sous-extensions quadratiques d'extensions cyclotomiques**

**1.** Soit $n \in \mathbb{Z} \setminus \{0\}$. Combien d'extensions quadratiques de $\mathbb{Q}$ sont contenues dans $\mathbb{Q}(\zeta_n)$ ? Vérifier en particulier qu'il y en a 7 pour $n = 60$.

**2.** (a) Soit $p$ un nombre premier impair. Calculer le discriminant de $\phi_p$ et en déduire que l'unique extension quadratique de $\mathbb{Q}$ contenue dans $\mathbb{Q}(\zeta_p)$ est $\mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right)$.

(b) Quelles sont les extensions quadratiques de $\mathbb{Q}$ contenues dans $\mathbb{Q}(\zeta_8)$ ?

(c) En déduire la liste des extensions quadratiques de $\mathbb{Q}$ contenues dans $\mathbb{Q}(\zeta_{60})$.

**3.** (a) Montrer que toute extension quadratique de $\mathbb{Q}$ est contenue dans une extension cyclotomique de $\mathbb{Q}$.

(b) *(Difficile)* Soit $d \in \mathbb{Z} \setminus \{0, 1\}$ sans facteurs carrés. Soit $n$ le plus petit entier naturel $n$ tel que $\sqrt{d} \in \mathbb{Q}(\zeta_n)$. Montrer que $n = |d|$ si $d \equiv 1 \mod 4$ et que $n = 4|d|$ si $d \not\equiv 1 \mod 4$.

**Exercice 6 : Polynômes cyclotomiques**

Soient $a$ et $b$ deux entiers naturels non nuls premiers entre eux. Le théorème de Dirichlet (1837) affirme qu'il existe une infinité de nombres premiers $p$ tels

que $p \equiv b \mod a$. Le but de cet exercice est d'établir ce théorème dans le cas particulier où $b = 1$.

**1.** Soit $P \in \mathbb{Z}[X] \setminus \mathbb{Z}$. Montrer que l'ensemble $\{d \in \mathbb{N} \mid \exists n \in \mathbb{N},\ d \mid P(n)\}$ est infini.

> **Indications :** Supposons cet ensemble $\Lambda$ fini, égal à $\{m_1, \cdots, m_r\}$. En particulier le coefficient constant $\alpha$ de $P$ est non nul puisque sinon on aurait $n \mid P(n)$ pour tout $n \geq 1$. Dès lors $P(m_1 \cdots m_r|\alpha|n)$ s'écrit sous la forme $|\alpha|Q(n)$ où $Q$ est un polynôme de $\mathbb{Z}[X] \setminus \mathbb{Z}$ à coefficient constant valant $\pm 1$. Aussi, on a $Q(n) = \pm 1$ modulo $m_k$ pour tout $1 \leq k \leq r$. En prenant $n_0 \in \mathbb{N}$ assez grand, on a $|Q(n_0)| > 1$ et l'existence d'un diviseur de $Q(n_0)$ contredit la finitude de $\Lambda$.

**2.** Soit $P = \frac{X^a - 1}{\phi_a} \in \mathbb{Z}[X]$. Montrer qu'il existe un nombre premier $p$ et un entier $x$ tels que $p$ divise $\phi_a(x)$ mais pas $P(x)$.

> **Indications :** Ecrivons $X^a - 1 = \Phi_a P$ dans $\mathbb{Z}[X]$. Par identité de Bézout, il existe $U, V \in \mathbb{Q}[X]$ vérifiant $\Phi_a U + PV = 1$ ; en chassant les dénominateurs, on a un $m \in \mathbb{N}$ non nul et des $U_0, V_0 \in \mathbb{Z}[X]$ vérifiant $\Phi_a U_0 + PV_0 = m$ dans $\mathbb{Z}[X]$. D'après 1., il existe $x \in \mathbb{N}$ et $p$ un diviseur premier de $\Phi_a(x)$ ne divisant pas $m$ ; cela implique $p \nmid P(x)$.

**3.** Calculer l'ordre de $x$ dans $\mathbb{Z}/p\mathbb{Z}$ et en déduire que $p \equiv 1 \mod a$.

> **Indications :** On déduit de la question précédente que $x^a - 1 = 0 \in \mathbb{F}_p$ mais $x^d - 1 \neq 0 \in \mathbb{F}_p$ pour $d$ un diviseur strict de $a$ (on rappelle $P = \prod_{d|a,\ d \neq a} \Phi_d$). Il s'ensuit que l'ordre de $x$ dans $\mathbb{F}_p^\times$ est $a$ et que $p - 1$ est donc divisible par $a$.

**4.** Conclure.

> **Indications :** On suppose que l'ensemble des nombres premiers $p$ tels que $p \equiv 1 \mod a$ est fini. On le note $\{p_1, \ldots, p_r\}$. On applique alors la démarche précédente avec $ap_1 \cdots p_r$ au lieu de $a$ : cela permet de trouver un nombre premier $p_{r+1} \cong 1 \mod ap_1 ... p_r$. Absurde !

**Exercice 7 : Galois inverse sur $\mathbb{Q}$, cas abélien fini**

On utilisera à bon escient les résultats :

- sur la structure des groupes abéliens finis ;
- sur la progression arithmétique faible de Dirichlet (exercice 6).

En pensant aux corps cyclotomiques, montrer que tout groupe abélien fini est groupe de Galois d'une extension galoisienne sur $\mathbb{Q}$.

**Indications :** Soient $G$ un groupe abélien fini et $n_1 \mid n_2 \mid \cdots \mid n_r$ ses facteurs invariants, de sorte que l'on a $G \cong \prod_i \mathbb{Z}/n_i\mathbb{Z}$. Par Dirichlet faible, il existe des premiers $p_i$ deux à deux distincts et respectivement congrus à 1 modulo $n_i$. Posons $m = \prod_i p_i$ et considérons $\xi$ une racine primitive $m$-ème de l'unité dans $\mathbb{C}$. L'extension $\mathbb{Q} \subseteq \mathbb{Q}(\xi)$ est galoisienne de groupe de Galois isomorphe à

$$(\mathbb{Z}/m\mathbb{Z})^\times \cong \prod\nolimits_i (\mathbb{Z}/p_i\mathbb{Z})^\times \cong \prod\nolimits_i \mathbb{Z}/(p_i - 1)\mathbb{Z}.$$

On en considère alors le sous-groupe $H = \prod_i n_i\mathbb{Z}/p_i\mathbb{Z}$ et par suite le corps fixe $K = \mathbb{Q}(\xi)^H$. Parce que $(\mathbb{Z}/m\mathbb{Z})^\times$ est abélien, tout sous-groupe est normal, et l'extension $\mathbb{Q} \subseteq K$ est donc galoisienne de groupe de Galois isomorphe à $(\mathbb{Z}/m\mathbb{Z})^\times/H \cong G$.

### Exercice 8 : Examen 2014

Pour quelles valeurs de $n \geq 1$ le corps $\mathbb{Q}(\zeta_n)$ (resp. $\mathbb{Q}(\zeta_n) \cap \mathbb{R} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$) s'écrit-il sous la forme $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, ..., \sqrt{a_r})$ où $a_j \in \mathbb{Q}^\times$ ? Expliciter les $a_j$ dans chaque cas.

**Indications :** Soit $n \geq 1$ tel que le corps $\mathbb{Q}(\zeta_n)$ s'écrit sous la forme $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, ..., \sqrt{a_r})$ avec $a_j \in \mathbb{Q}^\times$. Alors $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ est de 2-torsion. On en déduit que $n \in \{1, 2, 3, 4, 6, 8, 12, 24\}$. Réciproquement :
$n = 1$ : $\mathbb{Q}(\zeta_n) = \mathbb{Q}$.
$n = 2$ : $\mathbb{Q}(\zeta_n) = \mathbb{Q}$.
$n = 3$ : $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\sqrt{-3})$.
$n = 4$ : $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\sqrt{-1})$.
$n = 6$ : $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\sqrt{-3})$.
$n = 8$ : $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$.
$n = 12$ : $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\sqrt{-1}, \sqrt{3})$.
$n = 24$ : $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3})$.
Soit maintenant $n \geq 3$ tel que le corps $L_n = \mathbb{Q}(\zeta_n) \cap \mathbb{R}$ s'écrit sous la forme $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, ..., \sqrt{a_r})$ avec $a_j \in \mathbb{Q}^\times$. Alors $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times/\{\pm 1\}$ est de 2-torsion. On en déduit que $n \in \{3, 4, 5, 6, 8, 10, 12, 24\}$. Réciproquement :
$n = 3$ : $L_n = \mathbb{Q}$.
$n = 4$ : $L_n = \mathbb{Q}$.
$n = 5$ : $L_n = \mathbb{Q}(\sqrt{5})$.
$n = 6$ : $L_n = \mathbb{Q}$.
$n = 8$ : $L_n = \mathbb{Q}(\sqrt{2})$.
$n = 10$ : $L_n = \mathbb{Q}(\sqrt{5})$.
$n = 12$ : $L_n = \mathbb{Q}(\sqrt{3})$.
$n = 24$ : $L_n = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
Pour $n = 1$ ou 2, le résultat est évident.

### Exercice 9 : Cyclotomie sur $\mathbb{F}_q$

Soient $p$ un nombre premier, $q$ une puissance de $p$ et $r \geq 1$ un entier.

**1.** Déterminer le groupe $\mu_{p^r}(\mathbb{F}_q)$ des racines $p^r$-èmes de l'unité dans $\mathbb{F}_q$.

**Indications :** Comme $p^r$ et $q - 1$ sont premiers entre eux, il existe $a, b \in \mathbb{Z}$ vérifiant $p^r a + (q-1)b = 1$. Si $x$ est un élément de $\mu_{p^r}(\mathbb{F}_q)$, en particulier $x$ est non nul et on a $x = (x^{p^r})^a (x^{q-1})^b = 1$. D'où l'égalité $\mu_{p^r}(\mathbb{F}_q) = \{1\}$.

**2.** Montrer que toute extension finie de $\mathbb{F}_q$ est cyclotomique, c'est-à-dire engendrée par des racines de l'unité.

> **Indications :** Une extension de degré $r$ de $\mathbb{F}_q$ est le corps de décomposition de $X^{q^r-1}-1$.

Soient $n \geq 1$ un entier et $\Phi_n \in \mathbb{Z}[X]$ le $n$-ème polynôme cyclotomique sur $\mathbb{C}$. On note $\overline{\Phi}_n^{(p)}$ la réduction de $\Phi_n$ modulo $p$, que l'on peut voir comme un polynôme sur $\mathbb{F}_q$.
Supposons $n$ premier à $p$.

**3.** Montrer que les racines de $\overline{\Phi}_n^{(p)}$ sont exactement les racines primitives $n$-èmes de l'unité dans $\mathbb{F}_q$.

> **Indications :** On a $\overline{X^n-1}^{(p)} = \prod_{d|n} \overline{\Phi}_n^{(p)}$ et l'affirmation est alors immédiate par récurrence.

**4.** Montrer que $\overline{\Phi}_n^{(p)}$ est irréductible sur $\mathbb{F}_q$ si et seulement si $q$ est un générateur de $(\mathbb{Z}/n\mathbb{Z})^\times$.

> **Indications :** Supposons $\overline{\Phi}_n^{(p)}$ irréductible sur $\mathbb{F}_q$ et soit $\xi \in \overline{\mathbb{F}_p}$ une racine de $\overline{\Phi}_n^{(p)}$. Alors $\xi$ est de degré $\varphi(n)$ et on a $\xi^{q^{\varphi(n)}} = \xi$ mais $\xi^{q^f} \neq \xi$ si $1 \leq f < \varphi(n)$. Comme $\xi$ est une racine primitive $n$-ème de l'unité, cela signifie $n \mid q^{\varphi(n)}-1$ mais $n \nmid q^f - 1$. En particulier, $q$ est d'ordre $\varphi(n)$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$ et donc $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique engendré par $q$. Pour la réciproque, il refaire le même raisonnement dans l'autre sens.

**5.** En déduire que la réduction de $\Phi_8$ modulo $p$ est réductible pour tout nombre premier $p$.

> **Indications :** Le groupe $(\mathbb{Z}/8\mathbb{Z})^\times$ n'est pas cyclique. Donc $\Phi_8$ modulo $p$ est irréductible pour $p > 2$. De plus, $\Phi_8 \equiv (X-1)(X+1)(X^2+1) \mod 2$.

## Exercice 10 : Extensions de Kummer

Soit $K$ un corps. Soit $P = X^n - a \in \mathbb{Q}[X]$ avec $n \in \mathbb{N}^*$ et $a \in K^\times$.

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

> **Indications :** Évident par définition.

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

$$GA_1(\mathbb{Z}/n\mathbb{Z}) = \left\{ \begin{pmatrix} u & b \\ 0 & 1 \end{pmatrix} | u \in (\mathbb{Z}/n\mathbb{Z})^\times, b \in \mathbb{Z}/n\mathbb{Z} \right\}.$$

> **Indications :** Soit $\sigma \in \mathrm{Gal}(L/K)$. Soient $u \in (\mathbb{Z}/n\mathbb{Z})^\times$ et $b \in \mathbb{Z}/n\mathbb{Z}$ tels que $\sigma(\zeta_n) = \zeta_n^u$ et $\sigma(\sqrt[n]{a})$. Posons :
>
> $$f(\sigma) = \begin{pmatrix} u & b \\ 0 & 1 \end{pmatrix}.$$
>
> On vérifie aisément que $f : \mathrm{Gal}(L/K) \to GA_1(\mathbb{Z}/n\mathbb{Z})$ est un morphisme de groupes injectif.

**3.** On suppose que $K = \mathbb{Q}$, que $n$ est égal à un premier $p$ et que $a \notin (\mathbb{Q}^\times)^p$. Soit $L$ un corps de décomposition de $P$ sur $\mathbb{Q}$. Calculer le groupe $\mathrm{Gal}(L/\mathbb{Q})$.

**Indications :** Calculons $[L : \mathbb{Q}]$. On a bien sûr :

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

Or par la théorie de Kummer, $[L : \mathbb{Q}(\zeta_p)]$ est l'ordre de $a$ dans $\mathbb{Q}(\zeta_p)^\times/\mathbb{Q}(\zeta_p)^{\times p}$. Donc $[L : \mathbb{Q}(\zeta_p)]$ vaut 1 ou $p$. Si $a$ était une puissance $p$-ième dans $\mathbb{Q}(\zeta_p)$, alors :

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

serait une puissance $p$-ième dans $\mathbb{Q}$ : absurde, car $a \notin (\mathbb{Q}^\times)^p$. On en déduit que $[L : \mathbb{Q}(\zeta_p)] = p$.

Nous avons donc montré que $[L : \mathbb{Q}] = p(p-1)$, et donc que $\mathrm{Gal}(L/\mathbb{Q})$ est un sous-groupe de $GA_1(\mathbb{Z}/p\mathbb{Z})$ d'ordre $p(p-1)$. Comme $GA_1(\mathbb{Z}/p\mathbb{Z})$ est lui-même d'ordre $p(p-1)$, on obtient $\mathrm{Gal}(L/\mathbb{Q}) \cong GA_1(\mathbb{Z}/p\mathbb{Z})$

## Exercice 11 : Irréductibilité de polynômes

Soient $K$ un corps, $a \in K$, $r \geq 1$ et $p$ un nombre premier. Soit $P = X^{p^r} - a \in K[X]$.

**1.** On suppose que $p \neq 2$ ou $\mathrm{Car}(K) = p$ ou $r = 1$. Montrer que $P$ est irréductible si, et seulement si, $a \notin K^p$.

**Indications :** Si $a \in K^p$, alors $P$ n'est pas irréductible puisque

$$P = (X^{p^{r-1}} - b^{p^{r-1}})(X^{(p-1)p^{r-1}} + X^{(p-2)p^{r-1}} b^{p^{r-1}} + X^{(p-3)p^{r-1}} b^{2p^{r-1}} + ...),$$

où $b \in K$ est tel que $b^p = a$.
Réciproquement :

- Supposons $a \notin K^p$ et $p \neq 2$ et $\mathrm{Car}(K) \neq p$. La théorie de Kummer impose que $[K(\sqrt[p^r]{a}, \zeta_{p^r}) : K(\zeta_{p^r})]$ est l'ordre de la classe de $a$ dans $K(\zeta_p)^\times/(K(\zeta_p)^\times)^{p^r}$. Comme $a \notin K^p$, cet ordre est égal à $p^r$, et donc $P$ est irréductible sur $K(\zeta_{p^r})$. A fortiori, $P$ est irréductible sur $K$.
- Supposons $a \notin K^p$ et $\mathrm{Car}(K) = p$. Dans ce cas, $P$ est irréductible (voir proposition 6.3 du polycopiéde Jan Nekovar).
- Le cas restant ($p = 2$ et $r = 1$) est évident.

**2.** On suppose que $p = 2$, $\mathrm{Car}(K) \neq 2$ et $r \neq 1$. Montrer que $P$ est irréductible si, et seulement si, $a \notin K^2$ et $-4a \notin K^4$.

**Indications :** Si $a \in K^2$, on écrit $a = b^2$ et $P = (X^{2^{r-1}} + b)(X^{2^{r-1}} - b)$ n'est pas irréductible.
Si $-4a \in K^4$, on écrit $-4a = b^4$ et $P = (X^{2^{r-1}} + X^{2^{r-2}}b + \frac{b^2}{2})(X^{2^{r-1}} - X^{2^{r-2}}b + \frac{b^2}{2})$ est réductible.

Pour la réciproque, on aura besoin des lemmes suivants :

**Lemme 1 :** Soient $L$ un corps et $a \in L$ tels que $a \notin K^2$ et $-4a \notin K^4$. Alors $P = X^4 - a \in L[X]$ est irréductible.

*Preuve :* Comme $a \notin L^2$, $P$ n'admet pas de racines. De plus, si $b, c, d \in L$ sont tels que $P = (X^2 + bX + c)(X^2 - bX + d)$, on a les relations $c + d = b^2$, $b(c - d) = 0$ et $cd = -a$. On obtient alors que $b = 0$ ou $c = d$. Si $b = 0$, alors $c = -d$ et $c^2 = a$ : absurde ! Si $c = d$, alors $b^2 = 2c$ et $c^2 = -a$, et donc $b^4 = -4a$ : absurde ! On en déduit que $P$ est bien irréductible. □

**Lemme 2 :** Soient $L$ un corps et $a \in L$ tel que $P = X^4 - a \in L[X]$ est irréductible. Alors $X^8 - a \in L[X]$ est irréductible.

*Preuve :* Comme $X^4 - a$ est irréductible, on a $a \notin L^2$ et $-4a \notin L^4$. Si on avait $\sqrt{a} \in L(\sqrt{a})^2$, il existerait $x, y \in L$ tels que $\sqrt{a} = (x + y\sqrt{a})^2$, et on aurait $x^2 + ay^2 = 0$ et $2xy = 1$ : on obtiendrait alors $-4a = (2x)^4$, ce qui est absurde. Si on avait $-4\sqrt{a} \in L(\sqrt{a})^4$, on aurait $N_{L(\sqrt{a})/L}(-4\sqrt{a}) = -16a \in L^4$, donc $-a \in L^4$ et $L(\sqrt{a}) = L(i)$ : on en déduit que $a = 4 \cdot \frac{-1}{4} \cdot (-a) = 4(1+i)^{-4} \cdot (-a) \in L^2$, ce qui est absurde. On en déduit que $\sqrt{a} \notin L(\sqrt{a})^2$ et $-4\sqrt{a} \notin L(\sqrt{a})^4$. En utilisant le lemme 1, cela montre que $X^4 - \sqrt{a} \in L(\sqrt{a})[X]$ est irréductible, et donc que $[L(\sqrt[8]{a}) : L(\sqrt{a})] = 4$. Par conséquent, $[L(\sqrt[8]{a}) : L] = 8$ et $X^8 - a \in L[X]$ est irréductible. □

On revient maintenant à l'exercice. Supposons $a \notin K^2$ et $-4a \notin K^4$. On procède par récurrence sur $r$.
- Le cas $r = 2$ a été prouvé dans le lemme 1.
- Soit $r \geq 2$ tel que $X^{2^r} - a$ est irréductible sur $K$. Alors $[K(a^{\frac{1}{2^r}}) : K] = 2^r$ et $[K(a^{\frac{1}{2^r}}) : K(a^{\frac{1}{2^{r-2}}})] = 4$. On en déduit que $X^4 - a^{\frac{1}{2^{r-2}}} \in K(a^{\frac{1}{2^{r-2}}})[X]$ est irréductible. Par conséquent, en utilisant le lemme 2, $X^8 - a^{\frac{1}{2^{r-2}}} \in K(a^{\frac{1}{2^{r-2}}})[X]$ est irréductible. Cela prouve que $[K(a^{\frac{1}{2^{r+1}}}) : K(a^{\frac{1}{2^{r-2}}})] = 8$ et donc que $[K(a^{\frac{1}{2^{r+1}}}) : K] = 2^{r+1}$. On conclut que $X^{2^{r+1}} - a \in K[X]$ est irréductible.

## Exercice 12 : Théorie de Kummer

Soit $n > 1$. Soit $K$ un corps tel que $|\mu_n(K)| = n$.

**1.** Soient $a_1, ..., a_r$ des éléments de $K^\times$. Soit $L$ un corps de décomposition de $(T^n - a_1)....(T^n - a_r)$.

(a) Vérifier que $\mathrm{Gal}(L/K)$ est un groupe abélien de $n$-torsion.

Soit $\Delta$ le sous-groupe de $K^\times/K^{\times n}$ engendré par les classes de $a_1, ..., a_r$. On note aussi :

$$\Delta' := \mathrm{Ker}(K^\times/K^{\times n} \to L^\times/L^{\times n}).$$

(b) Vérifier que $\Delta$ est un sous-groupe de $\Delta'$.
On définit :

$$[.,.] : \mathrm{Gal}(L/K) \times \Delta' \to \mu_n(K), (\sigma, \overline{a}) \mapsto [\sigma, \overline{a}] := \frac{\sigma(\alpha)}{\alpha},$$

où $\alpha$ est une racine $n$-ième de $a$ dans $L$.
(c) Vérifier que $[.,.]$ est bien définie.
(d) Montrer que $[.,.]$ est une application bilinéaire non dégénérée. Montrer de plus que l'orthogonal de $\Delta$ pour $[.,.]$ est réduit à 0.
(e) En déduire que :
(i) l'application $f : \mathrm{Gal}(L/K) \to \mathrm{Hom}(\Delta', \mu_n(K)), \sigma \mapsto (\overline{a} \mapsto [\sigma, \overline{a}]))$ est un morphisme de groupes.
(ii) la composée $\mathrm{Gal}(L/K) \xrightarrow{f} \mathrm{Hom}(\Delta', \mu_n(K)) \xrightarrow{\mathrm{Res}} \mathrm{Hom}(\Delta, \mu_n(K))$ est injective.
(iii) l'application $g : \Delta' \to \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n(K)), \overline{a} \mapsto (\sigma \mapsto [\sigma, \overline{a}]))$ est un morphisme de groupes injectif.
(f) Montrer que $\Delta = \Delta'$ et que les morphismes $f$ et $g$ sont en fait des isomorphismes.

**2.** Soit $M$ une extension galoisienne finie de $K$.
(a) Soit $\chi : \mathrm{Gal}(M/K) \to \mu_n(K)$ un morphisme de groupes. Montrer qu'il existe $\alpha \in M^\times$ tel que $\alpha^n \in K^\times$ et $\chi(\sigma) = \sigma(\alpha)/\alpha$ pour tout $\sigma \in \mathrm{Gal}(M/K)$. On pourra utiliser le fait que les éléments de $\mathrm{Gal}(M/K)$ sont linéairement indépendants sur $K$.
(b) Supposons que $\mathrm{Gal}(M/K)$ est un groupe abélien de $n$-torsion. Montrer qu'il existe $a_1, ..., a_r \in K^\times$ tels que $L$ est un corps de décomposition de $(T^n - a_1)....(T^n - a_r)$.

**Indications :** Lire le paragraphe 15 du chapitre III du polycopié de Jan Nekovar.

### Exercice 13 (difficile) : Extensions abéliennes

Soient $K$ un corps de caractéristique nulle et $n$ un entier naturel. On suppose que, pour toute extension finie $L$ de $K$, l'indice $[L^\times : (L^\times)^n]$ est fini. Montrer que le corps $K$ possède un nombre fini d'extensions abéliennes de degré $n$.

### Exercice 14 : Extensions cycliques

Soient $K$ un corps et $\overline{K}$ une clôture algébrique de $K$.

**1.** Soit $\sigma \in \mathrm{Aut}(\overline{K}/K)$. Montrer que toute extension finie de $\overline{K}^{\langle\sigma\rangle}$ dans $\overline{K}$ est cyclique.

**Indications :** Soit $M$ une extension finie de $L = \overline{K}^{\langle\sigma\rangle}$ contenue dans $\overline{K}$. Notons $G = \mathrm{Aut}(M/L)$. Soit $\tau = \sigma|_M \in G$. On remarque que $L = M^{\langle\tau\rangle}$. Donc d'après le lemme d'Artin, $M/L$ est galoisienne de groupe de Galois $G = \langle\tau\rangle$. C'est donc une extension cyclique.

**2.** Montrer que si toute extension finie de $K$ dans $\overline{K}$ est cyclique, alors il existe $\sigma \in \mathrm{Aut}(\overline{K}/K)$ tel que $K = \overline{K}^{\langle\sigma\rangle}$.

> **Indications :** On commence par un lemme : **Lemme :** Soit $n \geq 1$. Le corps $K$ possède au plus une extension de de degré $n$ contenue dans $\overline{K}$.
>
> *Preuve :* Soient $M_1$ et $M_2$ deux telles extensions. Soit $N$ une extension finie de $K$ contenant $M_1$ et $M_2$ et contenue dans $\overline{K}$. Comme $N/K$ est cyclique, il existe au plus une extension de degré $n$ de $K$ contenue dans $N$. Donc $M_1 = M_2$. □
>
> Pour chaque nombre premier $p$, on note $a_p$ la borne supérieure de l'ensemble des entiers naturels $a$ tels qu'il existe une extension finie $L$ de $K$ de degré $p^a$. Pour chaque premier $p$, pour chaque $b \leq a_p$, on se donne $x_{p,b}$ tel que $K(x_{p,b})/K$ est de degré $p^b$. Soit $x \in \overline{K}$. Soit $n = [K(x) : K]$. On écrit $n = p_1^{c_1}...p_s^{c_s}$. On remarque $K(x)/K$ possède une extension intermédiaire de degré $p_i^{c_i}$ pour $1 \leq i \leq s$. On en déduit que $K(x) = K(x_{p_1,c_1}, ..., x_{p_s,c_s})$. Par conséquent, $\overline{K} = K((x_{p,b})_{p,b})$. En renumérotant, il existe $x_1, x_2, ... \in \overline{K}$ tels que $\overline{K} = K((x_i)_{i\geq 1})$. On note $K_n = K(x_1, ..., x_n)$ pour chaque $n \geq 0$. Par récurrence, on construit une suite $(\sigma_n)$ où, pour chaque $n$, $\sigma_n$ est un générateur de $\mathrm{Gal}(K_n/K)$ et $\sigma_{n+1}|_{K_n} = \sigma_n$. Soit alors $\sigma$ l'unique élément de $\mathrm{Aut}(\overline{K}/K)$ qui prolonge tous les $\sigma_n$. Comme pour chaque $n$ on a $K = K_n^{\langle\sigma_n\rangle}$, on a aussi $K = \overline{K}^{\langle\sigma\rangle}$.

**Exercice 15 : Sous-corps d'un corps algébriquement clos**

Soit $\Omega$ un corps algébriquement clos de caractéristique nulle. Soit $K$ un sous-corps de $\Omega$ tel que l'extension $\Omega/K$ est de degré fini. Le but de cet exercice est de montrer que $\Omega = K(\sqrt{-1})$.

**1.** Expliquer pourquoi $\Omega/K$ est galoisienne.

Soit $i$ une racine de $X^2 + 1$ dans $\Omega$. On pose $G = \mathrm{Gal}(\Omega/K(i))$. On suppose que $G$ n'est pas trivial et on se donne $p$ un nombre premier divisant l'ordre de $G$.

**2.** Montrer qu'il existe un sous-corps $L$ de $\Omega$ contenant $K(i)$ tel que $\Omega/L$ est une extension galoisienne de degré $p$.

**3.** Montrer qu'il existe $a \in L$ tel que le polynôme $P = X^p - a \in L[X]$ est irréductible et $\Omega = L[X]/(P)$.

**4.** Soit $\alpha \in \Omega$ une racine de $P$. Calculer $\prod_{\sigma\in\mathrm{Gal}(\Omega/L)} \sigma(\alpha)$.

**5.** Conclure.

**6.** Montrer qu'un élément non trivial de $\mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$ d'ordre fini est forcément d'ordre 2.

**Exercice 16 : Partiel 2013**

Soit $\overline{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$ et soit $a \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$.

**1.** Montrer qu'il existe un sous-corps $K$ de $\overline{\mathbb{Q}}$ tel que $a \notin K$ et que tout sous-corps de $\overline{\mathbb{Q}}$ contenant strictement $K$ contient $a$ ; on dit que $K$ est un sous-corps de $\overline{\mathbb{Q}}$ maximal sans $a$.

On choisit un nombre premier $p$ divisant $[K(a) : K]$. Soit $L$ une extension

finie non triviale de $K$ contenue dans $\overline{\mathbb{Q}}$. On note $M$ la clôture normale de $L$ dans $\overline{\mathbb{Q}}$ et $G := \mathrm{Gal}(M/K)$.

**2.** Montrer que $p$ divise $[L : K]$.

**3.** Montrer que $[L : K]$ est une puissance de $p$.

**4.** Montrer que $[K(a) : K] = p$ et que $K(a)$ est la seule sous-extension de $\overline{\mathbb{Q}}/K$ de degré $p$ sur $K$.

**5.** Montrer que $G$ est cyclique, puis que toute extension finie de $K$ est galoisienne cyclique.

**6.** Montrer qu'il existe $b \in K(a)$, avec $b^p \in K$, tel que $K(a) = K(b)$.

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

**Exercice 17 : Extensions d'Artin-Schreier**

Soient $K$ un corps de caractéristique $p > 0$ et $L/K$ une extension galoisienne de degré $p$. Soit $\sigma$ un générateur de $\mathrm{Gal}(L/K)$.

**1.** Montrer qu'il existe $x \in L$ vérifiant $\sigma(x) - x = 1$.

**Indications :** On a $\mathrm{Ker}(\sigma - \mathrm{Id}) = K$ et en tant qu'application $K$-linéaire $\sigma - \mathrm{Id}$ est donc de rang $p - 1$. De plus, parce que $\sigma$ est d'ordre $p$ dans $\mathrm{Gal}(L/K)$, on a $(\mathrm{Id} + \sigma + \cdots + \sigma^{p-1}) \circ (\sigma - \mathrm{Id}) = 0$ ; d'où l'inclusion $\mathrm{Im}(\sigma - \mathrm{Id}) \subseteq \mathrm{Ker}(\mathrm{Id} + \sigma + \cdots + \sigma^{p-1})$. Par indépendance linéaire des caractères, $\mathrm{Id} + \sigma + \cdots + \sigma^{p-1}$ n'est pas identiquement nulle sur $L$ et on a donc $\mathrm{Im}(\sigma - \mathrm{Id}) = \mathrm{Ker}(\mathrm{Id} + \sigma + \cdots + \sigma^{p-1}) \supseteq K$.

**2.** Montrer qu'il existe $a \in K^\times$ tel que $L$ soit le corps de décomposition de $X^p - X - a$.

**Indications :** Soit $x \in L$ vérifiant $\sigma(x) - x = 1$. Le polynôme minimal de $x$ sur $K$ est alors :

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

En posant $a = x^p - x$, on obtient que $L$ est le corps de décomposition de $X^p - X - a$.

**Exercice 18 : Partiel 2011**

Considérons le polynôme $P = X^4 - X - 1 \in \mathbb{Q}[X]$.

**1.** Montrer que $P$ a exactement deux racines réelles distinctes $x_1$ et $x_2$.

**2.** On écrit $(X - x_1)(X - x_2) = X^2 + aX + b$. Calculer $[\mathbb{Q}(a^2) : \mathbb{Q}]$.

**3.** En déduire qu'aucune des racines de $P$ n'est constructible à la règle et au compas.

**Indications :** Voir le corrigé du partiel 2011.

**Exercice 19 : Constructibilité et angles**

Soit $n$ un entier naturel. Montrer que l'angle de $n^\circ$ est constructible si, et seulement si, 3 divise $n$.

**Exercice 20 : Examen 2012**

Le polynôme $X^5 - 5X^2 + 1 \in \mathbb{Q}[X]$ est-il résoluble par radicaux ?

> **Indications :** Notons $P = X^5 - 5X^2 + 1$. Le polynôme $P(X-1)$ est 5-Eisenstein. On en déduit que $P$ est irréductible. On en déduit que le groupe de Galois de $P$ s'identifie à un sous-groupe transitif de $S_5$. Il contient donc un 5-cycle. On vérifie que $P$ possède exactement deux racines non réelles. On en déduit que la conjugaison complexe s'identifie à une transposition de $S_5$. Comme une transposition et un 5-cycle engendrent $S_5$, on en déduit que le groupe de Galois de $P$ est $S_5$. Ce groupe n'étant pas résoluble, $P$ n'est pas résoluble par radicaux.

**Exercice 21 : Un critère de résolubilité**

Soient $p$ un nombre premier et $K$ un corps de caractéristique strictement plus grande que $p$. Soit $f \in K[X]$ un polynôme irréductible de degré $p$. Soit $L$ un corps de décomposition de $f$ sur $K$. On suppose que $f$ possède deux racines distinctes $\alpha$ et $\beta$ dans $L$ telles que $L = K(\alpha, \beta)$. Montrer que l'extension $L/K$ est résoluble par radicaux.

> **Indications :** Voir l'implication (5) $\Rightarrow$ (2) du théorème 17.11 du chapitre III du polycopié de Jan Nekovar.

**Exercice 22 : Résolubilité par radicaux réels**

Soient $K$ un sous-corps de $\mathbb{R}$, $p > 2$ un nombre premier et $a \in K$ qui n'est pas une puissance $p$-ème dans $K$. Soit $x \in \mathbb{R}$ vérifiant $x^p = a$.

**1.** Montrer que $K \subseteq K(x)$ n'est pas galoisienne.

> **Indications :** Si $K \subseteq K(x)$ était galoisienne, elle contiendrait les conjugués de $x$, c'est-à-dire les $\xi^k x$ avec $\xi$ une racine primitive $p$-ème de 1 et $0 \leq k \leq p-1$. Or, parce que $p$ est impair, on a $\xi^k \notin \mathbb{R} \supseteq K(x)$ pour tout $1 \leq k \leq p-1$.

Une extension $K \subseteq L$ est dite *radicale réelle* s'il existe une tour d'extensions

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n \subseteq \mathbb{R}$$

telle que $L \subseteq K_n$ et, pour tout $i$, $K_{i+1} = K_i(x_i)$ avec $x_i^{n_i} \in K_i$ pour un certain entier $n_i \geq 1$. Un polynôme est dit *résoluble par radicaux réels* si son corps de décomposition l'est.

Soit $K \subseteq L$ une extension galoisienne radicale réelle.

**2.** En se ramenant à une tour avec degrés successifs premiers, montrer que $[L : K]$ est une puissance de 2.

**Indications :** Par définition, il existe une tour d'extensions radicales réelles élémentaires

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_n \subseteq \mathbb{R} \tag{1}$$

avec $L \subseteq K_n$. Si $K_{i+1} = K_i(x_i)$ avec $x_i^{n_i} \in K_i$ avec $n_i = \prod_{j=1}^{s} p_j^{(i)}$ avec les $p_j^{(i)}$ premiers (éventuellement avec répétition), on peut insérer des intermédiaires du type

$$K_i \subseteq K_i\Big(x_i^{\prod_{j=1}^{s-1} p_j^{(i)}}\Big) \subseteq K_i\Big(x_i^{\prod_{j=1}^{s-2} p_j^{(i)}}\Big) \subseteq \cdots \subseteq K_i\Big(x_i^{p_1^{(i)}}\Big) \subseteq K_{i+1} = K_i(x_i)$$

à chaque cran dans la suite (1). De cette manière, on peut supposer que dans (1), on a $[K_{i+1} : K_i]$ premier ; et puisque $K_n$ est inclus dans $\mathbb{R}$, ceux que l'on a insérés en plus le sont aussi. On montre ensuite par récurrence sur la longueur $n$ d'une telle suite que $K_1 \subseteq K_n$ est de degré $2^n$. Pour $n = 1$, le 1. donne que le degré est 2 et c'est fini. Ensuite, on applique l'hypothèse de récurrence à $K_1 \subseteq K_n$ avec $K_1 \subseteq L$ galoisienne et qui s'insère dans une suite de type (1) de longueur $n-1$ : $K_1 \subseteq K_n$ de degré $2^{n-1}$. De plus, $K_0 \subseteq K_1$ est de degré $p$. Par lemme de Cauchy ou théorème de Sylow, $\mathrm{Gal}(K_n^{\mathrm{norm}}/K)$ possède un sous-groupe $H$ d'ordre $p$. On note $M = K_n^H$ qui est alors d'indice $p$ dans $K_n$ et $M \subseteq K_n$ est galoisienne par lemme d'Artin. On a alors $p = 2$ par 1. et la récurrence est prouvée. Au final, $[L : K] \mid [K_n : K_0]$ est aussi une puissance de 2.

**3.** Donner un exemple de telle extension.

**Indications :** On peut prendre $\mathbb{Q}(\sqrt{2-\sqrt{2}}, \sqrt{2+\sqrt{2}})/\mathbb{Q}$ ou $\mathbb{Q}(\sqrt{2-\sqrt{3}}, \sqrt{2+\sqrt{3}})/\mathbb{Q}$.

**4.** Montrer que l'extension $\mathbb{Q} \subseteq \mathbb{Q}\big(\cos(\frac{2\pi}{7})\big)$ est radicale mais pas radicale réelle.

**Indications :** Comme $2\cos\big(\frac{2\pi}{7}\big)$ est zéro de $P := X^3 + X^2 - 2X - 1 \in \mathbb{Q}[X]$, qui est irréductible, $\cos\big(\frac{2\pi}{7}\big)$ est de degré 3 sur $\mathbb{Q}$. De plus, les autres racines de $P$ étant $2\cos\big(\frac{4\pi}{7}\big)$ et $2\cos\big(\frac{6\pi}{7}\big)$, et comme on a $\cos\big(\frac{4\pi}{7}\big) = 2\cos\big(\frac{2\pi}{7}\big)^2 - 1$, l'extension $\mathbb{Q} \subseteq \mathbb{Q}\big(\cos(\frac{2\pi}{7})\big)$ est galoisienne, de groupe de Galois isomorphe à $\mathbb{Z}/3\mathbb{Z}$. Elle est donc radicale (car le groupe de Galois est résoluble) mais pas radicale réelle par 2.

Soit $P \in K[X]$ un polynôme irréductible de degré 3.

**5.** Montrer que si $P$ a trois racines réelles $x, y, z$, alors aucune des extensions $K(x)/K$, $K(y)/K$ et $K(z)/K$ n'est radicale réelle (résultat dû à Hölder).

**Indications :** Supposons $K \subseteq K(x)$ radicale réelle. De plus $K(x) \subseteq K(x, y)$ est radicale quadratique ; et parce que $K(x, y)$ est un sous-corps de $\mathbb{R}$, $K \subseteq K(x, y)$ est radicale réelle. Or cette dernière est galoisienne, de degré 3 ou 6, ce qui contredit 2.

On rappelle les formules de Tartaglia-Cardan : les zéros du polynôme $X^3 +$

$bX + c$ sont les

$$\xi\sqrt[3]{-\frac{c}{2}+\sqrt{\frac{c^2}{4}+\frac{b^3}{27}}}+\xi^2\sqrt[3]{-\frac{c}{2}-\sqrt{\frac{c^2}{4}+\frac{b^3}{27}}}$$

pour $\xi$ parcourant les racines 3-èmes de l'unité.

**6.** Montrer que si $P$ n'a qu'une racine réelle $x$, alors $K(x)/K$ est radicale réelle.

> **Indications :** Quitte à utiliser le changement de variables usuel (qui ne modifie pas le nombre de racines réelles), on va supposer $P = X^3 + bX + c \in K[X]$ irréductible. Posons $\delta = \frac{c^2}{4} + \frac{b^3}{27}$.
> Si $\delta$ est strictement négatif, $\sqrt{\delta}$ est imaginaire pur et $-\frac{c}{2} \pm \sqrt{\delta}$ sont deux complexes conjugués. Il s'ensuite que leurs racines troisièmes sont aussi des complexes conjugués : on peut en choisir deux privilégiées compatibles, que l'on va noter $\sqrt[3]{-\frac{c}{2} \pm \sqrt{\delta}}$ et en appliquant la conjugaison complexe dans les formules de Cardan, on voit que les trois racines sont réelles. Si $\delta$ est nul, on a une racine double qui ne peut donc pas être complexe et donc trois racines réelles aussi.
> Au final on a dans notre cas $\delta > 0$. Alors $-\frac{c}{2} \pm \sqrt{\delta}$ sont réels et possèdent une racine troisième réelle que l'on va noter $\sqrt[3]{-\frac{c}{2} \pm \sqrt{\delta}}$. On a alors $x = \sqrt[3]{-\frac{c}{2} + \sqrt{\delta}} + \sqrt[3]{-\frac{c}{2} - \sqrt{\delta}}$, et il suffit de considérer la tour
>
> $$K \subseteq K(\sqrt{\delta}) \subseteq K\Big(\sqrt[3]{-\frac{c}{2} + \sqrt{\delta}}\Big) \subseteq K\Big(\sqrt[3]{-\frac{c}{2} + \sqrt{\delta}}, \sqrt[3]{-\frac{c}{2} - \sqrt{\delta}}\Big) \subseteq \mathbb{R}$$
>
> pour voir que $K \subseteq K(x)$ est radicale réelle.

**Exercice 23 : Descente pour les espaces vectoriels**

Soit $n \geq 1$ un entier. Soient $F \subseteq E$ une extension galoisienne (ie. normale et séparable) finie, de base $\{1, x_1, \ldots, x_{n-1}\}$. Notons $G = \mathrm{Gal}(E/F)$.

**1.** Rappeler pourquoi les éléments de $G$ sont linéairement indépendants sur $E$.

> **Indications :** Soit $\lambda_1 g_1 + \cdots + \lambda_k g_k = 0$ une relation de dépendance linéaire de longueur minimale sur $E$. On peut supposer cette relation de longueur $\geq 2$. Parce que les caractères sont distincts, on a l'existence d'un élément $y \in E$ avec $g_1(y) \neq g_2(y)$. On a d'une part $g_1(y) \sum_i \lambda_i g_i(x) = 0$, et d'autre part $\sum_i \lambda_i g_i(xy) = \sum_i \lambda_i g_i(x) g_i(y) = 0$. En soustrayant, on obtient une combinaison linéaire non triviale et strictement plus courte, ce qui est absurde.

Soit $V$ un espace vectoriel sur $E$, muni d'une action semi-linéaire de $G$, c'est-à-dire d'une action telle que, pour $g \in G, \lambda \in E, v \in V$, on a $g \cdot (\lambda v) = g(\lambda)v$. On définit son sous-$F$-espace vectoriel des $G$-invariants $V^G = \{v \in V \mid \forall g \in G,\ gv = v\}$.

**2.** Vérifier que l'application $E$-linéaire $V^G \otimes_F E \xrightarrow{\eta} V$ canonique est compatible à l'action de $G$.

> **Indications :** Pour tout $g \in G$, on a
>
> $$\eta \circ g(v \otimes e) = \eta(v \otimes g(e)) = \eta(g(v) \otimes g(e)) = g(e)g(v) = g(ev).$$

**3.** Montrer que $\eta$ est un isomorphisme.

> **Indications :** Montrons d'abord que $\eta$ est surjective. Notons $g_1 = \mathrm{Id}, \ldots, g_n$ les éléments de $G$. On renomme aussi $x_0 := 1 \in E$. Soit $v$ un élément non nul de $V$. Posons, pour tout $j \in [0, n-1]$, $v_j = \sum_i g_i(x_j v) \in V^G$. Par la question 1., la matrice $(g_i(x_j))_{ij}$ est inversible, et en inversant le système précédent, on obtient les $g_i(v)$ en combinaison linéaire des $v_j$. La relation donnant $g_1(v)$ affirme alors la surjectivité voulue.
> Montrons ensuite que $\eta$ est injective. En effet, si ce n'est pas le cas, soit $(v_1, \ldots, v_m)$ une famille de $V^G$ qui est $F$-libre mais non $E$-libre ; on la suppose aussi de longueur minimale. Soit $\sum_i \lambda_i v_i$ une combinaison linéaire non triviale sur $E$. Comme les $\lambda_i$ ne sont pas tous dans $F$, on peut supposer $\lambda_1 \notin F$ et $\lambda_m = 1$. Choisissons $g \in G$ avec $g(\lambda_1) \neq \lambda_1$. On obtient alors une relation $\sum_{i=1}^{m-1} (g(\lambda_i) - \lambda_i)v_i = 0$, qui contredit la minimalité de $m$.

**Exercice 24 : Hilbert 90 et applications**

Soient $K$ un corps et $L/K$ une extension galoisienne finie. Soit $G = \mathrm{Gal}(L/K)$. On rappelle que les éléments de $G$ sont linéairement indépendants.

**1.** On suppose que l'extension $L/K$ est cyclique de degré $n$. Soient $\sigma$ un générateur de $G$ et $x \in L$.

(a) Montrer que $\prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x) = 1$ si et seulement si il existe $y \in L^\times$ tel que l'on ait $x = \dfrac{\sigma(y)}{y}$.

> **Indications :** Pour le sens $\Leftarrow$ il suffit de constater que :
>
> $$\prod_{i=0}^{n-1} \sigma^i \left( \frac{\sigma(y)}{y} \right) = 1.$$
>
> Réciproquement, supposons que l'on a $\prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x) = 1$ ; en particulier, on a $x \in L^\times$. Comme les éléments de $G$ sont linéairement indépendants, l'application
>
> $$\mathrm{Id} + x^{-1}\sigma + (x^{-1}\sigma(x^{-1}))\sigma^2 + \cdots + (x^{-1}\sigma(x^{-1}) \cdots \sigma^{n-1}(x^{-1}))\sigma^{n-1}$$
>
> n'est pas identiquement nulle : on prend $z \in L$ qui ne l'annule pas et on note $y$ sa valeur en $z$. On a alors $\sigma(y) = xy$.

(b) En utilisant la question précédente appliquée à une extension $L/K$ bien choisie, exhiber deux fractions rationnelles $F, G \in \mathbb{Q}(X, Y)$ telles que l'application $\mathbb{Q}^2 \setminus \{(0,0)\} \to \mathbb{R}^2, (x, y) \mapsto (F(x, y), G(x, y))$ est bien définie et son image est exactement constituée des points à coordonnées rationnelles du cercle de centre $(0, 0)$ et de rayon 1.

**Indications :** Prenons $L = \mathbb{Q}(i)$. Un point à coordonnées rationnelles du cercle est un élément de $L$ tel que $\prod_{\sigma \in \mathrm{Gal}(L/\mathbb{Q})} \sigma(x) = 1$ et s'écrit donc $\dfrac{x-iy}{x+iy} = \dfrac{x^2-y^2}{x^2+y^2} - i\dfrac{2xy}{x^2+y^2}$. On pose donc $F = \dfrac{x^2-y^2}{x^2+y^2}$ et $G = \dfrac{-2xy}{x^2+y^2}$.

**2.** On ne suppose plus $L/K$ cyclique.

(a) Soit $f : G \to L^\times$ une fonction telle que, pour tous $s, t \in G$, on a $f(st) = s(f(t))f(s)$. Montrer qu'il existe $x \in L^\times$ tel que, pour tout $s \in G$, on a $f(s) = s(x)x^{-1}$.

**Indications :** Comme les éléments de $G$ sont linéairement indépendants, il existe $c \in L$ tel que $b = \sum_{t \in G} f(t)t(c) \neq 0$. On calcule alors, pour chaque $s \in G$ :

$$s(b) = \sum_{t \in G} s(f(t))st(c) = f(s)^{-1} \sum_{t \in G} f(st)st(c) = f(s)^{-1}b.$$

Donc $f(s) = s(b^{-1})(b^{-1})^{-1}$.

(b) Étant donnés un corps $E$ et un entier naturel $n$, on note $\mathbb{P}^n(E)$ l'espace projectif de dimension $n$, c'est-à-dire l'ensemble des droites de $E^{n+1}$. Montrer que l'action naturelle de $G$ sur $L^{n+1}$ induit une action de $G$ sur $\mathbb{P}^n(L)$. Montrer que $\mathbb{P}^n(L)^{\mathrm{Gal}(L/K)} = \mathbb{P}^n(K)$.

**Indications :** Le seul point difficile est l'inclusion $\mathbb{P}^n(L)^{\mathrm{Gal}(L/K)} \subseteq \mathbb{P}^n(K)$. Soit $(x_0, ..., x_n) \in L^{n+1} \setminus \{0\}$ tel que la droite qu'il engendre est fixée par $G$. Cela signifie qu'il existe $f : G \to L^\times$ telle que $s \cdot (x_0, ..., x_{n+1}) = f(s)(x_0, ..., x_{n+1})$ pour chaque $s \in G$. On en déduit que, pour chaque $s, t \in G$ :

$$\begin{aligned} f(st)(x_0, ..., x_n) &= (st) \cdot (x_0, ..., x_n) = s \cdot (t \cdot (x_0, ..., x_n))) \\ &= s \cdot (f(t)(x_0, ..., x_n))) = s(f(t))f(s)(x_0, ..., x_n))), \end{aligned}$$

ce qui montre que $f(st) = s(f(t))f(s)$. D'après (a), il existe $x \in L^\times$ tel que $f(s) = s(x)x^{-1}$ pour chaque $s$. On remarque alors que $(x_0x^{-1}, .., x_nx^{-1}) \in (L^{n+1})^G = K^{n+1}$. Donc la droite engendrée par $(x_0, ..., x_n)$ est contenue dans $\mathbb{P}^n(K)$.

**Exercice 25 : Extensions cycliques et normes**

Soit $n \geq 2$. Soit $K$ un corps tel que $|\mu_n(K)| = n$ et $\mathrm{Car}(K) \nmid n$. Soit $a \in K^\times$ pour lequel le corps $L = K(\sqrt[n]{a})$ vérifie $[L : K] = n$. Considérons :

$$N : L \to K, x \mapsto \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x).$$

Le but de cet exercice est de montrer que les assertions suivantes sont équivalentes :

(i) il existe une extension finie galoisienne $M/K$ contenant $L$ telle que $\mathrm{Gal}(M/K) \cong \mathbb{Z}/n^2\mathbb{Z}$ ;

(ii) $\mu_n \subseteq N(L^\times)$.

**1.** On suppose (i) et on note $\sigma$ un générateur de $\mathrm{Gal}(M/K)$.

(a) Montrer qu'il existe $b \in L$ tel que $M = L(\sqrt[n]{b})$.

**Indications :** Le groupe $\mathrm{Gal}(M/L)$ est un sous-groupe de $\mathrm{Gal}(M/K) \cong \mathbb{Z}/n^2\mathbb{Z}$ d'ordre $n$. Il est donc engendré par $\sigma^n$ et isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Comme $|\mu_n(K)| = n$, la théorie de Kummer montre qu'il existe $b \in L$ tel que $M = L(\sqrt[n]{b})$.

(b) Soit $c = \frac{\sigma(\sqrt[n]{b})}{\sqrt[n]{b}}$. Montrer que $c \in L$.

**Indications :** Il existe $\zeta \in \mu_n(K)$ tel que $\sigma^n(\sqrt[n]{b}) = \zeta \sqrt[n]{b}$. On calcule alors :

$$\sigma^n(c) = \frac{\sigma^{n+1}(\sqrt[n]{b})}{\sigma^n(\sqrt[n]{b})} = \frac{\sigma(\zeta \sqrt[n]{b})}{\zeta \sqrt[n]{b}} = c.$$

Donc $c \in M^{\mathrm{Gal}(M/L)} = L$.

(c) Montrer que $N(c)$ est un générateur de $\mu_n$. En déduire (ii).

**Indications :** On a :

$$N(c) = c\sigma(c)\sigma^2(c)...\sigma^{n-1}(c) = \frac{\sigma^n(\sqrt[n]{b})}{\sqrt[n]{b}} \in \mu_n(L).$$

Notons $\zeta = N(c)$. Pour chaque $s \geq 0$, on a alors $\sigma^{ns}(\sqrt[n]{b}) = \zeta^s \sqrt[n]{b}$. Pour $1 \leq s \leq n-1$, comme $M$ est engendré par $\sqrt[n]{b}$, on a $\sigma^{ns}(\sqrt[n]{b}) \neq \sqrt[n]{b}$ et donc $\zeta^s \neq 1$. On en déduit que $\zeta$ est un générateur de $\mu_n$. La propriété (ii) en découle immédiatement.

**2.** On suppose (ii) et on note $\tau$ un générateur de $\mathrm{Gal}(L/K)$. Soit $z \in L$ tel que $N(z)$ est un générateur de $\mu_n$.

(a) En utilisant la question 1.(a) de l'exercice 23, montrer qu'il existe $b \in L^\times$ tel que $z^n = \frac{\tau(b)}{b}$.

**Indications :** Comme $N(z) \in \mu_n$, on a $N(z^n) = 1$. La question 1.(a) de l'exercice 23 permet alors de conclure.

(b) Soit $M = L(\sqrt[n]{b})$. Montrer que $\tau$ se prolonge en un automorphisme de corps $\sigma \in \mathrm{Aut}(M/K)$.

**Indications :** Soit $i : L \hookrightarrow M$ l'injection naturelle. On remarque que $i$ et $i \circ \tau$ sont des corps de décomposition de $X^n - b \in L[X]$. Il existe donc un automorphisme de corps $\sigma : M \to M$ tel que $\sigma \circ i = i \circ \tau$. On en déduit que $\sigma$ est un élément de $\mathrm{Aut}(M/K)$ qui prolonge $\tau$.

(c) En utilisant que $z^n = \frac{\tau(b)}{b}$, montrer que $\frac{\sigma^n(\sqrt[n]{b})}{\sqrt[n]{b}}$ est un générateur de $\mu_n$.

**Indications :** On a $z^n = \frac{\tau(b)}{b} = \left(\frac{\sigma^n(\sqrt[n]{b})}{\sqrt[n]{b}}\right)^n$. On en déduit qu'il existe $\eta \in \mu_n$ tel que $\frac{\sigma(\sqrt[n]{b})}{\sqrt[n]{b}} = \eta z \in L$. On a alors :

$$\begin{aligned}\frac{\sigma^n(\sqrt[n]{b})}{\sqrt[n]{b}} &= \prod_{i=0}^{n-1} \sigma^i\left(\frac{\sigma(\sqrt[n]{b})}{\sqrt[n]{b}}\right) \\ &= N(\eta z) \\ &= N(z).\end{aligned}$$

(d) En déduire que $M/K$ est galoisienne cyclique de degré $n^2$.

**Indications :** On note $\zeta = \frac{\sigma^n(\sqrt[n]{b})}{\sqrt[n]{b}}$. On remarque que $\sigma^n \in \mathrm{Gal}(M/L)$ et que l'on a $\frac{\sigma^{ns}(\sqrt[n]{b})}{\sqrt[n]{b}} = \zeta^s$ pour chaque $s \geq 1$. Comme $\zeta$ est une racine primitive $n$-ième de l'unité, on en déduit que $\sigma^n$ est un générateur de $\mathrm{Gal}(M/L) \cong \mathbb{Z}/n\mathbb{Z}$. Il suit immédiatement que $M/K$ est galoisienne de degré $n^2$.

**Exercice 26 : Calcul de discriminant - Examen 2014**
Soient $a$ et $b$ deux éléments de $\mathbb{C}$. Soit $n \geq 2$. Calculer le discriminant du polynôme $X^n + aX + b$.

**Indications :** Notons $P = X^n + aX + b$. Soit $S$ l'ensemble des racines de $P$. Supposons que $0 \notin S$ (ie $b \neq 0$). On calcule :

$$\begin{aligned}
\Delta &= (-1)^{n(n-1)/2} \prod_{x \in S} P'(x) \\
&= (-1)^{n(n-1)/2} \prod_{x \in S} (nx^{n-1} + a) \\
&= (-1)^{n(n-1)/2} \prod_{x \in S} x^{-1}(nx^n + ax) \\
&= (-1)^{n(n-1)/2} (\prod_{x \in S} x)^{-1} \cdot \prod_{x \in S} (nx^n + ax) \\
&= (-1)^{n(n-1)/2} (-1)^n b^{-1} \cdot \prod_{x \in S} (a(1-n)x - nb) \\
&= (-1)^{n(n-1)/2} (-1)^n b^{-1} a^n (1-n)^n \cdot \prod_{x \in S} (x - nba^{-1}(1-n)^{-1}) \\
&= (-1)^{n(n-1)/2} b^{-1} a^n (1-n)^n \cdot P(nba^{-1}(1-n)^{-1}) \\
&= (-1)^{n(n-1)/2} (n^n b^{n-1} + a^n (1-n)^{n-1}).
\end{aligned}$$

Comme $\Delta$ est un polynôme en $a$ et $b$, la formule reste valable lorsque $b = 0$.

**Exercice 27 : Discriminant d'un polynôme cyclotomique**
Soient $p$ un nombre premier et $n$ un entier naturel non nul. Calculer le discriminant de $\phi_{p^n} = \sum_{k=0}^{p-1} X^{kp^{n-1}}$ au signe près.

**Indications :** Soit $\zeta \in \mathbb{C}$ une racine primitive $p^n$-ième de l'unité. Les racines de $\phi_{p^n}$ sont alors les $\zeta^k$ avec $1 \leq k \leq p^n$ non multiple de $p$. Le discriminant de $\phi_{p^n}$ est alors :

$$\Delta = \pm \prod_{\substack{k=1 \\ p \nmid k}}^{p^n} \phi'_{p^n}(\zeta^k).$$

En dérivant $(X^{p^{n-1}} - 1)\phi_{p^n} = X^{p^n} - 1$, on obtient :

$$(X^{p^{n-1}} - 1)\phi'_{p^n} + p^{n-1}X^{p^{n-1}-1}\phi_{p^n} = p^n X^{p^n-1}.$$

Par conséquent, on a $(\zeta^{kp^{n-1}} - 1)\phi'_{p^n}(\zeta^k) = p^n\zeta^{k(p^n-1)}$ pour $1 \leq k \leq p^n$ non multiple de $p$. En multipliant toutes ces relations, on obtient :

$$\phi_p(1)^{p^{n-1}}\Delta = \pm p^{np^{n-1}(p-1)}.$$

Par conséquent, $\Delta = \pm p^{np^{n-1}(p-1)-p^{n-1}}$.

**Exercice 28 : Résultant et discriminant**

Soit $A$ un anneau commutatif. Pour $n \in \mathbb{N}$, on note $A_n[X]$ le $A$-module des polynômes de degré strictement plus petit que $n$. On appellera base canonique de $A_n[X]$ la base $(X^{n-1}, X^{n-2}, ..., 1)$. Pour $(P, Q) \in A[X] \times A[X]$ avec $\deg P = n$ et $\deg Q = m$, on note $\mathrm{Res}(P, Q)$ le déterminant dans les bases canoniques de l'application $A$-linéaire $A_m[X] \times A_n[X] \to A_{m+n}[X]$ qui envoie $(U, V)$ sur $PU + QV$.

**1.** Écrire $\mathrm{Res}(P, Q)$ comme déterminant d'une matrice.

**2.** Comparer $\mathrm{Res}(P, Q)$ et $\mathrm{Res}(Q, P)$.

**3.** On suppose que $P$ est un polynôme unitaire.

(a) Montrer que $\mathrm{Res}(P, Q)$ est égal au déterminant de la multiplication par $Q$ sur l'anneau $A[X]/(P)$ dans la base $(X^{n-1}, X^{n-2}, ..., 1)$.

(b) Considérons $Q_1 \in A[X]$ et $Q_2 \in A[X]$ de degrés respectifs $m_1$ et $m_2$. Calculer $\mathrm{Res}(P, Q_1Q_2)$ en fonction de $\mathrm{Res}(P, Q_1)$ et $\mathrm{Res}(P, Q_2)$.

(c) Exprimer $\mathrm{Res}(P, (X-\lambda_1)...(X-\lambda_m))$ en fonction de $P(\lambda_1)...P(\lambda_m)$.

(d) En déduire une formule explicite pour $\Delta^2 = \prod_{i<j}(X_i - X_j)^2 \in \mathbb{Z}[X_1, ..., X_n]$ en fonction des polynômes symétriques élémentaires.