Fiche 7, exercice 1 :

Soit K un corps. Soit $G < \mathrm{Aut}K$ un sous-groupe.

Soit $k := K^G$. Soit Ω un corps algébriquement clos contenant K. On sait déjà (*cf.* cours) que le nombre de $k-$plongements de K dans Ω est fini de cardinal $\leq [K : k]$. Or, comme $k = K^G$, $G \subseteq \{k-\text{plongements de } K \text{ dans } \Omega\}$. Donc $|G| \leq [K : K^G]$.

En particulier, si $[K : K^G]$ est fini, on a déjà que $|G| \leq [K : K^G] < \infty$.

Montrons que $|G| \geq [K : K^G]$, si G est fini d'ordre r.

Par l'absurde : si $r > [K : K^G]$, alors il existe $u_0, ..., u_r \in K$ qui sont $k-$linéairement indépendants.

Le système :

$$(1) \qquad {}^\forall\sigma \in G, \;\; \sigma(u_0)a_0 + ... + \sigma(u_r)a_r = 0$$

à r équations et $r+1$ inconnues $a_0, ..., a_r$ a au moins une solution non triviale dans K^{r+1}.

Soit $(a_0, ..., a_r) \in K^{r+1} \setminus \{(0, ..., 0)\}$ une solution avec un nombre de coefficients $a_i \neq 0$ minimal.

Quitte à renuméroter et à diviser par le premier coefficient non nul, on peut supposer $a_0 = 1$.

On a : (pour $\sigma = 1$) : $u_0 + u_1a_1 + ... + u_ra_r = 0$. Comme les u_i sont $k-$linéairement indépendants, l'un des coefficients $a_i \notin k = K^G$, par exemple a_1. Soit $\tau \in G$ tel que $\tau(a_1) \neq a_1$.

On a donc :

$$\begin{aligned} &{}^\forall\sigma \in G,\, \tau(\sigma(u_0) + \sigma(u_1)a_1 + ... + \sigma(u_r)a_r) = 0 \\ \Leftrightarrow\; &{}^\forall\sigma \in G,\, \tau\sigma(u_0) + \tau\sigma(u_1)\tau(a_1) + ... + \tau\sigma(u_r)\tau(a_r) = 0 \\ (2) \qquad \Leftrightarrow\; &{}^\forall\sigma \in G,\, \sigma(u_0) + \sigma(u_1)\tau(a_1) + ... + \sigma(u_r)\tau(a_r) = 0 \end{aligned}$$

car $\tau G = G$.

Donc : (1) − (2) donne :

$${}^\forall\sigma \in G, \sigma(u_1)(\tau(a_1) - a_1) + ... + \sigma(u_r)(\tau(a_r) - a_r) = 0$$

ce qui donne une solution non triviale ($\tau(a_1) - a_1 \neq 0$) avec un nombre de coefficients non nuls $<$ au nombre de coefficients non nuls parmi les $(1, a_1, ..., a_r)$. Contradiction !

Donc $[K : K^G] \leq |G|$.

En particulier on a montré que si G est fini, alors $[K : K^G] < \infty$.

exo 2 :

On pose $s_1, ..., s_n \in k[x_1, ..., x_n]$ les polynômes tels que :

$$(T - x_1)...(T - x_n) = T^n - s_1 T^{n-1} + ... + (-1)^n s_n \in k[x_1, ..., x_n][T] \ .$$

Les s_i sont les *polynômes symétriques élémentaires.*
On a $k(s_1, ..., s_n) \subseteq k(x_1, ..., x_n)^{S_n} \subseteq k(x_1, ..., x_n)$. Or :

$$[k(x_1, ..., x_n) : k(x_1, ..., x_n)^{S_n}] = n! \ .$$

D'un autre côté, le polynôme $(T - x_1)...(T - x_n) \in k(s_1, ..., s_n)[T]$ donc x_1 est de degré $\leq n$ sur $k(s_1, ..., s_n)$. En faisant une division euclidienne sur le corps $k(s_1, ..., s_n, x_1)$, on voit que le polynôme $(T - x_2)...(T - x_n) \in k(s_1, ..., s_n, x_1)[T]$. Donc x_2 est de degré $\leq n - 1$ sur $k(s_1, ..., s_n, x_1)$, *etc*

Donc :

$$[k(x_1, ..., x_n) : k(s_1, ..., s_n)] \leq n!$$
$$\Rightarrow k(x_1, ..., x_n)^{S_n} = k(s_1, ..., s_n) \ .$$

exo 3 : Soit G le sous-groupe des automorphismes de $k(t)$ engendré par les changements de variables $t \mapsto -t$ et $t \mapsto 1 - t$. Soit $f(t) \in k(t)^G$. On a : $f(1 + t) = f(t)$. Soit $p(t), q(t) \in k[t]$ premiers entre eux tels que $f = p/q$. On a : $p(t)q(t + 1) = p(t + 1)q(t)$. D'après le lemme de Gauss, $p(t)$ divise $p(t+1)$ donc $p(t) = p(t+1)$. De même $q(t) = q(t+1)$. On peut donc supposer $f(t) \in k[t]$ pour la suite. En particulier, si k est de caractéristique nulle, le polynôme $f(t) - f(0)$ s'annule pour tout $t = n1_k$, $n \in \mathbb{Z}$. Donc ce polynôme est constant et $f(t) \in k$.

Remarque : Contrairement au cas fini, on a donc $k(t)^G = k = k(t)^{\mathrm{Aut}_k(k(t))}$ mais $G \neq \mathrm{Aut}_k(k(t))$.

Si k est de caractéristique p, alors $k(t^p - t^{2p}) \in k(t)^G$. Pour l'inclusion réciproque, On remarque que : $X^p - X^{2p} - (t^p - t^{2p}) \in k(t^p - t^{2p})[X]$ est un polynôme de degré $2p$ qui annule t. Donc t est de degré $\leq 2p$ sur $k(t^p - t^{2p})$. Or $[k(t) : k(t)^G] = |G| = 2p$. En effet, $G = \{t \mapsto \pm t + i \ : \ i \in \mathbb{Z}/p\mathbb{Z}\}$.

à propos des polynômes cyclotomiques :

Soit $\Phi_n(X) := \prod_{\substack{0 \leq k \leq n-1 \\ k \wedge n = 1}} (X - e^{2ik\pi/n}) \in \mathbb{C}[X]$.

On a aussi : $\Phi_n(X) = \prod (X - z)$ où le produit se fait sur les racines primitives $n-$ièmes de l'unité *i.e.* les éléments z d'ordre n dans le groupe $\mathbb{C}^\times$.

Toute racine $n-$ième u est une racine primitive $d-$ième pour un d qui divise n (unique car d est l'ordre de u).

Donc $\prod_{d|n} \Phi_d(X) = X^n - 1$.

Par récurrence, montrons que $\Phi_n \in \mathbb{Z}[X]$. On a $\Phi_1(X) = X - 1$ et si on suppose tous les $\Phi_d(X) \in \mathbb{Z}[X]$ pour tout $d < n$, alors comme $Q(X) := \prod_{d|n, d<n} \Phi_d(X)$ est unitaire à coefficients entiers, on peut faire la division

euclidienne de X^n-1 par $Q(X)$ en restant dans $\mathbb{Z}[X]$. Le résultat est unique et c'est forcément le même que celui de la division euclidienne sur $\mathbb{C}$. Donc $\Phi_n(X) \in \mathbb{Z}[X]$.

Inversion de Möbius :

Soit $\mu(k) := \begin{cases} (-1)^r \text{ si } k = p_1...p_r \text{où } p_1 < ... < p_r \text{ premiers} \\ 0 \text{ si } p^2|k \text{ pour un premier } p \end{cases}$.

On a : $\sum_{d|n} \mu(d) = 1$ si $n = 1$ et 0 si $n > 1$. En effet, si $n = p_1^{a_1}...p_r^{a_r} > 1$ où les p_i sont des nombres premiers distincts, alors :

$$\begin{aligned} \sum_{d|n} \mu(d) &= \sum_{k=0}^{r} \sum_{1\le i_1<...<i_k\le r} \mu(p_{i_1}...p_{i_k}) \\ &= \sum_{k=0}^{r} \sum_{1\le i_1<...<i_k\le r} (-1)^k \\ &= \sum_{k=0}^{r} \binom{r}{k} (-1)^k \\ &= (1-1)^r = 0 \ . \end{aligned}$$

On en déduit la formule d'inversion de Möbius qui donne $\Phi_n(X)$ en fonction des $X^d - 1$:

$$\begin{aligned} \prod_{d|n} (X^{n/d}-1)^{\mu(d)} &= \prod_{d|n} \prod_{k|n/d} \Phi_k(X)^{\mu(d)} \\ &= \prod_{k|n} \prod_{\substack{d|n \\ k|n/d}} \Phi_k(X)^{\mu(d)} \\ &= \prod_{k|n} \Phi_k(X)^{\sum_{\substack{d|n \\ k|n/d}} \mu(d)} \end{aligned}$$

or,

$$\sum_{\substack{d|n \\ k|n/d}} \mu(d) = \sum_{d|n/k} \mu(d)$$

car $d|n$ et $k|n/d \Leftrightarrow d|n/k$. D'où :

$$\sum_{\substack{d|n \\ k|n/d}} \mu(d) = 0$$

si $n/k > 1$.

Donc :

$$\prod_{d|n} (X^{n/d}-1)^{\mu(d)} = \Phi_n(X) \ .$$

Application : $\Phi_8(X) = (X^8-1)^1(X^4-1)^{-1}(X^2-1)^0(X-1)^0 = \frac{X^8-1}{X^4-1} = X^4+1$.

D'après le cours, $\Phi_8(X)$ est irréductible sur $\mathbb{Z}$ donc sur $\mathbb{Q}$.

Pourtant $\Phi_8(X) = X^4+1$ est réductible modulo p pour tout nombre premier p.

En effet, si $p=2$, $X^4+1 = (X+1)^4 \bmod 2$.

Si p est un nombre premier impair, alors : ...

Si -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$, alors : $X^4+1 = (X^2-\sqrt{-1})(X^2+\sqrt{-1})$.

Si 2 est un carré, alors $X^4+1 = (X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1)$.

Si -2 est un carré, alors $X^4+1 = (X^2-\sqrt{-2}X-1)(X^2+\sqrt{-2}X-1)$.

Or, le sous-groupe des carrés de $(\mathbb{Z}/p\mathbb{Z})^*$ est d'indice 2 (car c'est l'image du morphisme $(\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ de noyau $\{\pm 1\}$).

Donc si -1 n'est pas un carré, si 2 n'est pas un carré, $-2 = (-1)\times 2 \in ((\mathbb{Z}/p\mathbb{Z})^*)^2$.

Donc dans tous les cas, X^4+1 est réductible $\bmod p$.