Université Lyon 1 M1 — Théorie de Galois — semestre de printemps 2011

Corrigé de l'examen partiel
du mardi 22 mars 2011

Exercice 1:

a) On a pour tout $n \geq 1$:

$$\forall \theta \in \mathbb{R} \quad \cos(n\theta) = \mathrm{Re}\left(e^{in\theta}\right) = \mathrm{Re}\left((\cos\theta + i\sin\theta)^n\right)$$

$$= \mathrm{Re}\left(\sum_{k=0}^{n} \binom{n}{k} \cos^{n-k}\theta \; i^k \sin^k\theta\right)$$

$$= \sum_{\substack{k=0 \\ k \text{ pair}}}^{n} \binom{n}{k} \cos^{n-k}\theta \, (-1)^{k/2} \sin^k\theta$$

$$= \sum_{\substack{k=0 \\ k \text{ pair}}}^{n} \binom{n}{k} (-1)^{k/2} \cos^{n-k}\theta \, (1-\cos^2\theta)^{k/2}$$

Donc : $$T_n(X) = \sum_{\substack{k=0 \\ k \text{ pair}}}^{n} \binom{n}{k} (-1)^{k/2} X^{n-k} (1-X^2)^{k/2}$$

C'est un polynôme à coefficients entiers de degré $\leq n$ et de coefficient de degré n :

$$\sum_{\substack{k=0 \\ k \text{ pair}}}^{n} \binom{n}{k} (-1)^{k/2} (-1)^{k/2} = \sum_{\substack{k=0 \\ k \text{ pair}}}^{n} \binom{n}{k}$$

Or : $$\begin{cases} \displaystyle\sum_{\substack{k=0 \\ k \text{ pair}}}^{n} \binom{n}{k} + \sum_{\substack{k=0 \\ k \text{ impair}}}^{n} \binom{n}{k} = 2^n \\ \displaystyle\sum_{\substack{k=0 \\ k \text{ pair}}}^{n} \binom{n}{k} - \sum_{\substack{k=0 \\ k \text{ impair}}}^{n} \binom{n}{k} = (1-1)^n = 0 \end{cases} \Longrightarrow \sum_{\substack{k=0 \\ k \text{ pair}}}^{n} \binom{n}{k} = \frac{2^n}{2} = 2^{n-1}.$$

Donc $T_n(X) \in \mathbb{Z}[X]$ est de degré n et de coefficient dominant 2^{n-1}.

b) Pour tout $n \geq 1$:

$$\cos\left(\frac{2\pi}{n}\right) = \frac{1}{2}\left(\zeta_n + \zeta_n^{-1}\right)$$

Or ζ_n est algébrique sur $\mathbb{Q}$. Donc $\cos\left(\frac{2\pi}{n}\right)$ aussi.

On a :

c) $\cos 2\pi = 1$, $\cos\frac{2\pi}{2} = -1$, $\cos\frac{2\pi}{4} = 0$, $\cos\frac{2\pi}{8} = \cos\frac{\pi}{4} = \frac{\sqrt{2}}{2}$ ..

donc $\psi_1(X) = X - 1$, $\psi_2(X) = X + 1$, $\psi_4(X) = X$, $\psi_8(X) = X^2 - \frac{1}{2}$

d) On a $\zeta_n^2 - 2\cos\left(\frac{2\pi}{n}\right)\zeta_n + 1 = (\zeta_n - \zeta_n)(\zeta_n - \zeta_n^{-1}) = 0$

donc ζ_n est racine d'un polynôme de degré 2 à coefficients dans $\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)$.

On a : $\mathbb{Q} \subset \mathbb{Q}\left(\cos\frac{2\pi}{n}\right) \subset \mathbb{Q}(\zeta_n)$

Donc $\underbrace{[\mathbb{Q}(\zeta_n) : \mathbb{Q}]}_{=\varphi(n)} = \underbrace{\left[\mathbb{Q}(\zeta_n) : \mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right)\right]}_{\leq 2} \left[\mathbb{Q}\left(\cos\left(\frac{2\pi}{n}\right)\right) : \mathbb{Q}\right]$.

Si $n \geq 3$, $\zeta_n = \cos\frac{2\pi}{n} + i \underbrace{\sin\frac{2\pi}{n}}_{\neq 0} \notin \mathbb{R}$.

Donc $\zeta_n \notin \mathbb{Q}\left(\cos\frac{2\pi}{n}\right) \subset \mathbb{R}$

Donc $\mathbb{Q}\left(\cos\frac{2\pi}{n}\right) \subsetneq \mathbb{Q}(\zeta_n)$ et $\left[\mathbb{Q}(\zeta_n) : \mathbb{Q}\left(\cos\frac{2\pi}{n}\right)\right] = 2$

Ainsi $n \geq 3 \Rightarrow \boxed{\left[\mathbb{Q}\left(\cos\frac{2\pi}{n}\right) : \mathbb{Q}\right] = \frac{\varphi(n)}{2} = \deg \psi_n(X)}$

e) Soit $G := \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ le groupe de Galois de $\mathbb{Q}(\zeta_n)$ sur $\mathbb{Q}$.

Comme $\psi_n(X) \in \mathbb{Q}[X]$, on a pour tout $\sigma \in G$:

$0 = \sigma\left(\psi_n\left(\cos\frac{2\pi}{n}\right)\right) = \psi_n\left(\sigma\left(\cos\frac{2\pi}{n}\right)\right)$.

Donc $\sigma\left(\cos\frac{2\pi}{n}\right)$ est une racine de $\psi_n(X)$ pour tout $\sigma \in G$.

Or $G = \{\sigma_k \; ; \; 1 \le k \le n-1, \; k \wedge n = 1\}$

où pour tout k premier à n, σ_k est automorphisme de $\mathbb{Q}(\zeta_n)$ tel que $\sigma_k(\zeta_n) = \zeta_n^k$.

On a donc :

$$\sigma_k\left(\cos\left(\frac{2\pi}{n}\right)\right) = \sigma_k\left(\frac{1}{2}\left(\zeta_n + \zeta_n^{-1}\right)\right) = \frac{1}{2}\left(\zeta_n^{k} + \zeta_n^{-k}\right)$$

$$= \cos\frac{2k\pi}{n}$$

pour tout k premier à n.

On en déduit que les

$$\cos\frac{2k\pi}{n}, \quad 1 \le k \le n-1, \quad k \text{ premier à } n$$

sont des racines de $\Psi_n(X)$.

Or $\cos\frac{2k'\pi}{n} = \cos\frac{2k\pi}{n} \iff \frac{2k'\pi}{n} = \pm\frac{2k\pi}{n} \mod 2\pi$

$$\iff k' = \pm k \mod n$$

Donc $\left\{\cos\left(\frac{2k\pi}{n}\right) \;\middle|\; 1 \le k \le n-1, \; k \text{ premier à } n\right\} = \left\{\cos\frac{2k\pi}{n} \;\middle|\; 1 \le k \le \frac{n-1}{2}, \; k \text{ premier à } n\right\}$

et les racines $\cos\frac{2k\pi}{n}$, $1 \le k \le \frac{n-1}{2}$ (k premier à n) sont 2 à 2 distinctes.

Cela fait $\frac{\varphi(n)}{2}$ racines car $\{1 \le k \le n-1 \mid k \wedge n = 1\} = \{1 \le k \le \frac{n-1}{2} \mid k \wedge n = 1\} \sqcup \{\frac{n+1}{2} \le k \le n-1 \mid k \wedge n = 1\}$,

et on a une bijection : $\{1 \le k \le \frac{n-1}{2} \mid k \wedge n = 1\} \xrightarrow{1:1} \{\frac{n+1}{2} \le k \le n-1 \mid k \wedge n = 1\}$

$$k \longmapsto n-k$$

Comme $\Psi_n(X)$ est de degré $\frac{\varphi(n)}{2}$, on a trouvé toutes les racines de $\Psi_n(X)$.

f) Le polynôme $T_{s+1}(X) - T_s(X)$ est de degré $s+1 = \frac{n+1}{2}$.

Si $0 \le k \le s$, $T_{s+1}\left(\cos\frac{2k\pi}{n}\right) - T_s\left(\cos\frac{2k\pi}{n}\right) = \cos\left(\frac{2k(s+1)}{n}\pi\right) - \cos\left(\frac{2ks\pi}{n}\right)$

$$= \cos\left(\frac{k(n+1)\pi}{n}\right) - \cos\left(\frac{k(n-1)\pi}{n}\right)$$

$$= \cos\left(k\pi + \frac{k\pi}{n}\right) - \cos\left(k\pi - \frac{k\pi}{n}\right)$$

$$= (-1)^k \cos\left(\frac{k\pi}{n}\right) - (-1)^k \cos\left(-\frac{k\pi}{n}\right)$$

$$= 0$$

Donc le polynôme $T_{s+1}(X) - T_s(X)$ a au moins

$$\cos\left(\frac{2k\pi}{n}\right) \qquad 0 \leq k \leq s$$

comme racines.

Cela fait $s+1$ racines car $0 \leq k \leq s \Rightarrow 0 \leq \frac{2k\pi}{n} < \pi$

et cos est injective sur $[0, \pi]$.

Donc les racines de $T_{s+1}(X) - T_s(X)$ sont les $\cos\frac{2k\pi}{n}$, $0 \leq k \leq s$.

7)

Soit $0 \leq k \leq s$. Soit e le pgcd de k et n.

Alors $\frac{k}{n} = \frac{k'}{d}$ où $k' = \frac{k}{e}$ et $d = \frac{n}{e}$. En particulier $\underbrace{k' \wedge d}_{=1} = 1$

De plus, $k' = \frac{k}{e} \leq \frac{s}{e} = \frac{n-1}{2e} < \frac{d}{2}$

$\Rightarrow k' \leq \frac{d-1}{2}$ car d est impair

Donc : $\cos\left(\frac{2k\pi}{n}\right)$ est une racine de $\psi_d(X)$.

On a donc : $T_{s+1}(X) - T_s(X) \;\Big|\; \prod_{d|n} \psi_d(X)$

Or $T_{s+1}(X) - T_s(X)$ est de degré $s+1$

et $\prod_{d|n} \psi_d(X)$ est de degré :

$$1 + \sum_{\substack{d|n \\ d\geq 3}} \frac{\varphi(d)}{2} = 1 + \sum_{d|n} \frac{\varphi(d)}{2} - \frac{1}{2}$$

$$= \frac{n}{2} + \frac{1}{2} = s+1.$$

Donc $T_{s+1}(X) - T_s(X) = 2^s \prod_{d|n} \psi_d(X)$ car

$T_{s+1}(X) - T_s(X)$ a pour coefficient dominant 2^s

et chaque $\psi_d(X)$ est unitaire.

h) On cherche $\psi_7(X)$. Comme 7 est premier :

$$T_4(X) - T_3(X) = 2^3 \psi_1(X) \psi_7(X)$$

$$\Leftrightarrow \psi_7(X) = \frac{T_4(X) - T_3(X)}{8(X-1)}$$

Or $T_3(X) = 4X^3 - 3X$ et $T_4(X) = 8X^4 - 8X^2 + 1$

D'où :

$$\psi_7(X) = \frac{8X^4 - 4X^3 - 8X^2 + 3X + 1}{8(X-1)}$$

$$= \frac{8X^3 + 4X^2 - 4X - 1}{8}$$

$$= X^3 + \frac{X^2}{2} - \frac{X}{2} - \frac{1}{8}$$

i) Si $n = 2s$ est un entier pair, alors :

$$T_{s+1}\left(\cos\left(\frac{2k\pi}{n}\right)\right) - T_{s-1}\left(\cos\left(\frac{2k\pi}{n}\right)\right)$$

$$= \cos\left(\frac{2k(s+1)\pi}{n}\right) - \cos\left(\frac{2k(s-1)\pi}{n}\right)$$

$$= \cos\left(k\pi + \frac{2k\pi}{n}\right) - \cos\left(k\pi - \frac{2k\pi}{n}\right)$$

$= 0.$

Comme $T_{s+1}(X) - T_s(X)$ est de degré $s+1$, les racines de $T_{s+1}(X) - T_{s-1}(X)$ sont donc les

$$\cos\frac{2k\pi}{n}, \quad 0 \leq k \leq s.$$

Comme pour le cas impair, si $0 \leq k \leq s$ alors il existe d/n, $k' \leq \frac{d-1}{2}$ premier à d tel que $\frac{2k\pi}{n} = \frac{2k'\pi}{d}$

En particulier, $\cos\frac{2k\pi}{n}$ est une racine de $\psi_d(X)$.

Par conséquent $T_{s+1}(X) - T_{s-1}(X)$ divise $\prod_{d/n} \psi_d(X)$

Or $\prod_{d/n} \psi_d(X)$ est de degré $\sum_{d/n} \frac{\varphi(d)}{2} - \frac{\varphi(1)}{2} - \frac{\varphi(2)}{2} + 1 + 1$
$= \frac{n}{2} + 1 = s+1$

Puisque $T_{s+1}(X) - T_{s-1}(X)$ a pour coefficient 2^s,

on en déduit que $T_{s+1}(X) - T_{s-1}(X) = 2^s \prod_{d|n} \psi_d(X)$.

Exo. 2

a) Le groupe $\mathbb{F}_q^\times$ est d'ordre $q-1$. Donc :

$$\forall x \in \mathbb{F}_q, \quad x^q = x.$$

Par conséquent $\mathbb{F}_q \subset \{x \in \overline{\mathbb{F}_p} : x^q - x = 0\}$

Or $\{x \in \overline{\mathbb{F}_p} : x^q - x = 0\}$ a au plus q solutions.

Donc $\mathbb{F}_q = \{x \in \overline{\mathbb{F}_p} : x^q = x\}$

b)

Soit P un polynôme irréductible sur $\mathbb{F}_q$.

Si $P^2 \mid X^{q^n} - X$, alors $P \mid (X^{q^n} - X)'$

Or $\mathbb{F}_q$ est de caractéristique p. Donc $(X^{q^n} - X)' = -1$

Contradiction. Le polynôme $X^{q^n} - X$ est sans facteurs carrés.

c) Pour tout x racine de P, $x^{q^n} = x$.

Or l'ensemble $\{x \in \overline{\mathbb{F}_p} : x^{q^n} = x\}$ est un sous-corps de $\overline{\mathbb{F}_p}$ qui contient $\mathbb{F}_q$. Donc ce sous-corps contient K qui est le corps engendré sur $\mathbb{F}_q$ par les racines de P.

Notons $k := [\mathbb{F}_{q^n} : K]$.

On a : $k[K:\mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n$.

Or $[K:\mathbb{F}_q] = d$. En effet, soit α une racine de P. Alors :

$$[\mathbb{F}_q(\alpha):\mathbb{F}_q] = d \Rightarrow |\mathbb{F}_q(\alpha)| = q^d \Rightarrow \alpha^{q^d} = \alpha \Rightarrow \forall f \in \mathbb{F}_q(\alpha),\ f^{q^d} = f$$

$$\Rightarrow P \mid X^{q^d} - X$$

$\Rightarrow$ toutes les racines de P sont des racines de $X^{q^d} - X$.

Donc $K = \mathbb{F}_{q^d} \Rightarrow [K:\mathbb{F}_q] = d$.

Donc $d \mid n$ et $[\mathbb{F}_{q^n} : K] = \dfrac{n}{d}$.

d) Soit P un facteur irréductible de $X^{q^n} - X$ sur $\mathbb{F}_q$.

Alors P est de degré d qui divise n. Comme les facteurs irréductibles de $X^{q^n} - X$ sur $\mathbb{F}_q$ sont 2 à 2 distincts, on a :

$$X^{q^n} - X \;\Big|\; \prod_{\substack{P \text{ irréductible} \\ \text{unitaire} \\ \deg(P) \mid n}} P$$

Réciproquement, si P est irréductible, unitaire de degré d, alors si α est une racine de P, on a : $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = d$

$$\Rightarrow |\mathbb{F}_q(\alpha)| = q^d$$

$$\Rightarrow \alpha^{q^d} = \alpha$$

$$\Rightarrow P \mid X^{q^d} - X$$

(car P est le polynôme minimal de α sur $\mathbb{F}_q$).

Or si $d \mid n$, $q^d - 1 \mid q^n - 1 \Rightarrow X^{q^d - 1} - 1 \mid X^{q^n - 1} - 1$

$$\Rightarrow X^{q^d} - X \mid X^{q^n} - X \text{ sur } \mathbb{F}_q.$$

On a donc bien $X^{q^n} - X = \prod_P P$

où P décrit les polynômes irréductibles unitaires sur $\mathbb{F}_q$ de degré d avec $d \mid n$.

9/9

Exo. 3

a) On pose: $\sigma : \mathbb{C}(t) \longrightarrow \mathbb{C}(t)$ $\quad\quad$ $\tau : \mathbb{C}(t) \longrightarrow \mathbb{C}(t)$

$f(t) \longmapsto f\left(\frac{i}{t}\right)$ $\quad\quad$ $f(t) \longmapsto f(-t)$

On a : $\sigma^2(t) = \dfrac{i}{i/t} = t$ donc $\sigma^2 = Id$

$\tau^2(t) = -(-t) = t$ donc $\tau^2 = Id$

$\sigma\tau(t) = \dfrac{i}{-t} = \dfrac{-i}{t} = \tau\sigma(t)$ donc $\sigma\tau = \tau\sigma$

Donc $G = \{\sigma^i \tau^j \mid i, j \in \mathbb{Z}\} = \{1, \sigma, \tau, \sigma\tau\}$ est d'ordre 4.

D'après le lemme d'Artin, $[\mathbb{C}(t) : \mathbb{C}(t)^G] = |G| = 4$

b) Le polynôme $\prod_{g \in G} (X - g(t))$ est à coefficients dans $\mathbb{C}(t)^G$.

On a : $\prod_{g \in G} (X - g(t)) = (X-t)\left(X - \frac{i}{t}\right)(X+t)\left(X + \frac{i}{t}\right)$

$= (X^2 - t^2)\left(X^2 + \frac{1}{t^2}\right) = X^4 - \left(t^2 - \frac{1}{t^2}\right)X^2 - 1$

En particulier, $\mathbb{C}(y) \subset \mathbb{C}(t)^G \subset \mathbb{C}(t)$

De plus $[\mathbb{C}(t) : \mathbb{C}(y)] \leq 4$.

Comme $[\mathbb{C}(t) : \mathbb{C}(t)^G] = 4$, on a forcément :
$\mathbb{C}(t)^G = \mathbb{C}(y)$ et $X^4 - \left(t^2 - \frac{1}{t^2}\right)X^2 - 1$ est le polynôme minimal de t sur $\mathbb{C}(y) = \mathbb{C}(t)^G$.