Correction du devoir sur le théorème de Gauss : Les polygones constructibles

Préliminaires : preuve des deux lemmes donnés à utiliser sans démonstration

P1. Soient P et Q deux polynômes unitaires de Q[X] tels que leur produit est dans Z[X]. On veut montrer qu'alors ils sont tous deux dans Z[X].
Soient u et v les ppcm des dénominateurs de P et Q, on peut écrire $uP = P_1$ et $vQ = Q_1$ où P_1 et Q_1 sont dans Z[X]. Soit H = PQ. On a donc $uvH = P_1Q_1$.

❶ Soit p un diviseur premier de uv . Montrons que p divise soit *tous* les coefficients de P_1 soit *tous* les coefficients de Q_1. Notons $P(X) = \sum_{i=0}^{r} b_i X^i$ et $Q(X) = \sum_{j=0}^{s} c_j X^j$.

On raisonne par l'absurde : supposons que p ne puisse être mis en facteur ni P_1 dans ni dans Q_1, alors il existe h le plus petit indice i tel que p ne divise pas b_i et k le plus petit indice j tel que p ne divise pas c_j. Comme p divise P_1Q_1, il divise chaque coefficient, en particulier celui en X^{h+k} qui est $\sum_{i+j=h+k} b_i c_j$. Or le produit $b_i c_j$ est divisible par p pour $i < h$ *ou* $j < k$. Donc tous les termes sont divisibles par p sauf le terme en $b_h c_k$. Comme la somme est divisible par p, il y a contradiction (par Gauss : un des deux b_h ou c_k serait divisible par p).

❷ On fait la même chose pour tous les diviseurs premiers p de uv. Ils divisent soient tous les coefficients de P_1 soit tous ceux de Q_1 . On obtient donc deux nouveaux polynômes P_2 et Q_2 , à coeffcients dans Z, tels que $P_2 = \frac{1}{u_1}P_1$ et $Q_2 = \frac{1}{v_1}Q_1$, avec $u_1v_1 = uv$. Ainsi, $PQ = P_2Q_2$. De plus ces deux polynômes sont unitaires puisqu'à coeff dans Z et que P et Q le sont aussi.

❸ Il en résulte que $P = \frac{1}{u}P_1 = \frac{u_1}{u}P_2$ et $Q = \frac{v_1}{v}Q_2$. Or comme P et P_2 sont unitaires, on doit avoir $\frac{u_1}{u} = 1$ et de même pour Q, $\frac{v_1}{v} = 1$.

❹ Autrement dit $P = P_2$ et $Q = Q_2$. Ainsi P et Q sont dans Z[X].

P2. On sait que si n est le degré du polynôme minimal commun P de a et b sur K, K(a) et K(b) sont des K-ev de dim n, de base respective $\{1, a, a^2, ..., a^{n-1}\}$ et $\{1, b, b^2, ..., b^{n-1}\}$. Il en résulte que l'application $\sigma : K(a) \to K(b)$ $\sigma(a^k) = b^k$ pour $k < n$ est un isomorphisme *d'espace vectoriel*. Il faut voir que c'est un isomorphisme de corps. Pour cela il faut montrer :

❶ Que pour $k \geq n$ on a encore $\sigma(a^k) = b^k$: cela se fait en effectuant la division euclidienne de X^k par P(X), le reste R étant de degré $\leq n-1$ et $R(a) = a^k$ et $R(b) = b^k$ conduisent au résultat.

❷ Que si x et y sont dans K(a), $\sigma(xy) = \sigma(x)\,\sigma(y)$, ce qui se fait en décomposant sur la base, et en appliquant les propriétés précédentes de σ.

Partie 1 - Généralités sur les polynômes cyclotomiques

I.1. On trouve $\phi_1(X) = X-1$; $\phi_2(X) = X+1$; $\phi_3(X) = X^2+X+1$; $\phi_4(X) = X^2+1$.

I.2. Soit à montrer $X^n - 1 = \prod_{d|n} \Phi_d(X)$. Le polynôme $X^n - 1$ est unitaire de degré n et n'a que des racines simples. Le polynôme $\prod_{d|n} \Phi_d(X)$est aussi unitaire de degré $\sum_{d \mid n} \varphi(d)$. Or on sait que cette somme vaut n. De plus ce polynôme n'a aussi que des racines simples. En effet, pour deux diviseurs d et d' différents de n les racines de $\phi_d(X)$ et $\phi_{d'}(X)$ sont nécessairement différentes, car d'ordre différents. On a donc deux polynômes unitaires, de même degré, ayant tous les deux des racines simples, ces polynômes sont donc égaux.

I.3. Il en résulte un calcul par récurrence des polynômes cyclotomiques : On divise X^n-1 par tous les diviseurs sauf le diviseurs le plus élevé d, on en déduit $\phi_d(X)$. Ainsi, on a par exemple $\phi_5(X) = X^4+X^3+X^2+X+1$, $\phi_6(X) = X^2 - X +1$, etc ...
On en déduit aussi que, pour p premier $\phi_p(X) = X^{p-1}+X^{p-2}+ ... + X^2+X+1$. De même, on a $X^{p^2} - 1 = \Phi_1(X)\Phi_p(X)\Phi_{p^2}(X) = (X^p - 1)\Phi_{p^2}(X)$. ce qui aboutit (en introduisant un changement de variable $Y = X_p$ pour utiliser le polynôme précédent) à $\Phi_{p^2}(X) = X^{p(p-1)} + X^{p(p-2)} + ... X + 1$.

I.4. Les polynômes $\phi_n(X)$ sont à coefficients dans Z, par récurrence.

La propriété est vraie pour n = 1, on la suppose vraie pour tout d < n. On a $X^n - 1 = \phi_n(X) . Q$ où Q est un polynôme unitaire . On a $Q = \prod_{d|n \; d \neq n} \Phi_d(X)$ et donc Q est à coefficient dans Z.

Montrons qu'alors ϕ_n est à coefficients dans Z. On écrit $\phi_n(X) = X^h + a_{h-1}X^{h-1} + ... + a_1X + a_0$. Si ϕ_n n'est pas à coefficients dans Z, soit k l'indice le plus élevè tel que $a_k \notin Z$. Alors on a l'égalité : $(X^n - 1) - Q(X).(X^h + ... + a_{k+1}X^{k+1}) = Q(X).(a_kX^k + ... + a_1X + a_0)$.
Le membre de gauche est dans Z[X]. Celui de droite a pour coefficient de plus haut degré a_k. D'où la contradiction. Ainsi par récurrence, les polynômes cyclotomiques sont dans Z[X].

Partie II - $\phi_n(X)$ est le polynôme minimal de toute racine n^{ième} primitive de l'unité.

II.1. Soit ω une racine primitive de l'unité. Elle est racine de $X^n - 1$. Soit f son polynôme minimal, il divise $X^n - 1$. Il existe donc h(X) - à priori de Q(X) - tel que $X^n - 1 = f(X)h(X)$. Mais f est unitaire, donc h aussi, et d'aprés le lemme P1, f et h sont dans Z[X].
II.2. Soit p un nombre premier avec n, alors ω^p est aussi une racine n^{ième} primitive de l'unité. Soit g sont polynôme minimal. Par le même raisonnement qu'au II.1, il est dans Z[X]. On veut montrer que f = g. On raisonne par l'absurde en supposant $f \neq g$.

II.2.a. f et g comme polynômes minimaux d'éléments algébriques sont irréductibles, donc premiers entre eux. Comme ω^p est racine de $X^n - 1$, on a g | $X^n - 1$, donc g | h (du II.1). Il existe donc $k \in Z[X]$ tel que $X^n - 1 = f(X)g(X)k(X)$.

Mais $g(\omega^p) = 0$, donc ω est racine de $g(X^p)$, autrement dit f(X) | $g(X^p)$. Il existe donc $l \in Z[X]$ tel que $g(X^p) = f(X)\, l(X)$.

II.2.b. En prenant les classes modulo p (on sait alors que $b^p = b$, par le petit théorème de Fermat), on a donc $\overline{g(X^p)} = \overline{g(X)}^p$ et par conséquent $X^n - \bar{1} = \overline{f(X)} . \overline{g(X)} . \overline{k(X)}$ avec $\overline{g(X^p)} = \overline{f(X)} . \overline{l(X)} = \overline{g(X)}^p$. Si φ(X) est un diviseur irréductible de $\overline{f(X)}$ dans Z/pZ[X], alors φ(X) divise aussi $\overline{g(X)}$ (par Gauss) et donc $(\varphi(X))^2$ divise $X^n - \bar{1}$ dans Z/pZ[X]. En dérivant - les nombres premiers sont impairs ici, le cas p = 2 étant immédiat - on arrive à φ(X) divise nX^{n-1} qui est un polynôme non nul car n et p sont premiers entre eux. Il en résulte, φ(X) étant irréductible, que φ(X) = X, ce qui est impossible car X ne divise pas $X^n - \bar{1}$. Il y a donc contradiction à partir de $f \neq g$. On a donc f = g.
II.3. On vient de montrer que, dès que n et p sont premiers entre eux, ω^p est racine de f . On veut montrer que *toute* racine n^{ième} primitive est racine de f. Soit $u = \omega^h$ avec $h \wedge n = 1$, une telle racine n^{ième} primitive de l'unité. En écrivant $h = \prod_{i=1}^{k} p_i$ où les p_i sont premiers non nécessairement distincts, raisonnons par récurrence sur k. Si k = 1, c'est le cas de II.2. Supposons donc que $\omega^{p_1 \cdots p_{k-1}}$ soit racine de f. On lui fait jouer le même rôle que la racine primitive ω aux étapes II.1 et II.2, et alors $\left(\omega^{p_1 \cdots p_{k-1}}\right)^{p_k}$ c'est-à-dire u est aussi racine de f.
II.4. f est donc un polynôme irréductible, unitaire, dont toutes les racines n^{ième} primitives de l'unité sont racines. Comme c'est le polynôme minimal de l'une d'elle, il divise $\phi_n(X)$. Il lui est donc égal car ils sont tous deux unitaires et ont les mêmes racines. Donc $\phi_n(X)$ est irréductible et c'est le polynôme minimal de toute racine n^{ème} primitive de l'unité.

Partie III. Conditions nécessaires pour être un angle constructible.

III.1. Si $2\pi/mn$ est constructible, par report de symétrique, $2\pi/m$ et $2\pi/n$ le sont aussi. Réciproquement, si m et n sont premiers entre eux, par Bezout, il existe deux entiers a et b tels que an + bm =1, et $2\pi/mn = a.2\pi/m + b.2\pi/n$ est donc constructible car on sait faire la somme algébrique de deux angles constructibles.

Par récurrence sur r, dans l'écriture de $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ on est amené à déterminer les angles constructibles de la forme $2\pi/p^\alpha$ où p est un nombre premier.
III.2. Soit donc $2\pi/p^\alpha$ constructible. On note $q = p^\alpha$ et $\omega = \cos 2\pi/q + i \sin 2\pi/q$. On sait que $[Q(\cos 2\pi/q) : Q] = 2^m$ par le résultat de Wantzel. Par ailleurs ω est une racine primitive q^{ième} de l'unité. Son polynôme minimal (cyclotomique) est de degré $\varphi(q) = (p-1)p^{\alpha-1}$.
On a donc $[Q(\omega) : Q] = (p-1)p^{\alpha-1}$. D'autre part $\omega + \omega^{-1} = 2 \cos 2\pi/q$ et ainsi $\cos 2\pi/q \in Q(\omega)$, et ω est racine du polynôme $X^2 - 2\cos 2\pi/q\, X + 1$, d'ou ω est algébrique de degré 2 sur $Q(\cos 2\pi/q)$.
On a ainsi $[Q(\omega) : Q] = [Q(\omega) : Q(\cos 2\pi/q)] . [Q(\cos 2\pi/q) : Q]$, c'est-à-dire $(p-1)p^{\alpha-1} = 2^{m+1}$.
Comme p est premier différent de 2, il en résulte α = 1 et $p = 2^{m+1} + 1$.

III.3. Pour conclure que p est un nombre premier de Fermat, il suffit de montrer que m+1 est une puissance de 2. Ceci est vrai d'une manière générale : si $2^k + 1$ est premier, alors k est une puissance de 2 (sinon $2^{m2^a} + 1$ est divisible par $2^m + 1$ par des arguments classiques).

Partie IV. La condition nécessaire est suffisante.

IV.1. Si p est premier, $\varphi(p) = p-1$. Le polynôme minimal de ω - racine $p^{ème}$ et donc *primitive* de l'unité - sur Q est de degré p-1, c'est même précisément $X^{p-1}+X^{p-2}+ ... + X^2+X+1$ d'aprés I.3, donc $K = Q(\omega)$ est bien de dim p sur Q avec $\{1, \omega, ..., \omega^{p-2}\}$ comme base.

IV.2. Si $g \in G$, g est entièrement déterminé par $g(\omega)$. Or, par le polynôme minimal, on a que $\sum_{k=0}^{p-1} \omega^k$ donc $\sum_{k=0}^{p-1} g(\omega)^k$ et ainsi $g(\omega)$ est aussi racine du polynôme minimal de ω. Donc la valeur prise par $g(\omega)$ est l'une des racines $\omega, ..., \omega^{p-1}$ de ce polynôme, et, en utilisant le lemme donné, chaque g_k défini par $g_k(\omega) = \omega^k$ fourni un tel automorphisme *de corps*. Il y a donc p-1 éléments dans G, c'est-à-dire une puissance de 2 puisque p est un nombre premier de Fermat.

IV.3. l'application $\psi : G \to (Z/pZ)^*$ définie par $\psi(g_k) = \bar{k}$ est surjective, donc bijective par les cardinaux. Montrons que c'est aussi un morphisme. En effet si $g_k \circ g_{k'} = g_{k''}$, cela signifie que $\omega^k\omega^{k'} = \omega^{k''}$ et donc que $\omega^{kk'-k''} = 1$ soit $p \mid kk' - k''$ et donc $\overline{kk'} = \overline{k''}$. C'est donc un morphisme. ψ est donc un isomorphisme de groupe. Il en résulte donc - puisque c'est le cas de $(Z/pZ)^*$ - que G est *cyclique*. On notera dans la suite g un générateur de G.

IV.4. On a vu que $\{1, \omega, ..., \omega^{p-2}\}$ est une base de K sur Q, or comme $\omega^{p-1} = -(1 + \omega + ... + \omega^{p-2})$, il en est de même de $\{\omega, ..., \omega^{p-1}\}$, cette base pouvant s'écrire aussi, en réordonnant les termes, $\{g^h(\omega) / 1 \le h \le p-1\} = \mathbf{B}$ (on a $g^{p-1} = Id$).

IV.5. $K_i \subset K_{i+1}$ car $g^{2^{i+1}} = (g^{2^i})^2$. De plus comme g est générateur de G, $g^{2^n} = Id$ soit $K_n = K$.

IV.6. On a naturellement $Q \subset K_0 = \{ z \in K / g(z) = z\}$. Il faut montrer l'inclusion inverse. Soit donc $z_0 \in K_0$. Il s'écrit dans la base **B** sous la forme $z_0 = \sum_{k=0}^{p-2} \lambda_k g^k(\omega)$ avec $\lambda_k \in Q$ ($g^0(\omega)=\omega$).

On a $g(z_0) = \sum_{k=0}^{p-2} \lambda_k g^{k+1}(\omega)$. Or par hypothèse $g(z_0) = z_0$, il vient alors $\lambda_0 = \lambda_1 = \lambda_2 = ... = \lambda_{p-2}$. Et ainsi $z_0 = \lambda_0(\omega + g(\omega) + ... + g^{p-2}(\omega)) = \lambda_0(\omega + \omega^2 + ...+ \omega^{p-1}) = -\lambda_0 \in Q$. On a donc $Q = K_0$.

IV.7. Montrons d'abord que l'inclusion $K_0 \subsetneq K_1$ est *stricte*. Soit $z = \omega + g^2(\omega) + ... + g^{2^{n-2}}(\omega)$. D'une part $g^2(z) = z$ et donc $z \in K_1$. D'autre part $g(z) = g(\omega) + g^3(\omega) + ... + g^{2^n-1}(\omega)$. De part l'unicité de l'écriture sur la base **B**, on a $g(z) \neq z$ donc $z \notin K_0$.

On montre de même que l'inclusion $K_i \subsetneq K_{i+1}$ *stricte* pour tout i. Pour cela on considère l'élément $z = \omega + g^{2^{i+1}}(\omega) + g^{2^{i+2}}(\omega) + ... + g^{2^{i+1}(2^{n-i+1}-1)}(\omega)$.
On a alors $g^{2^{i+1}}(z) = z$ tandis que $g^{2^i}(z) \neq z$, ce qui prouve l'inclusion *stricte* $K_i \subsetneq K_{i+1}$.

IV.8. On note $f = g^{2^{n-1}}$. On a donc $K_{n-1} = \{z \in K / f(z) = z\}$. Soit λ tel que $f(\omega) = \omega^\lambda$.

IV.8.a. Comme $f^2 = Id$, on a $\omega = f^2(\omega) = f(\omega^\lambda) = \omega^{\lambda^2}$, par isomorphisme de corps, soit $\omega^{\lambda^2-1} = 1$. Il en résulte donc que $p \mid \lambda^2 - 1$, ou encore, dans Z/pZ que $\lambda^2 = 1$, et donc, puisque c'est un corps que $\lambda = 1$ ou $\lambda = -1$ dans Z/pZ (dans Z, on a $0 \le \lambda \le p-1$). Mais $\lambda = 1$ est impossible car on aurait $f = Id$, ce qui n'est pas (car g est générateur, d'ordre 2^n). On a donc $\lambda = -1$, ou encore $f(\omega) = \omega^{-1}$.

IV.8.b. $f(\cos 2\pi/p) = f[\frac{1}{2}(\omega+\omega^{-1})] = \frac{1}{2}[f(\omega) + f(\omega^{-1})] = \frac{1}{2}(\omega^{-1} + \omega) = \cos 2\pi/p$. On a donc bien $\cos 2\pi/p \in K_{n-1}$. De plus $Q(\cos 2\pi/p) \subset K_{n-1} \subsetneq K_n = K$.

IV.8.c. Par ailleurs $\cos 2\pi/p = \frac{1}{2}(\omega^{-1} + \omega)$ s'écrit aussi $\omega^2 - 2\omega\cos 2\pi/p + 1 = 0$ et donc ω est algébrique de degré 2 sur $Q(\cos 2\pi/p)$, soit $[K : Q(\cos 2\pi/p)] = 2$. Donc $[K: K_{n-1}] = 2$ car inférieur ou égal à 2 et différent de 1 à cause des inclusions strictes $K_i \subsetneq K_{i+1}$. Il en résulte, par des arguments de degrés - ou de dimension d'espaces vectoriels - que $K_{n-1} = Q(\cos 2\pi/p)$.

IV.9. On a $Q = K_0 \subset K_1 \subset ... \subset K_{n-1} \subset K_n = K = Q(\omega)$. Pour les degrés d'extensions, on peut aussi écrire $2^n = p - 1 = [K_n : Q] = [K_n : K_{n-1}].[K_{n-1} : K_{n-2}] ... [K_1 : K_0]$. On a ainsi n termes entiers, tous différents de 1, car les inclusions sont strictes, et de produit 2^n . Il en résulte que chaque terme est égal à 2, et on est donc en présence d'une tour d'extension quadratique (TEQ).

C'est en particulier vrai jusqu'à n-1 : $Q = K_0 \subset K_1 \subset ... \subset K_{n-1} = Q(\cos 2\pi/p)$ est une TEQ, ce qui prouve que $\cos 2\pi/p$ est un nombre constructible, c'est-à-dire l'angle $2\pi/p$ est constructible à la règle et au compas, et donc le polygône régulier associé aussi.

Les parties III et IV se résument en le *thèorème de Gauss* rappelé en début de devoir.