Ce cours a été rédigé en décembre 1994 alors que je préparais l'agrégation de mathématiques et mis à jour en juillet 2001.
Dans le cas où il comporterait des erreurs, merci de me les signaler.
Il est exclusivement mis en ligne par le site "la taverne de l'Irlandais" (http://www.tanopah.com).
Ce cours est du niveau Licence.

L'incroyable histoire des polynômes cyclotomiques !

Au sommaire :

1°) La genèse.

Si n est un entier naturel, on appelle polynôme cyclotomique nième ce que l'on note Φ_n et définit comme étant le produit de tous les monômes en X-α où α est une racine primitive nième de l'unité de **C**. Donc $\Phi_n \in \mathbf{C}[X]$.

Mais qu'est une racine primitive nième de l'unité ce que l'on abrège le plus souvent par "RPN" ? Rappelons d'abord que l'ensemble des racines nième de l'unité c'est-à-dire l'ensemble $G_n = \{x \in \mathbf{C} \text{ tel que } x^n = 1\}$ est un sous-groupe multiplicatif de **C**.
Le cardinal de G_n est égal à n.
On appelle alors racine primitive nième de l'unité tout élément de ce groupe l'engendrant.

Or vu que G_n est un sous-groupe multiplicatif de **C** qui est un corps, il est alors cyclique.
De plus les éléments de G_n sont du type $e^{\frac{2ik\pi}{n}}$ avec $k \in \mathbf{Z}$. On peut même écrire que :

$$G_n = \{\text{Exp}(2i\pi k/n) \text{ avec } k \in \{0. . n-1\}\}.$$

Si k est un entier compris entre 0 et n-1, on peut dire que:

$$e^{\frac{2ik\pi}{n}} \text{ est une racine primitive nième de l'unité } \Leftrightarrow \text{ Pgcd(k, n) = 1.}$$

En fait cela est valable pour tout entier naturel k à cause de la relation de Bezout qui sévit dans **Z**.

De part cela et du fait de la simplicité de ses racines, le polynôme cyclotomique de degré n est un polynôme de degré égal au cardinal de l'ensemble des entiers naturels compris entre 1 et n et premiers avec n. C'est également ce que l'on note $\varphi(n)$ où φ est la fonction indicatrice d'Euler.

Exerçons notre science sur quelques exemples :

- Les racines deuxièmes de l'unité sont -1 et 1. Elles forment le groupe multiplicatif G_2.
  Seule -1 engendre celui-ci !
  Le polynôme cyclotomique de rang 2 est donc : $\Phi_2(X) = X + 1$.

- Les racines troisièmes de l'unité sont 1, j et j^2. Seules les deux dernières engendrent le groupe G_3.
  Le polynôme cyclotomique de rang 3 est donc : $\Phi_3(X) = (X - j).(X - j^2) = X^2 - X + 1$.

- Les racines quatrièmes de l'unité sont 1, -1, i et -i. Elles forment le groupe G_4.
  Celui -ci ne peut être engendré que par i et -i. Ainsi : $\Phi_4(X) = (X - i).(X + i) = X^2 + 1$

Ce sont là les trois premiers polynômes cyclotomiques. Ils ont les deux propriétés que nous allons établir dans les deux paragraphes suivants : ils sont à coefficients entiers et sont irréductibles dans **Z**[X].

2°) Un polynôme tout entier.

Pour l'instant, la seule chose que nous sachions sur le polynôme cyclotomique est :

$$\Phi_n(x) = \prod_{\substack{k\in\{0...n-1\} \\ k \text{ premier avec } n}} \left(x - e^{2ik\pi/n}\right)$$

Φ_n est donc clairement un polynôme à coefficients complexes. Mais il est mieux que cela !

Proposition : Pour tout entier naturel non nul n, $\Phi_n \in \mathbf{Z}[X]$.
Autrement tout polynôme cyclotomique a ses coefficients entiers.

La preuve : *Cette affirmation peut paraître péremptoire. Pourtant elle est vraie. Démontrons-le !*
La première chose que nous dirons est que toutes les racines du polynôme X^n - 1 sont simples !
Pourquoi me direz-vous ? La réponse est la suivante :
Nous savons que : $(X^n - 1)' = n.X^{n-1}$
De plus, on peut écrire que :

$$\left(X^n - 1\right) - \frac{X}{n}.\left(X^{n-1}\right) = 1$$

Cette égalité est vraie dans $\mathbf{C}[X]$ qui est un anneau principal où sévit le théorème de Bezout.
Le polynôme X^n - 1 et sa dérivée sont donc premiers entre eux. Cela veut donc dire que les racines de X^n - 1 sont simples.

Comme toutes les racines de X^n - 1 sont simples, il en va alors de même pour celles de Φ_n.

Nous allons à présent établir l'égalité suivante :

$$X^n - 1 = \prod_{d/n} \Phi_d$$

Pour cela, nous allons prouver que les racines de l'un sont aussi celles de l'autre. Et réciproquement !

- Soit α une racine de X^n - 1.
  C'est une racine nième de l'unité donc un élément du groupe multiplication G_n.
  Dans ce groupe, cet élément a un ordre d c'est-à-dire un entier naturel tel que $\alpha^d = 1$.
  Cette égalité fait de α une racine d-ième de l'unité donc un élément de G_d.
  Qui plus est, comme l'ordre de α est égal au cardinal du groupe G_d, alors il engendre celui-ci.
  α est donc une racine d-ième <u>primitive</u> de l'unité. Ainsi α est une racine du polynôme cyclotomique Φ_d.

  Mais l'histoire ne s'arrête pas là ! En fait, dans tout groupe l'ordre de chaque élément divise nécessairement le cardinal de celui-ci.
  Dans le groupe G_n, l'élément α a pour ordre d. Donc d divise n.
  En conclusion : α est une racine du produit $\prod_{d/n} \Phi_d$.

- Soit β une racine du produit $\prod_{d/n} \Phi_d$.
  Il existe donc un polynôme cyclotomique Φ_d dont β est la racine. Qui plus est d divise n.
  Intéressons-nous à β^n.

$$\beta^n = \beta^{d\times\frac{n}{d}} = \left(\beta^d\right)^{\frac{n}{d}} = 1^{\frac{n}{d}} = 1$$

β est donc aussi une racine du polynôme $X^n - 1$.

Dans **C**[X], tous les polynômes sont entièrement scindés. Le fait que deux d'entre eux aient les mêmes racines veut dire qu'ils ont le même degré, sont associés et donc diffèrent d'un complexe.
Il existe donc un complexe c tel que :

$$X^n - 1 = c \times \prod_{d/n} \Phi_d$$

Or nos deux polynômes sont unitaires. Par conséquent, le nombre complexe c vaut nécessairement 1.
D'où l'égalité :

$$X^n - 1 = \prod_{d/n} \Phi_d$$

Notre démonstration n'est pas terminée. Le dernier acte commence maintenant. Nous allons prouver par récurrence sur n que tout polynôme est à coefficients entiers. Et cela va aller très vite !

- *Le stade initial :* nous savons que le seul générateur du groupe $G_2 = \{1 ; -1\}$ est -1.
  Donc $\Phi_2(X) = X + 1$. Chacun conviendra qu'il s'agit là d'un superbe élément de **Z**[X].

- *La propagation d'un rang au suivant :* supposons qu'au rang n, tous les polynômes cyclotomiques Φ_m lorsque $m \leq n$ sont à coefficients entiers.
  Qu'en est-il alors pour Φ_{n+1} ?
  La dernière chose que nous avons établie est que :

$$X^n - 1 = \Phi_{n+1} \times \prod_{\substack{d/n \\ d\neq n}} \Phi_d$$

  Par ce que nous avons supposé, il est clair que $\prod_{\substack{d/n \\ d\neq n}} \Phi_d$ est un polynôme à coefficients entiers !

  Imaginons que Φ_{n+1} ne le soit pas ! A ce moment, son produit avec $\prod_{\substack{d/n \\ d\neq n}} \Phi_d$ sortirait de **Z**[X].

  Ce qui n'est pas possible car celui-ci est ce si superbe et si entier spécimen qu'est $X^n - 1$.
  Par conséquent, les coefficients du cyclotomiques Φ_{n+1} sont nécessairement entiers !

D'où le théorème !

3°) Et en plus il est irréductible !

Nous savons désormais que les polynômes cyclotomiques font partie de l'anneau $\mathbf{Z}[X]$. Ils y sont même tellement bien qu'ils y sont irréductible !

Théorème : Tout polynôme cyclotomique est un irréductible de $Z[X]$.

La preuve : *La démonstration de cette démonstration sera un peu plus difficile que la précédente.*
Avant de nous lancer dans une attaque en règle de ce théorème, nous allons démontrer que :

Si
- α est une racine nième de l'unité.
- P est un irréductible de $\mathbf{Z}[X]$ et unitaire tel que $P(\alpha) = 0$
- p est un entier naturel premier ne divisant pas n

alors $P\left(\alpha^p\right) = 0$

Au boulot !
La première que nous dirons est que le fait que P soit unitaire découle de son irréductibilité et qu'il annule une racine nième.
Comme P est irréductible dans $\mathbf{Z}[X]$, il est alors irréductible dans $\mathbf{Q}[X]$.
En effet les irréductibles de tout anneau factoriel A[X] sont les irréductibles de A et les polynômes de A[X] non constants, primitifs et irréductibles dans K[X] où K est le corps des fractions de A.
Comme $\mathbf{Q}$ est un corps (donc $\mathbf{Q}[X]$ est principal), l'idéal des polynômes qui s'annule en α est alors nécessairement engendré par P.
Donc P divise $X^n - 1$ mais dans $\mathbf{Q}[X]$!
Mais rassurez-vous chers lectrices et lecteurs, cela est également vrai dans $\mathbf{Z}[X]$.
En effet si on note Q l'unique polynôme de $\mathbf{Q}[X]$ tel que $P = Q.(X^n-1)$ on peut alors trouver un $R \in \mathbf{Z}[X]$ primitif et tel que $Q = \lambda . R$ avec $\lambda \in \mathbf{Q}^*$.
De plus il existe deux entiers relatifs a et b tels que $\lambda = \frac{a}{b}$.
Il vient alors aux niveaux des coefficients dominants que b = a.
Et donc $Q = R \in \mathbf{Z}[X]$.
On a alors avec ces mêmes notations que $(\alpha^p)^n = (\alpha^n)^p = 1$. Autrement dit α^p est une racine nième de l'unité.
Supposons que $P(\alpha^p) \neq 0$. On a alors nécessairement que $Q(\alpha^p) = 0$.
Comme le polynôme $Q(X^p)$ s'annule en α tout comme P, le Pgcd de ces deux polynômes dans $\mathbf{Z}[X]$ s'y annule alors lui aussi (en particulier car $X-\alpha$ divise $Q(X^p)$ et P).
Par ce qui a été dit précédemment, P divise nécessairement ce Pgcd qui plongé dans $\mathbf{Q}[X]$ est dans l'idéal des polynômes s'annulant en α. Il vient alors que P divisant un diviseur de $Q(X^p)$, finit par diviser ce dernier.
Si l'on module tout cela par p, on a alors dans l'anneau $\mathbf{Z}/p\mathbf{Z}[X]$ que :

$$X^n - 1 = P.Q$$

en notant pareillement leur classes respectives.

$\mathbf{Z}/p\mathbf{Z}[X]$ étant intègre, il est clair que P et Q sont non nuls.
Or dans cet anneau de caractéristique p, en application de la formule du binôme en caractéristique p, on a que :

$$Q\left(X^p\right) = [Q(X)]^p$$

Et $Q\left(X^p\right)$ est non nul dans $\mathbf{Z}/p\mathbf{Z}[X]$!

Soit r un irréductible de $\mathbf{Z}/p\mathbf{Z}[X]$ divisant P.

Une chose : bien que P est irréductible dans Z[X], rien n'indique qu'il le soit sans $\mathbf{Z}/p\mathbf{Z}[X]$)

Comme P divisait $Q(X^p)$ dans Z[X], qu'il s'agit de polynômes non nul dans $\mathbf{Z}/p\mathbf{Z}[X]$, on a alors que r divise Q^p dans $\mathbf{Z}/p\mathbf{Z}[X]$.

Comme r est un irréductible de ce dernier anneau, nécessairement r divise Q dans $\mathbf{Z}/p\mathbf{Z}[X]$.

Donc r^2 divise $X^n - 1 = Q.P$.
Or par la relation évoquée tout à l'heure entre X^n-1 et sa dérivée, cette relation se conserve dans $\mathbf{Z}/p\mathbf{Z}[X]$.

Donc X^n-1 ne peut admettre dans une extension algébriquement close de $\mathbf{Z}/p\mathbf{Z}[X]$ que des racines simples.
D'où la contradiction avec le fait que r^2 divise X^n-1.
Par suite tombant sur une absurdité, il vient nécessairement que $P(\alpha^p)=0$.

Cette chose prouvée, nous allons lancer notre attaque principale qui fera passer au trépas le théorème ci-dessus visé !

Soit donc P un irréductible de **Z**[X] divisant Φ_n .
De part la définition de ce dernier, P annule nécessairement une racine primitive nième de l'unité qu'on notera α.
Toute racine primitive nième de l'unité est alors de la forme α^m avec m premier avec n.
La première partie de l'assertion découle de définition alors la que la seconde découle du fait que comme $\alpha = e^{\frac{2ik\pi}{n}}$ alors d'une part $\alpha^m = e^{\frac{2ikm\pi}{n}}$ et que de l'autre Pgcd(km, n)=1.
On a alors nécessairement que m est premier avec n.
Regardons alors la décomposition en produit de facteurs premiers de $m = \prod_{i=1}^{k} p_i$ où les p_i sont des premiers positifs de **Z** qui peuvent égaux entre eux.
On parle à ce sujet de décomposition primaire de m. Quoiqu'il en soit on a que $\forall i \in \{1..k\}$ p_i ne divise pas n. Ceci car p_i est premier avec n du fait de m).
En application de ce que l'on a montré en préambule à cette preuve, on a alors que $P(\alpha^{p_1})=0$.
Par récurrence sur i, vu que G_n l'ensemble des racines nièmes de l'unité est un groupe, on montre que finalement P s'annule en α^m et donc pour toutes les racines primitives nièmes de l'unité.
Donc Φ_n divise P dans **Z**[X]
En fait cette relation est dans **C**[X] mais en procédant à une division euclidienne dans **Q**[X] et dans **C**[X] par une histoire d'unicité on a la divisibilité dans **Q**[X]. Puis par un raisonnement analogue à ce qui a été fait au début de la présente preuve on se ramène sans problèmes dans **Z**[X].
Comme P est un irréductible, Φ_n est alors nécessairement associé à P vu que le degré de Φ_n est non nul.
Ce qui assure que Φ_n est un irréductible de **Z**[X].

Autrement dit : Ce qu'on voulait.

4°) Ailleurs.

Il est possible de définir les polynômes cyclotomiques sur tout corps algébriquement clos de la même manière que sur **C**. Mais sur des corps comme les $\mathbf{F}_p$, certains Φ_n sont réductibles.

Enfin et pour terminer si p est premier dans **Z** et si l'on considère les polynômes cyclotomiques définis sur **C**, on a que :

$$\Phi_p(X) = \sum_{i=0}^{p-1} X^i \ .$$