Racines de l'unité

Robert Rolland

11 mars 2000

1 Les définitions

On se place dans un anneau commutatif A. Le problème est de résoudre dans A l'équation $x^r = 1$.

Définition 1.1 *Un élément ξ de A est appelé une racine r^e de l'unité s'il vérifie dans le groupe A^* la relation $\xi^r = 1$. (en particulier ξ est d'ordre fini et son ordre divise r).*

Définition 1.2 *Un élément ξ de A est appelé une racine* **primitive** *r^e de l'unité s'il est d'ordre r dans A^*.*

2 Les théorèmes

Théorème 2.1 *Supposons maintenant que A soit un anneau intègre et $P \in A[X]$. Soient $a_1, \cdots, a_m$ des racines distinctes de P dans A. Alors $P(X)$ est divisible par $(X - a_1) \cdots (X - a_m)$.*

Preuve. $P(a_m) = 0$, donc $P(X)$ est divisible par $(X - a_m)$ dans $A[X]$. Ainsi $P(X) = (X - a_m)Q(X)$. Pour $1 \leq i \leq m - 1$, on a par hypothèse $P(a_i) = 0$, donc $(a_i - a_m)Q(a_i) = 0$, et puisque A est intègre, $Q(a_i) = 0$. Par suite $Q(X)$ a pour racines $a_1, \cdots, a_{m-1}$ et on conclut par récurrence.

Corollaire 2.1 *Si A est intègre un polynôme de degré n a au plus n racines dans A.*

Théorème 2.2 *Soit A un anneau intègre, soit G un sous groupe fini d'ordre r de A^*. Alors G est cyclique et c'est l'ensemble des racines r^e de l'unité dans A. On a dans $A[X]$ la relation*

$$X^r - 1 = \prod_{\xi \in G} (X - \xi).$$

Preuve. Soit $s = \omega(G)$ l'exposant de G. Alors s divise r et on a pour tout x de G l'égalité $x^s = 1$. Mais cette équation a au plus s racines dans A et comme on sait que les r éléments de G sont des solutions alors $s = r$ ce qui signifie que G est cyclique et que cette équation a exactement r racines qui sont tous les éléments de G. Cela implique la relation annoncée.

Remarquons qu'en particulier si A est fini, A^* est cyclique.

Donc si A est un anneau intègre fini, les résultats établis pour les groupes cycliques s'appliquent au groupe multiplicatif A^*.