11. Propriétés arithmétiques de corps algébriques

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **8 (1962)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **26.09.2024**

10. Les équations et les corps algébriques

La théorie des équations conduit à la notion *d'extension* ou *de corps de nombres algébriques.*

On considère l'ensemble des nombres rationnels R et une équation irréductible:

$$\varphi(x) = 0$$

à cœfficients dans R. L'ensemble des polynomes $f(x)$ à cœfficients dans R, définis au module $\varphi(x)$ près, est un corps: les 4 opérations élémentaires sont possibles pour les éléments de cet ensemble. Tout se passe encore comme si on ajoutait à R une irrationnelle α, racine de l'équation considérée; on dit que ce corps est *l'extension* $R(\alpha)$ de R par α.

Si $\alpha_1, \alpha_2 \ldots \alpha_n$ sont les différentes racines de l'équation

$$\varphi(x) = 0$$

on peut construire les extensions:

$$R(\alpha_1), \qquad R(\alpha_2), \ldots\ldots\ldots, R(\alpha_n).$$

Ces corps sont isomorphes, c'est-à-dire que l'on passe de l'un à l'autre par une substitution qui conserve les 4 opérations élémentaires et qui laisse invariants les éléments de R.

Plus généralement, on peut construire des *extensions algébriques finies*, en faisant successivement plusieurs extensions par adjonction d'une racine d'une équation à cœfficients dans le corps déjà formé.

Ce point de vue s'est dégagé progressivement dans la seconde moitié du XIX^e^ siècle.

Bibliographie: 1, 2, 7, 9, 13, 15, 17, 18, 19, 20, 30, 36, 44, 45, 46.

11. Propriétés arithmétiques de corps algébriques

Il a déjà été dit qu'on peut étendre aux corps algébriques la notion *d'entiers* et de *divisibilité* entre entiers, ce qui conduit à la construction des *idéaux.*

On peut aussi chercher des relations arithmétiques entre plusieurs corps algébriques; le point de départ de ces études semble être la loi de réciprocité quadratique de Legendre et Gauss.

On étudie la possibilité de solutions en entiers x (ou y) des congruences:

$$x^2 - q \equiv 0 \quad (\text{mod. } p)$$
$$y^2 - p \equiv 0 \quad (\text{mod. } p)$$

ou p et q sont 2 nombres premiers (positifs). La loi de réciprocité quadratique établit un lien entre ces 2 congruences: si l'un des nombres premiers p ou q est de la forme $4n+1$, avec n entier, ces 2 congruences sont simultanément possibles ou impossibles; si aucun des nombres p et q n'est de la forme $4n+1$, la possibilité d'une des congruences exclut celle de l'autre.

Or la possibilité de la congruence:

$$x^2 - q \equiv 0 \quad (\text{mod. } p)$$

peut être interprétée comme une condition nécessaire et suffisante pour que le nombre premier p soit décomposé en un produit de 2 idéaux premiers dans le corps quadratique engendré par $\sqrt{q}$. La loi de réciprocité quadratique établit ainsi un lien entre l'arithmétique dans les 2 corps quadratiques engendrés respectivement par $\sqrt{p}$ et $\sqrt{q}$.

On peut d'ailleurs démontrer cette loi en construisant le corps de $\sqrt{q}$ au moyen de racines qièmes de l'unité. L'idée de cette démonstration provient de recherches de GAUSS sur la construction des polygones réguliers. Cette démonstration introduit un lien entre l'arithmétique du corps des racines qièmes de l'unité et du corps quadratique engendré par $\sqrt{p}$.

D'autres *lois de réprocité* ont pu être démontrées et rassemblées dans la *théorie du corps des classes.*

Bibliographie: 1, 10, 17, 19, 20, 26, 27, 46.

12. NOTION GÉNÉRALE D'IDÉAUX

L'extension d'un corps par un nombre algébrique a conduit à introduire d'autres extensions et à les définir d'un point de vue plus axiomatique. La notion *d'anneau* est ainsi apparue importante: