

Galois : le « $2n$ » de la p. 414 et le « $2N$ » de la p. 444

Notes de lecture sur galois.pdf (Œuvres mathématiques, éd. Gabay), pages 414 et 444 du manuscrit original (pdf p. 38 et 68)

Ces deux « 2 » n'ont rien à voir l'un avec l'autre, et aucun ne dit simplement « un nombre pair ».

Page 414 : le « $2n$ » est le double du genre

Page 413, Galois écrit que le nombre de périodes distinctes de l'intégrale la plus générale attachée à une irrationnelle donnée est toujours pair, et il le note $2n$. Puis il énonce que « une somme quelconque de termes se réduit à n termes, plus des quantités algébriques et logarithmiques ». C'est le théorème d'Abel, et n est ce qu'on appellera plus tard le **genre** (Lie, p. 5 du pdf, dit que Galois possédait cette notion). Pour une intégrale elliptique, $n = 1$: deux périodes.

À la page 414, le $2n$ sert à compter les points de division. Diviser les $2n$ périodes en p parties égales donne $p^{2n} - 1$ valeurs non nulles, car on prend toutes les combinaisons $(a_1\omega_1 + \dots + a_{2n}\omega_{2n})/p$ avec a_i entier mod p , non tous nuls. Le groupe de l'équation est alors le groupe linéaire de $(\mathbb{Z}/p\mathbb{Z})^{2n}$, d'ordre $(p^{2n} - 1)(p^{2n} - p)\dots(p^{2n} - p^{2n-1})$. Pour $n = 1$, on retrouve le cas elliptique des pages 410 et 411, avec les substitutions $(k, l) \rightarrow (ak + bl, ck + dl) \bmod p$. L'équation de la division d'une somme de n termes en p parties est de degré p^{2n} , et Galois l'affirme soluble par radicaux.

Page 444 : le « $2N$ » est le double d'une constante

Ici N est une lettre pour une constante, et non un nombre pair. Le contexte est le fragment du second Mémoire, sur les équations primitives de degré p^2 . Le groupe réduit agit sur $p + 1$ lettres, avec des substitutions homographiques $k \rightarrow (mk + n)/(rk + s)$. Galois demande si un tel groupe peut contenir des substitutions d'ordre p tout en restant soluble par radicaux. Il suppose que les autres éléments sont d'ordre $p + 1$, et que ceux-ci échangent les lettres deux par deux.

1. Une substitution qui est son propre inverse force $s = -m$. On peut alors l'écrire $k \rightarrow m + N/(k - m)$, avec $N = m^2 + n$, c'est-à-dire un quart du discriminant de ses points fixes.
2. Conjuguer par une translation $k \rightarrow k + a$ change m en $m + a$ mais laisse N inchangé. Toutes ces substitutions ont donc le même N , ce que dit sa phrase « N est le même pour toutes les substitutions ».
3. Il écrit ensuite que deux de ces substitutions, d'indices m et n , commutent (c'est ce que dit son égalité). Le calcul donne exactement $(m - n)^2 = 2N$ pour $m \neq n$. Je l'ai vérifié par un calcul symbolique.
4. Tous les m sont dans $\mathbb{F}_p$, et deux d'entre eux diffèrent de $\pm\sqrt{2N}$. On a donc au plus trois valeurs : m , $m + d$ et $m - d$. Il faut alors que $2d = \pm d$, donc $3d = 0 \bmod p$, soit $p = 3$.

Pour p premier, $p = 3$ est donc le seul cas où ce groupe réduit peut contenir un élément d'ordre p . L'équation réduite est alors du quatrième degré, donc soluble par radicaux. C'est l'exception du degré 9 déjà annoncée à la page 395.

L'étape 3 est une reconstruction : le texte écrit l'égalité sans dire pourquoi les deux substitutions doivent commuter. Le calcul confirme seulement que cette égalité équivaut à $(m - n)^2 = 2N$.

Pour p premier impair, « pair » ne veut rien dire modulo p , puisque 2 est inversible et que tout élément est le double d'un autre. Le 2 de la page 444 est donc un vrai coefficient, qui vient du calcul de $(m - n)^2$.