

Astérisque

DAVID A. GAY

Normal extensions defined by a binomial equation

Astérisque, tome 41-42 (1977), p. 215-218

<http://www.numdam.org/item?id=AST_1977__41-42__215_0>

© Société mathématique de France, 1977, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (<http://smf4.emath.fr/Publications/Asterisque/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

NORMAL EXTENSIONS DEFINED BY A BINOMIAL EQUATION

by

David GAY*

Let F be a field and α a root of $x^n - a \in F[x]$. When is $F(\alpha)$ normal over F ? When is $F(\alpha)$ the splitting field of $x^n - a$ over F ? Consider the following

Examples (over the rational field \mathbb{Q}).

(1) $x^3 - 2$ ($\mathbb{Q}(\alpha)$ is not normal for any root α).

(2) $x^{12} - 1$ ($\mathbb{Q}(\alpha)$ is normal for any root α ; there exists a root β such that $\mathbb{Q}(\beta)$ is the splitting field).

(3) $x^6 + 3$ ($\mathbb{Q}(\alpha)$ is the splitting field for every root α).

(4) $x^6 + 27$ ($\mathbb{Q}(\alpha)$ is the splitting field for every root α).

(5) $x^{42} - 21^7$ (If $\sqrt[6]{21}$ is a real 6-th root of 21 and ζ a primitive 42-th root of 1, then $\sqrt[6]{21}$ and $\zeta\sqrt[6]{21}$ are roots of the binomial; $\mathbb{Q}(\sqrt[6]{21})$ is not normal; $\mathbb{Q}(\zeta\sqrt[6]{21})$ is the splitting field).

(6) $x^4 - 9$ ($\mathbb{Q}(\alpha)$ is normal for every root; for no root is $\mathbb{Q}(\alpha)$ the splitting field).

* Partially supported by Battelle Institute, Columbus, Ohio.

Background. Darbi [1] found all irreducible, normal binomials over \mathbb{Q} . Example (3) is from his list. Mann and Vélez [3] extended this list to include all binomials sharing the property of examples (3) and (4) : $\mathbb{Q}(\alpha)$ is the splitting field for every root α . They call such binomials uniformly normal. In case the exponent is a prime power, Schinzel [4 ; Proposition 1] has determined for an arbitrary field those binomials which are products of normal polynomials (thus including irreducible and uniformly normal binomials).

In this exposé we consider a binomial $x^n - a \in \mathbb{Q}[x]$ satisfying the property (shared by examples (2) - (5)) :

There exists a root α of $x^n - a$ such that $\mathbb{Q}(\alpha)$ is the splitting field of $x^n - a$.

Such a binomial is called partially normal and the special root α a generating root.

Results. In the theorem below we list all partially normal binomials (over \mathbb{Q}). Without loss of generality, we consider only those binomials $x^n - a$ with a an integer. For positive integer b , let $s(b)$ be the largest square integer dividing b and $f(b) = b/s(b)$, the square-free part of b . If c is a square-free integer ($s(c) = 1$), we denote by $\ell(c)$ the number of prime factors of the form $4k+3$. Let \mathbb{N} denote the natural numbers.

THEOREM. The partially normal binomials over \mathbb{Q} are

- (A) $x^m \pm b^m$, $m, b \in \mathbb{N}$.
- (B) $x^{2m} \pm b^m$, $m, b \in \mathbb{N}$ such that $f(b) > 1$ and, in case sign is negative and
 $m = 2m'$ with m' odd, then $f(b) \mid m'$ and $\ell(f(b))$ odd.
- (C) $x^{4m} - b^m$, $m, b \in \mathbb{N}$, m odd, $f(b) \mid m$, and $\ell(f(b))$ odd.
- (D) $x^{4m} + b^m$, $m, b \in \mathbb{N}$, $f(b) > 1$, and
 (a) if m is odd, then $f(b) \mid m$ and $\ell(f(b))$ even,

BINOMIAL EQUATION

(b) if m is even, then $f(b) \mid (m/2)$.

(E) $x^{6m} - b^m$, $m, b \in \mathbb{N}$, $(m, 6) = 1$, $3 \mid f(b)$, $f(b) \mid 3m$, and $\ell(f(b))$ even.

(F) $x^{6m} + b^m$, $m, b \in \mathbb{N}$, $(m, 3) = 1$, $4 \nmid m$, $3 \mid f(b)$ and

(a) if m is odd, then $f(b) \mid 3m$ and $\ell(f(b))$ even,

(b) if m is even, then $2 \mid f(b)$ and $f(b) \mid 6m$.

Moreover, the Galois group of a partially normal binomial is abelian iff it falls under case (A) or (B) .

Remarks. A more detailed version of theorem (with proof) together with some consequences of the notion of partially normal binomial over real fields can be found in [2] .

An investigation of normal extensions (of a field F) defined by a binomial equation might start with γ algebraic over F , $F(\gamma)$ normal over F , and $\gamma^m \in F$ for some m . From these assumptions, if n is the smallest positive integer such that $\gamma^n \in F$, one can show that a primitive n -th root of 1 is in $F(\gamma)$. It then follows that $x^n - \gamma^n$ is partially normal over F . The converse is not true : if $x^n - a$ is partially normal over F with generating root α , then it may be the case that $\alpha^t \in F$ for some $t < n$. [2, p. 21] .

-:-:-:-

BIBLIOGRAPHY

- [1] G. DARBI.- "Sulla riducibilità delle equazioni algebriche". Annali di Mat. pur. e appl., Ser. 4, 4 (1926), 185-208.
- [2] D. GAY, A. Mc. DANIEL, W. VELEZ.- "Partially normal radical extensions of the rationals". Battelle Mathematics Report N° 97 (1975).
- [3] H. MANN, W. VELEZ.- "On normal radical extensions of the rationals". Lin. and Multilin. Alg., 3 (1975), 73-80.
- [4] A. SCHINZEL.- "Les résidus de puissances et les congruences exponentielles". Rapport, Journées Arithmétiques, Caen (1976).

David GAY
Battelle
Advanced Studies Center
7, route de Drize
CH - 1227 CAROUGE (Suisse)