ON THE DISCRIMINANT OF CUBIC POLYNOMIALS

MARKUS ROST

Contents

1. Introduction

The starting point of this text was a certain presentation of the discriminant of cubic forms (see Lemma 1, for a quick grasp see Subsection 3.2).

I observed it after looking more closely at the parametrization of cubic cyclic extensions presented in [2] (see equation (1)).

At the beginning there were just formulas, I had no good explanation (see Remark 4). However, some weeks after writing a first version of this text, I found an interpretation (see Remark 5, in particular (3)). Comments are welcome anyway.

At some point I added brief descriptions of $\mathbf{Z}/n\mathbf{Z}$-torsors (first for $n = 3$, then also for $n = 2$).

Here one looks for an embedding of $\mathbf{Z}/n\mathbf{Z}$ into some affine algebraic group G which has no non-trivial torsors over fields (or local rings). The group G should be as small as possible, at least somewhat pleasant.

As for $\mathbf{Z}/2\mathbf{Z}$-torsors, there is such a group G which is an open subscheme of the affine line $\mathbf{A}^1$ (see Section 5).

For $\mathbf{Z}/3\mathbf{Z}$-torsors there is such a group G as well. It is an open subscheme of the projective line $\mathbf{P}^1$ (see Section 4). After removing the unit element in $G/(\mathbf{Z}/3\mathbf{Z})$ one ends up with the parametrization of cubic cyclic extensions presented in [2].

2. Preliminaries

Recall that the cubic polynomial

$$ax^3 + bx^2y + cxy^2 + dy^3$$

has the discriminant

$$b^2c^2 - 4ac^3 - 4db^3 - 27a^2d^2 + 18abcd$$

Date: August 17, 2018.

Let R be a ring and consider a normed cubic polynomial

$$P(x) = x^3 - Tx^2 + Qx - N$$

over R. Then its discriminant is

$$\Delta = T^2Q^2 - 4Q^3 - 4NT^3 - 27N^2 + 18TQN$$

If we let

$$L = R[x]/\big(P(x)\big)$$

be the cubic extension of R given by P, then we have

$$\begin{aligned} T &= \mathrm{trace}_{L/R}(x) \\ Q &= \mathrm{trace}_{L/R}(x^{\#}) \\ N &= \mathrm{norm}_{L/R}(x) \end{aligned}$$

where $x^{\#}$ is the adjoint of x (characterized by $xx^{\#} = \mathrm{norm}_{L/R}(x)$).

3. A presentation of the discriminant

Let

$$H = R[\eta]/\big(\eta^3 - N\big)$$

For the norm of such a cubic "Kummer" extension one has the formula

$$N_{H/R}(a + b\eta + c\eta^2) = a^3 + Nb^3 + N^2c^3 - 3Nabc$$

Lemma 1. *One has*

$$\Delta = (TQ - 9N)^2 - 4N_{H/R}(Q + T\eta + 3\eta^2)$$

Proof. By computation:

$$\begin{aligned} (TQ - 9N)^2 &= T^2Q^2 - 18TQN + 3 \cdot 27N^2 \\ N_{H/R}(Q + T\eta + 3\eta^2) &= Q^3 + NT^3 + 27N^2 - 9NQT \end{aligned}$$

□

3.1. The case of an element of norm 1.

Assume $N = 1$. Hence our polynomial is of the form

$$P(x) = x^3 - Tx^2 + Qx - 1$$

Lemma 1 yields

Corollary 2.

$$\Delta = (9 - TQ)^2 - 4(3 + T + Q)(3 + T\zeta + Q\zeta^2)(3 + T\zeta^2 + Q\zeta)$$

with

$$1 + \zeta + \zeta^2 = 0$$

□

3.2. **The case of an element of norm -1.** Sometimes it is convenient to consider the case $N = -1$ (this is equivalent to the case $N = 1$, one just has to replace x by $-x$).

In this case one has

$$P(x) = x^3 - Tx^2 + Qx + 1$$

and

$$\Delta = (9 + TQ)^2 - 4(3 - T + Q)(3 - T\zeta + Q\zeta^2)(3 - T\zeta^2 + Q\zeta)$$

again with $1 + \zeta + \zeta^2 = 0$.

Remark 3. It follows that if

$$Q = T - 3$$
$$N = -1$$

then Δ is a square. If Δ is invertible, this means that the cubic extension is cyclic.

Indeed, in [2] one finds the following description of cubic cyclic extensions:

$$x^3 - Tx^2 + (T - 3)x + 1 = 0 \tag{1}$$

The discriminant is $(T^2 - 3T + 9)^2$ and

$$\sigma(x) = \frac{1}{1 - x}$$

is an automorphism of the corresponding cubic extension of order 3.

Remark 4. I found Lemma 1 as follows.

From the description

$$x^3 - Tx^2 + (T - 3)x + 1$$

of a generic cubic cyclic extension in [2] (see above) it follows that if

$$Q = T - 3$$
$$N = -1$$

then $\Delta = (TQ + 9)^2$. Thus, if $N = -1$, then

$$Z(T, Q) = \Delta - (TQ + 9)^2$$

must be divisible by $Q - T + 3$ (as a polynomial in T, Q).

But the expressions Δ and $TQ + 9$ don't change if x is replaced by ζx with ζ a cube root of unity. Thus the polynomial Z is invariant under

$$T \mapsto \zeta T, \qquad Q \mapsto \zeta^2 Q$$

Therefore Z is divisible by $Q\zeta^2 - T\zeta + 3$ as well.

By working over $R = \mathbf{Q}$ (or $R = \mathbf{Z}$) one concludes

$$Z(T, Q) = cA(1)A(\zeta)A(\zeta^2) \qquad (A(t) = Qt^2 - Tt + 3)$$

where $1, \zeta, \zeta^2$ are the roots of $t^3 - 1$ (so that $1 + \zeta + \zeta^2 = 0$). The quantity c must be a constant for degree reasons. One finds $c = -4$.

It is then obvious to get rid of the condition $N = \pm 1$ by using cube roots of N.

Remark 5. Meanwhile I have found an interpretation. Here is a brief account.

Let us first write down things again: The cubic polynomial

$$f = ax^3 + bx^2y + cxy^2 + dy^3$$

has discriminant

$$\begin{aligned}\Delta &= b^2c^2 - 4ac^3 - 4db^3 - 27a^2d^2 + 18abcd \\ &= (bc - 9ad)^2 - 4\Phi\end{aligned}$$

with

$$\Phi = ac^3 + db^3 + 27a^2d^2 - 9abcd$$

The problem is to interpret the quantity Φ. And to explain why for $a = d = 1$ there is the factorization

$$\Phi_{a=d=1} = (3 + b + c)(3 + b\zeta + c\zeta^2)(3 + b\zeta^2 + c\zeta) \tag{2}$$

with $1 + \zeta + \zeta^2 = 0$.

It turns out that Φ is the determinant of a certain 3×3 matrix, namely

$$\Phi = \det A$$

with

$$A = \begin{pmatrix} 3ad & bd & ca \\ c & 3d & b \\ b & c & 3a \end{pmatrix}$$

Also the term $(bc - 9ad)^2$ appears as determinant, namely simply as

$$(bc - 9ad)^2 = \det \begin{pmatrix} B & 0 \\ 0 & B \end{pmatrix}, \qquad B = \begin{pmatrix} 3a & b \\ c & 3d \end{pmatrix}$$

This yields the presentation

$$\Delta = \det \begin{pmatrix} 3a & b \\ c & 3d \end{pmatrix}^2 - 4 \det \begin{pmatrix} 3ad & bd & ca \\ c & 3d & b \\ b & c & 3a \end{pmatrix} \tag{3}$$

of the discriminant.

Note that if $a = d = 1$, then A becomes

$$A_{a=d=1} = \begin{pmatrix} 3 & b & c \\ c & 3 & b \\ b & c & 3 \end{pmatrix} = 3 + b\sigma + c\sigma^2$$

where σ the permutation matrix

$$\sigma = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

This readily explains the factorization (2).

In particular: If $a = d = 1$ and $3 + b + c = 0$, then A vanishes on $(1, 1, 1)$, so $\det A = 0$ and from (3) it follows that Δ is a square. Hence the cubic extension associated to

$$x^3 + bx^2y - (b + 3)xy^2 + y^3$$

is cyclic (as long as it is separable, that is if $b^2 + 3b + 9$ is invertible).

How to find the matrix A (and B)? That's a longer story. Clearly the quantity Φ is not an invariant of the cubic form f. To get a hand on Φ one somehow has to break the GL_2-symmetry. It turns out that it is appropriate to choose from the beginning a non-degenerate quadratic form q up to multiplication with scalars. This reduces the symmetry group GL_2 to the similarity group $\mathrm{GO}(q)$ of q. (The groups $\mathrm{GO}(q)$ are the normalizers of the maximal tori in GL_2; if $q = xy$ then $\mathrm{GO}(q) = \mathbf{G}_{\mathrm{m}}^2 \rtimes \mathbf{Z}/2\mathbf{Z}$.)

After some juggling one obtains a certain linear morphism A between certain rank 3 modules. In the special case $q = xy$, the morphism A has the matrix presentation given above.

As a side result, one obtains a somewhat natural presentation of the discriminant Δ as a "square mod 4". That Δ is a square mod 4 is clear from the fact that Δ is the discriminant of a quadratic algebra, namely of the discriminant algebra of the cubic form. Under presence of the quadratic form $q = xy$ that algebra is of the form

$$T^2 - T(bc - 9ad) + \Phi$$

(For the discriminant algebra of a cubic algebra see [1].)

4. On the generic C_3-torsor

We conclude with some remarks about (1).

Remark 6. In [2] it is shown that equation (1) is versal for cyclic cubic extensions. One can show the following somewhat more precise remark: For any field k, any cubic cyclic field extension of k is given by (1) for some $T \in k$. This holds as well for the split cubic extension k^3 if and only if $|k| \geq 5$.

Remark 7. Consider the flat R-algebras of rank 2

$$A = R[\theta]/(\theta^2 + \theta + 1)$$
$$B = R[\eta]/(\eta^2 + 3\eta + 9)$$

The algebra homomorphism

$$j\colon B \to A$$
$$\eta \mapsto 3\theta$$

is injective if 3 is not a zero divisor. Let

$$\widetilde{\varphi}\colon A^\times \to A^\times$$
$$\widetilde{\varphi}(z) = \frac{z^3}{N_{A/R}(z)} = \frac{z^2}{\bar{z}}$$

where $\bar{z} = T_{A/R}(z) - z$ denotes the canonical involution on the quadratic algebra A. One finds that $\widetilde{\varphi}$ has image in B. More precisely: The map

$$\varphi\colon A^\times \to B^\times$$
$$\varphi(x + y\theta) = \frac{(x^3 - 3xy^2 + y^3) + xy(x - y)\eta}{x^2 - xy + y^2}$$

has the property

$$(j \circ \varphi)(z) = \widetilde{\varphi}(z)$$

Note that $\varphi(a) = a$ for $a \in R^\times$.

Moreover, φ is a group homomorphism. It suffices to check this for $R = \mathbf{Z}$. But then j is injective and the claim follows from the multiplicativity of $\widetilde{\varphi}$.

Let

$$C_3 = \{1, \theta, \theta^2\} \subset A^\times$$

(This is the constant group scheme $\mathbf{Z}/3\mathbf{Z}$ even in characteristic 3.)

One finds that the resulting sequence

$$1 \to C_3 \to \mathbf{G}_{\mathrm{m}}(A)/\mathbf{G}_{\mathrm{m}} \xrightarrow{\varphi} \mathbf{G}_{\mathrm{m}}(B)/\mathbf{G}_{\mathrm{m}} \to 1$$

of algebraic groups is exact. So if R is a local ring, the sequence

$$1 \to C_3 \to A^\times/R^\times \xrightarrow{\varphi} B^\times/R^\times \to H^1(R, C_3) \to 0$$

is exact (use $H^1\big(R, \mathbf{G}_{\mathrm{m}}(A)\big) = 0$ in some appropriate flat topology). To summarize:

Corollary 8. *For local rings R, there is a bijection between the group*

$$B^\times/\varphi(A^\times)$$

and the set of isomorphism classes of pairs (L, σ) where L is a cubic etale extension of R and σ is a R-automorphism of L of order 3.

Note that

$$\mathbf{G}_{\mathrm{m}}(A)/\mathbf{G}_{\mathrm{m}} = \mathbf{P}^1 \setminus \{u^2 - uv + v^2 = 0\}$$
$$\mathbf{G}_{\mathrm{m}}(B)/\mathbf{G}_{\mathrm{m}} = \mathbf{P}^1 \setminus \{U^2 - 3UV + 9V^2 = 0\}$$

The morphism φ extends to the morphism

$$\mathbf{P}^1 \to \mathbf{P}^1/C_3 \simeq \mathbf{P}^1$$

considered in[2].

5. On $\mathbf{Z}/2\mathbf{Z}$-torsors

Since we are about such things, let us also look at the case of quadratic etale extensions ($\mathbf{Z}/2\mathbf{Z}$-torsors).

Here one considers the groups of invertible matrices

$$G = \mathbf{A}^1 \setminus \{\tfrac{1}{2}\} = \operatorname{Spec} \mathbf{Z}[a][(1-2a)^{-1}] = \{\, X(a) \,\}$$
$$H = \mathbf{A}^1 \setminus \{\tfrac{1}{4}\} = \operatorname{Spec} \mathbf{Z}[b][(1-4b)^{-1}] = \{\, Y(b) \,\}$$

where

$$X(a) = \begin{pmatrix} 1 & a \\ 0 & 1-2a \end{pmatrix} \qquad (1 - 2a \neq 0)$$
$$Y(b) = \begin{pmatrix} 1 & b \\ 0 & 1-4b \end{pmatrix} \qquad (1 - 4b \neq 0)$$

There are the natural group homomorphisms

$$j \colon H \to G$$
$$j\big(Y(b)\big) = X(2b)$$

and

$$\varphi \colon G \to H$$
$$\varphi\big(X(a)\big) = Y(a - a^2)$$

Note that

$$(j \circ \varphi)(z) = z^2$$

The morphism φ yields the exact sequence

$$0 \to \mathbf{Z}/2\mathbf{Z} \to G \xrightarrow{\varphi} H \to 1 \tag{4}$$

of algebraic groups where

$$\mathbf{Z}/2\mathbf{Z} = \{X(0), X(1)\} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \right\}$$

If 2 is invertible, (4) becomes

$$1 \to \mu_2 \to \mathbf{G}_{\mathrm{m}} \xrightarrow{x \mapsto x^2} \mathbf{G}_{\mathrm{m}} \to 1$$

In characteristic 2, (4) becomes

$$0 \to \mathbf{F}_2 \to \mathbf{G}_{\mathrm{a}} \xrightarrow{x \mapsto x^2 + x} \mathbf{G}_{\mathrm{a}} \to 0$$

The resulting generic $\mathbf{Z}/2\mathbf{Z}$-torsor is

$$x^2 - x + b = 0$$

with discriminant $1 - 4b$.

Remark 9. It follows that a separable quadratic extension of a local ring has a generator of trace 1. Let us establish this directly.

Note first that for a separable extension the trace is an epimorphism. Then apply the following more general observation:

Lemma 10. *Let L/R be a quadratic extension whose trace map $T\colon L \to R$ is an epimorphism. If R is local, there exists a generator $x \in L$ with $T(x) = 1$.*

Proof. For x to be a generator means that 1, x is an R-basis of L. This holds if and only if it holds after passing to the residue class field k of R. Moreover, $T(x)$ is invertible if and only if its image in k is nonzero.

Therefore we may assume that R is a field. Then $x \in L$ is a generator if and only if $x \notin R$.

The affine line $T^{-1}(1) \subset L$ and the vector subspace $R \subset L$ meet in at most one point (one has $T^{-1}(1) \cap R = \emptyset$ if and only if $\operatorname{char} R = 2$). Hence $T^{-1}(1) \setminus R \neq \emptyset$ and the claim follows.

More explicitly: Let $t \in L$ be a generator with

$$t^2 - at + b = 0$$

The image of the trace map is $aR + 2R$. If a is invertible, one may take $x = ta^{-1}$. If $a = 0$, then 2 must be invertible and $x = t + 2^{-1}$ does the job. □

References

[1] M. Rost, *The discriminant algebra of a cubic algebra*, Preprint, 2002, ⟨www.math.uni-bielefeld.de/~rost/binary.html#cub-disc⟩.

[2] J. Serre, *Topics in Galois theory*, Research Notes in Mathematics, vol. 1, Jones and Bartlett Publishers, Boston, MA, 1992, Lecture notes prepared by Henri Damon [Henri Darmon], With a foreword by Darmon and the author.

Fakultät für Mathematik, Universität Bielefeld, Postfach 100131, D-33501 Bielefeld, Germany

E-mail address: rost *at* math.uni-bielefeld.de

URL: www.math.uni-bielefeld.de/~rost