123.

Extensions icosaédriques

Séminaire de Théorie des Nombres de Bordeaux 1979/80, n° **19**

L'exposé de J-P. SERRE a porté sur le contenu de la lettre suivante, que nous reproduisons avec l'autorisation de l'auteur; cette lettre répondait à une lettre circulaire envoyée par J. D. GRAY (University of New South Wales, Australia), qui recherchait un exposé moderne du contenu du livre de KLEIN sur l'Icosaèdre.

Princeton, March 17–25, 1978

dear M. GRAY,

I am sorry to have been so slow in answering your query about KLEIN's Icosahedron book. I have been looking at it, off and on, for the past weeks without being able to write anything.

First, I could not find any "modernized" treatment of the subject and I doubt there is one. The most recent I found is DICKSON's "Modern Algebraic Theories" (1930), chap. XIII. See also WIMAN's "Endliche Gruppen linearen Substitutionen" (Enzykl. Math. Wiss. I B3f), H. WEBER "Algebra II" and above all R. FRICKE's "Lehrbuch der Algebra II" (1926) which I find much more understandable than KLEIN. I hope you get more references from other people, for instance, ARNOLD, FRIED, BRIESKORN, HIRZEBRUCH; they could tell you about the relations of $\mathfrak{A}_5$, the exceptional root system E_8 and the surface $x^2+y^3+z^5=0$ (see for instance the recent papers of NARUKI in Invent. Math. and Math. Annalen).

Now, some remarks about the topics considered in KLEIN's book:

1. Fields of definition

Let $G=\mathfrak{A}_5$ be the icosahedral group. KLEIN uses in an essential way the fact that G acts faithfully on a curve X of genus 0, and that the quotient X/G is also of genus 0. He is not precise about fields of definition – and need not be since he uses explicit formulae, with only harmless irrationalities in them. Still, it is of some interest to look into the matter more closely:

Notice first that, to each such curve (with action of G), one can attach a *square root of* 5, which then must be in the ground field k, if X and the elements of G are defined over k (in which case I will say that X is a "G-curve over k"). Indeed, if one extends the ground field to its algebraic closure, the action of G gives an embedding $G \to \mathbf{PGL}_2$. If $c \in G$ is a chosen element of order 5, it will correspond to it a matrix A (defined up to multiplication by a scalar), with eigenvalues (λ, μ) such that λ/μ is a primitive 5th root of unity. If you put $x = 1 + 2\,(\lambda/\mu + \mu/\lambda)$ you find that $x^2 = 5$, and that x is intrinsically attached to c (it does not depend on the representative matrix, nor on the choice of the field extension).

So, if we want a G-curve over k, we must assume that k contains a square root of 5. Do so, and choose one such; call it $\sqrt{5}$. We restrict ourselves to G-curves whose corresponding square-root of 5 is the chosen one. Then one can prove that *there is indeed such a G-curve over k*, and that it is *unique*, up to *unique isomorphism* (i.e. if X and X' are two such, there is a unique isomorphism $f\colon X \to X'$ such that $f \circ g = g \circ f$ for all $g \in G$). The unicity assertions are easy (especially the last one which amounts to saying that the centralizer of G in $\mathbf{PGL}_2$ is reduced to $\{1\}$). The existence assertion could be deduced from the unicity ones by standard «descent» methods of algebraic geometry. One may also use a more explicit method, see below.

When we have the G-curve X over k, two natural questions arise:

a) is it true that X is isomorphic to the projective line $\mathbf{P}_1$, i.e. that X has a k-rational point, or equivalently that G can be embedded into $\mathbf{PGL}_2(k)$?

b) is it true that the quotient curve X/G is isomorphic to $\mathbf{P}_1$?

(Remember that a curve of genus 0 is not always isomorphic to $\mathbf{P}_1$ over the ground field! There is an "obstruction" which is a quaternion algebra.)

The answer to b) is "yes"; that is easy: there are three canonical points on X/G, where the covering $X \to X/G$ is ramified of order 2, 3, 5; these points, being unique, are rational over k. But a curve of genus 0 with a rational point is isomorphic to $\mathbf{P}_1$. Hence the result. (One may want to normalize the isomorphism between X/G and $\mathbf{P}_1$ so that the three canonical points correspond to $0, 1, \infty$; this is what Klein does.)

The answer to a) is more interesting: X is not always isomorphic to $\mathbf{P}_1$. More precisely, the quaternion algebra attached to X is the *standard* quaternion algebra $H_k = k \otimes H$, generated by i, j with $ij = -ji$, $i^2 = -1$, $j^2 = -1$. Hence *X is isomorphic to $\mathbf{P}_1$ if and only if H_k is* "split" (i.e. is isomorphic to the matrix algebra $\mathbf{M}_2(k)$ or equivalently *if and only if -1 is a sum of two squares in k*).

To show this, one may, for instance, give an explicit embedding of $G = \mathfrak{A}_5$ into the projective group of H_k, i.e. H_k^*/k^* (which is a "twisted form" of $\mathbf{PGL}_2$, in Galois parlance). One may do that using explicit formulae due to Coxeter (I believe); I don't have the reference here, but they are reproduced
1 in a recent paper of M.-F. Vignéras in Crelle. Another method is to use the representation of G as a Coxeter group in 3-space; this works over $\mathbf{Q}(\sqrt{5})$, and gives an embedding of G into $\mathbf{SO}_3(f)$, where f is some quadratic form in 3 variables over $\mathbf{Q}(\sqrt{5})$; one has then to check that the field of quaternions attached to f is indeed H_k. Both methods give at the same time an explicit construction of the G-curve X.

To sum up:

If we just want X over k, we need only $\sqrt{5} \in k$; if we also want that $X \simeq \mathbf{P}_1$, we need that -1 is a sum of two squares in k.

Note that both conditions can be met by adjoining quadratic numbers to k, i.e. $\sqrt{5}$ and $\sqrt{-d}$ for any rational $d > 0$. Hence they are harmless from the point of view of "solving equations".

One more remark on this: if, instead of $\mathfrak{A}_5$, we are interested in $G = \mathfrak{A}_4$ or $\mathfrak{S}_4$, then the situation is similar, but simpler: the condition $\sqrt{5} \in k$ disappears, the G-curve X always exists and is unique, and it is isomorphic to $\mathbf{P}_1$ if and only if the quaternion algebra H_k splits.

(In the above, I have implicity assumed that characteristic $k = 0$. If you are interested in the case where characteristic $k = p \neq 0$, here is what happens: if $p \neq 2$, the G-curve X exists if $G = \mathfrak{A}_4$, $\mathfrak{S}_4$, and if $G = \mathfrak{A}_5$ and $\sqrt{5} \in k$; if $p = 2$, it exists if $G = \mathfrak{A}_4$, $\mathfrak{A}_5$ and $\sqrt[3]{1} \in k$; it does not exist if $G = \mathfrak{S}_4$, $p = 2$. Whenever it exists, it is k-isomorphic to $\mathbf{P}_1$, since the BRAUER group of a finite field is 0.)

Note also the following: suppose we define X over $\mathbf{Q}(\sqrt{5})$, and let K be its function field. The action of $G = \mathfrak{A}_5$ on X defines an action of G on K, which leaves fixed the field of constants $\mathbf{Q}(\sqrt{5})$. This action can be extended to *an action of* $\mathfrak{S}_5$ on K, in such a way that the elements of $\mathfrak{S}_5 - \mathfrak{A}_5$ act on $\mathbf{Q}(\sqrt{5})$ by $\sqrt{5} \mapsto -\sqrt{5}$ ("semi-algebraic" action). In other terms, if we view X as a curve *over* $\mathbf{Q}$ ($\mathbf{Q}$-irreducible, but $\mathbf{Q}(\sqrt{5})$-reducible with two components), we have an action of $\mathfrak{S}_5$ on X. I mention this for two reasons:

a) this is what comes naturally from the modular form point of view, cf. below;

b) there is a very simple model for this action, namely the following: consider the quadric Y in projective space defined by the homogeneous equations

$$(*) \qquad x_1 + \ldots + x_5 = 0\,, \quad x_1^2 + \ldots + x_5^2 = 0\,.$$

There is a natural action of $\mathfrak{S}_5$ on Y (permutation of coordinates). Now, call X the "set" of straight lines on Y. It is well known that X has a natural structure of (reducible) curve, with two components (which can be separated on the field of the square root of the discriminant, which is here $\mathbf{Q}(\sqrt{5})$), each of genus 0. The action of $\mathfrak{S}_5$ on Y defines an action of $\mathfrak{S}_5$ on X, which is "our" curve X.

(Similarly, the curve of genus 0 with $\mathfrak{S}_4$-action can be defined as the conic $x_1 + \ldots + x_4 = 0$, $x_1^2 + \ldots + x_4^2 = 0$.)

2. "Solution" of the quintic equation

Assume first that $\sqrt{5}$ belongs to k, and let X, $X/G \simeq \mathbf{P}_1$ be as above. If z is a k-point of X/G, its inverse image in X is not in general rational over k; more precisely, the field of rationality of a lifting $x \in X$ of z is a Galois extension of k, whose Galois group is a subgroup of G. In particular, this group may be G itself. We may ask *whether we get in this way all Galois extensions of k with group* $G = \mathfrak{A}_5$. If so, the G-covering $X \to X/G$ would be quite analogous to the quadratic covering $x \mapsto x^2$ ($\mathbf{P}_1 \to \mathbf{P}_1$) which gives all quadratic extensions.

This is essentially the question answered by HERMITE and KLEIN. The result is "almost" *yes*, as you will see.

Let us first translate the question into a more geometric one. Let us call k'/k our given extension with Galois group G (it is associated to a quintic equation with square discriminant). The natural homomorphism $\mathrm{Gal}(k'/k) \simeq G \to \mathrm{Aut}(X)$ allows us to make $\mathrm{Gal}(k'/k)$ act on X. By "descent" (see for instance Weil's paper on the lowering of the field of constants, Amer. J. around 1955, or my "Cohomologie galoisienne"), this gives us a twisted curve $X_{k'}$ and we see easily that:

k'/k comes from the covering $X \to X/G$ if and only if $X_{k'}$ has a rational point over k.

Since $X_{k'}$ has genus 0, the last condition also means that the quaternion algebra $H_{k'}$ attached to $X_{k'}$ *splits over k.* This condition is not always fulfilled (one can construct counter-examples). But it can be met *by a suitable quadratic extension of k,* and in fact by many such; this (as Weil pointed out to me) is
2 the source of the "accessorische Irrationalität" mentioned by Klein in the last §§ of his book. Since quadratic extensions are regarded as harmless by Klein, Hermite, etc., you see why I say that the answer to the question above is "almost" yes!

To make this more concrete, one needs a simple description of the twisted curve $X_{k'}$, and the corresponding quaternion algebra $H_{k'}$. Here are two ways to do this, one using cohomology, one using quadratic forms:

i) It is well known that the cohomology group $H^2(G, \mathbf{Z}/2\mathbf{Z})$ is cyclic of order 2; it contains a unique non trivial element ξ, which corresponds to the central extension of G given by the "binary icosahedral group" of order 120. Since $G \simeq \mathrm{Gal}(k'/k)$, this gives an element $\xi_{k'} \in H^2(\mathrm{Gal}(k'/k), k'^*) \subset \mathrm{Br}(k)$. One can check (sauf erreur...) that the class of $H_{k'}$ is equal to $(-1,-1) + \xi_{k'}$, where $(-1,-1)$ is the class of the standard quaternion algebra.

ii) Suppose that k'/k is given as the Galois closure of a quintic field k_1/k. View k_1 as a 5-dimensional vector space over k, and consider the projective quadric $Y_{k'}$ defined by the equations

$$\mathrm{Tr}(z) = 0\,, \qquad \mathrm{Tr}(z^2) = 0 \quad (\text{for } z \in k_1)\,.$$

This quadric is obtained by Galois twisting from the quadric Y of p. 4. Hence its "curve of lines" is the twisted curve $X_{k'}$. From this, and the elementary geometry (resp. algebra) of quadrics (resp. quaternary quadratic forms), one deduces:

ii$_1$) the class of $H_{k'}$ is the sum of $(-1,-1)$ and the *Witt invariant* of the
3 quadratic form $\mathrm{Tr}(z^2)$ (on the subspace of k_1 of elements of trace 0); in other words, $H_{k'}$ is the unique quaternion algebra whose norm form is proportional to this quaternary quadratic form;

ii$_2$) *$X_{k'}$ has a rational point if and only if $Y_{k'}$ has one, i.e. if and only if there is a non zero element z of k_1 such that* $\mathrm{Tr}(z) = \mathrm{Tr}(z^2) = 0$.

In more concrete terms, this means that the answer to our original question is "yes" whenever k' can be generated by the roots of a quintic equation of the form $X^5 + aX^2 + bX + c = 0$, i.e. an equation *without X^4 and X^3 terms.* This fits with the results of Klein and Hermite.

Instead of assuming that $G = \mathfrak{A}_5$ and $\sqrt{5} \in k$, I could have assumed that $\sqrt{5} \notin k$, $G = \mathfrak{S}_5$, and that the quadratic subfield of k'/k is $k(\sqrt{5})$. The result would have been the same as in ii$_2$).

3. Connection with modular forms

There is not much to say: if we take the field K_5 of modular functions of level 5 with coefficients in $\mathbf{Q}(\sqrt[5]{1})$, it is well known by now (see for instance SHIMURA's book, or LANG's Elliptic Functions or DELIGNE-RAPOPORT) that the group $\mathbf{GL}_2(\mathbf{Z}/5\mathbf{Z})/\{\pm 1\}$ acts on K_5 in a "semi-linear" way, the field of invariants being just $\mathbf{Q}(j)$, the field of modular function of level 1. Moreover, the genus of K_5 is 0. Consider now the subfield of K_5 fixed under the action of the center (which is of order 2) of $\mathbf{GL}_2(\mathbf{Z}/5\mathbf{Z})/\{\pm 1\}$; call K_5' that field. It corresponds to a curve X of genus 0, with field of constants $\mathbf{Q}(\sqrt{5})$, and action of $G = \mathbf{PGL}_2(\mathbf{Z}/5\mathbf{Z})$; since the latter group is well known to be isomorphic to $\mathfrak{S}_5$, we have thus reconstructed the situation of § 1.

From this point of view, the problem of § 2 amounts to the following; suppose $\sqrt{5} \in k$ (resp. $\sqrt{5} \notin k$); let k'/k be a Galois extension with group $\mathfrak{A}_5$ (resp. with group $\mathfrak{S}_5$, and quadratic subfield equal to $k(\sqrt{5})$). Does there exist $j \in k$ such that k' is generated by the j-invariants $j_1, \ldots, j_6$ of the six elliptic curves which are 5-isogeneous to the curve with invariant j (i.e. the solutions of $T_5(X, j) = 0$ where T_5 is the transformation equation of order 5)? Answer: same as in § 2, i.e. "yes" if and only if the quaternion algebra $H_{k'}$ splits.

As for the modular interpretation of the "Hauptfläche"

$$Y: \sum x_i = 0, \quad \sum x_i^2 = 0,$$

see FRICKE, p. 124, 139, ...

I'll stop here. But I am well aware that the remarks above barely scratch the subject: there is so much more in KLEIN's book, and in FRICKE's! Invariants, hypergeometric functions, and everywhere, a wealth of beautiful formulae! Will you write down any of these? In case you do, please send me a copy.

Yours

J-P. SERRE