SOME CONTRIBUTIONS ON RATIONAL CUBIC GALOIS EXTENSIONS

Antonio Paques
and
Andrzej Solecki

RELATÓRIO TÉCNICO Nº 20/87

ABSTRACT. In these notes we prove that: (i) any Galois cubic extension of the field $\mathbb{Q}$ of the rational numbers is of the form $\mathbb{Q}(f) = \mathbb{Q}[X] / (f(X))$ with $f(X) = X^3 - 3X - G$, $G = 2\cos\Gamma$, for some $\Gamma \in S^1$; (ii) for $f(X) = X^3 - 3X - G$ the extension $\mathbb{Q}(f)$ is Galois iff for $\Gamma = \arccos(\frac{G}{2})$ and $\Gamma_j = \Gamma + j\frac{2\pi}{3}$ one has $G_j = 2\cos\Gamma_j \in \mathbb{Q}$, $j = 0,1,2$; (iii) if the extension $\mathbb{Q}(f)$ is non trivial it is of the form $\mathbb{Q}(\cos\gamma)$ and $\cos\gamma_1, \cos\gamma_2 \in \mathbb{Q}(\cos\gamma)$, where $\gamma = \frac{\Gamma}{3}$ and $\gamma_j = \gamma + j\frac{2}{3}$, $j = 0,1,2$; $\mathbb{Q}(f)$ is trivial iff all $\cos\gamma_j \in \mathbb{Q}$ and in this case $\mathbb{Q}(f) \simeq \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}$; (iv) the collection of all these extensions is parametrized by non-zero elements of the ring $\mathbb{Z}[\omega]$, where $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2} i \in \mathbb{C}$; (v) the natural generators of the Harrison group $T(\mathbb{Z}_3, \mathbb{Q})$ are indexed by ω and those rational primes that satisfy $p \equiv 1 \pmod 3$.

Universidade Estadual de Campinas
Instituto de Matemática, Estatística e Ciência da Computação
IMECC – UNICAMP
Caixa Postal 6065
13.081 - Campinas, SP
BRASIL

Maio – 1987

§ 1. INTRODUCTION.

We classify and present explicitly all cubic Galois extensions of the field $\mathbb{Q}$ of the rational numbers. Still, the definitions of this section embrace the more general case as they are taken from the Galois theory of rings.

All rings considered here are commutative and with unity. If R is a subring of S then their unities coincide. The standard notation $U(R)$ is used for the group of units of R. Let G

be an abelian finite group.

DEFINITION 1. If S is an overring of R, S is a Galois extension of R with the Galois group $Gal(S/R) = G$ if G is a subgroup of $AutS$ and

(i) the stabilizer $S^G = \{s \in S : \forall \sigma \in G, \sigma(s) = s\}$ is equal to R;

(ii) for any maximal ideal $p \subset S$ and any $\sigma \in G$; $\sigma \neq 1$, there exists $x \in S$ such that $\sigma(x) - x \notin p$.

(Conditions which can substitute (ii) in this definition are listed in [1], Theorem 1.3).

DEFINITION 2. Two Galois extensions S, S' of R with the same Galois group G are equivalent if there exists a bijection $S \to S'$ which is an isomorphism of rings and also an isomorphism of RG-modules.

As usually RG is the group ring of G with coefficients in R. From now on, let $G \simeq \mathbb{Z}_n$ be a cyclic group of order n. Then a class of equivalence of the above relation can be written as $[S,\sigma]$, where S is an Galois extension of R with Galois group $\mathbb{Z}_n$ and σ is a fixed generator of $\mathbb{Z}_n$. The set $T(\mathbb{Z}_n,R)$ of classes $[S,\sigma]$ becomes a group (cf. [4], p. 3 - 4) under the following operation: if $[S,\sigma], [S',\sigma'] \in T(\mathbb{Z}_n,R)$, let $[S,\sigma] * [S',\sigma'] = [S'',\sigma'']$ where $S'' = (S \otimes_R S')^{\delta\mathbb{Z}_n}$ with $\delta\mathbb{Z}_n$ being the copy of $\mathbb{Z}_n$ in $\mathbb{Z}_n \otimes \mathbb{Z}_n$ generated by $\sigma^{-1} \otimes \sigma'$, and $\sigma'' = \sigma \otimes id$ generating the copy of $\mathbb{Z}_n$ that acts on S''. The trivial element of the group $T(\mathbb{Z}_n,R)$ is $[R^n,\iota]$, where ι permutes cyclicly the copies of R in $\mathbb{R}^n$, $\iota(r_1,r_2,\ldots,r_n) = (r_n,r_1,\ldots,r_{n-1})$.

In case of a local ring R with $2 \in U(R)$ and $n = 3$ there is another description of $T(\mathbb{Z}_3,R)$ in [5] that originated from considering cubic polynomials $f \in R[X]$. It will be used in the next sections, so let us recall here the basic points of it. Consider

the set

$$T(R) = \{(b,c,d) \in R^3 : b \in U(R) \wedge d^2 = 2^2b^3 - 3^3c^2\}$$

and introduce the following operation in $T(R)$:

$$(b,c,d) * (b',c',d') = (bb', \tfrac{1}{2}(cd' + c'd), \tfrac{1}{2}(dd' - 3^3cc')).$$

Commutativity of the operation is evident, associativity follows from the direct application of the definition of $*$, the triple $(1,0,2)$ is the trivial element and the triple $(\frac{1}{b}, -\frac{c}{b^3}, \frac{d}{b^3})$ is inverse to (b,c,d). Thus, $(T(R),*)$ is an abelian group.

Next, define a certain type of triples which correspond to polynomials that are completely reducible over R.

DEFINITION 3. A triple $(x,y,z) \in T(R)$ is trivial if there exist $r_o, r_1, r_2 \in R$ such that

$$(X - r_o)(X - r_1)(X - r_2) = X^3 - xX - y$$

and

$$(r_1 - r_o)(r_2 - r_1)(r_o - r_2) = z.$$

Denote the subset of trivial triples by $T'(R)$. We have $(1,0,2) \in T'(R)$ as $0, -1, 1 \in R$ are the three required elements. If r_o, r_1, r_2 satisfy the definition for the triple $(x,y,z) \in T'(R)$ then $-\frac{r_2}{x}, -\frac{r_1}{x}, -\frac{r_o}{x} \in R$ satisfy the definition for $(\frac{1}{x}, -\frac{y}{x^3}, \frac{z}{x^3})$, so that $(x,y,z)^{-1} \in T'(R)$, too. Now, take two trivial triples $(x,y,z), (x',y',z') \in T'(R)$ corresponding to the ordered sets of roots $r_o, r_1, r_2 \in R$ and $r_o', r_1', r_2' \in R$, respectively, and define $s_o = r_1r_1' - r_2r_2'$, $s_1 = r_2r_2' - r_or_o'$ and $s_2 = r_or_o' - r_1r_1'$. By a straightforward and tedious calculation one can

prove that $xx' = -(s_0s_1 + s_1s_2 + s_2s_0)$, $\frac{1}{2}(yz' + y'z) = s_0s_1s_2$ and $\frac{1}{2}(zz' - 3^3yy') = (s_1 - s_0)(s_2 - s_1)(s_0 - s_2)$. So, the product of trivial triples is trivial and, consequently, $T'(R)$ is a subgroup of $T(R)$. Let $\tau(R)$ be the quotient group $T(R)/T'(R)$ whose elements are denoted by $[b,c,d]$, meaning the class represented by $(b,c,d) \in T(R)$.

In [5] the group $\tau(R)$ was introduced by inducing the operation $*$ on $\tau(R) = T(R)/\approx$, where the relation "$\approx$" was defined as follows: two triples (b,c,d), $(b',c',d') \in T(R)$ are equivalent (notation: $(b,c,d) \approx (b',c',d')$), if there exist trivial triples (x,y,z) and (x',y',z') such that $(b,c,d) * (x,y,z) = (b',c',d') * (x',y',z')$. However, it is not clear that this approach cut short much calculations as verifying that $\approx$ is indeed a relation of equivalence one has to check up that the product of trivial triples is trivial.

Before stating the main result of [5] let us also note that given $(b,c,d) \in T(R)$, where R is a local ring with $2 \in U(R)$, if $d \notin U(R)$ then necessarily $3^3c^2 \in U(R)$: from $d^2, 3^3c^2 \in p$ (p being the maximal ideal of R) it would follow $2^2b^3 \in p$, contradicting the assumptions $2, b \in U(R)$. Therefore, if $d \notin U(R)$ use the trivial triple $(3,2,0)$ to obtain $(b,c,d) * (3,2,0) = (3b,d,-3^3c^2)$. Obviously, $b' = 3b \in U(R)$ and $d' = -3^3c^2 \in U(R)$. Thus, any element in $\tau(R)$ can be represented by a triple $(b,c,d) \in T(R)$ with $d \in U(R)$.

We end up the introduction recalling the following result (cf. [5], Théorème 3.2 and Note 3.3):

THEOREM 4. Let R be a local ring with $2 \in U(R)$. The $\tau(R)$ is a group of exponent 3 isomorphic to $T(\mathbb{Z}_3,R)$. The isomorphism is given by

$$\tau(R) \to T(\mathbb{Z}_3,R) : [b,c,d] \mapsto [S,\sigma],$$

where $S = R[X]/(f)$, (f) is the ideal in $R[X]$ generated by $f(X) = X^3 - bX - c$, and for $x = X + (f) \in S$ the action of σ is given by

$$\sigma(x) = \frac{3b}{d} x^2 - \frac{9c + d}{2d} x - \frac{2b^2}{d}.$$

§ 2. AN ADDITIVE VERSION OF $\tau(\mathbb{Q})$

Starting with this section we restrict our attention to $R = \mathbb{Q}$, the field of rational numbers. As usually, $S^1 = \mathbb{R}/2\pi\mathbb{Z}$ is the additive group of angles.

LEMMA 5. The set $V = \{\alpha \in S^1 : \cos(\alpha + j\frac{2\pi}{3}) \in \mathbb{Q} \text{ for } j = 0,1,2\}$ is a subgroup of S^1.

PROOF. If $\alpha \in V$ we have

$$\cos((\alpha + j\frac{2\pi}{3}) + \frac{2\pi}{3}) - \cos((\alpha + j\frac{2\pi}{3}) - \frac{2\pi}{3}) = -\sqrt{3}\sin(\alpha + j\frac{2\pi}{3}),$$

so that

$$(1) \qquad \sqrt{3}\sin(\alpha + j\frac{2\pi}{3}) \in \mathbb{Q} \quad \text{for} \quad j = 0,1,2.$$

We have to show that if $\alpha, \beta \in V$ then $\alpha - \beta \in V$. Note that

$$\cos((\alpha - \beta) + j\frac{2\pi}{3}) =$$

$$= [\cos(\alpha + j\frac{2\pi}{3})] \cdot [\cos\beta] + [\frac{1}{3}] \cdot [\sqrt{3}\sin(\alpha + j\frac{2\pi}{3})] \cdot [\sqrt{3}\sin\beta]$$

and all values in brackets are rational numbers; thus, we have $\cos((\alpha - \beta) + j\frac{2\pi}{3}) \in \mathbb{Q}$ for $j = 0,1,2$. ∎

LEMMA 6. For every $[b,c,d] \in \tau(\mathbb{Q})$ there exist $G, K \in \mathbb{Q}$ such that $[b,c,d] = [3,G,K]$.

PROOF. For $[t] \in \tau(\mathbb{Q})$ we have $[t]^{-1} = [t^2]$ (cf. [5], Proposition 3.1); on the other hand, $(b,c,d) * (b,c,-d) = (b^2,0,-2b^3)$ is a trivial triple, so that $[b,c,d]^{-1} = [b,c,-d]$. Keeping also in mind that $b \neq 0$ and that the triple $(3,2,0)$ is trivial we perform the following calculations:

$$(b,c,d)^2 = (b^2,cd,2b^3 - 3^3c^2) = (b^2, \frac{cd}{b^3} b^3, (2 - \frac{3^3c^2}{b^3})b^3) =$$

$$= (1, \frac{cd}{b^3}, 2 - \frac{3^3c^2}{b^3}) * (b^2,0,2b^3) \approx (1, \frac{cd}{b^3}, 2 - \frac{3^3c^2}{b^3}) * (3,2,0) =$$

$$= (3, 2 - \frac{3^3c^2}{b^3}, -3^3 \frac{cd}{b^3}) \approx (3, 2 - \frac{3^3c^2}{b^3}, 3^3 \frac{cd}{b^3})^2.$$

Thus, putting $G = 2 - \frac{3^3c^2}{b^3}$, $K = 3^3 \frac{cd}{b^3}$ we have $[b,c,d] = [3,G,K]$. ∎

Here is the main result of this section.

THEOREM 7. The mapping

$$\tau(\mathbb{Q}) \to V/3V : [3,G,K] \mapsto \arccos \frac{G}{2} + 3V$$

is a group isomorphism.

PROOF. As $K^2 = 2^2 3^3 - 3^3 G^2 \geq 0$, we have $|G| \leq 2$ that is, there exists such $\Gamma \in S^1$ that

$$G = 2 \cos \Gamma. \tag{2}$$

As the consequence of $K^2 = (6\sqrt{3} \sin \Gamma)^2$ we may put

$$K = 6\sqrt{3} \sin \Gamma. \tag{3}$$

The choice of $-K$ instead of K would amount to the substitution of Γ by $-\Gamma$ and would give rise to another isomorphism. Thus, restating Lemma 6 we see that every element of $\tau(\mathbb{Q})$ is represented by a triple $(3, 2\cos\Gamma, 6\sqrt{3}\sin\Gamma)$ for a suitable $\Gamma \in S^1$. We

will show that: (i) starting with $(3,G,K) \in T(\mathbb{Q})$ we get $\Gamma \in V$, (ii) $(3,G,K)$ is trivial iff $\Gamma \in 3V$, (iii) equivalent triples give angles congruent modulo $3V$, (iv) multiplication of triples modulo trivial ones corresponds to the addition of angles, (v) the function is surjective.

Start with the identity

$$\cos\Gamma = 4\cos^3\frac{\Gamma}{3} - 3\cos\frac{\Gamma}{3}.$$

Multiply it by 2, put $Z = 2\cos\frac{\Gamma}{3}$, $G = 2\cos\Gamma$. The result is

(4) $$f(Z) = 0 \quad \text{where} \quad f(Z) = Z^3 - 3Z - G.$$

The roots are

(5) $$g_j = 2\cos\gamma_j, \quad j = 0,1,2, \text{ where } \gamma_j = \gamma + j\frac{2\pi}{3} \text{ and } 3\gamma = \Gamma.$$

Let us now proceed with the proof of the steps (i)-(v):

(i) if $(3,G,K) \in T(\mathbb{Q})$ then, by (2) and (3), we have

$$\cos\Gamma = \frac{G}{2} \in \mathbb{Q}, \quad \cos(\Gamma \pm \frac{2\pi}{3}) = -\frac{G}{4} \mp \frac{K}{12} \in \mathbb{Q}$$

and $\Gamma \in V$.

(ii) If the triple $(3,G,K)$ is trivial then $f(Z)$ given by (4) decomposes over $\mathbb{Q}$ and $\cos\gamma_j = \frac{g_j}{2} \in \mathbb{Q}$ for $j = 0,1,2$. But it means that $\gamma \in V$ and $\Gamma = 3\gamma \in 3V$. Conversely, if $\Gamma \in 3V$ then $\gamma \in V$ and the roots g_j, $j = 0,1,2$, given by (5) are in $\mathbb{Q}$ and the triple $(3,G,K)$ is trivial.

(iii) Let $(3,G,K)$, $(3,G',K') \in T(\mathbb{Q})$ be two equivalent triples. Then for a trivial triple $(1,x,y)$ we have

$$(3,G',K') = (3,G,K) * (1,x,y).$$

Note that $(1,x,y) * (3,2,0) = (3,y,-3^3x)$ corresponds to an angle in $3V$, call it 3Δ, as it was shown in (ii). Form $y = 2\cos 3\Delta$, $-3^3x = 6\sqrt{3}\sin 3\Delta$ we get

$$(1,x,y) = (1, -\frac{2\sqrt{3}}{9}\sin 3\Delta, 2\cos 3\Delta).$$

If $\Gamma = \arccos\frac{G}{2}$ and $\Gamma' = \arccos\frac{G'}{2}$; the equation involving the equivalent triples becomes

$$(3,2\cos\Gamma', 6\sqrt{3}\sin\Gamma') = (3,2\cos(\Gamma + 3\Delta), 6\sqrt{3}\sin(\Gamma + 3\Delta)),$$

that is $\Gamma' = \Gamma + 3\Delta$.

(iv) It is sufficient to verify that $(3,2\cos\Gamma, 6\sqrt{3}\sin\Gamma) *$ $(3,2\cos\Delta, 6\sqrt{3}\sin\Delta) = (3,2\cos(\Gamma+\Delta), 6\sqrt{3}\sin(\Gamma+\Delta)) * (3,2,0)$.

(v) If $\Gamma \in V$, form the polynomial f using the identity which precedes (4). By (1), $K = 6\sqrt{3}\sin\Gamma \in \mathbb{Q}$, that is, there exists a triple $(3,G,K) \in T(\mathbb{Q})$ that is sent into the class $\Gamma + 3V$.

Resuming the argument: in view of (i), the mapping defining Γ in terms of G and K via (2) and (3) has, in fact, its values in V. By (iii) it is well-defined on $\tau(\mathbb{Q})$ with values in $V/3V$. Then, (iv) shows that the mapping is a homomorphism. From (ii) it follows that it is injective and from (v) it follows that it is also surjective. ∎

§ 3. THE INTEGRAL PARAMETRIZATION OF $\tau(\mathbb{Q})$

Let $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i \in \mathbb{C}$ be the third root of unity and put $\mathbb{Z}[\omega] = \{A + B\omega \in \mathbb{C} : A, B \in \mathbb{Z}\}$. Taking the subset $\mathbb{Z}[\omega]^*$ of non-zero elements of this ring we may form its "projective line"

$L = \mathbb{Z}[\omega]^*/\mathbb{Z}^*$. It should be clear that L with the multiplication induced by multiplication in $\mathbb{C}$ becomes a group: only the existence of inverse classes deserves any proof but this, too, is evident from the fact that $\bar{\omega} = -1 - \omega \in \mathbb{Z}[\omega]$ and the equalities $[z]\cdot[\bar{z}] = [z\bar{z}] = [1]$.

In this section we will prove the following result.

THEOREM 8. $L/L^3 \cong \tau(\mathbb{Q})$.

The proof of Theorem 8 will follow some auxiliary statements and constructions.

First, consider the group ring $R\mathbb{Z}_3$ of the group $\mathbb{Z}_3$ generated by σ, and with coefficients in a ring R. If $v = v_o + v_1\sigma + v_2\sigma^2 \in U(R\mathbb{Z}_3)$, we define its transpose $v^t = v_o + v_2\sigma + v_1\sigma^2$ and we say that v is orthogonal if $v^{-1} = v^t$. Clearly, this loan of terms of linear algebra is due to the 3-dimensional representation of $\mathbb{R}\mathbb{Z}_3$ induced by the mapping $\sigma \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$. Orthogonal elements form a subgroup of $U(R\mathbb{Z}_3)$ which is denoted by $\mathrm{Ort}(R\mathbb{Z}_3)$.

We will need later the following fact which we have not managed to pinpoint to any specific textbook on group rings.

LEMMA 9. If $v \in \mathbb{R}\mathbb{Z}_3$ and $v^3 = 1$ then $v = \sigma^j$ for $j = 0, 1$ or 2.

PROOF. Consider the homomorphism of rings

$$\theta : \mathbb{R}\mathbb{Z}_3 \to \mathbb{C} : \sigma \mapsto \omega.$$

If $v^3 = 1$ then $\theta(v) = \omega^j$; so, $v \equiv \sigma^j \pmod{\mathrm{Ker}\,\theta}$, that is, $v = \sigma^j + xw$ where $w = 1 + \sigma + \sigma^2$ and $x \in \mathbb{R}$. But $w^2 = 3w$ and from $v^3 = 1$ we get

$$(3x)w(3x^2 + 3\sigma^j x + \sigma^{2j}) = 0.$$

It means that either $x = 0$ or $y_j(x) = 3x^2 + 3\sigma^j x + \sigma^{2j}$ is real and equal to zero or $y_j(x)$ is not real but it annihilates the element w. The second possibility does not occur as it would force $j = 0$ but $y_0(x) = 3x^2 + 3x + 1$ is positive for all $x \in \mathbb{R}$. The third one is also excluded as the annihilator of w is the principal ideal generated by $1 - \sigma$ and it is easy to see that $y_j(x)$ does not belong to it for $j = 1,2$ and any $x \in \mathbb{R}$. Thus, we must have $x = 0$ and $v = \sigma^j$. ∎

LEMMA 10. $\tau(\mathbb{Q}) \cong \mathrm{Ort}(\mathbb{Q}\mathbb{Z}_3)/(\mathrm{Ort}(\mathbb{Q}\mathbb{Z}_3))^3$.

PROOF. To begin with, to each triple of the form $(3,G,K) \in T(\mathbb{Q})$ we ascribe, as in the proof of Theorem 7, the angle Γ and, consequently, the ordered set $\{g_0,g_1,g_2\} \subset \mathbb{R}$ with g_j's given by (5). Next, define $h = h_0 + h_1\sigma + h_2\sigma^2 \in \mathbb{R}\mathbb{Z}_3$, where

$$(6) \qquad h_j = \frac{g_j + 1}{3} = \frac{2\cos(\gamma + j\,\frac{2\pi}{3}) + 1}{3}, \quad j = 0,1,2, \quad \gamma = \frac{\Gamma}{3}.$$

As the elements g_0,g_1,g_2 are the roots of $f(Z)$ given by (4), they satisfy the relations

$$g_0 + g_1 + g_2 = 0, \quad g_0g_1 + g_1g_2 + g_2g_0 = -3, \quad g_0g_1g_2 = G.$$

These relations and (6) yield

$$(7) \qquad h_0 + h_1 + h_2 = 1, \quad h_0h_1 + h_1h_2 + h_2h_0 = 0, \quad h_0h_1h_2 = \frac{G - 2}{3^3}.$$

The first two relations imply that $h \in \mathrm{Ort}(\mathbb{R}\mathbb{Z}_3)$.

Next, take two triples $(3, 2\cos\Gamma, 6\sqrt{3}\sin\Gamma)$ and $(3,2\cos\Gamma',6\sqrt{3}\sin\Gamma')$ that lead to $h = h_0 + h_1\sigma + h_2\sigma^2$ and $h' = h_0' + h_1'\sigma + h_2'\sigma^2$ respectively, where

$$h_o = \frac{2\cos\gamma + 1}{3}, \quad h'_o = \frac{2\cos\gamma' + 1}{3}, \quad 3\gamma = \Gamma, \quad 3\gamma' = \Gamma'.$$

Direct calculations using (7) and the identity $\cos\alpha\cos\beta = \frac{1}{2}(\cos(\alpha+\beta) + \cos(\alpha-\beta))$ show that

(8) $hh' = h''_o + h''_1\sigma + h''_2\sigma^2$ with $h''_j = \frac{2\cos((\gamma+\gamma') + j\frac{2\pi}{3})}{3}$, $j = 0,1,2.$

Hence, putting $G_j = 2\cos(\Gamma + j\frac{2\pi}{3})$ for $j = 0,1,2$ we get

(9) $H = h^3 = H_o + H_1\sigma + H_2\sigma^2$, where $H_j = \frac{G_j + 1}{3} \in \mathbb{Q}$ for $j = 0,1,2;$

so that $h^3 \in \mathrm{Ort}(\mathbb{R}\mathbb{Z}_3) \cap \mathbb{Q}\mathbb{Z}_3 = \mathrm{Ort}(\mathbb{Q}\mathbb{Z}_3)$. The announced isomorphism sends the class $[3, G, K]$ to the class of $H = h^3$ in $\mathrm{Ort}(\mathbb{Q}\mathbb{Z}_3)$ modulo the subgroup of third powers, $(\mathrm{Ort}(\mathbb{Q}\mathbb{Z}_3))^3$. It is well defined: if $(3,G,K)$ and $(3,G',K')$ represent the same class of $\tau(\mathbb{Q})$ then, by (iii) of the proof of Theorem 7, $\Gamma' - \Gamma = 3\Delta$ for some $\Delta \in V$, that is $\gamma' - \gamma = \Delta$ and $h'' = h'h^{-1} = h''_o + h''_1\sigma + h''_2\sigma^2$ with $h''_j = \frac{2\cos(\Delta + j\frac{2\pi}{3})}{3} \in \mathbb{Q}$, $j = 0,1,2$, that is $h' = hh''$ with $h'' \in \mathrm{Ort}(\mathbb{Q}\mathbb{Z}_3)$. Thus, we have $h'^3 \equiv h^3 (\mathrm{mod}\ (\mathrm{Ort}(\mathbb{Q}\mathbb{Z}_3))^3)$.

The mapping is injective: if starting with $(3,G,K)$ we obtain $h^3 \in (\mathrm{Ort}(\mathbb{Q}\mathbb{Z}_3))^3$ then, in virtue of Lemma 9, h is in $\mathrm{Ort}(\mathbb{Q}\mathbb{Z}_3)$ modulo third roots of unity in $\mathbb{R}\mathbb{Z}_3$, which are σ^j and σ^j is also in $\mathrm{Ort}(\mathbb{Q}\mathbb{Z}_3)$. But $h \in \mathrm{Ort}(\mathbb{Q}\mathbb{Z}_3)$ means that $\cos\gamma_j \in \mathbb{Q}$ for $j = 0,1,2$, that is, $\gamma \in V$, so that $3\gamma = \Gamma \in 3V$ and $(3,G,K)$ is trivial.

The mapping is surjective: if $r + s\sigma + t\sigma^2 \in \mathrm{Ort}(\mathbb{Q}\mathbb{Z}_3)$, take the triple $(3, 3r-1, 9(t-s))$. First, verify that it satisfies $K^2 = 2^2 3^3 - 3^3 G^2$ (and it is guaranteed by the orthogonality relations for $r + s\sigma + t\sigma^2$) and then verify that the triple is sent to $h^3 = r + s\sigma + t\sigma^2$, the desired image. ∎

The last part of the proof shows that (9) can be rewritten

must have $n + 3m \notin \mathbb{Q}^2$, too, and $n - m = 2x^2$, $n + 3m = 2y^2$ for some $x, y \in \mathbb{Z}$. But $y - x \equiv y + x \pmod 2$ and $2(y - x)(y + x) = 2y^2 - 2x^2 = 4m$, implying that both $y - x$ and $y + x$ are pair and, consequently, m is pair, the contradiction. ∎

The parametrization announced in the title of the section appears in the formulation of our next result.

LEMMA 12. The formulas

$$(12) \qquad \begin{cases} r = \dfrac{A^2 - AB}{A^2 - AB + B^2} \\ s = \dfrac{AB}{A^2 - AB + B^2} \\ t = \dfrac{-AB + B^2}{A^2 - AB + B^2} \end{cases}$$

describe the group isomorphism

$$\psi : L \to \mathrm{Ort}_1(\mathbb{Q}\mathbb{Z}_3) : [A + B\omega] \mapsto r + s\sigma + t\sigma^2,$$

where $\mathrm{Ort}_1(\mathbb{Q}\mathbb{Z}_3) = \{r + s\sigma + t\sigma^2 \in \mathrm{Ort}(\mathbb{Q}\mathbb{Z}_3) : r + s + t = 1\}$.

PROOF. Consider the group homomorphism

$$\varphi : \mathrm{Ort}_1(\mathbb{Q}\mathbb{Z}_3) \to GL(2,\mathbb{Q}) : \sigma \mapsto \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

It is the restriction of the classical ring homomorphism $\mathbb{R}\mathbb{Z}_3 \to L(2,\mathbb{R})$ induced by the image of σ defined as above. For $v = r + s\sigma + t\sigma^2 \in \mathrm{Ort}_1(\mathbb{Q}\mathbb{Z}_3)$ we have

$$\varphi(v) = \begin{pmatrix} r - t & -(s - t) \\ s - t & r - s \end{pmatrix}.$$

Orthogonality relations yield $\det(\varphi(v)) = 1$ and we get the characterization of $\mathrm{Im}\varphi$:

$M \in \mathrm{Im}\varphi$ iff $M = \begin{pmatrix} x & -(x-y) \\ x-y & y \end{pmatrix}$ for some $x, y \in \mathbb{Q}$ with $x^2 - xy + y^2 = 1$.

The equation $\varphi(v) = I_2$ brings readily $v = 1$, so that $\mathrm{Ort}_1(\mathbb{Q}\mathbb{Z}_3)$ is isomorphic to $\mathrm{Im}\,\varphi$.

Next, define the auxiliary monomorphism

$$\lambda : \mathbb{Z}[\omega]^* \to GL(2,\mathbb{Q}) : \omega \mapsto \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},$$

which is the matrix notation of multiplication of complex numbers using the basis $\{1,\omega\}$, and employ it to define

$$\eta : L \to \mathrm{Im}\,\varphi : [z] \mapsto \lambda(z)(\lambda(\bar{z}))^{-1}.$$

Note that $\lambda(\bar{z}) = \det(\lambda(z))(\lambda(z))^{-1}$, so that $\eta([z]) = \frac{1}{\det(\lambda(z))}(\lambda(z))^2$, which is clearly a well-defined homomorphism. Its explicit expression is

$$\eta([A + B\omega]) = \frac{1}{A^2 - AB + B^2} \begin{pmatrix} A^2 - B^2 & -(2AB - B^2) \\ 2AB - B^2 & A^2 - 2AB \end{pmatrix}.$$

If $\eta([\dot{z}]) = I_2$ then direct calculation forces $B = 0$, that is $z \in \mathbb{Z}$ or $[z] = 1 \in L$ and η is injective. Put $\psi = \varphi^{-1} \circ \eta$. We compare $\varphi(v)$ and $\eta([z])$ using two relations: $\mathrm{Tr}\varphi(v) = 3r - 1$ and $r + s + t = 1$. Hence, we obtain the formulas (12).

To show surjectivity of ψ we use Lemma 11. We take $v = r + s\sigma + t\sigma^2 \in \mathrm{Ort}_1(\mathbb{Q}\mathbb{Z}_3)$ and want to exhibit $z \in \mathbb{Z}[\omega]^*$ such that $\psi([z]) = v$. Put $r = \frac{m}{n}$ with $m, n \in \mathbb{Z}$, $\gcd(m,n) = 1$. By Lemma 11, there exist $B, C \in \mathbb{Z}$ such that $n - m = B^2$ and $n + 3m = C^2$. This gives $n = \frac{C^2 + 3B^2}{4}$ and as $B \equiv C \pmod 2$ we may put $A = \frac{B - C}{2} \in \mathbb{Z}$. Then $n = A^2 - AB + B^2$. By (11),

$K^2 = \frac{3^4B^2C^2}{n^2} = \left(\frac{9B(B-2A)}{A^2-AB+B^2}\right)^2$. Substituting $G = \frac{2A^2-2AB-B^2}{A^2-AB+B^2}$ and $K = 9\frac{B^2-2AB}{A^2-AB+B^2}$ in (10) we receive once more the formulas (12), so that we found the desired $z = A + B\omega$, and this completes the proof of the lemma. ∎

PROOF OF THEOREM 8. Note that $\{\pm 1\} \subset (\mathrm{Ort}(\mathbb{QZ}_3))^3$ and also that $\mathrm{Ort}(\mathbb{QZ}_3)/\{\pm 1\} \cong \mathrm{Ort}_1(\mathbb{QZ}_3)$. Therefore $\mathrm{Ort}_1(\mathbb{QZ}_3)/(\mathrm{Ort}_1(\mathbb{QZ}_3))^3 \cong \cong \mathrm{Ort}(\mathbb{QZ}_3)/\mathrm{Ort}(\mathbb{QZ}_3)^3$ and, consequently, the conjunction of Lemma 10 and Lemma 12 gives $L/L^3 \cong \tau(\mathbb{Q})$. ∎

§ 4. FINAL REMARKS

1) If we return to Theorem 4 and put $(b,c,d) = (3,3r-1,9(t-s))$, the automorphism $\sigma(x)$ will take the form

$$\sigma(x) = \frac{1}{t-s}(x^2 + (s-r)x - 2).$$

It should be noted, however, that the automorphism described by this formula permutates the roots g_j of the equation $f(X) = 0$ in a way that may be visualized as being induced by the clockwise permutation of the angles γ_j, so that the automorphism which appears implicitly in §2 and §3 and sends g_o to g_1 is, actually, equal to σ^2.

2) Let $G = 2\cos\Gamma$, $\Gamma \in V$ and write G in terms of B, C rather than using A, B (this change of coefficients expresses the diagonalization of the form $X^2 - XY + Y^2$ over $\mathbb{Q}$). We get $G = 2\frac{C^2-3B^2}{C^2+3B^2}$. Excluding the case of $C = 0$ which gives $G = -2$ and $\Gamma = \pi$ we may write

$$\cos\Gamma = \frac{1-(\sqrt{3}\frac{B}{C})^2}{1+(\sqrt{3}\frac{B}{C})^2}.$$

If the diagonalization of the form is applied to $A + B\omega$ (and then it is called "the passage to Cartesian coordinates") we get $z = A + B\omega = \frac{2A - B}{2} + \frac{\sqrt{3}\,B}{2} i = \frac{1}{2}(-C + \sqrt{3}\,Bi)$ and the ratio $[\sqrt{3}B : -C]$ represents $[z]$ of the projective line L. With an understandable abuse of the language, for $C \neq 0$ we may treat $[z] \in L$ as the angle $\Delta \in (-\frac{\pi}{2}, \frac{\pi}{2})$ such that $\tan\Delta = -\frac{\sqrt{3}\,B}{C}$. For $C = 0$ define $\Delta = \frac{\pi}{2}$. Recalling the formula $\cos 2\alpha = \frac{1 - \tan^2\alpha}{1 + \tan^2\alpha}$, we see that $\Gamma = 2\Delta$ (including the case $C = 0$). This formula expresses the isomorphism $L \to V : \Delta \mapsto 2\Delta$; the lack of rigour in permitting to talk of "angles" of L is compensated by the nice geometric interpretation of V.

3) Looking for generators of $\tau(\mathbb{Q})$ we will work in L/L^3. It will be enough to find factorization of elements in $\mathbb{Z}[\omega]$ and use it modulo third powers of the factors. The ring $\mathbb{Z}[\omega]$ is a unique factorization domain, it has 6 units $(-\omega)^j$, $j = 0, \ldots, 5$, and here is the description of its prime elements (cf. [3], Ch. XII and XV): they are $1 - \omega$ (which divides 3), rational primes q such that $q \equiv 2 \pmod 3$ and non-trivial divisor $a_p + b_p\omega$ of those rational primes p that satisfy $p \equiv 1 \pmod 3$. These divisors exist and are unique modulo the action of the group D_6 that preserves the form $X^2 - XY + Y^2$. In other words: if $\begin{pmatrix} a_p \\ b_p \end{pmatrix}$ is found, all other solutions are of the form $M\begin{pmatrix} a_p \\ b_p \end{pmatrix}$, where M is in the matrix group isomorphic to D_6 and generated by $\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}$. The element $1 - \omega$ has only 6 associates because $\overline{1 - \omega} = (-\omega^2)(1 - \omega)$.

Note that the set of 12 divisors of p in $\mathbb{Z}[\omega]$ breaks into

6 pairs of opposite numbers, that is, it forms 6 elements in L. One sees easily that they may be described as $[z]$, $[\omega z]$, $[\omega^2 z]$ and their inverses. On the other hand, $9\omega^2 = (1-\omega)^4$, that is $[\omega^2] = [(1-\omega)^4] \in L$ and $[\omega^2] \equiv [1-\omega] \pmod{L^3}$. Note also that a rational prime $q \in \mathbb{Z}[\omega]$ gives $[q] = [1]$ in L. Thus, we see that any class in L/L^3 can be presented using inverse elements and products of classes corresponding to divisors $a_p + b_p\omega$ of rational primes p with $p \equiv 1 \pmod 3$, one factor for each p, and of the class arising from ω.

This set of generators of $\tau(\mathbb{Q})$ is analogous to a natural choice of generators for $T(\mathbb{Z}_2,\mathbb{Q})$, the group of classes of quadratic extensions of $\mathbb{Q}$. As any quadratic extension is of the form $\mathbb{Q}[X]/(f)$, $f(X) = X^2 - n$; one may stay with a square-free n and then the factorization $n = (-1)^{\varepsilon} p_1 \dots p_k$, $\varepsilon = \pm 1$, $p_1,\dots,p_k \in P$, leads to the set of generators indexed by elements of the set $\{i\} \cup P$.

4) In 1770 Euler presented his description of objects which we call nowadays the rational orthogonal matrices of degree 3. If we use the notation with indexed variables h_u his result is stated as follows (cf. [2], p. 309): if $h_o,h_1,h_2,h_3 \in \mathbb{Z}$ and $\sum_{u=0}^{3} h_u = \ell$, then the matrix

$$\frac{1}{\ell}\begin{pmatrix} h_o^2+h_1^2-h_2^2-h_3^2 & 2(h_1h_2+h_oh_3) & 2(h_1h_3-h_oh_2) \\ 2(h_1h_2-h_oh_3) & h_o^2-h_1^2+h_2^2-h_3^2 & 2(h_2h_3+h_oh_1) \\ 2(h_1h_3+h_oh_2) & 2(h_2h_3-h_oh_1) & h_o^2-h_1^2-h_2^2+h_3^2 \end{pmatrix}$$ is in

$S\mathcal{O}(3,\mathbb{Q})$. We encounter here the elements of $S\mathcal{O}(3,\mathbb{Q})$, called "orthogonal circulants", of the form

$$\begin{pmatrix} r & t & s \\ s & r & t \\ t & s & r \end{pmatrix},$$

as images of elements of $\mathrm{Ort}(\mathbb{Q}\mathbb{Z}_3)$ under the natural 3-dimensional representation of $U(\mathbb{R}\mathbb{Z}_3)$. Before expressing r, s, t in terms of h_u's note that the Euler's parametrization, although obtained by solution of Diophantine equations, today is retold in classes of linear algebra as follows: take the algebra $\mathbb{H}$ of real quaternions, $\mathbb{H} = \{h_o + h_1 i + h_2 j + h_3 k : h_o, h_1, h_2, h_3 \in \mathbb{R}\}$. Considering the conjugation by a unit quaternion $h \in S^3$, $w \to h^{-1}wh$, as the orthogonal transformation of $\mathbb{R}^3 = \{xi + yj + zk : x,y,z \in \mathbb{R}\}$ and writing it in the matrix form in the basis $\{i,j,k\}$ one obtains exactly Euler's formulas. Elementary topological arguments show that the mapping $S^3 \to SO(3,\mathbb{R})$ is surjective. Moreover, one may use for conjugating $h \in \mathbb{H}\setminus\{0\}$. Then, putting $\ell = \sum_{u=0}^{3} h_u^2$ and $\tilde{h} = h_o - h_1 i - h_2 j - h_3 k$ we have $h^{-1}wh = \frac{1}{\ell}(\tilde{h}wh)$. Easy calculations show that in order to obtain the orthogonal circulant corresponding to $r + s\sigma + t\sigma^2 \in \mathrm{Ort}(\mathbb{Q}\mathbb{Z}_3)$ with $r = \frac{C^2 - B^2}{4n}$, $s = 2\frac{B^2 - BC}{4n}$, $t = 2\frac{B^2 + BC}{4n}$, $4n = C^2 + 3B^2$ we may use $h = C + B(i + j + k)$ and then we have $\ell = 4n$.

5) If we want to represent the trivial element of $\tau(\mathbb{Q})$ by a triple of the form $(3,G,K)$, the triple $(3,2,0)$ is not good as the underlying polynomial is not separable. The representative with the smallest possible denominator of G and K is obtained from $(3 + \omega)^3 = 19 + 18\omega$ and then $G = \frac{-286}{7^3}$, $K = \frac{-3240}{7^3}$.