LMD mokslo darbai, III tomas, 81–85

Cubic Legendre symbol

Hamletas MARKŠAITIS (VU)
e-mail: hamletas.marksaitis@maf.vu.lt

Introduction and notations

Let ζ_n be the primitive root of nth order of unity, e. g., $\zeta_n = \exp(2\pi\sqrt{-1}/n)$. We shall denote by $\langle g \rangle$ a cyclic group generated by g. Let $\langle s \rangle$ be the Galois group of the extension $\mathbb{Q}(\zeta_9)/\mathbb{Q}$. Let us assume that

$$\zeta_9^s = \zeta_9^2.$$

Let p be a rational prime such that

$$p \equiv 1 (\mathrm{mod}\ 9), \quad p \not\equiv 1 (\mathrm{mod}\ 27).$$

The prime p splits completely in the extension $\mathbb{Q}(\zeta_9)/\mathbb{Q}$. We can write

$$p = \mathrm{Nm}_{\mathbf{Q}(\zeta_9)/\mathbf{Q}}\pi = \prod_{j=1}^{6} \pi^{s^j},$$

where π is a prime number of $\mathbb{Q}(\zeta_9)$, because the class number of the field $\mathbb{Q}(\zeta_9)$ is equal 1.

Let $K_l(q)$ denote the subfield of $\mathbb{Q}(\zeta_q)$ of degree l over rational mumber field $\mathbb{Q}$. $K_3(p) \cdot K_3(9)$ denote compositum of the fields $K_3(p)$ and $K_3(9)$, where

$$p \equiv 1 (\mathrm{mod}\ 9), \quad p \not\equiv 1 (\mathrm{mod}\ 27).$$

The Galois group $G(K_3(p) \cdot K_3(9)/\mathbb{Q})$ of the extension $K_3(p) \cdot K_3(9)/\mathbb{Q}$ is isomorphic to direct product [1]

$$\langle \bar{\sigma} \rangle \times \langle \bar{\tau} \rangle, \quad \bar{\sigma}^3 = \bar{\tau}^3 = 1,$$

of the cyclic groups $\langle \bar{\sigma} \rangle$ and $\langle \bar{\tau} \rangle$. Let us assume that $\bar{\tau} = s^2$.

Let G be a group presented by generators σ, τ and relations

$$\sigma^3 = \tau^3 = z^3 = [\tau, z] = [\sigma, z] = 1,$$

where

$$z = [\tau, \sigma] = \tau\sigma\tau^{-1}\sigma^{-1}$$

is the commutator of τ and σ. There exists the group homomorphism

$$G \xrightarrow{f} \langle\bar{\sigma}\rangle \times \langle\bar{\tau}\rangle, \sigma \mapsto \bar{\sigma}, \quad \tau \mapsto \bar{\tau}.$$

Therefore, we have the exact sequence of groups

$$1 \to \langle z\rangle \to G \to G(K_3(p) \cdot K_3(9)/\mathbb{Q}) \to 1,$$

i. e. the central extension of the Galois group $G(K_3(p) \cdot K_3(9)/\mathbb{Q})$ by a cyclic group $\langle z\rangle$ of order 3. Thus we can consider the embedding problem: to construct a central extension K of $K_3(p) \cdot K_3(9)$ with the Galois group G such that the restriction of the action of G to the subfield $K_3(p) \cdot K_3(9)$ would coincide with f. We will also require that the central extension K of $K_3(p) \cdot K_3(9)$ would be ramified at the points p, 3.

The prime ideal $(\pi\pi^{s^3})$ of $K_3(9)$ is a cube of some prime ideal $\bar{\mathfrak{p}}$ in $K_3(p) \cdot K_3(9)$

$$(\pi\pi^{s^3}) = \bar{\mathfrak{p}}^3,$$

because p is ramified in the field $K_3(p)$. We are interested in the significant question whether $\bar{\mathfrak{p}}$ splits completely in K or not. We will show that for primes p, satisfying conditions

$$p \equiv 1 (\mathrm{mod}\ 9), \quad p \not\equiv 1 (\mathrm{mod}\ 27),$$

the answer depends on the values of some cubic Legendre symbol.

In order to solve the embedding problem in question it is convenient instead of $K_3(p) \cdot K_3(9)/\mathbb{Q}$ to consider the field

$$K_3(p) \cdot K_3(9) \cdot \mathbb{Q}(\zeta_3) = K_3(p) \cdot \mathbb{Q}(\zeta_9).$$

The Galois group of the extension $K_3(p) \cdot \mathbb{Q}(\zeta_9)/\mathbb{Q}$ is

$$\langle\bar{\sigma}\rangle \times \langle\bar{\tau}\rangle \times \langle s^3\rangle \simeq \langle\bar{\sigma}\rangle \times \langle s\rangle, \quad \bar{\sigma}^3 = \bar{\tau}^3 = s^6 = 1.$$

Thus, instead of K we will construct $K \cdot \mathbb{Q}(\zeta_3)$. The Galois group $G(K \cdot \mathbb{Q}(\zeta_3)/\mathbb{Q})$ is direct product $G \times \langle s^3\rangle$. In that case we have exact sequence of the groups

$$1 \to \langle z\rangle \to G \times \langle s^3\rangle \xrightarrow{f \times \mathrm{id}} G(K_3(p) \cdot K_3(9)/\mathbb{Q}) \times \langle s^3\rangle \to 1.$$

Thus we must construct explicitly the extension $K \cdot \mathbb{Q}(\zeta_3)$ of $K_3(p) \cdot \mathbb{Q}(\zeta_9)/\mathbb{Q}$ with the Galois group $G(K \cdot \mathbb{Q}(\zeta_3)/\mathbb{Q})$ isomorphic to $G \times \langle s^3 \rangle$ and ramified only at points p and 3. The decomposition of the prime p by product of prime divisors in $K_3(p) \cdot \mathbb{Q}(\zeta_9)$ is

$$(p) = (\prod_{j=1}^{6} \mathfrak{p}^{s^j})^3.$$

Now the above question is equivalent to one whether $\mathfrak{p}$ splits completely in $K \cdot \mathbb{Q}(\zeta_3)$ or not.

Construction of the field $K \cdot \mathbb{Q}(\zeta_3)$

At first we construct the compositum $K_3(p) \cdot \mathbb{Q}(\zeta_9)$ by adjoing the cubic root of some element of the field $\mathbb{Q}(\zeta_3)$. Let us remark that the prime 3 does not ramify in $K_3(p)$ [1], where

$$p \equiv 1 (\mathrm{mod}\ 9), \quad p \not\equiv 1 (\mathrm{mod}\ 27),$$

Let

$$p = \prod_{j=1}^{6} \pi^{s^j},$$

where π is a prime number of $\mathbb{Q}(\zeta_9)$ such that

$$\pi^{1-s+s^2-s^3+s^4-s^5} \equiv x^3 \left(\mathrm{mod}\ (1-\zeta_3)^4\right). \tag{1}$$

We claim that

$$K_3(p) \cdot \mathbb{Q}(\zeta_9) = \mathbb{Q}\left(\zeta_9, \sqrt[3]{\pi^{1-s+s^2-s^3+s^4-s^5}}\right).$$

It can be verified by simple computations. We remark that

$$\pi^{1-s+s^2-s^3+s^4-s^5} \in \mathbb{Q}(\zeta_3).$$

The condition (1) assures [2, 3] that the prime ideal $(1-\zeta_3)$ does not ramify in the extension

$$\mathbb{Q}\left(\zeta_3, \sqrt[3]{\pi^{1-s+s^2-s^3+s^4-s^5}}\right)/\mathbb{Q}(\zeta_3).$$

Also the prime ideal $(1-\zeta_9)$ does not ramify in the extension

$$\mathbb{Q}\left(\zeta_9, \sqrt[3]{\pi^{1-s+s^2-s^3+s^4-s^5}}\right)/\mathbb{Q}(\zeta_9).$$

We claim that

$$K \cdot \mathbb{Q}(\zeta_3) = \mathbb{Q}\left(\zeta_9, \sqrt[3]{\pi^{1-s+s^2-s^3+s^4-s^5}}, \sqrt[3]{\pi^{s+s^2-s^4-s^5}}\right).$$

It can be verified by simple computations.

Let

$$\alpha = \pi^{1-s+s^2-s^3+s^4-s^5},$$
$$\mu = \pi^{s+s^2-s^4-s^5}.$$

The Galois group G elements act on the elements $\sqrt[3]{\alpha}$, $\sqrt[3]{\mu}$ of the field $K \cdot \mathbb{Q}(\zeta_3)$ in the folowing way:

$$\zeta^s = \zeta^2, \qquad \sqrt[3]{\mu}^s = \xi_s \sqrt[3]{\mu}^2,$$
$$\sqrt[3]{\alpha}^\sigma = \zeta_3 \sqrt[3]{\alpha}, \qquad \sqrt[3]{\mu}^\sigma = \sqrt[3]{\mu},$$
$$\sqrt[3]{\alpha}^\tau = \xi_\tau \sqrt[3]{\alpha}, \qquad \sqrt[3]{\mu}^z = \zeta_3 \sqrt[3]{\mu}.$$

It easy to find the elements ξ_s and ξ_τ.

In order to give the answer to the above question let us remind the definition of cubic Legendre symbol [2]. Let k be a field such that $\zeta_3 \in k$. Let $\alpha \in k$, $\mathfrak{p}$ be prime unramified ideal of k, $\mathfrak{p} \nmid \alpha$. Then we can write

$$\alpha^{\frac{\mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{p}-1}{3}} \equiv \zeta_3^a \pmod{\mathfrak{p}}$$

for some $a \pmod 3$, $a \in \mathbb{Z}$. Because $\mathfrak{p}$ is unramified in k, the roots of 3th order of unity 1, ζ_3 and ζ_3^2 belong to different classes mod $\mathfrak{p}$. By definition

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_3 = \zeta_3^a.$$

It is obvious, that

$$\left(\frac{\alpha\beta}{\mathfrak{p}}\right)_3 = \left(\frac{\alpha}{\mathfrak{p}}\right)_3 \left(\frac{\beta}{\mathfrak{p}}\right)_3,$$

where $\mathfrak{p} \nmid \alpha, \mathfrak{p} \nmid \beta$.

Cubic Legendre symbol as the denominator function is extended multiplicatively.

Let the prime ideal $\mathfrak{p}$ of $K_3(p) \cdot \mathbb{Q}(\zeta_9)$ divides π. The prime ideal $\mathfrak{p}$ splits in $K \cdot \mathbb{Q}(\zeta_3)$ if and only if the cubic Legendre symbol

$$\left(\frac{\pi^{s+s^2-s^4-s^5}}{\pi}\right)_3 = 1.$$

The computations for primes p satisfying conditions

$$p \equiv 1 (\mathrm{mod}\ 9), \quad p \not\equiv 1 (\mathrm{mod}\ 27), \quad p < 200,$$

show that

$$\left(\frac{\pi^{s+s^2-s^4-s^5}}{\pi}\right)_3 \neq 1.$$

In general the question of finding the values of cubic Legendre symbol

$$\left(\frac{\pi^{s+s^2-s^4-s^5}}{\pi}\right)_3,$$

for prime elements π of $\mathbb{Q}(\zeta_9)$, $\pi | p$,

$$p \equiv 1 (\mathrm{mod}\ 9), \quad p \not\equiv 1 (\mathrm{mod}\ 27),$$

is very important and the answer to this question is not known.

References

[1] E. Artin, J. Tate, *Class Field Theory*, Harvard (1961).

[2] H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, I, Jahresbericht der Deutschen Mathematiker – Vereinigung, Leipzig und Berlin, **35**, 1–55 (1926).

[3] H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Ia, Jahresbericht der Deutschen Mathematiker – Vereinigung, Leipzig und Berlin, **36**, 233–311 (1926).

Kubinis Ležandro simbolis

H. Markšaitis

Nagrinėjamos kubinio Ležandro simbolio rekšmės, priklausančios nuo specialių skaičių. Šie skaičiai susiję su tam tikrais racionaliųjų skaičių kūno plėtiniais. Kubinio Ležandro simbolio reikšmės svarbios sprendžiant kai kuriuos Galua teorijos uždavinius.