

# On metacyclic extensions

Masanari Kida

University of Electro-Communications

September 9, 2008

# Introduction

## Brumer's quintic polynomial

$$\text{Bru}(a, b; X) = X^5 + (-3 + a)X^4 + (3 + b - a)X^3 + (-1 - a - 2b + a^2)X^2 + bX + a \in \mathbb{Q}(a, b)[X].$$

$\text{Bru}(a, b; X)$  is a generic  $D_5$ -polynomial over  $\mathbb{Q}$ .

$$\text{disc}(\text{Bru}(a, b; X)) = a^2 d(a, b)^2$$

$$d(a, b) = -4b^3 - (-a^2 + 30a - 1)b^2 - (-24a^3 + 34a^2 + 14a)b - (4a^5 - 4a^4 - 40a^3 + 91a^2 - 4a).$$

# Introduction

Brumer's quintic polynomial

$$\text{Bru}(a, b; X) = X^5 + (-3 + a)X^4 + (3 + b - a)X^3 + (-1 - a - 2b + a^2)X^2 + bX + a \in \mathbb{Q}(a, b)[X].$$

$\text{Bru}(a, b; X)$  is a generic  $D_5$ -polynomial over  $\mathbb{Q}$ .

$$\text{disc}(\text{Bru}(a, b; X)) = a^2 d(a, b)^2$$

$$d(a, b) = -4b^3 - (-a^2 + 30a - 1)b^2 - (-24a^3 + 34a^2 + 14a)b - (4a^5 - 4a^4 - 40a^3 + 91a^2 - 4a).$$

Brumer's quintic polynomial

$$\text{Bru}(a, b; X) = X^5 + (-3 + a)X^4 + (3 + b - a)X^3 + (-1 - a - 2b + a^2)X^2 + bX + a \in \mathbb{Q}(a, b)[X].$$

$\text{Bru}(a, b; X)$  is a generic  $D_5$ -polynomial over  $\mathbb{Q}$ .

$$\text{disc}(\text{Bru}(a, b; X)) = a^2 d(a, b)^2$$

$$d(a, b) = -4b^3 - (-a^2 + 30a - 1)b^2 - (-24a^3 + 34a^2 + 14a)b - (4a^5 - 4a^4 - 40a^3 + 91a^2 - 4a).$$

# Kida-Rikuna-Sato construction (I)

Consider an elliptic curve

$$E_a^* : y^2 + (1 - a)xy - ay = x^3 - ax^2.$$

$(0, 0)$  is a rational point of order 5. Setting

$$E_a = E_a^* / \langle (0, 0) \rangle,$$

we have an isogeny

$$\lambda^* : E_a^* \longrightarrow E_a$$

and an injective homomorphism

$$E_a(k) / \lambda^* E_a(k) \hookrightarrow \text{Hom}_{\text{cont}}(\text{Gal}(\bar{k}/k), \ker \lambda^*(\mathbb{Q}))$$

for any field extension  $k$  over  $\mathbb{Q}$ .

It follows that each point of  $E_a(k)$  defines a quintic cyclic extension over  $k$ .

# Kida-Rikuna-Sato construction (I)

Consider an elliptic curve

$$E_a^* : y^2 + (1 - a)xy - ay = x^3 - ax^2.$$

$(0, 0)$  is a rational point of order 5. Setting

$$E_a = E_a^* / \langle (0, 0) \rangle,$$

we have an isogeny

$$\lambda^* : E_a^* \longrightarrow E_a$$

and an injective homomorphism

$$E_a(k) / \lambda^* E_a(k) \hookrightarrow \text{Hom}_{\text{cont}}(\text{Gal}(\bar{k}/k), \ker \lambda^*(\mathbb{Q}))$$

for any field extension  $k$  over  $\mathbb{Q}$ .

It follows that each point of  $E_a(k)$  defines a quintic cyclic extension over  $k$ .

# Kida-Rikuna-Sato construction (I)

Consider an elliptic curve

$$E_a^* : y^2 + (1 - a)xy - ay = x^3 - ax^2.$$

$(0, 0)$  is a rational point of order 5. Setting

$$E_a = E_a^* / \langle (0, 0) \rangle,$$

we have an isogeny

$$\lambda^* : E_a^* \longrightarrow E_a$$

and an injective homomorphism

$$E_a(k) / \lambda^* E_a(k) \hookrightarrow \text{Hom}_{\text{cont}}(\text{Gal}(\bar{k}/k), \ker \lambda^*(\mathbb{Q}))$$

for any field extension  $k$  over  $\mathbb{Q}$ .

It follows that each point of  $E_a(k)$  defines a quintic cyclic extension over  $k$ .

# Kida-Rikuna-Sato construction (II)

## Theorem

Let  $E_{a,b}$  be a quadratic twist of  $E_a$  associated to  $k = \mathbb{Q}(\sqrt{d(a,b)})/\mathbb{Q}$ . Define  $E_{a,b}^*$  so that the following diagram is commutative.

$$\begin{array}{ccc} E_{a,b}^* & \xrightarrow{f^*} & E_a^* \\ \phi^* \downarrow & & \downarrow \lambda^* \\ E_{a,b} & \xrightarrow{f} & E_a \end{array}$$

Then there exists an injective homomorphism

$$\varphi : E_{a,b}(\mathbb{Q})/\phi^*(E_{a,b}^*(\mathbb{Q})) \hookrightarrow \text{Hom}_{\text{cont}}(\text{Gal}(\bar{k}/k), \ker \lambda^*(\mathbb{Q}))$$

and the image of  $\varphi$  correspond to  $D_5$ -extensions over  $\mathbb{Q}$  containing  $k$  defined by  $\text{Bru}(a, \beta; X)$  with some  $\beta$ .

# Strong and weak points

- The splitting field of  $\text{Bru}(a, \beta; X)$  is a 'Kummer extension' associated to the elliptic curves. This enables us to deduce various information on the polynomial and its splitting field.
- The group of the parameter is finite.
- We do not know how to control  $a$  to get all  $D_5$ -extensions over  $\mathbb{Q}$ .
- Other non-abelian extensions such as  $D_7$  and  $F_{20}$ -extensions can be constructed by this method.
- The degrees of elliptic curve isogenies are limited. Moreover We do not know whether the obtained polynomials are generic or not.

# Strong and weak points

- The splitting field of  $\text{Bru}(a, \beta; X)$  is a 'Kummer extension' associated to the elliptic curves. This enables us to deduce various information on the polynomial and its splitting field.
- The group of the parameter is finite.
- We do not know how to control  $a$  to get all  $D_5$ -extensions over  $\mathbb{Q}$ .
- Other non-abelian extensions such as  $D_7$  and  $F_{20}$ -extensions can be constructed by this method.
- The degrees of elliptic curve isogenies are limited. Moreover We do not know whether the obtained polynomials are generic or not.

# Strong and weak points

- The splitting field of  $\text{Bru}(a, \beta; X)$  is a 'Kummer extension' associated to the elliptic curves. This enables us to deduce various information on the polynomial and its splitting field.
- The group of the parameter is finite.
- We do not know how to control  $a$  to get all  $D_5$ -extensions over  $\mathbb{Q}$ .
- Other non-abelian extensions such as  $D_7$  and  $F_{20}$ -extensions can be constructed by this method.
- The degrees of elliptic curve isogenies are limited. Moreover We do not know whether the obtained polynomials are generic or not.

# Strong and weak points

- The splitting field of  $\text{Bru}(a, \beta; X)$  is a 'Kummer extension' associated to the elliptic curves. This enables us to deduce various information on the polynomial and its splitting field.
- The group of the parameter is finite.
- We do not know how to control  $a$  to get all  $D_5$ -extensions over  $\mathbb{Q}$ .
- Other non-abelian extensions such as  $D_7$  and  $F_{20}$ -extensions can be constructed by this method.
- The degrees of elliptic curve isogenies are limited. Moreover We do not know whether the obtained polynomials are generic or not.

# Strong and weak points

- The splitting field of  $\text{Bru}(a, \beta; X)$  is a 'Kummer extension' associated to the elliptic curves. This enables us to deduce various information on the polynomial and its splitting field.
- The group of the parameter is finite.
- We do not know how to control  $a$  to get all  $D_5$ -extensions over  $\mathbb{Q}$ .
- Other non-abelian extensions such as  $D_7$  and  $F_{20}$ -extensions can be constructed by this method.
- The degrees of elliptic curve isogenies are limited. Moreover We do not know whether the obtained polynomials are generic or not.

# Aim of this talk

Using a Kummer theory arising from algebraic tori, we construct Galois extensions with metacyclic Galois groups.

Preceding research:

Kishi-Imaoka: “Galois theory and modular forms”, 2004

Sase-Nakano: Tokyo J. Math., 2002

# Aim of this talk

Using a Kummer theory arising from algebraic tori, we construct Galois extensions with metacyclic Galois groups.

Preceding research:

Kishi-Imaoka: “Galois theory and modular forms”, 2004

Sase-Nakano: Tokyo J. Math., 2002

# More geometric viewpoint

There is an isogeny

$$R_{k/\mathbb{Q}}(E_a \times k) \sim E_a \times E_{a,b}$$

defined over  $\mathbb{Q}$  whose degree is a power of 2. (Milne, A. Sato, Kida,...)

On the groups of  $\mathbb{Q}$ -rational points we have a map

$$E_a(\mathbb{Q}) \times E_{a,b}(\mathbb{Q}) \longrightarrow R_{k/\mathbb{Q}}(E_a \times k)(\mathbb{Q}) = E_a(k)$$

up to 2-power torsion.

Moving to the quotients, we have an injection

$$E_{a,b}(\mathbb{Q})/\phi^*(E_{a,b}^*(\mathbb{Q})) \longrightarrow E_a(k)/\lambda^*(E_a^*(k)).$$

This is the map involved in the above theorem.

# More geometric viewpoint

There is an isogeny

$$R_{k/\mathbb{Q}}(E_a \times k) \sim E_a \times E_{a,b}$$

defined over  $\mathbb{Q}$  whose degree is a power of 2. (Milne, A. Sato, Kida,...)

On the groups of  $\mathbb{Q}$ -rational points we have a map

$$E_a(\mathbb{Q}) \times E_{a,b}(\mathbb{Q}) \longrightarrow R_{k/\mathbb{Q}}(E_a \times k)(\mathbb{Q}) = E_a(k)$$

up to 2-power torsion.

Moving to the quotients, we have an injection

$$E_{a,b}(\mathbb{Q})/\phi^*(E_{a,b}^*(\mathbb{Q})) \longrightarrow E_a(k)/\lambda^*(E_a^*(k)).$$

This is the map involved in the above theorem.

# Kummer theory (I)

Let  $\ell$  be an odd prime. For a field  $F$ , we define  $F_c = F(\zeta_\ell)$ .

Let  $k$  be a field with  $\text{char}(k) \neq \ell$ . Let  $n = [k_c : k]$ .

Suppose that there exists an integer-coefficient polynomial

$$\mathcal{P}(t) = c_1 + c_2 t + \cdots + c_n t^{n-1} \in \mathbb{Z}[t]$$

of degree  $n - 1$  satisfying certain appropriate conditions. Then the circulant matrix

$$\text{circ}(c_1, c_2, \dots, c_n) = \begin{bmatrix} c_1 & c_2 & \cdots & c_n \\ c_n & c_1 & \cdots & c_{n-1} \\ \vdots & \vdots & \cdots & \vdots \\ c_2 & c_3 & \cdots & c_1 \end{bmatrix}$$

# Kummer theory (I)

Let  $\ell$  be an odd prime. For a field  $F$ , we define  $F_c = F(\zeta_\ell)$ .

Let  $k$  be a field with  $\text{char}(k) \neq \ell$ . Let  $n = [k_c : k]$ .

Suppose that there exists an integer-coefficient polynomial

$$\mathcal{P}(t) = c_1 + c_2 t + \cdots + c_n t^{n-1} \in \mathbb{Z}[t]$$

of degree  $n - 1$  satisfying certain appropriate conditions. Then the circulant matrix

$$\text{circ}(c_1, c_2, \dots, c_n) = \begin{bmatrix} c_1 & c_2 & \cdots & c_n \\ c_n & c_1 & \cdots & c_{n-1} \\ \vdots & \vdots & \cdots & \vdots \\ c_2 & c_3 & \cdots & c_1 \end{bmatrix}$$

# Kummer theory (I)

Let  $\ell$  be an odd prime. For a field  $F$ , we define  $F_c = F(\zeta_\ell)$ .

Let  $k$  be a field with  $\text{char}(k) \neq \ell$ . Let  $n = [k_c : k]$ .

Suppose that there exists an integer-coefficient polynomial

$$\mathcal{P}(t) = c_1 + c_2 t + \cdots + c_n t^{n-1} \in \mathbb{Z}[t]$$

of degree  $n - 1$  satisfying certain appropriate conditions. Then the circulant matrix

$$\text{circ}(c_1, c_2, \dots, c_n) = \begin{bmatrix} c_1 & c_2 & \cdots & c_n \\ c_n & c_1 & \cdots & c_{n-1} \\ \vdots & \vdots & \cdots & \vdots \\ c_2 & c_3 & \cdots & c_1 \end{bmatrix}$$

# Kummer theory (II)

defines an endomorphism of degree  $\ell$  on the character module of  $R_{k_c/k}\mathbb{G}_m$ . Let  $\lambda$  be the corresponding self-isogeny of  $R_{k_c/k}\mathbb{G}_m$ . We can show that the points on  $\ker \lambda$  are all  $k$ -rational. Then we have a Kummer duality

$$R_{k_c/k}\mathbb{G}_m(k)/\lambda R_{k_c/k}\mathbb{G}_m(k) \cong \text{Hom}_{\text{cont}}(\text{Gal}(\bar{k}/k), \ker \lambda(k)).$$

This implies that every cyclic extension over  $k$  of degree  $\ell$  is of the form

$$k(\lambda^{-1}(P)), \quad P \in R_{k_c/k}\mathbb{G}_m(k).$$

# Fields admitting the Kummer theory

- If  $n$  is a prime and there exists an element  $\lambda \in \mathbb{Z}[\zeta_n]$  whose norm is  $\ell$ . Then we can find  $\mathcal{P}(t)$  satisfying our assumptions.
- The case where  $n = 4$  is always OK.
- Descent to  $\mathbb{Q}$  is possible for  $(\ell, n) = (3, 2), (5, 4), (7, 6), (11, 10)$ .

# Illustration of our main theorem by an example

We consider the case where  $\ell = 3$ . Let  $k = \mathbb{Q}$ . The polynomial

$$\mathcal{P}(t) = 2 - t$$

defines an isogeny of  $R_{\mathbb{Q}_c/\mathbb{Q}}\mathbb{G}_m$  of degree 3.

Let  $F/\mathbb{Q}$  be a quadratic extension,  $F \neq \mathbb{Q}(\sqrt{-3}) \implies n = 2$ .

We have a Kummer duality

$$R_{F_c/F}\mathbb{G}_m(F)/\lambda R_{F_c/F}\mathbb{G}_m(F) \cong \text{Hom}_{\text{cont}}(\text{Gal}(\bar{F}/F), \ker \lambda(k)).$$

# Illustration of our main theorem by an example

We consider the case where  $\ell = 3$ . Let  $k = \mathbb{Q}$ . The polynomial

$$\mathcal{P}(t) = 2 - t$$

defines an isogeny of  $R_{\mathbb{Q}_c/\mathbb{Q}}\mathbb{G}_m$  of degree 3.

Let  $F/\mathbb{Q}$  be a quadratic extension,  $F \neq \mathbb{Q}(\sqrt{-3}) \implies n = 2$ .

We have a Kummer duality

$$R_{F_c/F}\mathbb{G}_m(F)/\lambda R_{F_c/F}\mathbb{G}_m(F) \cong \text{Hom}_{\text{cont}}(\text{Gal}(\bar{F}/F), \ker \lambda(k)).$$

On the other hand we have an canonical isomorphism

$$R_{F_c/F}\mathbb{G}_m(F) \cong R_{F/\mathbb{Q}}(R_{F_c/F}\mathbb{G}_m)(\mathbb{Q})$$

and an isogeny of degree 2

$$R_{F/\mathbb{Q}}(R_{F_c/F}\mathbb{G}_m) = R_{F_c/\mathbb{Q}}\mathbb{G}_m \sim R_{\mathbb{Q}_c/\mathbb{Q}}\mathbb{G}_m \times \ker(N_{F_c/\mathbb{Q}_c} : R_{F_c/\mathbb{Q}_c}\mathbb{G}_m \rightarrow R_{\mathbb{Q}_c/\mathbb{Q}}\mathbb{G}_m)$$

given by

$$x \mapsto \left( N_{F_c/\mathbb{Q}_c}(x), \frac{x^2}{N_{F_c/\mathbb{Q}_c}(x)} \right).$$

In other words,

$$\begin{aligned} \mathbb{Q}[\mathrm{Gal}(F_c/\mathbb{Q})] &\cong \mathbb{Q}[\mathrm{Gal}(F/\mathbb{Q}) = \langle \sigma \rangle] \otimes \mathbb{Q}[\mathrm{Gal}(\mathbb{Q}_c/\mathbb{Q})] \\ &\cong \left(\frac{1-\sigma}{2}\right)\mathbb{Q}[\mathrm{Gal}(F_c/\mathbb{Q})] \oplus \left(\frac{1+\sigma}{2}\right)\mathbb{Q}[\mathrm{Gal}(F_c/\mathbb{Q})]. \end{aligned}$$

On the other hand we have an canonical isomorphism

$$R_{F_c/F}\mathbb{G}_m(F) \cong R_{F/\mathbb{Q}}(R_{F_c/F}\mathbb{G}_m)(\mathbb{Q})$$

and an isogeny of degree 2

$$R_{F/\mathbb{Q}}(R_{F_c/F}\mathbb{G}_m) = R_{F_c/\mathbb{Q}}\mathbb{G}_m \sim R_{\mathbb{Q}_c/\mathbb{Q}}\mathbb{G}_m \times \ker(N_{F_c/\mathbb{Q}_c} : R_{F_c/\mathbb{Q}}\mathbb{G}_m \rightarrow R_{\mathbb{Q}_c/\mathbb{Q}}\mathbb{G}_m)$$

given by

$$x \mapsto \left( N_{F_c/\mathbb{Q}_c}(x), \frac{x^2}{N_{F_c/\mathbb{Q}_c}(x)} \right).$$

In other words,

$$\begin{aligned} \mathbb{Q}[\text{Gal}(F_c/\mathbb{Q})] &\cong \mathbb{Q}[\text{Gal}(F/\mathbb{Q}) = \langle \sigma \rangle] \otimes \mathbb{Q}[\text{Gal}(\mathbb{Q}_c/\mathbb{Q})] \\ &\cong \left(\frac{1-\sigma}{2}\right)\mathbb{Q}[\text{Gal}(F_c/\mathbb{Q})] \oplus \left(\frac{1+\sigma}{2}\right)\mathbb{Q}[\text{Gal}(F_c/\mathbb{Q})]. \end{aligned}$$

On the other hand we have an canonical isomorphism

$$R_{F_c/F}\mathbb{G}_m(F) \cong R_{F/\mathbb{Q}}(R_{F_c/F}\mathbb{G}_m)(\mathbb{Q})$$

and an isogeny of degree 2

$$R_{F/\mathbb{Q}}(R_{F_c/F}\mathbb{G}_m) = R_{F_c/\mathbb{Q}}\mathbb{G}_m \sim R_{\mathbb{Q}_c/\mathbb{Q}}\mathbb{G}_m \times \ker(N_{F_c/\mathbb{Q}_c} : R_{F_c/\mathbb{Q}_c}\mathbb{G}_m \rightarrow R_{\mathbb{Q}_c/\mathbb{Q}}\mathbb{G}_m)$$

given by

$$x \mapsto \left( N_{F_c/\mathbb{Q}_c}(x), \frac{x^2}{N_{F_c/\mathbb{Q}_c}(x)} \right).$$

In other words,

$$\begin{aligned} \mathbb{Q}[\mathrm{Gal}(F_c/\mathbb{Q})] &\cong \mathbb{Q}[\mathrm{Gal}(F/\mathbb{Q}) = \langle \sigma \rangle] \otimes \mathbb{Q}[\mathrm{Gal}(\mathbb{Q}_c/\mathbb{Q})] \\ &\cong \left(\frac{1-\sigma}{2}\right)\mathbb{Q}[\mathrm{Gal}(F_c/\mathbb{Q})] \oplus \left(\frac{1+\sigma}{2}\right)\mathbb{Q}[\mathrm{Gal}(F_c/\mathbb{Q})]. \end{aligned}$$

Let  $P \in R_{F_c/F} \mathbb{G}_m(F)$  and  $L_P = F(\lambda^{-1}(P))$ .

Then  $L_P/F$  is a cyclic extension degree 3.

Our result implies

$$P \in R_{\mathbb{Q}_c/\mathbb{Q}} \mathbb{G}_m(\mathbb{Q}) \implies L_P/\mathbb{Q} \text{ is a } C_6\text{-extension}$$

$$P \in \ker(N_{F_c/\mathbb{Q}_c})(\mathbb{Q}) \implies L_P/\mathbb{Q} \text{ is a } D_3\text{-extension}$$

Let  $T$  be either  $R_{\mathbb{Q}_c/\mathbb{Q}} \mathbb{G}_m$  or  $\ker N_{F_c/\mathbb{Q}_c}$ . Then we have an injective homomorphism

$$T(\mathbb{Q})/\lambda T(\mathbb{Q}) \hookrightarrow \text{Hom}_{\text{cont}}(\text{Gal}(\bar{F}/F), \ker \lambda(F)).$$

The image consists of all  $C_6$  (resp.  $D_3$ )-extensions over  $\mathbb{Q}$  containing  $F$ .

Let  $P \in R_{F_c/F} \mathbb{G}_m(F)$  and  $L_P = F(\lambda^{-1}(P))$ .

Then  $L_P/F$  is a cyclic extension degree 3.

Our result implies

$$P \in R_{\mathbb{Q}_c/\mathbb{Q}} \mathbb{G}_m(\mathbb{Q}) \implies L_P/\mathbb{Q} \text{ is a } C_6\text{-extension}$$

$$P \in \ker(N_{F_c/\mathbb{Q}_c})(\mathbb{Q}) \implies L_P/\mathbb{Q} \text{ is a } D_3\text{-extension}$$

Let  $T$  be either  $R_{\mathbb{Q}_c/\mathbb{Q}} \mathbb{G}_m$  or  $\ker N_{F_c/\mathbb{Q}_c}$ . Then we have an injective homomorphism

$$T(\mathbb{Q})/\lambda T(\mathbb{Q}) \hookrightarrow \text{Hom}_{\text{cont}}(\text{Gal}(\bar{F}/F), \ker \lambda(F)).$$

The image consists of all  $C_6$  (resp.  $D_3$ )-extensions over  $\mathbb{Q}$  containing  $F$ .

# Metacyclic groups (I)

A group  $G$  is **metacyclic**  $\iff G$  has a cyclic normal subgroup  $N = \langle a \rangle$  such that  $G/N$  is also cyclic.

We assume that  $\#N = \ell$  is a prime.

Then there exists a subgroup  $H = \langle b \rangle$  of  $G$  isomorphic to  $G/N$  and we have  $G = N \rtimes H$ .

$\implies \exists x \in \mathbb{F}_\ell^\times : b^{-1}ab = a^x$ .

Setting  $r = \#H$ ,  $s = \text{order}(x)$ , we define

$$M_\ell(r|s) = \langle a, b \mid a^\ell = 1, b^r = 1, b^{-1}ab = a^x, \text{ord}(x \bmod \ell) = s \rangle.$$

It is known that the isomorphism class does not depend on the choice of  $x$ .

# Metacyclic groups (I)

A group  $G$  is **metacyclic**  $\iff G$  has a cyclic normal subgroup  $N = \langle a \rangle$  such that  $G/N$  is also cyclic.

We assume that  $\#N = \ell$  is a prime.

Then there exists a subgroup  $H = \langle b \rangle$  of  $G$  isomorphic to  $G/N$  and we have  $G = N \rtimes H$ .

$\implies \exists x \in \mathbb{F}_\ell^\times : b^{-1}ab = a^x$ .

Setting  $r = \#H$ ,  $s = \text{order}(x)$ , we define

$$M_\ell(r|s) = \langle a, b \mid a^\ell = 1, b^r = 1, b^{-1}ab = a^x, \text{ord}(x \bmod \ell) = s \rangle.$$

It is known that the isomorphism class does not depend on the choice of  $x$ .

# Metacyclic groups (I)

A group  $G$  is **metacyclic**  $\iff G$  has a cyclic normal subgroup  $N = \langle a \rangle$  such that  $G/N$  is also cyclic.

We assume that  $\#N = \ell$  is a prime.

Then there exists a subgroup  $H = \langle b \rangle$  of  $G$  isomorphic to  $G/N$  and we have  $G = N \rtimes H$ .

$\implies \exists x \in \mathbb{F}_\ell^\times : b^{-1}ab = a^x$ .

Setting  $r = \#H$ ,  $s = \text{order}(x)$ , we define

$$M_\ell(r|s) = \langle a, b \mid a^\ell = 1, b^r = 1, b^{-1}ab = a^x, \text{ord}(x \bmod \ell) = s \rangle.$$

It is known that the isomorphism class does not depend on the choice of  $x$ .

# Metacyclic groups (I)

A group  $G$  is **metacyclic**  $\iff G$  has a cyclic normal subgroup  $N = \langle a \rangle$  such that  $G/N$  is also cyclic.

We assume that  $\#N = \ell$  is a prime.

Then there exists a subgroup  $H = \langle b \rangle$  of  $G$  isomorphic to  $G/N$  and we have  $G = N \rtimes H$ .

$\implies \exists x \in \mathbb{F}_\ell^\times : b^{-1}ab = a^x$ .

Setting  $r = \#H$ ,  $s = \text{order}(x)$ , we define

$$M_\ell(r|s) = \langle a, b \mid a^\ell = 1, b^r = 1, b^{-1}ab = a^x, \text{ord}(x \bmod \ell) = s \rangle.$$

It is known that the isomorphism class does not depend on the choice of  $x$ .

# Metacyclic groups (I)

A group  $G$  is **metacyclic**  $\iff G$  has a cyclic normal subgroup  $N = \langle a \rangle$  such that  $G/N$  is also cyclic.

We assume that  $\#N = \ell$  is a prime.

Then there exists a subgroup  $H = \langle b \rangle$  of  $G$  isomorphic to  $G/N$  and we have  $G = N \rtimes H$ .

$\implies \exists x \in \mathbb{F}_\ell^\times : b^{-1}ab = a^x$ .

Setting  $r = \#H$ ,  $s = \text{order}(x)$ , we define

$$M_\ell(r|s) = \langle a, b \mid a^\ell = 1, b^r = 1, b^{-1}ab = a^x, \text{ord}(x \bmod \ell) = s \rangle.$$

It is known that the isomorphism class does not depend on the choice of  $x$ .

# Metacyclic groups (II)

We have

$M_\ell(r|s)$  is abelian  $\iff s = 1$ ,

$M_\ell(r|s)$  is a Frobenius group  $F_{\ell r}$   $\iff s = r$ ,

$M_\ell(r|s)$  is a dihedral group  $D_{2\ell}$   $\iff s = r = 2$ .

Évariste Galois already noticed that if a polynomial of prime degree  $\ell$  is solvable, then the Galois group is a Frobenius group.

# Main result

Let  $k$  be a base field and assume that there exists a Kummer theory over  $k$ . Let  $F$  be a cyclic extension of degree  $d$  dividing  $\ell - 1$  such that  $F \cap k_c = k$ . Then the Kummer theory over  $k$  lifts to  $F$ :

$$R_{F_c/F} \mathbb{G}_m(F) / \lambda R_{F_c/F} \mathbb{G}_m(F) \cong \text{Hom}_{\text{cont}}(\text{Gal}(\bar{F}/F), \ker \lambda(F)).$$

We consider  $R_{F/k}(R_{F_c/F} \mathbb{G}_m) = R_{F_c/k} \mathbb{G}_m$  and decompose the right hand side up to isogeny.

Note that

$$\text{Gal}(F_c/k) \cong \text{Gal}(F/k) \times \text{Gal}(F_c/F) = \langle \sigma \rangle \times \langle \tau \rangle.$$

According to the decomposition

$$\mathbb{Q}[\text{Gal}(F/k)] \cong \mathbb{Q}[x]/(x^d - 1) \cong \bigoplus_{s|d} \mathbb{Q}[x]/(\Phi_s(x))$$

with cyclotomic polynomials  $\Phi_s(x)$ , we have a decomposition

$$\mathbb{Q}[\text{Gal}(F_c/k)] = \mathbb{Q}[\text{Gal}(F/k)] \otimes \mathbb{Q}[\text{Gal}(F_c/F)] = \bigoplus_{s|d} \mathbb{Q}(s).$$

Note that

$$\mathrm{Gal}(F_c/k) \cong \mathrm{Gal}(F/k) \times \mathrm{Gal}(F_c/F) = \langle \sigma \rangle \times \langle \tau \rangle.$$

According to the decomposition

$$\mathbb{Q}[\mathrm{Gal}(F/k)] \cong \mathbb{Q}[x]/(x^d - 1) \cong \bigoplus_{s|d} \mathbb{Q}[x]/(\Phi_s(x))$$

with cyclotomic polynomials  $\Phi_s(x)$ , we have a decomposition

$$\mathbb{Q}[\mathrm{Gal}(F_c/k)] = \mathbb{Q}[\mathrm{Gal}(F/k)] \otimes \mathbb{Q}[\mathrm{Gal}(F_c/F)] = \bigoplus_{s|d} \mathbb{Q}(s).$$

Note that

$$\mathrm{Gal}(F_c/k) \cong \mathrm{Gal}(F/k) \times \mathrm{Gal}(F_c/F) = \langle \sigma \rangle \times \langle \tau \rangle.$$

According to the decomposition

$$\mathbb{Q}[\mathrm{Gal}(F/k)] \cong \mathbb{Q}[x]/(x^d - 1) \cong \bigoplus_{s|d} \mathbb{Q}[x]/(\Phi_s(x))$$

with cyclotomic polynomials  $\Phi_s(x)$ , we have a decomposition

$$\mathbb{Q}[\mathrm{Gal}(F_c/k)] = \mathbb{Q}[\mathrm{Gal}(F/k)] \otimes \mathbb{Q}[\mathrm{Gal}(F_c/F)] = \bigoplus_{s|d} \mathbb{Q}(s).$$

Let  $T(s)$  be an algebraic torus corresponding to  $\mathbb{Q}(s)$  (determined up to isogeny). Then we have an isogeny

$$R_{F/k}(R_{F_c/F}\mathbb{G}_m) \sim \prod_{s|d} T(s)$$

of degree dividing a power of  $d$ . In particular, the degree is prime to  $\ell$ .

## Theorem

*If  $P \in T(s)(k)$ , then the field  $L_P$  corresponding to  $P$  by the Kummer duality is an  $M_\ell(d|s)$ -extension over  $k$  containing  $F$  if it is Galois over  $k$ . Moreover we have an injective homomorphism*

$$e_j(T(s)(k)/\lambda T(s)(k)) \longrightarrow \text{Hom}_{\text{cont}}(\text{Gal}(\bar{F}/F), \ker \lambda(F))$$

*where  $e_j$  is a certain idempotent in  $\mathbb{F}_\ell[\text{Gal}(F/k)]$ .*

## Example ( $\ell = 5$ )

Let  $k = \mathbb{Q}$  and  $F$  be a cyclic extension of  $k$  of degree dividing 4 disjoint from  $\mathbb{Q}_c$ . Then  $\text{circ}(1, 1, -1, 0)$  induces a Kummer theory over  $k$  and over  $F$ .

$$R_{F_c/F}\mathbb{G}_m(F)/\lambda R_{F_c/F}\mathbb{G}_m(F) \cong \text{Hom}_{\text{cont}}(\text{Gal}(\bar{F}/F), \ker \lambda(F)).$$

Let  $P \in R_{F_c/F}\mathbb{G}_m(F)$  and set  $L_P = F(\lambda^{-1}(P))$ . Suppose that  $P$  corresponds to

$$a_1 = u_1\zeta + u_2\zeta^3 + u_3\zeta^4 + u_4\zeta^2 \in F_c.$$

Let  $a_2, a_3, a_4$  are conjugates by  $\tau : \zeta \mapsto \zeta^3$ .

The cyclic extension  $L_P$  over  $F$  is defined by

$$\begin{aligned}
 & T^5 + \text{tr}((\zeta^3 + \zeta^2 - 2)a_1a_3)/10T^3 \\
 & \quad + \text{tr}((\zeta^3 - 3\zeta^2 - 2\zeta - 1)a_1a_2a_3)/25T^2 \\
 & + (-N/25 + \text{tr}((\zeta^3 + \zeta^2)a_1^2a_2a_3)/25 + \text{tr}((-\zeta^3 + \zeta^2 + 1)a_2^2a_4^2)/25 \\
 & \quad - \text{tr}((\zeta^3 + \zeta^2 + 1)a_1^2a_3^2 + (-\zeta^3 - \zeta^2)a_2^2a_4^2)/100)T \\
 & + (-(-\text{tr}((-\zeta^3 - 3\zeta^2 - 4\zeta - 2)a_1^4a_2^2a_3^3)/625 - \text{tr}((2\zeta^2 + 2\zeta + 1)a_1^3a_2^2a_3^3a_4)/12 \\
 & \quad - \text{tr}((\zeta^3 + \zeta^2 + 2\zeta + 1)a_1^3a_2^2a_3^2a_4^2)/125)/N) \in \mathbb{Q}(u_1, u_2, u_3, u_4)[T],
 \end{aligned}$$

where  $N$  is the product  $a_i$ 's and  $\text{tr}$  denotes the trace map  $\sum_{i=0}^3 \tau^i$ .

If  $[F : \mathbb{Q}] = 4$ , then we have

$$\begin{aligned}
 R_{F_c/\mathbb{Q}}\mathbb{G}_m &\sim R_{\mathbb{Q}_c/\mathbb{Q}}\mathbb{G}_m \\
 &\times \ker \left( N_{F_c^{(\sigma^2)}/\mathbb{Q}_c} : R_{F_c^{(\sigma^2)}/\mathbb{Q}}\mathbb{G}_m \rightarrow R_{\mathbb{Q}_c/\mathbb{Q}}\mathbb{G}_m \right) \\
 &\times \ker \left( N_{F_c/F_c^{(\sigma^2)}} : R_{F_c/\mathbb{Q}}\mathbb{G}_m \rightarrow R_{F_c^{(\sigma^2)}/\mathbb{Q}}\mathbb{G}_m \right).
 \end{aligned}$$

$P \in R_{\mathbb{Q}_c/\mathbb{Q}}\mathbb{G}_m(\mathbb{Q}) \implies L_P/\mathbb{Q}$  is a  $C_{20}$ -extension,

$P \in \ker \left( N_{F_c^{(\sigma^2)}/\mathbb{Q}_c} \right) (\mathbb{Q}) \implies L_P/\mathbb{Q}_c$  is an  $M_5(4|2)$ -extension,

$P \in \ker \left( N_{F_c/F_c^{(\sigma^2)}} \right) (\mathbb{Q}) \implies L_P/\mathbb{Q}$  is an  $F_{20}$ -extension.

If  $[F : \mathbb{Q}] = 4$ , then we have

$$\begin{aligned}
 R_{F_c/\mathbb{Q}}\mathbb{G}_m &\sim R_{\mathbb{Q}_c/\mathbb{Q}}\mathbb{G}_m \\
 &\times \ker \left( N_{F_c^{\langle \sigma^2 \rangle}/\mathbb{Q}_c} : R_{F_c^{\langle \sigma^2 \rangle}/\mathbb{Q}}\mathbb{G}_m \rightarrow R_{\mathbb{Q}_c/\mathbb{Q}}\mathbb{G}_m \right) \\
 &\times \ker \left( N_{F_c/F_c^{\langle \sigma^2 \rangle}} : R_{F_c/\mathbb{Q}}\mathbb{G}_m \rightarrow R_{F_c^{\langle \sigma^2 \rangle}/\mathbb{Q}}\mathbb{G}_m \right).
 \end{aligned}$$

$P \in R_{\mathbb{Q}_c/\mathbb{Q}}\mathbb{G}_m(\mathbb{Q}) \implies L_P/\mathbb{Q}$  is a  $C_{20}$ -extension,

$P \in \ker \left( N_{F_c^{\langle \sigma^2 \rangle}/\mathbb{Q}_c} \right) (\mathbb{Q}) \implies L_P/\mathbb{Q}_c$  is an  $M_5(4|2)$ -extension,

$P \in \ker \left( N_{F_c/F_c^{\langle \sigma^2 \rangle}} \right) (\mathbb{Q}) \implies L_P/\mathbb{Q}$  is an  $F_{20}$ -extension.

Similarly if  $[F : \mathbb{Q}] = 2$ , we have an isogeny

$$R_{F_c/\mathbb{Q}}\mathbb{G}_m \sim R_{\mathbb{Q}_c/\mathbb{Q}}\mathbb{G}_m \times \ker(N_{F_c/\mathbb{Q}_c} : R_{F_c/\mathbb{Q}}\mathbb{G}_m \rightarrow R_{\mathbb{Q}_c/\mathbb{Q}}\mathbb{G}_m)$$

and we obtain

$$P \in R_{\mathbb{Q}_c/\mathbb{Q}}\mathbb{G}_m(\mathbb{Q}) \implies L/\mathbb{Q} \text{ is a } C_{10}\text{-extension,}$$

$$P \in \ker N_{F_c/\mathbb{Q}_c}(\mathbb{Q}) \implies L/\mathbb{Q} \text{ is a } D_5\text{-extension.}$$

# Relation to a result of Imaoka-Kishi and Sase-Nakano

Recall that  $\text{Gal}(F_c/F) = \langle \tau \rangle$ .

Define  $\varepsilon = \frac{1}{n} \sum_{i=0}^{n-1} \chi(\tau^i) \tau^{-i}$  where  $\chi(\tau^i)$  is an element of  $\mathbb{F}_\ell^*$  satisfying

$\zeta_\ell^{\tau^i} = \zeta_\ell^{\chi(\tau^i)}$ . With the same notation as before, we have

## Theorem

*Let  $P \in T(s)$  and suppose that  $P$  corresponds to  $a_1 \in F_c$ . Then  $a_1$  is congruent to an element in  $F_c^{\langle \tau^{\frac{n}{s}j} \sigma \rangle}$  modulo  $(F_c^*)^\ell$  for some  $j$  prime to  $s$  and we have*

$$L_{P,c} = F_c(\sqrt[\ell]{\varepsilon a_1}).$$

This description gives a compatibility of our theorem and theorems due to Imaoka-Kishi and Sase-Nakano.

# Relation to a result of Imaoka-Kishi and Sase-Nakano

Recall that  $\text{Gal}(F_c/F) = \langle \tau \rangle$ .

Define  $\varepsilon = \frac{1}{n} \sum_{i=0}^{n-1} \chi(\tau^i) \tau^{-i}$  where  $\chi(\tau^i)$  is an element of  $\mathbb{F}_\ell^*$  satisfying

$\zeta_\ell^{\tau^i} = \zeta_\ell^{\chi(\tau^i)}$ . With the same notation as before, we have

## Theorem

*Let  $P \in T(s)$  and suppose that  $P$  corresponds to  $a_1 \in F_c$ . Then  $a_1$  is congruent to an element in  $F_c^{\langle \tau^{\frac{n}{s}j\sigma} \rangle}$  modulo  $(F_c^*)^\ell$  for some  $j$  prime to  $s$  and we have*

$$L_{P,c} = F_c(\sqrt[\ell]{\varepsilon a_1}).$$

This description gives a compatibility of our theorem and theorems due to Imaoka-Kishi and Sase-Nakano

# Relation to a result of Imaoka-Kishi and Sase-Nakano

Recall that  $\text{Gal}(F_c/F) = \langle \tau \rangle$ .

Define  $\varepsilon = \frac{1}{n} \sum_{i=0}^{n-1} \chi(\tau^i) \tau^{-i}$  where  $\chi(\tau^i)$  is an element of  $\mathbb{F}_\ell^*$  satisfying

$\zeta_\ell^{\tau^i} = \zeta_\ell^{\chi(\tau^i)}$ . With the same notation as before, we have

## Theorem

*Let  $P \in T(s)$  and suppose that  $P$  corresponds to  $a_1 \in F_c$ . Then  $a_1$  is congruent to an element in  $F_c^{\langle \tau^{\frac{n}{s}j\sigma} \rangle}$  modulo  $(F_c^*)^\ell$  for some  $j$  prime to  $s$  and we have*

$$L_{P,c} = F_c(\sqrt[\ell]{\varepsilon a_1}).$$

This description gives a compatibility of our theorem and theorems due to Imaoka-Kishi and Sase-Nakano.