On linear relations in algebraic groups

P.Krasoń, Szczecin University

G. Banaszak, P. Krasoń

On arithmetic in Mordell-Weil groups,

Acta Arithmetica 150.4 2011 pp.315-337

Outline

Outline

Abelian variety - projective algebraic variety that is also an algebraic group, i.e., has a group law that can be defined by regular functions.

$$m : A \times A \to A$$

$$inv : A \to A$$

An affine group variety is called a linear algebraic group

Each such variety can be realized as closed subgroup of GL_n for some n

In particular $G_m = GL_1$ is a linear algebraic group.

Abelian variety - projective algebraic variety that is also an algebraic group, i.e., has a group law that can be defined by regular functions.

$$m : A \times A \to A$$

$$inv : A \to A$$

An affine group variety is called a linear algebraic group

Each such variety can be realized as closed subgroup of GL_n for some n

In particular $G_m = GL_1$ is a linear algebraic group.

Abelian variety - projective algebraic variety that is also an algebraic group, i.e., has a group law that can be defined by regular functions.

$$m : A \times A \to A$$

$$inv : A \to A$$

An affine group variety is called a linear algebraic group

Each such variety can be realized as closed subgroup of GL_n for some n

In particular $G_m = GL_1$ is a linear algebraic group.

Abelian variety - projective algebraic variety that is also an algebraic group, i.e., has a group law that can be defined by regular functions.

$$m : A \times A \to A$$

$$inv : A \to A$$

An affine group variety is called a linear algebraic group

Each such variety can be realized as closed subgroup of GL_n for some n

In particular $G_m = GL_1$ is a linear algebraic group.

Abelian variety - projective algebraic variety that is also an algebraic group, i.e., has a group law that can be defined by regular functions.

$$m : A \times A \to A$$

$$inv : A \to A$$

An affine group variety is called a linear algebraic group

Each such variety can be realized as closed subgroup of GL_n for some n

In particular $G_m = GL_1$ is a linear algebraic group.

$A(\mathbb{C}) = \mathbb{C}^g/\Lambda$ $\quad$ Λ- a lattice in $\mathbb{R}^{2g}$

Theorem

A torus $\mathbb{C}^g/\Lambda$ is the set of complex points $A(\mathbb{C})$ of an abelian variety iff there exists an $\mathbb{R}$-bilinear form

$$E : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{R}$$

such that

(1) $E(iv, iw) = E(v, w)$

(2) $(v, w) \to E(v, iw)$ *is a symmetric positive defined bilinear form*

(3) $E(v, w) \in \mathbb{Z}$ *for* $v, w \in \Lambda$

If such a form exists then $A \hookrightarrow \mathbb{P}^n$ (by means of θ-functions)

$A(\mathbb{C}) = \mathbb{C}^g/\Lambda$ $\quad$ Λ- a lattice in $\mathbb{R}^{2g}$

Theorem

A torus $\mathbb{C}^g/\Lambda$ is the set of complex points $A(\mathbb{C})$ of an abelian variety iff there exists an $\mathbb{R}$-bilinear form

$$E : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{R}$$

such that

(1) $E(iv, iw) = E(v, w)$

(2) $(v, w) \to E(v, iw)$ *is a symmetric positive defined bilinear form*

(3) $E(v, w) \in \mathbb{Z}$ *for* $v, w \in \Lambda$

If such a form exists then $A \hookrightarrow \mathbb{P}^n$ (by means of θ-functions)

$A(\mathbb{C}) = \mathbb{C}^g/\Lambda$ Λ- a lattice in $\mathbb{R}^{2g}$

Theorem

A torus $\mathbb{C}^g/\Lambda$ is the set of complex points $A(\mathbb{C})$ of an abelian variety iff there exists an $\mathbb{R}$-bilinear form

$$E : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{R}$$

such that

(1) $E(iv, iw) = E(v, w)$

(2) $(v, w) \to E(v, iw)$ *is a symmetric positive defined bilinear form*

(3) $E(v, w) \in \mathbb{Z}$ *for* $v, w \in \Lambda$

If such a form exists then $A \hookrightarrow \mathbb{P}^n$ (by means of θ-functions)

$A(\mathbb{C}) = \mathbb{C}^g/\Lambda$ $\quad$ Λ- a lattice in $\mathbb{R}^{2g}$

Theorem

A torus $\mathbb{C}^g/\Lambda$ is the set of complex points $A(\mathbb{C})$ of an abelian variety iff there exists an $\mathbb{R}$-bilinear form

$$E : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{R}$$

such that

(1) $E(iv, iw) = E(v, w)$

(2) $(v, w) \to E(v, iw)$ *is a symmetric positive defined bilinear form*

(3) $E(v, w) \in \mathbb{Z}$ *for* $v, w \in \Lambda$

If such a form exists then $A \hookrightarrow \mathbb{P}^n$ (by means of θ-functions)

$A(\mathbb{C}) = \mathbb{C}^g/\Lambda$ $\quad$ Λ- a lattice in $\mathbb{R}^{2g}$

Theorem

A torus $\mathbb{C}^g/\Lambda$ is the set of complex points $A(\mathbb{C})$ of an abelian variety iff there exists an $\mathbb{R}$-bilinear form

$$E : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{R}$$

such that

(1) $E(iv, iw) = E(v, w)$

(2) $(v, w) \to E(v, iw)$ *is a symmetric positive defined bilinear form*

(3) $E(v, w) \in \mathbb{Z}$ *for* $v, w \in \Lambda$

If such a form exists then $A \hookrightarrow \mathbb{P}^n$ (by means of θ-functions)

$A(\mathbb{C}) = \mathbb{C}^g/\Lambda$ Λ- a lattice in $\mathbb{R}^{2g}$

Theorem

A torus $\mathbb{C}^g/\Lambda$ is the set of complex points $A(\mathbb{C})$ of an abelian variety iff there exists an $\mathbb{R}$-bilinear form

$$E : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{R}$$

such that

(1) $E(iv, iw) = E(v, w)$

(2) $(v, w) \to E(v, iw)$ *is a symmetric positive defined bilinear form*

(3) $E(v, w) \in \mathbb{Z}$ *for* $v, w \in \Lambda$

If such a form exists then $A \hookrightarrow \mathbb{P}^n$ (by means of θ-functions)

$A(\mathbb{C}) = \mathbb{C}^g/\Lambda$ $\quad$ Λ- a lattice in $\mathbb{R}^{2g}$

Theorem

A torus $\mathbb{C}^g/\Lambda$ is the set of complex points $A(\mathbb{C})$ of an abelian variety iff there exists an $\mathbb{R}$-bilinear form

$$E : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{R}$$

such that

(1) $E(iv, iw) = E(v, w)$

(2) $(v, w) \to E(v, iw)$ *is a symmetric positive defined bilinear form*

(3) $E(v, w) \in \mathbb{Z}$ *for* $v, w \in \Lambda$

If such a form exists then $A \hookrightarrow \mathbb{P}^n$ (by means of θ-functions)

$A(\mathbb{C}) = \mathbb{C}^g/\Lambda$ Λ- a lattice in $\mathbb{R}^{2g}$

Theorem

A torus $\mathbb{C}^g/\Lambda$ is the set of complex points $A(\mathbb{C})$ of an abelian variety iff there exists an $\mathbb{R}$-bilinear form

$$E : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{R}$$

such that

(1) $E(iv, iw) = E(v, w)$

(2) $(v, w) \to E(v, iw)$ *is a symmetric positive defined bilinear form*

(3) $E(v, w) \in \mathbb{Z}$ *for* $v, w \in \Lambda$

If such a form exists then $A \hookrightarrow \mathbb{P}^n$ (by means of θ-functions)

$A(\mathbb{C}) = \mathbb{C}^g/\Lambda$ Λ- a lattice in $\mathbb{R}^{2g}$

Theorem

A torus $\mathbb{C}^g/\Lambda$ is the set of complex points $A(\mathbb{C})$ of an abelian variety iff there exists an $\mathbb{R}$-bilinear form

$$E : \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{R}$$

such that

(1) $E(iv, iw) = E(v, w)$

(2) $(v, w) \to E(v, iw)$ *is a symmetric positive defined bilinear form*

(3) $E(v, w) \in \mathbb{Z}$ *for* $v, w \in \Lambda$

If such a form exists then $A \hookrightarrow \mathbb{P}^n$ (by means of θ-functions)

$f : A \to B$ is called an isogeny if f is surjective and has finite kernel.

The product of an abelian variety A of dimension m, and an abelian variety B of dimension n, over the same field, is an abelian variety of dimension m + n.

An abelian variety is simple if it is not isogenous to a product of abelian varieties of lower dimension.

Any abelian variety is isogenous to a product of simple abelian varieties.

$$A \cong A_1^{e_1} \times \cdots \times A_r^{e_r}$$

$f : A \to B$ is called an isogeny if f is surjective and has finite kernel.

The product of an abelian variety A of dimension m, and an abelian variety B of dimension n, over the same field, is an abelian variety of dimension m + n.

An abelian variety is simple if it is not isogenous to a product of abelian varieties of lower dimension.

Any abelian variety is isogenous to a product of simple abelian varieties.

$$A \cong A_1^{e_1} \times \cdots \times A_r^{e_r}$$

$f : A \to B$ is called an isogeny if f is surjective and has finite kernel.

The product of an abelian variety A of dimension m, and an abelian variety B of dimension n, over the same field, is an abelian variety of dimension m + n.

An abelian variety is simple if it is not isogenous to a product of abelian varieties of lower dimension.

Any abelian variety is isogenous to a product of simple abelian varieties.

$$A \cong A_1^{e_1} \times \cdots \times A_r^{e_r}$$

$f : A \to B$ is called an isogeny if f is surjective and has finite kernel.

The product of an abelian variety A of dimension m, and an abelian variety B of dimension n, over the same field, is an abelian variety of dimension m + n.

An abelian variety is simple if it is not isogenous to a product of abelian varieties of lower dimension.

Any abelian variety is isogenous to a product of simple abelian varieties.

$$A \cong A_1^{e_1} \times \cdots \times A_r^{e_r}$$

there exists $A^\vee$ such that $A = A^{\vee\vee}$

polarisation - an isogeny $\lambda : A \to A^\vee$

principal polarisation - $deg\lambda = 1$

over $\mathbb{C}$ polarisation is equivalent to the choice of skew-symmetic form

$$\psi : \Lambda \times \Lambda \to \mathbb{Z}$$

$det\psi = 1$ - polarisation is principal

there exists $A^\vee$ such that $A = A^{\vee\vee}$

polarisation - an isogeny $\lambda : A \to A^\vee$

principal polarisation - $deg\lambda = 1$

over $\mathbb{C}$ polarisation is equivalent to the choice of skew-symmetic form

$$\psi : \Lambda \times \Lambda \to \mathbb{Z}$$

$det\psi = 1$ - polarisation is principal

there exists $A^\vee$ such that $A = A^{\vee\vee}$

polarisation - an isogeny $\lambda : A \to A^\vee$

principal polarisation - $deg\lambda = 1$

over $\mathbb{C}$ polarisation is equivalent to the choice of skew-symmetic form

$$\psi : \Lambda \times \Lambda \to \mathbb{Z}$$

$det\psi = 1$ - polarisation is principal

there exists $A^\vee$ such that $A = A^{\vee\vee}$

polarisation - an isogeny $\lambda : A \to A^\vee$

principal polarisation - $deg\lambda = 1$

over $\mathbb{C}$ polarisation is equivalent to the choice of skew-symmetic form

$$\psi : \Lambda \times \Lambda \to \mathbb{Z}$$

$det\psi = 1$ - polarisation is principal

there exists $A^\vee$ such that $A = A^{\vee\vee}$

polarisation - an isogeny $\lambda : A \to A^\vee$

principal polarisation - $deg\lambda = 1$

over $\mathbb{C}$ polarisation is equivalent to the choice of skew-symmetic form

$$\psi : \Lambda \times \Lambda \to \mathbb{Z}$$

$det\psi = 1$ - polarisation is principal

there exists $A^\vee$ such that $A = A^{\vee\vee}$

polarisation - an isogeny $\lambda : A \to A^\vee$

principal polarisation - $deg\lambda = 1$

over $\mathbb{C}$ polarisation is equivalent to the choice of skew-symmetic form

$$\psi : \Lambda \times \Lambda \to \mathbb{Z}$$

$det\psi = 1$ - polarisation is principal

Since λ is an isogeny there exists λ^{-1} in $Hom(A^\vee, A) \otimes \mathbb{Q}$

Rosati involution on $End^0(A) = End(A) \otimes \mathbb{Q}$

$$R_{inv} : \alpha \to \alpha' = \lambda^{-1} \circ \alpha^\vee \circ \lambda$$

Since λ is an isogeny there exists λ^{-1} in $Hom(A^\vee, A) \otimes \mathbb{Q}$

Rosati involution on $End^0(A) = End(A) \otimes \mathbb{Q}$

$$R_{inv} : \alpha \to \alpha' = \lambda^{-1} \circ \alpha^\vee \circ \lambda$$

Outline

Albert's classification

A/F - simple; $E = Z(End^0(A)) = Z(End(A) \otimes \mathbb{Q})$;
$E_0 = E^{R_{inv}}$

1. (I) $End^0(A) = E = E_0$ is a totally real number field $R_{inv} = id$
2. (II) $E = E_0$ is a totally real number field; $End^0(A)$ is a division algebra over E such that every component of $End^0(A) \otimes_{\mathbb{Q}} \mathbb{R}$ is isomorphic to $M_2(\mathbb{R})$;
$\beta \in End^0(A)$, ${}^t\beta = -\beta$; $R_{inv}(\alpha) = \beta^{-1}({}^t\alpha)\beta$
3. (III) $E = E_0$ is totally real; $End^0(A)$ is a division algebra over E such that every component of $End^0(A) \otimes_{\mathbb{Q}} \mathbb{R}$ is isomorphic to $\mathbb{H}$ $R_{inv}(\alpha) = {}^t\alpha$
4. (IV) E_0 is totally real; E - totally imaginary quadratic extension of E_0; $R_{inv}|_E = cc|_E$; $End^0(A)$ is a division algebra over E

Albert's classification

A/F - simple; $E = Z(End^0(A)) = Z(End(A) \otimes \mathbb{Q})$;
$E_0 = E^{R_{inv}}$

1. (I) $End^0(A) = E = E_0$ is a totally real number field $R_{inv} = id$
2. (II) $E = E_0$ is a totally real number field; $End^0(A)$ is a division algebra over E such that every component of $End^0(A) \otimes_{\mathbb{Q}} \mathbb{R}$ is isomorphic to $M_2(\mathbb{R})$;
   $\beta \in End^0(A)$, ${}^t\beta = -\beta$; $R_{inv}(\alpha) = \beta^{-1}({}^t\alpha)\beta$
3. (III) $E = E_0$ is totally real; $End^0(A)$ is a division algebra over E such that every component of $End^0(A) \otimes_{\mathbb{Q}} \mathbb{R}$ is isomorphic to $\mathbb{H}$ $R_{inv}(\alpha) = {}^t\alpha$
4. (IV) E_0 is totally real; E - totally imaginary quadratic extension of E_0; $R_{inv}|_E = cc|_E$; $End^0(A)$ is a division algebra over E

Albert's classification

A/F - simple; $E = Z(End^0(A)) = Z(End(A) \otimes \mathbb{Q})$;
$E_0 = E^{R_{inv}}$

1. (I) $End^0(A) = E = E_0$ is a totally real number field $R_{inv} = id$
2. (II) $E = E_0$ is a totally real number field; $End^0(A)$ is a division algebra over E such that every component of $End^0(A) \otimes_{\mathbb{Q}} \mathbb{R}$ is isomorphic to $M_2(\mathbb{R})$;
$\beta \in End^0(A)$, ${}^t\beta = -\beta$; $R_{inv}(\alpha) = \beta^{-1}({}^t\alpha)\beta$
3. (III) $E = E_0$ is totally real; $End^0(A)$ is a division algebra over E such that every component of $End^0(A) \otimes_{\mathbb{Q}} \mathbb{R}$ is isomorphic to $\mathbb{H}$ $R_{inv}(\alpha) = {}^t\alpha$
4. (IV) E_0 is totally real; E - totally imaginary quadratic extension of E_0; $R_{inv}|_E = cc|_E$; $End^0(A)$ is a division algebra over E

Albert's classification

A/F - simple; $E = Z(End^0(A)) = Z(End(A) \otimes \mathbb{Q})$;
$E_0 = E^{R_{inv}}$

1. (I) $End^0(A) = E = E_0$ is a totally real number field $R_{inv} = id$
2. (II) $E = E_0$ is a totally real number field; $End^0(A)$ is a division algebra over E such that every component of $End^0(A) \otimes_{\mathbb{Q}} \mathbb{R}$ is isomorphic to $M_2(\mathbb{R})$;
$\beta \in End^0(A)$, ${}^t\beta = -\beta$; $R_{inv}(\alpha) = \beta^{-1}({}^t\alpha)\beta$
3. (III) $E = E_0$ is totally real; $End^0(A)$ is a division algebra over E such that every component of $End^0(A) \otimes_{\mathbb{Q}} \mathbb{R}$ is isomorphic to $\mathbb{H}$ $R_{inv}(\alpha) = {}^t\alpha$
4. (IV) E_0 is totally real; E - totally imaginary quadratic extension of E_0; $R_{inv}|_E = cc|_E$; $End^0(A)$ is a division algebra over E

Outline

K - a number field

Theorem (A.Schinzel 1973)

If $\alpha_1, \ldots \alpha_k, \beta$ are non-zero elements of K and the congruence

$$\alpha_1^{x_1} \alpha_2^{x_2} \ldots \alpha_k^{x_k} \equiv \beta \ mod \ \mathfrak{p}$$

is soluble for almost all prime ideals $\mathfrak{p}$ of K then the corresponding equation is soluble in rational integers. i.e. there exist $n_1 \ldots \ n_k \in \mathbb{Z}$ such that $\beta = {\alpha_1}^{n_1} \ldots {\alpha_k}^{n_k}$

proved again by C.Khare by different methods

K - a number field

Theorem (A.Schinzel 1973)

If $\alpha_1, \ldots \alpha_k, \beta$ are non-zero elements of K and the congruence

$$\alpha_1^{x_1} \alpha_2^{x_2} \ldots \alpha_k^{x_k} \equiv \beta \ mod \ \mathfrak{p}$$

is soluble for almost all prime ideals $\mathfrak{p}$ of K then the corresponding equation is soluble in rational integers. i.e. there exist $n_1 \ldots \ n_k \in \mathbb{Z}$ such that $\beta = {\alpha_1}^{n_1} \ldots {\alpha_k}^{n_k}$

proved again by C.Khare by different methods

K - a number field

Theorem (A.Schinzel 1973)

If $\alpha_1, \ldots \alpha_k, \beta$ are non-zero elements of K and the congruence

$$\alpha_1^{x_1} \alpha_2^{x_2} \ldots \alpha_k^{x_k} \equiv \beta \ mod \ \mathfrak{p}$$

is soluble for almost all prime ideals $\mathfrak{p}$ of K then the corresponding equation is soluble in rational integers. i.e. there exist $n_1 \ldots \ n_k \in \mathbb{Z}$ such that $\beta = {\alpha_1}^{n_1} \ldots {\alpha_k}^{n_k}$

proved again by C.Khare by different methods

K - a number field

Theorem (A.Schinzel 1973)

If $\alpha_1, \ldots \alpha_k, \beta$ are non-zero elements of K and the congruence

$$\alpha_1^{x_1} \alpha_2^{x_2} \ldots \alpha_k^{x_k} \equiv \beta \ mod \ \mathfrak{p}$$

is soluble for almost all prime ideals $\mathfrak{p}$ of K then the corresponding equation is soluble in rational integers. i.e. there exist $n_1 \ldots \ n_k \in \mathbb{Z}$ such that $\beta = {\alpha_1}^{n_1} \ldots {\alpha_k}^{n_k}$

proved again by C.Khare by different methods

K - a number field

Theorem (A.Schinzel 1973)

If $\alpha_1, \ldots \alpha_k, \beta$ are non-zero elements of K and the congruence

$$\alpha_1^{x_1} \alpha_2^{x_2} \ldots \alpha_k^{x_k} \equiv \beta \ mod \ \mathfrak{p}$$

is soluble for almost all prime ideals $\mathfrak{p}$ of K then the corresponding equation is soluble in rational integers. i.e. there exist $n_1 \ldots \ n_k \in \mathbb{Z}$ such that $\beta = {\alpha_1}^{n_1} \ldots {\alpha_k}^{n_k}$

proved again by C.Khare by different methods

Theorem of A.Schinzel does not extend in full generality to the system of congruences.

Theorem (A. Schinzel 1973)

Let $\alpha_{i,j}, \beta_i \quad (i = 1, \ldots, h, j = 1, \ldots k)$ be non-zero elements of K, D a positive integer. If the system of congruences

$$\Pi_{j=1}^{k} \alpha_{ij}^{x_j} \equiv \beta_i \ mod\, \mathfrak{m} \qquad (i = 1, \ldots, h)$$

is soluble for all moduli $\mathfrak{m}$ prime to D then the corresponding system of equations is soluble in integers.

Theorem of A.Schinzel does not extend in full generality to the system of congruences.

Theorem (A. Schinzel 1973)

Let $\alpha_{i,j}, \beta_i \quad (i = 1, \ldots, h, j = 1, \ldots k)$ *be non-zero elements of* K, D *a positive integer. If the system of congruences*

$$\Pi_{j=1}^{k} \alpha_{ij}^{x_j} \equiv \beta_i \bmod \mathfrak{m} \qquad (i = 1, \ldots, h)$$

is soluble for all moduli $\mathfrak{m}$ *prime to* D *then the corresponding system of equations is soluble in integers.*

Theorem of A.Schinzel does not extend in full generality to the system of congruences.

Theorem (A. Schinzel 1973)

Let $\alpha_{i,j}, \beta_i \quad (i = 1, \ldots, h, j = 1, \ldots k)$ *be non-zero elements of* K, D *a positive integer.If the system of congruences*

$$\Pi_{j=1}^{k} \alpha_{ij}^{x_j} \equiv \beta_i \ mod\, \mathfrak{m} \qquad (i = 1, \ldots, h)$$

is soluble for all moduli $\mathfrak{m}$ *prime to* D *then the corresponding system of equations is soluble in integers.*

Theorem of A.Schinzel does not extend in full generality to the system of congruences.

Theorem (A. Schinzel 1973)

Let $\alpha_{i,j}, \beta_i \quad (i = 1, \ldots, h, j = 1, \ldots k)$ *be non-zero elements of* K, D *a positive integer.If the system of congruences*

$$\Pi_{j=1}^{k} \alpha_{ij}^{x_j} \equiv \beta_i \ mod\, \mathfrak{m} \qquad (i = 1, \ldots, h)$$

is soluble for all moduli $\mathfrak{m}$ *prime to* D *then the corresponding system of equations is soluble in integers.*

Counterexample: [A.Schinzel 1973]

$$2^x 3^y \equiv 1 \, mod \, p$$

$$2^y 3^z \equiv 4 \ mod \, p$$

for $p = 2, \ 3 \quad (x, y, z) = (0, 1, 0)$ resp. $(0, 0, 0)$

For other p, fix a primitive root $mod \, p$

$$xind2 + yind3 \equiv 0 \ mod \ p - 1,$$

$$yind2 + zind3 \equiv 2ind2 \ mod \ p - 1$$

Counterexample: [A.Schinzel 1973]

$$2^x 3^y \equiv 1 mod\, p$$

$$2^y 3^z \equiv 4 \ mod\, p$$

for $p = 2,\ 3 \quad (x, y, z) = (0, 1, 0)$ resp. $(0, 0, 0)$

For other p, fix a primitive root $mod\, p$

$$xind2 + yind3 \equiv 0 \ mod \ p - 1,$$

$$yind2 + zind3 \equiv 2ind2 \ mod \ p - 1$$

Counterexample: [A.Schinzel 1973]

$$2^x 3^y \equiv 1 mod\, p$$

$$2^y 3^z \equiv 4\ mod\, p$$

for $p = 2, 3$ $(x, y, z) = (0, 1, 0)$ resp. $(0, 0, 0)$

For other p, fix a primitive root $mod\, p$

$$xind2 + yind3 \equiv 0\ mod\ p - 1,$$

$$yind2 + zind3 \equiv 2ind2\ mod\ p - 1$$

Counterexample: [A.Schinzel 1973]

$$2^x 3^y \equiv 1 mod\, p$$

$$2^y 3^z \equiv 4\ mod\, p$$

for $p = 2,\ 3\ \ (x, y, z) = (0, 1, 0)$ resp. $(0, 0, 0)$

For other p, fix a primitive root $mod\ p$

$$xind2 + yind3 \equiv 0\ mod\ p - 1,$$

$$yind2 + zind3 \equiv 2ind2\ mod\ p - 1$$

Counterexample: [A.Schinzel 1973]

$$2^x 3^y \equiv 1 mod\, p$$

$$2^y 3^z \equiv 4 \ mod\, p$$

for $p = 2,\ 3 \quad (x, y, z) = (0, 1, 0)$ resp. $(0, 0, 0)$

For other p, fix a primitive root $mod\, p$

$$xind2 + yind3 \equiv 0 \ mod \ p - 1,$$

$$yind2 + zind3 \equiv 2ind2 \ mod \ p - 1$$

Counterexample: [A.Schinzel 1973]

$$2^x 3^y \equiv 1 mod\, p$$

$$2^y 3^z \equiv 4 \ mod\, p$$

for $p = 2,\ 3 \quad (x, y, z) = (0, 1, 0)$ resp. $(0, 0, 0)$

For other p, fix a primitive root $mod\, p$

$$xind2 + yind3 \equiv 0 \ mod \ p - 1,$$

$$yind2 + zind3 \equiv 2ind2 \ mod \ p - 1$$

$$gcd(\frac{(ind2)^2}{gcd(ind2, ind3)}, ind3) \mid ind2$$

$$t\frac{(ind2)^2}{gcd(ind2, ind3)} + zind3 = 2ind2$$

$$x = \frac{-tind3}{gcd(ind2, ind3)}, \qquad y = \frac{tind2}{gcd(ind2, ind3)} \qquad z$$

$$gcd(\frac{(ind2)^2}{gcd(ind2, ind3)}, ind3) \mid ind2$$

$$t\frac{(ind2)^2}{gcd(ind2, ind3)} + zind3 = 2ind2$$

$$x = \frac{-tind3}{gcd(ind2, ind3)}, \qquad y = \frac{tind2}{gcd(ind2, ind3)} \qquad z$$

$$gcd(\frac{(ind2)^2}{gcd(ind2, ind3)}, ind3) \mid ind2$$

$$t\frac{(ind2)^2}{gcd(ind2, ind3)} + zind3 = 2ind2$$

$$x = \frac{-tind3}{gcd(ind2, ind3)}, \qquad y = \frac{tind2}{gcd(ind2, ind3)} \qquad z$$

Outline

$A/F \qquad red_v : A(F) \to A(k_v)$

QUESTION (W.GAJDA 2002)

Let Σ be a subgroup of $A(F)$. Suppose that x is a point of $A(F)$ such that $red_v x$ lies in $red_v \Sigma$ for almost all places v of F. Does it then follow that x lies in Σ?

$A/F \qquad red_v : A(F) \to A(k_v)$

QUESTION (W.GAJDA 2002)

Let Σ be a subgroup of $A(F)$. Suppose that x is a point of $A(F)$ such that $red_v x$ lies in $red_V \Sigma$ for almost all places v of F. Does it then follow that x lies in Σ?

$A/F \qquad red_v : A(F) \to A(k_v)$

QUESTION (W.GAJDA 2002)

Let Σ be a subgroup of $A(F)$. Suppose that x is a point of $A(F)$ such that $red_v x$ lies in $red_V \Sigma$ for almost all places v of F. Does it then follow that x lies in Σ?

Outline

Theorem (Weston 2003)

Let A be an abelian variety over a number field F and assume that $\mathrm{End}_F A$ is commutative. Let Σ be a subgroup of $A(F)$ and suppose that $x \in A(F)$ is such that $\mathrm{red}_v x \in \mathrm{red}_v \Sigma$ for almost all places v of F. Then $x \in \Sigma + A(F)_{tors}$

this covers product of non-isogenous elliptic curves.

Theorem (Weston 2003)

Let A be an abelian variety over a number field F and assume that $End_F A$ is commutative. Let Σ be a subgroup of $A(F)$ and suppose that $x \in A(F)$ is such that $red_v x \in red_v \Sigma$ for almost all places v of F. Then $x \in \Sigma + A(F)_{tors}$

this covers product of non-isogenous elliptic curves.

Theorem (Weston 2003)

Let A be an abelian variety over a number field F and assume that $End_F A$ is commutative. Let Σ be a subgroup of $A(F)$ and suppose that $x \in A(F)$ is such that $red_v x \in red_v \Sigma$ for almost all places v of F. Then $x \in \Sigma + A(F)_{tors}$

this covers product of non-isogenous elliptic curves.

Theorem (Weston 2003)

Let A be an abelian variety over a number field F and assume that $End_F A$ is commutative. Let Σ be a subgroup of $A(F)$ and suppose that $x \in A(F)$ is such that $red_v x \in red_v \Sigma$ for almost all places v of F. Then $x \in \Sigma + A(F)_{tors}$

this covers product of non-isogenous elliptic curves.

Theorem (G.Banaszak, W.Gajda, P.K 2005)

Let A be a principally polarized abelian variety of dimension g defined over the number field F such that $End_{\overline{F}}(A) = \mathbb{Z}$ and $dim(A) = g$ is either odd or $g = 2$ or 6. Let P and $P_1 \dots P_r$ be non-torsion elements of $A(F)$ such that $P_1 \dots P_r$ are linearly independent over $\mathbb{Z}$. Denote by Λ the subgroup of $A(F)$ generated by $P_1 \dots P_r$. Then the following are equivalent:

(1) $P \in \Lambda$

(2) $r_v(P) \in r_v(\Lambda)$

Theorem (G.Banaszak, W.Gajda, P.K 2005)

Let A be a principally polarized abelian variety of dimension g defined over the number field F such that $End_{\overline{F}}(A) = \mathbb{Z}$ and $dim(A) = g$ is either odd or $g = 2$ or 6. Let P and $P_1 \dots P_r$ be non-torsion elements of $A(F)$ such that $P_1 \dots P_r$ are linearly independent over $\mathbb{Z}$. Denote by Λ the subgroup of $A(F)$ generated by $P_1 \dots P_r$. Then the following are equivalent:

(1) $P \in \Lambda$

(2) $r_v(P) \in r_v(\Lambda)$

Theorem (G.Banaszak, W.Gajda, P.K 2005)

Let A be a principally polarized abelian variety of dimension g defined over the number field F such that $End_{\overline{F}}(A) = \mathbb{Z}$ and $dim(A) = g$ is either odd or $g = 2$ or 6. Let P and $P_1 \dots P_r$ be non-torsion elements of $A(F)$ such that $P_1 \dots P_r$ are linearly independent over $\mathbb{Z}$. Denote by Λ the subgroup of $A(F)$ generated by $P_1 \dots P_r$. Then the following are equivalent:

(1) $P \in \Lambda$

(2) $r_v(P) \in r_v(\Lambda)$

Theorem (G.Banaszak, W.Gajda, P.K 2005)

Let A be a principally polarized abelian variety of dimension g defined over the number field F such that $End_{\overline{F}}(A) = \mathbb{Z}$ and $dim(A) = g$ is either odd or $g = 2$ or 6. Let P and $P_1 \dots P_r$ be non-torsion elements of $A(F)$ such that $P_1 \dots P_r$ are linearly independent over $\mathbb{Z}$. Denote by Λ the subgroup of $A(F)$ generated by $P_1 \dots P_r$. Then the following are equivalent:

(1) $P \in \Lambda$

(2) $r_v(P) \in r_v(\Lambda)$

Theorem (G.Banaszak, W.Gajda, P.K 2005)

Let A be a principally polarized abelian variety of dimension g defined over the number field F such that $End_{\overline{F}}(A) = \mathbb{Z}$ and $dim(A) = g$ is either odd or $g = 2$ or 6. Let P and $P_1 \dots P_r$ be non-torsion elements of $A(F)$ such that $P_1 \dots P_r$ are linearly independent over $\mathbb{Z}$. Denote by Λ the subgroup of $A(F)$ generated by $P_1 \dots P_r$. Then the following are equivalent:

(1) $P \in \Lambda$

(2) $r_v(P) \in r_v(\Lambda)$

Theorem (BGK 2005)

Let P and $P_1 \dots P_r$ be non-torsion elements of $A(F)$ such that $\mathcal{R}P$ is a free $\mathcal{R}$-module and $P_1 \dots P_r$ are linearly independent over $\mathcal{R}$. Denote by Λ the $\mathcal{R}$-submodule of $A(F)$ generated by $P_1 \dots P_r$. Assume that $r_v(P) \in r_v(\Lambda)$ for almost all primes v of F. Then there exists a natural number a such that $aP \in \Lambda$.

W. Gajda and K.Górnisiewicz refined this theorem to $a = 1$

Theorem (BGK 2005)

Let P and $P_1 \dots P_r$ be non-torsion elements of $A(F)$ such that $\mathcal{R}P$ is a free $\mathcal{R}$-module and $P_1 \dots P_r$ are linearly independent over $\mathcal{R}$. Denote by Λ the $\mathcal{R}$-submodule of $A(F)$ generated by $P_1 \dots P_r$. Assume that $r_v(P) \in r_v(\Lambda)$ for almost all primes v of F. Then there exists a natural number a such that $aP \in \Lambda$.

W. Gajda and K.Górnisiewicz refined this theorem to $a = 1$

Theorem (BGK 2005)

Let P and $P_1 \dots P_r$ be non-torsion elements of $A(F)$ such that $\mathcal{R}P$ is a free $\mathcal{R}$-module and $P_1 \dots P_r$ are linearly independent over $\mathcal{R}$. Denote by Λ the $\mathcal{R}$-submodule of $A(F)$ generated by $P_1 \dots P_r$. Assume that $r_v(P) \in r_v(\Lambda)$ for almost all primes v of F. Then there exists a natural number a such that $aP \in \Lambda$.

W. Gajda and K.Górnisiewicz refined this theorem to $a = 1$

Theorem (BGK 2005)

Let P and $P_1 \dots P_r$ be non-torsion elements of $A(F)$ such that $\mathcal{R}P$ is a free $\mathcal{R}$-module and $P_1 \dots P_r$ are linearly independent over $\mathcal{R}$. Denote by Λ the $\mathcal{R}$-submodule of $A(F)$ generated by $P_1 \dots P_r$. Assume that $r_v(P) \in r_v(\Lambda)$ for almost all primes v of F. Then there exists a natural number a such that $aP \in \Lambda$.

W. Gajda and K.Górnisiewicz refined this theorem to $a = 1$

Theorem (G.Banaszak 2008)

Let $P_1, \ldots, P_r$ be elements of $A(F)$ linearly independent over $\mathcal{R} = End_F(A)$. Let P be a point of $A(F)$ such that $\mathcal{R}P$ is a free $\mathcal{R}$-module. The following conditions are equivalent:

(1) $P \in \Sigma_{i=1}^{r} \mathbb{Z} P_i$

(2) $r_v(P) \in \Sigma_{i=1}^{r} \mathbb{Z} r_v(P_i)$

A. Perucca generalized this theorem to semiabelian varieties and removed the hypotheses that $\mathcal{R}P$ is a free $\mathcal{R}$-module

Theorem (G.Banaszak 2008)

Let $P_1, \ldots, P_r$ be elements of $A(F)$ linearly independent over $\mathcal{R} = End_{\overline{F}}(A)$. Let P be a point of $A(F)$ such that $\mathcal{R}P$ is a free $\mathcal{R}$-module. The following conditions are equivalent:

(1) $P \in \Sigma_{i=1}^{r} \mathbb{Z} P_i$

(2) $r_v(P) \in \Sigma_{i=1}^{r} \mathbb{Z} r_v(P_i)$

A. Perucca generalized this theorem to semiabelian varieties and removed the hypotheses that $\mathcal{R}P$ is a free $\mathcal{R}$-module

Theorem (G.Banaszak 2008)

Let $P_1, \ldots, P_r$ be elements of $A(F)$ linearly independent over $\mathcal{R} = End_{\overline{F}}(A)$. Let P be a point of $A(F)$ such that $\mathcal{R}P$ is a free $\mathcal{R}$-module. The following conditions are equivalent:

(1) $P \in \Sigma_{i=1}^{r} \mathbb{Z} P_i$

(2) $r_v(P) \in \Sigma_{i=1}^{r} \mathbb{Z} r_v(P_i)$

A. Perucca generalized this theorem to semiabelian varieties and removed the hypotheses that $\mathcal{R}P$ is a free $\mathcal{R}$-module

Theorem (G.Banaszak 2008)

Let $P_1, \ldots, P_r$ be elements of $A(F)$ linearly independent over $\mathcal{R} = End_F(A)$. Let P be a point of $A(F)$ such that $\mathcal{R}P$ is a free $\mathcal{R}$-module. The following conditions are equivalent:

(1) $P \in \Sigma_{i=1}^{r} \mathbb{Z} P_i$

(2) $r_v(P) \in \Sigma_{i=1}^{r} \mathbb{Z} r_v(P_i)$

A. Perucca generalized this theorem to semiabelian varieties and removed the hypotheses that $\mathcal{R}P$ is a free $\mathcal{R}$-module

THEOREM A (G.BANASZAK, P.KRASOŃ)

Let A/F be an abelian variety defined over a number field F. Assume that A is isogeneous to $A_1^{e_1} \times \cdots \times A_t^{e_t}$ with A_i simple, pairwise nonisogenous abelian varieties such that $dim_{End_{F'}(A_i)^0} H_1(A_i(\mathbb{C}); \mathbb{Q}) \geq e_i$ for each $1 \leq i \leq t$, where $End_{F'}(A_i)^0 := End_{F'}(A_i) \otimes \mathbb{Q}$ and F'/F is a finite extension such that the isogeny is defined over F'. Let $P \in A(F)$ and let Λ be a subgroup of $A(F)$. If $r_v(P) \in r_v(\Lambda)$ for almost all v of $\mathcal{O}_F$ then $P \in \Lambda + A(F)_{tor}$. Moreover if $A(F)_{tor} \subset \Lambda$, then the following conditions are equivalent:

1. $P \in \Lambda$
2. $r_v(P) \in r_v(\Lambda)$ *for almost all* v *of* $\mathcal{O}_F$.

THEOREM A (G.BANASZAK, P.KRASOŃ)

Let A/F be an abelian variety defined over a number field F. Assume that A is isogeneous to $A_1^{e_1} \times \cdots \times A_t^{e_t}$ with A_i simple, pairwise nonisogenous abelian varieties such that $\dim_{End_{F'}(A_i)^0} H_1(A_i(\mathbb{C}); \mathbb{Q}) \geq e_i$ for each $1 \leq i \leq t$, where $End_{F'}(A_i)^0 := End_{F'}(A_i) \otimes \mathbb{Q}$ and F'/F is a finite extension such that the isogeny is defined over F'. Let $P \in A(F)$ and let Λ be a subgroup of $A(F)$. If $r_v(P) \in r_v(\Lambda)$ for almost all v of $\mathcal{O}_F$ then $P \in \Lambda + A(F)_{tor}$. Moreover if $A(F)_{tor} \subset \Lambda$, then the following conditions are equivalent:

1. $P \in \Lambda$
2. $r_v(P) \in r_v(\Lambda)$ *for almost all* v *of* $\mathcal{O}_F$.

THEOREM A (G.BANASZAK, P.KRASOŃ)

Let A/F be an abelian variety defined over a number field F. Assume that A is isogeneous to $A_1^{e_1} \times \cdots \times A_t^{e_t}$ with A_i simple, pairwise nonisogenous abelian varieties such that $dim_{End_{F'}(A_i)^0} H_1(A_i(\mathbb{C}); \mathbb{Q}) \geq e_i$ for each $1 \leq i \leq t$, where $End_{F'}(A_i)^0 := End_{F'}(A_i) \otimes \mathbb{Q}$ and F'/F is a finite extension such that the isogeny is defined over F'. Let $P \in A(F)$ and let Λ be a subgroup of $A(F)$. If $r_v(P) \in r_v(\Lambda)$ for almost all v of $\mathcal{O}_F$ then $P \in \Lambda + A(F)_{tor}$. Moreover if $A(F)_{tor} \subset \Lambda$, then the following conditions are equivalent:

1. $P \in \Lambda$
2. $r_v(P) \in r_v(\Lambda)$ *for almost all* v *of* $\mathcal{O}_F$.

THEOREM A (G.BANASZAK, P.KRASOŃ)

Let A/F be an abelian variety defined over a number field F. Assume that A is isogeneous to $A_1^{e_1} \times \cdots \times A_t^{e_t}$ with A_i simple, pairwise nonisogenous abelian varieties such that $dim_{End_{F'}(A_i)^0} H_1(A_i(\mathbb{C}); \mathbb{Q}) \geq e_i$ for each $1 \leq i \leq t$, where $End_{F'}(A_i)^0 := End_{F'}(A_i) \otimes \mathbb{Q}$ and F'/F is a finite extension such that the isogeny is defined over F'. Let $P \in A(F)$ and let Λ be a subgroup of $A(F)$. If $r_v(P) \in r_v(\Lambda)$ for almost all v of $\mathcal{O}_F$ then $P \in \Lambda + A(F)_{tor}$. Moreover if $A(F)_{tor} \subset \Lambda$, then the following conditions are equivalent:

1. $P \in \Lambda$
2. $r_v(P) \in r_v(\Lambda)$ *for almost all* v *of* $\mathcal{O}_F$.

THEOREM A (G.BANASZAK, P.KRASOŃ)

Let A/F be an abelian variety defined over a number field F. Assume that A is isogeneous to $A_1^{e_1} \times \cdots \times A_t^{e_t}$ with A_i simple, pairwise nonisogenous abelian varieties such that $dim_{End_{F'}(A_i)^0} H_1(A_i(\mathbb{C}); \mathbb{Q}) \geq e_i$ for each $1 \leq i \leq t$, where $End_{F'}(A_i)^0 := End_{F'}(A_i) \otimes \mathbb{Q}$ and F'/F is a finite extension such that the isogeny is defined over F'. Let $P \in A(F)$ and let Λ be a subgroup of $A(F)$. If $r_v(P) \in r_v(\Lambda)$ for almost all v of $\mathcal{O}_F$ then $P \in \Lambda + A(F)_{tor}$. Moreover if $A(F)_{tor} \subset \Lambda$, then the following conditions are equivalent:

1. $P \in \Lambda$
2. $r_v(P) \in r_v(\Lambda)$ *for almost all* v *of* $\mathcal{O}_F$.

THEOREM A (G.BANASZAK, P.KRASOŃ)

Let A/F be an abelian variety defined over a number field F. Assume that A is isogeneous to $A_1^{e_1} \times \cdots \times A_t^{e_t}$ with A_i simple, pairwise nonisogenous abelian varieties such that $dim_{End_{F'}(A_i)^0} H_1(A_i(\mathbb{C}); \mathbb{Q}) \geq e_i$ for each $1 \leq i \leq t$, where $End_{F'}(A_i)^0 := End_{F'}(A_i) \otimes \mathbb{Q}$ and F'/F is a finite extension such that the isogeny is defined over F'. Let $P \in A(F)$ and let Λ be a subgroup of $A(F)$. If $r_v(P) \in r_v(\Lambda)$ for almost all v of $\mathcal{O}_F$ then $P \in \Lambda + A(F)_{tor}$. Moreover if $A(F)_{tor} \subset \Lambda$, then the following conditions are equivalent:

1. $P \in \Lambda$
2. $r_v(P) \in r_v(\Lambda)$ *for almost all* v *of* $\mathcal{O}_F$.

THEOREM A (G.BANASZAK, P.KRASOŃ)

Let A/F be an abelian variety defined over a number field F. Assume that A is isogeneous to $A_1^{e_1} \times \cdots \times A_t^{e_t}$ with A_i simple, pairwise nonisogenous abelian varieties such that $dim_{End_{F'}(A_i)^0} H_1(A_i(\mathbb{C}); \mathbb{Q}) \geq e_i$ for each $1 \leq i \leq t$, where $End_{F'}(A_i)^0 := End_{F'}(A_i) \otimes \mathbb{Q}$ and F'/F is a finite extension such that the isogeny is defined over F'. Let $P \in A(F)$ and let Λ be a subgroup of $A(F)$. If $r_v(P) \in r_v(\Lambda)$ for almost all v of $\mathcal{O}_F$ then $P \in \Lambda + A(F)_{tor}$. Moreover if $A(F)_{tor} \subset \Lambda$, then the following conditions are equivalent:

1. $P \in \Lambda$
2. $r_v(P) \in r_v(\Lambda)$ *for almost all* v *of* $\mathcal{O}_F$.

THEOREM A (G.BANASZAK, P.KRASOŃ)

Let A/F be an abelian variety defined over a number field F. Assume that A is isogeneous to $A_1^{e_1} \times \cdots \times A_t^{e_t}$ with A_i simple, pairwise nonisogenous abelian varieties such that $dim_{End_{F'}(A_i)^0} H_1(A_i(\mathbb{C}); \mathbb{Q}) \geq e_i$ for each $1 \leq i \leq t$, where $End_{F'}(A_i)^0 := End_{F'}(A_i) \otimes \mathbb{Q}$ and F'/F is a finite extension such that the isogeny is defined over F'. Let $P \in A(F)$ and let Λ be a subgroup of $A(F)$. If $r_v(P) \in r_v(\Lambda)$ for almost all v of $\mathcal{O}_F$ then $P \in \Lambda + A(F)_{tor}$. Moreover if $A(F)_{tor} \subset \Lambda$, then the following conditions are equivalent:

1. $P \in \Lambda$
2. $r_v(P) \in r_v(\Lambda)$ *for almost all* v *of* $\mathcal{O}_F$.

Problem

Let A/F be an abelian variety over a number field F and let $P \in A(F)$ and let $\Lambda \subset A(F)$ be a subgroup. Is there an effectively computable finite set S^{eff} of primes v of $\mathcal{O}_F$, depending only on A, P and Λ such that the following conditions are equivalent? :

(1) $P \in \Lambda$

(2) $r_v(P) \in r_v(\Lambda)$ *for every* $v \in S^{eff}$

Problem

Let A/F be an abelian variety over a number field F and let $P \in A(F)$ and let $\Lambda \subset A(F)$ be a subgroup. Is there an effectively computable finite set S^{eff} of primes v of $\mathcal{O}_F$, depending only on A, P and Λ such that the following conditions are equivalent? :

(1) $P \in \Lambda$

(2) $r_v(P) \in r_v(\Lambda)$ *for every* $v \in S^{eff}$

Problem

Let A/F be an abelian variety over a number field F and let $P \in A(F)$ and let $\Lambda \subset A(F)$ be a subgroup. Is there an effectively computable finite set S^{eff} of primes v of $\mathcal{O}_F$, depending only on A, P and Λ such that the following conditions are equivalent? :

(1) $P \in \Lambda$

(2) $r_v(P) \in r_v(\Lambda)$ *for every* $v \in S^{eff}$

THEOREM B (G.BANASZAK, P.KRASOŃ)

Let A/F satisfy the hypotheses of Theorem A. Let $P \in A(F)$ and let Λ be a subgroup of $A(F)$. There is a finite set of primes v of $\mathcal{O}_F$, such that the condition: $r_v(P) \in r_v(\Lambda)$ for all $v \in S^{fin}$ implies $P \in \Lambda + A(F)_{tor}$. Moreover if $A(F)_{tor} \subset \Lambda$, then the following conditions are equivalent:

(1) $P \in \Lambda$

(2) $r_v(P) \in r_v(\Lambda)$ *for* $v \in S^{fin}$.

THEOREM B (G.BANASZAK, P.KRASOŃ)

Let A/F satisfy the hypotheses of Theorem A. Let $P \in A(F)$ and let Λ be a subgroup of $A(F)$.There is a finite set of primes v of $\mathcal{O}_F$, such that the condition: $r_v(P) \in r_v(\Lambda)$ for all $v \in S^{fin}$ implies $P \in \Lambda + A(F)_{tor}$. Moreover if $A(F)_{tor} \subset \Lambda$, then the following conditions are equivalent:

(1) $P \in \Lambda$

(2) $r_v(P) \in r_v(\Lambda)$ *for* $v \in S^{fin}$.

THEOREM B (G.BANASZAK, P.KRASOŃ)

Let A/F satisfy the hypotheses of Theorem A. Let $P \in A(F)$ and let Λ be a subgroup of $A(F)$.There is a finite set of primes v of $\mathcal{O}_F$, such that the condition: $r_v(P) \in r_v(\Lambda)$ for all $v \in S^{fin}$ implies $P \in \Lambda + A(F)_{tor}$. Moreover if $A(F)_{tor} \subset \Lambda$, then the following conditions are equivalent:

(1) $P \in \Lambda$

(2) $r_v(P) \in r_v(\Lambda)$ *for* $v \in S^{fin}$.

Outline

Corollary (Weston)

Let A be an abelian variety defined over a number field such that $End_{\overline{F}}(A)$ is commutative. Then Theorem A holds for A.

Since $End_{\overline{F}}(A)$ is commutative,

A is isogeneous to $A_1 \times \cdots \times A_t$

with A_i simple, pairwise nonisogenous.

In this case the assumption of our theorem

$$dim_{End_{F'}(A_i)^0} H_1(A_i(\mathbb{C}); \mathbb{Q}) \geq 1$$

for each $1 \leq i \leq t$ always holds.

Since $End_{\overline{F}}(A)$ is commutative,

A is isogeneous to $A_1 \times \cdots \times A_t$

with A_i simple, pairwise nonisogenous.

In this case the assumption of our theorem

$$dim_{End_{F'}(A_i)^0} H_1(A_i(\mathbb{C}); \mathbb{Q}) \geq 1$$

for each $1 \leq i \leq t$ always holds.

Corollary

Let $A = E_1^{e_1} \times \cdots \times E_t^{e_t}$, where $E_1, \ldots, E_t$ are pairwise nonisogenous elliptic curves defined over F. Assume that $1 \leq e_i \leq 2$ if $End_F(E_i) = \mathbb{Z}$ and $e_i = 1$ if $End_F(E_i) \neq \mathbb{Z}$. Then Theorem A holds for A.

Corollary

Let $A = E_1^{e_1} \times \cdots \times E_t^{e_t}$, *where* $E_1, \ldots, E_t$ *are pairwise nonisogenous elliptic curves defined over* F. *Assume that* $1 \leq e_i \leq 2$ *if* $End_F(E_i) = \mathbb{Z}$ *and* $e_i = 1$ *if* $End_F(E_i) \neq \mathbb{Z}$. *Then Theorem A holds for A.*

Corollary

Let $A = E_1^{e_1} \times \cdots \times E_t^{e_t}$, *where* $E_1, \ldots, E_t$ *are pairwise nonisogenous elliptic curves defined over* F. *Assume that* $1 \leq e_i \leq 2$ *if* $End_F(E_i) = \mathbb{Z}$ *and* $e_i = 1$ *if* $End_F(E_i) \neq \mathbb{Z}$. *Then Theorem A holds for A.*

Observe that for an elliptic curve E/F we have

$dim_{End_F(E)^0} H_1(E(\mathbb{C}); \mathbb{Q}) = 2$ if $End_F(E) = \mathbb{Z}$

$dim_{End_F(E)^0} H_1(E(\mathbb{C}); \mathbb{Q}) = 1$ if $End_F(E) \neq \mathbb{Z}$ □

Observe that for an elliptic curve E/F we have

$dim_{End_F(E)^0} H_1(E(\mathbb{C}); \mathbb{Q}) = 2$ if $End_F(E) = \mathbb{Z}$

$dim_{End_F(E)^0} H_1(E(\mathbb{C}); \mathbb{Q}) = 1$ if $End_F(E) \neq \mathbb{Z}$ □

Observe that for an elliptic curve E/F we have

$dim_{End_F(E)^0} H_1(E(\mathbb{C}); \mathbb{Q}) = 2$ if $End_F(E) = \mathbb{Z}$

$dim_{End_F(E)^0} H_1(E(\mathbb{C}); \mathbb{Q}) = 1$ if $End_F(E) \neq \mathbb{Z}$ □

Outline

$E := E_d$ defined over $\mathbb{Q}$ $\quad y^2 = x^3 - d^2x$

E_d has *CM* by $\mathbb{Z}[i]$

K.Rubin, A.Silverberg showed that $rank E_d(\mathbb{Q})$ can reach 6.

$d = 34 \qquad rank E_d(\mathbb{Q}) = 2$

$d = 1254 \qquad rank E_d(\mathbb{Q}) = 3$

$d = 29274 \qquad rank E_d(\mathbb{Q}) = 4$

$d = 205015206 \qquad rank E_d(\mathbb{Q}) = 5$

$d = 61471349610 \qquad rank E_d(\mathbb{Q}) = 6$

$E := E_d$ defined over $\mathbb{Q}$ $\quad y^2 = x^3 - d^2x$

E_d has *CM* by $\mathbb{Z}[i]$

K.Rubin, A.Silverberg showed that $rank E_d(\mathbb{Q})$ can reach 6.

$d = 34 \qquad rank E_d(\mathbb{Q}) = 2$

$d = 1254 \qquad rank E_d(\mathbb{Q}) = 3$

$d = 29274 \qquad rank E_d(\mathbb{Q}) = 4$

$d = 205015206 \qquad rank E_d(\mathbb{Q}) = 5$

$d = 61471349610 \qquad rank E_d(\mathbb{Q}) = 6$

$E := E_d$ defined over $\mathbb{Q}$ $\quad y^2 = x^3 - d^2x$

E_d has *CM* by $\mathbb{Z}[i]$

K.Rubin, A.Silverberg showed that $rank E_d(\mathbb{Q})$ can reach 6.

$d = 34 \qquad rank E_d(\mathbb{Q}) = 2$

$d = 1254 \qquad rank E_d(\mathbb{Q}) = 3$

$d = 29274 \qquad rank E_d(\mathbb{Q}) = 4$

$d = 205015206 \qquad rank E_d(\mathbb{Q}) = 5$

$d = 61471349610 \qquad rank E_d(\mathbb{Q}) = 6$

$E := E_d$ defined over $\mathbb{Q}$ $\quad y^2 = x^3 - d^2x$

E_d has *CM* by $\mathbb{Z}[i]$

K.Rubin, A.Silverberg showed that $rank E_d(\mathbb{Q})$ can reach 6.

$d = 34 \qquad rank E_d(\mathbb{Q}) = 2$

$d = 1254 \qquad rank E_d(\mathbb{Q}) = 3$

$d = 29274 \qquad rank E_d(\mathbb{Q}) = 4$

$d = 205015206 \qquad rank E_d(\mathbb{Q}) = 5$

$d = 61471349610 \qquad rank E_d(\mathbb{Q}) = 6$

$E := E_d$ defined over $\mathbb{Q}$ $\quad y^2 = x^3 - d^2x$

E_d has *CM* by $\mathbb{Z}[i]$

K.Rubin, A.Silverberg showed that $rank E_d(\mathbb{Q})$ can reach 6.

$d = 34 \qquad rank E_d(\mathbb{Q}) = 2$

$d = 1254 \qquad rank E_d(\mathbb{Q}) = 3$

$d = 29274 \qquad rank E_d(\mathbb{Q}) = 4$

$d = 205015206 \qquad rank E_d(\mathbb{Q}) = 5$

$d = 61471349610 \qquad rank E_d(\mathbb{Q}) = 6$

$E := E_d$ defined over $\mathbb{Q}$ $\quad y^2 = x^3 - d^2x$

E_d has *CM* by $\mathbb{Z}[i]$

K.Rubin, A.Silverberg showed that $rank E_d(\mathbb{Q})$ can reach 6.

$d = 34 \qquad rank E_d(\mathbb{Q}) = 2$

$d = 1254 \qquad rank E_d(\mathbb{Q}) = 3$

$d = 29274 \qquad rank E_d(\mathbb{Q}) = 4$

$d = 205015206 \qquad rank E_d(\mathbb{Q}) = 5$

$d = 61471349610 \qquad rank E_d(\mathbb{Q}) = 6$

$E := E_d$ defined over $\mathbb{Q}$ $\quad y^2 = x^3 - d^2x$

E_d has *CM* by $\mathbb{Z}[i]$

K.Rubin, A.Silverberg showed that $rank E_d(\mathbb{Q})$ can reach 6.

$d = 34 \qquad rank E_d(\mathbb{Q}) = 2$

$d = 1254 \qquad rank E_d(\mathbb{Q}) = 3$

$d = 29274 \qquad rank E_d(\mathbb{Q}) = 4$

$d = 205015206 \qquad rank E_d(\mathbb{Q}) = 5$

$d = 61471349610 \qquad rank E_d(\mathbb{Q}) = 6$

$E := E_d$ defined over $\mathbb{Q}$ $\quad y^2 = x^3 - d^2x$

E_d has *CM* by $\mathbb{Z}[i]$

K.Rubin, A.Silverberg showed that $rank E_d(\mathbb{Q})$ can reach 6.

$d = 34 \qquad rank E_d(\mathbb{Q}) = 2$

$d = 1254 \qquad rank E_d(\mathbb{Q}) = 3$

$d = 29274 \qquad rank E_d(\mathbb{Q}) = 4$

$d = 205015206 \qquad rank E_d(\mathbb{Q}) = 5$

$d = 61471349610 \qquad rank E_d(\mathbb{Q}) = 6$

Let $A_d := E_d \times E_d$ defined over $\mathbb{Q}(i)$

PROPOSITION

There is a nontorsion point $P \in A_d(\mathbb{Q}(i))$ and a free $\mathbb{Z}[i]$-module $\Lambda \subset A_d(\mathbb{Q}(i))$ such that $P \notin \Lambda$ and $r_v(P) \in r_v(\Lambda)$ for all primes $v \nmid 2d$ in $\mathbb{Z}[i]$

Let $A_d := E_d \times E_d$ defined over $\mathbb{Q}(i)$

PROPOSITION

There is a nontorsion point $P \in A_d(\mathbb{Q}(i))$ and a free $\mathbb{Z}[i]$-module $\Lambda \subset A_d(\mathbb{Q}(i))$ such that $P \notin \Lambda$ and $r_v(P) \in r_v(\Lambda)$ for all primes $v \nmid 2d$ in $\mathbb{Z}[i]$

Since $rank E_d(\mathbb{Q}) \geq 2$ we can find $Q_1, Q_2 \in E_d(\mathbb{Q}(i))$ such that they are linearly independent over $\mathbb{Z}[i]$

$$P := \begin{bmatrix} 0 \\ Q_1 \end{bmatrix}, \; P_1 := \begin{bmatrix} Q_1 \\ 0 \end{bmatrix}, \; P_2 := \begin{bmatrix} Q_2 \\ Q_1 \end{bmatrix}, \; P_3 := \begin{bmatrix} 0 \\ Q_2 \end{bmatrix}.$$

$\Lambda := \mathbb{Z}[i]P_1 + \mathbb{Z}[i]P_2 + \mathbb{Z}[i]P_3 \subset A(\mathbb{Q}(i))$

Λ is free over $\mathbb{Z}[i]$ hence also free over $\mathbb{Z}$.

Λ is not free over $End_{\mathbb{Q}(i)} A = M_2(\mathbb{Z}[i])$.

$P \notin \Lambda$

Since $rank E_d(\mathbb{Q}) \geq 2$ we can find $Q_1, Q_2 \in E_d(\mathbb{Q}(i))$ such that they are linearly independent over $\mathbb{Z}[i]$

$$P := \begin{bmatrix} 0 \\ Q_1 \end{bmatrix}, \; P_1 := \begin{bmatrix} Q_1 \\ 0 \end{bmatrix}, \; P_2 := \begin{bmatrix} Q_2 \\ Q_1 \end{bmatrix}, \; P_3 := \begin{bmatrix} 0 \\ Q_2 \end{bmatrix}.$$

$\Lambda := \mathbb{Z}[i]P_1 + \mathbb{Z}[i]P_2 + \mathbb{Z}[i]P_3 \subset A(\mathbb{Q}(i))$

Λ is free over $\mathbb{Z}[i]$ hence also free over $\mathbb{Z}$.

Λ is not free over $End_{\mathbb{Q}(i)} A = M_2(\mathbb{Z}[i])$.

$P \notin \Lambda$

Since $rank E_d(\mathbb{Q}) \geq 2$ we can find $Q_1, Q_2 \in E_d(\mathbb{Q}(i))$ such that they are linearly independent over $\mathbb{Z}[i]$

$$P := \begin{bmatrix} 0 \\ Q_1 \end{bmatrix}, \; P_1 := \begin{bmatrix} Q_1 \\ 0 \end{bmatrix}, \; P_2 := \begin{bmatrix} Q_2 \\ Q_1 \end{bmatrix}, \; P_3 := \begin{bmatrix} 0 \\ Q_2 \end{bmatrix}.$$

$\Lambda := \mathbb{Z}[i]P_1 + \mathbb{Z}[i]P_2 + \mathbb{Z}[i]P_3 \subset A(\mathbb{Q}(i))$

Λ is free over $\mathbb{Z}[i]$ hence also free over $\mathbb{Z}$.

Λ is not free over $End_{\mathbb{Q}(i)} A = M_2(\mathbb{Z}[i])$.

$P \notin \Lambda$

Since $rank E_d(\mathbb{Q}) \geq 2$ we can find $Q_1, Q_2 \in E_d(\mathbb{Q}(i))$ such that they are linearly independent over $\mathbb{Z}[i]$

$$P := \begin{bmatrix} 0 \\ Q_1 \end{bmatrix}, \; P_1 := \begin{bmatrix} Q_1 \\ 0 \end{bmatrix}, \; P_2 := \begin{bmatrix} Q_2 \\ Q_1 \end{bmatrix}, \; P_3 := \begin{bmatrix} 0 \\ Q_2 \end{bmatrix}.$$

$\Lambda := \mathbb{Z}[i]P_1 + \mathbb{Z}[i]P_2 + \mathbb{Z}[i]P_3 \subset A(\mathbb{Q}(i))$

Λ is free over $\mathbb{Z}[i]$ hence also free over $\mathbb{Z}$.

Λ is not free over $End_{\mathbb{Q}(i)} A = M_2(\mathbb{Z}[i])$.

$P \notin \Lambda$

Since $rank E_d(\mathbb{Q}) \geq 2$ we can find $Q_1, Q_2 \in E_d(\mathbb{Q}(i))$ such that they are linearly independent over $\mathbb{Z}[i]$

$$P := \begin{bmatrix} 0 \\ Q_1 \end{bmatrix}, \; P_1 := \begin{bmatrix} Q_1 \\ 0 \end{bmatrix}, \; P_2 := \begin{bmatrix} Q_2 \\ Q_1 \end{bmatrix}, \; P_3 := \begin{bmatrix} 0 \\ Q_2 \end{bmatrix}.$$

$\Lambda := \mathbb{Z}[i]P_1 + \mathbb{Z}[i]P_2 + \mathbb{Z}[i]P_3 \subset A(\mathbb{Q}(i))$

Λ is free over $\mathbb{Z}[i]$ hence also free over $\mathbb{Z}$.

Λ is not free over $End_{\mathbb{Q}(i)} A = M_2(\mathbb{Z}[i])$.

$P \notin \Lambda$

Since $rank E_d(\mathbb{Q}) \geq 2$ we can find $Q_1, Q_2 \in E_d(\mathbb{Q}(i))$ such that they are linearly independent over $\mathbb{Z}[i]$

$$P := \begin{bmatrix} 0 \\ Q_1 \end{bmatrix}, \; P_1 := \begin{bmatrix} Q_1 \\ 0 \end{bmatrix}, \; P_2 := \begin{bmatrix} Q_2 \\ Q_1 \end{bmatrix}, \; P_3 := \begin{bmatrix} 0 \\ Q_2 \end{bmatrix}.$$

$\Lambda := \mathbb{Z}[i]P_1 + \mathbb{Z}[i]P_2 + \mathbb{Z}[i]P_3 \subset A(\mathbb{Q}(i))$

Λ is free over $\mathbb{Z}[i]$ hence also free over $\mathbb{Z}$.

Λ is not free over $End_{\mathbb{Q}(i)} A = M_2(\mathbb{Z}[i])$.

$P \notin \Lambda$

Let $\overline{Q_i} := r_v(Q_i)$ for $i = 1, 2$,

$\overline{P_i} := r_v(P_i)$ for $i = 1, 2, 3$ and $\overline{P} := r_v(P)$.

We will prove that $r_v(P) \in r_v(\Lambda)$ for all v of $\mathbb{Z}[i]$ over a prime $p \nmid 2d$.

The equation

$$\overline{P} = r_1\overline{P_1} + r_2\overline{P_2} + r_3\overline{P_3}.$$

in $E_v(k_v) \times E_v(k_v)$ with $r_1, r_2, r_3 \in \mathbb{Z}[i]$ is equivalent to a system of equations in $E_v(k_v)$:

$$r_1\overline{Q_1} + r_2\overline{Q_2} = 0$$

$$r_2\overline{Q_1} + r_3\overline{Q_2} = \overline{Q_1}$$

Let $\overline{Q_i} := r_v(Q_i)$ for $i = 1, 2$,

$\overline{P_i} := r_v(P_i)$ for $i = 1, 2, 3$ and $\overline{P} := r_v(P)$.

We will prove that $r_v(P) \in r_v(\Lambda)$ for all v of $\mathbb{Z}[i]$ over a prime $p \nmid 2d$.

The equation

$$\overline{P} = r_1\overline{P_1} + r_2\overline{P_2} + r_3\overline{P_3}.$$

in $E_v(k_v) \times E_v(k_v)$ with $r_1, r_2, r_3 \in \mathbb{Z}[i]$ is equivalent to a system of equations in $E_v(k_v)$:

$$r_1\overline{Q_1} + r_2\overline{Q_2} = 0$$

$$r_2\overline{Q_1} + r_3\overline{Q_2} = \overline{Q_1}$$

Let $\overline{Q_i} := r_v(Q_i)$ for $i = 1, 2$,

$\overline{P_i} := r_v(P_i)$ for $i = 1, 2, 3$ and $\overline{P} := r_v(P)$.

We will prove that $r_v(P) \in r_v(\Lambda)$ for all v of $\mathbb{Z}[i]$ over a prime $p \nmid 2d$.

The equation

$$\overline{P} = r_1\overline{P_1} + r_2\overline{P_2} + r_3\overline{P_3}.$$

in $E_v(k_v) \times E_v(k_v)$ with $r_1, r_2, r_3 \in \mathbb{Z}[i]$ is equivalent to a system of equations in $E_v(k_v)$:

$$r_1\overline{Q_1} + r_2\overline{Q_2} = 0$$

$$r_2\overline{Q_1} + r_3\overline{Q_2} = \overline{Q_1}$$

Let $\overline{Q_i} := r_v(Q_i)$ for $i = 1, 2$,

$\overline{P_i} := r_v(P_i)$ for $i = 1, 2, 3$ and $\overline{P} := r_v(P)$.

We will prove that $r_v(P) \in r_v(\Lambda)$ for all v of $\mathbb{Z}[i]$ over a prime $p \nmid 2d$.

The equation

$$\overline{P} = r_1\overline{P_1} + r_2\overline{P_2} + r_3\overline{P_3}.$$

in $E_v(k_v) \times E_v(k_v)$ with $r_1, r_2, r_3 \in \mathbb{Z}[i]$ is equivalent to a system of equations in $E_v(k_v)$:

$$r_1\overline{Q_1} + r_2\overline{Q_2} = 0$$

$$r_2\overline{Q_1} + r_3\overline{Q_2} = \overline{Q_1}$$

Let $\overline{Q_i} := r_v(Q_i)$ for $i = 1, 2$,

$\overline{P_i} := r_v(P_i)$ for $i = 1, 2, 3$ and $\overline{P} := r_v(P)$.

We will prove that $r_v(P) \in r_v(\Lambda)$ for all v of $\mathbb{Z}[i]$ over a prime $p \nmid 2d$.

The equation

$$\overline{P} = r_1\overline{P_1} + r_2\overline{P_2} + r_3\overline{P_3}.$$

in $E_v(k_v) \times E_v(k_v)$ with $r_1, r_2, r_3 \in \mathbb{Z}[i]$ is equivalent to a system of equations in $E_v(k_v)$:

$$r_1\overline{Q_1} + r_2\overline{Q_2} = 0$$

$$r_2\overline{Q_1} + r_3\overline{Q_2} = \overline{Q_1}$$

$$E_v(k_v) \cong \mathbb{Z}[i]/\gamma(v),$$

$c_1, c_2 \in \mathbb{Z}[i]$
$\overline{Q_1} = c_1 \bmod \gamma(v)$
$\overline{Q_2} = c_2 \bmod \gamma(v).$
the above system of equations is equivalent to the system of congruences in $\mathbb{Z}[i]/\gamma(v)$:

$$r_1 c_1 + r_2 c_2 \equiv 0 \bmod \gamma(v)$$

$$r_2 c_1 + r_3 c_2 \equiv c_1 \bmod \gamma(v).$$

If $c_1 \equiv 0 \bmod \gamma(v)$ or $c_2 \equiv 0 \bmod \gamma(v)$ then the last system of congruences trivially has a solution.

$$E_v(k_v) \cong \mathbb{Z}[i]/\gamma(v),$$

$c_1, c_2 \in \mathbb{Z}[i]$
$\overline{Q_1} = c_1 \bmod \gamma(v)$
$\overline{Q_2} = c_2 \bmod \gamma(v).$

the above system of equations is equivalent to the system of congruences in $\mathbb{Z}[i]/\gamma(v)$:

$$r_1 c_1 + r_2 c_2 \equiv 0 \bmod \gamma(v)$$

$$r_2 c_1 + r_3 c_2 \equiv c_1 \bmod \gamma(v).$$

If $c_1 \equiv 0 \bmod \gamma(v)$ or $c_2 \equiv 0 \bmod \gamma(v)$ then the last system of congruences trivially has a solution.

$$E_v(k_v) \cong \mathbb{Z}[i]/\gamma(v),$$

$c_1, c_2 \in \mathbb{Z}[i]$
$\overline{Q_1} = c_1 \bmod \gamma(v)$
$\overline{Q_2} = c_2 \bmod \gamma(v).$
the above system of equations is equivalent to the system of congruences in $\mathbb{Z}[i]/\gamma(v)$:

$$r_1 c_1 + r_2 c_2 \equiv 0 \bmod \gamma(v)$$

$$r_2 c_1 + r_3 c_2 \equiv c_1 \bmod \gamma(v).$$

If $c_1 \equiv 0 \bmod \gamma(v)$ or $c_2 \equiv 0 \bmod \gamma(v)$ then the last system of congruences trivially has a solution.

$$E_v(k_v) \cong \mathbb{Z}[i]/\gamma(v),$$

$c_1, c_2 \in \mathbb{Z}[i]$
$\overline{Q_1} = c_1 \bmod \gamma(v)$
$\overline{Q_2} = c_2 \bmod \gamma(v).$
the above system of equations is equivalent to the system of congruences in $\mathbb{Z}[i]/\gamma(v)$:

$$r_1 c_1 + r_2 c_2 \equiv 0 \bmod \gamma(v)$$

$$r_2 c_1 + r_3 c_2 \equiv c_1 \bmod \gamma(v).$$

If $c_1 \equiv 0 \bmod \gamma(v)$ or $c_2 \equiv 0 \bmod \gamma(v)$ then the last system of congruences trivially has a solution.

$$E_v(k_v) \cong \mathbb{Z}[i]/\gamma(v),$$

$c_1, c_2 \in \mathbb{Z}[i]$
$\overline{Q_1} = c_1 \bmod \gamma(v)$
$\overline{Q_2} = c_2 \bmod \gamma(v).$
the above system of equations is equivalent to the system of congruences in $\mathbb{Z}[i]/\gamma(v)$:

$$r_1 c_1 + r_2 c_2 \equiv 0 \bmod \gamma(v)$$

$$r_2 c_1 + r_3 c_2 \equiv c_1 \bmod \gamma(v).$$

If $c_1 \equiv 0 \bmod \gamma(v)$ or $c_2 \equiv 0 \bmod \gamma(v)$ then the last system of congruences trivially has a solution.

$c_1 \not\equiv 0 \bmod \gamma(v)$ and $c_2 \not\equiv 0 \bmod \gamma(v)$.

$D := gcd(c_1, c_2)$. Then

$$gcd\,(c_1^2/D,\, c_2) \;=\; D$$

and since $D \mid c_1$

the equation $r\, c_1^2/D + r_3 c_2 = c_1$
has a solution in $r,\ r_3 \in \mathbb{Z}[i]$.

$$r_1 := \frac{-rc_2}{D}, \quad r_2 := \frac{rc_1}{D}$$

$c_1 \not\equiv 0 \bmod \gamma(v)$ and $c_2 \not\equiv 0 \bmod \gamma(v)$.

$D := gcd(c_1, c_2)$. Then

$$gcd\left(c_1^2/D,\, c_2\right) \;=\; D$$

and since $D \mid c_1$

the equation $r\, c_1^2/D + r_3 c_2 = c_1$
has a solution in $r,\ r_3 \in \mathbb{Z}[i]$.

$$r_1 := \frac{-rc_2}{D}, \qquad r_2 := \frac{rc_1}{D}$$

$c_1 \not\equiv 0 \bmod \gamma(v)$ and $c_2 \not\equiv 0 \bmod \gamma(v)$.

$D := gcd(c_1, c_2)$. Then

$$gcd\,(c_1^2/D,\, c_2) \;=\; D$$

and since $D \mid c_1$

the equation $r\, c_1^2/D + r_3 c_2 = c_1$
has a solution in $r,\ r_3 \in \mathbb{Z}[i]$.

$$r_1 := \frac{-rc_2}{D}, \qquad r_2 := \frac{rc_1}{D}$$

$c_1 \not\equiv 0 \bmod \gamma(v)$ and $c_2 \not\equiv 0 \bmod \gamma(v)$.

$D := gcd(c_1, c_2)$. Then

$$gcd\left(c_1^2/D,\, c_2\right) \;=\; D$$

and since $D \mid c_1$

the equation $r\, c_1^2/D + r_3 c_2 = c_1$
has a solution in $r,\ r_3 \in \mathbb{Z}[i]$.

$$r_1 := \frac{-rc_2}{D}, \qquad r_2 := \frac{rc_1}{D}$$

$c_1 \not\equiv 0 \bmod \gamma(v)$ and $c_2 \not\equiv 0 \bmod \gamma(v)$.

$D := gcd(c_1, c_2)$. Then

$$gcd\,(c_1^2/D,\, c_2) \;=\; D$$

and since $D \mid c_1$

the equation $r\, c_1^2/D + r_3 c_2 = c_1$
has a solution in $r,\ r_3 \in \mathbb{Z}[i]$.

$$r_1 := \frac{-rc_2}{D}, \quad r_2 := \frac{rc_1}{D}$$

Outline

The methods of the proof of Main Theorem work for some algebraic tori over a number field F.

Let T/F be an algebraic torus and let F'/F be a finite extension that splits T.

Hence $T \otimes_F F' \cong \mathbb{G}_m^e := \underbrace{\mathbb{G}_m \times \cdots \times \mathbb{G}_m}_{e-times}$ where

$\mathbb{G}_m :=$ spec $F'[t, t^{-1}]$.

The methods of the proof of Main Theorem work for some algebraic tori over a number field F.

Let T/F be an algebraic torus and let F'/F be a finite extension that splits T.

Hence $T \otimes_F F' \cong \mathbb{G}_m^e := \underbrace{\mathbb{G}_m \times \cdots \times \mathbb{G}_m}_{e-times}$ where

$\mathbb{G}_m :=$ spec $F'[t, t^{-1}]$.

The methods of the proof of Main Theorem work for some algebraic tori over a number field F.

Let T/F be an algebraic torus and let F'/F be a finite extension that splits T.

Hence $T \otimes_F F' \cong \mathbb{G}_m^e := \underbrace{\mathbb{G}_m \times \cdots \times \mathbb{G}_m}_{e-times}$ where

$\mathbb{G}_m :=$ spec $F'[t, t^{-1}]$.

The methods of the proof of Main Theorem work for some algebraic tori over a number field F.

Let T/F be an algebraic torus and let F'/F be a finite extension that splits T.

Hence $T \otimes_F F' \cong \mathbb{G}_m^e := \underbrace{\mathbb{G}_m \times \cdots \times \mathbb{G}_m}_{e-times}$ where

$\mathbb{G}_m :=$ spec $F'[t, t^{-1}]$.

For any field extension $F' \subset M \subset \overline{F}$ we have $End_M(\mathbb{G}_m) = \mathbb{Z}$ and $H_1(\mathbb{G}_m(\mathbb{C}); \mathbb{Z}) = \mathbb{Z}$.

Hence the condition $e \leq dim_{End_{F'}(\mathbb{G}_m)^0} H_1(\mathbb{G}_m(\mathbb{C}); \mathbb{Q}) = 1$, analogous to the corresponding condition of our Theorem , means that $e = 1$.

Hence we can prove the analogue of the Main Theorem for one dimensional tori which is basically the A. Schinzel's Theorem .

The torsion ambiguity that appears in our Theorem can be in this case removed.

For any field extension $F' \subset M \subset \overline{F}$ we have $End_M(\mathbb{G}_m) = \mathbb{Z}$ and $H_1(\mathbb{G}_m(\mathbb{C}); \mathbb{Z}) = \mathbb{Z}$.

Hence the condition $e \leq dim_{End_{F'}(\mathbb{G}_m)^0} H_1(\mathbb{G}_m(\mathbb{C}); \mathbb{Q}) = 1$, analogous to the corresponding condition of our Theorem , means that $e = 1$.

Hence we can prove the analogue of the Main Theorem for one dimensional tori which is basically the A. Schinzel's Theorem .

The torsion ambiguity that appears in our Theorem can be in this case removed.

For any field extension $F' \subset M \subset \overline{F}$ we have $End_M(\mathbb{G}_m) = \mathbb{Z}$ and $H_1(\mathbb{G}_m(\mathbb{C}); \mathbb{Z}) = \mathbb{Z}$.

Hence the condition $e \leq dim_{End_{F'}(\mathbb{G}_m)^0} H_1(\mathbb{G}_m(\mathbb{C}); \mathbb{Q}) = 1$, analogous to the corresponding condition of our Theorem , means that $e = 1$.

Hence we can prove the analogue of the Main Theorem for one dimensional tori which is basically the A. Schinzel's Theorem .

The torsion ambiguity that appears in our Theorem can be in this case removed.

For any field extension $F' \subset M \subset \overline{F}$ we have $End_M(\mathbb{G}_m) = \mathbb{Z}$ and $H_1(\mathbb{G}_m(\mathbb{C}); \mathbb{Z}) = \mathbb{Z}$.

Hence the condition $e \leq dim_{End_{F'}(\mathbb{G}_m)^0} H_1(\mathbb{G}_m(\mathbb{C}); \mathbb{Q}) = 1$, analogous to the corresponding condition of our Theorem , means that $e = 1$.

Hence we can prove the analogue of the Main Theorem for one dimensional tori which is basically the A. Schinzel's Theorem .

The torsion ambiguity that appears in our Theorem can be in this case removed.

For any field extension $F' \subset M \subset \overline{F}$ we have $End_M(\mathbb{G}_m) = \mathbb{Z}$ and $H_1(\mathbb{G}_m(\mathbb{C}); \mathbb{Z}) = \mathbb{Z}$.

Hence the condition $e \leq dim_{End_{F'}(\mathbb{G}_m)^0} H_1(\mathbb{G}_m(\mathbb{C}); \mathbb{Q}) = 1$, analogous to the corresponding condition of our Theorem , means that $e = 1$.

Hence we can prove the analogue of the Main Theorem for one dimensional tori which is basically the A. Schinzel's Theorem .

The torsion ambiguity that appears in our Theorem can be in this case removed.

On the other hand A. Schinzel showed that his theorem does not extend in full generality to $\mathbb{G}_m/F \times \mathbb{G}_m/F$, hence it does not extend in full generality to algebraic tori T with $dim\ T > 1$.

The phrase *full generality* in the last sentence means *for any* $P \in T(F)$ *and any subgroup* $\Lambda \subset T(F)$.

On the other hand A. Schinzel showed that his theorem does not extend in full generality to $\mathbb{G}_m/F \times \mathbb{G}_m/F$, hence it does not extend in full generality to algebraic tori T with $dim\, T > 1$.

The phrase *full generality* in the last sentence means *for any* $P \in T(F)$ *and any subgroup* $\Lambda \subset T(F)$.

On the other hand A. Schinzel showed that his theorem does not extend in full generality to $\mathbb{G}_m/F \times \mathbb{G}_m/F$, hence it does not extend in full generality to algebraic tori T with $dim\, T > 1$.

The phrase *full generality* in the last sentence means *for any* $P \in T(F)$ *and any subgroup* $\Lambda \subset T(F)$.

Outline

Since the theorem is up to torsion we can assume $A = A_1^{e_1} \times \cdots \times A_t^{e_t}$

Put $c := |A(F)_{tor}|$ and $\Omega := c\,A(F)$.

Ω is torsion free.

we can assume $P \in \Omega, \quad P \neq 0, \Lambda \subset \Omega$ and $\Lambda \neq \{0\}$,

Let $P_1, \ldots, P_r, \ldots, P_s$ be such a $\mathbb{Z}$-basis of Ω that:

$$\Lambda = \mathbb{Z}d_1 P_1 + \cdots + \mathbb{Z}d_r P_r + \cdots + \mathbb{Z}d_s P_s.$$

where $d_i \in \mathbb{Z}\backslash\{0\}$ for $1 \leq i \leq r$ and $d_i = 0$ for $i > r$.

Since the theorem is up to torsion we can assume $A = A_1^{e_1} \times \cdots \times A_t^{e_t}$

Put $c := |A(F)_{tor}|$ and $\Omega := c\,A(F)$.

Ω is torsion free.

we can assume $P \in \Omega, \quad P \neq 0, \Lambda \subset \Omega$ and $\Lambda \neq \{0\}$,

Let $P_1, \ldots, P_r, \ldots, P_s$ be such a $\mathbb{Z}$-basis of Ω that:

$$\Lambda = \mathbb{Z}d_1P_1 + \cdots + \mathbb{Z}d_rP_r + \cdots + \mathbb{Z}d_sP_s.$$

where $d_i \in \mathbb{Z}\backslash\{0\}$ for $1 \leq i \leq r$ and $d_i = 0$ for $i > r$.

Since the theorem is up to torsion we can assume $A = A_1^{e_1} \times \cdots \times A_t^{e_t}$

Put $c := |A(F)_{tor}|$ and $\Omega := c\,A(F)$.

Ω is torsion free.

we can assume $P \in \Omega, \quad P \neq 0, \Lambda \subset \Omega$ and $\Lambda \neq \{0\}$,

Let $P_1, \ldots, P_r, \ldots, P_s$ be such a $\mathbb{Z}$-basis of Ω that:

$$\Lambda = \mathbb{Z}d_1 P_1 + \cdots + \mathbb{Z}d_r P_r + \cdots + \mathbb{Z}d_s P_s.$$

where $d_i \in \mathbb{Z}\backslash\{0\}$ for $1 \leq i \leq r$ and $d_i = 0$ for $i > r$.

Since the theorem is up to torsion we can assume $A = A_1^{e_1} \times \cdots \times A_t^{e_t}$

Put $c := |A(F)_{tor}|$ and $\Omega := c\,A(F)$.

Ω is torsion free.

we can assume $P \in \Omega, \quad P \neq 0, \Lambda \subset \Omega$ and $\Lambda \neq \{0\}$,

Let $P_1, \ldots, P_r, \ldots, P_s$ be such a $\mathbb{Z}$-basis of Ω that:

$$\Lambda = \mathbb{Z}d_1 P_1 + \cdots + \mathbb{Z}d_r P_r + \cdots + \mathbb{Z}d_s P_s.$$

where $d_i \in \mathbb{Z}\backslash\{0\}$ for $1 \leq i \leq r$ and $d_i = 0$ for $i > r$.

Since the theorem is up to torsion we can assume $A = A_1^{e_1} \times \cdots \times A_t^{e_t}$

Put $c := |A(F)_{tor}|$ and $\Omega := c\,A(F)$.

Ω is torsion free.

we can assume $P \in \Omega, \quad P \neq 0$, $\Lambda \subset \Omega$ and $\Lambda \neq \{0\}$,

Let $P_1, \ldots, P_r, \ldots, P_s$ be such a $\mathbb{Z}$-basis of Ω that:

$$\Lambda = \mathbb{Z}d_1 P_1 + \cdots + \mathbb{Z}d_r P_r + \cdots + \mathbb{Z}d_s P_s.$$

where $d_i \in \mathbb{Z}\backslash\{0\}$ for $1 \leq i \leq r$ and $d_i = 0$ for $i > r$.

Since the theorem is up to torsion we can assume $A = A_1^{e_1} \times \cdots \times A_t^{e_t}$

Put $c := |A(F)_{tor}|$ and $\Omega := c\,A(F)$.

Ω is torsion free.

we can assume $P \in \Omega, \quad P \neq 0, \Lambda \subset \Omega$ and $\Lambda \neq \{0\}$,

Let $P_1, \ldots, P_r, \ldots, P_s$ be such a $\mathbb{Z}$-basis of Ω that:

$$\Lambda = \mathbb{Z}d_1P_1 + \cdots + \mathbb{Z}d_rP_r + \cdots + \mathbb{Z}d_sP_s.$$

where $d_i \in \mathbb{Z}\backslash\{0\}$ for $1 \leq i \leq r$ and $d_i = 0$ for $i > r$.

put $\Omega_j := c\,A_j(F)$. Note that $\Omega = \bigoplus_{j=1}^{t} \Omega_j^{e_j}$.

For $P \in \Omega = \sum_{i=1}^{s} \mathbb{Z} P_i$ we write

$$P = n_1 P_1 + \cdots + n_r P_r + \cdots + n_s P_s$$

where $n_i \in \mathbb{Z}$

Let $K/\mathbb{Q}$ be a finite extension such that $D_i \otimes_{\mathbb{Q}} K \cong M_{d_i}(K)$ for each $1 \leq i \leq t$.
$D_i := \mathcal{R}_i \otimes_{\mathbb{Z}} \mathbb{Q}$

put $\Omega_j := c\,A_j(F)$. Note that $\Omega = \bigoplus_{j=1}^{t} \Omega_j^{e_j}$.

For $P \in \Omega = \sum_{i=1}^{s} \mathbb{Z} P_i$ we write

$$P = n_1 P_1 + \cdots + n_r P_r + \cdots + n_s P_s$$

where $n_i \in \mathbb{Z}$

Let $K/\mathbb{Q}$ be a finite extension such that $D_i \otimes_{\mathbb{Q}} K \cong M_{d_i}(K)$ for each $1 \leq i \leq t$.
$D_i := \mathcal{R}_i \otimes_{\mathbb{Z}} \mathbb{Q}$

put $\Omega_j := c\,A_j(F)$. Note that $\Omega = \bigoplus_{j=1}^{t} \Omega_j^{e_j}$.

For $P \in \Omega = \sum_{i=1}^{s} \mathbb{Z} P_i$ we write

$$P = n_1 P_1 + \cdots + n_r P_r + \cdots + n_s P_s$$

where $n_i \in \mathbb{Z}$

Let $K/\mathbb{Q}$ be a finite extension such that $D_i \otimes_{\mathbb{Q}} K \cong M_{d_i}(K)$ for each $1 \leq i \leq t$.

$D_i := \mathcal{R}_i \otimes_{\mathbb{Z}} \mathbb{Q}$

put $\Omega_j := c\,A_j(F)$. Note that $\Omega = \bigoplus_{j=1}^{t} \Omega_j^{e_j}$.

For $P \in \Omega = \sum_{i=1}^{s} \mathbb{Z} P_i$ we write

$$P = n_1 P_1 + \cdots + n_r P_r + \cdots + n_s P_s$$

where $n_i \in \mathbb{Z}$

Let $K/\mathbb{Q}$ be a finite extension such that $D_i \otimes_{\mathbb{Q}} K \cong M_{d_i}(K)$ for each $1 \leq i \leq t$.
$D_i := \mathcal{R}_i \otimes_{\mathbb{Z}} \mathbb{Q}$

Since $\Lambda \subset \Omega$ is a free subgroup of the free finitely generated abelian group Ω,

observe that $P \in \Lambda$ if and only if $P \otimes 1 \in \Lambda \otimes_{\mathbb{Z}} \mathcal{O}_K$.

The latter is equivalent to $P \otimes 1 \in \Lambda \otimes_{\mathbb{Z}} \mathcal{O}_\lambda$ for all prime ideals $\lambda \mid l$ in $\mathcal{O}_K$ and all prime numbers l.

Since $\Lambda \subset \Omega$ is a free subgroup of the free finitely generated abelian group Ω,

observe that $P \in \Lambda$ if and only if $P \otimes 1 \in \Lambda \otimes_{\mathbb{Z}} \mathcal{O}_K$.

The latter is equivalent to $P \otimes 1 \in \Lambda \otimes_{\mathbb{Z}} \mathcal{O}_\lambda$ for all prime ideals $\lambda \mid l$ in $\mathcal{O}_K$ and all prime numbers l.

Since $\Lambda \subset \Omega$ is a free subgroup of the free finitely generated abelian group Ω,

observe that $P \in \Lambda$ if and only if $P \otimes 1 \in \Lambda \otimes_{\mathbb{Z}} \mathcal{O}_K$.

The latter is equivalent to $P \otimes 1 \in \Lambda \otimes_{\mathbb{Z}} \mathcal{O}_\lambda$ for all prime ideals $\lambda \mid l$ in $\mathcal{O}_K$ and all prime numbers l.

Outline

Using Kummer maps for abelian varieties we prove the following:

Theorem

Let $Q_{ij} \in A_i(L)$ for $1 \leq j \leq r_i$ be independent over $\mathcal{R}_i$ for each $1 \leq i \leq t$. There is a family of primes w of $\mathcal{O}_L$ of positive density such that $r_w(Q_{ij}) = 0$ in $A_{i\,w}(k_w)_l$ for all $1 \leq j \leq r_i$ and $1 \leq i \leq t$.

Using Kummer maps for abelian varieties we prove the following:

Theorem

Let $Q_{ij} \in A_i(L)$ for $1 \leq j \leq r_i$ be independent over $\mathcal{R}_i$ for each $1 \leq i \leq t$. There is a family of primes w of $\mathcal{O}_L$ of positive density such that $r_w(Q_{ij}) = 0$ in $A_{i\,w}(k_w)_l$ for all $1 \leq j \leq r_i$ and $1 \leq i \leq t$.

Theorem

Let l be a prime number. Let $m \in \mathbb{N} \cup \{0\}$ for all $1 \leq j \leq r_i$ and $1 \leq i \leq t$. Let L/F be a finite extension and let $P_{ij} \in A_i(L)$ be independent over $\mathcal{R}_i$ and let $T_{ij} \in A_i[l^m]$ be aribitrary torsion elements for all $1 \leq j \leq r_i$ and $1 \leq i \leq t$. There is a family of primes w of $\mathcal{O}_L$ of positive density such that

$$r_{w'}(T_{ij}) = r_w(P_{ij}) \ \text{ in } \ A_{i,w}(k_w)_l$$

for all $1 \leq j \leq r_i$ and $1 \leq i \leq s$, where w' is a prime in $\mathcal{O}_{L(A_i[l^m])}$ over w and $r_{w'} : A_i(L(A_i[l^m])) \to A_{i,w}(k_{w'})$ is the corresponding reduction map.

Theorem

Let l be a prime number. Let $m \in \mathbb{N} \cup \{0\}$ for all $1 \leq j \leq r_i$ and $1 \leq i \leq t$.Let L/F be a finite extension and let $P_{ij} \in A_i(L)$ be independent over $\mathcal{R}_i$ and let $T_{ij} \in A_i[l^m]$ be aribitrary torsion elements for all $1 \leq j \leq r_i$ and $1 \leq i \leq t$.There is a family of primes w of $\mathcal{O}_L$ of positive density such that

$$r_{w'}(T_{ij}) = r_w(P_{ij}) \ \text{ in } \ A_{i,w}(k_w)_l$$

for all $1 \leq j \leq r_i$ and $1 \leq i \leq s$, where w' is a prime in $\mathcal{O}_{L(A_i[l^m])}$ over w and $r_{w'} : A_i(L(A_i[l^m])) \to A_{i,w}(k_{w'})$ is the corresponding reduction map.

Theorem

Let l be a prime number. Let $m \in \mathbb{N} \cup \{0\}$ for all $1 \leq j \leq r_i$ and $1 \leq i \leq t$.Let L/F be a finite extension and let $P_{ij} \in A_i(L)$ be independent over $\mathcal{R}_i$ and let $T_{ij} \in A_i[l^m]$ be aribitrary torsion elements for all $1 \leq j \leq r_i$ and $1 \leq i \leq t$.There is a family of primes w of $\mathcal{O}_L$ of positive density such that

$$r_{w'}(T_{ij}) = r_w(P_{ij}) \ \text{ in } \ A_{i,w}(k_w)_l$$

for all $1 \leq j \leq r_i$ and $1 \leq i \leq s$, where w' is a prime in $\mathcal{O}_{L(A_i[l^m])}$ over w and $r_{w'} : A_i(L(A_i[l^m])) \to A_{i,w}(k_{w'})$ is the corresponding reduction map.

Theorem

Let l be a prime number. Let $m \in \mathbb{N} \cup \{0\}$ for all $1 \leq j \leq r_i$ and $1 \leq i \leq t$.Let L/F be a finite extension and let $P_{ij} \in A_i(L)$ be independent over $\mathcal{R}_i$ and let $T_{ij} \in A_i[l^m]$ be aribitrary torsion elements for all $1 \leq j \leq r_i$ and $1 \leq i \leq t$.There is a family of primes w of $\mathcal{O}_L$ of positive density such that

$$r_{w'}(T_{ij}) = r_w(P_{ij}) \ \text{ in } \ A_{i,w}(k_w)_l$$

for all $1 \leq j \leq r_i$ and $1 \leq i \leq s$, where w' is a prime in $\mathcal{O}_{L(A_i[l^m])}$ over w and $r_{w'} : A_i(L(A_i[l^m])) \to A_{i,w}(k_{w'})$ is the corresponding reduction map.

Outline

Let D be a division algebra and let $K_i \subset M_e(D)$ denote the left ideal of $M_e(D)$ which consists of i-the column matrices of the form

$$\widetilde{\alpha}_i := \begin{bmatrix} 0 & \dots a_{1i} & \dots & 0 \\ 0 & \dots a_{2i} & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & \dots a_{ei} & \dots & 0 \end{bmatrix} \in K_i$$

For $\omega \in W$ put

$$\widetilde{\omega} := \begin{bmatrix} \omega \\ 0 \\ \vdots \\ 0 \end{bmatrix} \in W^e,$$

Theorem

Every nonzero simple submodule of the $M_e(D)$-module W^e has the following form

$$K_1\widetilde{\omega} = \{\widetilde{\alpha}_1\widetilde{\omega},\ \widetilde{\alpha}_1 \in K_1\} = \{\begin{bmatrix} a_{11}\,\omega \\ a_{21}\,\omega \\ \vdots \\ a_{e1}\,\omega \end{bmatrix},\ a_{i1} \in D,\ 1 \leq i \leq e\}$$

for some $\omega \in W$.

Let D_i be a finite dimensional division algebra over $\mathbb{Q}$ for every $1 \leq i \leq t$.

The trace homomorphisms: $tr_i : M_{e_i}(D_i) \to \mathbb{Q}$, for all $1 \leq i \leq t$, give the trace homomorphism $tr : \mathbb{M}_e(\mathbb{D}) \to \mathbb{Q}$, where $tr := \sum_{i=1}^{t} tr_i$.

Let W_i be a finite dimensional D_i-vector space for each $1 \leq i \leq t$. Then W is a finitely generated $\mathbb{M}_e(\mathbb{D})$-module.

The homomorphism tr gives a natural map of $\mathbb{Q}$-vector spaces

$$tr : Hom_{\mathbb{M}_e(\mathbb{D})}(W, \mathbb{M}_e(\mathbb{D})) \to Hom_{\mathbb{Q}}(W, \mathbb{Q}).$$

Let D_i be a finite dimensional division algebra over $\mathbb{Q}$ for every $1 \leq i \leq t$.

The trace homomorphisms: $tr_i : M_{e_i}(D_i) \to \mathbb{Q}$, for all $1 \leq i \leq t$, give the trace homomorphism $tr : \mathbb{M}_e(\mathbb{D}) \to \mathbb{Q}$, where $tr := \sum_{i=1}^{t} tr_i$.

Let W_i be a finite dimensional D_i-vector space for each $1 \leq i \leq t$. Then W is a finitely generated $\mathbb{M}_e(\mathbb{D})$-module.

The homomorphism tr gives a natural map of $\mathbb{Q}$-vector spaces

$$tr : Hom_{\mathbb{M}_e(\mathbb{D})}(W, \mathbb{M}_e(\mathbb{D})) \to Hom_{\mathbb{Q}}(W, \mathbb{Q}).$$

Let D_i be a finite dimensional division algebra over $\mathbb{Q}$ for every $1 \leq i \leq t$.

The trace homomorphisms: $tr_i : M_{e_i}(D_i) \to \mathbb{Q}$, for all $1 \leq i \leq t$, give the trace homomorphism $tr : \mathbb{M}_e(\mathbb{D}) \to \mathbb{Q}$, where $tr := \sum_{i=1}^{t} tr_i$.

Let W_i be a finite dimensional D_i-vector space for each $1 \leq i \leq t$. Then W is a finitely generated $\mathbb{M}_e(\mathbb{D})$-module.

The homomorphism tr gives a natural map of $\mathbb{Q}$-vector spaces

$$tr : Hom_{\mathbb{M}_e(\mathbb{D})}(W, \mathbb{M}_e(\mathbb{D})) \to Hom_{\mathbb{Q}}(W, \mathbb{Q}).$$

Let D_i be a finite dimensional division algebra over $\mathbb{Q}$ for every $1 \leq i \leq t$.

The trace homomorphisms: $tr_i : M_{e_i}(D_i) \to \mathbb{Q}$, for all $1 \leq i \leq t$, give the trace homomorphism $tr : \mathbb{M}_e(\mathbb{D}) \to \mathbb{Q}$, where $tr := \sum_{i=1}^{t} tr_i$.

Let W_i be a finite dimensional D_i-vector space for each $1 \leq i \leq t$. Then W is a finitely generated $\mathbb{M}_e(\mathbb{D})$-module.

The homomorphism tr gives a natural map of $\mathbb{Q}$-vector spaces

$$tr : Hom_{\mathbb{M}_e(\mathbb{D})}(W, \mathbb{M}_e(\mathbb{D})) \to Hom_{\mathbb{Q}}(W, \mathbb{Q}).$$

Lemma

The map tr is an isomorphism.

Outline

Assume $P \notin \Lambda$ $P \otimes 1 \notin \Lambda \otimes_{\mathbb{Z}} \mathcal{O}_\lambda$ for some $\lambda \mid l$ for some prime number l.

Hence $n_j \neq 0$ for some $1 \leq j \leq s$ in the expression

$$P = n_1 P_1 + \cdots + n_r P_r + \cdots + n_s P_s$$

Consider the equality in $\Omega \otimes_{\mathbb{Z}} \mathcal{O}_K$.

Since $P \notin \Lambda \otimes_{\mathbb{Z}} \mathcal{O}_\lambda$ then there is $1 \leq j_0 \leq s$ such that $\lambda^{m_1} \mid\mid n_{j_0}$ and $\lambda^{m_2} \mid d_{j_0}$ for natural numbers $m_1 < m_2$.

Consider the map of $\mathbb{Z}$-modules

$$\pi : \Omega \to \mathbb{Z}$$

$$\pi(R) := \mu_{j_0}$$

for $R = \sum_{i=1}^{s} \mu_i P_i$ with $\mu_i \in \mathbb{Z}$ for all $1 \leq i \leq s$.

Assume $P \notin \Lambda$ $P \otimes 1 \notin \Lambda \otimes_{\mathbb{Z}} \mathcal{O}_\lambda$ for some $\lambda \mid l$ for some prime number l.

Hence $n_j \neq 0$ for some $1 \leq j \leq s$ in the expression

$$P = n_1 P_1 + \cdots + n_r P_r + \cdots + n_s P_s$$

Consider the equality in $\Omega \otimes_{\mathbb{Z}} \mathcal{O}_K$.

Since $P \notin \Lambda \otimes_{\mathbb{Z}} \mathcal{O}_\lambda$ then there is $1 \leq j_0 \leq s$ such that $\lambda^{m_1} \mid\mid n_{j_0}$ and $\lambda^{m_2} \mid d_{j_0}$ for natural numbers $m_1 < m_2$.

Consider the map of $\mathbb{Z}$-modules

$$\pi : \Omega \to \mathbb{Z}$$

$$\pi(R) := \mu_{j_0}$$

for $R = \sum_{i=1}^{s} \mu_i P_i$ with $\mu_i \in \mathbb{Z}$ for all $1 \leq i \leq s$.

Assume $P \notin \Lambda$ $P \otimes 1 \notin \Lambda \otimes_{\mathbb{Z}} \mathcal{O}_\lambda$ for some $\lambda \mid l$ for some prime number l.

Hence $n_j \neq 0$ for some $1 \leq j \leq s$ in the expression

$$P = n_1 P_1 + \cdots + n_r P_r + \cdots + n_s P_s$$

Consider the equality in $\Omega \otimes_{\mathbb{Z}} \mathcal{O}_K$.

Since $P \notin \Lambda \otimes_{\mathbb{Z}} \mathcal{O}_\lambda$ then there is $1 \leq j_0 \leq s$ such that $\lambda^{m_1} \mid\mid n_{j_0}$ and $\lambda^{m_2} \mid d_{j_0}$ for natural numbers $m_1 < m_2$.

Consider the map of $\mathbb{Z}$-modules

$$\pi : \Omega \to \mathbb{Z}$$

$$\pi(R) := \mu_{j_0}$$

for $R = \sum_{i=1}^{s} \mu_i P_i$ with $\mu_i \in \mathbb{Z}$ for all $1 \leq i \leq s$.

Assume $P \notin \Lambda\ P \otimes 1 \notin \Lambda \otimes_{\mathbb{Z}} \mathcal{O}_\lambda$ for some $\lambda \mid l$ for some prime number l.

Hence $n_j \neq 0$ for some $1 \leq j \leq s$ in the expression

$$P = n_1 P_1 + \cdots + n_r P_r + \cdots + n_s P_s$$

Consider the equality in $\Omega \otimes_{\mathbb{Z}} \mathcal{O}_K$.

Since $P \notin \Lambda \otimes_{\mathbb{Z}} \mathcal{O}_\lambda$ then there is $1 \leq j_0 \leq s$ such that $\lambda^{m_1} \mid\mid n_{j_0}$ and $\lambda^{m_2} \mid d_{j_0}$ for natural numbers $m_1 < m_2$.

Consider the map of $\mathbb{Z}$-modules

$$\pi : \Omega \to \mathbb{Z}$$

$$\pi(R) := \mu_{j_0}$$

for $R = \sum_{i=1}^{s} \mu_i P_i$ with $\mu_i \in \mathbb{Z}$ for all $1 \leq i \leq s$.

Assume $P \notin \Lambda$ $P \otimes 1 \notin \Lambda \otimes_{\mathbb{Z}} \mathcal{O}_\lambda$ for some $\lambda \mid l$ for some prime number l.

Hence $n_j \neq 0$ for some $1 \leq j \leq s$ in the expression

$$P = n_1 P_1 + \cdots + n_r P_r + \cdots + n_s P_s$$

Consider the equality in $\Omega \otimes_{\mathbb{Z}} \mathcal{O}_K$.

Since $P \notin \Lambda \otimes_{\mathbb{Z}} \mathcal{O}_\lambda$ then there is $1 \leq j_0 \leq s$ such that $\lambda^{m_1} \mid\mid n_{j_0}$ and $\lambda^{m_2} \mid d_{j_0}$ for natural numbers $m_1 < m_2$.

Consider the map of $\mathbb{Z}$-modules

$$\pi \ : \ \Omega \to \mathbb{Z}$$

$$\pi(R) := \mu_{j_0}$$

for $R = \sum_{i=1}^{s} \mu_i P_i$ with $\mu_i \in \mathbb{Z}$ for all $1 \leq i \leq s$.

Lift $\pi \otimes \mathbb{Q}$ (by last Lemma) to

$$\widetilde{\pi} \in Hom_{\mathbb{M}_e(\mathbb{D})}(\Omega \otimes_{\mathbb{Z}} \mathbb{Q},\ \mathbb{M}_e(\mathbb{D}))$$

$\widetilde{s} \in Hom_{\mathbb{M}_e(\mathbb{D})}(\mathrm{Im}\widetilde{\pi},\ \Omega \otimes_{\mathbb{Z}} \mathbb{Q})$ such that $\widetilde{\pi} \circ \widetilde{s} = Id$.

Choose, for each $1 \leq i \leq t$, a lattice $\mathcal{L}'_i \subset \mathcal{L}_i$ such that $\mathcal{L}'_i$ is a free $\mathcal{R}_i$-module.

$\mathcal{L}_i$ - Riemann lattice $(A_i(\mathbb{C}) = \mathbb{C}^g/\mathcal{L}_i)$

Put $\mathcal{L} := \bigoplus_{i=1}^{t} \mathcal{L}_i$ and $\mathcal{L}' := \bigoplus_{i=1}^{t} \mathcal{L}'_i$.

Lift $\pi \otimes \mathbb{Q}$ (by last Lemma) to

$$\widetilde{\pi} \in Hom_{\mathbb{M}_e(\mathbb{D})}(\Omega \otimes_{\mathbb{Z}} \mathbb{Q},\ \mathbb{M}_e(\mathbb{D}))$$

$\widetilde{s} \in Hom_{\mathbb{M}_e(\mathbb{D})}(\mathrm{Im}\widetilde{\pi},\ \Omega \otimes_{\mathbb{Z}} \mathbb{Q})$ such that $\widetilde{\pi} \circ \widetilde{s} = Id$.

Choose, for each $1 \leq i \leq t$, a lattice $\mathcal{L}'_i \subset \mathcal{L}_i$ such that $\mathcal{L}'_i$ is a free $\mathcal{R}_i$-module.

$\mathcal{L}_i$ - Riemann lattice ($A_i(\mathbb{C}) = \mathbb{C}^g/\mathcal{L}_i$)

Put $\mathcal{L} := \bigoplus_{i=1}^{t} \mathcal{L}_i$ and $\mathcal{L}' := \bigoplus_{i=1}^{t} \mathcal{L}'_i$.

Lift $\pi \otimes \mathbb{Q}$ (by last Lemma) to

$$\widetilde{\pi} \in Hom_{\mathbb{M}_e(\mathbb{D})}(\Omega \otimes_{\mathbb{Z}} \mathbb{Q},\ \mathbb{M}_e(\mathbb{D}))$$

$\widetilde{s} \in Hom_{\mathbb{M}_e(\mathbb{D})}(\mathrm{Im}\widetilde{\pi},\ \Omega \otimes_{\mathbb{Z}} \mathbb{Q})$ such that $\widetilde{\pi} \circ \widetilde{s} = Id$.

Choose, for each $1 \leq i \leq t$, a lattice $\mathcal{L}'_i \subset \mathcal{L}_i$ such that $\mathcal{L}'_i$ is a free $\mathcal{R}_i$-module.

$\mathcal{L}_i$ - Riemann lattice ($A_i(\mathbb{C}) = \mathbb{C}^g/\mathcal{L}_i$)

Put $\mathcal{L} := \bigoplus_{i=1}^{t} \mathcal{L}_i$ and $\mathcal{L}' := \bigoplus_{i=1}^{t} \mathcal{L}'_i$.

Lift $\pi \otimes \mathbb{Q}$ (by last Lemma) to

$$\widetilde{\pi} \in \mathit{Hom}_{\mathbb{M}_e(\mathbb{D})}(\Omega \otimes_{\mathbb{Z}} \mathbb{Q},\ \mathbb{M}_e(\mathbb{D}))$$

$\widetilde{s} \in \mathit{Hom}_{\mathbb{M}_e(\mathbb{D})}(\mathrm{Im}\widetilde{\pi},\ \Omega \otimes_{\mathbb{Z}} \mathbb{Q})$ such that $\widetilde{\pi} \circ \widetilde{s} = \mathit{Id}$.

Choose, for each $1 \leq i \leq t$, a lattice $\mathcal{L}'_i \subset \mathcal{L}_i$ such that $\mathcal{L}'_i$ is a free $\mathcal{R}_i$-module.

$\mathcal{L}_i$ - Riemann lattice ($A_i(\mathbb{C}) = \mathbb{C}^g/\mathcal{L}_i$)

Put $\mathcal{L} := \bigoplus_{i=1}^{t} \mathcal{L}_i$ and $\mathcal{L}' := \bigoplus_{i=1}^{t} \mathcal{L}'_i$.

Lift $\pi \otimes \mathbb{Q}$ (by last Lemma) to

$$\widetilde{\pi} \in Hom_{\mathbb{M}_e(\mathbb{D})}(\Omega \otimes_{\mathbb{Z}} \mathbb{Q},\ \mathbb{M}_e(\mathbb{D}))$$

$\widetilde{s} \in Hom_{\mathbb{M}_e(\mathbb{D})}(\mathrm{Im}\widetilde{\pi},\ \Omega \otimes_{\mathbb{Z}} \mathbb{Q})$ such that $\widetilde{\pi} \circ \widetilde{s} = Id$.

Choose, for each $1 \leq i \leq t$, a lattice $\mathcal{L}'_i \subset \mathcal{L}_i$ such that $\mathcal{L}'_i$ is a free $\mathcal{R}_i$-module.

$\mathcal{L}_i$ - Riemann lattice ($A_i(\mathbb{C}) = \mathbb{C}^g/\mathcal{L}_i$)

Put $\mathcal{L} := \bigoplus_{i=1}^{t} \mathcal{L}_i$ and $\mathcal{L}' := \bigoplus_{i=1}^{t} \mathcal{L}'_i$.

Analyze

$$z(n,\lambda) : \mathcal{L}' \otimes_{\mathbb{Z}} \mathcal{O}_\lambda / \lambda^{\epsilon n} \mathcal{L}' \otimes_{\mathbb{Z}} \mathcal{O}_\lambda \to \mathcal{L} \otimes_{\mathbb{Z}} \mathcal{O}_\lambda / \lambda^{\epsilon n} \mathcal{L} \otimes_{\mathbb{Z}} \mathcal{O}_\lambda,$$

$l\,\mathcal{O}_K = \prod_{\lambda | l} \lambda^{\epsilon}$,

Here we need dimension condition

Use the reduction theorem

Analyze

$$z(n,\lambda) : \mathcal{L}' \otimes_{\mathbb{Z}} \mathcal{O}_\lambda / \lambda^{\epsilon n} \mathcal{L}' \otimes_{\mathbb{Z}} \mathcal{O}_\lambda \to \mathcal{L} \otimes_{\mathbb{Z}} \mathcal{O}_\lambda / \lambda^{\epsilon n} \mathcal{L} \otimes_{\mathbb{Z}} \mathcal{O}_\lambda,$$

$l\,\mathcal{O}_K = \prod_{\lambda \mid l} \lambda^{\epsilon}$,

Here we need dimension condition

Use the reduction theorem

Analyze

$$z(n,\lambda) : \mathcal{L}' \otimes_{\mathbb{Z}} \mathcal{O}_\lambda / \lambda^{\epsilon n} \mathcal{L}' \otimes_{\mathbb{Z}} \mathcal{O}_\lambda \to \mathcal{L} \otimes_{\mathbb{Z}} \mathcal{O}_\lambda / \lambda^{\epsilon n} \mathcal{L} \otimes_{\mathbb{Z}} \mathcal{O}_\lambda,$$

$l\,\mathcal{O}_K = \prod_{\lambda \mid l} \lambda^{\epsilon}$,

Here we need dimension condition

Use the reduction theorem

Analyze

$$z(n,\lambda) : \mathcal{L}' \otimes_{\mathbb{Z}} \mathcal{O}_\lambda / \lambda^{\epsilon n} \mathcal{L}' \otimes_{\mathbb{Z}} \mathcal{O}_\lambda \to \mathcal{L} \otimes_{\mathbb{Z}} \mathcal{O}_\lambda / \lambda^{\epsilon n} \mathcal{L} \otimes_{\mathbb{Z}} \mathcal{O}_\lambda,$$

$l\,\mathcal{O}_K = \prod_{\lambda \mid l} \lambda^{\epsilon}$,

Here we need dimension condition

Use the reduction theorem

By Reduction Theorem there is a set of primes w of $\mathcal{O}_L$ of positive density such that $r_w(\omega_k(i)) = 0$ for $1 \leq i \leq t$, $k_i + 1 \leq k \leq u_i$
and $r_w(\omega_k(i)) = r_w(T_k(i))$ for all $1 \leq i \leq t$, $1 \leq k \leq k_i$.

Choose such a prime w. Since $r_w(P) \in r_w(\Lambda)$ we take $Q \in \Lambda$ such that $r_w(P) = r_w(Q)$. Applying the reduction map r_w to the equation

$$M_2(P-Q) = \sum_{i=1}^{t}\sum_{k=1}^{k_i}(\alpha_k(i)_1 - \beta_k(i)_1)M_0\omega_k(i)$$

$$+\sum_{i=1}^{t}\sum_{k=k_i+1}^{u_i}(\alpha_k(i)_1 - \beta_k(i)_1)\omega_k(i),$$

we obtain

$$0 = \sum_{i=1}^{t}\sum_{k=1}^{k_i}(\alpha_k(i)_1 - \beta_k(i)_1)M_0\, r_w(\boldsymbol{T}_k(i)).$$

Since r_w is injective on torsion we have

$$0 = \sum_{i=1}^{t} \sum_{k=1}^{k_i} (\alpha_k(i)_1 - \beta_k(i)_1) M_0 \, \boldsymbol{T}_k(i).$$

and thus

$$\alpha_k(i) - \beta_k(i) \in \lambda^{an+b} K(i)_{1,\lambda}$$

On the other hand

$$\alpha_k(i) - \beta_k(i) \notin \lambda^{m_2} K(i)_{1,\lambda}$$

This part is P.K. Yuval Flicker

Theorem (Schinzel)

Let F be a number field, and $D > 0$ a rational integer. Let T be the torus $\mathbb{G}_m^n$. Fix $t_1, \ldots, t_r, t_0$ in $T(F)$. Suppose for each ideal $\mathfrak{m}$ in the ring $\mathcal{O}$ of integers of F, that is prime to D, there are $x_{1,\mathfrak{m}} \ldots, x_{r,\mathfrak{m}}$ in $\mathbb{Z}$ such that $t_1^{x_{1,\mathfrak{m}}} \cdots t_r^{x_{r,\mathfrak{m}}} \equiv t_0 (\mathrm{mod}\, \mathfrak{m})$. Then there are $x_1, \ldots, x_r \in \mathbb{Z}$ with $t_1^{x_1} \cdots t_r^{x_r} = t_0$.

Conjecture

Let F be a number field. Let G be a linear algebraic group over $\mathcal{O}$, viewed as a subgroup of some matrix group $\mathrm{GL}(n)$. Fix g_1, $\ldots$, g_r, g_0 in $G(F)$. Let $D > 0$ a rational integer, depending on $g_1, \ldots, g_r$. Suppose for each ideal $\mathfrak{m}$ in the ring $\mathcal{O}$ of integers of F, that is prime to D, there are $x_{1,\mathfrak{m}} \ldots, x_{r,\mathfrak{m}}$ in $\mathbb{Z}$ such that $g_1^{x_{1,\mathfrak{m}}} \cdots g_r^{x_{r,\mathfrak{m}}} \equiv g_0 (\mathrm{mod}\, \mathfrak{m})$. Then there are $x_1, \ldots, x_r \in \mathbb{Z}$ with $g_1^{x_1} \cdots g_r^{x_r} = g_0$.

If $g_i = \begin{pmatrix} 1 & u_i \\ 0 & 1 \end{pmatrix}$, when $F = \mathbb{Q}$ Conjecture states the following.

PROPOSITION

Suppose $u_0, u_1, \ldots, u_r$ are nonzero rational integers. Let $D > 0$ be an integer prime to the g.c.d. $u = (u_1, \ldots, u_r)$. Suppose for each $m > 1$ prime to D there are integers $x_{i,m}$ $(1 \leq i \leq r)$ with $x_{1,m}u_1 + \cdots + x_{r,m}u_r \equiv u_0 (\mathrm{mod}\, m)$. Then there are integers x_i $(1 \leq i \leq r)$ with $x_1 u_1 + \cdots + x_r u_r = u_0$.

If $g_i = \begin{pmatrix} 1 & u_i \\ 0 & 1 \end{pmatrix}$, when $F = \mathbb{Q}$ Conjecture states the following.

PROPOSITION

Suppose $u_0, u_1, \ldots, u_r$ are nonzero rational integers. Let $D > 0$ be an integer prime to the g.c.d. $u = (u_1, \ldots, u_r)$. Suppose for each $m > 1$ prime to D there are integers $x_{i,m}$ $(1 \leq i \leq r)$ with $x_{1,m}u_1 + \cdots + x_{r,m}u_r \equiv u_0 (\mathrm{mod}\, m)$. Then there are integers x_i $(1 \leq i \leq r)$ with $x_1 u_1 + \cdots + x_r u_r = u_0$.

When G is a Heisenberg group, say the unipotent radical of the upper triangular subgroup of SL(3), the following question comes up, first again in the context of integers. Suppose, instead of $u_0, u_1, \ldots, u_r$, say we have two sequences of integers $u_0, u_1, \ldots, u_r$ and $v_0, v_1, \ldots, v_r$; and for D prime to $(u_1, \ldots, u_r)$ and $(v_1, \ldots, v_r)$, for each m prime to D the equations $x_{1,m}u_1 + \cdots + x_{r,m}u_r \equiv u_0 (\mathrm{mod}\, m)$ and $x_{1,m}v_1 + \cdots + x_{r,m}v_r \equiv v_0 (\mathrm{mod}\, m)$ are solvable, with the same integral x's.

Thus $x_{i,m}$ are the same for the u's and for the v's. Then there is a solution to $x_1 u_1 + \cdots + x_r u_r = u_0$ and to $y_1 v_1 + \cdots + y_r v_r = v_0$. We should be able to choose $y_i = x_i$. Is this true? Yes it is, even more generally, in the context of G being the unipotent radical U of the upper triangular subgroup of SL(n).

Regarding the above diagonal, that is, the derived group $U/[U,U]$ of U, we have, in the context of $F = \mathbb{Q}$:

PROPOSITION

Suppose $u_{0,j}, u_{1,j}, \ldots, u_{r,j}$ $(1 \leq j < n)$ are nonzero integers. Let $D > 0$ be an integer prime to the g.c.d. $u_j = (u_{1,j}, \ldots, u_{r,j})$, all j. Suppose for each $m > 1$ prime to D there are integers $x_{i,m}$ $(1 \leq i \leq r)$ with $x_{1,m}u_{1,j} + \cdots + x_{r,m}u_{r,j} \equiv u_{0,j} \pmod{m}$ for all j. Then there are integers x_i $(1 \leq i \leq r)$ with $x_1 u_{1,j} + \cdots + x_r u_{r,j} = u_{0,j}$.

Regarding the above diagonal, that is, the derived group $U/[U,U]$ of U, we have, in the context of $F = \mathbb{Q}$:

PROPOSITION

Suppose $u_{0,j}, u_{1,j}, \ldots, u_{r,j}$ $(1 \leq j < n)$ are nonzero integers. Let $D > 0$ be an integer prime to the g.c.d. $u_j = (u_{1,j}, \ldots, u_{r,j})$, all j. Suppose for each $m > 1$ prime to D there are integers $x_{i,m}$ $(1 \leq i \leq r)$ with $x_{1,m}u_{1,j} + \cdots + x_{r,m}u_{r,j} \equiv u_{0,j} (\mathrm{mod}\, m)$ for all j. Then there are integers x_i $(1 \leq i \leq r)$ with $x_1 u_{1,j} + \cdots + x_r u_{r,j} = u_{0,j}$.

Theorem

Let Γ be a subgroup of $\mathrm{SL}(n, \mathcal{O})$ of finite index. Let ϕ be a nontrivial homomorphism from Γ to Γ. Suppose there is an infinite set S of prime ideals $\mathfrak{p}$ of $\mathcal{O}$ with the following property. For all $\mathfrak{p}$ in S, the homomorphism ϕ factors to give an homomorphism $\phi_{\mathfrak{p}} : \mathrm{SL}(n, \mathcal{O}/\mathfrak{p}) \to \mathrm{SL}(n, \mathcal{O}/\mathfrak{p})$, thus the following diagram exists and is commutative:

$$\begin{array}{ccc} \Gamma & \xrightarrow{\phi} & \Gamma \\ \downarrow{\scriptstyle \mathrm{mod}\,\mathfrak{p}} & & \downarrow{\scriptstyle \mathrm{mod}\,\mathfrak{p}} \\ \mathrm{SL}(n, \mathcal{O}/\mathfrak{p}) & \xrightarrow{\phi_{\mathfrak{p}}} & \mathrm{SL}(n, \mathcal{O}/\mathfrak{p}) \end{array}$$

Moreover, suppose $\phi_{\mathfrak{p}}$ is inner, thus $\phi_{\mathfrak{p}}(g) = \mathrm{Int}(x)g := xgx^{-1}$, for some $x = x(\phi_{\mathfrak{p}})$ in $\mathrm{GL}(n, \mathcal{O}/\mathfrak{p})$, for all $\mathfrak{p} \in S$. Then ϕ is an automorphism of Γ which is the restriction to Γ of the inner-conjugation action by an element of $\mathrm{GL}(n, F)$.

Proof:
Put $B = \prod_{\mathfrak{p} \in S} \mathcal{O}/\mathfrak{p}$. The ring $\mathcal{O}$ embeds in the ring B. Hence there is an injection $\mathrm{SL}(n, \mathcal{O}) \hookrightarrow \mathrm{SL}(n, B)$. So ϕ lies in a commutative diagram

$$\begin{array}{ccc} \Gamma & \xrightarrow{\phi} & \Gamma \\ \downarrow & & \downarrow \\ \mathrm{SL}(n, B) & \xrightarrow{\prod_{\mathfrak{p}} \phi_{\mathfrak{p}}} & \mathrm{SL}(n, B). \end{array}$$

and it is locally inner. Hence the representation $\phi : \Gamma \to \mathrm{GL}(n, F)$ and the identity – natural embedding – representation $\mathrm{id} : \Gamma \to \mathrm{GL}(n, F)$, have equal traces.

But id is irreducible, hence ϕ and id are conjugate by an element of $\mathrm{GL}(n, F)$, namely ϕ is the restriction to Γ of $\mathrm{Int}(x)$, for some $x \in \mathrm{GL}(n, F)$, and $\mathrm{Int}(x)$ takes Γ to itself.

But the index $[\mathrm{SL}(n, \mathcal{O}) : \Gamma]$ equals $[\mathrm{SL}(n, \mathcal{O}) : \mathrm{Int}(x)\Gamma]$, hence $\phi = \mathrm{Int}(x)$ is an automorphism of Γ.

and it is locally inner. Hence the representation $\phi : \Gamma \to \mathrm{GL}(n, F)$ and the identity – natural embedding – representation $\mathrm{id} : \Gamma \to \mathrm{GL}(n, F)$, have equal traces.

But id is irreducible, hence ϕ and id are conjugate by an element of $\mathrm{GL}(n, F)$, namely ϕ is the restriction to Γ of $\mathrm{Int}(x)$, for some $x \in \mathrm{GL}(n, F)$, and $\mathrm{Int}(x)$ takes Γ to itself.

But the index $[\mathrm{SL}(n, \mathcal{O}) : \Gamma]$ equals $[\mathrm{SL}(n, \mathcal{O}) : \mathrm{Int}(x)\Gamma]$, hence $\phi = \mathrm{Int}(x)$ is an automorphism of Γ.

and it is locally inner. Hence the representation $\phi : \Gamma \to \mathrm{GL}(n, F)$ and the identity – natural embedding – representation $\mathrm{id} : \Gamma \to \mathrm{GL}(n, F)$, have equal traces.

But id is irreducible, hence ϕ and id are conjugate by an element of $\mathrm{GL}(n, F)$, namely ϕ is the restriction to Γ of $\mathrm{Int}(x)$, for some $x \in \mathrm{GL}(n, F)$, and $\mathrm{Int}(x)$ takes Γ to itself.

But the index $[\mathrm{SL}(n, \mathcal{O}) : \Gamma]$ equals $[\mathrm{SL}(n, \mathcal{O}) : \mathrm{Int}(x)\Gamma]$, hence $\phi = \mathrm{Int}(x)$ is an automorphism of Γ.