Hermite の 5次方程式の標準形と versal S_5-曲面

Shinzo Bannai

Tokyo Metropolitan University

Contents

Introduction

- X, Y: normal algebraic varieties.
- $\pi : X \to Y$: finite surjective morphism.

$\Rightarrow$ π induces a finite extension of function fields $\mathbb{C}(X)/\mathbb{C}(Y)$.

<u>Definition</u>.

$\pi : X \to Y$ *is a Galois cover*

$\Leftrightarrow$ $\mathbb{C}(X)/\mathbb{C}(Y)$ *is a Galois extension.*

Notation:

$\pi : X \to Y$ is a G-cover

$\Leftrightarrow \pi$ is a Galois cover and

$\mathrm{Gal}(\mathbb{C}(X)/\mathbb{C}(Y)) \cong G$.

If $\pi : X \to Y$ is a G-cover, then
- $G \curvearrowright X$,
- $Y \cong X/G$, and
- $X \cong \tilde{Y}$ where $\tilde{Y}$ is the $\mathbb{C}(X)$-normalization of Y.

Definition.

X is a G-variety
$\Leftrightarrow X$ is a normal algebraic variety with faithful G-action, (i.e. $G \hookrightarrow \mathrm{Aut}(X)$)

X : G-variety,
$\pi : X \to X/G$: quotient morphism,
$\Rightarrow \pi : X \to X/G$ is a G-cover.

Definition.

$\mathrm{Fix}(X, G) = \{x \in X | G_x \neq \{1\}\}$

<u>Problem</u> 1.

- Y : normal projective variety
- G : finite group

Give a method to construct a G-cover

$$\pi : X \to Y,$$

over Y.

Problem 2. "Inverse Galois problem"

- K : field
- G : finite group

Give a method to construct a Galois extension K'/K of K such that $\mathrm{Gal}(K'/K) \cong G$.

The study of Galois covers is the geometric version of Galois theory.

Versal Galois covers

and

Versal G-varieties

Namba's Pull back construction

A method to construct new G-covers from known one's.

- $\pi : X \to Y$: G-cover
- W: normal algebraic variety

$$\begin{array}{ccc} & & X \\ & & \downarrow{\scriptstyle \pi} \\ W & & Y \end{array}$$

Namba's Pull back construction

A method to construct new G-covers from known one's.

- $\pi : X \to Y$: G-cover
- W: normal algebraic variety

If a G-indecomposable rational map $\nu : W \dashrightarrow Y$ exists,

$$\begin{array}{ccc} & & X \\ & & \downarrow \pi \\ W & \overset{}{\underset{\nu}{\dashrightarrow}} & Y \end{array}$$

Namba's Pull back construction

A method to construct new G-covers from known one's.

- $\pi : X \to Y$: G-cover
- W: normal algebraic variety

If a G-indecomposable rational map $\nu : W \dashrightarrow Y$ exists, then we can "pull back" the G-cover over Y, and construct a G-cover over W.

$$\begin{array}{ccc} Z & \overset{\mu}{\dashrightarrow} & X \\ {\scriptstyle \pi'}\downarrow & & \downarrow{\scriptstyle \pi} \\ W & \underset{\nu}{\dashrightarrow} & Y \end{array}$$

Definition.

$\varpi : X \to Y$ *is a versal* G*-cover*

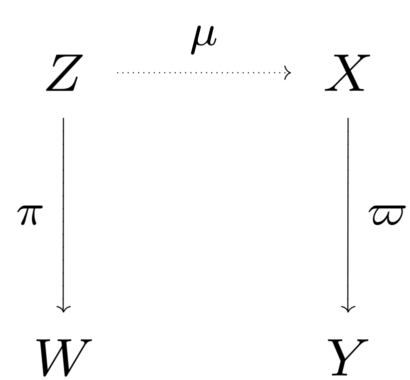
$\Leftrightarrow$ $\varpi : X \to Y$ *is a* G*-cover and*

$$\begin{array}{c} X \\ \Big\downarrow \varpi \\ Y \end{array}$$

Definition.
$\varpi : X \to Y$ *is a versal* G*-cover*
$\Leftrightarrow$ $\varpi : X \to Y$ *is a* G*-cover and for*
$\forall \pi : Z \to W$*:* G*-cover,*

$$\begin{array}{ccc} Z & & X \\ \pi \downarrow & & \downarrow \varpi \\ W & & Y \end{array}$$

Definition.
$\varpi : X \to Y$ *is a versal* G*-cover*
$\Leftrightarrow \varpi : X \to Y$ *is a* G*-cover and for*
$\forall \pi : Z \to W$*:* G*-cover,*
$\exists \mu : Z \dashrightarrow X$*:* G*-equivariant rational map*
such that $\mu(Z) \not\subset \mathrm{Fix}(X, G)$*.*



Definition.
$\varpi : X \to Y$ is a versal G-cover
$\Leftrightarrow$ $\varpi : X \to Y$ is a G-cover and for
$\forall \pi : Z \to W$: G-cover,
$\exists \mu : Z \dashrightarrow X$: G-equivariant rational map
such that $\mu(Z) \not\subset$ Fix(X, G).

$$\begin{array}{ccc} Z & \overset{\mu}{\dashrightarrow} & X \\ {\scriptstyle \pi}\downarrow & & \downarrow{\scriptstyle \varpi} \\ W & \underset{\nu}{\dashrightarrow} & Y \end{array}$$

ν is a G-indecomposable map and
$\pi : Z \to W$ can be recovered by Namba's method.

Definition.

X: G-*variety*

X *is a versal* G-*variety*

$\Leftrightarrow \pi : X \to X/G$ *is a versal* G-*cover.*

Remark 1.

X *is a versal* G-*variety*

$\Leftrightarrow \forall Z$: G-*variety,*

$\exists \mu : Z \dashrightarrow X$:G-*equivariant rational map*

such that $\nu(Z) \not\subset \mathrm{Fix}(X, G)$

Theorem 1 (M. Namba).

G : *finite group*

$\Rightarrow \exists X$: *versal G-variety.*

$X = (\mathbb{P}^1)^{|G|}$,
$G \curvearrowright (\mathbb{P}^1)^{|G|}$: permutation of coordinates.

Find a versal G-variety

Find a versal G-variety

$$\Downarrow$$

Compute the quotient

Find a versal G-variety

$\Downarrow$

Compute the quotient

$\Downarrow$

Use Namba's method to construct new G-varieties

<u>Definition</u> (essential dimension).

$\mathrm{ed}_{\mathbb{C}}(G) = \min\{\dim X | X$: *versal G-variety*$\}$

- X: versal G-variety

$\dim X = \mathrm{ed}_{\mathbb{C}}(G) = 1$

$\Rightarrow X = \mathbb{P}^1$, $G \cong C_n$ or D_{2n} (n: odd)

$\dim X = \mathrm{ed}_{\mathbb{C}}(G) = 2$
$\Rightarrow X$: rational
$G \cong D_{2n}$ (n: even), A_4, S_4, A_5, S_5,$C_2 \times C_2$,
. . .

Basic properties of versal G-varieties

- $\rho : G \hookrightarrow \mathrm{GL}(n, \mathbb{C})$: faithful irr. rep.
- X: G-variety

Fact 1.

X is versal

$\Leftrightarrow\ \exists\ \mu : \mathbb{C}^n \dashrightarrow X$

G-equivariant rational map

Remark 2.

$\mathbb{C}^n$ is a versal G-variety

- X: G-variety
- $H \subset G$: subgroup of G

Fact 2.

X: versal G-variety

$\Rightarrow X$: versal H-variety

Fact 3.
X: versal G-surface
$\Rightarrow X$ is a rational surface

Versal S_5-surfaces

Classify versal G-surfaces.

$$\Updownarrow$$

$$\begin{cases} \bullet \textbf{ Classify birational } G\textbf{-actions of } \mathbb{P}^2. \\ \bullet \textbf{ Determine which of them are versal}. \end{cases}$$

The group of birational automorphisms of $\mathbb{P}^2$ is called the **Cremona group of the plane**, denoted by $\mathrm{Cr}_2(\mathbb{C})$.

The classification of conjugacy classes of finite subgroups of $Cr_2(\mathbb{C})$ is finished.

J. Blanc: abelian case (2006)
Dolgachev–Iskovskikh: non-abelian case (2006)

$\underline{G \cong S_5}$

By **Dolgachev–Iskovskikh**(2006) there are three distinct conjugacy classes of S_5 in $\mathrm{Cr}_2(\mathbb{C})$.

- $X_1 = \mathbb{P}^1 \times \mathbb{P}^1$
- X_2: del Pezzo surface of degree 5
- X_3: del Pezzo surface of degree 3

Case 1. $X_1 = \mathbb{P}^1 \times \mathbb{P}^1$

- $A_5 \hookrightarrow \mathrm{Aut}(\mathbb{P}^1)$

Define $A_5 \curvearrowright \mathbb{P}^1 \times \mathbb{P}^1$ by

$$g(x,y) \mapsto (g(x),(12)g(12)(y)) \qquad g \in A_5$$

- $\sigma : \mathbb{P}^1 \times \mathbb{P}^1$, $\sigma(x,y) \mapsto (y,x)$

Then $G = \langle A_5, \Sigma \rangle = S_5$.

Lemma 1.

X_1 is not a versal S_5-surface.

- $p_1 : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^1$, $(x, y) \mapsto x$

faithful S_5-equivariant morphism

X_1 versal $S_5 \Rightarrow X_1$ versal $A_5 \Rightarrow \mathbb{P}^1$ versal A_5

- $\mathrm{ed}_{\mathbb{C}}(A_5) = 2 > \dim \mathbb{P}^1 = 1$

Case 2. X_2 del Pezzo surface of degree 5

$P_1 = [1,0,0], P_2 = [0,1,0], P_3 = [0,0,1], P_4 = [1,1,1] \in \mathbb{P}^2$.

- $\exists S_4 \hookrightarrow \mathrm{Aut}(\mathbb{P}^2)_{\{P_1,P_2,P_3,P_4\}}$.
- τ: standard Cremona transformation

$$[x,y,z] \dashrightarrow [yz,zx,xy]$$

X_2: blow up of $\mathbb{P}^2$ at $\{P_1,P_2,P_3,P_4\}$. Then S_4 and τ lift to automorphisms of X_2 and

$$G = \langle S_4, \tau\rangle \cong S_5 \hookrightarrow \mathrm{Aut}(X_2)$$

<u>or</u>

X_2 is isomorphic to

$$\bar{\mathcal{M}}_{0,5} = (\mathbb{P}^1)^5 /\!/ \mathrm{SL}(2)$$

The moduli space of five points on $\mathbb{P}^1$.

S_5 acts by permutating the factors of $(\mathbb{P}^1)^5$.

Lemma 2.

X_2 is a versal S_5-surface.

- $(\mathbb{P}^1)^5$ is a versal S_5-surface.
- $X_2 \cong (\mathbb{P}^1)^5 /\!/ \mathrm{SL}(2)$.

Case 3. X_3:del Pezzo surface of degree 3

- $[x_0, x_1, x_2, x_3, x_4]$: hom. coord. of $\mathbb{P}^4$.
- $S_5 \curvearrowright \mathbb{P}^4$ permutation of coordinates.

$$X_3 : \sum_{i=0}^{4} x_i = \sum_{i=0}^{4} x_i^3 = 0$$

Then X_3 is a del Pezzo surface of degree 3 and $S_5 \curvearrowright X_3$.

Lemma 3.

X_3 is a versal S_5-surface.

Theorem 2.

Let X be a versal S_5-surface, then X is birationally equivalent to X_2 or X_3 as G-surfaces.

$G_1 \cong G_2 \cong C_2 \times C_2$,

$G_1 \subset A_5$

$G_2 \not\subset A_5$

Corollary 1.

X_3 considered as a G_i-variety is versal.

The two $C_2 \times C_2$-varieties are birationally distinct.

proof of Lemma 3.

Hermite's standard form for quintics

Theorem 3 (Hermite).

L/K: seperable extension, $[L:K]=5$.
$\Rightarrow \exists \xi \in L$ such that $L=K(\xi)$ and
the minimal polynomial of ξ over K is

$$T^5+bT^3+dT+e=0$$

$X_3 \subset \mathbb{P}^4$

$$\sum_{i=0}^{4} x_i = \sum_{i=0}^{4} x_i^3 = 0$$

Recall

X is a versal S_5-variety

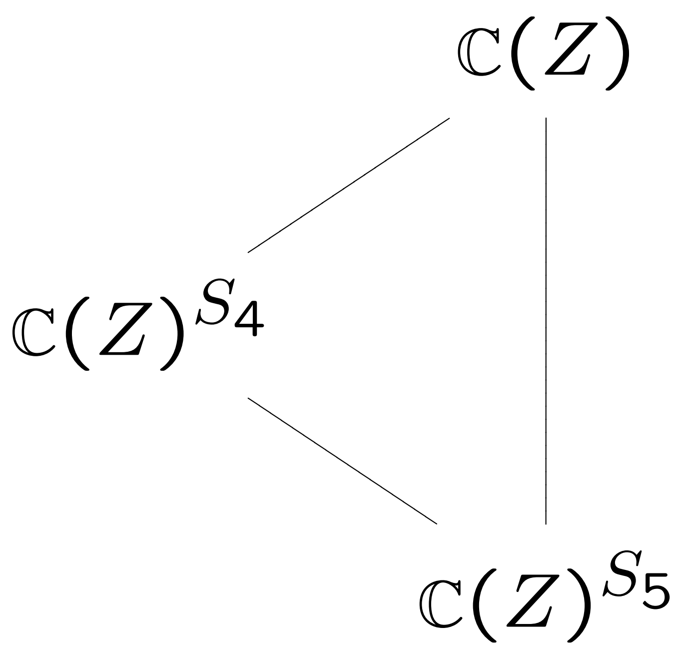
$\Leftrightarrow \forall Z$: S_5-variety,

$\exists \mu : Z \dashrightarrow X$:S_5-equivariant rational map

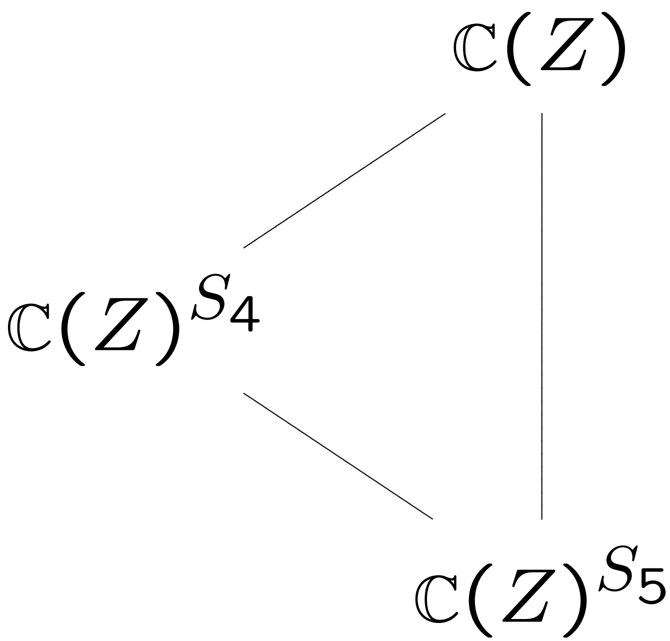
such that $\nu(Z) \not\subset \mathrm{Fix}(X, G)$

Z: S_5-variety
$\mathbb{C}(Z)$: function field of Z.

Z: S_5-variety
$\mathbb{C}(Z)$: function field of Z.

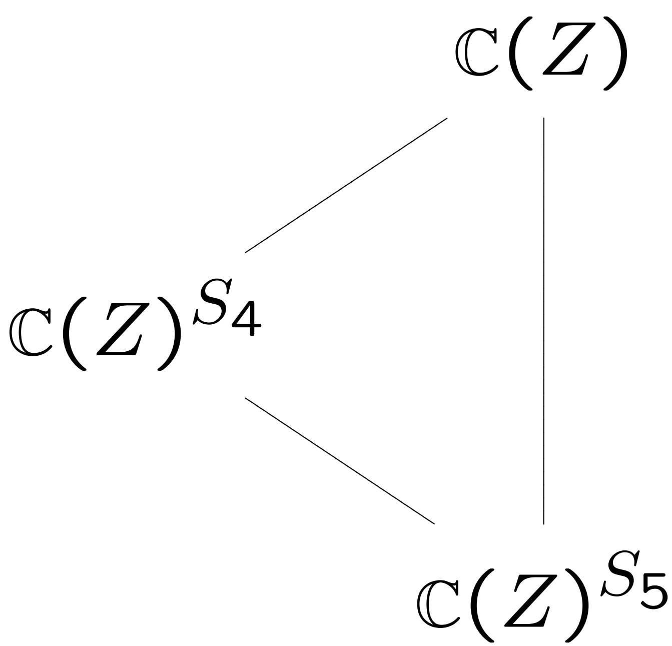


Z: S_5-variety
$\mathbb{C}(Z)$: function field of Z.



$$[\mathbb{C}(Z)^{S_4} : \mathbb{C}(Z)^{S_5}] = 5$$

Z: S_5-variety
$\mathbb{C}(Z)$: function field of Z.



$$[\mathbb{C}(Z)^{S_4} : \mathbb{C}(Z)^{S_5}] = 5$$
$$\Downarrow$$
$\exists \xi \in \mathbb{C}(Z)^{S_4}$ such that
$$\xi^5 + b\xi^3 + dx + e = 0$$

$\xi = \xi_0, \xi_1, \xi_2, \xi_3, \xi_4$: elements conjugate to ξ.

$$\prod_{i=0}^{5} (T - \xi_i) = T^5 + bT^3 + dT + e$$

$\xi = \xi_0, \xi_1, \xi_2, \xi_3, \xi_4$: elements conjugate to ξ.

$$\prod_{i=0}^{5} (T - \xi_i) = T^5 + cT^3 + dT + e$$

$$\Downarrow$$

$$\sum_{i=0}^{4} \xi_i = \sum_{i=0}^{4} \xi_i^3 = 0$$

Define $\mu : Z \dashrightarrow \mathbb{P}^4$ by

$$z \mapsto \mu(z) = [\xi_0(z), \xi_1(z), \xi_2(z), \xi_3(z), \xi_4(z)]$$

Then μ is S_5-equivariant and

$$\mu(Z) \subset X_3$$

since

$$\sum_{i=0}^{4} \xi_i = \sum_{i=0}^{4} \xi_i^3 = 0$$

$\square$

Remark 3.

If we consider

$$T^5 + cT^2 + dT + e = 0$$

we get

$$\sum_{i=0}^{4} \xi_i = \sum \xi_i \xi_j = 0$$

This equation defines an S_5-surface isomorphic to X_1, which is not versal.

Tschirnhaus transformations

covariants and

versal G-varieties

<u>Theorem</u> (Hermite).

L/K: seperable extension, $[L:K] = 5$.

$\Rightarrow \exists \xi \in L$ such that $L = K(\xi)$ and

the minimal polynomial of ξ over K is

$$T^5 + aT^3 + bT + c = 0$$

Tschirnhaus transformations and covariants

$\mathbb{A}^n$: affine n-space

G: finite group

Define $G \curvearrowright \mathbb{A}^n$ by permutation of coordinates

Definition.

A G-covariant Φ is a G-equivariant morphism

$$\Phi : \mathbb{A}^n \longrightarrow \mathbb{A}^n$$

$$\bar{a} = (a_1, \ldots, a_n) \mapsto \Phi(\bar{a}) = (\Phi_1(\bar{a}), \ldots, \Phi_n(\bar{a}))$$

S_n-covariant $\Leftrightarrow$ Tschirnhaus transformation

H. Kraft, **A result of Hermite and equations of degree 5 and 6**

P_n: set of monic polynomials of degree n

$p : \mathbb{A}^n \longrightarrow P_n$, $(a_1, \ldots, a_n) \mapsto \Pi(T - a_i)$

$\Phi : \mathbb{A}^n \longrightarrow \mathbb{A}^n$: S_n-covariant

$$\begin{array}{ccc} \mathbb{A}^n & \xrightarrow{\Phi} & \mathbb{A}^n \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle p} \\ P_n & \xrightarrow{\tilde{\Phi}} & P_n \end{array}$$

$f \in P_n(K)$: polynomial of degree n

L/K: splitting field of f

$G = \mathrm{Gal}(L/K)$

$$f = \prod (T - \eta_i), \quad \eta_i \in L$$

Φ_K: covariant defined over K
$\Rightarrow \Phi_L : L^n \to L^n$ is G-equivariant
$\Rightarrow \{(\Phi_L)_i(\bar{\eta})\}$ are conjugate over K
$\Rightarrow \tilde{f} = \prod (T - (\Phi_L)_i(\bar{\eta})) \in P_n(K)$

$\tilde{\Phi}_K : P_n \to P_n,\ f \mapsto \tilde{f}$ is called the

Tschirnhaus transformation associated to Φ_K.

Similarly by a G-covariant, we get a Tschirnhaus transformation for polynomials with Galois group G.

G-covariant over $\mathbb{C}$ $\Leftrightarrow$ versal G-variety

- $\rho : G \hookrightarrow \mathrm{GL}(n, \mathbb{C})$: faithful irr. rep.
- X: G-variety, $\dim(X) = \mathrm{ed}_{\mathbb{C}}(G)$

Fact 1.

X is versal

$\Leftrightarrow \exists \ \mu : \mathbb{C}^n \dashrightarrow X$

G-equivariant rational map

$$\Phi : \mathbb{C}^n \longrightarrow \mathbb{C}^n\text{: } G\text{-covariant over } \mathbb{C}$$

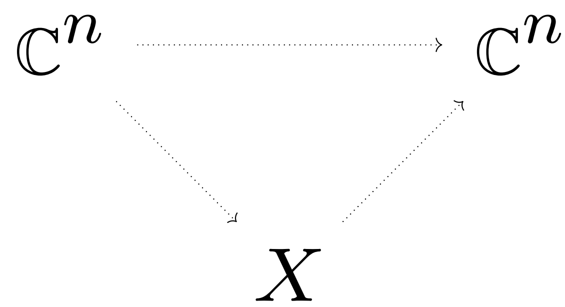
$$\Downarrow$$

$$\overline{\Phi(\mathbb{C}^n)} \subset \mathbb{C}^n \text{ is a versal } G\text{-variety}$$

$$X\text{: versal } G\text{-variety}$$

$$\Downarrow$$

$$\exists \mu : \mathbb{C}^n \dashrightarrow X$$

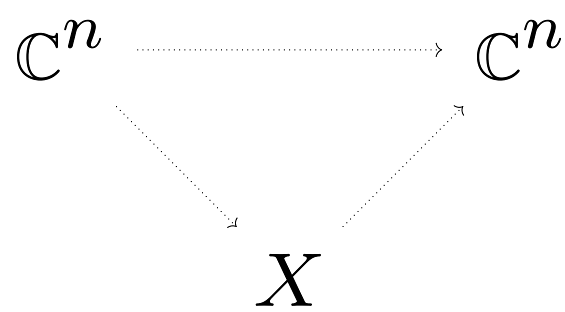


If we can find G-equivariant rational map,

$$\nu : X \dashrightarrow \mathbb{C}^n$$

Then we get a rational covariant

$$\Phi : \mathbb{C}^n \dashrightarrow \mathbb{C}^n$$



If we can find G-equivariant rational map,

$$\nu : X \dashrightarrow \mathbb{C}^n$$

Then we get a rational covariant

$$\Phi : \mathbb{C}^n \dashrightarrow \mathbb{C}^n$$

Rational Tschirnhaus transformation

$$\Updownarrow$$

Rational G-Covariant

$$\Updownarrow$$

Versal G-variety

Theorem **(Hermite).**

L/K: *seperable extension,* $[L:K]=5$.

$\Rightarrow \exists\xi \in L$ *such that* $L = K(\xi)$ *and the minimal polynomial of* ξ *over* K *is*

$$T^5 + aT^3 + bT + c = 0$$

Theorem (Hermite).

There is a S_5 *covariant* $\Phi : \mathbb{A}^n \longrightarrow \mathbb{A}^n$ *defined over* $\mathbb{Z}$ *such that*

$$\sum \Phi_i = \Phi_i^3 = 0$$

Theorem.

X_3: *is a versal* S_5*-surface*

Examples

Example 1.

$$T^n + a_{n-2}T^{n-2} + \cdots + a_1 T + a_0 = 0$$

$$\Updownarrow$$

$S_n \curvearrowright \mathbb{P}^n$: permutation of coordinates

$\mathbb{P}^{n-1} \subset \mathbb{P}^n : \sum x_i = 0$ is versal

Algebraic Torus

$N \cong \mathbb{Z}^n$, $M \cong \mathrm{Hom}_{\mathbb{Z}}(N, \mathbb{Z})$,

$T_N = \mathrm{Spec}\, \mathbb{C}[M] = \mathrm{Spec}\, \mathbb{C}[X_1^{\pm}, \ldots, X_n^{\pm}]$

$T_N = (\mathbb{C}^*)^n$: algebraic torus of dimension n

$G \subset \mathrm{Aut}_{\mathbb{Z}}(N)$: finite subgroup

Let $g = A = (a_{ij})$. We can define a G-action on T_N by

$$(X_k)^g = \prod X_l^{a_{lk}}$$

<u>Theorem</u> 4.

T_N *with above* G*-action is a versal* G*-variety.*

<u>Remark</u> 4.

Let $\rho : G \hookrightarrow \mathsf{GL}(s, \mathbb{Q})$ be a linear rep.

It can be shown that there exists a G-equivariant rational map $\mu : \mathbb{Q}^s \dashrightarrow T_N$ defined over $\mathbb{Q}$.

G acts on $\mathbb{C}[M]$ by permutating monomials.

$\{\underline{X}^{a_1}, \ldots, \underline{X}^{a_s}\}$: G-orbit of monomials

$$\nu : T_n \dashrightarrow \mathbb{C}^s, \underline{t} \mapsto (\underline{t}^{a_1}, \ldots, \underline{t}^{a_n})$$

becomes G-equivariant, and

$$\nu \circ \mu : \mathbb{Q}^s \dashrightarrow \mathbb{Q}^s$$

is a rational covariant defined over $\mathbb{Q}$.

Example 2.

Let G be the subgroup of Aut(N) generated by

$$\alpha = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \quad \beta = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Then $G \cong D_{12}$

$$T_N = \mathsf{Spec}\,\mathbb{C}[X^{\pm}, Y^{\pm}]$$

$$\begin{cases} X^{\alpha} = X/Y \\ Y^{\alpha} = X \end{cases} \qquad \begin{cases} X^{\beta} = Y \\ Y^{\beta} = X \end{cases}$$

$\{X, Y, X/Y, Y/X, 1/X, 1/Y\}$: G-orbit

$$\mu : T_N \to \mathbb{C}^6$$

$$(t_1, t_2) \mapsto (t_1, t_2, t_1/t_2, t_2/t_1, 1/t_1, 1/t_2)$$