# Some Observations on Klein Quartic, Groups, and Geometry

Cherng-tiao Perng

Norfolk State University

November 8, 2014

# Some Historic Background

**Theorem.** (Hurwitz, 1893) Let $X$ be a curve of genus $g \geq 2$ over a field of characteristic 0. Then $|\mathrm{Aut}(X)| \leq 84(g-1)$.

*Idea of proof.* (See p. 305 of [3]) Let $G := \mathrm{Aut}(X)$ have order $n$. Then the action of $G$ on the function field $K(X)$ gives rise a finite morphism of curves $f : X \to Y$ of degree $n$. Then Hurwitz's theorem implies that

$$(2g-2)/n = 2g(Y) - 2 + \sum_{i=1}^{s}(1 - 1/r_i),$$

where $r_i$'s are the ramification indices corresponding to the ramification points of $X$ lying over distinct points of $Y$.

# Hurwitz's Bound Continued

Since $g \geq 2$, the left hand side is $> 0$. Under the constraints $g(Y) \geq 0, s \geq 0, r_i \geq 2, i = 1, \cdots, s$ are integers, we see that the right hand side reaches a *minimum* if we take $g(Y) = 0, s = 3$, and $r_i$'s the integers $2, 3$ and $7$, namely

$$2g(Y)-2+\sum_{i=1}^{s}(1-1/r_i) = -2+(1-1/2)+(1-1/3)+(1-1/7) = 1/42.$$

This shows that

$$(2g-2)/n \geq 1/42 \Rightarrow n \leq 84(g-1).$$

QED

# The Klein Quartic

**Theorem.** (Klein, 1879) Assume $\mathrm{char}\ k \neq 3$. If $X$ is the curve given by

$$x^3y + y^3z + z^3x = 0,$$

the group $\mathrm{Aut}\ X$ is the simple group of order 168, whose order is the maximum $84(g-1)$ allowed by curves of genus 3.

**Note.** This is the main focus of today's talk, but we will need other tools.

# Sylow's Theorem

**Theorem.** (Sylow, 1872) Let $G$ be a finite group of order $p^r m$ with $r \geq 1$ and $p \nmid m$. Then there exists at least one subgroup $P$ of order $p^r$ (called a $p$-Sylow subgroup of $G$). More precisely, one has

(a) The number $n$ of $p$-Sylow subgroups satisfies $n|m$ and $n \equiv 1 \pmod{p}$.
(b) All the $p$-Sylow subgroups are conjugate.
(c) Any $p$-group in $G$ is contained in a $p$-Sylow subgroup.

# Projective Plane and the Klein Quartic Curve

**Definition.** The projective plane $\mathbb{P}^2$ over $\mathbb{C}$ is defined as follows:

$$\mathbb{P}^2 = \{[x_0 : x_1 : x_2] | x_0, x_1 \text{ and } x_2 \in \mathbb{C}, \text{ not all zero}\}/ \sim,$$

where the equivalence $\sim$ is taken by identifying $[x_0 : x_1 : x_2]$ and $[y_0 : y_1 : y_2]$ if there exists a nonzero $\lambda \in \mathbb{C}$ such that $y_i = \lambda x_i, i = 0, 1,$ and 2.

The Klein quartic curve $X$ in $\mathbb{P}^2$ is the curve given by the following equation:

$$x_0^3 x_1 + x_1^3 x_2 + x_2^3 x_0 = 0.$$

## Automorphism of order 7, 3 and 2

Let $\zeta = e^{\frac{2\pi i}{7}}$ be a primitive 7-th root of unity. It is easy to see that the mapping

$$S : [t_0 : t_1 : t_2] \mapsto [\zeta t_0 : \zeta^2 t_1 : \zeta^4 t_2]$$

defines an automorphism of order 7. Also there is an obvious automorphism of order 3 (the cyclic permutation of coordinates)

$$U : [t_0 : t_1 : t_2] \mapsto [t_1 : t_2 : t_0].$$

It is easy to check that ($[t_0 : t_1 : t_2]$ considered as row vector)

$$USU^{-1} = S^4, \tag{1}$$

so that the subgroup generated by $S$ and $U$ is a semi-direct product of order 21.

# Automorphism of order 7, 3 and 2 - Continued

Now the following automorphism represented in matrix is not so easy to find, but it can be checked that it is indeed one and it has order 2:

$$T := \frac{i}{\sqrt{7}} \begin{bmatrix} \zeta - \zeta^6 & \zeta^2 - \zeta^5 & \zeta^4 - \zeta^3 \\ \zeta^2 - \zeta^5 & \zeta^4 - \zeta^3 & \zeta - \zeta^6 \\ \zeta^4 - \zeta^3 & \zeta - \zeta^6 & \zeta^2 - \zeta^5 \end{bmatrix}. \tag{2}$$

It is readily checked that $T$ has order 2 and satisfies

$$TUT^{-1} = U^2, \tag{3}$$

so that the group generated by $U$ and $T$ is the dihedral group of order 6.

# The Size of Automorphism Group of the Klein Quartic

One checks that the 49 elements $S^aTS^b$ $(0 \leq a, b \leq 6)$ are all distinct. In particular, this shows that the cyclic subgroup generated by $S$ is not normal in the group $G$ generated by $S$, $T$ and $U$ (otherwise $TST \in < S >$ so $TS = S^iT$ for some $i$, and hence all the elements $S^aTS^b$ can be written as $S^jT$ for some $j$, a contradiction). Since the order of the group $G$ is divisible by $2 \cdot 3 \cdot 7 = 42$, we see that $|G| = 42, 84, 126$ or $168$. If follows from Sylow's theorem that the group $< S >$ must be normal in the first three cases, so $|G| = 168$, and by Hurwitz's Theorem, $\mathrm{Aut}(X) = G =< S, T, U >$. (See p. 273 of [1].)

# Simplicity of $G$

**Theorem.** The group $\mathrm{Aut}(X)$ is a simple group of order 168.
*Proof.* (Dolgachev) Suppose $H$ is a nontrivial normal subgroup of $G$. Assume that its order is divisible by 7. Since its Sylow 7-subgroup cannot be normal in $H$ (in $G$?), we see that $H$ contains all Sylow 7-subgroups of $G$. By Sylow's Theorem, their number is equal to 8. This shows that $|H| = 56$ or 84. In the first case, $H$ contains a Sylow 2-subgroup of order 8. Since $H$ is normal, all its conjugates are in $H$, and in particular, $T \in H$. The quotient group $G/H$ is of order 3. It follows from (3) that the coset of $U$ must be trivial. Since 3 does not divide 56, we get a contradiction.

# Simplicity of $G$ - Continued

In the second case, $H$ contains $S, T, U$ (why?) and hence coincides with $G$. So, we have shown that $H$ cannot contain an element of order 7. Suppose it contains an element of order 3. Since all such elements are conjugate, $H$ contains $U$. If follows from (1) that the coset of $S$ in $G/H$ is trivial, hence $S \in H$, contradicting the assumption. It remains to consider the case when $H$ is a 2-subgroup. Then $|G/H| = 2^a \cdot 3 \cdot 7$, with $a \leq 2$. It follows from Sylow's Theorem that the image of the Sylow 7-subgroup in $G/H$ is normal. Thus its preimage in $G$ is normal. This contradiction finishes the proof that $G$ is simple. QED

# The Reason Why in the Previous Slide

In addressing the obscurity of the argument in the previous slide, I came across an assertion by H. Coxeter in his book "The Beauty of Geometry" when I was reading the materials regarding Cayley numbers, i.e. the octonions (See p. 23 of [2]). It was mentioned that there is a symmetry group of the Fano plane which has size equal to 168, and it can be described by the subgroup in $S_7$ generated by the cycles (12)(36) and (1234567). Immediately I double checked it by putting it in Sage: the pleasant result I got is that the size of the group is 168. It made me wonder whether these two groups are isomorphic to each other. So I hastened to construct an explicit isomorphism (not the one by generators and relations which would make sense only to the experts) between the two groups. I managed to do that by Divide and Conquer. The result was then used to justify Professor Dolgachev's argument.

# A motivating way to derive the order 2 transformation $T$ (1)

• Here is the starting scenario: Suppose we do not know the complicated transformation $T$ of order 2 in formula (2). But we know $S, U$, and assume that $G =< S, T, U >$ is isomorphic to $A =< (1,2)(3,6),(1,2,3,4,5,6,7) >$. Is there a way to solve for $T$ explicitly? We describe below a motivating way to derive $T$.

• Taking clue from the behavior of order 2 element in $A$, we are led to the assumption that $TU = U^2T$. Since the transformation comes from geometry, it is natural to assume that $T$ can be represented by a unitary matrix, namely $TT^* = I$, where $T^*$ is the conjugate transpose of $T$. Coupled with the order 2 requirement, we see immediately that $T = T^*$.

# A motivating way to derive the order 2 transformation $T$ (2)

- Namely, we may write the unitary matrix $T$ as

$$T = \begin{bmatrix} a & d & e \\ \bar{d} & b & f \\ \bar{e} & \bar{f} & c \end{bmatrix}, \text{ where } a, b, \text{ and } c \text{ are real.}$$

- Given that $U = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$, we get that $TU = \begin{bmatrix} d & e & a \\ b & f & \bar{d} \\ \bar{f} & c & \bar{e} \end{bmatrix}$ and $U^2T = \begin{bmatrix} \bar{d} & b & f \\ \bar{e} & \bar{f} & c \\ a & d & e \end{bmatrix}$.

# A motivating way to derive the order 2 transformation $T$ (3)

• By requiring $TU = U^2T$ and using the assumption that $T$ is unitary, we see that $T$ is of the form

$$T = \begin{bmatrix} a & c & b \\ c & b & a \\ b & a & c \end{bmatrix},$$

where all entries are real, hence $T$ is an orthogonal matrix.

• The previous statement is equivalent to saying that $a^2 + b^2 + c^2 = 1$ and $ab + bc + ca = 0$, where $a, b$ and $c$ are real.

# A motivating way to derive the order 2 transformation $T$ (4)

- With $\zeta = e^{\frac{2\pi i}{7}}$, it is well-known that $1, \zeta, \zeta^2, \cdots, \zeta^6$ divide the unit circle into 7 equal parts, and that

$$1 + \zeta + \zeta^2 + \cdots + \zeta^6 = 0.$$

- For solving $a, b$ and $c$ from the previous slide, we first try $a = \zeta - \zeta^6, b = \zeta^2 - \zeta^5$ and $c = \zeta^3 - \zeta^4$ (these are purely imaginary but we may rescale later). They satisfy $a^2 + b^2 + c^2 = -7$. Hence by rescaling a factor of $\frac{i}{\sqrt{7}}$, we can ensure that $a^2 + b^2 + c^2 = 1$.

- Furthermore by adjusting the sign of $c$, we ensure the equality $ab + bc + ca = 0$.

# A motivating way to derive the order 2 transformation $T$ (5)

• Thus we have found an order 2 transformation in the following form

$$T' = \frac{i}{\sqrt{7}} \begin{bmatrix} \zeta - \zeta^6 & \zeta^4 - \zeta^3 & \zeta^2 - \zeta^5 \\ \zeta^4 - \zeta^3 & \zeta^2 - \zeta^5 & \zeta - \zeta^6 \\ \zeta^2 - \zeta^5 & \zeta - \zeta^6 & \zeta^4 - \zeta^3 \end{bmatrix}.$$

• By the above construction, any permutation of $a, b$ and $c$ would also yield an order 2 transformation such as

$$T = \frac{i}{\sqrt{7}} \begin{bmatrix} \zeta - \zeta^6 & \zeta^2 - \zeta^5 & \zeta^4 - \zeta^3 \\ \zeta^2 - \zeta^5 & \zeta^4 - \zeta^3 & \zeta - \zeta^6 \\ \zeta^4 - \zeta^3 & \zeta - \zeta^6 & \zeta^2 - \zeta^5 \end{bmatrix}.$$

• We note that Professor Dolgachev's formula for $T$ is a mirror reflection of the matrix $T'$ above. But it should be a typo, because it does not satisfy the condition $T^2 = I$.

# Summary

• The unity of mathematics: the eight squares theorem $\leftrightarrow$ factorization theory of octonions $\leftarrow$ Symmetry group of the Fano plane $\mathbb{P}^2(\mathbb{F}_2) \leftrightarrow \mathrm{PSL}(3,2) \leftrightarrow \mathrm{Aut}(X)$

• Computer algebra system (such as SAGE) as a useful tool for conducting research and/or for engaging students.

• A motivating way for deriving an element of order 2 in $\mathrm{Aut}(X)$.

# Acknowledgements

The author would like to thank his advisee, Kamaria Clark, for patiently listening to him and for working on the exercises that he has assigned. Without her participation, this exposition might not have been possible. Special thanks also to the computer algebra system SAGE.

# References

**References.**

[1] Igor V. Dolgachev, *Classical Algebraic Geometry - A Modern View*, Cambridge University Press, 2012.

[2] H.S.M. Coxeter, *The Beauty of Geometry - Twelve Essays*, Dover Publications, Inc., 1999.

[3] Robin Hartshorne, *Algebraic Geometry*, Springer-Verlag New York, Inc., 1977.