Automorphisms of Curves

Gebhard Martin, Prof. Dr. Christian Liedtke
Center for Mathematical Sciences, Technische Universität München

Chair of Algebra

Abstract

This thesis is about automorphisms of nonsingular, complete *curves* over algebraically closed fields. The *genus* of a curve gives a way to systemize the treatment of curves and curves of a certain genus have certain properties, which are exploited in this thesis. Curves of genus 0 are isomorphic to $\mathbb{P}^1$, curves of genus 1 carry a group structure after a choice of a basepoint (so-called *elliptic curves*), and curves of genus $g \geq 2$ have finite automorphism groups. We will compute the automorphism groups of curves of genus 0 and 1 and prove *Hurwitz's theorem* on automorphisms of curves of higher genus in characteristic 0. Hurwitz's theorem gives a sharp bound on the size of automorphism groups, which is linear in the genus. Finally, we state some bounds which also hold in positive characteristic, except for some special curves, as well as treat some of these exceptions in detail.

Automorphisms of Projective Space

Theorem:

$\mathrm{Aut}(\mathbb{P}^n_k) \cong PGL(n+1,k) = GL(n+1,k)/k^\times$

Corollary:

$\mathrm{Aut}(\mathbb{P}^1_k) \cong PGL(2,k) = GL(2,k)/k^\times$

We get a well known example by setting $k = \mathbb{C}$. The automorphisms of $\mathbb{P}^1_{\mathbb{C}}$ are the so-called *Möbius-transformations*.

Curves of Genus 1

Let X be a curve of genus 1 and $P_0 \in X$ be a closed point. Then (X, P_0) is called an *elliptic curve*. An elliptic curve (X, P_0) carries a group structure, such that P_0 plays the role of the neutral element. Using this group structure, we can define translations by any closed point and show that these translations are in fact automorphisms of the curve.

Furthermore, the subgroup N of translations is normal in $\mathrm{Aut}(X)$, in 1-to-1 correspondence with the closed points of X, and $\mathrm{Aut}(X)/N \cong \mathrm{Aut}(X, P_0)$, where $\mathrm{Aut}(X, P_0)$ denotes the stabilizer of P_0 under the action of $\mathrm{Aut}(X)$.

$\mathrm{Aut}(X, P_0)$ can be computed in characteristic $p \neq 2$ by using the 2-to-1 cover of $\mathbb{P}^1_k$ determined by $|2P_0|$. The *hyperelliptic involution* is an automorphism of order 2, which interchanges the two points of each fiber of this morphism. In characteristic 2, we use the closed immersion to $\mathbb{P}^2_k$ determined by $|3P_0|$ for some explicit calculations. In both of these cases, $\mathrm{Aut}(X, P_0)$ depends on the *j-invariant*:

Definition:

Let (X, P_0) be an elliptic curve over a field of characteristic $p \neq 2$ and let f be the morphism to $\mathbb{P}^1_k$ determined by $|2P_0|$. Apply an automorphism of $\mathbb{P}^1_k$, such that the branch points of f are $0, 1, \infty$ and $\lambda \in k - \{0, 1\}$. Then define the j-invariant of (X, P_0) by

$$j(X, P_0) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}$$

The j-invariant can also be defined in characteristic 2. Using this invariant and denoting the group of translations by X, we get the following classification of automorphisms of genus 1 curves:

Theorem:

Let X be a curve of genus 1. Then $\mathrm{Aut}(X)$ is isomorphic to

$$\begin{array}{rll} N \rtimes (\mathbb{Z}/2\mathbb{Z}) & \text{if} & j \neq 0, 1728 \\ N \rtimes (\mathbb{Z}/4\mathbb{Z}) & \text{if} & j = 1728 \text{ and char } k \notin \{2,3\} \\ N \rtimes (\mathbb{Z}/6\mathbb{Z}) & \text{if} & j = 0 \text{ and char } k \notin \{2,3\} \\ N \rtimes (\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}) & \text{if} & j = 0 = 1728 \text{ and char } k = 3 \\ N \rtimes (Q_8 \rtimes \mathbb{Z}/3\mathbb{Z}) & \text{if} & j = 0 = 1728 \text{ and char } k = 2 \end{array}$$

The semidirect products involved in the theorem are all nontrivial. The group law of the semidirect product of N with the stabilizer at P_0 is given by:

$$((\tau_P, \varphi_1), (\tau_Q, \varphi_2)) \mapsto (\tau_P \circ \tau_{\varphi_1(Q)}, \varphi_1 \circ \varphi_2)$$

See [1] and [2] for more information on elliptic curves.

References

1. Robin Hartshorne. Algebraic Geometry. Springer. 1977
2. Joseph H. Silverman. The Arithmetic of Elliptic Curves. Springer. 2009
3. Henning Stichtenoth. Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharacteristik. . 1973
4. Hans-Wolfgang Henn. Funktionenkörper mit großer Automorphismengruppe. . 1978
5. Igor V. Dolgachev. Classical Algebraic Geometry: A Modern View. Cambridge University Press. 2012
6. I. Shafarevich. Algebraic Geometry I. Springer. 1994
7. A. M. Macbeath. On a theorem of Hurwitz. Cambridge University Press. 1961

Hurwitz's Theorem

The automorphism group of curves of genus $g \geq 2$ is finite in every characteristic [1]. A generic curve of genus $g \geq 3$ has no automorphisms except the identity [6]. The most important result on automorphisms of curves over an algebraically closed field of characteristic 0 is given by the following theorem:

Hurwitz's Theorem:

Let C be a curve over an algebraically closed field k of characteristic $\mathrm{char}\, k = 0$ and let $g \geq 2$ be its genus. Then $|\mathrm{Aut}(C)| \leq 84(g-1)$

Some of the techniques used in the proof of Hurwitz's Theorem can be generalized to positive characteristic, giving the following result on prime divisors of $|\mathrm{Aut}(X)|$:

Theorem:

Let X be a curve over an algebraically closed field of characteristic p, let $g \geq 2$ be its genus and let $q \neq p$ be a prime number. Let $N(q)$ be the multiplicity of q in the prime factorization of $|\mathrm{Aut}(X)|$. Then

$$N(q) \leq \log_q(84(g-1))$$

The bound given in Hurwitz's Theorem is sharp. There are infinitely many values for which the bound is attained [7]. The lowest genus example is the Klein quartic [5]:

Example:

Let C be the curve over $\mathbb{C}$ given by the equation:

$$XY^3 + YZ^3 + ZX^3 = 0$$

Then $\mathrm{Aut}(C) \cong PSL(2,7)$ and in particular $|\mathrm{Aut}(C)| = 168 = 84(g-1)$.

Other Bounds

Stichtenoth Bound:

Let C be a curve. Let $g \geq 2$ be its genus. Then $|\mathrm{Aut}(C)| \leq 16g^4$, unless C is isomorphic to a Hermitian curve. [3]

Henn Bound:

Let C be a curve. If $g \geq 2$ and $G = |\mathrm{Aut}(C)| \geq 8g^3$, then C is birationally equivalent to a curve defined by an affine equation in one of the following families [4] :

1. $p = 2, k > 1$ and
$$Y^2 + Y + X^{2^k+1} = 0$$
Then G fixes a point, $|G| = 2^{2k+1}(2^k + 1)$ and $g = 2^{k-1}$.
2. $p > 2, n > 0, Q = p^n$ and
$$Y^2 - X^q + X = 0$$
Then $G/M \cong PGL(2,q)$ for some subgroup M of order 2, $|G| = 2q^3 - 2q$ and $g = p^r$.
3. $n > 0, q = p^n \geq 3$ and
$$Y^q + Y - X^{q+1} = 0$$
Then $G \cong PGU(3,q)$, $|G| = (q^3+1)q^3(q^2-1)$ and $g = \frac{1}{2}(q^2 - q)$.
4. $p = 2, n \geq 1, q_0 = 2^n, q = 2q_0^2$ and
$$X^{q_0}(X^q + X) - Y^q - Y = 0$$
Then $G \cong Sz(q)$, $|G| = q^2(q^2+1)(q-1)$ and $g = q_0(q-1)$.

Each of these examples is highly symmetric in a way which is only possible in positive characteristic. This becomes clear when looking at their automorphism groups: The first is a 2-group over a field of characteristic 2 and we can only bound the size of q-groups with q prime to p. The second and third groups would be infinite in characteristic 0 and the fourth is a group which exists only over fields of characteristic 2.