# On nilpotent automorphism groups of function fields

Nurdagül Anbar
(joint work with Burçin Güneş)

Sabancı University, İstanbul

3 March 2021, Carleton Finite Fields eSeminar

$K$: an algebraically closed field
$\mathrm{Char}(K)$: the characteristic of $K$
$F/K$: a function field with constant field $K$
$g(F)$: the genus of $F$
$\mathbb{P}_F$: the set of places of $F$

**Definition:** An automorphism $\sigma$ of $F/K$ is a field automorphism of $F$ such that $\sigma(\alpha) = \alpha$ for all $\alpha \in K$. The automorphism group

$$\mathrm{Aut}(F/K) = \{\sigma \ : \ \sigma \text{ is an automorphism of } F\}$$

**Example:** Rational Function Field, i.e., $F = K(x)$.
$\sigma : F \mapsto F$ defined by $x \mapsto \frac{ax+b}{cx+d}$ for some $a, b, c, d \in K$.
$\sigma$ is an automorphism of $F \iff ad - bc \neq 0$
In fact, $\mathrm{Aut}(F/K) \cong \mathrm{PGL}(2, K)$

If $g(F) = 1$, then $\mathrm{Cl}^0(F) \subseteq \mathrm{Aut}(F/K)$.

That is, if $g(F) = 0$ or $1$, then $\mathrm{Aut}(F/K)$ is infinite.

$K$: an algebraically closed field
Char($K$): the characteristic of $K$
$F/K$: a function field with constant field $K$
$g(F)$: the genus of $F$
$\mathbb{P}_F$: the set of places of $F$

**Definition:** An automorphism $\sigma$ of $F/K$ is a field automorphism of $F$ such that $\sigma(\alpha) = \alpha$ for all $\alpha \in K$. The automorphism group

$$\mathrm{Aut}(F/K) = \{\sigma \ : \ \sigma \text{ is an automorphism of } F\}$$

**Example:** Rational Function Field, i.e., $F = K(x)$.
$\sigma : F \mapsto F$ defined by $x \mapsto \frac{ax+b}{cx+d}$ for some $a, b, c, d \in K$.
$\sigma$ is an automorphism of $F \iff ad - bc \neq 0$
In fact, $\mathrm{Aut}(F/K) \cong \mathrm{PGL}(2, K)$

If $g(F) = 1$, then $\mathrm{Cl}^0(F) \subseteq \mathrm{Aut}(F/K)$.

That is, if $g(F) = 0$ or $1$, then $\mathrm{Aut}(F/K)$ is infinite.

$K$: an algebraically closed field
$\mathrm{Char}(K)$: the characteristic of $K$
$F/K$: a function field with constant field $K$
$g(F)$: the genus of $F$
$\mathbb{P}_F$: the set of places of $F$

**Definition:** An automorphism $\sigma$ of $F/K$ is a field automorphism of $F$ such that $\sigma(\alpha) = \alpha$ for all $\alpha \in K$. The automorphism group

$$\mathrm{Aut}(F/K) = \{\sigma \ : \ \sigma \text{ is an automorphism of } F\}$$

**Example:** Rational Function Field, i.e., $F = K(x)$.
$\sigma : F \mapsto F$ defined by $x \mapsto \frac{ax+b}{cx+d}$ for some $a, b, c, d \in K$.
$\sigma$ is an automorphism of $F \iff ad - bc \neq 0$
In fact, $\mathrm{Aut}(F/K) \cong \mathrm{PGL}(2, K)$

If $g(F) = 1$, then $\mathrm{Cl}^0(F) \subseteq \mathrm{Aut}(F/K)$.

That is, if $g(F) = 0$ or $1$, then $\mathrm{Aut}(F/K)$ is infinite.

$K$: an algebraically closed field
$\mathrm{Char}(K)$: the characteristic of $K$
$F/K$: a function field with constant field $K$
$g(F)$: the genus of $F$
$\mathbb{P}_F$: the set of places of $F$

**Definition:** An automorphism $\sigma$ of $F/K$ is a field automorphism of $F$ such that $\sigma(\alpha) = \alpha$ for all $\alpha \in K$. The automorphism group

$$\mathrm{Aut}(F/K) = \{\sigma \ : \ \sigma \text{ is an automorphism of } F\}$$

**Example:** Rational Function Field, i.e., $F = K(x)$.
$\sigma : F \mapsto F$ defined by $x \mapsto \frac{ax+b}{cx+d}$ for some $a, b, c, d \in K$.
$\sigma$ is an automorphism of $F \iff ad - bc \neq 0$
In fact, $\mathrm{Aut}(F/K) \cong \mathrm{PGL}(2, K)$

If $g(F) = 1$, then $\mathrm{Cl}^0(F) \subseteq \mathrm{Aut}(F/K)$.

That is, if $g(F) = 0$ or $1$, then $\mathrm{Aut}(F/K)$ is infinite.

$K$: an algebraically closed field
$\mathrm{Char}(K)$: the characteristic of $K$
$F/K$: a function field with constant field $K$
$g(F)$: the genus of $F$
$\mathbb{P}_F$: the set of places of $F$

**Definition:** An automorphism $\sigma$ of $F/K$ is a field automorphism of $F$ such that $\sigma(\alpha) = \alpha$ for all $\alpha \in K$. The automorphism group

$$\mathrm{Aut}(F/K) = \{\sigma \ : \ \sigma \text{ is an automorphism of } F\}$$

**Example:** Rational Function Field, i.e., $F = K(x)$.
$\sigma : F \mapsto F$ defined by $x \mapsto \frac{ax+b}{cx+d}$ for some $a, b, c, d \in K$.
$\sigma$ is an automorphism of $F \iff ad - bc \neq 0$
In fact, $\mathrm{Aut}(F/K) \cong \mathrm{PGL}(2, K)$

If $g(F) = 1$, then $\mathrm{Cl}^0(F) \subseteq \mathrm{Aut}(F/K)$.

That is, if $g(F) = 0$ or $1$, then $\mathrm{Aut}(F/K)$ is infinite.

# Known bounds for the case $g(F) \geq 2$

If $g(F) \geq 2$, then $\mathrm{Aut}(F/K)$ is finite. (Hurwitz (1893) and Schmid (1938))

(I) (Hurwitz, 1893) If $K = \mathbb{C}$, then $|\mathrm{Aut}(F/K)| \leq 84(g(F) - 1)$.

(II) (Roquette, 1970) If $p = \mathrm{Char}(K) > 0$ and $p \nmid |\mathrm{Aut}(F/K)|$, then $|\mathrm{Aut}(F/K)| \leq 84(g(F) - 1)$.

(III) (Stichtenoth, 1973) If $p = \mathrm{Char}(K) > 0$ and $p \mid |\mathrm{Aut}(F/K)|$, then

$$|\mathrm{Aut}(F/K)| \leq 16g(F)^4$$

with one exception: the Hermitian function fields $\mathcal{H}$ defined by $y^{p^n} + y = x^{p^n+1}$.

$$g(\mathcal{H}) = \frac{p^{2n} - p^n}{2} \quad \text{and} \quad |\mathrm{Aut}(\mathcal{H}/K)| = p^{3n}(p^{2n} - 1)(p^{3n} + 1).$$

# Known bounds for the case $g(F) \geq 2$

If $g(F) \geq 2$, then $\mathrm{Aut}(F/K)$ is finite. (Hurwitz (1893) and Schmid (1938))

(I) (Hurwitz, 1893) If $K = \mathbb{C}$, then $|\mathrm{Aut}(F/K)| \leq 84(g(F) - 1)$.

(II) (Roquette, 1970) If $p = \mathrm{Char}(K) > 0$ and $p \nmid |\mathrm{Aut}(F/K)|$, then $|\mathrm{Aut}(F/K)| \leq 84(g(F) - 1)$.

(III) (Stichtenoth, 1973) If $p = \mathrm{Char}(K) > 0$ and $p \mid |\mathrm{Aut}(F/K)|$, then

$$|\mathrm{Aut}(F/K)| \leq 16g(F)^4$$

with one exception: the Hermitian function fields $\mathcal{H}$ defined by $y^{p^n} + y = x^{p^n+1}$.

$$g(\mathcal{H}) = \frac{p^{2n} - p^n}{2} \quad \text{and} \quad |\mathrm{Aut}(\mathcal{H}/K)| = p^{3n}(p^{2n} - 1)(p^{3n} + 1).$$

# Known bounds for the case $g(F) \geq 2$

If $g(F) \geq 2$, then $\mathrm{Aut}(F/K)$ is finite. (Hurwitz (1893) and Schmid (1938))

(I) (Hurwitz, 1893) If $K = \mathbb{C}$, then $|\mathrm{Aut}(F/K)| \leq 84(g(F) - 1)$.

(II) (Roquette, 1970) If $p = \mathrm{Char}(K) > 0$ and $p \nmid |\mathrm{Aut}(F/K)|$, then $|\mathrm{Aut}(F/K)| \leq 84(g(F) - 1)$.

(III) (Stichtenoth, 1973) If $p = \mathrm{Char}(K) > 0$ and $p \mid |\mathrm{Aut}(F/K)|$, then

$$|\mathrm{Aut}(F/K)| \leq 16 g(F)^4$$

with one exception: the Hermitian function fields $\mathcal{H}$ defined by $y^{p^n} + y = x^{p^n+1}$.

$$g(\mathcal{H}) = \frac{p^{2n} - p^n}{2} \quad \text{and} \quad |\mathrm{Aut}(\mathcal{H}/K)| = p^{3n}(p^{2n} - 1)(p^{3n} + 1).$$

# Known bounds for the case $g(F) \geq 2$

If $g(F) \geq 2$, then $\mathrm{Aut}(F/K)$ is finite. (Hurwitz (1893) and Schmid (1938))

(I) (Hurwitz, 1893) If $K = \mathbb{C}$, then $|\mathrm{Aut}(F/K)| \leq 84(g(F) - 1)$.

(II) (Roquette, 1970) If $p = \mathrm{Char}(K) > 0$ and $p \nmid |\mathrm{Aut}(F/K)|$, then $|\mathrm{Aut}(F/K)| \leq 84(g(F) - 1)$.

(III) (Stichtenoth, 1973) If $p = \mathrm{Char}(K) > 0$ and $p \mid |\mathrm{Aut}(F/K)|$, then

$$|\mathrm{Aut}(F/K)| \leq 16g(F)^4$$

with one exception: the Hermitian function fields $\mathcal{H}$ defined by $y^{p^n} + y = x^{p^n+1}$.

$$g(\mathcal{H}) = \frac{p^{2n} - p^n}{2} \quad \text{and} \quad |\mathrm{Aut}(\mathcal{H}/K)| = p^{3n}(p^{2n} - 1)(p^{3n} + 1).$$

# Known bounds for the case $g(F) \geq 2$

If $g(F) \geq 2$, then $\mathrm{Aut}(F/K)$ is finite. (Hurwitz (1893) and Schmid (1938))

(I) (Hurwitz, 1893) If $K = \mathbb{C}$, then $|\mathrm{Aut}(F/K)| \leq 84(g(F) - 1)$.

(II) (Roquette, 1970) If $p = \mathrm{Char}(K) > 0$ and $p \nmid |\mathrm{Aut}(F/K)|$, then $|\mathrm{Aut}(F/K)| \leq 84(g(F) - 1)$.

(III) (Stichtenoth, 1973) If $p = \mathrm{Char}(K) > 0$ and $p \mid |\mathrm{Aut}(F/K)|$, then

$$|\mathrm{Aut}(F/K)| \leq 16g(F)^4$$

with one exception: the Hermitian function fields $\mathcal{H}$ defined by $y^{p^n} + y = x^{p^n+1}$.

$$g(\mathcal{H}) = \frac{p^{2n} - p^n}{2} \quad \text{and} \quad |\mathrm{Aut}(\mathcal{H}/K)| = p^{3n}(p^{2n} - 1)(p^{3n} + 1).$$

# Special types of groups

Let $F/K$ be a function field of $g(F) \geq 2$ and $G$ a subgroup of $\mathrm{Aut}(F/K)$.

(I) (Zomorrodian, 1985) If $K = \mathbb{C}$ and $G$ is nilpotent, then $|G| \leq 16(g(F) - 1)$. Moreover, if the equality holds, then $g(F) - 1$ is a power of 2.
Conversely, if $g - 1$ is a power of 2, then there exists $F/K$ of genus $g(F) = g$ with $|\mathrm{Aut}(F/K)| = 16(g - 1)$.

(II) (Nakajima, 1987) If $G$ is abelian, then $|G| \leq 4(g(F) + 1)$.

(III) (Korchmaros and Montanucci, 2020) If $G$ has order power of a prime $\ell \geq 3$, with $\ell \neq \mathrm{Char}(K)$, then $|G| \leq 9(g(F) - 1)$.

**Question:** Is there an upper bound for $|G|$ in terms of a linear polynomial in $g(F)$ when $\mathrm{Char}(K) > 0$ and $G$ is nilpotent?

## Special types of groups

Let $F/K$ be a function field of $g(F) \geq 2$ and $G$ a subgroup of $\mathrm{Aut}(F/K)$.

(i) (Zomorrodian, 1985) If $K = \mathbb{C}$ and $G$ is nilpotent, then $|G| \leq 16(g(F) - 1)$. Moreover, if the equality holds, then $g(F) - 1$ is a power of 2.
Conversely, if $g - 1$ is a power of 2, then there exists $F/K$ of genus $g(F) = g$ with $|\mathrm{Aut}(F/K)| = 16(g - 1)$.

(ii) (Nakajima, 1987) If $G$ is abelian, then $|G| \leq 4(g(F) + 1)$.

(iii) (Korchmaros and Montanucci, 2020) If $G$ has order power of a prime $\ell \geq 3$, with $\ell \neq \mathrm{Char}(K)$, then $|G| \leq 9(g(F) - 1)$.

**Question:** Is there an upper bound for $|G|$ in terms of a linear polynomial in $g(F)$ when $\mathrm{Char}(K) > 0$ and $G$ is nilpotent?

# Special types of groups

Let $F/K$ be a function field of $g(F) \geq 2$ and $G$ a subgroup of $\mathrm{Aut}(F/K)$.

(I) (Zomorrodian, 1985) If $K = \mathbb{C}$ and $G$ is nilpotent, then $|G| \leq 16(g(F) - 1)$. Moreover, if the equality holds, then $g(F) - 1$ is a power of 2.
Conversely, if $g - 1$ is a power of 2, then there exists $F/K$ of genus $g(F) = g$ with $|\mathrm{Aut}(F/K)| = 16(g - 1)$.

(II) (Nakajima, 1987) If $G$ is abelian, then $|G| \leq 4(g(F) + 1)$.

(III) (Korchmaros and Montanucci, 2020) If $G$ has order power of a prime $\ell \geq 3$, with $\ell \neq \mathrm{Char}(K)$, then $|G| \leq 9(g(F) - 1)$.

**Question:** Is there an upper bound for $|G|$ in terms of a linear polynomial in $g(F)$ when $\mathrm{Char}(K) > 0$ and $G$ is nilpotent?

# Special types of groups

Let $F/K$ be a function field of $g(F) \geq 2$ and $G$ a subgroup of $\mathrm{Aut}(F/K)$.

(I) (Zomorrodian, 1985) If $K = \mathbb{C}$ and $G$ is nilpotent, then $|G| \leq 16(g(F) - 1)$. Moreover, if the equality holds, then $g(F) - 1$ is a power of 2.
Conversely, if $g - 1$ is a power of 2, then there exists $F/K$ of genus $g(F) = g$ with $|\mathrm{Aut}(F/K)| = 16(g - 1)$.

(II) (Nakajima, 1987) If $G$ is abelian, then $|G| \leq 4(g(F) + 1)$.

(III) (Korchmaros and Montanucci, 2020) If $G$ has order power of a prime $\ell \geq 3$, with $\ell \neq \mathrm{Char}(K)$, then $|G| \leq 9(g(F) - 1)$.

**Question:** Is there an upper bound for $|G|$ in terms of a linear polynomial in $g(F)$ when $\mathrm{Char}(K) > 0$ and $G$ is nilpotent?

# Special types of groups

Let $F/K$ be a function field of $g(F) \geq 2$ and $G$ a subgroup of $\mathrm{Aut}(F/K)$.

(i) (Zomorrodian, 1985) If $K = \mathbb{C}$ and $G$ is nilpotent, then $|G| \leq 16(g(F) - 1)$. Moreover, if the equality holds, then $g(F) - 1$ is a power of 2.
Conversely, if $g - 1$ is a power of 2, then there exists $F/K$ of genus $g(F) = g$ with $|\mathrm{Aut}(F/K)| = 16(g - 1)$.

(ii) (Nakajima, 1987) If $G$ is abelian, then $|G| \leq 4(g(F) + 1)$.

(iii) (Korchmaros and Montanucci, 2020) If $G$ has order power of a prime $\ell \geq 3$, with $\ell \neq \mathrm{Char}(K)$, then $|G| \leq 9(g(F) - 1)$.

**Question:** Is there an upper bound for $|G|$ in terms of a linear polynomial in $g(F)$ when $\mathrm{Char}(K) > 0$ and $G$ is nilpotent?

# Special types of groups

Let $F/K$ be a function field of $g(F) \geq 2$ and $G$ a subgroup of $\mathrm{Aut}(F/K)$.

(I) (Zomorrodian, 1985) If $K = \mathbb{C}$ and $G$ is nilpotent, then $|G| \leq 16(g(F) - 1)$. Moreover, if the equality holds, then $g(F) - 1$ is a power of 2.
Conversely, if $g - 1$ is a power of 2, then there exists $F/K$ of genus $g(F) = g$ with $|\mathrm{Aut}(F/K)| = 16(g - 1)$.

(II) (Nakajima, 1987) If $G$ is abelian, then $|G| \leq 4(g(F) + 1)$.

(III) (Korchmaros and Montanucci, 2020) If $G$ has order power of a prime $\ell \geq 3$, with $\ell \neq \mathrm{Char}(K)$, then $|G| \leq 9(g(F) - 1)$.

**Question:** Is there an upper bound for $|G|$ in terms of a linear polynomial in $g(F)$ when $\mathrm{Char}(K) > 0$ and $G$ is nilpotent?

**Theorem:**(A., Güneş) Let $K$ be an algebraically closed field of characteristic $p > 0$ and let $F/K$ be a function field of genus $g \geq 2$. If $G$ is a nilpotent subgroup of $\mathrm{Aut}(F/K)$, then

$$|G| \leq 16(g-1)$$

except the case that the fixed field $F_0$ of $G$ is rational such that $F_0$ has a unique place ramified in $F$. Moreover, if the equality holds, then $g(F) - 1$ is a power of 2.

**Remark:** In the exceptional case, $G$ is a $p$-group and the unique ramified place of $F_0$ is totally ramified in $F$. Then $|G| \leq \frac{4p}{(p-1)^2} g(F)^2$ by a result of Stichtenoth (1973).

**Theorem:**(A., Güneş) Let $K$ be an algebraically closed field of characteristic $p > 0$ and let $F/K$ be a function field of genus $g \geq 2$. If $G$ is a nilpotent subgroup of $\mathrm{Aut}(F/K)$, then

$$|G| \leq 16(g-1)$$

except the case that the fixed field $F_0$ of $G$ is rational such that $F_0$ has a unique place ramified in $F$. Moreover, if the equality holds, then $g(F) - 1$ is a power of 2.

**Remark:** In the exceptional case, $G$ is a $p$-group and the unique ramified place of $F_0$ is totally ramified in $F$. Then $|G| \leq \frac{4p}{(p-1)^2} g(F)^2$ by a result of Stichtenoth (1973).

**Main Tool:** Galois extensions of function fields.

**Setting:**

$G \leq \mathrm{Aut}(F/K)$

$F^G := \{\beta \in F \mid \sigma(\beta) = \beta \text{ for all } \sigma \in G\} \subseteq F$

$F^G$ is a function field over $K$.

$F/F^G$ is a Galois extension of degree $|G|$.

By the Hurwitz genus formula,

$$2g(F) - 2 = |G|(2g(F^G) - 2) + \deg\left(\mathrm{Diff}(F/F^G)\right)$$

.

That is, $|G|$ is closely related to genus and the ramification.

**Main Tool:** Galois extensions of function fields.

**Setting:**

$G \leq \mathrm{Aut}(F/K)$

$F^G := \{\beta \in F \mid \sigma(\beta) = \beta \text{ for all } \sigma \in G\} \subseteq F$

$F^G$ is a function field over $K$.

$F/F^G$ is a Galois extension of degree $|G|$.

By the Hurwitz genus formula,

$$2g(F) - 2 = |G|(2g(F^G) - 2) + \deg\left(\mathrm{Diff}(F/F^G)\right)$$

.

That is, $|G|$ is closely related to genus and the ramification.

**Main Tool:** Galois extensions of function fields.

**Setting:**

$G \leq \mathrm{Aut}(F/K)$

$F^G := \{\beta \in F \mid \sigma(\beta) = \beta \text{ for all } \sigma \in G\} \subseteq F$

$F^G$ is a function field over $K$.

$F/F^G$ is a Galois extension of degree $|G|$.

By the Hurwitz genus formula,

$$2g(F) - 2 = |G|(2g(F^G) - 2) + \deg\big(\mathrm{Diff}(F/F^G)\big)$$

.

That is, $|G|$ is closely related to genus and the ramification.

**Main Tool:** Galois extensions of function fields.

**Setting:**

$G \leq \mathrm{Aut}(F/K)$

$F^G := \{\beta \in F \mid \sigma(\beta) = \beta \text{ for all } \sigma \in G\} \subseteq F$

$F^G$ is a function field over $K$.

$F/F^G$ is a Galois extension of degree $|G|$.

By the Hurwitz genus formula,

$$2g(F) - 2 = |G|(2g(F^G) - 2) + \deg\left(\mathrm{Diff}(F/F^G)\right)$$

.

That is, $|G|$ is closely related to genus and the ramification.

# Properties of Galois extensions

Let $F/E$ be a Galois extension of function fields. For $Q \in \mathbb{P}_E$ and $P \in \mathbb{P}_F$ such that $P \supseteq Q$, we write $P|Q$ and denote by
$e(P|Q)$ the ramification index of $P|Q$,
$d(P|Q)$ the different exponent of $P|Q$.
$G = \mathrm{Gal}(F/E)$

(I) Let $Q \in \mathbb{P}_E$ and $\mathcal{T} = \{P \in \mathbb{P}_F \ : \ P|Q\} = \{P_1, \ldots, P_r\}$. $G$ acts transitively on $\mathcal{T}$. Hence, for all $i, j \in \{1, \ldots, r\}$, we have

$$e(P_i|Q) = e(P_j|Q) =: e(Q) \quad d(P_i|Q) = d(P_j|Q) =: d(Q)$$

(II) By the "Fundamental Equality", $|G| = re(Q)$, i.e., $e(Q) \mid |G|$ and $r \mid |G|$.

(III) By the Hurwitz genus formula,

$$2g(F) - 2 = |G| \left( 2g(E) - 2 + \sum_{Q \in \mathbb{P}_E} \frac{d(Q)}{e(Q)} \right).$$

# Properties of Galois extensions

Let $F/E$ be a Galois extension of function fields. For $Q \in \mathbb{P}_E$ and $P \in \mathbb{P}_F$ such that $P \supseteq Q$, we write $P|Q$ and denote by
$e(P|Q)$ the ramification index of $P|Q$,
$d(P|Q)$ the different exponent of $P|Q$.
$G = \mathrm{Gal}(F/E)$

(I) Let $Q \in \mathbb{P}_E$ and $\mathcal{T} = \{P \in \mathbb{P}_F \ : \ P|Q\} = \{P_1, \ldots, P_r\}$. $G$ acts transitively on $\mathcal{T}$. Hence, for all $i, j \in \{1, \ldots, r\}$, we have

$$e(P_i|Q) = e(P_j|Q) =: e(Q) \quad d(P_i|Q) = d(P_j|Q) =: d(Q)$$

(II) By the "Fundamental Equality", $|G| = re(Q)$, i.e., $e(Q) \mid |G|$ and $r \mid |G|$.

(III) By the Hurwitz genus formula,

$$2g(F) - 2 = |G| \left( 2g(E) - 2 + \sum_{Q \in \mathbb{P}_E} \frac{d(Q)}{e(Q)} \right).$$

# Properties of Galois extensions

Let $F/E$ be a Galois extension of function fields. For $Q \in \mathbb{P}_E$ and $P \in \mathbb{P}_F$ such that $P \supseteq Q$, we write $P|Q$ and denote by
$e(P|Q)$ the ramification index of $P|Q$,
$d(P|Q)$ the different exponent of $P|Q$.
$G = \mathrm{Gal}(F/E)$

(I) Let $Q \in \mathbb{P}_E$ and $\mathcal{T} = \{P \in \mathbb{P}_F \ : \ P|Q\} = \{P_1, \dots, P_r\}$.
$G$ acts transitively on $\mathcal{T}$. Hence, for all $i, j \in \{1, \dots, r\}$, we have

$$e(P_i|Q) = e(P_j|Q) =: e(Q) \quad d(P_i|Q) = d(P_j|Q) =: d(Q)$$

(II) By the "Fundamental Equality", $|G| = re(Q)$, i.e., $e(Q) \mid |G|$ and $r \mid |G|$.

(III) By the Hurwitz genus formula,

$$2g(F) - 2 = |G| \left( 2g(E) - 2 + \sum_{Q \in \mathbb{P}_E} \frac{d(Q)}{e(Q)} \right).$$

# Properties of Galois extensions

Let $F/E$ be a Galois extension of function fields. For $Q \in \mathbb{P}_E$ and $P \in \mathbb{P}_F$ such that $P \supseteq Q$, we write $P|Q$ and denote by
$e(P|Q)$ the ramification index of $P|Q$,
$d(P|Q)$ the different exponent of $P|Q$.
$G = \mathrm{Gal}(F/E)$

(I) Let $Q \in \mathbb{P}_E$ and $\mathcal{T} = \{P \in \mathbb{P}_F \ : \ P|Q\} = \{P_1, \ldots, P_r\}$.
$G$ acts transitively on $\mathcal{T}$. Hence, for all $i, j \in \{1, \ldots, r\}$, we have

$$e(P_i|Q) = e(P_j|Q) =: e(Q) \quad d(P_i|Q) = d(P_j|Q) =: d(Q)$$

(II) By the "Fundamental Equality", $|G| = re(Q)$, i.e., $e(Q) \mid |G|$ and $r \mid |G|$.

(III) By the Hurwitz genus formula,

$$2g(F) - 2 = |G| \left( 2g(E) - 2 + \sum_{Q \in \mathbb{P}_E} \frac{d(Q)}{e(Q)} \right).$$

**Dedekind's Different Theorem:** Let $F/E$ be a Galois extension of function fields. For $Q \in \mathbb{P}_E$

(I) $d(Q) \geq e(Q) - 1$

(II) $d(Q) = e(Q) - 1$ if and only if $p \nmid e(Q)$.

**Definition:** We say, $Q$ is "tamely ramified" if $p \nmid e(Q)$. Otherwise, it is called "wildly ramified".

**Observartion:**

(I) If $Q$ is tamely ramified then $\frac{d(Q)}{e(Q)} = \frac{e(Q)-1}{e(Q)} \geq \frac{1}{2}$.

(II) If $Q$ is widely ramified then $\frac{d(Q)}{e(Q)} \geq 1$.

**Dedekind's Different Theorem:** Let $F/E$ be a Galois extension of function fields. For $Q \in \mathbb{P}_E$

(I) $d(Q) \geq e(Q) - 1$

(II) $d(Q) = e(Q) - 1$ if and only if $p \nmid e(Q)$.

**Definition:** We say, $Q$ is "tamely ramified" if $p \nmid e(Q)$. Otherwise, it is called "wildly ramified".

**Observartion:**

(I) If $Q$ is tamely ramified then $\frac{d(Q)}{e(Q)} = \frac{e(Q)-1}{e(Q)} \geq \frac{1}{2}$.

(II) If $Q$ is widely ramified then $\frac{d(Q)}{e(Q)} \geq 1$.

**Dedekind's Different Theorem:** Let $F/E$ be a Galois extension of function fields. For $Q \in \mathbb{P}_E$

(I) $d(Q) \geq e(Q) - 1$

(II) $d(Q) = e(Q) - 1$ if and only if $p \nmid e(Q)$.

**Definition:** We say, $Q$ is "tamely ramified" if $p \nmid e(Q)$. Otherwise, it is called "wildly ramified".

**Observartion:**

(I) If $Q$ is tamely ramified then $\frac{d(Q)}{e(Q)} = \frac{e(Q)-1}{e(Q)} \geq \frac{1}{2}$.

(II) If $Q$ is widely ramified then $\frac{d(Q)}{e(Q)} \geq 1$.

**Recall:** $F/K$ is a function field of genus $g \geq 2$ and $G \leq \mathrm{Aut}(F/K)$ nilpotent subgroup. Set $F_0 = F^G$ and $g_0 = g(F_0)$. By the Hurwitz genus formula,

$$2g - 2 = |G| \left( 2g_0 - 2 + \sum_{Q \in \mathbb{P}_{F_0}} \frac{d(Q)}{e(Q)} \right).$$

**Simple Case $g_0 \geq 1$:**

(I) $g_0 \geq 2 \implies 2g - 2 \geq |G|(2g_0 - 2) \geq 2|G| \implies |G| \leq (g - 1)$

(II) $g_0 = 1 \implies$ there exits a ramified place $Q \in \mathbb{P}_{F_0} \implies$
$2g - 2 \geq |G| \frac{d(Q)}{e(Q)} \geq \frac{|G|}{2} \implies |G| \leq 4(g - 1)$

From now on, we suppose that $g_0 = 0$.

**Recall:** $F/K$ is a function field of genus $g \geq 2$ and $G \leq \mathrm{Aut}(F/K)$ nilpotent subgroup. Set $F_0 = F^G$ and $g_0 = g(F_0)$. By the Hurwitz genus formula,

$$2g - 2 = |G| \left( 2g_0 - 2 + \sum_{Q \in \mathbb{P}_{F_0}} \frac{d(Q)}{e(Q)} \right).$$

**Simple Case $g_0 \geq 1$:**

(I) $g_0 \geq 2 \implies 2g - 2 \geq |G|(2g_0 - 2) \geq 2|G| \implies |G| \leq (g - 1)$

(II) $g_0 = 1 \implies$ there exits a ramified place $Q \in \mathbb{P}_{F_0} \implies$
$2g - 2 \geq |G|\frac{d(Q)}{e(Q)} \geq \frac{|G|}{2} \implies |G| \leq 4(g - 1)$

From now on, we suppose that $g_0 = 0$.

**Recall:** $F/K$ is a function field of genus $g \geq 2$ and $G \leq \text{Aut}(F/K)$ nilpotent subgroup. Set $F_0 = F^G$ and $g_0 = g(F_0)$. By the Hurwitz genus formula,

$$2g - 2 = |G| \left( 2g_0 - 2 + \sum_{Q \in \mathbb{P}_{F_0}} \frac{d(Q)}{e(Q)} \right).$$

**Simple Case $g_0 \geq 1$:**

(I) $g_0 \geq 2 \implies 2g - 2 \geq |G|(2g_0 - 2) \geq 2|G| \implies |G| \leq (g - 1)$

(II) $g_0 = 1 \implies$ there exits a ramified place $Q \in \mathbb{P}_{F_0} \implies$ $2g - 2 \geq |G| \frac{d(Q)}{e(Q)} \geq \frac{|G|}{2} \implies |G| \leq 4(g - 1)$

From now on, we suppose that $g_0 = 0$.

**Recall:** $F/K$ is a function field of genus $g \geq 2$ and $G \leq \mathrm{Aut}(F/K)$ nilpotent subgroup. Set $F_0 = F^G$ and $g_0 = g(F_0)$. By the Hurwitz genus formula,

$$2g-2 = |G|\left(2g_0 - 2 + \sum_{Q\in\mathbb{P}_{F_0}} \frac{d(Q)}{e(Q)}\right).$$

**Simple Case $g_0 \geq 1$:**

(I) $g_0 \geq 2 \Longrightarrow 2g-2 \geq |G|(2g_0-2) \geq 2|G| \Longrightarrow |G| \leq (g-1)$

(II) $g_0 = 1 \Longrightarrow$ there exits a ramified place $Q \in \mathbb{P}_{F_0} \Longrightarrow$ $2g-2 \geq |G|\frac{d(Q)}{e(Q)} \geq \frac{|G|}{2} \Longrightarrow |G| \leq 4(g-1)$

From now on, we suppose that $g_0 = 0$.

We investigate $g_0 = 0$ with respect to the number of ramified places.

**Definition:** Let $Q_1, \ldots, Q_r$ be all the ramified places of $F_0$ in $F/F_0$ with ramification indices $e_1, \ldots, e_r$, respectively. W.l.o.g., we assume that $e_1 \leq \ldots \leq e_r$. We say that $F$ is of type $(e_1, \ldots, e_r)$.

**Case $r \geq 5$:** Set $d_i := d(Q_i)$. By the Hurwitz genus formula,

$$2g - 2 = |G| \left( -2 + \sum_{i=1}^{r} \frac{d_i}{e_i} \right) \geq |G| \left( -2 + 5 \cdot \frac{1}{2} \right) = \frac{|G|}{2},$$

i.e., $|G| \leq 4(g-1)$.

Therefore, we need to investigate $1 \leq r \leq 4$. That is, we investigate function fields of type $(e_1, e_2, e_3, e_4)$, $(e_1, e_2, e_3)$, $(e_1, e_2)$ and $(e_1)$.

**Fact:** If $G$ is a finite nilpotent group, then $G$ has a normal subgroup of order $n$ for each divisor $n$ of $|G|$.

We investigate $g_0 = 0$ with respect to the number of ramified places.

**Definition:** Let $Q_1, \ldots, Q_r$ be all the ramified places of $F_0$ in $F/F_0$ with ramification indices $e_1, \ldots, e_r$, respectively. W.l.o.g., we assume that $e_1 \leq \ldots \leq e_r$. We say that $F$ is of type $(e_1, \ldots, e_r)$.

**Case $r \geq 5$:** Set $d_i := d(Q_i)$. By the Hurwitz genus formula,

$$2g - 2 = |G| \left(-2 + \sum_{i=1}^{r} \frac{d_i}{e_i}\right) \geq |G| \left(-2 + 5 \cdot \tfrac{1}{2}\right) = \frac{|G|}{2},$$

i.e., $|G| \leq 4(g-1)$.

Therefore, we need to investigate $1 \leq r \leq 4$. That is, we investigate function fields of type $(e_1, e_2, e_3, e_4)$, $(e_1, e_2, e_3)$, $(e_1, e_2)$ and $(e_1)$.

**Fact:** If $G$ is a finite nilpotent group, then $G$ has a normal subgroup of order $n$ for each divisor $n$ of $|G|$.

We investigate $g_0 = 0$ with respect to the number of ramified places.

**Definition:** Let $Q_1, \ldots, Q_r$ be all the ramified places of $F_0$ in $F/F_0$ with ramification indices $e_1, \ldots, e_r$, respectively. W.l.o.g., we assume that $e_1 \leq \ldots \leq e_r$. We say that $F$ is of type $(e_1, \ldots, e_r)$.

**Case $r \geq 5$:** Set $d_i := d(Q_i)$. By the Hurwitz genus formula,

$$2g - 2 = |G| \left(-2 + \textstyle\sum_{i=1}^{r} \frac{d_i}{e_i}\right) \geq |G| \left(-2 + 5 \cdot \frac{1}{2}\right) = \frac{|G|}{2},$$

i.e., $|G| \leq 4(g-1)$.

Therefore, we need to investigate $1 \leq r \leq 4$. That is, we investigate function fields of type $(e_1, e_2, e_3, e_4)$, $(e_1, e_2, e_3)$, $(e_1, e_2)$ and $(e_1)$.

**Fact:** If $G$ is a finite nilpotent group, then $G$ has a normal subgroup of order $n$ for each divisor $n$ of $|G|$.

We investigate $g_0 = 0$ with respect to the number of ramified places.

**Definition:** Let $Q_1, \dots, Q_r$ be all the ramified places of $F_0$ in $F/F_0$ with ramification indices $e_1, \dots, e_r$, respectively. W.l.o.g., we assume that $e_1 \leq \dots \leq e_r$. We say that $F$ is of type $(e_1, \dots, e_r)$.

**Case $r \geq 5$:** Set $d_i := d(Q_i)$. By the Hurwitz genus formula,

$$2g - 2 = |G| \left(-2 + \sum_{i=1}^{r} \frac{d_i}{e_i}\right) \geq |G| \left(-2 + 5 \cdot \frac{1}{2}\right) = \frac{|G|}{2},$$

i.e., $|G| \leq 4(g-1)$.

Therefore, we need to investigate $1 \leq r \leq 4$. That is, we investigate function fields of type $(e_1, e_2, e_3, e_4)$, $(e_1, e_2, e_3)$, $(e_1, e_2)$ and $(e_1)$.

**Fact:** If $G$ is a finite nilpotent group, then $G$ has a normal subgroup of order $n$ for each divisor $n$ of $|G|$.

We investigate $g_0 = 0$ with respect to the number of ramified places.

**Definition:** Let $Q_1, \ldots, Q_r$ be all the ramified places of $F_0$ in $F/F_0$ with ramification indices $e_1, \ldots, e_r$, respectively. W.l.o.g., we assume that $e_1 \leq \ldots \leq e_r$. We say that $F$ is of type $(e_1, \ldots, e_r)$.

**Case $r \geq 5$:** Set $d_i := d(Q_i)$. By the Hurwitz genus formula,

$$2g - 2 = |G| \left(-2 + \textstyle\sum_{i=1}^{r} \frac{d_i}{e_i}\right) \geq |G| \left(-2 + 5 \cdot \frac{1}{2}\right) = \frac{|G|}{2},$$

i.e., $|G| \leq 4(g-1)$.

Therefore, we need to investigate $1 \leq r \leq 4$. That is, we investigate function fields of type $(e_1, e_2, e_3, e_4)$, $(e_1, e_2, e_3)$, $(e_1, e_2)$ and $(e_1)$.

**Fact:** If $G$ is a finite nilpotent group, then $G$ has a normal subgroup of order $n$ for each divisor $n$ of $|G|$.

# The case $(2, 4, e_3)$

**Lemma:** Let $\ell$ be a prime number. Then $\ell \mid |G|$ if and only if $\ell \mid e_i$ for some $i$.

*Proof.* Suppose that $\ell \mid |G|$ and $\ell \nmid e_i$ for any $i$. Let $H \lhd G$ such that $[G : H] = \ell$.



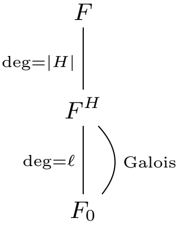

$\implies F^H/F_0$ is an unramified Galois extension of degree $\ell$
$\implies 2g(F^H) - 2 = -2\ell$
$\implies g(F^H) = -\ell + 1 < 0$, a contradiction.

**IN FACT**, if $\ell$ is a prime number, which divides **exactly** one of $e_i$, then $\ell = \mathrm{char}(K)$.

# The case $(2, 4, e_3)$

**Lemma:** Let $\ell$ be a prime number. Then $\ell \mid |G|$ if and only if $\ell \mid e_i$ for some $i$.

*Proof.* Suppose that $\ell \mid |G|$ and $\ell \nmid e_i$ for any $i$. Let $H \lhd G$ such that $[G : H] = \ell$.




$\Longrightarrow F^H/F_0$ is an unramified Galois extension of degree $\ell$

$\Longrightarrow 2g(F^H) - 2 = -2\ell$

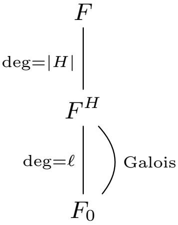
$\Longrightarrow g(F^H) = -\ell + 1 < 0$, a contradiction.

IN FACT, if $\ell$ is a prime number, which divides **exactly** one of $e_i$, then $\ell = \mathrm{char}(K)$.

# The case $(2,4,e_3)$

**Lemma:** Let $\ell$ be a prime number. Then $\ell \mid |G|$ if and only if $\ell \mid e_i$ for some $i$.

*Proof.* Suppose that $\ell \mid |G|$ and $\ell \nmid e_i$ for any $i$. Let $H \lhd G$ such that $[G:H]=\ell$.

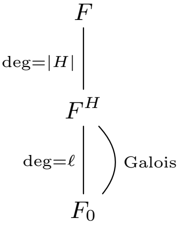



$\Longrightarrow F^H/F_0$ is an unramified Galois extension of degree $\ell$
$\Longrightarrow 2g(F^H)-2=-2\ell$
$\Longrightarrow g(F^H)=-\ell+1<0$, a contradiction.

IN FACT, if $\ell$ is a prime number, which divides **exactly** one of $e_i$, then $\ell=\mathrm{char}(K)$.

# The case $(2, 4, e_3)$

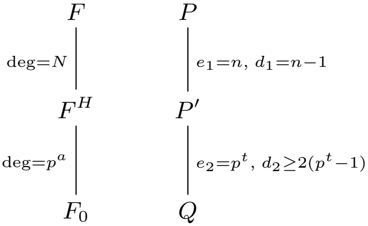
**Lemma:** Let $\ell$ be a prime number. Then $\ell \mid |G|$ if and only if $\ell \mid e_i$ for some $i$.
*Proof.* Suppose that $\ell \mid |G|$ and $\ell \nmid e_i$ for any $i$. Let $H \lhd G$ such that $[G : H] = \ell$.




$\Longrightarrow$ $F^H/F_0$ is an unramified Galois extension of degree $\ell$
$\Longrightarrow$ $2g(F^H) - 2 = -2\ell$
$\Longrightarrow$ $g(F^H) = -\ell + 1 < 0$, a contradiction.
**IN FACT**, if $\ell$ is a prime number, which divides **exactly** one of $e_i$, then $\ell = \mathrm{char}(K)$.

**Lemma:** Let $p = \mathrm{char}(K)$ and $|G| = p^a N$ with $a, N \geq 1$ and $\gcd(p, N) = 1$. Let $e(Q) = p^t n$ such that $\gcd(p, n) = 1$. Then $d(Q) \geq (e(Q) - 1) + n(p^t - 1)$.

*Proof.* Let $H \trianglelefteq G$ of index $p^a$. Set $P' = P \cap F^H$.




By the transitivity of different exponent,

$$d(Q) = e_1 d_2 + d_1 \geq 2n(p^t - 1) + n - 1 = (e(Q) - 1) + n(p^t - 1)$$

**The case $(2,4,e_3)$ :**

(I) $\mathrm{char}(K) = 2 \Longrightarrow Q_1$ and $Q_2$ are wildly ramified $\Longrightarrow$ $d_1/e_1, d_2/e_2 \geq 1$ and $d_3/e_3 \geq 1/2 \Longrightarrow |G| \leq 4(g-1)$

(II) $\mathrm{char}(K) \neq 2 \Longrightarrow e_3 = 2^a \ell^b$ for a prime $\ell > 2$ and $a, b \geq 0$

- $b > 0 \Longrightarrow \ell = \mathrm{Char}(K)$ and $d_3 \geq (2^a\ell^b - 1) + 2^a(\ell^b - 1) \Longrightarrow$ $|G| < 3(g-1)$
- Suppose that $b = 0$. Since $\mathrm{char}(K) \neq 2$,

$$2g - 2 = |G|\left(-2 + \frac{1}{2} + \frac{3}{4} + \frac{2^a - 1}{2^a}\right) = |G|\left(\frac{1}{4} - \frac{1}{2^a}\right).$$

Then the fact that $g \geq 2$ implies that $a \geq 3$; hence, $|G| \leq 16(g-1)$.

**Remark:**

$|G| = 16(g-1) \iff a = 3$, i.e., $F$ is of type $(2,4,8)$.

## The case $(2,4,e_3)$ :

(I) $\mathrm{char}(K)=2 \Longrightarrow Q_1$ and $Q_2$ are wildly ramified $\Longrightarrow$ $d_1/e_1, d_2/e_2 \geq 1$ and $d_3/e_3 \geq 1/2 \Longrightarrow |G| \leq 4(g-1)$

(II) $\mathrm{char}(K)\neq 2 \Longrightarrow e_3 = 2^a\ell^b$ for a prime $\ell > 2$ and $a, b \geq 0$

- $b>0 \Longrightarrow \ell = \mathrm{Char}(K)$ and $d_3 \geq (2^a\ell^b-1)+2^a(\ell^b-1) \Longrightarrow$ $|G| < 3(g-1)$
- Suppose that $b=0$. Since $\mathrm{char}(K)\neq 2$,

$$2g-2=|G|\left(-2+\frac{1}{2}+\frac{3}{4}+\frac{2^a-1}{2^a}\right)=|G|\left(\frac{1}{4}-\frac{1}{2^a}\right).$$

  Then the fact that $g\geq 2$ implies that $a\geq 3$; hence, $|G|\leq 16(g-1)$.

**Remark:**

$|G|=16(g-1) \Longleftrightarrow a=3$, i.e., $F$ is of type $(2,4,8)$.

## The case $(2, 4, e_3)$ :

(I) $\mathrm{char}(K) = 2 \implies Q_1$ and $Q_2$ are wildly ramified $\implies$ $d_1/e_1, d_2/e_2 \geq 1$ and $d_3/e_3 \geq 1/2 \implies |G| \leq 4(g-1)$

(II) $\mathrm{char}(K) \neq 2 \implies e_3 = 2^a \ell^b$ for a prime $\ell > 2$ and $a, b \geq 0$

- $b > 0 \implies \ell = \mathrm{Char}(K)$ and $d_3 \geq (2^a \ell^b - 1) + 2^a(\ell^b - 1) \implies$ $|G| < 3(g-1)$
- Suppose that $b = 0$. Since $\mathrm{char}(K) \neq 2$,

$$2g - 2 = |G|\left(-2 + \frac{1}{2} + \frac{3}{4} + \frac{2^a - 1}{2^a}\right) = |G|\left(\frac{1}{4} - \frac{1}{2^a}\right).$$

Then the fact that $g \geq 2$ implies that $a \geq 3$; hence, $|G| \leq 16(g-1)$.

**Remark:**

$|G| = 16(g-1) \iff a = 3$, i.e., $F$ is of type $(2, 4, 8)$.

**Theorem (A.-Güneş):**
Let $F/K$ be a function field of genus $g \geq 2$ and $G$ a nilpotent subgroup of $\mathrm{Aut}(F/K)$. Suppose that $F_0 := F^G$ is rational.

(I) If there are exactly 4 ramified places of $F_0$ in $F/F_0$, then $|G| \leq 8(g-1)$. Moreover, the equality holds when $\mathrm{Char}(K) \neq 2$, $F$ is of type $(2, 2, 2, 4)$ and $G$ is a 2-group.

(II) If there are exactly 3 ramified places of $F_0$ in $F/F_0$, then $|G| \leq 16(g-1)$. Moreover, the equality holds when $\mathrm{Char}(K) \neq 2$, $F$ is of type $(2, 4, 8)$ and $G$ is a 2-group.

(III) If there are exactly 2 ramified places of $F_0$ in $F/F_0$, then $|G| \leq 10(g-1)$. Moreover, the equality holds when $F$ is either of type $(2, 10)$ or $(5, 10)$ and $G$ is cyclic of order 10.

(IV) If there is exactly 1 ramified place of $F_0$ in $F/F_0$, then $G$ is a $p$-group and $|G| \leq \frac{4p}{(p-1)^2} g^2$, where $p = \mathrm{Char}(K)$.

## Example: $r = 3$

Let $p \neq 2$ and $F = K(x, y)$ of $g(F) = 2$ defined by $y^2 = x(x^4 - 1)$. For $\zeta$ primitive 8-th root of unity

$$\sigma : \begin{cases} x \mapsto \zeta^2 x \\ y \mapsto \zeta y \end{cases} \quad \text{and} \quad \tau : \begin{cases} x \mapsto -1/x \\ y \mapsto y/x^3 \end{cases} \quad \text{are in } \mathrm{Aut}(F/K).$$

- $G = \langle \sigma, \tau \rangle \leq \mathrm{Aut}(F/K)$ is a group of order 16, i.e., $|G| = 16(g(F) - 1)$.
- $F^G = K(t)$, where $t = (x^8 + 1)/2x^4$.
- $(t = -1)$, $(t = 1)$ and $(t = \infty)$ with ramification indices are 2, 4, 8, respectively.

$$F = K(x, y)$$

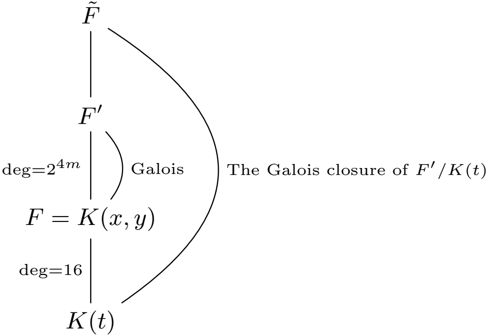
$y^2 = x(x^4 - 1)$ | deg=2

$$K(x)$$

$t = \frac{x^8+1}{2x^4}$ | deg=8

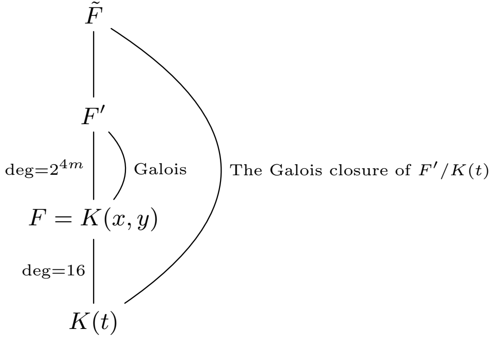
$$K(t)$$

For $m \geq 1$, the field $F$ has a unique maximal unramified abelian extension $F'$ such that $[F' : F] = 2^{4m}$.



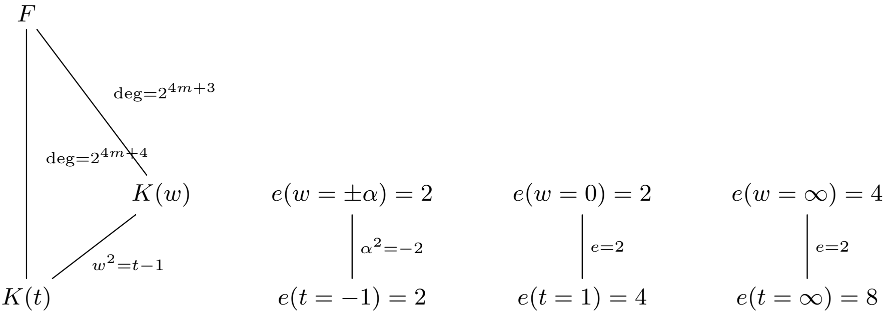

- $\tilde{F} = F'$, i.e., $F'/K(t)$ is Galois.
- $[F' : K(t)] = 2^{4m+4}$ and $g(F') = 2^{4m} + 1$, i.e., $\mathrm{Gal}(F'/K(t)) = 16(g(F') - 1)$
- $(t = -1)$, $(t = 1)$ and $(t = \infty)$ are the only ramified places of ramification indices are 2, 4, 8, respectively.

For $m \geq 1$, the field $F$ has a unique maximal unramified abelian extension $F'$ such that $[F' : F] = 2^{4m}$.



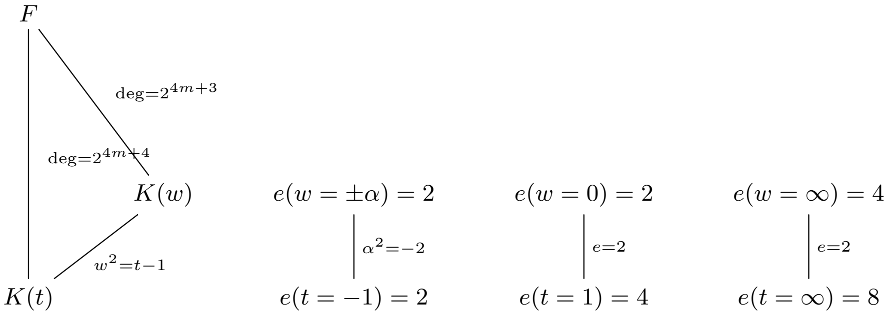

- $\tilde{F} = F'$, i.e., $F'/K(t)$ is Galois.
- $[F' : K(t)] = 2^{4m+4}$ and $g(F') = 2^{4m} + 1$, i.e., $\mathrm{Gal}(F'/K(t)) = 16(g(F') - 1)$
- $(t = -1)$, $(t = 1)$ and $(t = \infty)$ are the only ramified places of ramification indices are 2, 4, 8, respectively.

## Example: $r = 4$




- $F$ is of type $(2, 2, 2, 4)$.
- $g(F) = 2^{4m} + 1$ and $|G| = |\mathrm{Gal}(F/K(w))| = 2^{4m+3}$, i.e., $|G)| = 8(g(F) - 1)$.

## Example: $r = 4$




- $F$ is of type $(2, 2, 2, 4)$.
- $g(F) = 2^{4m} + 1$ and $|G| = |\text{Gal}(F/K(w))| = 2^{4m+3}$, i.e., $|G)| = 8(g(F) - 1)$.

**Example:** $r = 2$

(I) $p = 5$ and $F = K(x, y)$ of genus 2 defined by $y^5 - y = x^2$. Let $G = \langle\sigma\rangle$, where $\sigma(x) = -x$ and $\sigma(y) = y + 1$. Then $|G| = 10$ and $F^G = K(t)$ with $t = x^2$. $(t = 0)$ and $(t = \infty)$ are the only ramified places with ramification indices 2, 10 respectively. Therefore, $F$ is of type $(2, 10)$ with $|G| = 10(g(F) - 1)$.

(II) $p = 2$ and $F = K(x, y)$ of genus 2 defined by $y^2 - y = x^5$. Let $G = \langle\sigma\rangle$, where $\sigma(x) = \zeta x$ and $\sigma(y) = y + 1$, where $\zeta$ is a primitive 5-th root of unity. Then $|G| = 10$ and $F^G = K(t)$ with $t = x^5$. Similarly, $(t = 0)$ and $(t = \infty)$ are the only ramified places with ramification indices 5, 10, respectively. Therefore, $F$ is of type $(5, 10)$ with $|G| = 10(g(F) - 1)$.

**Example:** $r = 2$

(I) $p = 5$ and $F = K(x, y)$ of genus 2 defined by $y^5 - y = x^2$. Let $G = \langle\sigma\rangle$, where $\sigma(x) = -x$ and $\sigma(y) = y + 1$. Then $|G| = 10$ and $F^G = K(t)$ with $t = x^2$. $(t = 0)$ and $(t = \infty)$ are the only ramified places with ramification indices 2, 10 respectively. Therefore, $F$ is of type $(2, 10)$ with $|G| = 10(g(F) - 1)$.

(II) $p = 2$ and $F = K(x, y)$ of genus 2 defined by $y^2 - y = x^5$. Let $G = \langle\sigma\rangle$, where $\sigma(x) = \zeta x$ and $\sigma(y) = y + 1$, where $\zeta$ is a primitive 5-th root of unity. Then $|G| = 10$ and $F^G = K(t)$ with $t = x^5$. Similarly, $(t = 0)$ and $(t = \infty)$ are the only ramified places with ramification indices 5, 10, respectively. Therefore, $F$ is of type $(5, 10)$ with $|G| = 10(g(F) - 1)$.

**Example: $r = 1$, Stichtenoth (1973)**

Let $F = K(x, y)$ defined by $y^p + y = x^{p^n+1}$ where $p = \mathrm{Char}(K)$ and $n \geq 1$. Then $g(F) = \frac{p^n(p-1)}{2}$.

Let $G$ be the automorphism group fixing the unique pole $P$ of $x$ and $y$.

$G$ consists of automorphisms

$$\sigma : \begin{cases} x \mapsto x + d, \\ y \mapsto y + Q(x), \end{cases}$$

where $d \in K$, $\deg Q(x) \leq p^{n-1}$ such that $Q(x)^p + Q(x) = (x + d)^{p^n+1} - x^{p^n+1}$.

$\Longrightarrow |G| = p^{2n+1}$

$\Longrightarrow |G| = \frac{4p}{(p-1)} g(F)^2$.

**OPEN PROBLEM:** If $g - 1$ is an integer of power 2, then is there $F/K$ of genus $g$ with automorphism group of order $16(g - 1)$?

**Example: $r = 1$, Stichtenoth (1973)**

Let $F = K(x, y)$ defined by $y^p + y = x^{p^n+1}$ where $p = \mathrm{Char}(K)$ and $n \geq 1$. Then $g(F) = \frac{p^n(p-1)}{2}$.

Let $G$ be the automorphism group fixing the unique pole $P$ of $x$ and $y$. $G$ consists of automorphisms

$$\sigma : \begin{cases} x \mapsto x + d, \\ y \mapsto y + Q(x), \end{cases}$$

where $d \in K$, $\deg Q(x) \leq p^{n-1}$ such that $Q(x)^p + Q(x) = (x + d)^{p^n+1} - x^{p^n+1}$.

$\Longrightarrow |G| = p^{2n+1}$

$\Longrightarrow |G| = \frac{4p}{(p-1)} g(F)^2$.

**OPEN PROBLEM:** If $g - 1$ is an integer of power 2, then is there $F/K$ of genus $g$ with automorphism group of order $16(g - 1)$?

**Example: $r = 1$, Stichtenoth (1973)**

Let $F = K(x, y)$ defined by $y^p + y = x^{p^n+1}$ where $p = \mathrm{Char}(K)$ and $n \geq 1$. Then $g(F) = \frac{p^n(p-1)}{2}$.

Let $G$ be the automorphism group fixing the unique pole $P$ of $x$ and $y$. $G$ consists of automorphisms

$$\sigma : \begin{cases} x \mapsto x + d, \\ y \mapsto y + Q(x), \end{cases}$$

where $d \in K$, $\deg Q(x) \leq p^{n-1}$ such that $Q(x)^p + Q(x) = (x + d)^{p^n+1} - x^{p^n+1}$.

$\Longrightarrow |G| = p^{2n+1}$

$\Longrightarrow |G| = \frac{4p}{(p-1)} g(F)^2.$

**OPEN PROBLEM:** If $g - 1$ is an integer of power 2, then is there $F/K$ of genus $g$ with automorphism group of order $16(g - 1)$?

**Example: $r = 1$, Stichtenoth (1973)**

Let $F = K(x, y)$ defined by $y^p + y = x^{p^n+1}$ where $p = \mathrm{Char}(K)$ and $n \geq 1$. Then $g(F) = \frac{p^n(p-1)}{2}$.

Let $G$ be the automorphism group fixing the unique pole $P$ of $x$ and $y$. $G$ consists of automorphisms

$$\sigma : \begin{cases} x \mapsto x + d, \\ y \mapsto y + Q(x), \end{cases}$$

where $d \in K$, $\deg Q(x) \leq p^{n-1}$ such that $Q(x)^p + Q(x) = (x + d)^{p^n+1} - x^{p^n+1}$.

$\Longrightarrow |G| = p^{2n+1}$

$\Longrightarrow |G| = \frac{4p}{(p-1)} g(F)^2$.

**OPEN PROBLEM:** If $g - 1$ is an integer of power 2, then is there $F/K$ of genus $g$ with automorphism group of order $16(g - 1)$?

**Example: $r = 1$, Stichtenoth (1973)**

Let $F = K(x, y)$ defined by $y^p + y = x^{p^n+1}$ where $p = \mathrm{Char}(K)$ and $n \geq 1$. Then $g(F) = \frac{p^n(p-1)}{2}$.

Let $G$ be the automorphism group fixing the unique pole $P$ of $x$ and $y$. $G$ consists of automorphisms

$$\sigma : \begin{cases} x \mapsto x + d, \\ y \mapsto y + Q(x), \end{cases}$$

where $d \in K$, $\deg Q(x) \leq p^{n-1}$ such that
$Q(x)^p + Q(x) = (x + d)^{p^n+1} - x^{p^n+1}$.

$\Longrightarrow |G| = p^{2n+1}$

$\Longrightarrow |G| = \frac{4p}{(p-1)} g(F)^2$.

**OPEN PROBLEM:** If $g - 1$ is an integer of power 2, then is there $F/K$ of genus $g$ with automorphism group of order $16(g - 1)$?

**We wish you healthy days!**