A Galois Theory for Elliptic Subfields

1. Introduction

Let C/K be a curve of genus $g = g_C \geq 1$,
$F = \kappa(C)$ be its function field,
$\mathcal{E}_C = \mathcal{E}_F = \{F' \subset F : g_{F'} = 1\}$ its set of elliptic subfields,
$\mathcal{E}_F(n) = \{F' \in \mathcal{E}_F : [F : F'] = n\}$ those of fixed index n.

Problem 1: Determine (or classify) the set $\mathcal{E}_F$, or equivalently, the sets $\mathcal{E}_F(n)$, for all $n > 1$.

Notes: 1) $\#\mathcal{E}_F(n) < \infty, \forall n$. (Tamme, 1972)

2) If $g = 1$ (and K is algebraically closed), then by (usual) Galois theory we have (if $\mathrm{char}(K) \nmid n$) a natural bijection

$$\mathcal{E}_F(n) \ \stackrel{\sim}{\to}\ \{H \leq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} : \#H = n\}.$$

3) Each $F' \in \mathcal{E}_F$ is contained in a unique maximal elliptic subfield. Thus, by 2) it is enough to determine the subsets $\mathcal{E}_F^*$ and $\mathcal{E}_F^*(n)$ of maximal elliptic subfields (of index n).

4) If $g_F = 2$ (and $K = \mathbb{C}$), then:

(Picard, 1882) $\#\mathcal{E}_F^* = 0, 2,$ or ∞

(Bolza, 1886) $\#\mathcal{E}_F^* = \infty \Leftrightarrow J_C \sim E \times E$, for some elliptic curve E

Here: J_C denotes the Jacobian variety of the curve C.

In this talk: we'll restrict our attention to the latter case, i.e. to the case that $J_C \sim E \times E$. (Thus: $g = 2$.)

Theorem 0 ([K], 1994) If $g = 2$, then there is a natural bijection between the following sets:

(i) the set $\mathcal{E}_F^*(n)$ of maximal elliptic subfields of index n;

(i') the set of elliptic subgroups of J_C of degree n:

$$\{E \leq J_C : (E.\theta) = n\};$$

here $\theta \simeq C$ denotes the theta-divisor on J_C.

(ii) the set $\mathcal{R}(q_C, n^2)$ of primitive representations of n^2 by a certain positive definite quadratic form q_C in r variables, i.e.

$$\mathcal{R}(q_C, n^2) = \{(x_1, \ldots, x_r) \in \mathbb{Z}^r : \gcd(x_1, \ldots, x_r) = 1, \\ q_C(x_1, \ldots, x_r) = n^2\}$$

Remarks: 1) The quadratic form q_C is closely related to the Humbert invariant attached to a "singular abelian surface" (and hence may be called a generalized Humbert invariant). Note that q_C is determined only up to (improper) equivalence of quadratic forms.

2) If $J_C \sim E \times E$, then $r = rk(\mathrm{End}(E)) + 1 \in \{2, 3, 5\}$.

3) The bijection between $\mathcal{E}_F^*(n)$ and $\mathcal{R}(q_C, n^2)$ might be viewed as a first step towards a Galois theory for maximal elliptic subfields. However, this is only useful if we can describe the quadratic form q_C in an explicit manner.

Problem 2: (a) Given a curve C, determine/describe q_C.

(b) Which positive definite quadratic forms q can occur?

Aim: Give a complete answer to Problem 2 for certain subclass of curves of genus 2 (called curves of type d).

2. Curves of type d

Definition: A pair (E_1, E_2) of elliptic curves is said to be of type d if

$$\mathrm{Hom}(E_1, E_2) = \mathbb{Z}h, \quad \text{for some } h \text{ with } \deg(h) = d.$$

A curve C (of genus 2) is said to be of type d if there exists a pair (E_1, E_2) of elliptic curves of type d such that

$$J_C \simeq E_1 \times E_2.$$

Notes: 1) If (E_1, E_2) has type d, then $E_1 \sim E_2$ and E_i has no CM (i.e. $\mathrm{End}(E_i) = \mathbb{Z}$). Thus, if C has type d, then $r = 2$, so q_C is a binary quadratic form.

2) If $J_C \simeq E_1 \times E_2$, then E_1 and E_2 are not necessarily uniquely determined by C (up to isomorphism). However, it turns out that its type d is unique.

Problem 3: Do curves of type d exist? How many are there?

Remarks: 1) This problem is the analogue of a problem studied by Hayashida/Nishi (1965) (resp. by Ibukiyama/Katsura/Oort (1986)). These authors studied the existence/number of curves C with $J_C \simeq E_1 \times E_2$ in the case that

$$\mathrm{End}(E_1) \simeq \mathrm{End}(E_2) = \mathfrak{O}_k$$

is the ring of integers $\mathfrak{O}_k$ of an imaginary quadratic field k (resp. in the case that E_1, E_2 are supersingular).

2) As we shall see below, Problems 2 and 3 are closely related to each other.

3. Main Results

Theorem 1: If (E_1, E_2) has type d, then

$$\#(\{C : J_C \simeq E_1 \times E_2\}/\simeq) = H(d) - 2^{s-1},$$

where $s = \omega(d) = \#\{p : p|d\}$ is the number of prime divisors and

$$H(d) = \begin{cases} \tilde{h}(-4d) & \text{if } d \not\equiv 3 \pmod 4 \\ \tilde{h}(-4d) + \tilde{h}(-d) & \text{if } d \equiv 3 \pmod 4. \end{cases}$$

Here $\tilde{h}(D)$ denotes the number of classes of primitive positive definite binary quadratic forms of discriminant D modulo improper equivalence, i.e.

$$\tilde{h}(D) = \tfrac{1}{2}(h(D) + g(D)),$$

where $h(D)$ denotes the (usual) class number $(= \#$ equivalence classes modulo proper equivalence) and $g(D)$ denotes the number of genera of forms of discriminant D.

Corollary: There is no curve of type d

$$\Leftrightarrow \begin{cases} d = 1, 4, 12, 16, 28, 60 \ \text{ or} \\ d \equiv \pm 2 \pmod 8 \text{ and } h(-4d) = g(-4d) \ (= 2^{s-1}). \end{cases}$$

In particular, there are only finitely many d's for which there is no curve of type d.

Conjecture: There are precisely 21 values of $d \geq 1$ for which there is no curve of type d :

$$\begin{aligned} d = \ & 1, 2, 4, 6, 10, 12, 18, 22, 28, 30, 42, 58, 60, \\ & 70, 78, 102, 130, 190, 210, 330, 462. \end{aligned}$$

Remark: Gauss (Disquisitiones Arithmeticae) conjectured that there are only finitely many d's with $h(-4d) = g(-4d)$; this was proven by Chowla (1934). It is also conjectured that $d \le 1848$, but this does not seem to have been proved yet. This is known to be true for $d \le 10^{11}$ (Swift), and hence is true in general if we admit GRH = Generalized Riemann Hypothesis. (This requires a delicate refinement of the method of Hecke/Landau (1918).)

Theorem 2: Let C be a curve of type d.

(a) If $d \not\equiv 3 \pmod 4$, then q_C is a primitive binary quadratic form of discriminant $-16d$, and q_C is in the principal genus, i.e. $q_C \sim q_1^2$, for some quadratic form q_1. Moreover, q_C is not the principal class: $q_C \not\sim x^2 + 4dy^2$.

(b) If $d \equiv 3 \pmod 4$, then either q_C is as in (a) or $q_C = 4q$, where q is a primitive quadratic form of discriminant $-d$ which lies in the principal genus.

Theorem 3: If q is a quadratic form of the type given in Theorem 2, and if (E_1, E_2) has type d, then there exists a curve C (of type d) with

$$J_C \simeq E_1 \times E_2 \quad \text{and} \quad q_C \sim q.$$

In fact, there are $2^{\omega(d)-1}$ or $2^{\omega(d)-2}$ such curves C.

4. Application to elliptic subfields

Theorem 4: Suppose C is a curve of type d.

(a) If $d \not\equiv 3 \pmod 4$ or if $\#\mathcal{E}^*_C(n) \neq 0$ for some odd n, then there exist infinitely many primes p with $\#\mathcal{E}^*_C(p) \neq 0$.

(b) If $\#\mathcal{E}^*_C(n) = 0$ for all odd n ($\Rightarrow d \equiv 3 \pmod 4$), then there exist infinitely many primes p with $\#\mathcal{E}^*_C(2p) \neq 0$.

Proof. Use the fact (Dirichlet/Weber) that a primitive binary quadratic form represents infinitely many primes.

Theorem 5: Suppose C_1, C_2 are two curves of type d. If there exists a prime p such that $\#\mathcal{E}^*_{C_i}(p) \neq 0$, for $i = 1, 2$, then $q_{C_1} \sim q_{C_2}$ and hence

$$\#\mathcal{E}^*_{C_1}(n) = \#\mathcal{E}^*_{C_2}(n), \quad \text{for all } n > 1.$$

Proof. Use the fact (Piehler) that if two primitive binary quadratic forms of the same discriminant represent the same prime p, then they are equivalent.

5. Curves with a given Jacobian

Let A $(= E_1 \times E_2)$ be an abelian surface,

$NS(A) = \mathrm{Div}(A)/(\text{num. equiv.})$ its Néron-Severi group,

$\mathcal{P}(A) = \{cl(D) \in NS(A) : D^2 = 2, (D.\theta) > 0\}$

$= $ set of principal polarizations on A

Torelli's Theorem: The map $C \mapsto cl(C)$ induces a bijection

$$\{C : J_C \simeq A\}/\simeq \;\; \xrightarrow{\sim} \;\; \mathcal{P}(A)^{irr}/\,\mathrm{Aut}(A),$$

where $\mathcal{P}(A)^{irr} = \{cl(D) \in \mathcal{P}(A) : D \text{ is irreducible}\}$.

Here: $A = E_1 \times E_2$, where (E_1, E_2) is of type d,

$NS(A) = \mathbb{Z}D_1 + \mathbb{Z}D_2 + \mathbb{Z}D_3 \simeq \mathbb{Z}^3$, where the basis

D_1, D_2, D_2 is chosen such that

$(a, b, c)^2 := (aD_1 + bD_2 + cD_3)^2 = 2(ab - cd)$.

Thus: $\mathcal{P}(A) \xrightarrow{\sim} \{(a, b, c) \in \mathbb{Z}^3 : ab - cd = 1, a > 0\}$.

Proposition 1: The map $\theta = (a, b, c) \mapsto f_\theta = [ad, 2cd, b] := adx^2 + 2cdxy + by^2$ induces a bijection:

$$\mathcal{P}(A)/\,\mathrm{Aut}(A) \xrightarrow{\sim} \mathcal{H}(-4d)/\,\mathrm{GL}_2(\mathbb{Z}),$$

where $\mathcal{H}(D) = \{[a, b, c] : b^2 - 4ac = D, a > 0, \gcd(a, b, c)|2\}$.
Thus $\#(\mathcal{P}(A)/\,\mathrm{Aut}(A)) = H(d) = \#(\mathcal{H}(-4d)/\,\mathrm{GL}_2(\mathbb{Z}))$.

Main Difficulty: Via the above bijection, how can we identify the image of $\mathcal{P}(A)^{irr}$ in $\mathcal{H}(-4d)$?

Basic Idea: Use the generalized Humbert invariant q_C!

6. The Generalized Humbert Invariant q_C

Definition: Let (A, θ) be a principally polarized abelian surface (i.e. $\theta \in \mathcal{P}(A)$). The generalized Humbert invariant is

$$q_\theta(D) = (D.\theta)^2 - 2(D.D), \quad \text{for } D \in NS(A).$$

Properties: 1) The map q_θ defines a positive definite quadratic form on

$$NS(A, \theta) := NS(A)/\mathbb{Z}\theta.$$

2) If $A = E_1 \times E_2$, then $rk(NS(A, \theta)) = 2$ and $\operatorname{disc}(q_\theta) = -16d$.

Remark: The above definition and property 1) can be found in [K] = Elliptic curves on abelian surfaces, *Manusc. math.* 84 (1994). This paper also explains the connection between q_θ and the (classical) Humbert invariant (defined via period matrices).

Key Fact: $\theta \in \mathcal{P}(A)^{irr} \Leftrightarrow q_\theta$ does not represent 1.

Question: Given $\theta = (a, b, c) \in \mathcal{P}(A)$, what is the relation between the binary quadratic form f_θ (of discriminant $-4d$) and the binary quadratic form q_θ (of discriminant $-16d$)?

Lemma: Let $Cl(D)$ denote the group of equivalence classes of primitive binary quadratic forms of discriminant D. Then there is a unique group homomorphism

$$\rho = \rho_d : Cl(-4d) \to Cl(-16d) \text{ s. th. } \pi(\rho(cl(f))) = cl(f)^2,$$

where $\pi : Cl(-16d) \to Cl(-4d)$ is the canonical map.

Theorem 6: (a) If f_θ is primitive, then $q_\theta \sim \rho(f_\theta)$.

(b) If f_θ is not primitive, then $\frac{1}{2}f_\theta$ is primitive and $\frac{1}{4}q_\theta \sim (\frac{1}{2}f_\theta)^2$.

7. Numerical Examples

Assume: $J_C \simeq E_1 \times E_2$, where (E_1, E_2) has type $d \leq 20$. Then we have the following possibilities (and these all occur):

d	θ	q_C	degrees n of max. ellip. subfields, $n \leq 50$
3	$(2, 2, 1)$	$(4, 4, 4)$	$2, 14, 26, 38$
5	$(2, 3, 1)$	$(4, 0, 5)$	$2, 3, 7, 18, 23, 27, 42, 43, 47$
7	$(4, 2, 1)$	$(4, 4, 8)$	$2, 4, 8, 16, 22, 32, 44, 46$
8	$(3, 3, 1)$	$(4, 4, 9)$	$2, 3, 11, 18, 19, 27, 34, 43$
9	$(2, 5, 1)$	$(4, 0, 9)$	$2, 3, 5, 17, 26, 29, 30, 39, 41, 50$
11	$(3, 4, 1)$	$(5, 2, 9)$	$3, 4, 5, 9, 12, 15, 20, 23, 25, 31, 36, 37, 45$
11	$(6, 2, 1)$	$(4, 4, 12)$	$2, 6, 10, 18, 30, 46, 50$
13	$(2, 7, 1)$	$(4, 0, 13)$	$2, 7, 11, 19, 31, 34, 47$
14	$(3, 5, 1)$	$(8, 8, 9)$	$3, 5, 13, 19, 27, 45$
15	$(8, 2, 1)$	$(4, 4, 16)$	$2, 4, 8, 16, 32, 34, 38, 46$
15	$(4, 4, 1)$	$(4, 4, 16)$	$2, 4, 8, 16, 32, 34, 38, 46$
16	$(13, 5, 2)$	$(4, 4, 17)$	$2, 5, 8, 13, 29, 34, 37, 40, 50$
17	$(2, 9, 1)$	$(4, 0, 17)$	$2, 9, 13, 21, 33, 42, 49$
17	$(3, 6, 1)$	$(8, 4, 9)$	$3, 6, 7, 11, 14, 22, 23, 27, 31, 39, 46$
19	$(4, 5, 1)$	$(5, 4, 16)$	$4, 5, 7, 11, 17, 20, 25, 28, 35, 43, 44, 47, 49$
19	$(10, 2, 1)$	$(4, 4, 20)$	$2, 10, 14, 22, 34, 46, 50$

Recall: If $d = 1, 2, 4, 6, 10, 12, 18, 22, 28, 30, 42, 58, 60, 70, 78, 102, 130, 190, 210, 330, 462$, then there is *no* curve of type d.