Kummer theory on elliptic curves

Linda Raabe

Master thesis
Advisor: Professor Emmanuel Kowalski
at ETH Zürich
31.10.2012

Contents

1 Acknowledgements 4

2 Motivation 5

3 Known results 6

4 A criterion for the size of the Galois group in the case $\ell = 2$ 12

5 Numerical examples for the case $\ell = 2$ 16

6 Further Steps 18

Bibliography 20

1 Acknowledgements

First I want to thank my thesis advisor, Emmanuel Kowalski, for being a very patient, motivating and inspiring advisor. He has been an excellent advisor!
Furthermore I want to thank Philipp Habegger who was also always feeding me good ideas and new approaches.
I sincerely want to thank my boyfriend, friends and family. Their love and support has made everything much easier.
I specially thank Katharina Barth, Laura Hindersin, Sebastian Schön and Sonja Spies for proofreading my thesis and finding tons of mistakes.

2 Motivation

In 1988 Paul Erdős asked:

Question 2.1
Let a and b be positive integers with the property that for every $n > 0$ the set of prime numbers dividing $a^n - 1$ is equal to the set of prime numbers dividing $b^n - 1$. What can one say about a and b?

We call this the *support problem* since the set of prime numbers dividing a is called the *support* of a. In order to solve the support problem we need Kummer theory.

Theorem 2.1 (Kummer theory for the multiplicative group)
Let ℓ be a prime number and let K be a number field that contains all ℓ-th roots of unity. If $x \in K^*$ is not an ℓ-th power then $K(\sqrt[\ell]{x})$ is "big" which means that the Galois group $Gal(K(\sqrt[\ell]{x})/K)$ is maximal, i.e. $Gal(K(\sqrt[\ell]{x})/K) \cong \{\ell\text{-th roots of unity}\} \cong \mathbb{Z}/\ell\mathbb{Z}$.

To see that Kummer theory also works for elliptic curves we cite a theorem by Kowalski and sketch the proof at the end of the next chapter.

Theorem 2.2 ([Kow], theorem 3.3)
Let p_0 be a prime, $E(\mathbb{Q})$ an elliptic curve without complex multiplication and $P, Q \in E(\mathbb{Q})$ points of infinite order such that $(P \bmod p) \in (< Q > \bmod p)$ for all primes $p > p_0$. Then $P \in < Q >$.

3 Known results

From now on let K be a number field, $G = Gal(\bar{K}/K)$ its Galois group. Let E/K be an elliptic curve without complex multiplication.

Definition 3.1 (Irreducible and semi-simple)
Let R be a ring, M an R-module such that a group H acts on M R-lineary. Then M is called irreducible (or simple) if the only H-submodules are M itself and $\{0\}$.
M is called semi-simple if it is the direct sum of its irreducible H-submodules.

Proposition 3.2
Let M be semi-simple. Then

i) for all G-modules $N \subset M$ there exists a G-module N' such that $M = N' \bigoplus N$

ii) for all G-submodules $N \subset M$ there exists a projection $f : M \to N$ which commutes with G.

Proof
i): Let $N \subset M$ be a G-submodule. Since M is the sum of its irreducible submodules, we have $M = \bigoplus_{i=1}^{n} N_i$ and there must exist an $I \subset \{1, ..., n\}$ such that $N = \bigoplus_{i \in I} N_i$ and we get that $M = \bigoplus_{i \in I} N_i \oplus \bigoplus_{i \notin I} N_i$.
ii): Let $N \subset M$ be a G-submodule and $N' \subset M$ such that $M = N \bigoplus N'$. Then we can express $m \in M$ uniquely as $m = \sum_{i \in I} a_i n_i + \sum_{i \notin I} a_i n_i$ with $n_i \in N_i$ and $a_i \in R$ and we can find a projection $f : M \to N, m \mapsto \sum_{i \in I} a_i n_i$. □

Definition 3.3 (Cohomology group H^0 [Silv])
Let M be a G-module. The 0^{th} *cohomology group* is

$$H^0(G, M) = \{m \in M : m^\sigma = m \, \forall \sigma \in G\} = M^G.$$

Definition 3.4 (Cohomology group H^1 [Silv])
Let M be a G-module. The group of 1-cochains from G to M is defined by

$$C^1(G, M) = \{\text{maps } \xi : G \to M\}.$$

The group of 1-cocycles from G to M is given by

$$Z^1(G, M) = \{\xi \in C^1(G, M) : \xi_{\sigma\tau} = \xi_\sigma^\tau + \xi_\tau \, \forall \sigma, \tau \in G\}.$$

The group of 1-coboundaries from G to M is defined by

$$B^1(G, M) = \{\xi \in C^1(G, M) : \exists m \in M : \xi_\sigma = m^\sigma - m \, \forall \sigma \in G\}.$$

Since $\xi_\sigma^\tau = (m^\sigma - m)^\tau = m^{\sigma\tau} - m^\tau = m^{\sigma\tau} - m - (m^\tau - m) = \xi_{\sigma\tau} - \xi_\tau$ we have $B^1(G,M) \subset Z^1(G,M)$, so we can define the 1^{st} *cohomology group* as the quotient group

$$H^1(G,M) = \frac{Z^1(G,M)}{B^1(G,M)}.$$

In other words, $H^1(G,M)$ is the group of 1-cocycles $\xi : G \to M$ modulo the equivalence relation of two cocycles being equivalent if their difference is of the form $\sigma \mapsto m^\sigma - m$ for some $m \in M$.

Definition 3.5 (Commutant)
Let G be a group and S be a subgroup of G. Then the commutant of S in G is

$$\{g \in G | gs = sg \quad \forall s \in S\}.$$

Definition 3.6 (ℓ-torsion)
Let E be an elliptic curve, $\mathcal{O}$ the point at infinity and ℓ be a prime number. Then we call $E[\ell] := \{P \in E | \ell P = \mathcal{O}\}$ the ℓ-torsion points.

For a prime number ℓ, consider the representation $\rho_\ell : G \to Aut(E[\ell])$ and let $G_\ell = im\rho_\ell$ and $H_\ell = ker\rho_\ell$.

Remark
We know that $E[\ell]$, as an abelian group, is isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^2$. In other words: We can choose a basis $P, Q \in E[\ell]$ of $E[\ell]$ and get a linear action of $GL_2(\mathbb{Z}/\ell\mathbb{Z})$ on $E[\ell]$. Since G_ℓ is a subgroup of $GL_2(\mathbb{Z}/\ell\mathbb{Z})$, it also acts on $E[\ell]$ linearly.

In his paper [Rib], Ribet defines the following axioms that we need to state our main theorem:

Axiom ($B_{1,\ell}$)
The commutant of G_ℓ in $\mathbb{F}_\ell^{2\times 2}$ is equal to $\mathbb{Z}/\ell\mathbb{Z}$.

Axiom ($B_{2,\ell}$)
$E[\ell]$ is semi-simple as a G_ℓ-module over $\mathbb{Z}/\ell\mathbb{Z}$.

Axiom ($B_{3,\ell}$)
The cohomology group $H^1(G_\ell, E[\ell])$ vanishes.

Axiom (B_4)
For each finitely generated subgroup Γ of $E(K)$, the division group $\Gamma' = \{Q \in E(K) | mQ \in \Gamma \text{ for some } m \geq 1\}$ is such that Γ'/Γ has finite exponent.

At first the axioms may seem very random but later in the proof we will see that we really need all of them.
From Serre's famous theorem, the main theorem in [Ser], we know that axioms for almost all ℓ, i.e. for all but finitely many, $B_{1,\ell}, B_{2,\ell}$ and $B_{3,\ell}$ are true:

- $B_{1,\ell}$: The commutant of $GL_2(\mathbb{F}_\ell)$ in $\mathbb{F}_\ell^{2\times 2}$ is $\mathbb{Z}/\ell\mathbb{Z}$.
- $B_{2,\ell}$: $E[\ell]$ is semi-simple as a $GL_2(\mathbb{F}_\ell)$-module over $\mathbb{Z}/\ell\mathbb{Z}$ since it is already irreducible.
- $B_{3,\ell}$: For this let $\ell > 2$ be a prime number, $\sigma \in G_\ell$, $f \in H^1(G_\ell, E[\ell])$ and $\alpha \neq Id$ in the center of G_ℓ. Then α acts on $H^1(G_\ell, E[\ell])$ by $(\alpha f)(\sigma) = \alpha(f(\sigma))$ and we have

$$\begin{aligned} f(1) = f(1\cdot 1) = f(1) + 1\cdot f(1) = 2\cdot f(1) &\Rightarrow f(1) = 0. \\ 0 = f(1) = f(\alpha\alpha^{-1}) = f(\alpha) + \alpha\cdot f(\alpha^{-1}) &\Rightarrow \alpha\cdot f(\alpha^{-1}) = -f(\alpha^{-1}). \\ f(\sigma) = f(\alpha\sigma\alpha^{-1}) &= f(\alpha) + \alpha\cdot f(\sigma\alpha^{-1}) \\ &= f(\alpha) + \alpha\cdot f(\sigma) + \alpha\sigma\cdot f(\alpha^{-1}) \\ &= f(\alpha) + \alpha\cdot f(\sigma) - \sigma f(\alpha) \\ \Rightarrow \alpha f(\sigma) - f(\sigma) &= \sigma\cdot f(\alpha) - f(\alpha) = 0 \text{ in } H^1(G_\ell, E[\ell]). \end{aligned}$$

  So the map $f \mapsto \alpha f - f$ is the zero map and annihilates $H^1(G_\ell, E[\ell])$. Since $\beta = \alpha - Id$ is just multiplication by β we also get an inverse which is multiplication with β^{-1} (which exists since β is nonzero). Then β is the zero map and it is an automorphism of $H^1(G_\ell, E[\ell])$. Therfore $H^1(G_\ell, E[\ell])$ has to be zero.

The fact that also axiom B_4 is true is the following proposition.

Proposition 3.7
If K is a number field, then E satisfies B_4.

Proof
This is a consequence of the Mordell-Weil theorem: Since $E(K)$ is finitely generated, every subgroup is also finitely generated. Let Γ' be generated by $Q_1, ..., Q_r$. Then there exist $m_1, ..., m_r$ such that $m_i Q_i =: P_i \in \Gamma$. Let $m = lcm(m_1, ..., m_r)$ then for all $x = \sum_{i=1}^n a_i Q_i \in \Gamma$ we have $mx = \sum_{i=1}^n a_i m Q_i = \sum_{i=1}^n a_i \frac{m}{m_i} m_i Q_i = \sum_{i=1}^n a_i \frac{m}{m_i} P_i = 0 \in \Gamma$. Thus the exponent of Γ'/Γ is at most m and hence finite. □

Definition 3.8 (Linearly independent)
Let E be an elliptic curve and let $P_1, ..., P_t$ be points on $E(\mathbb{C})$. We say that these elements are *linearly independent* (over $\mathbb{Z}$) if the equation

$$a_1 P_1 + ... + a_t P_t = 0$$

implies that all $a_i = 0$. For a $\mathbb{Z}$-submodule N of $E(\mathbb{C})$, we say that the P_i are *linearly independent mod N*, if their images in $E(\mathbb{C})/N$ are linearly independent. When N is generated by a family of elements $\{Q_j\}$ of $E(\mathbb{C})$, we simply say that the P_i are linearly independent mod the Q_j.

Proposition 3.9 ([Rib])
Let $P_1, ..., P_t$ be linearly independent points on $E(K)$. Let ℓ be a prime number, then the images of the P_i in $E(K)/\ell E(K)$ are linearly independent over $\mathbb{Z}/\ell\mathbb{Z}$.

Proof
Suppose the P_i are not linearly independent. Then we can find a_i, not all zero, such that for all primes ℓ we have $\sum_{i=1}^{t} a_i P_i \equiv 0 \bmod \ell$. Then $Q := \sum_{i=1}^{t} a_i P_i$ is divisible by ℓ. But by axiom B_4 no point in $E(K)$ can be divisible by infinitely many primes. But because of this contradiction, the P_i must be linearly independent. □

Proposition 3.10 (Restriction-Inflation-Sequence)
We have the following exact sequence:

$$0 \to H^1(G_\ell/H_\ell, E[\ell]) \overset{Inf}{\to} H^1(G_\ell, E[\ell]) \overset{Res}{\to} H^1(H_\ell, E[\ell])$$

Proof
The proof can be found in [Silv, p. 417, Prop. 1.3]. □

The following paragraph is mostly summarized from [Rib].
Now let's start with the actual Kummer theory. Let ℓ be a prime that satisfies the axioms $B_{1,\ell}$, $B_{2,\ell}$ and $B_{3,\ell}$, for each rational point P on $E(K)$ we define the Kummer map

$$\xi(P) : H_\ell \to E[\ell], \sigma \mapsto \sigma(Q) - Q$$

where $Q \in E(\bar{K})$ is such that $\ell Q = P$.
The map $P \mapsto \xi(P)$ is the composition of a coboundary map

$$E(K)/\ell E(K) \hookrightarrow H^1(G_\ell, E[\ell])$$

and the restriction map

$$H^1(G_\ell, E[\ell]) \hookrightarrow H^1(H_\ell, E[\ell]).$$

For $P \in H_\ell$ we have $l\xi(P) = l(\sigma(Q) - Q) = \sigma(\ell Q) - \ell Q = \sigma(P) - P = P - P = \mathcal{O}$, therefore $\xi(P) \in E[\ell]$.
The restriction map is injective because by proposition 3.10 it has kernel $H^1(G_\ell, E[\ell])$ which vanishes by axiom $B_{3,\ell}$.
Furthermore we get an exact sequence $1 \to E[\ell](K) \to E(K) \overset{*\ell}{\to} \ell E(K) \to 1$. Thus we get a long exact sequence:

$$0 \longrightarrow H^0(G, E[\ell](K)) \longrightarrow H^0(G, E(K)) = E(K) \longrightarrow H^0(G, \ell E(K)) = \ell E(K) \xrightarrow{\delta}$$
$$H^1(G, E[\ell](K)) \longrightarrow H^1(G, E(K)) \longrightarrow H^1(G, E(K))$$

The kernel of the coboundary map above is $\ell E(K)$ and we get that the coboundary map $E(K)/\ell E(K) \hookrightarrow H^1(G_\ell, E[\ell])$ from before is injective.
Since those maps are injective whenever E satisfies $B_{3,\ell}$, $P \mapsto \xi(P)$ is also injective. It is also linear: Let $\ell Q = P, \sigma \in H_\ell$ and $a \in \mathbb{Z}$:

$$\xi(aP)(\sigma) = \sigma(aQ) - aQ = a(\sigma(Q) - Q) = a(\xi(P)(\sigma)).$$

Also, G acts on $E[\ell]$. Let $\tau \in G$, then:

$$\begin{aligned}
\xi(P)(\tau\sigma\tau^{-1}) &= \tau\sigma\tau^{-1}(Q) - Q \\
&= \tau(\sigma\tau^{-1}(Q) - \tau^{-1}(Q)) \\
&= \tau(\sigma\tau^{-1}(Q) - \sigma(Q) + \sigma(Q) - \tau^{-1}(Q)) \\
&= \tau(\sigma(\tau^{-1}(Q) - (Q)) + \sigma(Q) - \tau^{-1}(Q)) \\
&= \tau(\tau^{-1}(Q) - (Q) + \sigma(Q) - \tau^{-1}(Q)) \\
&= \tau(\sigma(Q) - (Q)) \\
&= \tau(\xi(P))
\end{aligned}$$

And therefore, the map $P \mapsto \xi(P)$ is an injective, linear map which is compatible with G.
Now let again $P_1, \ldots, P_n$ be points on E, not necessarily linearly independent. Then we let $\varphi_i = \xi(P_i)$ and $\varphi : H_\ell \to E[\ell]^n$ be the product of the $\varphi_i's$. Then the kernel of φ is the Galois group of the field $K(E[\ell], \frac{1}{\ell}P_i)$ which is obtained by adjoining all ℓ-torsion points and of the P_i.

Remark
We call the points $\frac{1}{\ell}P$ (ℓ-)division points.
It does not matter whether we adjoin one division point or all division points since the difference of two ℓ-division points is an ℓ-torsion point.

Theorem 3.11
Let E be an elliptic curve without complex multiplication and let ℓ be a prime such that axioms $B_{1,\ell}, B_{2,\ell}$ and $B_{3,\ell}$ hold. Let t be an integer with $1 \leq t \leq n$. Assume that the points $P_1, \ldots, P_t$ are linearly independent over $\mathbb{Z}$ modulo the points $P_{t+1}, \ldots, P_n$. Then the image of φ contains the group $N := E[\ell]^t \times 0^{n-t}$.

Proof
By 3.9, the points $P_1, \ldots, P_t$ are linearly independent in $E/\ell E$. Let $\varphi_i := \xi(P_i)$, $\varphi = (\varphi_1, \ldots, \varphi_n)$ and $M = \operatorname{im}\varphi$. Since ξ is injective, the φ_i are linearly independent.
Then since $\varphi_i(\tau\sigma\tau^{-1}) = \tau\varphi_i$, M is a G-submodule of $E[\ell]^n$. Suppose now, M does not contain $N := E[\ell]^t \times 0^{n-t}$.
Since $E[\ell]^n$ is G-semisimple, we can find a linear map $f : E[\ell]^n \to E[\ell]^n$ which commutes with G and whose kernel contains M but not N. Composing f with a suitable linear projection $E[\ell]^n \to E, (v_1, ..., v_n) \mapsto \sum_{i=1}^n b_i v_i$ we find a G-equivariant linear map $g : E[\ell]^n \to E$ whose kernel contains M but not N. Since g is linear, we can express it as $g(v_1, \ldots, v_n) = \sum_{i=1}^n a_i v_i$ with $a_i \in \mathbb{Z}/\ell\mathbb{Z}$ because of $B_{1,\ell}$.
Now g maps M to zero, so $\sum_{i=1}^n a_i\varphi_i = 0$, but g does not map N to zero, so there exist $R_1, \ldots, R_t$ such that $\sum_{i=1}^t a_i R_i \neq 0$. Therefore not all of the $a_1, \ldots, a_t$ can be zero and we found a sum $\sum_{i=1}^n a_i\varphi_i = 0$ where not all coefficients are zero, so the φ_i are not linearly independent. But this is a contradiction since we showed above that they are linearly independent. □

We want to use this result to sketch the proof of theorem 2.2 from before.

Proof (of theorem 2.2)
Lemma 5.1 in [Kow] tells us that for finite extensions K and L of $\mathbb{Q}$ we have $K \subset L$ if and only is almost all primes that are totally split in L are also totally split in K. So since a prime $\mathfrak{p}$ of good reduction which is split in $\mathbb{Q}(E[\ell], \frac{1}{\ell}Q)$ is by [Kow], Lemma 4.6, also split in $\mathbb{Q}(E[\ell])$ and Q is an ℓ-th power in $E(\mathbb{Q})$ mod $\mathfrak{p}$. But then also P is an ℓ-th power and so $\mathfrak{p}$ is also totally split in $\mathbb{Q}(E[\ell], \frac{1}{\ell}P)$. Thus we get $\mathbb{Q}(E[\ell], \frac{1}{\ell}Q) \subset \mathbb{Q}(E[\ell], \frac{1}{\ell}P)$ for all primes ℓ.
Here is where the Kummer theory comes in: Since the Galois group of $\mathbb{Q}(E[\ell], \frac{1}{\ell}Q, \frac{1}{\ell}P)$ is not maximal, the points P and Q cannot have been linearly independent. Thus we find $m, n \in \mathbb{Z} \setminus \{0\}$ such that $mP = nQ$ and now we get back to the first condition: We can look at $mP = nQ$ mod p for infinitely many p and comparing with $P \equiv n(p)Q$ mod p from the condition, we get $nQ \equiv n(p)mQ$ mod p. Since both points are of infinite order and because of Lemma 6.3 in [Kow] we find p such that $n|m$. So we can divide m by n and get $P = \frac{m}{n}Q + T$ where T is a torsion point. Lemma 6.4 in [Kow] tells us that $T = 0$ and hence $P \in < Q >$. $\square$

4 A criterion for the size of the Galois group in the case $\ell = 2$

From now on let K be a number field, $\lambda \in K \setminus \{0, 1\}$ and

$$E : y^2 = x(x-1)(x-\lambda) = x^3 - (\lambda+1)x^2 + \lambda x$$

an elliptic curve.
In the last chapter we proved that for all but finitely many prime numbers ℓ the Galois group of the ℓ-division points is maximal. One of the conditions was axiom $B_{1,\ell}$ which states that the Galois group of the ℓ-torsion point has to be "big". Our aim is to study the simplest case where not all of the axioms are true. Since for an elliptic curve in Legendre form all 2-torsion points are rational, we want to concentrate on curves in Legendre form. Then axiom $B_{1,2}$ fails and axioms $B_{2,2}$ and $B_{3,2}$ are true.
For a point P on E of infinite order, which is not already a double, two cases of Galois groups can occur: It could have order two or order four. During the next two chapters we will find a criterion for the size of this Galois group and show that actually both sizes occur. Looking at $\ell = 2$ gives us another nice simplification:

Theorem 4.1
Let $P = (x_P, y_P)$ be a point on $E(K)$, not a 2-torsion point, and $Q = (x, y)$ such that $2Q = P$. Then we have $K(x) = K(x, y)$.

Proof
Let $\sigma \in Gal(K(x,y)/K(x))$ which is not the identity then $\sigma(x) = x$ and

$$\sigma(y^2) = \sigma(x(x-1)(x-\lambda)) = x(x-1)(x-\lambda) = y^2.$$

We get $\sigma(y) = -y$ and hence $\sigma(Q) = -Q$. But this gives

$$2Q = \sigma(2Q) = -2Q \Rightarrow 4Q = \mathcal{O} \Rightarrow 2P = \mathcal{O} \lightning .$$

So there is no element in $Gal(K(x,y)/K(x))$ except for the identity and therefore $K(x,y) = K(x)$. □

Now that we only have to care about x we will compute its minimal polynomial. Let E, P and Q be as above. By [Silv], p. 54, we know that

$$x_P = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}$$

with

$$\begin{aligned} b_2 &= -4(\lambda+1) \\ b_4 &= 2\lambda \\ b_6 &= 0 \\ b_8 &= -\lambda^2 \end{aligned}$$

So we get

$$\begin{aligned} x_P &= \frac{x^4 - 2\lambda x^2 + \lambda^2}{4x^3 - 4(\lambda+1)x^2 + 4\lambda x} \\ \Leftrightarrow 0 &= x^4 - 2\lambda x^2 + \lambda^2 - x_P(4x^3 - 4(\lambda+1)x^2 + 4\lambda x) \\ \Leftrightarrow 0 &= x^4 - 4x_P x^3 + (4(\lambda+1)x_P - 2\lambda)x^2 - 4\lambda x_P x + \lambda^2 =: P_x. \end{aligned}$$

Now we want to find a criterion that helps us decide whether this polynomial factors into two quadratic polynomials or not. If it factors into two quadratics, we would have $P_x = (x^2 + ax + b)(x^2 + cx + d)$ with $a, b, c, d \in K$. So let's find out when this happens:

$$\begin{aligned} a + c &= -4x_P \\ ac + b + d &= 4(\lambda+1)x_P - 2\lambda \\ bc + ad &= -4x_P\lambda \\ bd &= \lambda^2. \end{aligned} \tag{4.1}$$

This gives

$$a = -4x_P - c \tag{4.2}$$

$$b = \frac{\lambda^2}{d} \qquad (\lambda \text{ is nonzero, so } b \text{ and } d \text{ are also nonzero}).$$

And those two combined with 4.1 give

$$\begin{aligned} \frac{\lambda^2}{d}c + (-4x_P - c)d &= -4x_P\lambda \\ \Leftrightarrow c(\frac{\lambda^2}{d} - d) &= -4x_P\lambda + 4x_P d. \end{aligned} \tag{4.3}$$

Now we get two cases: Either $\frac{\lambda^2}{d} - d$ is zero or nonzero.

Case 1: $\frac{\lambda^2}{d} = d$.
Since $-4x_P\lambda + 4x_P d = 0$ we get $\lambda = d = b$. Furthermore,

$$\begin{aligned}
ac + \lambda + \lambda &= 4(\lambda+1)x_P - 2\lambda \\
\Leftrightarrow ac &= 4(\lambda+1)x_P - 4\lambda \\
\Leftrightarrow c(-4x_P - c) &= 4(\lambda+1)x_P - 4\lambda \\
\Leftrightarrow -c^2 - 4x_P c - 4(\lambda+1)x_P + 4\lambda &= 0 \\
\Leftrightarrow c^2 + 4x_P c + 4(\lambda+1)x_P - 4\lambda &= 0 \\
\Leftrightarrow c &= -2x_P \pm \sqrt{4x_P^2 - 4(\lambda+1)x_P + 4\lambda} \\
\Leftrightarrow c &= -2x_P \pm 2\sqrt{x_P^2 - (\lambda+1)x_P + \lambda} \\
\Leftrightarrow c &= -2x_P \pm 2\frac{y_p}{\sqrt{x_P}} \\
\overset{4.2}{\Leftrightarrow} a &= -2x_P \mp 2\frac{y_p}{\sqrt{x_P}}.
\end{aligned}$$

So a and c are in $\mathbb{Q}$ if and only if x_P is a square in K.

Case 2: $\frac{\lambda^2}{d} \neq d$.
Now we can get back to the equation 4.3 and divide it by $\frac{\lambda^2}{d} - d$:

$$\begin{aligned}
\Rightarrow c &= \frac{1}{\frac{\lambda^2}{d} - d}(-4\lambda x_P + 4x_P d) \\
&= \frac{d}{\lambda^2 - d^2}(-4\lambda x_P + 4x_P d) \\
&= \frac{-4dx_P}{\lambda^2 - d^2}(\lambda - d) \\
&= -\frac{4dx_P}{\lambda + d} \\
\Rightarrow a &= -4x_P + \frac{4dx_P}{\lambda + d} \\
&= 4x_P(\frac{d}{\lambda + d} - 1) \\
&= 4x_P(\frac{d}{\lambda + d} - \frac{\lambda + d}{\lambda + d}) \\
&= -\frac{4x_P\lambda}{\lambda + d}
\end{aligned}$$

$$ac + b + d - (4(\lambda+1)x_P - 2\lambda) = 0$$

$$\Leftrightarrow \frac{-4dx_P}{\lambda + d}\frac{-4x_P\lambda}{\lambda + d} + \frac{\lambda^2}{d} + d - (4(\lambda+1)x_P - 2\lambda) = 0$$

$$\Leftrightarrow 16x_P^2 d\lambda + (\lambda+d)^2\frac{\lambda^2}{d} + (\lambda+d)^2 d - (\lambda+d)^2(4(\lambda+1)x_P - 2\lambda) = 0$$

Now one can show (the computations for this are ugly but easy to check) that this is equivalent to

$$d^4 + 4d^3(-(\lambda+1)x_P + \lambda) + 2\lambda d^2(8x_P^2 - 4(\lambda+1)x_P + 3\lambda) + 4\lambda^2 d(-(\lambda+1)x_P + \lambda) + \lambda^4 = 0$$

So if and only if the polynomial

$$P(X,\lambda,x_p) = X^4 + 4X^3(-(\lambda+1)x_P + \lambda) + 2\lambda X^2(8x_P^2 - 4(\lambda+1)x_P + 3\lambda) + 4\lambda^2 X(-(\lambda+1)x_P + \lambda) + \lambda^4$$

has a zero in K, we can compute

$$a = -\frac{4x_P\lambda}{\lambda+d}$$
$$b = \frac{\lambda^2}{d}$$
$$c = -\frac{4dx_P}{\lambda+d}$$

and get a factorization of P_x over K.
Altogether we turned a hard algebraic problem into a much easier arithmetic condition:

Theorem 4.2
Let $E : y^2 = x(x-1)(x-\lambda)$ be an elliptic curve and let $P = (x_P, y_P)$ be a point on $E(K)$ of infinite order which is not a rational double. Let $Q = (x,y) \in E(\bar{K})$ such that $2Q = P$. Then the Galois group of $K(x,y)$ is of order two if and only if x_P is a square in K or $P(X,\lambda,x_p)$ has a zero in K.

5 Numerical examples for the case $\ell = 2$

Firs we stay in the case of the chapter before: Let $E : y^2 = x(x-1)(x-\lambda)$ be an elliptic curve over $\mathbb{Q}$ (so all 2-torsion points are rational). We provided a criterion for the size of the Galois group. Now we want to see how often we get the full Galois group and if we get the small Galois group, we want to see how often we get that x_P is a rational square. We want to present two examples to show that actually both sizes of Galois groups can occur.

Let $E : y^2 = x(x-1)(x-11)$ and $P = (99, 924)$. Then

$$Q = (-\frac{1}{2}\sqrt{1440i - 1512} - 20i - 8, \frac{1}{4}\sqrt{(3840i + 9424)\sqrt{1440i - 1512} + 464960i - 3792}\sqrt{2})$$

is such that $2Q = P$. So $[\mathbb{Q}(E[2], \frac{1}{2}P) : \mathbb{Q}(E[2])] = [\mathbb{Q}(\sqrt{1440i - 1512}) : \mathbb{Q}] = 4$ and we have a maximal Galois group.

Let $E : y^2 = x(x-1)(x-7)$ and $P = (9, 12)$. Then

$$Q = (-9\sqrt{2} + 13, 3\sqrt{-9\sqrt{2} + 13}\sqrt{3\sqrt{2} - 4}\sqrt{3\sqrt{2} - 2})$$

is such that $2Q = P$. So $[\mathbb{Q}(E[2], \frac{1}{2}P) : \mathbb{Q}(E[2])] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and we don't have a maximal Galois group.

We will see that in our computations about half of the Galois groups are of the small type and that about two thirds of the small Galois groups admit a rational square x_P. Now we want to start with our computations in the computer program Sage.
First, we want to find some curves with positive rank and save them to save computing time later:

```
CurvesWithPositiveRank = []
ArrayOfL = range(-10000,10000)
for L1 in Set(range(-10000,10000)):
  for L2 in range(2,100):
    if gcd(L1, L2) == 1:
      ArrayOfL.append(Rational(L1)/Rational(L2))
for L in ArrayOfL:
  try:
    e = EllipticCurve([0,-L-1,0,L,0])
  except:
    n = n
```

```
  try:
    gen = e.gens()
  except:
    gen = e.gens(proof = False)
  if len(gen) > 0:
    CurvesWithPositiveRank.append(L)
```

Now let us look at the Galois groups we get.

```
GaloisGroups = [[],[],[],[],[]]
for L in CurvesWithPositiveRank:
  try:
    e = EllipticCurve([0,-L-1,0,L,0])
  except:
    n = n
  try:
    gen = e.gens()
  except:
    gen = e.gens(proof = False)
  if len(gen) > 0:
    num = x^4- e.b4()*x^2 - 2*e.b6()*x - e.b8()
    denom = 4*x^3 + e.b2()*x^2+ 2*e.b4()*x+e.b6()
    Px = (num - gen[0][0]*denom).factor_list()[0][0]
    ex = solve(Px == 0, x)[0].rhs()
    Py = minimal_polynomial(sqrt(ex*(ex-1)*(ex-L)))
    wy = solve(sqrt(ex*(ex-1)*(ex-L)) == x, x)[0].rhs()
    degy = Py.degree()
    degx = Px.degree(x)
    GaloisGroups[degx].append(L)
    if degx == 2:
      if sqrt(x_P) in QQ:
        xPSquare.append(L)
for i in [2,4]:
  sys.stdout.write("We have ")
  sys.stdout.write(str(len(GaloisGroups[i])))
  print(" 2-division Galois Groups of order "+str(i))
print(str(len(xPSquare))+" curves with x_P a rational square.")
print(str(len(GaloisGroups[2])+len(GaloisGroups[4]))+" curves checked.")
print("End: "+str(time.ctime()))
```

We see that in 2152 out of the 4115 cases we get a Galois group of order two. In 1472 of the 2152 cases with the small Galois group we get that x_P is a square.

Remark

Also in the case where not all two torsion groups are rational, both sizes of Galois groups can occur. One can show that $E_1 : y^2 = x^3+7x+8$ with $P = (1, 4)$ and $E : y^2 = x^3+2x+3$ with $P = (3, 6)$ admit a Galois group of order four and two, respectively.

6 Further Steps

In the last two chapters we analyzed the case $\ell = 2$. Our goal now is to find possible generalizations. There are several ways to generalize:

- One can try to compute criterions like 4.2 algebraically for $\ell \geq 3$. This will become very nasty very quickly since the polynomials for multiplication grow extremely fast.

- One could try to find a more general description of the criterion 4.2. For this we first look at the part of the criterion that involves the x-coordinate being a square and try to find a more universal approach. We want to examine the curve

$$D_\lambda : w^2 = (v^2 - 1)(v^2 - \lambda).$$

  Wee see that we have a map $D_\lambda \to E_\lambda, (v, w) \mapsto (v^2, vw)$. By homogenizing we can find the singular points on D_λ: The homogenized equation of $f = w^2 - (v^2 - 1)(v^2 - \lambda)$ is $F = w^2z^2 - (u^2 - z^2)(u^2 - \lambda z^2)$ and by derivating we get:

$$\begin{aligned}
&\frac{dF}{dw}(v, w, z) = 0 \Leftrightarrow w = 0 \text{ or } z = 0\\
&\frac{dF}{dv}(v, w, z) = 0 \Leftrightarrow v = 0 \text{ or } 2v^2 = z^2(1 + \lambda)\\
&\frac{dF}{dz}(v, w, z) = 0 \Leftrightarrow 2\lambda z^2 = w^2 + (\lambda + 1)v^2.
\end{aligned}$$

  A little bit of computation shows that the only singular point on D_λ is $[0 : 1 : 0]$ which is the point at infinity. Sadly, neither is our map $\pi : \tilde{D_\lambda} \to E_\lambda, (v, w) \mapsto (v^2, vw)$ an isogeny (since it sends the point $(0, 1)$ on $\tilde{D_\lambda}$ to $(0, 0)$ on E_λ which is not the basepoint of E_λ) nor is D_λ nonsingular. We could normalize D_λ to get a nonsingular elliptic curve $\tilde{D_\lambda}$. After this, we find a map $\pi : \tilde{D_\lambda} \to E_\lambda$ and by [Silv], p. 71, this map is the composition of an isogeny and a translation: $\pi(P) = \varphi(P) + \varphi(Q)$ for some $Q \in \tilde{D_\lambda}$. Then one could examine the isogeny φ further to get information on when the Galois group of the ℓ-division points of P is non-maximal.

- One could also try to generalize the above argument to arbitrary primes ℓ: Let again K be a number field, $E_\lambda : y^2 = x(x-1)(x-\lambda)$ with $\lambda \in K \setminus \{0, 1\}$ an elliptic curve over K such that $E[\ell] \subset E(K)$. Let now $H \subset E_\lambda(K)$ be a subgroup of order ℓ. Then there is a K-isogeny $\varphi : E_\lambda \to E_\lambda/H$ and we can consider the dual isogeny ${}^t\varphi : E_\lambda/H \to E_\lambda$. The degree of φ is $\ell = |H|$ and we know that the composition of

${}^t\varphi$ and φ is the mulitplication-by-ℓ map.
Suppose now $P \in E_\lambda(K)$ is a point of infinite order and $P = {}^t\varphi(P_1)$ where $P_1 \in E_\lambda(K)/H$. Then for $P_1 = \ell R_1$ and $\sigma \in Gal(K(\frac{1}{\ell}P, E[\ell]), K(E[\ell]))$ we have $P = \ell\ {}^t\varphi(R_1) =: \ell Q_1$ and $\sigma Q_1 - Q_1 = \sigma(\ {}^t\varphi(R_1)) - {}^t\varphi(R_1) = {}^t\varphi(\sigma(R_1) - R_1)$. There are only ℓ possibilities for the values of ${}^t\varphi(\sigma(R_1) - R_1)$ (the kernel of ${}^t\varphi$ is of order ℓ) then $\sigma Q_1 - Q_1$ is also restricted to at most ℓ values. Hence the Galois group cannot be maximal (here the Kummer map is injective, hence an isomorphism).

- The next step now would be to figure out whether the condition from the isogeny is the only obstruction, i.e. is this an equivalence?

To be continued...

Bibliography

[Coh] S. D. Cohen, *The distribution of Galois groups and Hilbert's irreducibility theorem*, 1979.

[Kow] Emmanuel Kowalski, *Some local-global applications of Kummer theory*, manuscripta mathematica, 2003.

[Per] Antonella Perucca, *On the order of the reduction of points on abelian varieties and tori*, PhD Thesis, Università di Roma la Sapienza, 2008.

[Rib] Kenneth A. Ribet, *Kummer theory on extensions of abelian varieties by tori*, Duke Mathematical Journal, 1979.

[Ser] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inventiones mathematicae, 1972.

[Silv] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, Second Edition, 2009.