Chapter 5

Descent on a family of superelliptic curves

Let q be a power of a prime p and let K be the rational function field $\mathbb{F}_q(t)$. For each integer $d > 1$, define $K_d = K(\zeta_d, t^{1/d})$, where ζ_d is a primitive d-th root of unity. When d is clear from the context, we sometimes write u for $t^{1/d}$. The results in this chapter, notably Theorem 5.1, generalize results of the paper [39] by Douglas Ulmer. The idea that the results in this paper could be generalized is also due to Douglas Ulmer. The results in this chapter are part of a larger, joint work together with Lisa Berger, Chris Hall, Jennifer Park, Karl Rubin, Shahed Sharif, Alice Silverberg, and Doug Ulmer. The people in this group have also contributed significantly to the work presented in this chapter. The entire project was initiated at the AIM conference "Cohomological Methods in Abelian Varieties", which was held in Palo Alto from 26–30 March 2012.

5.1 Definitions and statement of results

Choose an odd prime r different from p. Choose an integer ν and set $d = q^\nu + 1$. Assume that r divides d. We will consider the smooth projective curve C over K defined by the affine equation

$$y^r = x^{r-1}(x+1)(x+t). \tag{5.1}$$

Let $Q_\infty \in C(K)$ denote the point at infinity. We define

$$P_{i,j} = \left(\zeta_d^i t^{1/d}, \zeta_d^{jd/r+i} t^{1/d} (\zeta_d^i t^{1/d} + 1)^{d/r}\right).$$

for $0 \le i \le d-1$ and $0 \le j \le r-1$. We verify that $P_{0,j}$ is an element of $C(K_d)$ for each j. Using repeatedly that $d = q^\nu + 1$, and writing $u = t^{1/d}$, we have that

$$\begin{aligned}\left(\zeta_d^{jd/r} u(u+1)^{d/r}\right)^r &= u^r(u+1)^d \\ &= u^r(u+1)^{q^\nu+1} \\ &= u^r(u+1)(u+1)^{q^\nu} \\ &= u^r(u+1)(u^{d-1}+1) \\ &= u^{r-1}(u+1)(u+t).\end{aligned}$$

Hence we have $P_{0,j} \in C(K_d)$ for all j. Observe that $P_{i,j}$ is a $\mathrm{Gal}(K_d/K)$-conjugate of $P_{0,j}$ for all i and j, hence this computation shows that we have $P_{i,j} \in C(K_d)$ for all i and j.

Let J be the Jacobian of C. In this chapter, we will prove the following result.

Theorem 5.1. *The divisor classes $[P_{i,j}] - [Q_\infty]$ generate a subgroup of $J(K_d)$ of rank $(r-1)(d-2)$. Moreover, we have $J(K_d)[r^\infty] \cong (\mathbb{Z}/r\mathbb{Z})^3$.*

Remark 5.2. We will show that our assumption that r divides d gives a non-empty condition, in other words, that for all q there exists ν such that $d = q^\nu + 1$ is divisible by r. For such a ν to exist, it is necessary and sufficient that r is an odd prime divisor of $q^\mu + 1$ for some integer μ; if μ is the smallest such integer, we must have $\nu = \mu\ell$ for some odd integer ℓ. There are infinitely many r that satisfy this condition, as can be seen by observing that $q^{2^a} + 1$ and $q^{2^b} + 1$ are coprime integers for all distinct positive integers a and b. Since $q^a + 1$ divides $q^{a\ell} + 1$ for any odd integer ℓ, there exist infinitely many integers ν such that $d = q^\nu + 1$ is divisible by r.

5.2 Properties of C and J

We will use the projective model for C in $\mathbb{P}^2_K$ defined by

$$C' \colon Y^r Z = X^{r-1}(X+Z)(X+tZ).$$

The curve C' is non-singular at the unique point at infinity $Q_\infty = (0:1:0)$. The normalization map $C \to C'$ is bijective on $\overline{K}$-points; we will use this fact to identify $C(\overline{K})$ and $C'(\overline{K})$. Let $Q_0 = (0,0)$, $Q_1 = (-1,0)$, and

$Q_t = (-t, 0)$ be points on C. Note that Q_0 is the only singular point on C'. We write $\Delta = \{Q_0, Q_1, Q_t\}$. We consider the covering

$$\pi\colon C \to \mathbb{P}^1$$

of degree r induced by the function x. The ramification points of π are Q_0, Q_1, Q_t and Q_∞, each with ramification index r. Applying Riemann–Hurwitz gives that the genus of C is $r-1$. Note that C_{K_d} has an automorphism given by $(x, y) \mapsto (x, \zeta_d^{d/r} y)$; we denote this automorphism by ζ_r. The automorphism ζ_r of C_{K_d} induces an automorphism ζ_r of J_{K_d}. The Rosati-involution $\alpha \mapsto \alpha^\dagger$ on $\mathrm{End}(J_{K_d})$ sends ζ_r to its inverse: this simply restates the fact that ζ_r respects the polarization on J_{K_d}, which it does, coming from an automorphism of C_{K_d}. We let $\phi\colon J_{K_d} \to J_{K_d}$ be the endomorphism $1 - \zeta_r$.

Proposition 5.3. *The endomorphism ϕ is a separable isogeny of degree r^2. Its kernel is generated by $[Q_0] - [Q_\infty]$ and $[Q_1] - [Q_\infty]$.*

Proof. Let $g = r - 1$ be the genus of C. We claim that the endomorphism $(1-\zeta_r)^{r-1}$ and the separable isogeny $[r]\colon J \to J$ factor through each other. This follows from the well-known fact from algebraic number theory that the ideal (r) of the Dedekind domain $\mathbb{Z}[\zeta_r]$ decomposes as $(1-\zeta_r)^{r-1}$. It follows that:

$$\deg(1-\zeta_r)^{r-1} = \deg[r] = r^{2g} = r^{2(r-1)},$$

which proves that $\deg(1-\zeta_r) = r^2$.

For the final assertion, one easily verifies that the divisor classes $D_0 = [Q_0] - [Q_\infty]$ and $D_1 = [Q_1] - [Q_\infty]$ are contained in the kernel of ϕ. To see that the $mD_0 + nD_1$ are distinct elements of $J(K_d)$ for all pairs (m, n) with $m, n \in \{0, 1, \ldots, r-1\}$, and hence that $\ker(\phi)$ is generated by D_0 and D_1, it suffices to show that $x^m(x+1)^n$ is not an r-th power in $K_d(C)$ unless $r \mid m$ and $r \mid n$. This is a routine exercise in field theory. □

Lemma 5.4. *We have $J[\phi] = J[\phi^\dagger]$, as group schemes.*

Proof. The equality comes down to the observation that the endomorphisms $\phi = 1 - \zeta_r$ and $\phi^\dagger = 1 - \zeta_r^{-1}$ factor through each other. This follows from the fact that $(1-\zeta_r)/(1-\zeta_r^{-1}) \in \mathbb{Z}[\zeta_r]^*$. □

5.3 Relating certain divisors on C

By $\sim$ we denote linear equivalence in $\mathrm{Div}(C_{K_d})$.

Lemma 5.5. *We have the following relations in* $\mathrm{Div}(C_{K_d})$*:*

$$(r+1)Q_\infty \sim (r-1)Q_0 + Q_1 + Q_t, \tag{5.2}$$

$$\sum_{i=0}^{d-1}(P_{i,0} - Q_\infty) \sim Q_0 - Q_1, \tag{5.3}$$

and

$$\sum_{i=0}^{d-1}(P_{i,0} - P_{i,-i}) \sim Q_0 - Q_\infty. \tag{5.4}$$

Proof. Equation (5.2) follows from considering $\mathrm{div}(y) \sim 0$. We define $f, g \in K_d(C)$ as follows: $f = y - x(x+1)^{d/r}$ and $g = yx^{d/r-1} - u^{d/r}(x+1)^{d/r}$. Then (5.3) follows from considering $\mathrm{div}(f/x) \sim 0$ and (5.4) follows from $\mathrm{div}(f/xg) \sim 0$. □

Lemma 5.6. *Define* $D \in \mathrm{Div}(C_{K_d})$ *by*

$$D = \sum_{i=0}^{d-1}\sum_{j=0}^{[-1-i]}(P_{i,j} - Q_\infty),$$

where $[-1-i] \in \{0, \ldots, r-1\}$ *is congruent to* $-1-i$ *modulo* r*, then*

$$(1-\zeta_r)(D) \sim Q_0 - Q_\infty.$$

Hence the class of D *is a* $(1-\zeta_r)^2$*-torsion element of* $J(K_d)$*.*

Proof. A straightforward calculation shows $(1-\zeta_r)(\sum_{j=0}^{[-1-i]} P_{i,j}) = P_{i,0} - P_{i,-i}$; this uses that $\zeta_r(P_{i,j}) = P_{i,[j+1]}$ for all i and j with $0 \le i \le d-1$ and $0 \le j \le r-1$, where $[j+1]$ denotes $j+1$ if $j < r-1$, and 0 if $j = r-1$. Hence $(1-\zeta_r)(D) \sim Q_0 - Q_\infty$ follows from (5.4) and the fact that $\zeta_r(Q_\infty) = Q_\infty$. The last statement follows from $(1-\zeta_r)[Q_0 - Q_\infty] = 0$, as noted in Lemma 5.3. □

5.4 The homomorphism $(x - T)$

For any curve $\mathcal{C}$, we will denote by $\mathrm{Div}(\mathcal{C})$ the group of Weil divisors on $\mathcal{C}$, and by $\mathrm{Div}^0(\mathcal{C}) \subset \mathrm{Div}(\mathcal{C})$ its subgroup of degree-zero divisors. We will define the pivotal homomorphism

$$(x-T)\colon \mathrm{Div}^0(C_{K_d}) \to \prod_{Q \in \Delta} K_d^*/K_d^{*r}.$$

Its properties are described in Proposition 5.7. For an element v of the product $\prod_{Q\in\Delta} K_d^*/K_d^{*r}$, we conveniently write $v=(v_0,v_1,v_t)$, where v_i is the coordinate corresponding to Q_i.

Let $C^\circ_{K_d}\subset C_{K_d}$ be the complement of $\Delta\cup\{Q_\infty\}$. We define the homomorphism

$$(x-T)'\colon \operatorname{Div}(C^\circ_{K_d})\to\prod_{Q\in\Delta} K_d^*/K_d^{*r}$$

by defining it on a closed point $P\in C^\circ_{K_d}$ as follows

$$P\mapsto (x(P)-x(Q))_{Q\in\Delta}\,,$$

followed by taking the norm if the residue field of P is a proper field extension of K_d.

We now define the homomorphism

$$(x-T)\colon \operatorname{Div}^0(C_{K_d})\to\prod_{Q\in\Delta} K_d^*/K_d^{*r}$$

as follows: let $D\in\operatorname{Div}^0(C_{K_d})$ be a degree-zero divisor on C_{K_d}, then choose $D'\in\operatorname{Div}(C^\circ_{K_d})$ in such a way that D is linearly equivalent to D'. We define $(x-T)(D)$ to be $(x-T)'(D')$. For a proof that $(x-T)$ is well-defined, see [5, 6.2.2].

5.4.1 Descent

We fix a separable closure K_d^{sep} of K_d, and we let $\mathcal{G}$ be the absolute Galois group $\operatorname{Gal}(K_d^{\mathrm{sep}}/K_d)$ of K_d. For a finite $\mathcal{G}$-module M of cardinality coprime to p, we denote by $M^\vee$ the dual $\mathcal{G}$-module $\operatorname{Hom}(M,K_d^{\mathrm{sep}\,*})$, and we will abbreviate the Galois cohomology groups $H^i(\mathcal{G},M)$ by $H^i(M)$ for every integer $i\geq 0$.

Proposition 5.7. *There exists a homomorphism α from $H^1(J[\phi])$ to the group $\prod_{Q\in\Delta} K_d^*/K_d^{*r}$ such that the following diagram is commutative with exact bottom row.*

$$\begin{array}{ccccccccc}
 & & \operatorname{Div}^0(C_{K_d}) & & & & & & \\
 & & \downarrow & \searrow^{(x-T)} & & & & & \\
 & & J(K_d)/\phi J(K_d) & & & & & & \\
 & & \downarrow{\scriptstyle\partial} & & & & & & \\
0 & \longrightarrow & H^1(J[\phi]) & \xrightarrow{\alpha} & \prod_{Q\in\Delta} K_d^*/K_d^{*r} & \xrightarrow{\mathcal{N}} & K_d^*/K_d^{*r} & \longrightarrow & 0
\end{array}$$

Here ∂ is induced by the Galois cohomology coboundary map for the isogeny ϕ, and $\mathcal{N}$ is the map sending (a_0, a_1, a_t) to $a_1 a_t / a_0$.

Proof. The proof is based on arguments from the paper [5], where the theory of descent is developed in great generality.

Let E be $(\mathbb{Z}/r\mathbb{Z})^{\Delta}$, the $\mathcal{G}$-module of $\mathbb{Z}/r\mathbb{Z}$-valued functions on Δ. Note that the $\mathcal{G}$-action on Δ as well as E is trivial. There is a $\mathcal{G}$-module map $\alpha^\vee \colon E \to J[\phi]$ defined by $h \mapsto \sum_{Q \in \Delta} h(Q) \cdot [Q - Q_\infty]$. Proposition 5.3 shows that $\alpha^\vee$ is surjective. Its kernel R is the $\mathbb{Z}/r\mathbb{Z}$-submodule of E generated by the map ρ defined by $Q_0 \mapsto -1, Q_1 \mapsto 1, Q_t \mapsto 1$. The resulting short exact sequence of $\mathcal{G}$-modules

$$0 \to R \to E \xrightarrow{\alpha^\vee} J[\phi] \to 0 \tag{5.5}$$

is split-exact, since it consists of modules that are free as $\mathbb{Z}/r\mathbb{Z}$-modules and have trivial $\mathcal{G}$-action. Dualizing (5.5) and taking Galois cohomology, we obtain a split-exact sequence

$$0 \to H^1(J[\phi^\dagger]) \to H^1(E^\vee) \to H^1(R^\vee) \to 0. \tag{5.6}$$

By Lemma 5.4, $H^1(J[\phi^\dagger])$ is the same as $H^1(J[\phi])$. We compute that $H^1(E^\vee) = H^1(\mu_r^\Delta) = \prod_{Q \in \Delta} K_d^*/K_d^{*r}$, where the last step is Hilbert 90. Choosing the isomorphism $\mathbb{Z}/r\mathbb{Z} \xrightarrow{\sim} R$ given by $1 \mapsto \rho$, we identify $H^1(R^\vee)$ with $H^1(\mu_r) = K_d^*/K_d^{*r}$, where the last step is again Hilbert 90. With these identifications, the short exact sequence (5.6) becomes the bottom row in the diagram, and the map $H^1(E^\vee) \to H^1(R^\vee)$ corresponds to the $\mathcal{N}$ from the statement of the proposition.

The fact that the diagram is commutative is the content of Proposition 6.4 in [5]. □

It follows from Proposition 5.7 that $(x - T)$ induces a map $J(K_d) \to \prod_{Q \in \Delta} K_d^*/K_d^{*r}$. We will also denote this map by $(x - T)$. The map $(x - T)$ can be seen as a computation-friendly substitute for the coboundary map $\delta \colon J(K_d) \to H^1(J[\phi])$, since we have $(x - T) = \alpha \circ \delta$, where α is the injective map from Proposition 5.7. Moreover, Proposition 5.7 shows that the image of $(x - T)$ is contained in the kernel of $\mathcal{N}$, with $\mathcal{N}$ as in the statement of the proposition.

5.4.2 Some values of $(x - T)$

The rest of this subsection is devoted to the computation of $(x - T)(Q - Q_\infty)$ for $Q \in \Delta$.

Lemma 5.8. *Let $D \in \mathrm{Div}(C^\circ_{K_d})$. Then if $(x-T)'(D) = (v_0, v_1, v_t)$, we have $v_1 v_t / v_0 = v_0^{r-1} v_1 v_t = 1$.*

Proof. From equation (5.1) it follows that, if $P \in C^\circ_{K_d}$ is a closed point, then (the $\kappa(P)/K_d$-norm of) $x(P)^{r-1}(x(P)+1)(x(P)+t)$ is contained in K_d^{*r}. □

The following lemma states that $(x - T)$ can be "evaluated on the coordinates on which it makes sense".

Lemma 5.9. *Let $D \in \mathrm{Div}(C_{K_d})$ be a divisor supported outside of Q_∞. If $Q \in \Delta$ is such that D is also supported outside of Q, then we have*

$$(x-T)(D)_Q = \prod_P (x(P) - x(Q))^{\mathrm{ord}_P(D)}.$$

Proof. Choose a divisor $D' \in \mathrm{Div}(C^\circ_{K_d})$ that is linearly equivalent to D. Choose $g \in K_d(C)^*$ such that $D' = D + \mathrm{div}(g)$. Observe that $\mathrm{div}(g)$ is supported outside Q and Q_∞. Then

$$\begin{aligned}(x-T)(D)_Q &= (x-T)'(D')_Q \\ &= \prod_P (x(P) - x(Q))^{\mathrm{ord}_P(D')} \\ &= \prod_P (x(P) - x(Q))^{\mathrm{ord}_P(D + \mathrm{div}(g))} \\ &= \prod_P (x(P) - x(Q))^{\mathrm{ord}_P(D)} \prod_P (x(P) - x(Q))^{\mathrm{ord}_P(g)}.\end{aligned}$$

In the last expression however, the contribution of the second product is trivial:

$$\prod_P (x(P) - x(Q))^{\mathrm{ord}_P(g)} = \prod_P g(P)^{\mathrm{ord}_P(x - x(Q))} = g(Q)^r g(\infty)^{-r} = 1,$$

where the first equality is due to Weil reciprocity and the second one rests on the fact that for $Q \in \Delta$ we have $\mathrm{div}(x - x(Q)) = r \cdot Q - r \cdot Q_\infty$, as is shown by direct calculation. □

For future use, we apply Lemmas 5.8 and 5.9 to the computation of the images under $(x - T)$ of the divisors $Q_1 - Q_\infty$ and $P_i - Q_\infty$.

Proposition 5.10. *We have $(x-T)(Q_1 - Q_\infty) = (-1, 1/(1-t), t-1)$ and $(x-T)(P_{i,j} - Q_\infty) = (\zeta_d^i u, \zeta_d^i u + 1, \zeta_d^i u + t)$.*

Proof. For $\bullet \in \{0, 1, t, \infty\}$, let $D_\bullet \in \mathrm{Div}(C^\circ_{K_d})$ be a divisor that is linearly equivalent to $Q_\bullet$. Using Lemmas 5.8 and 5.9, one gets $(x-T)'(D_0) = (t, 1, t)$, $(x-T)'(D_1) = (-1, 1/(1-t), t-1)$, and $(x-T)'(D_t) = (-t, 1-t, t/(t-1))$. Applying (5.2), we then find $(x-T)'(D_\infty) = (1, 1, 1)$. Hence $(x-T)(Q_1 - Q_\infty) = (x-T)'(D_1 - D_\infty) = (-1, 1/(1-t), t-1)$.

Finally, we have $(x-T)(P_{i,j} - Q_\infty) = (x-T)(P_{i,j} - D_\infty) = (x-T)'(P_{i,j}) - (x-T)'(D_\infty) = (\zeta_d^i u, \zeta_d^i u + 1, \zeta_d^i u + t)$. □

5.5 The image of $(x - T)$

For this section, let $N \subset J(K_d)$ be the subgroup generated by the divisor classes $[P_{i,j} - Q_\infty]$, where $i \in \{0, \ldots, d-1\}$ and $j \in \{0, \ldots, r-1\}$. Observe that the known torsion elements $[Q_0 - Q_\infty]$, $[Q_1 - Q_\infty]$, $[Q_t - Q_1]$ and $[D] = [\sum_{i=0}^{d-1} \sum_{j=0}^{[-1-i]} (P_{i,j} - Q_\infty)]$ (the D is as in Lemma 5.6) are all contained in N by Lemmas 5.5 and 5.6. Therefore N contains all elements of $J(K_d)$ described so far.

Proposition 5.11. *We have* $\dim_{\mathbb{F}_r}(x-T)(N) = d$.

Proof. Since $(x-T)(P_{i,j} - Q_\infty) = (x-T)(\zeta_r^j(P_{i,0} - Q_\infty)) = (x-T)(P_{i,0} - Q_\infty)$, the dimension certainly cannot be larger than d. To show that it is precisely d, we project down from $\prod_{Q \in \Delta} K_d^*/K_d^{*r}$ to a finite-dimensional quotient space of dimension d, and conclude by showing that the projection is surjective.

For an irreducible polynomial π inside K_d, the valuation it induces on K_d^* is denoted $\mathrm{val}_\pi \colon K_d^* \to \mathbb{Z}$. We define the following map:

$$\begin{aligned} \mathrm{pr} \colon \prod_{Q \in \Delta} K_d^*/K_d^{*r} &\to \mathbb{F}_r^d \\ (v_0, v_1, v_t) &\mapsto (\mathrm{val}_{u+1}(v_1), \mathrm{val}_{u+\zeta_d^{-1}}(v_1), \mathrm{val}_{u+\zeta_d^{-2}}(v_1), \ldots, \mathrm{val}_{u+\zeta_d}(v_1)) \end{aligned}$$

By Proposition 5.10, we have $(x-T)(P_{i,j} - Q_\infty) = (\zeta_d^i u, \zeta_d^i u + 1, \zeta_d^i u + t)$. We see that pr maps the image of $P_{i,j} - Q_\infty$ to the i-th basis vector. Hence pr maps $(x-T)(N)$ surjectively onto $\mathbb{F}_r^d$. This establishes the proposition. □

Lemma 5.12. *The image under* $(x - T)$ *of the subgroup generated by* $[D]$ *and* $[Q_1 - Q_\infty]$ *has* $\mathbb{F}_r$*-dimension* 2.

Proof. Since $(x-T)(P_{i,j} - Q_\infty) = (x-T)(P_{i,0} - Q_\infty)$, as noted in the proof of Proposition 5.11, we see that the image of $D = \sum_{i=0}^{d-1} \sum_{j=0}^{[-1-i]} P_{i,j}$ is the same

as that of $\sum_{i=0}^{d-1}(d-i)(P_{i,0}-Q_\infty)$. If we resume the notation of the proof of Proposition 5.11, we find $\mathrm{pr}((x-T)(D)) = (0,-1,-2,\ldots,-d+1) \in \mathbb{F}_r^d$.

Proposition 5.10 gives $(x-T)(Q_1-Q_\infty) = (-1, 1/(1-t), t-1)$. Since in K_d we have the factorization $1-t = \prod_{i=0}^{d-1}(1-\zeta_d^i u)$, we get $\mathrm{pr}((x-T)(Q_1-Q_\infty)) = (-1,-1,-1,\ldots,-1)$. The lemma now follows. □

5.6 An algebraic lemma

We consider $\mathbb{F}_r$ as a $\mathbb{Z}[\zeta_r]$-module via the unique ring homomorphism $\mathbb{Z}[\zeta_r] \to \mathbb{F}_r$, whose kernel is the maximal ideal generated by $1-\zeta_r$. Then ζ_r acts as the identity on $\mathbb{F}_r$.

Lemma 5.13. *Let $R = \mathbb{Z}[\zeta_r]$ and $\phi = 1-\zeta_r$. Let M and N be R-modules with $N \subset M$.*

(i) There are positive integers e_i such that

$$M[r^\infty] = M[\phi^\infty] \cong \bigoplus_{i=1}^{t} R/(\phi^{e_i})$$

as R-modules, where $t = \dim_{\mathbb{F}_r} M[\phi]$.

(ii) There is an exact sequence

$$0 \to N[\phi] \to M[\phi] \to (M/N)[\phi] \to N \otimes_R \mathbb{F}_r \to M \otimes_R \mathbb{F}_r \to (M/N) \otimes_R \mathbb{F}_r \to 0,$$

where the middle map sends $m+N$ to $\phi m \otimes 1$.

Let $\rho = \dim_{\mathbb{Q}(\zeta_r)} N \otimes_{\mathbb{Z}} \mathbb{Q}$ be the rank of N as R-module, and let $V \subset M \otimes_R \mathbb{F}_r$ be the image of the map $N \to M \otimes_R \mathbb{F}_r$.

(iii) We have

$$\rho = \dim_{\mathbb{F}_r} V + \dim_{\mathbb{F}_r}(M/N)[\phi] - \dim_{\mathbb{F}_r} M[\phi].$$

Proof. Since the elements r and ϕ^{r-1} of $\mathbb{Z}[\zeta_r]$ generate the same ideal, they differ by a unit, and hence we have $M[r^\infty] = M[\phi^\infty]$. Localizing at the prime ideal (ϕ), we find, by the structure theorem for finitely generated modules over principal ideal domains:

$$M_{(\phi)} \cong R_{(\phi)}^s \oplus \bigoplus_{i=1}^{t} R/(\phi^{e_i}),$$

for some choice of non-negative integers s, t and e_i. Since localizing at (ϕ) does not affect ϕ-power torsion, we find $M[\phi^\infty] \cong \bigoplus_{i=1}^{t} R/(\phi^{e_i})$. From the isomorphism, it is clear that $t = \dim_{\mathbb{F}_r} M[\phi]$. This proves part (i).

The exact sequence given in part (ii) is the long exact sequence that results from applying $- \otimes_R \mathbb{F}_r$ to $0 \to N \to M \to M/N \to 0$.

Truncating the exact sequence of part (ii) at the fifth term, we get the exact sequence

$$0 \to N[\phi] \to M[\phi] \to (M/N)[\phi] \to N \otimes_R \mathbb{F}_r \to V \to 0. \tag{5.7}$$

Using

$$\dim_{\mathbb{F}_r} N \otimes_R \mathbb{F}_r = \dim_{\mathbb{F}_r} N_{(\phi)} \otimes_{R_{(\phi)}} \mathbb{F}_r = \rho + \dim_{\mathbb{F}_r} N[\phi],$$

and the fact that the $\mathbb{F}_r$-dimensions of the terms of (5.7) add up to zero, we obtain part (iii). This concludes the proof. □

5.7 Proof of the main theorem

As in section 5.6, we consider $\mathbb{F}_r$ as a $\mathbb{Z}[\zeta_r]$-module. Since the isogeny ϕ was defined as $1 - \zeta_r$, we may write $J(K_d)/\phi J(K_d) = J(K_d) \otimes_{\mathbb{Z}[\zeta_r]} \mathbb{F}_r$. By Proposition 5.7, we have a commutative diagram

$$\begin{array}{ccc} J(K_d) & \longrightarrow & J(K_d) \otimes_{\mathbb{Z}[\zeta_r]} \mathbb{F}_r \\ & \searrow^{(x-T)} & \downarrow \\ & & \prod_{Q \in \Delta} K_d^*/K_d^{*r} \end{array}$$

Let N be a $\mathbb{Z}[\zeta_r]$-submodule of $J(K_d)$. Then the image of N under $(x - T)$ can be identified with the image of the map $N \to J(K_d) \otimes_{\mathbb{Z}[\zeta_r]} \mathbb{F}_r$.

We conclude by giving the proof of Theorem 5.1.

Proof of Theorem 5.1. First, we determine $J(K_d)[r^\infty]$. By Proposition 5.3 and Lemma 5.13(i) we find that

$$J(K_d)[r^\infty] \cong \mathbb{Z}[\zeta_r]/(1 - \zeta_r)^{e_1} \oplus \mathbb{Z}[\zeta_r]/(1 - \zeta_r)^{e_2}$$

for some positive integers e_1, e_2. By Lemma 5.12, the classes of $[D]$ and $[Q_1 - Q_\infty]$ generate $J(K_d)[r^\infty] \otimes_{\mathbb{Z}[\zeta_r]} \mathbb{F}_r$, so by Nakayama's lemma $[D]$ and $[Q_1 - Q_\infty]$ generate $J(K_d)[r^\infty]$.

Let $N \subset J(K_d)$ be the subgroup generated by the divisor classes $[P_{i,j} - Q_\infty]$, for $0 \leq i \leq d-1$ and $0 \leq j \leq r-1$. From Proposition 5.11 and Lemma 5.13(iii) applied with $M = J(K_d)$ we find:

$$\mathrm{rank}_{\mathbb{Z}[\zeta_r]}(N) = d - 2 + \dim_{\mathbb{F}_r}(J(K_d)/N)[1-\zeta_r].$$

Since $N \otimes_{\mathbb{Z}[\zeta_r]} \mathbb{F}_p$ has dimension d, it follows from Proposition 5.11 that $N \otimes_{\mathbb{Z}[\zeta_r]} \mathbb{F}_p$ injects into $J(K_d) \otimes_{\mathbb{Z}[\zeta_r]} \mathbb{F}_p$, which by Lemma 5.13(ii) implies

$$\dim_{\mathbb{F}_r}(J(K_d)/N)[1-\zeta_r] = 0$$

Therefore, the $\mathbb{Z}$-rank of N is equal to $(r-1)(d-2)$. □