Journal of Number Theory 131 (2011) 561–577

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

The Galois closure of Drinfeld modular towers

Alp Bassa[a], Peter Beelen[b,*]

[a] CWI, Amsterdam, The Netherlands
[b] Technical University of Denmark, Department of Mathematics, Denmark

ARTICLE INFO

Article history:
Received 9 June 2010
Accepted 28 November 2010
Available online 18 December 2010
Communicated by Gebhard Böckle

Keywords:
Drinfeld modular curves
Galois closure
Asymptotically optimal towers of function fields

ABSTRACT

In this article we study Drinfeld modular curves $X_0(p^n)$ associated to congruence subgroups $\Gamma_0(p^n)$ of $\mathrm{GL}(2, \mathbb{F}_q[T])$ where p is a prime of $\mathbb{F}_q[T]$. For $n > r > 0$ we compute the extension degrees and investigate the structure of the Galois closures of the covers $X_0(p^n) \to X_0(p^r)$ and some of their variations. The results have some immediate implications for the Galois closures of two well-known optimal wild towers of function fields over finite fields introduced by Garcia and Stichtenoth, for which the modular interpretation was given by Elkies.

1. Introduction

The question of how many rational points a curve of genus g defined over a finite field $\mathbb{F}_q$ can have, has been a central and important one in number theory. Although this question is interesting in its own right, it received further attention after in the beginning of the eighties various applications in coding theory and other areas of discrete mathematics appeared. More precisely, curves with many points compared to their genus have been successfully applied in the construction of codes, hash functions, sequences and other combinatorial objects. One of the landmark results in the theory of curves defined over finite fields was the theorem of Hasse and Weil, which is the congruence function field analogue of the Riemann hypothesis. As an immediate consequence of this theorem one obtains an upper bound for the number of rational points on such a curve in terms of its genus and the cardinality of the finite field. It was noticed however by Ihara [13] and Manin [14] that this bound can be improved for large genus and the asymptotic study over a fixed finite field was then initiated by Ihara. An asymptotic upper bound on the number of rational points was given by Drinfeld and Vladut [2].

[*] Corresponding author.
E-mail addresses: alp.bassa@cwi.nl (A. Bassa), p.beelen@mat.dtu.dk (P. Beelen).

0022-314X/$ – see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.jnt.2010.10.006

Finding curves of large genera with many points is a difficult task and there have basically been three approaches: class field theory (see among others [16,17]), explicit constructions (see among others [3,5–7]) and reductions of modular curves of various types (see among others [11,13,21,22]). With these techniques it is possible to construct sequences of curves having many points compared to their genera asymptotically and in some cases even attaining the Drinfeld–Vladut bound, in which case the sequence of curves is called optimal. These sequences also had important implications in asymptotic coding theory.

For these applications, having explicit equations for optimal sequences of curves became important. In [5–7], Garcia and Stichtenoth gave explicit examples of optimal sequences of curves $(C_k)_{k\geqslant 0}$. These curves were defined recursively in such a way that each curve C_k is a cover of C_{k-1} (hence these sequences are called recursive towers). Although in these towers the individual covers $C_k \to C_{k-1}$ are Galois, the same does not hold for $C_k \to C_0$ for general k. However, one can look at a modification of these towers by replacing C_k by $\tilde{C}_k$, the Galois closure of C_k over C_0. The tower $(\tilde{C}_k)_{k\geqslant 0}$ thus obtained will be called its Galois closure. Galois towers in general have been studied in [8]. The Galois closure of the tower in [6], was investigated by Stichtenoth in [19] and applied to the construction of transitive, self-dual codes with good asymptotic properties. Also Zaytsev [23] treats the case of the Galois closure of the tower in [6] in the particular case, where the cardinality of the finite field is the square of an odd prime.

In [3,4], Elkies gave a modular interpretation for all known optimal recursive towers. More precisely he showed that all known examples of tame (respectively wild), optimal recursive towers correspond to reductions of classical (respectively Drinfeld) modular curves. Moreover he speculated that any optimal recursive tower has a modular interpretation.

Motivated by the above, we study in this paper towers of Drinfeld modular curves associated to the congruence subgroups $\Gamma_0(p^n)$ of $\mathrm{GL}(2, \mathbb{F}_q[T])$ for a prime p of $\mathbb{F}_q[T]$, some of their variations and their Galois closures. The reductions of all of them give optimal towers, as follows from the theory of Drinfeld modular curves. Combining our results and the modular interpretation of Elkies for the optimal towers in [5,6], we are able to obtain some interesting new consequences for their Galois closures. More precisely, we show that the Galois closure in each case can be obtained by just taking the composite of three conjugates, we investigate the Galois groups that are involved, investigate their structure and determine their exact cardinalities. The analogous case of tame towers, which corresponds to the reduction of classical modular curves, was worked out in [1].

2. Preliminaries

Let R denote $\mathbb{F}_q[T]$. For an element $\alpha \in R - \mathbb{F}_q$ one has the reduction-modulo-α map $\pi_\alpha : R \to R/\alpha R$. The map π_α is injective on $\mathbb{F}_q$ and we will identify $\mathbb{F}_q$ with its image. Sometimes we will write $r \bmod \alpha$ instead of $\pi_\alpha(r)$. Below α will usually be a power of a prime element $p \in R$. Note that $\#(R/\alpha R) < \infty$, so we can define

$$\rho(\alpha) := \#(R/\alpha R).$$

In case α is a prime element of R, the quotient ring $R/\alpha R$ is a finite field of cardinality $\rho(\alpha)$.

The following groups are basic in the theory of modular curves:

$$\begin{aligned}
\Gamma &:= \mathrm{GL}(2, R),\\
\Gamma_0(\alpha) &:= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma\colon\ c \equiv 0 \bmod \alpha \right\},\\
\Gamma(\alpha) &:= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma\colon\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod \alpha \right\}.
\end{aligned}$$

Note that $\Gamma(\alpha) \subset \Gamma_0(\alpha) \subset \Gamma$ and $\Gamma(1) = \Gamma_0(1) = \Gamma$. The group $\Gamma(\alpha)$ is the kernel of the group homomorphism $\pi_\alpha : \Gamma \to \mathrm{GL}(2, R/\alpha R)$ defined by reducing the entries of a matrix in Γ mod α.

Therefore it holds that $\Gamma(\alpha) \trianglelefteq \Gamma$. It is not true that π_α is surjective in general, but $\Gamma/\Gamma(\alpha)$ is isomorphic to a subgroup of $\mathrm{GL}(2, R/\alpha R)$ described in case α is a prime power in the following proposition.

Proposition 1. *Let p be a prime element of R and n a positive integer. Then*

$$\mathrm{GL}(2,R)/\Gamma\big(p^n\big) \cong \pi_{p^n}\big(\mathrm{GL}(2,R)\big) = \big\{M \in \mathrm{GL}\big(2, R/p^nR\big)\colon \det M \in \mathbb{F}_q^*\big\}.$$

Moreover

$$\#\pi_{p^n}\big(\mathrm{GL}(2,R)\big) = (q-1)\rho(p)^{3n}\big(1 - 1/\rho(p)^2\big).$$

Proof. The following proof is an adaptation of the proof of [18, Lemma I.38]. Let $M \in \mathrm{GL}(2, R/p^nR)$ and assume that $\det M \in \mathbb{F}_q^*$. Then there exists a matrix $B \in \mathrm{GL}(2,R)$ such that $\det B = 1/\det M$. Now choose any matrix $A \in M_{2\times 2}(R)$ such that $\pi_{p^n}(A) = \pi_{p^n}(B)M$. Note that $\pi_{p^n}(A) \in \mathrm{SL}(2, R/p^nR)$. By the structure theorem of modules over a principal ideal ring, there exist matrices $U, V \in \mathrm{SL}(2,R)$ such that UAV is a diagonal matrix with entries, say a_1 and $a_2 \in R$. Now define

$$W = \begin{pmatrix} a_2 & 1 \\ a_2 - 1 & 1 \end{pmatrix}, \qquad X = \begin{pmatrix} 1 & -a_2 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad A' = \begin{pmatrix} 1 & 0 \\ 1 - a_1 & 1 \end{pmatrix}.$$

Then a direct computation shows that

$$\pi_{p^n}(WUAVX) = \pi_{p^n}\big(A'\big).$$

This implies that

$$M = \pi_{p^n}\big(B^{-1}A\big) = \pi_{p^n}\big(B^{-1}U^{-1}W^{-1}A'X^{-1}V^{-1}\big).$$

To prove the last statement, it is enough to count the cardinality of $\mathrm{SL}(2, R/p^nR)$. The essential part in the reasoning is that any 2×2 matrix M, with entries from R/p^nR, congruent to the identity matrix modulo p, necessarily is invertible, i.e., is an element of $\mathrm{GL}(2, R/p^nR)$. This implies that

$$\#\,\mathrm{GL}\big(2, R/p^nR\big) = \rho(p)^{4(n-1)}\#\,\mathrm{GL}(2, R/pR) = \rho(p)^{4n}\big(1 - 1/\rho(p)\big)\big(1 - 1/\rho(p)^2\big).$$

This implies that

$$\#\mathrm{SL}\big(2, R/p^nR\big) = \#\,\mathrm{GL}\big(2, R/p^nR\big)/\#\big(R/p^nR\big)^* = \rho(p)^{3n}\big(1 - 1/\rho(p)^2\big). \qquad \square$$

3. Groups of Galois closure

Let $n > 1$ be an integer and $p \in R$ be a prime element. Associated to the group $\Gamma_0(p^n)$ is the Drinfeld modular curve $X_0(p^n)$ which has been studied extensively in the literature, cf. [9–12,20]. For $n > r > 0$ the curve $X_0(p^n)$ is a cover of $X_0(p^r)$, which in general is not Galois. The Galois closure of $X_0(p^n)$ over $X_0(p^r)$ has Galois group $\Gamma_0(p^r)/\Delta_r(p^n)$ with

$$\Delta_r\big(p^n\big) := \bigcap_{\sigma \in \Gamma_0(p^r)} \sigma\Gamma_0\big(p^n\big)\sigma^{-1}. \tag{1}$$

The group $\Delta_r(p^n)$ is the largest normal subgroup of $\Gamma_0(p^r)$ contained in $\Gamma_0(p^n)$, since if $H \trianglelefteq \Gamma_0(p^r)$ and $H \subset \Gamma_0(p^n)$, then $H \subset \bigcap_{\sigma\in\Gamma_0(p^r)} \sigma\Gamma_0(p^n)\sigma^{-1} = \Delta_r(p^n)$. The maximality of $\Delta_r(p^n)$ with respect to the above property will be used later. The group $\Delta_r(p^n)$ is called the normal core of $\Gamma_0(p^n)$ in $\Gamma_0(p^r)$. For convenience we also define $\Delta_r(p^r) = \Gamma_0(p^r)$.

We start by describing the group $\Delta_r(p^n)$ in more detail.

Proposition 2. *Suppose that $\rho(p) > 2$, then*

$$\Delta_r(p^n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(p^n):\ p^{n-r} | a-d \text{ and } p^{n-r} | bp^r \right\}.$$

Proof. We denote by H the subgroup of $\mathrm{GL}(2, R)$ of matrices

$$h = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

satisfying:

1) $p^n | c$,
2) $p^{n-r} | a-d$, and
3) $p^{n-r} | bp^r$.

One can check that H really is a subgroup. Clearly $H \subset \Gamma_0(p^n)$, so to prove the proposition it is enough to show that $H \trianglelefteq \Gamma_0(p^r)$ and that $\Delta_r(p^n) \subset H$, since then $\Delta_r(p^n) \supset H$ follows from the maximality of $\Delta_r(p^n)$.

First we prove that $H \trianglelefteq \Gamma_0(p^r)$. Conjugating an element $h \in H$ with a matrix

$$m = \begin{pmatrix} \alpha & \beta \\ \gamma p^r & \delta \end{pmatrix},$$

from $\Gamma_0(p^r)$ we find that

$$mhm^{-1} = \begin{pmatrix} -p^r\gamma(\alpha b + \beta d) + (\alpha a + \beta c)\delta & \alpha^2 b + \alpha\beta(d-a) - \beta^2 c \\ p^r\gamma(a-d)\delta - bp^{2r}\gamma^2 + c\delta^2 & p^r\gamma(\alpha b - \beta a) + (\alpha d - \beta c)\delta \end{pmatrix}. \tag{2}$$

Using properties 1), 2) and 3) of h, we see that $mhm^{-1} \in H$ and hence $H \trianglelefteq \Gamma_0(p^r)$.

Now we wish to prove that $\Delta_r(p^n) \subset H$. Let $f \in R$ such that $\gcd(f, p) = 1$. We define the matrix

$$A_f = \begin{pmatrix} 1 & 0 \\ fp^r & 1 \end{pmatrix}. \tag{3}$$

Note that $A_f \in \Gamma_0(p^r)$. For this matrix A_f and

$$h = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(p^n)$$

we have, using Eq. (2),

$$A_f \begin{pmatrix} a & b \\ c & d \end{pmatrix} A_f^{-1} = \begin{pmatrix} * & * \\ f(a-d)p^r - bf^2p^{2r} + c & * \end{pmatrix}. \tag{4}$$

This implies that if $A_f h A_f^{-1} \in \Gamma_0(p^n)$, then $p^{n-r} | (a-d) - bfp^r$. Here we used that $\gcd(p, f) = 1$. Since $\rho(p) > 2$, we can choose f_1, f_2 such that $\gcd(f_1, p) = \gcd(f_2, p) = 1$, while at the same time $f_1 \not\equiv f_2 \bmod p$. If $A_{f_1} h A_{f_1}^{-1} \in \Gamma_0(p^n)$ and $A_{f_2} h A_{f_2}^{-1} \in \Gamma_0(p^n)$, we conclude that $p^{n-r} | a-d$ and $p^{n-r} | bp^r$. This implies that

$$\Delta_r(p^n) \subset \Gamma_0(p^n) \cap A_{f_1} \Gamma_0(p^n) A_{f_1}^{-1} \cap A_{f_2} \Gamma_0(p^n) A_{f_2}^{-1} \subset H. \qquad \square$$

A direct corollary from (the proof of) Proposition 2 is the following:

Corollary 3. *Suppose that $\rho(p) > 2$. Choose f_1, f_2 such that $\gcd(f_1, p) = \gcd(f_2, p) = 1$, while at the same time $f_1 \not\equiv f_2 \bmod p$. Denote for $i = 1, 2$ by $A_{f_i} \in \Gamma_0(p^r)$, the matrix*

$$A_{f_i} = \begin{pmatrix} 1 & 0 \\ f_i p^r & 1 \end{pmatrix}.$$

Then

$$\Delta_r(p^n) = \Gamma_0(p^n) \cap A_{f_1} \Gamma_0(p^n) A_{f_1}^{-1} \cap A_{f_2} \Gamma_0(p^n) A_{f_2}^{-1}.$$

Remark 4. It is not difficult to choose A_{f_1} and A_{f_2} from the previous corollary explicitly. We can choose

$$A_{f_1} = \begin{pmatrix} 1 & 0 \\ p^r & 1 \end{pmatrix},$$

$$A_{f_2} = \begin{pmatrix} 1 & 0 \\ \alpha p^r & 1 \end{pmatrix} \quad \text{with } \alpha \in \mathbb{F}_q - \{0, 1\}, \text{ if } q > 2,$$

and

$$A_{f_2} = \begin{pmatrix} 1 & 0 \\ T p^r & 1 \end{pmatrix} \quad \text{if } q = 2.$$

Note that since it is assumed that $\rho(p) > 2$, in the latter case it holds that $\deg(p) > 1$, so that $\gcd(T, p) = 1$ and $T \not\equiv 1 \bmod p$.

Now we consider the case that $\rho(p) = 2$. This can occur only if $R = \mathbb{F}_2[T]$ and p is a polynomial of degree one.

Proposition 5. *Suppose that $\rho(p) = 2$, then*

$$\Delta_r(p^n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(p^n) \colon\ p^{n-r} \big| a - d - bp^r \text{ and } p^{n-r} \big| bp^{r+1} \right\}.$$

Proof. Similarly as in the proof of Proposition 2, we denote by H the subgroup of $\mathrm{GL}(2, R)$ of matrices

$$h = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

satisfying:

1) $p^n | c$,
2) $p^{n-r} | a - d - bp^r$, and
3) $p^{n-r} | bp^{r+1}$.

It is enough to show that $H \trianglelefteq \Gamma_0(p^r)$ and that $\Delta_r(p^n) \subset H$. Again one can check that H is a group. First we prove that $H \trianglelefteq \Gamma_0(p^r)$. Conjugating an element $h \in H$ with a matrix

$$m = \begin{pmatrix} \alpha & \beta \\ \gamma p^r & \delta \end{pmatrix},$$

from $\Gamma_0(p^r)$ we find using properties 1) and 2) that

$$p^r(a-d)\gamma\delta - bp^{2r}\gamma^2 + c\delta^2 \equiv bp^{2r}\gamma(\delta - \gamma) \bmod p^n.$$

It is clear from the definition of H, that p^{n-1} divides bp^{2r}. Moreover, since $\rho(p) = 2$ and m is invertible, we find that $\delta \equiv 1 \bmod p$. This implies that $\gamma(\delta - \gamma) \equiv 0 \bmod p$ and thus that

$$p^r(a-d)\gamma\delta - bp^{2r}\gamma^2 + c\delta^2 \equiv bp^{2r}\gamma(\delta - \gamma) \equiv 0 \bmod p^n.$$

Using that $a \equiv d + bp^r \pmod{p^{n-r}}$ and $c \equiv 0 \pmod{p^{n-r}}$, we see that the second condition for mhm^{-1} to be in H is equivalent to the statement

$$bp^r\bigl(p^r\beta(\alpha + \gamma) - \alpha(\alpha + 2\gamma - \delta)\bigr) \equiv 0 \quad \bigl(\text{mod } p^{n-r}\bigr).$$

By definition p^{n-r-1} divides bp^r, while $p^r\beta(\alpha + \gamma) - \alpha(\alpha + 2\gamma - \delta) \equiv -\alpha(\alpha + 2\gamma - \delta) \bmod p$. Reasoning as before, we see that p divides $\alpha(\alpha + 2\gamma - \delta)$, implying that mhm^{-1} also satisfies the second condition to be in H. The third condition for mhm^{-1} to be in H is directly seen to be satisfied as well. Hence we have showed that $H \trianglelefteq \Gamma_0(p^r)$.

Now we wish to prove that $\Delta_r(p^n) \subset H$. Choose $f_1 = 1$ and $f_2 = 1 + p$. Using Eqs. (3) and (4), we find that any element

$$h = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

from $\Gamma_0(p^n) \cap A_{f_1}\Gamma_0(p^n)A_{f_1}^{-1} \cap A_{f_2}\Gamma_0(p^n)A_{f_2}^{-1}$ satisfies that p^n divides each of the expressions c, $(a-d)p^r - bp^{2r} + c$ and $(a-d)(1+p)p^r - b(1+p)^2p^{2r} + c$. This implies that $h \in H$ as desired. □

Similarly as before, we obtain the following corollary.

Corollary 6. *Suppose that $\rho(p) = 2$. Choose $f_1 = 1$, $f_2 = 1 + p$ and for $i = 1, 2$ denote by $A_{f_i} \in \Gamma_0(p^r)$ the matrix*

$$A_{f_i} = \begin{pmatrix} 1 & 0 \\ f_i p^r & 1 \end{pmatrix}.$$

Then

$$\Delta_r\bigl(p^n\bigr) = \Gamma_0\bigl(p^n\bigr) \cap A_{f_1}\Gamma_0\bigl(p^n\bigr)A_{f_1}^{-1} \cap A_{f_2}\Gamma_0\bigl(p^n\bigr)A_{f_2}^{-1}.$$

4. The order of the group $\boldsymbol{\Delta_r(p^n)/\Gamma(p^n)}$

In this section we will compute the order of the groups $\Delta_r(p^n)/\Gamma(p^n)$. We start by giving an explicit description of these groups.

Lemma 7. *Suppose that $\rho(p) > 2$. We have that*

$$\Delta_r\big(p^n\big)/\Gamma\big(p^n\big) \cong \left\{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{GL}\big(2, R/p^nR\big)\colon\ ad \in \mathbb{F}_q^*,\ p^{n-r} | a-d \text{ and } p^{n-r} | bp^r\right\}.$$

In case $\rho(p) = 2$, we have that

$$\Delta_r\big(p^n\big)/\Gamma\big(p^n\big) \cong \left\{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{GL}\big(2, R/p^nR\big)\colon\ ad \in \mathbb{F}_q^*,\ p^{n-r} | a-d-bp^r \text{ and } p^{n-r} | bp^{r+1}\right\}.$$

Proof. This follows directly from Propositions 1, 2 and 5 using the reduction modulo p^n map π_{p^n}. □

Definition 8. Let a prime element $p \in R$ and a positive integer n be given, then we define:

$$t\big(R, p^n\big) = \#\big\{t \in R/p^nR\colon\ t^2 = 1\big\}$$

and

$$s\big(R, p^n\big) = \#\big(\mathbb{F}_q^* \cap \big(\big(R/p^nR\big)^*\big)^2\big).$$

Lemma 9. *For $n \geqslant 1$ and a prime element p of R we have*

$$t\big(R, p^n\big) = \begin{cases} 2 & \text{if } q \text{ is odd}, \\ \rho(p)^{\lfloor \frac{n}{2} \rfloor} & \text{if } q \text{ is even}. \end{cases}$$

Proof. We assume that $R = \mathbb{F}_q[T]$ and that $t \in R/p^nR$ satisfies $t^2 = 1$. Also we denote by $u \in R$ any element such that $\pi_{p^n}(u) = t$. Then it holds that p^n divides $(u-1)(u+1)$. If q is odd, p is relatively prime to either $u-1$ or $u+1$, so p^n divides either $u-1$ or $u+1$. This implies that $t = 1$ or $t = -1$. If q is even, the statement that p^n divides $(u-1)(u+1)$ is equivalent to the statement that p^n divides $(u+1)^2$. This in its turn is equivalent to saying that $p^{\lceil \frac{n}{2} \rceil}$ divides $u+1$ and hence implies that $u = 1 + mp^{\lceil \frac{n}{2} \rceil}$ for some $m \in R$. We conclude that all possibilities for t are represented by expressions of the form $1 + mp^{\lceil \frac{n}{2} \rceil}$, with $\deg_T m < (n - \lceil \frac{n}{2} \rceil) \deg_T p = \lfloor \frac{n}{2} \rfloor \deg_T p$. Therefore there are $q^{\lfloor \frac{n}{2} \rfloor \deg_T p} = \rho(p)^{\lfloor \frac{n}{2} \rfloor}$ possibilities for t if q is even. □

Remark 10. If the number $t(R, p^n)$ is equal to $t(R, p)$ there is an interesting consequence. For any element $a \in R$ such that $\gcd(a, p) = 1$ it holds that $\pi_{p^n}(a)$ is a square in R/p^nR if and only if $\pi_p(a)$ is a square in R/pR. From Lemma 9, we see that this is the case if and only if q is odd.

Lemma 11. *If $n \geqslant 1$ and p is a prime element of R, then*

$$s\big(R, p^n\big) = \begin{cases} (q-1)/2 & \text{if } q \text{ is odd and } \deg_T p \text{ is odd}, \\ q-1 & \text{otherwise}. \end{cases}$$

Proof. We know that $R^* = \mathbb{F}_q^*$. If q is odd, half of these elements are squares in R and hence also in R/p^nR. The other half of the elements will only be squares in R/pR if $\deg_T p$ is even. Since, by Remark 10, for odd q an element is a square in R/p^nR if and only if it is a square in R/pR, the lemma follows for odd q. If q is even, squaring acts as an automorphism on $R^* = \mathbb{F}_q^*$, implying that any element of R^* is a square. A fortiori, any element of $\mathbb{F}_q^*$ is a square in $(R/p^nR)^*$. □

Note that $s(R, p^n)$ actually does not depend on n.

Lemma 12. *Let $n > r > 0$ be integers and suppose that $\rho(p) > 2$. Then we have that*

$$\#\Delta_r(p^n)/\Gamma(p^n) = \begin{cases} s(R,p^n)t(R,p^{n-r})\rho(p)^{r+n} & \text{if } n \leqslant 2r, \\ s(R,p^n)t(R,p^{n-r})\rho(p)^{3r} & \text{if } n > 2r. \end{cases}$$

Proof. Using Lemma 7 and the assumption that $\rho(p) > 2$, it is enough to count for all $s \in \mathbb{F}_q^*$, the number of triples $(a,b,d) \in (R/p^nR)^3$ satisfying $p^n | ad - s$, $p^{n-r} | a - d$ and $p^{n-r} | bp^r$.

We claim that there are no solutions if $s \notin ((R/p^nR)^*)^2$. If q is even, then $(\mathbb{F}_q^*)^2 = \mathbb{F}_q^*$ and therefore the claim is trivial. Now suppose that q is odd. Since $p^n | ad - s$ and $p^{n-r} | a - d$, we find that $a^2 \equiv s \bmod p^{n-r}$. Therefore s is a square modulo p^{n-r}. By Remark 10, s is also a square modulo p^n, so the claim follows.

From now on, we suppose that $s \in ((R/p^nR)^*)^2$. Then there are $s(R,p^n)$ possibilities for s. We claim that for any such s, the number of $(a,d) \in (R/p^nR)^2$ satisfying $p^n | ad - s$ and $p^{n-r} | a - d$ equals $t(R,p^{n-r})\rho(p)^r$. From the conditions, it is clear that $p^{n-r} | a^2 - s$, which implies that $a^2 \equiv s \pmod{p^{n-r}}$. This leaves exactly $t(R,p^{n-r})\rho(p)^r$ possibilities for a. Given any such a, there exists exactly one $d \in R/p^nR$ such that $p^n | ad - s$ and by reducing modulo p^{n-r} we see that $d \equiv a^{-1}s \equiv a^{-1}a^2 \equiv a \bmod p^{n-r}$. This means that $p^{n-r} | a - d$ is satisfied for this d as well.

We claim that the number of $b \in R/p^nR$ such that $p^{n-r} | bp^r$ is equal to $\rho(p)^n$ if $n \leqslant 2r$ and equal to $\rho(p)^{2r}$ if $n > 2r$. Indeed, if $n \leqslant 2r$, the condition $p^{n-r} | bp^r$ is always satisfied, so that all b's in R/p^nR are possible. If $n > 2r$, then the condition simplifies to $p^{n-2r} | b$, meaning that all p^{2r} multiples of p^{n-2r} in R/p^nR are solutions.

Multiplying the number of possibilities for (a,d) with that for b, the lemma follows. □

We are left with the case that $\rho(p) = 2$. Note that in this case $R = \mathbb{F}_2[T]$ and $p = T$ or $p = T + 1$. Moreover, for any of these cases we have $s(R,p^n) = 1$ by Lemma 11. The following lemma deals with the case $\rho(p) = 2$ in detail.

Lemma 13. *Let $n > r > 0$ be integers and suppose that $\rho(p) = 2$. Then we have*

$$\#\Delta_r(2^n)/\Gamma(2^n) = \begin{cases} t(R,p^{n-r})2^{r+n} & \text{if } n \leqslant 2r, \\ t(R,p^{n-r})2^{3r} & \text{if } n > 2r,\ R = \mathbb{F}_2[T] \text{ and } n-r \text{ is even}, \\ t(R,p^{n-r})2^{3r+1} & \text{if } n > 2r,\ R = \mathbb{F}_2[T] \text{ and } n-r \text{ is odd}. \end{cases}$$

Proof. Using Lemma 7 and the fact that $s(R,p^n) = 1$, it is enough to count the number of triples $(a,b,d) \in (R/p^nR)^3$ satisfying

1) $p^n | ad - 1$,
2) $p^{n-r} | a - d - bp^r$, and
3) $p^{n-r-1} | bp^r$.

We now investigate the cases $n \leqslant 2r$ and $n > 2r$ separately.

Suppose that $n \leqslant 2r$. Then the three conditions on (a,b,d) reduce to the conditions $p^n | ad - 1$ and $p^{n-r} | a - d$. By exactly the same argument as in the proof of Lemma 12, we find that the possible number of (a,b,d) satisfying the conditions is $t(R,p^{n-r})\rho(p)^{r+n} = t(R,p^{n-r})2^{r+n}$.

From now on suppose that $n > 2r$. Since $R/pR = \mathbb{F}_2$, the third condition $p^{n-r-1}|bp^r$ implies that either $bp^r \equiv 0 \bmod p^{n-r}$ or $bp^r \equiv p^{n-r-1} \bmod p^{n-r}$. We distinguish these as two subcases. If $bp^r \equiv 0 \bmod p^{n-r}$, the conditions on (a,d) simplify to $p^n|ad-1$ and $p^{n-r}|a-d$. Similarly as before we find that if $bp^r \equiv 0 \bmod p^{n-r}$, there are $t(R, p^{n-r})2^r$ possibilities for (a,d) and 2^{2r} possibilities for b, giving a total of $t(R, p^{n-r})2^{3r}$ possibilities for (a,b,d) in the first subcase. Now we investigate the second possibility $bp^r \equiv p^{n-r-1} \bmod p^{n-r}$. In this subcase we find that there are 2^{2r} possibilities for b, while $d \equiv a + p^{n-r-1} \bmod p^{n-r}$. Moreover, since $p^n|ad-1$, we find that $a \equiv 1 \bmod p$ (and $d \equiv 1 \bmod p$) and hence that

$$1 \equiv ad \equiv a\bigl(a + p^{n-r-1}\bigr) = a^2 + ap^{n-r-1} \equiv a^2 + p^{n-r-1} \bmod p^{n-r}.$$

This implies that $a^2 \equiv 1 + p^{n-r-1} \bmod p^{n-r}$. Only if $1 + p^{n-r-1}$ is a square modulo p^{n-r}, we find $t(R, p^{n-r})2^r$ possibilities for a, otherwise none. Given a, the only possible choice for d is to choose it as the inverse of a modulo p^n. For this choice of d, it holds that

$$d \equiv \bigl(a^2 + p^{n-r-1}\bigr)d \equiv a^2 d + dp^{n-r-1} \equiv a + p^{n-r-1} \bmod p^{n-r}.$$

This means that subcase two gives an additional $t(R, p^{n-r})2^{3r}$ possibilities for (a,b,d), but only if $1 + p^{n-r-1}$ is a square modulo p^{n-r}.

To conclude the proof of the lemma, we need to determine exactly when $1 + p^{n-r-1}$ is a square modulo p^{n-r}. However, it is not hard to see that if $\rho(p) = 2$, this is the case exactly if $n - r$ is odd. □

5. Degrees and structure of the Galois closure

Let integers $n > r > 0$ and a prime $p \in R$ be given. Then $X_0(p^n)$ is a cover of $X_0(p^r)$ and we denote by $\tilde{X}_0^r(p^n)$ the Galois closure of $X_0(p^n)$ over $X_0(p^r)$. In this section we determine the degree of the Galois covers $\tilde{X}_0^r(p^n) \to X_0(p^r)$ and investigate its Galois group. We need some well-known facts from the literature [10].

Let n be a positive integer. The cover $X(p^n) \to X(1)$ is a Galois cover. Denoting by $Z = \{\alpha I\colon \alpha \in \mathbb{F}_q^*\}$ the center of $\mathrm{GL}(2,R)$, it holds that the Galois group of this cover equals $\mathrm{GL}(2,R)/\Gamma(p^n)Z$. Therefore, by Proposition 1, the degree of the cover equals

$$\#\bigl(\mathrm{GL}(2,R)/\Gamma\bigl(p^n\bigr)Z\bigr) = \rho(p)^{3n-2}\bigl(\rho(p)^2 - 1\bigr). \tag{5}$$

Similarly, the cover $X(p^n) \to X_0(p^n)$ has Galois group $\Gamma_0(p^n)/\Gamma(p^n)Z$. However, since

$$\Gamma_0\bigl(p^n\bigr)/\Gamma\bigl(p^n\bigr) \cong \left\{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{GL}\bigl(2, R/p^nR\bigr)\colon ad \in \mathbb{F}_q\right\},$$

we find that the degree of the cover $X_0(p^n) \to X(p^n)$ equals

$$\#\bigl(\Gamma_0\bigl(p^n\bigr)/\Gamma\bigl(p^n\bigr)Z\bigr) = \#\bigl(R/p^nR\bigr)^* \#\bigl(R/p^nR\bigr) = \bigl(\rho(p) - 1\bigr)\rho(p)^{2n-1}. \tag{6}$$

Eqs. (5) and (6) imply that the degree of the cover $X_0(p^n) \to X(1)$ is given by $(\rho(p) + 1)\rho(p)^{n-1}$, which in turn shows that the degree of the cover $X_0(p^n) \to X_0(p^r)$ is given by $\rho(p)^{n-r}$. With these facts in hand, we proceed our investigation of the Galois closure of $X_0(p^n)$ over $X_0(p^r)$. We make the following surprising observation:

Remark 14. The function field of the Galois closure $\tilde{X}_0^r(p^n)$ is obtained by taking the composite over the function field of $X_0(p^r)$ of all $\rho(p)^{n-r}$ conjugates of the function field of $X_0(p^n)$ (again over the function field of $X_0(p^r)$). However, from Corollaries 3 and 6, it follows that in this particular case taking the composite of just three conjugates is enough, even if the degree of the cover $X_0(p^n) \to X_0(p^r)$ is very large.

By the above remark, the degree of $\tilde{X}_0^r(p^n) \to X_0(p^r)$ is at most $\rho(p)^{3(n-r)}$ (in fact at most $\rho(p)^{n-r}(\rho(p)^{n-r}-1)(\rho(p)^{n-r}-2)$). However, using results from the previous sections, we can compute the exact extension degree, as we will see in the next theorem.

Theorem 15. *Let $n > r > 0$ be integers, $p \in R$ a prime and let $\tilde{X}_0^r(p^n)$ denote the Galois closure of $X_0(p^n)$ over $X_0(p^r)$.*

In case $n \leqslant 2r$, we have

$$\deg\bigl(\tilde{X}_0^r(p^n) \to X_0(p^r)\bigr) = \begin{cases} (\rho(p)-1)\rho(p)^{2n-2r-1} & \text{if } q \text{ and } \deg p \text{ are odd},\\ \frac{1}{2}(\rho(p)-1)\rho(p)^{2n-2r-1} & \text{if } q \text{ is odd and } \deg p \text{ is even},\\ (\rho(p)-1)\rho(p)^{2n-2r-\lfloor\frac{n-r}{2}\rfloor-1} & \text{if } q \text{ is even}. \end{cases}$$

In case $n > 2r$, we have

$$\deg\bigl(\tilde{X}_0^r(p^n) \to X_0(p^r)\bigr) = \begin{cases} (\rho(p)-1)\rho(p)^{3n-4r-1} & \text{if } q \text{ and } \deg p \text{ are odd},\\ \frac{1}{2}(\rho(p)-1)\rho(p)^{3n-4r-1} & \text{if } q \text{ is odd and } \deg p \text{ is even},\\ (\rho(p)-1)\rho(p)^{3n-4r-\lfloor\frac{n-r}{2}\rfloor-1} & \text{if } q \text{ is even and } \rho(p) > 2,\\ (\rho(p)-1)\rho(p)^{3n-4r-\lceil\frac{n-r}{2}\rceil-1} & \text{if } \rho(p) = 2. \end{cases}$$

Proof. Since both $\Gamma_0(p^r)$ and $\Delta_r(p^n)$ contain the center Z, the degree of this cover is simply given by the cardinality of the group $\Gamma_0(p^r)/\Delta_r(p^n)$. However,

$$\#\bigl(\Gamma_0(p^r)/\Delta_r(p^n)\bigr) = \frac{\#(\Gamma_0(p^r)/\Gamma(p^n))}{\#(\Delta_r(p^n)/\Gamma(p^n))} = \frac{(q-1)(\rho(p)-1)\rho(p)^{3n-r-1}}{\#(\Delta_r(p^n)/\Gamma(p^n))}.$$

The theorem now follows by case distinction from Lemmas 12 and 13. □

Now that we know the order of the Galois groups $\Gamma_0(p^r)/\Delta_r(p^n)$, the next step is to investigate its group structure. To this end, we introduce the following map:

Definition 16. Let $r > 0$ and $p \in R$ a prime element. Then we define the map

$$\phi_r : \Gamma_0(p^r) \to (R/pR)^*,$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d/a.$$

It is not hard to see that this is a well-defined homomorphism of groups and that its kernel $\mathrm{Ker}(\phi_r)$ consists of those matrices from $\Gamma_0(p^r)$ for which p divides $a-d$. For future reference we denote this kernel by $\Gamma_0^*(p^r)$, i.e., we define for any $r > 0$:

$$\Gamma_0^*(p^r) = \left\{\begin{pmatrix} a & b \\ c & dg \end{pmatrix} \in \Gamma_0(p^r) \colon\ p \mid a-d\right\}. \tag{7}$$

From Propositions 2 and 5 it follows that $\Delta_r(p^{r+1}) \subset \mathrm{Ker}(\phi_r) = \Gamma_0^*(p^r)$. This means that ϕ_r induces a map

$$\overline{\phi}_r : \Gamma_0\bigl(p^r\bigr)/\Delta_r\bigl(p^{r+1}\bigr) \to (R/pR)^*$$

with kernel given by $\Gamma_0^*(p^r)/\Delta_r(p^{r+1})$. Next we identify $\mathrm{Ker}(\overline{\phi}_r)$ with a Sylow subgroup of $\Gamma_0(p^r)/\Delta_r(p^{r+1})$, but first we state a lemma.

Lemma 17. *Let $a, b, c, d \in R$, $e > 0$, $k \geqslant 0$ integers and denote by $p \in R$ a prime element. Then*

$$\begin{pmatrix} a & b \\ cp^e & d \end{pmatrix}^k = \begin{pmatrix} a^k + \mathcal{O}(p^e) & b\frac{a^k - d^k}{a-d} + \mathcal{O}(p^e) \\ cp^e \frac{a^k-d^k}{a-d} + \mathcal{O}(p^{2e}) & d^k + \mathcal{O}(p^e) \end{pmatrix},$$

where $\mathcal{O}(p^m)$ denotes some element from R divisible by p^m.

Proof. This can be shown directly using induction on k. □

Proposition 18. *Let $r > 0$ and denote by ℓ the characteristic of R. The group $\Gamma_0(p^r)/\Delta_r(p^{r+1})$ has a normal, hence unique, ℓ-Sylow subgroup. Moreover, this ℓ-Sylow subgroup is elementary abelian.*

Proof. Since $(\Gamma_0(p^r)/\Delta_r(p^{r+1}))/\mathrm{Ker}(\overline{\phi}_r)$ can be identified with a subgroup of $(R/pR)^*$ and the order of $(R/pR)^*$ is relatively prime to ℓ, the result follows once we show that $\mathrm{Ker}(\overline{\phi}_r)$ is an ℓ-group. Let $g \in \mathrm{Ker}(\overline{\phi}_r)$ and let

$$A = \begin{pmatrix} a & b \\ cp^r & d \end{pmatrix}$$

be a representant of g in $\Gamma_0(p^r)$. Since $g \in \mathrm{Ker}(\overline{\phi}_r)$, the difference between the diagonal elements of A is divisible by p. Using Lemma 17 with $k = \ell$ and $e = r$, we see that

$$\begin{pmatrix} a & b \\ cp^r & d \end{pmatrix}^\ell = \begin{pmatrix} a^\ell + \mathcal{O}(p^r) & b\frac{a^\ell - d^\ell}{a-d} + \mathcal{O}(p^r) \\ cp^r \frac{a^\ell-d^\ell}{a-d} + \mathcal{O}(p^{2r}) & d^\ell + \mathcal{O}(p^r) \end{pmatrix}.$$

Since $a^\ell - d^\ell = (a-d)^\ell$ and $p | a-d$, we see that $A^\ell \in \Delta_r(p^{r+1})$. Therefore $g^\ell = 1$, the identity element in $\Gamma_0(p^r)/\Delta_r(p^{r+1})$. It remains to show that $\mathrm{Ker}(\overline{\phi}_r)$ is abelian, but a direct calculation of the commutator of two elements $g, h \in \mathrm{Ker}(\overline{\phi}_r)$ shows that $ghg^{-1}h^{-1} = 1$ □

Remark 19. Note that by the proof of Proposition 18, the quotient of $\Gamma_0(p^r)/\Delta_r(p^{r+1})$ by its ℓ-Sylow subgroup is a subgroup of the multiplicative group of the finite field R/pR, and hence is cyclic and of order relatively prime to ℓ. Therefore $\Gamma_0(p^r)/\Delta_r(p^{r+1})$ is an extension of an elementary abelian ℓ-group by a cyclic group of order relatively prime to ℓ.

Corollary 20. *For any $n > r > 0$, the group $\Gamma_0(p^r)/\Delta_r(p^n)$ has a normal, hence unique, ℓ-Sylow subgroup.*

Proof. For $n = r + 1$ the result follows from Proposition 18. Now let $n > r + 1$. The natural group homomorphism $\psi : \Gamma_0(p^r)/\Delta_r(p^n) \to \Gamma_0(p^r)/\Delta_r(p^{r+1})$, shows that the group $\Gamma_0(p^r)/\Delta_r(p^{r+1})$ is isomorphic to the quotient group of $\Gamma_0(p^r)/\Delta_r(p^n)$ by $\Delta_r(p^{r+1})/\Delta_r(p^n)$. The preimage under ψ of the (normal) ℓ-Sylow subgroup of $\Gamma_0(p^r)/\Delta_r(p^{r+1})$, is a normal ℓ-subgroup of $\Gamma_0(p^r)/\Delta_r(p^n)$. In fact, it is an ℓ-Sylow subgroup, since by Lemmas 12 and 13 the group $\Delta_r(p^{r+1})/\Delta_r(p^n)$ is an ℓ-group (since its order is a power of ℓ). □

As for $n = r+1$, we see that the group $\Gamma_0(p^r)/\Delta_r(p^n)$ is an extension of an ℓ-group by a cyclic group of order relatively prime to ℓ.

6. Towers of Drinfeld modular curves

In this section we will collect several consequences for some towers of Drinfeld modular curves and their Galois closures. The tower

$$\cdots \to X_0\big(p^{r+2}\big) \to X_0\big(p^{r+1}\big) \to X_0\big(p^r\big) \tag{8}$$

and several variants of it have been studied extensively by various authors, see among others [4–6, 11]. Our study in the previous sections gives rise to the tower

$$\cdots \to \tilde{X_0^r}\big(p^{r+2}\big) \to \tilde{X_0^r}\big(p^{r+1}\big) \to \tilde{X_0^r}\big(p^r\big) = X_0\big(p^r\big), \tag{9}$$

which is special in the sense that the cover $\tilde{X_0^r}(p^n) \to X_0(p^r)$ is Galois for any $n > r$. A tower having this property is called a Galois tower.

We will start by investigating the steps in the Galois tower (9). From Theorem 15 the order of the Galois groups occurring in these steps are readily computed and we will do so below. Also we investigate their group structure, but first we state and prove a lemma. For a group G, we denote by $[G, G]$ its commutator subgroup.

Lemma 21. *Suppose that $n > r > 0$ and denote by ℓ the characteristic of R. We have*

$$\big[\Delta_r\big(p^n\big), \Delta_r\big(p^n\big)\big] \subset \Delta_r\big(p^{n+1}\big)$$

and

$$g \in \Delta_r\big(p^n\big) \quad \Rightarrow \quad g^\ell \in \Delta_r\big(p^{n+1}\big).$$

Proof. A direct calculation shows that $[\Delta_r(p^n), \Delta_r(p^n)] \subset \Gamma_0(p^{n+1})$. Also, since $\Delta_r(p^n) \trianglelefteq \Gamma_0(p^r)$, we find that for any $\sigma \in \Gamma_0(p^r)$ we have

$$\sigma\big[\Delta_r\big(p^n\big), \Delta_r\big(p^n\big)\big]\sigma^{-1} = \big[\sigma\Delta_r\big(p^n\big)\sigma^{-1}, \sigma\Delta_r\big(p^n\big)\sigma^{-1}\big] = \big[\Delta_r\big(p^n\big), \Delta_r\big(p^n\big)\big].$$

This implies that

$$\big[\Delta_r\big(p^n\big), \Delta_r\big(p^n\big)\big] = \bigcap_{\sigma\in\Gamma_0(p^r)} \sigma\big[\Delta_r\big(p^n\big), \Delta_r\big(p^n\big)\big]\sigma^{-1} \subset \Delta_r\big(p^{n+1}\big).$$

To prove the second item, we use Lemma 17 with $k = \ell$ and $e = n$. With the notation as in that lemma, the assumption that $g \in \Delta_r(p^n)$ implies that $p^{n-r} | a - d - bp^r$ and hence that $p | a - d$. Similarly as in the proof of Proposition 18, we then find that $g^\ell \in \Gamma_0(p^{n+1})$. By definition of $\Delta_r(p^n)$, we have that for any $\sigma \in \Gamma_0(p^r)$, the element $\sigma^{-1}g\sigma$ is in $\Gamma_0(p^n)$, implying that $(\sigma^{-1}g\sigma)^\ell = \sigma^{-1}g^\ell\sigma \in \Gamma_0(p^{n+1})$. This implies that $g^\ell \in \bigcap_{\sigma\in\Gamma_0(p^r)} \sigma\Gamma_0(p^{n+1})\sigma^{-1} = \Delta_r(p^{n+1})$. □

We continue our investigating of the steps in the Galois tower (9).

Theorem 22. *Let $n > r > 0$ and denote by ℓ the characteristic of R. The Galois cover $\tilde{X}_0^r(p^n) \to \tilde{X}_0^r(p^{n-1})$ has Galois group isomorphic to $\Delta_r(p^{n-1})/\Delta_r(p^n)$. We have*

$$\#\Delta_r(p^r)/\Delta_r(p^{r+1}) = \begin{cases} (\rho(p)-1)\rho(p) & \text{if } q \text{ and } \deg p \text{ are odd}, \\ \frac{1}{2}(\rho(p)-1)\rho(p) & \text{if } q \text{ is odd and } \deg p \text{ is even}, \\ (\rho(p)-1)\rho(p) & \text{if } q \text{ is even}. \end{cases}$$

Moreover, for $n > r+1$, the Galois group of the cover $\tilde{X}_0^r(p^n) \to \tilde{X}_0^r(p^{n-1})$ is an elementary abelian ℓ-group.

If q is odd, its order is given by

$$\#\Delta_r(p^{n-1})/\Delta_r(p^n) = \begin{cases} \rho(p)^2 & \text{if } n \leqslant 2r+1, \\ \rho(p)^3 & \text{if } n > 2r+1. \end{cases}$$

If q is even and $\rho(p) > 2$, its order is given by

$$\#\Delta_r(p^{n-1})/\Delta_r(p^n) = \begin{cases} \rho(p) & \text{if } n-r \text{ is even and } n \leqslant 2r+1, \\ \rho(p)^2 & \text{if } n-r \text{ is odd and } n \leqslant 2r+1, \\ \rho(p)^2 & \text{if } n-r \text{ is even and } n > 2r+1, \\ \rho(p)^3 & \text{if } n-r \text{ is odd and } n > 2r+1. \end{cases}$$

If q is even and $\rho(p) = 2$, its order is given by

$$\#\Delta_r(p^{n-1})/\Delta_r(p^n) = \begin{cases} \rho(p) & \text{if } n-r \text{ is even and } n \leqslant 2r, \\ \rho(p)^2 & \text{if } n-r \text{ is odd and } n \leqslant 2r, \\ \rho(p)^2 & \text{if } n = 2r+1, \\ \rho(p)^3 & \text{if } n-r \text{ is even and } n > 2r+1, \\ \rho(p)^2 & \text{if } n-r \text{ is odd and } n > 2r+1. \end{cases}$$

Proof. Since $\Gamma_0(p^r)/\Delta_r(p^n)$ respectively $\Gamma_0(p^r)/\Delta_r(p^{n-1})$ are the Galois groups of the covers $\tilde{X}_0^r(p^n) \to \tilde{X}_0^r(p^r)$, respectively $\tilde{X}_0^r(p^{n-1}) \to \tilde{X}_0^r(p^r)$, we see that the degree of the cover $\tilde{X}_0^r(p^n) \to \tilde{X}_0^r(p^{n-1})$ is given by

$$\frac{\#\Gamma_0(p^r)/\Delta_r(p^n)}{\#\Gamma_0(p^r)/\Delta_r(p^{n-1})} = \frac{\#\Delta_r(p^{n-1})}{\#\Delta_r(p^n)}.$$

Moreover, the group $\Delta_r(p^{n-1})/\Delta_r(p^n)$ acts trivially on $\tilde{X}_0^r(p^{n-1})$, so it is the full Galois group of the cover $\tilde{X}_0^r(p^n) \to \tilde{X}_0^r(p^{n-1})$.

The cardinalities of the groups follow directly from Theorem 15, while from Lemma 21, we conclude that the group $\Delta_r(p^{n-1})/\Delta_r(p^n)$ is an elementary abelian ℓ-group if $n > r+1$. □

The only step in the tower (9) that might not be elementary abelian is the first one. We have seen though in Remark 19 that this step can be split into two: a tame cover with cyclic Galois group and an elementary abelian cover.

One may wonder when the cover $X_0(p^n) \to X_0(p^r)$ is Galois. This is easy to investigate now.

Proposition 23. *Let $n > r > 0$. The cover $X_0(p^n) \to X_0(p^r)$ is Galois if and only if $\rho(p) = 2$ and one of the following holds*:

1. $n = r + 1$, *or*
2. $r > 1$ *and* $n = r + 2$.

Proof. The cover $X_0(p^n) \to X_0(p^r)$ is Galois if and only if

$$\deg\big(\tilde{X}_0^r\big(p^{r+1}\big) \to X_0\big(p^r\big)\big) = \deg\big(X_0\big(p^{r+1}\big) \to X_0\big(p^r\big)\big).$$

However, we have

$$\deg\big(X_0\big(p^{r+1}\big) \to X_0\big(p^r\big)\big) = \rho(p)^{n-r},$$

while we can use Theorem 15 to compute $\deg(\tilde{X}_0^r(p^{r+1}) \to X_0(p^r))$. □

As follows from Proposition 23, the steps in the tower (8) are not Galois in general. We will now construct a slight variation of this tower with Galois steps.

Define $X_0^*(p^n)$ to be the modular curve corresponding to the congruence subgroup $\Gamma_0^*(p^n)$ from Eq. 7. For $r > 0$, we then obtain a tower

$$\cdots \to X_0^*\big(p^{r+2}\big) \to X_0^*\big(p^{r+1}\big) \to X_0^*\big(p^r\big). \tag{10}$$

Since $\Gamma_0^*(p^r)$ is the kernel of the map ϕ_r, for any $r > 0$, the cover $X_0^*(p^r) \to X_0(p^r)$ is Galois with Galois group $\Gamma_0(p^r)/\Gamma_0^*(p^r)$, which can be identified with a subgroup of $(R/pR)^*$. Therefore it is a cyclic group of order relatively prime to ℓ.

In fact more is true: Using Corollary 20, the tower (10) can be obtained from the tower (8) by taking the composition of the latter tower and $X_0^*(p^r)$. Since $\deg(X_0(p^n) \to X_0(p^r))$ is a power of ℓ, it is relatively prime to $\deg(X_0^*(p^r) \to X_0(p^r))$. This implies that

$$\deg\big(X_0^*\big(p^n\big) \to X_0^*\big(p^r\big)\big) = \deg\big(X_0\big(p^n\big) \to X_0\big(p^r\big)\big) = \rho(p)^{n-r}.$$

Note that for any $r > 0$, $X_0^*(p^{r+1}) \to X_0(p^r)$ is the Galois closure of $X_0(p^{r+1}) \to X_0(p^r)$ and that $X_0^*(p^{r+1})$ is fixed by the ℓ-Sylow subgroup of the Galois group. Therefore the steps in tower (10) are Galois of degree $\rho(p)$, with an elementary abelian ℓ-group.

Since $X_0^*(p^{r+1}) \to X_0(p^r)$ is the Galois closure of $X_0(p^{r+1}) \to X_0(p^r)$, one could hope that for $n > r > 0$, the cover $\tilde{X}_0^r(p^n) \to X_0^*(p^r)$ is the Galois closure of $X_0^*(p^n) \to X_0^*(p^r)$. This is indeed the case as the following proposition shows.

Proposition 24. *The Galois closure of* $X_0^*(p^n) \to X_0^*(p^r)$ *is given by* $\tilde{X}_0^r(p^n) \to X_0^*(p^r)$.

Proof. Similarly as for $X_0(p^n) \to X_0(p^r)$, see Eq. 1, the Galois closure of $X_0^*(p^n) \to X_0^*(p^r)$ is determined by the congruence subgroup

$$\Delta_r^*\big(p^n\big) := \bigcap_{\sigma \in \Gamma_0^*(p^r)} \sigma \Gamma_0^*\big(p^n\big)\sigma^{-1}.$$

We will show that $\Delta_r^*(p^n) = \Delta_r(p^n)$.

It is clear that $\tilde{X}_0^r(p^n) \to X_0^*(p^r)$ is Galois, and this implies that the Galois closure of $X_0^*(p^n) \to X_0^*(p^r)$ is covered by $\tilde{X}_0^r(p^n)$. This implies that $\Delta_r^*(p^n) \supset \Delta_r(p^n)$. On the other hand, we see that

$$\Delta_r\big(p^n\big) = \bigcap_{\sigma \in \Gamma_0^*(p^r)} \sigma \Gamma_0\big(p^n\big)\sigma^{-1} \supset \bigcap_{\sigma \in \Gamma_0^*(p^r)} \sigma \Gamma_0^*\big(p^n\big)\sigma^{-1} = \Delta_r^*\big(p^n\big),$$

where the first equality follows from the observation that the matrices A_{f_1} and A_{f_2} from Remark 4 and Corollary 6 are elements of $\Gamma_0^*(p^r)$. □

Remark 25. From the proof of Proposition 24, we see that, as in Remark 14, the Galois closure of the cover $X_0^*(p^n) \to X_0^*(p^r)$ is again obtained by taking the composite of just three of the $\rho(p)^{n-r}$ conjugates of $X_0^*(p^n)$ over $X_0^*(p^r)$. As seen above, the Galois group G of the Galois closure of $X_0^*(p^n) \to X_0^*(p^r)$ is just the ℓ-Sylow subgroup of the Galois group of $\tilde{X_0^r}(p^n)$ over $X_0(p^r)$. In particular, if $n = r+1$, the group G is an elementary abelian ℓ-group (see Proposition 18). For arbitrary $n > r > 0$, the order of G can immediately be obtained from Theorem 22.

We have already seen that tower (10) is closer to a Galois tower than tower (8) in the sense that the steps in the former tower are Galois. Similarly as in Proposition 23, we now investigate when the extension $X_0^*(p^n) \to X_0^*(p^r)$ is Galois.

Proposition 26. *The cover $X_0^*(p^n) \to X_0^*(p^r)$ is Galois if and only if*

1. $n = r+1$, *or*
2. $r > 1$, $n = r+2$ *and $\rho(p)$ is even.*

Proof. From Proposition 24, we see that $X_0^*(p^n) \to X_0^*(p^r)$ is Galois if and only if

$$\rho(p)^{n-r} = \deg\bigl(X_0^*(p^n) \to X_0^*(p^r)\bigr) = \deg\bigl(\tilde{X_0^r}(p^n) \to X_0^*(p^r)\bigr).$$

However, since

$$\deg\bigl(\tilde{X_0^r}(p^n) \to X_0^*(p^r)\bigr) = \frac{\deg(\tilde{X_0^r}(p^n) \to X_0(p^r))}{\deg(X_0^*(p^r) \to X_0(p^r))}$$

and

$$\deg\bigl(X_0^*(p^r) \to X_0(p^r)\bigr) = \deg\bigl(\tilde{X_0^r}(p^{r+1}) \to X_0(p^r)\bigr)/\rho(p),$$

the proposition now follows directly by using Theorem 15. □

7. Towers of function fields over finite fields

In [4], it is shown that the tower of function fields $F_0 \subset F_1 \subset F_2 \subset \cdots$ recursively defined by

$$F_0 = \mathbb{F}_{q^2}(x_0) \quad \text{and} \quad F_k = F_{k-1}(x_k), \quad \text{with} \quad x_k^q + x_k = \frac{x_{k-1}^q}{x_{k-1}^{q-1}+1}, \tag{11}$$

is in fact the reduction modulo $T+1$ of the Drinfeld tower (10) with $p = T$ and $r = 2$. This tower was first given in [6] and has become a classical example of a tower of function fields over a finite field, which has many rational places compared to its genus asymptotically (in fact it is asymptotically optimal, i.e. it attains the Drinfeld–Vladut bound). We denote its Galois closure by $F_0 \subset \tilde{F}_1 \subset \tilde{F}_2 \subset \cdots$. We sum up what we obtained in Theorem 15, Remark 25 and Proposition 26 for the tower (11) in the following corollary.

Corollary 27. *Define the tower $F_0 \subset F_1 \subset F_2 \subset \cdots$ as in Eq.* (11) *and denote by $F_0 = \tilde{F}_0 \subset \tilde{F}_1 \subset \tilde{F}_2 \subset \cdots$ its Galois closure, i.e. $\tilde{F}_k$ is the Galois closure of the extension F_k/F_0. Let $k > 0$ be an integer.*

1. *For all $k > 0$, the extension $\tilde{F}_k/F_0$ is Galois and its Galois group is an ℓ-group.*
2. *$\tilde{F}_k$ is the composite over F_0 of three conjugates of F_k over F_0.*
3. *For all $k > 0$, the Galois group of the extension $\tilde{F}_k/\tilde{F}_{k-1}$ is an elementary abelian ℓ-group.*
4. *If q is odd, the degree of the extension $\tilde{F}_k/F_0$ is given by*

$$[\tilde{F}_k : F_0] = \begin{cases} q^{2k-1} & \text{if } k = 1, 2, \\ q^{3k-3} & \text{if } k > 2. \end{cases}$$

   If q is even, the degree of the extension $\tilde{F}_k/F_0$ is given by

$$[\tilde{F}_k : F_0] = \begin{cases} q^{2k-1-\lfloor \frac{k}{2} \rfloor} & \text{if } k = 1, 2, \\ q^{3k-3-\lfloor \frac{k}{2} \rfloor} & \text{if } k > 2 \text{ and } q > 2, \\ q^{3k-3-\lceil \frac{k}{2} \rceil} & \text{if } k > 2 \text{ and } q = 2. \end{cases}$$

5. *The extension F_k/F_0 is Galois if and only if*
   - *$k = 1$, or*
   - *$k = 2$ and q is even.*

For $q = 2$, it was observed in [15] that two steps in tower (11) are Galois. We see that the same is true for any even q. For q an odd prime, the Galois closure of the tower (11) was studied in [23]. Extension degrees were not obtained there. In [19] the optimality of the Galois closure of the tower (11) was shown. Some basic properties of Galois closures of towers were investigated in [8].

Remark 28. In [5], the tower $E_0 \subset E_1 \subset E_2 \subset \cdots$ is introduced, recursively defined by

$$E_0 = \mathbb{F}_{q^2}(z_0) \quad \text{and} \quad E_k = E_{k-1}(z_k), \quad \text{with } z_k^q z_{k-1}^{q-1} + z_k = z_{k-1}^q.$$

This tower was shown to be related to the tower from Eq. (11) in [6]. More precisely, the variables x_i and z_i are connected by the relations $z_0^{q+1} = x_0^q/(x_0^{q-1} + 1)$ and $z_k = x_k x_{k-1}$ for $k > 0$.

This means that the tower of function fields $E_0 \subset E_1 \subset E_2 \subset \cdots$ can be obtained from the tower of function fields $F_0 \subset F_1 \subset F_2 \subset \cdots$, by composing the latter with the function field $E_0 = \mathbb{F}_{q^2}(z_0)$. This is a cyclic extension of F_0 of order $q + 1$. Since we know from Corollary 27 that the Galois group of the extension $\tilde{F}_k/F_0$ is an ℓ-group, the field $\tilde{F}_k$ is linearly disjoint from E_0 over F_0. This means that Corollary 27 also holds for the tower from [5]. More precisely, when we replace each F by an E in the statement of Corollary 27, the resulting statement is still true.

References

[1] A. Bassa, P. Beelen, On the construction of Galois towers, in: Proceedings of AGCT-11, CIRM, Marseilles, France, 2007, Geometry Cryptography and Coding Theory, in: Contemp. Math., vol. 487, 2009, pp. 9–20.

[2] V.G. Drinfeld, S.G. Vladut, The number of points of an algebraic curve, Funct. Anal. Appl. 17 (1983) 53–54, translated from the Russian paper in Funktsional. Anal. i Prilozhen.

[3] N.D. Elkies, Explicit modular towers, in: Proc. 35th Ann. Allerton Conf. on Communication, Control and Computing, Urbana, IL, 1997, pp. 23–32.

[4] N.D. Elkies, Explicit towers of Drinfeld modular curves, in: Progr. Math., vol. 202, 2001, pp. 189–198.

[5] A. Garcia, H. Stichtenoth, A tower of Artin–Schreier extensions of function fields attaining the Drinfeld–Vladut bound, Invent. Math. 121 (1995) 211–222.

[6] A. Garcia, H. Stichtenoth, On the asymptotic behaviour of some towers of function fields over finite fields, J. Number Theory 61 (1996) 248–273.

[7] A. Garcia, H. Stichtenoth, H. Rück, On tame towers over finite fields, J. Reine Angew. Math. 557 (2003) 53–80.

[8] A. Garcia, H. Stichtenoth, On the Galois closure of towers, in: Recent Trends in Coding Theory and Its Applications, in: AMS/IP Stud. Adv. Math., vol. 41, Amer. Math. Soc., 2007, pp. 83–92.

[9] E.-U. Gekeler, Drinfeld–Moduln und modulare Formen über rationalen Funktionenkörpern, Bonner Math. Schriften 119 (1980).

[10] E.-U. Gekeler, Drinfeld Modular Curves, Lecture Notes in Math., vol. 1231, 1986.

[11] E.-U. Gekeler, Asymptotically optimal towers of curves over finite fields, in: Proc. Conference on Algebra and Algebraic Geometry, Abhyankar 70, Springer-Verlag, 2000.

[12] D. Goss, π-adic Eisenstein series for function fields, Compos. Math. 41 (1980) 3–38.

[13] Y. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields, J. Math. Sci. Univ. Tokyo 28 (1981) 721–724.

[14] Yu.I. Manin, What is the maximum number of points on a curve over $\mathbb{F}_2$?, J. Math. Sci. Univ. Tokyo 28 (1981) 715–720.

[15] G. McGuire, A. Zaytsev, On the Zeta Functions of an optimal tower of function fields over $\mathbb{F}_4$, arXiv:0911.2128.

[16] H. Niederreiter, C.P. Xing, Rational Points on Curves Over Finite Fields, London Math. Soc. Lecture Note Ser., vol. 285, 2001.

[17] J.-P. Serre, Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini, C. R. Math. Acad. Sci. Paris 296 (1983) 397–402.

[18] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions, Iwanami Shoten Publishers, Princeton University Press, 1971.

[19] H. Stichtenoth, Transitive and self-dual codes attaining the Tsfasman–Vladut–Zink bound, IEEE Trans. Inform. Theory 52 (5) (2006) 2218–2224.

[20] M.A. Tsfasman, S.G. Vladut, Algebraic–Geometric Codes, Kluwer, Dordrecht, 1991.

[21] M.A. Tsfasman, S.G. Vladut, T. Zink, Modular curves, Shimura curves and Goppa codes, better than the Varshamov–Gilbert bound, Math. Nachr. 109 (1982) 21–28.

[22] S.G. Vladut, Yu.I. Manin, Linear codes and modular curves, J. Sov. Math. 30 (1985) 2611–2643.

[23] A. Zaytsev, The Galois closure of the Garcia–Stichtenoth tower, Finite Fields Appl. 13 (2007) 751–761.