Bachelor Thesis

Standard construction for certain finite fields

Author:
J.E.F. Rood
math@jobrood.nl

Supervisor:
Dr. B. de Smit

Universiteit Leiden

March 23, 2015

1 Introduction

A finite field always has p^n elements for some prime number p and a positive number n. Moreover for every prime number p and positive number n there exists a finite field with p^n elements. Furthermore any two fields of the same cardinality are isomorphic. For a prime number p and positive integer n a finite field of cardinality p can be represented as $\mathbb{Z}/p\mathbb{Z}$ and a field of cardinality p^n can be constructed as $(\mathbb{Z}/p\mathbb{Z})[X]/(f)$ with $f \in (\mathbb{Z}/p\mathbb{Z})[X]$ a monic irreducible polynomial of degree n.

We are looking for an algorithm such that on input of a prime number p and positive integer n it will give as output a field of cardinality p^n. A possible algorithm would be to randomly pick a polynomial of degree n and check if it is irreducible in $(\mathbb{Z}/p\mathbb{Z})[X]$. Such an algorithm is relatively fast, but such an algorithm could produce different output on multiple runs. Another example is the commonly used Conway polynomials, these are defined inductively as the minimal irreducible polynomial of a lexicographical ordering such that the Conway polynomial $c_{p,n}$ is compatible with the polynomials $c_{p,m}$ for all m dividing n. There are two algorithms to produce such a polynomial $c_{p,n}$, which results in a deterministic output, but these are also time consuming [8]. We would like an algorithm that combines the best aspect of the previous two examples, it has to be fast and it results in the same output every time it runs on the same input.

De Smit and Lenstra defined an effective construction for a finite field based upon prime ideals instead of polynomials [4]. For this construction there is a probabilistic algorithm that on input of a prime number p and positive integer n carries out the construction in polynomial time [5]. Moreover, it is a randomized algorithm of the type *Las Vegas algorithms* [10], so for a certain p and n it will always produce the same field. Thus the method of De Smit and Lenstra should combine the aspects we are looking for in the algorithm for a finite field. For some aspects of the method no proof has been published yet.

The purpose of this thesis is to prove for any prime number p and a positive integer n such that $\gcd(p, n) = 1$ that the definition of De Smit and Lenstra defines a construction of a finite field of cardinality p^n.

Definition 1. Let r be a prime number and define $\mathbf{r} := r \cdot \gcd(2, r)$. For $i \in \mathbb{Z}_{\geq 0}$ we define

$$A_{r,i} := \mathbb{Z}[X_0, X_1, X_2, ..., X_i]/(\sum_{i=0}^{r-1} X_0^{\frac{\mathbf{r}}{r}i}; X_j^r - X_{j-1} : 0 < j \leq i).$$

Note that the residue class of X_i is a primitive root $\zeta_{\mathbf{r}r^i}$ of order $\mathbf{r}r^i$. Also notice for $i \in \mathbb{Z}_{\geq 0}$ that $A_{r,i}$ is a ring and that $A_{r,j} \subset A_{r,i}$ for $j < i$. Thus we can define A_r as the union $\bigcup_{i=0}^{\infty} A_{r,i}$. In Section 2 we will show that the ring A_r is the ring of integers of the field $\mathbb{Q}(\zeta_{\mathbf{r}r^i} : i \geq 0)$. Also we will show that the Galois group of $\mathbb{Q}(\zeta_{\mathbf{r}r^i} : i \geq 0)$ over $\mathbb{Q}$ is the unit group $\mathbb{Z}_r^*$ of the ring of r-adic integers.

Notation. Denote the torsion subgroup of the Galois group of $\mathbb{Q}(\zeta_{\mathbf{r}r^j} : j > 0)$ over $\mathbb{Q}$ by Δ_r.

We will see in Lemma 12 that Δ_r is isomorphic to $(\mathbb{Z}/\mathbf{r}\mathbb{Z})^*$, which is also isomorphic to the Galois group of $\mathbb{Q}(\zeta_{\mathbf{r}})$ over $\mathbb{Q}$. The group Δ_r is cyclic of order $\varphi(\mathbf{r})$ where φ denotes the Euler phi function.

Definition 2. Define $B_{r,k}$ as the set $\{a \in A_{r,k} | \forall \delta \in \Delta_r : \delta(a) = a\}$ and B_r as the union $\bigcup_{i=0}^{\infty} B_{r,i}$.

Let p be a prime number. Notice that $B_{r,0} = \mathbb{Z}$ and thus $B_{r,0}/pB_{r,0}$ is a field of cardinality p. In this thesis we will look for ideals $\mathfrak{p}$ of the ring $B_{r,k}$ for all $k \in \mathbb{Z}_{\geq 0}$ such that $B_{r,k}/\mathfrak{p}B_{r,k}$ is a field with characteristic p, in other words prime ideals such that $p \in \mathfrak{p}$.

Notation. For prime numbers r and p such that $p \neq r$ we will denote the *set of prime ideals of B_r containing p* as $S_{p,r}$.

Theorem 3. *Let $l := \mathrm{ord}_r\left(\frac{p^{\varphi(\mathbf{r})}-1}{\mathbf{r}/r}\right)$, where ord_r is the r-adic valuation. The cardinality of $S_{p,r}$ is r^l and for every prime ideal $\mathfrak{P} \in S_{p,r}$ there is a unique prime ideal $\mathfrak{p}$ of $B_{r,l}$ such that $\mathfrak{P} = \mathfrak{p} \cdot B_r$.*

This implies that given generators of a prime ideal of $B_{r,l}$ containing p, we will have the generators for a prime ideal in $S_{p,r}$.

Definition 4. For i a non-negative integer, k a positive integer and r a prime number let $\eta_{r,k,i} := \sum_{\delta \in \Delta_r} \sigma_\delta(\zeta_{\mathbf{r}r^k}^{1+i\mathbf{r}r^{k-1}}) \in B_{r,k}$.

We will show that the elements $\eta_{r,k,i}$ with $0 \leq i < r$ form a module basis for $B_{r,k}[\frac{1}{r}]$ over $B_{r,k-1}[\frac{1}{r}]$. Combining this fact and Theorem 3 we will prove the following theorem.

Theorem 5. *For $\mathfrak{p} \in S_{p,r}$ there is a unique system $(a_{\mathfrak{p},j})_{0 \leq j < lr}$ of integers $a_{\mathfrak{p},j} \in \{0, 1, \ldots, p-1\}$ such that $\mathfrak{p}$ is generated as a module over B_r by p and $\{\eta_{r,j+1,i} - a_{\mathfrak{p},i+jr} : 0 \leq j < l, 0 \leq i < r\}$.*

As a consequence of Theorem 5 we can define a prime ideal of B_r as the smallest in a lexicographical ordering as done in Definition 6.

Definition 6. Let $\mathfrak{p}_{p,r}$ be the unique prime ideal in $S_{p,r}$ such that for every prime ideal $\mathfrak{q}$ in $S_{p,r}$ there is a $j \in \{0, 1, ..., lr-1\}$ such that for all $i < j$ we have $a_{\mathfrak{p}_{p,r},i} = a_{\mathfrak{q},i}$ and $a_{\mathfrak{p}_{p,r},j} \leq a_{\mathfrak{q},j}$.

Theorem 7. *Denote the prime ideal $\mathfrak{p}_{p,r} \cap B_{r,i}$ as $\mathfrak{p}_{p,r,i}$ and let $\overline{\eta_{p,r,k}} = \eta_{p,r,k} \pmod{\mathfrak{p}_{p,r,k}}$. For all $k \geq 0$ the field $\mathbb{F}_p(\overline{\eta_{r,l+k,0}})$ has cardinality p^{r^k}.*

For a non-negative integer k and distinct prime numbers p, r, the field of cardinality p^{r^k} constructed in Theorem 7 is the standard model for a field of cardinality p^{r^k} as defined by De Smit and Lenstra.

We conclude this thesis with an argument using tensor products, which proves that the defined construction of De Smit and Lenstra is a construction of a finite field of cardinality p^n for p a prime number and n a positive integer such that $\gcd(p, n) = 1$.

2 Cyclotomic rings

Let r be a prime number and define $\mathbf{r} := r \cdot \gcd(2, r)$. We consider the ring

$$\mathbb{Q}[X_0, X_1, X_2, ...]/(\sum_{i=0}^{r-1} X_0^{\frac{\mathbf{r}}{r} i}; X_j^r - X_{j-1} : j > 0).$$

The residue class $\zeta_{\mathbf{r}r^i}$ of X_i is a root of unity of order $\mathbf{r}r^i$. Note that this ring is a field which is generated as a field extension of $\mathbb{Q}$ by $\{\zeta_{\mathbf{r}r^j} : j \geq 0\}$.

Lemma 8. *For n a positive integer, let $q = \mathbf{r}r^n$. There is an isomorphism $(\mathbb{Z}/q\mathbb{Z})^* \to \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$, such that $a \mapsto (\zeta_q \mapsto \zeta_q^a)$.*

Proof. We know $\zeta_q^q = 1$ and $\zeta_q^j \neq 1$ for any $1 \leq j < q$. It follows that for an automorphism $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ the identities $\sigma(\zeta_q)^q = 1$ and $\sigma(\zeta_q)^j \neq 1$ hold. Now $\sigma(\zeta_q)$ is a root of $X^q - 1$, but not of $X^j - 1$ and thus $\sigma(\zeta_q) = \zeta_q^a$ where a is relatively prime to q. Thus there is an injection from $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ to $(\mathbb{Z}/q\mathbb{Z})^*$. Proposition 6.2 (b) in Milne's course notes [9] gives us that $\#\,\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) = \varphi(q) = \#(\mathbb{Z}/q\mathbb{Z})^*$, therefore our injection is even a bijection. □

Notation. The cyclic group of m elements we will denote as C_m.

For a prime power q Gauss [6] showed that $(\mathbb{Z}/q\mathbb{Z})^*$ is isomorphic to either the cyclic group $C_{\varphi(q)}$ or the product of two cyclic groups C_2 and $C_{q/4}$ depending on $q \pmod 2$, combined with Lemma 8 we find:

$$\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \cong \begin{cases} C_2 \times C_{q/4} & \text{if } 2|q \text{ and } q \neq 2, \\ C_{\varphi(q)} & \text{else.} \end{cases}$$

Then for $q = \mathbf{r}r^n$ with $n \geq 0$ a positive integer we have $\#\,\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) = \varphi(\mathbf{r})r^n$.

Definition 9. Let K be an algebraic field extension of $\mathbb{Q}$. The *ring of integers* $\mathfrak{O}_K$ of K is the set of all $a \in K$ such that a is a root of a monic polynomial $f \in \mathbb{Z}[X]$. For an element $x \in \mathfrak{O}_K$ we say it is integral over $\mathbb{Z}$.

From Proposition 6.2 (b) in Milne's course notes [9] we have that $\mathbb{Z}[\zeta_q]$ is the ring of integers of $\mathbb{Q}(\zeta_q)$. Thus the ring $A_{r,i}$ as in Definition 1 is the ring of integers of $\mathbb{Q}(\zeta_{\mathbf{r}r^i})$.

Lemma 10.

I. *For a chain of field extensions $K_0 \subset K_1 \subset ...$ we have the identity of rings of integers*

$$\mathfrak{O}_{\cup_{i\geq 0} K_i} = \bigcup_{i>0} \mathfrak{O}_{K_i}.$$

II. *For an extension of fields $K \subset L$ with $G = \mathrm{Aut}(L/K)$ we have the identity of rings of integers*

$$\mathfrak{O}_L^G = \mathfrak{O}_{L^G}.$$

Proof. Note that for a chain of field extensions $K_0 \subset K_1 \subset ...$ we have

$$\begin{aligned} x \in \bigcup_{i\geq 0} \mathfrak{O}_{K_i} &\Leftrightarrow \text{there is an } i \geq 0 \text{ such that } x \in \mathfrak{O}_{K_i} \\ &\Leftrightarrow \text{there is an } i \geq 0 \text{ such that } x \in K_i \text{ and } x \text{ is integral over } \mathbb{Z}. \\ &\Leftrightarrow x \in \bigcup_{i\geq 0} K_i \text{ and } x \text{ is integral over } \mathbb{Z}. \\ &\Leftrightarrow x \in \mathfrak{O}_{\cup_{i\geq 0} K_i}. \end{aligned}$$

Likewise we have the following equivalences for the fields $K \subset L$ with $G = \mathrm{Aut}(L/K)$.

$$\begin{aligned} x \in \mathfrak{O}_{L^G} &\Leftrightarrow x \in L^G \text{ and } x \text{ is integral over } \mathbb{Z}. \\ &\Leftrightarrow x \in L \text{ and for every } \sigma \in G \text{ we have } \sigma(x) = x \\ &\quad \text{and } x \text{ is integral over } \mathbb{Z}. \\ &\Leftrightarrow x \in \mathfrak{O}_L^G. \end{aligned}$$

□

Since the ring A_r is defined as the union over the $A_{r,i}$ it is the ring of integers of the field $\mathbb{Q}(\zeta_{\mathbf{r}r^i} : i \geq 0)$ by Lemma 10.I. The ring $B_{r,i}$ defined in Definition 2 is the ring of integers of the field $\mathbb{Q}(\zeta_{\mathbf{r}r^j} : 0 \leq j \leq i)^{\Delta_r}$ by Lemma 10.II and then B_r is the ring of integers of the field $\bigcup_{i\geq 0} \mathbb{Q}(\zeta_{\mathbf{r}r^j} : 0 \leq j \leq i)^{\Delta_r} = \mathbb{Q}(\zeta_{r^j} : j \geq 0)^{\Delta_r}$ again by Lemma 10.I.

The Galois group of $\mathbb{Q}(\zeta_{\mathbf{r}r^i} : i \geq 0)$ over $\mathbb{Q}$ is isomorphic to the projective limit $\varprojlim_{k\geq 0} \mathrm{Gal}(\mathbb{Q}(\zeta_{\mathbf{r}r^k})/\mathbb{Q})$ by Theorem 28.14 of Stevenhagen's course notes [11].

Definition 11. The ring of *r-adic numbers* is defined as $\varprojlim_{k\geq 0} \mathbb{Z}/r^k\mathbb{Z}$ and denoted as $\mathbb{Z}_r$.

Notation. For $u \in \mathbb{Z}_r^*$, the ring automorphism σ_u denotes the automorphism in $\mathrm{Gal}(\mathbb{Q}(\zeta_{\mathbf{r}r^i} : i \geq 0)/\mathbb{Q})$ that sends $\zeta_{\mathbf{r}r^k}$ to $\zeta_{\mathbf{r}r^k}^{\overline{u}}$ for all $k \geq 0$ and where $\overline{u} = u \pmod{\mathbf{r}r^k}$.

Remark. The limit $\varprojlim_{k\geq 0} (\mathbb{Z}/r^k\mathbb{Z})^*$ is isomorphic to $\mathbb{Z}_r^*$.

Therefore $\mathrm{Gal}(\mathbb{Q}(\zeta_{\mathbf{r}r^i} : i \geq 0)/\mathbb{Q}) \cong \mathbb{Z}_r^*$ and thus for every $u \in \mathbb{Z}_r^*$ there is an unique ring automorphism σ_u of A_r. The Galois group of $\mathbb{Q}(\zeta_{\mathbf{r}r^i} : i \geq 0)$ over $\mathbb{Q}$ acts as an automorphism group on the ring of integers A_r and $\mathbb{Z}$. Recall that Δ_r is defined as the torsion subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_{\mathbf{r}r^i} : i \geq 0)/\mathbb{Q})$.

Lemma 12. *The group Δ_r is cyclic of order $\varphi(\mathbf{r})$.*

For a proof of this lemma see Corollary 4.5.10 of Gouvea [7].

Corollary 13. *The field degree of $\mathbb{Q}(\zeta_{\mathbf{r}r^j} : 0 \leq j \leq i)^{\Delta_r}$ over $\mathbb{Q}$ is r^i.*

3 Galois extensions and ring of integers

In this section let K be a finite Galois extension of $\mathbb{Q}$ with degree n. Also we say that an ideal I of $\mathfrak{O}_K$ divides another ideal J if $J \subset I$

Lemma 14. *Let p be a prime number and P be the set of prime ideals dividing the ideal $p\mathfrak{O}_K$. There are unique integers $e, f, g \geq 1$ such that*

(1) $\#P = g$,

(2) $[\mathfrak{O}_K : \mathbb{Z}/p\mathbb{Z}] = f$ *for all* $\mathfrak{p} \in P$,

(3) $\sup\{i : \mathfrak{p}^i | p\mathfrak{O}_K\} = e$ *for all* $\mathfrak{p} \in P$,

(4) $efg = n$,

(5) $p\mathfrak{O}_K = \prod_{\mathfrak{p}\in P} \mathfrak{p}^e$.

Notation. The number e in the previous Lemma is called the ramification index and the number f is called the residue degree.

Lemma 15. *Let L be a Galois extension of K and let $\mathfrak{q} \subset \mathfrak{O}_L$ be a prime ideal, then there is an unique prime ideal $\mathfrak{p} \subset \mathfrak{O}_K$ s.t. $\mathfrak{p} = \mathfrak{q} \cap \mathfrak{O}_K$.*

Lemma 14 and 15 are well known statements from algebraic number theory and a proof can be found in Chapter 8 of Ash [1] or section 3 of Milne [9].

Definition 16. The *decomposition group* of a prime ideal $\mathfrak{P}$ of $\mathfrak{O}_K$ is the subgroup $D_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) : \sigma(\mathfrak{P}) = \mathfrak{P}\}$ of $\mathrm{Gal}(K/\mathbb{Q})$.

Lemma 17. *For a given ideal $\mathfrak{P}$ of $\mathfrak{O}_K$ such that $p \in \mathfrak{P}$, the number of elements of $D_{\mathfrak{P}}$ is equal to the product of the ramification index e and the residue degree f.*

Proof. The Galois group $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on the prime ideals above p as shown in Theorem 8.1. of [11]. Thus the orbit of $\mathfrak{P}$ contains g elements. Note that $D_{\mathfrak{P}}$ is the stabilizer of the prime ideal $\mathfrak{P}$ and from Lemma 14 and the orbit-stabilizer theorem we find that $D_{\mathfrak{P}} = \frac{[K:\mathbb{Q}]}{g} = fe$. □

An element $\sigma \in D_{\mathfrak{P}}$ naturally induces an element of $\mathrm{Gal}((\mathfrak{O}_K/\mathfrak{P})/\mathbb{F}_p)$, that is the map $x + \mathfrak{P} \mapsto \sigma(x) + \mathfrak{P}$.

Lemma 18. *The natural map $D_{\mathfrak{P}} \to \mathrm{Gal}((\mathfrak{O}_K/\mathfrak{P})/\mathbb{F}_p)$ is surjective.*

For a proof of this lemma see Lemma 8.4. of [11].

Definition 19. The *inertia group* $I_{\mathfrak{P}}$ is the kernel of $D_{\mathfrak{P}} \to \mathrm{Gal}((\mathfrak{O}_K/\mathfrak{P})/\mathbb{F}_p)$.

Thus the induced map $D_{\mathfrak{P}}/I_{\mathfrak{p}} \to \mathrm{Gal}((\mathfrak{O}_K/\mathfrak{P})/\mathbb{F}_p)$ is bijective.

Lemma 20. *The number of elements of $I_{\mathfrak{P}}$ is the ramification index e.*

Proof. The number of elements in $\mathrm{Gal}((\mathfrak{O}_K/\mathfrak{P})/\mathbb{F}_p)$ is f as defined in Lemma 14. Thus because the bijection $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ has f elements, while by Lemma 17 the number of elements of $D_{\mathfrak{P}}$ is fe. Thus $\#I_{\mathfrak{P}} = e$. □

Corollary 21. *If the ramification index is 1, then the number of elements in $I_{\mathfrak{P}}$ is 1, thus $D_{\mathfrak{P}}/I_{\mathfrak{P}} = D_{\mathfrak{P}}$ and therefore $D_{\mathfrak{P}} \to \mathrm{Gal}((\mathfrak{O}_K/\mathfrak{P})/\mathbb{F}_p)$ is bijective.*

In the situation that we can apply this Corollary, we can calculate the residue degree as the order of the decomposition group.

4 Frobenius

Let K be a finite Galois extension of $\mathbb{Q}$ and $k \in \mathbb{Z}_{\geq 0}$ and p a prime number.

Definition 22. For $\mathfrak{P} \subset \mathfrak{O}_K$ a prime ideal of the ring of integers of K such that $p \in \mathfrak{P}$ and the ramification index $e = 1$, a *Frobenius of* $\mathfrak{P}$ is an element $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(K)$ satisfying the following conditions:

(1) $\sigma(\mathfrak{P}) = \mathfrak{P}$

(2) For every $\alpha \in \mathfrak{O}_K$, $\sigma(\alpha) \equiv \alpha^p \pmod{\mathfrak{P}}$.

For a proof of existence see p. 140 of [9]. This map should not be confused with the Frobenius map defined on a finite field.

Notation. For q a power of p, we denote the *Frobenius* $\mathbb{F}_q \to \mathbb{F}_q, x \mapsto x^p$ in $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ as F.

Lemma 23. *The Frobenius defined in Definition 22 is unique and its order is equal to the residue degree f.*

Proof. Let σ be a map satisfying Definition 22 for a prime ideal $\mathfrak{P} \subset \mathfrak{O}_K$ with ramification index 1. Then σ is an element of $D_{\mathfrak{P}}$. Since by assumption the ramification index is 1, we can apply Corollary 21 and thus $\phi : D_{\mathfrak{P}} \to \mathrm{Gal}((\mathfrak{O}_K/\mathfrak{P})/\mathbb{F}_p)$ is an isomorphism. Under that isomorphism ϕ the map σ is sent to the map $x + \mathfrak{P} \mapsto \sigma(x) + \mathfrak{P}$. By the second condition in Definition 22 this is the map F. Thus $\phi(\sigma) = F$ and thus Frobenius of $\mathfrak{P}$ is unique.

Because F is a generator of $\mathrm{Gal}((\mathfrak{O}_K/\mathfrak{P})/\mathbb{F}_p)$, it has order f. By the isomorphism ϕ the Frobenius of $\mathfrak{P}$ will then also have order f. □

Notation. We denote the Frobenius of a prime ideal $\mathfrak{P}$ as $\mathrm{Frob}_{\mathfrak{P}}$.

Let p, r be distinct prime numbers and let $\mathfrak{p}$ be a prime ideal of $B_{r,k}$ such that $p \in \mathfrak{p}$. For the remainder of the thesis we will use these notations. In order to define a Frobenius of $\mathfrak{p}$ we need to determine the ramification index of $B_{r,k}$.

Lemma 24. *The ramification index over $\mathbb{Q}$ of a prime ideal containing p in $A_{r,i}$ and $B_{r,i}$ is 1 for all $i \geq 0$.*

Proof. In the case of $A_{r,i}$ see Proposition 6.2 (d) of Milne [9]. In the case of $B_{r,i}$, let $i \in \mathbb{Z}_{>0}$ and assume there is a prime ideal $\mathfrak{P}$ in $B_{r,i}$ dividing (p) with ramification index $e > 1$. Let $\mathfrak{Q} \subset A_{r,i}$ a prime ideal dividing $\mathfrak{P}$. Thus $\mathfrak{P}^e|(p)$ and $\mathfrak{Q}|\mathfrak{P}$ and thus $\mathfrak{Q}^e|(p)$. This contradicts our first result and thus every ideal of $B_{r,k}$ containing p has ramification index 1. □

Lemma 25. *Let $\mathfrak{q}$ be a prime ideal of $A_{r,k}$ such that $p \in \mathfrak{q}$. The map* $\mathrm{Frob}_{\mathfrak{q}}$ *is the image of $p \in (\mathbb{Z}/\mathbf{r}r^k/Z)^*$ by the isomorphism of Lemma 8.*

Proof. The image of p is the map σ defined by $\sigma(\zeta_{\mathbf{r}r^k}) = \zeta^p_{\mathbf{r}r^k}$. Let $a \in A_{r,k}$, then there are $a_1, a_2, ..., a_t \in \mathbb{Z}$ such that $a = \sum_{i=1}^t a_i \zeta^i_{\mathbf{r}r^k}$. Now observe that $\sigma(a) = \sum_{i=1}^t a_i \zeta^{pi}_{\mathbf{r}r^k} \equiv a^p \pmod{p}$. Since $p \in \mathfrak{q}$, we have $pA_{r,k} \subset \mathfrak{q}$ and thus $\sigma(a) \equiv a^p \pmod{\mathfrak{q}}$. Now assume that $a \in \mathfrak{q}$, then $\sigma(a) \equiv a^p \equiv 0 \pmod{\mathfrak{q}}$ and thus $\sigma(a) \in \mathfrak{q}$. Now both statements of Definition 22 are satisfied and thus the map $\mathrm{Frob}_{\mathfrak{q}}$ is σ.

□

This lemma, the functoriality of the Frobenius element [3] and Lemma 24 give us that for a prime ideal $\mathfrak{p} \subset \mathfrak{q}$ of $B_{r,k}$ the $\mathrm{Frob}_{\mathfrak{p}}$ corresponds to $p \in (\mathbb{Z}/\mathbf{r}r^k\mathbb{Z})^*/\Delta_r$.

5 Computing the residue degree of $B_{r,k}$

Using Lemma 23 we can compute the degree f of the residue field with the order of $\mathrm{Frob}_{\mathfrak{p}}$ in $\mathrm{Gal}(\mathbb{Q}(\zeta_{r^j} : k > j \geq 0)^{\Delta_r}/\mathbb{Q})$, which we found to be equal to the order of p in $(\mathbb{Z}/\mathbf{r}r^k\mathbb{Z})^*/\Delta_r$. To compute the latter we have the following theorem.

Theorem 26. *For* $l := \mathrm{ord}_r\left(\frac{p^{\varphi(\mathbf{r})}-1}{\mathbf{r}/r}\right)$*, the order of* $\overline{p}$ *in* $(\mathbb{Z}/r^n\mathbb{Z})^*/\Delta_r$ *is* 1 *for* $\gcd(r,2) \leq n \leq l$ *and it is* r^{n-l} *for* $n \geq l$*.*

Before we prove this theorem we will first consider two lemmas.

Lemma 27. *For* $n \geq \gcd(r,2)$ *the map* $\psi : (\mathbb{Z}/r^n\mathbb{Z})^* \to (\mathbb{Z}/\mathbf{r}r^{n-1}\mathbb{Z})^*$ *defined for every* $a \in \mathbb{Z}$ *by* $a + r^n\mathbb{Z} \mapsto a^{\varphi(\mathbf{r})} + \mathbf{r}r^{n-1}\mathbb{Z}$ *is a well-defined homomorphism with kernel* Δ_r*.*

Proof. First let $r = 2$ and thus $\mathbf{r} = 4$ and $n \geq 2$ and thus we have $\psi : (\mathbb{Z}/2^n\mathbb{Z})^* \to (\mathbb{Z}/2^{n+1}\mathbb{Z})^*, a + 2^n\mathbb{Z} \mapsto a^2 + 2^{n+1}\mathbb{Z}$. First we will show that ψ is well-defined. Let $a, b \in \mathbb{Z}$ such that $a + 2^n\mathbb{Z} = b + 2^n\mathbb{Z}$, in other words there is an $c \in \mathbb{Z}$ such that $a = b + c \cdot 2^n$. Then we have

$$\begin{aligned}\psi(a + 2^n\mathbb{Z}) &= a^2 + 2^{n+1}a\mathbb{Z} + 2^{2n}\mathbb{Z} = a^2 + 2^{n+1}\mathbb{Z} \\ &= (b + c \cdot 2^n)^2 + 2^{n+1}\mathbb{Z} \\ &= b^2 + c \cdot 2^{n+1} + c \cdot 2^{2n} + 2^{n+1}\mathbb{Z} \\ &= b^2 + 2^{n+1}\mathbb{Z} = \psi(b + 2^n\mathbb{Z})\end{aligned}$$

and this shows that ψ is well-defined.

Secondly we will show that ψ is a homomorphism. Clearly $\psi(1) = 1$. Also for $a, b \in \mathbb{Z}$ we have

$$\psi(ab + 2^n\mathbb{Z}) = (ab + 2^n\mathbb{Z})^2 = (ab)^2 + 2^{n+1}ab\mathbb{Z} + 2^{2n}\mathbb{Z} = (ab)^2 + 2^{n+1}\mathbb{Z},$$

on the other hand we have

$$\begin{aligned}\psi(a + 2^n\mathbb{Z})\psi(b + 2^n\mathbb{Z}) &= (a + 2^n\mathbb{Z})^2(b + 2^n\mathbb{Z})^2 \\ &= a^2b^2 + (a^2b_2 + ab^2)2^{n+1}\mathbb{Z} + 2^{2n}\mathbb{Z} \\ &= (ab)^2 2^{n+1}\mathbb{Z}.\end{aligned}$$

Thus $\psi(a + 2^n\mathbb{Z})\psi(b + 2^n\mathbb{Z}) = (ab)^2 + 2^{n+1}\mathbb{Z} = \psi(ab + 2^n\mathbb{Z})$ and thus ψ is a homomorphism in the case $r = 2$.

Thirdly the kernel of ψ for $r = 2$ consists of the elements $a + 2^n\mathbb{Z}$ where $a \in \mathbb{Z}$ such that $a^2 \equiv 1 \pmod{2^{n+1}}$. Then also $a^2 \equiv 1 \pmod{2^n}$ and since $(\mathbb{Z}/2^n\mathbb{Z})^* \cong C_2 \times C_{2^{n-2}}$ as mentioned after Lemma 8, we know that the set that consists of all elements with an order in $(\mathbb{Z}/2^n\mathbb{Z})^*$ that divides 2 for $n = 2$ is $\{\pm 1\} \subset (\mathbb{Z}/2^n\mathbb{Z})^*$, and for $n > 2$ is $\{\pm 1, 2^{n-1} \pm 1\} \subset (\mathbb{Z}/2^n\mathbb{Z})^*$. But for the elements $2^{n-1} \pm 1$ we have $(2^{n-1} \pm 1)^2 \equiv 1 \pm 2^n \pmod{2^{n+1}} \not\equiv 1 \pmod{2^{n+1}}$. Thus the kernel is $\Delta_r \cong \langle -1 \rangle \subset (\mathbb{Z}/2^n\mathbb{Z})^*$

Now let r an odd prime number and $n \geq 1$. The map $\psi : (\mathbb{Z}/r^n\mathbb{Z})^* \to (\mathbb{Z}/r^n\mathbb{Z})^*, a \bmod r^n \mapsto a^{\varphi(\mathbf{r})} \bmod r^n$ clearly is an endomorphism. The kernel consists of the elements a such that $\mathrm{ord}(a) | r - 1$. As mentioned before $(\mathbb{Z}/r^n\mathbb{Z})^* \cong C_{\varphi(r)r^{n-1}}$, of which the subgroup Δ_r consist of all elements of order dividing $r - 1$, since Δ_r has order $r - 1$ as stated in Lemma 12. □

Corollary 28. *The induced homomorphism* $\overline{\psi} : (\mathbb{Z}/r^n\mathbb{Z})^*/\Delta_r \to (\mathbb{Z}/\mathbf{r}r^{n-1}\mathbb{Z})^*$ *is injective. Thus for an* $a \in \mathbb{Z}\setminus r\mathbb{Z}$*, the order in* $(\mathbb{Z}/r^n\mathbb{Z})^*/\Delta_r$ *of* $(a+r^n\mathbb{Z})$ mod Δ_r *is equal to the order in* $(\mathbb{Z}/\mathbf{r}r^{n-1}\mathbb{Z})^*$ *of* $a^{\varphi(\mathbf{r})} + \mathbf{r}r^{n-1}\mathbb{Z}$*.*

Lemma 29. *Let* $a \in \mathbb{Z}$ *such that* $a \equiv 1 \bmod \mathbf{r}$*,* $n \geq 0$ *and let* $l' := \mathrm{ord}_r(a-1)$*. The order of* $a \pmod{r^n}$ *in* $(\mathbb{Z}/r^n\mathbb{Z})^*$ *is* 1 *for* $n \leq l'$ *and* $r^{n-l'}$ *for* $n \geq l'$*.*

Proof. First we will address the case $n \leq l'$. By definition l' is the greatest power of r that divides $a-1$. Thus the order of $a \pmod{r^n}$ in $(\mathbb{Z}/r^n\mathbb{Z})^*$ is 1 for $n \leq l'$.

Let $n > l'$ and $m \geq 0$. Now let $a_m = a^{r^m}$ and $l_m = \mathrm{ord}_r(a_m - 1)$. Putting $x = a_m - 1$ for a given m we find that by the binomium theorem that

$$\begin{aligned}(1+x)^r &\equiv 1 + rx \pmod{rx^2, x^r} \\ &\equiv 1 + rx \pmod{r^{\min(2l_m+1, rl_m)}}.\end{aligned}$$

Note that for $r = 2$ we have $l' \geq 2$ and for r an odd prime integer we have $l' \geq 1$. Now for $m = 0$ we have $\mathrm{ord}_r(rx) = l_m + 1 < \min(2l_m+1, rl_m)$ and thus we find that $\mathrm{ord}_r(a_0^r - 1) = \mathrm{ord}_r(rx) = l_0 + 1$. Moreover, we have $l_1 = l_0 + 1$ and thus for $m = 1$ we also have $\mathrm{ord}_r(rx) = l_m + 1 < \min(2l_m+1, rl_m)$ and thus $\mathrm{ord}_r(a_m^r - 1) = \mathrm{ord}_r(rx) = l_m + 1$. Now iteratively we find that $l_m = l_0 + m$ and that $l' + m + 1 = \mathrm{ord}_r(a_m^r - 1) = \mathrm{ord}(a^{r^{m+1}})$ for $m > 0$. Thus $r^n | (a^{n-l'} - 1)$ and $r^n \not| (a^{n-l'-1} - 1)$, so the order of $a \pmod{r^n}$ in $(\mathbb{Z}/r^n\mathbb{Z})^*$ is $r^{n-l'}$ □

Proof. (Theorem 26). Notice for r an odd prime number that Fermat's little theorem states that for $a \in \mathbb{Z} \setminus r\mathbb{Z}$ we have $a^{r-1} \equiv 1 \pmod{r}$. For $r = 2$ with $a \in \mathbb{Z}\setminus r\mathbb{Z}$ we have that $a^2 \equiv 1 \bmod 8$, since $(1+2b)^2 = 1+4b+4b^2 = 1+8b(b+1)$ for $b \in \mathbb{Z}$. Thus we can apply Lemma 29 to Corollary 28 for an element $a \in \mathbb{Z} \setminus r\mathbb{Z}$. Let $l' := \mathrm{ord}_r(a^{\varphi(\mathbf{r})} - 1)$, then

$$\mathrm{ord}_{(\mathbb{Z}/r^n\mathbb{Z})^*/\Delta_r}(a + r^n\mathbb{Z} \bmod \Delta_r) = \begin{cases} 1 & \text{if } n + \gcd(2,r) - 1 \leq l', \\ r^{n+\gcd(2,r)-1-l'} & \text{if } n + \gcd(2,r) - 1 \geq l'. \end{cases}$$

To simplify we use $l := \mathrm{ord}_r\left(\frac{p^{\varphi\mathbf{r}}-1}{\mathbf{r}/r}\right)$ instead of l':

$$\mathrm{ord}_{(\mathbb{Z}/r^n\mathbb{Z})^*/\Delta_r}(a + r^n\mathbb{Z} \bmod \Delta_r) = \begin{cases} 1 & \text{if } n \leq l, \\ r^{n-l} & \text{if } n \geq l. \end{cases}$$

□

Corollary 30. *The residue degree* f *of* $B_{r,k}$ *is 1 for* $k \leq l$ *and is* r^{k-l} *for* $k \geq l$*.*

6 Prime ideals of B_r

In the last section we determined the residue degree for the rings $B_{r,k}$. In this section we will determine the number of prime ideals of their union B_r. Recall that we defined $l := \mathrm{ord}_r\left(\frac{p^{\varphi \mathbf{r}}-1}{\mathbf{r}/r}\right)$

Lemma 31. *For $k \geq l$ the number of prime ideals g of $B_{r,k}$ is equal to the number of prime ideals of $B_{r,l}$.*

Proof. In the previous section we determined the residue degree of $B_{r,k}$, while in Lemma 24 we determined the ramification index and Corollary 13 gives us the field degree. Now we can calculate with lemma 14 the number of prime ideals g as $\frac{n}{ef} = \frac{r^k}{1 \cdot r^{k-l}}$, which is equal to the number of prime ideals of $B_{r,l}$. □

Corollary 32. *For every prime ideal $\mathfrak{p}_l \subset B_{r,l}$ and every $k \geq l$ the ideal $\mathfrak{p}_l B_{r,k}$ is a prime ideal.*

Proof. Lemma 15 gives us that for every prime ideal $\mathfrak{q} \subset B_{r,k}$ there is a unique prime ideal of $\mathfrak{p} \subset B_{r,l}$ such that $\mathfrak{p} = \mathfrak{q} \cap B_{r,l}$. Note that $\mathfrak{q}$ divides $\mathfrak{p}B_{r,l}$ and Lemma 31 gives that the number of prime ideals of $B_{r,k}$ is equal to $B_{r,l}$, thus $\mathfrak{q} = \mathfrak{p}B_{r,l}$. □

Lemma 33. *For every prime ideal $\mathfrak{p} \subset B_{r,l}$ the ideal $\mathfrak{p}B_R = \bigcup_{i=l}^{\infty} \mathfrak{p}B_{r,i}$ is a prime ideal of B_r.*

Proof. Let $a, b \in B_r$ and $ab \in \mathfrak{p}B_r$. There is a $k > l$ such that $ab \in \mathfrak{p}B_{r,k}$ and also there is a $k' > k$ such that $a, b \in B_{r,k'}$. Since $\mathfrak{p}B_{r,k} \subset \mathfrak{p}B_{r,k'}$ we have that $ab \in \mathfrak{p}B_{r,k'}$ and since it is prime either $a \in \mathfrak{p}B_{r,k'}$ or $b \in \mathfrak{p}B_{r,k'}$. Thus either $a \in \mathfrak{p}B_r$ or $b \in \mathfrak{p}B_r$, making $\mathfrak{p}B_r$ a prime ideal. □

In the introduction we denoted $S_{p,r}$ as the set of prime ideals of B_r containing p and it now follows that $S_{p,r}$ has at least as many prime ideals containing p as $B_{p,l}$.

Lemma 34. *For $\mathfrak{p}$ a prime ideal of $B_{r,l}$ the quotient $B_r/\mathfrak{p}B_r$ is a field.*

Proof. We know that $B_{r,k}/\mathfrak{p}B_{r,k}$ is a finite field. Because of the primality of $\mathfrak{p}B_r$ the ring $B_r/\mathfrak{p}B_r$ is an integral domain, which implies that $B_r/\mathfrak{p}B_r$ is a commutative ring. Now we only have to find an inverse for elements of $B_r/\mathfrak{p}B_r$. Let $a \in B_r$, then there is an positive integer k such that $a \in B_{r,k}$. There is an element $b \in B_{r,k}$, such that $ab \equiv 1 \pmod{\mathfrak{p}B_{r,k}}$. Then b is also in B_r and since $\mathfrak{p}B_{r,k} \subset \mathfrak{p}B_r$ also $ab \equiv 1 \pm od\mathfrak{p}B_r$. Therefore $\overline{b}$ is the inverse of $\overline{a}$ in $B_r/\mathfrak{p}B_r$. □

Theorem 3. *The cardinality of $S_{p,r}$ is r^l and for every prime ideal $\mathfrak{P} \in S_{p,r}$ there is a unique prime ideal $\mathfrak{p}$ of $B_{r,l}$ such that $\mathfrak{P} = \mathfrak{p} \cdot B_{r,l}$.*

Proof. Let $\mathfrak{q} \in S_{p,r}$, then by Lemma 15 there is a unique prime ideal $\mathfrak{p}$ of $B_{r,l}$ such that $\mathfrak{p} = \mathfrak{q} \cap B_{r,l}$. Likewise for $k \geq l$ we find $\mathfrak{p}B_{r,k} = \mathfrak{q} \cap B_{r,k}$, since by Lemma 31 the primes of $B_{r,k}$ and $B_{r,l}$ correspond. It follows that $\bigcup_{i=l}^{\infty} \mathfrak{p}B_{r,i} \subset \mathfrak{q}$, and then by Lemma 34 it follows that $\mathfrak{p}B_r = \mathfrak{q}$. □

7 Finding bases

In the previous section we found that there are r^l distinct prime ideals of B_r that contain p and in this section we will make a choice among these prime ideals.

In the quotient $B_r/\mathfrak{p}$, where $\mathfrak{p} \in S_{p,r}$, the elements of $B_{r,l}$ are mapped under the quotient map to an element in $\mathbb{F}_p$. To know where elements of $B_{r,k}$ are mapped to under the quotient map, we will have to look at the ring generators of $B_{r,k+1}$ over $B_{r,k}$. The bases of the rings $A_{r,k}$ and $A_{r,k+1}$ will help use find the generators of $B_{r,k}$. A visual representation is given in Figure 1 which shows the steps we make towards finding the ring generators of $B_{r,k+1}$.

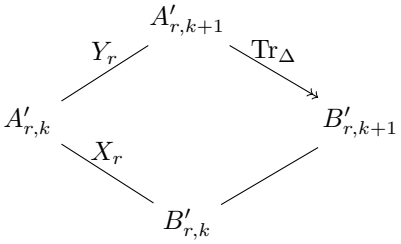

Figure 1: bases

Before we look at any basis, we will need to add $\frac{1}{r}$ to our rings to avoid some problems with the traces for $r = 2$. The localization should also make our lives easier for any prime r, when we want to find a basis for $A_{r,k}[\frac{1}{r}]$ as a module over $B_{r,k}[\frac{1}{r}]$.

Notation. We will denote the ring $B_{r,k}[\frac{1}{r}]$, $B_r[\frac{1}{r}]$, $A_{r,k}[\frac{1}{r}]$ and $A_r[\frac{1}{r}]$ as respectively $B'_{r,k}$, B'_r, $A'_{r,k}$ and A'_r.

Notation. We will write the set of the first n natural numbers $\{0, 1, 2, ..., n-1\}$ as $\mathbb{N}_n$.

Consider the sets X_r which we define for $r = 2$ as the set $\{1, \zeta_4\}$ and for r equal to an odd prime number as the set $\{\zeta_r^i : i \in (\mathbb{Z}/r\mathbb{Z})^*\}$.

Lemma 35. *The set X_r is a basis for $A'_{r,i}$ as a module over $B'_{r,i}$ for all $i \geq 0$.*

Proof. The set X_r is a basis for $A_{r,0} = \mathbb{Z}[\zeta_{\mathbf{r}}]$ over $\mathbb{Z}$ thus also for $A'_{r,i}$ over $B'_{r,i}$ with $i = 0$. Proposition 6.2(d) from [9] for ζ_r implies that the discriminant of $A_{r,0}$ over $\mathbb{Z}$ is a power of r. Thus the greatest common divisor of this discriminant and of the discriminant of $B_{r,i}$ over $\mathbb{Z}$ is thus also a r power. Now we observe $B_{r,i}$ and $A_{r,i}$ for $i > 0$, we know that $B_{r,i} \cdot A_{r,0} \subset A_{r,i}$ and thus $B'_{r,i} \cdot A'_{r,0} \subset A'_{r,i}$.

Lemma 8 and Corollary 13 tell us that the fields $\mathbb{Q}[\zeta_{\mathbf{r}}]$, $\mathbb{Q}[\zeta_{\mathbf{r}r^i}]^{\Delta_r}$ and $\mathbb{Q}[\zeta_{\mathbf{r}r^i}]$ have respectively degree $\varphi(\mathbf{r}), r^i$ and $\varphi(\mathbf{r})r^i$ over $\mathbb{Q}$ and therefore we can apply Lemma 6.5 from [9]. Applying our knowledge about the discriminant we see that for some $N \in \mathbb{Z}_{>0}$ the relation $A_{r,i} \subset \frac{1}{r^N} A_{r,0} \cdot B_{r,i}$ holds. Since $\frac{1}{r^N} \in \mathbb{Z}'$ it follows that the relation $A'_{r,0} \cdot B'_{r,i} = \frac{1}{r^N} A'_{r,0} \cdot B'_{r,i}$ holds and thus $A'_{r,i} \subset A'_{r,0} \cdot B'_{r,i}$. Thus we find that $A'_{r,i} = A'_{r,0} \cdot B'_{r,i}$ and thus the set X_r is also a basis for $A'_{r,i}$ over $B'_{r,i}$ □

Remark. The set $\{1, \zeta_4\}$ is not a basis for $\mathbb{Z}[\zeta_8] = A_{2,1}$ over $\mathbb{Z}[\sqrt{2}] = B_{2,1}$, since $\zeta_8 = \frac{\sqrt{2}(1+\zeta_4)}{2}$.

Lemma 36. *The trace Tr_{Δ_r} from $A'_{r,i}$ to $B'_{r,i}$ is surjective for all $i \geq 0$.*

Proof. From Lemma 12 it follows that $\#\Delta_r = \varphi(\mathbf{r})$ and thus $\mathrm{Tr}_{\Delta_r}(B_{r,i}) = \varphi(\mathbf{r}) \cdot B_{r,i}$. Now for $r = 2$ we find that $\mathrm{Tr}_{\Delta_r}(B'_{r,i}) = B'_{r,i}$ and thus the trace Tr_{Δ_2} from $A'_{2,i}$ to $B'_{2,i}$ is surjective. Now for r an odd prime number, notice that $\zeta_r \in A_{r,i}$ and that $\mathrm{Tr}_{\Delta_r}(\zeta_r) = \zeta_r + \zeta_r^2 + ... + \zeta_r^{r-1} = -1$. The image $\mathrm{Tr}_{\Delta_r}(A_{r,i})$ is an ideal in $B_{r,i}$ and since $-1 \in \mathrm{Tr}_{\Delta_r}(A_{r,i})$ it follows that $\mathrm{Tr}_{\Delta_r}(A_{r,i}) = B_{r,i}$. □

Lemma 37. *For odd prime numbers r the natural map $\Delta_r \hookrightarrow (\mathbb{Z}/r\mathbb{Z})^*$ is injective.*

Proof. Let $\alpha \in \Delta_r$ such that $\alpha \neq 1$ and notice that $\alpha^{r-1} = 1$, since by Lemma 12 we have $\#\Delta_r = r - 1$. Note that the zeros in $\mathbb{Z}_r$ of the polynomial $X^{r-1} - 1$ are precisely the elements of Δ_r. Note that $(X - \alpha)(X - 1)|X^{r-1} - 1$ and we have the natural map $q : \mathbb{Z}_r \to \mathbb{Z}/r\mathbb{Z}$ such that for $(a_i)_{i\geq 0} \in \mathbb{Z}_r$ we have $q((a_i)_{i\geq 0}) = a_1$. Note that if $q(\alpha) = 1$, then $(X - q(\alpha))(X - 1) = (X - 1)^2$ and then $X^{r-1} - 1$ would be inseparable in $\mathbb{F}_r[X]$. We know that $X^{r-1} - 1$ is separable in $\mathbb{F}_r[X]$, so we have a contradiction and thus $q(\alpha) \neq 1$. □

Let $Y_{r,k}$ for $r = 2$ be the set $\{1, \zeta_{\mathbf{r}r^{k+1}}\}$ and for $r \neq 2$ be the set $\{\zeta^{\delta}_{\mathbf{r}r^{k+1}} : \delta \in \Delta_r\} \cup \{1\}$.

Lemma 38. *The set $Y_{r,k}$ forms a basis for $A'_{r,k+1}$ as an $A'_{r,k}$-module for $k \geq 0$.*

Proof. The set $\{1, \zeta_{\mathbf{r}r^i}, \zeta^2_{\mathbf{r}r^i}, ..., \zeta^{\varphi(\mathbf{r}r^i)-1}_{\mathbf{r}r^i}\}$ is a module basis for $A_{r,i}$ over $\mathbb{Z}$ for all $i \geq 0$, as also shown in Theorem 6.4 of [9]. Let $a \in A_{r,k+1}$, then there are $z_i \in \mathbb{Z}$ such that $a = \sum_{i\in\mathbb{N}_{\varphi(\mathbf{r}r^{k+1})}} z_i\zeta^i_{\mathbf{r}r^{k+1}}$. Now let $y_n := \sum_{j\in\mathbb{N}_{\varphi(\mathbf{r}r^k)}} z_{n+jr}\cdot\zeta^j_{\mathbf{r}r^k}$. Then the element a can be written as $\sum_{i\in\mathbb{N}_r} y_i\zeta^i_{\mathbf{r}r^{k+1}}$. Thus for $k \geq 0$ the set $\{\zeta^i_{\mathbf{r}r^{k+1}} : i \in \mathbb{N}_r\}$ is a module basis for $A_{r,k+1}$ over $A_{r,k}$. Now for $r = 2$ the lemma holds. Now assume $r \neq 2$ such that we can apply Lemma 37. Lemma 37 tells us that for every element y of $Y_{r,k}$ there precisely is one element ζ of $\{\zeta^i_{\mathbf{r}r^{k+1}} : i \in \mathbb{N}_r\}$ such that $\zeta = \zeta^u_{\mathbf{r}r^k} y$ for $u \in \mathbb{Z}$. Thus the lemma holds also for $r \neq 2$. □

Lemma 39. *Let $\epsilon, \delta \in \Delta_r$. The element $\mathrm{Tr}_{\Delta_r}(\sigma_\delta(\zeta_r)\sigma_\epsilon(\zeta_{\mathbf{r}r^k}))$ is equal to the element $\mathrm{Tr}_{\Delta_r}(\zeta_{\mathbf{r}r^k}\sigma_{\epsilon^{-1}\delta}(\zeta_{\mathbf{r}}))$.*

Proof. The trace of $\sigma_\delta(\zeta_r)\sigma_\epsilon(\zeta_{\mathbf{r}r^k})$ can be written as the sum of conjugates. Some manipulations with automorphisms give the identities below.

$$\begin{aligned}
\mathrm{Tr}_{\Delta_r}(\sigma_\delta(\zeta_r)\sigma_\epsilon(\zeta_{\mathbf{r}r^k})) &= \sum_{u\in\Delta_r} \sigma_u(\sigma_\delta(\zeta_r)\sigma_\epsilon(\zeta_{\mathbf{r}r^k})) \\
&= \sum_{u\in\Delta_r} \sigma_u(\sigma_\delta(\zeta_r))\sigma_u(\sigma_\epsilon(\zeta_{\mathbf{r}r^k})) \\
&= \sum_{u\in\Delta_r} \sigma_{u\delta}(\zeta_r)\sigma_{u\epsilon}(\zeta_{\mathbf{r}r^k})
\end{aligned}$$

Further notice that Δ_r is a multiplicative group. Thus multiplying with an element is an automorphism of Δ_r. Thus we can continue with our manipulations

using $v = \epsilon u$.

$$\sum_{u\in\Delta_r} \sigma_{u\delta}(\zeta_r)\sigma_{u\epsilon}(\zeta_{\mathbf{r}r^k}) = \sum_{v\in\Delta_r} \sigma_{v\epsilon^{-1}\delta}(\zeta_{\mathbf{r}})\sigma_v(\zeta_{\mathbf{r}r^k}) = \mathrm{Tr}_{\Delta_r}(\sigma_{\epsilon^{-1}\delta}(\zeta_r)\zeta_{\mathbf{r}r^k})$$

□

Now we will recall a definition from the introduction, which are the elements in the form of the previous lemma, since $\zeta_r = \zeta_{\mathbf{r}r^k}^{\mathbf{r}r^{k-1}}$.

Definition 4. Define the elements $\eta_{r,k,i}$ as $\mathrm{Tr}_{\Delta_r}(\zeta_{\mathbf{r}r^k}^{1+i\mathbf{r}r^{k-1}})$.

Lemma 40. *The ring $B'_{r,k+1}$ is generated as a module over $B'_{r,k}$ by the set $\{\eta_{r,k+1,i+1} : i \in \mathbb{N}_{r-1}\} \cup \{1\}$.*

Proof. For r an odd prime number Lemma 38 gives a module basis for $A'_{r,k+1}$ over $A'_{r,k}$, such that for $\overline{\delta} = \delta \pmod{\mathbf{r}r^k}$ we have the relation

$$A'_{r,k+1} = \bigoplus_{\delta\in\Delta_r} \left(\zeta_{\mathbf{r}r^{k+1}}^{\overline{\delta}} A'_{r,k}\right) \oplus A'_{r,k}.$$

Lemma 35 gives in the same case a module basis for $A'_{r,k}$ over $B'_{r,k}$ such that for $\overline{\epsilon} = \epsilon \pmod{\mathbf{r}r^k}$ we have

$$A'_{r,k+1} = \bigoplus_{\delta\in\Delta_r,\epsilon\in\Delta_r} \left(\zeta_{\mathbf{r}r^{k+1}}^{\overline{\epsilon}}\zeta_{\mathbf{r}}^{\overline{\delta}} B'_{r,k}\right) \oplus A'_{r,k}.$$

For $r = 2$ Lemma 38 gives a module basis for $A'_{r,k+1}$ over $A'_{r,k}$, and we have the relation

$$A'_{r,k+1} = A'_{r,k} \oplus \zeta_{\mathbf{r}r^{k+1}} A'_{r,k}.$$

Furthermore we find a module basis for $A'_{r,k}$ over $B'_{r,k}$ from Lemma 35 such that

$$A'_{r,k+1} = (B'_{r,k} \oplus \zeta_4 B'_{r,k}) \oplus (\zeta_{\mathbf{r}r^{k+1}} B'_{r,k} \oplus \zeta_{\mathbf{r}r^{k+1}}\zeta_4 B'_{r,k}).$$

For r equal to an odd prime number we define the sets E, D as Δ_r and for $r = 2$ we will define E, D as $\{0, 1\}$.

There are elements $b_{\delta,\epsilon} \in B'_{r,k}$ and $a^\dagger \in A'_{r,k}$ such that an element $a \in A'_{r,k+1}$ can be writen as:

$$a = a^\dagger + \sum_{\delta\in D,\epsilon\in E} b_{\delta,\epsilon}\zeta_{\mathbf{r}r^{k+1}}^{\overline{\epsilon}}\zeta_{\mathbf{r}}^{\overline{\delta}}.$$

Lemma 36 states that for $b \in B'_{r,k+1}$ there is an $a_b \in A'_{r,k+1}$ such that $b = \mathrm{Tr}_{\Delta_r}(a_b)$. Thus there are $c_{\delta,\epsilon} \in B'_{r,k}, a_b^\dagger \in A'_{r,k}$ such that

$$b = \mathrm{Tr}_{\Delta_r}(a_b^\dagger + \sum_{\delta\in D,\epsilon\in E} c_{\delta,\epsilon}\zeta_{\mathbf{r}r^{k+1}}^{\overline{\epsilon}}\zeta_{\mathbf{r}}^{\overline{\delta}}).$$

From Lemma 39 and the linearity of the trace over $B'_{r,k+1}$ we find that

$$b = \mathrm{Tr}_{\Delta_r}(a_b^\dagger) + \sum_{\delta\in D,\epsilon\in E} c_{\delta,\epsilon}\,\mathrm{Tr}_{\Delta_r}(\zeta_{\mathbf{r}r^{k+1}}\zeta_{\mathbf{r}}^{\overline{\epsilon^{-1}}\cdot\overline{\delta}}).$$

Note that $\epsilon^{-1}\Delta_r = \Delta_r$ for all $\epsilon \in \Delta_r$. Thus for each $\delta' \in \Delta_r$ we can define $d_{\delta'} := \sum_{\delta,\epsilon\in\Delta_r:\epsilon^{-1}\delta=\delta'} b_{\delta,\epsilon}$ such that we have

$$b = \mathrm{Tr}_{\Delta_r}(a^\dagger) + \sum_{\delta'\in\Delta_r} d_{\delta'}\eta_{r,k+1,\overline{\delta'}}.$$

The element $\mathrm{Tr}_{\Delta_r}(a^\dagger)$ is an element of $B'_{r,k}$ since $a^\dagger \in A_{r,k}$ and for all $\delta' \in \Delta_r$ is $d_{\delta'}$ an element of $B'_{r,k}$, because it is the sums of elements of $B'_{r,k}$. Thus every element of $B'_{r,k+1}$can be written as the sum of products of an element of $\{\eta_{r,k+1,i+1} : i \in \mathbb{N}_{r-1}\} \cup \{1\}$ times an element of $B'_{r,k}$. □

8 The Standard Construction

Corollary 30 gives that $B'_{r,l}$ is mapped into $\mathbb{F}_p$ by the natural quotient map of a prime ideal from $S_{p,r}$. Theorem 3 tells us that given generators for an ideal of $B_{r,l}$ we have generators for an ideal in $S_{p,r}$. Using a relation between the ideals containing p of $B'_{r,l}$ and $B_{r,l}$ we can use the ring generators of $B'_{r,l}$ over $\mathbb{Z}$ to order $S_{p,r}$. We will use use the smallest prime ideal in terms of this ordering to define our standard field of characteristic p and degree r^l.

Theorem 5. *For $\mathfrak{P} \in S_{p,r}$ there is a unique system $(a_{\mathfrak{P},j})_{0\leq j<lr}$ of integers $a_{\mathfrak{P},j} \in \mathbb{N}_p$ such that $\mathfrak{P}$ is generated as a module over B_r by p and $\{\eta_{r,j+1,i} - a_{\mathfrak{P},i+jr} : j \in \mathbb{N}_l, i \in \mathbb{N}_r\}$.*

Proof. First we will find a set of ring generators for $B'_{r,l}$ over $\mathbb{Z}$. Lemma 40 tells us that the set $\{\eta_{r,j+1,i} : i \in \mathbb{N}_{r-1}\}\cup\{1\}$ generates $B'_{r,j+1}$ as a module over $B'_{r,j}$. If we take the union of these sets for $j < l$, then $\{\eta_{r,j+1,i} : i \in \mathbb{N}_l, j \in \mathbb{N}_{r-1}\}\cup\{1\}$ we find a set of ring generators for $B'_{r,l}$ over $B'_{r,0} = \mathbb{Z}$.

Given a prime ideal $\mathfrak{p}$ of $B_{r,l}$ such that $p \in \mathfrak{p}$, then by Lemma 7.6 of [2] the localization of the quotient $(B_{r,k}/\mathfrak{p})[\frac{1}{r}]$ is canonically isomorphic to the quotient $B'_{r,k}/\mathfrak{p}B'_{r,k}$. Note that $\gcd(p, r) = 1$ and thus $(B_{r,k}/\mathfrak{p})[\frac{1}{r}] = (B_{r,k}/\mathfrak{p})$ and Corollary 30 gives then that $B'_{r,k}/\mathfrak{p}B'_{r,k} \cong \mathbb{Z}/p\mathbb{Z}$. Note that a ring generator of $B'_{r,k}$ is sent to an $a \in \mathbb{Z}/p\mathbb{Z}$ by the quotient map of $\mathfrak{p}B'_{r,k}$. Thus for $j \in \mathbb{N}_{lr}$ we can define $a_{\mathfrak{p}B_r,j}$ as the element in $\mathbb{N}_p$ such that for $j \in \mathbb{N}_l$ and $i \in \mathbb{N}_r$ we have $\eta_{r,j+1,i} - a_{\mathfrak{p}B_r,i+jr} \equiv 0 \pmod{\mathfrak{p}B'_{r,l}}$. Then follows that $\mathfrak{p}B'_{r,l} = (p, \eta_{r,j+1,i} - a_{\mathfrak{P},i+jr} : j \in \mathbb{N}_l, i \in \mathbb{N}_r)$.

Now we will show that the generating set of $\mathfrak{p}$ and $\mathfrak{p}B'_{r,l}$ are equal. In the ring $B_{r,l}$ the ideal $(p, \eta_{r,j+1,i} - a_{\mathfrak{P},i+jr} : j \in \mathbb{N}_l, i \in \mathbb{N}_r) \subset \mathfrak{p}$ has p-power index and after localization we have $(p, \eta_{r,j+1,i} - a_{\mathfrak{P},i+jr} : j \in \mathbb{N}_l, i \in \mathbb{N}_r) = \mathfrak{p}'$ and thus the p-power was also an r-power and since $\gcd(p, r) = 1$ we find that$(p, \eta_{r,j+1,i} - a_{\mathfrak{P},i+jr} : j \in \mathbb{N}_l, i \in \mathbb{N}_r) = \mathfrak{p}$.

By Theorem 3 are the ideals in $S_{p,r}$ of the form $\mathfrak{q}B_r$ with $\mathfrak{q} \subset B_{r,l}$ a prime ideal such that $p \in \mathfrak{q}$, in other words the generating set of $\mathfrak{q}$ is also the generating set of an ideal in $S_{p,r}$. □

Now every prime ideal in $S_{p,r}$ corresponds to a system $(a_{\mathfrak{p},j})_{j\in\mathbb{N}_{lr}}$ of integers $a_{\mathfrak{p},j} \in \mathbb{N}_p$. Thus we can lexicographically order the set of prime ideals by this system.

Definition 6. Define $\mathfrak{p}_{p,r}$ as the prime ideal such that for a prime ideal $\mathfrak{q}$ in $S_{p,r}$ there is a $j \in \mathbb{N}_{lr}$ such that for $i < j$ $a_{\mathfrak{p}_{p,r},i} = a_{\mathfrak{q},i}$ and $a_{\mathfrak{p}_{p,r},j} \leq a_{\mathfrak{q},j}$.

The prime ideal $\mathfrak{p}_{p,r}$ will function as the prime ideal under which we take the quotient.

Theorem 7. *Denote the prime ideal $\mathfrak{p}_{p,r} \cap B_{r,i}$ as $\mathfrak{p}_{p,r,i}$ and let $\overline{\eta_{p,j,i}} = \eta_{p,j,i} \pmod{\mathfrak{p}_{p,r,k}}$. For all $k \geq 0$ the field $\mathbb{F}_p(\overline{\eta_{r,l+k,0}})$ has cardinality p^{r^k}.*

Proof. First note that $\overline{\eta_{r,l,0}} \in \mathbb{F}_p$ by Theorem 5 and thus for $k = 0$ the Lemma follows. For all $k > 0$ the ring $B'_{r,k+l}$ is generated as a module over $B'_{r,k+1-1}$ by the set $\{\eta_{r,k+l,i+1} : i \in \mathbb{N}_{r-1}\} \cup \{1\}$ and notice that

$$\eta_{r,j,0} = -\operatorname{Tr}_{\Delta_r}(\zeta_{\mathbf{r}r^k} \cdot -1) = -\operatorname{Tr}_{\Delta_r}\left(\zeta_{\mathbf{r}r^k} \cdot \sum_{i\in\mathbb{N}_{r-1}} \zeta_r^{i+1}\right) = -\sum_{i\in\mathbb{N}_{r-1}} \eta_{r,j,i+1}.$$

Thus we can change the base by removing $\eta_{r,k+l,r-1}$ and adding $\eta_{r,k+l,0}$, now we have a relative integral basis for $B_{r,k+l}$ over $B_{r,k+l-1}$. Furthermore by Corollary 30 we have $[B_{r,l+k}/\mathfrak{p}_{p,r,l+k} : B_{r,l+k-1}/\mathfrak{p}_{p,r,l+k-1}] = r$ and thus the set $\{\overline{\eta_{r,k+l,i}} : i \in \mathbb{N}_{r-1}\} \cup \{1\}$ is a vector basis for $B_{r,l+k}/\mathfrak{p}_{p,r,l+k}$ over $B_{r,l+k-1}/\mathfrak{p}_{p,r,l+k-1}$.

Since $\overline{\eta_{r,k+l,0}}$ is an element in a vector basis containing 1, we have that $\overline{\eta_{r,k+l,0}} \notin B_{r,l+k-1}/\mathfrak{p}_{p,r,l+k-1}$. This means that $\overline{\eta_{r,k+l,0}}^{p^{r^{k-1}}} \neq \overline{\eta_{r,k+l,0}}$, while $\overline{\eta_{r,k+l,0}}^{p^{r^k}} = \overline{\eta_{r,k+l,0}}$ that is to say $\mathbb{F}_p(\overline{\eta_{r,k+l,0}})$ has cardinality p^{r^k}. □

So we find that $\mathbb{Z}/p\mathbb{Z}$ is our field $\mathbb{F}_p$ for a prime number p and for $r^k > 1$ a prime power such that $\gcd(p, r) = 1$ we found our standard field $\mathbb{F}_{p^{r^k}}$ as $\mathbb{F}_p(\overline{\eta_{r,k+l,0}})$.

Note that for fields k, K, L such that $K \cong k[X]/(f(X)$ and $L \cong k[X]/(g(X))$ with irreducible polynomials $g, f \in k[X]$ we have an identity for tensor products

$$K \otimes_k L \cong L[X]/(f(X)).$$

For a prime number p and positive integer n there are prime numbers $r_1, r_2, ..., r_t$ and positive numbers $a_1, a_2, ..., a_t$ such that $n = \prod_{i=1}^{t} r_i^{a_i}$ and for the field F with cardinality p^n we can apply this identity to find

$$F \cong F_1 \otimes_k F_2 \otimes_k ... \otimes_k F_t$$

where F_i is the finite field of cardinality $p^{r_i^{a_i}}$ for $i \in \{1, 2, ..., t\}$. Thus in fact have we shown that the algorithm of De Smit and Lenstra constructs correctly the finite fields of cardinality p^n where p is a prime number and n an integer such that $p \nmid n$.

In the construction given by De Smit and Lenstra [4] there is a method such that $\mathbb{F}_{p^{p^k}}$ for p a prime number and k a positive integer is defined. With this remaining case the tensor product argument shows that the definition of De Smit and Lenstra is correct for $\mathbb{F}_{p^n}$ for p a prime number and n any positive integer.

References

[1] Robert B. Ash. A course in algebraic number theory, 2003. Chapter 8.1.3.

[2] Pete L. Clark. Commutative algebra. `http://math.uga.edu/~pete/`.

[3] Keith Conrad. Math 676. quadratic characters associated to quadratic fields.

[4] Bart de Smit and Hendrik W. Lenstra. Standard models for finite fields: the definition.

[5] Bart de Smit and Hendrik W. Lenstra. Standard models for finite fields. In Gary L Mullen, editor, *Handbook of finite fields*, Discrete Mathematics and Its Applications. CRC Press, Hoboken, NJ, 2013.

[6] Carl F. Gauss. Disquisitiones arithmeticae. 1801.

[7] Fernando Q. Gouvea. *p-adic Numbers: An Introduction*. Structure and Bonding. U.S. Government Printing Office, 1997.

[8] Frank Lübeck. Conway polynomials for finite fields. `http://www.math.rwth-aachen.de/~Frank.Luebeck/data/ConwayPol/index.html`. Retrieved 2014-7-2.

[9] James S. Milne. Algebraic number theory (v3.06), 2014. Available at www.jmilne.org/math/.

[10] Vreda Pieterse and Paul E. Black. Algorithms and theory of computation handbook, 1999. `http://www.nist.gov/dads/HTML/lasVegas.html` (retrieved:2014-07-02).

[11] Peter Stevenhagen. Algebra 3, 2012. websites.math.leidenuniv.nl/algebra.