Scientific Research Publishing

Advances in Pure Mathematics, 2017, 7, 451-466
http://www.scirp.org/journal/apm
ISSN Online: 2160-0384
ISSN Print: 2160-0368

Lattice Models of Finite Fields

Lucian M. Ionescu, Mina M. Zarrin

Mathematics Department, Illinois State University, Normal, IL, USA
Email: LMIones@ilstu.edu, MZarrin@ilstu.edu

How to cite this paper: Ionescu, L.M. and Zarrin, M.M. (2017) Lattice Models of Finite Fields. *Advances in Pure Mathematics*, **7**, 451-466.
https://doi.org/10.4236/apm.2017.79030

Received: July 27, 2017
Accepted: August 21, 2017
Published: August 24, 2017

Abstract

Finite fields form an important chapter in abstract algebra, and mathematics in general, yet the traditional expositions, part of Abstract Algebra courses, focus on the axiomatic presentation, while Ramification Theory in Algebraic Number Theory, making a suited topic for their applications, is usually a separated course. We aim to provide a geometric and intuitive model for finite fields, involving algebraic numbers, in order to make them accessible and interesting to a much larger audience, and bridging the above mentioned gap. Such lattice models of finite fields provide a good basis for later developing their study in a more concrete way, including decomposition of primes in number fields, Frobenius elements, and Frobenius lifts, allowing to approach more advanced topics, such as Artin reciprocity law and Weil Conjectures, while keeping the exposition to the concrete level of familiar number systems. Examples are provided, intended for an undergraduate audience in the first place.

Keywords

Finite Fields, Algebraic Number Fields, Ramification Theory, Frobenius Element, Congruence Zeta Function, Weil Zero

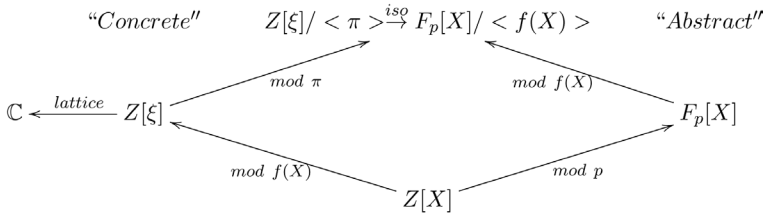
1. Introduction

Finite fields are important mathematical structures, taking the learner from the familiar realm of congruence arithmetic to algebraic number theory territory, and providing new tools for mathematical physics and cryptography, for example.

We aim to highlight a pedagogical tool for the introduction of higher dimensional finite fields, which balances the traditional "axiomatic", top-down approach of Abstract Algebra, with a constructive, yet intuitive approach, using what we call *lattice models*.

The "standard" way in an Abstract Algebra course of introducing such higher

dimensional finite fields, is to extends the primary finite field F_p, as a quotient of a polynomial ring $F_p[X]/\langle f(X)\rangle$ (e.g. MIT Modern Algebra Course, [1], Ch. 6 etc.). The lattice model approach *extends the lattice of integers first*, to place it in the context of complex numbers, followed by the quotient modulo a prime. In this way it mimics the elementary case of primary finite fields $F_p = Z/pZ$, providing also a geometric intuition accompanied by the corresponding analytic-topologic tools available.



Remark *Before comparing the two approaches, let us note that specialization* (*everywhere!*) *led to a fragmentation of the mathematical curriculum too, while the number of course a student may take remained essentially the same. This led teachers and researchers alike to advocate the need for a reintegration of Mathematics in various ways, for example in combination with teaching History of Mathematics* (*historical motivations*) [2], *Preface* 1*st ed., p.*12[1]: "*One of the disappointments experienced by most mathematics students is that they never get a course on mathematics*". *As a more modest goal of our paper, we believe that providing bridges between usually curricular separated ares in Mathematics, provides a* "*better circulation*" *of the underlying knowledge, and provides the student with more thinking power* (*links/synapses*). *The current tendency in Mathematics, and in fact in in general, is analytical specialization* (*well justified by the exponential growth of knowledge*); *there is a need for compensatory synthetic integration of symbiotic topics, supporting one another.*

Comparing with the concept of group, the "abstract way" is to define the algebraic structure with one binary operation, and then derive their properties from "axioms", perhaps too soon, before the student has enough examples to develop the "feeling" and intuition of what they are. The two dual, symbiotic types of groups, are the non-commutative groups of transformations, which always act on some space, and those we call Abelian, which in fact are "discrete vector spaces" on which the first kind act upon. The "unified" approach through generalization and abstraction has its price: treating alike the two becomes the norm, and the differences in interpretation neglected.

In this modern algebraic way of introducing algebraic structures abstractly, through general definitions, and then quickly deriving their properties, one would immediately ask the question of existence and uniqueness. The latter can be addressed in complete generality, without even knowing if they exist. Existence is proven, of course, by constructing finite fields explicitly.

[1]We further invite the reader to see the whole first paragraph.

For primary finite fields F_p, in characteristic p, this is easy: the well known Abelian groups Z/nZ, taught while doing congruence arithmetic, or rather viewed as rings Z/nZ, are easily shown to be fields, when $n=p$ is a prime number; but the other high dimensional finite fields are F_p^d are harder to construct, and the "future algebraist", the student, learns by heart the recipes for constructing field extensions.

Pedagogically, examples should be provided first, worked with them to the point the student begins to like them, and then "frame them" in the appropriate axiomatic context.

The lattice models of finite field presented in this paper represent construction of F_p^d, generalizing the above simple case of wrapping the 1-dimensional lattice Z, with period corresponding to the prime ideal pZ. By using higher dimensional lattice, instead of the standard adjunction of "roots" construction, we provide a geometric interpretation, with a corresponding graphical representation which brings geometry up-front, to enjoy and play with ... if time allows it!

Of course, there is a price to pay: some new number systems need to be introduced along the way, still extensions using the standard algebraic construction, but so important that they need to be made well known well before the theory of finite fields takes off: Gaussian and Eisenstein integers [3] [4], and their generalizations (cyclotomic extensions).

And yet here again, one can borrow the geometric interpretation of complex numbers as representing 2D-rotations, and still provide enough geometric intuition, to overcome the abstract "magical act" of adjoining new symbols; at least this is the opinion of one of the authors.

The article is organized as follows. The next section §0, introduces finite fields abstractedly, as in most textbooks of abstract algebra. Section §0 constructs finite fields as congruence rings of integers in number fields (algebraic extensions of the rationals). The geometric interpretation is emphasized. We conclude §0 discussing briefly some important topics at hand, like Frobenius elements and Weil zeros.

2. Finite Fields: The "Abstract Way"

We will recall the basic facts about finite fields, as introduced in most standard texts of abstract algebra. To keep it self-contained, and simple, we use a brief presentation available on the web [5]. See [6] for additional theoretical details and [7] for a computational approach.

Definition 2.1 *A finite field is a field which is finite!*

The additive order of the unit $1+\cdots+1=0$ is called the characteristic of the finite field. It is always a prime p. For example $F_3=Z/3Z$ has characteristic $p=3$.

Recalling some basic properties are in order.

Proposition 2.1 *A finite field F of characteristic p has* $q=p^n$ *elements. It is*

a vector space of dimension n over the primary field F_p: $n=[F,F:p]$.

Theorem 1 (*i*) (*Existence and Uniqueness*) *For each p and n there exists a finite field of characteristic p with* p^n *elements.*

(ii) Two such finite fields with the same number of elements are isomorphic.

It is therefore natural to denote a *generic* finite field as F_q, with $q=p^n$, as if it is a specific one. By abuse of notation, yet well justified by the uniqueness modulo isomorphism, we write $F_p=Z/pZ$, without further comments (LHS is a "any" finite field of characteristic *p*, while the RHS is the preferred, specific construction of one such field).

The "standard" way to construct higher dimensional finite fields with a given number of elements p^n, and of course prescribed characteristic *p*, uses the standard algebraic construction of field extensions via polynomial rings and their quotients by ideal generated by irreducible polynomials.

We reproduce here the Example 1.88, from [6], p. 34.

Example 2.1 *Let the prime field be* F_3. *As an example of the formal process of root adjunction, consider the irreducible polynomial* $f(x)=x^2+x+2\in F_3[x]$. *Let* θ *be a "root" of f, that is,* θ *is the residue class* $x+(f)$ *in* $L=F_3[x]/(f)$. *The other root of f in L is* $2\theta+2$, *since*

$$f(2\theta+2)=(2\theta+2)^2+(2\theta+2)+2=\theta^2+\theta+2=0.$$

We obtain the algebraic extension $L=F_3(\theta)$ consisting of the nine elements $0,1,2,\theta,\theta+1,\theta+2,2\theta,2\theta+1,2\theta+2$, *i.e.* an instance of F_{3^2}.

3. What *Are* Number Fields?

The algebraic structure we call *field* was first introduced by Dedekind [8] ([2], Ch. 12). The usual number systems *Q*, *R* and *C* are the traditional examples of fields. When solving algebraic equations defined by polynomials, we are "forced" to extend our number system, and adjoin formal roots of polynomials as new "numbers". We can treat these either as new *symbols*, and *construct* the new number system, for example $C=\{x+iy\,|\,x,y\in R,i^2=-1\}$, as real linear combinations of 1 and the symbol *i* subject to the relation $i^2=-1$, or more formally, in the abstract (algebra), as quotients of polynomials modulo the ideal generated by the polynomial defining the relation:

$$C=R[X]/\langle X^2+1\rangle=\{a+bI\,|\,a,b\in R,I=[X]\},$$

Here $[X]$ denotes the congruence class of *X* modulo the ideal, satisfying the required relation: $I^2+1=[X^2+1]=0$ (since $X^2+1\equiv 0\ mod\ X^2+1$).

We will call this construction the *standard algebraic construction* of a field extension.

Now "integers" play a central role in arithmetic, in various rings, and they satisfy the structure of lattices. Initially we may call "integers" the subring of a field extension which emerges as a corresponding field of fractions, but field extensions require more care when defining the concept of *algebraic integer of a field extension*.

Definition 3.1 *A latice* $\mathcal{L}$ *is a Z-submodule of a ring.*

In particular a lattice is a finitely generated abelian group, and can be interpreted and visualized as a "discrete (finite dimensional) vector space" (by abuse of language, when there are still relations among generators).

Two good examples of such lattices of algebraic integers are the Gaussian integers and Eisenstein integers [3] [4].

3.1. Gaussian Integers

Complex numbers are a familiar example of field extension of the reals. To keep the theory algebraic, and to investigate it from an arithmetic point of view, neglect the Cauchy reals as non-realistic numbers [9], and consider the quadratic extension $Q\left(\sqrt{-1}\right)$ over the rationals *Q*. Even better, since these fields are fields of fractions, focus on the extension of integers: $Z[i]$[2].

The ring $Z[i]=\{m+in|m,n\in Z\}$ is called the ring of Gaussian integers. The rational primes *p* may factor in this larger arithmetic number system:

The prime 2 is special, and "ramifies" as $2=i^{-1}(1+i)^2$[3].

$p\cong 1 \bmod 4$ splits into a product of conjugate primes, for example $5=(2+i)(2-i)$;

$p\cong -1 \bmod 4$ is *inert*, *i.e.* it remains a prime in $Z[i]$; for example $p=3$.

For more facts about Gaussian integers see [3]. For a more technical account, including relations to Galois theory, see [10].

3.2. Eisenstein Integers

Similarly, taking a cubic root of unity ω instead of the 4-th root of unity *i*, we obtain the Eisenstein integers $Z[\omega]$, with its own primes and classes of rational primes ramifying ($p=3$), and splitting or being inert, according to a similar condition $p\cong\pm 1$, but this time modulo 3. Alternatively, one may look at the analog of Fermat's Two Squares Theorem, about representing primes $p=m^2+n^2$, except this time we use a different quadratic form (norm): x^2-xy+y^2, instead of the usual one $x^2+y^2=N(x+iy)$ in $Z[i]$.

For more details, see [4].

3.3. From Number Fields to Finite Fields

Now the idea for constructing higher dimensional finite fields, is to consider the congruence rings of algebraic integers, modulo a prime, the obvious analog of the construction of primary finite fields $F_p=Z/pZ$.

As a quick example, $Z[i]/3Z$ yields F_{3^2}, while $Z[i]/(2+i)Z\cong Z/5Z=F_5$.

Besides being a more natural construction, it provides the geometric background for a better understanding of finite fields as *Klein geometries* (Galois fields)[4].

[2]In general the extension of integers might not coincide with the algebraic integers of the corresponding field extension.

[3]Recall that we have more units here: $1,-1,i,-i$.

[4]...not to mention the connection with Galois Theory, splitting polynomials and Frobenius elements.

4. Lattice Models: The "Geometric Way"

We will proceed by way of example. Recall that the primary fields F_p can be constructed as ing quotients Z/pZ, where p is a prime number, the characteristic. geometrically, Z can be viewed as a 1-dimensional lattice, or as an infinite oriented graph[5].

The prime p defines a period, and the covering map $\phi(k) = k \bmod p$ is a discrete geometric analog of the familiar covering map of the circle $x \bmod 1$, sometimes used to define angles, sine and cosine. Algebraically, ϕ is a group (ring) homomorphism: the quotient map of the ring Z by the ideal pZ.

Now let's consider a 2D-example: the Gaussian integers, as a lattice, modulo a prime ideal $\mathcal{P}$.

Since $Z[i]$ is a principal ideal domain (PID), we need only consider $\mathcal{P} = Z[i]\pi$ with Gaussian prime π "sitting" over a rational prime p: $N(\pi) = p$.

For example $2+i$ is a Gaussian prime over 5, completely splitting it: $5 = (2+i)(2-i)$. Recall that other rational primes of the form $p \cong -1 \bmod 4$ are *inert*, *i.e.* are Gaussian primes too and $N(p) = p^2$.

There is also the special case of the *ramified prime* 2[6], which factors with multiplicity: $2 = (1+I)^2 \cdot (-i)$ [3]).

Remark *The factorization may also be written in an initially misleading way as* $2 = (1+i)(1-i)$, *but* $1+i$ *and its conjugate* $1-i$ *are the "same" prime, modulo a unit* $\pm 1, \pm i$.

Consider the same algebraic quotient map $\phi(z) = z \bmod \pi$. Since π is prime, the quotient ring $K = Z[i]/(\pi)$ is a field of characteristic p, *i.e.* F_{p^f}. The norm $N(\pi) = p^f$ gives the dimension $f = [K : F_p]$.

Excepting the case of the ramified prime $p = 2$, we have the following two cases. For inert (rational) primes $p \cong 3 \bmod 4$, $\pi = p$ is the only prime over p, and $f = 2$; otherwise $p = \pi\overline{\pi}$ splits and $N(\pi) = p$.

Example 4.1 *Let* $p = 5$ *and* $\pi = 2+i$. *Then* $K = Z[i]/(\pi)$ *is a lattice model of* F_5 (*the abstract finite field with* 5 *elements*). *We can see its canonical residue classes as the Gaussian integers in the fundamental region of the lattice* $\mathcal{L} = \{a\pi + b\overline{\pi} \mid a, b \in Z\}$, *for example with* a, b *non-negative integers, such that* $N(z) < p$ (*again considering the projection on the integers*).

Another example of lattice model, providing an alternative construction to the "standard" algebraic extension from Example 0.1, is the following.

Example 4.2 *Consider again* $Z[i]$ *as a quadratic extension and* $p = 3$ *the rational inert prime. Then the quotient lattice* $Z[i]/(3)$ *has* $q = 3^2$ *elements, representing the finite field* F_{3^2}.

5. Applications to Weil Zeros

There are several topics of Algebraic Number Theory which may benefit from

[5]The interested reader may lookup partial ordered set, POSet for short, too, as a generalization.

[6]Divides the discriminant of the quadratic extension $[Z(i) : Z]$.

the introduction of finite fields as quotients of lattices of algebraic integers:

a) Ramification Theory, in the context of Galois Theory of such extensions;

b) The Frobenius element, as a generator of the Galois group of the corresponding extensions, controlling the factorization of prime ideals in extensions of number fields;

c) Quadratic Reciprocity using the connection between the Frobenius element and Legendre symbol in congruence rings of number fields; finally,

d) Applications to Weil Conjectures, and notably to the finite characteristic Riemann Hypothesis via the characteristic polynomial of a lift of the Frobenius element, having eigenvalues the Weil zeros of the Weil polynomial, *i.e.* the reciprocal of the numerator of the Hasse-Weil Congruence Zeta Function [11].

The first three applications are essentially described in [12]. In this article we will focus on this later important application to Algebraic Geometry, which can be accessed relatively easily, in a computational oriented way, using for example SAGE as a mathematical software. In this brief note, we will only point the way. For an exposition, see the classical texts, for example [13] [14]; additional explanations and computations can be found in the lecture notes of the first author [15].

5.1. Solving Algebraic Equations over Finite Fields

Quadratic equations were studied since ancient times, e.g. Appolonius' theory of conic sections. Replacing the usual number system with finite fields places the problem in the context of Algebraic Geometry.

Following [14], Ch. 8, consider the solution $X\left(F_q\right)$ of the equation $y^2 = x^d + D$ over the finite field F_q with $q = p^n$ elements. It is an algebraic *affine curve* of *degree d*. Denote the corresponding number of elements N_n, and the associated *congruence zeta function*[7]

$$Z_{X/Fp}\left(T\right) = \frac{P\left(T\right)}{\left(1-T\right)\left(1-pT\right)}, \quad P\left(T\right) = \prod_{i=1}^{2g}\left(1-\omega_i T\right),$$

where $g = \left(d-1\right)/2$ is called the *genus of the curve*, and w_i are algebraic numbers we will call the *Weil zeros* of the *Frobenius polynomial* $h\left(u\right) = u^{2g}P\left(1/u\right)$[8]. We will not go in depth explaining the terminology, and just use it to exemplify the relation with factorization of primes and lattice models of finite fields.

Example 0.4 *The cubic* ($d = 3$) *curve* $X : y^2 = x^3 + D$, *is an elliptic curve of genus* $g = 1$, *which should be pictured topologically* (*over complex numbers*) *as a torus* (*when completed with the point at infinity*: *the projective curve*).

Regarding the fixed prime *p*, whether F_p has *m*-roots of unity or not decides the form of $P\left(T\right)$ and N_n. In what follows we will assume $m \mid p-1$, *i.e.* F_p has *m*-roots of unity[9] Then $P\left(T\right) = \left(1-wT\right)\left(1-\overline{w}T\right)$ is a quadratic polynomial and the number of affine points is $N_n = p^n - w^n - \overline{w}^n$, where $\overline{w}$

[7]Conform Weil Conjectures/Deligne Theorem.

[8] w_i are reciprocal of the zeros of the "Frobenius polynomial" $P\left(T\right)$.

[9]Cauchy Theorem for the multiplicative group $\left(F_q^{\times}, \cdot\right)$

denotes complex conjugation [13], Ch. 18§2, p. 302 (where the +1 stands for the point at infinity; see also [14], p. 292).

Remark *Later we will see how Weil zeros* w_i *are related to Gauss and Jacobi sums, which are valued in the cyclotomic numbers of roots of unity of order* $l(l-1)$ *and* $l-1$ *respectively, if* $l=m \mid p-1$ *is a prime.*

Part of *Weil Conjectures* [16] is that $w\overline{w}=p$, *i.e.* the *Riemann Hypothesis* holds in finite characteristic [14]. Moreover, introducing the *defect* $a_p=w+\overline{w}$, $P(T)=1-a_pT+pT^2$.

Remark *The coefficients of the Betti polynomial* $P(T)$ *are related to Weil zeros as a consequence of a deeper connection with the characteristic polynomial of the Frobenius element* $h(u)$: $a_p=Tr(Frob)$, $p=det(Frob)$.

Example 5.2 *The elliptic curve* $m=3$ [13], p. 306, *has* $N_1=p+w+\overline{w}$, *where the Weil zeros split the prime* $p=w\overline{w}$ *in the cyclotomic extension* $Z(\zeta_3)$ *of Eisenstein integers* (*assuming* $3 \mid p-1$). *In terms of primary primes* $\pi,\overline{\pi}$, $\pi \cong 2 \bmod 3$ (*associated to* $w,\overline{w}$), *we have* [13], Th. 4, p. 305 (*affine points*; $6=l\cdot(l-1)$ *with* $l=3$):

$$N_p=p+2Re(\rho(4))\pi, \quad \rho(x)=\left(\frac{4D}{\pi}\right)_6\pi.$$

As a concrete example take $D=1$.

If $p=13$ then $\pi=-1+3\omega$ is a primitive prime, and together with $\overline{\pi}=-1+3\omega^2$ split p:

$$p:13=(-1+3\omega)(-1+3\omega^2):\pi\overline{\pi}.$$

Since $\rho(4)=\omega^2$, the Weil zero is $w=-\omega\pi$, associated to π (Units: $\{\pm1,\pm\omega,\pm\omega^2\}$).

Now the number of affine (finite) points in F_p is:

$$N_1=13+2Re(\omega\pi)=13+2(\omega^2+\omega)=13-2=11,$$

consistent with a direct check and counting argument:

$$X(F_{13})=\{(4,0),(10,0),(12,0),(0,\pm1),(2,\pm3),(5,\pm3),(6,\pm3)\}.$$

Example 5.3 *As another example consider* $D=5$ *and* $p=19$. *Note that* $\pi=5+3\omega$ *is primary and splits p*:

$$19=(5+3\omega)(5+3\omega^2), 5+3\omega\cong 2 \bmod 3.$$

From the above formula we obtain the number of points ([17], p. 8)[10]:

$$N_1=p+\pi+\overline{\pi}=19+5+\omega+5+\omega^2=26.$$

Then $a_p=-2Re(\pi)=-7$ and Weil zeros are $w=-\pi$ and its conjugate:

$$P(T)=(1-wT)(1-\overline{w}T)=1+7T+19T^2, \quad N_1^{proj}=P(1)=27.$$

Remark *One may use SAGE* (*recently renamed as CoCalc*) [18] *to conveniently compute Dirichlet characters* (*like* ρ *above*), *and Jacobi sums, which*

[10]We need Jacobi sums for this: see §5.3.

are instrumental in computing the number of points.

Well, what does this problem of counting the number of solutions, with its associated congruence zeta function, have to do with lattice models of finite fields!? For this we need to recall some facts about the Galois group of an extension, and the relation with the *Frobenius element*, which will turn out to be present as the numerator of the zeta function.

5.2. Frobenius Element

Following [19], consider a number field extension $Q(\xi)/Q$ which is Galois, and how a rational prime p decomposes in it, with π such a prime factor (assuming a principal ideal domain case for simplicity). Then the Galois group of the number field extension $Gal\left(Q(\xi)/Q\right)$ is related to the Galois extension of the corresponding (lattice models of) finite fields:

$$1\to I(\pi/p)\to D(\pi/p)\to Gal\left(F_q/F_p\right)\to 1,$$

where $D(\pi/p)$, the *decomposition group* consists in Galois automorphisms preserving the ideal generated by π, each of its elements therefore inducing an automorphism of the corresponding finite fields extension $Gal\left(F_q/F_p\right)$, in a surjective manner. The kernel of this projection, the *inertia group*, will not be used in what follows.

If p is unramified, then the kernel (the *inertia group*) is trivial, and the above surjection becomes an isomorphism. Then one can "pull-back" the Frobenius automorphism $x\mapsto x^p$ of $Gal\left(F^q/F^p\right)$, where we recall that $F^q=Z[\xi]/\pi$ and $F_p=Z/p$ are lattice models of finite fields constructed in number fields *viewed* (*embedded*) *as subfields of the complex numbers*.

Definition 5.1 *In the context above* (π *prime in* $Z[\xi]$ *over the unramified rational prime* p), *the Frobenius element* $Frob_p^{\pi}\in Aut_Z\left(Z[\xi]\right)$ *is the unique Galois automorphism which induces the Frobenius automorphism* $Fr(x)=x^p$ *in the finite field extension* F_q/F_p, *of lattice models.*

At this stage the Frobenius elements may depend on the choice of prime π over p. But these Frobenius elements are conjugate to each other, so if the Galois group is Abelian, then the Frobenius element is unique, and will be denoted by $Frob_p$.

Example 5.4 *Consider* $Q[i]$, *with* i *a forth root of unity, and its Gaussian integers* $Z[i]$. *The only ramified prime is* 2; *otherwise* $p\cong 1$, *mod* 4 *or course, splits, or* $p\cong -1$ *is inert.*

The decomposition group $D(p)$ is trivial in the split and ramified cases, and equals $G=Gal\left(Q(i):Q\right)\cong Z_2$ (multiplicative group $\{-1,1\}$) otherwise.

Thus the Frobenius element is 1 when $p\equiv 1$ and -1 otherwise, *i.e.* $Frob_p=\left(\frac{-1}{p}\right)$ is given by the *Legendre symbol* (the unique multiplicative character of order 2).

Alternatively, we can compute the *lift to* $Z[i]$ *of the Frobenius* x^p, from the

"abstract" setup, using our lattice model, to the ring of algebraic integers[11]:

$$(a+ib)^p \equiv a+bi^p \ mod\ pZ[i].$$

Since $i^p = \left(\frac{-1}{p}\right) i$ "on the nose", *i.e.* not just *mod* p, we conclude that the lift has the following closed formula in terms of the multiplicative quadratic residue character $\rho_2(z) = (z/p)$:

$$Frob_p(a+ib) = a+\left(\frac{-1}{p}\right)b, \quad Frob_p = \sigma^k, k = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

The last form was written in terms of the generator of *G*, here complex conjugation.

Example 5.5 *The above example can be generalized to quadratic extensions* $Q(\sqrt{d})$, *where d is square free* ([19], p. 3). *The Frobenius element, in* $Z/pZ^\times$, *is* $Frob_p = (d/p)$, *so that* $Frob_p(a+\sqrt{d}b) = a+(-1/p)\sqrt{d}b$, *i.e.* $Frob_p = \sigma^{ord(-1/p)}$ *as before.*

Example 5.6 *In the cyclotomic case* $Q(\xi_n)$, *the primes that ramify are those which divide n. The Galois group is isomorphic to the multiplicative group of roots of unity, and therefore isomorphic to* $(Z/nZ^\times, \cdot)$, *with a Galois element* $\sigma_m : \xi \mapsto \xi^m$, *with* $m \in Z/nZ^\times$ *relatively prime to n.*

In the non-ramified case $p \in Z/nZ^\times$, the Frobenius element is, again as expected:

$$Frob_p\left(\sum_{k=0,\cdots,n-2} c_k \xi_n^k\right) = \sum c_k Frob_p(\xi_n)^k, \quad Frob_p(\xi) = \xi_n^p.$$

As another quadratic extension example, consider $Q(\omega)$, corresponding to a cubic root of unity $\omega^3 = 1$, and its Eisenstien integers $Z[\omega]$. Then the corresponding Frobenius element is, similarly to the Gaussian integers case:

$$Frob_p(a+\omega b) = a+\rho_3(p)\omega b.$$

Remark *At this stage, one may further look into the correspondence between how the prime p factors into* $Z[\xi]$, *and how the primitive polynomial* $f(x)$, *of* ξ *factors in* $F_p[x]$, *reflecting the commutativity of the diamond diagram from the introduction.*

It is conceptually important to piece together these Frobenius elements as a map depending on the prime *p*, called the *Artin map*: $Frob: p \mapsto Frob_p$ [12]. For cyclotomic extensions, If we identify the Galois group $Gal(Q(\xi_n)/Q)$ with $(Z_n^\times, \cdot)$, then the Artin map is simply the "identity" map:

$$p \mapsto Frob_p = (p\ mod\ n),\ p \in Z_n^\times.$$

For example, with $m = 4$ and *p* an odd prime, the Galois group is generated

[11]It is enough to consider the extension of *Z*, and not the full algebraic closure in $Q(i)$, which incidenltally, here coincide.

[12]In a more general setup [12], Ch. 5, $Frob(p) = \left(\frac{L/K}{P}\right)$ is called the *Artin symbol.*

by conjugation $G=\langle\sigma\rangle$, since $Z_4^{\times}\cong Z_2$, and $Frob(p)=p \bmod 4$ as an element of $Z_4^{\times}$. This is essentially the Legendre symbol $\frac{p}{4}$, when identifying Z_4 with the 4-th roots of unity, via exponentiation (the Galois group identification).

Once we know the Frobenius element, its characteristic polynomial can be computed easily:

$$P\left(Frob_p\right)(t)=det\left(Frob_p-tI\right).$$

For example, in the cyclotomic setup, with $m=4$ (Gaussian integers), the matrix of $Frob_p=\sigma^{(-1/p)}$ in the basis $1,i$ is:

$$Split: p\equiv 1 \bmod 4: \quad Frob_p=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$$

$$Inert: p\equiv -1 \bmod 4: \quad Frob_p=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$$

and the characteristic polynomials are, respectively:

$$P(T)=(1-T)^2, \quad P(T)=1-T^2.$$

Similarly, for a quadratic extension, for example $m=3$ (Eisenstein integers), the matrices of the Frobenius elements I and σ, and their matrices are essentially the same (but computed in a different basis $1,\omega$).

Now let's see how the Frobenius element, or rather its lift and the corresponding characteristic polynomial is related to the Hasse-Weil congruence zeta function.

5.3. Weil Zeros and Jacobi Sums

We will only document the facts with an example, following [13] [14] [20] [21], and leave the general case for a separate study.

Let $y^2=x\left(x^2+1\right)$ define an elliptic curve over F_q. Since the RHS of its defining equation $f(x)$, splits in $Z[i]$, we will work with Gaussian integers in the number fields side of the "picture".

For $p\cong 3 \bmod 4$, the prime is inert in $Z[i]$, which corresponds to the factor x^2+1 being irreducible in F_p and the Frobenius element complex conjugation.

Theorem 5, [13], p. 307, with $D=-1$, yields the number of *projective* points[13], according to the type of prime:

$$Inert: N_p=1+p, \quad Split: N_p=p+1-2Re\left(\rho_4(-1)\pi\right),$$

where π is a primary prime splitting p and ρ_4 is a character of order 4.

We will focus on the split case $p\cong 1 \bmod 4$ (Ramification Theory parameters: $g=2$, $e=1$, $f=1$).

To have a "nice" description of the lift of Frobenius Fr_p on C preserving our

[13]The +1 stands for the point at infinity.

curve, and not some "deformation" of identity (the Frobenius element) $(x,y)\mapsto\left(x^q+f(x,y),y^q+g(x,y)\right)$ [20], p. 10, we use Weierstrass coordinates. The elliptic curve is then the quotient of $\mathbf{C}$ by our lattice $\Lambda=Z[i]$ of (Gaussian) algebraic integers:

$$e(\tau z):(\mathbf{C},+)\to(\mathbf{C}^{\times},\cdot),\quad \mathbf{C}/Z[i]\cong E(\mathbf{C}),$$

where here $\tau=2\pi i$. Then the Frobenius lift $Fr_p(z)=z\cdot c$ is multiplication by some lattice element $c=a+ib\in Z[i]$ [20] [21].

Remark *Alternatively, we could lift the Frobenius to the p-adic completion, and taking advantage of Hasse principle for finding the above "perturbations"* $f(x,y)$ *and* $g(x,y)$.

If the curve is defined by a polynomial in the powers of the variables (Weil curves), e.g. Riemann surfaces $y^2=x^s+D$ ([14] p. 292) and Fermat curves $x^m+y^m=z^m$ ([13] [22]), then Jacobi sums provide a powerful tool to compute the number of points.

Then $N_p=1+p-a_p$, with the *defect* given by the Jacobi sum $a_p=2ReJ(c_2,c_4)$, which also yields the Weill zeros $w,\bar{w}$ of the (reciprocal of) "Betti polynomial"[14]:

$$Z_p(T)=\frac{L_p(T)}{(1-T)(1-pT)},$$
$$L_p(T)=(1-wT)(1-\bar{w}T),\quad w\bar{w}=q.$$

Then $w=-J(c_2,c_4)$ is primary [13] and our lift of Frobenius is given by $c=w=\pi$, conform with [21], with $a_p=Tr(Fr_p)$ and $p=det(Fr_p)$ (Riemann Hypothesis, part of the Weil Conjectures; see also [11], Lecture #8, Hasse's Theorem):

$$CharPoly(Fr_p):\ \ det[Fr_p-u\,Id]=u^2-a_pu+p,u=1/T.$$

Rewriting the number of points as in [20] $N=q-2d\sqrt{q}+1$, and the Weil zero as $w=e^{i\theta}\sqrt{q}$, one may interpret the "Betti coefficient" $d=Re(e^{i\theta})$ via a comparison with the Jacobi sum, as phase of the 2-cocycle of the Fourier coefficients of the Dirichlet characters (Gauss sums)... but this is another story!

Remark *A similar discussion applies to our previous example of elliptic curve* $y^2=x^3-D$ ([13], p. 304; [17], p. 7), *with Eisenstein integers replacing Gaussian integers.*

Remark *For higher dimensional extensions* F_{p^f}, *needed when the genus of the curve excedes* $g=1$, *can be implemented via cyclotomic extensions* $Z[\xi_m]$, *such that the dimension* $n=\phi(m)$ *factors as* $g\cdot f$ *with* $f=ord(p)$ *is the order of multiplication by p in* $Z/mZ^{\times}$ *and g the ramification genus of the prime p.*

6. Conclusions and Further Developments

There are various styles of teaching (and designing) Abstract Algebra. We

[14]The numerator of the Zeta function is a local L-function having a cohomological interpretation.

attempted to plead that, in the case of finite fields, the abstract approach to the introduction of the algebraic structure ("axiomatic"/top-down design), can be supplemented by the specific construction we call *lattice models*, which introduces the number fields first, as more "familiar" to the student used to solve polynomial equations, and presenting F_{p^n} as a congruence ring, in perfect analogy to the way we introduce the primary finite fields $F_p = Z/pZ$.

6.1. Motivation, Goals and Contributions

One motivation of this article for emphasizing lattice models of finite fields is the need for a pedagogical introduction to finite fields as part of an Abstract Algebra course, with strong ties with number fields ("number systems" in their natural habitat of complex numbers), with best results after covering Galois Theory, of course. As mentioned in the introduction, a discussion of the residue fields in the context of decomposition of primes in algebraic number fields, implies a long wait in providing such concrete examples of extensions of finite fields [23]. Bridging mathematical topics in general, is a much needed way to balance specialization [2], p. 12.

In our case at hand, the bonus is some extra intuition, but more importantly, a rich *geometric framework* for bridging and interpreting other abstract algebra concepts, like Galois Groups, Frobenius elements, paving the road towards understanding *General Reciprocity Laws* the "right way" [24].

The second goal, which in fact started the current project, was to provide a direct approach to Weil Conjectures, to be understood not in their natural "habitat" of abstract Algebraic Geometry, but in the more geometric and topological context of complex manifolds, by using lattice models of finite fields. Then the Frobenius element of the number can be related to a Frobenius lift of the Frobenius automorphism. Then the numerator of the Weil Congruence zeta function is the characteristic polynomial of the lift of the Frobenius element, allowing to count numbers of solutions without the use of a Weil cohomology (e.g. Grothendieck's approach via l-adic cohomology).

Our main contribution in this open effort for bridging the modern abstract ("axiomatic") exposition of finite fields and traditional concrete, by example, approach using the familiar "number systems", is the emphasis on the concrete examples of finite fields we call *lattice models*, with the early benefit of learning of how primes decompose: Ramification Theory. As a "bonus", as mentioned before, this bridge may constitute a shortcut to understanding Frobenius lifts, via Frobenius elements, in a more familiar context, towards understanding more advanced topics like congruence zeta function and Weil Conjectures, without having to "cross-over" to p-adic analysis and etale cohomology.

Regarding other studies in this direction, we noticed only highly specialized articles and presentations, either focusing on ramification theory, or in attempting the construction of a lift of Frobenius directly, by not so accessible to students [20]. This provided additional motivation for starting this project.

6.2. Towards Other Applications: Algebraic Topology/Geometry

Once "in motion", if one wishes, Lefshetz formula, as well as algebraic topology/geometry technics, such as Riemann-Roch/Hurwitz Th., may be used on this characteristic zero "side" of number fields and lattice models of finite fields, in the natural and familiar framework of the complex numbers. This direction of continuing the combined study of finite fields in concrete applications to Algebraic Topology and Algebraic geometry, benefitting even more from an intuitive understanding via graphical representations, will be the subject of future faculty-student research projects.

On the concrete complementary side, *SAGE/CoCalc programs* [25] were specifically designed to allow for computer explorations of the presented topics of Algebraic Number Theory [18], which, in our opinion, constitute interesting studies, accessible for undergraduate research. Further programs for representing graphically the corresponding lattices, Frobenius orbits etc., are envisaged as further developments, with student help.

References

[1] MIT Open Course 18.703, Modern Algebra, Spring 2013, Textbook: Abstract Algebra by I. N. Herstein, Macmillan, 1986.

[2] Stillwell, J. (2000) Mathematics and Its History. 2nd Edition (Revised), Springer, UTM, New York.

[3] https://en.wikipedia.org/wiki/Gaussian_integer

[4] https://en.wikipedia.org/wiki/Eisenstein_integer

[5] Lange, T. Finite Fields (Chapter of Draft Book "Discrete Mathematics"). https://hyperelliptic.org/tanja/teaching/CCI11/online-ff.pdf

[6] Lidl, R. and Niederreiter, H. Finite Fields and Their Applications. https://math.boisestate.edu/~liljanab/MATH508/FiniteFields_and_Applications.pdf

[7] John, K. (2004) Computations in Finite Fields. http://johnkerl.org/doc/ffcomp.pdf

[8] Dedekind's Contributions to the Foundations of Mathematics, Stanford Encyclopedia of Philosophy, 2008. https://plato.stanford.edu/entries/dedekind-foundations/

[9] Wildberger, N.J. (1999) Real Fish, Real Numbers, Real Jobs. *The Mathematical Intelligencer*, **21**, 4-7. https://doi.org/10.1007/BF03024838 www.researchgate.net/publication/225795896_Real_fish_real_numbers_real_jobs

[10] Stark, H.M. (1992) Algebraic Number Theory, Galois Theory and Zeta Functions. In: Waldschmidt, M., Moussa, P., Luck, J.-M. and Itzykson, C., Eds., *Number Theory to Physics*, 313-393.

[11] Sutherland, A. (2015) 18.783 Elliptic Curves. Massachusetts Institute of Technology: MIT Open Course Ware. Spring. https://ocw.mit.edu https://ocw.mit.edu/courses/mathematics/18-783-elliptic-curves-spring-2015/index.htm

[12] R.B. Algebraic Number Theory, Ch.8. http://www.math.uiuc.edu/~r-ash/Ant/AntChapter8.pdf

[13] Ireland, K. and Rosen, M. (2010) A Classical Introduction to Modern Number Theory. GTM Series 84, Springer, New York.

[14] Lorenzini, D. (1996) An Invitation to Arithmetic Geometry. Graduate Studies in

Mathematics Vol. 9. https://doi.org/10.1090/gsm/009

[15] Ionescu, L.M. (2015) Topics in Number Theory MAT 410.

[16] Ossermann, B. Weil Conjectures. https://www.math.ucdavis.edu/~osserman/math/pcm.pdf

[17] Wang, W. Notes on Character Sums. http://wstein.org/edu/2010/414/projects/wen_wang.pdf

[18] Ionescu, L.M. SAGE/CoCalc Programs for Algebraic Number Theory. http://my.ilstu.edu/~lmiones/

[19] Yott, D. Frobenius Elements, the Cheboratev Density Theorem, and Reciprocity. https://math.berkeley.edu/~dyott/Frobenius%20elements.pdf

[20] Ang, L. The Lefschetz Fixed Point Theorem and Solutions of Polynomial Equations over Finite Fields. http://math.uchicago.edu/may/REU2014/REUPapers/Li,Ang.pdf

[21] Silverman, J. (2009) The Arithmetic of Elliptic Curves, GTM. Springer. https://doi.org/10.1007/978-0-387-09494-6

[22] Lemmermeyer, F. (2000) Reciprocity Laws: From Euler to Eisenstein. Springer Monographs in Mathematics. https://doi.org/10.1007/978-3-662-12893-0

[23] Tian, Y. Lectures on Algebraic Number Theory. http://www.math.uni-bonn.de/people/tian/ANT.pdf

[24] Ash, A. and Gross, R. (2006) Fearless Symmetry: Exposing the Hidden Patterns of Numbers. Princeton University Press.

[25] CoCalc, A.K.A. SAGE, Collaborative Calculation in the Cloud. https://cocalc.com/app

Appendix. SAGE/CoCalc Programs

Programs for computing the Weil zeros of $EC: y^2 = x^3 + D$ are available from [18]. They can be easily adapted to other cases, for example to Riemann Surfaces or Fermat Curves. The programs can also be used to compute Jacobi sums, and for other Algebraic Number Theory studies using technology.