JP Journal of Algebra, Number Theory and Applications
Volume 17, Number 2, 2010, Pages 97-116
Published Online: September 6, 2010
This paper is available online at http://pphmj.com/journals/jpanta.htm

L-FUNCTIONS ATTACHED TO SEMIDIRECT PRODUCTS ARISING IN THE THEORY OF FIELDS

A. E. ÖZLÜK and C. SNYDER

Department of Mathematics and Statistics
University of Maine
Orono, ME 04469, U. S. A.
e-mail: ali.ozluk@umit.maine.edu
chip.snyder@umit.maine.edu

Abstract

We consider *L*-functions and zeta functions attached to finite groups. In particular, we study various semidirect products of the multiplicative group of a finite field acting on its additive group. We define *L*-functions and zeta functions with respect to number fields using the zeta and *L*-functions of groups attached to the residue class fields as factors in the Euler product. We then examine some of their analytic properties.

1. Introduction

This project was inspired by an idea of Cahit Arf (1910-1997). Arf's plan was to start with a finite field and consider the representations of the semidirect product of its multiplicative group acting on its additive group by multiplication and then create some sort of "*L*-function" attached to these representations. Arf then thought of extending this procedure to local fields, in particular finite extensions of the *p*-adic rationals. Finally, he envisioned using the previous information to construct a zeta function of a global field, e.g. the field of rationals.

2010 Mathematics Subject Classification: 11M41.
Keywords and phrases: *L*-functions, zeta functions, finite groups, semidirect products.
Received March 1, 2010

However, Arf never formalized this programme and, as far as we are aware, did not publish anything on this topic; see his collected works [1]. The purpose of this note is to take a modest first step in this programme in the case of finite fields. We consider all semidirect products of the multiplicative group of a finite field acting on its additive group and determine which, up to isomorphism, arise as the action of field multiplication. Using ideas in Artin's papers on (non-abelian) *L*-functions, we then construct *L*-functions and zeta functions attached, first to arbitrary finite groups, and then to our semidirect products. For a different, more general, approach to *L*-series attached to finite groups, see Lang's article, [4], and in his text, [5], Exercise 8 of Chapter XVIII.

At this point we come to the real novelty of this note. Again inspired by Artin's works, we define a global zeta function as an Euler product of the (reciprocals of) our zeta functions for finite fields. The reason for constructing these global zeta functions is that it takes into account the relation between multiplication and addition on the finite fields. We are then able to relate some analytic results about these zeta functions to information about the semidirect products. See the theorem below for more details.

2. Some Semidirect Products

For general information on semidirect products, see for example the nice presentation in Dummit and Foote's text, [3].

Let *p* be a prime. Let $H = \langle b \rangle \simeq C(p)$ and let $K = \langle a \rangle \simeq C(p-1),$ where $C(n)$ denotes any cyclic group of order *n*. (Unless otherwise noted, we shall write our groups multiplicatively.) Notice that the group of automorphisms of *H*, $\mathrm{Aut}(H)$ $= \{\vartheta_j \mid j = 1, \ldots, p-1\} \simeq C(p-1)$ where $\vartheta_j(b) = b^j.$ But then there are $p-1$ homomorphisms from *K* into $\mathrm{Aut}(H),$ namely $\varphi_j : K \to \mathrm{Aut}(H)$ given by $a \mapsto \vartheta_j$ for $j = 1, \ldots, p-1.$ Each of these homomorphisms determines a semidirect product $H \rtimes_{\varphi_j} K$ with the presentation

$$\langle a, b \mid a^{p-1} = b^p = 1, aba^{-1} = b^j \rangle.$$

We now consider which of these $p-1$ groups are isomorphic. To this end, we start with the following proposition.

Proposition 1. *Let* $H_1, \ H_2, \ K_1, \ K_2$ *be groups and* $\varphi_i : K_i \to \mathrm{Aut}(H_i)$ *homomorphisms for* $i = 1, 2.$ *Suppose that* $\psi_H : H_1 \to H_2$ *and* $\psi_K : K_1 \to K_2$ *are isomorphisms*. *Furthermore, let* $\psi_H^* : \mathrm{Aut}(H_2) \to \mathrm{Aut}(H_1)$ *be given by* $\vartheta_2 \mapsto \psi_H^{-1}\vartheta_2\psi_H.$ *Then*

$$(\psi_H, \psi_K) : H_1 \rtimes_{\varphi_1} K_1 \to H_2 \rtimes_{\varphi_2} K_2$$

given by

$$(h, k) \mapsto (\psi_H(h), \psi_K(k))$$

is an isomorphism if and only if

$$\varphi_1 = \Psi_H^* \circ \varphi_2 \circ \psi_K.$$

(The φ_j in this proposition should not be confused with those in the previous paragraph.)

The proof is straightforward and left to the reader.

We apply this proposition to the examples above. Suppose that (ψ_H, ψ_K) is an isomorphism of $H \rtimes_{\varphi_j} K$ onto $H \rtimes_{\varphi_i} K.$ Say $\psi_K(a) = a^n$ for some *n* relatively prime to $p - 1,$ and $\psi_H(b) = b^m$ for some *m* relatively prime to *p*. Hence by the proposition, $b^j = \varphi_j(a)(b) = \psi_H^*\varphi_i\psi_K(a)(b).$ But

$$\psi_H^*\varphi_i\psi_K(a)(b) = b^{i^n}$$

as can be see by a simple calculation. Since $(n, \ p - 1) = 1,$ we see that *i* and *j* must have the same order mod *p* and conversely.

This argument shows that if *i* and *j* are not of the same order mod *p*, then there is no isomorphism of the type given in Proposition 1 between $H \rtimes_{\varphi_i} K$ and $H \rtimes_{\varphi_j} K.$ However, we have not as yet ruled out the possibility of a more general type of isomorphism between these two groups.

We now claim that this possibility cannot occur. For suppose that $\psi : H \rtimes_{\varphi_i} K \to H \rtimes_{\varphi_j} K$ is an isomorphism. Then notice that $\psi(H \times \langle 1 \rangle) = H \times \langle 1 \rangle,$ since $H \times \langle 1 \rangle$ is the unique *p*-Sylow subgroup of the two semidirect products, for recall that this subgroup is normal in the two semidirect products. The next theorem then shows that there exists an isomorphism of the type described in Proposition 1.

Proposition 2. *Suppose that* $\psi : H_1 \rtimes_{\varphi_1} K_1 \to H_2 \rtimes_{\varphi_2} K_2$ *is an isomorphism such that* $\psi(H_1 \times \langle 1 \rangle) = H_2 \times \langle 1 \rangle$. *Then there exist isomorphisms* $\psi_H : H_1 \to H_2$ *and* $\psi_K : K_1 \to K_2$ *such that the mapping* $(\psi_H, \psi_K) : H_1 \rtimes_{\varphi_1} K_1 \to H_2 \rtimes_{\varphi_2} K_2$ *given by* $(\psi_H, \psi_K)(h_1, k_1) = (\psi_H(h_1), \psi_K(k_1))$ *is an isomorphism*.

Once again we leave the proof to the reader.

As above let $H = \langle b \rangle \simeq C(p)$ and $K = \langle a \rangle \simeq C(p-1)$ for *p* a prime. Let *g* be a primitive root modulo *p*. Let $\varphi : K \to \text{Aut}(H)$ be the group homomorphism given by $a \mapsto \varphi_a$, where $\varphi_a(b) = b^{g^m}$, for some $m \in \{1, ..., p-1\}$. Let *d* be a positive divisor of $p-1$. Finally, let

$$G = HK = H \rtimes_d K = \langle a, b \,|\, a^{p-1} = b^p = 1, aba^{-1} = b^{g^d} \rangle.$$

Notice that we have interpreted this construction as an internal semidirect product. However, we shall also consider this product externally as

$$H \rtimes_d K = \{(b^\nu, a^\mu) \,|\, \mu = 1, ..., p-1, \nu = 1, ..., p\},$$

where the group operation is given by

$$(\beta, \alpha) * (\beta', \alpha') = (\beta\varphi_a(\beta'), \alpha\alpha'),$$

with $\varphi_a(b) = b^{g^d}$.

In particular, if $\mathbb{F}_p$ is the prime field of order *p*, then

$$\mathbb{F}_p^+ \rtimes_\mu \mathbb{F}_p^\times \simeq H \rtimes_1 K,$$

where μ is the homomorphism given by the field multiplication, i.e., $\mu : \mathbb{F}_p^\times \to \text{Aut}(\mathbb{F}_p^+)$ with $\mu(\alpha)(\beta) = \alpha\beta$. (Notice that we have characterized $\mathbb{F}_p^+ \rtimes_\mu \mathbb{F}_p^\times$ in the family of all semidirect products of the form $\mathbb{F}_p^+ \rtimes_\varphi \mathbb{F}_p^\times$).

On the other hand, we see

$$H \rtimes_{p-1} K \simeq H \oplus K \simeq C(p(p-1)).$$

More generally we now determine the isomorphism classes of semidirect products of the additive and multiplicative groups of an arbitrary finite field, $\mathbb{F}_q$ of order p^m, p is a prime. To this end, let H be isomorphic to $\mathbb{F}_q^+$. Hence $H \simeq C(p)^m$, the direct sum of m copies of $C(p)$. Moreover, let $K = \langle a \rangle \simeq C(q-1) \simeq \mathbb{F}_q^\times$.

Next, let $\varphi : K \to \mathrm{Aut}(H) \simeq GL_m(\mathbb{F}_p)$, be a homomorphism and let the semidirect product of H with K with respect to φ be $H \rtimes_\varphi K$. Finally, if M and N are subgroups of some group G, we write $M \sim N$ to mean that M and N are conjugate subgroups, i.e., $N = gMg^{-1}$ for some $g \in G$.

Proposition 3. *Let* $H \simeq C(p)^m$ *and* $K \simeq C(p^m - 1)$, *say* $K = \langle a \rangle$, *for some prime p. Let* $\varphi_j : K \to \mathrm{Aut}(H)$ *be homomorphisms for* $j = 1, 2$. *Then*

$$H \rtimes_{\varphi_1} K \simeq H \rtimes_{\varphi_2} K \quad \textit{iff} \quad \langle \varphi_1(a) \rangle \sim \langle \varphi_2(a) \rangle.$$

Proof. Suppose $\psi : H \rtimes_{\varphi_1} K \to H \rtimes_{\varphi_2} K$ is an isomorphism. Since H is the unique p-Sylow subgroup in the semidirect product, we see $\psi(H) = H$. Hence by Proposition 2 there are automorphisms ψ_H and ψ_K of H and K such that $(\psi_H, \psi_K) : H \rtimes_{\varphi_1} K \to H \rtimes_{\varphi_2} K$ is an isomorphism. But then $\varphi_1 = \psi_H^* \circ \varphi_2 \circ \psi_K$. This implies $\varphi_1(a) = \psi_H^* \varphi_2(\psi_K(a)) = \psi_H^{-1} \varphi_2(\psi_K(a)) \psi_H = \psi_H^{-1} \varphi_2(a)^k \psi_H$, for some $(k, p^m - 1) = 1$. Therefore, $\langle \varphi_1(a) \rangle \sim \langle \varphi_2(a) \rangle$.

The converse follows by reversing the argument. □

We now determine which homomorphisms on K yield semidirect products isomorphic to $\mathbb{F}_q^+ \rtimes_\mu \mathbb{F}_q^\times$, where μ is given by multiplication in $\mathbb{F}_q$.

Proposition 4. *Let* $\mathbb{F}_q$ *be a finite field of order* $q = p^m$, p *be a prime. Let* $\mu : \mathbb{F}_q^\times \to \mathrm{Aut}(\mathbb{F}_q^+)$ *be the homomorphism determined by multiplication in the field. Moreover, assume* $\varphi : \mathbb{F}_q^\times \to \mathrm{Aut}(\mathbb{F}_q^+)$ *is any homomorphism. Then*

$$\mathbb{F}_q^+ \rtimes_\varphi \mathbb{F}_q^\times \simeq \mathbb{F}_q^+ \rtimes_\mu \mathbb{F}_q^\times$$

if and only if $|\varphi(a)| = q - 1$, *where a is any generator of* $\mathbb{F}_q^\times$.

Proof. For starters notice that $|\mu(a)| = q-1$. Hence by the previous proposition $|\varphi(a)| = q-1$. Now let us identify $\mathrm{Aut}(\mathbb{F}_q^+)$ with $GL_m(\mathbb{F}_p)$. It suffices to show that all cyclic subgroups $\langle A \rangle$ of order $q-1$ in $GL_m(\mathbb{F}_p)$ are conjugate. To this end, let $p_A(x) = \det(Ix - A)$ be the characteristic polynomial of A. Hence $p_A(x)$ is a polynomial in $\mathbb{F}_p[x]$ of degree m. But since $|A| = q-1$, we claim that $p_A(x)$ is irreducible in $\mathbb{F}_p[x]$ for otherwise $p_A(x) = \prod_{i=1}^{r} p_i(x)^{n_i}$ for some r, $n_i \in \mathbb{N}$ and irreducible $p_i(x) \in \mathbb{F}_p[x]$ of degree $m_i < m$. Notice then that $m = \sum_i n_i m_i$. Now let α_i be a root of $p_i(x)$. Hence A is similar to the matrix $((\alpha_i^{(j)} I_{m_i})^{n_i})$, where $(\alpha_i^{(j)} I_{m_i})^{n_i}$ is the block diagonal matrix with n_i copies of $\alpha_i^{(j)} I_{m_i}$ on the main diagonal, with $\alpha_i^{(j)} I_{m_i}$ the m_i by m_i diagonal matrix for which $\alpha_i^{(j)}$ are on the main diagonal and where $\alpha_i^{(j)}$ are the conjugates of α_i over $\mathbb{F}_p$. Since conjugate elements have the same multiplicative order, we see that $|A| = \mathrm{lcm}(|\alpha_i| : i = 1, \ldots, r)$. Hence

$$|A| \leq \prod_{i=1}^{r} |\alpha_i| \leq \prod_{i=1}^{r} (p^{m_i} - 1) < p^m - 1 = |A|$$

a contradiction. Thus $p_A(x)$ is irreducible. If β is a root of this polynomial, then $\beta \in \mathbb{F}_q$. Since $\mathbb{F}_q/\mathbb{F}_p$ is a Galois extension, $p_A(x)$ splits in distinct factors in $\mathbb{F}_q[x]$. Hence A is conjugate to a diagonal matrix with an element (and all its conjugates) of order $q-1$ in $\mathbb{F}_q^\times$. Now, if A and A' are two matrices of order $q-1$, then A and A' are conjugate to diagonal matrices with the element α^n and $\alpha^{n'}$, respectively in the upper left corner, where here n and n' are relatively prime to $q-1$ and where α is some fixed primitive $q-1$st root of unity. But then the subgroups $\langle A \rangle$ and $\langle A' \rangle$ are conjugate, as desired. □

3. *L*-functions and the Zeta-function of a Finite Group

Let G be a finite group of order $n = |G|$. Let ϱ be a complex linear representation of G of finite degree, $\deg \varrho$. See [3] or [6] for background on linear representations. We define the L-function of G with respect to ϱ by

$$L_G(X, \varrho) = \prod_{g \in G} \det(I - \varrho(g) x_g)^{1/|G|},$$

where $\det(I - \varrho(g)x)$ is the characteristic polynomial of $\varrho(g)$ and $X = X_G = (x_g)_{g \in G}$ is an n-tuple of independent variables. This definition is motivated by Artin's work on *L*-functions, see [2].

Moreover, we define the zeta function of *G* by

$$\zeta_G(X) = \prod_{\varrho \in \hat{G}} L_G(X, \varrho)^{\deg(\varrho)},$$

where $\hat{G}$ is a maximal set of inequivalent irreducible representations of *G*.

Now notice that for representations ϱ_i $(i = 1, 2)$ of *G* we have

$$L_G(X, \varrho_1 \oplus \varrho_2) = L_G(X, \varrho_1) L_G(X, \varrho_2),$$

because $\det(I - (\varrho_1 \oplus \varrho_2)(g)x) = \det(I - \varrho_1(g)x)\det(I - \varrho_2(g)x)$.

Therefore, we have the following relation

$$\zeta_G(X) = L_G(X, \varrho_{\text{reg}}),$$

where ϱ_{reg} is the regular representation on *G*, because $\varrho_{\text{reg}} = \sum_{\varrho \in \hat{G}} (\deg \varrho)\varrho$.

We now write $\log L_G(X, \varrho)$ in terms of the character $\chi = \chi_\varrho$ of ϱ. To this end consider ϱ as a matrix representation of degree *d*; we thus have (up to conjugation)

$$\varrho(g) = \begin{pmatrix} \varepsilon_1 & & 0 \\ & \ddots & \\ 0 & & \varepsilon_d \end{pmatrix},$$

where the ε_i are the eigenvalues of $\varrho(g)$ and hence *n*th-roots of unity. Thus for each $g \in G$ letting $x_g = z_g$ be a complex number of modulus less than 1, we have

$$\log \det(I - \varrho(g) z_g) = \sum_{j=1}^{d} \log(1 - \varepsilon_j z_g) = -\sum_{j=1}^{d} \sum_{m=1}^{\infty} \frac{1}{m} \varepsilon_j^m z_g^m$$

$$= -\sum_{m=1}^{\infty} \frac{1}{m} \left(\sum_{j=1}^{d} \varepsilon_j^m \right) z_g^m = -\sum_{m=1}^{\infty} \frac{1}{m} \chi(g^m) z_g^m.$$

Therefore,

$$\log L_G(X, \varrho) = -\frac{1}{|G|}\sum_{g\in G}\sum_{m=1}^{\infty}\frac{1}{m}\chi(g^m)x_g^m.$$

We now have the following result.

Proposition 5. *Let G be a finite group of order* $n = |G|$. *Then*

$$\zeta_G(X) = \prod_{g\in G}(1 - x_g^{|g|})^{\frac{1}{|g|}}.$$

Proof. Recall that

$$\chi_{\text{reg}}(g) = \begin{cases} n, & \text{if } g = 1, \\ 0, & \text{otherwise.} \end{cases}$$

Without loss of generality we assume $x_g = z_g$, where z_g is complex of modulus less than 1. Then

$$\log\zeta_G(X) = \log L_G(X, \varrho_{\text{reg}}) = -\frac{1}{n}\sum_{g\in G}\sum_{m=1}^{\infty}\frac{1}{m}\chi_{\text{reg}}(g^m)z_g^m = -\sum_{g\in G}\sum_{\substack{m=1\\ g^m=1}}^{\infty}\frac{1}{m}z_g^m$$

$$= -\sum_{g\in G}\sum_{t=1}^{\infty}\frac{1}{|g|t}z_g^{|g|t}\sum_{g\in G}\frac{1}{|g|}\log(1 - z_g^{|g|}) = \log\prod_{g\in G}(1 - z_g^{|g|})^{1/|g|},$$

which proves the result. □

We isolate another result which is analogous to the classical case of Artin L-functions, see [2].

Proposition 6 (Restriction)**.** *Suppose* $\eta : G \to H$ *is an epimorphism of finite groups. Let* ϱ *be a representation on H. Then*

$$L_H(X_H, \varrho) = L_G(\eta X_G, \varrho\circ\eta),$$

where $\eta X_G = (x_{\eta(g)})_{g\in G}$.

Proof. This follows since

$$L_G(\eta X_G, \varrho\circ\eta)^{|G|} = \prod_{g\in G}\det(I - \varrho(\eta(g))x_{\eta(g)}) = \prod_{h\in H}\det(I - \varrho(h)x_h)^{[G:H]}. \ \square$$

4. The Zeta Function of Some Groups Associated with Finite Fields

We now come to the computation of the zeta function of some groups associated with finite fields. In particular we consider the semidirect products considered earlier; but first some general observations. We let $x_g = x,$ for all $g \in G$ and thus have

$$L_G(x, \varrho) = \prod_{g \in G} \det(I - \varrho(g)x)^{1/|G|}, \quad \zeta_G(x) = \prod_{g \in G}(1 - x^{|g|})^{1/|g|}.$$

Hence, if ϱ is the trivial representation, $\varrho = 1,$ then

$$L_G(x, 1) = 1 - x.$$

In order to compute the zeta function of a finite group, we need only determine the number of elements of the group of any given order. We first consider some simple examples.

Let $G = C(n)$ be any cyclic group of order *n*. Then for each divisor *l* of *n*, there are $\varphi(l)$ elements in *G* of order *l*. Hence the zeta function attached to *G* is given by

$$\zeta_{C(n)}(x) = \prod_{l \mid n}(1 - x^l)^{\frac{\varphi(l)}{l}}.$$

In particular if $G = \mathbb{F}_q^{\times} \simeq C(q - 1),$ then the zeta function attached to *G* is given by

$$\zeta_{\mathbb{F}_q^{\times}}(x) = \prod_{l \mid q-1}(1 - x^l)^{\frac{\varphi(l)}{l}}.$$

As another simple example, consider $G = \mathbb{F}_q^{+},$ with $q = p^m,$ p is a prime. Hence $G \simeq C(p)^m.$ Then notice that for each $a \in \mathbb{F}_q$

$$|a| = \begin{cases} 1, & \text{if } a = 0, \\ p, & \text{otherwise.} \end{cases}$$

Thus the zeta function is given by

$$\zeta_{\mathbb{F}_q^{+}}(x) = (1 - x)(1 - x^p)^{\frac{q-1}{p}}.$$

Next, we now carry this computation out for the various semidirect products which we have associated with $\mathbb{F}_p$:

$$G = C(p) \rtimes_d C(p-1) = \mathbb{F}_p^{+} \rtimes_d \mathbb{F}_p^{\times} = \langle a, b \,|\, a^{p-1} = b^{p} = 1, aba^{-1} = b^{g^d} \rangle$$

$$= \{b^i a^j \,|\, i = 1, \dots, p;\ j = 1, \dots, p-1\},$$

for $\mathbb{Z}_p^{\times} = \langle g \rangle$ and $d \,|\, p-1$.

We start with a lemma.

Lemma 1. *Let* $G = \mathbb{F}_p^{+} \rtimes_d \mathbb{F}_p^{\times}$. *Then for any integers* i, j, μ,

$$(b^i a^j)^{\mu} = \begin{cases} b^{i(g^{\mu jd}-1)/(g^{jd}-1)} a^{\mu j} & \textit{if } dj \not\equiv 0 \bmod p-1, \\ b^{i\mu} a^{\mu j} & \textit{otherwise.} \end{cases}$$

Proof. Let $de = p-1$. Notice that $a^e b^i a^{-e} = b^{ig^{de}} = b^i$. Hence $a^e \in Z$, the center of G. Thus $(b^i a^{ej})^{\mu} = b^{i\mu} a^{\mu ej}$, which establishes the lemma for $dj \equiv 0 \bmod p-1$. Now suppose $dj \not\equiv 0 \bmod p-1$. Notice the lemma is trivially true for $\mu = 1$. Suppose it is true for $\mu - 1$. Then

$$(b^i a^j)^{\mu} = (b^i a^j)^{\mu-1} b^i a^j = b^{i(g^{(\mu-1)jd}-1)/(g^{jd}-1)} a^{(\mu-1)j} b^i a^j$$

$$= b^{i(g^{(\mu-1)jd}-1)/(g^{jd}-1)} a^{(\mu-1)j} b^i a^{-(\mu-1)j} a^{\mu j}$$

$$= b^{i(g^{(\mu-1)jd}-1)/(g^{jd}-1)+ig^{(\mu-1)jd}} a^{\mu j} = b^{i(g^{\mu jd}-1)/(g^{jd}-1)} a^{\mu j},$$

as desired. □

From this we further obtain the following

Lemma 2. *Let* $G = \mathbb{F}_p^{+} \rtimes_d \mathbb{F}_p^{\times}$. *Then*

$$|\, b^i a^j \,| = \begin{cases} \dfrac{p(p-1)}{(j,\ p-1)}, & \textit{if } i \not\equiv 0 \bmod p,\ dj \equiv 0 \bmod p-1, \\ \dfrac{p-1}{(j,\ p-1)}, & \textit{if } dj \not\equiv 0 \bmod p-1 \ \textit{ or } \ (dj \equiv 0 \bmod p-1,\ i \equiv 0 \bmod p). \end{cases}$$

Proof. Suppose $p-1 \mid dj$. Then $(b^i a^j)^\mu = b^{i\mu} a^{j\mu}$. Hence if $(b^i a^j)^\mu = 1$, then either (i) $p \nmid i$, $p \mid \mu$, and $p-1 \mid j\mu$, or (ii) $p \mid i$ and $p-1 \mid j\mu$. For (i), $| b^i a^j | = \frac{p(p-1)}{(j,\ p-1)}$, and for (ii), $| b^i a^j | = \frac{p-1}{(j,\ p-1)}$.

Now, suppose $p-1 \nmid dj$. If $(b^i a^j)^\mu = b^{i(g^{\mu dj}-1)/(g^{dj}-1)} a^{j\mu} = 1$, then $p-1 \mid \mu j$. Hence $| b^i a^j | = \frac{p-1}{(j,\ p-1)}$. □

From this result we have

Lemma 3. *Let* $G = \mathbb{F}_p^+ \rtimes_d \mathbb{F}_p^\times$. *Then the following table gives the orders of all the elements of G and the number of elements of a given order*:

order $= l$	*if* $l \mid pd$	*if* $l \mid p-1,\ l \nmid d$
no. of elements	$\varphi(l)$	$p\varphi(l)$

Proof. As before, let $de = p-1$. Notice from the previous lemma that if $p \nmid i$ and $e \mid j$, then

$$| b^i a^j | = \frac{pd}{(j/e,\ d)}.$$

Otherwise $| b^i a^j | = \frac{p-1}{(j,\ p-1)}$. Hence if $l \mid pd$, then there are $\varphi(l)$ elements with order l. If, on the other hand, $l \mid p-1$ but $l \nmid d$, then there are $p\varphi(l)$ such elements. □

From this we have the following proposition.

Proposition 7. *Let* $G = \mathbb{F}_p^+ \rtimes_d \mathbb{F}_p^\times$, *where* $d \mid p-1$. *Then*

$$\zeta_G(x) = \prod_{l \mid pd} (1-x^l)^{\frac{\varphi(l)}{l}} = \prod_{\substack{l \mid p-1 \\ l \nmid d}} (1-x^l)^{\frac{p\varphi(l)}{l}}.$$

In particular, for $G = \mathbb{F}_p^+ \rtimes_\mu \mathbb{F}_p^\times = C(p) \rtimes_1 C(p-1)$,

$$\zeta_G(x) = (1-x)(1-x^p)^{\frac{p-1}{p}} \prod_{1 \neq l \mid p-1} (1-x^l)^{\frac{p\varphi(l)}{l}},$$

whereas if $G = \mathbb{F}_p^+ \rtimes_{p-1} \mathbb{F}_p^\times = C(p) \oplus C(p-1),$ *then*

$$\zeta_G(x) = \prod_{l \mid p(p-1)} (1 - x^l)^{\frac{\varphi(l)}{l}}.$$

We now compute the zeta function of a semidirect product of the additive and multiplicative groups of an arbitrary finite field $\mathbb{F}_q$ of order *q*, where $q = p^m$, p is a prime. Then the additive group $\mathbb{F}_q^+$ is isomorphic to $H = C(p)^m$; while $\mathbb{F}_q^+ \simeq K = C(q-1)$. We shall present $H = C(p)^m$ multiplicatively as

$$H = \langle b_1, \dots, b_m : b_i^p = 1, b_i b_j = b_j b_i, \; i, \; j = 1, \dots, m \rangle,$$

and *K* generated by *a*, say.

Now, let $\varphi : K \to \mathrm{Aut}(H)$ be a group homomorphism, determined by $a \mapsto \varphi_a$. Since $\mathrm{Aut}(H) \simeq GL_m(\mathbb{F}_p)$, we identify φ_a with a matrix $A \in GL_m(\mathbb{F}_p)$ given as follows:

Write $\underline{b}^{\underline{\nu}} = b_1^{\nu_1} \cdots b_m^{\nu_m}$, where $\underline{\nu} = (\nu_1, \dots, \nu_m)^t \in \mathbb{F}_p^m$; then $\varphi_a(\underline{b}^{\underline{\nu}}) = \underline{b}^{A\underline{\nu}}$. Now, let $G = H \rtimes_\varphi K = H \rtimes_A K$ with *H* and *K* as above. Hence *G* can be presented as

$$G = \langle b_1, \dots, b_m, a \,|\, b_i^p = a^{q-1} = 1, b_i b_j = b_j b_i, a\underline{b}^{\underline{\nu}} a^{-1} = \underline{b}^{A\underline{\nu}} \rangle.$$

Next, we study some properties of the matrix *A*. First notice that the order of *A*, $|A|$, divides $q-1$. Now factor the characteristic polynomial $p_A(x) = \det(Ix - A) = \prod_{i=1}^r p_i(x)^{n_i}$ for some positive integers r, n_i and $p_i(x)$ distinct irreducible polynomials in $\mathbb{F}_p[x]$ and with the degree of $p_i(x)$ equal to m_i, say. We know that $p_A(x)$ factors into linear factors in $\overline{\mathbb{F}}_p$, an algebraic closure of $\mathbb{F}_p$. Hence

$$p_i(x) = \prod_{j=1}^{m_i} (x - \alpha_i^{(j)}),$$

where $\mathbb{F}_{p^{m_i}} = \mathbb{F}_p(\alpha_i)$ and $\alpha_i^{(j)}$ range over all the conjugates of α_i over $\mathbb{F}_p$. But then *A* is similar to the diagonal matrix $((\alpha_i^{(j)} I_{m_i})^{(n_i)}) \in GL_m(\overline{\mathbb{F}}_p)$, where

$((\alpha_i^{(j)} I_{m_i})^{(n_i)})$ is as above. Hence $|A| = \mathrm{lcm}(|\alpha_i|)$. In particular, $|\alpha_i|$ divides $|A|$, and therefore, $\alpha_i \in \mathbb{F}_q^{\times}$. From this we see that *A* is similar to a diagonal matrix in $GL_m(\mathbb{F}_q)$.

Now, for some notation. If $M \in GL_m(\mathbb{F}_p)$, then let $\mathcal{N}(M)$ be the null space of *M*, i.e., $\mathcal{N}(M) = \{\underline{\nu} \in \mathbb{F}_p^m \mid M\underline{\nu} = \underline{0}\}$. In particular, if μ is an integer, then let $d_\mu = d(\mu) = \dim \mathcal{N}(A^\mu - I)$, where *A* is given above. Hence $d(\mu)$ is the dimension of the eigenspace of A^μ in $\mathbb{F}_p^m$ associated with the eigenvalue 1.

We now compute the orders of the elements in $G = H \rtimes_A K$. First notice that since $a\underline{b}^{\underline{\nu}}a^{-1} = \underline{b}^{A\underline{\nu}}$, we have

$$a^\mu \underline{b}^{\underline{\nu}} a^{-\mu} = \underline{b}^{A^\mu \underline{\nu}}.$$

Therefore,

$$(\underline{b}^{\underline{\nu}} a^\mu)^n = \underline{b}^{(I + A^\mu + \cdots + A^{\mu(n-1)})\underline{\nu}} a^{\mu n},$$

for any positive integer *n*, as can easily be seen by induction on *n*.

Next, let $\langle \cdot, \cdot \rangle$ be the standard inner product on $\mathbb{F}_p^m$. For any integer μ, we may decompose $\mathbb{F}_p^m$ as

$$\mathbb{F}_p^m = \mathcal{N}(A^\mu - I) \oplus \mathcal{N}(A^\mu - I)^\perp.$$

Thus, if $\underline{\nu} \in \mathbb{F}_p^m$, then $\underline{\nu} = \underline{\nu}_1 + \underline{\nu}'$ for unique $\underline{\nu}_1 \in \mathcal{N}$ and $\underline{\nu}' \in \mathcal{N}^\perp$. Using this decomposition of $\underline{\nu}$, notice that

$$(\underline{b}^{\underline{\nu}} a^\mu)^n = \underline{b}^{n\underline{\nu}_1} \underline{b}^{(I + A^\mu + \cdots + A^{\mu(n-1)})\underline{\nu}'} a^{\mu n},$$

since $\underline{\nu}_1 \in \mathcal{N}(A^\mu - I)$, and thus $A^\mu \underline{\nu}_1 = \underline{\nu}_1$.

From this we can prove the following

Lemma 4.

$$(\underline{b}^{\underline{\nu}} a^\mu)^n = 1 \quad \mathit{iff} \quad \mu n \equiv 0 \bmod q - 1,\ n\underline{\nu}_1 = \underline{0}\ (\mathit{in}\ \mathbb{F}_p^m).$$

Proof. Suppose $(\underline{b}^{\underline{\nu}}a^{\mu})^n = 1.$ From above we then have

$$1 = (\underline{b}^{\underline{\nu}}a^{\mu})^n = \underline{b}^{n\underline{\nu}_1}\underline{b}^{(I+A^{\mu}+\cdots+A^{\mu(n-1)})\underline{\nu}'}a^{\mu n}.$$

This implies in particular that $\mu n \equiv 0 \bmod q - 1.$ But now we show that for $\mu n \equiv 0 \bmod q - 1,$

$$\underline{b}^{(I+A^{\mu}+\cdots+A^{\mu(n-1)})\underline{\nu}'} = 1.$$

To see this, recall from above that A is similar to a diagonal matrix $D \in GL_m(\mathbb{F}_q).$ Hence we see that $A^{\mu} = B^{-1}D^{\mu}B$ for some B, where

$$D^{\mu} = \begin{pmatrix} I_{d(\mu)} & 0 \\ 0 & D' \end{pmatrix},$$

where D' is diagonal with elements of the form $\beta_i^{\mu} \neq 1,$ for some $\beta_i \in \mathbb{F}_q,$ on the main diagonal. From this we see

$$I + A^{\mu} + \cdots + A^{\mu(n-1)} = B^{-1}\begin{pmatrix} nI_{d(\mu)} & 0 \\ 0 & (1+\beta_i^{\mu} + \cdots + \beta_i^{\mu(n-1)})\delta_{ij} \end{pmatrix}B$$

$$= B^{-1}\begin{pmatrix} nI_{d(\mu)} & 0 \\ 0 & \left(\dfrac{\beta_i^{\mu n} - 1}{\beta_i^{\mu} - 1}\right)\delta_{ij} \end{pmatrix}B = B^{-1}\begin{pmatrix} nI_{d(\mu)} & 0 \\ 0 & 0 \end{pmatrix}B,$$

when $\mu n \equiv 0 \bmod q - 1.$ But then again for $\mu n \equiv 0 \bmod q - 1,$ we have

$$(I + A^{\mu} + \cdots + A^{\mu(n-1)})\underline{\nu}' = B^{-1}\begin{pmatrix} nI_{d(\mu)} & 0 \\ 0 & 0 \end{pmatrix}B\underline{\nu}'$$

$$= B^{-1}\begin{pmatrix} nI_{d(\mu)} & 0 \\ 0 & 0 \end{pmatrix}(0, \ldots, 0, \nu'_{d(\mu)+1}, \ldots, \nu'_m)^t = \underline{0},$$

as desired.

Summarizing we have that if $(\underline{b}^{\underline{\nu}}a^{\mu})^n = 1,$ then $\mu n \equiv 0 \bmod q - 1$ and $\underline{b}^{n\underline{\nu}_1} = 1.$ Therefore, $\mu n \equiv 0 \bmod q - 1$ and $n\underline{\nu}_1 = \underline{0}.$

The converse follows easily from this argument. □

From this we immediately obtain

Proposition 8. *Let* $G = C(p)^m \rtimes_A C(q-1)$ *be as above. Then*

$$|\,\underline{b}^{\underline{\nu}}a^{\mu}\,| = \begin{cases} \dfrac{p(q-1)}{(\mu,\ q-1)} & \textit{if}\ \ \underline{\nu}_1 \neq \underline{0}, \\[2ex] \dfrac{(q-1)}{(\mu,\ q-1)} & \textit{if}\ \ \underline{\nu}_1 = \underline{0}, \end{cases}$$

where $\underline{\nu} = \underline{\nu}_1 + \underline{\nu}'$ *with* $\underline{\nu}_1 \in \mathcal{N}(A^{\mu} - I)$ *and* $\underline{\nu}' \in \mathcal{N}(A^{\mu} - I)^{\perp}$.

Now, we can finally count the number of elements in *G* of any given order. To this end, let $N(k)$ be the number of elements of *G* of order *k*. Then we have

Proposition 9. *Let* $G = C(p)^m \rtimes_A C(q-1)$ *be as above. Then the order of any element divides* $p(q-1)$. *Moreover, if* $l \,|\, q-1$, *then*

$$N(pl) = \varphi(l)(p^m - p^{m-d((q-1)/l)}) \ \textit{and}\ \ N(l) = \varphi(l)(p^{m-d((q-1)/l)}),$$

where $d(\mu) = \dim \mathcal{N}(A^{\mu} - I)$.

Proof. By the previous proposition notice that for any given μ

$$N\left(\frac{p(q-1)}{\mu,\ q-1}\right) = p^m - p^{m-d(\mu)} \ \text{ and }\ N\left(\frac{q-1}{(\mu,\ q-1)}\right) = p^{m-d(\mu)}.$$

Also, notice that if $(\mu,\ q-1) = (\mu',\ q-1)$, then $d(\mu) = d(\mu')$. Moreover,

$$\#\{\mu' \bmod q-1 \,|\, (\mu,\ q-1) = (\mu',\ q-1)\} = \varphi\left(\frac{q-1}{(\mu,\ q-1)}\right).$$

Hence if $\dfrac{q-1}{(\mu,\ q-1)} = l$, then the cardinality of the above set is $\varphi(l)$. From this and the above arguments the proposition follows easily. □

From this we immediately obtain the following

Proposition 10. *Let* $G = C(p)^m \rtimes_A C(q-1)$. *Then*

$$\zeta_G(x) = \prod_{l\,|\,q-1} (1 - x^{pl})^{\frac{\varphi(l)}{pl}(p^m - p^{m-d((q-1)/l)})}(1 - x^{l})^{\frac{\varphi(l)}{l}(p^{m-d((q-1)/l)})},$$

with $d(\mu) = \dim \mathcal{N}(A^{\mu} - I)$.

In particular, if $G = \mathbb{F}_q^+ \rtimes_\mu \mathbb{F}_q^\times$, *then*

$$\zeta_G(x) = (1-x)(1-x^p)^{\frac{q-1}{p}} \prod_{1 \neq l \mid q-1} (1-x^l)^{\frac{q\varphi(l)}{l}},$$

whereas if $G = \mathbb{F}_q^+ \oplus \mathbb{F}_q^\times$, *then*

$$\zeta_G(x) = \prod_{l \mid q-1} (1-x^{pl})^{\frac{\varphi(l)}{pl}(q-1)}(1-x^l)^{\frac{\varphi(l)}{l}}.$$

We note in passing that $\zeta_{\mathbb{F}_q^\times}(x)$ and $\zeta_{\mathbb{F}_q^+}(x)$ are both factors of the zeta function $\zeta_G(x)$ given in Proposition 10.

5. *L*-functions and Zeta Functions

In order to define our main families of *L*-functions and zeta functions, let *K* denote a number field. For each maximal ideal $\mathfrak{p}$ of $\mathfrak{o}$, the ring of integers of *K*, let $G_\mathfrak{p}$ be some finite group associated with the residue class field $\mathfrak{o}/\mathfrak{p}$ and let $\varrho_\mathfrak{p}$ be a complex linear representation on $G_\mathfrak{p}$. We formally define

$$L_K(s, \{\varrho_\mathfrak{p}\}_\mathfrak{p}) = \prod_\mathfrak{p} L_{G_\mathfrak{p}}(N\mathfrak{p}^{-s}, \varrho_\mathfrak{p})^{-1}, \quad \zeta_K^{\{G_\mathfrak{p}\}}(s) = \prod_\mathfrak{p} \zeta_{G_\mathfrak{p}}(N\mathfrak{p}^{-s})^{-1},$$

for $s \in \mathbb{C}$ and where $\mathfrak{p}$ ranges over all the maximal ideals of $\mathfrak{o}$ and so $\mathfrak{o}/\mathfrak{p}$ is a finite residue class field with $N_\mathfrak{p}$ elements.

In particular, notice that if each $\varrho_\mathfrak{p} = 1$, then

$$L_K(s, \{1\}) = \prod_\mathfrak{p} (1 - N\mathfrak{p}^{-s})^{-1} = \zeta_K(s),$$

the Dedekind zeta function of *K*, since $L_{G_\mathfrak{p}}(x, 1) = 1 - x$, as we have already seen above.

Here is an example of a zeta function. Let $G_\mathfrak{p} = (\mathfrak{o}/\mathfrak{p})^+$, the additive group of the residue class field $\mathfrak{o}/\mathfrak{p} = \mathbb{F}_{N\mathfrak{p}}$. Then

$$\zeta_K^{\{G_\mathfrak{p}\}}(s) = \prod_{\mathfrak{p}} \zeta_{\mathbb{F}_{N\mathfrak{p}}^+}(N\mathfrak{p}^{-s})^{-1}$$

$$= \prod_{\mathfrak{p}} (1 - N\mathfrak{p}^{-s})^{-1}(1 - N\mathfrak{p}^{-ps})^{-\frac{N\mathfrak{p}-1}{p}} = \zeta_K(s)\prod_{\mathfrak{p}} (1 - N\mathfrak{p}^{-ps})^{-\frac{N\mathfrak{p}-1}{p}},$$

which is regular for $\sigma = \mathrm{Re}(s) > 1$ with a simple pole at $s = 1$, since $\zeta_K(s)$ is regular on $\sigma > 1$ with a simple pole at $s = 1$ and $\zeta^*(s) = \prod_{\mathfrak{p}} (1 - N\mathfrak{p}^{-ps})^{-\frac{N\mathfrak{p}-1}{p}}$ converges absolutely and uniformally on compact subsets of $\sigma > 0$. To see this last claim, notice that

$$\log \zeta^*(s) = \sum_{\mathfrak{p}} \sum_{m \geq 1} \frac{N\mathfrak{p} - 1}{p} \frac{1}{mN\mathfrak{p}^{mps}} \ll 1,$$

uniformly on compact subsets of $\sigma > 0$. Thus, we have

$$\mathrm{Res}_{s=1}\zeta_K^{\{\mathbb{F}_{N\mathfrak{p}}^+\}}(s) = \kappa(K)c(K, \{\mathbb{F}_{N\mathfrak{p}}^+\}),$$

where $\kappa(K)$ is the residue of $\zeta_K(s)$ at $s = 1$ and

$$c(K, \{\mathbb{F}_{N\mathfrak{p}}^+\}) = \prod_{\mathfrak{p}} (1 - N\mathfrak{p}^{-p})^{-\frac{N\mathfrak{p}-1}{p}}.$$

We note, too, that since $\zeta^*(s)$ is an absolutely convergent product for $\sigma > 0$, the zeros of $\zeta_K^{\{\mathbb{F}_{N\mathfrak{p}}^+\}}(s)$ with positive real part are precisely those of $\zeta_K(s)$. If we let $K = \mathbb{Q}$, then notice that

$$\zeta_{\mathbb{Q}}^{\{\mathbb{F}_p^+\}}(s) = \zeta(s)\prod_{p} (1 - p^{-ps})^{-\frac{p-1}{p}},$$

where $\zeta(s)$ is the Riemann zeta function. Hence its residue at $s = 1$ is the constant

$$\prod_{p} (1 - p^{-p})^{-\frac{p-1}{p}}.$$

Now, we come to a (perhaps) more important example of a zeta function of an algebraic number field K. This time let $G_{\mathfrak{p}}^{A_{\mathfrak{p}}} = \mathbb{F}_q^+ \rtimes_{A_{\mathfrak{p}}} \mathbb{F}_q^\times$ for $q = N\mathfrak{p}$ and where $A_{\mathfrak{p}}$ is some matrix (as before) for which its order $|A_{\mathfrak{p}}|$ divides $q-1$. Then

$$\zeta_K^{\{G_{\mathfrak{p}}^{A_{\mathfrak{p}}}\}_{\mathfrak{p}}}(s) = \prod_{\mathfrak{p}} \zeta_{G_{\mathfrak{p}}^{A_{\mathfrak{p}}}}(N\mathfrak{p}^{-s})^{-1}.$$

In light of Proposition 10, it is not hard to see that this zeta function converges for $\sigma > 1$.

Instead of carrying this out in general we now consider the case where $K = \mathbb{Q}$. Let $G_p^{d_p} = \mathbb{F}_p^+ \rtimes_{d_p} \mathbb{F}_p^\times$ with some $d_p \mid p-1$. Then

$$\zeta_{\mathbb{Q}}^{\{G_p^{d_p}\}}(s) = \prod_p \zeta_{G_p^{d_p}}(p^{-s})^{-1} = \prod_p \zeta_{\mathbb{F}_p^+ \rtimes_{d_p} \mathbb{F}_p^\times}(p^{-s})^{-1},$$

and so by Proposition 7,

$$\zeta_{\mathbb{Q}}^{\{G_p^{d_p}\}}(s) = \prod_p \prod_{l \mid pd_p} (1 - p^{-ls})^{-\frac{\varphi(l)}{l}} \prod_{\substack{l \mid p-1 \\ l \nmid d_p}} (1 - p^{-ls})^{-\frac{p\varphi(l)}{l}}.$$

We now have the following theorem.

Theorem 1. *For each prime p let* $G_p^{d_p} = \mathbb{F}_p^+ \rtimes_{d_p} \mathbb{F}_p^\times$ *with some* $d_p \mid p-1$. *Then the zeta function* $\zeta_{\mathbb{Q}}^{\{G_p^{d_p}\}}(s)$ *converges to a meromorphic function on* $\sigma = \mathrm{Re}(s) > 0$ *which is regular except for a pole at* $s = 1$. *This pole is simple if and only if*

$$\sum_{\substack{p \\ 2 \nmid d_p}} \frac{1}{p}$$

converges. If the sum diverges, then the order of the pole is equal to 2.

In particular, $\zeta_{\mathbb{Q}}^{\{\mathbb{F}_p^+ \oplus \mathbb{F}_p^\times\}}(s)$ *has a simple pole at* $s = 1$, *whereas* $\zeta_{\mathbb{Q}}^{\{\mathbb{F}_p^+ \rtimes_\mu \mathbb{F}_p^\times\}}(s)$ *has a double pole at* $s = 1$.

Sketch of the Proof. By Proposition 7,

$$\zeta_{\mathbb{Q}}^{\{G_p^{d_p}\}}(s) = \prod_p (1 - p^{-s})^{-1} \prod_p \prod_{1 \neq l \mid pd_p} (1 - p^{-ls})^{-\frac{\varphi(l)}{l}} \prod_{\substack{1 \neq l \mid p-1 \\ l \nmid d_p}} (1 - p^{-ls})^{-\frac{p\varphi(l)}{l}}.$$

The first product is $\zeta(s)$, the Riemann zeta function, which has a simple pole at $s = 1$. Moreover, for $\sigma = \mathrm{Re}(s)$

$$\log \frac{\zeta_{\mathbb{Q}}^{\{G_p^{d_p}\}}(\sigma)}{\zeta(\sigma)} = \sum_p \left(\sum_{1 \neq l \mid pd_p} \frac{\varphi(l)}{l} \sum_{m \geq 1} \frac{1}{mp^{ml\sigma}} + \sum_{\substack{l \mid p-1 \\ l \nmid d_p}} \frac{\varphi(l)}{l} \sum_{m \geq 1} \frac{1}{mp^{ml\sigma - 1}} \right)$$

$$= \frac{1}{2} \sum_{\substack{p \\ 2 \nmid d_p}} \frac{1}{p^{2\sigma - 1}} + O(1),$$

where the implicit constant depends on σ. The rest of the proof follows immediately.

□

Notice that the parity of d_p determines how -1 acts on $\mathbb{F}_p^+$ in the semidirect product $\mathbb{F}_p^+ \rtimes_{d_p} \mathbb{F}_p^\times$; namely, -1 acts trivially if and only if d_p is even. Thus the theorem shows that the action of -1 in the semidirect products radically influences the behavior of the zeta function near $s = 1$.

References

[1] C. Arf, The Collected Papers, Turkish Mathematical Society, 1990.

[2] E. Artin, Über eine neue Art von *L*-Reihen, Collected Papers, Nr. 3, Addison-Wesley, 1965.

[3] D. Dummit and R. Foote, Abstract Algebra, 2nd ed., Prentice-Hall, New Jersey, 1999.

[4] S. Lang, *L*-series of a covering, Proc. Nat. Acad. Sci. U. S. A. 42(7) (1956), 422-424.

[5] S. Lang, Algebra, Addison-Wesley Publishing Co., Inc., Reading, Mass., 1965.

[6] J. P. Serre, Linear representations of finite groups, Graduate Texts in Mathematics, Vol. 42, Springer-Verlag, New-York, Heidelberg, 1977.