APPLICATIONS OF THE FROBENIUS DENSITY THEOREM

LUCAS MASON-BROWN

1. Polynomials

Let $f(x)$ be a polynomial with integer coefficients, irreducible over $\mathbb{Q}$. For every prime $p \in \mathbb{Z}$, we obtain a polynomial $\bar{f}(x) \in \mathbb{F}_p[x]$ by reducing the coefficients mod p. We say that $f(x)$ is *reducible everywhere* if $\bar{f}(x)$ is reducible over $\mathbb{F}_p$ for every prime p not dividing the discriminant of f.

In this section, we will prove two basic facts about such polynomials (and some other interesting results along the way). First, that if the degree of $f(x)$ is prime, $f(x)$ cannot be reducible everywhere. Second, that if n is composite, there exists a polynomial of degree n that is reducible everywhere. To prove these facts, we will employ the Frobenius density theorem, which relates behavior of a polynomial under reduction to the Galois group of its splitting field. More precisely:

Frobenius Density Theorem. *Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree n and G the galois group of its splitting field. Let $d = (d_1, d_2, ..., d_t)$ be a partition of n, and let S be the set of primes q not dividing the discriminant of $f(x)$ for which $f(x)$ modulo q has decomposition type d. Then S has natural density equal to $1/\#G$ times the number of $\sigma \in G$ of cycle pattern d (identifying G in the natural way with a subgroup of S_n).*

In particular, this theorem allows us to compute the natural density of $\{\text{q prime} \mid \bar{f}(x) \text{ irreducible over } \mathbb{F}_q\}$ by counting the n-cycles in the Galois group. For the purposes of what follows, we will need to strengthen this theorem slightly:

Frobenius Density Theorem$'$. *Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree n and G the galois group of its splitting field. Let $d = (d_1, d_2, ..., d_t)$ be a partition of n, and let S be the set of primes q not dividing the discriminant of $f(x)$ for which $f(x)$ modulo q has decomposition type d. Then S is either empty or of positive natural density equal to $1/\#G$ times the number of $\sigma \in G$ of cycle pattern d (identifying G in the natural way with a subgroup of S_n).*

Proof. See Rosen. □

This version of the theorem has the following important consequence: an irreducible monic polynomial $f(x) \in \mathbb{Z}[x]$ is *reducible everywhere* if and only if its Galois group is n-cycle free.

Before proving the main results of this section, we will apply the Frobenius density theorem to the following, somewhat tangential question: given integers a and n, modulo what proportion of primes is a an nth power? The reciprocity laws provide a partial answer to this question. For example, if a happens to be prime, quadratic reciprocity tells us that a is a square modulo 1 out of every 2 primes. Similarly, rational cubic reciprocity indicates that a is a cube modulo 2 out of every 3 primes. This is a good start, but the reciprocity laws only go so far. What if n is large? Or if a is composite? We will use the Frobenius density theorem to answer these more general questions. But first, the following lemma:

Lemma 1.1. *Let p be prime and $f(x) = x^p - a$. Then $f(x)$ is reducible if and only if a is a pth power.*

Proof. If a is a pth power, say $a = b^p$, then the linear factor $x - b$ divides $f(x)$. Hence, $f(x)$ is reducible over $\mathbb{Q}$.

Conversely, suppose $f(x)$ is reducible over $\mathbb{Q}$. Hence,

$$\prod_{i=0}^{p-1}(x - \zeta_p^i \sqrt[p]{a}) = x^p - a = g(x)h(x)$$

for some $g(x), h(x) \in \mathbb{Q}[x]$ of degree less than p. Let d be the degree of $g(x)$. Then the constant term of the polynomial $g(x)$ has form $c = \omega \sqrt[p]{a}^d$ where ω is some pth root of unity. It follows that $c^p = a^d$. Since d is prime to p, we have $dr + ps = 1$ for some $r, s \in \mathbb{Z}$. Hence

$$a = a^{dr+ps} = a^{dr}a^{ps} = (c)^{pr}a^{ps} = (c^r a^s)^p$$

So, a is a pth power, as desired. □

Proposition 1.1. *Suppose $a \in \mathbb{Z}$ is not a cube. Then a is a cube modulo 2 out of every 3 primes.*

Proof. Let $f(x) = x^3 - a$. $f(x)$ is irreducible by the lemma. The splitting field K for the polynomial $f(x)$ is formed by adjoining $\sqrt[3]{a}$ and a primitive cube root of unity to $\mathbb{Q}$. Since $[\mathbb{Q}(\sqrt[3]{a}) : \mathbb{Q}] = 3$ and $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = \phi(3) = 2$ and $(3, 2) = 1$, it follows that $[K : \mathbb{Q}] = 3 \cdot 2 = 6$. The Galois group G must therefore be the full symmetric group S_3.

For any prime q, a is a cube mod q if and only if $f(x)$ is reducible mod q. It follows from the Frobenius density theorem that the natural density of $\{$q prime : a is a cube mod $q\}$ is the proportion of elements of G that are not 3-cycles. As we have seen, G is isomorphic to S_3 and S_3 contains two 3-cycles. Hence, the density of $\{$q prime : a is a cube mod $q\}$ is precisely $1 - 2/6 = 2/3$. □

Proposition 1.2. *Suppose $a \in \mathbb{Z}$ is not a fifth power. Then a is a fifth power modulo 4 out of every 5 primes.*

Proof. Let $f(x) = x^5 - a$. $f(x)$ is irreducible by the lemma. The splitting field K for the polynomial $f(x)$ is the adjunction $\mathbb{Q}(\sqrt[5]{a}, \zeta_5)$. Since $[\mathbb{Q}(\sqrt[5]{a}) : \mathbb{Q}] = 5$ and $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = \phi(5) = 4$ and $(5, 4) = 1$, it follows that $[K : \mathbb{Q}] = 5 \cdot 4 = 20$

Define $\sigma : K \to K$ by $\sigma(\sqrt[5]{a}) = \zeta_5 \sqrt[5]{a}$ and $\tau : K \to K$ by $\tau(\zeta_5) = \zeta_5^2$. Both of these maps define field automorphisms and are therefore elements of the Galois group G. G

acts faithfully on the set of roots $\{\sqrt[5]{a},\ \zeta_5\sqrt[5]{a},\ \zeta_5^2\sqrt[5]{a},\ \zeta_5^3\sqrt[5]{a},\ \zeta_5^4\sqrt[5]{a}\}$. This action induces an injective homomorphism $i : G \to S_5$. One easily verifies that $i\sigma = (1\ 2\ 3\ 4\ 5)$ and $i\tau = (2\ 3\ 5\ 4)$. Since $i\sigma$ has order 5, and $i\tau$ has order 4, the subgroup $\langle i\sigma, i\tau\rangle$ has at least 20 elements. On the other hand, $\langle i\sigma, i\tau\rangle$ has at most 20 elements, since it is a subgroup of iG, which has order $[K : \mathbb{Q}] = 20$. It follows that $\langle i\sigma, i\tau\rangle = iG$.

The elements of $\langle(1\ 2\ 3\ 4\ 5), (2\ 3\ 5\ 4)\rangle$ can be enumerated explicitly (I have organized them by cycle-type):

$$\{e, (1\ 2)(3\ 5), (1\ 3)(4\ 5), (1\ 4)(2\ 3), (1\ 5)(2\ 4), (2\ 5)(3\ 4),$$
$$(1\ 2\ 4\ 3), (1\ 2\ 5\ 4), (1\ 3\ 2\ 5), (1\ 3\ 4\ 2), (1\ 4\ 3\ 5), (1\ 4\ 5\ 2), (1\ 5\ 2\ 3), (1\ 5\ 3\ 4), (2\ 3\ 5\ 4), (2\ 4\ 5\ 3),$$
$$(1\ 2\ 3\ 4\ 5), (1\ 3\ 5\ 2\ 4), (1\ 4\ 2\ 5\ 3), (1\ 5\ 4\ 3\ 2)\}$$

All elements but the 5-cycles fix at least one root. There are four 5-cycles in iG and so it follows from Frobenius that the density of $\{\text{q prime} \mid a \text{ is a fifth power mod } q\}$ is precisely $1 - 4/20 = 4/5$ □

In fact, this pattern continues. More explicitly:

Proposition 1.3. *Suppose p is a prime and $a \in \mathbb{Z}$ is not a pth power. Then a is a pth power modulo $p-1$ out of every p primes.*

Proof. Let $f(x) = x^p - a$. $f(x)$ is irreducible by the lemma.The splitting field K for the polynomial $f(x)$ is the adjunction $\mathbb{Q}(\sqrt[p]{a}, \zeta_p)$. Since $[\mathbb{Q}(\sqrt[p]{a}) : \mathbb{Q}] = p$ and $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \phi(p) = p-1$ and $(p, p-1) = 1$, it follows that $[K : \mathbb{Q}] = p(p-1)$.

Consider the set of automorphisms $S = \{\sigma_{(m,n)} : \sqrt[p]{a} \mapsto \zeta_p^m\sqrt[p]{a}, \zeta_p \mapsto \zeta_p^n \mid m \in \mathbb{Z}/p\mathbb{Z}, n \in (\mathbb{Z}/p\mathbb{Z})^*\}$. Since distinct pairs (m, n) give rise to distinct automorphisms, S has $p(p-1)$ elements. Since $S \subseteq Gal(K/\mathbb{Q})$ and $\#Gal(K/\mathbb{Q}) = [K : \mathbb{Q}] = p(p-1)$, S must therefore be the entirety of $Gal(K/\mathbb{Q})$. Let $Gal(K/\mathbb{Q})$ act on $\{\sqrt[p]{a}, \zeta_p\sqrt[p]{a}, ..., \zeta_p^{p-1}\sqrt[p]{a}\}$ in the usual way. Under what conditions does the automorphism $\sigma_{(m,n)}$ have a fixed point?

Let $\zeta_p^x\sqrt[p]{a}$ be a root. We have $\sigma_{(m,n)}(\zeta_p^x\sqrt[p]{a}) = \zeta_p^{nx+m}\sqrt[p]{a}$. Hence, $\sigma_{(m,n)}$ has a fixed point if and only if the equation $nx + m = x$ has a solution mod p. If $n \not\equiv 1 \mod p$, then $n-1$ is a unit mod p. In this case, $nx + m = x \mod p$ is solvable and indeed $x = -m(n-1)^{-1}$ is a solution. If $n \equiv 1 \mod p$, then $nx + m = x$ has a solution mod p if and only if $m \equiv 0$ mod p. Therefore, $\sigma_{(m,n)}$ has a fixed point for every (m, n) except the following $p-1$: $(1, 1), (2, 1), ..., (p-1, 1)$. It follows from Frobenius that $\{\text{q prime} \mid a \text{ is a } p\text{th power mod } q\}$ has density equal to $1 - \frac{p-1}{p(p-1)} = 1 - \frac{1}{p} = \frac{p-1}{p}$, as desired.

□

We can generalize this result to arbitrary exponents. To do so, we will need the following two lemmas:

Lemma 1.2. *Let $a, t \in \mathbb{Z}$ and $f(x) = x^t - a$ irreducible. If K is a splitting field for $f(x)$ over $\mathbb{Q}$, then $Gal(K/\mathbb{Q})$ is isomorphic to the matrix group $G_t = \{\left(\begin{smallmatrix} m & n \\ 0 & 1 \end{smallmatrix}\right) \mid m \in (\mathbb{Z}/t\mathbb{Z})^*, n \in \mathbb{Z}/t\mathbb{Z}\}$.*

Proof. For every $m \in (\mathbb{Z}/t\mathbb{Z})^*$ and $n \in \mathbb{Z}/t\mathbb{Z}$, there is an automorphism $\sigma_{(m,n)} : \zeta_t \mapsto \zeta_t^m, \sqrt[t]{a} \mapsto \zeta_t^n \sqrt[t]{a}$. Define the map $\phi : G_t \to Gal(K/\mathbb{Q})$ by $\phi\left(\begin{smallmatrix} m & n \\ 0 & 1 \end{smallmatrix}\right) = \sigma_{(m,n)}$. One easily verifies that ϕ is a group homomorphism. Since field automorphisms preserve algebraic equations, every element $\sigma \in Gal(K/\mathbb{Q})$ takes ζ_t to some primitive tth root of unity and $\sqrt[t]{a}$ to some tth root of a, i.e. $\sigma(\zeta_t) = \zeta_t^m$ and $\sigma(\sqrt[t]{a}) = \zeta_t^n \sqrt[t]{a}$, for some $m \in (\mathbb{Z}/t\mathbb{Z})^*$ and $n \in \mathbb{Z}/t\mathbb{Z}$. The map $\sigma \mapsto \left(\begin{smallmatrix} m & n \\ 0 & 1 \end{smallmatrix}\right)$ is an inverse of ϕ. Thus, ϕ is a group isomorphism. □

Lemma 1.3. *For any prime power p^l, the number of pairs $(m,n) \in (\mathbb{Z}/p^l\mathbb{Z})^* \times \mathbb{Z}/p^l\mathbb{Z}$ for which the equation $mx + n \equiv x \mod p^l$ has a solution is given by*

$$\frac{p^{2l+2} - 2p^{2l+1} + p^{2l-1} + p - 1}{p^2 - 1}$$

Proof. We can, equivalently, consider the solvability of the equation $(m-1)x \equiv -n \mod p^l$. There are two cases to consider.

Case 1. $m-1$ is a unit

If $m-1$ is a unit mod p^l, then the equation is solvable for all values of n. $m-1$ is a unit for all but p^{l-1} values of m. That is, $p^l - 2p^{l-1}$ values of m. Thus, Case 1 contributes $p^l(p^l - 2p^{l-1}) = p^{2l} - 2p^{2l-1}$ pairs.

Case 2. $m-1$ is not a unit

In this case, $m - 1 = kp^r$ for $1 \leq r \leq l$ and $p \dagger k$. For a particular choice of r, there are $\varphi(p^{l-r})$ such m in $(\mathbb{Z}/p^l\mathbb{Z})^*$. For each of these, the equation is solvable if and only if $n \equiv 0$ mod p^r. There are p^{l-r} such n in $\mathbb{Z}/p^l\mathbb{Z}$. Thus, Case 2 contributes a total of

$$\sum_{r=1}^{l} \varphi(p^{l-r})(p^{l-r}) = p^{2l-2} - p^{2l-3} + p^{2l-4} - p^{2l-5} + ... + 1$$

pairs.

Hence, the total number of pairs $(m,n) \in (\mathbb{Z}/p^l\mathbb{Z})^* \times \mathbb{Z}/p^l\mathbb{Z}$ for which $mx + n \equiv x$ mod p^l is solvable comes to

$$\begin{aligned} p^{2l} - 2p^{2l-1} + p^{2l-2} - p^{2l-3} + p^{2l-4} - p^{2l-5} + ... + 1 &= -p^{2l-1} + \sum_{i=0}^{l}(p^2)^i - p\sum_{i=0}^{l-1}(p^2)^i \\ &= -p^{2l-1} + \frac{p^{2l+2} - 1}{p^2 - 1} - p\frac{p^{2l} - 1}{p^2 - 1} \\ &= \frac{p^{2l+2} - 2p^{2l+1} + p^{2l-1} + p - 1}{p^2 - 1} \end{aligned}$$

□

Proposition 1.4. *Let t be an integer with prime factorization $t = \prod_{i=1}^{s} p_i^{l_i}$. Suppose the polynomial $f(x) = x^t - a$ is irreducible over $\mathbb{Q}$. Let $S = \{q \text{ prime} \mid a \text{ is a } t\text{th power mod } q\}$. Then the natural density of S equals*

$$\prod_{i=1}^{s} \frac{p_i^{2l_i+2} - 2p_i^{2l_i+1} + p_i^{2l_i-1} + p_i - 1}{p_i^{2l_i+2} - p_i^{2l_i+1} - p_i^{2l_i} + p_i^{2l_i-1}}$$

Proof. This follows straightforwardly from the previous two lemmas and the Chinese Remainder Theorem. Let K be a splitting field for $f(x)$ over $\mathbb{Q}$. Since $f(x)$ is irreducible, lemma 1.3 implies that $Gal(K/\mathbb{Q})$ is isomorphic to the matrix group $G_t = \{\left(\begin{smallmatrix} m & n \\ 0 & 1 \end{smallmatrix}\right) \mid m \in (\mathbb{Z}/t\mathbb{Z})^*, n \in \mathbb{Z}/t\mathbb{Z}\}$. The order of $Gal(K/\mathbb{Q})$ is thus $t\varphi(t) = \prod_{i=1}^{s} p_i^{l_i}(p_i^{l_i} - p_i^{l_i-1}) = \prod_{i=1}^{s} p_i^{2l_i} - p_i^{2l_i-1}$. The action of an element $\left(\begin{smallmatrix} m & n \\ 0 & 1 \end{smallmatrix}\right)$ on the set of roots $\{\zeta_t^x \sqrt[t]{a} \mid x \in \mathbb{Z}/t\mathbb{Z}\}$ is described by the equation $\left(\begin{smallmatrix} m & n \\ 0 & 1 \end{smallmatrix}\right)(\zeta_t^x \sqrt[t]{a}) = \zeta_t^{mx+n} \sqrt[t]{a}$. Hence, $\left(\begin{smallmatrix} m & n \\ 0 & 1 \end{smallmatrix}\right)$ has a fixed point if and only if $mx + n \equiv x \mod t$ has a solution in x. Let k_i denote the number of pairs (solutions mod $p_i^{l_i}$. By the Chinese Remainder Theorem, the number of solutions mod t is given by the product $\prod_{i=1}^{s} k_i$. Therefore, by Frobenius, the natural density of S is

$$\frac{\prod_{i=1}^{s} k_i}{\#Gal(K/\mathbb{Q})} = \prod_{i=1}^{s} \frac{p_i^{2l_i+2} - 2p_i^{2l_i+1} + p_i^{2l_i-1} + p_i - 1}{(p_i^2 - 1)(p_i^{2l_i} - p_i^{2l_i-1})} = \prod_{i=1}^{s} \frac{p_i^{2l_i+2} - 2p_i^{2l_i+1} + p_i^{2l_i-1} + p_i - 1}{p_i^{2l_i+2} - p_i^{2l_i+1} - p_i^{2l_i} + p_i^{2l_i-1}}$$

□

We now shift our attention to the main focus of this section: namely, the connection between degree and *everywhere-reducibility.* We begin by considering polynomials of prime degree.

Proposition 1.5. *Let $f(x)$ be a polynomial with integer coefficients, irreducible over $\mathbb{Q}$. Furthermore, suppose $f(x)$ has prime degree, p. Then $f(x)$ is irreducible modulo infinitely many primes. In particular, $\{q \text{ prime} \mid \bar{f}(x) \text{ irreducible over } \mathbb{F}_q\}$ has positive natural density.*

Proof. Let $\{\alpha_1, \alpha_2, ..., \alpha_p\}$ be the roots of $f(x)$ in an algebraic closure, and let $K = \mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_p)$. The galois group $Gal(K/\mathbb{Q})$ acts faithfully on $\{\alpha_1, \alpha_2, ..., \alpha_p\}$. This action induces an injective homomorphism $i : Gal(K/\mathbb{Q}) \to S_p$

By the Frobenius density theorem, it suffices to show that $iGal(K/\mathbb{Q})$ contains a p-cycle.

Since the action of $Gal(K/\mathbb{Q})$ on $\{\alpha_1, \alpha_2, ..., \alpha_p\}$ is transitive, p must divide the order of $Gal(K/\mathbb{Q})$. Hence, $iGal(K/\mathbb{Q})$ contains an element of order p. Let σ be one such element. Suppose σ has cycle type $(d_1, d_2, ..., d_m)$. That is, σ can be written as the product of m disjoint cycles of lengths $d_1, d_2, ..., d_m$. We have

$$p = order(\sigma) = lcm\{d_i\}_{i=1}^{m}$$

Hence, p divides $\prod_{i=1}^{m} d_i$. Since p is prime, this means p divides d_j for some $j \leq m$. On the other hand, $d_j \leq p$. Thus, $d_j = p$. It follows that σ is a p-cycle.

□

Of course, the proof of this theorem relies crucially on the primality of $degf(x)$. The theorem is in general false for polynomials of composite degree, as we will soon see.

Example 1.1.

Let $f(x) = x^4 + 1$. The roots of $f(x)$ in $\mathbb{C}$ are precisely $e^{\pi i/4}, e^{3\pi i/4}, e^{5\pi i/4}$, and $e^{7\pi i/4}$. Suppose $f(x)$ is reducible in $\mathbb{Q}[x]$. Since $f(x)$ has no rational roots, $f(x)$ must therefore split as the product of integer quadratic polynomials, i.e. there are integers a, b, c, and d such that $x^4+1 = (x^2+ax+b)(x^2+cx+d) = x^4+(a+c)x^3+(b+d+ac)x^2+(ad+bc)x+bd$. Clearly $a + c = 0$ and either $b = d = 1$ or $b = d = -1$. Hence, $b + d + ac = 0$ implies $a^2 = \pm 2$, a contradiction. It follows that $f(x)$ is irreducible over $\mathbb{Q}$.

Let K be the splitting field for $f(x)$. Clearly, $K = \mathbb{Q}(\zeta_8)$, where ζ_8 is a primitive eight root of unity. It follows that $Gal(K/\mathbb{Q}) \cong (\mathbb{Z}/8\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. However, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has no elements of order 4, and is therefore 4-cycle free as a subgroup of S_4. It follows from the Frobenius density theorem that $f(x)$ is reducible everywhere.

One useful criterion for everywhere-reducibility is provided by Rosen. Let Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial with roots $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ in $\mathbb{C}$. Let $K = \mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_n)$ and $L = \mathbb{Q}(\alpha_1)$. Furthermore, let $G = Gal(K/\mathbb{Q})$ and $H = Gal(K/L)$. A cyclic subgroup $C \subseteq G$ is a *cyclic complement* of H in G if $G = CH$ and $C \cap H = \{1\}$.

Proposition 1.6. *$f(x)$ is reducible everywhere if and only if H does not admit a cyclic complement in G.*

Proof. For simplicity, identify G with its image in S_n. Suppose $f(x)$ is *not* reducible everywhere. Hence, G contains an n-cycle, σ. Since every element of H fixes α_1, H is n-cycle-free. Hence, $\langle\sigma\rangle \cap H = \{1\}$. Keeping in mind that the index of H in G is n,we have $\#\langle\sigma\rangle H = \#\langle\sigma\rangle\#H = n(\frac{\#G}{n}) = \#G$. Hence, $G = \langle\sigma\rangle H$, i.e. H admits a cyclic complement.

Conversely, suppose H admits a cyclic complement, C, in G. Let σ generate C. Since G is a transitive subgroup of S_n, we have $G\alpha_1 = \{\alpha_1, \alpha_2, ..., \alpha_n\}$. But $G\alpha_1 = CH\alpha_1 = C\alpha_1 = \langle\sigma\rangle\alpha_1$. It follows that σ is an n-cycle. □

The next lemma establishes sufficient conditions for the existence of everywhere-reducible polynomials of a given degree n [1] :

Lemma 1.4. *Let $n \in \mathbb{Z}$ and G a group. Suppose G satisfies the following three properties:*

1. *$G \cong Gal(K/\mathbb{Q})$ for some field extension $K/\mathbb{Q}$*
2. *G contains a subgroup of index n*
3. *G contains no elements of order divisible by n*

Then there is a an irreducible polynomial $f(x) \in \mathbb{Z}[x]$ of degree n that is reducible everywhere.

[1] This lemma is a modified form of Lemma 2.1 appearing in [1]. The conditions in the original lemma are too weak to establish the claim. The proof, however, is essentially the same.

Proof. Let $H \subseteq G$ be a subgroup of index n. Let $\mathbb{Q}(\alpha) \subseteq K$ be the fixed field of H (identifying G with the galois group $Gal(K/\mathbb{Q})$). Let $f(x)$ be a minimal polynomial for α over $\mathbb{Q}$ and $L \subseteq K$ its splitting field. Since $L/\mathbb{Q}$ is normal, $Gal(K/L)$ is a normal subgroup of $Gal(K/\mathbb{Q})$ and

$$Gal(L/\mathbb{Q}) \cong Gal(K/\mathbb{Q})/Gal(K/L)$$

The relationship between $Gal(K/L)$ and H is given by

$$Gal(K/L) = \bigcap_{\sigma \in G} \sigma H \sigma^{-1}$$

. Suppose $\bar{\sigma} \in Gal(K/\mathbb{Q})/Gal(K/L)$ is an element of order n. Then $\sigma \in Gal(K/\mathbb{Q})$ has order divisible by n, which contradicts condition 3). It follows that $Gal(L/\mathbb{Q})$ contains no elements of order n. The result follows from Frobenius.

□

As it turns out, such a G exists for every composite n. To see this, we will examine the square-free and non-square-free cases separately.

Proposition 1.7. *If n is divisible by a square, there is an irreducible polynomial $f(x) \in \mathbb{Z}(x)$ of degree n, which is reducible everywhere.*

Proof. Let $n = p^2 m$, and let $G = \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$. G is abelian and thus realizable as a galois group. The trivial subgroup has index n, and G has no elements of order n, since G is non-cyclic. It follows from the lemma that there is a polynomial $f(x) \in \mathbb{Z}(X)$ of degree n, which is reducible everywhere. Since H is trivial, the galois group of $f(x)$ is G. □

Proposition 1.8. *If n is square-free, there is an irreducible polynomial $f(x) \in \mathbb{Z}(X)$ of degree n, which is reducible everywhere.*

Proof. Let $n = pm$ with p prime. Since n is square-free, m is prime to p. Hence, $\bar{p} \in \mathbb{Z}/m\mathbb{Z}^*$. Let t denote the order of $\bar{p}$ in $\mathbb{Z}/m\mathbb{Z}^*$. Let A denote the additive group of the finite field $\mathbb{F}_{p^t}$ and $\mu_m \subset \mathbb{F}_{p^t}$ the m mth roots of unity. μ_m acts on A by multiplication. We define G as the semi-direct product $A \rtimes \mu_m$ under this action.

G is solvable and therefore realizable as a galois group. Furthermore, if $H \subset A$ is a hyperplane (i.e. a $\mathbb{F}_p$-subspace of codimension 1), H has index $pm = n$ in G. Hence, G satisfies conditions 1) and 2) of the lemma. It is left for us to show that no element of G has order divisible by n.

Let $(a, b) \in A \rtimes \mu_m$. If $b = 1$ then $(a, b) \in A$ so $o(a, b)$ divides p. Otherwise, we have

$$\begin{aligned}
&(a,b)^1 = (a,b)\\
&(a,b)^2 = (a+ab,b^2)\\
&(a,b)^3 = (a+ab+ab^2,b^3)\\
&\vdots\\
&(a,b)^m = (a+ab+...+ab^{m-1},b^m) = (a\frac{b^m-1}{b-1},b^m) = (0,1)
\end{aligned}$$

Hence, the order of an element of G divides either m or p. In particular, its order is not divisible by n. □

It is less clear in the square-free case what the galois group of $f(x)$ looks like. However, it turns out the galois group of $f(x)$ is G. We will prove this fact, but first the following lemma:

Lemma 1.5. *The mth roots of unity span $\mathbb{F}_{p^t}$ as a vector space over $\mathbb{F}_p$.*

Proof. Let $\zeta_m \in \mathbb{F}_{p^t}$ be a primitive mth root of unity. Since $\mathbb{F}_{p^t}/\mathbb{F}_p$ is galois, it suffices to show that $Gal(\mathbb{F}_{p^t}/\mathbb{F}_p(\zeta_m)) = \{1\}$. The galois group $Gal(\mathbb{F}_{p^t}/\mathbb{F}_p)$ is cyclic, generated by the Frobenius automorphism $x \to x^p$. Suppose $\sigma \in Gal(\mathbb{F}_{p^t}/\mathbb{F}_p)$ fixes ζ_m. Hence $\zeta_m^{p^k} = \zeta_m$ for some integer k. In other words, $p^k \equiv 1 \mod m$. Hence, k is divisible by t, the order of p modulo m, i.e. $k = at$ for some positive integer a. But for any $x \in \mathbb{F}_{p^t}$, we have $x^{p^{at}} = x(x^{p^{at}-1}) = x(x^{(p^t-1)(1+p^t+p^{2t}+...+p^{(a-1)t})}) = x(x^{p^t-1})^{1+p^t+p^{2t}+...+p^{(a-1)t}} = x$. Hence, σ is the identity automorphism, which completes the proof. □

Proposition 1.9. *In Proposition* 1.8*, The galois group of $f(x)$ is G.*

Proof. Since the galois group of $f(x)$ is the quotient

$$G/\bigcap_{\sigma\in G}\sigma H\sigma^{-1}$$

we need to show that $\bigcap_{\sigma\in G}\sigma H\sigma^{-1} = \{(0,1)\}$. Let $(h,1) \in H$ and $x \in \mu_m$. Then

$$\begin{aligned}
(0,x)(h,1)(0,x)^{-1} &= (0,x)(h,1)(0,x^{-1})\\
&= (xh,x)(0,x^{-1})\\
&= (xh,1)
\end{aligned}$$

Hence, $\bigcap_{\sigma\in G}\sigma H\sigma^{-1} \subseteq \bigcap_{x\in\mu_m} xH$.

Suppose $r \in \bigcap_{x\in\mu_m} xH$ and $r \neq 0$. Then $r \in xH$ for every $x \in \mu_m$. Or, in other words, $x \in Hr^{-1}$ for every $x \in \mu_m$. Therefore, Hr^{-1} contains the subspace spanned by the

mth roots of unity, which is $\mathbb{F}_{q^t}$ by the lemma. This is a contradiction, since Hr^{-1} is a hyperplane. It follows that $\bigcap\limits_{\sigma \in G} \sigma H \sigma^{-1} = \{(0,1)\}$, as desired. □

2. Galois Sets

Let k be any perfect field and $\bar{k}$ an algebraic closure. For the purposes of this paper, k will either be $\mathbb{Q}$ or $\mathbb{F}_p$. As usual, let $\mathbb{P}^r(\bar{k})$ denote the projective space of dimension r over $\bar{k}$. Let $Gal(\bar{k}/k)$ act on $\mathbb{P}^r(\bar{k})$ in the natural way, i.e. by $\sigma[\alpha_0, \alpha_1, ...\alpha_r] = [\sigma\alpha_0, \sigma\alpha_1, ...\sigma\alpha_r]$.

Definition 2.1. *A Galois set over k is a finite subset of $\mathbb{P}^r(\bar{k})$ which is invariant under the action of $Gal(\bar{k}/k)$.*

A Galois set is *reducible* if it is the union of two disjoint nonempty Galois subsets. Clearly, S is irreducible if and only if G acts transitively on S.

Proposition 2.1. *A finite subset $S \subset \mathbb{P}^r(\bar{k})$ is Galois if and only if it is the vanishing set of a finite collection of homogenous polynomials with coefficients in k. In other words, a set is Galois if and only if finite and algebraic .*

Proof. Suppose S is the vanishing set of a finite collection of homogenous polynomials with coefficients in k. Clearly, S is finite, and if $s \in S$ is a root of the polynomial $f(x)$, so is σs for any $\sigma \in Gal(\bar{k}/k)$, since $f(\sigma s) = \sigma f(s) = \sigma 0 = 0$. Hence, S is a Galois set.

Conversely, suppose S is a Galois set. Since the union of algebraic sets is algebraic, we can assume without loss of generality that S is irreducible. We know that $\mathbb{P}^r(\bar{k})$ is the disjoint union of affine spaces $\bar{k}^r \sqcup \bar{k}^{r-1} \sqcup ... \sqcup \{0\}$. Since each of these affine spaces is closed under the action of $Gal(\bar{k}/k)$ and S is assumed irreducible, S must be contained in one of them. Thus, we can reduce to the affine case.

Let $I = \{f(x) \in k[x_1, x_2, ..., x_r] \mid f(s) = 0, \forall s \in S\}$. I is an ideal in the polynomial ring $k[x_1, x_2, ..., x_r]$. Now let s be an element of S with coordinates $(s_1, s_2, ..., s_r)$. Evaluation at s defines a surjective ring homomorphism

$$\phi : k[x_1, x_2, ..., x_r] \longrightarrow k[s_1, s_2, ..., s_r] = k(s_1, s_2, ..., s_r)$$

with kernel equal to I. Hence, ϕ induces an isomorphism $\bar{\phi} : k[x_1, x_2, ..., x_r]/I \cong k(s_1, s_2, ..., s_r)$. Since $k(s_1, s_2, ..., s_r)$ is a field, I is a maximal ideal.

Suppose p is a point in $\bar{k}^r$ satisfying every polynomial in I. Let $p = (p_1, p_2, ..., p_r)$. Evaluation at p, once again, defines a surjective ring homomorphism

$$\psi : k[x_1, x_2, ..., x_r] \longrightarrow k[p_1, p_2, ..., p_r] = k(p_1, p_2, ..., p_r)$$

The kernel of this map is an ideal containing I. But we know that I is maximal. Hence, $ker\psi = I$ and ψ induces a field isomorphism $\bar{\psi} : k[x_1, x_2, ..., x_r]/I \cong k(p_1, p_2, ..., p_r)$.

Composing $\bar{\psi}$ with the inverse of $\bar{\phi}$ yields a field isomorphism

$$\bar{\psi} \circ \bar{\phi}^{-1} : k(s_1, s_2, ..., s_r) \longrightarrow k(p_1, p_2, ..., p_r)$$

which we will call σ. From definitions it is obvious that $\sigma(s_i) = p_i$ for all $i \leq r$. Moreover, since both $k(s_1, s_2, ..., s_r)$ and $k(p_1, p_2, ..., p_r)$ are subdfields of $\bar{k}$, σ extends to a field automorphism $\bar{k} \to \bar{k}$. Thus, p is an element of S, which completes the proof.

□

A morphism in the category of Galois sets is a map $f : U \to V$ which commutes with the action of $Gal(\bar{k}/k)$, i.e. such that $f(\sigma(u)) = \sigma(f(u))$ for every $\sigma \in Gal(\bar{k}/k)$ and every $u \in U$. Since morphisms respect the Galois action, isomorphic Galois sets have the same orbit structure. In particular, if U is irreducible and $U \cong V$, then V is irreducible as well.

Clearly, any map between Galois sets defined by polynomials is a morphism, in the sense defined above. As it turns out, any morphism between Galois sets is defined by polynomials (piecewise, on irreducible components). In other words, the category of irreducible Galois sets over k is precisely the category of irreducible zero-dimensional projective algebraic sets.

Proposition 2.2. *Let U and V be irreducible Galois sets over k and $\phi : U \to V$ a morphism. Then ϕ is defined by a collection of homogenous polynomials of equal degree with coefficients in k. In other words, ϕ is a morphism of projective algebraic sets.*

Proof. $\mathbb{P}^t(\bar{k})$ is the disjoint union of affine spaces $\bar{k}^t \sqcup \bar{k}^{t-1} \sqcup ... \sqcup \{0\}$, each closed under the action of $Gal(\bar{k}/k)$. Since U and V are irreducible, each is contained in an affine space, say $\bar{k}^r$ and $\bar{k}^s$, respectively.

Let $U = \{P_1, P_2, ..., P_m\}$. We will use superscripts to pick out coordinates. Hence $P_1 = (P_1^1, P_1^2, ..., P_1^r)$. Let $H = Gal(\bar{k}/k(P_1^1, P_1^2, ..., P_1^r))$. For every $\sigma \in H$ we have $\sigma\phi(P_1)^1 = \phi(\sigma P_1)^1 = \phi(P_1)^1$. Since $\phi(P_1)^1$ is fixed by every element of H and $\bar{k}/k(P_1^1, P_1^2, ..., P_1^r)$ is Galois, $\phi(P_1)^1$ must be an element of the base field, $k(P_1^1, P_1^2, ..., P_1^r)$. But the P_1^j are algebraic, so $k(P_1^1, P_1^2, ..., P_1^r) = k[P_1^1, P_1^2, ..., P_1^r]$. Hence, $\phi(P_1)^1 \in k[P_1^1, P_1^2, ..., P_1^r]$. It follows that there is a polynomial $f \in k[x_1, x_2, ..., x_r]$ such that $f(P_1) = \phi(P_1)^1$.

Since U is irreducible, for every $P_i \in U$ there is a $\sigma \in Gal(\bar{k}/k)$ such that $P_i = \sigma P_1$. Hence

$$f(P_i) = f(\sigma P_1) = \sigma f(P_1) = \sigma\phi(P_1)^1 = \phi(\sigma P_1)^1 = \phi(P_i)^1$$

Thus, we have shown that the first coordinate function of ϕ is a polynomial map. One can similarly show, replacing 1 with i, that *every* coordinate function is a polynomial map. Thus, ϕ is defined by a collection of polynomials. We can homogenize these polynomials to obtain a collection of homogenous polynomials of equal degree.

□

Given any polynomial $f(x) \in k[x]$ with roots $\alpha_1, \alpha_2, ..., \alpha_n \in \bar{k}$, the set of points $S = \{[\alpha_1, 1], [\alpha_2, 1], ..., [\alpha_n, 1]\}$ forms a Galois subset of the projective line. In fact, any Galois subset of $\mathbb{P}^1(\bar{k})$ can be described in this fashion.

Proposition 2.3. *Suppose $S \subset \mathbb{P}^1(\bar{k})$ is a Galois set. Then S is the vanishing set of some homogenous polynomial $f(x_1, x_2)$ with coefficients in k.*

Proof. We can assume without loss of generality that S is irreducible. Indeed, if every irreducible component is the vanishing set of a homogenous polynomial, then S is the vanishing set of their product. Since for any automorphism σ, $\sigma[1,0] = [1,0]$, the point at infinity is fixed under the action of G. Thus, either $S = \{[1,0]\}$ or $S = \{[\alpha_1, 1], [\alpha_2, 1], ..., [\alpha_n, 1]\}$ for some collection of algebraic numbers $\alpha_1, \alpha_2, ..., \alpha_n$ transitive under the action of $Gal(\bar{k}/k)$. In the first case, S is the vanishing set of the homogenous polynomial $f(x_1, x_2) = x_2$. In the second case, we can construct $f(x_1, x_2)$ explicitly.

Let $g(x_1) = \prod_{i=1}^{n}(x_1 - \alpha_i)$. I claim $g(x_1)$ has coefficients in k. Indeed, for any $\sigma \in Gal(\bar{k}/k)$

$$\sigma g(x_1) = \prod_{i=1}^{n}(x_1 - \sigma\alpha_i) = \prod_{i=1}^{n}(x_1 - \alpha_i)$$

with the final equality following from transitivity. Since the coefficients are fixed by $Gal(\bar{k}/k)$ and $\bar{k}/k$ is Galois, they must be contained in k. Let $f(x_1, x_2)$ denote the homogenization of $g(x_1)$. $f(x_1, x_2)$ is a homogenous polynomial whose vanishing set is S. □

Thus, the category of Galois sets provides a more general setting for the theory developed in Section 1. Ultimately, we will show that the important theorems from the first section generalize to all Galois sets.

First we must extend the notion of reduction mod p to Galois sets over $\mathbb{Q}$. Let S be a Galois set contained in $\mathbb{P}^r(\bar{\mathbb{Q}})$. By Proposition 2.1, S is the vanishing set of a finite collection of rational homogenous polynomials, say $f_1(\boldsymbol{x}), f_2(\boldsymbol{x}), ..., f_n(\boldsymbol{x})$. For a fixed prime p, let $\bar{f}_i(\boldsymbol{x})$ denote the polynomial formed by

(1) Clearing the denominators in $f_i(\boldsymbol{x})$ so that all coefficients are integers
(2) Dividing out by all common factors so that the coefficients are coprime
(3) Reducing the resulting coefficients mod p

The $\bar{f}_i(\boldsymbol{x})$ are homogenous polynomials defined over $\mathbb{F}_p$. Their vanishing set is a Galois subset of $\mathbb{P}^r(\mathbb{F}_p)$, which we will call S_p or *the reduction of S mod p*. In general of course, S_p may not be irreducible. However, in the special case where $S \subset \mathbb{P}^1(\bar{\mathbb{Q}})$, S is the vanishing set of a rational polynomial and its behavior under reduction is governed by the theorems from Section 1. In particular, if $\#S$ is prime, then S_p is irreducible for infinitely many p (Proposition 1.5).

It is important to note that Galois isomorphisms reduce to Galois isomorphisms mod p. Indeed, if $\phi : U \to V$ is a Galois isomorphism, both ϕ and ϕ^{-1} are polynomial maps defined over $\mathbb{Q}$ (Proposition 2.2). Hence, $\bar{\phi}$ and $\overline{\phi^{-1}}$ are polynomial maps defined over $\mathbb{F}_p$, inverse to one another.

We will now show that every Galois set is isomorphic to a Galois subset of the projective line. To do this, we will appeal to the following general fact about vector spaces over infinite fields

Lemma 2.1. *Let V be a vector space over an infinite field F. Then the union of finitely many proper subspaces of V is a proper subset of V.*

Proof. We proceed by induction on n. If $n = 1$, the claim is trivially satisfied. Now suppose that for every collection of $n - 1$ proper subspaces of V, their union is proper as well.

Let $\{U_1, U_2, ..., U_n\}$ be a collection of proper subspaces of V. We can assume, without loss of generality, that there are no containments among the U_i. Otherwise, $\bigcup_{i=1}^{n} U_i$ is the union of some collection of $n - 1$ U_i's, which is a proper subset of V by the induction hypothesis.

For each $i \leq n$, the set $\{U_i \cap U_j \mid i \neq j\}$ is a collection of $n-1$ proper subspaces of U_i. Hence, by the induction hypothesis, their union is a proper subset of U_i. Denote by $\widetilde{U_i}$ the nonempty set $U_i - \bigcup_{i \neq j} U_i \cap U_j$.

We will now suppose that $\bigcup_{i=1}^{n} U_i = V$ and derive a contradiction. Let $x_1 \in \widetilde{U_1}$, $x_2 \in \widetilde{U_2}$ and consider the set $S = \{\alpha x_1 + x_2 \mid \alpha \in F\}$. For every $\alpha \in F$ we have $\alpha x_1 \in U_1$ and $x_2 \notin U_1$. Thus, $\alpha x_1 + x_2$ cannot be an element of U_1. It follows that every element of S is contained in some U_i for $i \neq 1$. Since F is infinite, there are infinitely many vectors in S. Thus, by the pigeonhole principle, there are distinct elements $\alpha x_1 + x_2$ and $\beta x_1 + x_2$ contained in the same U_i. Hence, $(\alpha - \beta)x_1 = (\alpha x_1 + x_2) - (\beta x_1 + x_2) \in U_i$, from which it follows that $x_1 \in U_i$, a contradiction. We conclude that $\bigcup_{i=1}^{n} U_i$ is a proper subset of V. □

Proposition 2.4. *Let S be a Galois set contained in $\mathbb{P}^r(\bar{\mathbb{Q}})$. Then there is a Galois set S' contained in $\mathbb{P}^1(\bar{\mathbb{Q}})$ such that $S \cong S'$.*

Proof. We proceed by induction on r. If $r = 1$, the claim is trivially satisfied. Now suppose every Galois subset of $\mathbb{P}^{r-1}(\bar{\mathbb{Q}})$ is isomorphic to a Galois subset of the projective line, and let S be a Galois subset of $\mathbb{P}^r(\bar{\mathbb{Q}})$. It suffices to exhibit an isomorphism f from S onto a Galois subset of $\mathbb{P}^{r-1}(\bar{\mathbb{Q}})$.

We regard $\mathbb{P}^{r-1}(\bar{\mathbb{Q}})$ as a subset of $\mathbb{P}^r(\bar{\mathbb{Q}})$ under the natural identification $[x_1, x_2, ..., x_r] \mapsto [x_1, x_2, ..., x_r, 0]$. We construct the desired isomorphism f by projecting onto $\mathbb{P}^{r-1}(\bar{\mathbb{Q}})$ from an appropriately chosen rational point in $\mathbb{P}^r(\bar{\mathbb{Q}})$.

Let $S = \{P_1, P_2, ..., P_n\}$ and $P_i = [P_i^1, P_i^2, ..., P_i^{r+1}]$ for each $i \leq n$. There are finitely many lines (at most $\binom{n}{2}$) connecting pairs of points in S. For each of these lines, we can intersect with $\mathbb{P}^r(\mathbb{Q})$ to obtain a proper subspace of $\mathbb{P}^r(\mathbb{Q})$. Let U denote the union of these subspaces. By Lemma 2.1, there is a point $P_0 \in \mathbb{P}^r(\mathbb{Q})$ not contained in U or $\mathbb{P}^{r-1}(\mathbb{Q})$. Let $P_0 = [P_0^1, P_0^2, ..., P_0^{r+1}]$. We define $f(P_i)$ to be the (unique) point in the intersection $\overline{P_0 P_i} \cap \mathbb{P}^{r-1}(\bar{\mathbb{Q}})$. Since P_0 is collinear with no two points in S, f is one-to-one. All we need to show is that f is a morphism, i.e. that it respects the Galois action.

The line connecting P_0 and any P_i is the set of points $\{[aP_0^1 + bP_i^1, aP_0^2 + bP_i^2, ..., aP_0^{r+1} + bP_i^{r+1}] \mid a, b \in \bar{\mathbb{Q}}\}$. Hence, $\overline{P_0 P_i}$ intersects $\mathbb{P}^{r-1}(\bar{\mathbb{Q}})$ if and only if $aP_0^{r+1} + bP_i^{r+1} = 0$ and not both a and b are 0. Since $P_0 \notin \mathbb{P}^{r-1}(\bar{\mathbb{Q}})$ by assumption, we have that $P_0^{r+1} \neq 0$. Thus, one can solve for a in the equation above: $a = -b\frac{P_i^{r+1}}{P_0^{r+1}}$. Hence

$$f(P_i) = [bP_i^1 - bP_0^1 \frac{P_i^{r+1}}{P_0^{r+1}}, bP_i^2 - bP_0^2 \frac{P_i^{r+1}}{P_0^{r+1}}, ..., bP_i^r - bP_0^r \frac{P_i^{r+1}}{P_0^{r+1}}, 0]$$

where $b \neq 0$. We can write this out more compactly by dividing all coordinates by b and multiplying by P_0^{r+1}

$$\begin{aligned} f(P_i) &= [P_i^1 P_0^{r+1} - P_0^1 P_i^{r+1}, P_i^2 P_0^{r+1} - P_0^2 P_i^{r+1}, ..., P_i^r P_0^{r+1} - P_0^r P_i^{r+1}, 0] \\ &= [\det\left(\begin{smallmatrix} P_i^1 & P_0^1 \\ P_i^{r+1} & P_0^{r+1} \end{smallmatrix}\right), \det\left(\begin{smallmatrix} P_i^2 & P_0^2 \\ P_i^{r+1} & P_0^{r+1} \end{smallmatrix}\right), ..., \det\left(\begin{smallmatrix} P_i^r & P_0^r \\ P_i^{r+1} & P_0^{r+1} \end{smallmatrix}\right), 0] \end{aligned}$$

Let $\sigma \in G$. Since P_0 is rational and, hence, fixed by σ we have

$$\begin{aligned} f(\sigma P_i) &= [\sigma P_i^1 P_0^{r+1} - P_0^1 \sigma P_i^{r+1}, \sigma P_i^2 P_0^{r+1} - P_0^2 \sigma P_i^{r+1}, ..., \sigma P_i^r P_0^{r+1} - P_0^r \sigma P_i^{r+1}, 0] \\ &= \sigma[P_i^1 P_0^{r+1} - P_0^1 P_i^{r+1}, P_i^2 P_0^{r+1} - P_0^2 P_i^{r+1}, ..., P_i^r P_0^{r+1} - P_0^r P_i^{r+1}, 0] \\ &= \sigma f(P_i) \end{aligned}$$

Hence, f commutes with the action of G and is therefore an isomorphism onto its image. □

We are now prepared to generalize the results from Section 1 to arbitrary Galois sets.

Proposition 2.5. *Let S be an irreducible Galois set of prime cardinality p. Then S_q is irreducible for a positive density of primes.*

Proof. By Proposition 2.4, there is a Galois set S' contained in $\mathbb{P}^1(\bar{\mathbb{Q}})$ such that $S \cong S'$. As noted above, the isomorphism $S \cong S'$ induces an isomorphism $S_q \cong S'_q$ for every prime q. Hence, S_q is irreducible if and only if S'_q is irreducible. By Proposition 2.2, S' has form $\{[\alpha_1, 1], [\alpha_2, 1], ..., [\alpha_p, 1]\}$ where $\alpha_1, \alpha_2, ..., \alpha_p$ are the roots of some irreducible polynomial $f(x) \in \mathbb{Z}[x]$ of prime degree p. Clearly, S'_q is irreducible if and only if $f(x)$ is irreducible mod q. Hence, applying Proposition 1.5: density$\{q$ prime $\mid S_q$ irreducible$\}$ = density$\{q$ prime $\mid$ S'_q irreducible$\}$ = density$\{q$ prime $\mid f(x)$ irreducible mod $q\} > 0$ □

Proposition 2.6. *Let n be any positive composite integer.Then there is an irreducible Galois set S of cardinality n such that S_q is reducible for all but finitely many primes.*

Proof. By Propositions 1.7 and 1.8, there is an irreducible polynomial $f(x) \in \mathbb{Z}[x]$ of degree n which is reducible everywhere. Let $g(x, y)$ be the homogenization of $f(x)$ and S the vanishing set of $g(x, y)$. Then S has cardinality n and S_q is reducible for every prime q not dividing the discriminant of f. □

Next, we would like to generalize the Frobenius density theorem to arbitrary Galois sets. For this, we will need to introduce some notation. For every polynomial there is an associated group, the Galois group over $\mathbb{Q}$ of its splitting field. For Galois sets, there is an analogous construction. As usual, let S be a Galois set and $G = Gal(\bar{\mathbb{Q}}/\mathbb{Q})$. The action of G on S induces a group homomorphism $G \to \mathrm{Perm}(S)$. Let K denote the kernel of this map and let $G_S = G/K$. We will call G_S the *Galois group of S*. If S is a subset of $\mathbb{P}^1(\bar{\mathbb{Q}})$ its points are the roots of some rational polynomial. In this case, the Galois group of the polynomial is the Galois group of S. Indeed, suppose $S = \{[\alpha_1, 1], [\alpha_2, 1], ..., [\alpha_n, 1]\}$ where $\alpha_1, \alpha_2, ..., \alpha_n$ are the roots of some $f(x) \in \mathbb{Q}[x]$. If an element of G fixes every $[\alpha_i, 1]$, it fixes the field $\mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_n)$ and vice versa. Hence, $K = Gal(\bar{\mathbb{Q}}/\mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_n))$, from which it follows that $G_S = G/K = Gal(\mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_n)/\mathbb{Q})$ which is the Galois group of $f(x)$.

Proposition 2.7. *Let S be an irreducible Galois set with n elements. Let $d = (d_1, d_2, ..., d_t)$ be a partition of n, and let R be the set of rational primes q for which the reduction S_q has orbit structure d. Then R is either empty or of positive natural density equal to $1/\#G_S$ times the number of $\sigma \in G_S$ of cycle pattern d (identifying G_S in the natural way with a subgroup of S_n).*

Proof. By Proposition 2.4, there is a Galois set S' contained in $\mathbb{P}^1(\bar{\mathbb{Q}})$ such that $S \cong S'$. By Proposition 2.2, S' has form $\{[\alpha_1, 1], [\alpha_2, 1], ..., [\alpha_n, 1]\}$ where $\alpha_1, \alpha_2, ..., \alpha_n$ are the roots of some irreducible degree-n polynomial $f(x) \in \mathbb{Z}[x]$. As noted above, G_S is simply the Galois group of $f(x)$.

The isomorphism $S \cong S'$ induces an isomorphism $S_q \cong S'_q$ for every prime q. Hence, S_q and S'_q have the same orbit structure. Of course, the orbit structure of S'_q is the decomposition type of $f(x)$ mod q. Thus, the set of primes q for which S_q has orbit structure d is precisely the set of primes for which $f(x)$ mod q has decomposition type d. The result follows from Frobenius. □

For every element s of a Galois set S, define the stabilizer subgroup $\text{Stab}(s) = \{\bar{\sigma} \in G_S \mid \sigma(s) = s\}$. If S is irreducible, the orbit of s is the entirety of S. Thus, the index of $\text{Stab}(s)$ in G_S is the cardinality of S. We have the following proposition:

Proposition 2.8. *Let S be an irreducible Galois set with n elements, including the element s. Then the set of primes q for which S_q is irreducible has positive natural density if and only if Stab(s) admits a cyclic complement in G_S.*

Proof. This is almost exactly the proof of proposition 1.6. For simplicity, identify G_S with its image in S_n. Suppose the set of primes q for which S_q is irreducible has positive natural density. By Proposition 2.7, G_S must contain an n-cycle, σ. Since every element of $\text{Stab}(s)$ fixes s, $\text{Stab}(s)$ is n-cycle-free. Hence, $\langle\sigma\rangle \cap \text{Stab}(s) = \{1\}$. Keeping in mind that $[G_S : \text{Stab}(s)] = n$, we have $\#\langle\sigma\rangle\text{Stab}(s) = \#\langle\sigma\rangle\#\text{Stab}(s) = n(\frac{\#G_S}{n}) = \#G_S$. Hence, $G_S = \langle\sigma\rangle\text{Stab}(s)$, i.e. $\text{Stab}(s)$ admits a cyclic complement in G_S.

Conversely, suppose $\text{Stab}(s)$ admits a cyclic complement, C, in G_S. Let σ generate C. Since G_S is a transitive subgroup of S_n, we have $(G_S)s = S$. But $(G_S)s = C\ \text{Stab}(s)s = Cs = \langle\sigma\rangle s$. It follows that σ is an n-cycle. Then by Proposition 2.7, the set of primes q for which S_q is irreducible has positive natural density. □

3. An Application to Elliptic Curves

Let E be an elliptic curve defined over $\mathbb{Q}$ with no complex multiplication. For any prime ℓ, let $E[\ell]$ denote the ℓ-torsion subgroup, i.e. the set of points on E of order dividing ℓ. Algebraically, $E[\ell]$ is a two-dimensional vector space over $\mathbb{F}_\ell$. Since addition on E is defined by polynomial equations, $E[\ell]$ is a Galois set.

The Galois group $G_{E[\ell]}$ acts on $E[\ell]$ in the natural way. Fixing an isomorphism $E[\ell] \cong \mathbb{F}_\ell^2$, we obtain a faithful representation:

$$\psi_\ell : G_{E[\ell]} \hookrightarrow GL_2(\mathbb{F}_\ell)$$

In fact, ψ_ℓ is an isomorphism for all but finitely many ℓ (see [3]). For now, select ℓ so that ψ_ℓ is an isomorphism. In this case, $E[\ell] - \mathcal{O}$ is irreducible, since $GL_2(\mathbb{F}_\ell)$ acts transitively on $\mathbb{F}_\ell^2 - 0$. Denote by S_ℓ the set of primes modulo which $E[\ell] - \mathcal{O}$ is irreducible. Rosen has demonstrated in [2] that S_ℓ has positive natural density.

Proposition 3.1. *Suppose ℓ is a prime for which ψ_ℓ is an isomorphism (since E has no complex multiplication, this is true for all but finitely many ℓ). Then, S_ℓ has positive natural density.*

Proof. Our proof will closely follow Rosen's. Under the chosen isomorphism $E[\ell] \cong \mathbb{F}_\ell^2$, the column vector $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ corresponds to an element of $E[\ell] - \mathcal{O}$. Let H denote its stabilizer. H is the set of all matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ such that:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Hence, H is the set of all matrices

$$\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}$$

where $b \in \mathbb{F}_\ell$ and $d \in \mathbb{F}_\ell^*$. By Proposition 2.8, it suffices to show that H admits a cyclic complement in $GL_2(\mathbb{F}_\ell)$. Note that H has order $\ell(\ell-1)$. Since $GL_2(\mathbb{F}_\ell)$ has order $(\ell^2-1)(\ell^2-\ell)$, the index of H in $GL_2(\mathbb{F}_\ell)$ is ℓ^2-1. Thus, if H admits a cyclic complement, it must have order ℓ^2-1. The non-split Cartan subgroup is one such cyclic subgroup. To define this group, select a basis for $\mathbb{F}_{\ell^2}$ as a vector space over $\mathbb{F}_\ell$. For any $x \in \mathbb{F}_{\ell^2}^*$, multiplication by x defines an invertible linear map $\mathbb{F}_{\ell^2} \to \mathbb{F}_{\ell^2}$. Let M_x be the matrix associated to this map with respect to the selected basis. The assignment $x \mapsto M_x$ defines an injective group homomorphism $\mathbb{F}_{\ell^2}^* \to GL_2(\mathbb{F}_\ell)$. The image of this homomorphism, which we will denote by C, is the non-split Cartan subgroup. Since C is cyclic of order ℓ^2-1, it suffices to show that $C \cap H = \{I\}$.

Let $C = \langle M \rangle$. Since M has order ℓ^2-1, its eigenvalues are distinct primitive elements of $\mathbb{F}_{\ell^2}^*$. Hence $M = T \left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right) T^{-1}$ for some $T \in GL_2(\mathbb{F}_{\ell^2})$ and α, β primitive in $\mathbb{F}_{\ell^2}^*$. Since 1 is an eigenvalue of every element of H, if $M^n \in H$, ℓ^2-1 divides n, from which it follows that $M^n = I$. Thus, $C \cap H = \{I\}$, as desired.

□

Having established that the density of S_ℓ is positive, the question then becomes: can we evaluate this density precisely? In other words, modulo what proportion of primes is $E[\ell] - \mathcal{O}$ irreducible? In this section, we will derive an explicit formula for the density of S_ℓ.

We begin by analyzing the conjugacy classes in $GL_2(\mathbb{F}_\ell)$. We will consider four separate cases, which together partition $GL_2(\mathbb{F}_\ell)$:

Case 1: M is diagonalizable over $\mathbb{F}_\ell$ with two distinct eigenvalues
Case 2: M is diagonalizable over $\mathbb{F}_\ell$ with one repeated eigenvalue
Case 3: M is non-diagonalizable over $\mathbb{F}_\ell$ with one repeated eigenvalue in $\mathbb{F}_\ell$
Case 4: M is non-diagonalizable over $\mathbb{F}_\ell$ with two distinct, conjugate eigenvalues in $\mathbb{F}_{\ell^2}$

Since the diagonalizability and eigenvalues of a matrix are preserved under conjugation, each case is a union of conjugacy classes. In each case, we will compute: the number of conjugacy classes, the size of each class, the order of a centralizer, and the maximal order of an element.

Case 1. These are matrices conjugate to $\left(\begin{smallmatrix}\alpha & 0\\ 0 & \beta\end{smallmatrix}\right)$, where α and β are distinct elements of $\mathbb{F}_\ell^*$. Hence, conjugacy classes correspond to sets $\{\alpha, \beta\}$ of distinct, nonzero eigenvalues, of which there are $(\ell-1)(\ell-2)/2$. Moreover, since $\alpha, \beta \in \mathbb{F}_\ell^*$, the order of every element divides $\ell - 1$, with equality iff $\mathrm{lcm}(o(\alpha), o(\beta)) = \ell - 1$.

The centralizer of the matrix $\left(\begin{smallmatrix}\alpha & 0\\ 0 & \beta\end{smallmatrix}\right)$ is the subgroup of $GL_2(\mathbb{F}_\ell)$ consisting of all diagonal matrices, which has order $(\ell-1)^2$. Thus, the order of each conjugacy class is given by $(\ell-1)(\ell^2-\ell)/(\ell-1)^2 = \ell(\ell+1)$ Multiplying the number of classes by the order of each class, we see that Case 1 contributes a total of $(\ell-2)(\ell-1)\ell(\ell+1)/2$ matrices to $GL_2(\mathbb{F}_\ell)$.

Case 2. These are matrices conjugate to $\left(\begin{smallmatrix}\alpha & 0\\ 0 & \alpha\end{smallmatrix}\right)$, where $\alpha \in \mathbb{F}_\ell^*$. Thus, Case 2 contains $\ell - 1$ conjugacy classes, one for each nonzero eigenvalue. Moreover, since $\alpha \in \mathbb{F}_\ell^*$, the order of every element divides $\ell - 1$, with equality iff α is primitive.

The centralizer of $\left(\begin{smallmatrix}\alpha & 0\\ 0 & \alpha\end{smallmatrix}\right)$ is the entirety of $GL_2(\mathbb{F}_\ell)$. Hence, every conjugacy class in Case 2 is a singleton (In other words, Case 2 corresponds to the center of $GL_2(\mathbb{F}_\ell)$). Hence, Case 2 contributes $\ell - 1$ matrices to $GL_2(\mathbb{F}_\ell)$.

Case 3. These are matrices conjugate to $\left(\begin{smallmatrix}\alpha & 1\\ 0 & \alpha\end{smallmatrix}\right)$. Hence, Case 3 contains $\ell - 1$ conjugacy classes. Since

$$\begin{pmatrix}\alpha & 1\\ 0 & \alpha\end{pmatrix}^n = \begin{pmatrix}\alpha^n & n\alpha\\ 0 & \alpha^n\end{pmatrix}$$

the order of every matrix divides $\ell(\ell-1)$, with equality iff α is primitive. Suppose $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$ commutes with $\left(\begin{smallmatrix}\alpha & 1\\ 0 & \alpha\end{smallmatrix}\right)$. Hence

$$\begin{pmatrix}a\alpha & a+b\alpha\\ c\alpha & c+d\alpha\end{pmatrix} = \begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}\alpha & 1\\ 0 & \alpha\end{pmatrix} = \begin{pmatrix}\alpha & 1\\ 0 & \alpha\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix} = \begin{pmatrix}a\alpha + c & b\alpha + d\\ c\alpha & d\alpha\end{pmatrix}$$

Thus, $c = 0$ and $a = d$. It follows that the centralizer of $\left(\begin{smallmatrix}\alpha & 1\\ 0 & \alpha\end{smallmatrix}\right)$ is the set of matrices $\left(\begin{smallmatrix}a & b\\ 0 & b\end{smallmatrix}\right)$, where $a \in \mathbb{F}_\ell$ and $b \in \mathbb{F}_\ell^*$. Thus, the centralizer of a Case 3 matrix has order $\ell(\ell-1)$. It follows that each conjugacy class has order $\ell^2 - 1$. So, Case 3 contributes a total of

$(\ell-1)^2(\ell+1)$ matrices to $GL_2(\mathbb{F}_\ell)$.

Case 4. Conjugacy classes in Case 4 correspond to irreducible characteristic polynomials, of which there are $(\ell^2-\ell)/2$. The order of a matrix divides ℓ^2-1, since the eigenvalues are contained in $\mathbb{F}_{\ell^2}^*$. Equality is obtained iff either eigenvalue is primitive (in this case, both eigenvalues are primitive, since the eigenvalues are conjugates of another). Since Cases 1 through 4 partition $GL_2(\mathbb{F}_\ell)$, we can compute the total contribution from Case 4 by subtracting the contributions from Cases 1 through 3 from the order of $GL_2(\mathbb{F}_\ell)$:

$$(\ell^2-1)(\ell^2-\ell)-[(\ell-2)(\ell-1)\ell(\ell+1)/2+(\ell-1)+(\ell-1)^2(\ell+1)]=\frac{\ell^2(\ell-1)^2}{2}$$

Hence, each class in Case 4 has order

$$(\frac{\ell^2(\ell-1)^2}{2})/(\frac{\ell^2-\ell}{2})=\ell^2-\ell$$

Thus, the order of a centralizer is $(\ell^2-1)(\ell^2-\ell)/(\ell^2-\ell)=\ell^2-1$.

These results are summarized in the following table:

Case	# of Classes	Class Size	Order of a Centralizer	Total Contribution
1	$(\ell-1)(\ell-2)/2$	$\ell(\ell+1)$	$(\ell-1)^2$	$(\ell-2)(\ell-1)\ell(\ell+1)/2$
2	$\ell-1$	1	$(\ell^2-1)(\ell^2-\ell)$	$\ell-1$
3	$\ell-1$	ℓ^2-1	$\ell(\ell-1)$	$(\ell-1)^2(\ell+1)$
4	$(\ell^2-\ell)/2$	$\ell^2-\ell$	ℓ^2-1	$\ell^2(\ell-1)^2/2$

We are now prepared to compute the density of S_ℓ. Let D denote the number of ℓ^2-1 cycles in $GL_2(\mathbb{F}_\ell)$. By Frobenius (Proposition 2.7), the density of S_ℓ is D divided by the order of $GL_2(\mathbb{F}_\ell)$.

First, note that every generator of C is an ℓ^2-1 cycle. Indeed, if x is a generator, $\langle x\rangle\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)=\langle x\rangle H\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)=CH\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)=GL_2(\mathbb{F}_\ell)\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)=\mathbb{F}_\ell^2-0$. Hence, D is at least $\varphi(\ell^2-1)$, where φ is the Euler phi-function. But we can do better. Let B be any subgroup conjugate to C. Since the order of C is not in general prime, the intersection $B\cap C$ may be nontrivial. However, no generator in one is also contained in the other. Being conjugate to the generators of C, the generators of B must also be ℓ^2-1 cycles. Thus, if k is the number of subgroups conjugate to C, D is at least $k\varphi(\ell^2-1)$. We now proceed to compute the integer k.

Lemma 3.1. $Z(C)=C$

Proof. Since C is abelian, $C\subseteq Z(C)$. Hence, $\ell^2-1\leq \#Z(C)$. On the other hand, $Z(C)\subseteq Z(x)$ for every $x\in C$. Suppose x generates C, so that its order is ℓ^2-1. Thus, x is diagonalizable over $\mathbb{F}_{\ell^2}$ with distinct, primitive eigenvalues. In particular, x is Case 4, and its centralizer has order ℓ^2-1. Thus, $\#Z(C)\leq\ell^2-1$, which forces $Z(C)=\ell^2-1$. □

Proposition 3.2. $\#N(C) = 2(\ell^2 - 1)$

Proof. Let x be an element of the normalizer. Conjugation by x induces a group automorphism $\lambda_x : C \to C$. Since $C \cong \mathbb{F}_{\ell^2}^*$, λ_x corresponds to a group automorphism $\mathbb{F}_{\ell^2}^* \to \mathbb{F}_{\ell^2}^*$, which extends to a field automorphism $\mathbb{F}_{\ell^2} \to \mathbb{F}_{\ell^2}$, since λ_x respects addition. Thus, we obtain a group homomorphism:

$$\lambda : N(C) \longrightarrow Gal(\mathbb{F}_{\ell^2}/\mathbb{F}_\ell) = \langle \sigma_\ell : t \mapsto t^\ell \rangle$$

The kernel of this map is the centralizer of C, which, by the lemma, is simply C. I claim, in addition, that this map is surjective. Let M generate C, so that

$$M = T \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^\ell \end{pmatrix} T^{-1}$$

for $T \in GL_2(\mathbb{F}_{\ell^2})$ and α primitive in $\mathbb{F}_{\ell^2}^*$. Hence

$$\sigma_\ell(M) = M^\ell = T \begin{pmatrix} \alpha^\ell & 0 \\ 0 & \alpha^{\ell^2} \end{pmatrix} T^{-1} = T \begin{pmatrix} \alpha^\ell & 0 \\ 0 & \alpha \end{pmatrix} T^{-1}$$

Since M and $\sigma_\ell(M)$ have the same set of eigenvalues, namely α and α^ℓ, they must belong to the same conjugacy class. In other words, there is a matrix $Q \in GL_2(\mathbb{F}_\ell)$ such that $\sigma_\ell(M) = QMQ^{-1}$. For any $M^n \in C$ we have

$$\sigma_\ell(M^n) = (\sigma_\ell M)^n = (QMQ^{-1})^n = QM^nQ^{-1}$$

So, in fact, $\lambda_Q = \sigma_\ell$. Thus, λ is surjective, and the following sequence is exact:

$$0 \longrightarrow C \to N(C) \longrightarrow Gal(\mathbb{F}_{\ell^2}/\mathbb{F}_\ell) \longrightarrow 0$$

Hence, $N(C) = \langle C, Q \rangle$ and $\#N(C) = \#Gal(\mathbb{F}_{\ell^2}/\mathbb{F}_\ell)\#C = 2(\ell^2 - 1)$.

□

The number of subgroups conjugate to C is the index of its normalizer in $GL_2(\mathbb{F}_\ell)$. Since $\#N(C) = 2(\ell^2 - 1)$, there are

$$[GL_2(\mathbb{F}_\ell) : N(C)] = \frac{(\ell^2-1)(\ell^2-\ell)}{2(\ell^2-1)} = \frac{\ell^2-\ell}{2}$$

subgroups conjugate to C. As noted above, each conjugate contributes $\varphi(\ell^2 - 1)$ $\ell^2 - 1$ cycles. Thus, D is bound by

$$D \geq \frac{(\ell^2-\ell)\varphi(\ell^2-1)}{2}$$

On the other hand, D is bound above by the number of elements in $GL_2(\mathbb{F}_\ell)$ of order $\ell^2 - 1$.

Proposition 3.3. *$GL_2(\mathbb{F}_\ell)$ contains $\frac{(\ell^2-\ell)\varphi(\ell^2-1)}{2}$ elements of order $\ell^2 - 1$.*

Proof. Let R denote the set of matrices of order $\ell^2 - 1$. R is invariant under conjugation, and is thus a union of conjugacy classes. Each conjugacy class in R corresponds to a set $\{\alpha, \beta\}$ of conjugate, primitive eigenvalues in $\mathbb{F}_{\ell^2}^*$, of which there are $\varphi(\ell^2 - 1)/2$. Moreover, each conjugacy class has order $\ell^2 - \ell$ (see table on previous page). Thus, R has order $\frac{(\ell^2-\ell)\varphi(\ell^2-1)}{2}$. □

Thus, the number of $\ell^2 - 1$ cycles in $GL_2(\mathbb{F}_\ell)$ is exactly $\frac{(\ell^2-\ell)\varphi(\ell^2-1)}{2}$ (note: we have inadvertently shown that *every* matrix of order $\ell^2 - 1$ is an $\ell^2 - 1$ cycle!). It follows from Proposition 2.7 that the density of S_ℓ is given by

$$\frac{D}{\#GL_2(\mathbb{F}_\ell)} = \frac{(\ell^2 - \ell)\varphi(\ell^2 - 1)/2}{(\ell^2 - 1)(\ell^2 - \ell)} = \frac{\varphi(\ell^2 - 1)}{2(\ell^2 - 1)}$$

References

[1] R. Guralnick, M. Schacher, and J. Sonn, *Irreducible Polynomials Which are Locally Reducible Everywhere.* Proceedings of the American Mathematical Society **133** (2005)

[2] M. Rosen, *Polynomials Modulo P and the Theory of Galois Sets.* Theory and Applications of Finite Fields **10** (2011)

[3] J-P Serre, *Proprietes Galoisiennes des Points D'ordre Finis des Courbes Elliptiques.* Invent. Math. **15** (1972)