In this lecture we prove the existence and uniqueness of finite fields and then demonstrate some basic properties of finite fields.

1 Review of Algebraic Closure

Recall that the ***algebraic closure*** of a field F is an extension Ω of F such that all polynomials $f \in F[x]$ have a root in Ω.

Fact 1.1. (a) The algebraic closure of $\mathbb{F}_p$, denoted $\overline{\mathbb{F}_p}$, exists.
(b) For any extension $K \supseteq \mathbb{F}_p$ there is a subfield of $\overline{\mathbb{F}_p}$ isomorphic to K.

Proof sketch. We argue that the algebraic closure exists using ***Zorn's Lemma***. Zorn's lemma (which is equivalent to the Axiom of Choice) allows us to find a maximal element in posets with a certain property. In particular, Zorn's Lemma states that if every chain in poset $\mathcal{P}$ has an upper bound, then there is a maximal element in $\mathcal{P}$. Consider the poset consisting of all extensions of $\mathbb{F}_p$, ordered by "containment". Formally, for extensions $K, L \supseteq \mathbb{F}_p$ we say $K \preceq L$ if K is isomorphic to a subfield of L. Given a chain $K_1 \prec K_2 \prec K_3 \prec \cdots$ we can informally write $\bigcup_{i\in\mathbb{N}} K_i$ as the upper bound for the chain. (More formally we should write $\varinjlim K_i$). Thus, Zorn's lemma applies and we can find a maximal element in this poset. Call this maximal element Ω. We claim that Ω is algebraically closed. Indeed, if there were some polynomial $f \in \mathbb{F}_p[x]$ with no root in Ω then we could adjoin a root of f to Ω to obtain a larger field extension, contradicting the maximality of Ω.

The second property, that for any extension $K \supseteq \mathbb{F}_p$ there is a subfield of Ω isomorphic to K, is clear by the above construction of Ω.

We remark that the algebraic closure is unique up to isomorphism. $\square$

2 Existence and Uniqueness of Finite Fields

Theorem 2.1. (a) Let K be a finite field. Then K has prime characteristic, and $|K|$ is a prime power.
(b) Let q be a power of prime p. There is a unique subfield $\mathbb{F}_q$ of $\overline{\mathbb{F}_p}$ with q elements, namely $\left\{x \in \overline{\mathbb{F}_p} \;\middle|\; x^q = x\right\}$.
(c) All finite fields of order q are isomorphic to $\mathbb{F}_q$.

Proposition 2.2. Finite fields have prime characteristic and prime power order.

Proof. If the characteristic were not prime then there would be non-zero zero-divisors, which is impossible. So the characteristic must be prime.

Recall that K is a vector space over $\mathbb{F}_p$. If the dimension of K as an $\mathbb{F}_p$ vector space is r, then $|K| = p^r$. $\square$

Lemma 2.3. $x \mapsto x^q$ is an automorphism of $\overline{\mathbb{F}_p}$.

Proof. We must check that the map is a homomorphism with respect to $+, \cdot$ and that it is a bijection.

- By the binomial formula, and the fact that $p \mid \binom{p}{k}$ for any integer $k \in [1, p-1]$ we have

$$(x+y)^q = x^q + y^q.$$

- Trivially $(xy)^q = x^q y^q$.
- Finally, again using the binomial formula we have that $(x-y)^q = x^q + (-1)^q y^q$. Thus, $x^q = y^q$ if and only if $(x-y)^q = 0$, or equivalently $x = y$[1].

$\square$

Lemma 2.4. The set of points fixed by an automorphism $\phi : F \to F$ is a subfield of F.

Proof. We must verify that this set is closed under addition, multiplication, and taking additive and multiplicative inverses.

- First, observe that $\phi(1) = 1, 0 = \phi(0) = \phi(1-1) = \phi(1) + \phi(-1) = 1 + \phi(-1)$, so $\phi(-1) = -1$.
- If $\phi(x) = x, \phi(y) = y$ then $\phi(x+y) = \phi(x) + \phi(y) = x + y$, and $\phi(xy) = \phi(x)\phi(y) = xy$.

[1] To see this it is helpful to consider the case of even and odd characteristic separately.

- If $\phi(x) = x$ then $\phi(-x) = \phi(-1)\phi(x) = -x$, and $\phi(x^{-1})x = \phi(x^{-1})\phi(x) = \phi(x^{-1}x) = \phi(1) = 1$, so $\phi(x^{-1}) = x^{-1}$.

∎

Claim 2.5. $x^q - x$ has q distinct roots in $\overline{\mathbb{F}_p}$.

Proof. $\frac{d}{dx}(x^q - x) = -1$. If $x^q - x$ had a repeated root then it would have zero derivative at the root. Hence the polynomial has no repeated roots. Over a field, a degree-q polynomial has q roots (counted with multiplicity). Hence $x^q = x$ has q distinct roots in $\overline{\mathbb{F}_p}$. ∎

Corollary 2.6. $\mathbb{F}_q = \left\{x \in \overline{\mathbb{F}_p} \mid x^q = x\right\}$ is a field of order q.

Proof. This is immediate by combining Lemma 2.3, Lemma 2.4, and Claim 2.5. ∎

Proposition 2.7. $\mathbb{F}_q$ is the unique subfield of $\overline{\mathbb{F}_p}$ of order q.

Proof. Let K be a subfield of $\overline{\mathbb{F}_p}$ of order q. Then by Lagrange's theorem $x^{q-1} = 1$ for all $x \in K^\times$, and $x^q = x$ for all $x \in K$. Hence, $K \subseteq \mathbb{F}_q$ where $\mathbb{F}_q$ is the field defined in Corollary 2.6. But $|K| = |\mathbb{F}_q|$ so we must have $K = \mathbb{F}_q$. ∎

Proposition 2.8. There is a unique field of order q up to isomorphism.

Proof. Recall Fact 1.1: for any field extension K of $\mathbb{F}_p$ there is a subfield K' of $\overline{\mathbb{F}_p}$ isomorphic to K. Thus, if we have any two field extensions K_1, K_2 of order q then they are both isomorphic to the unique – as was proven in Proposition 2.7 – subfield of $\overline{\mathbb{F}_p}$ of order q, and hence are also isomorphic to each other. ∎

3 The Multiplicative group of $\mathbb{F}_q$

Theorem 3.1. $\mathbb{F}_q^\times$ is cyclic.

Lemma 3.2. For any $n \in \mathbb{N}$,

$$\sum_{d|n} \phi(d) = n.$$

Proof. Partition $[n]$ into subsets S_d where S_d is the set of $x \in [n]$ with $\gcd(x, n) = d$. Then $|S_d| = \phi(n/d)$. Thus,

$$n = \sum_{d|n} |S_d| = \sum_{d|n} \phi(n/d) = \sum_{d|n} \phi(d).$$

∎

Proposition 3.3. For any $d \mid q-1$, the number of order-d elements of $\mathbb{F}_q^\times$ is either $\phi(d)$ or 0.

Proof. Suppose there is some $x \in \mathbb{F}_q^\times$ of order d. Then (x) (the subgroup generated by x) is an order d subgroup of $\mathbb{F}_q^\times$. Observe that all $y \in (x)$ satisfy $y^d = 1$. Thus (x) is a set of d solutions to $y^d = 1$. Furthermore, because $\mathbb{F}_q$ is a field, there are at most d solutions to $y^d = 1$. In particular, that means that all elements $y \in \mathbb{F}_q^\times$ of order d are contained in (x), because such an element must satisfy $y^d = 1$.

If $y = x^i$ for some $i \in [d]$ and $\gcd(i, d) \neq 1$ then the order of y must be smaller than d. All elements $y = x^i$ with $\gcd(i, d) = 1$ are indeed of order d. Thus, the number of elements of order d is precisely $\phi(d)$ (i.e., $|\mathbb{Z}_d^\times|$). ∎

Corollary 3.4. $|\mathbb{F}_q^\times|$ is cyclic.

Proof. Applying Proposition 3.3 and Lemma 3.2 we find

$$|\mathbb{F}_q^\times| \le \sum_{d|q-1} \phi(d) = q - 1.$$

But of course $|\mathbb{F}_q^\times| = q - 1$. So $\mathbb{F}_q^\times$ must have exactly $\phi(d)$ elements of order d for all $d \mid q-1$. In particular, $\mathbb{F}_q^\times$ has $\phi(q-1) \ge 1$ elements of order $q-1$. ∎