M3P8 LECTURE NOTES 6: FINITE FIELDS

1. Finite Fields

Let K be a finite field; that is, a field with only finitely many elements. Then K has characteristic p for some prime p, and is in particular a finite dimensional $\mathbb{F}_p$ vector space. Thus its order is a power p^r of p.

If we fix a particular prime power p^r, then two questions naturally arise: does there exist a field of order p^r? If so, can we classify fields of order p^r up to isomorphism? We will see that in fact, up to isomorphism, there is a unique field of order p^r.

2. The Frobenius Automorphism

Let p be a prime. For any ring R, the map $x \mapsto x^p$ on R certainly satisfies $(xy)^p = x^p y^p$. On the other hand,

$$(x+y)^p = x^p + \binom{p}{1} x^{p-1} y + \binom{p}{2} x^{p-2} y^2 + \cdots + y^p.$$

The binomial coefficients $\binom{p}{r}$ are divisible by p for $1 \leq r \leq p-1$, so if R has characteristic p, we have $(x+y)^p = x^p + y^p$. Thus, when R has characteristic p, the map $x \mapsto x^p$ is a ring homomorphism from R to R, called the *Frobenius endomorphism* of R.

If R is a field of characteristic p, then the Frobenius endomorphism is injective. If in addition R is finite, then any injective map from R to R is surjective; in particular the Frobenius endomorphism is an isomorphism from R to R when R is a finite field of characteristic p. In this case we call the map $x \mapsto x^p$ the Frobenius *automorphism.*

Composing the Frobenius endomorphism with itself, we find that for any r, $x \mapsto x^{p^r}$ is also an endomorphism of any ring R of characteristic p.

We have:

Proposition 2.1. *Let K be a field of characteristic p, such that $\alpha^{p^r} = \alpha$ for all $\alpha \in K$. Let $P(X)$ be an irreducible factor of $X^{p^r} - X$ over $K[X]$. Then every element β of $K[X]/\langle P(X)\rangle$ satsifies $\beta^{p^r} - \beta$.*

Proof. Let L be the subset of $K[X]/\langle P(X)\rangle$ consisting of all β such that $\beta^{p^r} = \beta$. Then L contains K. Moreover, since $P(X) = 0$ in $K[X]/\langle P(X)\rangle$ and $P(X)$ divides $X^{p^r} - X$, we have $X^{p^r} = X$ in $K[X]/\langle P(X)\rangle$. On the other hand, L is closed under addition, since if β, γ lie in L, then $(\beta+\gamma)^{p^r} = \beta^{p^r} + \gamma^{p^r} = \beta + \gamma$. Similarly L is closed under multiplication. Thus L must be all of $K[X]/\langle P(X)\rangle$. □

Corollary 2.2. *There exists a field K of characteristic p such that:*

(1) *$\alpha^{p^r} = \alpha$ for all $\alpha \in K$, and*
(2) *the polynomial $X^{p^r} - X$ of $K[X]$ factors into linear factors.*

Proof. We construct a tower of fields $K_0 = \mathbb{F}_p \subsetneq K_1 \subsetneq K_2$ satisfying (1) as follows: Suppose we have constructed K_i. If $X^{p^r} - X$ factors into linear factors over $K_i[X]$ we are done. Otherwise, choose a nonlinear irreducible factor $P(X)$ of $X^{p^r} - X$ in $K_i[X]$, and set $K_{i+1} = K_i[X]/P(X)$. Then K_{i+1} is strictly larger than K_i and still satisfies (1). On the other hand, in any field satisfying (1), every element is a root of $X^{p^r} - X$. Since this polynomial can have at most p^r roots, this process must eventually terminate. □

Since $X^{p^r} - X$ has degree p^r, we expect the field K constructed above to have p^r elements. To prove this we need an additional tool.

3. Derivatives

Definition 3.1. Let R be a ring, and let $P(X) = r_0 + r_1 X + \cdots + r_n X^n$ be an element of $R[X]$. The *derivative* $P'(X)$ of $P(X)$ is the polynomial $r_1 + 2r_2 X + \cdots + nr_n X^{n-1}$.

Note that just as for differentiation in calculus, we have a Leibnitz rule: $(PQ)'(X) = P(X)Q'(X) + Q(X)P'(X)$. From this we deduce:

Lemma 3.2. *Let K be a field, and let $P(X)$ be a polnyomial in $K[X]$ with a multiple root in K. Then $P(X)$ and $P'(X)$ have a common factor of degree greater than zero.*

Proof. Let a be the multiple root; then we can write $P(X) = (X-a)^2 Q(X)$. Applying the Leibnitz rule we get $P'(X) = 2(X-A)Q(X) + (X-A)^2 Q'(X)$ and it is clear that $X - a$ divides both $P(X)$ and $P'(X)$. □

Corollary 3.3. *Let K be a field of characteristic p. Then $X^{p^r} - X$ has no repeated roots in K.*

Proof. Let $P(X) = X^{p^r} - X$. Then $P'(X) = -1$, so $P(X)$ and $P'(X)$ have no common factor. □

Corollary 3.4. *There exists a finite field of p^r elements.*

4. The multiplicative group

Rather than show immediately that there is a unique finite field of p^r elements, we make a detour to study the multiplicative group of a finite field. This is not strictly necessary to prove uniqueness, but will simplify the proof, and is of interest in its own right.

Let K denote a field of p^r elements. The goal of this section is to show that $K^\times$ is cyclic. Note that $K^\times$ is an abelian group of order $p^r - 1$, so by Lagrange's theorem, we have $a^{p^r - 1} = 1$ for all $a \in \mathbb{F}_{p^r}^\times$.

Recall that the order of an element a of $K^\times$ is the smallest positive integer d such that $a^d = 1$. Since $a^{p^r-1} = 1$, the order of a is a divisor of $p^r - 1$. On the other hand, if d is a divisor of $p^r - 1$, then any element of order dividing d is a root of the polynomial $X^d - 1$. But if $p^r - 1 = de$, then we can write

$$X^{p^r} - X = X(X^d - 1)(X^{d(e-1)} + X^{d(e-2)} + \cdots + X^d + 1)$$

and since $X^{p^r} - X$ factors into distinct linear factors over K, $X^d - 1$ also factors into distinct linear factors over K. Thus, for any d dividing $p^r - 1$, there are *exactly* d elements of $K^\times$ of order dividing d.

In fact, we have the following:

Proposition 4.1. *Let A be an abelian group of order n, and suppose that A has exactly d elements of order dividing d, for all d dividing n. Then A is cyclic.*

The remainder of this section will be devoted to proving this proposition. As a corollary, we deduce that the multiplicative group of any finite field is cyclic.

Consider the cyclic group $\mathbb{Z}/n\mathbb{Z}$. The order of any element in this group is a divisor of n. We let $\Phi(n)$ denote the number of elements of $\mathbb{Z}/n\mathbb{Z}$ of exact order n. Since $[1]$ in $\mathbb{Z}/n\mathbb{Z}$ has order n, $\Phi(n)$ is nonzero.

Lemma 4.2. *For any d dividing n, the cyclic group $\mathbb{Z}/n\mathbb{Z}$ contains a unique subgroup of order d.*

Proof. The cyclic subgroup of $\mathbb{Z}/n\mathbb{Z}$ generated by $\frac{n}{d}$ is clearly a subgroup of order d. Conversely, if x is an element of a subgroup of $\mathbb{Z}/n\mathbb{Z}$ of order d, then the order of x divides d, so dx is divisible by n, and hence (by unique factorization) x is divisible by $\frac{n}{d}$. Thus x is in the subgroup of $\mathbb{Z}/n\mathbb{Z}$ generated by $\frac{n}{d}$ and the claim follows. □

As a consequence, we deduce that for any d dividing n, $\Phi(d)$ is the number of elements of $\mathbb{Z}/n\mathbb{Z}$ of order d.

Corollary 4.3. *For any n, we have*

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

Proof. Since every element of $\mathbb{Z}/n\mathbb{Z}$ has order d for some d dividing n, the sum over all d dividing n of the number of elements of order d is just the number of elements of $\mathbb{Z}/n\mathbb{Z}$, which is n. □

Proof of the Proposition: We must show that A contains an element of order n. In fact, we will show, by induction on d, that A contains $\Phi(d)$ elements of order d for all d. Since $\Phi(n)$ is nonzero this suffices.

If $d = 1$, the only element of order 1 is the identity of A; since $\Phi(1) = 1$ the base case holds.

Assume the claim is true for all $d' < d$. The number of elements of A of order dividing d is d, so the number of elements of exact order d is $d - \sum_{d'|d, d'<d} \Phi(d')$. By the corollary this is precisely $\Phi(d)$. □

5. Uniqueness

We now turn to the question of showing that any two fields of p^r elements are isomorphic. Let K be such a field. The cyclicity of $K^\times$ immediately shows:

Proposition 5.1. *Any finite field K of characteristic p is generated over $\mathbb{F}_p$ by a single element.*

Proof. Let α be an element of K, that generates $K^\times$ as an abelian group. Then $\mathbb{F}_p(\alpha)$ is contained in K, but contains α^n for all n, so $K = \mathbb{F}_p(\alpha)$. □

As a corollary, we deduce:

Proposition 5.2. *For any prime p and any $d > 0$, there exists an irreducible polynomial of degree d in $\mathbb{F}_p[X]$.*

Proof. Let K be a finite field of p^d elements, and let α be an element of K that generates K over $\mathbb{F}_p$. We then have a surjective map

$$\mathbb{F}_p[X] \to K$$

taking X to α; its kernel is generated by an irreducible polynomial $P(X)$ of degree d. □

We also have the following trick:

Let $P(X)$ be an irreducible polynomial of degree r in $\mathbb{F}_p[X]$. Then $\mathbb{F}_p[X]/\langle P(X)\rangle$ is a field K of order p^r. Hence $X^{p^r} - X$ is zero for in K. Thus $P(X)$ divides $X^{p^r} - X$. We thus have:

Lemma 5.3. *Every irreducible polynomial of degree r in $\mathbb{F}_p[X]$ is a divisor of $X^{p^r-1} - 1$.*

Corollary 5.4. *Any two finite fields K, K' of cardinality p^r are isomorphic.*

Proof. Choose $\alpha \in K$ such that α generates K over $\mathbb{F}_p$. We can then write $K \cong \mathbb{F}_p[X]/\langle P(X)\rangle$, where $P(X)$ is the minimal polynomial of α. In particular $P(X)$ is irreducible of degree R. Since $P(X)$ divides $X^{p^r-1} - 1$ in $\mathbb{F}_p[X]$, it also divides $X^{p^r-1} - 1$ in $K'[X]$; since in $K'[X]$ the latter factors into linear factors, there exists a root α' of $P(X)$ in $K'[X]$. Then the map $\mathbb{F}_p[X] \to K'$ that sends X to α' induces a map:

$$\mathbb{F}_p[X]/\langle P(X)\rangle \to K'.$$

Since this is a map of fields it is injective; since both fields have the same cardinality it is also surjective. □