Chapter 7

Finite fields

7.1 The order of a finite field

Definition 7.1. *The* characterisitic *of a ring A is the additive order of 1, ie the smallest integer $n > 1$ such that*

$$n \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{n \text{ terms}} = 0,$$

if there is such an integer, or ∞ if there is not.

Examples: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ all have infinite characteristic.
$\mathbb{F}_p = \mathbb{Z}/(p)$ has characteristic p.

Proposition 7.1. *The characteristic of an integral domain A is either a prime p, or else ∞.*

In particular, a finite field has prime characteristic.

Proof. Suppose A has characteristic $n = ab$ where $a, b > 1$. By the distributive law,

$$\underbrace{1 + \cdots + 1}_{n \text{ terms}} = (\underbrace{1 + \cdots + 1}_{a \text{ terms}})(\underbrace{1 + \cdots + 1}_{b \text{ terms}}).$$

Hence

$$\underbrace{1 + \cdots + 1}_{a \text{ terms}} = 0 \text{ or } \underbrace{1 + \cdots + 1}_{b \text{ terms}} = 0,$$

contrary to the minimal property of the characteristic. □

Proposition 7.2. *Suppose the finite field F has characteristic p. Then F contains p^n elements, for some n.*

Proof. The elements $\{0, 1, 2, \ldots, p-1\}$ form a subfield of F isomorphic to $\mathbb{F}_p$. We can consider F as a vector space over this subfield. Let $e_1, e_2, \ldots, e_n$ be a basis for this vector space. Then the elements of F are

$$x_1e_1 + x_2e_2 + \cdots + x_ne_n \qquad (0 \le x_1, x_2, \ldots, x_n < p).$$

Thus the order of F is p^n. □

7.2 On cyclic groups

Let us recall some results from elementary group theory.

Proposition 7.3. *The element g^i in the cyclic group C_n has order $n/\gcd(n,i)$.*

Proof. This follows from

$$(g^i)^e = 1 \iff n \mid ie \iff \frac{n}{\gcd(n,i)} \mid e.$$

□

Corollary 7.1. *C_n contains $\phi(n)$ generators, namely the elements g^i with $0 \le i < n$ for which $\gcd(n,i) = 1$.*

Proposition 7.4. *The cyclic group $C_n = \langle g \rangle$ has just one subgroup of each order $d \mid n$, namely the cyclic subgroup $C_d = \langle g^{n/d} \rangle$.*

Proof. Suppose $g^i \in H$, where $H \subset C_n$ is a subgroup of order d, Then

$$(g^i)^d = g^{id} = 1 \implies n \mid id \implies n/d \mid i \implies g^i \in C_n.$$

Thus $H \subset C_n \implies H = C_n$, since the two subgroups have the same order. □

7.3 Möbius inversion

This is a technique which has many applications in number theory and combinatorics. Recall that the Möbius function $\mu(n)$ is defined for positive integers n by

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ has a square factor} \\ (-1)^r & \text{if } n \text{ is square-free and has } r \text{ prime factors} \end{cases}$$

Thus

$$\mu(1) = 1,\ \mu(2) = -1,\ \mu(3) = -1,\ \mu(4) = 0,\ \mu(5) = -1,$$
$$\mu(6) = 1,\ \mu(7) = -1,\ \mu(8) = 0,\ \mu(9) = 0,\ \mu(10) = 1.$$

Theorem 7.1. *Given an arithmetic function $f(n)$, suppose*

$$g(n) = \sum_{d \mid n} f(n).$$

Then

$$f(n) = \sum_{d \mid n} \mu(n/d) g(n).$$

Proof. Given arithmetic functions $u(n), v(n)$ let us defined the arithmetic function $u \circ v$ by

$$(u \circ v)(n) = \sum_{d|n} u(d)v(n/d) = \sum_{n=xy} u(x)v(y).$$

(Compare the convolution operation in analysis.) This operation is commutative and associative, ie $v \circ u = u \circ v$ and $(u \circ v) \circ w = u \circ (v \circ w)$. (The latter follows from

$$((u \circ v) \circ w)(n) = \sum_{n=xyz} u(x)v(y)w(z).)$$

Lemma 7.1. *We have*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Suppose $n = p_1^{e_1} \cdots p_n^{e_n}$. Then it is clear that only the factors of $p_1 \cdots p_r$ will contribute to the sum, so we may assume that $n = p_1 \cdots p_r$.

But in this case the terms in the sum correspond to the terms in the expansion of

$$\underbrace{(1-1)(1-1)\cdots(1-1)}_{r \text{ products}}$$

giving 0 unless $r = 0$, ie $n = 1$. ◻

Let us define $\delta(n)$, $\epsilon(n)$ by

$$\delta(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise,} \end{cases}$$
$$\epsilon(n) = 1 \text{ for all } n$$

It is easy to see that

$$\delta \circ f = f$$

for all arithmetic functions f. Also the lemma above can be written as

$$\mu \circ \epsilon = \delta,$$

while the result we are trying to prove is

$$g = \epsilon \circ f \implies f = \mu \circ g.$$

This follows since

$$\mu \circ g = \mu \circ (\epsilon \circ f) = (\mu \circ \epsilon) \circ f = \delta \circ f = f.$$

◻

7.4 Primitive roots

Theorem 7.2. *The multiplicative group $F^\times = F \setminus \{0\}$ of a finite field F is cyclic.*

Proof. If F has order p^b then $F^\times$ has order $p^n - 1$. It follows (by Lagrange's Theorem) that all the elements of $F^\times$ satisfy

$$x^{p^n-1} = 1,$$

ie

$$U(x) = x^{p^n-1} - 1 = 0.$$

Since this polynomial has degree $p^n - 1$, and we have $p^n - 1$ roots, it factorizes completely into linear terms:

$$U(x) = \prod_{a \in F^\times} (x - a).$$

Now suppose $d \mid p^n - 1$. Since

$$f(x) = x^d - 1 \mid U(x)$$

it follows that $x^d - 1$ factorizes completely into linear terms, say

$$f(x) = \prod_{0 \le i < d} (x - a_i).$$

Lemma 7.2. *Suppose there are $\sigma(d)$ elements of order d in $F^\times$. Then*

$$\sum_{e \mid d} \sigma(e) = d.$$

Proof. Any element of order $e \mid d$ must satisfy the equation $f(x) = 0$; and conversely any root of the equation must be of order $e \mid d$. The result follows on adding the elements of each order. □

Lemma 7.3. *We have*

$$\sum_{e \mid d} \phi(e) = d.$$

Proof. Since the function $\phi(d)$ is multiplicative, so (it is easy to see) is $\sum_{e \mid d} \phi(d)$. Hence it is only necessary to prove the result for $d = p^n$, ie to show that

$$\phi(p^d) + \phi(p^{d-1}) + \cdots + \phi(1) = p^d,$$

which follows at once from the fact that $\phi(p^n) = p^n - p^{n-1}$. □

From the two Lemmas, on applying Möbius inversion,

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

In particular,

$$\sigma(p^n - 1) = \phi(p^n - 1) \geq 1,$$

from which the theorem follows, since any element of this order will generate $F^\times$. □

Remarks:

1. It is not necessary to invoke Möbius inversion to deduce from the two Lemmas that $\sigma(d) = \phi(d)$, since it follows by simple induction that if the result holds for $e < d$ then it holds for d.

2. For a slight variant on this proof, suppose $a \in F^\times$ has order d. Then a satisfies the equation $f(x) = x^d - 1 = 0$, as do the d elements $a^i (0 \leq i < d)$. Moreover any element of order d satisfies this equation. It follows that the elements of order d are all in the cyclic subgroup $C_d = \langle a \rangle$. But we know from elementary group theory that there are just $\phi(d)$ elements of order d in C_d, namely the elements a^i with $gcd(i, n) = 1$.

   It follows that the number $\sigma(d)$ of elements of order d in $F^\times$ is either $\phi(d)$ or 0. But since $\sum_{d|p^n-1} \phi(d) = p^n - 1$, all the $p^n - 1$ elements of $F^\times$ can only be accounted for if $\sigma(d) = \phi(d)$ for all $d \mid p^n - 1$.

Definition 7.2. *A generator of* $(\mathbb{Z}/p)^\times$ *is called a* primitive root mod p.

Example: Take $p = 7$. Then

$$2^3 \equiv 1 \bmod 7;$$

so 2 has order 3 mod 7, and is not a primitive root.

However,

$$3^2 \equiv 2 \bmod 7, \; 3^3 \equiv 6 \equiv -1 \bmod 7.$$

Since the order of an element divides the order of the group, which is 6 in this case, it follows that 3 has order 6 mod 7, and so is a primitive root.

If g generates the cyclic group G then so does g^{-1}. Hence

$$3^{-1} \equiv 5 \bmod 7$$

is also a primitive root mod 7.

Proposition 7.5. *There are* $\phi(p-1)$ *primitive roots* mod p. *If* π *is one primitive root then the others are* π^i *where* $0 \leq i < p-1$ *and* $\gcd(p-1, i) = 1$.

This follows from Proposition 7.3 above.

Examples: Suppose $p = 11$. Then $(\mathbb{Z}/11)^\times$ has order 10, so its elements have orders 1,2,5 or 10. Now

$$2^5 = 32 \equiv -1 \bmod 11.$$

So 2 must be a primitive root mod 11.

There are

$$\phi(10) = 4$$

primitive roots mod 11, namely

$$2, 2^3, 2^7, 2^9 \bmod 11,$$

ie

$$2, 8, 7, 6.$$

Suppose $p = 23$. Then $(\mathbb{Z}/23)^\times$ has order 22, so its elements have orders 1,2,11 or 28.

Note that since $a^{22} = 1$ for all $a \in (\mathbb{Z}/29)^\times$, it follows that $a^{11} = \pm 1$.

Working always modulo 23,

$$2^5 = 32 \equiv 9 \implies 2^{10} \equiv 81 \equiv 12 \implies 2^{11} \equiv 24 \equiv 1.$$

So 2 has order 11. Also

$$3^2 \equiv 2^5 \implies 3^{10} \equiv 2^{25} \equiv 2^3 \implies 3^{11} \equiv 3 \cdot 8 \equiv 1.$$

So 3 also has order 11. But

$$5^2 \equiv 2 \implies 5^{10} \equiv 2^5 \equiv 9 \implies 5^{11} \equiv 45 \equiv -1.$$

Since $5^2 \equiv 2 \implies 5^4 \equiv 2^2 = 4$, we conclude that 5 is a primitive root modulo 23.

7.5 Uniqueness

Theorem 7.3. *Two fields F, F' of the same order p^n are necessarily isomorphic.*

Proof. If $a \in F^\times$ then $a^{p^n-1} = 1$, ie a is a root of the polynomial

$$U(x) = x^{p^n-1} - 1.$$

Hence

$$U(x) = \prod_{a \in F^\times} (x - a),$$

since the number $p^n - 1$ of elements is equal to the degree of $U(x)$.

Now suppose $U(x)$ factorises over $\mathbb{F}_p$ into irreducible polynomials

$$U(x) = f_1(x) \cdots f_r(x).$$

We know that $F^\times$ is cyclic. Let π be a generator, so that

$$F = \{0, 1, \pi, \pi^2, \ldots, \pi^{p^n-2}\}.$$

Then π is a factor of $U(x)$, and so of one of its irreducible factors, say $f_1(x)$. It follows that if $f(x) \in \mathbb{F}_p[x]$ then

$$f(\pi) = 0 \iff f_1(x) \mid f(x).$$

For otherwise we could find $u(x), v(x)$ such that

$$f(x)u(x) + f_1(x)v(x) = 1;$$

and this would give a contradiction on setting $x = \pi$.

Now pass to F', where $U(x)$ will factor in the same way. Let π' be a root of $f_1(x)$ in F'. Then we claim that the map $\Theta : F \to F'$ given by

$$\pi^r \mapsto \pi'^r \qquad (0 \leq r < p^n - 1)$$

(together with $0 \mapsto 0$) is a homomorphism.

It is easy to see that $\Theta(xy) = \Theta(x)\Theta(y)$. It remains to show that $\Theta(x + y) = \Theta(x) + \Theta(y)$. Suppose $x = \pi^a,\ y = \pi^b,\ x + y = \pi^c$. Then π satisfies the equation

$$f(x) = x^a + x^b - x^x.$$

It follows that

$$f_1(x) \mid f(x).$$

On passing to F',

$$f(\pi') = 0 \implies \pi'^a + \pi'^b = \pi'^c,$$

as required.

Finally, a homomorphism $\Theta : F \to F'$ from one field to another is necessarily injective. For if $x \neq 0$ then x has an inverse y, and then

$$\Theta(x) = 0 \implies \Theta(1) = \Theta(xy) = \Theta(x)\Theta(y) = 0,$$

contrary to fact that $\Theta(1) = 1$. (We are using the fact that Θ is a homomorphism of additive groups, so that $\ker \Theta = 0$ implies that Θ is injective.) Since F and F' contain the same number of elements, we conclude that Θ is bijective, and so an isomorphims. □

7.6 Existence

Theorem 7.4. *There exists a field F of every prime power p^n.*

Proof. We know that if $f(x) \in \mathbb{F}_p[x]$ is of degree d, then $\mathbb{F}_p[x]/(f(x))$ is a field of order p^n. Thus the result will follow if we can show that there exist irreducible polynomials $f(x) \in \mathbb{F}_p[x]$ of all degrees $n \geq 1$.

There are p^n monic polynomials of degree n in $\mathbb{F}_p[x]$. Let us associate to each such polynomial the term x^n. Then all these terms add up to the generating function

$$\sum_{n \in \mathbb{N}} p^n x^n = \frac{1}{1 - px}.$$

Now consider the factorisation of each polynomial

$$f(x) = f_1(x)^{e_1} \cdots f_r(x)^{e_r}$$

into irreducible polynomials. If the degree of $f_i(x)$ is d_i this product corresponds to the power

$$x^{d_1 e_1 + \cdots + d_r e_r}.$$

Putting all these terms together, we obtain a product formula analagous to Euler's formula. Suppose there are $\sigma(n)$ irreducible polynomials of degree n. Let $d(f)$ denote the degree of the polynomial $f(x)$. Then

$$\begin{aligned}
\frac{1}{1-px} &= \prod_{\text{irreducible } f(x)} \left(1 + x^{d(f)} + x^{2d(f)} + \cdots\right) \\
&= \prod_{\text{irreducible } f(x)} \frac{1}{1 - x^{d(f)}} \\
&= \prod_{d \in \mathbb{N}} (1 - d^n)^{-\sigma(d)}.
\end{aligned}$$

As we have seen, we can pass from infinite products to infinite series by taking logarithms. When dealing with infinite products of functions it is usually easier to use logarithmic differentiation:

$$f(x) = u_1(x) \cdots u_r(x) \implies \frac{f'(x)}{f(x)} = \frac{u_1'(x)}{u_1(x)} + \cdots + \frac{u_r'(x)}{u_r(x)}.$$

Extending this to infinite products, and applying it to the product formula above,

$$\frac{p}{1-px} = \sum_{d \in \mathbb{N}} \frac{d\sigma(d) x^{d-1}}{1 - x^d} = \sum_{d \in \mathbb{N}} \sum_{t \geq 1} x^{td-1}$$

(This is justified by the fact that terms on the right after the nth only involve powers greater than x^n.)

Comparing the terms in x^{n-1} on each side,

$$p^n = \sum_{d|n} d\sigma(d).$$

Applying Möbius inversion,

$$n\sigma(n) = \sum_{d|n} \mu(n/d) p^d.$$

The leading term p^n (arising when $d = 1$) will dominate the remaining terms. For these will consist of terms $\pm p^e$ for various different $e < n$. Thus their absolute sum is

$$\begin{aligned}
&\leq \sum_{e \leq n-1} p^e \\
&= \frac{p^n - 1}{p - 1} \\
&< p^n.
\end{aligned}$$

It follows that $\sigma(n) > 0$. ie there exists at least one irreducible polynomial of degree n. □

Corollary 7.2. *The number of irreducible polynomials of degree n over $\mathbb{F}_p$ is*

$$\frac{1}{n}\sum_{d|n}\mu(n/d)p^d.$$

Examples: The number of polynomials of degree 3 over $\mathbb{F}_2$ is

$$\frac{1}{3}\left(\mu(1)2^3+\mu(3)2\right)=\frac{2^3-2}{3}=2,$$

namely the polynmials $x^3+x^2+1,\ x^3+x+1$.

The number of polynomials of degree 4 over $\mathbb{F}_2$ is

$$\frac{1}{4}\left(\mu(1)2^4+\mu(3)2^2+\mu(1)2\right)=\frac{2^4-2^2}{4}=3.$$

(Recall that $\mu(4)=0$, since 4 has a square factor.)

The number of polynomials of degree 10 over $\mathbb{F}_2$ is

$$\frac{1}{10}\left(2^{10}-2^5-2^2+2\right)=\frac{990}{10}=99$$

The number of polynomials of degree 4 over $\mathbb{F}_3$ is

$$\frac{1}{4}\left(3^4-3^2\right)=\frac{72}{8}=9.$$