Chapter 7

Finite fields

7.1 The characteristic of a 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 no such integer the ring is said to be of characteristic 0.

Examples: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all of characteristic 0.
$\mathbb{F}_p = \mathbb{Z}/(p)$ is of characteristic p.

Proposition 7.1. *The characteristic of an integral domain A is either a prime p, or else* 0.

In particular, a finite field is of 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. *In a field F of characteristic p the elements* $0, 1, \ldots, p-1$ *form a subfield isomorphic to* $\mathbb{F}_p = \mathbb{Z}/(p)$. *This is the only subfield of F isomorphic to* $\mathbb{F}_p$.

Proof. It is easily verified that the map $\theta : \mathbb{F}_p \to F$ sending

$$0 \mapsto 0, 1 \mapsto 1, 2 \mapsto 1+1, \ldots, p-1 \mapsto \underbrace{1+1+\cdots+1}_{p-1 \text{ terms}}$$

is an injective homomorphism.

Conversely, any homomorphism $\theta : \mathbb{F}_p \to F$ must send $0 \mapsto 0, 1 \mapsto 1, 2 \mapsto 1+1$, etc. □

Definition 7.2. *We call this subfield (which we identify with* $\mathbb{F}_p$*) the* prime subfield *of* F*.*

Proposition 7.3. *In a field* F *of characteristic* p

$$(a+b)^p = a^p + b^p.$$

Proof. By the binomial theorem,

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

Lemma 7.1. *The prime* p *divides each binomial coefficient* $\binom{p}{r}$ *for* $1 \le r \le p-1$*.*

Proof. We have

$$\binom{p}{r} = \frac{p(p-1)\cdots(p-r+1)}{1 \cdot 2 \cdots r}.$$

The result follows (this may require a little thought) since p divides the top but not the bottom. □

The Proposition follows at once. □

Corollary 7.1 (1)**.** *If* F *is a field of characteristic* p *the map* $\Phi : F \to F$ *given by* $a \mapsto a^p$ *is an injective homomorphism.*

Proof. We have seen that Φ preserves addition, and it is evident that it preserves multiplicatioon: $(ab)^p = a^p b^p$. It is injective since $a^p = 0 \implies a = 0$. □

Corollary 7.2. *If* F *is a finite field of characteristic* p *then* Φ *is an automorphism of* F*.*

Proof. It follows by the Pigeon-Hole Principle that Φ is bijective in this case. □

Φ is known as the Frobenius automorphism. The group of automorphisms of a field k is called the "galois group" of k. It is not hard to see th$\widehat{\text{t}}$he galois group of a finite field is the cyclic group generated by Φ.

Proposition 7.4. *A finite field F of characteristic p contains p^e elements, for some $e \geq 1$.*

Proof. We can consider F as a vector space over its prime subfield $\mathbb{F}_p$. Let $e_1, e_2, \ldots, e_d$ be a basis for this vector space. Then each elements of F is uniquely expressible in the form

$$x_1e_1 + x_2e_2 + \cdots + x_de_d \qquad (x_i \in \mathbb{F}_p).$$

There are p choices for each coefficient x_i, hence p^d choices in all. □

7.2 Our main result

Recall that a finite field must contain p^e elements. We say that the field is *of order p^e*.

Theorem 7.1. *There exists a finite field of each prime-power order p^e, and this field is unique up to isomorphism.*

We start by proving an auxiliary result, of some importance on its own account. Then we show that there is at most one field with p^e elements. Finally we prove that this field exists.

7.3 $F^\times$ is cyclic

Recall that the multiplicative group $A^\times$ of a ring A is the group formed by the invertible elements of A. For example, $\mathbb{Z}^\times = \{\pm 1\}$.

If k is a field then its multiplicative group $k^\times = k \setminus \{0\}$, since every non-zero element of k is invertible.

Theorem 7.2. *The multiplicative group $F^\times$ of a finite field F is cyclic.*

Interestingly, the proof of this result is no simpler for the prime fields $\mathbb{F}_p$ then it is for general finite fields $\mathbb{F}_q$ with $q = p^e$.

Proof. We suppose throughout the proof that F is a field of order p^e, so that $\mathbb{F}^\times = F \setminus \{0\}$ is a group of order $p^e - 1$.

We will show by a counting argument that $F^\times$ contains an element of order $p^e - 1$, which must be a generator of this group.

The multiplicative order d of any element $a \in F^\times$ must divide $p^e - 1$, by Lagrange's Theorem (in group theory). Let the number of elements of order $d \mid p^e - 1$ in $F^\times$ be $f(d)$.

These elements all satisfy the polynomial equation $x^d = 1$ over the field $\mathbb{F}_p$. It follows that $f(d) \leq d$. (The theorem that a polynomial of degree d has at most d roots holds just as well over finite fields as it does over $\mathbb{R}$ or $\mathbb{C}$.)

But we can do better. If a is one element of order d then the d elements $1, a, a^2, \ldots, a^{d-1}$ all satisfy the equation, and so must give all its roots. These elements form a cyclic group of order d.

Lemma 7.2. *If $G = \langle g \rangle$ is a cylic group of order d generated by g then g^r has order d if and only if* $\gcd(d, r) = 1$.

Proof. Suppose $\gcd(d, r) = 1$; and suppose a^r has order e. Then $a^{re} = 1 \implies d \mid re \implies d \mid e$ since $\gcd(r, d) = 1$.

Conversely, suppose $\gcd(d, r) = e > 1$. Let $d = ef,\ r = es$. Then $e = d/f = r/s \implies rf = ds$. Hence $(a^r)^f = (a^d)^s = 1$, and a^r has order smaller than d. □

If follows that $f(d)$ is either 0 (if there are no elements of order d) or else $\phi(d)$. (Recall that $\phi(d)$ is the number of numbers $r \in \{1, \ldots, d-1\}$ coprime to d.)

Now consider the additive group $\mathbb{Z}/(n)$. This is a cyclic group of order n. It certainly has elements of each order $d \mid n$; for if $n = de$ then e has order d. Moreover, if r has order d then $n \mid dr \implies de \mid dr \implies e \mid r$.

Thus the elements of order d are all multiples of e, lying in the cyclic subgroup generated by e. So the Lemma above shows that there are precisely $\phi(d)$ elements in $\mathbb{Z}/(n)$ of order d. Hence

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

Returning to the group $\mathbb{F}^\times$, we saw that there were either 0 or $\phi(d)$ elements of order d for each $d \mid p^e - 1$. But from the formula above, to account for $p^e - 1$ elements there must be $\phi(d)$ elements of each order $d \mid p^e - 1$. In particular there must be $\phi(p^e - 1) > 0$ elements of order $p^e - 1$: that is, generators of the group $\mathbb{F}^\times$. □

7.3.1 Primitive roots

Definition 7.3. *We call a generator of the multiplicative group $\mathbb{F}_p^\times$ a* primitive root *modulo p.*

Corollary 7.3. *There are exaclty $\phi(p-1)$ primitive roots modulo p for each prime p. If π is one primitive root then the others are π^r for r coprime to d.*

Example: Suppose $p = 23$. There are $\phi(22) = 10$ primitive roots modulo 23.

In general there is no better way of finding a primitive root other than trying $2, 3, 5, 6, \ldots$ successively. (There is no need to try 4, since if 2 is not a primitive root then 2^2 certainly cannot be.)

Let us try 2. We know that any element of $\mathbb{F}_{23}^{\times}$ has order $d \mid 22$, ie $d = 1, 2, 11$ or 22. Evidently 2 does not have order 1 or 2.

Working modulo 23 throughout, $2^5 = 32 \equiv 9$. Hence $2^{10} \equiv 9^2 = 81 \equiv 12$; and so $2^{11} \equiv 24 \equiv 1$. So 2 has order 11 and is not a primitive root modulo 23.

Moving on to 3, we have $3^3 = 27 \equiv 4$. Hence $3^6 \equiv 16 \equiv -7$, and so $3^{12} \equiv 49 \equiv 3 \implies 3^{11} \equiv 1$. So 3 is not a primitive root either.

Next we try 5. We have

$$5^2 = 25 \equiv 2 \implies 5^{10} = (5^2)^5 \equiv 2^5 = 32 \equiv 9 \implies 2^{11} \equiv 45 \equiv -1.$$

So we have found a primitive root mod 23.

From the last Lemma, knowing one primitive root π, the full set is π^d, where d runs over d coprime to p. In this case there are $\phi(22) = 11$ primitive roots, namely 5^d for $d = 1, 3, 5, 7, 9, 13, 17, 19, 21$. Note that the inverse of 5^d is 5^{22-d}, which may be easier to calculate.

From the work above,

$$\begin{aligned}
5^3 &\equiv 5 \cdot 5^2 \equiv 5 \cdot 2 = 10,\\
5^5 &\equiv 25 \cdot 5^3 = 250 \equiv 20 \equiv -3,\\
5^7 &\equiv -75 \equiv -6,\\
5^9 &\equiv 5 \cdot 2^4 = 80 \equiv 11,\\
5^{13} &\equiv 11^{-1} \equiv -2,\\
5^{15} &\equiv -50 \equiv -4,\\
5^{17} &\equiv -3^{-1} \equiv -8,\\
5^{19} &\equiv 5^{10} \cdot 5^9 \equiv 99 \equiv 7,\\
5^{21} &\equiv 5 \cdot 5^7 \cdot 5^{13} \equiv 60 \equiv -9.
\end{aligned}$$

Thus the primitive roots modulo 23 are: $-9, -8, -6, -4, -2, 5, 7, 10, 11$. (It is a matter of personal preference whether or not to replace remainders $> p/2$ by ther negative equivalent.)

7.3.2 Uniqueness

First an auxiliary result.

Proposition 7.5. *Suppose F is a field of order p^e. Let*

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

Then every element $a \in F$ satisfies $U(x) = 0$; and

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

Proof. $F^\times = F \setminus \{0\}$ has order $p^e - 1$. So by Lagrange's Theorem every elements $a \in F^\times$ satisfies the equation

$$x^{p^e - 1} - 1.$$

If we multiply the equation by x then 0 will also satisfy the equation:

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

Since this polynomial has degree p^e, and we have p^e roots, it factorizes completely over F into linear terms:

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

(A polynomial of degree d over any field k has at most d roots, just like a polyomial over $\mathbb{R}$ or $\mathbb{C}$.) □

Note that we can express this result in the form: $\Phi^e(a) = a$ for all $a \in F$. $U(x)$ is sometimes called the *universal polynomial* of the field F.

A little result we shall need later.

Lemma 7.3. *The universal polynomial $U(x)$ is* separable*, ie it has no multiple roots.*

Proof. If α is a multiple root of $f(x)$ then $f'(\alpha) = 0$. But the derivative

$$U'(x) = -1$$

never vanishes. □

Theorem 7.3. *If F, F' are two fields of the same order p^e then there exists an isomorphism $\Phi : F \to F'$.*

Proof. Let π be a generator of $F^\times$; and let $m(x)$ be the minimal polynomial of π over $\mathbb{F}_p$. Since $U(\pi) = 0$ it follows that

$$m(x) \mid U(x).$$

Note that this is a result in the polynomial ring $\mathbb{F}_p[x]$.

Now pass to F'. Then

$$m(x) \mid U(x) = \prod_{b \in F'} (x - b).$$

Since $U(x)$ factors over F' into linear polynomials, so does $m(x)$, say

$$m(x) = (x - b_1) \cdots (x - b_d).$$

Choose π' to be any of $b_1, \ldots, b_d$. We define the map $\Theta : F \to F'$ by

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

and $0 \mapsto 0$. Since π is of order $p^e - 1$, while π', even if it is not a generator of $F'^\times$, still satisfies the equation $x^{p^e-1} = 1$, the map is well-defined; for

$$\pi^r = \pi^s \implies \pi^{r-s} = 1 \implies (p^e - 1) \mid r - s \implies \pi'^{(r-s)} = 1 \implies \pi'^r = \pi'^s.$$

We claim that Θ is a homomorphism. It is easy to see that multiplication is preserved:

$$\pi^r \pi^s = \pi^{r+s} \mapsto \pi'^{(r+s)} = \pi'^r \pi'^s.$$

For addition, suppose $a + b = c$, where

$$a = \pi^r,\ b = \pi^s,\ c = \pi^t.$$

Let $f(x) = x^r + x^s - x^t$. Then

$$f(\pi) = 0 \implies m(x) \mid f(x) \implies f(\pi') = 0 \implies \pi'^r + \pi'^s - \pi'^t = 0.$$

The same argument holds if $a + b = 0$, with $g(x) = x^r + x^s$:

$$g(\pi) = 0 \implies m(x) \mid g(x) \implies f(\pi') = 0 \implies \pi'^r + \pi'^s = 0.$$

Finally, a non-zero homomorphism $\Theta : F \to F_2$ 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 isomorphim. $\square$

7.4 Existence

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

We give two very different proofs — take your choice. The first constructs $\mathbb{F}_{p^e}$ by a series of smaller extensions. The second uses a counting argument to show that there exist irreducible polynomials over $\mathbb{F}_p$ of every degree.

7.4.1 First proof: a tower of extensions

Proof. The result is trivial if $e = 1$, so will assume that $e > 1$. The universal polynomial

$$U_e(x) = x^{p^e} - x$$

(we add the suffix e since we will be considering other extensions of $\mathbb{F}_p$) has just p linear factors over $\mathbb{F}_p$, namely $x, x-1, x-2, \ldots x-p+1$. Let f(x) be any other irreducible factor over $\mathbb{F}_p$. Suppose $f(x)$ is of degree f. Then $\mathbb{F}_p[x]/(f(x))$ is an extension field of degree f over $\mathbb{F}_p$, containing p^f elements. This field is generated by $\alpha = x \mod f(x)$, ie the elements of the field are polynomials in α with coefficients in $\mathbb{F}_p$, eg

$$\beta = a_0 + a_1\alpha + \cdots + a_{f-1}\alpha^{f-1},$$

with $a_i \in \mathbb{F}_p$.

Now $U(\alpha) = 0$ since $f(\alpha) = 0$ and $f(x) \mid U(x)$. In other words, $\Phi^e(\alpha) = \alpha$. In addition, $\Phi^e(a_i) = a_i$ for $0 \le i < f$. Hence

$$\Phi^e(\beta) = \beta$$

for all elements β of the field, since Φ^e preserves addition and multiplication.

We know there is only one field of order p^f so we can denote it by $\mathbb{F}_{p^f}$.

Now suppose π is a generator of the multiplicative group $\mathbb{F}_{p^f}^{\times}$. Then π is of order $p^f - 1$. But $\Phi^e(\pi) = \pi$, ie $\pi^{p^e} = \pi \implies \pi^{p^e-1} = 1$ also. Hence

$$p^f - 1 \mid p^e - 1.$$

We need a simple arithmetic result.

Lemma 7.4. *$p^f - 1 \mid p^e - 1$ if and only if $f \mid e$.*

Proof. Suppose first that $f \mid e$, say $e = fd$. We have $x - 1 \mid x^d - 1$ in $\mathbb{Z}[x]$. Substituting $x = y^f$,

$$y^f - 1 \mid (y^f)^d - 1 = y^e - 1.$$

The result follows on setting $y = p$.

Conversely, suppose $f \nmid e$, say

$$e = fq + r$$

where $0 < r < f$. Let $h(x) = x^f - 1$. Then

$$x^f \equiv 1 \bmod h(x) \implies (x^f)^d \equiv 1 \bmod h(x) \implies x^e \equiv x^r \bmod h(x).$$

Setting $x = p$,

$$p^e \equiv p^r \bmod p^f - 1 \implies p^e - 1 \equiv p^r - 1 \bmod p^f - 1.$$

But $p^f - 1 \mid p^e - 1$, by hypothesis. Hence $p^f - 1 \mid p^r - 1$, which is impossible since $p^r - 1 < p^f - 1$. □

We see therefore that

$$f \mid e.$$

If $f = e$ we are done. Otherwise we repeat the same construction with $\mathbb{F} = \mathbb{F}_{p^f}$ playing the role of $\mathbb{F}_p$. Thus we start with an irreducible factor $f(x)$ of $U_e(x)$ over $\mathbb{F}$ of degree $d > 1$ (we know there is such a factor since there are only p^f linear factors), and consider the extension field $\mathbb{F}[x]/(f(x))$ of order p^g, where $g = fd$. Again, the field is generated by $\alpha = x \bmod f(x)$, ie its elements are polynomials in α,

$$\beta = a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1},$$

with $a_i \in \mathbb{F}$. As before,

$$\Phi^e(\alpha) = \alpha,\ \Phi^e(a_i) = a_i \implies \Phi^e(\beta) = \beta.$$

Now we choose a generator π of $\mathbb{F}^{p^g}$. This is of order $p^g - 1$, and

$$\Phi^e(\pi) = \pi \implies \pi^{p^e - 1} = 1.$$

Hence

$$p^g - 1 \mid p^e - 1 \implies g|e.$$

Thus we have constructed a larger field $\mathbb{F}_{p^g}$, with $f \mid g \mid e$. Continuing in this way, we must finally reach the field $\mathbb{F}_{p^e}$. □

7.4.2 Second proof: a counting argumeng

Proof. We know that if $f(x) \in \mathbb{F}_p[x]$ is of degree n, 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 $n \geq 1$.

[Conversely, if $\mathbb{F}_{p^e}$ exists then there is an irreducible polynomial over $\mathbb{F}_p$ of degree e. For consider the minimial polynomial $m(x)$ of a generator π of $\mathbb{F}_{p^e}^\times$. If this has degree d then π generates an extension field of degree d over $\mathbb{F}_p$, containing p^d elements. But this field must contain all the powers of π, ie all the elements of $\mathbb{F}_{p^e}^\times$. Since it also contains 0 it is in fact the whole of $\mathbb{F}_{p^e}$, so that $d = e$.]

Möbius inversion

It is convenient at this point to introduce an auxiliary idea, used widely in combinatorics and elsewhere outside of number theory.

Definition 7.4. *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

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

By an *arithmetic function* we mean a function with values in $\mathbb{N} \setminus \{0\}$.

Theorem 7.5. *Given an arithmetic function $f(n)$, suppose*

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

Then

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

Proof.

Lemma 7.5. *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 $n = 1$. □

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

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

[This is analogous to 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

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

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

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

□

The following multiplicative form of this result can be proved in the same way.

Corollary 7.4. *Given an arithmetic function $f(n)$, suppose*

$$g(n) = \prod_{d|n} f(n).$$

Then

$$f(n) = \prod_{d|n} g(n)^{\mu(n/d)}.$$

Return to second proof

There are p^n monic polynomials of degree n in $\mathbb{F}_p[x]$. Let us associate to each such polynomial the weight 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

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

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,

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

(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,

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

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 7.5. *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

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