11. FINITE FIELDS

§11.1. A Field With 4 Elements

Probably the only finite fields which you'll know about at this stage are the fields of integers modulo a prime p, denoted by $\mathbb{Z}_p$. But there are others. Now although $\mathbb{Z}_4$ is not a field because $2.2 = 0$ in this ring, there *is* a field of order 4.

Example 1: The following tables define addition and multiplication for a field of order 4.

+	**A**	**B**	**C**	**D**
A	A	B	C	D
B	B	A	D	C
C	C	D	A	B
D	D	C	B	A

×	**A**	**B**	**C**	**D**
A	A	A	A	A
B	A	B	C	D
C	A	C	D	B
D	A	D	B	C

Clearly the additive identity is A and the multiplicative identity is B. We could write A as 0 and B as 1. Also, since D = B + C we could write D = 1 + C. Using this notation the addition and multiplication tables become:

+	**0**	**1**	**C**	**1 + C**
0	0	1	C	1 + C
1	1	0	1+C	C
C	C	1 + C	0	1
1+C	1 + C	C	1	0

×	**0**	**1**	**C**	**1+C**
0	0	0	0	0
1	0	1	C	1+C
C	0	C	1+C	1
1+C	0	1+C	1	C

These table could be reconstructed just by knowing just two facts about the field:

(1) $1 + 1 = 0$;
(2) $C^2 = 1 + C$.

From property (1) we deduce that $x + x = x(1 + 1) = 0$ for each of the four values of x.

And knowing that $C^2 = 1 + C$ enables us to find the values of $C(1 + C)$ and $(1 + C)^2$.

Now notice that this field contains the subfield {0, 1} (see the shaded portion of the tables) which is our old friend $\mathbb{Z}_2$ and so it is an extension of $\mathbb{Z}_2$ by an element C that satisfies $C^2 = 1 + C$, or equivalently $C^2 + C + 1 = 0$ (remember that subtraction is the same as addition mod 2 since $1 + 1 = 0$ implies that $1 = -1$).

So C is a zero of the quadratic $x^2 + x + 1$. And we recognise this as a prime quadratic over $\mathbb{Z}_2$. It has no zeros within $\mathbb{Z}_2$ so we have extended $\mathbb{Z}_2$ by an invented number C so as to get a larger system in which the quadratic does factorise. This is the same way in which complex numbers were introduced. There we had the prime quadratic $x^2 + 1$

with no real zeros and we invented the number ‘i’ to extend the reals to give the field of complex numbers in which $x^2 + 1$ now has zeros.

§11.2. The Characteristic of a Field

We define the **characteristic** of a field F to be the additive order of 1, the multiplicative identity, except that if 1 has infinite order, as it does in the field $\mathbb{C}$ and all its subfields, we say that the field has **characteristic zero**.

Clearly if a field F has characteristic n then:

$$nx = (n1)x = 0x = 0$$

for all $x \in$ F.

Finite fields have finite characteristic, but note that it’s possible to have infinite fields with finite characteristic. For example the set of all rational functions $\frac{a(x)}{b(x)}$ with $a(x)$, $b(x) \in \mathbb{Z}_p[x]$ is an example of an infinite field of characteristic p.

Example 2:
$\mathbb{Z}_p$ and all its extensions have characteristic p.

Theorem 1: If the characteristic of a field is finite, it must be prime.
Proof: Suppose the characteristic of F is n where:

$$n = ab \text{ and } 1 < a, b < n.$$

Then $n1 = (a1)(b1)$ and so, since the Cancellation Law holds in fields, either $a1 = 0$ or $b1 = 0$. Clearly this is a contradiction.

Theorem 2: The order of a finite field F must be p^n for some prime p and some positive integer n.
Proof: Let p be the characteristic of F and let

$$K = \{n1 \mid n \in \mathbb{Z}\}.$$

(Note that we write it as $n1$ rather than just n because n is an integer while $n1$ is an element of the field.)
Clearly $K \cong \mathbb{Z}_p$.

Now F is a finite-dimensional vector space over K. Suppose that $|F/K| = n$ and let $a_1, a_2, \ldots, a_n$ be a basis. Then every element of F can be written uniquely as a linear combination of the a_i with coefficients from K and hence there are p^n of them.

We define K to be the **prime subfield** of F.

Polynomials of the form $x^N - x$ play an important part in the theory of finite fields, especially in the case where N is a prime power.

Theorem 3: If p divides N then $x^N - x$ splits into unique linear factors over $\mathbb{Z}_p$.
Proof: Suppose $x^N - x = a(x)^2q(x)$ where the degree of $a(x)$ is at least 1.

Differentiating $x^N - x$ we get $Nx^{N-1} - 1 = 0 - 1 = -1$. But, differentiating $a(x)^2q(x)$ by the product rule we get a multiple of $a(x)$. Clearly this is a contradiction.

It may seem odd to be using calculus in the case of finite fields. Indeed we can't define derivatives in the usual way as limits of quotients in a finite field. But we *can* define the derivative of a polynomial in a purely formal way and we can prove the product rule directly from this definition.

Theorem 4: In a field of characteristic p

$$(x + y)^{p^n} = x^{p^n} + y^p$$

for all x, y and all $n \geq 1$.

Proof: For $n = 1$ we have $(x + y)^p = x^p + y^p$ since all the other binomial coefficients are multiples of p and hence are zero in $\mathbb{Z}_p$. Suppose the theorem is true for n.

Then $$\begin{aligned}(x + y)^{p^{n+1}} &= ((x + y)^{p^n})^p \\ &= (x^{p^n} + y^{p^n})^p \\ &= x^{p^{n+1}} + y^{p^{n+1}}.\end{aligned}$$

§11.3. Construction of Field Extensions

When we're dealing with subfields of the complex numbers we could define $F[f(x)]$ to be the smallest field of $\mathbb{C}$ that contains all the zeros of $f(x)$ because we know of at least one field that contains them all, namely the field of complex numbers. But when it comes to polynomials

over fields, such as $\mathbb{Z}_p$, we don't have an obvious field that contains all the zeros. We have to carry out our field extensions in a different way.

Recall how we defined the ring of integers mod n as $\mathbb{Z}_n = \{0, 1, 2, ..., n - 1\}$. These are the possible remainders when we divide an integer by n. We make this into a ring, a mathematical structure with operations of addition and multiplication, by defining the operations in $\mathbb{Z}_n$ to be addition modulo n and multiplication modulo n. By this we mean that we add or multiply two elements and then take the remainder on dividing by n.

Example 3: $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ and in $\mathbb{Z}_7$ we have
$4 + 5 = 2$ and $4.5 = 6$.

You'll recall that $\mathbb{Z}_n$ is a field if and only if n is prime. The same idea can be extended to prime polynomials to get extensions of any field.

Suppose $P(x)$ is a polynomial of degree n over a field F. We create an 'indeterminate' u such that $P(u) = 0$ in the same way that we created the imaginary number i such that $i^2 + 1 = 0$ when extending the real numbers to the complex numbers.

Suppose that $P(x)$ has degree n.
We define $F[u \mid P(u) = 0]$ to be the set of all polynomials in u of the form

$$a_{n-1}u^{n-1} + ... + a_1u + a_0$$

where each $a_i \in$ F. These are the possible remainders on dividing a polynomial in u by the polynomial P(u). At this stage u is an indeterminate – we haven't yet put P(u) = 0.

We add these expressions in the usual way and multiply them **modulo** P(u). That is, we multiply two expressions of the above form as polynomials but we take the remainder on dividing by P(u).

The reason for changing the indeterminate from x to u is that we consider f(x) to be a polynomial in x while f(u) is that polynomial reduced modulo P(u), that is, simplified under the assumption that P(u) = 0.

Example 4: Take P(x) = $x^2 + 1$ over $\mathbb{R}$. This is prime over $\mathbb{R}$. So $\mathbb{R}[u \mid u^2 + 1 = 0]$ is
$\{a + bu \mid a, b \in \mathbb{R}\}$. We add and multiply as follows:
$(a_1 + b_1u) + (a_2 + b_2u) = (a_1 + a_2) + (b_1 + b_2)u$ and
$(a_1 + b_1u)(a_2 + b_2u) = a_1a_2 + (a_1b_2 + a_2b_1)u + b_1b_2u^2$
$= (a_1a_2 - b_1b_2) + (a_1b_2 + a_2b_1)u.$
You'll recognise that $\mathbb{R}[u \mid u^2 + 1 = 0]$ is simply the field of complex numbers where the indeterminate u is more usually written as i.

We will show that, up to isomorphism, there is exactly one field of order p^n for every prime p and every integer $n \geq 1$. We call this the **Galois Field of Order p^n** and denote it by **GF(p^n)**. We'll now use the above technique to construct a field GF(8).

Example 5: The polynomial $P(x) = x^3 + x + 1$ is prime over $\mathbb{Z}_2$. $\mathbb{Z}_2[u \mid u^3 + u + 1 = 0]$

$= \{0, 1, u, u + 1, u^2, u^2 + 1, u^2 + u, u^2 + u + 1\}$.

The addition table for this field is:

+	**0**	**1**	***u***	***u*+1**
0	0	1	u	u+1
1	1	0	u+1	u
u	u	u+1	0	1
***u*+1**	u+1	u	1	0
$\boldsymbol{u^2}$	u^2	u^2+1	u^2+u	u^2+u+1
$\boldsymbol{u^2}$**+1**	u^2+1	u^2	u^2+u+1	u^2+u
$\boldsymbol{u^2}$**+*u***	u^2+u	u^2+u+1	u^2	u^2+1
$\boldsymbol{u^2}$**+*u*+1**	u^2+u+1	u^2+u	u^2+1	u^2

+	$\boldsymbol{u^2}$	$\boldsymbol{u^2}$ **+1**	$\boldsymbol{u^2}$**+*u***	$\boldsymbol{u^2}$**+*u*+1**
0	u^2	u^2+1	u^2+u	u^2+u+1
1	u^2+1	u^2	u^2+u+1	u^2+u
u	u^2+u	u^2+u+1	u^2	u^2+1
***u*+1**	u^2+u+1	u^2+u	u^2+1	u^2
$\boldsymbol{u^2}$	0	1	u	u+1
$\boldsymbol{u^2}$**+1**	1	0	u+1	u
$\boldsymbol{u^2}$**+*u***	u	u+1	0	1
$\boldsymbol{u^2}$**+*u*+1**	u+1	u	1	0

The addition table is independent of the prime polynomial $P(x)$. In this case we simply work modulo 2 with the coefficients.

When it comes to multiplication we'll have u^3 and u^4. Since $u^3 + u + 1 = 0$ we have $u^3 = u + 1$. Remember that $-1 = 1$ because we're using $\mathbb{Z}_2$ for the coefficients. Then $u^4 = u^2 + u$, and so on.

×	**0**	**1**	***u***	***u*+1**
0	0	0	0	0
1	0	1	u	u+1
u	0	u	u^2	u^2+u
***u*+1**	0	u+1	u^2+u	u^2+1
***u*²**	0	u^2	u+1	u^2+u+1
***u*²+1**	0	u^2+1	1	u^2
u*²+*u	0	u^2+u	u^2+u+1	1
***u*²+*u*+1**	0	u^2+u+1	u^2+1	u

×	***u*²**	***u*² +1**	***u*²+*u***	***u*²+*u*+1**
0	0	0	0	0
1	u^2	u^2+1	u^2+u	u^2+u+1
u	u+1	1	u^2+u+1	u^2+1
***u*+1**	u^2+u+1	u^2	1	u
***u*²**	u^2+u	u	u^2+1	1
***u*²+1**	u	u^2+u+1	u+1	u^2+u
u*²+*u	u^2+1	u+1	u	u^2
***u*²+*u*+1**	1	u^2+u	u^2	u + 1

If you feel that the above discussion is logically a little unsatisfactory let me point out that there's a perfectly rigorous way of doing all this using quotient rings. You may remember quotient groups in group

theory where the elements are cosets. Something similar can be done for rings, and $F[u \mid P(u) = 0]$ is simply the quotient ring $F[x]/P(x)$. But since our excursion into ring theory will be brief we won't bother introducing quotient rings here.

Theorem 5: $P(x)$ is prime over F if and only if
$F[u \mid P(u) = 0]$ is a field.

Proof: Suppose $P(x)$ is composite, and that $P(x) = Q(x)R(x)$ where $Q(x)$ and $R(x)$ have lower degree than $P(x)$.

Then in $F[u|P(u) = 0]$, the product $Q(u)R(u) = P(u) = 0$.

If $F[u|P(u) = 0]$ is a field then at least one of $Q(u)$ and $R(u)$ would be 0. But this can only happen if $P(x)$ divides $Q(x)$ or $R(x)$, which is impossible as they have lower degree than $P(x)$.

Now suppose that $P(x)$ is prime over F. All but one of the field axioms are obvious and they work even if $P(x)$ isn't prime. The one axiom to be checked is the existence of a multiplicative inverse for all non-zero elements.

Suppose that $a(u)$ is a non-zero element of $F[u|P(u) = 0]$. Since $a(u) \neq 0$, $P(x)$ doesn't divide $a(x)$.

Since P(x) is prime over F this means that a(x) and P(x) are coprime over F. The greatest common divisor of a(x) and P(x) is therefore 1.

Just as with greatest common divisors of integers it can be shown that the greatest common divisor of a(x) and P(x) can be expressed in the form

a(x)h(x) + P(x)k(x) for some h(x), k(x) $\in$ F[x].

[Euclid's algorithm for finding GCDs works for polynomials just as it does for integers and by obtaining 1 as the GCD and working backwards through the algorithm one can obtain an equation of the above form.]

So 1 = a(x)h(x) + P(x)k(x) and substituting $x = u$ and we get

$$\begin{aligned} 1 &= a(u)h(u) + P(u)k(u) \\ &= a(u)h(u) \text{ since } P(u) = 0. \end{aligned}$$

It follows that h(u) is the multiplicative inverse of a(u).

So given any prime polynomial P(x) over a field F we can construct an extension of F over which P(x) has a zero. We can continue extending until we obtain an extension over which P(x) splits completely into linear factors. Finally we can do this for composite polynomials by extending by zeros from different prime polynomials.

Theorem 6: If F is any field and a(x) $\in$ F[x] there exists an extension of F over which a(x) splits into linear factors.
Proof: We prove this by induction on the degree of a(x).

We can write $a(x) = P(x)g(x)$ where $P(x), g(x) \in F[x]$ and $P(x)$ is prime over F.

We've seen how to construct an extension K of F over which $P(x)$, and hence $a(x)$, has a zero, α. Hence we can write $a(x) = (x - \alpha)g(x)$ for some $g(x) \in K[x]$.

Since $g(x)$ has smaller degree than $a(x)$ we can assume by induction that there's an extension H of K over which $g(x)$ splits into linear factors and over this field $a(x)$ will split into linear factors.

Theorem 7: For all prime powers p^n there exists a field of order p^n.

Proof: Let $a(x) = x^{p^n} - x$ and let K be an extension of $\mathbb{Z}_p$ over which $a(x)$ splits into linear factors. Let H be the set of zeros of $a(x)$ in K.

It's easy to check that H is a subfield of K, for if $x^{p^n} = x$ and $y^{p^n} = y$ then $(x + y)^{p^n} = x^{p^n} + y^{p^n} = x + y$.

Closure under multiplication and inverses are easily checked.

Since $a(x)$ has no repeated zeros $|H| = p^n$.

Over a smaller field, such as $\mathbb{Z}_p$, $x^{p^n} = x$ will factorise into monic prime factors, but these will not all be linear. The remarkable thing, however, is that every monic prime polynomial whose degree divides n will appear exactly once in this factorisation.

§11.4. The Multiplicative Group of a Finite Field

For any field F the non-zero elements form a group $F^{\#}$ under multiplication. We call this the **multiplicative group** of F. If F has order p^n its multiplicative group has order $p^n - 1$.

Theorem 8: If F is a finite field then $F^{\#}$ is cyclic.
Proof: $F^{\#}$ is a direct sum of cyclic groups of prime power order. If there is more than one direct summand whose order is divisible by p then in $F^{\#}$ there are at least p^2 zeros of the polynomial $x^p - 1$, a contradiction.

Example 6: Find the order of the smallest field F over which $x^{14} - x$ splits completely into linear factors.
Solution: $x^{14} - x = x(x^{13} - 1)$ so we need F to contain an element of order 13.

If $|F| = p^n$ then 13 divides $p^n - 1$ and so $p^n = 1 + 13k$ for some integer k.

The smallest possibility is where $p^n = 27$. But will $x^{14} - x$ split completely over a field of order 27? The answer is "yes" because in such a case $F^{\#}$ is a cyclic group of order 26 and so will contain 12 elements of order 13 and these, together with 0 and 1, will provide 14 distinct zeros for $x^{14} - x$.

Theorem 9: If F is a field of order p^n then $x^{p^n} = x$ for all $x \in F$.

Proof: The order of $F^{\#}$ is $p^n - 1$ and so if $x \neq 0$ then

$$x^{p^n - 1} = 1 \text{ and so } x^{p^n} = x.$$

This is true for $x = 0$ as well.

Corollary: In a field of order p^n the polynomial $x^{p^n} - x$ has p^n distinct zeros.

Theorem 10: Let $P(x)$ be a prime polynomial of degree m over $\mathbb{Z}_p$.

Then $P(x)$ divides $x^{p^n} - x$ if and only if m divides n.

Proof: Suppose m divides n. Let $F = \mathbb{Z}_p[u|P(u) = 0]$.

Clearly $P(x)$ is the minimum polynomial of u over $\mathbb{Z}_p$.

Since F has order p^m we must have $u^{p^m} = u$.

So $u^{p^{2m}} = (u^{p^m})^{p^m} = u^{p^m} = u$ and so on.

Hence $u^{p^n} = u$ and so u is a zero of $x^{p^n} - x$.

This means that $P(x)$ divides $x^{p^n} - x$.

Suppose now that P(x) divides $x^{p^n} - x$.
Let F be a finite degree extension of $\mathbb{Z}_p$ over which $x^{p^n} - x$ splits and let β be a zero of $\pi(x)$ in F.

Then $|\mathbb{Z}_p[\beta]/\mathbb{Z}_p| = m$ so $|F:\mathbb{Z}_p[\beta]| = n/m$
whence m divides n.

Corollary:

Over $\mathbb{Z}_p$, $x^{p^n} - x$ is the product of all the monic prime polynomials over $\mathbb{Z}_p$ whose degree divides n.

Proof: We just need to note that since $x^{p^n} - x$ has no repeated zeros each monic prime polynomial only occurs once in the above factorisation.

Example 7: The minimum polynomials of the 8 elements of GF[8] above are as follows:

0	1	α	$\alpha^2 + 1$	$\alpha^2 + \alpha$	$\alpha + 1$	α^2	$\alpha^2 + \alpha + 1$
x	$x+1$	$x^3 + x + 1$			$x^3 + x^2 + 1$		

Example 8: The prime polynomials over $\mathbb{Z}_2$ of degrees 1 and 3 are:

$$x,\ x + 1,\ x^3 + x + 1,\ x^3 + x^2 + 1 \text{ and so}$$
$$x^8 - x = x(x + 1)(x^3 + x + 1)(x^3 + x^2 + 1).$$

The prime polynomials over $\mathbb{Z}_2$ of degrees 1, 2 and 4 are:
$x,\ x + 1,\ x^2 + x + 1,\ x^4 + x + 1,\ x^4 + x^3 + 1$ and
$$x^4 + x^3 + x^2 + x + 1$$
and so $x^{16} - x = x(x + 1)(x^2 + x + 1)(x^4 + x + 1)$
$$(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1).$$

Example 9: Since $x^{32} - x$ is the product of all prime polynomials over $\mathbb{Z}_2$ whose degrees divide 5 then

$$(x^{32} - x)/(x^2 - x)$$

must be the product of all prime polynomials of degree 5. Hence there must be 30/5 = 6 of them.

Example 10: $(x^{256} - x)/(x^{16} - x)$ has degree 240. Since it is the product of all prime polynomials of degree 8 over $\mathbb{Z}_2$ there must be 240/5 = 48 such polynomials.

Theorem 11: If F is a field of order p^n and $\pi(x)$ is a prime polynomial of degree n over $\mathbb{Z}_p$ then $F \cong \mathbb{Z}_p[x]/\pi(x)\ \mathbb{Z}_p[x]$.

Proof: Since $xp^n - x$ is the product of all prime polynomials over $\mathbb{Z}_p$ whose degree divides n, $\pi(x)$ divides $xp^n - x$.

The elements of F will be zeros of $xp^n - x$ and so one of them at least will be a zero of $\pi(x)$. Then $\alpha \rightarrow x + \pi(x)$ $\mathbb{Z}_p[x]$ is the required isomorphism.

Corollary: All fields of order p^n are isomorphic to one another.

Finite fields must have order p^n for every prime p and every $n \geq 1$. But we cannot yet be sure that there exists a field for every prime power. Of course if there was no field of order p^n this would mean that there would be no prime polynomial of degree n over $\mathbb{Z}_p$. This seems unlikely, but can we be sure that this is impossible?

§11.5. The Number of Monic Prime Polynomials over $\mathbb{Z}_p$.

Let P_n be the number of monic prime polynomials of degree n over $\mathbb{Z}_p$. Clearly $P_1 = p$.

Theorem 12: For all n and all primes p, $\sum_{d|n} d.P_d = p^n$.

Example 11: Find the number of prime polynomials of degree 20 over $\mathbb{Z}_2$, that is, find P_{20}.

Solution: $P_1 = 2$.

$$P_2 = \frac{4-2}{2} = 1.$$

$$P_4 = \frac{16-2-2}{4} = 3.$$

$$P_5 = \frac{32-2}{5} = 6.$$

$$P_{10} = \frac{1024-2-2-30}{10} = 99.$$

$$P_{20} = \frac{1048576-2-2-12-30-990}{20} = 52377.$$

We define the Möbius function to be:

$\mu(1) = 1$;

$\mu(p_1p_2...p_k) = (-1)^k$ if p_1, ..., p_k are distinct primes;

$\mu(n) = 0$ if n is divisible by the square of a prime.

Theorem 13: If $n > 1$ then $\sum_{d|n} \mu(d) = 0$.

Proof: Let $n = p_1^{n_1} \ldots p_k^{n_k}$ where $p_1, \ldots, p_k$ are distinct primes.

$$\sum_{d|n} \mu(d) = \mu(1) + \sum_{i} \mu(p_i) \sum_{i,j} \mu(p_i p_j) + \ldots$$

$$= 1 - \binom{k}{1} + \binom{k}{2} - \ldots = (1-1)^k = 0.$$

Example 12:

$$\sum_{d|24} \mu(d) = \mu(1) + \mu(2) + \mu(3) + \mu(4) + \mu(6) + \mu(12)$$

$$= 1 - 1 - 1 + 0 + 1 + 0 = 0.$$

Theorem 14: $P_n = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d = \frac{1}{n} \sum_{d|n} \mu(d)\, p^{n/d}$.

Proof:

$$\sum_{d|n} \mu(d)\, p^{n/d} = \sum_{d|n} \mu(d) \sum_{c|\frac{n}{d}} c P_c$$

$$= \sum_{\substack{c,d \\ cd|n}} \mu(d)\, c P_c$$

$$= \sum_{c|n} c P_c \sum_{d|\frac{n}{c}} \mu(d)$$

$$= \sum_{c=n} c\mathrm{P}_c \text{ since } \sum_{d|m} \mu(d) = 0 \text{ if } m > 1,$$

by Theorem 13.

$$= n\mathrm{P}_n .$$

Similarly $\displaystyle\sum_{d|n} \mu\left(\frac{n}{d}\right) p^d = n\mathrm{P}_n$ so the two expressions are equal.

Example 13: The square-free divisors of 20 are 1, 2, 5 and 10. Hence the number of monic prime polynomials over $\mathbb{Z}_2$ of degree 20 is

$$\mathrm{P}_{20} = \frac{2^{20} - 2^{10} - 2^4 + 2^2}{20} = 52377.$$

§11.6. Galois Groups of Finite Fields

The Galois Theory of finite fields is not very interesting. For a start the elements of finite fields are roots of unity and so every polynomial over a finite field is soluble by radicals. Moreover, as we now show, the Galois groups of finite fields are cyclic.

Theorem 15: If F is a field of order p^n then $\theta(x) = x^p$ is an automorphism of order n.

Proof: If $x, y \in \mathrm{F}$ then $x + y \to (x + y)^p = x^p + y^p$ and

$$xy \to (xy)^p = x^p y^p.$$

Clearly $\theta^n(x) = x^{p^n} = x$ for all x so $\theta^n = 1$, the identity automorphism.

If $\theta^d = 1$ for some proper divisor d of n then $x^{p^d} = x$ for all $x \in F$ and so $|F| = p^d$, a contradiction.

This automorphism is called the **Frobenius automorphism**.

Theorem 16: If F is a field of order p^n and K is its prime subfield then G(F/K) is a cyclic group of order n, generated by the Frobenius automorphism.

Proof: Let $a(x) = x^{p^n} - x$ and let $\pi(x)$ be a prime factor of $a(x)$ over K of degree n. [Remember that $a(x)$ is the product of all prime polynomials over K whose degree divides n so there will be a prime divisor of degree n.]

Let $\sigma \in F$ be a zero of $\pi(x)$. Then $1, \sigma, \sigma^2, ..., \sigma^{n-1}$ is a basis for F over K and hence every automorphism of F is determined by its effect on σ. But σ must map to one of the n zeros of $\pi(x)$ and so there are at most n elements in G(F/K). It follows that the Frobenius automorphism generates G(F/K).

EXERCISES FOR CHAPTER 11

Exercise 1:
(i) Write down the addition and multiplication tables for GF[9].

(ii) Find the minimum polynomial of each of the elements of GF[9].

(iii) Find all possible generators for the multiplicative group of GF[9].

(iv) Find the Galois group of GF[9] over its prime subfield.

Exercise 2: Let $a(x) = x^{10} + x^5 + 1$.
(i) Show that $a(x)$ splits into distinct linear factors over GF[16].

(ii) Hence or otherwise factorise $a(x)$ into prime factors over $\mathbb{Z}_2$.

Exercise 3:
(a) Factorise the polynomial $x^8 + x + 1$ into prime polynomials over $\mathbb{Z}_2$.

(b) Suppose $u^{2^n} = u + 1$ in some finite field F of characteristic 2 and let K be the prime subfield of F.

(i) Show that $u^{2^{2n}} = u$.

(ii) By considering the degree of the minimum polynomial of u over K show that:

$x^{2^n} + x + 1$ is composite over $\mathbb{Z}_p$ for all $n \geq 3$.

Exercise 4: Find a generator of the multiplicative group of $\mathbb{Z}_{11}[x^2 + 1]$.

Exercise 5: Find the number of prime polynomials of degree 12 over $\mathbb{Z}_2$.

Exercise 6: Find the number of prime polynomials of degree 18 over $\mathbb{Z}_2$.

Exercise 7: Find the number of prime polynomials of degree 24 over $\mathbb{Z}_p$.

Exercise 8: Prove that if p, q are primes then for all m there exists a prime polynomial of degree q^m over $\mathbb{Z}_p$.

Exercise 9: Find the Galois group G(GF(243)/ $\mathbb{Z}_3$).

SOLUTIONS FOR CHAPTER 11

Exercise 1:

Now $x^2 + 1$ is prime over $\mathbb{Z}_3$ so GF[9] = $\mathbb{Z}_3[u|u^2 + 1 = 0]$. The elements of GF[9] are 0, 1, 2, u, $u + 1$, $u + 2$, $2u$, $2u + 1$ and $2u + 2$.

ADDITION

+	**0**	**1**	**2**	***u***	***u* + 1**
0	0	1	2	u	$u + 1$
1	1	2	0	$u + 1$	$u + 2$
2	2	0	1	$u + 2$	u
u	u	$u + 1$	$u + 2$	$2u$	$2u + 1$
***u* + 1**	$u + 1$	$u + 2$	u	$2u + 1$	$2u + 2$
***u* + 2**	$u + 2$	u	$u + 1$	$2u + 2$	$2u$
2*u*	$2u$	$2u + 1$	$2u + 2$	0	1
2*u* + 1	$2u + 1$	$2u + 2$	$2u$	1	2
2*u* + 2	$2u + 2$	$2u$	$2u + 1$	2	0

+	***u* + 2**	**2*u***	**2*u* + 1**	**2*u* + 2**
0	$u + 2$	$2u$	$2u + 1$	$2u + 2$
1	u	$2u + 1$	$2u + 2$	$2u$
2	$u + 1$	$2u + 2$	$2u$	$2u + 1$
u	$2u + 2$	0	1	2
***u* + 1**	$2u$	1	2	0
***u* + 2**	$2u + 1$	2	0	2
2*u*	2	u	$u + 1$	$u + 2$
2*u* + 1	0	$u + 1$	$u + 2$	u
2*u* + 2	2	$u + 2$	u	$u + 1$

MULTIPLICATION

$\times$	**0**	**1**	**2**	u	$u+1$
0	0	0	0	0	0
1	0	1	2	u	$u+1$
2	0	2	1	$2u$	$2u+2$
u	0	u	$2u$	2	$u+2$
$u+1$	0	u+1	$2u+2$	$u+2$	$2u$
$u+2$	0	$u+2$	$2u+1$	2u + 2	1
$2u$	0	$2u$	u	1	$2u+1$
$2u+1$	0	$2u+1$	$u+2$	$u+1$	2
$2u+2$	0	$2u+2$	$u+1$	$2u+1$	u

$\times$	$u+2$	$2u$	$2u+1$	$2u+2$
0	0	0	0	0
1	$u+2$	$2u$	$2u+1$	$2u+2$
2	$2u+1$	u	$u+2$	$u+1$
u	2u + 2	1	$u+1$	$2u+1$
$u+1$	1	$2u+1$	2	u
$u+2$	u	$u+1$	$2u$	2
$2u$	$u+1$	2	$2u+2$	$u+2$
$2u+1$	$2u$	$2u+2$	u	1
$2u+2$	2	$u+2$	1	$2u$

For example, $(2u + 2)^2 = 4u^2 + 8u + 4$

$= u^2 + 2u + 1$

$= 2 + 2u + 1 = 2u.$

(ii)

Element	Minimum Polynomial
0	x
1	$x + 2$
2	$x + 1$
u	$x^2 + 1$
$2u$	
$u + 1$	$x^2 + x + 2$
$2u + 1$	
$u + 2$	$x^2 + 2x + 2$
$2u + 2$	

(iii) $(u + 1)^2 = 2u$, $(2u)^2 = -1$, so $u + 1$ has order 8 and so $u + 1$ generates the multiplicative group of GF[9]. So do $(u + 1)^3$, $(u + 1)^5$ and $(u + 1)^7$.
Hence the generators are $u + 1$, $2u + 1$, $2u + 2$ and $u + 2$.

(iv) $G(GF[9]/ \mathbb{Z}_3) \cong \mathbf{C}_2$ and is generated by the automorphism $x \to x^3$.

Exercise 2:
(i) In GF[16], $x^{16} - x = x(x^5 - 1)a(x)$ splits into 16 distinct linear factors and hence so $a(x)$ splits into 14 linear factors.

(ii) $x^{16} - x = x(x - 1)(x^4 + x^3 + x^2 + x + 1)a(x)$ is the product of all the prime polynomials over $\mathbb{Z}_2$ whose degree is 1, 2 or 4.
Hence the prime factors of $a(x)$ have degrees 2 or 4.

Since $x^2 + x + 1$ is the only prime quadratic it must divide a(x) and the other prime factors must be two of the three prime quartics:

$$x^4 + x + 1,\ x^4 + x^3 + 1,\ x^4 + x^3 + x^2 + x + 1.$$

But $x^4 + x^3 + x^2 + x + 1$ already occurs so

$$a(x) = (x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1).$$

Exercise 3:

(a) (i) $x^2 + x + 1$ and $x^4 + x + 1$ have no zeros in $\mathbb{Z}_2$ and hence they must be prime.

(ii) $x^8 + x + 1 = (x^2 + x + 1)(x^6 + x^5 + x^3 + x^2 + 1)$.

(b) (i) $u^{2^{2n}} = (u^{2^n})^{2^n} = (u + 1)^{2^n} = u^{2^n} + 1 = u$.

(ii) Suppose that $x^{2^n} + x + 1$ is prime over K.
This will be the minimum polynomial of u over K.

Since $x^{2^{2n}} - x$ is the product of all prime polynomials whose degree divides $2n$ it follows that $2^n \mid 2n$, that is 2^{n-1} divides n. If $n \geq 3$ this is a contradiction.

Exercise 4:

We can easily show that $x^2 + 1$ is prime over $\mathbb{Z}_{11}$ and so

$$\mathbb{Z}_{11}[x^2 + 1] \cong \mathrm{GF}(121).$$

Let i be an indeterminate such that $i^2 = -1$.
We're looking for $a + bi$ of order 120, where $a, b \in \mathbb{Z}_{11}$.
We can systematically try various combinations of a, b until we find a generator. Since $\varphi(120) = 32$, about 1 in 3 of the elements of $\mathbb{Z}_{11}^{\#}$ will be a generator.

Clearly $b = 0$ will not work, so let's try $\alpha = 1 + i$.
Then $\alpha^2 = 2i$ so

$$\alpha^3 = 2i(1 + i) = -2 + 2i, \alpha^4$$
$$= -4, \alpha^5 = -4 - 4i \text{ and}$$
$$\alpha^6 = -8i = 3i.$$

Hence $\alpha^{15} = (-2 + 2i)(-4)^3 = 128(1 - i) = 7 - 7i$
and so $\alpha^{60} = 7^4(1 - i)^4 = 5^2(-2i)^2 = -12 = -1$.
So the order of α doesn't divide 60 and so must be a multiple of 8.

$$\alpha^{40} = (-4)^{10} = 5^5 = 25.125 = 3.4 = 12 = 1$$

so α has order 40.

Now we might try $\alpha = 2 + i$, but surely there's an easier way!

If we find elements of order 3, 5 and 8 and multiply them we will get an element of order 120.

In $\mathbb{C}$ an element of order 3 is $\omega = \frac{-1 + \sqrt{3}i}{2}$. Let's adapt this to $\mathbb{Z}_{11}[i]$.

Squaring the elements of $\mathbb{Z}_{11}$ we soon find that $5^2 = 3$. And ½ in $\mathbb{Z}_{11}$ is clearly 6.

So let's try $(-1 + 5i).6 = -6 + 30i = 5 + 8i$. Indeed this does have order 3.

Finding an element of order 5 is easy because there is one inside $\mathbb{Z}_{11}$ itself since $|\mathbb{Z}_{11}^{\#}| = 10$. Since $2^5 = -1$, $4^5 = 1$. So 4 has order 5.

For an element of order 8 we need a square root of i.
Let $(a + b\mathrm{i})^2 = \mathrm{i}$.
Therefore $a^2 - b^2 = 0$ and $2ab = 1$.
So $b = \frac{1}{2a} = \frac{6}{a}$.

Thus $a^2 = \frac{36}{a^2}$ and so $a^4 = 36$, whence $a^2 = \pm 6 = 5$ or 6.

Since $5 = 16$, mod 11, we can take $a = \pm 4 = 4, 7$.

Let's take $a = 7$. Then $b = \frac{6}{7} = 6.8 = 48 = 4$.

So $7 + 4\mathrm{i}$ has order 8.

Alternatively we could observe that in $\mathbb{C}$, $\frac{1 + \mathrm{i}}{\sqrt{2}}$ has order 8. But $x^2 - 2$ has no zeros in $\mathbb{Z}_{11}$.

However we can write $\frac{1 + \mathrm{i}}{\sqrt{2}} = \frac{-1 + \mathrm{i}}{\sqrt{2}\mathrm{i}}$ and since $3^2 = -2$ then 3 can play the role of $\sqrt{2}\mathrm{i}$ in this field.

Finally, $\frac{1}{3} = 4$ in $\mathbb{Z}_{11}$, so we try $4(-1 + \mathrm{i}) = 7 + 4\mathrm{i}$.
Indeed $7 + 4\mathrm{i}$ does have order 8.

Hence $(5 + 8\mathrm{i}).4.(7 + 4\mathrm{i}) = 4(3 + 76\mathrm{i}) = 4(3 - \mathrm{i}) = 1 - 4\mathrm{i}$ has order 120 and so is a generator of the multiplicative group.

Exercise 5: Let P_n be the number of (monic) prime polynomials of degree n over $\mathbb{Z}_2$.
Then $P_1 = 2$, $P_2 = 1$ and $P_3 = 2$.

$1.P_1 + 2.P_2 + 4.P_4 = 2^4$ so $P_4 = \dfrac{16 - 2 - 2}{4} = 3.$

$1.P_1 + 2.P_2 + 3.P_3 + 6.P_6 = 2^6$ so $P_6 = \dfrac{64 - 2 - 2 - 6}{6} = 9.$

$1.P_1 + 2.P_2 + 3.P_3 + 4\,P_4 + 6.P_6 + 12.P_{12} = 2^{12}$.

so $P_{12} = \dfrac{4096 - 2 - 2 - 6 - 12 - 54}{12} = 335.$

Alternatively:

$$\pi(12) = \frac{\mu(1)2^{12} + \mu(2)2^6 + \mu(3)2^4 + \mu(4)2^3 + \mu(6)2^2 + \mu(12)2^1}{12}$$

$$= \frac{2^{12} - 2^6 - 2^4 + 2^2}{12} = 335.$$

Exercise 6: The number of prime polynomials of degree 18 over $\mathbb{Z}_2$ is

$$P_{18} = \frac{1}{18}[2^{18} - 2^9 - 2^6 + 2^3]$$

$$= \frac{1}{18}[262144 - 512 - 64 + 8]$$

$$= 14532.$$

Exercise 7:

$$P_{24} = \frac{1}{24}[\mu(1)p^{24} + \mu(2)p^{12} + \mu(3)p^8 + \mu(4)p^6 + \mu(6)p^4 + \mu(8)p^3 + \mu(12)p^2 + \mu(24)p]$$

$$= \frac{1}{24}[p^{24} - p^{12} - p^8 + p^4].$$

This is the number of monic prime polynomials of degree 24. The total number of prime polynomials is therefore $\frac{(p-1)}{24}[p^{24} - p^{12} - p^8 + p^4]$.

Exercise 8: The number of monic prime polynomials of degree q^m over $\mathbb{Z}_p$ is $\frac{1}{q^n}[\mu(1)p^{q^n} + \mu(q)p^{q^{n-1}}]$

$$= \frac{1}{q^n}[p^{q^n} - p^{q^{n-1}}] > 0$$

Exercise 9: $243 = 3^5$ so $G(GF(243)/\mathbb{Z}_3) \cong \mathbf{C}_5$.