13. FINITE FIELDS

§13.1. A Field With 4 Elements

Probably the only finite fields which you will 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.

$+$

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>A</td>
<td>B</td>
<td>C</td>
<td>D</td>
</tr>
<tr>
<td>B</td>
<td>B</td>
<td>A</td>
<td>D</td>
<td>C</td>
</tr>
<tr>
<td>C</td>
<td>C</td>
<td>D</td>
<td>A</td>
<td>B</td>
</tr>
<tr>
<td>D</td>
<td>D</td>
<td>C</td>
<td>B</td>
<td>A</td>
</tr>
</tbody>
</table>

$\times$

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>B</td>
<td>A</td>
<td>B</td>
<td>C</td>
<td>D</td>
</tr>
<tr>
<td>C</td>
<td>A</td>
<td>C</td>
<td>D</td>
<td>B</td>
</tr>
<tr>
<td>D</td>
<td>A</td>
<td>D</td>
<td>B</td>
<td>C</td>
</tr>
</tbody>
</table>

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:

$+$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>C</th>
<th>1+C</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>C</td>
<td>1+C</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1+C</td>
<td>C</td>
</tr>
<tr>
<td>C</td>
<td>C</td>
<td>1+C</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1+C</td>
<td>1+C</td>
<td>C</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

$\times$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>C</th>
<th>1+C</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>C</td>
<td>1+C</td>
</tr>
<tr>
<td>C</td>
<td>0</td>
<td>1+C</td>
<td>1</td>
<td>C</td>
</tr>
<tr>
<td>1+C</td>
<td>0</td>
<td>1+C</td>
<td>1</td>
<td>C</td>
</tr>
</tbody>
</table>

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 portions 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 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.

§13.2. Fields as Quotient Rings

When we were dealing with subfields of the complex numbers we could define $F[f(x) = 0]$ to be the smallest field that contains all the zeros of $f(x)$ because we had 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 do not have an obvious field that contains all the zeros. We have to carry out our field extensions in a different way.

**Theorem 1:** If \( \pi(x) \in F[x] \) is a prime polynomial of degree \( n \) then \( F[x]/\pi(x)F[x] \) is a field which contains a zero of \( \pi(x) \).

**Proof:** The elements of \( F[x]/\pi(x)F[x] \) are the cosets \( a(x) + \pi(x)F[x] \) with two cosets \( a(x) + F[x] \) and \( b(x)F[x] \) being equal if and only if the representatives \( a(x) \) and \( b(x) \) differ by a multiple of \( \pi(x) \). The only field axiom which is not fairly obvious is the existence of multiplicative inverses so we just prove this crucial axiom. A typical element of this quotient ring is \( a(x) + \pi(x)F[x] \) for some \( a(x) \in F[x] \) with degree less than \( n \) and \( a(x) + F[x] \) is non-zero in the quotient ring if and only if \( \pi(x) \) does not divide \( a(x) \). Since \( \pi(x) \) is prime this must mean that \( a(x) \) is coprime with \( \pi(x) \). So, for some \( h(x), k(x) \in F[x] \) we can write

\[
a(x)h(x) + \pi(x)k(x) = 1.
\]

But then \( (a(x) + \pi(x)F[x]), (h(x) + \pi(x)F[x]) = 1 + \pi(x)F[x] \), the multiplicative identity in the quotient. Hence \( a(x) + \pi(x)\mathbb{Z}_p[x] \) has an inverse under multiplication.

Finally, \( \alpha = x + \pi(x)F[x] \) is a zero of \( \pi(x) \) since \( \pi(\alpha) = \pi(x) + \pi(x)F[x] = \pi(x)F[x] \), the zero element of the quotient ring.

**Example 2:** The quadratic \( x^2 + x + 1 \) is prime over \( \mathbb{Z}_2 \) and so \( \mathbb{Z}_2[x]/(x^2 + x + 1)\mathbb{Z}_2[x] \) is a field of order 4. These 4 elements are \( 0 + \mathbb{Z}_2[x], 1 + \mathbb{Z}_2[x], x + \mathbb{Z}_2[x] \) and \( x + 1 + \mathbb{Z}_2[x] \), corresponding to 0, 1, C and 1 + C respectively in example 1.

**Example 3:** The polynomial \( x^3 + x + 1 \) is prime over \( \mathbb{Z}_2 \). If \( \alpha = x + (x^3 + x + 1)\mathbb{Z}_2[x] \) then the elements of \( \mathbb{Z}_2[x]/(x^3 + x + 1) \mathbb{Z}_2[x] \) are 0, 1, \( \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1 \alpha^2 + \alpha \) and \( \alpha + \alpha + 1 \). The addition and multiplication tables for this field are:

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>( \alpha )</th>
<th>( \alpha + 1 )</th>
<th>( \alpha^2 )</th>
<th>( \alpha^2 + 1 )</th>
<th>( \alpha^2 + \alpha )</th>
<th>( \alpha^2 + \alpha + 1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>( \alpha )</td>
<td>( \alpha + 1 )</td>
<td>( \alpha^2 )</td>
<td>( \alpha^2 + 1 )</td>
<td>( \alpha^2 + \alpha )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>( \alpha + 1 )</td>
<td>( \alpha )</td>
<td>( \alpha^2 + 1 )</td>
<td>( \alpha^2 )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 + \alpha )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
</tr>
<tr>
<td>( \alpha )</td>
<td>( \alpha + 1 )</td>
<td>0</td>
<td>1</td>
<td>( \alpha^2 + \alpha )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 )</td>
<td>( \alpha^2 + \alpha )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
</tr>
<tr>
<td>( \alpha + 1 )</td>
<td>( \alpha + 1 )</td>
<td>( \alpha )</td>
<td>0</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 + \alpha )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 )</td>
<td>( \alpha^2 + \alpha )</td>
</tr>
<tr>
<td>( \alpha^2 )</td>
<td>( \alpha^2 + 1 )</td>
<td>( \alpha^2 + \alpha )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 )</td>
<td>( \alpha^2 + \alpha )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 )</td>
<td>( \alpha^2 + \alpha )</td>
</tr>
<tr>
<td>( \alpha^2 + 1 )</td>
<td>( \alpha^2 + 1 )</td>
<td>( \alpha^2 + \alpha )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 )</td>
<td>( \alpha^2 + \alpha )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 )</td>
<td>( \alpha^2 + \alpha )</td>
</tr>
<tr>
<td>( \alpha^2 + \alpha )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 + \alpha )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 )</td>
<td>( \alpha^2 + \alpha )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 )</td>
<td>( \alpha^2 + \alpha )</td>
</tr>
<tr>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 + \alpha )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 )</td>
<td>( \alpha^2 + \alpha )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 )</td>
<td>( \alpha^2 + \alpha )</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>x</th>
<th>0</th>
<th>1</th>
<th>( \alpha )</th>
<th>( \alpha + 1 )</th>
<th>( \alpha^2 )</th>
<th>( \alpha^2 + 1 )</th>
<th>( \alpha^2 + \alpha )</th>
<th>( \alpha^2 + \alpha + 1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>( \alpha )</td>
<td>( \alpha + 1 )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 + 1 )</td>
<td>( \alpha^2 + \alpha )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>( \alpha )</td>
<td>( \alpha + 1 )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 + 1 )</td>
<td>( \alpha^2 + \alpha )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
</tr>
<tr>
<td>( \alpha )</td>
<td>( \alpha )</td>
<td>( \alpha^2 )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 + 1 )</td>
<td>( \alpha^2 + \alpha )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
</tr>
<tr>
<td>( \alpha + 1 )</td>
<td>( \alpha + 1 )</td>
<td>( \alpha^2 + \alpha )</td>
<td>( \alpha^2 + 1 )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 + 1 )</td>
<td>( \alpha^2 + \alpha )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
</tr>
<tr>
<td>( \alpha^2 )</td>
<td>( \alpha^2 )</td>
<td>( \alpha^2 + \alpha )</td>
<td>( \alpha^2 + 1 )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 + 1 )</td>
<td>( \alpha^2 + \alpha )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
</tr>
<tr>
<td>( \alpha^2 + 1 )</td>
<td>( \alpha^2 + 1 )</td>
<td>( \alpha^2 + \alpha )</td>
<td>( \alpha^2 + 1 )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 + 1 )</td>
<td>( \alpha^2 + \alpha )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
</tr>
<tr>
<td>( \alpha^2 + \alpha )</td>
<td>( \alpha^2 + \alpha )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 + 1 )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 + 1 )</td>
<td>( \alpha^2 + \alpha )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
</tr>
<tr>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 + 1 )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 + 1 )</td>
<td>( \alpha^2 + \alpha )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
<td>( \alpha^2 + \alpha + 1 )</td>
</tr>
</tbody>
</table>
We obtain these entries by using mod 2 arithmetic when it comes to addition and the relation $\alpha^3 = \alpha + 1$ (from which we conclude $\alpha^4 = \alpha^2 + \alpha$ etc) when it comes to multiplication.

§13.3. 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 is possible to have infinite fields with finite characteristic. For example the set of all rational functions $a(x)/b(x)$ with $a(x), b(x) \in \mathbb{Z}_p[x]$ is an example of an infinite field of characteristic $p$.

Example 4: $\mathbb{Z}_p$ and all of its extensions have characteristic $p$.

Theorem 2: If the characteristic of a field is finite, it must be prime.
Proof: Suppose the characteristic of $F$ is $n$ where $n = ab$ 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 3: 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 $[F:K] = n$ 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.

The field $K$ in Theorem 3 is called the prime subfield of $F$.

Theorem 4: In a field of characteristic $p$ $(x + y)^p = x^p + y^p$ 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 $(x + y)^{p^{n+1}} = ((x + y)^p)^{p^n} = (x^p + y^p)^{p^n} = x^{p^{n+1}} + y^{p^{n+1}}$.

§13.4. 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 5: 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 5: Find the order of the smallest field $F$ over which $x^{14} - x$ splits completely into linear factors.

123
Solution: $x^{14} - x = x(x^{13} - 1)$ so we need $F$ to contain an element of order 13 other than 1. 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 $F^#$ will contain 12 elements of order 13 and these, together with 0 and 1, will provide 14 distinct zeros for $x^{14} - x$.

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. Such a polynomial does not usually split into linear factors, but if $N$ is a multiple of the field characteristic then no prime factor is repeated.

**Theorem 6:** If $p$ divides $N$ then $x^N - x$ has no repeated prime factors.

**Proof:** Suppose $x^N - x = a(x)^2 q(x)$ 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 $a(x)^2 q(x)$ 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 cannot define derivatives in the usual way as limits of quotients. But we can define the derivative of polynomials in a purely formal way and prove the product rule directly from this definition.

**Theorem 7:** 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 $x^{p^n-1} = 1$ 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.

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

**Theorem 8:** Let $\pi(x)$ be a prime polynomial of degree $m$ over $\mathbb{Z}_p$. Then $\pi(x)$ divides $x^{p^m} - x$ if and only if $m$ divides $n$.

**Proof:** Suppose $m$ divides $n$. Let $F = \mathbb{Z}_p[x]/\pi(x)\mathbb{Z}_p[x]$ and let $\alpha = x + \pi(x)\mathbb{Z}_p[x]$. Clearly $\pi(x)$ is the minimum polynomial of $\alpha$ over $\mathbb{Z}_p$. Since $F$ has order $p^m$ we must have $\alpha^{p^m} = \alpha$. So $\alpha^{p^{2m}} = \alpha (\alpha^{p^m})^{p^m} = \alpha^{p^m} = \alpha$ and so on. Hence $\alpha^{p^n} = \alpha$. So $\alpha$ is a zero of $x^{p^n} - x$ and hence $\pi(x)$ must divide it.

Suppose now that $\pi(x)$ divides $x^{p^n} - x$ and let $\beta$ 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 roots each monic prime polynomial only occurs once in the above factorisation.
Example 5: The minimum polynomials of the 8 elements of GF[8] above are as follows:

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>α</td>
<td>α^2 + 1</td>
<td>α^2 + α</td>
<td>α + 1</td>
</tr>
<tr>
<td>x</td>
<td>x+1</td>
<td>x^3 + x + 1</td>
<td>x^3 + x^2 + 1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Example 6: The prime polynomials over Z_2 of degrees 1 and 3 are:

- x, x + 1, x^3 + x + 1, x^3 + x^2 + 1
- x^8 - x = x(x + 1)(x^3 + x + 1)(x^3 + x^2 + 1).

The prime polynomials over 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
- 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 7: x^{32} - x is the product of all prime polynomials over 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 8: (x^{256} - x)/(x^{16} - x) has degree 240. Since it is the product of all prime polynomials of degree 8 over Z_2 there must be 240/5 = 48 such polynomials.

Theorem 9: If F is a field of order p^n and π(x) is a prime polynomial of degree n then F ≅ Z_p[x]/π(x)Z_p[x].

Proof: Let α ∈ F be a zero of π(x). Then α → x + π(x)Z_p[x] is the required isomorphism.

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

Up to isomorphism there is just one field of order p^n for any prime power. We call this GF[p^n]. We also know that there are no fields whose order is not a prime power. But we cannot yet be sure that there is 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 Z_p. This seems unlikely, but can we be sure that this is impossible?

Theorem 10: If F is any field and f(x) ∈ F[x] there exists an extension of F over which f(x) splits into linear factors.

Proof: We prove this by induction on the degree of f(x). We can write f(x) = π(x)g(x) where π(x), g(x) ∈ F[x] and π(x) is prime over F. We have seen how to construct an extension K of F over which π(x), and hence f(x), has a zero, α. Hence we can write f(x) = (x - α)g(x) for some g(x) ∈ K[x]. Since g(x) has smaller degree than f(x) we can assume by induction that there is an extension H of K over which g(x) splits into linear factors and over this field f(x) will split into linear factors.

Theorem 11: For all prime powers p^n there exists a field of order p^n.

Proof: Let f(x) = x^{p^n} - x and let K be an extension of Z_p over which f(x) splits into linear factors. Let H be the set of zeros of f(x) in K. It is 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 is easily checked. Since f(x) has no repeated zeros |H| = p^n.
§13.5. 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 $p$, $\sum_{d|n} dP_d = p^n$.

**Example 9:** Find the number of prime polynomials of degree 20 over $\mathbb{Z}_2$, that is, find $P_{20}$.

- $P_1 = 2$.
- $P_2 = \frac{4 - 2}{2} = 1$.
- $P_4 = \frac{16 - 2 - 2}{4} = 3$.
- $P_5 = \frac{32 - 2}{5} = 6$.
- $P_{10} = \frac{1024 - 2 - 2}{10} = 99$.
- $P_{20} = \frac{1048576 - 2 - 2}{20} = 52377$.

We define the Mobius 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 $n = p_1^{n_1} ... p_k^{n_k}$ where $p_1, ..., p_k$ are distinct primes.

$$\sum_{d|n} \mu(d) = \mu(1) + \sum_i \mu(p_i) + \sum_{i,j} \mu(p_i p_j) + ... = 1 - \binom{k}{1} - \binom{k}{2} - ... = (1 - 1)^k = 0.$$ 

**Example 10:** $\sum_{d|24} \mu(d) = \mu(1) + \mu(2) + \mu(3) + \mu(4) + \mu(6) + \mu(12)$

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

**Theorem 14:** $P_n = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) \frac{P_d}{n} = \frac{1}{n} \sum_{d|n} \mu(d) P_{n/d}$.

**Proof:** $\sum_{d|n} \mu(d) P_{n/d} = \sum_{d|n} \mu(d) \sum_{d'|d} P_{d'}$

$$= \sum_{c,d} \mu(d)cP_c$$

$$= \sum_{c|n} cP_c \sum_{d|c} \mu(d)$$
\[
\sum_{c=n} cP_c \text{ since } \sum_{d|m} \mu(d) = 0 \text{ if } m > 1, \text{ by Theorem 13.}
\]
\[
= nP_n.
\]

**Example 11:** 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
\[
P_{20} = \frac{2^{20} - 2^{10} - 2^4 + 2^2}{20} = 52377.
\]

§13.6. **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 \( x, y \in F \) then \( x + y \rightarrow x^p + y^p = (x + y)^p \) and \( xy \rightarrow (xy)^p = x^py^p \).

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 \( f(x) = x^{p^n} - x \) and let \( \pi(x) \) be a prime factor of \( f(x) \) over \( K \) of degree \( n \).

[Remember that \( f(x) \) 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 \( \sigma \). But \( \sigma \) must map to one of the \( n \) zeros of \( \pi(x) \) and so there are at most \( m \) elements in \( G(F/K) \). It follows that the Frobenius automorphism generates \( G(F/K) \).

**EXERCISES FOR CHAPTER 13**

**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 \( f(x) = x^{10} + x^5 + 1 \).
(i) Show that \( f(x) \) splits into distinct linear factors over GF[16].
(ii) Hence or otherwise factorise \( f(x) \) 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 the number of prime polynomials of degree 18 over $\mathbb{Z}_2$.

Exercise 5: Find the number of prime polynomials of degree 18 over $\mathbb{Z}_2$.

Exercise 6: Find the number of prime polynomials of degree 24 over $\mathbb{Z}_p$.

Exercise 7: 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 8: Find the Galois group $G(GF(243)/\mathbb{Z}_3)$. 
Exercise 1:

Now \( x^2 + 1 \) is prime over \( \mathbb{Z}_3 \) so \( GF[9] = \mathbb{Z}_3[u] \) where \( u^2 + 1 = 0 \).

The elements of \( GF[9] \) are 0, 1, 2, \( u \), \( u + 1 \), \( u + 2 \), \( 2u \), \( 2u + 1 \) and \( 2u + 2 \).

\[
\begin{array}{cccccccccc}
+ & 0 & 1 & 2 & u & u + 1 & u + 2 & 2u & 2u + 1 & 2u + 2 \\
0 & 0 & 1 & 2 & u & u + 1 & u + 2 & 2u & 2u + 1 & 2u + 2 \\
1 & 1 & 2 & 0 & u + 1 & u + 2 & u & 2u + 1 & 2u + 2 & 2u \\
2 & 2 & 0 & 1 & u + 2 & u & u + 1 & 2u + 2 & 2u & 2u + 1 \\
u & u & u + 1 & u + 2 & 2u & 2u + 1 & 2u + 2 & 0 & 1 & 2 \\
u + 1 & u + 1 & u + 2 & u & 2u + 1 & 2u + 2 & 2u & 1 & 2 & 0 \\
u + 2 & u + 2 & u & u + 1 & 2u + 2 & 2u & 2u + 1 & 2 & 0 & 2 \\
2u & 2u & 2u + 1 & 2u + 2 & 0 & 1 & 2 & u & u + 1 & u + 2 \\
2u + 1 & 2u + 1 & 2u + 2 & 2u & 1 & 2 & 0 & u + 1 & u + 2 & u \\
2u + 2 & 2u + 2 & 2u & 2u + 1 & 2 & 0 & 2 & u + 2 & u & u + 1 \\
\end{array}
\]

\[
\begin{array}{cccccccccc}
\times & 0 & 1 & 2 & u & u + 1 & u + 2 & 2u & 2u + 1 & 2u + 2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 2 & u & u + 1 & u + 2 & 2u & 2u + 1 & 2u + 2 \\
2 & 0 & 2 & 1 & 2u & 2u + 1 & 2u + 2 & 2u + 1 & u + 1 & u + 1 \\
u & 0 & u & 2u & u & u + 2 & u + 2 & 2u + 1 & u + 1 & u + 1 \\
u + 1 & 0 & u + 1 & 2u + 2 & u + 2 & 2u + 1 & 2 & u + 1 & 2 & u \\
u + 2 & 0 & u + 2 & 2u + 1 & 2u + 2 & 1 & u & u + 1 & 2u & 2 \\
2u & 0 & 2u & u & 1 & 2u + 1 & u + 1 & 2 & 2u + 2 & u + 2 \\
2u + 1 & 0 & 2u + 1 & u + 2 & u + 1 & 2 & 2u & 2u + 2 & u & 1 \\
2u + 2 & 0 & 2u + 2 & u + 1 & 2u + 1 & u & 2 & u + 2 & 1 & 2u \\
\end{array}
\]

(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) \( G(GF[9]/\mathbb{Z}_3) \cong C_2 \) and is generated by the automorphism \( x \to x^3 \).
Exercise 2:
(i) In GF[16] \( x^{16} - x = x(x^5 - 1)f(x) \) splits into 16 distinct linear factors and hence so does \( f(x) \).
(ii) \( x^{16} - x = x(x - 1)(x^4 + x^3 + x^2 + x + 1)f(x) \) is the product or all the prime polynomials over \( \mathbb{Z}_2 \) whose degree is 1, 2 or 4. Hence the prime factors of \( f(x) \) have degrees 2 or 4.
Since \( x^2 + x + 1 \) is the only prime quadratic it must divide \( f(x) \) 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 \( f(x) = (x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1) \).

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) \( u^{2^{2n}} = (u^2)^{2^n} = (u + 1)^2 = u^2 + 1 = u \).
(ii) Suppose that \( x^{2^n} - x \) 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 \( 2^n | 2n \), that is \( 2^{n-1} \) divides n. If \( n \geq 3 \) this is a contradiction.

Exercise 4: Find the number of prime polynomials of degree 12 over \( \mathbb{Z}_2 \).
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 \( P_4 = \frac{16 - 2 - 2}{4} = 3. \)
1. \( P_1 + 2. P_2 + 3. P_3 + 6. P_6 \) so \( P_6 = \frac{64 - 2 - 2 - 6}{6} = 9. \)
so \( P_{12} = \frac{4096 - 2 - 2 - 6 - 12 - 54}{12} = 335. \)
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 5: 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 6:
\[
P_{24} = \frac{1}{24} \{\mu(1)p^{24} + \mu(2)p^{12} + \mu(3)p^8 + \mu(4)p^6 + \mu(6)p^4 + \mu(8)p^3 + \mu(12)p^2 + \mu(24)p\}
\]
\[
= \frac{1}{24} \{p^{24} - p^{12} - p^8 + p^6\}.
\]
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 7:** 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 8:** \( 243 = 3^5 \) so \( G(\text{GF}(243)/\mathbb{Z}_3) \equiv C_5 \).