

MATH 523 LECTURE NOTES

Summer 2008

These notes are intended to provide additional background from abstract algebra that is necessary to provide a good context for the study of algebraic coding theory. In particular, we need to show how to construct all finite fields and we need to investigate their properties.

1 The definition of a field

We begin with the definition of a field. In linear algebra, we need to be able to add, subtract, multiply, and divide scalars. Similarly, in working with polynomials we need to be able to add, subtract, multiply, and divide the coefficients. This leads to the definition of a field, which generalizes the properties of the set \mathbf{Q} of rational numbers, the set \mathbf{R} of real numbers, and the set \mathbf{C} of complex numbers.

Let F be a set on which two binary operations are defined, called addition and multiplication, and denoted by $+$ and \cdot respectively. Then F is called a **field** with respect to these operations if the following properties hold:

(i) Closure. For all $a, b \in F$ the sum $a + b$ and the product $a \cdot b$ are uniquely defined and belong to F .

(ii) Associative laws. For all $a, b, c \in F$,

$$a + (b + c) = (a + b) + c \quad \text{and} \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c .$$

(iii) Commutative laws. For all $a, b \in F$,

$$a + b = b + a \quad \text{and} \quad a \cdot b = b \cdot a .$$

(iv) Distributive laws. For all $a, b, c \in F$,

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad \text{and} \quad (a + b) \cdot c = (a \cdot c) + (b \cdot c) .$$

(v) Existence of identity elements. The set F contains an additive identity element, denoted by 0 , such that for all $a \in F$,

$$a + 0 = a \quad \text{and} \quad 0 + a = a .$$

The set F also contains a multiplicative identity element, denoted by 1 (and assumed to be different from 0) such that for all $a \in F$,

$$a \cdot 1 = a \quad \text{and} \quad 1 \cdot a = a .$$

(vi) Existence of inverse elements. For each $a \in F$, the equations

$$a + x = 0 \quad \text{and} \quad x + a = 0$$

have a solution $x \in F$, called an additive inverse of a , and denoted by $-a$.

For each nonzero element $a \in F$, the equations

$$a \cdot x = 1 \quad \text{and} \quad x \cdot a = 1$$

have a solution $x \in F$, called a multiplicative inverse of a , and denoted by a^{-1} .

In addition to the examples \mathbf{Q} , \mathbf{R} , and \mathbf{C} mentioned earlier, the set \mathbf{Z}_2 of congruence classes of integers modulo 2 also satisfies the axioms of a field. This is an extremely important example because of our interest in coding theory. The addition and multiplication tables for \mathbf{Z}_2 are given below.

$$\begin{array}{c|cc} + & [0] & [1] \\ \hline [0] & [0] & [1] \\ [1] & [1] & [0] \end{array} \qquad \begin{array}{c|cc} \cdot & [0] & [1] \\ \hline [0] & [0] & [0] \\ [1] & [0] & [1] \end{array}$$

If p is a prime number, then the set \mathbf{Z}_p of congruence classes modulo p forms a field, so there is no limit to the size of a finite field. We will show that it is also possible to construct fields with p^n elements, for any prime p and any $n \geq 1$. As an example, we next exhibit a field with 4 elements.

The following set of matrices, with entries from \mathbf{Z}_2 , forms a field under the operations of matrix addition and multiplication:

$$F = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \right\}.$$

Here we have omitted the brackets from the congruence classes $[0]$ and $[1]$, so that we simply have $1 + 1 = 0$, etc. You should check that F is closed under addition and multiplication. The associative and distributive laws hold for all matrices. You can check that these particular matrices commute under multiplication. The additive identity is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, and the multiplicative identity is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Each element is its own additive inverse, and $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$.

It is important to note that the set \mathbf{Z} of integers does *not* satisfy the axioms of a field, since the only nonzero elements with multiplicative inverses are 1 and -1 . The existence of multiplicative inverses is the only axiom that does not hold. We say that a set R is a **commutative ring with identity** if it is a set with two operations $+$ and \cdot which satisfy all the axioms of a field except the existence of multiplicative inverses. According to this definition, for any positive integer n the set of congruence classes \mathbf{Z}_n is a commutative ring with identity.

2 Polynomials over a field

Let F be any field. If $a_m, a_{m-1}, \dots, a_1, a_0 \in F$, then any expression of the form

$$a_mx^m + a_{m-1}x^{m-1} + \dots + a_1x + a_0$$

is called a **polynomial over F** in the **indeterminate x** with coefficients a_m, a_{m-1}, \dots, a_0 . The set of all polynomials with coefficients in F is denoted by $F[x]$. If n is the largest nonnegative integer such that $a_n \neq 0$, then we say that the polynomial $f(x) = a_nx^n + \dots + a_0$ has **degree n** , written $\deg(f(x)) = n$, and a_n is called the **leading coefficient** of $f(x)$. If the leading coefficient is 1, then $f(x)$ is said to be **monic**.

According to this definition, the zero polynomial (each of whose coefficients is zero) has no degree. For convenience, it is often assigned $-\infty$ as a degree. A constant polynomial a_0 has degree 0 when $a_0 \neq 0$. Thus a polynomial belongs to the coefficient field if and only if it has degree 0 or $-\infty$.

Two polynomials are equal by definition if they have the same degree and all corresponding coefficients are equal. It is important to distinguish between the polynomial $f(x)$ as an element of $F[x]$ and the corresponding polynomial function from F into F defined by substituting elements of F in place of x . If $f(x) = a_mx^m + \dots + a_0$ and $c \in F$, then $f(c) = a_mc^m + \dots + a_0$. In fact, if F is a finite field, it is possible to have two different polynomials that define the same polynomial function. For example, let F be the field \mathbf{Z}_5 and consider the polynomials $x^5 - 2x + 1$ and $4x + 1$. For any $c \in \mathbf{Z}_5$, $c^5 \equiv c \pmod{5}$, and so

$$c^5 - 2c + 1 \equiv -c + 1 \equiv 4c + 1 \pmod{5},$$

which shows that as polynomial functions $x^5 - 2x + 1$ and $4x + 1$ are identical.

For the polynomials

$$f(x) = a_mx^m + a_{m-1}x^{m-1} + \dots + a_1x + a_0$$

and

$$g(x) = b_nx^n + b_{n-1}x^{n-1} + \dots + b_1x + b_0,$$

the sum of $f(x)$ and $g(x)$ is defined by just adding corresponding coefficients. The product $f(x)g(x)$ is defined to be

$$a_mb_nx^{n+m} + \dots + (a_2b_0 + a_1b_1 + a_0b_2)x^2 + (a_1b_0 + a_0b_1)x + a_0b_0.$$

The coefficient c_k of x^k in $f(x)g(x)$ can be described by the formula

$$c_k = \sum_{i+j=k} a_ib_j = \sum_{i=0}^k a_ib_{k-i}.$$

This definition of the product is consistent with what we would expect to obtain using a naive approach: Expand the product using the distributive law repeatedly (this amounts to multiplying each term by every other) and then collect similar terms.

If $f(x)$ and $g(x)$ are nonzero polynomials in $F[x]$, then $f(x)g(x)$ is nonzero and

$$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x)) .$$

If $f(x), g(x), h(x) \in F[x]$ and $f(x)$ is nonzero, then $f(x)g(x) = f(x)h(x)$ implies $g(x) = h(x)$.

Let $f(x), g(x) \in F[x]$. If $f(x) = q(x)g(x)$ for some $q(x) \in F[x]$, then we say that $g(x)$ is a **factor** or **divisor** of $f(x)$, and we write $g(x) \mid f(x)$. Let $f(x) = a_mx^m + \dots + a_0 \in F[x]$. An element $c \in F$ is called a **root** of the polynomial $f(x)$ if $f(c) = 0$, that is, if c is a solution of the polynomial equation $f(x) = 0$.

Theorem 2.1 (Division Algorithm) *For any polynomials $f(x), g(x) \in F[x]$, with $g(x) \neq 0$, there exist unique polynomials $q(x), r(x) \in F$ such that*

$$f(x) = q(x)g(x) + r(x) ,$$

where either $\deg(r(x)) < \deg(g(x))$ or $r(x) = 0$.

Corollary 2.2 *Let $f(x) \in F[x]$ be a nonzero polynomial, and let $c \in F$. Then c is a root of $f(x)$ if and only if $x - c$ is a factor of $f(x)$. That is, $f(c) = 0$ if and only if $(x - c) \mid f(x)$. A polynomial of degree n with coefficients in the field F has at most n distinct roots in F .*

A monic polynomial $d(x) \in F[x]$ is called the **greatest common divisor** of $f(x), g(x) \in F[x]$ if

- (i) $d(x) \mid f(x)$ and $d(x) \mid g(x)$, and
- (ii) if $h(x) \mid f(x)$ and $h(x) \mid g(x)$ for some $h(x) \in F[x]$, then $h(x) \mid d(x)$.

The greatest common divisor of $f(x)$ and $g(x)$ is denoted by $\gcd(f(x), g(x))$.

If $\gcd(f(x), g(x)) = 1$, then the polynomials $f(x)$ and $g(x)$ are said to be **relatively prime**.

Theorem 2.3 *For any nonzero polynomials $f(x), g(x) \in F[x]$, the greatest common divisor $\gcd(f(x), g(x))$ exists and can be expressed as a linear combination of $f(x)$ and $g(x)$, in the form*

$$\gcd(f(x), g(x)) = a(x)f(x) + b(x)g(x)$$

for some $a(x), b(x) \in F[x]$.

The Euclidean Algorithm can be used to find the greatest common divisor of two polynomials. Let $f(x), g(x) \in F[x]$ be nonzero polynomials. We can use the division algorithm to write $f(x) = q(x)g(x) + r(x)$, with $\deg(r(x)) < \deg(g(x))$ or $r(x) = 0$. If $r(x) = 0$, then $g(x)$ is a divisor of $f(x)$, and so $\gcd(f(x), g(x)) = g(x)$. If $r(x) \neq 0$, then it is easy to check that $\gcd(f(x), g(x)) = \gcd(g(x), r(x))$. This step reduces the degrees of the polynomials involved, and so repeating the procedure leads to the greatest common divisor of the two polynomials in a finite number of steps.

Proposition 2.4 *Let $p(x), f(x), g(x) \in F[x]$. If $p(x) \mid f(x)g(x)$ and $\gcd(p(x), f(x)) = 1$, then $p(x) \mid g(x)$.*

A nonconstant polynomial is said to be **irreducible over the field F** if it cannot be factored in $F[x]$ into a product of polynomials of lower degree. It is said to be **reducible over F** if such a factorization exists. Then a polynomial of degree 2 or 3 is irreducible over the field F if and only if it has no roots in F . A nonconstant polynomial $p(x) \in F[x]$ is irreducible over F if and only if for all $f(x), g(x) \in F[x]$, $p(x) \mid (f(x)g(x))$ implies $p(x) \mid f(x)$ or $p(x) \mid g(x)$.

Theorem 2.5 (Unique Factorization) *Any nonconstant polynomial with coefficients in the field F can be expressed as an element of F times a product of monic polynomials, each of which is irreducible over the field F . This expression is unique except for the order in which the factors occur.*

Let F be a field, and let $p(x)$ be a fixed polynomial over F . If $a(x), b(x) \in F[x]$, then we say that $a(x)$ and $b(x)$ are **congruent modulo $p(x)$** , written $a(x) \equiv b(x) \pmod{p(x)}$, if $p(x) \mid (a(x) - b(x))$. The set $\{b(x) \in F[x] \mid a(x) \equiv b(x) \pmod{p(x)}\}$ is called the **congruence class** of $a(x)$, and will be denoted by $[a(x)]$. The collection of all congruence classes modulo $p(x)$ will be denoted by $F[x]/\langle p(x) \rangle$.

We first note that congruence of polynomials defines an equivalence relation. Then since $a(x) \equiv b(x) \pmod{p(x)}$ if and only if $a(x) - b(x) = q(x)p(x)$ for some $q(x) \in F[x]$, the polynomials in the congruence class of $a(x)$ modulo $p(x)$ must be precisely the polynomials of the form $b(x) = a(x) + q(x)p(x)$, for some $q(x)$. When working in \mathbf{Z}_n with congruence classes modulo n , it is often easiest to work with the smallest nonnegative number in the class. Similarly, when working with congruence classes of polynomials, the polynomial of lowest degree in the congruence class is a natural representative. The next proposition guarantees that this representative is unique.

Proposition 2.6 *Let F be a field, and let $p(x)$ be a nonzero polynomial in $F[x]$. For any $a(x) \in F[x]$, the congruence class $[a(x)]$ modulo $p(x)$ contains a unique representative $r(x)$ with $\deg(r(x)) < \deg(p(x))$ or $r(x) = 0$.*

Proposition 2.7 *Let F be a field, and let $p(x)$ be a nonzero polynomial in $F[x]$. For any polynomials $a(x), b(x), c(x)$, and $d(x)$ in $F[x]$, the following conditions hold:*

- (a) *If $a(x) \equiv c(x) \pmod{p(x)}$ and $b(x) \equiv d(x) \pmod{p(x)}$, then $a(x) + b(x) \equiv c(x) + d(x) \pmod{p(x)}$ and $a(x)b(x) \equiv c(x)d(x) \pmod{p(x)}$.*
- (b) *If $a(x)b(x) \equiv a(x)c(x) \pmod{p(x)}$ and $\gcd(a(x), p(x)) = 1$, then $b(x) \equiv c(x) \pmod{p(x)}$.*

Proposition 2.8 *Let F be a field, and let $p(x)$ be a nonzero polynomial in $F[x]$. For any $a(x) \in F[x]$, the congruence class $[a(x)]$ has a multiplicative inverse in $F[x]/\langle p(x) \rangle$ if and only if $\gcd(a(x), p(x)) = 1$.*

Theorem 2.9 *Let F be a field, and let $p(x)$ be a nonconstant polynomial over F . Then $F[x]/\langle p(x) \rangle$ is a field if and only if $p(x)$ is irreducible over F .*

Example. Let $F = \mathbf{Z}_2$ and let $p(x) = x^2 + x + 1$. Then $p(x)$ is irreducible over \mathbf{Z}_2 since it has no roots in \mathbf{Z}_2 , and so $\mathbf{Z}_2[x]/\langle x^2 + x + 1 \rangle$ is a field. The congruence classes modulo $x^2 + x + 1$ can be represented by $[0]$, $[1]$, $[x]$ and $[1 + x]$, since these are the only polynomials of degree less than 2 over \mathbf{Z}_2 . Addition and multiplication are given in the following tables, which have been simplified by omitting all brackets for the congruence classes.

Addition in $\mathbf{Z}_2[x]/\langle x^2 + x + 1 \rangle$.

+	0	1	x	$1 + x$
0	0	1	x	$1 + x$
1	1	0	$1 + x$	x
x	x	$1 + x$	0	1
$1 + x$	$1 + x$	x	1	0

Multiplication in $\mathbf{Z}_2[x]/\langle x^2 + x + 1 \rangle$.

×	0	1	x	$1 + x$
0	0	0	0	0
1	0	1	x	$1 + x$
x	0	x	$1 + x$	1
$1 + x$	0	$1 + x$	1	x

Returning to the earlier example of a field with 4 elements, let

$$F = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \right\}.$$

Let I denote the identity matrix, and let $X = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$. Then $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = I + X$, and $X^2 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = I + X$. This shows that addition and multiplication behave just like the similar operations in $\mathbf{Z}_2[x]/\langle x^2 + x + 1 \rangle$. To give the corresponding tables for F , we can simply substitute I in place of 1 and X in place of x in the addition and multiplication tables for $\mathbf{Z}_2[x]/\langle x^2 + x + 1 \rangle$.

If $q(x)$ is irreducible over \mathbf{Z}_p , then $\mathbf{Z}_p[x]/\langle q(x) \rangle$ has p^n elements if $\deg(q(x)) = n$, since there are exactly $p^n - 1$ polynomials over \mathbf{Z}_p of degree less than n (including 0 gives p^n elements). It is possible to show that there exist polynomials of degree n irreducible over \mathbf{Z}_p for each integer $n > 0$. This guarantees the existence of a finite field having p^n elements, for each prime number p and each positive integer n .

Let R be a commutative ring with identity element 1. An element $a \in R$ is said to be **invertible** if there exists an element $b \in R$ such that $ab = 1$. The element a is also called a **unit** of R , and its multiplicative inverse is usually denoted by a^{-1} . Since $0 \cdot b = 0$ for all $b \in R$, it is impossible for 0 to be invertible. Furthermore, if $a \in R$ and $ab = 0$ for some nonzero $b \in R$, then a cannot be a unit since multiplying both sides of the equation by the inverse of a (if it existed) would show that $b = 0$. An element a such that $ab = 0$ for some $b \neq 0$ is called a **divisor of zero**. A commutative ring R with identity is called an **integral domain** if for all $a, b \in R$, $ab = 0$ implies $a = 0$ or $b = 0$. For any field F with identity 1, any subring of F that contains 1 is an integral domain. The converse is true in the sense that given any integral domain it is possible to construct a field of quotients in which there is an isomorphic copy of the integral domain.

Let R be a commutative ring. A nonempty subset I of R is called an **ideal** of R if (i) $a \pm b \in I$ for all $a, b \in I$ and (ii) $ra \in I$ for all $a \in I$ and $r \in R$.

It is clear that the set $\{0\}$ is an ideal, which we will refer to as the **trivial** ideal. The set R is also always an ideal. Among commutative rings with identity, fields are characterized by the property that these two ideals are the only ideals of the ring.

Let R be a commutative ring with identity 1. For any $a \in R$, let Ra denote the set $I = \{x \in R \mid x = ra \text{ for some } r \in R\}$. Then Ra is an ideal of R that contains a . It is obvious from the definition of an ideal that any ideal that contains a must also contain Ra , and so we are justified in saying that Ra is the smallest ideal that contains a . Furthermore, $R \cdot 1$ consists of all of R , since every element $r \in R$ can be expressed in the form $r \cdot 1$. Thus R is the smallest ideal (in fact, the only ideal) that contains 1.

Let R be a commutative ring with identity, and let $a \in R$. The ideal

$$Ra = \{x \in R \mid x = ra \text{ for some } r \in R\}$$

is called the **principal ideal** generated by a . The notation $\langle a \rangle$ will also be used.

If F is any field, then in the ring $F[x]$ of polynomials over F every ideal is a principal ideal domain. To show this, let I be any ideal of $F[x]$. If $I = \{0\}$, then 0 serves as a generator. If I is nonzero, then it must contain some polynomial of positive degree, so we can choose a monic polynomial $f(x)$ in I of minimal degree. It is clear that $\langle f(x) \rangle \subseteq I$. To show the reverse inclusion, let $g(x)$ be any polynomial in I . Then we can use the division algorithm to write $g(x) = q(x)f(x) + r(x)$, where $r(x) = 0$ or $\deg(r(x)) < \deg(f(x))$. Since $r(x) = g(x) - q(x)f(x)$, it belongs to I . The choice of $f(x)$ dictates that $r(x) = 0$, so $f(x)$ is a factor of $g(x)$, showing that $I \subseteq \langle f(x) \rangle$. Since a generator of I is a divisor of every element of I , it is easy to see that there is only one monic generator for I .

Our next step is to investigate the factor ring $F[x]/\langle p(x) \rangle$ when $p(x)$ is not irreducible. In this case the factor ring must have proper nontrivial ideals, since it is not a field. We will see that these ideals are still principal ideals.

Proposition 2.10 *Let $p(x)$ be a nonconstant polynomial in $F[x]$, of degree n .*

(a) *The factor ring $F[x]/\langle p(x) \rangle$ (the set of cosets of $\langle p(x) \rangle$) is a commutative ring with 1.*

(b) *$F[x]/\langle p(x) \rangle$ is a vector space of dimension n (over F).*

Proof. (b) Each coset $f(x) + \langle p(x) \rangle$ contains a unique representative of degree $< n$, the remainder on division of $f(x)$ by $p(x)$. Thus the cosets $1 + \langle p(x) \rangle$, $x + \langle p(x) \rangle$, \dots , $x^{n-1} + \langle p(x) \rangle$ form a basis for $F[x]/\langle p(x) \rangle$ over F . \square

Proposition 2.11 *Let $p(x)$ be a nonconstant polynomial in $F[x]$, of degree n . Let I be a proper nonzero ideal of $F[x]/\langle p(x) \rangle$.*

(a) *$I = \langle [g(x)] \rangle$, where $g(x)$ is the monic polynomial of lowest degree in I .*

(b) *$g(x)$ is a factor of $p(x)$.*

(c) *$I = \{[a(x)g(x)] \mid \deg(a(x)) < n - \deg(g(x))\}$, and so I is a subspace of $F[x]/\langle p(x) \rangle$ with dimension $n - \deg(g(x))$.*

Proof. (a) Choose a monic polynomial $g(x)$ in I that has minimal degree. Since I is an ideal and $\langle [g(x)] \rangle$ is the smallest ideal that contains $g(x)$, we have $\langle [g(x)] \rangle \subseteq I$. To prove the reverse inclusion, if $f(x)$ is any polynomial in I , we can use the division algorithm to write $f(x) = q(x)g(x) + r(x)$, where either $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$. Then $r(x) = f(x) - q(x)g(x)$ belongs to I since $f(x), g(x) \in I$ and I is closed under subtraction and under multiplication by any polynomial in $F[x]/\langle p(x) \rangle$. Because $g(x)$ is a polynomial of minimal degree in I , we can't have $r(x) \in I$ and $\deg(r(x)) < \deg(g(x))$. It follows that $r(x) = 0$, so $g(x)$ is a factor of $f(x)$ and therefore $I \subseteq \langle [g(x)] \rangle$.

(b) Use the division algorithm to write $p(x) = q(x)g(x) + r(x)$, where either $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$. As in part (a), we have $r(x) \in I$, since $p(x) \equiv 0$. Again, we must have $r(x) = 0$, and so $g(x)$ is a factor of $p(x)$.

(c) By definition, $\langle [g(x)] \rangle$ is the set of all polynomials $[a(x)g(x)]$ such that $[a(x)]$ belongs to $F[x]/\langle p(x) \rangle$, so we need to consider the products for all polynomials $a(x)$ of degree $< n$. But if $\deg(a(x)) \geq n - \deg(g(x))$, then $\deg(a(x)g(x)) = \deg(a(x)) + \deg(g(x)) \geq n$, and so we can reduce the degree using the congruence. That is, we divide by $p(x)$ and take the remainder, which will have degree $< n$. We get $a(x)g(x) = b(x)p(x) + r(x)$, for some $b(x)$, and then since $p(x) = q(x)g(x)$ from part (b) of the proof, we have $r(x) = (a(x) - b(x)q(x))g(x)$. Since $\deg(r(x)) < n$, it follows that $a(x) - b(x)q(x)$ has degree less than $n - \deg(g(x))$. This is exactly what we need to prove the first part of (c). From this we can easily find the dimension of I . In fact, for a basis for I we can use $g(x) + \langle p(x) \rangle$, $xg(x) + \langle p(x) \rangle$, \dots , $x^{k-1}g(x) + \langle p(x) \rangle$, where $k = n - \deg(g(x))$. \square

Corollary 2.12 *Let $p(x)$ be a nonconstant polynomial in $F[x]$, of degree n . The proper nontrivial ideals of $F[x]/\langle p(x) \rangle$ are in one-to-one correspondence with the proper divisors of $p(x)$.*

Example. Our later theory of finite fields will allow us to give the following factorization of $x^{15} - 1$ over $F = \mathbf{Z}_2$. (See Theorem 4.9).

$$x^{15} - 1 = (x - 1)(x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^4 + x^3 + 1)(x^4 + x + 1)$$

In $Z_2[x]/\langle x^{15} - 1 \rangle$ there are 2^5 ideals, since we get all of the factors of $x^{15} - 1$ by choosing a subset of its irreducible factors. Of course, of these only 30 are proper and nonzero.

For example, in $Z_2[x]/\langle x^{15} - 1 \rangle$, the ideal $\langle x^4 + x + 1 \rangle$ has dimension $15 - 4 = 11$, and has as its basis $[x^4 + x + 1]$, $[x(x^4 + x + 1)]$, $[x^2(x^4 + x + 1)]$, \dots , $[x^{10}(x^4 + x + 1)]$.

We need to give a definition that will be used in the exercises. An element e of a commutative ring R with 1 is said to be **idempotent** if $e^2 = e$. Of course, 0 and 1 are idempotent elements, but R may have other idempotent elements that are interesting. Note, however, that in a field 0 and 1 are the only idempotents. If e is idempotent, then $e(1 - e) = 0$ and $1 - e$ is also idempotent. (A quick calculation shows that $(1 - e)^2 = (1 - e)(1 - e) = 1 - e - e + e^2 = 1 - e$.)

Exercises

In these exercises, let F be a field, let $p(x)$ be a nonconstant polynomial in $F[x]$, and let $R = F[x]/\langle p(x) \rangle$.

1. If $f(x)$ is any polynomial, show that $\langle [f(x)] \rangle = \langle [d(x)] \rangle$ in R , where $d(x) = \gcd(f(x), p(x))$.
2. Suppose that $p(x) = g(x)h(x)$, where $\gcd(g(x), h(x)) = 1$. Show that in R we have $\langle [g(x)] \rangle = \{[f(x)] \in R \mid f(x)h(x) \equiv 0 \pmod{p(x)}\}$.
3. Suppose that $p(x) = g(x)h(x)$, where $\gcd(g(x), h(x)) = 1$.
 - (a) Show that there exists an idempotent coset $[e(x)]$ in R such that $\langle [g(x)] \rangle = \langle [e(x)] \rangle$.
 - (b) Show that $\langle [g(x)] \rangle = \{[f(x)] \mid f(x)e(x) \equiv f(x) \pmod{p(x)}\}$ and that $\langle [g(x)] \rangle = \{[f(x)] \mid f(x)(1 - e(x)) \equiv 0 \pmod{p(x)}\}$.

Hint: Write $1 = a(x)g(x) + b(x)h(x)$ and consider $e(x) = a(x)g(x)$.
4. In $Z_2[x]/\langle x^{15} - 1 \rangle$, find the idempotent generator for the ideal $\langle x^4 + x + 1 \rangle$.

3 Extension Fields

The field F is said to be an **extension field** of the field K if K is a subset of F which is a field under the operations of F . In this situation we also say that K is a **subfield** of F .

Let F be an extension field of K and let $u \in F$. If there exists a nonzero polynomial $f(x) \in K[x]$ such that $f(u) = 0$, then u is said to be **algebraic** over K . If there does not exist such a polynomial, then u is said to be **transcendental** over K . For example, in the extension field \mathbf{R} of \mathbf{Q} , the element $\sqrt{2}$ is algebraic over \mathbf{Q} , but π is transcendental over \mathbf{Q} . (This fact about π isn't easy to prove.)

Proposition 3.1 *Let F be an extension field of K , and let $u \in F$ be algebraic over K . Then there exists a unique monic irreducible polynomial $p(x) \in K[x]$ such that $p(u) = 0$. It is characterized as the monic polynomial of minimal degree that has u as a root. Furthermore, if $f(x)$ is any polynomial in $K[x]$ with $f(u) = 0$, then $p(x) \mid f(x)$.*

Proof. Let I be the set of all polynomials $f(x) \in K[x]$ such that $f(u) = 0$. It is easy to see that I is closed under sums and differences, and if $f(x) \in I$, then $g(x)f(x) \in I$ for all $g(x) \in K[x]$. Thus I is an ideal of $K[x]$, and so $I = \langle p(x) \rangle$ for any nonzero polynomial $p(x) \in I$ that has minimal degree. If $f(x), g(x) \in K[x]$ with $f(x)g(x) \in I$, then we have $f(u)g(u) = 0$, which implies that either $f(u) = 0$ or $g(u) = 0$, and so we see that I is a prime ideal. This implies that the unique monic generator $p(x)$ of I must be irreducible. Finally, since $I = \langle p(x) \rangle$, we have $p(x) \mid f(x)$ for any $f(x) \in I$. \square

Let F be an extension field of K , and let u be an algebraic element of F . The monic polynomial $p(x)$ of minimal degree in $K[x]$ such that $p(u) = 0$ is called the **minimal polynomial** of u over K . The degree of the minimal polynomial of u over K is called the **degree** of u over K .

In a field F , the intersection of any collection of subfields of F is again a subfield. In particular, if F is an extension field of K and $u \in F$, then the intersection of all subfields of F that contain both K and u is a subfield of F . This intersection is contained in any subfield that contains both K and u . This guarantees the existence of the field defined below.

Let F be an extension field of K , and let $u_1, u_2, \dots, u_n \in F$. The smallest subfield of F that contains K and u_1, u_2, \dots, u_n will be denoted by $K(u_1, u_2, \dots, u_n)$. It is called the **extension field of K generated by u_1, u_2, \dots, u_n** . If $F = K(u)$ for a single element $u \in F$, then F is said to be a **simple extension** of K .

If F is an extension field of K , and $u_1, u_2, \dots, u_n \in F$, then it is possible to construct $K(u_1, u_2, \dots, u_n)$ by adjoining one u_i at a time. That is, we first construct $K(u_1)$, and then consider the smallest subfield of F that contains $K(u_1)$ and u_2 . This would be written as $K(u_1)(u_2)$, but it is clear from the definition

of $K(u_1, u_2)$ that the two fields are equal. This procedure can be continued to construct $K(u_1, u_2, \dots, u_n)$. It is thus sufficient to describe $K(u)$ for a single element, which we do in the next proposition.

Proposition 3.2 *Let F be an extension field of K . If $u \in F$ is algebraic over K , then $K(u) \cong K[x]/\langle p(x) \rangle$, where $p(x)$ is the minimal polynomial of u over K .*

Proof. Suppose that the minimal polynomial $p(x)$ for u has degree n . Since $K(u)$ is a field, it is closed under products and sums, so because it contains u it must also contain all elements of F of the form $c_0 + c_1u + \dots + c_ku^k$, where $c_i \in K$. Since $p(u) = 0$, we have a relation of the form $a_0 + a_1u + \dots + u^n$. We can use this relation to reduce any polynomial in u to one of the form $c_0 + c_1u + \dots + c_ku^k$, where $k < n$. This subset of F turns out to be a field. To see this, given any nonzero element of the form $c = c_0 + c_1u + \dots + c_{n-1}u^{n-1}$, consider the corresponding polynomial $c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$. Because $p(x)$ is irreducible, and $\deg(c(x)) < \deg(p(x))$, we have $\gcd(p(x), c(x)) = 1$. Therefore there exist polynomials $d(x)$ and $t(x)$ with $c(x)d(x) + t(x)p(x) = 1$. Substituting $x = u$ gives us $c \cdot d(u) = 1$, which shows that c has a multiplicative inverse.

We conclude that $K(u)$ corresponds to elements of the form $c_0 + c_1u + \dots + c_{n-1}u^{n-1}$, where we use ordinary multiplication of polynomials but reduce the degree by using the identity $u^n = a_0 - a_1u - \dots - a_{n-1}u^{n-1}$. Thus $K(u)$ has exactly the same addition and multiplication as $K[x]/\langle p(x) \rangle$. \square

Proposition 3.3 *Let K be a field and let $p(x) \in K[x]$ be any irreducible polynomial. Then there exists an extension field F of K and an element $u \in F$ such that the minimal polynomial of u over K is $p(x)$.*

Proof. The extension field F is constructed as $K[x]/\langle p(x) \rangle$, and K is viewed as isomorphic to the subfield consisting of all cosets determined by the constant polynomials. The element u is the coset determined by x , and it follows that $p(u) = 0$. Since $p(x)$ is irreducible, it must be the minimal polynomial for u over K . \square

If F is an extension field of K , then the multiplication of F defines a scalar multiplication, considering the elements of K as scalars and the elements of F as vectors. This gives F the structure of a vector space over K , and allows us to make use of the concept of the dimension of a vector space.

Proposition 3.4 *Let F be an extension field of K and let $u \in F$ be an element algebraic over K . If the minimal polynomial of u over K has degree n , then $K(u)$ is an n -dimensional vector space over K .*

Proof. We have already shown that $K[x]/\langle p(x) \rangle$ has dimension n as a vector space over K . \square

Let F be an extension field of K . The dimension of F as a vector space over K is called the **degree** of F over K , denoted by $[F : K]$. If the dimension of F over K is finite, then F is said to be a **finite** extension of K .

In the next proposition, by using the notion of the degree of an extension, we are able to give a useful characterization of algebraic elements. The proposition implies, in particular, that every element of a finite extension must be algebraic.

Proposition 3.5 *Let F be an extension field of K and let $u \in F$. The following conditions are equivalent:*

- (1) u is algebraic over K ;
- (2) $K(u)$ is a finite extension of K ;
- (3) u belongs to a finite extension of K .

Proof. It is clear that (1) implies (2) and (2) implies (3). To prove (3) implies (1), suppose that $u \in E$ for an extension E with $K \subseteq E \subseteq F$ and $[E : K] = n$. The set $1, u, u^2, \dots, u^n$ contains $n + 1$ elements, and these cannot be linearly independent in an n -dimensional vector space. Thus there exists a relation $a_0 + a_1u + \dots + a_nu^n = 0$ with scalars $a_i \in K$ that are not all zero. This shows that u is a root of a polynomial in $K[x]$. \square

Counting arguments often provide very useful tools. In case we have extension fields $K \subseteq E \subseteq F$, we can consider the degree of E over K and the degree of F over E . The next theorem shows that there is a very simple relationship between these two degrees and the degree of F over K . It will play a very important role in our study of extension fields.

Theorem 3.6 *Let E be a finite extension of K and let F be a finite extension of E . Then F is a finite extension of K , and*

$$[F : K] = [F : E][E : K].$$

Proof. Let $[F : E] = n$ and let $[E : K] = m$. Let u_1, u_2, \dots, u_n be a basis for F over E and let v_1, v_2, \dots, v_m be a basis for E over K . We claim that the set B of nm products $u_i v_j$ (where $1 \leq i \leq n$ and $1 \leq j \leq m$) is a basis for F over K .

We must first show that B spans F over K . If u is any element of F , then $u = \sum_{i=1}^n a_i u_i$ for elements $a_i \in E$. For each element a_i we have $a_i = \sum_{j=1}^m c_{ij} v_j$, where $c_{ij} \in K$. Substituting gives $u = \sum_{i=1}^n \sum_{j=1}^m c_{ij} v_j u_i$, and so B spans F over K .

To show that B is a linearly independent set, suppose that $\sum_{i,j} c_{ij} v_j u_i = 0$ for some linear combination of the elements of B , with coefficients in K . This expression can be written as $\sum_{i=1}^n \left(\sum_{j=1}^m c_{ij} v_j \right) u_i$. Since the elements u_1, u_2, \dots, u_n form a basis for F over E , each of the coefficients $\sum_{j=1}^m c_{ij} v_j$ (which belong to E) must be zero. Then since the elements v_1, v_2, \dots, v_m form a basis for E over K , for each i we must have $c_{ij} = 0$ for all j . This completes the proof. \square

Corollary 3.7 *Let F be a finite extension of K . Then the degree of any element of F is a divisor of $[F : K]$.*

Proof. If $u \in F$, then $[F : K] = [F : K(u)][K(u) : K]$. \square

Definition 3.8 *Let K be a field and let $f(x) = a_0 + a_1x + \dots + a_nx^n$ be a polynomial in $K[x]$ of degree $n > 0$. An extension field F of K is called a **splitting field for $f(x)$ over K** if there exist elements $r_1, r_2, \dots, r_n \in F$ such that (i) $f(x) = a_n(x - r_1)(x - r_2) \cdots (x - r_n)$ and (ii) $F = K(r_1, r_2, \dots, r_n)$.*

In the above situation we usually say that $f(x)$ **splits** over the field F . The elements r_1, r_2, \dots, r_n are roots of $f(x)$, and so F is obtained by adjoining to K a complete set of roots of $f(x)$.

Theorem 3.9 *Let $f(x) \in K[x]$ be a polynomial of degree $n > 0$. Then there exists a splitting field F for $f(x)$ over K , with $[F : K] \leq n!$.*

Proof. The proof is by induction on the degree of $f(x)$. If $\deg(f(x)) = 1$, then K itself is a splitting field. Assume that $\deg(f(x)) = n$ and that the theorem is true for any polynomial $g(x)$ with $\deg(g(x)) < n$ over any field K . Let $p(x)$ be an irreducible factor of $f(x)$. There exists an extension field E of K in which $p(x)$ has a root r . We now consider the field $K(r)$. Over this field $f(x)$ factors as $f(x) = p(x)q(x) = (x - r)g(x)$ for some polynomial $g(x)$ of degree $n - 1$. Thus by the induction hypothesis there exists a splitting field F of $g(x)$ over $K(r)$, say $F = K(r)(r_1, r_2, \dots, r_{n-1})$, with $[F : K(r)] \leq (n - 1)!$. Then $F = K(r, r_1, r_2, \dots, r_{n-1})$ and it is clear that $f(x)$ splits over F . Finally, $[F : K] = [F : K(r)][K(r) : K] \leq (n - 1)!n = n!$. \square

The proof of the next theorem will be omitted, even though the theorem is crucial in determining the structure of all finite fields.

Theorem 3.10 *Let $f(x)$ be a polynomial over the field K . The splitting field of $f(x)$ over K is unique up to isomorphism.*

Exercises

- Find the splitting fields over \mathbf{Z}_2 for the following polynomials:
 - $x^2 + x + 1$
 - $x^2 + 1$
 - $x^3 + x + 1$
 - $x^3 + x^2 + 1$
- Find the splitting field for $x^p - x$ over \mathbf{Z}_p .
- Show that if F is an extension field of K of degree 2, then F is the splitting field over K for some polynomial.

4 The structure of finite fields

With the field theory we have developed it is now possible to give a complete description of the structure of all finite fields.

If F is any finite field, then the smallest subfield of F that contains the identity element 1 is called the **prime subfield** of F . The elements of F form an abelian group under addition, so 1 is an element with some finite order n . That is, n is the smallest positive integer with $n \cdot 1 = 0$, and we say that F has **characteristic** n . If n were composite, say $n = a \cdot b$ for integers a and b less than n , then it follows from the distributive law that $(a \cdot 1) \cdot (b \cdot 1) = n \cdot 1 = 0$. In any field the product of nonzero elements must be nonzero, so this would give a contradiction. It follows that 1 has prime order, and it is easy to see that 1 determines a subfield isomorphic to \mathbf{Z}_p . In summary, if F is a finite field, then it has characteristic p for some prime number p , and its prime subfield is isomorphic to \mathbf{Z}_p .

Proposition 4.1 *Let F be a finite field of characteristic p . Then F has p^n elements, for some positive integer n .*

Proof. Let K be the prime subfield of F , which is isomorphic to \mathbf{Z}_p . Since F is finite, it must certainly have finite dimension as a vector space over K , say $[F : K] = n$. If v_1, v_2, \dots, v_n is a basis for F over K , then each element of F has the form $a_1v_1 + a_2v_2 + \dots + a_nv_n$ for elements $a_1, a_2, \dots, a_n \in K$. Thus to define an element of F there are n coefficients a_i , and for each coefficient there are p choices, since K has only p elements. Therefore the total number of ways in which an element in F can be defined is p^n . \square

Theorem 4.2 *Let F be a finite field with p^n elements. Then F is the splitting field of the polynomial $x^{p^n} - x$ over the prime subfield of F .*

Proof. Let F be a finite field of characteristic p . Then as in the previous proposition, F is an extension of degree n of its prime subfield K , which is isomorphic to \mathbf{Z}_p . Since F has p^n elements, the order of the multiplicative group F^\times of nonzero elements of F is $p^n - 1$. Therefore $x^{p^n - 1} = 1$ for all $0 \neq x \in F$, and so $x^{p^n} = x$ for all $x \in F$. The polynomial $f(x) = x^{p^n} - x$ has at most p^n roots, and so its roots must be precisely the elements of F . Thus F is the splitting field of $f(x)$ over K . \square

Corollary 4.3 *Two finite fields are isomorphic if and only if they have the same number of elements.*

Proof. Let F and E be finite fields with p^n elements, containing prime subfields K and L , respectively. Then $K \cong \mathbf{Z}_p \cong L$ and so $F \cong E$ by Theorem 3.10, since both F and E are splitting fields of $x^{p^n} - x$ over K and L , respectively. \square

Lemma 4.4 *Let F be a field of prime characteristic p , and let $n \in \mathbf{Z}^+$. Then $\{a \in F \mid a^{p^n} = a\}$ is a subfield of F .*

Proof. Let $E = \{a \in F \mid a^{p^n} = a\}$. With the exception of the coefficients of x^p and y^p , each binomial coefficient $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ in the expansion of $(x \pm y)^p$ contains p in the numerator but not the denominator, because p is prime. Since $\text{char}(F) = p$, this implies that $(x \pm y)^p = x^p \pm y^p$, for all $x, y \in F$. Applying this formula inductively to $(a \pm b)^{p^k}$ for $k \leq n$ shows that $(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n}$, and it follows immediately that E is closed under addition and subtraction.

Since $(ab)^{p^n} = a^{p^n} b^{p^n}$, it is clear that E is closed under multiplication. To complete the proof, we only need to observe that if $a \in E$ is nonzero, then $(a^{-1})^{p^n} = (a^{p^n})^{-1} = a^{-1}$, and so $a^{-1} \in E$. \square

Proposition 4.5 *Let F be a field with p^n elements. Each subfield of F has p^m elements for some divisor m of n . Conversely, for each positive divisor m of n there exists a unique subfield of F with p^m elements.*

Proof. Let K be the prime subfield of F . Any subfield E of F must have p^m elements, where $m = [E : K]$. Then $m|n$ since $n = [F : K] = [F : E][E : K]$.

Conversely, suppose that $m|n$ for some $m > 0$. Then $p^m - 1$ is a divisor of $p^n - 1$, and so $g(x) = x^{p^m - 1} - 1$ is a divisor of $f(x) = x^{p^n - 1} - 1$. Since F is the splitting field of $xf(x)$ over K , with distinct roots, it must contain all p^m distinct roots of $g(x)$, and these roots form a subfield of F . Furthermore, any other subfield with p^m elements must be a splitting field of $g(x)$, and so it must consist of precisely the same elements. \square

Lemma 4.6 *Let F be a field of characteristic p . If n is a positive integer not divisible by p , then the polynomial $x^n - 1$ has no repeated roots in any extension field of F .*

Proof. Let c be a root of $x^n - 1$ in an extension E of F . A direct computation shows that we must have the factorization

$$x^n - 1 = (x - c)(x^{n-1} + cx^{n-2} + c^2x^{n-3} + \dots + c^{n-2}x + c^{n-1}).$$

With the notation $x^n - 1 = (x - c)f(x)$, we only need to show that $f(c) \neq 0$. Since $f(x)$ has n terms, we have $f(c) = nc^{n-1}$, and then $f(c) \neq 0$ since $p \nmid n$. \square

Theorem 4.7 *For each prime p and each positive integer n , there exists a field with p^n elements.*

Proof. Let F be the splitting field of $f(x) = x^{p^n} - x$ over the field \mathbf{Z}_p . Since $x^{p^n} - x = x(x^{p^n-1} - 1)$ and $p^n - 1$ is not divisible by p , it follows from the lemma that $f(x)$ has distinct roots. The set of all roots of $f(x)$ is a subfield of F , and so we conclude that F must consist of precisely the roots of $f(x)$, of which there are exactly p^n elements. \square

Definition 4.8 Let p be a prime number and let $n \in \mathbf{Z}^+$. The field (unique up to isomorphism) with p^n elements is called the Galois field of order p^n , denoted by $GF(p^n)$.

Theorem 4.9 Let $F = GF(p^n)$, and let $p^n = q$. The irreducible factors of $x^{q^m} - x$ in $F[x]$ are precisely the monic irreducible polynomials in $F[x]$ whose degree divides m .

Proof. The splitting field for $f(x) = x^{q^m} - x$ over F is $GF(q^m)$, so the degree of any root of an irreducible factor of $f(x)$ must be a divisor of $m = [GF(q^m) : GF(q)]$. Thus the degree of any irreducible factor is a divisor of m .

On the other hand, let $p(x)$ be any irreducible polynomial of degree k such that $k|m$. Adjoining a root u of $p(x)$ gives a field $F(u)$ with q^k elements, which must be isomorphic to a subfield of $GF(q^m)$ since $k|m$. Since $p(x)$ is still the minimal polynomial of the image of u in $GF(q^m)$, it follows that $p(x)$ is a factor of $x^{q^m} - x$. \square

Let $f(x)$ be an irreducible polynomial over the finite field K , and suppose that $f(x)$ has a root in the extension F , with $|F| = p^n$. Then the elements of F are the roots of $x^{p^n} - x$, and $f(x) \mid x^{p^n} - x$, so there are several consequences. First, since $x^{p^n} - x$ has no repeated roots the same condition holds for $f(x)$. Secondly, $f(x)$ splits over F since F contains all the roots of $f(x)$. This proves that if K is a finite field, $f(x) \in K[x]$ is an irreducible polynomial, and F is any extension field of K that contains a root u of $f(x)$, then $K(u)$ is a splitting field for $f(x)$ over K .

We need the following result from group theory to give a direct proof that the multiplicative group F^\times of any finite field F is cyclic.

Let G be a finite abelian group. If $a \in G$ is an element of maximal order in G , then the order of every element of G is a divisor of the order of a .

Proof. Let a be an element of maximal order in G , and let x be any element of G different from the identity. If $o(x) \nmid o(a)$, then in the prime factorizations of the respective orders there must exist a prime p that occurs to a higher power in $o(x)$ than in $o(a)$. Let $o(a) = p^\alpha n$ and $o(x) = p^\beta m$, where $\alpha < \beta$ and $p \nmid n, p \nmid m$. Now $o(a^{p^\alpha}) = n$ and $o(x^m) = p^\beta$, and so the orders are relatively prime since $p \nmid n$. It follows that the order of the product $a^{p^\alpha} x^m$ is equal to np^β , which is greater than $o(a)$, a contradiction. \square

Theorem 4.10 The multiplicative group of nonzero elements of a finite field is cyclic.

Proof. Let F be a finite field with p^n elements, and let $k = p^n - 1$, so that $|F^\times| = k$. Let a be an element of F^\times of maximal order, with $o(a) = m$. By the

previous lemma, each element of F^\times satisfies the polynomial $x^m - 1$. Since F is a field, there are at most m roots of this polynomial, and so $k \leq m$. This implies that $m = k$ and F^\times is cyclic. \square

An extension field F of K is said to be a **simple** extension of K if $F = K(u)$ for some $u \in F$. In this case u is called a **primitive element** of F .

Theorem 4.11 *Any finite field is a simple extension of its prime subfield.*

Proof. Let F be a finite field with prime subfield K . The multiplicative group F^\times is cyclic, and so it is clear that $F = K(u)$ for any generator u of F^\times . \square

Corollary 4.12 *For each positive integer n there exists an irreducible polynomial of degree n in $\mathbf{Z}_p[x]$.*

Proof. Given $n \in \mathbf{Z}^+$, there exists an extension F of \mathbf{Z}_p of degree n . Then F is a simple extension of \mathbf{Z}_p , and so if u is any generator of F , then the minimal polynomial $p(x)$ of u over \mathbf{Z}_p must be an irreducible polynomial of degree n . \square

Exercises

1. Give a multiplication table for $GF(3^2)$. Find all generators for the cyclic group $GF(3^2)^\times$, and find the minimal polynomial of each generator over \mathbf{Z}_3 .
2. Find all generators for the cyclic group of nonzero elements of $GF(2^4)$, and find the minimal polynomial of each generator over \mathbf{Z}_2 .
3. Let m, n be positive integers with $\gcd(m, n) = d$. Show that over any field the greatest common divisor of $x^m - 1$ and $x^n - 1$ is $x^d - 1$. *Hint:* Use the Euclidean algorithm.
4. If E and F are subfields of $GF(p^k)$ with p^m and p^n elements respectively, use the previous exercise to show that $E \cap F$ contain p^d elements, where $d = \gcd(m, n)$.