Finite Fields with Prime Power Elements

The goal is to construct finite fields with p^n elements from the polynomial rings $\mathbb{F}_p[x]$. The construction will be very similar to that of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ from $\mathbb{Z}$, where p is a prime number.

the ring of integers $\mathbb{Z}$	the ring of polynomials $\mathbb{F}[x]$
Division with Remainder: For positive $m, n \in \mathbb{Z}$, there exist nonnegative $q, r \in \mathbb{Z}$ such that $m = qn + r$ with $r < n$.	For $f(x), g(x) \in \mathbb{F}[x]$ with $g(x) \neq 0$, there exist $q(x), r(x)$ such that $f(x) = q(x)g(x) + r(x)$ and $\deg r(x) < \deg g(x)$ or $r(x) = 0$.
Bezout's identity For positive $m, n \in \mathbb{Z}$, there exist $a, b \in \mathbb{Z}$ such that $\gcd(m, n) = am + bn$.	For $f(x), g(x) \in \mathbb{F}[x]$,there exist $a(x), b(x) \in \mathbb{F}[x]$ such that $\gcd(f(x), g(x)) = a(x)f(x) + b(x)g(x)$.
prime number p	irreducible polynomial $p(x)$
the quotient ring $\mathbb{Z}/nZ$	the quotient ring $\mathbb{F}[x]/\langle p(x)\rangle$ (p(x) not necessarily irreducible)
$\mathbb{Z}/nZ$ is a field iff n is prime	$\mathbb{F}[x]/\langle p(x)\rangle$ is a field iff $p(x)$ is irreducible.

Definition 1. *A set R, together with two binary operations $+, \cdot$, is called a ring if the following axioms hold.*

- *(Associativity of addition) $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$.*
- *(Associativity of multiplication) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$.*
- *(Commutativity of addition) $a + b = b + a$ for all $a, b \in R$,*
- *(Distributivity of multiplication over addition) $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in R$,.*
- *(Existence of additive identity) There is an element in R, denoted by 0, such that $a + 0 = a$ for all $a \in R$.*
- *(Existence of additive inverses) For every element $a \in R$, there exists an element $(-a) \in R$ such that $a + (-a) = 0$.*

R is said to be commutative *if*

- *(Commutativity of multiplication) $a \cdot b = b \cdot a$ for all $a, b \in R$,.*

R is said to contain the multiplicative identity (or with 1) if

- *(Existence of multiplicative identity) There is an element in R, denoted by 1, such that $1 \cdot a = a$ for all $a \in R$.*

In short, a commutative ring with 1 satisfies all the field axioms except "existence of multiplicative inverse".

Examples 2. *The follwing are rings.*

1. *Any field $\mathbb{F}$.*
2. $\mathbb{Z}$
3. $\mathbb{Z}/nZ$
4. *$LT(V, V)$, the set of linear transformation from V to itself.*
5. $Fun(\mathbb{F}, \mathbb{F})$
6. $\mathbb{F}[x]$.

7. $\mathbb{F}[x_1, ..., x_k]$

Proposition 3. ***(Division with Remainder)*** *Given $f(x), g(x) \in \mathbb{F}[x]$ with $g(x) \neq 0$, there exist unique $q(x), r(x)$ such that $f(x) = q(x)g(x) + r(x)$ and $\deg r(x) < \deg g(x)$ or $r(x) = 0$.*

Proof. Fix $g(x)$. We proceed by induction on $\deg f(x)$.

When $\deg f(x) < \deg g(x)$ or when $f(x) = 0$, there's nothing to prove. We can simply set $q(x) = 0$ and $r(x) = f(x)$. This serves as our base case.

Now the induction hypothesis is that the statement is true whenever $\deg f(x) < n$. (Since we have shown this for $n = \deg g(x)$, we can assume that $n \geq \deg g(x) = m$). When $\deg f(x) = n$, let $f(x) = \alpha_n x^n + ... + \alpha_0$ and let $g(x) = \beta_m x^m + ... + \beta_0$. Then one easily sees that $f(x) - \alpha_n \beta_m^{-1} x^{n-m} g(x)$ has degree less than n. By induction hypothesis, there exist $q_1(x), r(x)$ such that $f(x) - \alpha_n \beta_m^{-1} x^{n-m} g(x) = q_1(x)g(x) + r(x)$ and $\deg r(x) < \deg g(x)$ or $r(x) = 0$. Let $q(x) = q_1(x) + \alpha_n \beta_m^{-1} x^{n-m}$, the equation above becomes $f(x) = q(x)g(x) + r(x)$ with $\deg r(x) < \deg g(x)$ or $r(x) = 0$, which completes the proof. $\square$

This allows us to perform Euclidean Algorithm: Given $f(x), g(x) \in \mathbb{F}[x]$ with $g(x) \neq 0$, we can successively write down a sequence of equations:

$$\begin{aligned}
f(x) &= q_0(x)g(x) + r_0(x) \\
g(x) &= q_1(x)r_0(x) + r_1(x) \\
r_0(x) &= q_2(x)r_1(x) + r_2(x) \\
r_1(x) &= q_3(r)r_2(x) + r_3(x) \\
&... \\
r_{n-2}(x) &= q_n(r)r_{n-1}(x) + r_n(x) \\
r_{n-1}(x) &= q_{n+1}(x)r_n(x) + 0
\end{aligned}$$

such that $\deg r_i(x) < \deg r_{i-1}(x)$ for all i.

Another consequence of proposition 3 is the following.

Proposition 4. ***(Root Theorem)*** *Let $\alpha \in \mathbb{F}$. Then for $p(x) \in \mathbb{F}[x]$, $p(\alpha) = 0$ if and only if $(x - \alpha)|p(x)$.*

Proof. Assume $p(\alpha) = 0$. By Proposition 3, there exist $q(x) \in \mathbb{F}[x], r \in \mathbb{F}$ such that $p(x) = q(x)(x - \alpha) + r$. When $x = \alpha$, this becomes $0 = r$, so $x - \alpha | p(x)$.

Conversely, assume $(x - \alpha)|p(x)$. Then there exists $q(x) \in \mathbb{F}[x]$ such that $(x - \alpha)q(x) = p(x)$. When $x = \alpha$, this becomes $0 = p(\alpha)$. $\square$

Definition 5. *A non-constant polynomial $p(x)$ is said to be* irreducible *if there do not exist two non-constant polynomials $f(x), g(x) \in \mathbb{F}[x]$ such that $p(x) = f(x)g(x)$.*

Question 6. *Is x^2+1 irreducible in $\mathbb{R}[x]$? in $\mathbb{C}[x]$? in $\mathbb{F}_2[x]$? Is 6 irreducible in $\mathbb{F}_7[x]$? Is $2x+2$ irreducible in $\mathbb{F}_7[x]$?*

Examples 7.

1. *All polynomials with degree 1 are irreducible in $\mathbb{F}[x]$.*
2. *Constants polynomials are **not** considered irreducible in $\mathbb{F}[x]$.*
3. *When $\mathbb{F}=\mathbb{C}$, the Fundamental Theorem of Algebra and the Root Theorem together imply that the irreducible polynomials in $\mathbb{C}[x]$ are linear (i.e. of degree 1).*
4. *When $\mathbb{F}=\mathbb{R}$, it can be shown that the irreducible polynomials in $\mathbb{R}[x]$ are either linear or quadratic (i.e. of degree 2) with negative discriminant.*
5. *When $\mathbb{F}=\mathbb{F}_2$, we will show that a complete list of irreducible polynomials in $\mathbb{F}_2[x]$ of degree 3 is : x^3+x+1, x^3+x^2+1.*

For $\mathbb{F}[x]$, define $\langle p(x)\rangle=\{p(x)\cdot f(x)|f(x)\in\mathbb{F}[x]\}$, i.e. the set polynomials that are divisible $p(x)$. It's easy to show that $\langle p(x)\rangle$ is a subspace of $\mathbb{F}[x]$ so that we can define the quotient vector space $\mathbb{F}[x]/\langle p(x)\rangle$. Elements in $\mathbb{F}[x]/\langle p(x)\rangle$ are equivalence classes, and are denoted by $[f(x)]_{\langle p(x)\rangle}$ (or simply by $[f(x)]$ when no confusion arises) as usual. It can be shown that $[f(x)]=[g(x)]$ if and only if $p(x)|f(x)-g(x)$. Finally, it's an easy exercise to show that the binary operations $+,\cdot$ defined by

$$\begin{aligned}[f(x)]+[g(x)] &= [f(x)+g(x)]\\ [f(x)]\cdot[g(x)] &= [f(x)g(x)]\end{aligned}$$

are well defined and turn $\mathbb{F}[x]/\langle p(x)\rangle$ into a ring. The proof is exactly the same as that for $\mathbb{Z}/n\mathbb{Z}$.

Definition 8. *Let $f(x),g(x)\in\mathbb{F}[x]$, the* greatest common divisor *of $f(x)$ and $g(x)$, denoted by $\gcd(f(x),g(x))$, is the monic polynomial, with greatest degree, that divides both $f(x)$ and $g(x)$. Recall that a polynomial is called* monic *if it's leading coefficient is 1.*

Proposition 9. *(**Bezout's Identity**) Let $f(x),g(x)\in\mathbb{F}[x]$. There exist $a(x),b(x)\in\mathbb{F}[x]$ such that $\gcd(f(x),g(x))=a(x)f(x)+b(x)g(x)$.*

Proof. The proof will be similar to the analogous statement for $\mathbb{Z}$, so we only sketch it. We will also refer to the Euclidean Algorithm above. It's an easy exercise to show that $\gcd(g(x),r(x))=\gcd(g(x),q(x)g(x)+r(x))$ for arbitrary $g(x),r(x),q(x)\in\mathbb{F}[x]$. Applying this result multiple times to the Euclidean Algorithm above, we get $\gcd(f(x),g(x))=\gcd(g(x),r_0(x))=\gcd(r_0(x),r_1(x))=\gcd(r_1(x),r_2(x))=...=\gcd(r_{n-1}(x),r_n(x))$. Now since $r_n(x)$ divides $r_{n-1}(x)$, you may have guessed that $\gcd(r_{n-1}(x),r_n(x))=r_n(x)$. This is close, but not quite correct because $r_n(x)$ needs not be monic. To remedy this, we need to scale $r_n(x)$ by a constant $\alpha\in\mathbb{F}$ to make it monic. (More explicitly, if the leading coefficient of $r_n(x)$ is β, we pick $\alpha=\beta^{-1}$.) In summary, we have $\gcd(f(x),g(x))=\alpha r_n(x)$.

The second to last equation in the Euclidean Algorithm allows us to express $r_n(x)$ as a linear combination of $r_{n-1}(x)$ and $r_{n-2}(x)$: $r_n(x)=r_{n-2}(x)-q_n(x)r_{n-1}(x)$. The third to last equation allows us to do the substitution $r_{n-1}(x) = r_{n-3}(x) - q_{n-1}(x)r_{n-2}(x)$ so that $r_n(x) = r_{n-2}(x) - q_n(x)r_{n-1}(x) = r_{n-2}(x) - q_n(x)(r_{n-3}(x) - q_{n-1}(x)r_{n-2}(x)) = (1 + q_n(x)q_{n-1}(x))r_{n-2}(x) - q_n(x)r_{n-3}(x)$ can be written as a linear combination of $r_{n-2}(x)$ and $r_{n-3}(x)$. We can repeat this process and eventually find $a(x), b(x) \in \mathbb{F}[x]$ such that $r_n(x) = a(x)f(x) + b(x)g(x)$.

In conclusion, $\gcd(f(x), g(x)) = \alpha r_n(x) = \alpha a(x)f(x) + \alpha b(x)g(x)$ □

Theorem 10. *$\mathbb{F}[x]/\langle p(x)\rangle$ is a field if and only if $p(x)$ is irreducible.*

Proof. Assume $p(x)$ is irreducible. We have seen that $\mathbb{F}[x]/\langle p(x)\rangle$ is a ring. In order to prove that $\mathbb{F}[x]/\langle p(x)\rangle$ is a field, it suffices to verify that multiplicative inverse exists. Let $[f(x)]$ be a non-zero element in $\mathbb{F}[x]/\langle p(x)\rangle$, note that this is equivalent to saying that $p(x)$ does not divide $f(x)$. Since $p(x)$ is irreducible, its only monic factors are $\alpha p(x)$ and 1, where $\alpha \in \mathbb{F}$ is some constant that makes $\alpha p(x)$ monic. Since $p(x)$ does not divide $f(x)$, neither does $\alpha p(x)$, so $\gcd(p(x), f(x)) = 1$. By Bezout, there exist $a(x), b(x) \in \mathbb{F}[x]$ such that $1 = a(x)p(x) + b(x)f(x)$. Passing to the quotient space, this becomes $[1] = [a(x)][p(x)] + [b(x)][f(x)] = [b(x)][f(x)]$. Thus $[b(x)]$ is the multiplicative inverse of $[f(x)]$.

Conversely, assume $p(x)$ is not irreducible, then $p(x) = f(x)g(x)$ for some $f(x), g(x) \in \mathbb{F}[x]$ with degrees ≥ 1. Since $f(x), g(x)$ are not divisible by $p(x)$, $[f(x)], [g(x)] \neq 0$. Suppose by contradiction that $\mathbb{F}[x]/\langle p(x)\rangle$ is a field, then $[f(x)]^{-1}$, $[g(x)]^{-1}$ exist. It follows that $[0] = [f(x)]^{-1} \cdot [0] \cdot [g(x)]^{-1} = [f(x)]^{-1}[p(x)][g(x)]^{-1} = [f(x)]^{-1}[f(x)][g(x)][g(x)]^{-1} = [1]$, which is a contradiction. □

Theorem 11. *Let $p(x) \in \mathbb{F}_p[x]$ be an irreducible polynomial with degree n. Then $\mathbb{F}_p[x]/\langle p(x)\rangle$ is a field with p^n elements.*

Proof. We need to count the number of elements in $\mathbb{F}_p[x]/\langle p(x)\rangle$.

First of all, we will show that every class in $\mathbb{F}_p[x]/\langle p(x)\rangle$ can be represented by a polynomial with degree less than n. Indeed, let $[f(x)] \in \mathbb{F}_p[x]/\langle p(x)\rangle$. Perform division with remainder, we can find $g(x), r(x)$ such that $f(x) = g(x)p(x) + r(x)$ with $\deg r(x) < n$. Since $p(x) | f(x) - r(x)$, $[f(x)] = [r(x)]$.

We next show that if $r_1(x)$ and $r_2(x)$ are distinct polynomials with degrees $< n$, then $[r_1(x)] \neq [r_2(x)]$. Indeed, since $\deg(r_1(x) - r_2(x)) < n = \deg p(x)$, $p(x) \nmid (r_1(x) - r_2(x))$. Thus $[r_1(x)] \neq [r_2(x)]$.

Combine the results from the last two paragraphs, we see that the number of elements in $\mathbb{F}_p[x]/\langle p(x)\rangle$ is the same as the number of polynomials in $\mathbb{F}_p[x]$ with degree $< n$, which is p^n. □

Fact 12. *For any positive integer n, there exists an irreducible polynomial in $\mathbb{F}_p[x]$ with degree n.*

Corollary 13. *For any positive integer n and prime number p, there exists a field with p^n elements.*