Galois' Theorem and Polynomial Arithmetic

Sometimes, a finite field is also called a Galois Field. It is so named in honour of Évariste Galois, a French mathematician. Galois is the first one who established the following fundamental theorem on the existence of finite fields:

> An order-n finite field exists if and only if $n = p^m$ for some prime p (p is called the characteristic of this finite field) and some positive integer m.

In fact, an order-n finite field is unique (up to isomorphism). All finite fields of the same order are structurally identical. We usually use $GF(p^m)$ to represent the finite field of order p^m. As we have shown above, addition and multiplication modulo a prime number p form a finite field. The order of the field is p^1. However, modulo arithmetic on its own will not let us to construct a finite field with order of p^m for $m > 1$. For example, $2^3 = 8$, and we've already know $(Z_8, +, *)$ is not a field. One way to construct a finite field with $m >1$ is using the **polynomial basis**. The field is constructed as a set of p^m polynomials along with two polynomial operations.

Here a polynomial $f(x)$ is a mathematical expression in the form $a_n x^n + a_{n-1}x^{n-1} + ... + a_0$. The highest exponent of x is the **degree** of the polynomial. For example, the degree of $x^5 + 3x^3 + 4$ is 5. In a polynomial, a_n, a_{n-1}, ... , a_0 are called **coefficients**. If in a polynomial, the coefficients a_n, a_{n-1}, ... , a_1 are all 0, or in other words, the polynomial is in the form of a_0, we call this polynomial a **constant**. We can add, subtract polynomials by combine the terms in the polynomials with the same powers. For example:

- Polynomial addition: $(x^5 + 3x^3 + 4)+(6x^6 + 4x^3) = 6x^6 + x^5 + 7x^3 + 4$

$$\begin{array}{r} x^5 + 3x^3 + 4 \\ +\ 6x^6 + \quad + 4x^3 \\ \hline 6x^6 + x^5 + 7x^3 + 4 \end{array}$$

- Polynomial subtraction: $(x^5 + 3x^3 + 4)-(6x^6 + 4x^3) = -6x^6 + x^5 - x^3 + 4$

$$\begin{array}{r} x^5+3x^3+4 \\ -\quad 6x^6+\quad +4x^3 \\ \hline -6x^6+x^5-1x^3+4 \end{array}$$

We can also multiply two polynomials. The general rule is that each term in the first polynomial has to multiply each term in the second polynomial, then sum the resulted polynomials up. For example:

- Polynomial multiplication: $(x^5 + 3x^3 + 4)*(6x^6 + 4x^3) = 6x^{11} + 18x^9 + 4x^8 + 36x^6 + 16x^3$

$$\begin{array}{r} x^5+3x^3+\ 4 \\ \times \qquad\qquad 6x^6+\ 4x^3 \\ \hline 4x^8+12x^6+\ 16x^3 \\ 6x^{11}+18x^9 \qquad +24x^6 \\ \hline 6x^{11}+18x^9+4x^8+36x^6+16x^3 \end{array}$$

We can also divide polynomials using long division. For example:

- Polynomial division: $(6x^{11} + 18x^9 + 4x^8 + 36x^6 + 16x^3) \div (x^5 + 3x^3 + 4) = 6x^6 + 4x^3$

$$\begin{array}{r} 6x^6+\qquad 4x^3 \\ x^5+3x^3+\ 4\ \overline{)\ 6x^{11}+18x^9+4x^8+36x^6+16x^3} \\ \underline{6x^{11}+\ 18x^9+\qquad 24x^6} \\ 4x^8+12x^6+16x^3 \\ \underline{4x^8+12x^6+16x^3} \\ 0 \end{array}$$

But in many cases the divisors cannot divide the dividends, which means you will have remainders. For example:

- Polynomial division with remainder: $(3x^6 + 7x^4 + 4x^3 + 5) \div (x^4 + 3x^3 + 4) = 3x^2 - 9x + 34$ with remainder $-98x^3 - 12x^2 + 26x - 131$

$$
\begin{array}{r}
3x^2-9x+34 \\
x^4+3x^3+4\,\overline{)\,3x^6+\qquad 7x^4+4x^3\qquad\qquad +5} \\
\underline{3x^6+9x^5\qquad\qquad +12x^2\qquad\qquad\quad} \\
-9x^5+7x^4+4x^3-12x^2\qquad +5 \\
\underline{-9x^5-27x^4\qquad\qquad -36x\qquad\quad} \\
34x^4+4x^3-12x^2+36x+5 \\
\underline{34x^4+102x^3+\qquad\quad 136} \\
-98x^3-12x^2+36x-131
\end{array}
$$

If a polynomial is divisible only by itself and constants, then we call this polynomial an **irreducible polynomial.** We will see later that irreducible polynomials have properties similar to prime numbers.

If the coefficients are taken from a field *F*, then we say it is a **polynomial over F.** With polynomials over field *GF*(*p*), you can add and multiply polynomials just like you have always done but the coefficients need to be reduced modulo *p*. For example, compare the above results with polynomials over *GF*(11):

- $(x^5 + 3x^3 + 4)+(6x^6 + 4x^3) = 6x^6 + x^5 + 7x^3 + 4$
- $(x^5 + 3x^3 + 4)-(6x^6 + 4x^3) = 5x^6 + x^5 + 10x^3 + 4$
- $(x^5 + 3x^3 + 4)*(6x^6 + 4x^3) = 6x^{11} + 7x^9 + 4x^8 + 3x^6 + 5x^3$
- $(3x^6 + 7x^4 + 4x^3 + 5) \div (x^4 + 3x^3 + 4) = 3x^2 + 3x + 3$ with remainder $x^3 + 10x^2 + 4x + 1$

Similar to integers, you can do modular arithmetic with polynomials over a field. Now the operands and modulus are polynomials. Let $f(x)= a_n x^n + a_{n-1}x^{n-1} + ... + a_0$ and $g(x)= b_m x^m + b_{m-1}x^{m-1} + ... + b_0$ be two polynomials over a field *F*, then there is a unique polynomial $r(x)$ of degree smaller than m and another unique polynomial $h(x)$, both over *F*, such that $f(x) = h(x)*g(x)+r(x)$. The polynomial $r(x)$ is called the remainder of $f(x)$ modulo $g(x)$. For polynomials $a(x)$, $b(x)$ and $g(x)$ which are over the same field, we say $a(x)$ is congruent to $b(x)$ modulo $g(x)$ written $a(x) \equiv b(x) \bmod g(x)$, if $m(x)$ divides $a(x)-b(x)$. For example (all polynomials are over *GF*(3)):

- $2x^2 \equiv 2 \bmod (x^2-1)$
- $x^4 \equiv 1 \bmod (x^2-1)$
- $x^3 \equiv x \bmod (x^2-1)$

- $2x^2+x^4 \equiv 0 \bmod (x^2-1)$
- $2x^2*x^4 \equiv 2 \bmod (x^2-1)$
- $2x^2+x^3 \equiv x+2 \bmod (x^2-1)$

Always remember there are two moduli involved: a polynomial modulus and an integer modulus. You need to reduce the result from the polynomial operations by modulo the polynomial modulus and then reduce the coefficients modulo the integer modulus. Take one of the above examples: $2x^2+x^4 = x^4+2x^2$, you reduce this result by dividing by x^2-1:

$$
\begin{array}{r}
x^2+3 \\
x^2-1 \overline{)\ x^4+2x^2} \\
\underline{x^4-x^2} \\
3x^2 \\
\underline{3x^2-3} \\
3
\end{array}
$$

The remainder 3 is then reduced modulo 3: $3 \equiv 0 \bmod 3$. So the final result is $2x^2+x^4 \equiv 0 \bmod (x^2-1)$.

Useful Links

- Polynomial Calculator
- Long Division of Polynomials
- Long Multiplication of Polynomials

Prev
Chapter 4. Finite Fields

Up
Home

Next
$GF(p^m)$