Chapter 3: Polynomials

Chapter Contents.

• It is noted that polynomials are always defined with respect to some field F.

• This field has two operations + and •. The pseudo-operation - (minus) is defined.

• It is noted that, for a given field, a polynomial of degree m has *not more than* m roots. The number of roots usually depends on what field is used.

• The set of polynomials over a field F forms a commutative ring.

• The notion of dividing polynomials to get a quotient and remainder is discussed. The remainder has degree less than that of the divisor polynomial. The reader is reminded how to do division.

• A polynomial can usually be factored into a product of polynomials of lesser degree. When this is not the case, the polynomial is called *irreducible*.

• A pair of polynomials has some greatest common divisor polynomial which can be expressed according to the Euclidean Division Algorithm as a linear combination of those polynomials, with polynomials as the two coefficients.

• An elaborate construction then takes place. An ideal is formed inside the polynomial ring by selecting some polynomial f(x) of order m and by taking as that ideal all multiples of f(x) with zero remainder. This ideal then forms the top row of a "chart" which partitions the polynomial ring into rows of polynomials , where each row is characterized by some particular remainder polynomial. The rows are then abstracted and are considered to be elements of a ring called the residue class ring, and denoted by Poly[x,F]/ (f(x),m), where F is the field over which the polynomials are defined.

• If the field F = GF(p), then the chart has p^m rows, there are p^m possible remainders, and the residue class ring has p^m elements.

• If f(x) is irreducible, then the residue class ring is itself a field. This larger field is called an *extension field* of the original *ground field* over which the polynomials were defined

• Since the only finite fields are the Galois fields GF(q), the fancy residue class ring field must in fact be equivalent to GF(p^m). We then write,

$$GF(p^m) = \text{Poly}[x,GF(p)]/ (f(x),m, \text{irreducible})$$

• A comparison is made between Chapter 1 and Chapter 3

Chapter 3: Polynomials

A Polynomial has an implied Field F, and Roots

When one speaks of a polynomial like $f(x) = a + b \bullet x + c \bullet x^2$, one usually thinks of x and the coefficients a,b,c as lying in the field of real numbers, or perhaps in the field of complex numbers. In this case, the operations + and • are those we are used to. Also, the meaning of x^2 is $x \bullet x$.

In general, one can define a polynomial with respect to an arbitrary field F. In this case, the coefficients and x both lie in the field F, and the operations + and • are those of field F.

We shall be particularly interested in studying the case where the field F is GF(p). We know all about the fields GF(p) from the last chapter.

When F is the complex numbers, we know an interesting fact. A polynomial of degree n has n roots, and you can write the polynomial as a product of factors.

$$f(x, \text{degree } n) = (x - a_1) \bullet (x - a_2) \bullet (x - a_3) \ldots\ldots (x - a_n)$$

The roots a_i are the complex numbers that make $f(x) = 0$. It may be that some of the roots are the same.

By the way, the symbol minus "-" has just appeared for the first time. This refers to addition (field operation +) of the additive inverse of a field element. Minus is not some new operation. In other words,

$a - b$ *means* $a + (-b)$ where $(-b)$ is the field element which satisfies $b + (-b) = 0$.

When F is the real numbers, it is no longer true that a polynomial of degree n has n roots. In this case, we know only that the polynomial f(x) of degree n has *at most* n roots, but it might have less. Remember that the roots have to lie in the field you are talking about.

Example: $f(x) = 1 + x^2$

(a) For F = complex numbers, we can factor this as $f(x) = (x - i) \bullet (x+i)$, and we have two roots, $\pm i$.

(b) For F = reals, we cannot factor f(x), it has no roots.

(c) For F = GF(2), the world of a binary bit, again we can factor the polynomial. But the result is a little unnerving to the uninitiated:

$$f(x) = 1 + x^2 = (1-x) \bullet (1-x) = (1-x)^2$$

There are two roots, they are both 1. The cross terms -2x = 2x = 0 according to our general rule that px = 0 for elements in GF(p).

The moral here is that one must keep carefully in mind what field F one is dealing with.

Polynomials form a Commutative Ring

Consider the set of all polynomials over some field F. We certainly know how to add and multiply polynomials, because we know the + and • operations of the field F. We have an identity for operation • : it is the polynomial f(x) = 1, where 1 is the • identity of field F. However, we are definitely lacking inverses for most polynomials, such as $f(x) = 1 + x^2$. Thus, our set of polynomials does not itself form a *field* over the field F. It forms a commutative *ring* over the field F. It is commutative because • is commutative because it goes with a field.

Notice that the + and • operations of this "ring of polynomials" derive from the + and • operations of the underlying field in which x and the polynomial coefficients lie.

Basic facts about a polynomial ring over a field F

Here we mimic the corresponding section of Chapter 1.

1. **Division Algorithm**. Relative to a divisor polynomial d(x), a polynomial n(x) has a unique quotient polynomial q(x), and a remainder polynomial r(x):

$n(x)/d(x) = q(x) + r(x)/d(x)$ "Rem(n(x)/d(x)) = r(x)"

$n(x) = q(x) \bullet d(x) + r(x)$

The remainder polynomial r(x) has degree less than the divisor polynomial d(x).

As an example, let's work in the field GF(2), and let $n(x) = 1 + x^2 + x^5$, and let d(x) = 1+x. It is perhaps useful to remind calculator-era readers how long division works. Recall that in GF(2), the symbols + and - have the same meaning.

$$
\begin{array}{rl}
 & x^4 + x^3 + x^2 \\
\cline{2-2}
x + 1 \;\big|\; & x^5 + x^2 + 1 \\
 & \underline{x^5 + x^4} \\
 & \quad x^4 + x^2 + 1 \\
 & \quad \underline{x^4 + x^3} \\
 & \quad\quad x^3 + x^2 + 1 \\
 & \quad\quad \underline{x^3 + x^2} \\
 & \quad\quad\quad 1
\end{array}
$$

So the idea is to put largest powers first in both divisor and dividend, then turn the crank. So here is our result:

$$(1 + x^2 + x^5)/(1 + x) = (x^2 + x^3 + x^4) \quad + \quad (1)/(1+x)$$

which can also be expressed in the other forms:

$$(1 + x^2 + x^5) = (x^2 + x^3 + x^4)\bullet(1+x) + (1) \qquad \text{Rem}[\ \frac{1 + x^2 + x^5}{1+x}\ ] = r(x) = 1$$

Fact: Here is a useful observation about working in GF(p). Suppose the divisor d(x) is a polynomial of degree m. We know that all remainders must have degree less than this. How many possible remainders are there? There are m coefficients in the remainder, and each coefficient must take one of the p values in the field GF(p). Thus, there are p^m possible remainders of degree m-1 or less, where we have included the possibility that all coefficients are 0.

Definition: A polynomial with coefficients in a field F is *irreducible with respect to F* if it cannot be factored into a non-trivial product of polynomials, each of which has coefficients in F. A trivial product would be one in which one of the factors was an element of F, such as 1. An irreducible polynomial is to polynomials as a prime number is to integers.

2. **Factorization Theorem**. Any polynomial can be uniquely decomposed into a product of factors where each factor is an irreducible polynomial raised to an integer power:

$$f(x) \quad = \quad [p_1(x)\ ]^{m_1} \bullet [p_2(x)]^{m_2} \bullet [p_3(x)]^{m_3} \quad ...$$

3. **Euclidean Division Algorithm**. Every pair of polynomials $n_1(x)$ and $n_2(x)$ has some largest common divisor polynomial. You can write this divisor as a unique linear combination of the two polynomials, where the coefficients are again polynomials:

$$d(x) = a(x)\bullet(n_1(x)) \ - b(x)\bullet(n_2(x))$$

There is a mechanical procedure for finding d, a, b once you are given n_1, and n_2. See Rhee, *Error Correcting Coding Theory*, page 25. Basically, it is the same algorithm used for the integer analog.

If $n_1(x)$ is an irreducible polynomial, and $n_2(x)$ is known not to be a multiple of $n_1(x)$, then the largest common divisor must be d(x) = 1.

The Residue Class Decomposition.

Now we are going to exactly repeat the discussion of Chapter 1 about decomposing a ring based on some ideal of the ring. First, we have to find a candidate ideal. We know from the integer ring case that you could make an ideal by taking all multiples of some integer N. In the polynomial case, you can form an ideal within the ring of polynomials by considering all polynomials which are multiples of some

specified polynomial. Let's call the specified one f(x). And let's denote by (f(x)) the set of all polynomials which are multiples of f.

There is nothing mysterious about this. If F(x) is a multiple of f(x), it just means that when you factor F(x) until you can factor no more (as in item 2 above), then you will find f(x) is one of the factors. This is trivial, but the point should not be missed. For example, if field = reals, we have

$(x^2 - 1) = (x + 1)\bullet(x - 1)$ so $(x^2 - 1)$ is a "multiple" of either $(x + 1)$ or $(x - 1)$

So we have come up with an ideal I of the ring R of polynomials over field F. The ideal consists of only those polynomials in R which are multiples of f(x).

So now we make the chart, just as before. Here is our Chapter 1 chart for general ring R and ideal I:

$i_1=0$	i_2	i_3	i_4	...	i_n
r_1	$r_1+ i_2$	$r_1+ i_3$	$r_1+ i_4$	...	$r_1+ i_n$
r_2	$r_2+ i_2$	$r_2+ i_3$	$r_2+ i_4$	...	$r_2+ i_n$
more rows like the above					

We now apply this to our polynomial situation

$i_1(x)=0$	$i_2(x) = q(x)\bullet f(x)$ for all possible q(x)
$r_1(x)$	$r_1(x)+ i_2(x) = q(x)\bullet f(x) + r_1(x)$, for all possible q(x)
$r_2(x)$	$r_2(x)+ i_2(x) = q(x)\bullet f(x) + r_2(x)$, for all possible q(x)
more rows like the above	

First look at the top row, which is the ideal. We separate out the function 0 and put it first. Then, instead of trying to list off specific elements of the ideal going to the right, we instead write this list by saying that the polynomial q(x) can be any polynomial in R. As q(x) takes on all possible polynomials, we get our list. It is of course infinite.

Now look at the next row. We pick some $r_1(x)$ from the ring R of polynomials and plop it down in the left column, then we form the row as instructed by the previous prototype chart. Now suddenly one sees an interesting coincidence of the notation. The polynomials $r_i(x)$ which are the residue class (row) leaders, look like "remainder" polynomials, and the q(x) notation suggests "quotient" polynomials. In fact, all polynomials in the second row list have $r_1(x)$ as their remainder when they are divided by f(x), and q(x) is in fact the quotient. There are as many polynomials in the second row as there are quotient polynomialsq(x). This number is of course infinite.

Suppose in the left column you pick a remainder function from R which has degree larger than the degree of f(x). This just means that you have a "repeat row", and it is repeating some other row which has the correct "proper" remainder function that has degree less than f(x). The row is a repeater, because you can absorb the improper remainder into q(x) and this make it some q'(x), which is just some other item in the same row.

This same idea occurred in the integer ring example. We did not include the row {6} there, for example, because it was a repeat of the row {1}.

So here is the general idea of the above chart. Across the top you have the ideal which is the set of all polys which are multiples of f(x) with *no* remainder. Then each row is represented by some possible remainder (of degree less than that of f(x)) you could get by dividing f(x) into elements of the poly ring.

How many rows are there? If the underlying field is the reals, say, then of course there are an infinite number of possible remainders. However, if the field is GF(p), then we already know from the previous section that there are only p^m possible remainders (including the zero remainder), if the degree of f(x) is m.

We are now rapidly closing on the target of all our efforts. Admittedly, it has taken a while.

We considered the ring of polynomials over a field F, and we considered an ideal consisting of all polynomials which were multiples of some selected polynomial f(x). We then used this ideal to construct the "chart" which partitions the ring into rows of polynomials, the residue classes. There is one row for each possible remainder polynomial, and the polynomials in a row are "indexed" by the quotient polynomial. The number of rows equals the number of possible remainder polynomials , and the first row corresponds to remainder 0.

In the special case that the field of the polynomials is GF(p), we know that there are p^m rows, if the degree of f(x) is m.

We know from Chapter 1 that these rows can be considered elements of a new ring known as the residue class ring. We indicated this new ring by the notation R/I. Here, we might use this notation:

residue class ring = Polys[x, F]/ (f(x)) (R = polys over field F)/(I = multiples of f(x))

So, if F = GF(p), and if f(x) is a poly of degree m, then the residue class ring has p^m elements.

Here then comes the *coupe de grace*, which lets us conclude this chapter the same way we concluded Chapter 1.

Theorem: If a polynomial f(x) is *irreducible* over F, then the residue class ring Polys[x, F] / (f(x)) is a *field*.

Proof: It goes exactly the same was as at the end of Chapter 1. We have to show that for some {r(x)} we can find an inverse {s(x)} such that {r(x)}• {s(x)} = {1}. We can mimic every statement of the previous proof, except we replace n with f(x), the divisor polynomial here. Thus, using The Euclidean Divisor

Algorithm, we note that since f(x) is irreducible and r(x) has smaller degree than f(x), we know they cannot be multiples, so their largest common divisor is 1. We expand this as

$$1 = N(x)r(x) - M(x)f(x) \qquad \text{which says } \text{Rem}[\frac{N(x)r(x)}{f(x)}] = 1$$

We expand N(x)r(x) = K(x)f(x) + s(x), where s(x) has degree less than f(x). This then yields:

$$\text{Rem}[\frac{r(x)s(x)}{f(x)}] = 1 \qquad \text{which implies that } r(x) \bullet s(x) = 1 \text{ and hence } \{r(x)\} \bullet \{s(x)\} = \{1\}.$$

Thus, if f(x) is irreducible, then the residue class ring Polys[x,GF(p)] / (f(x)) is a field.

Implication: Find some irreducible polynomial f(x) of degree m defined on the field GF(p). Then the residue class ring Polys[x, GF(p)] / (f(x)) is a field with p^m elements. But from Chapter 1 we know that all finite fields must be equivalent to the Galois Fields, so we have explicity constructed GF(p^m)!

The field F in the above discussion is sometimes called the *base field* or the *ground field*, and the residue class ring field is then called the *extension field*. We have now a method whereby we start with a ground field that we know about, namely GF(p), and we construct a pile of new extension fields GF(p^m), where m = any integer. From our construction, we should be able to learn everything about GF(p^m) and therefore everything about any finite field.

Comparison Between Chapter 3 and Chapter 1.

In Chapter 1 we considered the residue class ring Z/ (p) for p = prime and showed it was a field having p elements. This got us used to working with a residue class ring . We knew all along that this field was equivalent to Z_p , the modulo-p field, so we did not really need Z/ (p) , it was just practice.

In Z/(p) the ring Z was integers. We partitioned up the integers into rows, where the integers in each row had something in common: some remainder r < p when divided by p.

In Chapter 3, we really need the residue class ring. We need something with p^m elements, and we realize that a polynomial f(x) of degree m defined over GF(p) has exactly p^m remainders. This suggests that instead of using Z the ring of integers, we use Polys[x,GF(p)], the ring of polynomials over the field GF(p). Then the divisor must be an irreducible polynomial of degree m, so we end up with this final result:

$$GF(p^m) = \text{Polys}[x,GF(p)] \ / \ (f(x),m)$$

Obviously, there are p remainders which are constants independent of x. These remainders are just elements of GF(p). One can consider these remainders to be generating GF(p) as a subfield of GF(p^m). So GF(p) is the ground field, and GF(p^m) is the extension field, something that is constructed at a higher level over the ground field. Here we see that "over the ground field" means that the polynomials have coefficients in the ground field GF(p).