Chapter Contents.

• Definition of group, ring, and field.

• Definition of the Galois Fields GF(q)

• The binary world is the simplest such field, GF(2)

GROUP SECTION

• Subgroups, cosets, coset decomposition chart, and normal subgroups.

• The Factor Group G/H formed from a group G and a subgroup H.

• Cyclic groups and cyclic subgroups; order n means $g^n = 1$.

• Generator of a cyclic group; if order n=prime, all elements except the identity are generators.

• The order of any cyclic subgroup must divide the size of the group evenly.

• Additive cyclic groups; summary of their properties

• Example of an additive cyclic group: { Mod-n,+}

RING SECTION

• Ideals, residue classes, residue class decomposition chart.

• The Residue Class Ring R/I formed from a ring R and an ideal I.

• Principle Ideals, and Principle Ideal Rings.

• A Principle Ideal forms an additive cyclic group

• The size of any principle ideal of a ring must divide the size of the ring evenly.

• Important example of a ring: Z_n = {Mod-n,+,•}

• Important example of a Residue Class Ring: Z/ (n)

• The ring Z/ (n) is the same as the ring Z_n

• Some basic facts about the integer ring Z:

1) Division Algorithm
2) Factorization Theorem
3) Euclidean Division Algorithm

4) definition of relatively prime

• If n = prime, the modulo-n residue class ring Z/(n) and Z_n forms a *field*.

Chapter 1: Modern Algebra

Chapter 1: Modern Algebra **3**
Groups, Rings and Fields. 3
Subgroups, cosets , coset leaders, coset decomposition, N/n = m, normal subgroups. 4
The Factor Group G/H formed from a group G and a subgroup H. 5
Cyclic Groups and Cyclic Subgroups. 6
Additive Cyclic Groups 7
Ideals, residue classes , residue class leaders, residue class decomposition, N/n = m. 8
Residue Class Ring of R with respect to ideal I 9
Principle Ideals, and Principle Ideal Rings. 10
Important Example of a ring: Z_n = {Mod-n,+,•} 10
Important Example of a Residue Class Ring: Z / (n) 12
Basic facts about the integer ring Z. 13
Residue Class Ring Z/(n) is a field if n is prime. 14

Chapter 1: Modern Algebra

The purpose of this chapter is to point out and give recognizable names to some of the animals which inhabit the landscape of modern algebra. We do so in a non-rigorous manner, because we want to get done as fast as possible. We try to include only those ideas that are necessary for our development to come in later chapters. Not everything is proved, because the proofs all exist in standard texts. We are more interested in showing how things are *defined* and how they fit together.

Groups, Rings and Fields.

A *field* is a heavy duty algebraic entity. It is hard to be a field. A field has all kinds of properties. A field F is a set of N elements, and two operations called + and • such that:

Closed under	Associative	Identity exists	Inverses exists	Commutative
+	(a+b)+c=a+(b+c)	0	x + (-x) = 0	a+b = b+a
•	(a•b)•c=a•(b•c)	1	x• (x^{-1}) = 1	a•b = b•a
	a•(b+c) = a•b + a•c (distributive property)			

Closed under some operation means that if you apply the operation to two elements in some set, the result is also in that set. Either of the first lines above defines a (commutative) *group* with respect to its single operation. The number of elements in a group is called its *order*. We might denote each of these groups as follows (F stands for the elements of the field F):

{ F, +} order N {F - 0, •} order N-1

Notice that for the multiplicative group, we have to exclude the 0 element since it has no inverse, so this group is one smaller than the additive group. One often speaks of the "non-zero elements" of a field when talking about the • operation.

All three lines above define a commutative *ring* if you knock out items " • identity exists" and "• inverses exist". If you add these two back in, you get a *field*. Thus, a field must have an identity relative to •, and every element (except element 0) must have an inverse relative to •.

Note that rings and fields have two operations + and •. A group has only one operation.

In general, a group may or may not be commutative with respect to its operation. Similarly, a ring may or may not be commutative with respect to •, but it is always commutative with respect to +. A field requires that both operations be commutative.

Another word for commutative is *abelian*.

Infinite Fields: The are several *infinite* fields we are extremely familiar with: the complex numbers, the real numbers. The integers are only a ring because, for example, the inverse of 5 is 1/5th which is not an integer. For these fields, + and • are what we are used to.

Galois Fields: There are many *finite* fields as well. For any prime number p (p = 2,3,5,7,11,...), and for any integer m (m = 1,2,3....) , there exists a finite field which contains p^m elements. These finite fields are given the name GF(p^m), where GF = Galois Field in honor of the frustrated Frenchman Mr. Evariste

Galois, who died in a duel in 1832 at age 20, after writing down much of what he knew about math the night before. Apparantly, his math was better than his shooting.

These are the only finite fields there are. Any finite field you come up with is equivalant to one of the Galois Fields. In general, the meaning of operations + and • for the elements of Galois fields is *not* what we are used to. Much more on this subject in later chapters.

The Binary World: We shall generally be interested in Galois Fields in which p = 2, so this means GF(2^m). In the special case m=1, we get GF(2). This field has only two elements, so they must be 0 and 1 (see properties list above). Here are the + and • tables for GF(2):

+	0	1
0	0	1
1	1	0

•	0	1
0	0	0
1	0	1

The field GF(2) is the lonely world of a binary digit -- a bit. Notice that addition is XOR, while multiplication is the normal thing.

GROUP SECTION

Subgroups, cosets , coset leaders, coset decomposition, N/n = m, normal subgroups.

Consider a group G with N elements and some operation *. Later on, we may identify * with either + or •, depending on our context. In the + case, the term "product of group elements" a*b of course means the sum of group elements a+b.

Suppose G has a *subgroup* H of n elements. Obviously, H has to contain the identity 1 if it is really a sub-group -- a group within a group. [Again, if * = +, identity is called 0, since a+0 = a.]

It turns out that N/n = m, an integer. That is to say, the order of any subgroup divides evenly into the order of the group. The reason for this is the following. You can arrange the group elements into a little chart where the top row contains the subgroup elements h_i. Then you randomly pick some other group elements and put them into the leftmost column under 1, and you then form a multiplication table like so:

h_1=1	h_2	h_3	h_4	...	h_n
g_1	g_1*h_2	g_1*h_3	g_1*h_4	...	g_1*h_n
g_2	g_2*h_2	g_2*h_3	g_2*h_4	...	g_2*h_n
more rows like the above					

If you pick the g's for the left column clumsily, you end up with some repeat rows. It is possible to pick them so that all rows are different. In this case, it turns out (but we are not proving it here) that every

group element appears exactly once somewhere in the chart. Since the chart has N elements, and a row has n elements, this is why N/n must be an integer m. The rows of the chart care called *cosets*, and the first item in each row is called the *coset leader*. for that coset. The cosets partition the group G.

Since we only care about groups in which a*b = b*a, it does not matter on which side you write the h's in the little products. This means g*h = h*g, which you can rewrite as $g^{-1}*h*g = h$. Thus, $g^{-1}*H*g = H$. This last thing means that if you sandwich g^{-1} and g around any element of H, you get an element of H. When this is true, as in our case where things are commuative, the subgroup is called a *normal subgroup*, or *invariant subgroup*.

The Factor Group G/H formed from a group G and a subgroup H.

Suppose you have a G and a H as shown above, and you have your group elements put into a chart by the coset decomposition above. Since a*b = b*a for our group, we know that H must be a normal subgroup. We also know that N/n = m, an integer.

It is possible now to define a new group which has m elements. These elements are the rows of the chart! Although each row contains more than one element of group G, you think of the entire row as one element of the new group we are talking about. A standard notation is to label each row by some representative element, like the coset leader, and put this in curly brackets. Thus, the top row of the chart is our first group element which is {1}, and the next row is $\{g_1\}$ and so on.

Now we have to define what it means to "multiply" two rows of the chart. We write

$\{g_1\} * \{g_2\} = \{g_3\}$, where $g_3 = g_1 * g_2$

What does this mean? Suppose each row has n elements. Suppose you create all the products possible by multiplying some element of row 1 by some element of row 2. There are n^2 of these products. The claim is that all of these products will lie in the same row of the chart, which we have called row 3. Obviously, many of these products must be the same, since row 3 only contains n elements.

The general idea is that you can represent a row by any of its elements. All the elements of a row have something in common. Notice that the operation* in our new group , whose elements are the rows, is defined in terms of what * does to elements of the underlying group G.

Do the m rows $\{g_i\}$ really form a group with m elements? Yes, but we are not proving it, just claiming that it is true. Thus, for example, for any row $\{g_1\}$, there must be an inverse row $\{g_2\}$ such that

$\{g_1\} * \{g_2\} = \{$identity row $\}$ [identity row is {1} for •, and is {0} for +]

Since H is a subgroup, the inverse of the top row must be the top row: {1}•{1} = {1}.

This new group whose elements are the rows or cosets of the group G with respect to the normal subgroup H has a special name and notation. It is called the *factor group* of G with respect ot H, and the notation for this new group is G/H. This is just a notation, we are not trying to divide group G by group H.

factor group = G/H has m = (N/n) elements, the rows (cosets) of the chart.

It is certainly not obvious why anybody in their right mind would have any interest in such a curiosity as this "factor group".

Cyclic Groups and Cyclic Subgroups.

If g is in an element of group G, then so is g*g = g^2, and g*g*g = g^3 , and so on. If the group has a finite number N of elements, you must, as you keep increasing this power, come to a point where $g^n = 1$. After this point, if you keep raising the power, things just repeat: for example, $g^{n+1} = g$, and so on.

If you find that you have exhausted all the elements of the group in this way, then it must be that n = N. In this case, G is called a *cyclic group*. The other possibility is that you reach the point $g^n = 1$ *before* all group elements have been hit. In this case, you have found a *cyclic subgroup* of the group. Of course this may happen when n = 2, so the cyclic subgroup can be as small as 2 elements, 1 and g. Thus,

Fact: Any group element g of any group G must be in *some* cyclic subgroup of G by the above construction.

Fact: The order of any cyclic subgroup of a group must divide evenly into the order of the group.

Proof: We already know from the coset decomposition that the order of *any* subgroup H of a group G must divide evenly into the order of G, so saying this for a cyclic subgroup is nothing new.

Here is what a cyclic group looks like:

$\{ 1, g, g^2, g^3, ...g^{n-1}\}$ = cyclic group, order = n elements, $g^n = 1$

Notice that every element of the group can be written as a power of g, for power = 0,1,2....n-1.

Definition: An element g which allows a cyclic group to be fully enumerated as above is called a *generator*. In general, not every group element can serve as a generator. Certainly not the identity. There may exist several *alternative generators* of the same cyclic group.

Fact: If g is a generator of a cyclic group of order n, then $g_1 + g^m$ (with 1<m<n) is the generator of a cyclic subgroup of order N = n/GCD(n,m).

Proof: This will be proven as Fact 6 in Chapter 4, where cyclic subgroups of GF(q) are explored in great detail. For now, we state some Corollaries to the above Fact, and then prove one of them.

Corollary 1: Element $g_1 = g^m$ is an alternative generator to g if n is prime. Even if n is not prime, this can still happen whenever n and m are "relatively prime", that is, when GCD(n,m) = 1.

Corollary 2: All elements (except 1) of a cyclic group of prime order n are alternative generators. This is a direct result of Corollary 1.

Corollary 3: If n/m = k, then $g_1 = g^m$ is *not* an alternative generator to g. In this case, g_1 generates a smaller cyclic subgroup of order n/GCD(n,m) = n/m = k.

Proof of Corollary 3: Let n/m = k, an integer. Since m>1, k < n. If you try to list off the group elements using g^m as a generator, you get $\{1, g^m, g^{2m}, g^{3m} \ldots g^{(k-1)m}\}$. Then next element in the list would be g^{km} but $g^{km} = g^n = 1$. The next element would then be $g^{(k+1)m} = g^m$, so you would then just repeat things. You know that the cyclic group has n elements, but you have only been able to enumerate k of them, and k < n.

Example: let n = 12, m = 3, and k = n/m = 4. Then here is our partial enumeration:

$\{ 1, g^3, g^6, g^9 \}$ $\quad g^{12} = 1$ only get 4 elements out of the 12.

Additive Cyclic Groups

We now want to take a closer look at a cylic group in the case that * = +. In this case, the term "powers of g" means "multiples of g", since for example $\mathbf{g^3} = \mathbf{g*g*g} = \mathbf{g+g+g} = 3\mathbf{g}$.

The notation "3**g**" means just the sum shown. The thing "3" is not in the group. The 3 is a scalar multiple of the ring element **r**. It happens that the scalar in question, 3, is a member of the field of integers.

If you go look at the definition of a "vector space over a field F", you will see that additive group elements form a vector space over the field of integers. This just means that the only scalars you are allowed to have are integers, and the "vectors" are the group elements. So we might consider putting group elements in bold, to show they are vectors, and then put any scalar integers in non-bold (as above).

Recall that, for any cyclic group, $\mathbf{g^n} = 1$, where 1 is the identity of the group, and n is the order of the cyclic group, ie, the number of elements. For an additive cyclic group, this statement becomes $n\mathbf{g} = \mathbf{0}$, since the nth power of g is n**g**, and since **0** is the identify for + .

Thus, we can enumerate the elements of an additive cyclic group as follows:

$\{ \mathbf{0}, \mathbf{g}, 2\mathbf{g}, 3\mathbf{g}, \ldots.(n-1)\mathbf{g}\}$ = cyclic group, order = n elements, $n\mathbf{g} = \mathbf{0}$

Fact: If the order n of an additive cyclic group is a *prime number*, then any element (other than 0) can serve as the generator. Thus, if n is prime, we could take **h** = 3**g** and enumerate the above as,

$\{ \mathbf{0}, \mathbf{h}, 2\mathbf{h}, 3\mathbf{h}, \ldots.(n-1)\mathbf{h}\}$ = cyclic group, order = n elements, $n\mathbf{h} = \mathbf{0}$

Proof: This is just a special case of our general result on cyclic groups of prime order presented earlier.

Summary of the properties of an additive cyclic group of order n:

1) the identity element is **0**
2) every element must have have an inverse such that $\mathbf{g} + \mathbf{(-g)} = \mathbf{0}$.
3) the group can be enumerated as $\{ \mathbf{0}, \mathbf{g}, 2\mathbf{g}, 3\mathbf{g}, \ldots.(n-1)\mathbf{g} \}$ for at least one g.
4) g is by definition a generator
5) $n\mathbf{g} = \mathbf{0}$ for this generator g
6) if n is prime, then all non-zero group elements are generators.
7) if n is prime, then $n\mathbf{a} = \mathbf{0}$ for any non-zero **a** in the group.

Example of an additive cyclic group: {Mod-n,+}

The "mod-n additive group" has as its elements {**0**,**1**,**2**,**3**,..**n-1**}, and the + operation is mod-n addition, which is to say,

a + **b** = Rem[(a+b)/n] **1**.

Here is a list of observations about mod-n:

1) there is no element **n**.
2) the identity element is **0**.
3) the group is cyclic with**1** as a generator, and n**1** = **0**
4) all non-zero elements can be written as multiples of the generator,**m** = m**1**.
5) the inverse of element **m** is **(-m)** = (n-m)**1.** Thus, **m** + **(-m)** = m**1** + (n-m)**1** = n**1** = **0**.
6) if n is prime, then any element **m** (other than **0**) is a generator, and n**m** = **0**.
7) mod-n forms a principle ideal within the integers (see below)

The reason the group is cyclic is that the elements can be written as **m** = m**1**, that is, all elements of this additive group are multiples of the generator **1**. As will become clearer below, mod-n is an ideal within the ring of integers, since a**m** = **m**a = b yields an integer, and because mod-m consists of multiples of an integer.

RING SECTION

Ideals, residue classes , residue class leaders, residue class decomposition, N/n = m.

We are now going to repeat the above song and dance almost verbatim, but this time for a *ring* instead of a *group*. A ring has two operations • and +, whereas a group has only one operation, so things will be just a little different. We started the above harangue by imagining that group G had a subgroup H. Here we might suppose that a ring R has a subring. But this turns out to be not the right thing, the correct sub-thing is called an *ideal*, and one uses the letter I.

So what is an *ideal* I of *ring* R? With respect to the + operation, I is a subgroup of R. Thus, I must contain the additive identity, which we normally call 0. With respect to the • operation, I does this: r•I = I•r = I. This means that if you pick any r in R, and any i in I, the product r•i lies somewhere in I, and so does the other product i•r. In particular, we have i•I = I, so I is closed under • as well as +. So an ideal is in fact a subring of R, but it is more general since r•I = I even for r not in I.

So let R have N elements, and assume there is an I with n elements. As before, we are going to build a chart, and we will then claim that N/n = m = an integer.

As before, we lay down I itself as the top row. Since we are really thinking about the + operation now, the top left element is the + identity 0 (the thing you put in r + 0 = r). We next start picking random elements of R and plop them down in the left column, then we form rows by doing sums of the left element with the things along the top. Here is the new chart for ring R with respect to 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	etc

Again, we make the claim that if you pick the left elements right and get things so that you throw out any repeating rows, you end up with a coset decomposition that partitions the ring. Each ring element appears exactly one place in the chart. Thus, as before, we conclude that N/n = m, and integer.

Because mathmaticians cannot leave well enough alone, they decided that they had to invent a new name for everything since we are doing rings instead of groups. Thus, what was called a coset before is now called a *residue class*. A residue class is a row of the chart. And the first item in a row is now the *residue class leader*. Big deal.

Residue Class Ring of R with respect to ideal I

Before, our next step was to claim that you could make a fancy new group by considering each row of the chart to be an element of that new group. This was the factor group of G with respect to H. Here we are going to do the same thing, but as you might expect, the new "thing" which has the rows as elements is going to be a ring, not a group, since R is a ring. Thus, admittedly, we cannot call this thing a factor group. So they make a new name. This new ring with m elements being the rows of the above chart is called the *residue class ring*, or the *quotient ring* To be consistent, they should have called other thing a *coset group,* but they called it a factor group instead. The notation is pretty much the same:

residue class ring = R/I has m = (N/n) elements, the rows (residue classes) of the chart.

As before, we now have to say what it means to do the + and • operations on a "row" of the chart. Now we have two operations to worry about instead of one. Here we go:

$\{r_1\} \bullet \{r_2\} = \{r_3\}$, where $r_3 = r_1 \bullet r_2$
$\{r_1\} + \{r_2\} = \{r_4\}$, where $r_4 = r_1 + r_2$

Again, $\{r_2\}$ is an element of the new "residue class ring", and r_2 is some representative element of the row of the chart which this element refers to. We need then to make exactly the same interpretation as before for what the above lines mean, only here we say the same thing for each operator + and •.

For example, if you form all products between elements of two rows, the results all lie in the same row. And the same applies if you make all possible sums. Of course the results row might not be the same row, so we have used r_3 and r_4 above.

You may remember that a ring does not in general have a 1 element, but it always has a 0 element. Thus, every row $\{r_1\}$ must have some corresponding "negative" row $\{r_2\}$ such that

$\{r_1\} + \{r_2\} = \{0\}$

And as before, since our ideal I is a subgroup of R relative to +, we know that the negative of the top row is itself. This is expressed by the incredibly boring statement: {0} + {0} = {0 }. Since we might not have a {1} row, we have nothing to say about {1}. (yet)

Principle Ideals, and Principle Ideal Rings.

Now we are ready to pursue the ring analog of the cyclic subgroup discussion above.

If **i** is in an element of ring R, then so is any multiple of **i**, such as 3**i**. If the ring has a finite number n of elements, you must, as you keep adding more terms, come to a point where n**i**= **0**. After this point, if you keep adding **i**, things just repeat, for example, (n+1)**i**= **i**.

This set of multiples of some ring element **i** together with **0** forms an additive cyclic group of order n, as discussed in much detail above. We have,

{ 0, **i**, 2**i**, 3**i**, ...(n-1)**i**} = additive cyclic group of order n

If you find that you have exhausted all the elements of the ring in this way, then it must be that n = the size of the ring. The other possibility is that you reach the point n**i**= 0 *before* all ring elements have been hit. In this case, you have found an additive *cyclic subgroup* of the ring of order n

In the case of rings, we are more interested in ideals than we are in subgroups. The above subgroup may or may not be an ideal of R. Remember than for an ideal, it must be true that r•I = I•r = I for elements r that are outside the ideal as well as inside. The above enumeration and the fact that it forms an additive cyclic subgroup within R does not make it an ideal.

If it is not an ideal, then we have nothing more to say. If the subgroup is an ideal, then it is called a *principle ideal*. Thus, a principle ideal is one in which all members of the ideal are multiples of one element. We can restate what we have just said as:

Fact: A principle ideal of size n within a ring forms an additive cyclic group of order n.

If every ideal in a ring is a principle ideal, then the ring as a whole is called a *principle ideal ring*. We can now go back and consider the case we quietly skipped. If you have exhausted all ring elements by taking multiples of some r, then the set of all these multiples is an ideal of the ring. Every ring is an ideal of itself, just look at the definition of an ideal. Thus, in this case of exhaustion, you again end up with a principle ideal ring.

Fact: The order of any principle ideal of a ring must divide evenly into the size of the ring.

Proof: We already know from the residue class decomposition that the order of *any* ideal I of a ring R must divide evenly into the size of R, so saying this for a principle ideal is nothing new.

Important Example of a ring: $\mathbf{Z}_n$ = {Mod-n,+,•}

Earlier we discussed the additive cyclic group {Mod-n,+} which consisted of n elements {**0**,**1**,**2**....**n-1**} with addition defined by **a** + **b** = Rem[(a+b)/n] **1**. The additive generator is **1**. Any element can be written in the form **m** = m**1**, a multiple of the additive generator.

In order to have a ring, we need a second operation •. It is defined in a manner similar to +, so here are both operations:

$\mathbf{a} \bullet \mathbf{b} = \text{Rem}[ab/n]\ \mathbf{1}$ $\qquad$ $\mathbf{a} + \mathbf{b} = \text{Rem}[(a+b)/n]\ \mathbf{1}$

Claim: {Mod-n,+,•} forms a "ring with identity". The usual notation for this thing is $Z_{\mathbf{n}}$.

Proof: Since this ring is so important, we will make a reasonable attempt to do a real proof:

1) The elements of Mod-n are clearly *closed* under this •, since ab/n always produces a remainder in the range (0,n-1).

2) Also, ab/n = ba/n so we have $\mathbf{a} \bullet \mathbf{b} = \mathbf{b} \bullet \mathbf{a}$ and we have *commutative*.

3) The *associativity* proof requires Little Lemma 1 below, then you get:

$$(a \bullet b) \bullet c = \text{Rem}[ab/n]\ \mathbf{1} \bullet \mathbf{c} = \text{Rem}\left\{ \frac{\text{Rem}(ab/n)\ c}{n} \right\} \mathbf{1} = \text{Rem}\ \{ (abc)/n \}\ 1$$

Since this result is symmetric in a, b and c, it must be equal to any grouping (x•y)•z you want, in particular it is equal then to a•(b•c) so we have associative.

4) The *distributive* property looks like this:

$$\mathbf{a} \bullet (\mathbf{b} + \mathbf{c}) = \text{Rem}[a(b+c)/n]\ 1 = \text{Rem}\left[\frac{ab + ac}{n}\right]\ \mathbf{1}$$

$$\mathbf{a} \bullet \mathbf{b} + \mathbf{a} \bullet \mathbf{c} = \text{Rem}(ab/n)\mathbf{1} + \text{Rem}(ac/n)\ \mathbf{1} = \text{Rem}\left[\frac{\text{Rem}(ab/n) + \text{Rem}(ac/n)}{n} \right] \mathbf{1}$$

and these are equal from Little Lemma 2 below.

5) The element 1 is a identify for •, since $\mathbf{1} \bullet \mathbf{m} = (1m)\mathbf{1} = m\ \mathbf{1} = \mathbf{m}$.

Thus, we have shown that {mod-n, + • } has all the properties of a ring, and it has a multiplicative identity as well, so it is a "ring with identity".

Little Lemma 1: $\qquad \text{Rem}\left\{ \frac{\text{Rem}(x/n)\ y}{n} \right\} = \text{Rem}[\ (xy)/n]$

Proof: Write Rem(x/n) as x - Xn, where X = integer. Then LHS = $\text{Rem}\left\{ \frac{(x - Xn)\ y}{n} \right\}$. But the numerator term nXy is a multiple of n and so can be deleted from inside the remainder, leaving Rem(xy/n).

Little Lemma 2: $\qquad \text{Rem}\left[\frac{x + y}{n} \right] = \text{Rem}\left[\frac{\text{Rem}(x/n) + \text{Rem}(y/n)}{n} \right]$

Proof: Write Rem(x/n) as x - Xn where X = integer. Write Rem(y/n) as y - Yn where Y = integer. The RHS then becomes Rem[$\frac{x - Xn + y - Yn}{n}$] But the Xn and Yn numerator terms are multiples of n and so contribute nothing to the remainder, leaving Rem [(x+y)/n].

Important Example of a Residue Class Ring: Z / (n)

Suddenly all of the above residue class business is going to start making sense. The classic example is to let R be Z, the ring of integers -- plain old integers, plus and minus and 0. The + and • operations are the regular operations we are used to.

Consider the set of integers which are multiples of 5. We could pick any integer n, but 5 sounds nice:

0 ±5 ±10 ±15 ±20 .....

Notice that this set forms an additive cyclic group (as discussed above) with generator 5. You cannot, for example, generate a 14 by adding two things in the above list, you can only generate other elements in the list.

The list forms an *ideal* within the full set of integers because it is first of all an additive subgroup, and second of all, multiplication of any element of this set by an integer gives an integer, whether or not that integer is in this set. Since the ideal consists of multiples of some ring element, it is a principle ideal.

Fact: The only ideals you can make inside the set of integers are principle ideals like this, so R is a principle ideal ring. (no proof)

The usual notation for an this ideal is (5), where the parentheses are supposed to suggest all multiples of the thing inside. Since the ring is Z, the integers, we are now going to form the residue class ring which has the notation Z/(5) , or more generally, R/I = Z/ (n).

In building the residue class chart, we are going to make a slight change in notation. Instead of putting the residue class leaders on the left edge of our chart, we will put them as the middle column of the chart, and we will mark it with a ** so you can find this column. So here is the chart which is the residue class (row) decomposition of ring R with respect to ideal I. The top row as usual is the ideal.

			**					
...	-10	-5	0	5	10	15	...	{0}
...	-9	-4	1	6	11	16	...	{1}
...	-8	-3	2	7	12	17	...	{2}
...	-7	-2	3	8	13	18	...	{3}
...	-6	-1	4	9	14	19	...	{4}

That's it. There are only 5 rows. Any other rows would be repeats. Notice that we have *partitioned* the integers into the rows -- each integer appears in exactly one place in this chart. The column on the far right is the conventional manner in which each row is labelled, as discussed earlier. Each row is represented by the element in the column **.

Notice now an interesting way to think of the residue class leader labels 0,1,2,3,4 under the **. All the elements in a row have something in common. All integers in the second row have remainder 1 when you divide them by 5, and this 1 is the label of the leader. So the leader (row label if you will) is the *remainder* of what you get by dividing any row element by 5.

The notion of *remainder* is the key point here. Each row corresponds to a possible remainder. The top row is the ideal which goes with remainder 0.

So the residue class ring thing has 5 elements -- the five rows of the above chart. Consider this:

{1} + {4} = {0 }

Let's find the "additive inverse row" of the second row {1}. It is the last row {4}! Add any pair of items one from each of these rows, and you get something in the first row {0}. And the first row is its own inverse, which brings us back to the inexplicably exciting fact that {0} + {0} = {0 }.

We wish now to explicitly write down the + and • tables for our residue class ring. Addition {i} + {j} means we to normal addition i + j, then decide what row the answer goes into. Clearly, it goes into the row determined by Rem[(i+j)/5]. And Multiplication {i}•{j} means we do normal ij multiplication, then divide by 5 to see what row the result is in. Thus:

{i} + {j} = {k} where k = Rem[(i+j)/5] = (i+j)mod-5
{i} • {j} = {k} where k = Rem[(ij)/5] = (ij)mod-5

Fact: The residue class ring we have just constructed is equivalent to the mod n ring discussed at length above. In other words, Z/ (5) = Z_5. More generally, Z/(n) = Z_n = { mod-n,+,• }

Proof: Both rings have the same number of elements and the same + and • tables, QED.

Basic facts about the integer ring Z.

Most of these are so obvious, you hesitate to write them down. However, each item carries over into the polynomial world we are about to enter, so we need a solid starting point.

1. **Division Algorithm**. Relative to a divisor integer d, an integer n has a unique quotient integer q, and a remainder integer r:

n/d = q + r/d or n = q•d + r "Rem(n/d) = r"

The second form is nicer since you can avoid talking about the / operation. This operation does not even exist in the ring of integers R, so we will steer clear of it.

Example: 32= 6•5 + 2

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

$n = (p_1)^{m_1} \cdot (p_2)^{m_2} \cdot (p_3)^{m_3} \cdots$

Example: $451,008 = 2^6 \bullet 3^5 \bullet 29^1$

3. **Euclidean Division Algorithm**. Every pair of integers n_1 and n_2 has some largest common divisor. You can write this divisor as a unique linear combination of the two numbers, where the coefficients are integers:

$d = a\bullet(n_1) - b\bullet(n_2)$ { replace b with -b to get the usual form}

Example: $7 = 13\bullet(973) - 42\bullet(301)$ 7 is largest common divisor of 973 and 301.

This last result is not as obvious as previous ones. There is a mechanical procedure for finding d, a, b once you are given n_1, and n_2. See Peterson and Weldon, *Error Correcting Codes,* p 146 for example.

Definition: If the integers n_1 and n_2 have no common factors other than 1 [$GCD(n_1,n_2) = 1$], then n_1 and n_2 are said to be *relatively prime*. In this case, from 3 above one can be guaranteed of the existence of integers a,b such that $1 = a\bullet(n_1) - b\bullet(n_2)$. This occurs, for example, if n_1 is a prime number p, and n_2 is any integer that is not a multiple of p.

Residue Class Ring Z/(n) is a <u>field</u> if n is prime.

We now close this chapter by coming back to the subject of fields, which is where we started the chapter. We have seen how you can take a ring R and an ideal I and how you can make a chart, and then the rows become elements of something called the residue class ring. We did an example, which was seen to be equivalent to the modulo n ring Z_n where n = 5. Here is a fundamental new result:

Big Fact: If n is a prime number, then the residue class ring Z/(n) above is a *field*. Since we have shown already that Z/(n) = Z_n , this means that Z_n is a field when n is prime.

Proof: The proof is really the same whether you do it for Z/(n), or for Z_n. In the former case, we add a few brackets to talk about residue class rows. In the latter, we just talk about remainders, not rows.

Consider an arbitrary row {r} described by remainder r. We need to show that there exists an inverse row {s} under the operation • such that {r}•{s} = 1.

Since n is prime, and since r < n, we know that n and r are relatively prime, and their greatest common divisor is 1. Using the Euclidean Division Algorithm above, we claim that integers N and M must exist such that 1 = Nr -Mn. This says that there exists an N such that 1 = Rem(Nr/n). Now expand Nr = Kn + s, where s < n. This gives $1 = \text{Rem}(\frac{Knr + sr}{n}) = \text{Rem}(sr/n)$. Thus, according to the definition of the operation •, we have found s such that **r•s = 1.** { The Zn proof just ended here.} These remainders of course are representative of rows, so this means {r}•{s} = {1}.

Thus, every row has a multiplicative inverse, and this was the only missing factor which prevents our residue class ring Z/(n) from being a field. The result is true only if n is prime!

The implication is that some row in the chart must be the identity {1}, and each row must now have an "inverse" row in the multiplicative sense:

identity: $\{r_1\} \bullet \{1\} = \{r_1\}$ inverse: $\{r_1\} \bullet \{r_2\} = \{1\}$

In our example, 5 is a prime number, so these things must be true. Identity {1} is the second row of our chart (the row containing the integer 1) , as is easy to verify. The inverse of row {3} is row {2}. Every row has an inverse row. Recall that the first row is the additive identity {0}, which is different from {1}.

If you try doing the case n = 4 and make the chart, you find a most annoying thing. Yes, the row containing 1 is still the identity {1}, but certain rows don't have any inverses. You multiply some row by all the other rows, and you never get {1} as the answer! Think about the row {2}. It now contains only even numbers. Row {1} contains only odd numbers. What row could there be that such that {2}•{r} = {1} ? There is no such row {r}.

So n = 4 does not make a field. Our n must be a prime number, then all the rows will have inverses, and then Z/(n) will be a field.