Galois Field Multipliers and Dividers

7.1.91

Goal is to understand scramblers, which are circuits that I think do the above. Best source I have right now is the Pederson book, Chapter 7. However, it is relying on some math which I have forgotten yet again, so time to review.

These notes were written before my Galois Theory book. This file is called "scrambler math". Printed out on 7.29.91.

Part I: algebra leading up to notion of a "quotient ring" R/I and GF(m).

Group we know. Has only one operation, closure, inverse, identity, associativity, such as integers under addition.

Ring is a two-operation deal, such as integers under addition and multiplication. Under the + operation it is an abelian group. Under the * operation it is closed, associative. Under both + and * you have distributive.

Field is a ring with extra stuff: abelian under *, inverse under * (except for 0), identity under *.

Subgroup H of G is obvious.

You can make a **chart** and decompose a group G using a subgroup H as follows. Put elements of H across the top, with 1 in leftmost column. Then pick **coset leaders** from G and put in left column under the 1. Then multiply either gH or Hg to build the left or right cosets. If H is an **invariant subgroup**, which will normally be our case, the cosets are the same, so no need to distinguish them

So now your group G is "partitioned" into the cosets of some subgroup H.

Now consider the notion of a coset itself as an element of a fancier group:

{ g1 }*{g2} = {g3}

Here we are defining the * operation for this fancy group. If you take any element g1 in coset #1, and multiply it by any element g2 in coset #2, the product always lies in coset #3. So all members of a coset are closely related. You could write this as C1*C2 = C3. But you can in effect label a coset by any one of its members, hence the {g} notation is OK.

So we know what * means for this new group. It is closed because you cannot get some CN coset that does not exist. This is because cosets partition the group.

Identity? This must be the first line of the chart, the coset that is H itself. Take some g in a coset, multiply by h in H, result is in same coset. So you might say something like:

{ hi}*{g1} = (g1} identity

What about inverse? Start with {g1} or coset #1. Find $g1^{-1}$ wherever it is in the chart. It is in some coset coset #2. The product is 1, which lies in {h}. So you get

$$\{g1\}*\{g1^{-1}\} = \{hi\}$$

So every coset has an inverse coset, so to speak.

Final property is associative. Want to show that (C1*C2)*C3 = C1*(C2*C3). Here is where the other notation comes in handy. Write

$$(\{g1\}*\{g2\})*\{g3\} = (\{g1 \bullet g2\})*\{g3\} = \{g1 \bullet g2 \bullet g3\}$$

If you started with parens on other side, get same result. In other words, this new group is associative because the group operation for G is associative

This group whose elements are cosets of G by H is called a **factor group**. We just proved conclusively that is is a group.

Example 1: I think this will turn out to be the key example. Consider group G = integers under operation +. Consider H = integers of the form mN, where N is some number like 3. You can then partition G with a chart into cosets like this:

0	...	-9	-6	-3	3	6	9	12	...
1	...	-8	-5	-2	4	7	10	13	...
2	...	-7	-4	-1	5	8	11	14	...

Done. There are three coset leaders, there are only 3 cosets. The integers are now partitioned into three sets as shown. If we consider the factor group, there are three elements which we could choose to call {0}, {1}, {2}. Notice that {0}*{1} = {1}. Also, {1}*{2} = {3} = {0}. Pretty simple. We decompose the integers into the three cosets.

Now back to the ring:

Ring is a two-operation deal, such as integers under addition and multiplication. Under the + operation it is an abelian group. Under the * operation it is closed, associative. Under both + and * you have distributive.

Ideal I is a subgroup of the ring R under +, and it is sort of "closed" under * in the sense that RI = I. You can multiply any i by and r and you get r*i = i' in the ideal.

Example: ring = integers under + and *. Consider only those that are multiple of 3 to be an ideal. For example, 9 is in the ideal. Now 2*9 = 18 is in the ideal, etc. Obviously any n(mN) = (nmN) = (kN) is still in the ideal you started with.

Now redo the whole coset decomposition. Top row is the ideal. Coset leaders on the left. The Ring then partitions into the cosets. Since we are now in a two-operation situation, the cosets havea new name, they are called residue classes. For integers N=3, chart looks same as above

0	...	-9	-6	-3	3	6	9	12	...
1	...	-8	-5	-2	4	7	10	13	...
2	...	-7	-4	-1	5	8	11	14	...

Top row is the ideal I. Each row is a coset = residue class. As before, you can regard each row as an element of a fancier group. Let {1} represent the second row. As before, under + these classes form the factor group. But now we have another operation * to think about. Maybe they form a ring, lets see.

Closure under * ? {r1}*{r2} = {r1•r2} seems the right way to define *. But the ring R is closed under •, so get some {r3}, and done. In general, it all falls out. The algebra of the ring R more or less ascends to be the algebra of the factor group = **residue class ring** thing.

So, for a ring R and ideal I, you get R/I = factor group under + = residue class ring under + and *. I think other books calls this the **quotient ring**.

Nothing too mysterious really.

Book goes on to claim that if you take R = integers, the only ideals there are are those like we had above, where you say i = kn. Ie, a multiple of some number n. They want to denote the residue classes now by notation (n) where n = 0,1,2,...m-1. Fine. An ideal that is a multiple of numbers is called a principle ideal, and the whole ring that decomposes into such things is a principle ideal ring.

Claim: if m = prime, the quotient ring is a field (meaning * inverse exists, etc.)

Field is a ring with extra stuff: abelian under *, inverse under * (except for 0), identity under *.

So if m is not prime, something must be missing. Notation used is to say {0} = the ideal itself = 0. Thus, if we have some {k} + {0} = {k}, you might as well thinmk of {0} as 0. Identify must be this:
{k}*{1} = {k}. Now lets look for inverse. $\{k\}*\{k^{-1}\} = \{1\}$ in theory. For the case m=3, lets try this:
$\{2\}*\{2^{-1}\} = \{1\}$. What does this mean? See chart again:

0	...	-9	-6	-3	0	3	6	9	12	...	= {0}
1	...	-8	-5	-2	1	4	7	10	13	...	= {1}
2	...	-7	-4	-1	2	5	8	11	14	...	= {2}

Notice that {2}*{2} = {1}. I have repeated the coset leader in the middle of the chart. Thus, we can conclude that $\{2\}*\{2^{-1}\} = \{1\}$ implies that $\{2^{-1}\} = \{2\}$, so each class probably has an inverse. Now lets make a chart for m = 4:

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

Now consider again $\{2\}*\{2^{-1}\} = \{1\}$. Exhaust things:

{2}*{0} = {0} / it happens that {2} + {0} = {2}
{2}*{1} = {2}
{2}*{2} = {0}
{2}*{3} = {2}

Horrors! You do not see any {1} on the right, so $\{2^{-1}\}$ does not exist!

So I see how for general m you can fail to get a field.

Here is the proof that you do get a field for prime m. All you have to do is construct the inverse and you have it. Start with some class {s}. Let m = prime. Now we use a very basic fact of numbers which I will not try to prove here: Suppose two integers R and S have a greatest common divisor D. Then the claim is that you can find integers a and b such that:

D = aR - bS

Now, what is the greatest common divisor between s amd m? If m is prime, it is 1. thus write

1 = am - bs or bs = am + 1

Now, you know that the integer am is in class {0} and am+1 is in class {1}. You know that s is in {s}. And you know that the integer b must exist, and it is in some calss {b}. So you have

bs = am + 1 implies {b}*{s} = {1}

and thus you have shown that the inverse of {s} exists, and you have a field.

When m = prime, the quotient ring R/I for R = integers and I is the ideal of multiples of "m", is a field. This field is called **Galois Field GF(m).** The operations here are {1}*{2} or {1} + {2} type things. the things like {1} are the cosets of residue classes.

Part 2: The Analogy between Polynomials and the Integer Ring

Here we go:

integer	∅	polynomial in x with coefficients in some field F
a + b = c	∅	a(x) + b(x) = c(x), addition comes from F
a*b = c	∅	a(x) * b(x) = c(x), multiplication comes from F
k is multiple of m k = nm	∅	k(x) is multiple of m(x): k(x) = n(x)m(x)
p/d = q + r/d	∅	p(x)/d(x) = q(x) + r(x)/d(x) r= remainder poly

m = prime	∅	m(x) not divisible by any other nontrivial polys
ring of integers	∅	ring of polynomials over F
ideal = multiples of integer m	∅	ideal = multiples of a poly g(x)
m = prime integer	∅	g(x) is prime poly
d = ar - bs	∅	d(x) = a(x)r(x) - b(x)s(x)
set of integers partitions into classes called {k}	∅	set of polys partitions into classes of some sort
quotient ring R/I	∅	quotient ring (f(x)) / I(g(x))

Despite all this, things are not yet ringing clearly. So more words are now needed. Lots of notational issures are arising.

Why do polys form a ring?

Ring is a two-operation deal, such as integers under addition and multiplication. Under the + operation it is an abelian group. Under the * operation it is closed, associative. Under both + and * you have distributive.

You can add and multiply polys because we know how to deal with their coefficients in some field, and because we know how to multiply x's:

$$(3x + 2x^2)(2x) = (6x^2 + 4x^3)$$

Add is abelian and closed. Multi is also closed. OK, no problem.

Why do "multiples of a poly" form an ideal?

Ideal I is a subgroup of the ring R under +, and it is sort of "closed" under * in the sense that RI = I. You can multiply any i by and r and you get r*i = i' in the ideal.

Let g(x) be a poly in the ideal I. Let f(x) be any poly in R. Is it true that g(x) f(x) is still in I ? By "multiple" is meant multiplication by any poly in R. So the ideal must be the set of polys in R that are exactly divisible by g(x). Suppose g(x) = (1+x) over the reals = your field. Then 2(1+x) is in the same ideal with g(x). But (2+x) is not! You cannot evenly divide (2+x) by (1+x). Also, x or any power of x is not in the ideal.

What about (2+2x)? this is 2(1+x). You can divide this by (1+x). It is in the ideal. It appears somewhere in the first row of the chart.

Next, what are the residue classes of g(x)? You form them by starting with top row, and **add** some ring element not in the top line:

g(x)	q(x)g(x) for all possible q(x)
g(x) + r(x)	q(x)g(x) + r(x) for all possible q(x) and all possible r(x) not in ideal.

So here we have a symbolic top row = the ideal based on g(x). Then I have represented all other rows by a single line. The condition on r(x) is that r(x) is all polys that are NOT in the top row. Look at some row labelled by r(x). It contains all polys which have *remainder* r(x) when you divide by g(x). In the integers case, rows were similarly labelled by the remainder of division! Notice that, if degree of g(x) is n, then all polys in the ideal (top row) are degree n or higher. Thus, we know that all polys of degree less than n make viable r(x) candidates.

In the integer case, there were only rows labelled k = 0,1,2,,, m-1. If you tried to make higher rows, you found that you duplicated an earlier row. Eg, if you have m=3, the row made by adding 4 to the top row is same as row made by adding 1. Here the same thing happens. The results seems clear:

Each unique row (= coset = residue class = element of quotient group) is characterized by a remainder that is less in degree than g(x). For each such remainder, there is a row. Each poly in a coset corresponds to the possible quotient poly q(x) you get when you divide by g(x).

Just as we did with the integer ring ideal thing, we might as well formally label the rows by the remainder function itself. This is just the case where q(x) = 0. So here again is the chart:

0	q(x)g(x) for all possible q(x)	top row = ideal
$r_1(x)$	$q(x)g(x) + r_1(x)$ for all possible q(x)	
$r_2(x)$	$q(x)g(x) + r_2(x)$ for all possible q(x)	

... and so on for every possible remainder poly of degree less than the degree of g(x)

So now it makes sense to label each row or coset by the remainder {r(x)}. The first row is {0}, meaning you get zero remainder for polys in that row.

Assume g(x) has more than one term. Then no powers of x are in the first row, so they must appear in other rows. So we might take $h(x) = x^n - g(x)$. I feel pretty sure this is not in the top row. So here is another way to view the chart:

0	q(x)g(x) for all possible q(x)
x^k	$g(x)q(x) + x^k$ for all possible q(x)

So you would have rows for k = 0, 1, 2 ... n-1. But this is only n possible remainders. There are many more remainders, so we have not exhausted the chart with thie labelling.

Now consider this equation: $\{ r1(x) + r2(x)\} = \{ r1(x) \} + \{ r2(x) \}$

We must be adding classes here, and this is quotient group addition. Here is what it means. Take all polys in the r1 class, and form all sums with all polys in the r2 class. Then all of these sum polys end up being in the same class with each other. Why is this true? Because the the remainder of a sum of polys is the sum of the remainders of the individual polys! Remaindering is a linear operation. And because the rows are labelled by the remainder, the above is true.

Consider this possibility: $\{a\, f(x) + bk(x)\} = \{ af(x) \} + \{ bk(x) \}$

This is just s restatement of the above where we use some new polys, as in $f_1(x) = af(x)$. So can we take out our constant? We can make a definition of what a scalar does to a class:

$$a \{ r(x) \} + \{ ar(x) \}$$

Thus, with this definition, we generate the class which is functions of remainder ar(x). This is not the same class as {r(x)} of course. With this understanding of scalar mult on a class, we can say

$$\{a\, f(x) + bk(x)\} = \{ af(x) \} + \{ bk(x) \} = a \{f(x) \} + b \{k(x) \}$$

I have proven this is true.