PROFESSOR: So we're slightly into chapter seven, which is the algebra chapter. We're talking about a number of algebraic objects, starting with integers and groups and fields. Polynomials. Our objective in this chapter is simply to get to finite fields so that you have some sense what they are, how they can be constructed, what their parameters are, how you can operate with them by addition, multiplication, so forth, as you would expect in a field. Subtraction, division.

And that's really all we're aiming to do. I'm trying to give you a short course in algebra, really, in two lectures or fewer. And clearly I'm going to miss a lot of things. In particular, I'm not going to cover even everything that's in chapter seven, which itself is a highly compressed introduction to finite fields.

I'm trying to do this while remaining faithful to the philosophy of this course and other courses at MIT, which is that you should really prove everything and show why things are true, and not simply make assertions. So it's a little tough and it forces me to go a little fast, but I hope that you can keep up, and especially with the assistance of the notes or the many possible other things you could read on this subject, which are listed in the notes, you'll be able to keep up. And some of you, of course, have seen this in other places in more extended form.

Now, this will get us in a position to start to talk about Reed-Solomon codes, which are the single major accomplishment of the field of algebraic coding theory. Certainly for getting to capacity on the additive white Gaussian noise channel and for lots of other things, they're an extremely useful and widely implemented class of codes. And we'll be able to maybe just get to the beginning of that by Wednesday.

And then I won't be here again next week, but fortunately we have an expert on campus who is far more expert than I in Reed-Solomon codes, their decoding algorithms, who has agreed to talk for two lectures, maybe one more focused on Reed-Solomon codes and one, I hope, on his whole philosophy of life. Perhaps. I don't know how it's going to come out, but I'll see it on TV when I get back.

Anyway, Ralf Koetter will be lecturer for Monday and Wednesday next week. I think you'll enjoy the change of pace.

OK. So where are we in chapter seven? We're not very far. We're talking about these various algebraic objects. We've started with integers just to get you into the feel of it. We mainly talked about integer factorization, the Euclidean division algorithm, things that you've known for a very long time, basically here because A, we're going to be using integers as we go along, and their factorization properties, B, it's a model for polynomials, which behave very much the same way as integers because they're both principal ideal domains.

In particular, we looked at the integers mod n with the rules of mod n arithmetic, which we're going to call Zn. This is simply 0 through n minus 1 with the mod n arithmetic rules.

And then we went on to groups. We first gave the standard axioms for groups, and then I gave you an alternative set of axioms which focused on this permutation property. If you add, I'm calling the group operation addition, because essentially all the groups we talk about are going to be abelian -- if we add a group element to the group, what do we get back? We get the whole group again. It's permuted, it's the entire group, it's in a different order. All right?

And with this and the identity, this plus the identity and the associativity axiom are also a sufficient set of axioms for the group.

And I think this is really the most useful thing to think about with a group. We've also called it the group property when we talked about codes. You know, if you add the code word to all the elements in the code, you get the code back. And you saw how useful that was for seeing certain symmetry properties of minor linear block codes.

So we even talked about cyclic groups, specifically finite cyclic groups. And we showed that all them basically are isomorphic to z mod n. A cyclic group is defined by a single generator. If we identify that generator with one, G plus G is identified with 2, and so forth, then we get an addition table which is exactly the same addition

table as Zn. And that's what we mean when we say two groups are isomorphic. So all finite cyclic groups look like Zn. You can think of them as being images of Zn. All right? It's the only one you need to know about.

OK. So that's where we are any questions on this material? Pretty easy, I think. Terribly easy if you've ever seen any of this before. Probably takes a little absorbing if you haven't.

OK. Now the next natural subject to talk about is subgroups. And what is a subgroup? A subgroup simply a subset of elements in the group which, together with the group operation already specified in G, which we're calling circle plus, is itself a group.

What does that mean? Well, associativity comes for free, because we already have that property for circle plus in G. Obviously H has to include the identity in order to satisfy the group axioms. And finally, the third group axiom is this permutation or group property that if we add any element of the subgroup to itself, we have to stay within the subgroup and ultimately generate the whole subgroup. That means that subtraction, cancellation hold in the subgroup. All right?

So that's clear. What's an example of a subgroup? If we have -- we talked about Z10 as the group. What would be a subgroup? Anybody?

AUDIENCE: [INAUDIBLE]

PROFESSOR: 0 to 4. OK. So you're proposing that H is the elements 0, 1, 2, 3, 4 out of G. Does that work? This doesn't include 0. But suppose I add 3 and 4?

AUDIENCE: I assume that you have modules for a reason.

PROFESSOR: No. In this group, the group operations modulo 10 addition. Subgroup has to have the same operation as the group it came from. What you've got here is you've already got, in essence, a quotient group. Or at least that's where you're headed. So this is not a subgroup. Thank you for the suggestion. Fails. Anyone else? What?

AUDIENCE: 0,1?

PROFESSOR: 0,1. OK. Let's try that. And it contains the identity 0 plus 1 is certainly in the group. How about 1 plus 1? It's not in the group. 0 and 5? That sounds more promising. Now, 0 plus -- what's the addition table of this? 0, 5, 0, 5, 0, 5. What's 5 plus 5? It's 10. But mod-10 , that's 0.

So it seems we do have a group. And in fact, this is a finite cyclic group generated by 5, and has two elements, so it's isomorphic to Z2. In other words, the addition table looks just like the addition table of Z2 with a relabeling.

OK. Any other subgroups of Z10? The even integers. There. Now we're really smoking. H equals 0,2,4,6,8. Those are all the even integers in Z10. And again, evens plus evens equal evens. So we get a group of five elements, satisfies is the group property, and it's isomorphic to what? Z5 -- yeah. This is obviously the same group is 0, 1, 2, 3, 4, just doubling everything. Operates the same way. So it's change of labels.

OK. So there are some examples of subgroups. Let's take another good example. Let's just take the set of all integers. That's an infinite group. Mathematicians call it cyclic, even though it doesn't cycle. What's a subgroup of that?

AUDIENCE: Even integers.

PROFESSOR: All even integers! Very good. Check. Does that include 0? Yes. Does it have the group property, even plus even is even? Clearly subtraction holds, and so forth.

So this is the subgroup. Interestingly, there's a one-to-one correspondence between Z and 2Z, so the subgroup is as big as the group itself. You get into the whole issue of transfinite numbers. But that's not where we're headed here.

OK. We'll just keep that in mind for now. Obviously 3Z, 4Z, 5Z, and all the multiples of n are going to be a subgroup of the integers for any integer n. So more generally, we could take H equals nZ.

What's a coset? Coset is also, in the abelian case, called a translate of a subgroup.

A coset, for instance, is in the form H plus G for some G in the group, not in the subgroup.

Now if G is in the subgroup, we get nothing. The coset is just H again by the group property of H. So the interesting cases are where G is not in H. Let me give you some examples.

Let's take G equals Z10 and H equals 0,2,4,6,8. You might call that 2Z10 It's the set of all elements which are twice the elements in Z10. OK. What is a coset? If I add any element in this group to H -- let's add one, for instance. So H plus 1 consists of the elements 1,3,5,7,9.

Well, that's interesting. That seems to exhaust all of the elements of Z10. Let's take the Z equals the Z10, and H simply equal to 0 and 5, which we might call 5Z10.

And all right. Now H plus 0, H plus 5 is just equal to itself. H plus 1 is equal to 1,6. H plus 2 is equal to 2,7. H plus 3 is equal to 3, 8. H plus 4 is equal to 4,9.

So we begin to see some properties of cosets here for which proofs are given in the notes. First of all is that two cosets are either the same or disjoint. H plus 2 is the same as H. H plus 1 is completely disjoint from H. Same over here. If I had H plus 5, that would be the same as H. H plus 6 would be completely disjoint from H and would be the same as H plus 1. In fact, I can take any of the elements of a coset as its representative, and I'm going to get the same coset, take any element outside the coset, and I'll get a completely distinct coset. This follows just very easily from the cancellation property. All right?

So the cosets, the distinct cosets, form a disjoint partition of G. We certainly have a coset that contains every element of G. Just take H plus that element G. That's going to contain G because H contains 0. So there is a coset that contains every element of G. Any two cosets, distinct cosets, are disjoint, so that's what we mean by a disjoint partition. We list all the elements of G in this way.

And in the finite case, that gives us a early famous theorem attributed to Lagrange. What does that mean? This means that H has to divide G. If G has size 1,10 and all

the cosets have the same size, by the way, again by the cancellation property -- this means that G has to consist of an integer number of cosets, all of which have the size of H. OK? And therefore some integer times H is equal to H, which is the same thing as H divides G. OK?

If G is a finite group, I mean by this kind of determinant notation, the size of H. The size of H divides the size of G. Or more elegantly, the cardinality of H divides the cardinality of G. But why say cardinality when you can say size? I shouldn't have put it here. Where H is any subgroup, any subgroup, of course, that's finite is itself a finite group.

So that's going to turn out to be quite a powerful theorem. And it just follows this little exercise. And we see it's satisfied, certainly, by these two examples. In fact, it's pretty easy to see that the subgroups of Zm are going to correspond to the divisors of m in the same way. We're going to get a subgroup for every divisor of m, and in the case of cyclic groups, this is the way it's going to come out. Just pick any divisor. You get a subgroup isomorphic to Zd. Again, this is done with more care in the notes.

Suppose we have the infinite case here. Suppose we have Z and 2Z. So let me draw that case. G equals Z. H equals 2Z. And all right. What's H? H is the set dot dot dot minus 2,0,2,4, dot dot dot.

So this is H. And what's H plus 1, or in fact, plus any odd number? It's going to be the odd integers. H equals minus 1,1,3,5, and so forth.

So again, this works in the infinite case, that the distinct cosets form a disjoint partition of an infinite group G. But of course, we don't get Lagrange's theorem as a corollary, because I already said, there's a one-to-one correspondence between Z and 2Z, paradoxically. So the cardinality of Z and 2Z are the same. More elegant language.

Nonetheless, you see, this is a useful partition and standard partition into the even integers and the odd integers. And we could also write this as 2Z and this is 2Z plus

1. So we can divide the integers into even integers and odd integers.

All right. Now we can actually add cosets, subtract cosets. In these cases, we can even multiply cosets. But let's just talk about staying within the group operation. Given any abelian -- let's continue to say G is abelian -- how would you add two cosets?

Coset addition is defined as follows. H plus G -- we want to have some addition operation, which I'll just indicate by plus -- H plus G prime, what's going to equal? We define that to equal H plus G plus G prime.

And that makes sense. I mean, if we really write all this out, we get H plus H plus G plus G prime. H plus H is just H again. So it's sort of a proof of that. If you go through in detail, any element of this coset plus any element of this coset is going to be an element of this coset.

So this itself is a coset. So we now have an addition table for cosets. So in fact, it's easy to show that the cosets themselves form a group called a quotient group. Start over here. Cosets of H in G under coset addition -- that's going to be Z -- form a group. We just defined coset addition.

And it's easy to check that they themselves form a group called the quotient group. Usually written G slash H and pronounced G mod H. And we can can mod out anything. We do the arithmetic in these quotient groups by modding out any elements of H.

And let's take an example. Here's a good one. For example, the cosets of 2Z in Z, namely, 2Z and 2Z plus 1. Under coset addition. What is coset addition here? If I add any even integer to any even integer, I get an even integer. Any odd to even, I get an odd integer. Odd to odd gives that. I mean, odd to even gives that, and odd to odd gives me back evens again.

So that's the addition table. The subgroup itself, x is the identity. This is clearly isomorphic to Z2 with this addition table.

In fact, this is a very good way of constructing the cyclic group Z2, or more generally, Zn. So this would be called Z mod 2Z. And it's isomorphic to Z2, or in general, Z mod nZ is isomorphic to Zn.

A very good way of thinking of Zn is as residue classes or equivalence classes, modulo n. The cosets of nZ. are nZ itself, nZ plus 1, nZ plus 2, up to nZ plus n minus 1. And if you add them together, they follow the rules of mod n arithmetic. If you just add the residues together and then reduce mod n.

So we can think of Zn as being -- a coset is an equivalence class. It's all the elements of the group that are equivalent, modular of the subgroup H. Or in the case of integers, it's all integers that are equivalent modulo the subgroup nZ. They have the same remainder after division by n. They have the same residue. These are all equivalence class notions.

And how do you add them? You add them in the ordinary way, and then you take everything modulo m. In other words, you do mod-m arithmetic.

OK. So I didn't quite go to quotient groups in the notes, but perhaps I should have. Probably I should have, because this is maybe the most powerful idea in group theory, and certainly closely related to this little bit of number theory that we're doing in the integers mod n. And of course, it has vastly greater applications than just that.

OK. And you could do the same thing over here. This is basically doing the same kind of thing. But I won't take time to do that. So here's another view of the integers mod-n that may be helpful as we go forward.

All right. I think that's all I want to say about that. Yeah. Good. All right. Here would be a good place to start on fields.

OK. Fields. Obviously very important in algebra. Fields are like groups, only more so. Groups are a set of elements with a single operation, which we've been calling addition. A field is a set of elements with two operations, which we'll call addition and multiplication.

So what do we have? We have a set of elements F. We're going to be particularly interested where the set is finite. Those are called finite fields. And we're going to have two operations, which I'll continue to write addition by simple plus and multiplication with an asterisk, just to be very explicit about everything. And after a while, you can write these things as you would in ordinary arithmetic, with just ordinary plus and juxtaposition for multiplication.

And what are the axioms of a field? They're presented in an elegant way in the notes, which obviously go back a long way, but I got from Bob Gallager, and I like. All right.

Under addition -- so let's write it this way. Now, just considering the addition operation is an abelian group. Commutative group. Which means it has an identity, and we will continue to call that identity 0. Just as we do in the real field, let's say. OK. Think of the real field, if you like, as a model for all fields here. All right. So that's axiom one.

Axiom two. If we take the non-zero elements of the field, which I write by F star, explicitly that's F not including 0 -- not a very good notation, but I'll use it -- and the multiplication operation, that, too is an abelian group. So this, of course, is why we spent a little time on groups, abelian groups, so we'd eventually be able to deal with fields. And its identity is called 1. Meaning that under multiplication, 1 times anything is equal to itself.

And then we have something about how the operations distribute, the usual distributive law that A times B plus C is equal to A times B plus D times C, where I've written out all of these. So this is how addition and multiplication interact again in a way that you're accustomed to, and after a while, you don't need to write all these parentheses.

OK. So that's actually almost a simpler set of axioms than for groups, once we understand the group axioms. And so let's check. Is the real field, is the set of all real numbers under ordinary real addition and multiplication, is that a field?

What do we have to check? We have to check that under addition, we're going to take the additive identity as being equal to 0. Under our reduced set of group axioms, the main thing we have to check is if we add any real number to the reals, we get the reals again and the one-to-one correspondence is the permutation. Is that correct? Yes, it is. And so this is OK.

Now under multiplication, if we take the non-zero real numbers, here's the question. If I have some alpha not equal to 0, is alpha times the reals, not including 0 -- the non-zero real numbers -- equal to R star? And here I'm really implying a one-to-one correspondence. So I might write it more that way.

I pose this question rather abstractly, but you can easily convince yourself that it's true. Any non-zero number, if I multiply it by any non-zero number, I get a non-zero number. Is the correspondence one to one? Yes, because I can divide out this number and get alpha. So alpha x on R star by multiplication to give R star again, and this is a one-to-one correspondence.

But it's obvious why I have to leave out 0, right? 0 times any real number is 0. So at O, R star is simply equal to zero set. So we always have to leave out 0 from multiplication. 0 doesn't have an inverse. Everything else does have an inverse.

Under the standard group operations, that's what we have to check. That would be the alternate question, does every non-zero real number have an inverse? That's easier to see, the answer is yes. Multiplicative inverse. Inverse of alpha is 1 over alpha.

AUDIENCE: [INAUDIBLE]

PROFESSOR: Yes. I've used the alternative set of axioms, including the permutation property. To check whether there's an abelian group, I've asked if alpha R star is the permutation of R star. And without going through details, I claim it is. Thank you.

All right. So we checked that. Of course, the distributive law holds. So the real field is a field, which you probably were willing to accept on faith, anyway.

Similarly, you go through exactly the same arguments for the complex field. What about the binary field? We think we understand that by now. Here the operations are mod-2 addition and mod-2 multiplication. I've written down explicitly the addition and multiplication tables.

Under addition, we simply have Z2 again. F2. The additive group of F2 is simply Z2. We forget about multiplication. We've seen quite a few times now that that's a group.

Under multiplication, what are the non-zero elements of F2? Just one element. one. This includes the identity? Yes. Is it a group? Yeah. It's a trivial group. 1 times 1 equals 1. 1 under multiplication is isomorphic to the trivial group 0 under addition. Its group table is 1 times 1 is 1.

Sure enough. That's the identity permutation. Sometimes when things get too trivial, it's a little hard to check. But yes. And distributive is easy to check. OK?

So that's all it takes to define a field. Of course, by the inverse property, when we have addition, this also implies an inverse and a subtraction operation and a cancellation and additive identities. We have a field element on both sides of a plus b equals a plus c, then b plus b equals c. That's what I mean by cancellation.

Similarly under multiplication, we get a multiplicative inverse. 1 over alpha, for any alpha in F. We, therefore, are able to define division. And we have cancellation for multiplicative identity.

So we immediately get a lot from these group properties. We get all the properties you expect of fields. You can add, subtract, multiply, or divide, all in the usual way that we do over the real field.

OK. Let's stay over here. I think my next topic is prime fields. Yes. So prime fields. When we talked about the factorization properties of the integers, we talked about primes p. And now I'm going to talk about Fp is going to be a field with a finite number of elements where the number is a prime.

So what are the elements in this field going to be? Are they simply going to be 0, 1 up through p minus 1 again, the same elements as were in the cyclic group with p elements where I'm restricting m now to be a prime p? And for my addition operation and my multiplication operation, I'm going to just let these be mod-p addition and multiplication now. And I claim that this is a field.

So actually, the proof follows very close to what I just did for F2. F2 is a model for this. But it's a little harder to check this. Under a, under the addition operation, Fp really is just Zp again, so that's OK. That's an abelian group. Zmod-p. Or the quotient group, Zmod-pZ. We can also again think of this as Zmod-pZ, if we want.

So everything is going to become mod-Z. That's a very useful way of thinking of it. So we're really thinking of these as remainders or representatives of the residue classes of pZ in Z. This is pZ, this is pZ plus 1 up to Z minus 1, up to pZ plus p minus 1. This is the same as pZ minus 1.

OK. The real question is, if we take the non-zero elements of Fp, is this closed? And does every element have an inverse? Or equivalently, when we multiply by a particular element, do we just get a permutation of this?

The reason that p has to be a prime -- let's suppose we take two of these things, a and b, and we multiply them. What's the multiplicative rule? a times b is just ab mod-p. That's what I defined multiplication as.

Now the question is, could that possibly be 0? Which is the same as saying, could a times b be a multiple of p, where a and b are taken from the non-zero elements of the field? And here, because p is a prime, it's clear that you can't multiply two non-zero numbers which are less than p and get a multiple of the prime p.

If p were not a prime, then you could. If we took n equals 10 again, let's say, and we multiplied 2 times 5 from the 10 elements of these residue classes, 2 times 5 is, in fact, equal to 0 mod-10, and therefore Fp star, or F10 star, would not be closed under multiplication. We would get a 0.

But in this case, we easily prove, because it's a prime, that it's not equal to 0. And

therefore it's in Fp star, so it is closed under multiplication.

And the other thing we have to check is that it's one-to-one. In other words, can a star b equal to a star c, and by the cancellation property, which holds in --

Sorry. We've got to establish the cancellation property holds under mod-b arithmetic, but it does, and so we get the cancellation property, that this is true if and only if b equals c.

So in other words, as we run through all of these multiples for any particular alpha, we're going to get a permutation. We need to get the same set back. Everything is finite. We're going to get a bunch of distinct elements of the same size as the set itself. Therefore, it has to be the set again.

I haven't said that very well again. That's why we have notes. It's written up correctly in the notes.

But we have basically checked everything that we need to check, showed that Fp star is an abelian group under multiplication when p is a prime, and clearly not when p is not a prime.

AUDIENCE: [INAUDIBLE] the inverse, there is inverse of a?

PROFESSOR: Yes. But basically, we have to prove that if I take any of these, if I take a particular one, say, alpha, and multiply times all of them in Fp star, that I'm just going to get Fp star again. And to prove that, I have to prove that alpha times a is not equal to alpha times b if a not equal to b. That's all I need to prove, right? And that comes from the properties of mod-p arithmetic. That is what is to be proved. I need to use mod-p arithmetic to prove that.

AUDIENCE: [INAUDIBLE]

PROFESSOR: Oh. I have to check the identity is in here. The identity is in here. It has one. I'm sorry. I should have checked that, too. But 1 is the identity for multiplication.

And then from this property, since we multiply alpha p star, we get Fp star again.

That includes one. All right? So it's got to be one of these guys which, times alpha, gives 1, and that shows the existence of an inverse. So you can do it any way you want.

But the key to the proof is to prove this, and that's why I focused on the permutation property. Permutation property is really what you prove to demonstrate this.

OK? Good. Everyone seems to be following closely here. Any further questions?

This is important, because we've got our first finite field. The integers mod-p are a finite field of size p for any prime state. We've got F2, F3, F5, F7, and so forth.

OK. Further on this subject. We have two closely related propositions. One, every finite field with prime p elements is isomorphic to Fp. So if you give me a finite field, you tell me it has p elements, I'll show you that it basically has the same addition and multiplication tables with relabeling.

And secondly, every finite field with an arbitrary number of elements, for every finite field, the integers of the field form a prime field for some P. You understand my abbreviations.

And the proofs of these are very closely related. What do I mean by the integers of a field, of a finite field?

OK. Well, let's start from the very most basic thing. What do we know? We know that the field contains 0 and 1, and those are going to be two of the integers of the field. So 0 and 1 are in F.

Let's use the closure under addition. Clearly 1 plus 1 is in F. We're going to call that 2. 1 plus 1 plus 1 is in F. We're going to call that 3. And so forth.

And of course, since the field is finite, eventually this is going to have to repeat. And from the fact it repeats, you're basically going to show that at some point, one of these is going to be equal to 0. So there's going to be some n. The first repeat is going to be n equal to 0 in F.

OK. So that's what I mean by the integers. The integers clearly form a subgroup of the additive group of F, to form a subgroup under addition. And in fact, a cyclic subgroup. I'm skipping over some of the details here, but that's a claim at this point that I haven't really demonstrated.

But just from a subgroup property, let's attack number one up here. Suppose we have a field with p elements, and the additive group of the field has p elements. It consists of the same elements. And by Lagrange's theorem, what are the possible orders of that subgroup? What are the possible number of elements in that subgroup, the sizes of the subgroup? The order of a group is its size.

Well, it has to divide p. There aren't many things that divide a prime p. There's 1 and there's p. OK? So the subgroup either has a single element or it's all of the group.

If there's a single element -- let's to keep an open mind here -- then what that means is that if I take G and I add it to itself, since it's a subgroup, it has to give an element of the group. But there is only one element of the group. Let's say G is the single element in this subgroup. I guess it could only be 1. Let's start out with one. So suppose one is the only element of the subgroup. Then I get the equation 1 plus 1 equals 1, which by cancellation implies that 1 equals 0.

OK, well, that can't be true. In a field the multiplicative identity is not the additive identity. So that can't be true. That would only be true if we had a field with one element, and fields implicitly always have at least two elements, 0 and 1. F2 is the smallest finite field. I suppose we could set up a single element that sort of satisfies all these axioms, but then, what is the multiplicative group?

All right. So this can't happen. So that means this subgroup has to have p elements. It has to consist of all the elements of the field. So that means the integers are all the elements of the field.

But now the isomorphism, then, is that this is isomorphic Fp under the isomorphism. This corresponds to 2, this corresponds to 3, and so forth, in Fp. You can see, you

know, 2 is 1 plus 1, 3 is 1 plus 1 plus 1, so 2 plus 3 is going to be 5 1's. Mod size the field, whenever this cycles. So this is going to have to be p, and basically, that shows --

AUDIENCE: [INAUDIBLE] to prove that it is isomorphical [UNINTELLIGIBLE] multiplying 1 plus 1 into 1 plus 1 plus 1. But it is typical --

PROFESSOR: I really have only used the additive property here. I don't think multiplication enters into it. OK, here's where the multiplicative property adds in. I have to prove not only that this is isomorphic to Fp as an additive group, but the multiplication tables are isomorphic under the same relabeling.

So for that, I have to show that 2 times 3, when I've defined 3 and 3 this way, gives me the same result as multiplying 2 and 3 in F p mod-p. But again, I could do this just because sort of mod-p commutes with addition and multiplication. If I multiply 1 plus 1, two 1's times three 1's, so I'm going to get six 1's, and that's exactly what I get in Fp, reducing everything mod-p. So I have to check that also to prove this isomorphism. And this is done carefully in the notes.

The distributive law holds because the distributive law holds for sums of n 1's. 1 plus 1 times 1 plus 1 plus 1 plus 1, it's going to be the same regardless of where you put it in, how you put the parentheses.

OK. So with some sorry hand-waving here, we've basically given the idea of how to prove this. It's basically Lagrange that the additive subgroup has to be of size 1 or p, and we prove quickly that actually p is the only case that works. And then we extend all the arithmetic properties by just observing they'll hold for 1 plus 1 plus 1. Yeah?

AUDIENCE: [INAUDIBLE] the line 1 plus 1 plus 1 like that? Might we [UNINTELLIGIBLE PHRASE] 1 is equal to 0. What is actually [UNINTELLIGIBLE PHRASE]? Should we state that 1 has to be different than 0?

PROFESSOR: Yeah. I guess I could simply get around that by stating that the multiplicative identity has to be different from the additive identity. It clearly follows from this, and I think I

put it as an exercise, 0 times any group element has got to be equal to 0. So this is how 0 behaves under multiplication from these axioms.

But 1, as the multiplicative identity, has to satisfy that rule, so clearly, 0 cannot equal to 1. Unless, in some trivial sense, there is only one element in the groups if there's any non-zero element. So this implies that 0 is not equal to 1. Just could have included that as an axiom. Yeah?

AUDIENCE: Assume a and b [INAUDIBLE]

PROFESSOR: Excuse me?

AUDIENCE: Assume a and b, [UNINTELLIGIBLE] does not include 0?

PROFESSOR: Correct. Yeah, you're right. OK. So it follows from this that 1 is not 0.

Yeah. I'm sorry I don't personally have a lot of patience for these fine details. For mathematicians, it's important to keep them all in mind. But my effort is to make these propositions plausible enough so that you can believe them, and you can go back and read a real proof and see that the proof must be correct intuitively, without just mechanically checking it.

OK. Let me just again outline how this works. It's very similar. Again, given any finite field, if we define the integers of the field in this way, we show that eventually they form a cyclic group. Their cyclic group is something that has a single generator. The generator is 1. So eventually it has to cycle for some number n.

Now could n be a non-prime? No, because this is a field, and if n were non-prime, then we would be able to find two integers that multiplied together gave 0. And that's forbidden by the axioms of the field.

So the only possibility is that n is a prime, and in that case, we have found what's called a subfield, a subset of the elements of the field which itself is a field under the field axioms. And the field has p elements, and we already know that every finite field with p elements is isomorphic to Fp. So it can only be that the set of integers is

a subfield which is isomorphic to Fp for some prime p. OK?

So within any finite field, we're always going to find, just by writing out the integers and seeing how they behave under the additive property that there are exactly p of them. So every finite field has a prime called the characteristic. The prime characteristic of the field. This is defined as the characteristic. The size of the integer subfield is the characteristic of the field.

And it has an interesting property, a very important property. Suppose we take this p and we multiply it by any field element called data in the field. By the distributive law, this is just equal to 1 plus 1 plus -- so what do I mean by this? I mean beta -- whenever I write an integer times a field element, I mean beta plus beta plus so forth, p times. But this is equal to 1 plus 1, so forth, by the distributive law, I guess, times theta, p times. And what is this equal to? This is equal to 0. So this is equal to 0 times beta, which fortunately I just told you always must equal 0.

OK. So the conclusion is that if we add any field element to itself p times, we're going to get 0 for all beta in the field where p is the characteristic of the field.

Now in digital communications, we're almost always dealing with a case where the characteristic of the field is going to be 2. The prime subfield is just going to be the two elements 0 and 1. 1 plus 1 is going to be equal to 0.

So subtraction will be the same as addition. And in that particular case, we will have that the sum beta plus beta of any 2 field elements in a field of characteristic two is going to be equal to 0. Just as we had for code words in binary linear codes.

Binary linear codes are not fields, they're vector spaces, but it's a similar property here. You add any element of field of characteristic 2 to itself, and you're going to get 0. So this shows that addition is the same as subtraction. Beta equals minus beta in a field of characteristic 0. Which is a little bit more general.

OK. So we have some fields now, and we find these fields are the only field of prime size, and that every finite field has an important subfield and a prime subfield. And that has important properties, consequences for the field itself.

All right. I think that's everything I want to say about prime fields. Now we go on to the next important algebraic object, polynomials. And again, it's hard to know just how detailed to be, because of course you've all seen polynomials, and you intuitively or formally know something about their algebraic properties, their factorization properties, and so forth. So I'm going to go pretty quickly, and this will be in the nature of a review.

A polynomial -- maybe the simplest way -- how do you define a polynomial? What does it look like? It looks like this. F0 plus F1 times x plus F2 times x squared, so forth, plus Fm times x to the m. That's what it looks like if it's a non-zero polynomial. Or even if it's just -- you could consider all 0 coefficients to be the zero polynomial.

But in general, the convention is, we write f of x equal to that if x is non-zero. What are these f's? These are called the coefficients of the polynomial. And where do they live? We need the coefficients to be in some common field. You've often seen these in the real or complex field. Here they're going to be in finite fields. In particular, very shortly, they're going to be prime fields.

But in general, we'll just say these f's have to be in some field. So we're talking about a polynomial over F where F is some field. So there's always some underlying field if there isn't a vector space. Some similarities between this and vector spaces.

And we usually adopt the convention that Fm is not equal to 0. All right? So we only write the polynomial out to its last non-zero coefficient. In general, this could go up to an arbitrary degree, but well, a polynomial, by definition has a finite degree, which means it has a finite m for which the polynomial can be written in this way. And if the Fm is the highest non-zero coefficient, then we say the degree of f of x is m.

So all polynomials have a finite degrees, except for 1. There is the zero polynomial, which we have to account for somehow. And here we'll just call it f of x equals 0. Informally, it's a polynomial, all of those coefficients are 0. But we'll just define it by its properties. Zero polynomial plus any other polynomial is equal to the identity under addition for the polynomials?

What's the degree of the zero polynomial? Anyone have a definition for the degree of the zero polynomial? Is this well-defined? Undefined? OK. Well, I'll suggest to you that it should be defined as minus infinity. This actually makes a lot of things come out nicely, but it is on the other hand, you don't have to do this. If you like, you can define the degree of 0 to be minus infinity. It's just a convention.

OK. So the set of all polynomials over F0. What's x here? I've got this thing x. What should I think of this as being? Is this an element of a field, or is it something else?

In math, it's usually called an indeterminate. It's just a placeholder. It's something else we stick in order to define the polynomial. It doesn't have a value, in principle.

A comment is made in the notes that with real and complex polynomials, you often think of x as being a real or complex number. In other words, you evaluate the polynomial at some alpha in the real or the complex field by just substituting alpha for x. And in fact, two polynomials are equal if they evaluate to the same value for all the alphas and they're unequal if not true.

When we get to finite fields, it's important this be an indeterminate. Because consider x and x squared as polynomials over the binary field F2. What are the values of these? We'll call this F1 of x equals x, F2 of x equals x squared. Then F1 of 0 is 0 and F1 of 1 is 1. Right? If I evaluate these at field elements, the two field elements, I get 0 and 1. F2 of 0 is equal to 0, and F2 of 1 is equal to 1.

But these are not the same polynomial, all right? So x is not to be considered as a field element. It's to be considered just as a placeholder, a way of holding up these polynomials. It's actually most important in multiplication. But we gather common terms in x. This is the multiplication rule. But it's just something we introduce to define the polynomial.

All right. So the set of all polynomials over F in x, or in x over F, is simply written as F square brackets of x. That's the convention. So that's what I will write when I mean that. And it includes all sequences like this of finite degree, starting at 0, ending somewhere. And also the zero polynomial.

How do you add polynomials? Let's talk about the arithmetic properties of polynomials. You know how to do this. If you have F0 plus F1 plus F2 and so forth, you have some other polynomial doesn't have to be the same degree -- G of x is G0 plus G1 x, up there -- how do you add these together? Component-wise. Sum is F0 plus G0 plus F1 plus G1 x plus 2x squared and so forth. That's an example.

So you basically insert dummy 0's out here above the highest degree term in G. You add them up component-wise. The addition operation is where? In this field, you have addition operation in that failed field, so you can do this. And you get some result which is clearly itself a polynomial. If all the coefficients are 0, you declare that the result is 0. Otherwise the result has some degree. If you add two polynomials with different degree, the degree of the resulting polynomial is going to be the higher degree. If they have the same degree, you could get cancellation in the highest order term, and get a result which is of lower degree, all the way down to 0. All right?

So addition is component-wise the degree of the result is less than or equal to the max degree of the components. So we do addition.

How do we do multiplication? You all know how to do polynomial multiplication. Example. F0 plus F1 of x times G0 plus G1 of x. What do you do? You just multiply it out term by term. F0 G0 plus F1 G0 x plus F0 G1 x plus F1 G1 x squared. You can combine these two together. And that's your answer, which clearly is a polynomial.

So that's one way of doing it, is multiply out term by term, collect the terms. The result of this is that what you get is a convolution for each of the coefficients in the new polynomial. You convolve, just by the ordinary rules of polynomial addition, you can basically turn this around, you convolve it, and you'll get these coefficients. This is written out in the notes.

So we know how to do polynomial multiplication. What are some of its properties? How is this defined again in F? We see we're now going to need the multiplicative of

properties of our field F. All of these products and ultimately convolutions are performed in F. That's why we did these coefficients to be in a field, so we can do all these things.

All right. What are some of the properties? What is the degree of the product of two polynomials? It's going to be the sum of the degrees, right? Provided that both the polynomials are not 0. The highest non-zero term is clearly going to be a term of this kind, and it's going to be a coefficient of x to the sum of the degrees. And since F1 and G1 are both non-zero, by the way we write polynomials, them this highest order term is going to be non-zero.

But we also have to basically have another rule that 0 times f of x is equal to 0. So that's the way we multiply by 0. And how does the degree formula work in this case? Well, this is why I defined the degree of 0 to be minus infinity. So the degree of the product 0 times f of x is -- I've defined this to be the degree of 0 plus the degree of f of x. This is finite. This is minus infinity. So the sum is minus infinity, and so it holds. OK? That's why we defined the degree of 0 to be minus infinity. We don't have to, but it's just so that the sum of the degrees formula continues to work, even if we're multiplying by 0.

Is there a multiplicative identity for polynomials? Yeah. What is the multiplicative identity? 1. OK. So one times f of x is equal to f of x.

So that's one of the properties of a field. Gee. The set of all polynomials over F in x, is this a field? Let's go back and check our field axioms. Under addition, does f of x form an abelian group? Does it have the group property? If we add two polynomials, do we get another polynomial? Do we have cancellation, if F1 plus F2 equals F1 plus F3, is it necessarily true that F2 equals F3?

Yeah, it is. In fact, this looks very much under addition. These look like vectors. If we confine ourselves to the set of all polynomials of degree m or less, we can add them. And it looks very much like the vector space f to the m. Set of all polynomials of degree m or less corresponds to the vector space Fm, which does have the group property under addition.

So in fact, for f of x, yes. It is an abelian group under addition with identity being the 0 polynomial. And all of f of x is an infinite abelian group. If we just take polynomials of degree m or less and restrict Fp to be a finite group, then there are only p to the m elements, and we would have a finite abelian group.

OK. Well. Are the polynomials an abelian group under multiplication? It has an identity. It has all the arithmetic properties you might expect. It's commutative. f of x times g of x is equal to g of x times f of x. So it's abelian.

It has cancellation. f of x g of x is equal to f of x h of x. That's true if and only if g of x is equal to h of x. Is it missing anything? Inverse, right? Very good. Just like the integers. Not all the polynomials have inverses.

Which are the polynomials that do have inverses?

AUDIENCE: [INAUDIBLE]

PROFESSOR: No. There are more than that. So now we're getting into polynomial factorization. And the particular topic is units, which are the invertible polynomials. And what are they? Does the 0 polynomial have an inverse? We're a little unsure, are we? What could it possibly be?

If it had an inverse, this would mean 0 times f of x is -- well, 0 times f of x would have to be a one-to-one map to all of f of x. But it isn't. It simply maps to 0. Doesn't have an inverse.

What about the non-zero polynomials that have degree 0? In other words, the degree 0 polynomial, is simply something that looks like this. fx equals f0, where f0 is not equal to 0.

Is that invertible? Yeah, because f0 is in the field, and it has an inverse. So this has inverse 1 over f of x, if you like, equals just f0 minus 1. 1 over f0. By the rules, you multiply these two things, and you get 1.

OK. So the units in this -- well, I'm sorry. Take a degree 1 or a higher polynomial --

does that have an inverse?

Let's suppose we take a degree 1 polynomial -- say, F0 plus F1 x -- and what I want to find is its inverse. Let's call it g of x. Is it possible to find a g of x such that the product of these two is 1?

Clearly not, because by our degree rule, what is the degree of this product going to be? The degree is going to be the sum of this degree plus this degree, the degree of f plus the degree of g, which is going to have to be at least 1. Provided that g of x is not 0, but clearly g of x is not the solution we're looking for here, either. So this can't be true, and the invertible polynomials are the degree 0 polynomials, which means they're basically the non-zero elements of F. Yes. Considered as polynomials.

AUDIENCE: And how are the [UNINTELLIGIBLE PHRASE]?

PROFESSOR: Yes, indeed.

AUDIENCE: [INAUDIBLE]

PROFESSOR: Ah, no. We haven't introduced modulo polynomials and right. The powers and the indices are the integers from 0 up to some finite number.

OK. It's time to quit. We'll finish this. We'll, I believe, to be able to certainly finish chapter seven, maybe get a little bit into chapter eight, next time, on Wednesday. And we'll see you then.