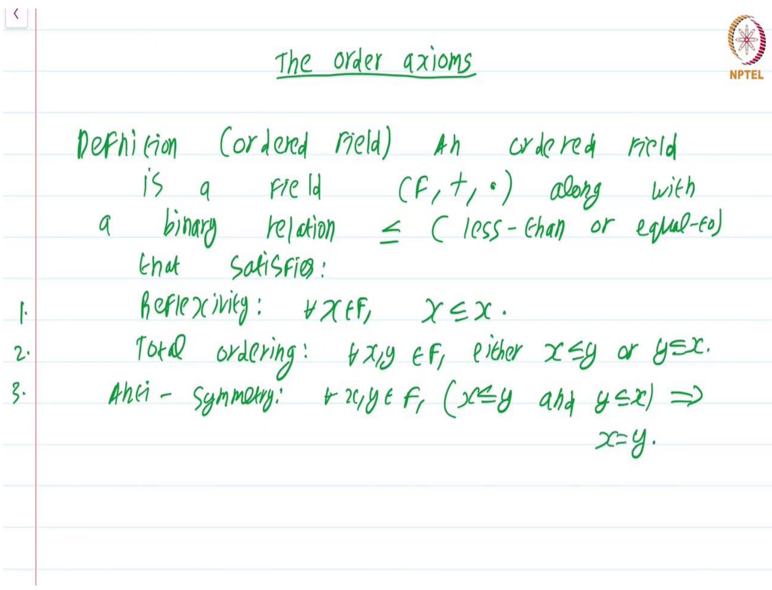
Real Analysis - I
Dr. Jaikrishnan J
Department of Mathematics
Indian Institute of Technology, Palakkad

Lecture – 4.2
Order Axioms

(Refer Slide Time: 00:13)



So, we have seen the field axioms, which give the algebraic properties of an arbitrary field. These axioms are modeled on the familiar properties that are possessed by the rational numbers. Now I mentioned in the last module on the algebraic axioms that, there are even fields that are finite, not only that, they are very important in cryptography. Now I am going to put some more axioms that rules out finite fields also, and at the same time brings forth additional structure to the rational numbers which was so far lacking.

Definition (ordered field): An ordered field, is a field $(F, +, \cdot)$ of course I can denote the multiplication by dot. Last time I did it by times, it really does not make a difference, along with a binary relation which we denote as $\leq$, that satisfies certain axioms:

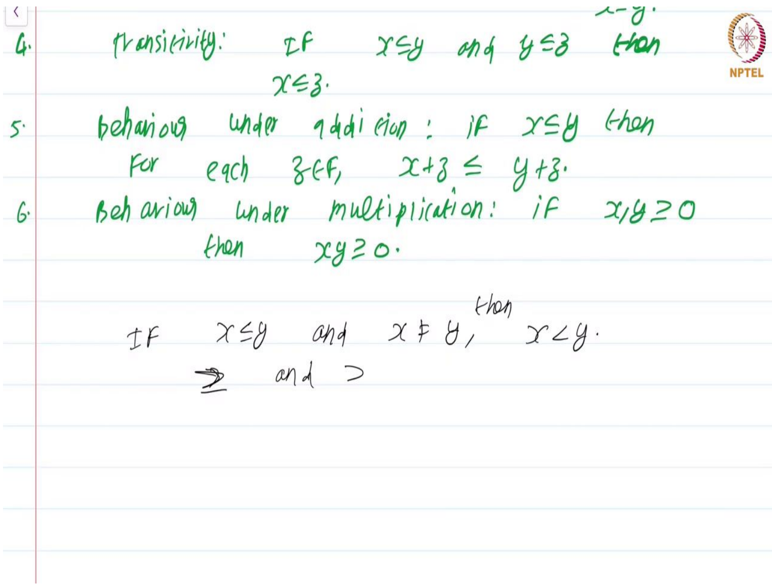
1. Reflexivity: This should remind you of something from the last week, $\forall x \in F,\ x \leq x$.

2. Total ordering: This just says that any two elements are comparable. $\forall x, y \in F$, either $x \leq y$ or $y \leq x$. Note I say either $x \leq y$ or $y \leq x$. But as we have seen in the modules

on logic, whenever we use ‘or’ , we mean inclusive ‘or’. It is possible that both $x \leq y$ and $y \leq x$ and that happens precisely when $x = x$, that is the content of the next axiom.

3. Anti-symmetry says that, $\forall x, y \in F,\ x \leq y$ and $y \leq x$, forces $x = y$; the only element that is less than or equal to itself and greater than or equal to itself is the element itself.

(Refer Slide Time: 03:21)



4. Transitivity: says that if $x \leq y$ and $y \leq z$ then $x \leq z$. This is just the familiar transitive property that you have already seen when we studied equivalence relations. Now, so far the axioms that I have listed does not interact with any of the existing field operations. So, the axioms that I have listed so far is what are known as the axioms of an ordered set. Now I am going to introduce the behaviour under addition and multiplication.

5. Behaviour under addition: which merely says that, if $x \leq y$, then for each $z \in F$, $x + z \leq y + z$.

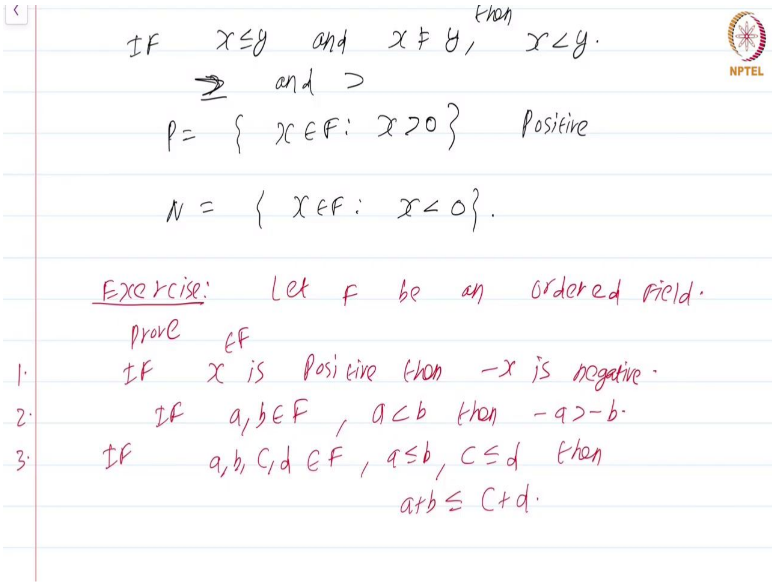
6. Behaviour under multiplication: if $x, y \geq 0$; recall 0 was our notation for the additive identity, then the product $xy \geq 0$. So, this characterizes the properties of an ordered field.

These are the six axioms that we have in addition to the axioms that we listed about the field properties. So, we just set up some notation.

If $x \leq y$ and $x \neq y$ then we write $x < y$.

Note this is just the notation, this is not a theorem or anything, this is just the notation. Similarly we have $\geq$, I leave it to you to formulate what $\geq$ and $>$ are, they are just followed directly from the $\leq$ relation.

(Refer Slide Time: 06:05)



We also call the set $P = \{x \in F : x > 0\}$, this is positive numbers. These are the elements that belong to the set are called positive and similarly we have the set $N = \{x \in F : x < 0\}$.

So, we have that an element of ordered field is either positive, negative or is 0. Now let us, I am going to give you a fairly straightforward exercise; again these are just basic manipulations will give you the proof.

let F be an ordered field, you are now have to prove the following,

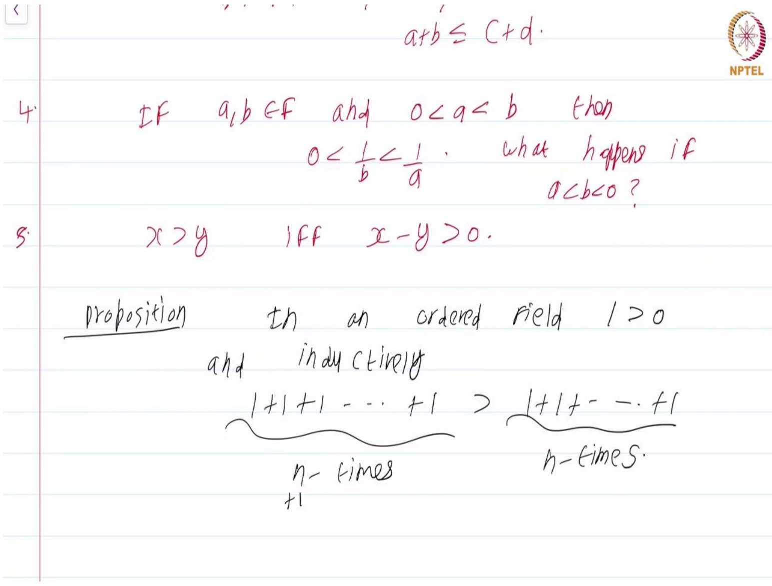
1. If x is positive, then -x is negative.

2. If $a, b \in F$, and you have a < b, then -a > -b.

3. If $a, b, c, d \in F$, and $a \leq b, c \leq d$ then $a + b \leq c + d$.

Note this is just a minor variant of one of the axioms; but still it requires a proof, you cannot just take it for granted.

(Refer Slide Time: 08:20)



4. If $a, b \in F$ and you have 0 < a < b, then $0 < \dfrac{1}{b} < \dfrac{1}{a}$, the reciprocal of a larger number will be smaller. Note that $\dfrac{1}{a}$ and $\dfrac{1}{a}$ are the inverses of a and b; it is another notation for the inverses. What happens if you had a< b < 0? Think about what happens in this scenario?

Another exercise is:

Show that x > y if and only if x - y > 0.

Now in an ordered field, you have familiar properties that you already know from the rational field, but certain things will require a proof. Let me state a proposition,

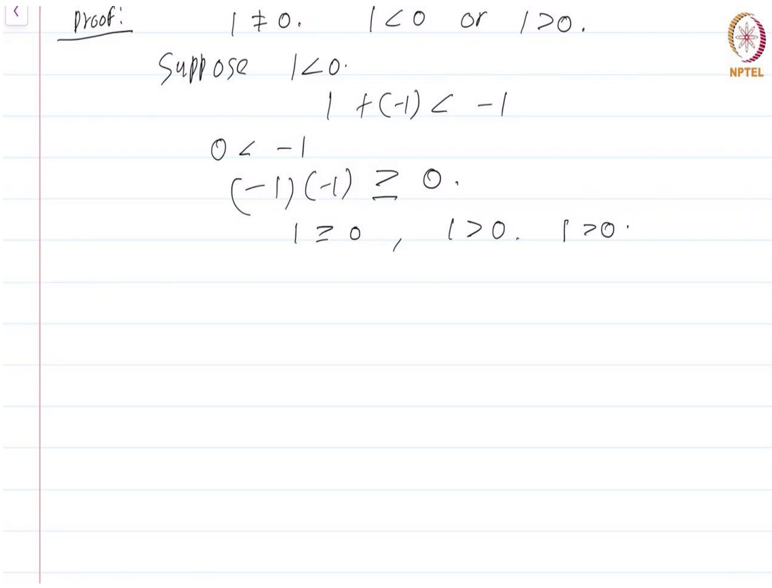
In an ordered field 1 > 0.

So, this I mean, so far what we are proving are all utterly basic and trivial facts; but the thing that you should remember is that, we are doing it in a new structure called an ordered field, where you have specifically listed the properties that the field has and you are trying to derive whatever new property you want just from these basic axioms.

Not only do you have 1 > 0, and inductively,

$$\underbrace{1+1+....+1}_{n+1 times} > \underbrace{1+1+...1}_{n times}.$$

(Refer Slide Time: 11:10)



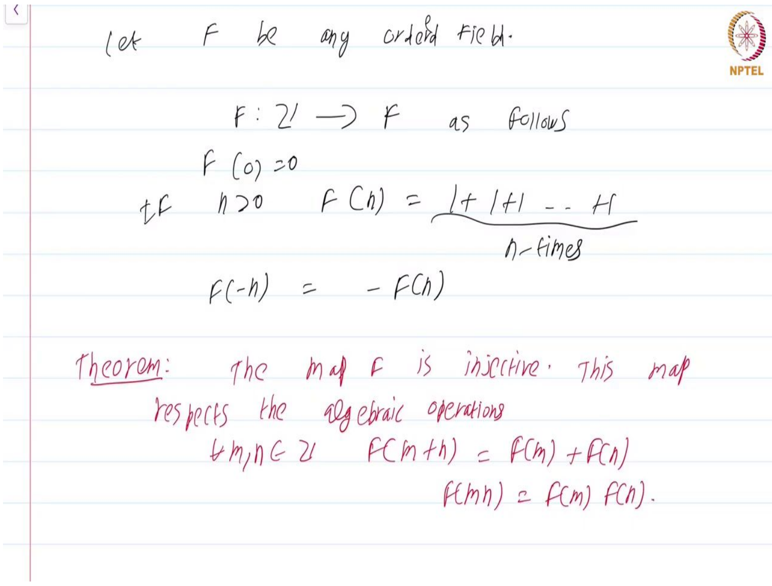
Proof: $1 \neq 0$ because that was one of the hypotheses in the field, field axioms. And by total ordering; that means, either 1 < 0 or 1 > 0. Suppose 1 < 0, then I can add -1 to both sides by one of the field axioms, the behaviour under addition and conclude that 1 + -1 < -1; which in turn gives that 0 < -1 because 1 + -1 is just 0.

Now, what we do is, we use the behaviour under multiplication; we multiply since -1 > 0, $(-1)(-1) \geq 0$. To be precise I can just write $(-1)(-1) \geq 0$, I cannot actually write > 0; but it is not really a problem, because (-1)(-1) is anyway 1. We get $1 \geq 0$. But we already know $1 \neq 0$. So we can actually conclude 1 > 0, which is a direct contradiction to what we started out with. We started out with suppose 1 < 0 and we got 1 > 0. So, this is a contradiction. So, 1 is always greater than 0, that is the conclusion.

Now the second part of the proposition about the inductive behaviour is left as an exercise for you to do.

Now I started off by saying that these axioms of a field , an ordered field are all modeled after the familiar properties that the rational numbers $\mathbb{Q}$ have. So, it is no surprise that we can actually embed $\mathbb{Q}$inside any field, any ordered field. Now it is difficult for me to make these things precise; because we do not have the required background from abstract algebra. So, I will take a simplistic presentation and hope that in your abstract algebra course, you see it in greater detail.

(Refer Slide Time: 13:38)



So, let F be any ordered field, note that I am just saying let F be any ordered field. I am forgetting that there are binary operations + and , and there is a binary relation which is "less than or equal to". In mathematical, it is customary in mathematical literature to just forget that we are dealing with sets that have additional structure; like an addition or a multiplication or an order and just treat the set itself as the one that has all of these built in.

So, I will just say let F be a field with the understanding that there is an underlying addition, there is an underlying multiplication and then there is an underlying "less than or equal to" relation.

Let F be any ordered field, we can define a map from the $\mathbb{Z}$ to F as follows. We just set F(0) = 0, and if n > 0; then we set just $F(n) = \underbrace{1 + 1 + 1 + \ldots + 1}_{n\ times}$. Note that the 1 on the right is the multiplicative identity of the field F and has nothing to do with the one in the integers.

Similarly, we just set F(-n) = - F(n). Again note carefully the minus on the left hand side of this equation is the minus that is coming from the integers; whereas the minus on the right hand side is supposed to be the additive inverse in the field F. Now we have a major theorem the map F.

Theorem: The map F injective. This map respects the algebraic operations.

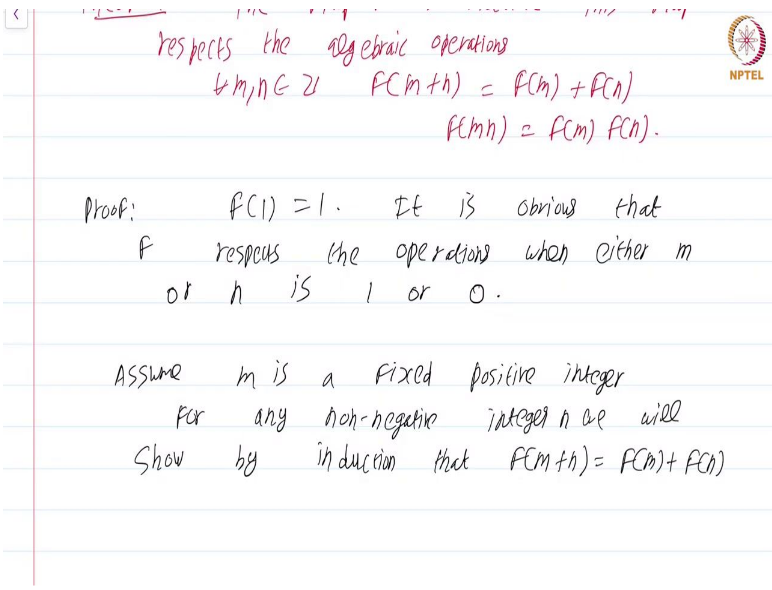
What do I mean by this map respects the algebraic operations? Well, this is where a bit of abstract algebra is required. But let me just give an ad hoc definition; it just means that

$\forall m, n \in \mathbb{Z},\ F(m+n) = F(m) + F(n)$, and

F(mn) = F(m)F(n).

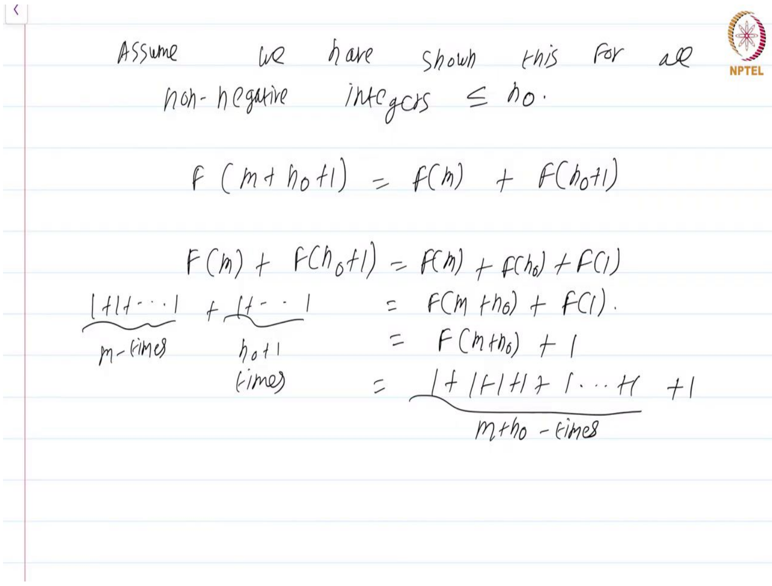
Again note carefully the operations on the left hand side of both equations is the addition and multiplication in the integers; whereas the operation on the right hand side is coming from the field. If you are familiar with a bit of ring theory; what this proposition, what this theorem really says is that, you have an injective homomorphism from the integers into any ordered field.

(Refer Slide Time: 16:44)



Proof: The proof is a bit tricky. So, what we will do is, we will first prove the second part . That the map F respects the algebraic operations; first of all note that F(1) = 1. So, because F(1) = 1, it is obvious that F respects the operations when either m or n is 1 or 0. Just check that when you have either m or n to be 1 or 0; then it is obvious that the operations respect the algebraic structure.

(Refer Slide Time: 17:49)



Now what we will do is, since we have shown this for when m or n is 1 or 0. We will assume that m is a fixed integer, m is a fixed positive integer. And then we will apply induction to show that for any non-negative integer, we will show by induction that F(m + n) = F(m) + F(n).

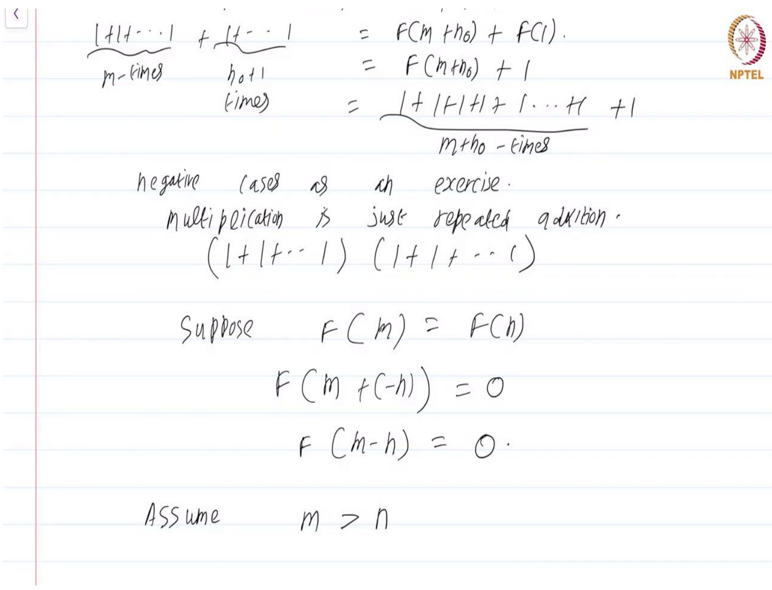
We will show that addition is respected whenever m is a fixed positive integer and you take a non negative integer n. So, assume that we have shown this for all nonnegative integers less than or equal to n_0.

We are going to use proof by strong induction, then we have to show that $F(m+n_0+1) = F(m) + F(n_0+1)$. But observe that the right hand side $F(m) + F(n_0+1)$ is actually $F(m) + F(n_0) + F(1)$. Why is this true? This is true, because the inductive induction hypothesis says that, $F(n_0+1)$ is just $F(n_0) + F(1)$. But now again by the, this is not just, this is not the inductive hypothesis sorry about that; this comes from the fact that whenever you have one of the quantities to be 1 or 0, then the algebraic operations are respected. Now for this to proceed with the proof, what we will do is; we will write this as $F(m+n_0) + F(1)$. Why can we do this? We can do this, because whenever you have a fixed integer m all the way up to n_0, we already know that the result is satisfied.

So, $F(m) + F(n_0)$, I can rewrite as $F(m + n_0)$. But this is the same as $F(m + n_0 + 1)$, this is just $F(m + n_0 + 1)$. But, what is $F(m + n_0 + 1)$? This is just $\underbrace{1+1+1+1+1+....+1}_{m+n_0\ times}$ plus an additional 1; which is obviously equal to the left hand side.

We can argue informally also by writing $F(m) = \underbrace{1+1+1+....+1}_{m\ times}$ and $F(n_0+1) = \underbrace{1+1+1+....+1}_{n_0+1\ times}$ and see that it is equal to LHS also; but the formal argument with induction is needed to make this mathematically precise.

(Refer Slide Time: 21:44)



Now I leave the negative cases as an exercise; it follows immediately from the definition of F(-n) is just -F(n) from that this will follow.

Now, what about multiplication? Multiplication I will just skip, multiplication is just repeated addition, is just repeated addition in the integers, repeated addition. And the same thing is true in the field when you are multiplying elements of the form (1 + 1 +...+ 1 + 1) (1 + 1 + 1+...+ 1); using distributivity you can convert it to repeated additions. So, by using the fact that multiplication is just repeated addition, it is very trivial to prove that the same algebraic, the operation of multiplication is also respected by the map F.

Now let us we, we still have to show that F is injective. So, suppose, F(m) = F(n); then we immediately get F(m +(-n)) = 0 , which means F(m - n) = 0. Now what we will do is, assume m > n. Why can we assume this? Well if not, just interchange the role of n and m, if m < n, then just take n - m instead.

(Refer Slide Time: 24:02)

Suppose $F(n) = F(m)$

$$F(m + (-n)) = 0$$

$$F(m-n) = 0.$$

Assume $m > n$

$$\underbrace{1 + 1 + \cdots 1}_{m-n \text{ times}} = 0.$$

impossible.

$$\mathbb{Z} \subseteq F$$

$1, 1+1, 1+1+1, \ldots$

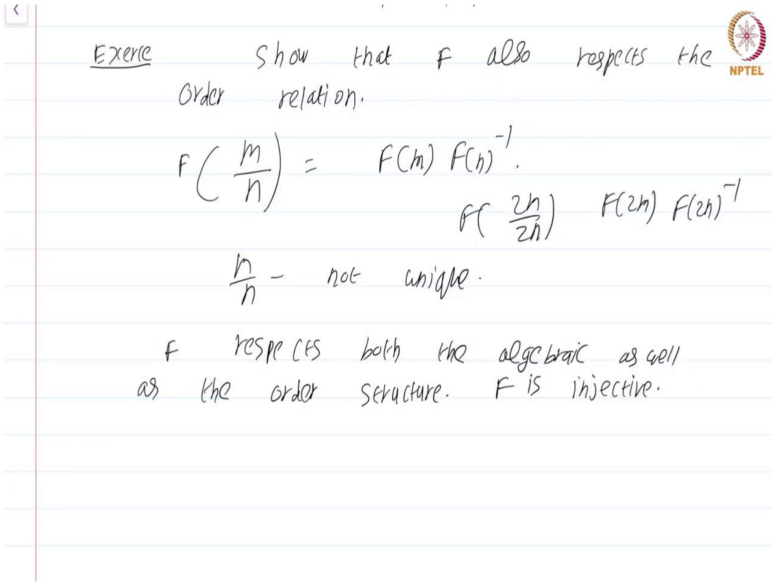
$-1, -(1+1), -(1+1+1), \ldots$

But that means, $\underbrace{1 + 1 + ... + 1}_{m-n\ times}$; but you have just proved as an exercise, as a part of the previous proposition that one is always 1 + 1 +...+ 1 + 1 is always greater when 1 + 1+....+ 1, times lesser and inductively it will be greater than 0, this is not possible, this is impossible, ok.

So, the net conclusion is that, you must have the map F to be injective.

So, the upshot is the integers are actually sitting inside any field in disguise; they are sitting as 1, 1 + 1, 1 + 1+ 1 and the negatives of these, - 1, - (1 + 1), -(1+ 1 + 1),... so on.

(Refer Slide Time: 25:10)



Now I am going to give you one more exercise,

Show that F also respects the order relation.

You have to first formulate what it means for F to respect the order relation, then you have to show that it in fact respects the order relation.

So, we now have a map F on the integers; we can now extend this map F to all rational numbers $\frac{m}{n}$, where $n \neq 0$ in the following way, you can write it as $F(m)F(n)^{-1}$.

Now, there is a bit of checking to do, first of all we have to check that this map is well defined, several problems can arise; F(n) could turn out to be 0, but that is not possible because we have shown that this map F on the integers is injective and only 0 goes to 0. Second thing what can happen is, recall from our discussion on equivalence classes that this representation of rational number $\frac{m}{n}$ is not unique; you can write it as many different rational numbers.

You have to show that the formula on the right hand side does not change, if you change the representation. If you write it as $F(\frac{2m}{2n})$, you should not get a different value of F, it should not turn out that $F(2m)F(2n)^{-1}$ is different that should not happen, it should give the same value in the field, that is also easy to check, but a bit or tedious.

Once this is done, we will know that this map is well defined. And it is not very hard to check that F respects both the algebraic as well as the order structure. F respects both the algebraic structure as well as the order structure and F will be still injective.

In other words, $\mathbb{Q}$ is sitting inside any ordered field in a disguised form; just like the integers are sitting inside any ordered field in a disguised form. In particular, in this discussion we have shown that ordered fields have to be infinite and all ordered fields must contain copies of $\mathbb{Z}$ and copies of $\mathbb{Q}$.

This is a course on Real Analysis and you have just watched the module on Order Axioms.