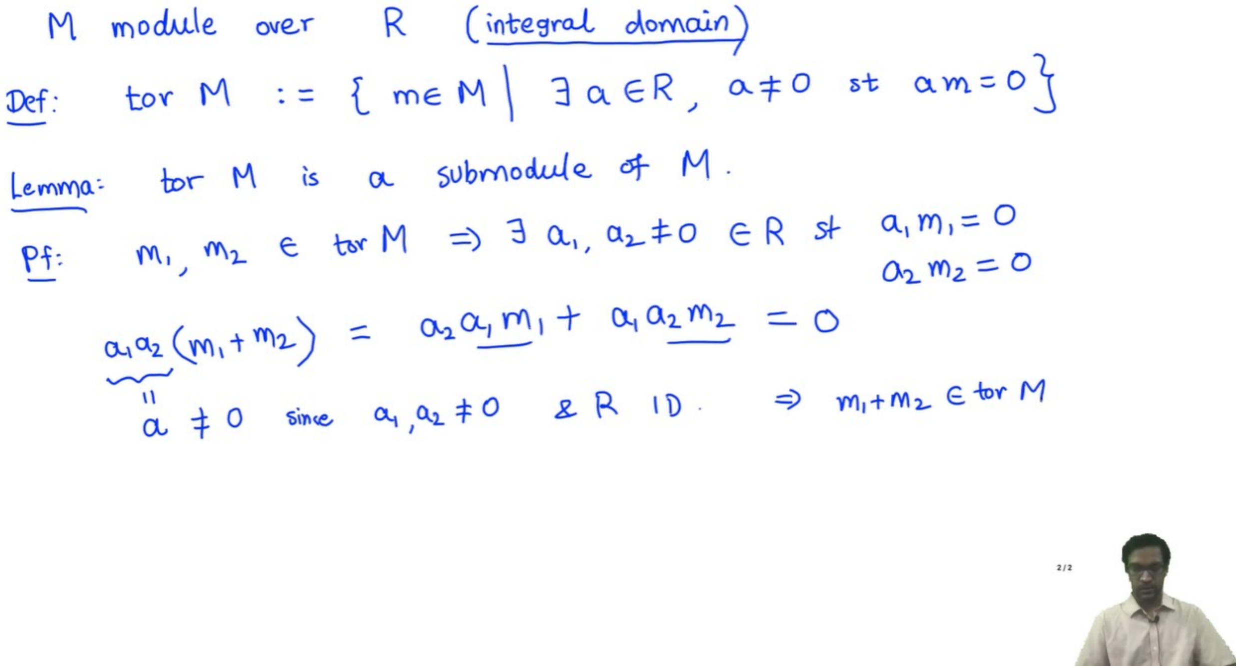
Algebra - I
Prof. S. Viswanath & Prof. Amritanshu Prasad
Department of Mathematics
Indian Institute of Technology, Madras

Lecture 68 [Primary decomposition]

Let us talk about the notion of Primary Decomposition of Modules . So, suppose I have a module M. So, the setup is the following. Suppose M is a module over an integral domain R ok. So, integral domain remember means that R is a commutative ring without any 0 divisors ok. So, if I have a module over an integral domain, then it makes sense to define the following notion. So, here is a definition .

So, it is a subset of M . We will call it tor of M . This is the set of all elements m in M such that there exist a element a in Ra is not 0 such that $am = 0$. So, if I scalar multiply ma , then I get 0 for some non-zero a ok . So, the set of all such elements is denoted tor$M$. So, observe of course 0, the the element 0, the module is certainly in tor of M and in fact, here is a little lemma tor of M is actually a sub module of M. So, tor M is a sub module ok. So, let us check what is this involved . So, we need to check that the hm , well it is closed under addition as well as under scalar multiplication .



M module over R (integral domain)

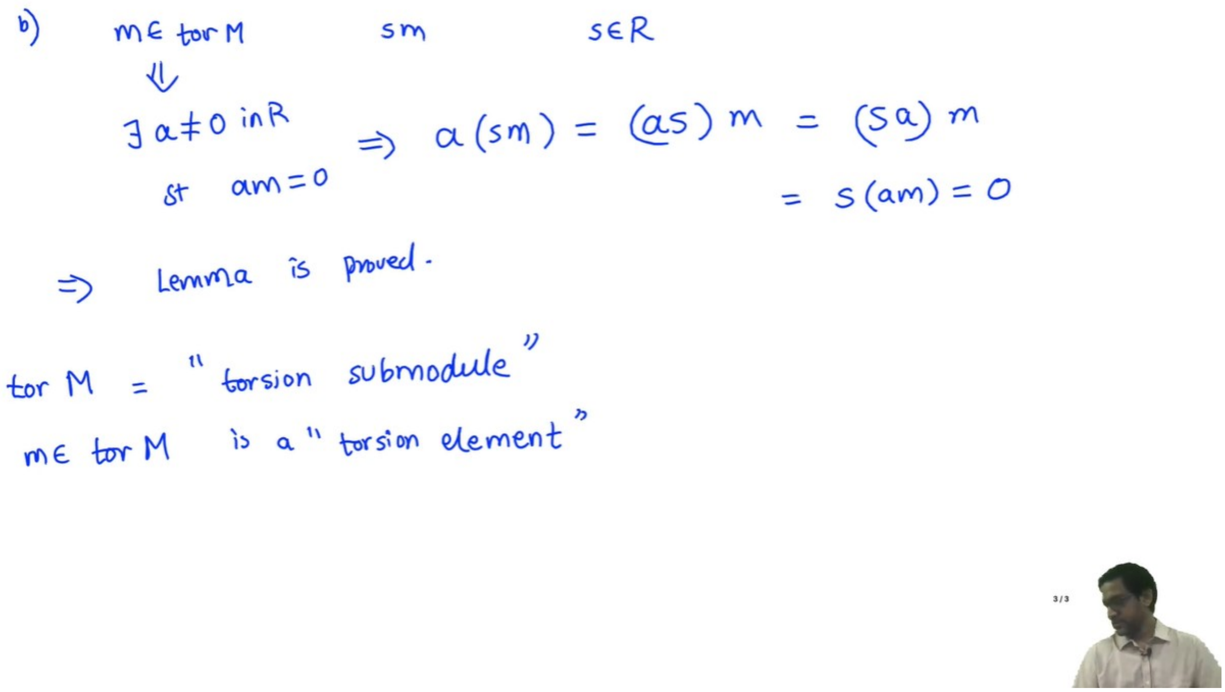
Def: $\text{tor } M := \{ m \in M \mid \exists\, a \in R,\ a \neq 0 \text{ st } am = 0 \}$

Lemma: tor M is a submodule of M.

Pf: $m_1, m_2 \in \text{tor } M \Rightarrow \exists\, a_1, a_2 \neq 0 \in R$ st $a_1 m_1 = 0$
$a_2 m_2 = 0$

$$\underbrace{a_1 a_2}_{\overset{\shortparallel}{a}} (m_1 + m_2) = a_2 a_1 \underline{m_1} + a_1 a_2 \underline{m_2} = 0$$

$a \neq 0$ since $a_1, a_2 \neq 0$ & R ID. $\Rightarrow m_1 + m_2 \in \text{tor } M$



b) $m \in \text{tor} M$ $\quad sm \quad s \in R$

$\Downarrow$

$\exists\, a \neq 0$ in R st $am = 0$ $\Rightarrow a(sm) = (as)m = (sa)m$

$= s(am) = 0$

$\Rightarrow$ Lemma is proved.

tor M = "torsion submodule"

$m \in$ tor M is a "torsion element"

3/3

So, suppose I have two elements m_1 and $m_2 \in \text{tor}M$ what does that mean? It means that you know there exist a_1, a_2 both non-zero elements of the ring R , such that $a_1 m_1 = 0$, $a_2 m_2 = 0$ and now the question is . So, suppose I I now want to show that $m_1 + m_2$ is also in tor M for which I must produce an element a non-zero element which kills $m_1 + m_2$ ok . So, observe that there is a ready made element which will do the job which is the product of a_1 and a_2 . So, if I look at $a_1 a_2(m_1 + m_2)$, so since the ring is commutative I can switch the the order of $a_1 a_2$ as I choose . So, for example, in the first so I will use the distributivity property . In the first term, I will think of it as $a_2 a_1 m_1 + a_1 a_2 m_2$. Now, $a_1 m_1 = 0$, $a_2 m_2 = 0$. So, this is just going to be the element 0 of my module .

The other important observation here is that this scalar a which kills $m_1 + m_2$ let us call it a. This guy is not 0 ok and why is that? Because both a_1 and a_2 were non-zero and the ring was assumed to be an integral domain to start with ok. So, this is an important observation here. Since a_1 and a_2 are both non-zero and the ring R is an integral domain , a itself is not 0 ok. So, what does this imply? This means that $m_1 + m_2$, this element is also in tor of M because it is killed by some non-zero scalar .

Now, similarly we need to look at the the next property which is that if I am given. So, this is just the first axiom of being a sub module second axiom. So, let us go to the next page. So, if I take an element of tor M I need to show that any scalar multiple of that is also in tor M. So, I need to look at any any scalar multiple let me call it sm . Ah s is any element of the ring R . I need to prove that this is also an element of tor M .

Now, if m is in tor M means it is killed by some scalar a . There exists a non-zero in R such that $am = 0$. Now observe that the same a will do the job . Now observe this means that if I look at a acting on sm by the axiom of the the module axiom, this is $(as)m$, but as is the same as sa because the ring is commutative and now that is the same as $s(am)$ and that is of course 0 ok.

Def: If $M = \text{tor}\, M$, then M is said to be a torsion module.

Remark: Fix $m \in M$, $\text{ann}(m) := \{a \in R \mid am = 0\}$

⊙ $\text{ann}(m)$ is an ideal of R.

(Check!)

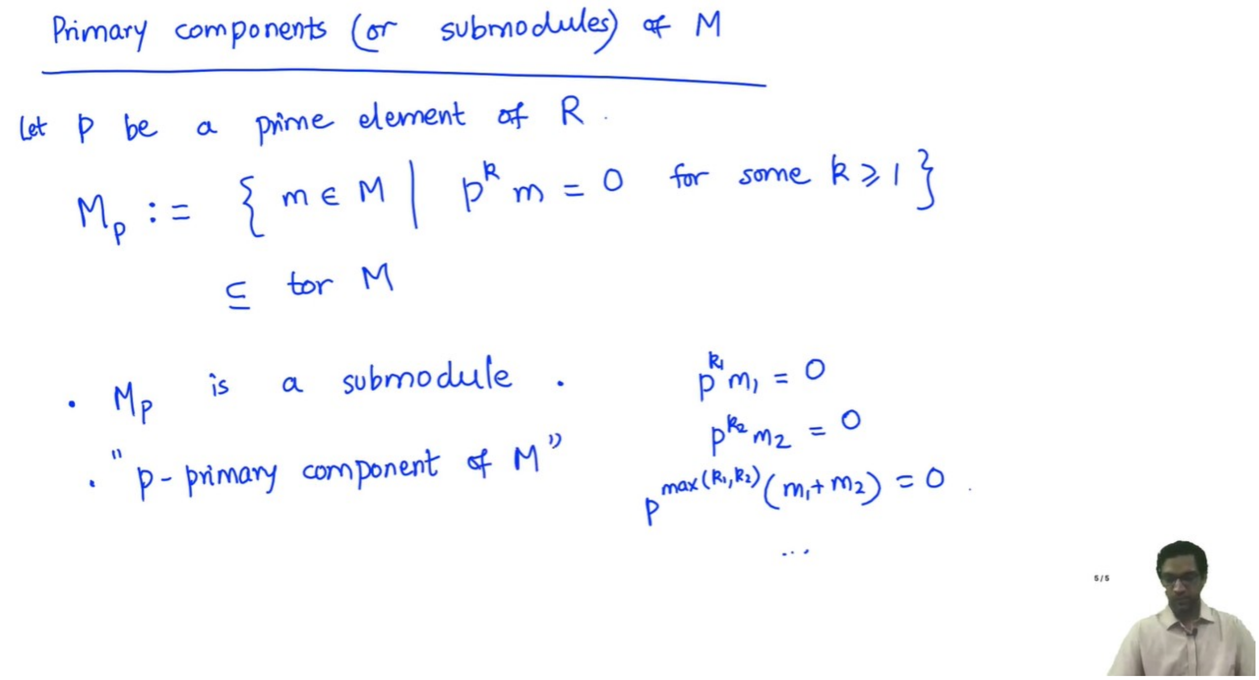
$m \in \text{tor}\, M \iff \text{ann}(m) \neq (0)$.

So, we we keep using the fact that the ring is commutative and also, we use the fact that it is an integral domain . So, what does this mean? So, finally this proves the lemma, therefore the lemma is proved . So, in particular it implies that tor M is a sub module ok. Now, so we call element. So, this is called tor M is usually called the torsion sub module ok. This is called the torsion sub module of m and the elements of tor M are usually called torsion elements. So, if it if I have an element m in tor M is usually called a torsion element , any any element of tor M is called a torsion element ok. So, this is the first little definition and property that we need .

Now if M itself is tor M, so this is the definition if every element is a torsion element . So, if M itself coincides with its sub module tor M, then we say m is a torsion module M is said to be a torsion module ok and another little remark another way of of sort of thinking about this this definition torsion modules . So, we can fix an element. So, fix an element $m \in M$ and define what is called its annihilator. So, the annihilator of that element m is all elements of the ring which annihilated all elements of the ring, such that $am = 0$ ok. So, this is the definition. It is called the annihilator of m and it is an easy exercise which I will leave you to do that this is an ideal.

So, annihilator of any element is always an ideal of the ring is an ideal is an ideal of R ok. So, we had used the fact that R is commutative in this case . So, the annihilator is an ideal and check and the the torsion elements are. So, m is an element of tor M is another way of saying that its annihilator is not the zero ideal. It certainly contains at least one non-zero element ok. So, this is another equivalent way of thinking about torsion elements. They are exactly the elements whose annihilator is not 0 ok.

Now, let me define the the key objects that we will be interested in which are called the primary components or the primary sub modules ok. So, this is like well the definition is very similar. So, so let us do the following. Let P be a prime element of the ring R. So, R is an integral domain and you know what the definition of prime elements are they have the property that if P divides a product ab, then P must divide one of them ok. So, if I have a prime element, then so throughout I am making the same assumption that R is an integral domain and M is a module over R . We can define what is called M sub P, ok.



Primary components (or submodules) of M

Let p be a prime element of R.

$$M_p := \{ m \in M \mid p^k m = 0 \text{ for some } k \geq 1 \}$$

$$\subseteq \text{tor } M$$

- M_p is a submodule.
- "p-primary component of M"

$p^{k_1} m_1 = 0$

$p^{k_2} m_2 = 0$

$p^{\max(k_1,k_2)}(m_1 + m_2) = 0$.

...

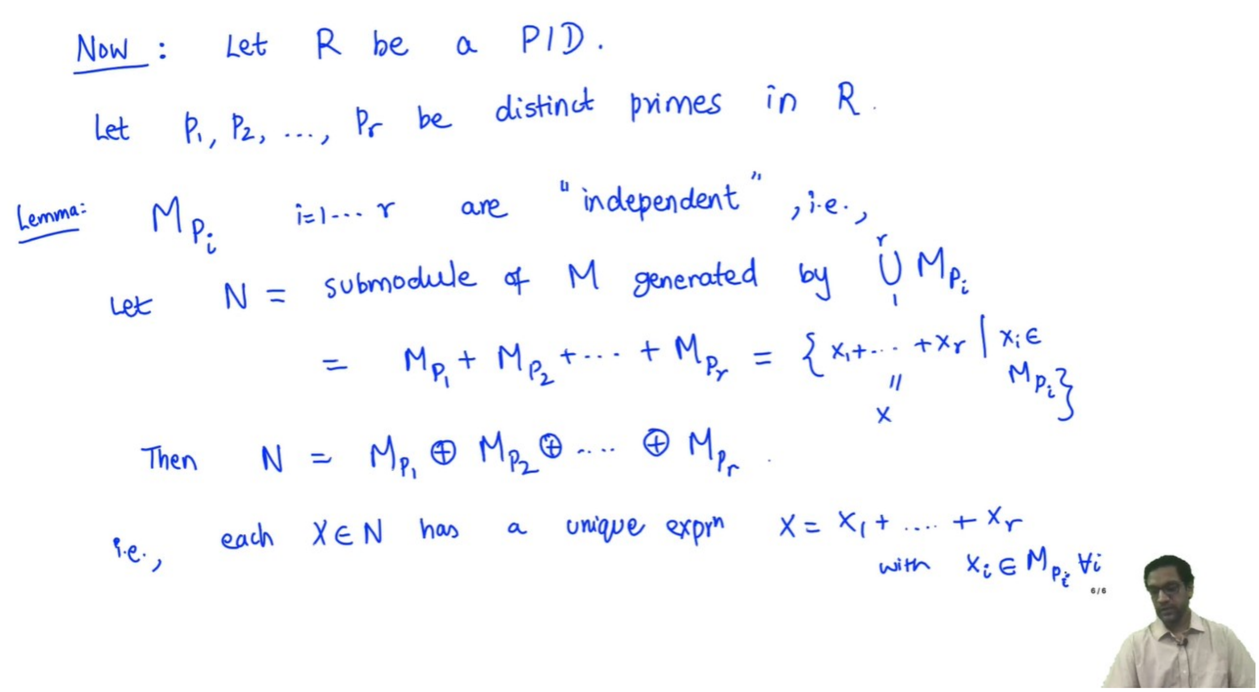
5 / 5

So, what is this? This is almost like the definition of the torsion module. You take those elements of m which are annihilated by sum power of P, such that P^k annihilates m for some k greater than or equal to 1 ok. So, what does this mean ? It is like torsion element some sense. So, so observe the most obvious inclusion here . An element is an M_P . Of course means it is a torsion element because it is killed by some power of P ok and a power of P here since P is non-zero power of P cannot be 0 also ok.

So, this is a special kind of torsion element which are killed by powers of the fixed prime P and the key point here is that M_P is also sub module . So, observe that M_P is a sub module of tor M or mM_P is in fact a sub module . And why is this? Well the proof is almost same as what we did in the case of tor M. So, I will just quickly indicate the proof. Observe if I have two elements m_1 and m_2 and if m_1 is killed by some power of P, $P_1^k m_1 = 0$ is killed by $P_2^k m_2 = 0$, then in this case $m_1 + m_2$ is certainly going to be killed by well certainly the higher of the two is enough.

So, I just need to take $P^{max\{k_1,k_2\}}(m_1 + m_2) = 0$. I do not even need to take the product ok and similarly the other axiom, ok. So, it is a it is a very easy quick check that M_P is in fact a sub module ok and this this sub module is called the P primary component. So, we usually call this the, so this is for the fixed prime P . This is called the P primary sub module or the P primary component of M ok . It is really a sub of tor$M$ rather than all of M ok

Now let us make a further assumption on on R . So, now so I am going to make an additional assumption. Let R be a PID ok a Principal Ideal Domain. So, which means not just an integral domain, but one in which every ideal is generated by a single element ok. So, suppose I have distinct primes now. So, let $P_1, P_2, ..., P_r$ be distinct primes pair wise distinct primes in the ring R . Now, for each of them I can look at the corresponding P primary or P_i primary component ok. So, look at M_{p_i} which is all elements which are annihilated by some



Now : Let R be a PID.

Let $P_1, P_2, \dots, P_r$ be distinct primes in R.

Lemma: M_{p_i} $i=1 \dots r$ are "independent", i.e.,

Let N = submodule of M generated by $\bigcup_{1}^{r} M_{p_i}$

$= M_{p_1} + M_{p_2} + \dots + M_{p_r} = \{ \underset{\overset{\shortparallel}{x}}{x_1 + \dots + x_r} \mid x_i \in M_{p_i} \}$

Then $N = M_{p_1} \oplus M_{p_2} \oplus \dots \oplus M_{p_r}$.

i.e., each $x \in N$ has a unique exprn $x = x_1 + \dots + x_r$ with $x_i \in M_{p_i} \; \forall i$

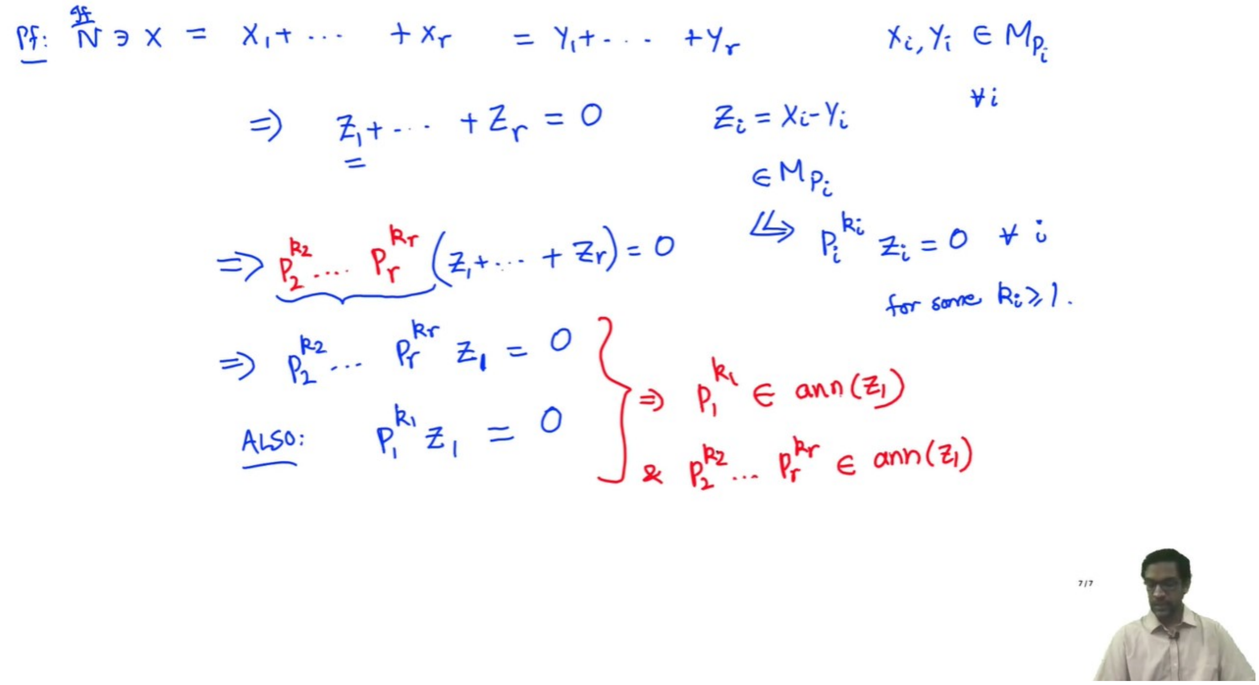
6/6

power of p_i ok. So, these are the primary components I claim that these these sub modules corresponding to distinct primes are. So, then here is the little lemma $M_{p_i}; i$ goes from 1 to r are what we will call independent sub modules .

What does independent mean? Well this is something we encountered while talking about direct products of many sub modules and so on. What it says is that the the sub module generated by these R you know by by $M_{P_1}, M_{P_2}, ..., M_{p_r}$, the union of these that is just their internal direct sum ok. So, let me write this out properly. So, they are independent i e what do I mean? Let N denote the sub module generated by their union. So, let this be the sub module of N of M generated by these mM pis 1 to r. Now what is this really? So, we usually write this like this $M_{P_1} + M_{P_2} + ... + M_{p_r}$. In other words, the sub module is well what does it comprise exactly elements which are of the form $X_1 + X_2 + ... + X_r$ where each $X_i \in M_{P_i}$.

So, this is actually the collection of all sums $X_1 + X_2 + ... + X_r$, where each X_i comes from the appropriate sub module M_{P_i} . So, this is exactly the sub module generated by their union ok . So, let N denote the sub module generated by their union, then N is just the direct sum. The internal direct sum N is actually the internal direct sum of these guys . This is what independence means ok. So, independence just saying that the sort of the sum of those sub modules is actually the direct sum of the sub modules ok and if you recall what this direct sum means going back to the lecture on direct sums and so on.

This just says that if you take an element, so let us call such an element Xwhich is the sum of these X_rs, then X can be written in this manner in a unique way ok. Each element X in in the sum of these sub modules is can be written as $X_1 + X_2 + ... + X_r$ where each $X_i \in M_{P_i}$in a unique manner ok. So, i.e, all this is really unraveling the definition of independence i e what I mean is each $X \in N$ has a unique expression as a sum $X_1 + X_2 + ... + X_r$ with each X_i coming from the appropriate sub module for all i ok. So, this is my definition of independence ok.



$\underline{\text{Pf:}}$ $\overset{\text{If}}{N} \ni X = X_1 + \cdots + X_r = Y_1 + \cdots + Y_r$ $\quad X_i, Y_i \in M_{P_i}$ $\forall i$

$\Rightarrow \underline{Z_1} + \cdots + Z_r = 0 \qquad Z_i = X_i - Y_i \in M_{P_i}$

$\Leftrightarrow P_i^{k_i} Z_i = 0 \ \forall i$ for some $k_i \geq 1$.

$\Rightarrow \underbrace{P_2^{k_2} \cdots P_r^{k_r}}(Z_1 + \cdots + Z_r) = 0$

$\Rightarrow P_2^{k_2} \cdots P_r^{k_r} Z_1 = 0$

$\underline{\text{ALSO:}}$ $\quad P_1^{k_1} Z_1 = 0$

$\Rightarrow P_1^{k_1} \in \text{ann}(Z_1)$

$\&\ P_2^{k_2} \cdots P_r^{k_r} \in \text{ann}(Z_1)$

So, it is *a* lengthy definition, but the proof itself is very simple . So, let us prove this what we need to show? We need to show that if X has two such expressions, then those two expressions coincide ok. So, here is the proof. So, let us suppose X . So, let us pick an $X \in N$. So, let us take $X \in N$ and if possible if this guy has two different such expressions $X_1 + X_2 + ... + X_r = Y_1 + Y_2 + ... + Y_r$ ok where X_i and Y_i come from M_{p_i} for all i , then so as is standard in all these proofs we subtract the two expressions. So, this implies that if I take $X_i - Y_i = Z_i$'s . This means that $Z_1 + Z_2 + ... + Z_r$ 0 where my definition of Z_i it is just $X_i - Y_i$ ok and observe the difference of these two guys also in the module M_{P_i} ok.

So, now I have this now from here I will try and prove that each of the Z is is 0 which is all I need . So, observe that what are these Z is. Well they all belong to the appropriate M pis means the following means that sum power of P_i. So, let me call that power k_i, ${P_i}^{k_i}$ kills Z_i ok. For some numbers $k_i s$ greater than or equal to 1 ok. So, what does this mean ? So, let us start out. I want to prove that Z_1 is 0 for example, ok . So, to do that let us let me do the following. I will multiply this left hand side by ${P_2}^{k_2}{P_3}^{k_3}...{P_r}^{k_r}$ and so on, ok.

So, let let me start here. So, what do we mean $Z_1 + Z_2 + ... + Z_r = 0$. So, let us multiply both sides of this equation by ${P_2}^{k_2}$. This is the scalar, now this is an element of the ring . This is the scalar that I want to use, ok. So, this acting on $Z_1 + Z_2 + ... + Z_r = 0$. Now, observe that if I look at the other term $Z_2, Z_3, ..., Z_r$, each of them is killed by an appropriate power of P_2 right. So, this scalar ${P_2}^{k_2}, ..., {P_r}^{k_r}$. It kills all the terms in this sum except for Z_1 itself ok. So, all the other fellows are 0, Z_1 alone survives its $P_2 P_3$ ${P_r}^{k_r} Z_1 = 0$ ok.

Now, remember however, we also knew that Z_1 was killed by ${P_1}^{k_1}$ ok. So, these are my two equations which will tell me that Z_1 itself must be 0 . Why is this? Because observe these two equations are of the following form . It says that Z_1 is annihilated by two elements ok. So, what does this mean? It says that ${P_1}^{k_1}$ belongs to the annihilator of Z_1 and the the other product ${P_2}^{k_2}...{P_r}^{k_r}$ also belongs to the annihilator ok, but remember these two elements ${P_1}^{k_1}$

BUT $\gcd(p_1^{k_1}, p_2^{k_2} \dots p_r^{k_r}) = 1$

$$\Rightarrow (p_1^{k_1}, p_2^{k_2} \dots p_r^{k_r}) = (1) = R$$

$\Rightarrow$ BUT $(p_1^{k_1}, p_2^{k_2} \dots p_r^{k_r}) \subseteq ann(z_1)$

$$\Rightarrow (\underline{\underline{1}}) = ann(z_1)$$

$$\Rightarrow 1 \cdot z_1 = 0 \quad \Rightarrow z_1 = 0.$$

and $P_2P_3P_r$ to the corresponding k_is . These two elements are relatively prime, right. They do not have any common prime factors here .

So, what does that mean? So, if you recall from the lecture on PIDs and so on .this means that so, but the gcd of these two elements is 1 means that the ideal generated by them . So, look at the ideal generated by these two elements . This ideal is just the whole ring. It is the ideal generated by 1, ok. So, what does that mean? In particular it means that so remember I have I have already said let us go back here. I have said ${P_1}^{k_1}$ belongs to the this belongs to the annihilator and this belongs to the annihilator ok which means that the ideal generated by the two of them is a subset of the annihilator ok. So, I but then that ideal is the whole ring r ok. So, which means that the ring R itself must be the annihilator right so, but remember I know that this ideal generated by these two elements must be contained in the annihilator of Z_1 which means that the annihilator is the whole ring . There is no other way out . In particular it means that the specific element 1 annihilates Z_1 which means that one must annihilate Z_1 . What does that mean? That just means that Z_1 is 0 ok . Now the same proof applies to the to the other elements. You can just replace Z_1 by any of the other zis multiply by the product of all the prime factors other than the ith prime factor, ok. So, the proof works similarly for the other cases ok.

So, that that is the end of the proof. So, what have we proved if you take the the the primary components corresponding to distinct primes are always independent meaning their sum is actually the direct sum ok. Now, that is one thing done that is an important statement. And now here is the the main theorem that we shall be interested in ok which concerns primary components. So, if I have R, so I will put in a few more assumptions. Now if R is a PID that I already used and M is R module, but I need some more adjectives. I want M to be a finitely generated ok torsion module . So, remember torsion module means every element of M is a torsion element. It is killed by some non-zero element of the ring . So, I have I have thrown in these two adjectives. It should be finitely generated and it should be a torsion module, ok over this ring R .

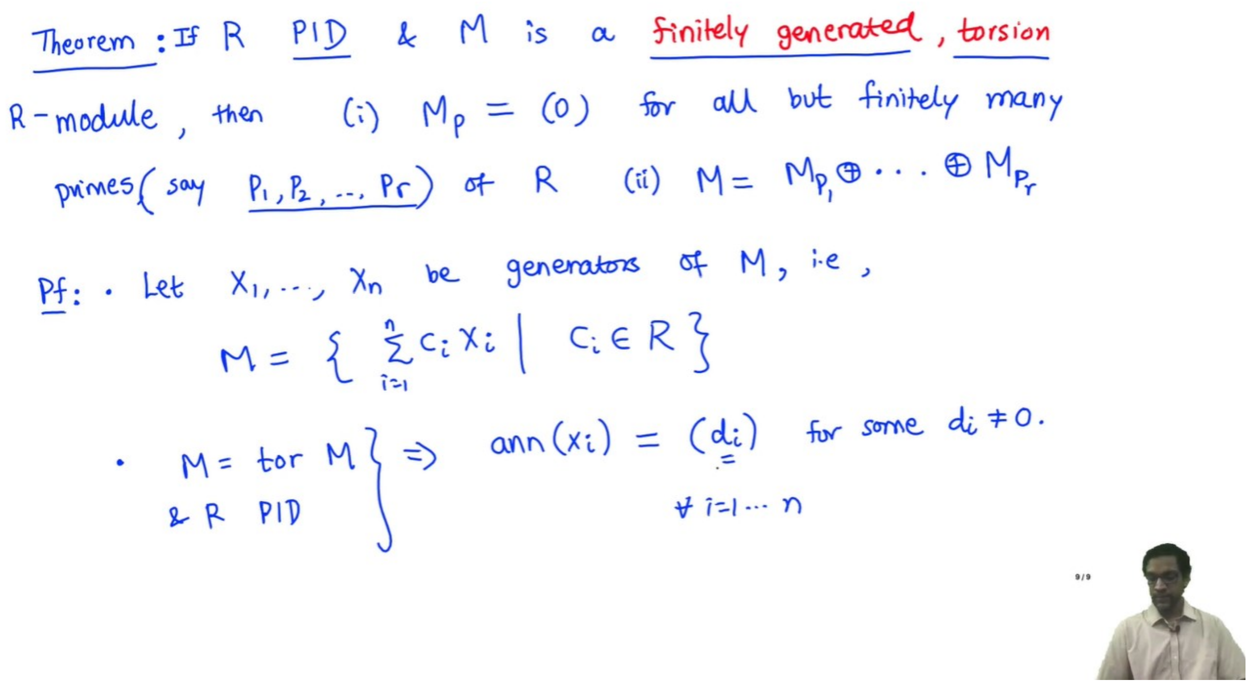
Ah then if R is a PID and M is a finitely generated torsion R module, then two statements one these primary components $M_P = (0)$ for all, but finitely many primes for all, but finitely many . So, notice that the ring itself may have infinitely many primes for all, but finitely many primes P of R ok. The ring may have infinitely many primes, but we are saying that the primary component M_P will be 0 for all for almost all those primes ok except for some finitely many of them and statement two, so let us give these primes a name for all, but finitely many primes P of r. So, let us call these primes $P_1, P_2, ..., P_r$ all, but finitely many primes say $P_1, P_2, ..., P_r$.

So, I will just give the primes a name of r ok . So, $M = M_{P_1} \oplus M_{P_2} \oplus .... \oplus M_{P_r}$ are the the only ones which are non-zero and property two says M is actually the direct sum of these M Pis. You take the non-zero primary components whichever primes give you non-zero answers and the direct sum of those primary components is actually the whole module M ok . So, we we have already developed many of the ingredients we need for this proof . So, so observe that M is finitely generate. So, I am going to use all my hypotheses. So, first let us take let $X_1, X_2, ..., X_r$ maybe not the same are X_n be generators ok. So, remember finitely generated module just means there are finitely many elements such that the sub module generated by these finitely many elements by the set of these elements is the whole model ok. So, let $X_1, X_2, ..., X_n$ be generators of M . What does that mean? In other words, M is just the span ok to use a vector space term, this is just all elements of the form $\sum_{i=1}^{n} C_i X_i$ linear combinations of these generators. The set of all such elements will give you the entire module M ok. Now this is the first assumption that it is finally generated.

Now, let me use my second assumption. I am I am also given that m is tor M ok that m is a torsion module. In particular it means that each of these generators is a torsion element ok . So, which means that each generator X_i is has a non-zero annihilator right . It has it has got at least one non-zero element which annihilates it . And remember in this case I I have assumed that R is a PID, right a principal Ideal Domain . So, and recall I already mentioned the annihilator is a ideal of my ring R, ok. So, it is since the ring is a PID, this ideal must be singly generated ok. There must be a principal ideal ok. So, the annihilator looks like this for some (d_i) which is not 0 ok. So, I have used the fact its M is torsion and R is a PID. So, both assumptions have been used in this step ok and this is for all I this is for all i equals 1 to n .

Now where are we going to manufacture these primes from ? Where what are those finitely many primes? They are going to come from the di's ok. So, look at the dis I have a principal ideal domain which if you recall is also unique factorization domain. I can factorize every element of R uniquely into a product of of powers of primes. So, I look at this prime factorization of all the di's ok. So, consider you know each (d_i) has a prime factorization each (d_i) has a prime factorization . So, I can look at all the primes which occur in the factorizations of all the (d_i)'s ok. So, that is going to be my my set of primes, ok. So, consider the set P . So, consider P prime of r such that P occurs in the prime factorization. In other words, P divides d_i for some i ok. So, I will take the union of the prime factors of all the is, so for some i from 1 to n .

So, take the collection of all primes which divide the di's and this is only a finite set because there are only finitely many di's and each d_i will have some finitely many prime factors ok. So, this this full collection of primes which I get let me call them $\{P_1, P_2, ..., P_r\}$ ok. Now, consider these M_{P_i}'s. The claim is that M is actually the direct sum of these M_{P_i}'s ok. So, I am going to prove the second part of my my theorem which is that I can find finitely many



Theorem: If R PID & M is a finitely generated, torsion R-module, then (i) $M_p = (0)$ for all but finitely many primes (say $P_1, P_2, \ldots, P_r$) of R (ii) $M = M_{P_1} \oplus \cdots \oplus M_{P_r}$

Pf: • Let $X_1, \ldots, X_n$ be generators of M, i.e,

$$M = \{ \sum_{i=1}^{n} c_i X_i \mid c_i \in R \}$$

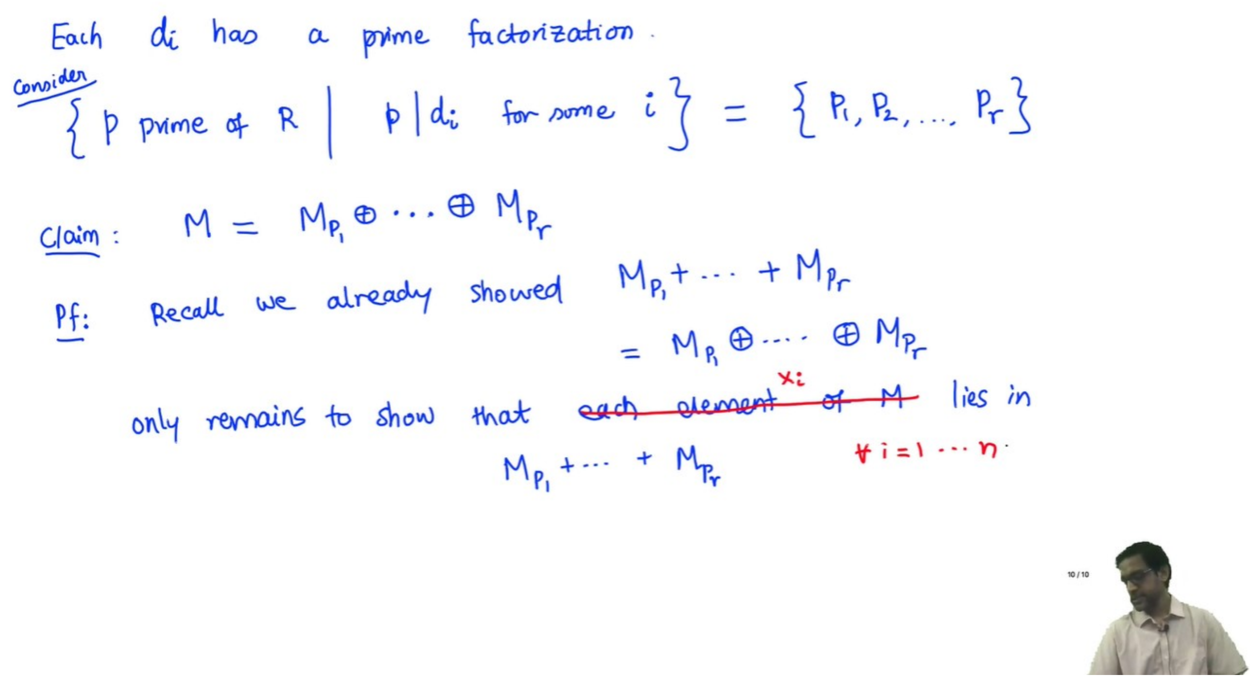
• $\left.\begin{matrix} M = \text{tor } M \\ \& \; R \text{ PID} \end{matrix}\right\} \Rightarrow \text{ann}(x_i) = (\underset{=}{d_i})$ for some $d_i \neq 0$. $\forall\, i = 1 \cdots n$

prime such that M is the direct sum of those guys, then I will show that for all the other primes M Pis actually 0 ok. So, M is the direct sum that is the claim ok. So, let us try and prove this claim now .

So, recall we have already shown independence ok. So, which means that I I know that these M_{P_i}'s their sum is equal to the direct sum that I have already shown, ok. So, proof recall we already showed independence meaning the sub module generated by these components is actually a direct sum ok. So, what remains to show is that this sum $M_{P_1} \oplus M_{P_2} \oplus .... \oplus M_{P_r}$, this is equal to the whole module M ok. So, I need to show that every element of M can be obtained as a sum of elements $X_1 + X_2 + X_r$ coming from the corresponding mis ok. So, only remains to show that each element of M lies in the sum $M = M_{P_1} \oplus M_{P_2} \oplus .... \oplus M_{P_r}$.

And in fact, I do not need to worry about every element of M being the sum. It is enough to prove that the generators belong ok because if once the $X_i$is belong, then every other element is after all linear combination of the X is right. So, they they would also automatically belong . So, it is really a question of showing that the generators belong. So, let me just say I do not even need to do this. I can actually do something simpler. I can just show that the generators X_i only remains to show that X_i lies in this sum for all i equals 1 to 1 ok. So, this is a simpler step. So, let us try proving this ok.

So, now to do this we need a little lemma . So, let me state my lemma first . So, I need to show every generator belongs. So, here is an intermediary step . It is a lemma let a be a non-zero element of R ok and suppose I have an element of M which is annihilated by a such that $aX = 0$ ok, now if a can be written as $a = bc$. Suppose a can be written like this with b and c relatively prime ok, so I am I am able to split a into two pieces and the two pieces are relatively prime , then I can split X into two pieces as a sum of two pieces Y and Z with the following property that Y is killed by b and Z is killed by c ok . So, where what are Y and Z also elements of I should have said with Y, Z belonging to M ok.



Each d_i has a prime factorization.

Consider $\{ p \text{ prime of } R \mid p \mid d_i \text{ for some } i \} = \{ P_1, P_2, \dots, P_r \}$

Claim: $M = M_{P_1} \oplus \dots \oplus M_{P_r}$

Pf: Recall we already showed $M_{P_1} + \dots + M_{P_r}$

$= M_{P_1} \oplus \dots \oplus M_{P_r}$

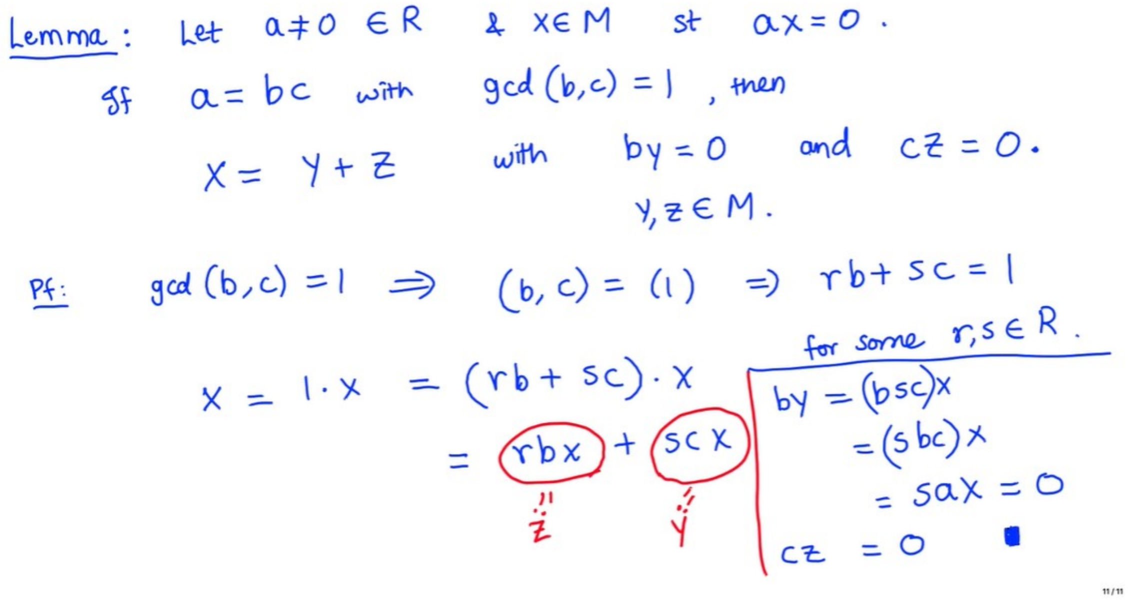
only remains to show that ~~each element of M~~ x_i lies in $M_{P_1} + \dots + M_{P_r}$ $\forall i = 1 \dots n$.

So, what is this? This (Refer time: 31:43) it is an interesting statement. It says that if X is annihilated by a and a can be split into these two pieces, well split now means has a product of two relatively prime elements of the ring, then the element that it annihilates the element X can also be written as a sum of two elements Y and Z, where Y is killed by one part of a that is by b and Z is killed by c ok.

So, it is an interesting little statement and the proof is rather simple . So, observe that since a can be written as b, c with $(b, c) = 1$, so all this is under the same assumption as my theorem that R is a PID . So, observe as before gcd of b and c is 1 means that the ideal generated by b and c is the the whole ring which means the ideal generated by $(b, c) = 1$. The whole ring which implies in particular that I can write some one as a linear combination for some r and s belonging to ring R ok . So, this is the this is the important property that we keep using.

Now, observe that. So, this this is where my splitting is going to come from. So, my element X which I want to split into two pieces. I think of it as one times $1 \cdot X$, I write as $(rb + sc) \cdot X$ ok. So, what is this this is $rbX + scX$ and these are going to be my Y and Z ok. So, let me define Y and Z here. So, this fellow here is going to be y. So, I will define Y to be this element and I will define Z to be this element ok. So, these are my definitions. So, we need to check that these two elements do the job . What does that mean? Well I of course their elements of M is clear, but let us check that they are annihilated by b and c respectively ok.

So, for Y let us check. Suppose I hit Y with b . What is by? Well this is b acting on scx ok, but now I can use my properties of the module, the axioms of a module. This is bscx and use the fact that the ring is commutative think of it as $sbcX$ and sbc is just saX ok because bc is a and $aX = 0$ ok. So, this just shows that $bY = 0$ and the proof for Z is similar. So, you hit c on rb and then combine the b and the c together to get an a. So, this is the same



Lemma: Let $a \neq 0 \in R$ & $x \in M$ st $ax = 0$.

If $a = bc$ with $\gcd(b,c) = 1$, then

$x = y + z$ with $by = 0$ and $cz = 0$.

$y, z \in M$.

Pf: $\gcd(b,c) = 1 \Rightarrow (b,c) = (1) \Rightarrow rb + sc = 1$ for some $r, s \in R$.

$$x = 1 \cdot x = (rb + sc) \cdot x = \underset{\underset{z}{\|}}{rbx} + \underset{\underset{y}{\|}}{scx}$$

$by = (bsc)x$

$= (sbc)x$

$= sax = 0$

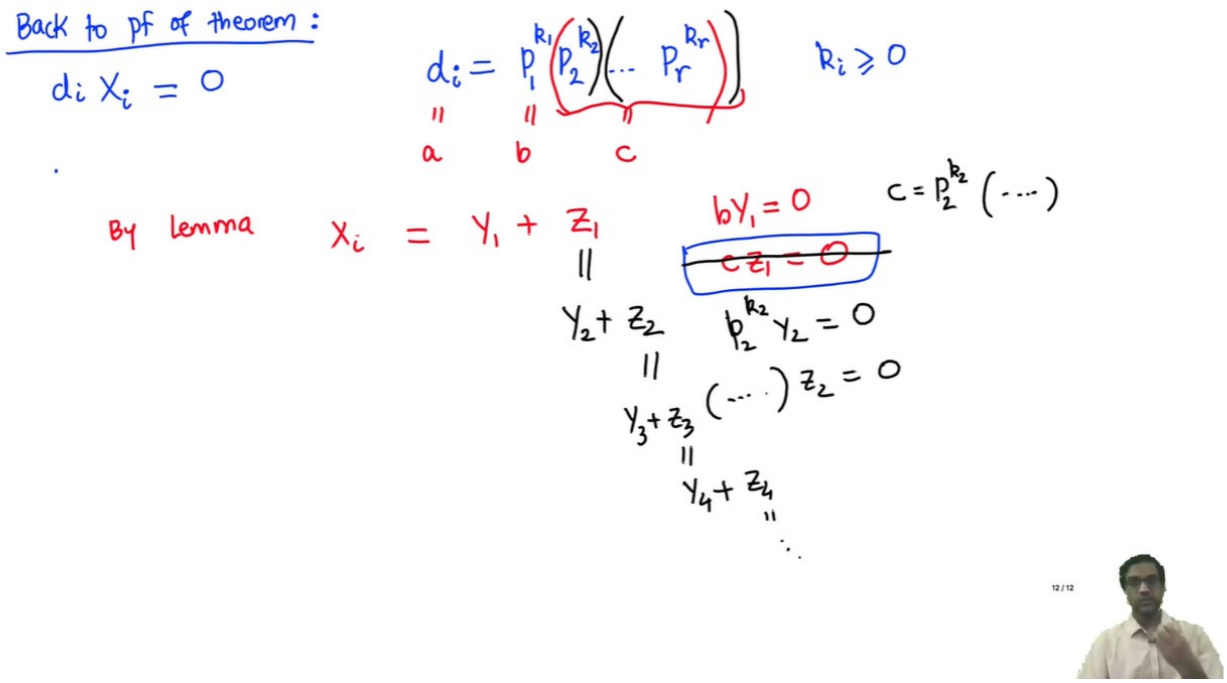
$cz = 0$ ■

11/11

proof ok. So, we are done. So, what this means is that if you have a as a product of bc, then X can also be similarly split in as Y times $ZY + Z$. Now why is this interesting or important for us? Because we are trying to show the following that each element X_i lies in this sum right . What that means is I need to be able to split X_i into several smaller pieces. I need to be able to write X_i as a sum of an element from $M_{P_1}+$ another element from M_{P_2} and so on till an element from Mp_r .

Now, this splitting comes because of this lemma. Why? Bcause the element X_1 is killed by some element d_i right. So, now observe let us go back to the proof of the theorem. So, let us now complete back to the proof of the theorem. So, let us do the proof now back to proof of theorem . So, what we need to do here is to say . Let us look at this element X_i . It is killed by d_i right that is the property we started out with, but d_i it can be written in terms of its prime factorization. So, I just factorize d_i . So, what what is d_i ? It will be some some prime. So, well we have we have call those primes $P_1, P_2, ..., P_r$. So, maybe I will just use that . So, let me say d_i looks like ${P_1}^{k_1}$. So, ok, so just do this. So, I mean the i is and so on are not. So, important anyway. So, let us do this. So, ${P_1}^{k_1}$, ${P_2}^{k_2}$ till ${P_r}^{k_r}$ ok and now of course, not all the primes will occur in the factorization of all the d_i's necessarily.

So, I will just say the ki's could be 0 or some number greater than equal to 0 . So, I take the prime factorization. The key point is that only $P_1, P_2, ..., P_r$ can occur, none of the other primes can occur in this decomposition because that is how I define my primes. I took the d_i's, I factorize each of them and I collected together all the primes that result ok. So, the di is this, this product. Now what does this imply ? Now let us use the lemma. So, by the lemma, so I am now going to first split this di into two pieces. I will look at ${P_1}^{k_1}$ and the rest ok. So, I will think of this as my a sorry to apply the lemma. I will think of this as my a, this as my b and this element as my c ok. B and c remember are relatively prime, a is a



Back to pf of theorem:

$d_i X_i = 0$

$$\underset{a}{\overset{\shortparallel}{d_i}} = \underset{b}{p_1^{k_1}}\,\underbrace{(p_2^{k_2})(\dots p_r^{k_r})}_{c} \qquad k_i \geq 0$$

By lemma $X_i = Y_1 + Z_1$ $\quad bY_1 = 0$ $\quad \boxed{\cancel{cZ_1 = 0}}$ $\quad c = p_2^{k_2}(\dots)$

$$Z_1 = Y_2 + Z_2 \qquad p_2^{k_2} Y_2 = 0 \qquad (\dots) Z_2 = 0$$

$$Z_2 = Y_3 + Z_3, \quad Z_3 = Y_4 + Z_4, \quad Z_4 = \dots$$

12 / 12

product and a which is d_i kills X_i ok. So, now by lemma what can I do? I know that X_i can be split into two pieces I can write it as. So, let me just call it for now $Y_1 + Z_1, bY_1 = 0$, $cZ_1 = 0$ ok.

So, I split into two pieces, but c itself is again a similar sort of thing. It is a product of the remaining primes from P_2 onwards ok. Now I can repeat the analysis with c . What do I mean by that ? So, here is what we will do. We will think of $cZ_1 = 0$. Start with this equation .

Apply the lemma again to c, ok. So, what does c look like? It is this product . Again I split into two pieces. So, let us try using some other color. So, this first term alone is separate, the remaining terms are separate ok. So, when I write c_i will think of writing c as a product of ${P_2}^{k_2}$. So, maybe I will just do this here, c can be written as ${P_2}^{k_2}$ is one term and all the rest is another term, ok and these two are relatively prime again. Apply the lemma it says that if if $cZ_1 = 0$, then Z_1 can be again split into two pieces. So, I will let me call this $Y_2 + Z_2$ ok. Now what property does it have? So, I have replaced this equation by there is an element called Y_2 which is killed by ${P_2}^{k_2}$ and there is the element Z_2 which is killed by the product of the remaining prime factors .

Now repeat the process with Z_2. Z_2 again will split into two pieces, $Y_3 + Z_3$ Z, this will split into two pieces $Y_4 + Z_4$ and so on. So, this is some sort of inductive procedure ok. So, what are you finally doing? You are successively splitting this X_i into smaller and smaller and smaller pieces ok. So, I hope you are convinced that what we get at the end of this process is the final equation. This X_i here has been written as $Y_1 + Y_2 + ... + Y_r$ where each $Y_i$has the following property that $Y_i$or Y_j is killed by the corresponding sum power of P_j. So, P_j power k_j acting on Y_j 0 1 to r ok . And and this implies that Y_j is belong to the corresponding M_{p_j} 's ok. So, this completes the proof because what we have done therefore is to show that each of the generators. So, recall this is what we needed to show here that each of the generators each element X_i of M lies in the sum of these elements ok.

Now, there was still the the other part of the theorem which we needed to prove, right. Let us go up. So, we have we have done this show that M is actually the direct sum, but why why are all the other M_P is 0, ok . Let us just prove that the remaining M_P's are all 0 as a consequence of what we have just proved ok. Still need to show the last bit of the theorem.

Now, let us claim if P_is not one of the P_is then M_P must be a 0 ok. Why is this ? Well again let us see proof. Suppose I have an element in M_P . Suppose X belongs to M_P what does this mean? It means that it is killed by sum power of P, right $P^kX = 0$ for some k greater than equal to 1 . Now we have already shown that X is just the the direct sum of hm you know the M pis. So, let me first write X as X_1+ ok. So, we we can write X as a sum $X_1 + X_2 + ... + X_r$, where each X_i comes from the corresponding M_{P_i} . Now P^kX is therefore $P^kX_1 + ... + P^kX_r$ ok and this is a 0 . That is our assumption, ok.

Now, observe that each of these terms P^kX_1 is in the the first module M_{P_1} right because it is just X_1 multiplied by some sum scalar and this guy is in the final module M_{p_r} and what are we obtaining here that the sum of elements from these different sub modules is a 0 ok, but we have already shown that these sub modules are independent which means that if you know the the element zero, if it can be written as a sum of elements from these modules, each of those those components must be a 0 ok.

So, this means by the independence of the M, M_{P_i} that each of these $P^kX_i = 0$ ok for all i equals 1 to r and why is this by the independence . Now again we are you know we just repeat the familiar argument. What does this mean? It means that P^k belongs to the annihilator of X_i , ok. We we also know that well the annihilator of X_i is d_i ok . So, what does this mean? This says that so $P^{k_i}s$ in the annihilator and so this means that hm I mean we can we can complete the proof in in one of two ways. So, observe that P^k and d_i are are relatively prime here. I mean just to repeat the sort of argument we have used before. So, observe P to the k. So, remember P_is not one of those primes which divides d_i . So, P^k and d_i are actually relatively prime to each other which means that both P^k and d_i are elements of annihilator of x. So, this means that the ideal generated by P^k and d_i must be the whole thing but both of them are are in the annihilator.

So, this means that the ideal generated by them is in the annihilator and like we already did before this means that X_i is 1 is in the annihilator which means X_i is 0 which is a contradiction . So, we we assume to start with that X_i with a non-zero element . I mean they are the non-zero generators ok . So, so I mean the maybe I did not put that into the my initial step of the proof. So, let us go up hm be non-zero . I mean there is no point in taking a zero generator here be non-zero generators of M . So, these di's are are naught units. So, this is this is not the whole whole whole ring here ok. So, that that completes the proof of this theorem. So, this is a this is a very interesting and important theorem. It says that when you have a finitely generated torsion module over a PID, then you know torsion means everything is killed by some element of the ring, but it is actually enough to just look at prime power elements ok. Just look at things which are killed by powers of some primes ok and only finitely many such primes finally matter. All the other guys are 0 and those finitely many primes will you know they they will sort of the the the primary components of those when you take the direct sum, that will give you the whole module M, ok .

$$X_i = y_1 + y_2 + \cdots + y_r \qquad p_j^{k_j} y_j = 0 \quad \forall j = 1 \cdots r$$

$$y_j \in M_{p_j} \qquad ■$$

<u>Claim:</u> $p \neq p_i$ $i = 1 \cdots r$ then $M_p = (0)$.

<u>Pf:</u> $x \in M_p \Rightarrow p^k x = 0$ for some $k \geq 1$.

Write $x = x_1 + \cdots + x_r \qquad x_i \in M_{p_i}$

$$p^k x = \underbrace{p^k x_1}_{M_{p_1}} + \cdots + \underbrace{p^k x_r}_{\substack{\in \\ M_{p_r}}} = 0$$

$$\Rightarrow p^k x_i = 0 \qquad \forall i = 1 \cdots r$$ (by independence of the M_{p_i})

$$\Rightarrow p^k \in \operatorname{ann}(x_i) = (d_i)$$

$$\gcd(p^k, d_i) = 1 \Rightarrow (p^k, d_i) = (1) \subseteq \operatorname{ann}(x_i)$$

$$\Rightarrow 1 \cdot x_i = 0$$

$$\Rightarrow x_i = 0$$ <u>contradiction</u>