Modules over Principal Ideal Domains

Let henceforth R denote a commutative ring with 1. It is called a domain iff it has no zero-divisors, i.e. if $ab = 0$ then either a or b is zero. Or equivalently, two non-zero elements can never multiply to zero. Another way of putting it is that the trivial ideal (0) is prime. We call a domain a principal ideal domain (PID) iff every ideal is generated by one element.

In a PID every ideal is free. Conversely if we have a ring R with a free ideal, this necessarily is generated by one element, because if f, g are two basis elements $0 \neq fg \in Rf \cap Rg$. Thus if we are looking for rings R such that any submodule of a free module is free, R necessarily has to be a PID. The remarkable thing is that this necessary condition is also sufficient.

Let us first start with some general remarks true for all domains R.

Fact 1: *If $\phi : M \to F \to 0$ denotes a surjective map onto a free module, then there is a submodule $0 \to M' \to M$ such that the restriction of ϕ to M' is an isomorphism.*

One says that $\phi : M \to F \to 0$ splits. Indeed we can write M as a direct sum of $\mathrm{Ker}(\phi)$ and M'.

Proof: If f_i is a basis for F chose $e_i \in M$ such that $\phi(e_i) = f_i$. The elements e_i will obviously be linearly independent, as their images are, and they will generate a free submodule M'. (If we define $\psi(f_i) = e_i$ we get a map $\psi : F \to M$ such that $\phi(\psi) = id$, but of course $\psi(\phi) \neq id$)

From now on we will assume R is a domain

Given an R-module M, we say that m is a torsion element if there is $0 \neq r \in R$ such that $rm = 0$. The elements $r \in R$ which kills an element m form an ideal, denoted the Annihilator $Ann(m)$ of m. If m is an element, it generates a cyclic module Rm which is isomorphic to $R/Ann(m)$. The cyclic module Rm is free iff $Ann(m) = 0$.

Now if R is a domain, then the torsion elements form a submodule $T(M)$ - the torsion module of M. If $T(M) = 0$ one says that M is torsion-free

Fact 2: *We can write down the short exact sequence*

$$0 \to T(M) \to M \to M/T(M) \to 0$$

where $M/T(M)$ is torsion-free.

Proof: If $rm \in T(M)$ then $srm = 0$ for some $0 \neq s$, but this shows that $m \in T(M)$ already.

We say that a submodule $0 \to M' \to M$ is saturated if $rm \in M'$ implies that $m \in M'$. The torsion submodule of a module is always saturated.

If $Q(R)$ is the quotient field of R we can form $M \otimes_R Q(R)$. This will kill all the torsion elements. Furthermore if $0 \to M' \to M$ is a submodule of a torsion free module M then the intersection $M' \otimes_R Q(R) \cap M \subset M \otimes_R Q(R)$ gives you the saturation of M' in MBy that is meant the smallest saturated submodule of M containing M'.

The basic fact is the following theorem

Theorem 1 :*Every finitely generated torsion-free module over a PID R is free.*

Remark: Finitely generated is essential. $\mathbb{Q}$ is a torsion-free $\mathbb{Z}$-module, but it is not free. (No two elements are linearly independent, yet $\mathbb{Q}$ is obviously not a cyclic $\mathbb{Z}$ module.

We start with the following technical lemma.

Lemma 1 :*If C is a cyclic submodule of a torsion-free module M and $rz \in C$ then the module generated by C and z is cyclic.*

Proof: If $z \in C$ there is nothing to prove. If $rz = sw$ with w the cyclic generator of C, we can assume that the elements r, s have no common divisor d ((d) a proper ideal) because if otherwise we could write $r'dz = s'dw$ and thus $d(r'z - s'w) = 0$ and because of M torsion free we get $r'z - s'w = 0$. Now assume that $mr + ns = 1$ (By assumption r, s generate the whole of R in particular 1). Consider the element $u = nz + mw$ we get that $ru = w$ and $su = z$. Thus $u \in < C, z >$ is a generator.

We now observe that if M is a finitely generated module over R then M is Notherian. That means we cannot have an infinitely ascending sequence of ideals. In particular any element $m \in M$ will belong to a maximal cyclic submodule Z.

It is now clear how we can proceed by induction. More precisely. We can form an ascending sequence of free submodules M_n defined inductively as follows. In torsion-free M/M_n consider a maximal cyclic Z_n and consider M_{n+1} to be its pre-image in M. As $M/M_{n+1} = (M/M_n)/Z_n$ and the right-hand side is obviously torsion-free (Z_n is saturated) the induction can continue. Note also that if M_n is free, so will M_{n+1} be, by Fact 1. As M is Noetherian the process has to stop after a finite number of steps, and it can only stop at $M = M_N$ for some N.

Corollary: *If M is a finitely generated submodule of a free module it is free.*

We will have occasion to improve on this corollary later.

Now to the second theorem

Theorem 2 :*If M is a finitely generated torsion-module. It can be written as a direct sum of cyclic modules.*

Remark 1: This is not true if finitely generated is not assumes. The simplest example being $\mathbb{Q}/\mathbb{Z}$.

Remark 2: A natural strategy would be to show that every maximal cyclic subgroup of can be 'split off' and then proceed by induction. However, this approach leads to technical difficulties.

First it is convenient to state a general fact for any torsion-module, finitely generated or not.

Let M_p denote $m \in M$ such that $p^k m = 0$ for some k and (p) is a maximal ideal (i.e. p is a prime). Those form sub-modules and we have

Fact 3:*We have $T(M) = \bigoplus_p T(M)_p$*

Proof: If $rm = 0$ then write r as a product of prime-powers. This shows that the sum on the right exhausts $T(M)$. If p, q are different primes, then any powers of each are relatively prime which means $mp^k + nq^l = 1$ for suitable m, n. So if $m \in T(M)_p \cap T(M)_q$ then m is killed by one, hence already dead, i.e. equal to zero.

Thus we can reduce the case to considering modules killed by the powers of a fixed prime p. If M is finitely generated we get that a fixed power of p kills all the elements, by considering the maximum of the necessary powers for each generator. Thus the descending sequence

$$M \supset pM \supset p^2M \supset \ldots p^NM = (0)$$

reaches zero after a finite number of steps.

We can thus argue inductively on a minimal counterexample M.

To say that M is a direct sum of cyclic modules, means that we have generators e_i such that if $\sum_i \alpha_i e_i = 0$ then all $\alpha_i e_i = 0$. (Note that this is weaker than linearly independence where we conclude that all $\alpha_i = 0$. In a torsion module we can never have any non-empty set of linearly independent elements.)

Now let us proceed. We can assume that pM has a basis (in the weaker sense defined above) pf_i. Now the elements f_i will form a basis for a submodule M' containing pM. But we cannot expect M' to be the whole of M. Its image in M/pM which is a vector-space over the field R/pR may not be the whole space. Where do we look for the missing elements? Consider in M the sub-module M_p consisting of elements killed by p (thus not just some power of p. M_p will also be a vector space over R/pR It will contain the subspace $M_p \cap M' = M'_p$ and hence have a complement to that. Choose a basis for the complement (N) and add to the f_i, we only need to show that they generate all of M. Given any element $m \in M$ we can write $pm = \sum_i \alpha_i p f_i$ consider $m - \sum_i \alpha_i f_i$ which will belong to M_p, its component in N will be generated by the g_i.

Note: It would be nice if any lifting of a basis of M/pM would be a basis for M but this is not true. Consider $M = \mathbb{Z}_2 \oplus \mathbb{Z}_4$. The images of the two elements $e_1 = (0, 1)$ and $e_2 = (1, 1)$ form a basis for $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, however they do not form a basis for M as $2e_1 = 2e_2 = (0, 2) \neq 0$

However the following is true

Proposition: *If $e_1, \ldots e_n$ is any lifting of a basis for M/pM they will generate M*

Proof: Given any $m \in M$ we can find α_i such that $m - \sum_i \alpha_i e_i \in pM$. Set $m - \sum_i \alpha_i e_i = pm'$ and apply the same argument on m', this means there are λ_i such that $m' - \sum_i \lambda_i e_i \in pM$. Thus $m - \sum_i \alpha_i e_i - \sum_i p\lambda_i e_i \in p^2M$ and continue.

What will we get? The cyclic submodules will all be of the form R/p^iR and the decomposition will be described by a finite sequence $n_1, n_2 \ldots n_k$ where n_i denotes the number of factors R/p^iR. The natural question is whether that sequence will be determined by the module. To answer this we need to look at this intrinsically.

We first note that the map $x \to px$ will act accordingly on each cyclic summand $C = R/p^kR$.

$$0 \to R/pR \to R/p^kR \to R/p^{k-1}R \to 0$$

We find that

a) $C/pC \equiv R/pR$ and hence $\dim_{R/pR} M/pM = n_1 + n_2 + \dots n_k$
and that
b) each summand R/p^kR is moved to $R/p^{k-1}R$, thus pM is associated to the sequence $(n_2, n_3 \dots n_k)$.

The conclusion is that the numbers $n_1, n_2, \dots n_k$ can be recaptured intrinsically from the numbers

$$\dim_{R/pR} M/pM \geq \dim_{R/pR} pM/p^2M \geq \dim_{R/pR} p^2M/p^3M \geq \dots$$

Note: For each module M we have a surjective linear map $p : M/pM \to pM/p^2M \to 0$ given by multiplication by p. This explains that the numbers are non-increasing.

Note: In the way we constructed the basis for the torsion group, we can order it as follows

$$\begin{array}{llllll}
e_1, e_2 \dots e_{n_1}, & e_{n_1+1} \dots e_{n_1+n_2}, & \dots, & e_{n_1+n_2+\dots n_{k-1}+1}, & e_{n_1+n_2+\dots n_{k-1}+2}, & \dots, e_{n_1+n_2+\dots n_{k-1}+n_k} \\
, \quad , & pe_{n_1+1} \dots pe_{n_1+n_2}, & \dots, & pe_{n_1+n_2+\dots n_{k-1}+1}, & pe_{n_1+n_2+\dots n_{k-1}+2}, & \dots, pe_{n_1+n_2+\dots n_{k-1}+n_k} \\
& \dots \quad \dots \quad \dots & & & & \\
, \quad , \quad , \quad , & p^{k-1}e_{n_1+n_2+\dots n_{k-1}+1}, & & p^{k-1}e_{n_1+n_2+\dots n_{k-1}+2}, & \dots, & p^{k-1}e_{n_1+n_2+\dots n_{k-1}+n_k}
\end{array}$$

The first row gives a basis for the whole module M, while the second gives a basis for pM, the third for p^2M and the last for $p^{k-1}M$ (Note that $p^kM = 0$). We can also think of the first as a basis for M/pM the second a basis for pM/p^2M etc. Finally the 'diagonal' gives a basis for M_p - submodule of elements killed by p. If we include the elements just above the diagonal, we get those that are killed by p^2 and so on.

This gives us a clue as how to write down a matrix A i.e. an element of $\mathrm{End}(M)$ with respect to that basis. The element Ae_1 will be of order p, thus it will be written as a combination of the e_i $(i \leq n_1)$, $pe_i (n_1 < i \leq n_2)$, $p^2e_i (n_2 < i \leq n_3)$,... and similarly for the other basis elements. Thus the matrix A will naturally split up into blocks. If i belongs to level k ($n_{k-1} <\leq n_k$ and j belongs to level l then the entry a_{ij} is of form $p^m a$ where $m = \max(l-k, 0)$ and $a \in R/p^nR$ where $n = \min(k, l)$.

Observe that $\mathrm{Hom}(M \oplus N, P) = \mathrm{Hom}(M, P) \oplus \mathrm{Hom}(N, P)$ and $\mathrm{Hom}(P, M \oplus N) = \mathrm{Hom}(P, M) \oplus \mathrm{Hom}(P, N)$ thus $\mathrm{End}(M)$ splits up as a direct sum of modules such as $\mathrm{Hom}(R/p^kR, R/p^lR)$. Now if 1 is a generator it will land on an element killed by k. This is automatic if $l \leq k$ but if $l > k$ we need to prefigure it with a factor p^{l-k}. Clearly the map is determined by the mage of 1.

Let us consider a specific example, namely let $M = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ and let $e_2, e_4.e_8$ be a basis. A typical element of $\psi \in \mathrm{End}(M)$ will be given by a matrix

$$\begin{pmatrix} 1 & 0 & 1 \\ 2 & 1 & 3 \\ 4 & 2 & 7 \end{pmatrix}$$

We have that $\dim M/2M = 3$ and ψ will induce an element of $\mathrm{End}(M/2M)$ by ignoring possible p-factors in the end and consider the image of a in $R/p^{k-1}R \to R/p^kR \to R/pR \to 0$. This yields

$$\begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

We have that $\dim 2M/4M$ with a basis given by the images of $2e_4$ and $2e_8$. If we had $e_4 \mapsto xe_2 + ae_4 + pbe_8$ and $e_8 \mapsto ye_2 + ce_4 + de_8$ with $x, y \in R/pR, a, b, c \in R/p^2R$ and $d \in R/p^3R$ we get $2e_4 \mapsto a2e_4 + p2be_8$ and $2e_8 \mapsto c2e_4 + d2e_8$ The matrix will be $\begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix}$ where $\bar{x}$ denotes modulo the appropriate power of 2. Not surprisingly the matrix will be $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. In fact given a map $F \in \mathrm{End}(M/pM)$ it induces a unique map $f \in \mathrm{End}(pM/p^2M)$ by the condition $fp = pF$, where p here denotes multiplication by p. Thus $\mathrm{End}(M/pM)$ contains all the information. However it does not contain enough information to recapture $\mathrm{End}(M)$. We have of course that $\mathrm{End}(\mathbb{Z}/4\mathbb{Z}) = \mathbb{Z}/4\mathbb{Z}$ given by any element $d \in \mathbb{Z}/4\mathbb{Z}$ such that $1 \mapsto d$. But $d = d'(2)$ does of course not imply $d = d'$.

Now in the general case we can write this direct sum in its most economical form, by indeed considering maximal cyclic submodules. Such a maximal cyclic factor can be obtained by combining all the primary cyclic factors with maximal length. In this way we get a number d. Then we proceed and split off the next factor which will be associated to a number d_1 dividing d and so on. A simple example will clarify. Given a direct sum decomposition as below

$$\begin{array}{llll} |\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}||\mathbb{Z}/4\mathbb{Z} & \oplus & \mathbb{Z}/4||\mathbb{Z}/8\mathbb{Z}| & |\mathbb{Z}/16\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}| \\ |\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}||\mathbb{Z}/9\mathbb{Z}| & & |\mathbb{Z}/27\mathbb{Z}| & || \\ |\mathbb{Z}/5\mathbb{Z}| & |\mathbb{Z}/25\mathbb{Z} \oplus \mathbb{Z}/25\mathbb{Z}||\mathbb{Z}/125\mathbb{Z}||\mathbb{Z}/625\mathbb{Z}| & & \end{array}$$

We can encode this information more compactly as

prime	1	2	3	4
2	3	2	1	2
3	3	1	1	
5	1	2	1	1

We now pick the highest power from each prime, which are $2^4, 3^3, 5^4$ then we struck it off and get

prime	1	2	3	4
2	3	2	1	1
3	3	1		
5	1	2	1	

We continue and get this time $2^4, 3^2, 5^3$ proceeding we get consecutively
$2^3, 3, 5^2 \quad 2^2, 3, 5^2 \quad 2^2, 3, 5 \quad 2 \quad 2 \quad 2$. Reversing we get

$$2|2|2|60|300|600|18000|270000$$

which presents the torsion group as a sum of 10 cyclic subgroups of increasing lengths. The order of the group is of course the product of all those numbers which

turns out to be

$$3919040000000000000$$

Now we are ready for a more precise statement

Theorem 3 :*Let M be a finite free module over R and let N be a submodule. Then we can find a basis e_i for M such that for suitable d_i we have that $d_i e_i$ is a basis for N. Furthermore we can assume that $d_1|d_2\dots$ with the d_i unique up to units (i.e. the ideals (d_i) are unique).*

Proof: We first replace M with its saturation $\bar{N}$. (As $\bar{N}$ is saturated $F = M/\bar{N}$ is torsion free and hence free and can be split up M and we can write $M = \bar{N} \oplus F'$ for some lifting of F).

Now in $\bar{N}$ consider an element e_1 such that the image $\bar{e_i}$ in $\bar{N}/N$ is a generator of one of the factors (killed by d_1). We would like to claim that Re_1 is a maximal cycle in $\bar{N}$, but if we set $e_1 = \lambda e$ for some e we get $\bar{e_1} = \lambda\bar{e}$ in $\bar{N}/N$ from which does not necessarily follow that $\lambda = 1$ only that $\lambda = 1(d_1)$ which is not good enough. Thus we need to find the cyclic saturation (Z) of Re_1 and rename e_1 as one of its generators. Then it follows that $d_1 e_1 \in N$ and that Rde_1 is also a maximal cyclic in N. We can find a free complement $N_1 \subset N$ to it, and it is easy to check that its saturation $\bar{N_1}$ is likewise a complement to Z in $\bar{N}$. Now we simply proceed by induction, observing that along the way we are creating a basis $e_1, e_2\dots$ for $\bar{N}$ as well as one $d_1 e_1, d_2 e_2\dots$ for N.

Note: The proof above shows that given any maximal cyclic subgroup of a torsion group T, it can be split off. We simply write T as a quotient of a free-module.