Advanced Algebra II

FREE MODULES, MODULES OVER PRINCIPAL IDEAL DOMAIN

We start the discussion of free module and projective modules. Then we work on modules over principal ideal domain. The key result here is that a submodule of a free module over principal ideal domain is again free. As applications, one have an integrated view of *fundamental theorem of finite generated abelian groups* and the *Jordan canonical form.*

Definition 0.1. *Let R be a ring, and M be a module. One can define the notion of "linear independent" and "span" as we did in linear algebra. That is, a subset $X \subset M$ is linearly independent if for any $x_1, ..., x_n \in X$, $\sum r_i x_i = 0$ implies that $r_i = 0$ for all i. A subset $X \subset M$ spans M if every element $x \in M$ can be written as $\sum r_i x_i$ for some $x_i \in X, r_i \in R$. A spanning independent subset is called a basis.*

Example 0.2. *A vector space has a basis. And two basis have the same cardinality.*

Example 0.3. *There is no basis in general. For example, let $M = \mathbb{Z}_4$ be an $\mathbb{Z}$-module. Then there is no independent subset.*

Theorem 0.4. *Let R be a ring with identity and F a unitary ${}_R\mathfrak{M}$. The following are equivalent:*

1. *F has a non-empty basis.*
2. *there is a subset $X \subset F$ such that $F \cong \bigoplus_{x \in X} Rx$ with each $Rx \cong R$ as ${}_R\mathfrak{M}$.*
3. *there is a set X and a function $\imath : X \to F$ satisfying the following "universal property": for all function $f : X \to M$ to $M \in {}_R\mathfrak{M}$, there is a unique ${}_R\mathfrak{M}$-homomorphism $\bar{f} : F \to M$ such that $\bar{f} \circ \imath = f$.*

A unitary ${}_R\mathfrak{M}$ satisfying the above condition is called a free module.

Proof. If F has a basis X, then one can verify that $F \cong \bigoplus_{x \in X} Rx$ with each $Rx \cong R$ as ${}_R\mathfrak{M}$. And vice versa.

Moreover, if there is a subset $X \subset F$ such that $F \cong \bigoplus_{x \in X} Rx$ with each $Rx \cong R$ as ${}_R\mathfrak{M}$. Let $\imath : X \to F$ be the inclusion. One can verify that there is the universal property.

Lastly, if there is a set X and a function $\imath : X \to F$ satisfying the following universal property. We claim that $\imath(X) \subset F$ such that $F \cong \bigoplus_{x \in \imath(X)} R$. To see this, one note that there are $\imath_x : R \to F$ and there are $p_x : F \to R$ by the universal property. Hence one sees that $F \cong \bigoplus_{x \in X} R$. □

Proposition 0.5. *Let $0 \to M \to N \xrightarrow{\varphi} F \to 0$ be a short exact sequence such that F is free, then the sequence split.*

Proof. Let $X \subset F$ be a basis. For each $x \in X$ we pick $a_x \in N$ maps to x. Hence we have a function $f : X \to N$. By the universal property, we have $\bar{f} : F \to N$. One notices that $\varphi \bar{f}|_X = \mathbf{1}_F|_X$. By the uniqueness, $\varphi \bar{f} = \mathbf{1}_F$. Thus the sequence split. ☐

Let F be a free module over R, we would like to define the rank of F, denoted $\operatorname{rank}(F)$, to be the cardinality of its basis. However, this is not always well-defined. We say that a ring with identity has the *invariant dimension property* if the cardinality of two basis of a free module is the same. Hence the rank is well-defined. The following theorem shows that this is well-defined if R is a commutative ring with identity.

Theorem 0.6. *Let R be a ring with identity, $I \lhd (\neq) R$ an ideal. Let F be free module with basis X. Then F/IF is a free R/I-module with basis $\pi(X)$. And $|(\pi(X)| = |X|$. (Where $\pi : F \to F/IF$ is the canonical surjection).*

Remark 0.7. *Let $I \lhd R$ an ideal an $M \in {}_R\mathfrak{M}$. Then $IM := \{\sum a_i x_i | a_i \in I, x_i \in M\}$ is a submodule.*

Moreover, M/IM is a R/I-module by considering $R/I \times M/IM \to M/IM$ sending $(r+I)(x+IM) \mapsto rx + IM$.

Proof. For $u + IF \in F/IF$, we can write $u = \sum r_i x_i$ with $x_i \in X, r_i \in R$. It's clear that $\pi(X)$ spans F/IF.

On the other hand, we claim that $\pi(X)$ is linearly independent. If $\sum (r_i + I)(x_i + IF) = 0$, then $\sum r_i x_i \in IF$. We can write $\sum r_i x_i = \sum a_j y_j$ with $a_j \in I, y_j \in F$. Since X is a basis, each $y_j = \sum b_{ji} x_i$ for $b_{ji} \in F$. Combining all these, one has

$$\sum r_i x_i = \sum_j \sum_i a_j b_{ji} x_i = \sum_i (\sum_j r_i b_{ji}) x_i.$$

By the linear independence of X, we have $r_i = \sum r_i b_{ji} \in I$. Hence $r_i + I = 0 + I$ for all i, it follows that $\pi(X)$ is linearly independent.

It suffices to show that $X \to \pi(X)$ is injective. (It's surjective anyway). This is clear by the independence of $\pi(X)$. For example, if $x_1 + IF = x_2 + IF$, then $x_1 - x_2 + IF = 0x_1 + 0x_2 + IF$ which is impossible. ☐

Corollary 0.8. *Let $R \neq 0$ be a commutative ring with identity. Then R has the "invariant dimensional property".*

Proof. By Zorn's Lemma, there exist an maximal ideal $\mathfrak{m} \lhd R$. For a free module $F \in {}_R\mathfrak{M}$ with basis X_1, X_2, then $\pi(X_1), \pi(X_2)$ are basis of a free $R/\mathfrak{m}$-module F/IF. Note that $R/\mathfrak{m}$ is a field, and hence F/IF is a vector space. Hence

$$|X_1| = |\pi(X_1)| = |\pi(X_2)| = |X_2|.$$

☐

Therefore, for a free module F over a commutative ring with identity. One can define the rank of F by $|X|$, where X is a basis of F.

Theorem 0.9. *Let R be a PID. Then every submodule G of a free module F is free with* $\mathrm{rank} G \leq \mathrm{rank} F$.

Proof. Let $X = \{x_i | i \in I\}$ be a basis of F. We fix a well-ordering $\leq$ on I. Let $i+1$ denote the immediate successor of i. Let $F_i := \sum_{j \leq i} Rx_j$. For convenience, we add an extra element ∞ to I, that is, let $J = I \cup \{\infty\}$ with $\infty \notin I$ and $i < \infty$ for all $i \in I$. Then every element in I has an immediate successor in J. We can write $F = F_\infty$.

Let $G_i := G \cap F_i$. We would like to prove by transfinite induction.

Consider first the case that $\mathrm{rank} F = 1$. $F = Rx \cong R$, $G < F$ is a submodule, hence $G \cong I \lhd R$. R is PID, so $I = (c) = Rc$ for some $c \in R$. The homomorphism $R \to Rc$ is an isomorphism if $c \neq 0$. Thus G is free of rank 0 or 1.

We consider now

$$G_{i+1}/G_i = G_{i+1}/(G_{i+1} \cap F_i) \cong (G_{i+1} + F_i)/F_i < F_{i+1}/F_i.$$

One checks that $F_{i+1}/F_i \cong Rx_i$ is free. Thus, G_{i+1}/G_i is 0 or free.

If $G_{i+1}/G_i = 0$, then $G_{i+1} = G_i$ is free with $\mathrm{rank} G_{i+1} = \mathrm{rank} G_i \leq \mathrm{rank} F_i \leq \mathrm{rank} F_{i+1}$. we are done by transfinite induction.

If G_{i+1}/G_i is free of rank 1. Note that the sequence $0 \to G_i \to G_{i+1} \to G_{i+1}/G_i \to 0$ split. In particular, $G_{i+1} \cong G_i \oplus G_{i+1}/G_i$. We have G_{i+1} is free with $\mathrm{rank} G_{i+1} = \mathrm{rank} G_i + 1 \leq \mathrm{rank} F_i + 1 = \mathrm{rank} F_{i+1}$. ☐

Theorem 0.10. *A finitely generated torsion free module $M \in {}_R\mathfrak{M}$ over a principal ideal domain R is free.*