Math 210B Lecture 18 Notes

Daniel Raban

February 22, 2019

1 Nakayama's Lemma and Structure Theory of Finitely Generated Modules Over PIDs

1.1 Nakayama's lemma and consequences

Lemma 1.1 (Nakayama)**.** *If M is a finitely generated module over a local ring (R, m) such that $M/mM = 0$, then $M = 0$.*

Proof. Let $m_1, \dots, m_n \in M$ generate M. Then $mM = M$, so $m_1 \in mM$; that is there exist $a_i \in m$ such that $m_1 = \sum_{i=1}^n a_i m_i$. So $(1 - a_1)m_1 = \sum_{i=1}^n a_i m_i$. and $1 - a_1 \in R^\times = R \setminus m$. So $m_1 \in \operatorname{span}(\{m_2, \dots, m_n\})$. By recursion, M can be generated by 0 elements, so $M = 0$. $\square$

Corollary 1.1. *Let M be a finitely generated R-module, where (R, m) is local. Let $X \subseteq M$ be such that $\{x + mM : x \in X\}$ generates M/mM as an R/m-vector space. Then X generates M as an R-module.*

Proof. Let $N = Rx \subseteq M$. Then $N + mM = M$. Now $M/N = (N + mM)/N = m(M/N)$. So by Nakayama's lemma, $M/N = 0$, so $M = N$. $\square$

Here's how we use this.

Example 1.1. Do the tuples $(111, 107, 50)$, $(23, -17, 41)$, $(30, -8, 104)$ span $\mathbb{Q}^3$ as a $\mathbb{Q}$-vector space? They will if they span $\mathbb{Z}_{(p)}^3$ for a prime p. By Nakayama's lemma, it suffices to check if they generate $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{Z}/p\mathbb{Z}$. For $p = 3$, the tuples are $(0, -1, -1)$, $(-1, 1, -1)$, and $(0, 1, -1)$. These triples span $\mathbb{F}_3^3$, so the otiginal set spans $\mathbb{Q}^3$.

Lemma 1.2. *Let (R, m) be local, and let M be a finitely generated free module over R. Let $X \subseteq M$. If the image of X in M/mM is R/m-linearly independent, then X is R-linearly independent and can be extended to a basis of M.*

Proof. Let $\overline{X}$ be the image of X in M/mM. Extend $\overline{X}$ to a basis $\overline{B}$ of M/mM. By the corollary, any lift B of $\overline{B}$ spans M, and we can choose B to contain X. We claim that B is R-linearly independent. Say $B = \{m_1, \ldots, m_n\}$. Consider $\sum_{i=1}^n a_i m_i \in M$, where $a_i \in R$ and are not all 0. Let $k \geq 0$ be minimal such that $a_i \notin m^{k+1}$ for some i. Then we have a map $m^k/m^{k+1} \otimes_R M \cong m^k/m^{k+1} \otimes M/mM \to m^k M/m^{k+1}M$. These are both vector spaces over R/m. This map is an isomorphism if $M = R$. In general, $M \cong \bigoplus_{i=1}^n R$, and tensor products distribute over direct sums, so $m^k M/m^{k+1}M \cong \bigoplus_{i=1}^n m^k/m^{k+1}$. Then $\sum_{i=1}^n a_i \otimes m_i \mapsto \sum_{i=1}^n a_i m_i$, so if the latter is 0, so is the former. But $\sum_{i=1}^n a_i \otimes m_i \neq 0$ since the m_i are a basis of M/mM. □

1.2 Structure theory of finitely generated modules over PIDs

Let R be a PID, and let $Q = Q(R)$.

Lemma 1.3. *Any finitely generated R-submodule of Q is cyclic (generated by a single element).*

Proof. If $M \subseteq Q$ is a finitely generated R-submodule ,then $M = \sum_{i=1}^n R\alpha_i$, where $\alpha_i \in Q$. Then there exists a nonzero $d \in R$ such that $d\alpha_i \in R$ for all i. Then $dM \subseteq M$, so $dM = (a)$, where $a \in R$. Since $d : M \to dM$ is an isomorphism, $M = R(a/d)$. □

Proposition 1.1. *Let V be an n-dimensional Q-vector space, and let $M \subseteq V$ be a finitely generated R-submodule. Then there exists a basis $B = \{v_1, \ldots, v_n\}$ of V such that M is a fer R-module with basis $\{v_1, \ldots, v_k\}$ ($k \leq n$).*

Proof. WIthout loss of generality, $M \neq 0$. Take $m_1 \in M \setminus \{0\}$. Then $Qm_1 \subseteq V$ is a 1-dimensional Q-vector space. Then $M \cap Qm_1 = Rv_1$ for some $v_1 \in M$ by the lemma. Let $\overline{M} = M/Rv_1$, and let $\overline{V} = V.Qv_1$. Then $\overline{M} \to \overline{V}$ is an injection. By induction on n, there exist $v_2, \ldots, v_n \in V$ such that $\overline{M}$ is free on $v_2 + Rv_1, \ldots, v_k + Rv_1$ with $k \leq n$, and $v_i + Rv_1$ form a basis of $\overline{V}$ for $2 \leq i \leq n$. Then $M = \bigoplus_{i=1}^k Rv_i$, and $V = \bigoplus_{i=1}^n Qv_i$. □

Corollary 1.2. *Every finitely generated torsion-free module over a PID is free.*

Proof. Let M be a finitely generated torsion-free R-module. Then we have an map $M \to M \otimes_R Q$, which is an injection, since the kernel is $M_{\mathrm{tor}} = 0$. It follows by the proposition that M is free. □

Corollary 1.3. *Any submodule of a free R-module of rank n is free of rank $\leq n$.*

Proposition 1.2. *Let R be a ring, and let $\pi : M \to F$ be a surjection of R-modules with F free. Then there exists a spitting $\iota : F \to M$ such that ι is injection and $\pi \circ \iota = \mathrm{id}_F$. Moreover, $M = \ker(\pi) \oplus \iota(F)$; i.e. F is a direct summand of M.*

Proof. Let B be a basis of F. For each $b \in B$, let $m_b \in M$ be such that $\pi(m_n) = b$. Define $\iota : F \to M$ by $\iota(b) = m_b$ using the universal property of F. We get $\pi \circ \iota = \mathrm{id}_F$ (since linear maps that agree on a basis are equal). Then $\pi(m - \iota \circ \pi(m)) = \pi(m) - (\pi \circ \iota)(\pi(m)) = \pi(m) - \pi(m) = 0$. So $m - \iota \circ \pi(m) \in \ker(\pi)$. So $M = \ker(\pi) + \mathrm{im}(\iota)$. If $m \in \ker(\pi)$ and $m = \iota(n)$, then $0 = \pi(m) = (\pi \circ \iota)(n) = n$, so $m = 0$. So these have trivial intersection, giving us $M = \ker(\pi) \oplus \mathrm{im}(\iota)$. $\square$