# Graduate Algebra, Fall 2014
# Lecture 35

Andrei Jorza

2014-11-21

## 3 Modules

### 3.4 Modules over PIDs (continued)

#### 3.4.1 Free modules (continued)

We'll use twice the following obvious result.

**Lemma 1.** *Suppose $M = M' \oplus M''$ is an $R$-module and $M \subset N$ is a submodule. Then $N = (N \cap M') \oplus (N \cap M'')$.*

*Proof.* If $f$ is projection to $M''$ and $n \in N$ then $f(n - f(n)) = 0$ so $n - f(n) \in N \cap M'$. But $f(n) \in N \cap M''$ and the result follows. $\square$

**Proposition 2.** *If $R$ is a PID and $M$ is a submodule of the free module $N$ of rank $n$. Then $M$ is free of rank $m \leq n$ .*

*Proof.* By induction on $\operatorname{rank}_R(N)$. For rank 1, every submodule of $R$ is a necessarily principal ideal so it is free of rank 1 or 0. Indeed the map $R \to (a)$ sending $r$ to $ra$ is an $R$-module isomorphism for any integral domain.

Suppose we know it for rank $n$ and want to show it for rank $n+1$. Let $v_1, \ldots, v_{n+1}$ be a basis of $N \cong R^{n+1}$ and let $f : N \to R$ be the projection to $Rv_{n+1}$. Then $\ker f = R^n$ is free of rank $n$ and so every submodule of $\ker f$ is free of rank $\leq n$. We get the commutative diagram of exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R^n & \longrightarrow & R^{n+1} & \longrightarrow & R & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & M \cap R^n & \longrightarrow & M & \longrightarrow & f(M) & \longrightarrow & 0 \end{array}$$

The map $f$ yields $R^{n+1} \cong R^n \oplus R$ and the previous lemma shows that $M \cong (M \cap R^n) \oplus f(M)$. Finally the inductive hypothesis gives that $M \cap R^n \subset R^n$ and $f(M)$ are free and so $M$, their direct sum, is also free. $\square$

**Corollary 3.** *If $M$ is a submodule of $N$ as above there exist $a_1 \mid \ldots \mid a_m$ and a basis $y_1, \ldots, y_n$ of $N$ such that $a_1 y_1, \ldots, a_m y_m$ is a basis of $M$.*

*Proof.* Again we prove by induction. For $n = 1$ it is immediate. Suppose we know it for $n - 1$.

Examining the result we see that if $M$ has basis $a_i y_i$ then $a_1$ is the gcd of all the basis elements of $M$ and thus of all the elements of $M$. Therefore we seek $a_1$ this way.

For $f \in \operatorname{Hom}_R(M, R)$ the image $f(M) \subset R$ is an principal ideal $(a_f)$. Consider the collection $S = \{(a_f) | f \in \operatorname{Hom}_R(M, R)\}$. The ring $R$ is a PID and so is Noetherian which implies that every ascending chain of ideals is stationary and thus has a maximum. Zorn's lemma therefore implies that the set $S$ has a maximum element $(a_1) = (a_f)$ so $f(M) = (a_1)$ for some $f \in \mathrm{Hom}_R(M, R)$. Let's in fact show that $a_1$ is then a gcd for all the elements of $M$.

Since $(a_1) = f(M)$ there exists $m \in M$ such that $f(m) = a_1$. Pick any other $g \in \mathrm{Hom}_R(M, R)$. We first show that $a_1 \mid g(m)$. If $d = \gcd(a_1, g(m))$ there exist $r, s$ such that $d = ra_1 + sg(m) = rf(m) + sg(m)$. Take $h = rf + sg \in \mathrm{Hom}_R(M, R)$. Note that $h(m) = d$ so $(a_1) \subset (d) \subset h(M)$. But $(a_1)$ was maximal in $S$ and certainly $h(M)$ is in $S$ so $(a_1) = h(M)$ and therefore $(a_1) = (d)$ which implies that $a_1 \mid g(m)$ as desired.

Suppose $v_1, \ldots, v_n$ is a basis of $R^n$. Then $m = \sum \alpha_i v_i$. Let $g_i$ be projection to the coefficient of $v_i$. The above shows that $a_1 \mid g_i(m) = \alpha_i$ so $\alpha_i = a_1 c_i$ and so $m = \sum a_1 c_i v_i$. Write $y_1 = \sum c_i v_i$ in which case $m = a_1 y_1$. Then $a_1 = f(m) = a_1 f(y_1)$ so $f(y_1) = 1$.

I claim that $R^n \cong \ker f \oplus Ry_1$. Suppose $x \in R^n$. Then $f(x - f(x)y_1) = 0$ as $f(y_1) = 1$ and so $x - f(x)y_1 \in \ker f$. Moreover, for the same reason, $\ker f \cap Ry_1 = 0$ and the conclusion follows. Now the lemma shows that $M \cong (M \cap \ker f) \oplus (M \cap Ry_1)$.

Note that if $x = ay_1$ for some $x \in M$ then $f(x) = a$ is divisible by $a_1$ and so $M \cap Ry_1 = a_1 y_1$. By the inductive hypothesis we can find a basis $y_2, \ldots, y_n$ of $\ker f$ and $a_2 \mid \ldots \mid a_m$ such that $a_2 y_2, \ldots, a_m y_m$ is a basis of $M \cap ker f$. Thus $a_i y_i$ is a basis of $M$.

It suffices to check that $a_1 \mid a_2$. If $g$ is projection to $y_2$ in $\mathrm{Hom}_R(M, R)$ then $g(M) = (a_2)$ which must be contained in $(a_1)$. (If not take the gcd and the argument from the above yields a contradiction.) $\square$