# Graduate Algebra, Fall 2014 <br> Lecture 34 

Andrei Jorza

2014-11-19

## 3 Modules

### 3.3 Noetherian rings and modules (continued)

Theorem 1 (Hilbert basis theorem). If $R$ is a Noetherian ring then $R[X]$ is a Noetherian ring. Inductively, $R\left[X_{1}, \ldots, X_{n}\right]$ is a Noetherian ring for all $n \geq 0$.

Proof. Let $I$ be an ideal of $R[X]$. We want to show that $I$ is finitely generated as an $R[X]$-module but we'll do something better: we'll show that it is finitely generated as an $R$-module, i.e., there exist $M_{i} \in R[X]$ such that $I=R M_{1}+\cdots+R M_{n}$ in which case $R[X] M_{1}+\cdots+R[X] M_{n}=R[X] I=I$. We'll do this as follows: we will find a finitely generated $R$-module $J$ containing $I$. Since $R$ is a Noetherian ring and $J$ is finitely generated it follows that $J$ is Noetherian. But then every $R$-submodule of $J$ (including $I$ ) is finitely generated over $R$ and the conclusion follows.

For a polynomial $P(X)=a_{0}+a_{1} X+\cdots+a_{n} X^{n}$ let $i(P)=a_{n}$. Let $i(I)=\{i(P) \mid P \in I\}$. Then $i(I)$ is an ideal. For $r \in R$ have $r i(P)=i(r P)$. If $\operatorname{deg} P \leq \operatorname{deg} Q$ then $i(P)+i(Q)=i\left(P X^{\operatorname{deg} Q-\operatorname{deg} P}+Q\right)$ and so $i(I)$ is an ideal of $R . R$ is a Noetherian ring so $i(I)=\left(a_{1}, \ldots, a_{n}\right)$ is finitely generated and let $P_{i} \in R[X]$ such that $i\left(P_{i}\right)=a_{i}$. Let $r=\max \operatorname{deg} P_{i}$.

We choose the $R$-module $J$ generated by $P_{1}, \ldots, P_{n}, 1, X, \ldots, X^{r-1}$ so $J=\sum R P_{i}+\sum_{i=0}^{r-1} R X^{i}$. Let's show that $I \subset J$.

Suppose $P(X) \in I$ of the form $P(X)=b_{0}+b_{1} X+\cdots+b_{m} X^{m}$. We'll show that $P(X) \in J$ by induction on $m$. If $m<r$ the already $P \in J$. Suppose now that $m \geq r \geq \operatorname{deg} P_{i}$ for all $i$. Write $b_{m}=\sum u_{i} a_{i}$. Then $P(X)-\sum u_{i} P_{i}(X) X^{m-\operatorname{deg} P_{i}} \in I$ has degree $\leq m-1$. By induction we deduce that $P(X)-\sum u_{i} P_{i}(X) X^{m-\operatorname{deg} P_{i}} \in J$ but then $P(X) \in J$ as desired.

Thus $I \subset J$ as an $R$-module and the argument from the beginning of the proof yields that $I$ is finitely generated as an $R$ and thus also as an $R[X]$-module. We deduce that $R[X]$ is a Noetherian ring.

### 3.4 Modules over PIDs

In this section we'll prove the following theorem.
Theorem 2. If $R$ is a PID and $M$ is a finitely generated module over $R$ then there exists $r \geq 0$ and $x_{1}, \ldots, x_{n} \in R$ such that

$$
M \cong R^{r} \oplus R /\left(x_{1}\right) \oplus \cdots \oplus R /\left(x_{n}\right)
$$

where $x_{1}|\ldots| x_{n}$.
Corollary 3. Specializing to $R=\mathbb{Z}$ and knowing that abelian groups are $\mathbb{Z}$-modules we get the classification of finitely generated abelian groups.

### 3.4.1 Free modules

Definition 4. Suppose $R$ is an integral domain and $M$ is an $R$-module. The rank $\operatorname{rank}_{R}(M)$ of $M$ is the largest number of $R$-linearly independent elements of $M$.

Lemma 5. Any $n+1$ elements of $R^{n}$ are linearly dependent and so $\operatorname{rank}_{R}\left(R^{n}\right)=R$.
Proof. Pick $m_{1}, \ldots, m_{n+1} \in R^{n} \subset(\operatorname{Frac} R)^{n}$ which is a vector space. Thus $v_{i}$ are Frac $R$-linearly dependent and, clearing denominators, they are $R$-linearly dependent.

Proposition 6. 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 . 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 $f: N \rightarrow R$ be the projection to $R v_{n+1}$. Then ker $f$ is free of rank $n$ and so every submodule of $\operatorname{ker} f$ is free of rank $\leq n$. Thus $M \cap \operatorname{ker} f$ is free of rank $m \leq n$ and let $u_{1}, \ldots, u_{m}$ be a basis of $M \cap \operatorname{ker} f$.

To be continued.

