Graduate Algebra, Fall 2014
Lecture 32

Andrei Jorza

2014-11-14

3 Modules

3.1 Basics

Definition 1. A **module** over a ring R is an abelian group M together with a binary scalar multiplication $R \times M \to M$ such that $r(m+n) = rm + rn$, $(r+s)m = rm + sm$, $r(sm) = (rs)m$ and $1m = m$.

Example 2.

1. Any vector space over a field F is a module over F.
2. Any ideal I of a ring R is a module over R.
3. If I is an ideal of R then R/I is a module over R.
4. Any abelian group is a $\mathbb{Z}$-module.
5. A more exotic example. $R = \mathbb{R}[X]$ and $M = C^\infty(\mathbb{R}, \mathbb{R})$. Define $P(X) \cdot f$ as the function $(P(X) \cdot f)(x) = (P(\partial/\partial_x)f)(x)$. Then M is an R-module.
6. $R[X]$ is an R-module for all rings R.

Definition 3 (Direct sums)**.** Suppose $\{M_i\}_{i \in S}$ is a collection of R-modules where S is some indexing set. Define $\oplus_{i \in S} M_i$ as the set of tuples $\{\oplus m_i | m_i \in M_i\}$ such that all but finitely many of the m_i are 0. Then $\oplus M_i$ is an R-module with component-wise addition and scalar multiplication.

Definition 4 (Free modules)**.** A free R-module is any module of the form $\oplus_{i \in S} R$ where S is any indexing set. Finitely generated free modules are of the form R^n.

Example 5.

1. Free abelian groups are free $\mathbb{Z}$-modules.
2. Every module over a field, being a vector space, is free.

Definition 6. A homomorphism of R-modules is a map $f : M \to N$ which is a homomorphism of underlying abelian groups such that $f(rm) = rf(m)$. Write $\mathrm{Hom}_R(M, N)$ for the abelian group of homomorphisms. Since one can multiply a homomorphism by an element of R, the abelian group $\mathrm{Hom}_R(M, N)$ also has the structure of an R-module.

Example 7.

1. $\mathrm{Hom}_R(R, M) \cong M$
2. If G and H are abelian groups then $\mathrm{Hom}(G, H)$ is the same as $\mathrm{Hom}_{\mathbb{Z}}(G, H)$ as $\mathbb{Z}$-modules.
3. $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/(n/(m, n))\mathbb{Z}$.

Definition 8. A submodule $M \subset N$ is a subgroup of N such that $rm \in M$ for all $m \in M$ and $r \in R$.

Definition 9. If $M \subset N$ is a submodule then N/M as abelian group carries the structure of R-module, called the quotient module.

Definition 10. If $f : S \to R$ is a ring homomorphism and M is an R module then f^*M is the S-module M with scalar multiplication $s \cdot m := f(s)m$.

Example 11. Suppose M is an R-module and $r \in R$. Consider the ring homomorphism $e : R[X] \to R$ sending $P(X)$ to $P(r)$. What is e^*M? It is the same underlying abelian group M but with scalar multiplication $P(X) \cdot m$ given by $P(r)m$.

3.2 Isomorphism theorems

Proposition 12. *If $f : M \to N$ is an R-module hom then*

1. $\ker f \subset M$ *is a submodule*
2. $\operatorname{Im} f \subset N$ *is a submodule*
3. $\operatorname{Im} f \cong M/\ker f$

Also define $\operatorname{coker} f := N/\operatorname{Im} f$ *is the quotient module.*

Proposition 13. *Let $N, M \subset L$ be R-modules.*

1. $M \cap N$ *is an R-module.*
2. $M + N = \{m + n | m \in M, n \in N\}$ *is an R-module.*
3. $(M + N)/N \cong N/M \cap N$.

Proposition 14. *Let $N \subset M \subset L$ be R-modules.*

1. M/N *is a submodule of* L/N.
2. $(L/N)/(M/N) \cong L/M$.

3.3 Noetherian rings and modules

Definition 15. An R-module M satisfies the ascending chain condition (ACC) resp. the descending chain condition (DCC) if for every increasing chain of submodules $M_1 \subset M_2 \subset \ldots \subset M$ (resp. descending chain of submodules $M \supset M_1 \supset M_2 \supset \ldots$) the chain becomes stationary, i.e., $M_n = M_{n+1} = \ldots$ for n large enough.

Modules M satisfying ACC are called **Noetherian** and modules M satisfying DCC are called **Artinian**.

Example 16.

1. Every ideal of $\mathbb{Z}$ is Noetherian since $(m) \subset (n)$ implies $n \mid m$. No ideal of $\mathbb{Z}$ is Artinian: indeed $(n) \supsetneq (n^2) \supsetneq \ldots$.
2. Ideals of $\mathbb{Z}/n\mathbb{Z}$ are both Noetherian and Artinian.
3. Ideals in PIDs are Noetherian (see the proof of UFD for PID).
4. In $\mathbb{Z}[X_1, \ldots]$ the ideal $(X_1, \ldots)$ is not Noetherian.