IDEAL THEORY IN PRÜFER DOMAINS

FELIX GOTTI

Preliminary on Modules

Definitions and Examples. Modules over commutative rings are generalizations of vector spaces that play a fundamental role in commutative algebra and, in particular, in ideal theory. For the rest of this section, let R be a commutative ring with identity.

Definition 1. An additive abelian group M is a *module* over R (or an *R-module*) if there is an action of R on M, that is a map $R \times M \to M$ given by $(r, m) \mapsto rm$, satisfying the following properties:

(1) $r(m_1 + m_2) = rm_1 + rm_2$ for all $r \in R$ and $m_1, m_2 \in M$,
(2) $(r_1 + r_2)m = r_1 m + r_2 m$ for all $r_1, r_2 \in R$ and $m \in M$,
(3) $(r_1 r_2)m = r_1(r_2 m)$ for all $r_1, r_2 \in R$ and $m \in M$, and
(4) $1m = m$ for all $m \in M$.

It is clear from the above definition that vector spaces are precisely modules over fields. On the other hand, it is not hard to see that there is a canonical action of $\mathbb{Z}$ over any abelian group A turning A into a $\mathbb{Z}$-module, namely, $na := a + \cdots + a$ (the addition of n copies of a) and $(-n)a := -na$ for all $n \in \mathbb{N}_0$ and $a \in A$. Also, for $n \in \mathbb{N}$, it is easy to verify that the additive abelian group R^n is an R-module over R under the action $r(a_1, \dots, a_n) := (ra_1, \dots, ra_n)$. Under this action, R^n is called the *free module of rank n* over R.

Let M be an R-module. A subgroup N of M is called an *R-submodule* of M if it is is closed under the action of R, that is, $rn \in N$ for all $r \in R$ and $n \in N$. One can readily prove that N is a submodule of M if and only if N is nonempty and $x + ry \in N$ for all $r \in R$ and $x, y \in N$. Every commutative ring R is an R-module over itself, and every ideal I of R is clearly an R-submodule. If N is an R-submodule of M, then the quotient group M/N is an R-module under the action $r(m + N) := rm + N$.

For R-modules M_1 and M_2, a map $\varphi\colon M_1 \to M_2$ is called an *R-module homomorphism* if φ is a group homomorphism satisfying that $\varphi(rm) = r\varphi(m)$ for all $r \in R$ and $m \in M$. In this case, $\ker \varphi$ is an R-submodule of M_1, and it follows that φ is injective if and only if $\ker \varphi = \{0\}$. When φ is bijective, it is called an *isomorphism* of R-modules. The canonical group isomorphism $M_1/\ker \varphi \cong \varphi(M_1)$ (from the First Isomorphism Theorem) is, indeed, an isomorphism of R-modules. If N_1 and N_2 are two R-submodules of M, then the subgroups $N_1 + N_2$ and $N_1 \cap N_2$ are R-submodules, and the canonical group isomorphism $(N_1+N_2)/N_1 \cong N_2/(N_1 \cap N_2)$ is also an isomorphism of R-modules.

The R-module M is *finitely generated* if there exist $m_1, \dots, m_n \in M$ such that $M = Rm_1 + \dots + Rm_n$. Clearly, every commutative ring R with identity is a finitely generated R-module over itself. In addition, if N is an R-submodule of a finitely generated R-module M, then the quotient M/N is also a finitely generated R-module (verify this).

Proposition 2. *Let R, S, and T be commutative rings with identities. If S is a finitely generated R-module and T is a finitely generated S-module, then T is a finitely generated R-module.*

Proof. Since S is a finitely generated R-module, we can take $s_1, \dots, s_m \in S$ such that $S = \sum_{i=1}^m Rs_i$. In addition, since T is a finitely generated S-module, we can take $t_1, \dots, t_n \in T$ such that $T = \sum_{j=1}^n St_j$. Thus, $T = \sum_{j=1}^n \big(\sum_{i=1}^m Rs_i\big)t_j = \sum_{i=1}^m \sum_{j=1}^n Rs_it_j$, whence T is a finitely generated R-module. $\square$

Nakayama's Lemma. Let M be an R-module. If I is an ideal of R, then

$$IM := \Big\{ \sum_{i=1}^n r_i m_i : r_1, \dots, r_n \in I \text{ and } m_1, \dots, m_n \in M \Big\}$$

is an R-submodule of M. Let us argue the following useful result, known as Nakayama's Lemma.

Lemma 3 (Nakayama's Lemma)**.** *Let R be a commutative ring with identity, and let I be an ideal of R. Then the following statements are equivalent.*

(a) *I is contained in every maximal ideal of R.*
(b) *If M is a finitely generated R-module such that $IM = M$, then $M = \{0\}$.*
(c) *If S is a submodule of a finitely generated R-module M such that $IM + S = M$, then $S = M$*

Proof. (a) $\Rightarrow$ (b): Suppose that M is a finitely generated R-module such that $IM = M$. Now assume, by way of contradiction, that $M \neq \{0\}$. Write $M = Rm_1 + \dots + Rm_n$ for $m_1, \dots, m_n \in M$ assuming that $n \in \mathbb{N}$ is taken as smallest as possible. Since $M \neq \{0\}$, we see that $m_1 \neq 0$. As $m_1 \in M = IM$, we can take $a_1, \dots, a_n \in I$ such that $m_1 = \sum_{i=1}^n a_i m_i$. Then $(1 - a_1)m_1 = \sum_{i=2}^n a_i m_i$. Since $a_1 \in I$ belongs to every maximal ideal, one can easily see that $1 - a_1 \in R^\times$. This implies that $n \geq 2$ and also that $a_1 = \sum_{i=2}^n (1 - a_1)^{-1} a_i m_i$, which contradicts the minimality of n.

(b) $\Rightarrow$ (c) Let M be a finitely generated R-module, and let S be an R-submodule of M satisfying $IM + S = M$. Then M/S is also a finitely generated R-module. In addition, since $IM + S = M$, it follows that $M/S = (IM+S)/S = I(M/S)$. Therefore M/S is trivial by our hypothesis in part (b), which implies that $S = M$.

(c) $\Rightarrow$ (a) Let J be a maximal ideal of R. Then J is an R-submodule of the finitely generated R-module of R. Since $IR+J$ is an ideal of R containing the maximal ideal J, either $IR+J = R$ or $IR+J = J$. Since $J \neq R$, part (c) ensures that $IR+J \neq R$. As a result, $I + J = IR + J = J$, which implies that $I \subseteq J$. $\square$

Department of Mathematics, MIT, Cambridge, MA 02139
Email address: fgotti@mit.edu