Peter Geertz-Larson

Math 434

University of Puget Sound

April 2012

Modules

Introduction

In class we have studied the mathematical structure of vector spaces which are defined for fields and abelian groups. A module is generalization of a vector space in that a module is defined for a Ring and an abelian group. With this comparatively relaxed definition of modules we are able to learn a lot about the structure and behavior of other mathematical structures.

Preliminary Definitions and Theorems

With a new mathematical structure comes new definitions and theorems. While these definitions and theorems will feel similar, or exactly the same in some cases, as those for other mathematical structures, they are necessary in order to proceed.

Definition 1 Let R be a ring and M an ableian group (with operation $+$). M is a **left R-module** if for every r in R and every m in M there exists rm in M subject to:

- $r(a+b) = ra + rb$
- $r(sa) = (rs)a$
- $(r+s)a = ra + sa$

for all a, b in M and all r, s in R.

Right modules are defined similarly, where the elements of R are multiplied on the right of elements from M. If R is a ring with unity element 1 and if $1m = m$ for all m in M, then M is a **unital R-module**. If R is a ring with unity, then it is assumed that all R- modules are unital. Note: From here on, unless otherwise stated, an R-module is a left R-module.

Examples

1. Since a ring is defined to be an abelian group, any ring is a module over itself.

2. Any abelian group is a module over $\mathbb{Z}$.

3. If R is a field, a unital R-module is a vector space over R.

4. Let R be a ring, I a left ideal of R. Let M contain all of the cosets of I with representatives from R. Then M is an R-module with operations defined by

   - $(r + I) + (s + I) = (r + s) + I$
   - $r(s + I) = rs + I \qquad$ for $r, s \in R$.

   Proof Let $a, b \in R$. Then the cosets $a + I$ and $b + I \in M$. $(a + I)(b + I) = (a + b) + I = (b + a) + I = (b + I)(a + I)$ since R is an abelian group. Hence M is an abelian group. Moving on to the three properties of modules, let r and s be in R as well.

   - $r((a + I) + (b + I)) = r(a + b) + I = (ra + rb) + I = (ra + I) + (rb + I)$ since elements of R distribute.
   - $r(sa + I) = rsa + I = (rs)a + I = (rs)(a + I)$ since multiplication of elements of R is associative.
   - $(r + s)(a + I) = (r + s)a + I = (ra + sa) + I = (ra + I) + (sa + I)$ since elements of R distribute.

   If I is a two sided ideal, then M is the quotient ring R/I.

Definition 2 If M is a left R-module and a right S-module and if $r(ms) = (rm)s$ for all r in R, s in S, and m in M then M is a **R, S-bimodule**.

Example Using the previous example of a ring over itself as a module, it is plain to see that any ring will be a bimodule over itself, since rings are defined to be associative.

Definition 3 An abelian subgroup S of an R-module M is a **submodule** of M if S is also an R-module. Which is to say, when $r \in R$ and $s \in S$ then $rs \in S$.

Example A nice example of a submodule comes from our now prototypical example of a ring R over itself. Any left ideal I of R is a submodule of R when thought of as a left R-module. Similarly a right ideal is a submodule of R when thought of as a left R-module and a two sided ideal is a submodule of R when thought of as an R, R-bimodule.

Definition 4 Let R be a ring, M be an R-module, and N be a submodule of M. The **quotient module** M/N is the group of cosets of N with representatives from M with operations defined as

- $(a + N) + (b + N) = (a + b) + N$
- $r(a + N) = ra + N$

where $r \in R$ and $a, b \in M$.

As with other mathematical structures, there are homormorphisms of modules and the theorems and definitions that come along with them.

Definition 5 Given two R-modules M and N, a function $\phi : M \to N$ is a **module homomorphism** if for all $a, b \in M$ and $r \in R$

- $\phi(a + b) = \phi(a) + \phi(b)$
- $\phi(ra) = r\phi(a)$

Definition 6 If M and N are two R-modules and $\phi : M \to N$ is a ring homomorphism, the kernal of ϕ (ker ϕ) is the set

$$\ker \phi = \{m \in M | \phi(m) = 0\}$$

Definition 7 If M and N are two R-modules and $\phi : M \to N$ is a ring homomorphism, the image of ϕ is the set $\{\phi(m) | m \in M\}$

$\ker \phi$ is a submodule of M and the image of ϕ is a submodule of N. The proof of these statements is trivial. Similar to homomorphisms of other structures, ϕ is **injective** if ϕ is one to one (equivalently $\ker \phi$ is trivial) and ϕ is **surjective** if the image of ϕ is N. If ϕ is both injective and surjective then we say ϕ is bijective and ϕ is a module **isomorphism**.

We also now define the **canonical projection**. Also given an R-module M and a submodule of M, N, the canonical projection $\phi : M \to M/N$ is the mapping $\phi(m) = m + N$.

As alluded to earlier, we have the module verisons of the three group isomorphism theorems from Judson [2].

Theorem 1 (Ice-1) If M, N are R-modules and $\phi : M \to N$ is a surjective module homomorphism and $\ker \phi = K$ then

$$N \cong \frac{M}{K}$$

Proof Using the first isomorphism theorem for groups, we have the group isomorphism $\rho : M/K \to N$ defined by $\rho(m + K) = \phi(m)$. All we need to do is show that this group isomorphism is also a module isomorphism. Let m be in M and r be in R. Then

$$\rho(r(m + K)) = \rho(rm + K) = \phi(rm) = r\phi(m) = r\rho(m + K).$$

The operation $(+)$ is preserved since ρ is a group isomorphism. Hence ρ is a module isomorphism and we are done.

Before the next isomorphism theorem we note that the intersection of two submodules of a given module is a submodule and state a quick definition. The **sum** of two R-modules M and N is the set

$$M + N = \{m + n | m \in M, n \in N\}.$$

Theorem 2 (Ice-2) If M, N are two submodules of some R-module L then

$$\frac{(M+N)}{M} \cong \frac{N}{(M \cap N)}$$

Proof Again we can call on the equivalent group isomorphism theorem from Judson [2] that gives us the surjective group homormorphism $\phi : N \to (M+N)/N$ defined by $\phi(n) = n + M$ with $\ker \phi = M \cap N$. All we need to do is prove that ϕ is a module homomorphism and since ϕ is a group homomorphism we already know the operation $(+)$ is preserved. So consider $r \in R$ and $n \in N$. Then

$$\phi(r(n+M)) = \phi(rn + M) = rn = r\phi(n+M)$$

and we are done.

Theorem 3 (Ice-3) If L, M, N are R-modules with L a submodule of N and N a submodule of M.

$$\frac{M}{N} \cong \frac{M/L}{N/L}$$

Proof For a third time we call on the equivalent group isomorphism theorem that gives us a group homomorphism $\phi : M/L \to M/N$ defined by $\phi(mL) = mN$ with $\ker \phi = N/L$. Consider $r \in R$ and $m \in M$. Then

$$\phi(r(m+L)) = \phi(rm + L) = rm + N = r(m+N) = r\phi(m+L)$$

and we are done.

Definition 8 An R-module M is **cyclic** if an element $\hat{m} \in M$ such that every $m \in M$ can be written $m = r\hat{m}$ for some r from R. Notationally: $\langle \hat{m} \rangle = M$.

The Structure of Modules over a Principal Ideal Domain

Definition 9 If M is an R-module, $M_1, \ldots, M_n$ are submodules of M such that $M_i \cap (M_1 + \ldots + M_{i-1} + M_{i+1} + \ldots + M_n) = 0$, and $M = M_1 + \ldots + M_n$ then M is the **internal direct sum** of the M_i's. Notationally: $M = M_1 \oplus \cdots \oplus M_n$

Similar to direct products of groups, constructing a new module as the direct sum of the M_i's is the **external direct sum**.

Definition 10 An R-module M is **finitely generated** if there is a set $\{b_i \in M | 1 \leq i \leq m\}$ and every m in M can be expressed as $m = r_1 b_1 + r_2 b_2 + \cdots + r_n b_n$ where $r_i \in R$.

It is important to note that generating a module is not limited to finite sets. A set of generating elements of a module M always exists since M itself is a generating set.

Definition 11 A subset $\{m_1, \ldots, m_n\}$ is a basis of an R-module M if every m in M can be expressed as $m = r_1 m_1, r_2 m_2, \ldots, r_n m_n$ where $r_i \in R$ for $1 \leq i \leq n$. If $\{x_1, \ldots, x_k\}$ is another set that generates M, then $k \geq n$.

Definition 12 If a module M has basis $\{m_1, \ldots, m_n\}$ then the **rank** of M is n.

Sometimes we say rank M or has rank n.

Definition 13 An unital R-module M is **free** if M has a basis (either infinite or finite).

Given a basis, we are able to construct a free module with the method described pg. 42 of Rowen [4].

The following Theorems and proofs come from Gray [1].

Theorem 4 If M is an R-module, then M is isomorphic to a quotient module of a free module.

Proof Let S be a subset of M that generates M and create a free module F on S as the method from Rowen [4]. Define a module homomorphism $\phi : F \to M$ by $\phi(s) = s \in M$. Since S generates M, ϕ is surjective and hence $M \cong F/\ker\phi$.

With this theorem in hand we are now on our way to proving an important structural theorem for modules but we need a few more lemmas and theorems before we get there.

Lemma 1 If $\{m_1, \ldots, m_n\}$ is a basis for a free R-module M where R is a principal ideal domain and $s_1 = \sum_{i=1}^{n} \alpha_i m_i$, then a basis $\{s_1, s_2, \ldots, s_n\}$ can be formed if and only if the α_i's are relatively prime.

Proof

$(\Rightarrow)$

Suppose $M = Rs_1 \oplus \cdots \oplus Rs_n$ and suppose $\alpha_i = d\beta_i$ for $1 \leq i \leq n$. Since $s_1 \neq 0, d \neq 0$. Then $d(\sum \beta_i m_i + Rs_1) = s_1 + Rs_1 = Rs_1$. However, M/Rs_1 is free with basis $\{(s_2 + Rs_1), \ldots, (s_n + Rs_1)\}$, so that $\sum \beta_i m_i + Rs_1 = Rs_1$. Thus $\sum \beta_i r_i = r \sum \alpha_i m_i$, but M is free, hence $\beta_i = r\alpha_i = rd\beta_i$ for $1 \leq i \leq n$ with at least one $\beta_1 \neq 0$. Therefore $rd = 1$ and $d|1$, so 1 is the gcd of the α_i's.

$(\Leftarrow)$

For the other direction, we use induction on the rank of M. If the gcd of α_1 is 1, then $R\alpha_1 = R$, α must be a unity, and $\alpha_1 m$ is a basis. Assume $n > 1$ and that the result holds for any module of rank $< n$. Let $s_1 = \sum_{i=1}^{n} \alpha_i m_1$. $R\alpha_1 + \cdots + R\alpha_n$ is an ideal of R and hence principal. Let $R\alpha_1 + \cdots + R\alpha_n = Rd$ where $d\beta_i = \alpha_i$ for $2 \leq i \leq n$. Then $R = R\beta_2 + \cdots + R\beta_n$ and if $t_2 = \sum_{i=2}^{n} \beta_i m_i$, then there is a basis $\{t_2, \ldots t_n\}$ for $Rm_1 + \cdots Rm_n$ and $\{m_1, t_2, \ldots t_n\}$ is a basis for M with $s_1 = \alpha_1 m_1 + dt_2$. If $\gcd(\alpha, d)$ is 1, then we need to show there is a s_2 such that $M = Rs_1 \oplus Rs_2$.

Since R is a PID we can write $1 = x\alpha + yd$ for $x, y \in R$. Let $s_2 = -ym_1 + xt_2$. This gives us

$$m_1 = x\alpha_1 m_1 + ydm_1 + xdt_2 - xdt_2 = xs_1 - ys_2$$

and

$$t_2 = x\alpha_1 t_2 + ydt_2 + y\alpha_1 m_1 - y\alpha_1 m_1 = ys_1 + \alpha_1 s_2.$$

Thus $Rs_1 + Rs_2 = Rm_1 + Rt_2 = M$.

Now suppose $s \in Rs_1 \cap Rs_2$. Then $s = u(\alpha_1 m_1 + dt_2) = v(-ym_1 + xt_2)$. Since $\{m_1, t_2\}$ is a basis for a free module $u\alpha_1 = -vy$ and $ud = vx$. Thus $u = u(x\alpha_1 + yd) = -vyx + vyx = 0$.

As a corollary to this lemma, we get a property of modules that is virtually the same as a property of vector spaces.

Corollary 1 If M is a free module of rank m over a principal ideal domain, then any basis of M has m elements.

Theorem 5 Let M be an R-module with finite rank m where R is a principal ideal domain. If N is a submodule of M, then rank $N = n \leq m$.

Proof Let $S = \{x_1, \ldots, x_m\}$ be a minimal generating set of M, F the free module with S as a basis and $\rho : F \to M$ defined as the map in the previous theorem. Since N can be expressed as the quotien module of a submodule of F, namely $\{f \in F | \rho(f) \in N\}$, we can consider M to be free. We induct on the rank of M. If $m = 1$, M is isomorphic to R and the rank of any submodule of R is 0 or 1. Thus rank $N \leq 1$.

Let $A = \{a \in R | x - ax_1 \in Rx_2 + \cdots + Rx_m\}$. A is an ideal of R, so $A = Ra_1$ for some $a_1 \in A$. Let $y - a_1 x_1 \in Rx_2 + \cdots + Rx_m$ and $N_1 = N \cap (Rx_2 + \cdots + Rx_m)$. Our claim is that $N = N_1 + R_y$. Suppse $r_1 x_1 + \cdots + r_m x_m \in N$. Then $r_1 \in A$ such that $r_1 = ra_1, r \in R$. But then

$$r_1x_1 + \cdots + r_m x_m - ry = r_1 x_1 + \cdots r_m x_m - r(y - a_1 x_1) - r_1 x_1 \in N \cap (Rx_2 + \cdots Rx_m) = N_1$$

so that $N \subset N_1 + R_y$. However, clearly $N_1 + Ry \subset N$. N_1 is a submodule of $Rx_2 + \cdots Rx_m$, a module of rank $m - 1$. So by induction rank $N_1 = n - 1 \leq m - 1$ and hence rank $N \leq m$.

Corollary 2 Let R be a principal ideal domain. If M is a free R-module with rank m then every submodule N of M is free and has rank less than or equal to m.

Proof From the previous theorem, N has a minimal generating set $S = \{x_1, \ldots, x_n\}$. Form a free module F with S as a basis and let $\rho : F \to N$ be defined as earlier. If $\ker \rho = \{0\}$, N is free. Suppose $0 \neq x = \sum r_i x_i \in \ker \rho$. Let $Rd = Rr_1 + \cdots + Rr_n$. Not all r_i are zero, so $d \neq 0$. Let $da_i = r_i$ for $1 \leq i \leq n$ such that $R = Ra_1 + \cdots + Ra_n$. Let $x' = \sum a_i x_i$. So $\rho(x') \in M$, so let $\rho(x') = \sum c_i y_i$, where $\{y_1, \ldots y_m\}$ is a basis for M. Then $\sum dc_i y_i = d(\rho(x')) = \rho(x) = 0$. Since M is free, $dc_i = 0$ for $1 \leq i \leq n$ and $c_i = 0$ for $1 \leq i \leq n$. Thus $\rho(x') = 0$. We can complete $\{x'\}$ to a basis $\{x', x'_2, \ldots, x'_n\}$ for F. Letting $F' = Rx'_2 + \cdots Rx'_n$ we see that $\rho(F') = N$ so that N is generated by a set of $n-1$ elements, contradicting the minimaility of $\{x_1, \ldots, x_n\}$. Hence $\ker \rho$ must be zero and N is free.

Theorem 6 Let R be a principal ideal domain. If M is a free R-module of rank m and N is a submodule of M, then there is a basis $\{a_1, a_2, \ldots, a_m\}$ of M and $b_i \in R$ for $1 \leq i \leq m$ such that

- $b_i | b_{i+1}$ for $1 \leq i \leq m$ with a $b_n \neq 0$ such that $b_j = 0$ where $n+1 \leq j \leq m$.
- $\{b_1 a_1, \ldots, b_n a_n\}$ is a basis for N

The proof of this theorem is very involved and is therefore omitted. However, if the reader is curious the proof is on pages 51-53 of Gray[1].

Theorem 7 If R is a principal ideal domain then a finitely generated R-module is the direct sum of a finite number of cyclic modules.

Proof Let M be a finitely generated R module and let $\rho : F \to M$ be the surjective map, where F is free. Then F has a basis $\{f_1, f_2, \ldots, f_n\}$ such that $\ker \rho$ has a basis $\{a_1 f_1, a_2 f_2, \ldots, a_m f_m\}$ where a_i divides a_{i+1} for $1 \leq i \leq m-1$. If some $a_i | 1$ then $\{f_1, \ldots, f_n\} \subset \ker \rho$ and so $\{f_1, \ldots, f_n\}$ can be excluded from the bases.

Hence

$$M \cong \frac{Rf_1 \oplus \cdots \oplus Rf_n}{R/Ra_1 \oplus \cdots \oplus R/Ra_n}$$

Let $\phi : Rf_1 \oplus \cdots \oplus Rf_n \to R/Ra_1 \oplus \cdots \oplus R/Ra_n$ be the mapping defined by

$$\phi(r_1 f_1 + \cdots + r_n f_n) = (r_1 + Ra_1) + \cdots + (r_n + Ra_n).$$

Suppose

$$\phi(r_1 f_1 \cdots r_n f_n) = Ra_1 + \cdots + Ra_1 = 0$$

$\Rightarrow r_i = s_i a_i$ for some $s_i \in R$ and $1 \leq i \leq n$. Hence $r_i f_i \in Rd_i f_i$. Any element from $Ra_1 f_1 \oplus \cdots \oplus Ra_n f_n$ is mapped to the zero element, hence $\ker \phi = Ra_1 f_1 \oplus \cdots \oplus Ra_n f_n$. The surjectivity of ϕ is easy to see and is omitted.

Hence

$$M \cong \frac{Rf_1 \oplus \cdots \oplus Rf_n}{Ra_1 f_1 \oplus \cdots \oplus Ra_n f_n} \cong \frac{R}{Ra_1} \oplus \cdots \oplus \frac{R}{Ra_n}.$$

Where $a_1 \not| 1$ and if $m < n$, then $a_i = 0$ for $m + 1 \leq i \leq n$. The only thing left to show is that each R/Ra_i is cyclic however this is trivial since $1 + Ra_i \in R/Ra_i$ for $1 \leq i \leq n$.

As corollaries to this theorem we get the Fundamental Theorem of Finitely Generated Abelian Groups and the Fundamental Theorem of Finite Abelian Groups from Judson [2].

Corollary 3 (Fundamental Theorem of Finitely Generated Abelian Groups) Every finite abelian group is isomorphic to the direct sum of cyclic groups of the form

$$\mathbb{Z}_{p_1^{\alpha_1}} \oplus \mathbb{Z}_{p_2^{\alpha_2}} \oplus \cdots \oplus \mathbb{Z}_{p_n^{\alpha_n}} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$$

where $\alpha_i \in \mathbb{Z}$ and the p_i's are not necessarily distinct primes.

Corollary 4 (Fundamental Theorem of Finite Abelian Groups) Every finite abelian group is the direct sum of cyclic groups of the form

$$\mathbb{Z}_{p_1^{\alpha_1}} \oplus \mathbb{Z}_{p_2^{\alpha_2}} \oplus \cdots \oplus \mathbb{Z}_{p_n^{\alpha_n}}$$

where $\alpha_i \in \mathbb{Z}$ and the p_i's are not necessarily distinct primes.

Conclusion

The generalization from vector spaces to modules yields unexpected results. We find that there are quite a few similarities but by wading through familiar definitions and theorems for modules and with just a few more complicated results, we are able to achieve a fundamental theorem about their structure and as a result we get two important theorems from group theory as corollaries.

References

[1] Gray, Mary. *A Radical Approach to Algebra*.
Addison-Wesley Publishing Company, 1970. 43-70.

[2] Judson, Thosmas W. *Abstract Algebra: Theory and Applications*. Edition 2.0.
PWS Publishing Company, 2011.

[3] Lambek, Joachim. *Lectures On Rings And Modules*.
Blaisdell Publishing Company, 1966.

[4] Rowen, Louis. *Ring Theory*. Volume 1.
Academic Press, Inc., 1988.