1. Modules

Covention: This semester all rings will be assumed to have 1.

Definition. Let R be a ring. A left R-module is a set M with two operations:

(1) binary operation $+$ on M, that is a map $+ : M \times M \to M$
(2) an action of R on M, that is, a map $R \times M \to M$
$(r, m) \mapsto rm$

satisfying the following axioms:

M1: $(M, +)$ is an abelian group
M2: $(r + s)m = rm + sm$ for all $r, s \in R$ and $m \in M$
M3: $(rs)m = r(sm)$ for all $r, s \in R$ and $m \in M$
M4: $r(m + n) = rm + rn$ for all $r \in R$ and $m, n \in M$
M5: $1 \cdot m = m$ for all $m \in M$

Elements of R are often called *scalars*.

Remark: (1) Similarly one defines right R-modules, where the action is denoted by $(r, m) \mapsto mr$, and axioms M2-M5 are replaced by their "mirror" images.
(2) If R is commutative, left R-modules = right R-modules
From now on by an R-module we will mean a left R-module.

1.1. Basic examples of modules.

1. Assume that R is a field. Then R-modules = vector spaces over R

2. Let R be any ring and $n \in \mathbb{N}$. Let $R^n = \{(r_1, \ldots, r_n) : r_i \in R\}$. Then R^n is an R-module where

$$r(r_1, \ldots, r_n) = (rr_1, \ldots, rr_n).$$

R^n is called the standard free R-module of rank n.

3. Let R be any ring, S a subring of R with 1. Then R is an S-module with action = left-multiplication.

In particular, any ring R is a module over itself.

4. Let R be any ring. I an ideal of R. Then R/I is an R-module where $r(a + I) = ra + I$.

1.2. **Modules over some special rings.**

<u>Modules over $\mathbb{Z}$</u>

Claim 1.1. *Modules over $\mathbb{Z}$ = abelian groups.*

"Proof". If M is a $\mathbb{Z}$-module, then $(M, +)$ is an abelian group by definition. Conversely, if A is an abelian group, we can turn A into a $\mathbb{Z}$-module by setting

$$na = \begin{cases} \underbrace{a + \ldots + a}_{n \text{ times}} & \text{if } n > 0 \\ 0 & \text{if } n = 0 \\ \underbrace{a + \ldots + a}_{-n \text{ times}} & \text{if } n < 0 \end{cases}$$

Module axioms trivially holds.

There is no other way to make M a $\mathbb{Z}$-module since for any $n \in \mathbb{N}$ and $a \in A$ we must have $na = (\underbrace{1 + \ldots + 1}_{n \text{ times}})a = \underbrace{a + \ldots + a}_{n \text{ times}}$ by M2 and M5; similarly we must have $0 \cdot a = a$ and $(-n) \cdot a = -(na)$.

In other works, an action of $\mathbb{Z}$ on M is completely determined by addition on M. □

<u>Modules over $F[x]$ where F is a field</u>

Claim 1.2. *Modules over $F[x]$ = pairs (V, A) where V is a vector space over F and $A : V \to V$ a linear transformation.*

Sketch of the proof. (see [DF,pp. 340-341] for more details) Let V be an $F[x]$-module. Then V can also be considered as an F-module = F-vector space.

Define a mapping $A : V \to V$ by $A(v) = xv$. By module axioms A is a linear transformation form V to V.

Conversely, given an F-vector space V and a linear transformation $A : V \to V$, we want to make V into $F[x]$-module such that $xv = A(v)$ for all $v \in V$. By module axioms we are forced to set

$$(x^2)v = x(xv) = A(xv) = A(A(v)) = A^2(v).$$

Similarly, $x^n v = A^n v$ for any $n \in \mathbb{N}$, and finally for any $p(x) \in F[x]$ we must have $p(x)v = (p(A))v$, that is,

$$(c_n x^n + \ldots + c_0)v = (c_n A^n + \ldots + c_0)(v) \qquad (***)$$

Thus, once we decided how x acts on V, the action of any element of $F[x]$ has to be given by (***). We still have to verify that (***) indeed defines an $F[x]$-module structure on V, but this verification is routine. □

1.3. **Submodules, quotient modules and homomorphisms.**

Definition. Let M be an R-module. A subset N of M is called an R-submodule if

(1) N is a subgroup of $(M, +)$
(2) for any $r \in R$, $n \in N$ we have $rn \in N$.

Example: Let R be a ring, $M = R$ (with action by left multiplication). Then submodules of R = left ideals of R.

Definition. If M is an R-module and N is a submodule of M, we can define the quotient module M/N. As a set M/N is just the quotient group M/N, and R-action is given by

$$r(m + N) = rm + N \text{ for all } r \in R, m \in M.$$

Definition. If M and N are R-modules, a mapping $\varphi : M \to N$ is called a homomorphism of R-modules (alternatively φ is an R-linear mapping) if

(1) φ is a homomorphism of abelian group
(2) $\varphi(rm) = r\varphi(m)$ for all $r \in R, m \in M$.

1.4. **Modules and group actions.**

Definition. Let G be a group. The integral group ring $\mathbb{Z}[G]$ is defined as follows: as a set $\mathbb{Z}[G]$ is the collection of formal finite linear combinations of elements of G with integral coefficients, that is,

$$\mathbb{Z}[G] = \{ \sum_{g \in G} n_g g : n_g \in \mathbb{Z} \text{ and only finitely many } n_g \text{ are nonzero.} \}$$

Addition and multiplication on $\mathbb{Z}[G]$ are defined by setting
$(\sum_{g \in G} n_g g) + (\sum_{g \in G} m_g g) = \sum_{g \in G} (n_g + m_g) g$ and
$(\sum_{g \in G} n_g g) \cdot (\sum_{g \in G} m_g g) = \sum_{g \in G} l_g g$ where $l_g = \sum_{h \in G} n_h m_{h^{-1}g}$.
In other words, multiplication in $\mathbb{Z}[G]$ is obtained by first setting $g \cdot h$ to be the product of g and h in G and then uniquely extending to arbitrary elements of $\mathbb{Z}[G]$ by distributivity.

Theorem (HW#1, Problem 6). *Let M be an abelian group. Show that there is a natural bijection between $\mathbb{Z}[G]$-module structures on M and actions of G on M by group automorphisms (that is, actions of G on M such that for any $g \in G$ the map $m \mapsto gm$ is an automorphism of the abelian group $(M, +)$).*