1 Rings and modules

Rings. A *ring* is a tuple $(R, +, \cdot, 0, 1)$, where $(R, +)$ is an abelian group, 0 being its additive identity (called *zerp*), and $(R, \cdot)$ is a monoid, 1 being the multiplicative identity (called *unity*), such that for any $x, y, z \in R$, $(x+y)z = xz + yz$, $x(y+z) = xy + xz$. The last two identities are called distributivity of $+$ over $\cdot$, and that of $\cdot$ over $+$, respectively.

By abuse of notation, $(R, +, \cdot, 0, 1)$ is just denoted as R.

A ring R is commutative if $(R, \cdot)$ is.

Domains, Division rings and Fields. A ring R is called a *domain* if $xy = 0$ implies $x = 0$ or $y = 0$. A domain R is called a division ring if given $x \in R - \{0\}$ there is $x^{-1} \in R$ such that $xx^{-1} = x^{-1}x = 1$. A division ring R is called a field if $(R, \cdot)$ is commutative.

Exercise 1.1. (Wedderburn's little theorem) A finite domain is a field.

Homomorphism of rings. Let R and S be rings. A homomorphism of rings $\phi : R \to S$ is a group homomorphism $\phi : (R, +) \to (S, +)$, which is also a homomorphism of monoids $\phi : (R, \cdot) \to (S, \cdot)$.

An *embedding* is an injective homomorphism.

A *quotient* is a surjective homomorphism.

Let R be a ring. An R-algebra is a ring homomorphism $\phi : R \to S$. By abuse of notation, we will say S is an R-algebra. If $\phi : R \to S$ and $\psi : R \to T$ are to R-algebras, then an R-algebra homomorphism $S \to T$ is a ring homomorphism $\theta : S \to T$ such that $\theta \circ \phi = \psi$.

Ideals and quotients Let R be a ring. A subgroup $I \subset (R, +)$ is called a left (right) ideal if given $x \in I$, $y \in R$, $xy \in I$ (or $yx \in I$, resp.).

For a two sided ideal I, the quotient group R/I admits the structure of a ring in a natural way and the quotient map $R \to R/I$ is a ring homomorphism.

A ring R has a characteristic if $\{n \in \mathbb{N} : nx = 0, \forall x \in R\}$ is nonempty, and its minimum element is called the *characteristic* of R.

Exercise 1.2. In a similar way one can define a ring without unity, just by dropping the requirement that there is a unity. A ring homomorphism between rings without unities is is defined similarly as well.

(a) Any ring without unity can be embedded in a ring with unity.

(b) Any ring without unity but having a characteristic can be embedded in a ring

with unity of the same characteristic.

Example 1.1. (a) Let R be a ring. Then $M_n(R)$ is the R-algebra of $n \times n$-matrices. (b) The real quaternions. Let $A = M_2(\mathbb{C})$. The subset of elements of the form

$$\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$$

forms a subring $\mathbb{H}$. An $\mathbb{R}$-basis of $\mathbb{H}$ is given by $1, i, j, k$, where 1 stands for the identity matrix, and the other elements are defined in such a way that $a+bi+cj+dk$ corresponds to the matrix

$$\begin{pmatrix} a + b\sqrt{-1} & c + d\sqrt{-1} \\ -c + d\sqrt{-1} & a - b\sqrt{-1} \end{pmatrix}$$

Verify that $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$. The ring $\mathbb{H}$ is a division algebra, and is non-commutative.

(c) The group ring. Let R be a ring and G a finite group. Let $R[G]$ be the set of maps $a : G \to R$. Note that these maps correspond to formal sums of the form

$$\sum_{g \in G} a(g)g, \ a_g \in R.$$

We define addition and multiplication as follows. If $a, b \in R[G]$ then

$$(a + b)(g) = a(g) + b(g),$$

$$(ab)(g) = \sum_{xy=g} a(x)b(y) = \sum_{z \in G} a(z)b(z^{-1}g).$$

The zero is given by $0(g) \equiv 0$, the unity is given by $1(e_G) = 1$ and $1(g) = 0$ for $g \neq e_G$. Note that $R[G]$ is naturally an R-algebra.

Exercise 1.3. $*$(a) Is there any finite group G such that $\mathbb{H}$ is isomorphic as an $\mathbb{R}$-algebra to $\mathbb{R}[G]$?

(b) Let R be a ring. Then there is a canonical isomorphism of R-algebras

$$R[x]/(x^n - 1) \to R[\mathbb{Z}/n\mathbb{Z}].$$

(c) The real quaternions $\mathbb{H}$ and $M_2(\mathbb{R})$ both are $\mathbb{R}$-algebras and have the same underlying real vector spaces. But they are not isomorphic as $\mathbb{R}$-algebras.

The opposite ring Let R be a ring. The opposite ring R^{op} has the same additive group as R, but a different multiplication $\odot$, defined by $a \odot b = ba$.

Note that if R is a commutative ring, then $R = R^{op}$ in the sense that the multiplications are *same*.

Exercise 1.4. (a) Let k be a commutative ring and $R = M_n(k)$. Then $R \to R^{op} : A \mapsto {}^tA$ is an isomorphism of rings.

(b) Let k be a commutative ring, G a finite group, and $R = k[G]$. Then $g \mapsto g^{-1}$ induces an isomorphism of rings $R \xrightarrow{\sim} R^{op}$.

(c) Let $\mathbb{H}$ be the quaternion ring over $\mathbb{R}$. The quaternionic conjugation $a + bi + cj + dk \mapsto a - bi - cj - dk$ induces an isomorphism of rings $\mathbb{H} \xrightarrow{\sim} \mathbb{H}^{op}$.

However, there are rings which are not isomorphic to their opposites.

Modules Let R be a ring. A left R-module is an abelian group M together with a homomorphism of rings $\phi : R \to \mathrm{End}_{\mathbb{Z}}(M)$. A right R-module is an abelian group V together with a homomorphism of rings $\rho : R^{op} \to \mathrm{End}_{\mathbb{Z}}(V)$.

Let M be a left module, and set for $a \in R$, $m \in M$, $am := \phi(a)m$. Then the condition that ϕ is a ring homomorphism is equivalent to the following: $\forall a, b \in R$, $\forall m, m' \in M$, $0_R m = 0_M$, $1_R m = m$, $(a + b)m = ab + bm$, $(ab)m = a \cdot bm$, $a(m + m') = am + am'$.

Similarly if V is a right module, set for $a \in R$, $v \in V$, $va := \rho(a)v$. Then the condition that ρ is a ring homomorphism is equivalent to the following:

$\forall a, b \in R$, $\forall v, v' \in V$, $v0_R = 0_V$, $v1_R = v$, $v(a + b) = va + vb$, $v(ab) = (va)b$, $(v + v')a = va + va'$.

Homomorphism of modules Let R be a ring and M, M' two left R-modules. A group homomorphism $f : M \to M'$ is called an R-module homomorphism (also called R-linear) if for each $r \in R$, $m \in M$, $f(rm) = rf(m)$. Similarly for a homomorphism between two right R-modules.

An R-module isomorphism is an R-linear map which is a bijection. Two R-modules are isomorphic as R-modules if there is an R-module isomorphism between them.

Submodules Let M be an R-module and let $M' \subset M$ be a subgroup. Then M' is called an R-submodule if for $r \in R$, $m \in M'$, we have $rm \in M'$. Note that in this case, M' becomes an R-module in a natural way and the inclusion $M' \hookrightarrow M$ is an injective R-module homomorphism.

Exercise 1.5. (a) If R is a commutative ring, then a left R-module is automatically a right R-module.

(b) Let R be a ring such that there is an isomorphism of rings $\alpha : R^{op} \xrightarrow{\sim} R$. If M is a left R-module, then the composite $R^{op} \xrightarrow{\alpha} R \xrightarrow{\phi} \mathrm{End}_{\mathbb{Z}}(M)$ gives rise to a right module structure on M. Similarly, a right R-module structure ρ on V gives rise to a left module structure by composing ρ with α^{-1}.

(c) Given an R-module homomorphism $f : E \to M$, the image $f(E)$ is a submodule of M.

Example 1.2. (a) Let R be a ring. Then R is automatically a left as well as a right module under R. The left (right) R-submodules of R are precisely the left (right) ideals in R.

(b) Let k be a field and V a vector space over k. Then V is a k-module.

(c) Any abelian group is a $\mathbb{Z}$-module.

(d) The free module. Let R be a ring, and consider for any $n > 0$, the direct sum $M = R^{\oplus n}$. Then R acts on M on the left naturally as $a(a_1, \ldots, a_n) = (aa_1, \ldots, aa_n)$. Similarly on the right. Any left (right) R-module which is isomorphic to $R^{\oplus n}$ for some $n > 0$ is called free of rank $= n$.

(e) Let $f : R \to S$ be a ring homomorphism. Then S is a left module under R in the following way. Let $r \in R$, $s \in S$. Then $rs := f(r)s$. Also, S is a right module under R by $sr := sf(r)$. Therefore every algebra is automatically a (both left and right) module.

(f) If I is a two ideal in a ring R, then the ring R/I is automatically a (both left and right) module under R.

(g) Let L/k be a Galois extension of fields with $G = Gal(L/k)$. Then L is naturally a left $k[G]$ module by $(\sum_{g\in G} a_g g)x = \sum_{g\in G} a_g gx$.

Exercise 1.6. (a) If k is a field, then every k-module is free.

(b) If M_i is an R-module for $i \in I$, I being a set, then the abelian groups $\oplus_{i\in I} M_i$ and $\prod_{i\in I} M_i$ are both R-modules in a natural way.

(c) Let $0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ be a short exact sequence of R-modules (i.e. it is a short exact sequence of abelian groups and all maps are R-linear). If $M \to M''$ has an R-linear section s, then $M' \oplus M'' \to M : (x, y) \mapsto x + s(y)$ is an R-module isomorphism with an inverse given by $M \to M' \oplus M'' : z \mapsto (z - sp(z), p(z))$.

(d) Let L/k be a Galois extension of fields with $G = Gal(L/k)$. Then L is actually a free $k[G]$-module of rank 1. (Hint: Normal basis theorem)

$*$(e) If G is a finite group whose order is invertible in a field k, then $k[G]$ is semisimple in the following sense. Let $M' \subset M$ be a submodule. Then there is another submodule $M'' \subset M$ such that $M = M' \oplus M''$.

$*$(f) Give an example to show the following. Suppose M' and M'' are two R-modules such that $M' \oplus M''$ is free. It does not necessarily imply that M' and M'' are both free.

Finitely generated modules. Let R be a ring and M a left R-module. M is called a finite R-module or a finitely generated R-module, if there is a surjective homomorphism $R^{\oplus n} \to M$ of R-modules. Equivalently, M is finitely generated if there are finitely many elements $m_1, \ldots, m_n$ such that given any element $m \in M$ there are elements $r_1, \ldots, r_n \in R$ such that $m = \sum_{i=1}^{n} r_i m_i$.