Some Useful Definitions

We summarize here a few of the definitions that will be used during the course. The arrangement will be slightly different from that which appears in your text. In this and other handouts HK will be used to refer to the Math 4330 textbook *Linear Algebra* by K. Hoffman and R. Kunze, 2nd edition, Prentice-Hall, 1971.

Definition 1. [HK, p. 82] A *group* G is a non-empty set, together with a single binary operation denoted here by $\star$

$$\begin{array}{rcl} \star:\, G\times G & \longrightarrow & G \\ (g,h) & \mapsto & g\star h \end{array}$$

for all $g,h\in G$ such that the following axioms are satisfied:

1. Associativity:
$$g\star(h\star k) = (g\star h)\star k$$
for all $g,h,k\in G$;
2. An identity $e\in G$ exists:
$$e\star g = g\star e = g$$
for all $g\in G$;
3. Inverses exist:
For each $g\in G$ there exists an element $g'\in G$ such that
$$g\star g' = g'\star g = e$$

It is easy to check that

The identity is unique:
$$e = e\star e' = e'$$
for $e,e'\in G$ two possibly different identities satisfying 2. above.

Inverses are unique:

$$\begin{array}{rcl} g''\star(g\star g') & = & (g''\star g)\star g' \\ g''\star e & = & e\star g' \\ g'' & = & g' \end{array}$$

for $g',g''\in G$ two possibly different inverses of $g\in G$.

G is called an *abelian* group in case G also satisfies

4. $$g \star h = h \star g$$

   for all $g, h \in G$,

In many examples the operation $\star$ is called “multiplication” and is denoted by $\cdot$ (or simply juxtaposition), the identity is denoted by 1 (“one”), and the inverse of g by g^{-1}.

In cases where G is an abelian group, in many cases the operation $\star$ is denoted by $+$, the operation is called “addition”, the identity is denoted 0 (“zero”), and the inverse of g is denoted by $-g$.

Definition 2. [HK, p. 2] A *field* F is a non-empty set, together with two operations called *addition* and *multiplication*, denoted by $+$ and $\cdot$, respectively. They satisfy

1. F is a abelian group with respect to $+$ with identity element 0.
2. $F^* = F \setminus \{ 0 \}$ is an abelian group with respect to $\cdot$ with identity element 1.
3. left and right distributive laws:

   $$(x+y)z = xz + yz$$
   $$x(y+z) = xy + xz$$

   for all $x, y, z \in F$.

Note in particular that $0 \neq 1$ in a field.

Remark 3. If this definition is altered by omitting commutativity for multiplication, one obtains the definition of a *skew field*. Many results of linear algebra still hold in this more general situation (e.g., solutions of systems of equations, matrices, row reduction, dimension of vector spaces) others (e.g., eigenvalues, determinants) either no longer hold or take a substantially different form. We will not pursue this topic here.

Definition 4. [HK, p. 140] An *associative ring* R is a non-empty set, together with two operations called *addition* and *multiplication*, denoted by $+$ and $\cdot$, respectively, which satisfy the following axioms:

1. R is a abelian group with respect to $+$ with identity element 0.
2. multiplication $\cdot$ is associative,
3. the left and right distributive laws hold.

Furthermore, we require that R has an *identity* element 1

$$1 \cdot x = x \cdot 1 = x$$

for all $x \in R$.

Note that it is no longer required that every non-zero element have a multiplicative inverse nor that multiplication be commutative. Thus $\mathbb{Z}$ (the integers), $F^{m\times m}$ (m by m matrices over a field F), and $F[x]$ (polynomials over a field F) are all associative rings.

It is easy to check that for any ring, the following hold:

1. $0 \cdot r = r \cdot 0 = 0$ for all $r \in R$.
2. $(-1) \cdot r = r \cdot (-1) = -r$ for all $r \in R$.
3. $(-r)s = r(-s) = -(rs)$ for all $r, s \in R$.

E.g. for the first, compute $(0+0)r$ two different ways.

Definition 5. A ring R is *commutative*, if $xy = yx$ for all $x, y \in R$.

Definition 6. [HK, p. 164] Let R be an associative ring (with identity). Let M be an additively written abelian group with identity element 0.

Then M is called a left R-*module*, if there is an operation

$$\begin{array}{rcl} \cdot : R \times M & \longrightarrow & M \\ (r, m) & \mapsto & r \cdot m \end{array}$$

for all $m \in M$ and for all $r \in R$ such that the following axioms hold:

1. $1 \cdot m = m$
2. $(rs) \cdot m = r \cdot (s \cdot m)$
3. $r \cdot (m+n) = r \cdot m + r \cdot n$
4. $(r+s) \cdot m = r \cdot m + s \cdot m$

for all $m, n \in M$ and all $r, s \in R$.

One normally abbreviates $r \cdot m$ simply as rm.

One can define a right R-module in a similar manner by writing the element from the ring on the right. The concepts of left and right are different for non-commutative rings since condition 2. depends on the order of the operation in R.

Definition 7. [HK, p. 28] Let F be a field and V be an abelian group written additively. V is a vector space over F simply means that V is an F-module.

Definition 8. [HK, p. 119] Let R be a commutative ring. An R-module A which is also a ring such that the scalar multiplication and multiplication are compatible, that is, satisfy:

5. $r(ab) = (ra)b = a(rb)$ for all $r \in R$ and $a, b \in A$

is called an R-*algebra*.

Many of the R-algebras that we will consider are for the case where $R = F$ is a field. For example, $F[x]$ (polynomials), $F[[x]]$ (formal power series), and $F^{m\times m}$ for F a field are all F-algebras. The first two are commutative and for $m > 1$ the last one is not.

We have now given definitions of the main collections of objects that are studied in this course. The main content however is in the study of the functions which preserve the structures of these. We start with the first object defined.

Definition 9. Let G_1 and G_2 be groups. A function $f : G_1 \longrightarrow G_2$ is called a *group homomorphism* if $f(g \star h) = f(g) \star f(h)$ for all $g, h \in G_1$. Note that the first $\star$ denotes the operation in G_1 and the second $\star$ is that of G_2.

Note that it follows immediately that $f(e) = e$ where the first e is the identity of G_1 and the second the identity of G_2: Now

$$f(e) = f(e \star e) = f(e) \star f(e)$$

hence multiplying both sides by $f(e)^{-1}$ yields the result.

Definition 10. Let R_1 and R_2 be associative rings with identity. A function $f : R_1 \longrightarrow R_2$ is a *ring homomorphism* if

1. $f(r + s) = f(r) + f(s)$ for all $r, s \in R_1$.
2. $f(r \cdot s) = f(r) \cdot f(s)$ for all $r, s \in R_1$.
3. $f(1) = 1$.

A field homomorphim is just a special case of a ring homomorphism (a field is just a special type of ring).

Definition 11. Let M_1 and M_2 be modules over the same ring R (with 1). A function $f : M_1 \longrightarrow M_2$ is an R-*module homomorphism* if

1. $f(m + n) = f(m) + f(n)$ for all $m, n \in M_1$.
2. $f(r \cdot m) = r \cdot f(m)$ for all $r \in R$ and all $m \in M_1$.

Remark 12. If V_1 and V_2 are vector spaces over a field F, a linear transformation $T : V_1 \longrightarrow V_2$ is just an F-module homomorphism.

Definition 13. Let A_1 and A_2 be R-algebras over the commutative ring R (with 1). A function $f : A_1 \longrightarrow A_2$ is an R-*algebra homomorphism* if

1. f is an R-module homomorphism,
2. f is a ring homomorphism.