MATH 436 Notes: Rings.

Jonathan Pakianathan

November 13, 2003

1 Rings

Definition 1.1 (Rings). *A ring R is a set with two binary operations $+$ and $\cdot$ called addition and multiplication respectively such that:*

(1) $(R, +)$ is an Abelian group with identity element 0.
(2) $(R, \cdot)$ is a monoid with identity element 1.
(3) Multiplication distributes over addition:

$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ and } (b + c) \cdot a = b \cdot a + c \cdot a$$

for all $a, b, c \in R$.

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

On occasion we will consider rings that satisfy a weaker version of (2) where we drop one or more of the conditions of a monoid. If $(R, \cdot)$ is a semigroup without 1 we say R is a ring without identity and if $(R, \cdot)$ is nonassociative we call R a nonassociative ring.

A motivating example of a ring is the integers $\mathbb{Z}$ under the usual addition and multiplication. In general we try to mimic basic properties of this ring in the study of other rings.

Definition 1.2 (Subrings). *If $(R, +, \cdot)$ is a ring and $S \subseteq R$ is itself a ring under the same operations (with the same multiplicative identity 1) then we call S a subring of R.*

For example, the integers $\mathbb{Z}$ are a subring of the rational numbers $\mathbb{Q}$.

As usual when dealing with rings we will write ab for $a \cdot b$ in general. We will write $-a$ for the additive inverse of a and $\sum_{i=1}^{k} a_i$ for $a_1 + \cdots + a_k$. Note there is no ambiguity in this expression as $(R, +)$ is associative and commutative. A double sum $\sum_{i,j=1}^{m,n} a_i b_j$ is equally unambiguous and stands for $a_1b_1 + a_1b_2 + \cdots + a_1b_n + \cdots + a_mb_1 + \cdots + a_mb_n$. However note in a noncommutative ring, it will be important to keep the a_i's to the left of the b_j's in each of the individual products!

Definition 1.3 (Group of units). *The group of units $U(R)$ of a ring $(R, +, \cdot)$ are the group of units of the monoid $(R, \cdot)$ i.e.,*

$$U(R) = \{u \in R | \exists v \in R \text{ such that } uv = 1 = vu\}.$$

Notice that in a ring $(R, +, \cdot)$, only distributivity relates the two operations. Thus it is only distributivity that adds anything new to the study of $(R, +, \cdot)$ over the separate study of the Abelian group $(R, +)$ and monoid $(R, \cdot)$ of the sort conducted in previous sections.

We prove some basic facts about rings next:

Proposition 1.4. *If R is a ring then*
(a) $0 \cdot x = 0$ for all $x \in R$.
(b) $-x = (-1) \cdot x$ for all $x \in R$.
(c) $(\sum_{i=1}^{k} a_i)(\sum_{j=1}^{m} b_j) = \sum_{i,j=1}^{k,m} a_i b_j$.

Proof. **Proof of (a):** Since (a) regards the behaviour of the additive identity 0 with regards to the other operation $\cdot$ we know the proof will use distributivity. Whenever we use distributivity, in a proof in this proposition, we will put a D over the equals sign. Hence we use:

$$0 \cdot x = (0 + 0) \cdot x \stackrel{D}{=} 0 \cdot x + 0 \cdot x.$$

Adding $-(0 \cdot x)$ to both sides we conclude $0 = 0 \cdot x$ as desired.

Proof of (b): Note

$$x + (-1) \cdot x = 1 \cdot x + (-1) \cdot x \stackrel{D}{=} (1 + -1) \cdot x = 0 \cdot x = 0$$

where in the last step we used part (a).

Thus $(-1) \cdot x$ is the additive inverse of x and hence $(-1) \cdot x = -x$.

Proof of (c): We first prove the case when $k = 1$ by induction on m. If $m = 1$ it is trivial, if $m = 2$ it follows from distributivity so assume $m > 2$ and that it is proven for all smaller m.

Then

$$a_1 \cdot (b_1 + \cdots + b_{m-1} + b_m) \stackrel{D}{=} a_1 \cdot (b_1 + \cdots + b_{m-1}) + a_1 \cdot b_m$$

By the induction hypothesis we have $a_1 \cdot (b_1 + \cdots + b_{m-1}) = a_1 b_1 + \cdots + a_1 b_{m-1}$, and so we have

$$a_1 \cdot (\sum_{k=1}^{m} b_k) = \sum_{k=1}^{m} (a_1 b_k)$$

as desired.

A similar proof works for the case $m = 1$ and k arbitrary.

Now we prove the general case by induction on k. For $k = 1$ we have proven it so suppose $k > 1$ and it has been proven for all smaller values.

Then

$$(\sum_{i=1}^{k} a_i)(\sum_{j=1}^{m} b_j) \stackrel{D}{=} (\sum_{i=1}^{k-1} a_i)(\sum_{j=1}^{m} b_j) + a_k(\sum_{j=1}^{m} b_j).$$

Thus by the induction hypothesis, we have

$$(\sum_{i=1}^{k} a_i)(\sum_{j=1}^{m} b_j) = \sum_{i,j=1}^{k-1,m} a_i b_j + \sum_{j=1}^{m} a_k b_j = \sum_{i,j=1}^{k,m} a_i b_j$$

as desired. □

Example 1.5 (Zero Ring). *Suppose R is a ring with $0 = 1$. Then by the previous proposition we have $x = 1 \cdot x = 0 \cdot x = 0$ for all $x \in R$.*

Thus $R = \{0\}$. This ring is called the zero ring.

Thus if R is a ring other than the zero ring, then $1 \neq 0$ in R. Since $0 \cdot x = 0$ for all $x \in R$, we conclude that 0 is never a unit in a nonzero ring.

From now on we will assume that a ring R is nonzero unless explicitly stated otherwise.

Lemma 1.6 (The importance of units). *Fix $a \in R$.*
The equations $ax = b$ and $xa = b$ have unique solutions $x \in R$ for any $b \in R$ if and only if a is a unit.

Proof. First assume a is a unit, thus a^{-1} exists and is unique as we have seen in our previous study of monoids. The equations $ax = b$ and $xa = b$ then have unique solutions $x = a^{-1}b$ and $x = ba^{-1}$ respectively.

Conversely if a is such that $ax = b$ and $xa = b$ have solutions for any b, then by setting $b = 1$ we find that a has both a right and left inverse in R. By monoid theory, this implies x has a two-sided inverse and hence is a unit. □

Since the equations $ax = b$ and $xa = b$ are basic to algebra, rings with more units generally pose less difficulties.

We have already seen that 0 is never a unit in a nonzero ring. Thus the rings where all other nonzero elements are units are particularly nice - we define these next:

Definition 1.7 (Division rings and Fields). *A nonzero ring R such that all nonzero elements are units is called a division ring.*

A field is a commutative division ring.

In a field, when $a \neq 0$, we will sometimes denote the unique solution of $ax = b$ by $\frac{b}{a}$. We will avoid this convention in a noncommutative division ring as in general $a^{-1}b \neq ba^{-1}$.

Example 1.8 (Basic Fields). *The reader should be familiar with the fields $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ of rational numbers, real numbers and complex numbers respectively, with their usual addition and multiplication.*

In the homework, you have also looked at the field $\mathbb{F}_p$ of integers modulo p under the induced addition and multiplication from the integers.

In the homework you will look at $\mathbb{H}$, the noncommutative division ring of quaternions which is a major example of a noncommutative division ring. It turns out to play major roles in both topology and number theory. Hamilton found this division ring, and hence the notation $\mathbb{H}$.

Note that if u is a unit and $ux = uy$ then it follows upon left multiplication by u^{-1} that $x = y$. However notice that $0x = 0 = 0y$ does not in general imply $x = y$. Thus a determination of the elements a which we may cancel in a ring is important. This motivates the next definition:

Definition 1.9. *If x and y are nonzero elements such that $xy = 0$ we say that they are a zero divisor pair. We call x a left zero divisor and y a right zero divisor.*

An element z that is both a left and a right zero divisor is called a zero divisor.

Notice that 0 is not considered a zero divisor by this definition.

Proposition 1.10 (Cancellation and Zero divisors). *Let R be a ring. Let a be a nonzero element of R.*
(1) $(ax = ay \implies x = y$ for all $x, y \in R) \leftrightarrow (a$ is not a left zero divisor).
(2) $(xa = ya \implies x = y$ for all $x, y \in R) \leftrightarrow (a$ is not a right zero divisor).

Proof. We will only prove (1). The proof of (2) is similar.
$\Leftarrow$: Suppose a is not a left zero divisor and $ax = ay$. Then $ax - ay = 0$ and hence $a(x - y) = 0$. Since a is not a left zero divisor, we have $x - y = 0$ and so $x = y$ as desired.
$\Rightarrow$: We prove the contrapositive. If a is a left zero divisor then there is nonzero x with $ax = 0 = a0$. Thus $ax = a0 \not\Rightarrow x = 0$. □

Since cancellation is in general desirable, this motivates the next definition:

Definition 1.11 (Integral Rings and Domains). *A ring R is called an Integral ring if it has no left or right zero divisors.*

A commutative Integral ring is called an Integral Domain (abbreviated as ID). In general the word domain will be reserved for concepts about commutative rings.

Note since units are never zero divisors, it follows that all division rings are integral rings and that all fields are integral domains.

In general any subring of a field is an integral domain as it inherits cancellation from the field. Thus for example $\mathbb{Z}$ is an integral domain (which is not a field itself).

Example 1.12 (Unique solutions in integral rings). *It is easy to see that in an integral ring R, given nonzero a, the equations $ax = b$ and $xa = b$ have at most one solution $x \in R$ for any given $b \in R$.*

For example consider $2x = b$ in the integral domain $\mathbb{Z}$. For b an odd integer, there is no solution for $x \in \mathbb{Z}$. For b an even integer, there is a unique solution for $x \in \mathbb{Z}$.

We now look at some further examples of rings:

Example 1.13 ($Mat_n(\mathbb{R})$). *The set of $n \times n$ matrices with real entries is denoted $Mat_n(\mathbb{R})$. It follows from basic linear algebra that $(Mat_n(\mathbb{R}), +, \cdot)$ is a ring where $+$ is the componentwise addition of matrices and $\cdot$ is matrix multiplication. (we will also prove this when we later consider the more general case of matrices with entries in a prescribed ring.)*

Recall from linear algebra that

$$\mathbb{A}adj(\mathbb{A}) = det(\mathbb{A})\mathbb{I} = adj(\mathbb{A})\mathbb{A}$$

for any $\mathbb{A} \in Mat_n(\mathbb{R})$.

Here $adj(\mathbb{A})$ *is the transpose of the cofactor matrix* $\mathbb{C}$ *whose* (i,j)*-entry is the determinant of* $\mathbb{A}(i,j)$*, where* $\mathbb{A}(i,j)$ *is the matrix obtained from deleting the* i*th row and* j*th column of* $\mathbb{A}$.

It follows from this identity that if $\mathbb{A} \neq \mathbb{O}$ *but* $det(\mathbb{A}) = 0$ *then* $\mathbb{A}$ *and* $adj(\mathbb{A})$ *form a zero divisor pair (in both orders) and so* $\mathbb{A}$ *is a zero divisor of* $Mat_n(\mathbb{R})$.

It also follows that if $det(\mathbb{A}) \neq 0$ *then* $\mathbb{A}^{-1} = \frac{1}{det(\mathbb{A})}Adj(\mathbb{A})$ *exists and so* $\mathbb{A}$ *is a unit.*

Thus in $Mat_n(\mathbb{R})$*, nonzero elements are either units or zero divisors.*

It also is easy to see from this discussion that $Mat_n(\mathbb{R})$ *is not an integral ring when* $n > 1$.

Note for example if $\mathbb{A} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ *then there exists infinitely many distinct matrices* $\mathbb{X}$ *with* $\mathbb{AX} = \mathbb{O}$ *and so the equation* $\mathbb{AX} = \mathbb{B}$ *may have infinitely many distinct solutions when* $\mathbb{A}$ *is a zero divisor!*

We will next deal with general matrices - but before that let us introduce a useful symbol:

Definition 1.14 (Kronecker delta symbol). *Given an index set* I *and* $i, j \in I$ *we define the Kronecker delta symbol* δ_{ij} *with values in a ring* R *as follows:*

$$\delta_{ij} = \begin{cases} 1 \text{ if } i = j \\ 0 \text{ if } i \neq j. \end{cases}$$

Notice in R *we have* $\sum_{j=1}^{n} a_j\delta_{jk} = a_k = \sum_{j=1}^{n} \delta_{jk}a_j$ *for any* $1 \leq k \leq n$*, and* $a_j \in R$.

Example 1.15 (Matrix ring of a general ring R**).** *Let* R *be a ring and* $Mat_n(R)$ *denote the set of* $n \times n$ *matrices with entries in* R*. Given* $\mathbb{A} \in Mat_n(R)$ *we denote the entry in the* i*th row and* j*th column of* $\mathbb{A}$ *by* $\mathbb{A}_{ij}$ *and refer to it as the* (i,j)*-entry.*

The identity matrix $\mathbb{I}$ *is defined by* $\mathbb{I}_{ij} = \delta_{ij}$ *where* δ_{ij} *is the Kronecker symbol.*

The zero matrix $\mathbb{O}$ *is defined by* $\mathbb{O}_{ij} = 0$ *for all* $1 \leq i, j \leq n$.

We define a binary operation of addition $+$ on $Mat_n(R)$ as follows: Given $\mathbb{A}, \mathbb{B} \in Mat_n(R)$ we define $\mathbb{C} = \mathbb{A} + \mathbb{B}$ by $\mathbb{C}_{ij} = \mathbb{A}_{ij} + \mathbb{B}_{ij}$.

Since $(R, +)$ is an Abelian group, it is a simple check that $(Mat_n(R), +)$ is an Abelian group with additive identity $\mathbb{O}$.

We define a binary operation of matrix multiplication $\cdot$ on $Mat_n(R)$ by $\mathbb{D} = \mathbb{A} \cdot \mathbb{B}$ given by $\mathbb{D}_{ij} = \sum_{k=1}^{n} \mathbb{A}_{ik}\mathbb{B}_{kj}$.

Since $\mathbb{A}_{ij} = \sum_{k=1}^{n} \mathbb{A}_{ik}\delta_{kj}$ and $\mathbb{B}_{ij} = \sum_{k=1}^{n} \delta_{ik}\mathbb{B}_{kj}$ it follows that $\mathbb{I}$ is a (two-sided) identity for $(Mat_n(R), \cdot)$.

Consider the product $(\mathbb{AB})\mathbb{C}$. A simple computation shows that its (i, s)-entry is given by $\sum_{j=1}^{n}(\sum_{k=1}^{n} \mathbb{A}_{ik}\mathbb{B}_{kj})\mathbb{C}_{js}$. By distributivity and associativity of R we may write this as $\sum_{j,k=1}^{n} \mathbb{A}_{ik}\mathbb{B}_{kj}\mathbb{C}_{js}$. A similar computation shows that we get the same expression when considering $\mathbb{A}(\mathbb{BC})$ and so we see that $(Mat_n(R), \cdot)$ is a monoid.

The (i, j)-entry of $\mathbb{C}(\mathbb{A}+\mathbb{B})$ is computed to be $\sum_{k=1}^{n} \mathbb{C}_{ik}(\mathbb{A}_{kj}+\mathbb{B}_{kj})$. Since R has distributivity, this is equal to $\sum_{k=1}^{n}[\mathbb{C}_{ik}\mathbb{A}_{kj} + \mathbb{C}_{ik}\mathbb{B}_{kj}]$. Rearranging the finite sum, we see that this is the same as the (i, j)-entry of the matrix $\mathbb{CA} + \mathbb{CB}$. Thus $\mathbb{C}(\mathbb{A} + \mathbb{B}) = \mathbb{CA} + \mathbb{CB}$. Similarly one can prove $(\mathbb{A} + \mathbb{B})\mathbb{C} = \mathbb{AC} + \mathbb{BC}$.

Thus we see that $(Mat_n(R), +, \cdot)$ is a ring in general. It is called the ring of $n \times n$ matrices with entries in the ring R.

The group of units of $Mat_n(R)$ is called the general linear group $GL_n(R)$.

Definition 1.16 (Homomorphisms). *A function $f : R_1 \to R_2$ between rings is called a homomorphism of rings if*
(1) $f : (R_1, +) \to (R_2, +)$ is a homomorphism of groups.
(2) $f : (R_1, \cdot) \to (R_2, \cdot)$ is a homomorphism of monoids.

Notice in particular that this requires $f(1) = 1$.

As usual, we have special names if f satisfies extra hypothesis:
f is called a monomorphism of rings if it is injective.
f is called an epimorphism of rings if it is surjective.
f is called an isomorphism of rings if it is bijective.

It is easily verified that the composition of two ring homomorphisms is a ring homomorphism, and that identity maps are ring homomorphisms.

Thus we have a category Ring whose objects are the rings, and whose morphisms are the ring homomorphisms. We let as usual $Hom_{Ring}(R_1, R_2)$ denote the set of ring homomorphisms between R_1 and R_2.

Given a ring R, we refer to the elements $Hom_{Ring}(R, R)$ as ring endomorphisms of R. This set forms a monoid under composition.

The group of units in the monoid is called the group of ring automorphisms of R and is denoted $Aut_{Ring}(R)$. The elements of $Aut_{Ring}(R)$ are called ring automorphisms of R.

Example 1.17. *Fix a ring R and positive integers n and m. Since $Mat_m(R)$ is itself a ring we may consider $Mat_n(Mat_m(R))$.*

The reader may easily verify that $Mat_n(Mat_m(R))$ is isomorphic as a ring to $Mat_{nm}(R)$.