1. ELEMENTARY PROPERTIES

§1.1. Definitions

Ring Theory is a part of abstract algebra. The other main part of abstract algebra is Group Theory, and it is assumed that you are already familiar with Group Theory. (See my notes on *Group Theory*.)

The abstract approach is one that considers many algebraic systems at the one time. At school you learnt about the systems of integers, real numbers and polynomials. At university you learnt about $n \times n$ matrices. These are all examples of rings.

In ring theory we study not just a few individual systems, but the whole world of this type of system. Some of the examples will be very useful – others will just be curiosities. You have heard of rings that give the wearer great powers. Abstraction gives a mathematician great power, in being able to prove theorems for a whole bunch of mathematical systems at once. So a ring will be defined as a mathematical system that satisfies certain properties, called the ring axioms. These form the basis of the theory. We don't ask what the objects that make up a ring. They

could be numbers, or polynomials, or matrices, or other mathematical entities that we've never even heard of.

As we develop ring theory we add additional properties, so that we study certain classes of rings. One of the goals of Ring Theory (as in Group Theory) is to classify all rings. This means finding concrete examples that are models for all abstract rings.

Of course this is a hopelessly impossible task. But what we can hope for is to classify certain classes of rings. In group theory we have a classification of all finite abelian groups, and all finite simple groups. (The former is fairly easy – the latter was an enormous project that was finally accomplished many years ago by an army of group theorists who wrote thousands of papers that complete this classification.)

In these notes we'll achieve the classification of finite fields of prime order (easy) and the nil-semisimple rings with descending chain condition on right ideals (hard). You probably don't know what 'nil-semisimple' or 'descending chain condition' mean. Don't worry – you will.

What distinguishes Ring Theory from Group Theory is that groups only have one binary operation which we call addition or multiplication. Rings have two operations which we call addition and multiplication. We could study them by focussing on just one operation at a time, but the Distributive Law, [$a(b + c) = ab + ac$] is a ring axiom that binds these two operations together. So, let's begin. What, exactly, is a ring?

A **ring** R is a set on which binary operations of + and × are defined such that:

- (R, +) is an abelian group,
- (R, ×) is a semigroup, that is, it is closed and associative,
- × is distributive over +.

I will write a × b as ab and powers as a^n in the usual way. Some books also insist that a ring has a multiplicative identity, but I don't. This means that ideals of rings, which we'll define shortly, can be considered as subrings.

As I said you've lived with particular rings for many years. You began your mathematical journey in kindergarten, or before, when you learnt to count. Then you learnt your addition and multiplication tables in primary school. But it wasn't until you learnt about negative numbers that you mastered your first ring, the ring of integers, which we denote by $\mathbb{Z}$.

By then you knew about fractions and so you had a knowledge of a second ring, the ring, $\mathbb{Q}$, the ring of rational numbers. You then learnt about decimals and hence you met a third ring of real numbers, $\mathbb{R}$, and then finally, the ring of complex numbers, $\mathbb{C}$.

But really, this was just one ring, with several important subrings. You learnt a fair amount of algebra, and you naively thought that the Laws of Algebra were always true.

When you met your next ring, the ring of polynomials, you just assumed that the algebra you first learnt would continue to apply. And by and large you were correct.

The two important Rules of Algebra that you learnt: the fact that you can multiply things in either order and get the same answer, and that if a product is zero then one of the factors must be zero. These continue to work for the ring of polynomials. Of course polynomials usually don't have inverses under multiplication, but you were fine with that. It didn't make a huge difference. You learnt things like the fact that quadratic equations have at most two solutions.

When you met matrices you met a ring where you had to learn the rules of algebra all over again. Both the Commutative Law for Multiplication and the Cancellation Law break down. So, too, do many of the 'facts' you had learnt about algebra that are built on these assumptions. For example, quadratic equations involving matrices can have infinitely many solutions. When you met the concept of similar matrices you wondered why, with an expression such as $S^{-1}DS$, you can't just cancel the S's. It then dawned on you that what you learnt at school only applied to numbers, real or complex. In effect, most of that algebra is just the algebra of fields, which are rather special types of ring.

Now, I said that a ring is an abelian group under addition and a semigroup under multiplication, with the distributive laws binding the additive and multiplicative structures together. But this is a very compact description. Let's flesh it out by listing all the ring axioms.

RING AXIOMS
(1) Closure Law for Addition: $a + b \in R$ for all $a, b \in R$.
(2) Associative Law for Addition: $(a + b) + c = a + (b + c)$ for all $a, b, c \in R$.
(3) Identity under Addition: There exists $0 \in R$ such that $a + 0 = a = 0 + a$ for all $a \in R$.
(4) Inverses under Addition: For all $a \in R$ there exists $-a \in R$ such that: $a + (-a) = (-a) + a$ for all $a \in R$.
(5) Commutative Law under Addition: $a + b = b + a$ for all $a, b \in R$.
(6) Closure Law under Multiplication: $ab \in R$ for all $a, b \in R$.
(7) Associative Law under Multiplication: $(ab)c = a(bc)$ for all $a, b \in R$.
(8) Distributive Laws: $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$ for all $a, b, c \in R$.

Axioms (1) – (4) are the axioms for a group, though we usually use multiplicative notation.
Axioms (1) – (5) are the axioms for an abelian group.
Axioms (6), (7) are the axioms for a monoid.
Axioms (1) – (8) are the axioms for a ring.

A **field** is a commutative ring in which there is an identity, 1, under multiplication, where $1 \neq 0$ and where every non-zero element has a multiplicative inverse. These extra axioms are as follows.

FIELD AXIOMS are the ring axioms plus
(9) Identity under Multiplication: There exists $1 \in R$, with $1 \neq 0$, such that $a1 = a = 1a$ for all $a \in R$.
(10) Inverses under Multiplication: For all $a \in R$ with $a \neq 0$, there exists $a^{-1} \in R$ such that: $aa^{-1} = 1 = a^{-1}a$ for all $a \in R$.
(11) Commutative Law under Multiplication: $ab = ba$ for all $a, b \in R$.

Axioms (1) – (10) are the axioms for a **division ring**.

You have met many examples of field, but you have probably never seen a division ring that isn't a field, That is because there are no finite examples of such non-commutative fields and it's not easy to provide a simple example of an infinite one. We may get to see one later.

§1.2. Elementary Properties

You'll notice that there are some Rules of Algebra that are missing. Some aren't there because they're not always true for rings in general, such as the commutative law for multiplication. Others are missing, even though they're true for all rings, because they can be deduced from the other axioms.

For example you'll be familiar with the fact that if you multiply by zero you get zero. This is, in fact, true for all rings but, because we can prove it from the other axioms, we omit it from the list of axioms.

Theorem 1: Let R be a ring. Then for all a, b $\in$ R:

(A) If a + b = a + c then b = c;

(B) a0 = 0 = 0a;

(C) (–a)b = –ab = a(–b);

(D)(–a)(–b) = ab.

Proof:

(A) (–a) + [a + b] = (–a) + [a + c]

$\therefore$ [(–a) + a] + b = [(–a) + a] + c by Axiom 2

$\therefore$ 0 + b = 0 + c by Axiom 4

$\therefore$ b = c by Axiom 3.

(B) $0 + a0 = a0 = a(0 + 0)$ by Axiom 3 twice
$= a0 + a0$ by Axiom 8
Hence $0 = a0$ by Theorem 1A.

(C) $ab + (-ab) = 0$ by Axiom 4
$= 0b$ by Theorem 1 (2)
$= [a + (-a)]b$ by Axiom 4
$= ab + (-a)b$ by Axiom 8
$\therefore -ab = (-a)b$ by Theorem 1A.
$a(-b) = -ab$ is proved similarly.

(D) $(-a)(-b) + (-ab) = (-a)(-b) + (-a)b$ by Theorem 1C
$= (-a)(-b + b)$ by Axiom 8
$= (-a)0$ by Axiom 4
$= 0$ by Theorem 1B
$= ab + (-ab)$ by Axiom 4
$\therefore (-a)(-b) = ab$ by Theorem 1 (1) and Axiom 5 ✋☺

Theorem 2 (Cancellation Law for Fields):
Suppose a, b, c are elements of the field F.
If $a \neq 0$ then $ab = ac$ implies that $b = c$.
Proof: Suppose $a \neq 0$. Then a^{-1} exists by Axiom 10.
Suppose that $ab = ac$.
$\therefore a^{-1}(ab) = a^{-1}(ac)$.
$\therefore (a^{-1}a)b = (a^{-1}a)c$ by Axiom 6.
$\therefore 1b = 1c$ by Axiom 10.
$\therefore b = c$ by Axiom 9.

There is a class of rings that lies between the commutative rings and field. An integral domain is a commutative ring with a multiplicative identity that satisfies the following axiom.

INTEGRAL DOMAIN AXIOMS are the ring axioms plus
(9) Identity under Multiplication: There exists $1 \in R$, with $1 \neq 0$, such that $a1 = a = 1a$ for all $a \in R$.
(11) Commutative Law under Multiplication: $ab = ba$ for all $a, b \in R$.
(13) If $ab = 0$ then $a = 0$ or $b = 0$.

Theorem 3 (Cancellation Law for Integral Domains):
Suppose a, b, c are elements of the integral domain R.
If $a \neq 0$ then $ab = ac$ implies that $b = c$.
Proof: Suppose that $ab = ac$.
$\therefore ab + (-ac) = 0$ by Axiom 4
$\therefore ab + a(-c) = 0$ by Theorem 1C
$\therefore a[b + (-c)] = 0$ by Axiom 8
$\therefore b + (-c) = 0$ by Axiom 13
$\therefore [b + (-c)] + c = 0 + c$
$\therefore b + [(-c) + c] = c$ by Axioms 2 and 3
$\therefore b + 0 = c$ by Axiom 4
$\therefore b = c$ by Axiom 3.

We define subtraction by $a - b = a + (-b)$ and we could provide a shorter proof of the above theorem by noting that $ab = ac$ implies that $a(b - c) = 0$ which, because $a \neq 0$, implies that $b = c$. However it is only an illusion that this proof is simpler because we are so used to basic algebra. To do things 'properly' we would need to prove a few properties of subtraction first.

Of course, from now on we won't be doing things 'properly' that is by highlighting every axiom as we proceed. That would be too tedious. When doing integral domain a you can more or less proceed using what you've learnt about the algebra of fields (the algebra you learnt at school) provided you don't use multiplicative inverse. When working with rings in general you must also avoid rearranging factors and cancelling.

In a general ring with multiplicative identity some elements may have multiplicative inverses. However you must not cancel the x's in an expression such as $x^{-1}yx$. The x and its inverse must be adjacent before you can cancel.

Consider the following 'proof' that an element of a ring has at most two square roots.

'Theorem': Suppose that $a^2 = b^2 = c$ in a ring.
'Proof': Suppose that $a^2 = b^2$
$\therefore a^2 - b^2 = 0$
$\therefore (a - b)(a + b) = 0$
$\therefore a - b = 0$ or $a + b = 0$.
$\therefore a = b$ or $a = -b$.

This is a valid proof for a field, and even for an integral domain. But we have unconsciously used two things that are not always true in a ring.

For a start $(a - b)(a + b) = a^2 + ab - ba - b^2$. This can only be simplified if $ab = ba$.

Secondly the cancellation law doesn't hold in a general ring.

Some of the ring axioms appear to contain redundant information. For example in Axiom 3 we say that $x + 0 = 0 = 0 + x$. This is so that the axioms can be independent of one another. But in the light of the commutative law of addition, which holds for all rings, this extra information is indeed redundant. But when we come to multiplication, which may be non-commutative, both parts of the axiom are required.

We say that e is a **left identity** for a ring R if $ex = x$ for all $x \in R$ and a **right identity** if $xe = x$ for all $x \in R$. It is only an identity, satisfying Axiom 9, if it is both a left identity and a right identity. There are rings that have a left identity and no right identity, and vice versa.

Example 1: Let R be the set of a 2×2 real matrices of the form $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$. Then $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ for all a, b and

so $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is a left identity for R. But $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ and so $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is not a right identity.

Similar remarks can be made about multiplicative inverses. Suppose R has a 2-sided identity, 1. We say that y is a **left inverse** for x if yx = 1 and we say that z is a **right inverse** for x if xz = 1.

There are rings with a 2-sided multiplicative identity,1, that have elements with a left identity and no right identity, and vice versa.
$\mathbb{N}$ $\mathbb{Z}$ $\mathbb{Q}$ $\mathbb{R}$ $\mathbb{C}$

Example 2: Let R = {f: $\mathbb{R} \to \mathbb{R}$} with:
$(f + g)(x) = f(x) + g(x)$ and
$(fg)(x) = g(f(x))$.
Clearly R has a 2-sided identity, namely the identity function $1(x) = x$.
Let $e(x) = e^x$ and let $g(x) = \begin{cases} \log x \text{ if } x > 0 \\ 1 \text{ if } x \le 0 \end{cases}$
Then $(eg)(x) = g(e(x)) = g(e^x) = \log(e^x) = x$.
But if $(ge)(x) = e(g(x)) = x$ then $e^{g(x)} = x$, which is not possible if $x \le 0$.

So $e(x)$ has a left inverse, but no right inverse. In fact it has infinitely many left inverse since we could define $g(x)$ any way we liked for $x \le 0$ and it would still be a left inverse. A similar example can be constructed for right inverses.

However if an element of a ring has a left inverse and a right inverse, they must be equal and so there can only be one of each.

Theorem 4: Suppose R is a ring with a 1.
If $x \in R$ has a left inverse, a, and a right inverse, b, then $a = b$. This will be the only left inverse and the only right inverse.
Proof: $a = a1 = a(xb) = (ax)b = 1b = b$.

The concepts of left and right inverse are connected with the properties of functions being 1-1 and/or onto. A function $f:S \to S$ has a left inverse if and only if it is 1-1 and a right inverse if and only if it is onto.

An element of a ring is called a **unit** if it has a multiplicative inverse. In a field every non-zero element is a unit, while in $\mathbb{Z}$ there are just two units, 1 and –1. The units of $M_n(F)$ are the non-singular, or invertable matrices. The set of units of R is denoted by $\mathbf{R}^{\#}$.

Theorem 5: If R is a ring with a 1, $(R^{\#}, \times)$ is a group.
Proof: Suppose that $u, v \in R^{\#}$.
Then u^{-1} and v^{-1} exist, and are in R.
Now $(uv)(v^{-1}u^{-1}) = u(vv^{-1})u^{-1} = 1$.
Moreover $(v^{-1}u^{-1})(uv) = 1$.
Hence $(uv)^{-1}$ exists and is equal to $v^{-1}u^{-1}$, so $uv \in R^{\#}$.
Also $u^{-1} \in R^{\#}$ since $(u^{-1})^{-1}$ and $1 \in R^{\#}$.

§1.3. Rings of Small Order

A **zero** ring is one where every product is 0. Essentially the structure is just that of the additive group.

Given any abelian group G, we define **Zero(G)** to be the zero ring on G, that is where we define $xy = 0$ for all $x, y \in G$. Clearly this multiplication is associative!

We'll now embark on a quest to classify all finite rings. However, we won't get very far because the number of possibilities will soon get out of hand.

We begin with the smallest ring, which is {0}. With 2 elements, they'll be 0 and x, with $x^2 = 0$ or x. Clearly in the first case we get Zero($\mathbb{Z}_2$) and in the second case we get the ring $\mathbb{Z}_2$. These $\mathbb{Z}_2$'s look the same but in the first case it's the abelian group and in the second case it's the ring.

Theorem 6: If R is a ring of prime order p then

$$R \cong \text{Zero}(\mathbb{Z}_p) \text{ or the ring } \mathbb{Z}_p.$$

Proof: The additive group is a group of order p which, from our knowledge of group theory, means that it has to be the cyclic group $\mathbb{Z}_p$.

So R = {0, x, 2x, …, (p−1)x}. The multiplication is completely determined by knowing x^2. Clearly $x^2 = kx$ for some k with $0 \le k < p$.

Case 1: $k = 0$: Then $R \cong \text{Zero}(\mathbb{Z}_p)$.

Case 2: $k > 0$:

Then k^{-1} exists as an element of the field $\mathbb{Z}_p$.

Define $\Phi: R \to \mathbb{Z}_p$ by $r\Phi = k^{-1}r$.

Then $(ax + bx)\Phi = k^{-1}(ax + bx)$
$= k^{-1}(ax) + k^{-1}(bx)$
$= (ax)\Phi + (bx)\Phi$.
Also $[(ax)(bx)]\Phi = [abx^2]\Phi = [(ab)kx]\Phi = k^{-1}(ab)x$ and
$(ax)\Phi(bx)\Phi = (k^{-1}ax)(k^{-1}bx)$
$= k^{-2}abx^2 = k^{-2}abkx = k^{-1}(ab)x$.
Then Φ is clearly a ring isomorphism, and so R is isomorphic to the field $\mathbb{Z}_p$. ✋☺

Theorem 7: There are 11 rings of order 4.
Three of them have additive group $\mathbb{Z}_4$ and the elements will have the form 0, x, 2x, 3x.
Eight of them have additive group $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ and the elements will have the form 0, a, b, a + b.
The multiplication tables are as follows. (Multiplication by 0 is omitted to save space.)

R1	**x**	**2x**	**3x**
x	0	0	0
2x	0	0	0
3x	0	0	0

Zero($\mathbb{Z}_4$)

R2	**x**	**2x**	**3x**
x	x	2x	3x
2x	2x	0	2x
3x	3x	2x	x

$\mathbb{Z}_4$

R3	**x**	**2x**	**3x**
x	2x	0	2x
2x	0	0	0
3x	2x	0	2x

R4	**a**	**b**	**a+b**
a	0	0	0
b	0	0	0
a+b	0	0	0

Zero($\mathbb{Z}_2 \oplus \mathbb{Z}_2$)

R5	a	b	a+b
a	0	0	0
b	0	b	b
a+b	0	b	b

$\mathbb{Z}_2 \oplus \mathbb{Z}_2$

R6	a	b	a+b
a	a	0	a
b	0	b	b
a+b	a	b	a+b

$\mathbb{Z}_2 \oplus$ Zero($\mathbb{Z}_2$)

R7	a	b	a+b
a	a	b	a+b
b	b	a+b	a
a+b	a+b	a	b

GF(4)

R8	a	b	a+b
a	a	b	a+b
b	a	b	a+b
a+b	0	0	0

R9	a	b	a+b
a	0	a	a
b	a	b	a+b
a+b	a	a+b	b

R10	a	b	a+b
a	b	0	b
b	0	0	0
a+b	b	0	b

R11	a	b	a+b
a	a	a	0
b	b	b	0
a+b	a+b	a+b	0

Proof: omitted.

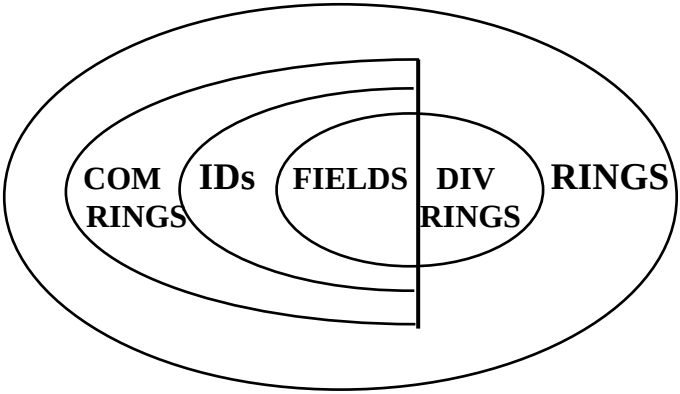
There are 11 rings of order p^2 for all primes p and they correspond to the above. See Benjamin Fine: *Classification of Finite Rings of Order* p^2 Mathematics Magazine Vol 66 No 4, Oct 1993 p248. ✋

Here are the numbers of rings of order up to 16:

order	1	2	3	4	5	6	7	8	9
# rings	1	2	2	11	2	4	2	52	11

order	10	11	12	13	14	15	16
# rings	4	2	22	2	4	4	390

§1.4. Examples of Rings



Perhaps the only field that you know is the field of complex numbers, and its many subfields. Less familiar examples are some of the finite fields, integers modulo a prime. There are other finite fields. These are discussed in my notes on *Galois Theory*. A really big field is the field of all rational functions. These have the form $\frac{a(x)}{b(x)}$ where $b(x) \neq 0$. They add and multiply in the usual way.

When it comes to integral domains we'll need to look to infinite examples, because finite integral domains are, in fact, fields.

Theorem 8: Every finite integral domain is a field.
Proof: Let R be an integral domain of finite order *n*.
Let R and let x be a non-zero element of R.
By the Cancellation Law, multiplication by x is 1-1.
Since R is finite this function is onto.
So, xy = 1 for some y $\in$ R, and so x has a multiplicative inverse. ✋☺

So if all finite integral domains are fields, the interesting ones will be infinite. Many of these are subrings of the field of complex numbers, such as the ring of Gaussian Integers, complex numbers of the form $a + bi$ where a, b are integers. But another familiar example of an integral domain is the ring of real polynomials F[x].

As I said we will have to wait for an example of a division ring that's not a field.

When it comes to non-commutative rings, the obvious place to look is the ring of $n \times n$ matrices, and its many subrings.

§1.5. The Isomorphism Theorems

A non-empty subset S of a ring is a **subring** if it is closed under +, − and ×. We use the same notation as for groups: $S \leq R$.

Examples 3:
$\mathbb{Z} \leq \mathbb{Q}$. The set of matrices with determinant 1 is a subring of $M_n(F)$, the ring of $n \times n$ matrices over the field F.

A **left ideal** I, of R, is a subring where $rx \in I$ for all $r \in R$ and $x \in I$. That is you can multiply any element of I on the left by any element of R and it remains in I.

A **right ideal** I, of R,is a subring where $xr \in I$ for all $r \in R$ and $x \in I$.

An **ideal** (sometime we'll say '2-sided ideal' is one that is both left and right.

A useful piece of notation is the product **ST** of two subrings of R. ST is the set of all sums and differences of products st, where $s \in S$ and $t \in T$. So ST is the set of all elements of the form $\pm s_1t_1 \pm s_2t_2 \pm \ldots \pm s_nt_n$ for some n and some $s_i \in S$ and $t_i \in T$. In general ST is not a subring, because $s_1t_1s_2t_2$ may not be able to be written as an element of S times an element of T. However if either S or T is at least a one-sided ideal ST may be, not only a subring, but also at least a one-sided ideal.

Theorem 9:
(1) Suppose S is a left ideal of R and T is a subring.
Then ST is a left ideal of R.
(2) Suppose T is a right ideal of R and S is a subring.
Then ST is a left ideal of R.
Proof: To show that ST is a subring it is sufficient to prove that products of the form $s_1t_1s_2t_2$ are in ST whenever $s_{1,}\, s_2 \in S$ and $t_1, t_2 \in T$ since the product of elements of ST will be a sum of elements of this form.
Suppose $s_1, s_2 \in S$ and $t_1, t_2 \in T$.
(1) Suppose that S is a left ideal. Then $t_1s_2 = s_3$ for some $s_3 \in S$ and so $s_1t_1s_2t_2 = s_1s_3t_2$ which is contained in ST. Clearly ST is a left ideal, since S is.
(2) Suppose that T is a right ideal. Then $t_1s_2 = t_3$ for some $t_3 \in T$ and so $s_1t_1s_2t_2 = s_1t_3t_2$ which is contained in ST. Clearly ST is a right ideal, since T is.

In particular, $R^2 = RR$ is a 2-sided ideal of R. Just remember that R^2 contains more than just the squares of the elements of R. It consists of all sums of products of elements of R.

We can extend this multiplication of ideals to many factors. In particular, for any $n \geq 1$, R^n is the 2-sided ideal generated by all products with n factors.

A ring R is **nilpotent** if $R^n = 0$ for some n. This means that every product with sufficiently many factors is 0. Clearly a nilpotent ring cannot contain a multiplicative identity.

A related concept is that of a **nilpotent element**. The element x is nilpotent if $x^n = 0$ for some n.

We use the same notation for 2-sided ideals as for normal subgroups: $I \trianglelefteq R$.

The **trivial ideal** is $\{0\}$, which we denote by the same symbol, **0**.

A **proper ideal** is one that is not the ring itself. We will often talk about a proper non-trivial ideal, meaning one that lies between the two extremes.

A **maximal ideal** of a ring R, is a proper ideal, M, where there's no ideal, I, with $M < I < R$. A **minimal ideal** of a ring R, is a non-trivial ideal, M, where there's no ideal, I, with $0 < I < M$.

We extend the adjectives to left ideals, right ideals and subrings.

Examples 4:
(1) $2\mathbb{Z} \trianglelefteq \mathbb{Z}$. In fact it is a maximal ideal. $\mathbb{Z}$ has no minimal ideals.
(2) The set of matrices of the form $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ is a left ideal of the ring of matrices over a field but it's not a right ideal. It is, in fact a minimal left ideal. This is left as an exercise.

The **sum** of two subrings S and T of a ring R is:
$\mathbf{S + T} = \{s + t \mid s \in S, t \in T\}$.

The **intersection** of two subrings S and T of a ring R is $S \cap T$, as usual.

If S, T are 2-sided ideals of R and $S \cap T = 0$ we say that the sum is a **direct sum** and write it as $\mathbf{S \oplus T}$.

If S, T are any two rings, their (external) direct sum is
$\mathbf{S \oplus T} = \{(s, t) \mid s \in S, t \in T\}$.

Example 5:
$15\mathbb{Z} + 27\mathbb{Z} = 3\mathbb{Z}$. This is because GCD(15, 27) = 3 and so 3 can be written in the form 15h + 27k. with $h, k \in \mathbb{Z}$.

$15\mathbb{Z} \cap 27\mathbb{Z} = 135\mathbb{Z}$ since LCM(15, 27) = 135.

$(15\mathbb{Z})\ (27\mathbb{Z}) = 405\ \mathbb{Z})$ since $15 \times 27 = 405$.

$135\mathbb{Z} = 27\mathbb{Z} \oplus 5\mathbb{Z}$ but we can't write it as $15\mathbb{Z} \oplus 27\mathbb{Z}$ because their intersection is not zero.

If I is a 2-sided ideal of the ring R then the **quotient ring R/I** is defined to be $\{a + I \mid a \in R\}$, made into a ring under the operations:

$(a + I) + (b + I) = (a + b) + I$;
$(a + I)(b + I) = ab + I$

It's easy to check that these are well-defined operations, that is, they are independent of the representatives. Remember that $a + I = b + I$ if and only if $b - a \in I$.

Example 6: If *m* is an integer the set of all multiples is a 2-sided ideal. That is, $m\mathbb{Z} \trianglelefteq \mathbb{Z}$.
The coset $5 + 7\mathbb{Z} = \{\ldots, -9, -2, 5, 12, 17, \ldots\}$.
Note that this is also $17 + 7\mathbb{Z}$.
In $\mathbb{Z} / 7\mathbb{Z}$ we have $(5 + 7\mathbb{Z}) + (4 + 7\mathbb{Z}) = 9 + 7\mathbb{Z} = 2 + 7\mathbb{Z}$.
And $(5 + 7\mathbb{Z})(4 + 7\mathbb{Z}) = 20 + 7\mathbb{Z} = 6 + 7\mathbb{Z}$.
Apart from the notation, this is what we think of when we talk about the integers modulo 7. In fact we define the ring of integers mod 7 by $\mathbb{Z}_7 = \mathbb{Z}/7\mathbb{Z}$.

Ring homomorphisms are functions, or maps that take sums to sums and products to products. But, before we express this in symbols, let me explain the notation that we'll be using for functions. Instead of the usual $\varphi(x)$ we'll write the image of x under φ as $x\varphi$. This may look a bit strange, but when it comes to composition of functions it will seem more natural.

The **product** of two functions $\varphi: S \to T$ and $\theta: T \to U$ is $\varphi\theta: S \to U$ where $x(\varphi\theta) = (x\varphi)\theta$. This looks like an associative law, though x, φ and θ come from different sets. This is like the **composition** of functions, only backwards. You may remember that $\theta \circ \varphi$ was defined by $(\theta \circ \varphi)(x) = \varphi(\theta(x))$. So with $\theta \circ \varphi$ you have to remember that φ is applied first. With our new notation the functions

are employed in the order in which they're written – from left to right.

If R, S are rings a map $\varphi: R \to S$ is a **homomorphism** if, for all $a, b \in R$:

(1) $(a + b)\varphi = a\varphi + b\varphi$;

(2) $(ab)\varphi = (a\varphi)(b\varphi)$.

A homomorphism φ is an **isomorphism** if it is 1-1 and onto.

If there exists an isomorphism $\varphi: R \to S$ we say that R is **isomorphic to** S, and we write $R \cong S$.

An **automorphism** of R is an isomorphism from R to R.

The **kernel** of a homomorphism $\theta: R \to S$ is

$$\textbf{ker } \theta = \{r \in R \mid r\theta = 0\}.$$

The **image** of θ is $\textbf{im } \theta = \{r\theta \mid r \in R\}$, as usual.

Example 7: If $f(x)$ is a polynomial in x, with integer coefficients, we can define $\varepsilon: \mathbb{Z}[x] \to \mathbb{Z}$ by:
$f(x)\,\varepsilon$ = the square of the sum of the coefficients of f(x), which is $f(1)^2$. It's obvious that f is a homomorphism.
$\ker \varepsilon = \{f(x) \in \mathbb{Z}[x] \mid f(1) = 0.\} = (x - 1)\,\mathbb{Z}[x]$ and
$\text{im } \varepsilon = \{0, 1, 4, 9, 16, \ldots\}$ the set of perfect squares.

In the same way as in group theory we have the three isomorphism theorems.

Theorem 10 (FIRST ISOMORPHISM THEOREM):
If $\varphi:R\to S$ is a homomorphism and
$K = \ker \varphi$ then $K \trianglelefteq R$ and $R/K \cong \text{im } \varphi$.
Proof: Define $\Psi:R/\ker \varphi \to \text{im } \varphi$ by $(r + K)\Psi = r\varphi$. ✋☺

Theorem 11 (SECOND ISOMORPHISM THEOREM):
If $S \leq R$ and $T \trianglelefteq R$ then $S \cap T \trianglelefteq S$ and

$$(S + T)/T \cong S/(S \cap T).$$

Proof: Define the homomorphism $\varphi:S\to ST/T$ by
$s\varphi = s + T$ and use the First Isomorphism Theorem. ✋☺

Theorem 12 (THIRD ISOMORPHISM THEOREM):
If $I, J \trianglelefteq R$ then $J/I \trianglelefteq R/I$ and $R/J \cong (R/I)/(J/I)$.
Proof: Define $\varphi:R/I \to R/J$ by $(r + I)\varphi = r + J$. We can show that this is well-defined. Now use the First Isomorphism Theorem. ✋☺

A ring R is **simple** if R is not a zero ring and 0 and R are the only 2-sided ideals of R. A commutative ring with 1 is simple if and only if it is a field.

Theorem 13: $M_n(F)$ is simple.
Proof: Suppose I is a non-zero ideal of $M_n(F)$, let $A = (a_{ij})$ be a non-zero element of I and let $a_{rs} \neq 0$. By pre- and post- multiplying by suitable matrices we can make all other components zero. By multiplying by a suitable scalar matrix we can make this non-zero component take any desired value, and by pre- and post- multiplying by suitable permutation matrices we can move this to any

position. All these products will remain within I. Now, adding such matrices together we can thus obtain any $n \times n$ matrix and so $I = M_n(F)$.

If G is a (multiplicative) group, we define the **group ring** to be the set of all formal linear combinations of the elements of G with addition and multiplication defined in the obvious way. It is denoted by FG.

So **FG** = $\{\Sigma\lambda_i g_i \mid \lambda_i \in F, g_i \in G\}$. The group elements are a basis for FG and so, if G is finite, FG is finite-dimensional.

A ring R has the **descending chain condition** (**DCC**) on right ideals if every descending chain of right ideals has a least. That is, if

$$I_0 \geq I_1 \geq I_2 \geq \ldots$$

is an infinite sequence of right ideals, each containing the next, then for some n, $I_n = I_{n+1} = \ldots$ Another way of expressing DCC on right ideals is that there's no infinite strictly descending sequence of right ideals:

$$I_0 > I_1 > I_2 > \ldots$$

DCC on left ideals and DCC on 2-sided ideals are defined similarly. A ring R has the **ascending chain condition** (**ACC)** on right ideals if every ascending chain of right ideals has a greatest. ACC on left ideals and ACC on 2-sided ideals are defined similarly.

Example 8: $\mathbb{Z}$ has the ascending chain condition but not the descending chain condition on ideals.

Proof: The ideals of $\mathbb{Z}$ all have the form $m\mathbb{Z}$ for $m \in \mathbb{Z}$, where $m \geq 0$.

If $m\,\mathbb{Z} < n\,\mathbb{Z}$ then n is a proper divisor of m, and so $n < m$. If there was an infinite strictly increasing ideals in $\mathbb{Z}$ then there would be an infinite strictly decreasing chain of non-negative integers.

However $\mathbb{Z} > 2\,\mathbb{Z} > 4\,\mathbb{Z} > 8\,\mathbb{Z} > \ldots$ is an infinite strictly descending chain of ideals and so $\mathbb{Z}$ does not satisfy the DCC.

§1.6. Algebras

Most rings of any interest come with even more than just the ring structure. They're also vector spaces. An **algebra** over a field F, or an **F-algebra**, is a ring A that is also a vector space over F. Definitions for rings extend quite naturally to algebras, such as subalgebras, algebra homomorphisms (ring homomorphisms that are also linear transformations), and direct sums. Algebra ideals are ring ideals that are subspaces and quotient algebras are formed in the usual way. As you'd expect, all three isomorphism theorems hold.

If you think of some of the important rings you've met you'll find that they are automatically algebras. Fields are algebras over themselves. The ring of polynomials over a field F is an algebra over F. The ring of $n \times n$ matrices over F is an F-algebra. One can make every vector space into an algebra (a zero algebra) by

defining every product to be zero. Not all interesting rings, however, are algebras. For example the archetypal ring, the ring of integers is not an algebra.

The theory of algebras is not really a separate study from the theory of rings. In fact often, we use the terms interchangeably (provided the ring can easily be viewed as an algebra).

An important way of constructing examples of rings is to take a semigroup and to take all formal linear combinations of these elements over some field. A **semigroup algebra** is one formed from a semigroup in the following way. If X is a semigroup and F is a field, then $\mathbf{FX} = \{\lambda_1 x_1 + \ldots + \lambda_n x_n \mid n \geq 0$ and $\lambda_i \in F, x_i \in X$ for each $i\}$. Here, if $n = 0$ we take the empty sum to be the zero element.

If X is the semigroup $\{1, x, x^2, \ldots,\}$, under the usual multiplication, and F is any field, then FX is simply $F[x]$ the ring (in fact the algebra) of polynomials over F.

You can construct the ring of $n \times n$ matrices over F in this way by taking the semigroup made up from the standard basis matrices E_{ij} that have a 1 in the i-j position and zeros elsewhere.

One can construct algebras one has never met in this way.

Example 9: Let S be any set and define multiplication by:

$$xy = y \text{ for all } x, y \in S.$$

The associative law holds for S and so S is a semigroup. We can make S into an algebra, $\mathbb{Z}_3$S. In this algebra:

$(2s + t)(s + 2t) = 2s^2 + ts + 4st + 2t^2$

$= 2s^2 + ts + st + 2t^2$ since $4 = 1$ in $\mathbb{Z}_3$

$= 2s + s + t + 2t$ using the semigroup multiplication

$= 3s + 3t = 0$

A special case of semigroup algebras are group algebras. These are simply algebras where we start with a group G as our semigroup. Algebras of the form FG, where F is a field and G is a group, are important in the Representation Theory of groups. These are studied in my set of notes on *Representation Theory*.

§1.7. Some Interesting Examples of Rings

We finish the chapter with more examples of rings and algebras. These are in different ways quite curious and some will be used in later chapters as counter-examples.

Example 10: The Prüfer 2-group is:

$$P = \langle a_0, a_1, a_2, .. \mid 2a_0 = 0, 2a_{i+1} = a_i \text{ for each } i \rangle$$

It is an infinite abelian group. Moreover it's not even finitely generated. Yet every proper subgroup is a finite cyclic group of order 2^n, for some n. Therefore all the elements have finite order.

The generator a_0 has order 2, a_1 has order 4, and so on. In general the generator a_n has order 2^{n+1}. The elements are of the form:

$m_0a_0 + m_1a_1 + \ldots + m_ka_k$ for some k, with the $m_i \in \mathbb{Z}$.

But since $2a_{i+1} = a_i$ for all i, and $2a_0 = 0$, we may assume that each $m_i = 0$ or 1.

So every element can be written in the form:

$a_{n_1} + a_{n_2} + \ldots + a_{n_k}$ for some k, where

$$n_1 < n_2 < \ldots < n_k.$$

Then $(a_2 + a_3 + a_4) + (a_1 + a_3 + a_4) = a_1 + a_2 + 2a_3 + 2a_4$

$= a_1 + a_2 + 3a_3$

$= a_1 + 2a_2 + a_3$

$= 2a_1 + a_3$

$= a_0 + a_3$.

Now consider the zero ring on P. So the product of any two generators $a_ia_j = 0$. Then $P^2 = 0$.

Example 11: Let $\Omega = \left\{\frac{2m}{2n+1}\right\}$ with $m, n \in \mathbb{Z}$.

It's easy to show that this is a subring of $\mathbb{Q}$.

It's not an algebra over $\mathbb{Q}$ since R contains $\frac{1}{3}$ but not $\frac{1}{6}$.

And since $\mathbb{Q}$ has no proper subfields, it can't be an algebra over any other field. So this is a good counter-example to show that some rings are not algebras. Yet we file this example away as a counterexample to something else in a later chapter.

Example 12: Matrices are normally finite, but there's no reason why we can't consider infinite matrices as infinite arrays, with infinitely many rows and columns. The only trouble that can arise is if we want to make a ring out of these because a product will involve infinitely many terms. One way to get a ring out of infinite matrices is to restrict the rows to only have finitely many non-zero entries. We will still have infinitely many terms if we multiply two such matrices, but all but a finite number of these will be zero.

A **row finite matrix**, over a field F, is an infinite matrix in which every row has only finitely many non-zero components. That is, for all r there exists N such that $a_{rs} = 0$ whenever $s >$ N. The number N depends on r and it might be that, for example N = r. In fact such a matrix would be lower-triangular, with zeros above the diagonal.

The set of all row finite matrices over F is then an F-algebra. The set of all lower-triangular matrices over F will be a subalgebra.

Example 13: Let $\mathbb{Z}_2\langle x, y\rangle$ be the $\mathbb{Z}_2$ algebra of all rational functions, over $\mathbb{Z}_2$, in non-commuting indeterminates x, y. These are formal fractions of the form $\dfrac{f(x, y)}{g(x, y)}$ where $f(x, y)$ and $g(x, y)$ are polynomials, over $\mathbb{Z}_2$ in the non-commuting variables x, y. A typical element could be:

$$\frac{x^5y + yxy^2}{xy + yx}.$$

These add and multiply in the obvious way, but without the benefit of the equation $xy = yx$. These fractions are formal fractions so that we can't even cancel by x in the above example. So, for example:

$$\frac{xy}{y+1} + \frac{y^2}{xy+yx} = \frac{xy(xy+yx) + y^2(y+1)}{(y+1)(xy+yx)}$$
$$= \frac{xyxy + xy^2x + y^3 + y^2}{yxy + y^2x + xy + yx}$$

Example 14: Let $X = \{a_x \mid x \in \mathbb{Q} \text{ and } 0 < x < 1\}$. That is, X consists of indeterminates indexed by the rational numbers between 0 and 1 (excluding both). Examples of elements of X will be $a_{0.5}$, $a_{0.3}$ and $a_{0.0001}$.
We make X into a semigroup be defining:

$$a_x a_y = \begin{cases} a_{x+y} \text{ if } x + y < 1 \\ 0 \text{ if } x + y \geq 1 \end{cases}.$$

One needs to check that this operation is associative. But it's not difficult to see that, regardless of brackets, any product is a_T where T is the sum of the subscripts in the product, or 0 if this total is greater than or equal to 1.
So $a_{0.3}\, a_{0.6} = a_{0.9}$ and $(a_{0.6})^2 = 0$ since $1.2 > 1$.

Consider the semigroup algebra $\mathbb{R}X$. This will be an $\mathbb{R}$-algebra. An example of a calculation in this algebra is:
$(\pi a_{0.2} + \sqrt{2}a_{0.6})(3a_{0.1} + a_{0.5})$
$= 3\pi a_{0.2}\, a_{0.1} + \pi a_{0.2}\, a_{0.5} + 3\sqrt{2}a_{0.6}\, a_{0.1} + \sqrt{2}a_{0.6}\, a_{0.5}$
$= 3\pi a_{0.3} + (\pi + 3\sqrt{2})a_{0.7}$.

This is an example of a ring in which every element is nilpotent, while the ring itself is not.

Example 15: Let $R = \{ax + by \mid a, b \in \mathbb{Q}\}$ where:

$$x^2 = x,\ yx = y,\ xy = y^2 = 0.$$

This looks like it be yet another example of a semigroup algebra, but note that {x, y} is not a semigroup since it doesn't contain 0, yet $y^2 = 0$.

The associative law isn't obvious but we can prove it as follows.

- (xx)x = x(xx) simplifies to x = x,
- (yx)x = y(xx) simplifies to y = y
- all other instances of the associative law involving x, y simplify to 0 = 0.

Another proof of the associative law involves constructing an isomorphic model of this ring within the ring of 2×2 matrices by taking $x = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. As well as checking that they satisfy the equations we must also check that they are additively independent.

So R is a $\mathbb{Q}$-algebra. It looks like it might be an example of an algebra that's not a semigroup algebra. Yet, if we take A = x and B = x + y we get $A^2 = AB = A$, $BA = B^2$ and so {A, B} is a semigroup, S with multiplication table:

	A	B
A	A	A
B	B	B

Since {A, B} is a basis for R, R is the semigroup algebra $\mathbb{Q}S$.

EXERCISES FOR CHAPTER 1

Exercise 1: Which of the rings of order 4 are zero rings, commutative rings, rings with 1, integral domains, nilpotent, simple?

Exercise 2: Find all the non-trivial proper left ideals, right ideals, 2-sided ideals of the rings R1 to R11, of order 4.

Exercise 3: Show that no two rings R1–R11 are isomorphic.
HINT: Find ring-theoretic properties that distinguish them, such as

- Is the ring under addition cyclic?
- Does the ring have a 1?
- Is the ring a zero ring?
- Is the ring a field?
- Does the ring have **nilpotent elements**? (These are non-zero elements r where $r^n = 0$ for some n.)

Exercise 4: Show that $I = \begin{pmatrix} * & 0 \\ * & 0 \end{pmatrix}$, meaning the set of all matrices of the form $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$, is a minimal left ideal of the ring $R = M_2(F)$, for any field F.

Exercise 5:
(a) Prove that R = $\{ax + by \mid a, b \in \mathbb{Q}\}$ is a $\mathbb{Q}$-algebra where: $x^2 = 0$, $xy = yx = x$, $y^2 = y$.
(b) Show that the only non-zero idempotent of R (that's an element that equals its own square) is y.
(c) Show that R is not a semigroup algebra $\mathbb{Q}X$ for any semigroup X.

SOLUTIONS FOR CHAPTER 1

Exercise 1:
Zero: R1, R4.
Commutative: R1,l R2, R3, R4, R5, R6, R7, R9, R10.
Ring with 1: R2, R6, R7, R9.
Integral Domain: R7.
Nilpotent: R1, R3, R4.
Simple: R7.

Exercise 2:
R1 – R3: Here the additive group is $\mathbb{Z}_4$, and so the only possibility is $\{0, 2x\}$.
In fact, $\{0, 2x\}$ is a 2-sided ideal in all three cases.

For the rings **R4-R11** you scan the rows for right ideals and the columns for left ideals.
$\{0, u\}$, where u = a, b or a+ b, will be a right ideal if the elements in the u-row are 0 or u.
$\{0, u\}$, will be a right ideal if the elements in the u-column are 0 or u.

R4: {0, a}, {0, b} and {0, a + b} are all 2-sided ideals.
R5, R6: {0, a}, {0, b} are both 2-sided ideals.
R7: No ideals, left, right or 2-sided. Note that R7 is a field and field never have proper non-trivial ideals.
R8: {0, a} and {0, b} are left ideals. {0, a + b} is a 2-sided ideal.
R9: {0, a} is a 2-sided ideal.
R10: {0, b} is a 2-sided ideal.
R11: {0, a} and {0, b} are right ideals and {0, a + b} is a 2-sided ideal.

Exercise 3: We just need to investigate various ring-theoretic properties to distinguish them.

	cyclic under +	**has 1**	**zero ring?**	**Nilpt elts?**
R1	√		√	√
R2	√	√		√
R3	√			√
R4			√	√
R5				√
R6		√		
R7		√		
R8				√
R9		√		√
R10				√
R11				√

By considering these properties alone, R1-R5 and R9 are not isomorphic to any other.
We still need to distinguish between R6 and R7 and between R8, R10 and R11.
Now R7 is a field and R6 is not, so they are not isomorphic.
R10 is commutative, while R8 and R11 are not.
So this just leaves the question as to whether R8 and R11 are isomorphic. In fact they are anti-isomorphic in that there exists Φ:R8 $\rightarrow$ R11 such that $(xy)\Phi = (y\Phi)(x\Phi)$.
But R8 has 2 one-sided left ideals{0, a} and {0, b} but R11 has no one-sided left ideals (though it has 2 one-sided right ideals).

Exercise 4: Clearly I is an abelian group under addition.
Since $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} u & 0 \\ v & 0 \end{pmatrix} = \begin{pmatrix} au + bv & 0 \\ cu + dv & 0 \end{pmatrix} \in$ I, this shows that I is a left ideal.
NOTE: We don't have to check that I is closed under multiplication because that is included in the left ideal calculation.
To show minimality we need do more than show that I has no proper non-trivial ideal, because an ideal of I need not be an ideal of R. In fact $\begin{pmatrix} 0 & 0 \\ * & 0 \end{pmatrix}$ is an ideal of I, but not of R.

Now suppose that J is an ideal of R with 0 < J.

Let $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ be a no-zero element of J.

Since $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} b & 0 \\ a & 0 \end{pmatrix}$, we may assume that $a \neq 0$.

Now $\begin{pmatrix} a^{-1} & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in$ J and

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in \text{J.}$$

Hence $\begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} = x\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + y\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in$ J and so, J = I.

Exercise 5: (a) Everything is obvious except the associative law for the two basis elements *x*, *y*. There are 8 instances to check.

(xx)x = 0 = x(xx);
(xx)y = 0 = x(xy);
(xy)x = 0 = x(yx);
(xy)y = x = x(yy);
(yx)x = 0 = y(xx);
(yx)y = x = y(xy);
(yy)x = x = y(yx);
(yy)y = y = y(yy).

(b) Suppose that $(ax + by)^2 = ax + by$.
Then $a^2x^2 + b^2y^2 + abxy + abyx = ax + by$.
Hence $2abx + b^2y = ax + by$ and since {x, y} is a basis:

$$2ab = a \text{ and } b^2 = b.$$

Hence $b = 0$ or 1.

If $b = 0$ then $a = 0$ and so a = 0 which can't be part of a basis.
So $b = 1$ and hence $2a = a$ and so $a = 0$. Hence x = $\underline{y}$.

(c) For R to be a semigroup algebra we would need to have a basis {A, B} that's closed under multiplication.
Let A = ax + by and B = cx + dy. Now A^2 = A or B.

Case 1: A^2 = A:
By (2), A = y and B^2 = A = y.
Since B must be linearly independent from A we must have $c \neq 0$.
Now $B^2 = d^2y + 2cdx$ and hence $2cd = 0$ and $d^2 = 1$.
Since c ≠ 0 the first equation gives d = 0, contradicting the second equation.
So case 1 cannot arise.

Case 2: A^2 = B:
Then $2ab = c$ and $b^2 = d$.

Case 2A: B^2 = B: Then, by (2), B = y and so
$c = 0$ and $d = 1$.
Hence $ab = 0$ and $b^2 = 1$. Thus $a = 0$ and $b = \pm 1$.
This would mean that A = $\pm y$.
But then A, B would not be linearly independent. So this case cannot arise.

Case 2B: B^2 = A:
Then $2cdx + d^2y = ax + by$ and so $2cd = a$ and $d^2 = 1$.

So we have four equations:

$$2ab = c, \quad b^2 = \mathrm{d}, \quad 2cd = a \text{ and } d^2 = 1.$$

Clearly $d \neq -1$ so $d = 1$.

Then $b = \pm 1$ and $a = 2c = 4ab = \pm 4a$ whence $a = c = 0$, contradicting the fact that {A, B} is linearly independent.