

# Algebra 2 Notes

by Tyler Wright

[github.com/Fluxanoia](https://github.com/Fluxanoia)

[fluxanoia.co.uk](https://fluxanoia.co.uk)

*These notes are not necessarily correct, consistent, representative of the course as it stands today, or rigorous. Any result of the above is not the author's fault.*

**These notes are in progress.**

# Contents

<b>1</b>	<b>The Fundamentals</b>	<b>3</b>
1.1	Rings (1.1)	3
1.2	Properties of Rings (1.3)	3
1.3	Units (1.6-7)	3
1.4	Fields (1.9)	3
1.5	Subrings (1.14-15)	3
1.6	The Gaussian Integers (1.17, 1.19)	4
1.7	Product Rings (1.20)	4
1.8	Distributivity of Taking Units (1.22)	4
1.9	Polynomials (1.23)	4
1.10	Ring Homomorphisms (2.7, 2.12)	4
1.11	Ring Isomorphisms (2.1)	5
1.12	The Kernel (2.13, 2.18)	5
1.13	Ideals (2.15-16)	5
1.14	Preservation of Satisfaction (2.20)	5
1.15	Cosets (2.22)	5
<b>2</b>	<b>Quotients</b>	<b>6</b>
2.1	Quotient Rings (2.24-25)	6
2.2	The Homomorphism Theorem (3.1)	6
2.3	Chinese Remainder Theorem (3.4)	6
2.4	Properties of the Integers (3.6)	6
2.5	Composition of Ideals (3.8)	7
2.6	Ideals with Units (3.10)	7
2.7	Classification of Fields (3.11)	7
2.8	Homomorphisms from Fields (3.13)	7
2.9	Induced Ideals (3.15)	7
2.10	The Isomorphism Theorems (3.17)	8
	2.10.1 The First Isomorphism Theorem	8
	2.10.2 The Second Isomorphism Theorem	8
	2.10.3 The Third Isomorphism Theorem	8
<b>3</b>	<b>Integral Domains and Fields</b>	<b>9</b>
3.1	Integral Domains (4.1)	9
3.2	Preservation of Isomorphism	9
3.3	Relating Integral Domains and Fields (4.3)	9
3.4	Subrings of Integral Domains (4.4)	9
3.5	Field of Fractions (4.6)	10

# 1 The Fundamentals

## 1.1 Rings (1.1)

A ring is a set with two binary operations, addition and multiplication, such that they are both commutative, associative, and addition is distributive over multiplication, so for  $a$ ,  $b$ , and  $c$  in some ring:

$$(a + b)c = ac + bc.$$

We also have that rings must contain 'zero' and 'one' elements, the additive and multiplicative identities, and every element of the ring has an additive inverse.

## 1.2 Properties of Rings (1.3)

For a ring  $R$  with  $a$ ,  $b$ , and  $c$  in  $R$ :

- if  $a + b = b$  then  $a = 0$ ,  $0$  is unique,
- if  $a \cdot x = x$  for all  $x$  in  $R$ , then  $a = 1$ ,  $1$  is unique,
- if  $a + b = 0 = a + c$  then  $b = c$ ,  $-a$  is unique,
- we have  $0 \cdot a = 0$ ,
- we have  $-1 \cdot a = -a$ ,
- we have  $0 = 1$  if and only if  $R = \{0\}$ .

## 1.3 Units (1.6-7)

For a ring  $R$ , with  $r$  in  $R$ , if there exists some  $s$  such that  $rs = 1$  then  $r$  is a unit and  $s = r^{-1}$  is the multiplicative inverse of  $r$ . We write  $R^\times$  to be the set of all units in  $R$ , which is an abelian group under multiplication.

## 1.4 Fields (1.9)

A non-zero ring  $R$  is a field if  $R \setminus \{0\} = R^\times$ .

## 1.5 Subrings (1.14-15)

For a ring  $R$ ,  $S \subseteq R$  is a subring of  $R$  if it is a ring and contains zero and one. This is equivalent to saying  $S$  is closed under addition, multiplication, and additive inverses, and contains  $1$ .

## 1.6 The Gaussian Integers (1.17, 1.19)

We define the Gaussian integers as:

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\},$$

which is the smallest subring of  $\mathbb{C}$  containing  $i$ . Generally, for  $\alpha$  in  $\mathbb{C}$ ,  $\mathbb{Z}[\alpha]$  is the smallest subring containing  $\alpha$  and for a ring  $R$  with a subring  $S$ , for some  $\beta$  in  $R$ , we have  $S[\beta]$  is the smallest subring of  $R$  containing  $S$  and  $\beta$ .

## 1.7 Product Rings (1.20)

For  $R$  and  $S$  rings, we have that  $R \times S$  is a ring under component-wise addition and multiplication.

## 1.8 Distributivity of Taking Units (1.22)

For rings  $R$  and  $S$ ,  $(R \times S)^\times = R^\times \times S^\times$ .

*Proof.* We consider:

$$\begin{aligned} (r, s) \in (R \times S)^\times &\iff (r, s)(p, q) = (1, 1) \text{ for some } (p, q) \in R \times S \\ &\iff rp = 1 \text{ and } sq = 1 \text{ for some } p \in R \text{ and } q \in S \\ &\iff r \in R^\times \text{ and } s \in S^\times, \end{aligned}$$

as required. □

## 1.9 Polynomials (1.23)

For a ring  $R$  and a symbol  $x$ , we have that the following is a ring:

$$R[x] = \{a_0 + a_1x + \cdots + a_nx^n : n \in \mathbb{Z}_{\geq 0}, (a_i)_{i \in [n]} \in R^n\}.$$

## 1.10 Ring Homomorphisms (2.7, 2.12)

For  $R$  and  $S$  rings, a map  $\varphi$  from  $R$  to  $S$  is a ring homomorphism if it preserves addition and multiplication. This implies that 0 and 1 are fixed points of  $\varphi$  and taking additive inverses is preserved by  $\varphi$ .

We have some properties of ring homomorphisms:

- $\varphi(0) = 0$ ,
- $\varphi(-a) = -\varphi(a)$ ,
- the image of  $\varphi$  is a subring of  $S$ ,
- homomorphisms are preserved under composition.

### 1.11 Ring Isomorphisms (2.1)

A ring isomorphism is a bijective ring homomorphism.

### 1.12 The Kernel (2.13, 2.18)

The kernel of a homomorphism is the set of values it maps to 0. This is not necessarily a ring. The kernel is  $\{0\}$  if and only if the homomorphism is injective.

### 1.13 Ideals (2.15-16)

For a ring  $R$  with  $I \subseteq R$ ,  $I$  is an ideal if it is an additive subgroup of  $R$  and for all  $r$  in  $R$  and  $i$  in  $I$ ,  $ri$  is in  $I$ . The kernel of homomorphisms are ideals.

### 1.14 Preservation of Satisfaction (2.20)

For a ring  $R$  with  $r$  in  $R$ , if for some  $n$  in  $\mathbb{Z}_{\geq 0}$  we have  $(a_i)_{i \in [n]}$  in  $\mathbb{Z}^n$  such that:

$$a_n r^n + \cdots + a_1 r + a_0 = 0,$$

then for any homomorphism  $\varphi$  on  $R$  to some other ring  $S$ , we have that:

$$\varphi(a_n r^n + \cdots + a_1 r + a_0) = 0.$$

### 1.15 Cosets (2.22)

For a ring  $R$  with  $r$  in  $R$  and an ideal  $I$  of  $R$ , the coset of  $r$  modulo  $I$  is the set:

$$r + I = \{r + i : i \in I\}.$$

For each  $r$  and  $s$  in  $R$ , we define a relation by:

$$r \sim s \iff r - s \in I,$$

which is an equivalence relation, with equivalence classes the cosets of  $R$  modulo  $I$ . Thus, cosets are either identical or disjoint.

## 2 Quotients

### 2.1 Quotient Rings (2.24-25)

The set of cosets modulo  $I$  of a ring  $R$  forms a ring, the quotient ring  $R/I$  of  $R$  by  $I$ . We define the operations for  $a$  and  $b$  in  $R$ :

$$\begin{aligned}(a + I) + (b + I) &= (a + b) + I, \\ (a + I)(b + I) &= ab + I.\end{aligned}$$

### 2.2 The Homomorphism Theorem (3.1)

For a homomorphism  $\varphi$  from  $R$  to  $S$ , taking  $I = \text{Ker}(\varphi)$ , we have that  $R/I \cong \varphi(R)$ , via the map  $r + I \mapsto \varphi(r)$ .

*Proof.* We consider the proposed map and name it  $\psi$ . We can see that  $\psi$  is well defined as for some  $r$  in  $R$ , for any  $r'$  in  $r + I$ ,  $r' = r + i$  for some  $i$  in  $I$  so:

$$\varphi(r') = \varphi(r) + \varphi(i) = \varphi(r).$$

Additionally,  $\psi$  is trivially a homomorphism, and is surjective by the definition of the image, so we consider injectivity. If for some  $r$  in  $R$ , we have  $\psi(r + I) = 0$  then:

$$\varphi(r) = 0 \implies r \in I \implies r + I = I,$$

so  $\psi$  is an isomorphism. □

### 2.3 Chinese Remainder Theorem (3.4)

For positive, coprime integers  $m$  and  $n$ :

$$\mathbb{Z}/(mn\mathbb{Z}) \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}).$$

### 2.4 Properties of the Integers (3.6)

We have the following properties of  $\mathbb{Z}$ :

- every ideal of  $\mathbb{Z}$  is of the form  $n\mathbb{Z}$  for some non-negative integer  $n$ ,
- every ring  $R$  admits a unique homomorphism from  $\mathbb{Z}$  to  $R$ ,
- every ring  $R$  contains a unique subring which is either isomorphic to  $\mathbb{Z}$  or  $\mathbb{Z}/n\mathbb{Z}$  for some non-negative integer  $n$ .

## 2.5 Composition of Ideals (3.8)

For  $I$  and  $J$  ideals of a ring  $R$ :

- $I \cap J$  is an ideal,
- $I + J$  is an ideal,
- $IJ = \{\sum_{k=1}^n i_k j_k : n \in \mathbb{N}, (i_k)_{k \in [n]} \in I^n, (j_k)_{k \in [n]} \in J^n\}$  is an ideal.

## 2.6 Ideals with Units (3.10)

For an ideal  $I$  of a ring  $R$ , if  $I$  contains  $r$  in  $R^\times$ , then  $I = R$ .

*Proof.* By definition, we have some  $s$  such that  $rs = 1$ , so  $1$  is in  $I$  as it is an ideal. But then for any  $x$  in  $R$ , we must have  $1 \cdot x$  in  $I$ , so  $I = R$ .  $\square$

## 2.7 Classification of Fields (3.11)

A ring  $R \neq \{0\}$  is a field if and only if the only ideals of  $R$  are  $\{0\}$  and  $R$ .

*Proof.* ( $\implies$ ) We have that  $R^\times = R \setminus \{0\}$ , so every non-zero ideal contains a unit, so must be  $R$  by (2.6).

( $\impliedby$ ) For  $r \neq 0$  in  $R$ , we take  $I = \{rx : x \in R\}$  which is a non-zero ideal. By assumption,  $I = R$  so  $1$  is in  $I$ , thus  $rx = 1$  for some  $x$  in  $R$ . Thus,  $r$  is a unit.  $\square$

## 2.8 Homomorphisms from Fields (3.13)

For a ring homomorphism  $\varphi$  from  $R$  to  $S \neq \{0\}$ , if  $R$  is a field,  $\varphi$  is injective.

*Proof.* The kernel of  $\varphi$  is either  $R$  or  $\{0\}$  by (2.7), so we consider the cases. If the kernel is  $R$ , then  $S = \{0\}$ , a contradiction, so the kernel must be  $\{0\}$ .  $\square$

## 2.9 Induced Ideals (3.15)

For a surjective ring homomorphism  $\varphi$  from  $R$  to  $R'$ , with  $I \subseteq R$  and  $I' \subseteq R'$  ideals, we have that:

1.  $\varphi(I)$  is an ideal of  $R'$ ,
2.  $\varphi^{-1}(I')$  is an ideal of  $R$  containing  $\text{Ker}(\varphi)$ ,
3. there is a bijection from the ideals of  $R$  containing  $\text{Ker}(\varphi)$  to the ideals of  $R'$ .

*Proof of (3).* We will show that  $I = \varphi^{-1}(\varphi(I))$  (the case for  $I' = \varphi(\varphi^{-1}(I'))$  is analogous). For  $x$  in  $I$ , we have that  $\varphi(x)$  is in  $\varphi(I)$  so  $x$  is in  $\varphi^{-1}(\varphi(I))$ . Thus,  $I \subseteq \varphi^{-1}(\varphi(I))$ . For  $x$  in  $\varphi^{-1}(\varphi(I))$ , we have that  $\varphi(x)$  is in  $\varphi(I)$ , so  $\varphi(x) = \varphi(y)$  for some  $y$  in  $I$ . As  $\varphi(x - y) = 0$ ,  $x - y$  is in  $\text{Ker}(\varphi)$  so we have  $x = (x - y) + y$  which is in  $I$ , as required.  $\square$

## 2.10 The Isomorphism Theorems (3.17)

We take  $R$  to be a ring.

### 2.10.1 The First Isomorphism Theorem

This is the same as the Homomorphism Theorem.

### 2.10.2 The Second Isomorphism Theorem

For  $I \subseteq J \subseteq R$  ideals of  $R$ , we have that  $J/I$  is an ideal of  $R/I$  and:

$$\frac{R/I}{J/I} \cong R/J.$$

### 2.10.3 The Third Isomorphism Theorem

For a subring  $S$  of  $R$ , and  $I$  an ideal of  $R$ , we have that  $S + I$  is a subring with  $I \subseteq S + I$  and  $S \cap I \subseteq S$  ideals and:

$$\frac{S + I}{I} \cong \frac{S}{S \cap I}.$$



## 3 Integral Domains and Fields

### 3.1 Integral Domains (4.1)

For a ring  $R$ ,  $a \neq 0$  in  $R$  is a zero divisor if for some  $b \neq 0$  in  $R$ ,  $ab = 0$ . We say  $R$  is an integral domain if it has no zero divisors.

### 3.2 Preservation of Isomorphism

Ring isomorphisms preserve units and zero divisors, so the domain is a field / integral domain if and only if the codomain is a field / integral domain.

### 3.3 Relating Integral Domains and Fields (4.3)

We have that:

1. all fields are integral domains,
2.  $R$  is an integral domain if and only if for all  $a \neq 0$  in  $R$ , the map  $x \mapsto ax$  is injective,
3. every finite integral domain is a field.

*Proof.* (1) Suppose we have  $a$  and  $b$  in some field, such that  $a \neq 0$  and  $ab = 0$ . Thus,  $a^{-1}ab = 0$ , so  $b = 0$ .

(2) ( $\Leftarrow$ ) We have that  $ax = 0$  if and only if  $x = 0$  as  $R$  has no zero divisors, so the map is injective by (1.12).

( $\Rightarrow$ ) We appeal to the contrary and suppose  $ax = 0$  for some non-zero  $a$  and  $x$  in  $R$ . As such, the mapping via  $a$  has a non-zero kernel, a contradiction by (1.12).

(3) If a integral domain  $R$  is finite, then the mapping in (2) is surjective, so for any  $a$  in  $R$ , there is some  $x$  in  $R$  such that  $ax = 1$ .  $\square$

### 3.4 Subrings of Integral Domains (4.4)

Every subring of an integral domain is an integral domain.

### 3.5 Field of Fractions (4.6)

For an integral domain  $R$ , we can consider fractions:

$$\left\{ \frac{a}{b} : a \in R, b \in R, b \neq 0 \right\},$$

and define an equivalence relation:

$$(a, b) \sim (c, d) \iff ad = bc.$$

with the set of equivalence classes  $K$ , forming a field under the ring operations:

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &= \frac{ad + bc}{bd}, \\ \frac{a}{b} \cdot \frac{c}{d} &= \frac{ac}{bd}, \end{aligned}$$

along with the expected additive and multiplicative inverses and identities. This is the field of fractions of  $R$ , denoted  $f.f.(R)$ . We have that  $R$  is isomorphic to a subring of  $K$ , and if there is an injective homomorphism between two integral domains, there is an induced injection between their respective fields of fractions.