Algebra 2 Notes

by Tyler Wright

github.com/Fluxanoia 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

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

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:

$$R[x] = \{a_0 + a_1 x + \cdots + a_n x^n : n \in \mathbb{Z}_{\geq 0}, (a_i)_{i \in [n]} \in R^n\}.$$

1.10 Ring Homomorphisms (2.7, 2.12)

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

We have some properties of ring homomorphisms:

- $\varphi(0) = 0$,
- $\varphi(-a) = -\varphi(a)$,
- the image of φ) 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 φ 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:

$$(a+I)+(b+I)=(a+b)+I,$$
$$(a+I)(b+I)=ab+I.$$

2.2 The Homomorphism Theorem (3.1)

For a homomorphism φ from R to S, taking $I=\mathrm{Ker}(\varphi)$, 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 ψ. We can see that ψ 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, ψ 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:

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

so ψ 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 $I = R$. □

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

($\Longleftarrow$) 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. □

2.8 Homomorphisms from Fields (3.13)

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

Proof. The kernel of φ 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 $\{0\}$. □

2.9 Induced Ideals (3.15)

For a surjective ring homomorphism φ 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 $\mathrm{Ker}(\varphi)$,
3. there is a bijection from the ideals of R containing $\mathrm{Ker}(\varphi)$ 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 $\varphi^{-1}(\varphi(x))$. Thus, $I \subseteq \varphi^{-1}(\varphi(I))$. For x in $\varphi^{-1}(\varphi(x))$, 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. □

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) ($\Longleftarrow$) 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).
($\Longrightarrow$) 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 $ax = 1$. □

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:

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

along with the expected additive and multiplicative inverses and identites. 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.

3.6 Maximal Ideals (4.8)

For a ring R, an ideal $I \subset R$ is maximal if there is no ideal J such that $I \subset J \subset R$.

3.7 Prime Ideals (4.9)

For a ring R, an ideal $I \subset R$ is prime if for all ab in I, either a or b is in I.

3.8 Maximal and Prime Ideals and their Quotients (4.12-13)

For a ring R with $I \subset R$ an ideal:

1. I is maxmimal if and only if R/I is a field,
2. I is prime if and only if R/I is an integral domain.

Thus, every maximal ideal is prime since all fields are integral domains.

Proof. (1) By (2.9), there's a bijection from ideals of R containing I amd ideals of R/I. Thus, the ideals of R/I are 0 and R/I if and only if the ideals of R containing I are I and R, which is true if and only if I is maximal.

(2) We consider a and b in R and consider $\bar{a} = a + I$ and $\bar{b} = b + I$:

$$a \in I \iff \bar{a} = I,$$
$$b \in I \iff \bar{b} = I,$$
$$ab \in I \iff \bar{a}\bar{b} = I.$$

Thus, if I is prime and $\bar{a}\bar{b} = I$ then either a or b is in I. Also, if R/I is an integral domain and we have ab in I, then either $\bar{a}$ or $\bar{b}$ is in I so either a or b is in I. $\square$

3.9 Existence of Maximal Ideals (4.16)

Every ring $R \neq \{0\}$ has a maximal ideal.

3.10 Ideals within Maximal Ideals (4.17)

For a ring R, every ideal $I \subset R$ is contained in some maximal ideal.

4 Principal Ideal, Euclidean, and Unique Factorisation Domains

4.1 Noetherian Rings (5.1)

A ring R is Noetherian if every increasing chain of ideals in R is finite.

4.2 Finitely Generated Ideals (5.3)

For a ring R with $I \subseteq R$ an ideal, I is generated by $i_1, \ldots, i_n$ in I for some n in $\mathbb{Z}_{>0}$ if:

$$I = i_1R + \cdots + i_nR = (i_1, \ldots, i_n).$$

4.3 Finite Generated Ideals in Noetherian Rings (5.4)

A ring is Noetherian if and only if every ideal of R is finitely generated.

Proof. ($\Longrightarrow$) For an ideal $I \subseteq R$, we consider i_1 in I and take $I_1 = (i_1)$. If $I_1 = I$ then we are done, otherwise we consider i_2 in $I \setminus I_1$ and take $I_2 = (i_1, i_2)$. Following this process, we get $I_1 \subset I_2 \subset \cdots \subset I_n$, for some n in $\mathbb{Z}_{>0}$ as R is Noetherian. Thus, we get a finite generating set $(i_1, \ldots, i_n)$ for I.

($\Longleftarrow$) If we have a chain of ideals $I_1 \subset I_2 \subset \cdots$, then $I = \bigcup_{k \in \mathbb{Z}_{>0}} I_k$ is finitely generated by some $(i_1, \ldots, i_n)$ by assumption. For each k in $[n]$, i_k must be in I_{m_k} for some m_k, so taking $m = \max(m_1, \ldots, m_n)$, $I_m = I$ as required. □

4.4 Preservation of Noetherian Rings (5.5-6)

All quotients of, products of, and polynomials with coefficients in a Noetherian ring are Noetherian rings.

Proof of Quotients. For a Noetherian ring R with I an ideal of R, we consider φ from R to R/I mapping $r \mapsto r + I$. By (2.9), we have a bijection from ideals in R containing I and ideals of R/I via φ which preserves the Noetherian property. □

4.5 Divisibility (5.10-12)

For an integral domain R, we say that b in R divides a in R if there exists c in R such that $a = bc$. Thus, a is in (b) and similarly $(a) \subseteq (b)$. We note that such a c is unique.

If a and b both divide each other ($(a) = (b)$, or $a = b\varepsilon$ for some unit ε in R), we say they are associates. For some $p \neq 0$ in R where p is not a unit, have that:

$$p \text{ irreducible} \iff \big[p = ab \implies a \in R^\times \text{ or } b \in R^\times\big],$$
$$p \text{ prime} \iff \big[p \,|\, ab \implies p \,|\, a \text{ or } p \,|\, b\big] \iff (p) \text{ is a non-zero prime ideal.}$$

4.6 Irreducible Primes (5.14)

For an integral domain R, primes of R are irreducible.

Proof. For a prime p in R with b and c in R such that $p = bc$, so b and c both divide p. By the definition of primes, we have that p divides bc so either p divides b or p divides c. As such, if p divides b then p and b are associate so c is a unit (and similarly for p dividing c). □

4.7 (5.16)