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. $\square$

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:

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

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

1.16 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 Fundamental Results

2.1 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. $\square$