Algebra I

Evan Halloran

Abstract

1

[1]The content of these notes is largely based on *A First Course in Abstract Algebra* by Joseph Rotman.

Contents

Chapter 1

Introduction: What is Algebra?

Classically speaking, the field of math known as **algebra** refers to the solving of equations, especially polynomial equations. High school students devote a considerable portion of their time to solving linear and quadratic equations, which can be solved explicitly. The following formulae have been known for millennia:

Theorem 1 (Linear formula)**.** *If $ax + b = 0$ and $a \neq 0$, then the unique complex solution is $x = -b/a$.*

Theorem 2 (Quadratic formula)**.** *If $ax^2 + bx + c = 0$ and $a \neq 0$, then the two complex solutions are*

$$x_1, x_2 = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

There are also (very complicated) formulas to solve cubic and quartic equations by radicals and rational functions. In general, one can use complex analysis to prove that any polynomial of degree at least one has a complex solution.

Theorem 3 (Fundamental Theorem of Algebra)**.** *Any polynomial equation of one variable with complex coefficients of degree at least 1*

$$a_n z^n + a_{n-1} z^{n-1} + ... + a_1 z + a_0$$

must have a solution in the complex numbers $\mathbb{C}$.

The proof of this theorem is non-constructive—even though every polynomial admits a solution in the complex numbers, we may not always have a formula for it. Since formulae for the roots of linear, quadratic, cubic, and quartic polynomials exist, we may ask ourselves if polynomials of degree ≥ 5 admit a solution in terms of radicals and rational functions. The answer, as **Evariste Galois** proved, is no:

Theorem 4 (Galois)**.** *There is no explicit formula to solve a general polynomial equation of degree greater than* 4 *using only radicals and rational functions.*

Galois proved this result by observing that the existence of a solution formula by radicals would have forced some symmetries on the solutions of a general polynomial equation of degree n, which does not exist if $n \geq 5$. Galois was able to expand the field of alegbra by leagues before he died in a duel at 20 years old. By inventing group theory and field theory, he was able to prove exactly when a polynomial of degree ≥ 5 admits a solution in terms of radical and rational functions.

Contemporary abstract algebra is concerned with the study of algebraic structures, primarily groups, rings, and fields. The history of algebra follows a sort of **sonata structure**: the **exposition** is concerned with the millennia-old problem of finding solutions to polynomial equations; the **development** focuses on the abstracting of algebraic properties into structures such as groups, rings, and fields; and the **recapitulation** returns to the original question: in a beautiful feat of ingenuity, group theory and field theory are reconciled under **Galois theory**, and the insolvability of the general quintic (and higher order) polynomial is proven.

Pedagoically speaking, undergraduate contemporary abstract algebra is split into three semester-long courses: a first course in **group theory**; a second course in **ring theory**; and a third course in **field and Galois theory**.

Chapter 2

Groups

2.1 Some Set Theory

Very roughly speaking, a set is a *collection* of objects/elements. It can be defined rigorously using the ZFC[1] axioms. While we are not going to elaborate on the axiomatic definition of sets, one thing to always keep in mind is that the collection of "all..." might *not* be a set. For example, the collection of all sets is *not* a set, as no set can be an element of itself. In fact, the collection of all sets of size 1 (called singleton sets) is not a set.

Definition. Two sets X and Y are equal if they contain exactly the same elements, that is $x \in X \iff x \in Y$. The set X is a **subset** of Y if all elements of X are also elements of Y.

Definition. The **empty set** is a set with no element.

Definition. Given any set X, its power set $\mathcal{P}(X)$ is the set of all subsets of X.

Functions

Definition. A **binary relation** between two sets X and Y is a subset of $X \times Y$.

Definition. A **function/map** $f : X \to Y$ is a binary relation $\Gamma_f \subseteq X \times Y$ such that for every $x_0 \in X$, there is a unique $(x, y) \in \Gamma_f$ with $x = x_0$. We call Γ_f the **graph** of f, X the **domain/source** of f, and Y the **codomain/target** of f.

Example. 1. Given any X, we have $\mathrm{id}_X : X \to X$

[1] ZF stands for Zermelo and Fraenkel, the two mathematicians who proposed the axioms; C stands for the axiom of choice.

Equivalence Relations

Exercises

1. (a) Let $f : X \to Y$ be a function, and let $\{S_i : i \in I\}$ be a family of subsets of X. Prove that

$$f\left(\bigcup_{i\in I} S_i\right) = \bigcup_{i\in I} f(S_i).$$

   (b) If S_1 and S_2 are subsets of a set X, and if $f : X \to Y$ is a function, prove that $f(S_1 \cap S_2) \subseteq f(S_1) \cap f(S_2)$. Give an example in which $f(S_1 \cap S_2) \neq f(S_1) \cap f(S_2)$.

2. Let $f : X \to Y$ and $g : Y \to Z$ be two maps of sets. Show that:

   (a) If $g \circ f$ is injective, then so is f.

   (b) If $g \circ f$ is surjective, then so is g.

   In particular, if $g \circ f$ is bijectivem then f is injective and g is surjective. However, we do not know if f is surjective or g is injective.

   (c) Give an explicit example where $g \circ f$ is injective, but g is not.

   (d) Give an explicit example where $g \circ f$ is surjective, but f is not.

3. Let X and Y be two finite sets. Let $\mathrm{Map}(X, Y)$ be the set of all maps from X to Y.

   (a) Show that $|X \times Y| = |X| \times |Y|$ and $|\mathrm{Map}(X, Y)| = |Y|^{|X|}$. The latter justifies the alternative notation Y^X for the mapping set $\mathrm{Map}(X, Y)$. From this, explain why it is reasonable to say $0^0 = 1$. [2]

   (b) Construct a bijection from the power set $\mathcal{P}(X)$ to the mapping set $\mathrm{Map}(X, \{0, 1\})$. What is the cardinality of $\mathcal{P}(X)$?

4. Let X and Y be sets, and let $f : X \to Y$ be a function.

   (a) If S is a subset of X, prove that the restriction $f|_S$ is equal to the composite $f \circ i$, where $i : S \to X$ is the inclusion map.

   (a) If $\mathrm{im} f = A \subseteq Y$, prove that there exists a surjection $f' : X \to A$ with $f = jf'$, where $j : A \to Y$ is the inclusion.

[2] Nevertheless, 0^0 is still undefined. This is because the two-variable function $f(x, y) = x^y$, with natural domain $[0, \infty) \times \mathbb{R} - \{0\} \times (-\infty, 0]$, does not have a limit when $(a, b) \to (0, 0)$.

5. Let $f : X \to Y$ be a function. If $B_i \subseteq Y$ is a family of subsets of Y, prove that

$$f^{-1}\left(\bigcup_i B_i\right) = \bigcup_i f^{-1}(B_i) \text{ and } f^{-1}\left(\bigcap_i B_i\right) = \bigcap_i f^{-1}(B_i).$$

6. Let $f : X \to Y$ be a map between two finite sets with the same cardinality (number of elements). Show that f is injective iff f is surjective (and hence iff it is a bijection).

7. Determine whether $f : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ given by

$$f(a/b, c/d) = (a + c)/(b + d)$$

is a function.

8. Let $f : X \to Y$ be a function. Define a relation on X by $x \equiv x'$ if $f(x) = f(x')$. Prove that $\equiv$ is an equivalence relation. If $x \in X$ and $f(x) = y$, the equivalence class $[x]$ is usually denoted by $f^{-1}(y)$, the inverse image of $\{y\}$.

2.2 Permutations

Definition. A **permutation** of a set X is a bijection $\alpha : X \to X$. If X is a finite set with n elements, an **arrangement** of X is a non-repeating listing $x_1, ..., x_n$ of all elements in X.

From the definition, an arrangement of a set X with n elements is the same data as a bijection $\{1, 2, ..., n\} \to X$, $i \mapsto x_i$. So a permutation α of $X = \{1, 2, ..., n\}$ is also an arrangement of those numbers.

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \alpha(1) & \alpha(2) & \dots & \alpha(n) \end{pmatrix}$$

Example. 1. There is only one permutation of $X = \emptyset$, namely the empty map.

2. For a singleton set $X = \{x\}$, there is also only one permutation.

3. For a set with two elements $X = \{a, b\}$, we have two permutations:

$$a \longrightarrow a \qquad\qquad a \to b$$
$$b \searrow b$$

Definition. Let X be a set. The **symmetric group** S_X on X is the set of all permutations of X. When $X = \{1, ..., n\}$, we write S_n for S_X. This is also called the symmetric group on n letters.

Exercises

1. Determine whether each statement is true or false and provide reasoning.

   (a) The symmetric group on n letters is a set of n elements.

   (b) If $\sigma \in S_6$, then $\sigma^n = \mathrm{id}$ for some $n \geq 1$.

   (c) If α, $\beta \in S_n$, then $\alpha\beta$ is an abbreviation for $\alpha \circ \beta$.

   (d) If α, β are cycles in S_n, then $\alpha\beta = \beta\alpha$.

   (e) If σ, τ are r-cycles in S_n, then $\sigma\tau$ is an r-cycle.

   (f) If $\sigma \in S_n$ is an r-cycle, then $\alpha\sigma\alpha^{-1}$ is an r-cycle for every $\alpha \in S_n$.

   (g) If $\sigma\alpha\sigma^{-1} = \omega\alpha\omega^{-1}$, then $\sigma = \omega$.

2. Find $\mathrm{sgn}(\alpha)$ and α^{-1}, where

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}.$$

3. If $n \geq 3$, show that if $\alpha \in S_n$ commutes with every $\beta \in S_n$, then $\alpha = (1)$.

4. Define $f : \{0, 1, 2, ..., 10\} \to \{0, 1, 2, ..., 10\}$ by

$$f(n) = \text{the remainder after dividing } 4n^2 - 3n^7 \text{ by } 11.$$

   (a) Show that f is a permutation.

   (b) Compute the parity of f.

   (c) Compute the inverse of f.

5. If $n \geq 2$, prove that the number of even permutations in S_n is $\frac{1}{2}n!$.

2.3 Groups

Definition. Let X be a set. A **binary operation** is a map $- \cdot - : X \to X$. The set together with the binary operation $(X, \cdot\,)$ is

- a **semi-group** if $\cdot$ is associative, i.e. $\forall x, y, z \in X : (x \cdot y) \cdot z = x \cdot (y \cdot z)$;
- a **monoid** if it is a semi-group with a multiplicative unit 1_X such that $\forall x \in X : 1_X \cdot x = x = x \cdot 1_X$;

- a **group** if it is a monoid with multiplicative inverses: $\forall x \in X$, $\exists x^{-1}$ such that $x \cdot x^{-1} = 1_X = x^{-1} \cdot x$;
- an **abelian group** if it is a group whose multiplication is commutative: $x \cdot y = y \cdot x$.

In summary, a group is a set X with a binary operation $\cdot$ such that $\cdot$ is associative, unital, and has inverses. $(X, \cdot\,)$ is called abelian if $\cdot$ is commutative. Note that under normal arithmetic, $+$ is not a binary operation on $\{0, 1\}$ because $1 + 1 = 2 \notin \{0, 1\}$. Binary operations are **closed** by definition.

Example. Recall that we have inclusion of number systems: $\mathbb{N}_+ \subseteq \mathbb{N} \subseteq \mathbb{Z}$. The positive integers under the binary operation of addition $(\mathbb{N}_+, +)$ is a semi-group but not a monoid. The natural integers under addition $(\mathbb{N}, +)$ is a monoid but not a group. The integers under addition $(\mathbb{Z}, +)$ is an abelian group.

Example. Switching to multiplication, we have the inclusion; $(\mathbb{N}_{>0}, \times) \subseteq (\mathbb{N}, \times) \subseteq (\mathbb{Z}, \times)$. In each of these structures, multiplication is a binary operation, associative, and unital (1 is a unit in each). As none of these structures meet the inverse requirement, they are all monoids. There are two ways to make them a group:

1. We can formally add inverses. For $(\mathbb{N}_{>0}, \times)$, this amounts to creating
$$\left(\mathbb{Q}_{>0} = \left\{ \frac{p}{q} \;\middle|\; p, q \in \mathbb{N}_+ \right\}, \times\right)$$
which is a group. Notice that $(\mathbb{Q}_{\geq 0}, \times)$ is not a group because 0 does not have an inverse: $0 \cdot x = 0 \neq 1$.
2. We can restrict each set to its invertible elements. Thus $(\{1\}, \times)$ and $(\{\pm 1\}, \times)$ are both groups. Notice that there is no group structure on $\emptyset$ because groups must have a unit.

Example. Let X be a set and consider the set of maps $\mathrm{Map}(X, X) = \{f : X \to X\}$ under function composition. The binary operation is closed: $f \circ g : X \to X \to X$ is indeed a map from X to X. Composition is associative: $(f \circ g) \circ h = f \circ (g \circ h)$. The unit in this structure is the identity map id_X. So far, this is enough to show that $(\mathrm{Map}(X, X), \circ)$ is a monoid.

Proposition 4.1. *Let $(G, *\,)$ be a group. Then*

1. *G has a unique unit,*

2. $\forall g \in G$, g has a unique inverse.

Proof. 1. Suppose 1_G, $1'_G$ are both units. Then

$$1_G = 1_G \cdot 1'_G = 1'_G.$$

2. Suppose $g \in G$ has two inverses g', g''. Then

$$g' = g' \cdot 1_G = g' \cdot (g \cdot g'') = (g' \cdot g) \cdot g'' = 1_G \cdot g'' = g''.$$

□

Proposition 4.2. *1. $[g^{-1}]^{-1} = g$,*

2. $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$,

3. $xy = x'y \iff x = x' \iff yx = yx'$.

Exercises

1. Determine whether each statement is true or false and provide reasoning.

   (a) The function $e : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, defined by $e(m, n) = m^n$, is an associative operation.

   (b) Every group is abelian.

   (c) The set of all positive real numbers is a group under multiplication.

   (d) The set of all positive numbers is a group under addition.

   (e) For all $a, b \in G$, where G is a group, $aba^{-1}b^{-1} = 1$.

2. If $a_1, a_2, ..., a_n$ are (not necessarily distinct) elements in a group G, prove that

$$(a_1 a_2 \dots a_n)^{-1} = a_n^{-1} \dots a_2^{-1} a_1^{-1}.$$

3. **Matrix representation of complex numbers**. Let $z = a + bi \in \mathbb{C}$ be a complex number where $a, b \in \mathbb{R}$. Consider the linear transformation

$$m_z : \mathbb{R}^2 \to \mathbb{R}^2, \quad \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x' \\ y' \end{pmatrix}, \text{ where } x' + iy' = z(x + iy).$$

   Check that the matrix representation of m_z with respect to the standard basis is $\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$. This defines a map of sets:

$$F : \mathbb{C} \to M_2(\mathbb{R}), \quad a + bi \to \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

   Verify the following properties of F:

(a) F is injective.

(b) F preserves addition and subtraction, i.e. $F(z_1 \pm z_2) = F(z_1) \pm F(z_2)$.

(c) F preserves multiplication, i.e. $F(z_1 z_2) = F(z_1) \cdot F(z_2)$.

(d) $\det(F(z)) = |z|^2$. This implies $F(z)$ is an invertible matrix iff $z \neq 0$.

(e) $F(z^{-1}) = (F(z))^{-1}$ when $z \neq 0$. This implies F preserves division, i.e. $F(z_1/z_2) = F(z_1) \cdot (F(z_2))^{-1}$ for any $z_1 \neq 0$.

(f) $F(\bar{z}) = (F(z))^T$, where $(-)^T$ means transpose of matrices.

(g) Eigenvalues of $F(z)$ are z and $\bar{z}$.

4. Check that the set of 3×3 upper triangular real matrices with non-zero diagonal entries

$$\mathrm{UT}_3(\mathbb{R}) := \{A = (a_{ij})_{3\times 3} \in M_3(\mathbb{R}) \mid a_{ij} = 0 \text{ for all } 1 \leq j < i \leq 3; a_{kk} \neq 0 \text{ for all } 1 \leq k \leq 3\}$$

is a group under matrix multiplication.

5. Let $G = \mathrm{GL}(2, \mathbb{Q})$, and let

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

2.4 Subgroups and Lagrange's Theorem

Definition. Let G be a group. A **subgroup** H of G is a non-empty subset that is closed under group multiplication and inverses:

- if $h_1, h_2 \in H$, then $h_1 h_2 \in H$;
- if $h \in H$, then $h^{-1} \in H$.

We write $H \leq G$ for subgroups and $H < G$ for proper subgroups, i.e. $H \leq G$ and $H \neq G$.

Examples.

1. $\{1_G\} \leq G$ is the trivial subgroup
2. $\mathbb{Z} \leq \mathbb{Q} \leq \overline{\mathbb{Q}} \leq \mathbb{R} \leq \mathbb{C}$ are subgroups under addition
3. $\{\pm 1\} \leq \mathbb{R}_+ \leq \mathbb{R} - \{0\} \leq \mathbb{C} - \{0\}$ are subgroups under multiplication
4. $\mu_n = \{z \in \mathbb{C} \mid z^n = 1\} \leq S^1 = U(1) \leq \mathbb{C} - \{0\}$ are subgroups under multiplication

Theorem 5 (Lagrange)**.** *let G be a finite group and $H \leq G$ a subgroup. Then $|H|$ divides $|G|$.*

Proof. The strategy is to decompose G as a disjoint union of subsets $G_1, G_2, ..., G_m$ that have size equal to H. For if

$$G = G_1 \sqcup G_2 \sqcup ... \sqcup G_m,$$

then clearly $|G| = |H| \cdot m$. □

Exercises

1. (a) Show that a left coset $\langle(1\ 2)\rangle$ in S_3 may not be equal to a right coset of $\langle(1\ 2)\rangle$ in S_3; that is, there is $\alpha \in S_3$ with $\alpha\langle(1\ 2)\rangle \neq \langle(1\ 2)\rangle\alpha$.

   (b) Let G be a finite group and let $H \leq G$ be a subgroup. Prove that the number of left cosets of H in G is equal to the number of right cosets of H in G.

2.5 Homomorphisms

Definition. Let $(G, *)$ and $(H, \cdot)$ be two groups. A **group homomorphism** from G to H is a map of sets $f : G \to H$ such that for all $g_1, g_2 \in G$, $f(g_1 * g_2) = f(g_1) \cdot f(g_2)$. An **isomorphism** is a bijective group homomorphism $f : G \to H$, and G and H are called **isomorphic** (written $G \cong H$) if there exists an isomorphism $f : G \to H$. An **endomorphism** of a group G is a group homomorphism $f : G \to G$. An **automorphism** of G is a group isomorphism $f : G \xrightarrow{\cong} G$.

Proposition 5.1. *Let $f : G \to H$ be a group homomorphism.*

(a) $f(1_G) = 1_H$.

(b) $f(g^{-1}) = [f(g)]^{-1}$ for all $g \in G$.

(c) If f is an isomorphism, then so is $f^{-1} : H \to G$.

(d) If $f_1 : G \to H, f_2 : H \to K$ are two group homomorphisms, then $f_2 \circ f_1 : G \to K$ is a group homomorphism.

Proof. (a) Note that $1_g = 1_g * 1_G$ implies that $f(1_G) = f(1_G * 1_G) = f(1_G) \cdot f(1_G)$. By cancellation, $f(1_g) = 1_H$.

(b) The element $f(g^{-1})$ is a right inverse of $f(g)$, since $f(g) \cdot f(g^{-1}) = f(g * g^{-1}) = f(1_G) = 1_H$. Similarly, it is a left inverse: $f(g^{-1}) \cdot f(g) = f(g^{-1} * g) = f(1_G) = 1_H$. Thus $f(g^{-1}) = [f(g)]^{-1}$.

(c) We want to show that for all $h_1, h_2 \in H$, $f^{-1}(h_1 \cdot h_2) = f^{-1}(h_1) * f^{-1}(h_2)$. Since f is bijective, there exist g_1, g_2 such that $f(g_1) = h_1$ and $f(g_2) = h_2$. Then

$$f^{-1}(h_1 \cdot h_2) = f^{-1}(f(g_1) \cdot f(g_2)) = f^{-1}(f(g_1 * g_2)) = g_1 * g_2 = f^{-1}(h_1) * f^{-1}(h_2).$$

(d) Denote the group multiplication in K by $\square$. Then

$$(g \circ f)(a * b) = g(f(a * b)) = g(f(a) \cdot f(b)) = g(f(a)) \,\square\, g(f(b))$$

so that $g \circ f$ is a group homomorphism.

□

The set of all automorphisms of G is a group under composition. This is a subgroup of the symmetric group on G as a set $S_G = \{f : G \to G \text{ bijective}\}$, i.e. $\mathrm{Aut}(G) \leq S_G$.

Examples.

1. There are unique group homomorphisms $\{1\} \to G$, $f : G \to \{1\}$.
2. For all groups G, the map $\mathrm{id} : G \to G$ is a group homomorphism:
$$\mathrm{id}(g_1 * g_2) = g_1 * g_2 = \mathrm{id}(g_1) * \mathrm{id}(g_2).$$
3. If $H \leq G$ is a subgroup, then $i : H \to G$ is a group homomorphism.
4. For any positive $a > 0$ the two maps $a^{(-)} : (\mathbb{R}, +) \overset{\cong}{\longleftrightarrow} (\mathbb{R}_{>0}, \times) : \log_a(-)$ are group isomorphisms:
$$a^{x+y} = a^x \cdot a^y$$
$$\log_a(x \cdot y) = \log_a x + \log_a y.$$
5. For $n \geq 1$ an integer, the two maps $(-)^n : (\mathbb{R}_{>0}, \times) \overset{\cong}{\longleftrightarrow} (\mathbb{R}_{>0}, \times) : \sqrt[n]{-}$ are inverse group automorphisms:
$$(xy)^n = x^n y^n$$
$$\sqrt[n]{xy} = \sqrt[n]{x} \cdot \sqrt[n]{y}.$$
6.

2.6 Quotient Groups

Theorem 6 (First Isomorphism Theorem)**.** *Let $F : H \to G$ be a group homomorphism. Then* $\mathrm{Im}f \overset{\cong}{\leftarrow} H/\ker f$.

2.7 Group Actions

Theorem 7 (Cayley)**.** *Any finite group G is isomorphic to a subgroup of $G_{|S|}$.*

Proof. It suffices to construct an injective group homomorphism $f : G \to S_G \cong S_{|G|}$. By the First Isomorphism Theorem, it'll then follow that $G/\ker f = G \cong \mathrm{im}f$. Remember that S_G is the set of all bijections $\alpha : G \to G$. We define f to send a group element g to the mapping L_g corresponding to left multiplication of g, i.e. $f(g) = L_g$ such that $L_g(g') = gg'$. More explicitly, $f : G \to S_G$, $g \mapsto (L_g : G \to G, g' \mapsto gg')$. We claim this is an injective group homomorphism. Notice that $|S_G| = G! > |G|$ unless $|G| = 1, 2$ so that f cannot be surjective in general. There are three things to verify: firstly, that $f(g) = L_g \in S_G$; secondly, that f is a group homomorphism; and thirdly, that $\ker f = \{1_G\}$. Proceeding in this order, notice that $L_g : G \to G$ is bijective because it has inverse $L_{g^{-1}}$: $(L_{g^{-1}} \circ L_g)(g') = g^{-1}(gg') = g'$ and similarly $(L_g \circ L_{g^{-1}})(g') = g'$, thus $L_g \circ$ □

Remark. $g \mapsto (R_g : g' \mapsto g'g)$. This is a group homomorphism $G^{\mathrm{op}} \to S_G$.

Chapter 3

Commutative Rings

3.1 First Properties

Definition. A **ring** is a set R with two binary operations $+$, $\times$ such that $(R, +, \times)$ is an abelian group and $(R, \times)$ is a semi-group ($\times$ is associative).

Proposition 7.1. *Let $(R, +, \times)$ be a ring, $r \in R$.*

1. $0_R \times r = 0_R = r \times 0_R$,
2. *Let $-r$ be the additive inverse of r. Then $-r = (-1_R) \times r = r \times (-1_R)$,*
3. 1_R *is unique,*
4. *If $1_R = 0_R$, then $R = \{0_R\}$. This is called the zero ring.*

Proposition 7.2. *If R is a commutative ring, then the binomial formula holds in R:*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

3.2 Fields

3.3 Polynomials

3.4 Homomorphisms

3.5 Greatest Common Divisors

3.6 Unique Factorization