MATH 4108: Abstract Algebra II

Frank Qiang
Instructor: Jennifer Hom

Georgia Institute of Technology
Spring 2024

Contents

Lecture 1

Jan. 8 — Rings and Fields

1.1 Lots of Definitions

Recall the definitions of a ring and a field:

Definition 1.1 (Ring)**.** A *ring* $R = (R, +, \cdot)$ is a non-empty set R together with two binary operations $+$ and $\cdot$, called addition and multiplication respectively, which satisfy:

(R1) *Associative law for addition*: $(a + b) + c = a + (b + c)$ for all $a, b, c \in R$.

(R2) *Commutative law for addition*: $a + b = b + a$ for all $a, b \in R$.

(R3) *Existence of zero*: There exists $0 \in R$ such that $a + 0 = a$ for all $a \in R$.

(R4) *Existence of additive inverses*: For all $a \in R$, there exists $-a \in R$ such that $a + (-a) = 0$.[1]

(R5) *Associative law for multiplication*: $(ab)c = a(bc)$ for all $a, b, c \in R$.

(R6) *Distributive laws*: $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ for all $a, b, c \in R$.

Definition 1.2 (Commutative ring)**.** In this class, we will mostly be interested in *commutative rings*, which satisfy the following additional property for multiplication:

(R7) *Commutative law for multiplication*: $ab = ba$ for all $a, b \in R$.

Definition 1.3 (Ring with unity)**.** A ring *with unity* satisfies the additional property that

(R8) *Existence of unity*: There exists $1 \neq 0 \in R$ such that and $a1 = 1a = a$ for $a \in R$.

Note that a ring need not be commutative to have a unity.

Definition 1.4 (Domain)**.** A commutative ring with unity is called a *(integral) domain* if it has the following cancellation property:

(R9) *Cancellation*: For all $a, b \in R$ and $c \neq 0$, $ca = cb$ implies $a = b$.

(R9') *No zero divisors*: For all $a, b \in R$, $ab = 0$ implies $a = 0$ or $b = 0$.

The conditions (R9) and (R9') are equivalent.

Definition 1.5 (Field)**.** A commutative ring with unity is called a *field* if it has the following additional property for multiplicative inverses:

(R10) *Existence of multiplicative inverses*: For all $a \neq 0 \in R$, there exists $a^{-1} \in R$ such that $aa^{-1} = 1$.

[1] Note that we'll usually write $a - b$ in place of $a + (-b)$.

Example 1.5.1. Some examples of rings are $\mathbb{Z}/2\mathbb{Z}$, which also happens to be a field. The ring $\mathbb{Z}$ is a domain. The set $M_{2\times 2}(\mathbb{R})$ is a non-commutative ring with unity, and has zero divisors. The ring $\mathbb{Q}$ is a field.[2] The real polynomials in a single variable $\mathbb{R}[x]$ form a ring, which is a domain but not a field. The complex numbers $\mathbb{C}$ and the real numbers $\mathbb{R}$ both form a field. The even integers $2\mathbb{Z}$ form a commutative ring without unity. In general, $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with unity, and is a field if and only if n is prime (and has zero divisors otherwise, if n is composite).

Remark. If $(R, +, \cdot)$ is a ring, then $(R, +)$ is an abelian group. If $(K, +, \cdot)$ is a field, then $(K^*, \cdot)$ is an abelian group, where $K^* = K \setminus \{0\}$.

Definition 1.6 (Group of units)**.** Let R be a commutative ring with unity. The *group of units* of R is

$$U = \{u \in R \mid \text{there exists } v \in R \text{ such that } uv = 1\}.$$

Exercise 1.1. Show that U is in fact a group under multiplication.

Definition 1.7 (Associate)**.** If $a, b \in R$ such that $a = ub$ for some $u \in U$, then a and b are called *associates*, denoted by $a \sim b$.

Exercise 1.2. Show that $\sim$ is in fact an equivalence relation.

Example 1.7.1. The group of units of $\mathbb{Z}$ is $\{1, -1\}$. The group of units of a field K is $K^* = K \setminus \{0\}$.

Exercise 1.3. Let $R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. Check the following:

1. R is a commutative ring with unity.
2. The group of units of R is $\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}, |a^2 - 2b^2| = 1\}$.

Definition 1.8 (Divisor)**.** Let D be an integral domain, $a \in D \setminus \{0\}$, $b \in D$. Then a divides b, or a is a *divisor* or *factor* of b, denoted by $a|b$, if there exists $z \in D$ such that $az = b$. We write $a \nmid b$ if a does not divide b. We say that a is a *proper divisor* or that a *properly divides* b if z is not a unit.

Remark. Equivalent, a is a proper divisor of b if and only if $a|b$ and $b \nmid a$.

Definition 1.9 (Subring)**.** A *subring* U of a ring R is a non-empty subset of R with the property that for all $a, b \in R$, $a, b \in U$ implies $a + b \in U$ and $ab \in U$, and $a \in U$ implies $-a \in U$.

Remark. Equivalently, U is a subring of R if and only if $a, b \in U$ implies $a - b \in U$ and $ab \in U$.

Remark. We automatically have $0 \in U$ since we can pick any $a \in U$, and then $0 = a - a \in U$.

Definition 1.10 (Subfield)**.** A *subfield* of a field K is a subset E containing at least two elements such that $a, b \in E$ implies $a - b \in E$ and $a \in E, b \in E \setminus \{0\}$ implies $ab^{-1} \in E$. If E is a subfield and $E \neq K$, then we say E is a *proper* subfield.

Remark. As before, we can replace the last condition with the equivalent statement that $a, b \in E$ implies $ab \in E$ and $a \in E \setminus \{0\}$ implies $a^{-1} \in E$.

Definition 1.11 (Ideal)**.** An *ideal* of R is a non-empty subset I of R with the properties that $a, b \in I$ implies $a - b \in I$ and $a \in I, r \in R$ implies $ra \in I$.

Remark. All ideals are subrings, but the converse is not true in general.

Example 1.11.1. The integers $\mathbb{Z}$ form a subring of $\mathbb{R}$ but not an ideal.

[2] In fact, $\mathbb{Q}$ is somehow the smallest field containing $\mathbb{Z}$.

Remark. We trivially have that $\{0\}$ and R are both ideals of R. An ideal I is called *proper* if $\{0\} \subsetneq I \subsetneq R$.

Theorem 1.1. *Let $A = \{a_1, \ldots, a_n\}$ be a finite subset of a commutative ring R. Then the set*

$$Ra_1 + \cdots + Ra_n = \{x_1a_1 + \cdots + x_na_n \mid x_i \in R\}$$

is the smallest ideal of R containing A.

Proof. See Howie. Check this is indeed an ideal and is contained in any other ideal containing A. □

Definition 1.12 (Ideals generated by elements of a ring)**.** The set $Ra_1 + \cdots + Ra_n$ is the *ideal generated by* $a_1, \ldots, a_n$, denoted by $\langle a_1, \ldots, a_n\rangle$. If the ideal is generated by a single element $a \in R$, then we say that $Ra = \langle a\rangle$ is a *principal ideal*.

Example 1.12.1. In $\mathbb{Z}$, the ideal $\langle 2\rangle = 2\mathbb{Z}$ are the even numbers. We have $\langle 2, 3\rangle = \mathbb{Z}$, but $\langle 6, 8\rangle = \langle 2\rangle$.

Theorem 1.2. *Let D be an integral domain with group of units U and let $a, b \in D \setminus \{0\}$. Then*

1. *$\langle a\rangle \subseteq \langle b\rangle$ if and only if $b|a$,*
2. *$\langle a\rangle = \langle b\rangle$ if and only if $a \sim b$,*
3. *$\langle a\rangle = D$ if and only if $a \in U$.*

Proof. See Howie. □

Definition 1.13 (Homomorphism of rings)**.** A *homomorphism* from a ring R to a ring S is a mapping $\varphi : R \to S$ such that $\varphi(a +_R b) = \varphi(a) +_S \varphi(b)$ and $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$.

Example 1.13.1. The zero mapping $\varphi(a) = 0$ is always a homomorphism. The inclusion map $\iota : 2\mathbb{Z} \to \mathbb{Z}$ or $\iota : \mathbb{Z} \to \mathbb{Q}$ is a homomorphism.

Theorem 1.3. *Let R, S be rings and $\varphi : R \to S$ a homomorphism. Then*

1. *$\varphi(0_R) = 0_S$,*
2. *$\varphi(-r) = -\varphi(r)$ for all $r \in R$,*
3. *the image $\varphi(R)$ is a subring of S.*

Proof. See Howie. □

Definition 1.14 (Monomorphism)**.** Let $\varphi : R \to S$ be a homomorphism. If φ is injective, we say that φ is a *monomorphism* or an *embedding*.

Example 1.14.1. The inclusion map $\varphi : \mathbb{Z} \to \mathbb{R}$ given by $\varphi(n) = n$ is an embedding.