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*

$$Ra_1 + \cdots + Ra_n = \{x_1 a_1 + \cdots + x_n a_n \mid x_i \in R\}$$

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.

Lecture 2

Jan. 10 — Field of Fractions, Polynomials

2.1 Isomorphisms

Definition 2.1 (Isomorphism)**.** If a homomorphism $\varphi : R \to S$ is both one-to-one and onto, then φ is an *isomorphism* and we say R and S are *isomorphic*, denoted $R \cong S$.

Definition 2.2 (Automorphism)**.** An isomorphism $\varphi : R \to R$ is called an *automorphism*.

Example 2.2.1. For any ring R, the identity map $\varphi : R \to R$ with $\varphi = \mathrm{id}$ is an automorphism.

Exercise 2.1. The complex conjugation $\varphi : \mathbb{C} \to \mathbb{C}$ with $\varphi(z) = \overline{z}$ is an automorphism.

Definition 2.3 (Kernel)**.** Let $\varphi : R \to S$ be a homomorphism. The *kernel* of φ is

$$\ker \varphi = \phi^{-1}(0_S) = \{a \in R : \varphi(a) = 0_S\}.$$

Exercise 2.2. For any homomorphism φ, $\ker \varphi$ is an ideal.

Definition 2.4 (Residue class)**.** Let I be an ideal of a ring R and $a \in R$. The set

$$a + I = \{a + x \mid x \in I\}$$

is the *residue class* of a modulo I.

Exercise 2.3. The set R/I of residue classes modulo I forms a ring with respect to the operations

$$(a + I) + (b + I) = (a + b) + I \quad \text{and} \quad (a + I)(b + I) = ab + I.$$

Exercise 2.4. The map $\theta_I : R \to R/I$ with $\theta_I(a) = a + I$ is a surjective homomorphism onto R/I with kernel I. This map θ_I is called the *natural homomorphism* from R to R/I.

Example 2.4.1. Consider $\mathbb{Z}$ and $I = \langle n \rangle = n\mathbb{Z}$. Then $\theta_I : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ with $\theta_I(a) = a + \langle n \rangle$ is the natural homomorphism. There are n residue classes, which are

$$\langle n \rangle, \quad 1 + \langle n \rangle, \quad \ldots, \quad (n - 1) + \langle n \rangle.$$

Theorem 2.1. *Let $n \in \mathbb{Z}_{>0}$. Then $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime.*

Proof. See Howie. $\square$

Remark. If $n = 0$, then $\mathbb{Z}/0\mathbb{Z} \cong \mathbb{Z}$.

Theorem 2.2. *Let $\varphi : R \to S$ be a surjective homomorphism with kernel K. Then there is an isomorphism $\alpha : R/K \to S$ such that the following diagram commutes (i.e. $\varphi = \alpha \circ \theta_K$):*

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "\theta_K"'] & S \\ R/K \arrow[ur, "\alpha"] & \end{tikzcd}$$

Proof. See Howie. But the general idea is to define $\alpha : R/K \to S$ by $\alpha(a+K) = \varphi(a)$. Then need to check that α is well-defined and an isomorphism. □

2.2 Field of Fractions

The motivating question is: How do we get from $\mathbb{Z}$ to $\mathbb{Q}$? Recall that

$$\mathbb{Q} = \{a/b \mid a, b \in \mathbb{Z}, b \neq 0\},$$

where $a/c = b/d$ if $ad = bc$. We add and multiply fractions by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \quad \text{and} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

How do we do this more generally (construct a field out of an arbitrary integral domain)?

Definition 2.5 (Field of fractions of a domain)**.** Let D be an integral domain and

$$P = D \times (D \setminus \{0\}) = \{(a, b) \mid a, b \in D, b \neq 0.\}$$

Define an equivalence relation $\equiv$ on P by $(a, b) \equiv (a', b')$ if $ab' = a'b$. Then the *field of fractions* of D is

$$Q(D) = P/{\equiv}.$$

We denote the equivalence class $[a, b]$ by a/b, i.e. $a/b = c/d$ if $ad = bc$. We define addition and multiplication on $Q(D)$ by

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \quad \text{and} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Exercise 2.5. Do the following:

1. Check that $\equiv$ is an equivalence relation.
2. Check that these operations are well-defined.
3. Check that $Q(D)$ is a commutative ring with unity.
   - The zero element is $0/b$ for $b \neq 0$.
   - The unity element is a/a for $a \neq 0$.
   - The negative of a/b is $(-a)/b$ or equivalently $a/(-b)$.
   - The multiplicative inverse of a/b is b/a for $a, b \neq 0$.
4. Complete the previous exercise and check that $Q(D)$ is a field.

Exercise 2.6. The map $\phi : D \to Q(D)$ defined by $\phi(a) = a/1$ is a monomorphism. In particular, the field of fractions $Q(D)$ contains D as a subring and $Q(D)$ is the smallest field containing D, in the sense that if K is a field with the property that there exists a monomorphism $\theta : D \to K$, then there exists a monomorphism $\psi : Q(D) \to K$ such that the following diagram commutes:

$$\begin{tikzcd} D \arrow[r, "\theta"] \arrow[d, "\varphi"'] & K \\ Q(D) \arrow[ur, "\psi"] & \end{tikzcd}$$

2.3 The Characteristic of a Field

Note that for $a \in R$, we might write $a + a$ as $2a$ and $a + a + \cdots + a$ (n times) as na. Furthermore, $0a = 0_R$ and $(-n)a = n(-a)$ for $n \in \mathbb{Z}_{>0}$. Thus na has meaning for all $n \in \mathbb{Z}$.[1]

Exercise 2.7. For $a, b \in R$ and $m, n \in \mathbb{Z}$, we have $(ma)(nb) = (mn)(ab)$.

Definition 2.6 (Characteristic of a ring)**.** For an arbitrary ring R, there are two possibilities:

1. $m1_R$ for $m \in \mathbb{Z}$ are all distinct. In this case, we say that R has *characteristic* 0.
2. There exists $m, n \in \mathbb{N}$ such that $m1_R = (m + n)1_R$. In this case, we say that R has *characteristic* n, where n is the least positive n for which this property holds.

We denote the characteristic of R by $\operatorname{char} R$. If $\operatorname{char} R = n$, then $na = 0_R$ for all $a \in R$ since

$$na = (n1_R)a = 0a = 0.$$

Example 2.6.1. We have $\operatorname{char} \mathbb{Z}/n\mathbb{Z} = n$.

Theorem 2.3. *The characteristic of a field is either* 0 *or a prime.*

Proof. Let K be a field and suppose $\operatorname{char} K = n \neq 0$ and n is not prime. Then we can write $n = rs$ where $1 < r, s < n$. The minimal property of n implies that $r1_K \neq 0$ and $s1_K \neq 0$. But then

$$r1_K \cdot s1_K = rs1_K = n1_K = 0,$$

which is impossible since K is a field and thus has no zero divisors. □

Remark. Note the following:

1. If K is a field with $\operatorname{char} K = 0$, then K has a subring isomorphic to $\mathbb{Z}$, i.e. elements of the form $n1_K$ for $n \in \mathbb{Z}$, and K has a subfield isomorphic to $\mathbb{Q}$, i.e.

   $$P(K) = \{m1_K/n1_K \mid m, n \in \mathbb{Z}, n \neq 0\}.$$

   This is the *prime subfield* of K, and any subfield of K must contain $P(K)$.
2. If K is a field with $\operatorname{char} K = p$, then the prime subfield of K is

   $$P(K) = \{1_K, 2 \cdot 1_K, \ldots, (p-1) \cdot 1_K\},$$

   which is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

[1] This is saying that any abelian group is naturally a *module* over the integers $\mathbb{Z}$.

Remark. In other words, every field of characteristic 0 is an *extension* of $\mathbb{Q}$ (contains $\mathbb{Q}$ as a subfield), and every field of characteristic p is an *extension* of $\mathbb{Z}/p\mathbb{Z}$ (contains $\mathbb{Z}/p\mathbb{Z}$ as a subfield).

Remark. If $\operatorname{char} K = 0$, then writing $a/n1_K$ as a/n is fine. But if $\operatorname{char} K = p$, then a/n does not make sense when $p|n$ (since $p \cdot 1_K = 0$).

Theorem 2.4. *If K is a field with $\operatorname{char} K = p$, then for all $x, y \in K$, $(x+y)^p = x^p + y^p$.*

Proof. See Howie. Uses the binomial theorem. □

2.4 Polynomials

Let R be a ring, then we have the polynomial ring over R

$$R[X] = \{a_0 + a_1X + \cdots + a_nX^n \mid a_i \in R, n \in \mathbb{N}\}.$$

If $f \in R[X]$, then it has *degree* n if the last nonzero element in the sequence $\{a_0, a_1, \dots\}$ is a_n, denoted $\partial f = n$. By convention, the zero polynomial has degree $-\infty$. The coefficient a_n is called the *leading coefficient*, and if $a_n = 1$, then f is *monic*. Addition and multiplication work as expected:

$$(a_0 + a_1X + \cdots + a_mX^m) + (b_0 + b_1X + \cdots + b_nX^n) = (a_0 + b_0) + (a_1 + b_1)X + \dots$$

and

$$(a_0 + a_1X + \cdots + a_mX^m)(b_0 + b_1X + \cdots + b_nX^n) = c_0 + c_1X + \dots$$

where

$$c_k = \sum_{i+j=k}^{k} a_ib_j.$$

The ground ring R sits inside of the polynomial ring $R[X]$. Take the monomorphism $\theta : R \to R[X]$ by $\theta(a) = a$, i.e. an element a maps to the constant polynomial a.

Theorem 2.5. *Let D be an integral domain. Then*

1. *$D[X]$ is an integral domain.*
2. *If $p, q \in D[X]$, then $\partial(p+q) \leq \max(\partial p, \partial q)$.*
3. *If $p, q \in D[X]$, then $\partial(pq) = \partial p + \partial q$.*
4. *The group of units of $D[X]$ coincides with the group of units of D.*

Proof. Statements (2) and (3) are left as exercises.

(1) We need to show that $D[X]$ has no zero divisors. For this, suppose that p, q are nonzero polynomials with leading coefficients a_m and b_n respectively. Then the leading coefficient of pq is a_mb_n, which is nonzero since D is an integral domain and thus has no zero divisors. So pq is nonzero.

(4) Let $p, q \in D[X]$ and suppose $pq = 1$. Since $\partial(pq) = \partial(1) = 0$, we must have $\partial p = \partial q = 0$. Thus $p, q \in D$ and $pq = 1$ if and only if p and q are in the group of units of D. □

Since $D[X]$ is a domain, we can consider polynomials in the variable Y with coefficients in $D[X]$:

$$D[X, Y] = (D[X])[Y].$$

We can repeat this to get polynomials in n variables: $D[X_1, X_2, \dots, X_n]$, which is an integral domain.