

MATH 4108: Abstract Algebra II

Frank Qiang
Instructor: Jennifer Hom

Georgia Institute of Technology
Spring 2024

Contents

| | | |
|----------|--|-----------|
| 1 | Jan. 8 — Rings and Fields | 2 |
| 1.1 | Lots of Definitions | 2 |
| 2 | Jan. 10 — Field of Fractions, Polynomials | 5 |
| 2.1 | Isomorphisms | 5 |
| 2.2 | Field of Fractions | 6 |
| 2.3 | The Characteristic of a Field | 7 |
| 2.4 | Polynomials | 8 |
| 3 | Jan. 17 — Irreducible Polynomials | 9 |
| 3.1 | Principal Ideal Domains and Irreducible Polynomials | 9 |
| 3.2 | Irreducible Polynomials over \mathbb{C} , \mathbb{R} , \mathbb{Q} , and \mathbb{Z} | 10 |
| 4 | Jan. 22 — Field Extensions | 14 |
| 4.1 | More on Irreducibility | 14 |
| 4.2 | Field Extensions | 15 |

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 $a1 = 1a = a$ 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 $aa^{-1} = 1$.

¹Note 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. Equivalently, 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.

²In 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 $A = \{a_1, \dots, a_n\}$ be a finite subset of a commutative ring R . Then the set

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

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 . \square

Definition 1.12 (Ideals generated by elements of a ring). The set $Ra_1 + \dots + Ra_n$ is the *ideal generated* by a_1, \dots, a_n , denoted by $\langle a_1, \dots, a_n \rangle$. 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. \square

Definition 1.13 (Homomorphism of rings). A *homomorphism* from a ring R to a ring S is a mapping $\varphi : R \rightarrow S$ 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 $\iota : 2\mathbb{Z} \rightarrow \mathbb{Z}$ or $\iota : \mathbb{Z} \rightarrow \mathbb{Q}$ is a homomorphism.

Theorem 1.3. Let R, S be rings and $\varphi : R \rightarrow S$ 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. \square

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

Example 1.14.1. The inclusion map $\varphi : \mathbb{Z} \rightarrow \mathbb{R}$ 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 $\varphi : R \rightarrow S$ 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 $\varphi : R \rightarrow R$ is called an *automorphism*.

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

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

Definition 2.3 (Kernel). Let $\varphi : R \rightarrow S$ 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 $\theta_I : R \rightarrow R/I$ 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 $\theta_I : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ with $\theta_I(a) = a + \langle n \rangle$ is the natural homomorphism. There are n residue classes, which are

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

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. □

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

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

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ \theta_K \downarrow & \nearrow \alpha & \\ R/K & & \end{array}$$

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

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 $\varphi : D \rightarrow Q(D)$ defined by $\varphi(a) = a/1$ 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 $\theta : D \rightarrow K$, then there exists a monomorphism $\psi : Q(D) \rightarrow K$ such that the following diagram commutes:

$$\begin{array}{ccc} D & \xrightarrow{\theta} & K \\ \varphi \downarrow & \nearrow \psi & \\ Q(D) & & \end{array}$$

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 $\text{char } R$. If $\text{char } R = n$, then $na = 0_R$ for all $a \in R$ since

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

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

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

Proof. Let K be a field and suppose $\text{char } K = n \neq 0$ 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 $\text{char } K = 0$, 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 $\text{char } K = p$, then the prime subfield of K is

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

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

¹This 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 $\text{char } K = 0$, then writing $a/n1_K$ as a/n is fine. But if $\text{char } K = p$, 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 $\text{char } K = p$, 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

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

The ground ring R sits inside of the polynomial ring $R[X]$. Take the monomorphism $\theta : R \rightarrow R[X]$ 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 $a_m b_n$, 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.

Lecture 3

Jan. 17 — Irreducible Polynomials

3.1 Principal Ideal Domains and Irreducible Polynomials

Definition 3.1. The field of fractions of $D[X]$ consists of *rational forms*

$$\frac{a_0 + a_1X + \cdots + a_mX^m}{b_0 + b_1X + \cdots + b_nX^n}$$

where $b_0 + b_1X + \cdots + b_nX^n \neq 0$, denoted by $D(X)$.

Definition 3.2. A domain D is a *principal ideal domain* (PID) if all of its ideals are principal.¹

Example 3.2.1. The integers \mathbb{Z} is a PID, since every ideal is of the form $\langle n \rangle$.

Definition 3.3. A non-zero, non-unit element p in a domain D is *irreducible* if it has no proper factors.

Definition 3.4. A domain D is a *unique factorization domain* (UFD) if every non-unit $a \neq 0$ in D has an essentially unique² factorization into irreducible elements.

Example 3.4.1. Again \mathbb{Z} is a UFD, e.g. $12 = 2 \cdot 2 \cdot 3 = (-2) \cdot 2 \cdot (-3)$.

Theorem 3.1. *Every PID is a UFD.*

Proof. See Howie. □

Theorem 3.2. *If K is a field, then $K[X]$ is a PID.*

Proof. See Howie. □

Theorem 3.3. *Let p be an element in a PID D . Then the following are equivalent:*

1. p is irreducible.
2. $\langle p \rangle$ is maximal.
3. $D/\langle p \rangle$ is a field.

In particular if $f \in K[X]$, then $K[X]/\langle f \rangle$ is a field if and only if f is irreducible.

Proof. See Howie. □

¹Recall that a principal ideal is one generated by a single element.

²As in, unique up to use of associates or adding in units.

Definition 3.5. Let D be a domain and $\alpha \in D$. Let $\sigma_\alpha : D[X] \rightarrow D$ defined by

$$\sigma_\alpha(a_0 + a_1X + \cdots + a_nX^n) = a_0 + a_1\alpha + \cdots + a_n\alpha^n.$$

Note that we often write $\sigma_\alpha(f)$ as $f(\alpha)$. If $f(\alpha) = 0$, we say α is a *root* of f , or a *zero*.

Exercise 3.1. Check that σ_α is a homomorphism.

Theorem 3.4. Let K be a field, $\beta \in K$ and f a non-zero polynomial in $K[X]$. Then β is a root of f if and only if $X - \beta \mid f$.

Proof. See Howie. □

Example 3.5.1. We have $X^2 + 1$ in $\mathbb{R}[X]$ is irreducible, so $\mathbb{R}[X]/\langle X^2 + 1 \rangle$ is a field. In fact this field is isomorphic to the complex numbers \mathbb{C} .

Exercise 3.2. Do the following:

1. Show that $\varphi : \mathbb{R}[X] \rightarrow \mathbb{C}$ given by

$$\varphi(a_0 + a_1X + \cdots + a_nX^n) = a_0 + a_1i + \cdots + a_ni^n$$

is a surjective homomorphism.³

2. Show that $\ker \varphi = \langle X^2 + 1 \rangle$.

So by the first isomorphism theorem we can conclude that $\mathbb{R}[X]/\langle X^2 + 1 \rangle = \mathbb{R}[\ker \varphi] \cong \varphi(\mathbb{R}[X]) = \mathbb{C}$.

Theorem 3.5. Let K be a field and $g \in K[X]$ an irreducible polynomial. Then $K[X]/\langle g \rangle$ is a field containing K up to isomorphism.

Proof. Since g is irreducible, $K[X]/\langle g \rangle$ is a field. Now define $\varphi : K \rightarrow K[X]/\langle g \rangle$ by

$$\varphi(a) = a + \langle g \rangle.$$

(Left as an exercise to check that φ is a homomorphism.) We need to show that φ is injective. For this, take $a, b \in K$. If $a + \langle g \rangle = b + \langle g \rangle$, then $a - b \in \langle g \rangle$. But K is a field, so this happens precisely when $a = b$. Thus φ embeds K into $K[X]/\langle g \rangle$, as desired. □

3.2 Irreducible Polynomials over \mathbb{C} , \mathbb{R} , \mathbb{Q} , and \mathbb{Z}

Our goal now is to study irreducible polynomials. Note that linear polynomials are irreducible, and recall that every polynomial in \mathbb{C} factorizes, essentially uniquely, into linear factors. Furthermore, complex roots of real polynomials come in conjugate pairs, hence

$$g = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{R}[X]$$

factors as

$$g = a_n(X - \beta_1) \cdots (X - \beta_r)(X - \gamma_1)(X - \bar{\gamma}_1) \cdots (X - \gamma_s)(X - \bar{\gamma}_s)$$

³Note that there's some technicality about this φ not being a σ_α since we defined σ_α for α in the base domain, and i is kind of somewhere else.

in $\mathbb{C}[X]$, where $\beta_1, \dots, \beta_r \in \mathbb{R}$ and $\gamma_1, \dots, \gamma_s \in \mathbb{C} \setminus \mathbb{R}$ and $r + 2s = n$. Thus over $\mathbb{R}[X]$, g factors as

$$g = a_n(X - \beta_1) \dots (X - \beta_r)(X^2 - (\gamma_1 + \bar{\gamma}_1)X + \gamma_1\bar{\gamma}_1) \dots (X^2 - (\gamma_s + \bar{\gamma}_s)X + \gamma_s\bar{\gamma}_s)$$

in $\mathbb{R}[X]$, where the quadratic factors are irreducible in $\mathbb{R}[X]$.

Exercise 3.3. A quadratic $aX^2 + bX + c \in \mathbb{R}[X]$ is irreducible if and only if its discriminant $b^2 - 4ac < 0$.

Now we have pretty much characterized irreducible polynomials in $\mathbb{R}[X]$. But what about $\mathbb{Q}[X]$?

Theorem 3.6. Let $g = a_0 + a_1X + a_2X^2 \in \mathbb{Q}[X]$. Then

1. If g is irreducible over \mathbb{R} , then it is irreducible over \mathbb{Q} .
2. If $g = a_2(X - \beta_1)(X - \beta_2)$ with $\beta_1, \beta_2 \in \mathbb{R}$, then g is irreducible in $\mathbb{Q}[X]$ if and only if β_1 and β_2 are irrational.

Proof. (1) We show the contrapositive. If g factors as

$$g = a_2(X - q_1)(X - q_2) \in \mathbb{Q}[X],$$

then g also factors in $\mathbb{R}[X]$.

(2) If β_1 and β_2 are rational, then g factors in $\mathbb{Q}[X]$ and is thus not irreducible. For the other direction, if β_1 and β_2 are irrational, then $g = a_2(X - \beta_1)(X - \beta_2)$ is the only factorization in $\mathbb{R}[X]$ since $\mathbb{R}[X]$ is a UFD, so there is no factorization in $\mathbb{Q}[X]$ into linear factors. \square

Example 3.5.2. Are the following polynomials irreducible in $\mathbb{R}[X]$? In $\mathbb{Q}[X]$?

1. $X^2 + X + 1$ is irreducible over \mathbb{R} and \mathbb{Q} since $b^2 - 4ac = -3$.
2. $X^2 - X - 1$ has roots $(-1 \pm \sqrt{5})/2$, so it factors over \mathbb{R} but is irreducible over \mathbb{Q} .
3. $X^2 + X - 2$ factors as $(X + 2)(X - 1)$ over \mathbb{R} and \mathbb{Q} .

Now that we have studied irreducible polynomials in $\mathbb{R}[X]$ and $\mathbb{Q}[X]$, can a polynomial in $\mathbb{Z}[X]$ be irreducible over \mathbb{Z} but not \mathbb{Q} ? The answer is no!

Theorem 3.7 (Gauss's lemma). Let f be a polynomial in $\mathbb{Z}[X]$, irreducible over \mathbb{Z} . Then f is irreducible over \mathbb{Q} .

Proof. For sake of contradiction, suppose $f = gh$ with $g, h \in \mathbb{Q}[X]$ and $\partial g, \partial h < \partial f$. Then there exists $n \in \mathbb{Z}_{>0}$ such that $nf = g'h'$ where $g', h' \in \mathbb{Z}[X]$. Let n be the smallest positive integer with this property. Let

$$\begin{aligned} g' &= a_0 + a_1X + \dots + a_kX^k \\ h' &= b_0 + b_1X + \dots + b_lX^l. \end{aligned}$$

If $n = 1$, then $g' = g$ and $h' = h$, a contradiction. Now $n \geq 1$, so let p be a prime factor of n .⁴ Without loss of generality, assume p divides g' , i.e. $g' = pg''$ where $g'' \in \mathbb{Z}[X]$. Then

$$\frac{n}{p}f = g''h',$$

contradicting the minimality of n . Hence f cannot be factored over \mathbb{Q} . \square

⁴Lemma: Either p divides all the coefficients of g' or p divides all the coefficients of h' . Proof left as an exercise.

Example 3.5.3. Show that $g = X^3 + 2X^2 + 4X - 6$ is irreducible over \mathbb{Q} .

Proof. If g factors over \mathbb{Q} , it factors over \mathbb{Z} and at least one factor must be linear, i.e.

$$g = X^3 + 2X^2 + 4X - 6 = (X - a)(X^2 + bX + c)$$

where $a, b, c \in \mathbb{Z}$. We must have $ac = 6$, so $a \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$ and $g(a) = 0$. We can check this:

| a | 1 | -1 | 2 | -2 | 3 | -3 | -6 | 6 |
|--------|---|----|---|-----|----|-----|-----|------|
| $g(a)$ | 1 | -9 | 1 | -10 | 51 | -27 | 306 | -174 |

Hence g is irreducible over \mathbb{Z} and thus also irreducible over \mathbb{Q} . □

We could do this trick since the degree was 3, forcing a linear factor. What about degrees higher than 3?

Theorem 3.8 (Eisenstein's criterion). *Let $f = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$. Suppose there exists a prime p such that*

1. $p \nmid a_n$,
2. $p \mid a_i$ for $i = 0, \dots, n-1$,
3. $p^2 \nmid a_0$.

Then f is irreducible over \mathbb{Q} .

Proof. By Gauss's lemma, it suffices to show that f is irreducible over \mathbb{Z} . Suppose for sake of contradiction that $f = gh$ for

$$g = b_0 + b_1X + \cdots + b_rX^r \quad \text{and} \quad h = c_0 + c_1X + \cdots + c_sX^s,$$

$r, s < n$, and $r + s = n$. Note that $a_0 = b_0c_0$, so $p \mid a_0$ from (2) implies that $p \mid b_0$ or $p \mid c_0$. Since $p^2 \nmid a_0$, it cannot be both. Without loss of generality, assume $p \mid b_0$ and $p \nmid c_0$. Now suppose inductively that p divides b_0, \dots, b_{k-1} where $1 \leq k \leq r$. Then

$$a_k = b_0c_k + b_1c_{k-1} + \cdots + b_{k-1}c_1 + b_kc_0$$

and since p divides $a_k, b_0c_k, b_1c_{k-1}, \dots, b_{k-1}c_1$, it follows that $p \mid b_kc_0$. Since $p \nmid c_0$ by assumption, we must have $p \mid b_k$. Thus $p \mid b_r$ and since $a_n = b_rc_s$, we have $p \mid a_n$, contradicting (1). Hence f is irreducible. □

Example 3.5.4. The polynomial

$$X^5 + 2X^3 + \frac{8}{7}X^2 - \frac{4}{7}X + \frac{2}{7}$$

is irreducible over \mathbb{Q} .

Proof. Multiply by 7 and take the integer polynomial $7X^5 + 14X^3 + 8X^2 - 4X + 2$. Taking $p = 2$ satisfies Eisenstein's criterion, so this polynomial is irreducible over \mathbb{Z} and thus also irreducible over \mathbb{Q} . □

Example 3.5.5. If $p > 2$ is prime, then show that

$$f = 1 + X + X^2 + \cdots + X^{p-1}$$

is irreducible over \mathbb{Q} .

Proof. First observe that

$$f = \frac{X^p - 1}{X - 1}.$$

Let $g(X) = f(X + 1)$. Then

$$\begin{aligned} g(X) &= \frac{(X + 1)^p - 1}{(X + 1) - 1} = \frac{1}{X}((X + 1)^p - 1) = \frac{1}{X} \sum_{i=0}^p \binom{p}{i} X^{p-i} - 1 \\ &= \frac{1}{X} \sum_{i=0}^{p-1} \binom{p}{i} X^{p-i} = \sum_{i=0}^{p-1} \binom{p}{i} X^{p-i-1}. \end{aligned}$$

Note that $\binom{p}{1}, \binom{p}{2}, \dots, \binom{p}{p-1}$ are all divisible by p , so g is irreducible by Eisenstein's criterion. Now if f factors as $f = uv$, then $g(X) = u(X + 1)v(X + 1)$, which is a contradiction since g is irreducible. \square

Lecture 4

Jan. 22 — Field Extensions

4.1 More on Irreducibility

The following excerpt is from Howie:

Another device for determining irreducibility over \mathbb{Z} (and consequently over \mathbb{Q}) is to map the polynomial onto $\mathbb{Z}_p[X]$ for some suitably chosen prime p . Let $g = a_0 + a_1X + \cdots + a_nX_n \in \mathbb{Z}[X]$, and let p be a prime not dividing a_n . For each i in $\{0, 1, \dots, n\}$, let \bar{a}_i denote the residue class $a_i + \langle p \rangle$ in the field $\mathbb{Z}_p = \mathbb{Z}/\langle p \rangle$, and write the polynomial $\bar{a}_0 + \bar{a}_1X + \cdots + \bar{a}_nX_n$ as \bar{g} . Our choice of p ensures that $\partial \bar{g} = n$. Suppose that $g = uv$, with $\partial u, \partial v < \partial g$ and $\partial u + \partial v = \partial g$. Then $\bar{g} = \bar{u}\bar{v}$. If we can show that \bar{g} is irreducible in $\mathbb{Z}_p[X]$, then we have a contradiction, and we deduce that g is irreducible. The advantage of transferring the problem from $\mathbb{Z}[X]$ to $\mathbb{Z}_p[X]$ is that \mathbb{Z}_p is finite, and the verification of irreducibility is a matter of checking a finite number of cases.

Example 4.0.1. Show that

$$g = 7X^4 + 10X^3 - 2X^2 + 4X - 5$$

is irreducible over \mathbb{Q} .

Proof. Let $p = 3$ and

$$\bar{g} = X^4 + X^3 + X^2 + 1$$

This has no linear factors since

$$\bar{g}(0) = 1, \quad \bar{g}(1) = 2, \quad \bar{g}(-1) = 1.$$

So suppose

$$\bar{g} = X^4 + X^3 + X^2 + X + 1 = (X^2 + aX + b)(X^2 + cX + d)$$

in $\mathbb{Z}_3[x]$. Then for some $a, b, c, d \in \mathbb{Z}_3 = \{-1, 0, 1\}$, we have

$$\begin{cases} X^3 & a + c = 1 \\ X^2 & b + ac + d = 1 \\ X & ad + bc = 1 \\ 1 & bd = 1 \end{cases}$$

The first case is if $b = d = 1$, but this implies $ac = -1$, so $a = \pm 1$ and $c = \mp 1$. But $a + c = 1$, so this cannot happen. The second case is if $b = d = -1$. This implies that $ac = 0$ and $a + c = 1$. So if $a = 0$, then $c = 1$, so $1 = ad + bc = b$, which is a contradiction with $b = -1$. If $c = 0$, then $1 = ad + bc = d$,

which is a contradiction with $d = -1$. Thus \bar{g} is irreducible in $\mathbb{Z}_3[x]$, so g is irreducible in $\mathbb{Z}[x]$, and by Gauss's lemma, g is irreducible in $\mathbb{Q}[x]$. \square

Remark. If we had tried $p = 2$, then we have $\bar{g} = x^4 + 1 \in \mathbb{Z}_2[x]$, which is not in fact irreducible since

$$\bar{g} = x^4 + 1 = (x + 1)^4 \in \mathbb{Z}_2[x].$$

4.2 Field Extensions

Definition 4.1. Let K, L be fields and $\varphi : K \rightarrow L$ an injective homomorphism. Then L is a *field extension* of K , denoted $L : K$.

Example 4.1.1. We have $\mathbb{C} : \mathbb{R}$ is a field extension.

Definition 4.2. Recall that V is a K -vector space if

1. V is an abelian group under $+$,
2. For $a, b \in K$ and $x, y \in V$, we have

$$(i). a(x + y) = ax + ay, \quad (ii). (a + b)x = ax + bx, \quad (iii). (ab)x = a(bx), \quad (iv). 1x = x.$$

Remark. If $L : K$ is a field extension, then L is a vector space over K .

Definition 4.3. A *basis* for a vector space is a linearly independent spanning set.

Example 4.3.1. The complex numbers \mathbb{C} is a \mathbb{R} -vector space with basis $\{1, i\}$. Bases are not unique, since $\{1 + i, 1 - i\}$ is another basis for \mathbb{C} .

Example 4.3.2. If there is a vector space that we know to be a field, then it is automatically a field extension of its ground field.

Definition 4.4. The *dimension* of L is the cardinality of a basis for $L : K$.¹ The dimension is also called the *degree* of $L : K$, denoted $[L : K]$. We say that L is a *finite extension* if $[L : K]$ is finite, and an *infinite extension* otherwise.

Example 4.4.1. We have $[\mathbb{C} : \mathbb{R}] = 2$, which is finite. On the other hand, $\mathbb{R} : \mathbb{Q}$ is an infinite extension.

Theorem 4.1. Let $L : K$ be a field extension. Then $L = K$ if and only if $[L : K] = 1$.

Proof. (\Rightarrow) If $L = K$, then $\{1\}$ is a basis for $L : K$, and thus $[L : K] = 1$.

(\Leftarrow) If $[L : K] = 1$, then $\{x\}$ is a basis for $L : K$ for some $x \in L$. Then there exists some $a \in K$ such that $1 = ax$, so $x = a^{-1} \in K$. For every $y \in L$, there exists $b \in K$ such that $y = bx$. But then

$$y = bx = b(a^{-1}) \in K,$$

so $y \in K$ as well by closure. Thus $L = K$ as desired. \square

Remark. Let $L : K$ and $M : L$ be field extensions with

$$K \xrightarrow{\alpha} L \xrightarrow{\beta} M$$

¹Note that this is well-defined since any two bases of L have the same length.

Then $M : K$ is also a field extension.

Theorem 4.2. *For field extensions $L : K$ and $M : L$, we have $[M : L][L : K] = [M : K]$.*

Proof. Suppose $\{a_1, a_2, \dots, a_r\}$ is a linearly independent subset of M over L and $\{b_1, b_2, \dots, b_s\}$ is a linearly independent subset of L over K . Now we claim that

$$\{a_i b_j \mid 1 \leq i \leq r, 1 \leq j \leq s\}$$

is a linearly independent subset of M over K . To see this, suppose

$$\sum_{i=1}^r \sum_{j=1}^s \lambda_{ij} a_i b_j = 0$$

for some $\lambda_{ij} \in K$. We can rewrite this as

$$\sum_{i=1}^r \left(\sum_{j=1}^s \lambda_{ij} b_j \right) a_i = 0.$$

Since the a_i are linearly independent over L , it follows that

$$\sum_{j=1}^s \lambda_{ij} b_j = 0$$

for each $i = 1, \dots, r$. Since the b_j are linearly independent over K , it follows that $\lambda_{ij} = 0$ for each i, j , which proves the claim. Returning to the main proof, if $[M : L]$ or $[L : K]$ is infinite, then r or s can be made arbitrarily large, so

$$\{a_i b_j \mid 1 \leq i \leq r, 1 \leq j \leq s\}$$

can also be made arbitrarily large, and hence $[M : K]$ is infinite. Now suppose $[M : L] = r < \infty$ and $[L : K] = s < \infty$. Let $\{a_1, a_2, \dots, a_r\}$ be a basis for $M : L$ and $\{b_1, b_2, \dots, b_s\}$ be a basis for $L : K$. We will show that

$$\{a_i b_j \mid 1 \leq i \leq r, 1 \leq j \leq s\}$$

is a basis for $M : K$. Since we already showed that $\{a_i b_j\}$ is linearly independent, it only remains to show that they span M over K . For each $z \in M$, there exist $\lambda_1, \dots, \lambda_r \in L$ such that

$$z = \sum_{i=1}^r \lambda_i a_i.$$

Then for each $\lambda_i \in L$, there exist $\mu_{i1}, \dots, \mu_{is} \in K$ such that

$$\lambda_i = \sum_{j=1}^s \mu_{ij} b_j.$$

Combining this yields

$$z = \sum_{i=1}^r \sum_{j=1}^s \mu_{ij} a_i b_j$$

as desired, which finishes the proof. □

Example 4.4.2. Consider $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

Exercise 4.1. Show that $\mathbb{Q}[\sqrt{2}]$ is a field. (Hint: $1/(a + b\sqrt{2}) = (a - b\sqrt{2})/(a^2 - 2b^2)$.)

Definition 4.5. Let K be a subfield of L and S a subset of L . The *subfield of L generated over K by S* , denoted $K(S)$, is the intersection of all subfields of L containing $K \cup S$. If $S = \{\alpha_1, \dots, \alpha_n\}$ is finite, we write $K(\alpha_1, \dots, \alpha_n)$.

Theorem 4.3. Let E be the elements in L that can be expressed as quotients of finite K -linear combinations of finite products of elements in S . Then $K(S) = E$.

Proof. To see that $K(S) \subseteq E$, simply check that E is a subfield of L containing $K \cup S$.

For $E \subseteq K(S)$, note that any subfield of L containing K and S must contain all finite products of elements in S , all linear combinations of such products, and all quotients of such linear combinations. This is precisely what it means to have $E \subseteq K(S)$. \square

Definition 4.6. A *simple extension* of K is $K(\alpha)$, i.e. S has a single element $\alpha \notin K$.

Example 4.6.1. The previous example $\mathbb{Q}(\sqrt{2})$ is a simple extension.

Theorem 4.4. Let L be a field, K a subfield, and $\alpha \in L$. Then either

1. $K(\alpha)$ is isomorphic to $K(X)$, the field of rational forms with coefficients in K ,
2. or there exists a unique monic polynomial $m \in K[X]$ with the property that for all $f \in K[X]$,
 - (a) $f(\alpha) = 0$ if and only if $m \mid f$,
 - (b) the field $K(\alpha)$ coincides with $K[\alpha]$, the ring of all polynomials in α with coefficients in K ,
 - (c) and $[K[\alpha] : K] = \deg m$.

Proof. Suppose there does not exist nonzero $f \in K[X]$ such that $f(\alpha) = 0$. Then there exists a map $\varphi : K(X) \rightarrow K(\alpha)$ with $f/g \mapsto f(\alpha)/g(\alpha)$, which is defined since $g(\alpha) = 0$ only if g is the zero polynomial. Note that φ is a surjective homomorphism,² which one can check as an exercise. Now we show that φ is also injective. To see this, suppose

$$\varphi(f/g) = \varphi(p/q),$$

which happens if and only if

$$f(\alpha)q(\alpha) - p(\alpha)g(\alpha) = 0$$

in L . This happens if and only if $fq - pg = 0$ in $K[X]$, which happens if and only if $f/g = p/q$ in $K(X)$. This completes the first case of the theorem. (Second case of the theorem to be done next class.) \square

Example 4.6.2. Continuing the same example, note that

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} = \{a_0 + a_1\sqrt{2} + a_2\sqrt{2}^2 + a_3\sqrt{2}^3 + \dots + a_n\sqrt{2}^n \mid a_i \in \mathbb{Q}\},$$

which falls in the second case of the previous theorem.

Remark. We also have $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}[X]/\langle X^2 - 2 \rangle$.

²Also check that φ is well-defined.