Contents

Motivation and Introduction

Main purpose of this course is to study Galois theory — a field that arose in trying to study roots of polynomials.

Consider $f(x) = ax^2 + bx + c$. If we want to find a general, closed-form expression for the roots of the function, we complete the square.

$$\text{roots} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

We found these roots by by the coefficients, $\mathbb{Q}$, addition, subtraction, multiplication, division, and square root (raising to the $1/2$ power: see Math 310 notes, Page 104). Naturally, this leads us to ask whether we can do this for cubic polynomials with the same operations. Obviously, we have to change from $1/2$ power to the $1/3$ power, but Cardano showed that it was possible to solve a cubic and quartic equation using these traditional operations and radicals.

Évariste Galois invented his theory to prove there is no such closed formula by radicals for any polynomial of degree 5 or above.

For example, $x^5 - x + 1$ does not have roots given by radicals.

Example: A Solvable Polynomial

Consider the polynomial $f(x) = x^2 - 2$. We know that the roots of this polynomial are $\pm\sqrt{2}$. From this, we want to create a set $K(f)$ that satisfies the following rules:

- $\mathbb{Q} \subseteq K(f)$.
- $K(f)$ must contain the roots of f.
- $K(f)$ must be closed under the traditional operations: $+, -, \times, /$
- $K(f)$ must be the smallest field that satisfies the above three requirements.

Claim: $K(f) = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

- $\mathbb{Q} \subseteq K(f)$, because we can set $b = 0$.
- $\sqrt{2} = 0 + (1)(\sqrt{2})$, $-\sqrt{2} = 0 + (-1)(\sqrt{2})$
- Let $a + b\sqrt{2}$ and $c + d\sqrt{2}$ be elements of $K(f)$. Then,
  - $(a + b\sqrt{2}) \pm (c + d\sqrt{2}) = (a \pm c) + (b \pm d)\sqrt{2}$
  - $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$
  - Set $c + d\sqrt{2} \neq 0$

$$\begin{aligned}\frac{a + b\sqrt{2}}{c + d\sqrt{2}} &= \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{c^2 - 2d^2}\\ &= \frac{1}{c^2 - 2d^2}\left((ac - 2bd) + (bc - ad)\sqrt{2}\right)\\ &= \frac{ac - 2bd}{c^2 - 2d^2} + \frac{bc - ad}{c^2 - 2d^2}\sqrt{2}\end{aligned}$$

- $K(f)$ is indeed the smallest set.

  - Note that $K(f)$ is a $\mathbb{Q}$-vector space, with basis $\{1, \sqrt{2}\}$. Therefore, $\dim_{\mathbb{Q}} K(f) = 2$. $K(f)$ is known as the "splitting field" of f.

We want to consider a bijective function $\varphi : K(f) \to K(f)$ with the following properties:

- $\varphi(r) = r$ for every $r \in \mathbb{Q}$
- $\varphi(x + y) = \varphi(x) + \varphi(y)$
- $\varphi(xy) = \varphi(x)\varphi(y)$

We denote the collection of all such φ as $\text{Aut}(K(f)/\mathbb{Q})$. This is a group under the operation $\circ$ (composition). Specifically, we have

$$\begin{aligned}\varphi(a + b\sqrt{2}) &= \varphi(a) + \varphi(b)\varphi(\sqrt{2})\\ &= a + b\varphi(\sqrt{2}).\end{aligned}$$

Notice

$$\begin{aligned}\left(\varphi(\sqrt{2})\right)^2 - 2 &= \varphi\left(\left(\sqrt{2}\right)^2 - 2\right)\\ &= \varphi(0)\\ &= 0.\end{aligned}$$

Therefore, $\varphi(\sqrt{2}) = \pm\sqrt{2}$. Therefore, we have that the elements of $\text{Aut}(K(f)/\mathbb{Q})$ as the following:

$$\begin{aligned}\varphi_0 &: a + b\sqrt{2} \mapsto a + b\sqrt{2}\\ \varphi_1 &: a + b\sqrt{2} \mapsto a - b\sqrt{2}\\ \varphi_1 &\circ \varphi_1 = \varphi_0\end{aligned}$$

Thus,

$$\begin{aligned}\text{Aut}(K(f)/\mathbb{Q}) &= \{\varphi_0, \varphi_1\}\\ &\cong \mathbb{Z}/2\mathbb{Z}\end{aligned}$$

Example: A Harder Polynomial

Let $f(x) = (x^2 - 2)(x^2 - 3)$. Our roots are $\{\pm\sqrt{2}, \pm\sqrt{3}\}$. We want to form $K(f)$ with the same properties. Let

$$\begin{aligned}K(f) &= \mathbb{Q}(\sqrt{2}, \sqrt{3})\\ &= \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}.\end{aligned}$$

Just as with our previous example, $K(f)$ is a vector space over $\mathbb{Q}$, with basis $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$, so $\dim_{\mathbb{Q}} K(f) = 4$.

Now, we want $\text{Aut}(K(f)/\mathbb{Q})$. If $\varphi \in \text{Aut}(K(f)/\mathbb{Q})$, then

$$\begin{aligned}\varphi(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a + b\varphi(\sqrt{2}) + c\varphi(\sqrt{3}) + d\varphi(\sqrt{6})\\ &= a + b\varphi(\sqrt{2}) + c\varphi(\sqrt{3}) + d\varphi(\sqrt{2})\varphi(\sqrt{3}).\end{aligned}$$

Thus, we need to know $\varphi(\sqrt{2})$ and $\varphi(\sqrt{3})$. So,

$$\begin{aligned}f(\varphi(\sqrt{2})) &= \left(\left(\varphi(\sqrt{2})\right)^2 - 2\right)\left(\left(\varphi(\sqrt{2})\right)^2 - 3\right)\\ &= 0\end{aligned}$$

and the same is the case with $\varphi(\sqrt{3})$. So,

$$\begin{aligned}\varphi(\sqrt{2}) &\in \{\pm\sqrt{2}, \pm\sqrt{3}\}\\ \varphi(\sqrt{3}) &\in \{\pm\sqrt{2}, \pm\sqrt{3}\}.\end{aligned}$$

Suppose $\varphi(\sqrt{2}) = \sqrt{3}$. Then,

$$\begin{aligned}\left(\left(\varphi(\sqrt{2})\right)^2\right) &= (\sqrt{3}^2 - 1)\\ &= 0\\ &= (\varphi(2) - 3)\\ &= -1.\ \perp\end{aligned}$$

Thus,

$$\begin{aligned}\varphi(\sqrt{2}) &\in \{\pm\sqrt{2}\}\\ \varphi(\sqrt{3}) &\in \{\pm\sqrt{3}\},\end{aligned}$$

and we have the maps as:

$$\begin{aligned}\varphi_0 &: \sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto \sqrt{3}\\ \varphi_1 &: \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto \sqrt{3}\\ \varphi_2 &: \sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}\\ \varphi_3 &: \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}\end{aligned}$$

Example: A Cubic Polynomial

Consider the function $f(x) = x^3 - 2$. The function has one real root, $r_1 = \sqrt[3]{2}$, and two complex roots. Let's examine $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$; r_2 and r_3 are not in $Q(\sqrt[3]{2})$. We could instead consider $\mathbb{Q}(\sqrt[3]{2}, r_1, r_2)$.

$$\begin{aligned}x^3 - 2 &= (x - r_1)(x^2 + r_1 x + r_1^2)\\ r_2 &= \frac{-r_1 + \sqrt{r_1^2 - 4r_1^2}}{2}\\ &= r_1\frac{-1 + \sqrt{-3}}{2}\\ &= r_1\zeta_3\\ r_3 &= r_1\frac{-1 - \sqrt{-3}}{2}\\ &= r_1\zeta_3^2\end{aligned}$$

However, including r_2 and r_3 is excessive — all we need is $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. Therefore, the basis of this vector space is $\{1, r_1, r_1^2, \zeta_3, \zeta_3 r_1, \zeta_3 r_1^2\}$ (note that $\zeta_3^2 = -1 - \zeta_3$). Therefore, $\dim_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{2}, \zeta_3) = 6$, and $\mathbb{Q}(\sqrt[3]{2}, \zeta_3) = K(f)$.Additionally, we have $\text{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\varphi_0\}$, but $\dim_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{2}) = 3$. For the full field extension, we need to find $\varphi(\sqrt[3]{2})$ and $\varphi(\zeta_3)$.

$$\begin{aligned}\varphi(\sqrt[3]{2}) &\in \{r_1, \zeta_3 r_1, \zeta_3^2 r_1\}\\ \varphi(\zeta) &\in \{\zeta_3, \zeta_3^2\}\\ \varphi_0 &: r_1 \mapsto r_1, \zeta_3 \mapsto \zeta_3\\ \varphi_1 &: r_1 \mapsto \zeta_3 r_1, \zeta_3 \mapsto \zeta_3\\ \varphi_2 &: r_1 \mapsto r_1, \zeta_3 \mapsto \zeta_3^2\\ \varphi_3 &: r_1 \mapsto \zeta_3^2 r_1, \zeta_3 \mapsto \zeta_3\\ \varphi_4 &: r_1 \mapsto \zeta_3 r_1, \zeta_3 \mapsto \zeta_3^2\\ \varphi_5 &: r_1 \mapsto \zeta_3^2 r_1, \zeta_3 \mapsto \zeta_3^2\end{aligned}$$

Therefore,

$$\begin{aligned}\text{Aut}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}) &= 6\\ &= \dim_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{,}\sqrt[3]{2})\end{aligned}$$

Rings

Consider the integers under the normal operations, $(\mathbb{Z}, +, \cdot)$; this will serve as the motivation for rings in the future.

Definition of a Ring

Let R be a nonempty set with operations $(+, \cdot)$, with the following properties:

(1) $(R, +)$ is an abelian group:

- Closed: $r_1 + r_2 \in R,\ \forall r_1, r_2 \in R$
- Identity: $\exists 0_R,\ r + 0_R = 0_R + r = r$
- Associativity: $r_1 + (r_2 + r_3) = (r_1 + r_2) + r_3$
- Inverse: $\forall r \in R,\ \exists -r \in R, r + (-r) = 0_R$
- Commutativity: $r_1 + r_2 = r_2 + r_1$

(2) Closure under Multiplication: $r_1 \cdot r_2 \in R,\ \forall r_1, r_2 \in R$

(3) Associativity under Multiplication: $r_1 \cdot (r_2 \cdot r_3) = (r_1 \cdot r_2) \cdot r_3$

(4) Distributivity: $r_1 \cdot (r_2 + r_3) = r_1 \cdot r_2 + r_2 \cdot r_3, (r_1 + r_2) \cdot r_3 = r_1 \cdot r_3 + r_2 \cdot r_3$

We say $(R, +, \cdot)$ is a ring if it satisfies all these properties.

If $\exists 1_R \in R$ such that $r \cdot 1_R = 1_R \cdot r = r$, then we say R is a ring with identity, and 1_R is the multiplicative identity. If multiplication is commutative, then R is known as a commutative ring.

Examples

(1) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ are commutative rings with identity value of 1.

(2) $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ is a commutative ring with identity $1_R = [1]_n$.

(3) $(\mathbb{R}[x], +, \cdot)$, where $\mathbb{R}[x] = \left\{ \sum_{i=0}^{n} a_i x^i \mid a_i \in \mathbb{R} \right\}$, is a commutative ring with identity.

(4) $(2\mathbb{Z}, +, \cdot)$ is a commutative ring *without* identity.

(5) $(\text{Mat}_n(\mathbb{R}), +, \cdot)$, where $\text{Mat}_n(\mathbb{R})$ refers to $n \times n$ matrices with real entries, is a *non*commutative ring with identity.

Division Rings and Fields

Let R be a ring with identity. We say R is a *division ring* if $\forall r \in R \setminus \{0_R\}$, $\exists r^{-1} \in R$ with $r \cdot r^{-1} = 1_R = r^{-1} \cdot r$. If R is also commutative, then R is a *field*.

Examples

(1) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, and $(\mathbb{C}, +, \cdot)$ are all fields.

(2) Let p be prime, and set $F = \mathbb{Z}/p\mathbb{Z}$. Then, F is a field; we denote this $\mathbb{F}_p$.

(3) Define

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = -1, ij = k = -ji, jk = i = -kj, ki = j = -ik\}.$$

Then, $\mathbb{H}$ is a division ring, known as the Hamiltonian quaternions. Note that $\mathbb{C} \subset \mathbb{H}$.

Properties of Rings

Proposition 4.1: Let R be a ring.

(1) $0_R a = a 0_r = 0\ \forall a \in R$
(2) $(-a)b = a(-b) = -(ab)\ \forall a, b \in R$
(3) $(-a)(-b) = ab\ \forall a, b \in R$
(4) If $\exists 1_R \in R$, then 1_R is unique, and $-a = (-1_R)a$.

Proof of (1): Let $a \in R$. Then,

$$\begin{aligned} 0_R a &= (0_R + 0_R)a && \text{Additive Inverse} \\ 0_R a &= 0_R a + 0_R a && \text{Distributivity} \\ 0_R a + (-0_R a) &= 0_R a + 0_R a(-0_R a) \\ 0_R &= 0_R a. && \text{Additive Inverse} \end{aligned}$$

Proof of (2): Let $a, b \in R$. Note that $-(ab)$ is the unique inverse such that $ab + (-(ab)) = 0_R$ via group theory. We have

$$\begin{aligned} ab + (-a)b &= (a + (-a))b && \text{Distributivity} \\ &= (0_R)b && \text{Additive Inverse} \\ &= 0_R. && \text{By Property (1)} \end{aligned}$$

Thus, $(-a)b = -(ab)$.

Zero Divisor and Units in Rings

Let $a \in R$, $a \neq 0_R$. If $\exists b \in R$ with $b \neq 0_R$ such that $ab = 0_R = ba$, then we say a is a zero divisor.

If $1_R \in R$, we say $u \in R$ is a unit if $\exists v \in R$ (can be equal to u) with $uv = 1_R = vu$. The collection of units in R is denoted $R^\times$.

Exercise: Show that $R^\times$ is a group under multiplication.

Examples

(1) Let $R = \mathbb{Z}/6\mathbb{Z}$. Note that $[2]_6[3]_6 = [6]_6 = [0]_6$, so both $[2]_6$ and $[3]_6$ are both zero divisors. Additionally, $[4]_6[3]_6 = [6]_6 = [0]_6$. Meanwhile, since $(\mathbb{Z}/6\mathbb{Z})^\times = \{[1]_6, [5]_6\}$, those are the two units of $\mathbb{Z}/6\mathbb{Z}$.

(2) $\mathbb{Z}$ has no zero divisors. $\mathbb{Z}^\times = \{\pm 1\}$.

(3) $\mathbb{Q}$ has no zero divisors. $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$.

(4) $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}, i^2 = -1\}$ has no zero divisors (as $\mathbb{C}$ is a field). $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

Subrings

Let $(R, +, \times)$. If $S \subseteq R$ is a nonempty subset, and $(S, +, \cdot)$ is a ring, then S is a subring of R. To see S is a subring, it is enough to show:

- $S \neq \emptyset$.
- S is closed under subtraction.
- S is closed under multiplication of elements in S.

Examples

(1)

$$\underbrace{\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}}_{\text{subrings}}$$

(2) $\mathbb{R} \subseteq \mathbb{R}[x]$ is a subring.

(3) $S = \{[0]_4, [2]_4\} \subseteq \mathbb{Z}/4\mathbb{Z}$ is a subring.

Integral Domains

Let R be a commutative ring with identity. We say R is an integral domain if R has no zero divisors.

Examples

(1) $\mathbb{Z}$, the integers, is an integral domain, that is not a field.

(2) All fields are integral domains.

(3) $\mathbb{Z}/6\mathbb{Z}$ is *not* an integral domain, as it has zero divisors.

(4) $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain if n is composite.

Integral domains are nice due to allowance of cancellations. For example, if $2m = 2n$ in $\mathbb{Z}$, then we find $2(m-n) = 0$, and since $\mathbb{Z}$ has no zero divisors, it must be the case that $m = n$.

However, in a ring that is not an integral domain, such as $\mathbb{Z}/6\mathbb{Z}$, we cannot use the same technique to find the solution to a similar equation. For example, $3 \cdot 2 = 0 = 3 \cdot 4$, but $2 \neq 4$.

Proposition: Equations in Integral Domains

Let R be an integral domain. If $a, b, c \in R$ with $a \neq 0_R$, and $ab = ac$, then $b = c$.

Proof:

$$\begin{aligned} ab &= ac \\ a(b-c) &= 0_R \end{aligned}$$

Since $a \neq 0$,

$$\begin{aligned} b - c &= 0_R \\ b &= c. \end{aligned}$$

Theorem: Finite Integral Domains and Fields

If R is an integral domain, and $\text{card}(R) < \infty$,then R is a field.

Proof: Let $a \in R$, $a \neq 0_R$. Note $ab \neq 0_R$ for all $b \in R$, $b \neq 0_R$.

Define $\varphi_a : R \setminus \{0_R\} \to R \setminus \{0_R\}$, $b \mapsto ab$. If $\varphi_a(b) = \varphi_a(c)$, then $ab = ac$, and by our previous result, $b = c$ — therefore, φ_a is injective.

Since $R \setminus \{0_R\}$ is finite, and φ_a is injective, then φ_a is surjective. In particular, this means $\exists b \in R \setminus \{0_R\}$ with $\varphi_a(b) = 1_R$; therefore, $ab = 1_R$. Since R is commutative, $ba = 1_R$, so $b = a^{-1}$.

Examples of Abstract Rings

Ring of Integers in a Field

Let $d \in \mathbb{Z}$, d is square-free (there is no square that divides d). Set $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$. This is a field (can be verified as a subfield of $\mathbb{C}$).

We can define

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} & d \equiv 2, 3 \mod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{a + b\left(\frac{1+\sqrt{d}}{2}\right) \mid a, b \in \mathbb{Z}\right\} & d \equiv 1 \mod 4 \end{cases}.$$

Then, $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a subring of $\mathbb{Q}(\sqrt{d})$. This is known as the ring of integers of $\mathbb{Q}(\sqrt{d})$. This set behaves in $\mathbb{Q}(\sqrt{d})$ the same say that $\mathbb{Z}$ does inside $\mathbb{Q}$. The set $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is the collection of all roots in $\mathbb{Q}(\sqrt{d})$ of monic (coefficient of highest degree is 1) polynomials with coefficients in $\mathbb{Z}$.

For example, if $d = -1$, defining $\mathbb{Q}(i)$, then we can verify that $\mathbb{Z}[i]$ is a root of a monic polynomial with coefficients in $\mathbb{Z}$.

Ring of Matrices

Let R be a ring. Then,

$$\text{Mat}_n(R) = \{n \times n \text{ matrices with entries in } R\}$$

is a ring under matrix addition and multiplication.

Ring of Functions

Let $L^1(\mathbb{R})$ be all functions $f : \mathbb{R} \to \mathbb{R}$ such that

$$\int_{\mathbb{R}} |f(x)| dx$$

exists. The set $L^1(\mathbb{R})$ is a ring under pointwise addition and convolution, where convolution is defined as

$$(f * g)(x) = \int_{\mathbb{R}} f(x - y) g(y) dy.$$

This is a commutative ring without identity.

Group Ring

Let K be a field and G a group. Set $K[G]$ to be all formal linear combinations of the form

$$\alpha = \sum_{x \in G} a_x x,$$

with $a_x \in K$, $x \in G$, with $a_x = 0$ for all but finitely many x.

Given

$$\alpha = \sum_{x \in G} a_x x$$
$$\alpha = \sum_{y \in G} b_y y,$$

define

$$\begin{aligned} \alpha + \beta &= \sum_{x \in G} (a_x + b_x) x \\ \alpha\beta &= \sum_{x \in G} \sum_{y \in G} a_x b_y xy \\ &= \sum_{z \in G} \left(\sum_{xy = z} a_x b_y \right) z. \end{aligned}$$

This is a ring under these operations, known as the group ring. It is commutative if and only if G is abelian.

Polynomials under a Ring

Let R be a ring. Set

$$R[x] = \left\{\sum_{i=1}^{n} a_i x^i \mid a_i \in R, n \in \mathbb{Z}_{\geq 0}\right\}$$

to be the all polynomials with coefficients in R. This is a ring under polynomial addition and multiplication. If R is commutative, then $R[x]$ is commutative.

Proposition: Polynomial Properties

Let R be an integral domain, with $p(x), q(x) \in R[x] \setminus \{0\}$. Then:

(1) $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$

(2) $R[x]^\times = R^\times$

(3) $R[x]$ is an integral domain.

Proof of (1): Let

$$\begin{aligned} p(x) &= a_m x^m + \cdots + a_1 x + a_0 \\ q(x) &= b_n x^n + \cdots + b_1 x + b_0 \end{aligned}$$

with $a_m, b_n \neq 0$ — $\deg(p) = m$ and $\deg(q) = n$. Then,

$$p(x)q(x) = a_m b_n x^{m+n} + \text{lower degree terms},$$

and since $a_m b_n \neq 0$ as R is an integral domain with $a_m, b_n \neq 0$, $\deg(pq) = m + n$.

Ring Homomorphism

Let R and S be rings. A ring homomorphism between R and S is a map $\varphi : R \to S$ that satisfies the following properties for all $r_1, r_2 \in R$:

(1) $\varphi(r_1 +_R r_2) = \varphi(r_1) +_S \varphi(r_2)$

(2) $\varphi(r_1 \cdot_R r_2) = \varphi(r_1) \cdot_S \varphi(r_2)$

The kernel of a ring homomorphism φ is given by

$$\ker(\varphi) : \{r \in R \mid \varphi(r) = 0_S\}$$

A bijective ring homomorphism is called an isomorphism. If there exists such a bijection between R and S, we say R and S are isomorphic.

If φ is an isomorphism, we write

$$\varphi : R \xrightarrow{\simeq} S$$

Examples: Ring Homomorphisms

Not a Ring Homomorphism

Let $R = \mathbb{Z}$ and $S = 2\mathbb{Z}$. Define

$$\begin{aligned} \varphi : \mathbb{Z} &\to 2\mathbb{Z} \\ n &\mapsto 2n. \end{aligned}$$

Let $m, n \in \mathbb{Z}$. We have

$$\begin{aligned} \varphi(m+n) &= 2(m+n) \\ &= 2m + 2n \\ &= \varphi(m) + \varphi(n). \end{aligned}$$

However,

$$\begin{aligned}\varphi(mn) &= 2(mn)\\ \varphi(m)\varphi(n) &= 4(mn).\end{aligned}$$

Homomorphism between Integers and Integers Modulo n

Consider $R = \mathbb{Z}$ and $S = \mathbb{Z}/n\mathbb{Z}$. Define

$$\begin{aligned}\varphi : \mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z}\\ a &\mapsto [a]_n.\end{aligned}$$

Let $a, b \in \mathbb{Z}$. We have

$$\begin{aligned}\varphi(a+b) &= [a+b]_n\\ &= [a]_n + [b]_n\\ &= \varphi(a) + \varphi(b).\end{aligned}$$

Additionally, we have

$$\begin{aligned}\varphi(ab) &= [ab]_n\\ &= [a]_n[b]_n\\ &= \varphi(a)\varphi(b).\end{aligned}$$

So, φ is a ring homomorphism. Note that

$$\begin{aligned}\ker(\varphi) &= \{a \in \mathbb{Z} \mid \varphi(a) = [0]_n\}\\ &= \{a \in \mathbb{Z} \mid [a]_n = [0]_n\}\\ &= \{a \in \mathbb{Z} \mid n|a\}\\ &= n\mathbb{Z}.\end{aligned}$$

Homomorphism Between the Polynomials and Reals

Let $S = \mathbb{R}[x]$ and $T = \mathbb{R}$. Define

$$\begin{aligned}\varphi_a : \mathbb{R}[x] &\to \mathbb{R}\\ f &\mapsto f(a)\end{aligned}$$

Let $f(x), g(x) = \mathbb{R}[x]$. Then,

$$\begin{aligned}\varphi_a(f(x) + \varphi(g)(x)) &= \varphi_a((a_0+b_0) + \cdots + (a_m+b_m)x^m + b_{m+1}x^{m+1} + \cdots b_n x^n)\\ &= (a_0+b_0) + \cdots + (a_m+b_m)a^m + b_{m+1}a^{m+1} + \cdots + b_n a^n\\ &= \varphi_a(f(x)) + \varphi_a(g(x)).\end{aligned}$$

Similarly, we can verify that $\varphi_a(f(x)g(x)) = \varphi_a(f(x))\varphi_a(g(x))$. So, φ_a is a ring homomorphism. Note that

$$\begin{aligned}\ker(\varphi_a) &= \{f(x) \in \mathbb{R}[x] \mid f(a) = 0\}\\ &= \{f(x) \in \mathbb{R}[x] \mid (x-a)|f(x)\}\\ &= (x-a)\mathbb{R}[x]\end{aligned}$$

Homomorphism between Matrices

Define

$$\begin{aligned} R &= \left\{\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in \mathrm{Mat}_2(\mathbb{R})\right\} \\ S &= \mathbb{R}, \end{aligned}$$

and

$$\begin{aligned} \varphi &: R \to S \\ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} &\mapsto a. \end{aligned}$$

Then,

$$\begin{aligned} \varphi\left(\begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix}\right) &= \varphi\left(\begin{bmatrix} a_1 + a_2 & b_1 + b_2 \\ 0 & d_1 + d_2 \end{bmatrix}\right) \\ &= a_1 + a_2 \\ &= \varphi\left(\begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix}\right) + \varphi\left(\begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix}\right), \end{aligned}$$

and

$$\begin{aligned} \varphi\left(\begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix}\begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix}\right) &= \varphi\left(\begin{bmatrix} a_1a_2 & a_1b_2 + b_1d_2 \\ 0 & d_1d_2 \end{bmatrix}\right) \\ &= a_1a_2 \\ &= \varphi\left(\begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix}\right)\varphi\left(\begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix}\right). \end{aligned}$$

So φ is a ring homomorphism that is surjective but not injective. Note

$$\ker(\varphi) = \left\{\begin{bmatrix} 0 & b \\ 0 & d \end{bmatrix} \mid b, d \in \mathbb{R}\right\}.$$

Proposition: Fundamental Theorem of Ring Homomorphisms

Let $\varphi : R \to S$ be a ring homomorphism.

(1) The image of φ, $\varphi(R) = \{s \in S \mid s = \varphi(r) \text{ for some } r \in R\}$, is a subring of S.

(2) The kernel, $\ker(\varphi)$, is a subring of R.

Additionally, for any $r \in R$, and $a \in \ker(\varphi)$, $ar \in \ker(\varphi)$ and $ra \in \ker(\varphi)$.

Proof of (2): To show $\ker(\varphi)$ is a subring, we must show that $\ker(\varphi)$ is non-empty, closed under subtraction, and closed under multiplication.

First, since $\varphi(0_R) = 0_S$ (verify this), $\ker(\varphi)$ is non-empty.

Let $a, b \in \ker(\varphi)$. We have

$$\begin{aligned} \varphi(a - b) &= \varphi(a + (-b)) \\ &= \varphi(a) + \varphi(-b) \\ &= \varphi(a) - \varphi(b) && \text{check } \varphi(-b) = -\varphi(b) \\ &= 0_S - 0_S \\ &= 0_S. \end{aligned}$$

Thus, $a - b \in \ker(\varphi)$, and $\ker(\varphi)$ is closed under subtraction.

To show $\ker(\varphi)$ is closed under multiplication, we will prove the general case. Let $a \in \ker(\varphi)$ and $r \in R$. We have

$$\begin{aligned}\varphi(ra) &= \varphi(r)\varphi(a)\\ &= \varphi(r)0_S\\ &= 0_S.\end{aligned}$$

Similarly, $\varphi(ar) = 0_S$. So, $ar, ra \in \ker(\varphi)$.

The stronger condition that we found for $\ker(\varphi)$ (closed under multiplication of all elements of the ring, not merely those from the subring) forms what we call an ideal.

Quotient Rings

Defining an Equivalence Relation on a Ring

Set $K = \ker(\varphi)$. We will define a relation on R, $\sim$, where $r_1 \sim r_2$ if $r_1 - r_2 \in K$. We want to see if $\sim$ is an equivalence relation:

- Reflexive: $r \sim r$ since $r - r = 0_R \in K$.
- Symmetric: $r_1 \sim r_2$ implies $r_1 - r_2 = k$ for some $k \in K$. Since k is a subring, $-k \in K$, so $r_2 - r_1 \in K$.
- Transitive: suppose $r_1 \sim r_2$ and $r_2 \sim r_3$. This means there are elements $k_1, k_2 \in K$ with $r_1 - r_2 = k_1$ and $r_2 - r_3 = k_2$. Since K is a subring, $(r_1 - r_2) + (r_2 - r_3) = r_1 - r_3 = k_1 + k_2 \in K$. Thus, $r_1 \sim r_3$.

Since $\sim$ is reflexive, symmetric, and transitive, $\sim$ is an equivalence relation on R.

Since $\sim$ is an equivalence relation on R, we will want to examine equivalence classes of R under $\sim$. Specifically, for $r \in R$, we have

$$\begin{aligned}[r]_K &= \{\tilde{r} \in R \mid r - \tilde{r} \in K\}\\ &= \{\tilde{r} \in R \mid r - \tilde{r} = k \text{ for some } k \in K\}\\ &= \{r + k \mid k \in K\}\\ &= r + K.\end{aligned}$$

We will define the set

$$R/K = \{r + K \mid r \in R\}$$

to be the set of all equivalence classes.

Example: Let $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $a \mapsto [a]_n$. Then, $\ker(\varphi) = n\mathbb{Z}$. Then, $R/K = \mathbb{Z}/n\mathbb{Z}$.

Let $r_1 + K, r_2 + K \in R/K$. The new question is whether or not we can define addition and multiplication on R/K. Suppose that the following are the definition of multiplication and addition on R/K.

$$\begin{gathered}(r_1 + K) + (r_2 + K) = (r_1 + r_2) + K\\ (r_1 + K)(r_2 + K) = (r_1 r_2) + K.\end{gathered}$$

Suppose $r_1 + K = \tilde{r}_1 + K$ and $r_2 + K = \tilde{r}_2 + K$. This means there are $k_1, k_2 \in K$ with $r_1 - \tilde{r}_1 = k_1$, $r_2 - \tilde{r}_2 = k_2$, or that $r_1 = \tilde{r}_1 + k_1$, $r_2 = \tilde{r}_2 + k_2$.

To see if the map is well-defined, we have

$$\begin{aligned}(r_1 + K) + (r_2 + K) &= (r_1 + r_2) + K\\ &= (\tilde{r}_1 + k_1 + \tilde{r}_2 + k_2) + K\\ &= (\tilde{r}_1 + k_1) + K + (\tilde{r}_2 + k_2) + K\\ &= (\tilde{r}_1 + K) + (\tilde{r}_2 + K)\end{aligned}$$

since $\tilde{r}_1 + k_1 - \tilde{r}_1 = k \in K$.

Thus, our addition is well-defined.

Examining multiplication, we see that

$$\begin{aligned}(r_1+K)(r_2+K) &= r_1r_2+K\\ &= (\tilde{r}_1+k_1)(\tilde{r}_2+k_2)+K\\ &= \tilde{r}_1\tilde{r}_2+\underbrace{k_1\tilde{r}_2+\tilde{r}_1k_2+k_1k_2}_{\in K \text{ since } K=\ker(\varphi)}+K\\ &= \tilde{r}_1\tilde{r}_2+K.\end{aligned}$$

Therefore, our multiplication is well-defined.

We can show that R/K is a ring (verify for yourself).

Note: This construction would not have worked if K was merely a subring, as multiplication would not be well-defined.

Ideals

Let $I \subseteq R$ be a subring.

(1) If $ra \in I$ for every $r \in R$, we say I is a left-ideal of R.

(2) If $ar \in I$ for every $r \in R$, then we say I is a right-ideal of R.

(3) If I is a left-ideal and a right-ideal of R, then we say I is an ideal of R.

If $I \subseteq R$ is an ideal, we define $r_1 \sim_I r_2$ if $r_1 - r_2 \in I$, and $R/I = \{r + I \mid r \in I\}$. Addition and multiplication in R/I are defined as

$$\begin{aligned}(r_1+I)+(r_2+I) &= (r_1+r_2)+I\\ (r_1+I)(r_2+I) &= r_1r_2+I.\end{aligned}$$

Examples of Ideals

(1) $n\mathbb{Z} \subseteq \mathbb{Z}$ is an ideal; if $nk \in n\mathbb{Z}$, and $m \in \mathbb{Z}$, then $m(nk) = n(mk) \in n\mathbb{Z}$.

(2) Let $R = \mathbb{Z}[x]$. Set $\langle x^2\rangle = \{f(x)x^2 \mid f(x) \in \mathbb{Z}[x]\}$. This is an ideal.

(3) Let R be a ring. If $r \in R$, we define $\langle r\rangle = \{ar \mid a \in R\}$.

(4) Set $I = \{(2n, 0) \mid n \in \mathbb{Z}\}$ in $\mathbb{Z}\times\mathbb{Z}$. Let $(a, b) \in \mathbb{Z}\times\mathbb{Z}$. Then, $(a, b)(2n, 0) = (2an, 0) \in I$, meaning I is an ideal.

(5) Define $R = \left\{\begin{bmatrix} a & b\\ 0 & d\end{bmatrix} \in \operatorname{Mat}_2(\mathbb{R})\right\}$. Consider $I = \left\{\begin{bmatrix} a & 0\\ 0 & d\end{bmatrix} \mid a, b \in \mathbb{R}\right\}$. Then,

$$\begin{aligned}\begin{bmatrix} a & b\\ 0 & d\end{bmatrix}\begin{bmatrix} s & 0\\ 0 & t\end{bmatrix} &= \begin{bmatrix} as & bt\\ 0 & dt\end{bmatrix}\\ \begin{bmatrix} s & 0\\ 0 & t\end{bmatrix}\begin{bmatrix} a & b\\ 0 & d\end{bmatrix} &= \begin{bmatrix} sa & sb\\ 0 & td\end{bmatrix}.\end{aligned}$$

Therefore, I is a subring but not an ideal.

(6) Let $R = \mathbb{Z}[x]$. Consider $I = \langle 2, x\rangle = \{2f(x) + g(x) \mid f(x), g(x) \in \mathbb{Z}[x]\}$. Then,

$$\begin{aligned}(2f_1(x)+xg(x))(2f_2(x)+xg_2(x)) &= 2\left(f_1(x)(2f_2(x)+xg_2(x))\right)+x(g_1(x)(2f_2(x)+xg_2(x)))\\ h(x)\left(2f(x)+xg(x)\right) &= 2(f(x)h(x))+x(g(x)h(x)),\end{aligned}$$

meaning I is an ideal.

Examples of Quotient Rings

(1) Let $R = \mathbb{Z}$, $I = n\mathbb{Z}$. Then, $R/I = \mathbb{Z}/n\mathbb{Z}$.

(2) Let $R = \mathbb{R}[x]$, $I = \langle x^2 \rangle$ as defined earlier. Then,

$$\begin{aligned} R/I &= \mathbb{R}[x]/\langle x^2 \rangle \\ &= f(x) + \langle x^2 \rangle. \end{aligned}$$

Other examples include

$$\begin{aligned} f(x) &= a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{R}[x] \\ f(x) + \langle x^2 \rangle &= a_1 x + a_0 + \langle x^2 \rangle \in \mathbb{R}[x]/\langle x^2 \rangle \\ \mathbb{R}[x]/\langle x^2 \rangle &= \{a + bx + \langle x^2 \rangle \mid a, b \in \mathbb{R}\}. \\ (a + bx + \langle x^2 \rangle)(c + dx\langle x^2 \rangle) &= ac + adx + bcx + bdx^2 + \langle x^2 \rangle \\ &= (ac) + (ad + bc)x + \langle x^2 \rangle \\ (x + \langle x^2 \rangle)^2 &= x^2 + \langle x^2 \rangle \\ &= \langle x^2 \rangle. \end{aligned}$$

(3) Let $R = \mathbb{Z} \times \mathbb{Z}$, $I = \{(2n, 0) \mid n \in \mathbb{Z}\}$. Then,

$$\begin{aligned} R/I &= \{(a, b) + I \mid a, b \in \mathbb{Z}\}. \\ (a, b) + I &= ([a]_2, b) + I && \text{where } [a]_2 \text{ is } a \text{ modulo } 2. \end{aligned}$$

We would expect that $\varphi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} \to R/I$, $([a]_2, b) \to (a, b) + I$ is an isomorphism (verify for yourself).

Isomorphisms to Quotient Rings

Let $R = \mathbb{Z}[x]$, $I = \langle 2, x \rangle$, $J = \langle 2 \rangle = \{2f(x) \mid f(x) \in \mathbb{Z}[x]\}$.

$$\begin{aligned} R/J &= \{f(x) + \langle 2 \rangle \mid f(x) \in \mathbb{Z}[x]\} \\ f(x) + \langle 2 \rangle &= g(x) + \langle 2 \rangle \end{aligned}$$

if $2|(f(x) - g(x))$, meaning all coefficients of $f(x) - g(x)$ are divisible by 2. Therefore,

$$\begin{aligned} f(x) + \langle 2 \rangle &= 5 + 4x + 7x^2 - 5x^3\langle 2 \rangle \\ &= (1 + (2)(2)) + 2(2x) + x^2 + 2(3x^2) - x^3 - 2(2x^3) + \langle 2 \rangle \\ &= 1 + x^2 - x^3 + \langle 2 \rangle \\ &= 1 + x^2 - 2(x^3) + x^3 + \langle 2 \rangle \\ &= 1 + x^2 + x^3 + \langle 2 \rangle. \\ (1 + x + x^2 + \langle 2 \rangle) + (x + \langle 2 \rangle) &= 1 + 2x + x^2 + \langle 2 \rangle \\ &= 1 + x^2 + \langle 2 \rangle. \end{aligned}$$

Therefore, we can consider

$$\begin{aligned} \mathbb{Z}[x]/\langle 2 \rangle &= \mathbb{Z}[x]/2\mathbb{Z}[x] \\ &\cong \mathbb{Z}/2\mathbb{Z}. \end{aligned}$$

$$\begin{aligned} R/I &= \mathbb{Z}[x]/\langle 2, x \rangle \\ f(x) + \langle 2, x \rangle &= a_n x^n + \cdots + a_1 x + a_0 + \langle 2, x \rangle \\ &= a_0 + \langle 2, x \rangle \\ &= \begin{cases} 0 & 2|a_0 \\ 1 & 2 \nmid a_0 \end{cases}, \end{aligned}$$

So, we can consider

$$\mathbb{Z}[x]/\langle 2, x \rangle \cong \mathbb{Z}/2\mathbb{Z}.$$

Isomorphism Example: Complex Numbers to Matrices

Consider the set

$$R = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in \mathrm{Mat}_2(\mathbb{R}) \right\}.$$

We can verify that R is a ring.

Define

$$\begin{aligned} \varphi : \mathbb{C} &\to R \\ a + bi &\mapsto \begin{bmatrix} a & b \\ -b & a \end{bmatrix}. \end{aligned}$$

We can verify that φ is a bijective map.

Let $a + bi, c + di \in \mathbb{C}$. Then,

$$\begin{aligned} \varphi((a+bi)+(c+di)) &= \varphi((a+c)+(b+d)i) \\ &= \begin{bmatrix} a+c & b+d \\ -(b+d) & a+c \end{bmatrix} \\ &= \begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \\ &= \varphi(a+bi) + \varphi(c+di), \end{aligned}$$

and

$$\begin{aligned} \varphi((a+bi)(c+di)) &= \varphi((ac-bd)+(ad+bc)i) \\ &= \begin{bmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{bmatrix} \\ \varphi(a+bi)\varphi(c+di) &= \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \\ &= \begin{bmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{bmatrix}. \end{aligned}$$

Therefore, $\mathbb{C} \cong R$.

First Isomorphism Theorem

Let $\varphi : R \to S$ be a homomorphism. We have $R/\ker\varphi \cong \varphi(R)$.

Proof of the First Isomorphism Theorem

We want to show that $R/\ker(\varphi) \cong \varphi(R)$. Without loss of generality, assume φ is surjective. Let $K = \ker(\varphi)$.

We define $\Phi : R/K \to S$, $r + K \mapsto \varphi(r)$. We must show that Φ is a well-defined map. Let $r_1 + K = r_2 + K$ (meaning $r_1 - r_2 \in K$). This means $r_1 = r_2 + k$ for some $k \in K$. Applying Φ, we have

$$\begin{aligned} \Phi(r_1 + K) &= \varphi(r_1) \\ &= \varphi(r_2 + k) \\ &= \varphi(r_2) + \varphi(k) \\ &= \varphi(r_2) \\ &= \Phi(r_2 + K). \end{aligned}$$

Let $r_1 + K,\ r_2 + K \in R/K$. Observe

$$\begin{aligned}\Phi((r_1 + K) + (r_2 + K)) &= \Phi((r_1 + r_2) + K)\\ &= \varphi(r_1 + r_2)\\ &= \varphi(r_1) + \varphi(r_2)\\ &= \Phi(r_1 + K) + \Phi(r_2 + K),\end{aligned}$$

and

$$\begin{aligned}\Phi((r_1 + K)(r_2 + K)) &= \Phi(r_1 r_2 + K)\\ &= \varphi(r_1 r_2)\\ &= \varphi(r_1)\varphi(r_2)\\ &= \Phi(r_1 + K)\Phi(r_2 + K),\end{aligned}$$

meaning Φ is a homomorphism.

Let $s \in S$. Since φ is surjective, there exists $r \in R$ with $\varphi(r) = s$. So, $\Phi(r + K) = \varphi(r) = s$. Thus, Φ is surjective.

Let $r + K \in \ker(\Phi)$. Then,

$$\begin{aligned}\Phi(r + k) &= 0_S\\ &= \varphi(r),\end{aligned}$$

meaning $r \in \ker(\varphi) = K$. So, $r + K = 0_R + K = 0_{R/K}$. Thus, Φ is injective.

Using the First Isomorphism Theorem: Example 1

Let $\varphi : \mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}$, $a_0 + a_1x + \cdots + a_nx^n \mapsto [a_0]_2$.

To apply the first isomorphism theorem, we must check that this is a ring homomorphism. Let

$$\begin{aligned}f &= a_0 + a_1x + \cdots + a_mx^m\\ g &= b_0 + b_1x + \cdots + b_mx^m\end{aligned}$$

be elements in $\mathbb{Z}[x]$. Note that

$$\begin{aligned}\varphi(f + g) &= \varphi((a_0 + b_0) + \cdots)\\ &= [a_0 + b_0]_2\\ &= [a_0]_2 + [b_0]_2\\ &= \varphi(f) + \varphi(g)\end{aligned}$$

and

$$\begin{aligned}\varphi(fg) &= \varphi((a_0b_0) + \cdots)\\ &= [a_0b_0]_2\\ &= [a_0]_2 + [b_0]_2\\ &= \varphi(f)\varphi(g).\end{aligned}$$

So φ is a homomorphism. Note that $\varphi(0) = [0]_2$ and $\varphi(1) = [1]_2$. The first isomorphism theorem gives that $\mathbb{Z}[x]/\ker\varphi \cong \mathbb{Z}/2\mathbb{Z}$.

We claim that $\ker\varphi = \langle 2, x\rangle$.

If $2f(x) + xg(x) \in \langle 2, x\rangle$, and we write $f(x) = a_0 + a_1x + \cdots + a_nx^n$, then

$$\begin{aligned}\varphi(2f(x) + g(x)) &= \varphi(2)\varphi(f(x)) + \varphi(x)\varphi(g(x))\\ &= [0]_2[a_0]_2 + [0]_2\varphi(g(x))\\ &= [0]_2,\end{aligned}$$

so $\langle 2, x\rangle \subseteq \ker\varphi$.

Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \ker(\varphi)$, meaning

$$\begin{aligned}[0]_2 &= \varphi(f(x))\\ &= [a_0]_2.\end{aligned}$$

Therefore, $a_0 = 2k$. So,

$$\begin{aligned}f(x) &= 2kx(a_1 + a_2x + \cdots + a_nx^{n-1})\\ &\in \langle 2, x\rangle.\end{aligned}$$

Thus, $\ker(\varphi) \subseteq \langle 2, x\rangle$, meaning $\ker(\varphi) = \langle 2, x\rangle$.

By the first isomorphism theorem, $\mathbb{Z}[x]/\langle 2, x\rangle \cong \mathbb{Z}/2\mathbb{Z}$.

Using the First Isomorphism Theorem: Example 2

We want to find the ring that is isomorphic to $(\mathbb{Z}\times\mathbb{Z})/(2\mathbb{Z}\times 5\mathbb{Z})$. We define

$$\begin{aligned}\varphi : \mathbb{Z}\times\mathbb{Z} &\to \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}\\ (m,n) &\mapsto ([m]_2, [n]_5).\end{aligned}$$

We will start by showing homomorphism as follows:

$$\begin{aligned}\varphi((m_1,n_1)+(m_2,n_2)) &= \varphi((m_1+m_2, n_1+n_2))\\ &= ([m_1+m_2]_2, [n_1+n_2]_5)\\ &= ([m_1]_2+[m_2]_2, [n_1]_5+[n_2]_5)\\ &= ([m_1]_2, [n_1]_5) + ([m_2]_2, [n_2]_5)\\ &= \varphi((m_1,n_1)) + \varphi((m_2,n_2)),\end{aligned}$$

and similarly for multiplication

$$\begin{aligned}\varphi((m_1,n_1)(m_2,n_2)) &= \varphi((m_1m_2, n_1n_2))\\ &= ([m_1m_2]_2, [n_1n_2]_5)\\ &\vdots\\ &= \varphi((m_1,n_1))\varphi((m_2,n_2))\end{aligned}$$

Let $([a]_2, [b]_5) \in \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$. Then, $\varphi((a,b)) = ([a]_2, [b]_5)$. Thus, φ is surjective.

Finally, we have $(m,n) \in \ker(\varphi)$ if and only if $[m]_2 = [0]_2$ and $[n]_5 = [0]_5$, meaning $m \in 2\mathbb{Z}$ and $n \in 5\mathbb{Z}$. Therefore, $\ker(\varphi) = 2\mathbb{Z}\times 5\mathbb{Z}$.

Using the First Isomorphism Theorem: Example 3

Consider the map $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$, $n \mapsto ([n]_2, [n]_5)$. Note

$$\begin{aligned}\varphi(m+n) &= ([m+n]_2, [m+n]_5)\\ &= ([m]_2+[n]_2, [m]_5+[n]_5)\\ &= ([m]_2, [m]_5) + ([n]_2, [n]_5)\\ &= \varphi(m)+\varphi(n),\end{aligned}$$

and

$$\varphi(mn) = \varphi(m)\varphi(n).$$

We want to find if this map is surjective. Let $([a]_2, [b]_5) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. We are trying to find $n \in \mathbb{Z}$ such that $[n]_2 = [a]_2$ and $[n]_5 = [b]_5$, or $n \equiv a$ modulo 2 and $n \equiv b$ modulo 5.

$$\begin{aligned}
n - a &\equiv 2k \text{ for some } k \in \mathbb{Z} \\
n &\equiv a + 2k \\
a + 2k &\equiv b \text{ modulo } 5 \\
2k &= b - a \text{ modulo } 5 \\
k &= 3(b - a) \text{ modulo } 5 \\
n &= a + 2(3(b - a)) \\
&= a + 6(b - a).
\end{aligned}$$

So $\varphi(a + 6(b - a)) = ([a]_2, [b]_5)$. Thus, φ is surjective.

Finally, we desire $\ker(\varphi)$. Observe that

$$\begin{aligned}
\ker(\varphi) &= \{n \in \mathbb{Z} \mid [n]_2 = [0]_2, [n]_5 = [0]_5\} \\
&= \{n \in \mathbb{Z} \mid 2|n, 5|n\} \\
&= \{n \in \mathbb{Z} \mid 10|n\} \\
&= 10\mathbb{Z}.
\end{aligned}$$

Thus, the first isomorphism theorem gives $\mathbb{Z}/10\mathbb{Z} \equiv \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Proposition: Ring Homomorphisms and Ideals

Let R be a ring and $I \subseteq R$ be an ideal. The map

$$\begin{aligned}
\varphi &: R \to R/I \\
r &\mapsto r + I
\end{aligned}$$

is a surjective ring homomorphism with $\ker(\varphi) = I$. The proof is left as an exercise to the reader.

Using the First Isomorphism Theorem: Example 3

Let A be a ring and X be any non-empty set. Let R be the set of functions from X to A.

We have R is a ring.

$$\begin{aligned}
(f + g)(x) &= f(x) +_A g(x) \\
(fg)(x) &= f(x) \cdot_A g(x).
\end{aligned}$$

Fix $x_0 \in X$. We define $E_{x_0} : R \to A$ by

$$E_{x_0}(f) = f(x_0).$$

We have

$$\begin{aligned}
E_{x_0}(f + g) &= (f + g)(x_0) \\
&= f(x_0) + g(x_0) \\
&= E_{x_0}(f) + E_{x_0}(g)
\end{aligned}$$

and

$$\begin{aligned}
E(x_0)(fg) &= (fg)(x_0) \\
&= f(x_0)g(x_0) \\
&= E_{x_0}(f)E_{x_0}(g).
\end{aligned}$$

Therefore, E_{x_0} is a homomorphism. Additionally, E_{x_0} is surjective, since we can find $f_a : X \to A$, $x \mapsto a$, meaning $E_{x_0}(f_a) = f_a(x_0) = a$.

If $f \in \ker(E_{x_0})$, then $E_{x_0}(f) = 0_A$. However, $E_{x_0}(f) = f(x_0)$. Then,

$$\begin{aligned}\ker(\varphi) &= \{f : X \to A \mid f(x_0) = 0_A\}\\ &= \mathcal{M}_{x_0}.\end{aligned}$$

By the first isomorphism theorem, we can see that $R/\mathcal{M}_{x_0} \cong A$.

Other Isomorphism Theorems

Let R be a ring.

Diamond Isomorphism Theorem: Let A be a subring of R and I an ideal of R. Define $A + I = \{a + i \mid a \in A, i \in I\}$. This is an ideal of R. We also have that $A \cap I$ is an ideal in A, and $(A + I)/I \equiv A/A \cap I$.

$$\begin{tikzcd}
& A+I & \\
I \arrow[ur, "\cong"] & & A \arrow[ul] \\
& A \cap I \arrow[ul] \arrow[ur, "\cong"] &
\end{tikzcd}$$

Third Isomorphism Theorem: Let I, J be ideals of R with $I \subseteq J$. Then, J/I is an ideal of R/I with $(R/I)/(J/I) \cong R/J$.

Lattice Isomorphism Theorem: Let $I \subseteq R$ be an ideal. The correspondence $A \leftrightarrow A/I$ is an inclusion-preserving bijection between the subrings A of R that contain I and the subrings of R/I. Moreover, A is an ideal if and only if A/I is an ideal.

Using the Third Isomorphism Theorem

Let $R = \mathbb{Z}$, $I = 12\mathbb{Z}$, and $J = 4\mathbb{Z}$. By the third isomorphism theorem, $J/I = 4\mathbb{Z}/12\mathbb{Z}$ is an ideal of $R/I = \mathbb{Z}/12\mathbb{Z}$, and

$$\begin{aligned}(R/I)/(J/I) &= (\mathbb{Z}/12\mathbb{Z})/(4\mathbb{Z}/12\mathbb{Z})\\ &\cong \mathbb{Z}/4\mathbb{Z}.\end{aligned}$$

Applying the Isomorphism Theorems

Consider the rings $3\mathbb{Z}$ and $12\mathbb{Z}$. We have that $12\mathbb{Z} \subseteq 3\mathbb{Z}$ as an ideal. Therefore, we can form the quotient ring $3\mathbb{Z}/12\mathbb{Z}$. We might ask how it's related to other $\mathbb{Z}/n\mathbb{Z}$, or to $\mathbb{Z}/12\mathbb{Z}$.

Note that $3\mathbb{Z}/12\mathbb{Z}$ starts with elements in $3\mathbb{Z}$ and examines elements in $12\mathbb{Z}$. We might ask whether or not $3\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z}$. However,

$$\begin{aligned}3\mathbb{Z}/12\mathbb{Z} &= \{a + 12\mathbb{Z} \mid a \in 3\mathbb{Z}\}\\ &= \{3b + 12\mathbb{Z} \mid b \in \mathbb{Z}\}.\end{aligned}$$

We can define

$$\begin{aligned}\varphi : 3\mathbb{Z} &\to \mathbb{Z}/4\mathbb{Z}\\ 0 + 12\mathbb{Z} &\mapsto [0]_4,\\ 3 + 12\mathbb{Z} &\mapsto [3]_4,\\ 6 + 12\mathbb{Z} &\mapsto [2]_4,\\ 9 + 12\mathbb{Z} &\mapsto [1]_4.\end{aligned}$$

which we look at by aiming for $12\mathbb{Z}$ to be the kernel of φ. Then, by the first isomorphism theorem, $3\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z}$.

If we want to examine $3\mathbb{Z}/12\mathbb{Z}$ in relation to $\mathbb{Z}/12\mathbb{Z}$, we see that $3\mathbb{Z}/12\mathbb{Z} \cong \langle [3]_{12} \rangle \subseteq \mathbb{Z}/12\mathbb{Z}$.

Further Examination of Ideals

Let $I, J \subseteq R$ be ideals. We define

(1) the sum, $I + J = \{i + j \mid i \in I, j \in J\}$,

(2) the product, IJ, the collection of finite sums of elements of the form xy, where $x \in I$ and $y \in J$, and

(3) The nth power of I, denoted I^n, which is the collection of finite sums of elements of the form $x_1, \dots, x_n \in I$.

Exercises:

(1) $I + J$ is the smallest ideal containing I and J.

(2) $IJ \subseteq I \cap J$.

Let R be a ring with $1_R \neq 0_R$. Let $A \subseteq R$.

(1) Let $\langle A\rangle$ be the smallest ideal that contains A. It is called the ideal *generated* by A.

(2) We set $RA = \{r_1a_1 + \cdots + r_na_n \mid r_i \in R, a_i \in A\}$ for any $n \in \mathbb{Z}_{\geq 0}$. Additionally, AR is analogous to RA. We set $RAR = \{r_1a_1\tilde{r}_1 + \cdots + r_na_n\tilde{r}_n \mid r_i, \tilde{r}_i \in R, a_i \in A\}$.

(3) If A is a single element a, we write $\langle a\rangle$ to denote the ideal generated by A and refer to this as a principal ideal. If A is finite, then we say $\langle A\rangle$ is a finitely generated ideal.

For example, if $R = \mathbb{Z}[x_1, x_2, \dots]$, then $I = \langle x_1, x_2, \dots\rangle$ is not finitely generated.

Note: If R is commutative, then $\langle a\rangle = Ra$ and if R is not commutative, $\langle a\rangle = RaR$. For R commutative, we say that for $b \in \langle a\rangle$, $b = ra$ for some $r \in R$. We say a divides b — if a divides b, then $\langle b\rangle \subseteq \langle a\rangle$.

Principal Ideal: Example 1

Every ideal in $\mathbb{Z}$ is a principal ideal.

Let $I \subseteq \mathbb{Z}$ be a nonzero ideal (the zero ideal is generated by 0). Let $m \in I, m \neq 0$. Since I is an ideal, if $m \in I$, so too is $-m \in I$. Therefore, we know there is a positive integer in I.

By the well-ordering principle, let $n \in I$ be the smallest positive integer in I. Let $a \in I$, $a \neq 0$. Write $a = nq + r$ for $q, r \in \mathbb{Z}$, and $0 \leq r < n$. Then, we have $r = a - nq$. Since $a \in I$ and $n \in I$, $r \in I$. Therefore, $r = 0$, and $n|a$. Thus, $I = n\mathbb{Z}$.

Principal Ideal: Example 2

Let $R = \mathbb{Z}[x]$. Consider $I = \langle 2, x\rangle$. We claim that I is not a principal ideal.

Suppose toward contradiction that $\langle 2, x\rangle = \langle f(x)\rangle$ for some $f(x) \in \mathbb{Z}[x]$. Therefore, $2 = f(x)g(x)$ for some $g(x) \in \mathbb{Z}[x]$. Since degrees add, $\deg(2) = \deg(f) + \deg(g)$, or $0 = f(x)g(x)$. Therefore, $f(x), g(x) \in \mathbb{Z}$. Therefore, we must have that $f(x) \in \{\pm 1, \pm 2\}$.

So, we have elements of $\langle 2, x\rangle$ of the form $2s(x) + xt(x)$. So we have constant term divisible by 2, meaning $f(x) \neq \pm 1$, so $f(x) = \pm 2$.

Then, $x = 2h(x)$ for some $h(x) \in \mathbb{Z}[x]$. However, we have that $h(x)$ has integer coefficients. Therefore, $\langle 2, x\rangle \neq \langle f(x)\rangle$ for any $f(x) \in \mathbb{Z}[x]$.

Proposition: Ideals in Unital Rings

Let I be an ideal of R.

(1) $I = R$ if and only if I contains a unit.

(2) If R is commutative, then R is a field if and only if the only ideals in R are $\langle 0_R\rangle$ and R.

Proof of (1): Suppose $I = R$. Then, $1_R \in I$, and 1_R is a unit.

Suppose I contains a unit, u. Then, we have $u^{-1} \in R$. Since I is an ideal, we have $uu^{-1} \in I$, and $uu^{-1} = 1_R$. Letting $r \in R$, using the fact that I is an ideal, $(r)(1_R) = r \in I$. Thus, $I = R$.

Proof of (2): Suppose R is a field. Let I be any nonzero ideal. Every nonzero element in I is a unit, meaning $I = R$.

Suppose $\langle 0_R \rangle$ and R are the only ideals in R. Let $r \in R$, $r \neq 0_R$. Since $r \neq 0$, $\langle r \rangle = R$. Thus, $1_R \in \langle r \rangle$. Thus, $1_R = sr$ for some $s \in R$, implying every nonzero element of R has an inverse.

Corollary: Field Homomorphisms

Let F be a field, and $\varphi : F \to R$ be a homomorphism. Then, φ is either the zero map ($\varphi(f) = 0_R$) or φ is injective.

Proof: Since $\ker(\varphi)$ is an ideal in F by the first isomorphism theorem, then $\ker(\varphi) = \langle 0_F \rangle$ or $\ker(\varphi) = R$. If $\ker(\varphi) = \langle 0_F \rangle$, then φ is injective, and if $\ker(\varphi) = F$, then φ is the zero map.

Maximal Ideals

(1) An ideal $\mathcal{M} \subseteq R$ is a maximal ideal if $\mathcal{M} \neq R$ and the only ideals containing $\mathcal{M}$ are $\mathcal{M}$ and R. The collection of maximal ideals is denoted m-spec(R) or maxspec(R).

(2) An ideal $\mathfrak{p} \subseteq R$ with $\mathfrak{p} \neq R$ is a prime ideal if whenever $ab \in \mathfrak{p}$, then $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. We denote the collection of prime ideals Spec(R).

For example, $\text{Spec}(\mathbb{Z}) = \{0\mathbb{Z}, p\mathbb{Z}\}$ for p prime, and $\text{maxspec}(\mathbb{Z}) = \{p\mathbb{Z}\}$.

Aside: Let R be commutative. The set Spec(R) is a topological space. Let $A \subseteq R$ be any subset. Closed sets look like

$$\begin{aligned} V(A) &= \{\mathcal{P} \in \text{Spec}(R) \mid A \subset \mathcal{P}\} \\ &= V(I) \\ &= \langle A \rangle \end{aligned}$$

For example, if $R = \mathbb{R}[x, y]$, if $f(x, y) = y - x^2$, then $V(f) = \{(a, b) \in \mathbb{R}^2 \mid f(a, b) = 0\}$. The topology on Spec($R$) is called the Zariski topology.

Let $\varphi : R \to S$ be a ring homomorphism. If $\mathcal{P} \in \text{Spec}(S)$, then $\varphi^{-1}(\mathcal{P})$ is a prime ideal in R. We get a map $\varphi^*(\text{Spec}(S)) \to \text{Spec}(R)$ given by $\mathcal{P} \to \varphi^{-1}(\mathcal{P})$.

We get a contravariant functor that takes $R \mapsto \text{Spec}(R)$, mapping from the category of rings to the category of topological spaces.

Proposition: Existence of Maximal Ideals

Let R be a ring. Every proper ideal is contained in a maximal ideal.

Let I be a proper ideal. Let $\mathcal{S}$ be the collection of all proper ideals that contain I. We know that $\mathcal{S}$ is non-empty as $I \in \mathcal{S}$. Then, $\mathcal{S}$ has a partial ordering under inclusion.

Let $\mathcal{C}$ be a chain of ideals (that is, totally ordered subset) in $\mathcal{S}$, and

$$J = \bigcup_{A \in \mathcal{C}} A.$$

Since $\mathcal{C} \neq \emptyset$, there is at least one A in the union with $0_R \in A$. So, $J \neq \emptyset$. Let $a, b \in J$. There exists A with $a \in A$ and b with $b \in B$. Since $\mathcal{C}$ is a chain, either $A \subseteq B$ or $B \subseteq A$. So, a and b are both in either A or B. Thus, $a - b$ and ab are in either A or B. Thus, $a - b$ and ab are elements in J, meaning J is an ideal.

If $J = R$, then $1_R \in J$, meaning 1_R is an element of some $A \in \mathcal{C}$. Since $A \in \mathcal{S}$ is a proper ideal, this would be a contradiction.

Therefore, J is an upper bound for $\mathcal{C}$. Since every chain in $\mathcal{S}$ has an upper bound in $\mathcal{S}$, then, by Zorn's Lemma, there is a maximal element in $\mathcal{S}$.

Proposition: Maximal Ideals, Quotient Rings, and Fields

An ideal $\mathcal{M} \subseteq R$ of a commutative ring with identity is maximal if and only if $R/\mathcal{M}$ is a field.

Suppose $\mathcal{M}$ is maximal. Let $x + \mathcal{M} \neq 0 + \mathcal{M}$. We want to show that $x + \mathcal{M}$ has an inverse.

Consider $\langle x, \mathcal{M} \rangle$, the ideal generated by x and $\mathcal{M}$. We have $\mathcal{M} \subset \langle x, \mathcal{M} \rangle$, as $x \notin \mathcal{M}$. Therefore, $\langle x, \mathcal{M} \rangle = R$ by the definition of a maximal ideal. Therefore, $1_R \in \langle x, \mathcal{M} \rangle$, meaning $1_R = xu + mv$ for some $u, v \in R$, $m \in \mathcal{M}$. Note

$$\begin{aligned}(x + \mathcal{M})(u + \mathcal{M}) &= xu + \mathcal{M}\\ &= (1_R - mv) + \mathcal{M}\\ &= 1_R + \mathcal{M},\end{aligned}$$

meaning $x + \mathcal{M}$ has an inverse, meaning $R/\mathcal{M}$ is a field.

Suppose $R/\mathcal{M}$ is a field. Assume we have $\mathcal{M} \subset I \subset R$ for some ideal I. From the third isomorphism theorem, we have $I/\mathcal{M}$ is an ideal of $R/\mathcal{M}$. Specifically, by our construction, $I/\mathcal{M}$ is a proper nonzero ideal of $R/\mathcal{M}$, but since $R/\mathcal{M}$ is a field, no such proper nonzero ideal exists, meaning no such I exists.

Examples: Maximal Ideals

(1) Let $R = \mathbb{Z}$. Given $m \in \mathbb{Z}$, we know $m\mathbb{Z}$ is a maximal ideal if and only if m is prime. If $p|m$ and $p \neq m$, then $m\mathbb{Z} \subsetneq p\mathbb{Z}$. Additionally, if p is prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field. Additionally, $\mathbb{Z}/m\mathbb{Z}$ is not an integral domain if m is composite.

(2) Let $R = F[x]$ for F a field. Let $\alpha \in F$ and consider $\mathcal{M}_\alpha = \langle x - \alpha \rangle$. We claim that $F[x]/\mathcal{M}_\alpha \cong \mathcal{F}$, meaning $\mathcal{M}$ is a maximal ideal.

Let $\varphi : F[x] \to F$, $x \mapsto \alpha, f(x) \mapsto f(\alpha)$. Let $f(x), g(x) \in F[x]$. Then,

$$\begin{aligned}\varphi(f + g) &= (f + g)(\alpha)\\ &= f(\alpha) + g(\alpha)\\ &= \varphi(f) + \varphi(g)\end{aligned}$$

and

$$\begin{aligned}\varphi(fg) &= (fg)(\alpha)\\ &= f(\alpha)g(\alpha)\\ &= \varphi(f)\varphi(g).\end{aligned}$$

Let $\beta \in F$. Then,

$$\begin{aligned}\varphi(\beta + (x - \alpha)) &= \beta + (\alpha - \alpha)\\ &= \beta.\end{aligned}$$

Thus, φ is surjective. Finally, we have $f(x) \in \ker(\varphi)$ if and only if $f(\alpha) = 0$. However, $f(\alpha) = 0$ if and only if $(x - \alpha)|f(x)$. Therefore, $\ker(\varphi) = \langle x - \alpha \rangle$.

(3) Let $R = \mathbb{Z}[x]$. Let $\mathcal{M} = \langle 2, x \rangle$. We saw that $\mathbb{Z}[x]/\langle 2, x \rangle \cong \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Therefore, we know that $\mathcal{M}$ is a maximal ideal by the above categorization.

(4) Let $R = \mathbb{F}_2[x]$. Consider the ideal $\mathcal{M} = \langle x^2 + x + 1 \rangle$.

$$\begin{aligned}R/\mathcal{M} &= \left\{ f(x) + \langle x^2 + x + 1 \rangle \mid f(x) \in \mathbb{F}_2[x] \right\}\\ f(x) &= \left\{ (x^2 + x + 1)q(x) + r(x) \mid q(x), r(x) \in \mathbb{F}_2[x],\ r(x) = 0 \text{ or } \deg r(x) < 2 \right\}.\end{aligned}$$

So,

$$f(x) + \mathcal{M} = r(x) + \mathcal{M},$$

meaning

$$R\mathcal{M} = \{0 + \mathcal{M}, 1 + \mathcal{M}, x + \mathcal{M}, 1 + x + \mathcal{M}\}.$$

This is a field.

$+$	$0+\mathcal{M}$	$1+\mathcal{M}$	$x+\mathcal{M}$	$x+1+\mathcal{M}$
$0+\mathcal{M}$	0	1	x	$x+1$
$1+\mathcal{M}$	1	0	$1+x$	x
$x+\mathcal{M}$	x	$1+x$	0	1
$x+1+\mathcal{M}$	$1+x$	x	1	0

$\times$	$0+\mathcal{M}$	$1+\mathcal{M}$	$x+\mathcal{M}$	$x+1+\mathcal{M}$
$0+\mathcal{M}$	0	0	0	0
$1+\mathcal{M}$	0	1	x	$x+1$
$x+\mathcal{M}$	0	x	$1+x$	1
$x+1+\mathcal{M}$	0	$1+x$	x	1

Specifically, this is a field of order 4. Note that $\mathbb{F}_2 \hookrightarrow R/\mathcal{M}$. We say $R/\mathcal{M} \cong \mathbb{F}_4$.

Note: For every p prime and every $n \in \mathbb{Z}$ positive, there is exactly one field of order p^n up to isomorphism.

(5) Let $R = \mathbb{Z}[i]$. Set $\mathcal{M} = \langle 3 \rangle$. This is a maximal ideal, and $|\mathbb{Z}[i]/\langle 3 \rangle| = 9$.

Proposition: Prime Ideals, Quotient Rings, and Integral Domains

Let R be a commutative ring with identity. An ideal $\mathfrak{p} \subseteq R$ is a prime ideal if and only if $R/\mathfrak{p}$ is an integral domain.

Let $\mathfrak{p} \subseteq R$ be a prime ideal. Let $x, y \in R$ with $(x+\mathfrak{p})(y+\mathfrak{p}) = 0+\mathfrak{p}$. We have

$$xy + \mathfrak{p} = 0 + \mathfrak{p}$$

meaning

$$xy \in \mathfrak{p},$$

so, since $\mathfrak{p}$ is prime,

$$x \in \mathfrak{p}$$

or

$$y \in \mathfrak{p}$$

so $x + \mathfrak{p} = 0 + \mathfrak{p}$ or $y + \mathfrak{p} = 0\mathfrak{p}$.

In the reverse direction, assume $R/\mathfrak{p}$ is an integral domain. Let $xy \in \mathfrak{p}$. Then,

$$\begin{aligned}(x+\mathfrak{p})(y+\mathfrak{p}) &= xy + \mathfrak{p}\\ &= 0 + \mathfrak{p},\end{aligned}$$

implying that $x + \mathfrak{p}$ or $y + \mathfrak{p}$ is equal to $0 + \mathfrak{p}$, or $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

Examples: Prime Ideals

(1) If $R = \mathbb{Z}[x]$, then $\mathfrak{p} = \langle x \rangle$ is a prime ideal that is not a maximal ideal, as $\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}$.

Corollary: Maximal Ideals and Prime Ideals

Let R be a commutative ring with identity. Then, $\operatorname{maxspec}(R) \subseteq \operatorname{Spec}(R)$.

Direct Products

Let R and S be rings. The set

$$R \times S = \{(r, s) \mid r \in R, s \in S\}$$

is a ring under component-wise multiplication and addition.

Exercise: Let $R_1, \dots, R_n$ be rings. Let

$$\varphi : R \to R_1 \times \cdots \times R_n$$

be a map. Define

$$\begin{aligned}\pi_j : R_1 \times \cdots \times R_n &\to R_j\\ (r_1, \dots, r_n) &\mapsto r_j.\end{aligned}$$

Show φ is a homomorphism if and only if $\pi_j \circ \varphi$ is a homomorphism for each j.

Comaximal Ideals

Recall that $a\mathbb{Z} + b\mathbb{Z} = \gcd(a, b)\mathbb{Z}$. If $\gcd(a, b) = 1$, then $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$. Conversely, if $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$, then $am + bn = 1$ for some $m, n \in \mathbb{Z}$. Thus, $\gcd(a, b) = 1$.

Let I, J be ideals in a commutative ring R. We say I and J are comaximal if $I + J = R$.

Chinese Remainder Theorem

Let $I_1, \dots, I_n$ be ideals in a commutative ring R. The map

$$\begin{aligned}\varphi : R &\to R/I_1 \times R/I_2 \times \cdots \times R/I_n\\ r &\mapsto (r + I_1, r + I_2, \dots, r + I_n)\end{aligned}$$

is a ring homomorphism with kernel $I_1 \cap \cdots \cap I_n$. If I_i, I_j are comaximal for all $1 \leq i, j \leq n$ with $i \neq j$, then φ is surjective, and $I_1 \cap \cdots \cap I_n = (I_1)(I_2)\cdots(I_n)$, so

$$R/\left((I_1)(I_2)\cdots(I_n)\right) \cong R/(I_1 \cap \cdots \cap I_n) \cong R/I_1 \times \cdots \times R/I_n.$$

Corollary to the Chinese Remainder Theorem (1)

Let $n = p_1^{e_1} \cdots p_r^{e_r} \in \mathbb{Z}$. Then,

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{e_r}\mathbb{Z}.$$

Moreover,

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \left(\mathbb{Z}/p_1^{e_1}\mathbb{Z}\right)^\times \times \cdots \times \left(\mathbb{Z}/p_r^{e_r}\mathbb{Z}\right)^\times.$$

Corollary to the Chinese Remainder Theorem (2)

Let $n_1, \dots, n_k$ be positive integers that are pairwise relatively prime. Then, for any $a_1, \dots, a_k \in \mathbb{Z}$, there is a $x \in \mathbb{Z}$ satisfying

$$\begin{aligned}x &\equiv a_1 \mod n_1\\ &\vdots\\ x &\equiv a_k \mod n_k\end{aligned}$$

This solution is unique modulo $n_1, \dots, n_k$. If we set

$$m_i = n_1 \cdots \hat{n}_i \cdots n_k,$$

and y_i as the inverse of m_i mod n_i. The solution x is given by

$$x = a_1 y_1 m_1 + \cdots + a_k y_k m_k.$$

We will prove the Chinese Remainder Theorem by induction, with the base case of $n = 2$:

$$\begin{aligned}\varphi : R &\to R/I_1 \times R/I_2\\ r &\mapsto (r + I_1, r + I_2).\end{aligned}$$

We can verify that this is a homomorphism, with $\ker(\varphi) = I_1 \cap I_2$. Assume I_1 and I_2 are comaximal: $I_1 + I_2 = R$. In particular, there exist $x \in I_1$ and $y \in I_2$ such that $x + y = 1_R$. Note that

$$\begin{aligned}\varphi(x) &= (x + I_1, x + I_2)\\ &= (0 + I_1, 1_R - y + I_2)\\ &= (0 + I_1, 1_R + I_2)\end{aligned}$$

and

$$\varphi(y) = (1_R + I_1, 0 + I_2).$$

Let $(r_1 + I_1, r_2 + I_2) \in R/I_1 \times R/I_2$. Set $z = r_2x + r_1y$. Then,

$$\begin{aligned}\varphi(z) &= (r_2x + r_1y + I_1, r_2x + r_1y + I_2)\\ &= (r_1 + I_1, r_2 + I_2).\end{aligned}$$

So, φ is surjective, and we get $R/I_1 \cap I_2 \cong R/I_1 \times R/I_2$.

We also have that $(I_1)(I_2) \subseteq I_1 \cap I_2$. Let $z \in I_1 \cap I_2$. We have

$$\begin{aligned}z &= z(1_R)\\ &= z(x + y)\\ &= zx + zy\\ &\in (I_1)(I_2).\end{aligned}$$

Therefore, $R/(I_1)(I_2) \cong R/I_1 \cap I_2$.

Suppose the result holds for all values up to $2 \leq n \leq k - 1$. Write $J_1 = I_1$ and $J_2 = (I_2)(I_3)\cdots(I_k)$. We only need to show that J_1 and J_2 are comaximal, then apply $n = 2$ to J_1, J_2 and $n = k - 1$ to split up J_2.

For each $i \in \{2, \dots, k\}$, there are elements $x_i \in I_1$ and $y_i \in I_i$ such that $x_i + y_i = 1_R$. We have $x_i + y_i \equiv y_i (\text{mod } I_1)$, so

$$1_R = (x_2 + y_2)(x_3 + y_3) \times (x_k + y_k)$$

is an element of $J_1 + J_2$.

Localization

Where does $\mathbb{Q}$ come from?

Consider the sets $\mathbb{Z}$ and $\Sigma = \mathbb{Z} \setminus \{0\}$. Set

$$\Sigma^{-1}\mathbb{Z} = \{(a, b) \mid a \in \mathbb{Z}, b \in \Sigma\}.$$

Define $\sim$ on $\Sigma^{-1}\mathbb{Z}$ by

$$(a, b) \sim (c, d) \text{ if } ad = bc.$$

This is an equivalence relation:

Reflexivity:

$$\begin{aligned}(a, b) &\sim (a, b)\\ ab &= ab.\end{aligned}$$

Symmetry:

$$\begin{aligned}(a, b) &\sim (c, d)\\ ad &= bc\\ bc &= ad\\ (c, d) &= (a, b)\end{aligned}$$

Transitivity: Suppose $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$, meaning $ad = bc$ and $cf = de$. We need to show $af = be$.

$$\begin{aligned}ad - bc &= 0\\ cf - de &= 0\\ adf - bcf &= 0\\ bcf - bde &= 0\\ (adf - bcf) + (bcf - bde) &= 0\\ (af - be)(d) &= 0\end{aligned}$$

and since $d \neq 0$ and we are in $\mathbb{Z}$,

$$af = be,$$

meaning $(a, b) \sim (e, f)$.

Let $\frac{a}{b}$ denote the equivalence class containing (a, b). We define

$$\begin{aligned}\frac{a}{b} + \frac{c}{d} &= \frac{ad + bc}{bd}\\ \frac{a}{b} \cdot \frac{c}{d} &= \frac{ac}{bd}.\end{aligned}$$

Exercise: Show that addition and multiplication are well-defined, and make the collection of equivalence classes into a field.

The field of equivalence classes $\Sigma^{-1}\mathbb{Z}$ under the defined addition and multiplication forms the field $\mathbb{Q}$.

Let R be a ring. We say $\Sigma \subseteq R$ is multiplicatively closed if, given $a, b \in \Sigma$, $ab \in \Sigma$.

(1) $\Sigma = \mathbb{Z} \setminus \{0\}$ is multiplicatively closed.

(2) Let $r \in R$. Then, $\Sigma = \{r^n \mid n \in \mathbb{Z}\}$.

(3) Let $\mathfrak{p} \in R$. Then, $R \setminus \mathfrak{p}$ is multiplicatively closed (verify this).

Universal Property

Let R be a commutative ring with identity and $\Sigma \subseteq R$ a multiplicatively closed subset with $1_R \in \Sigma$. There is a unique commutative ring $\Sigma^{-1}R$ and ring homomorphism

$$\pi : R \to \Sigma^{-1}R$$

satisfying for any homomorphism $\psi : R \to S$ that sends 1_R to 1_S and $\psi(\Sigma) \subseteq S^\times$, there is a unique homomorphism

$$\Psi : \Sigma^{-1}R \to S$$

such that $\Psi \circ \pi = \psi$.

$$\begin{tikzcd} R \arrow[r, "\pi"] \arrow[dr, "\psi"'] & \Sigma^{-1}R \arrow[d, "\Psi"] \\ & S \end{tikzcd}$$

Let $\mathcal{F} = \{(r, d) \mid r \in R, d \in \Sigma\}$. Define a relation $(r_1, d_1) \sim (r_2, d_2)$ if $x(r_1 d_2 - r_2 d_1) = 0$ for some $x \in \Sigma$.

We claim that $\sim$ is an equivalence relation.

(i) It is clear that $(r,d) \sim (r,d)$.

(ii) If $(r_1,d_1) \sim (r_2,d_2)$, it is clear that $(r_2,d_2) \sim (r_1,d_1)$.

(iii) Suppose $(r_1,d_1) \sim (r_2,d_2)$, and $(r_2,d_2) \sim (r_3,d_3)$. We have $x, y \in \Sigma$ such that

$$\begin{aligned} x(r_1d_2 - r_2d_1) &= 0 \\ y(r_2d_3 - r_3d_2) &= 0. \end{aligned}$$

Therefore, we have

$$\begin{aligned} d_3yx(r_1d_2 - r_2d_1) &= 0 \\ d_1xy(r_2d_3 - r_3d_2) &= 0. \end{aligned}$$

Adding together, we have

$$\begin{aligned} d_3yx(r_1d_2 - r_2d_1) + d_1xy(r_2d_3 - r_3d_2) &= d_3xyr_1d_2 - d_1xyr_3d_2 \\ d_2xy(r_1d_3 - r_3d_1) &= 0 \end{aligned}$$

Since $d_2, x, y \in \Sigma$, $d_2xy \in \Sigma$, and we have $(r_1,d_1) \sim (r_3d_3)$.

Since $\sim$ is an equivalence relation on $\mathcal{F}$, we set $\Sigma^{-1}R$ to be the equivalence classes of $\sim$ on $\mathcal{F}$. We denote the equivalence class containing (r,d) as $\frac{r}{d}$. We define addition and multiplication as

$$\begin{aligned} \frac{r_1}{d_1} + \frac{r_2}{d_2} &= \frac{r_1d_2 + r_2d_1}{d_1d_2} \\ \frac{r_1}{d_1}\frac{r_2}{d_2} &= \frac{r_1r_2}{d_1d_2}. \end{aligned}$$

These operations are well defined, and make $\Sigma^{-1}R$ into a commutative ring with $1_{\Sigma^{-1}R} = \frac{1}{1}$.

Defining $\pi : R \to \Sigma^{-1}R$ with $r \mapsto \frac{r}{1}$, we can verify that π is a homomorphism. Let $\psi : R \to S$ with $\psi(\Sigma) \subseteq S^\times$, and $\psi(1_R) = 1_S$. Then, we define $\Psi : \Sigma^{-1}R \to S$ as $\frac{r}{d} \mapsto \psi(r)\psi(d)^{-1}$.

To show this map is well-defined, let $\frac{a}{b} = \frac{c}{d}$. So, $x(ad - bc) = 0$ for some $x \in \Sigma$. Since ψ is a homomorphism,

$$\psi(x)(\psi(a)\psi(d) - \psi(b)\psi(c)) = 0.$$

Since $x \in \Sigma$, $\psi(x) \in S^\times$, meaning

$$\psi(a)\psi(d) - \psi(b)\psi(c) = 0.$$

Since $b, d \in \Sigma$, $\psi(b), \psi(d) \in S^\times$. Therefore,

$$\begin{aligned} \psi(a)\psi(d) &= \psi(c)\psi(b) \\ \psi(a)\psi(b)^{-1} &= \psi(c)\psi(d)^{-1}. \end{aligned}$$

We can easily verify that Ψ is a ring homomorphism, and $\Psi \circ \pi = \psi$.

For example, if $R = \mathbb{Z}$ and $\Sigma = \mathbb{Z} \setminus \{0\}$, then $\Sigma^{-1}\mathbb{Z} = \mathbb{Q}$, then for $\pi : \mathbb{Z} \hookrightarrow \mathbb{Q}$, and a homomorphism from $\mathbb{Z}$ into a set S, there must exist a map from $\mathbb{Q}$ to S.

Consider $\mathbb{Z}$ with $\Sigma = \mathbb{Z} \setminus p\mathbb{Z}$. Then, $\Sigma^{-1}\mathbb{Z} = \{(a,b) \mid a \in \mathbb{Z}, p \nmid b\} = \mathbb{Z}_{\langle p \rangle}$. We saw on an earlier homework assignment that $\mathbb{Z}_{\langle p \rangle}/p\mathbb{Z}_{\langle p \rangle} \cong \mathbb{F}_p$, meaning it is a maximal ideal (as if $a \nmid p$, then a/b is a unit in $\mathbb{Z}_{\langle p \rangle}$). The only other ideals are $p^m\mathbb{Z}_{\langle p \rangle}$, so we have a chain

$$p\mathbb{Z}_{\langle p \rangle} \supseteq p^2\mathbb{Z}_{\langle p \rangle} \supseteq \cdots.$$

Corollary to the Universal Property

Given π, ψ, and Ψ as defined above, we have the following.

(1) $\ker\pi = \{r \in R \mid xr = 0 \text{ for some } x \in \Sigma\}$. In particular, π is an injection if Σ does not contain zero or any zero divisors.

(2) $\Sigma^{-1}R = 0$ if and only if $0 \in \Sigma$.

Recall that $\pi(r) = \frac{r}{1}$. Recall that $r \in \ker\pi$ if and only if $\frac{r}{1} = \frac{0}{1}$, which is true if and only if $x(r\cdot 1 - 0\cdot 1) = 0$ for some $x \in \Sigma$, meaning $xr = 0$.

$\Sigma^{-1}R = 0$ if and only if $(1,1) \sim (0,1)$, which is true if and only if $x\cdot 1 = 0$ for some $x \in \Sigma$, which is only true if $x = 0 \in \Sigma$.

The ring $\Sigma^{-1}R$ is called the localization of R at Σ. If R is an integral domain and $\Sigma = R\setminus\{0\}$, then $\Sigma^{-1}R$ is known as the field of fractions of R, or $\text{Frac}(R)$.

Corollary: Field of Fractions

Let R be an integral domain, $\Sigma = R\setminus\{0\}$. Let $F = \text{Frac}(R)$. Let K be any field that contains a subring $S \cong R$. Then, any field of K generated by S (i.e., the intersection of all subfields that contain S) is isomorphic to F.

The proof is left as an exercise for the reader.

For an outline, consider $\varphi : R \xrightarrow{\simeq} S \subseteq K$. Recall that $\Sigma = R\setminus\{0\}$. Consider $\varphi(\Sigma)$ from R to K, and use the universal property.

Localization Examples

(1) Let R be an integral domain, $R[x]$ be the set of polynomials. Then, for $\Sigma = R[x]\setminus\{0\}$,

$$\text{Frac}(R[x]) = \left\{\frac{f(x)}{g(x)} \mid f(x), g(x) \in R[x], g(x) \neq 0\right\}$$

is the field of rational functions.

(2) Let R be a commutative ring with identity, and let $f \in R$. Set $\Sigma = \{f^n \mid n \geq 0\}$. We form $\Sigma^{-1}R$, denoted R_f. Then, $R_f = 0$ if and only if $f^n = 0$ for some $n \geq 0$.

If f is not nilpotent, then $R_f \neq 0$, meaning f is invertible in R_f. We have

$$R_f \cong R[x]/\langle xf - 1\rangle.$$

(3) Consider $R = K[x,y]/\langle xy\rangle$ for K any field. We set $f = x$. Note that f is not nilpotent, but f is a zero divisor. Note that f is invertible in R_f.

Consider $\pi : R \to R_f$, $g \mapsto \frac{g}{1}$. We have $y \mapsto \frac{y}{1}$. However, in R_f, x is invertible, so $1 = \frac{x}{x} \in R_f$. So, $\frac{y}{1} = \frac{y}{1}\cdot\frac{x}{x} = \frac{xy}{x} = \frac{0}{x} = \frac{0}{1}$. In this case, we do not have that R injects into R_f.

Exercise: For $\pi : R \to R_f$, we have $\pi(R) = K[x] \subseteq R_f = K[x, x^{-1}]$.

Proposition: Localization by Prime Ideal

The ring R is the zero ring if and only if $R_{\mathfrak{p}} = 0$ for all $\mathfrak{p} \in \text{Spec}(R)$.

If $R = 0$, then clearly $R_{\mathfrak{p}} = 0$ for all $\mathfrak{p} \in \text{Spec}(R)$.

In the reverse direction, suppose $R_{\mathfrak{p}} = 0$ for all $\mathfrak{p} \in \text{Spec}(R)$. Pick $r \in R$, $r \neq 0$. Set

$$I = \text{Ann}_R(r) = \{x \in R \mid xr = 0\}$$

to be the annihilator of r. We can verify that I is an ideal. Since $r \neq 0$, $1_R \notin I$, meaning I is a proper ideal. Since I is a proper ideal, $I \subset \mathcal{M}$ for some maximal ideal $\mathcal{M}$.

Consider $R_{\mathcal{M}}$. We have $\frac{r}{1} \in R_{\mathcal{M}}$. However, as $\mathcal{M}$ is maximal, $\mathcal{M}$ is prime, so $R_{\mathcal{M}} = 0$. There exists $s \in \Sigma = R \setminus \mathcal{M}$ such that $sr = 0$. So, $s \in I$. However, $I \subset M$, and $s \notin \mathcal{M}$. Thus, $r = 0$.

Vector Spaces and Polynomials

Let $\mathbb{F}$ be a field. We say V is a $\mathbb{F}$-vector space if V is an Abelian group under addition with the scalar product $\mathbb{F} \times V \to V, (\alpha, v) \to \alpha v$ satisfying

(a) $(a+b)v = av + bv$ for all $a, b \in \mathbb{F}$, $v \in V$

(b) $(ab)v = a(bv)$

(c) $a(v+w) = av + aw$ for all $a \in \mathbb{F}$, $v, w \in V$

(d) $1v = v$ for all $v \in V$.

A set $B \subseteq V$ is said to be linearly independent if whenever

$$\sum_{i=1}^{m} a_i v_i = 0 \Rightarrow a_1 = a_2 = \cdots = a_m = 0$$

For $B \subseteq V$, the $\mathbb{F}$-span of B is

$$\text{span}_{\mathbb{F}}(B) = \{a_1 v_1 + \cdots + a_m v_m \mid a_i \in \mathbb{F}\}.$$

If $\text{span}_{\mathbb{F}}(B) = V$, then we say B spans V. If B is linearly independent and spans V, then we say B is a $\mathbb{F}$-basis for V.

Examples: Vector Spaces and Bases

(1) The set $\mathbb{F}^n = \{(a_1, \dots, a_m) \mid a_i \in \mathbb{F}\}$ is an $\mathbb{F}$-vector space with basis

$$B = \{e_i\}_{i=1}^{n}.$$

(2) $V = \mathbb{F}[x]$ is an $\mathbb{F}$-vector space with basis $\{1, x, x^2, \dots\}$.

Proposition: Basis Maximality

Let $B = \{v_1, \dots, v_n\}$ be a spanning set for V. Assume no proper subset of B spans V. Then, B is a basis for V.

Assume $a_1 \neq 0$. We have

$$v_1 = \frac{-1}{a_1}\left(a_2 v_2 + \cdots + a_n v_n\right),$$

so $v \in \text{span}_{\mathbb{F}}(v_2, \dots, v_n)$. Thus,

$$V = \text{span}_{\mathbb{F}}\left(v_1, v_2, \dots, v_n\right) \subseteq \text{span}_{\mathbb{F}}(v_2, \dots, v_n),$$

which is a contradiction as we assumed no proper subset of B spanned V.

Proposition: Finite Spanning Sets and Basis

Let B be a finite spanning set of V. Then, B contains a basis for V.

The proof is clear from the definition of basis.

Example: Basis of a Vector Space

Let $f \in \mathbb{F}[x]$. Consider $V = \mathbb{F}[x]/\langle f(x)\rangle$ (the quotient space of $\mathbb{F}[x]$ formed by $f(x)$). Then, for $g(x) \in \mathbb{F}[x]$, we can write $g(x) = f(x)q(x) + r(x)$, where $r(x) = 0$ or $\deg(r(x)) < \deg(f(x))$. Then,

$$\begin{aligned} g(x) + \langle f(x)\rangle &= (f(x)q(x) + r(x)) + \langle f(x)\rangle \\ &= r(x) + \langle f(x)\rangle. \end{aligned}$$

Therefore,

$$\left\{1 + \langle f(x)\rangle, x + \langle f(x)\rangle, \dots x^{n-1} + \langle f(x)\rangle\right\}$$

where $n = \deg(f(x))$ is a spanning set for $\mathbb{F}[x]/\langle f(x)\rangle$.

Suppose

$$\begin{aligned} (a_0 + \langle f(x)\rangle) + (a_1 x + \langle f(x)\rangle) + \cdots + (a_{n-1}x^{n-1} + \langle f(x)\rangle) &= 0 + \langle f(x)\rangle \\ \sum_{i=0}^{n-1} a_i x^i + \langle f(x)\rangle &= 0 + \langle f(x)\rangle. \end{aligned}$$

Then, $f(x) | \sum_{i=0}^{n-1} a_i x^i$. However, $\deg(f(x)) = n$, so we must have $a_0 = a_1 = \cdots = a_{n-1} = 0$.

Theorem: Reordering a Basis

Let $B = \{v_1, \dots, v_n\}$ be a basis for V. Let $A = \{w_1, \dots, w_m\}$ be linearly independent vectors. Then, there is a reordering of B such that $\{w_1, \dots, w_i, v_{i+1}, \dots, v_n\}$ is a basis for V.

We will prove this by induction. For the base case, we have $i = 0$, which means there is no replacement, and the hypothesis of the theorem is satisfied.

The induction hypothesis is that $S = \{w_1, \dots, w_i, v_{i+1}, \dots, v_n\}$ is a basis for V. Since S is spanning,

$$w_{i+1} = a_1 w_1 + \cdots + a_i w_i + a_{i+1} v_{i+1} + \cdots + a_n v_n.$$

If $a_{i+1} = a_{i+2} = \cdots = a_n = 0$, then $w_{i+1} \in \text{span}_{\mathbb{F}}(w_1, \dots, w_i)$, which contradicts A being linearly independent.

After reordering, we can assume $a_{i+1} = 0$. Thus,

$$v_{i+1} = \frac{1}{a_{i+1}}\left(w_{i+1} - a_1 w_1 - \cdots - a_i w_i - a_{i+2} v_{i+2} - \cdots - a_n v_n\right) \tag{$*$}$$

Hence,

$$\text{span}_{\mathbb{F}}\left(w_1, \dots, w_i, v_{i+1}, \dots, v_n\right) = \text{span}_{\mathbb{F}}\left(w_1, \dots, w_{i+1}, v_{i+1}, \dots, v_n\right).$$

Suppose $b_1 w_1 + \cdots + b_{i+1} w_{i+1} + b_{i+1} v_{i+1} + \cdots b_n v_n = 0$. We replace w_{i+1}, and find

$$\begin{aligned} 0 &= b_1 w_1 + \cdots + b_{i+1}\left(a_1 w_1 + \cdots + a_i w_i + a_{i+1} v_{i+1} + \cdots + a_n v_n\right) + b_{i+2} v_{i+2} + \cdots + b_n v_n \\ &= (b + 1 + b_{i+1} a_1) w_1 + \cdots + b_{i+1} a_{i+1} v_{i+1} + \cdots + (b_{i+2} + b_{i+1} a_{i+1}) v_{i+1} + \cdots + (b_n + b_n a_n) v_n \end{aligned}$$

Since $\{w_1, \dots, w_i, v_{i+1}, \dots, v_n\}$ is a coefficient, we know all coefficients are zero. Specifically, $b_{i+1} a_{i+1} = 0$. Since $a_{i+1} \neq 0$ by assumption, we know that $b_{i+1} = 0$. Then,

$$b_1 w_1 + \cdots b_i w_i + b_{i+2} + \cdots + b_n v_n = 0.$$

So, $b_{i+1} = b_1 = \cdots = b_i = \cdots = b_n$.

Corollary: Linearly Independent Sets in Vector Spaces

(1) Let V have a finite basis with n elements. Any linearly independent set must have n or fewer elements. Any spanning set must have n or greater elements.

(2) If V has a finite basis with n elements, any other basis must also have n elements.

Finite-Dimensional Vector Spaces

Let V have a basis of n elements over a field $\mathbb{F}$. We say the dimension of V over $\mathbb{F}$ is n, and write $\dim_{\mathbb{F}} V = n$. We say V is finite-dimensional if such n is finite; otherwise, we say V is infinite-dimensional.

Examples: Dimensions of Vector Spaces

(1) $\dim_{\mathbb{R}} \mathbb{R}^n = n$

(2) $\dim_{\mathbb{C}} \mathbb{C}^n = n$, $\dim_{\mathbb{R}} \mathbb{C}^n = 2n$ (verify this for yourself)

(3) $\dim_{\mathbb{Q}} \mathbb{R} = \infty$

(4) For $\deg(f(x)) = n$, $\dim_{\mathbb{F}}(\mathbb{F}[x]/\langle f(x)\rangle) = n$

Subspaces

Let $W \subseteq V$ be a subgroup. If W is closed under scalar multiplication, then W is known as a subspace of V.

(1) $\mathbb{Q}^n$ is a $\mathbb{Q}$-subspace of $\mathbb{R}^n$, but it is *not* an $\mathbb{R}$-subspace of $\mathbb{R}^n$ (it is not closed under scalar multiplication by $\mathbb{R}$).

(2) $W = \{a + bx \mid a, b \in \mathbb{F}\}$ is an $\mathbb{F}$-subspace of $\mathbb{F}[x]$.

Corollary: Basis and Subspace

Let A be a set of linearly independent vectors in a finite-dimensional vector space V. There is a basis of V that contains A. In particular, if $W \subseteq V$ is a subspace and A is a basis of W, then there is a basis of V that contains A.

Taking $B = \{v_1, \dots, v_n\}$ as a basis for V, we replace vectors in B with vectors from A.

Linear Transformations

Let V, W be $\mathbb{F}$-vector spaces. A map $T : V \to W$ is said to be a linear transformation if, for all $v_1, v_2 \in V$ and $\alpha, \beta \in \mathbb{F}$,

$$T(\alpha v_1 + \beta v_2) = \alpha T(v_1) + \beta T(v_2).$$

The collection of all linear transformations between V and W is denoted $\operatorname{Hom}_{\mathbb{F}}(V, W)$.

Lemma: Isomorphism of Finite-Dimensional Vector Spaces

If V is an $\mathbb{F}$-vector space of dimension n, then $V \cong \mathbb{F}^n$ as $\mathbb{F}$-vector spaces.

Let $B = \{v_1, \dots, v_n\}$ be a basis of V. Define

$$\begin{aligned} T : \mathbb{F}^n &\to v \\ (a_1, \dots, a_n) &\mapsto a_1 v_1 + \cdots a_n v_n. \end{aligned}$$

Let $(a_1, \dots, a_n), (b_1, \dots, b_n) \in \mathbb{F}^n$, $\alpha \in \mathbb{F}$. We have

$$\begin{aligned} T\left(\alpha(a_1, \dots, a_n) + (b_1, \dots, b_n)\right) &= T\left((\alpha a_1 + b_1, \dots, \alpha a_n + b_n)\right) \\ &= (\alpha a_1 + b_1)v_1 + \cdots + (\alpha a_n + b_n)v_n \\ &= \alpha(a_1 v_1 + \cdots + a_n v_n) + (b_1 v_1 + \cdots + b_n v_n) \\ &= \alpha T((a_1, \dots, a_n)) + T((b_1, \dots, b_n)). \end{aligned}$$

Let $v \in V$. Then, $v = a_1 v_1 + \cdots + a_n v_n$ for some $a_1, \dots, a_n \in \mathbb{F}$. So,

$$\begin{aligned} T((a_1, \dots, a_n)) &= a_1 v_1 + \cdots + a_n v_n \\ &= v. \end{aligned}$$

Suppose $T((a_1, \dots, a_n)) = T((b_1, \dots, b_n))$. Then,

$$\begin{aligned} a_1 v_1 + \cdots + a_n v_n &= b_1 v_1 + \cdots + b_n v_n \\ 0 &= (a_1 - b_1)v_1 + \cdots + (a_n - b_n)v_n. \end{aligned}$$

Since $\{v_1, \dots, v_n\}$ is linearly independent, $a_i - b_i = 0$ for all $i \in \{1, \dots, n\}$, meaning $a_i = b_i$ for all i. Thus, T is bijective.

Example: Vector Space Bases

(1) Define $\mathfrak{SL}_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{Mat}_2(\mathbb{R}) \mid a + d = 0 \right\}$. This is a 3-dimension $\mathbb{R}$-vector space with basis

$$\mathcal{B} = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \right\}.$$

(2) We define $\text{SL}_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{Mat}_2(\mathbb{R}) \mid ad - bc = 1 \right\}$ as a Lie group.

(3) If $\mathbb{F}$ is a finite field with q elements, we want to consider the vector space $V = \mathbb{F}^n$ and find the number of potential bases.

After selecting v_1 (for which there are $q^n - 1$ choices), we choose v_2 by throwing away $\mathbb{F}_{v_1}$, meaning there are $q^n - q$ choices for v_2. Iteratively, we have, for v_{i+1}, $q^n - q^i$ choices. Therefore, there are

$$\prod_{i=0}^{n-1} q^n - q^i$$

choices of basis for $\mathbb{F}^n$.

Theorem: Dimension of Quotient Space

Let V be an F-vector space and W a subspace. Then, V/W is a vector space and $\dim_F(V) = \dim_F(W) + \dim_F(V/W)$ (including infinite-dimensional spaces).

Note that $V/W = \{v + W \mid v \in V\}$ is an abelian group. We define scalar multiplication as $\alpha(v + W) = \alpha v + W$. This can be verified as a vector space.

Assume V is finite-dimensional. Let $\{w_1, \dots, w_m\}$ be a basis for W. By our earlier lemma, we can expand this set to a basis of V, $\{w_1, \dots, w_m, v_{m+1}, \dots, v_n\}$. Define $\pi : V \to V/W$ as $v \to v + W$.

This is a surjective linear map with $W \subseteq \ker \pi$. We claim that $\{v_{m+1} + W, \dots, v_n + W\}$ is a basis for V/W. Let $v \in V$. Write

$$v = \sum_{i=1}^{m} a_i w_i + \sum_{j=m+1}^{n} a_j v_j$$

meaning

$$\pi(v) = W + \sum_{j=m+1}^{n} a_j(v + W),$$

meaning $\{v_{m+1} + W, \dots, v_n + W\}$ spans V/W. To show linear independence, suppose $\sum_{j=m+1}^{n} a_j(v + W) = 0 + W$. Then,

$$\left(\sum_{j=m+1}^{n} a_j v_j \right) + W = 0 + W$$

meaning

$$\sum_{j=m+1}^{n} a_j v_j \in W.$$

However, since $\{w_1, \dots, w_m, v_{m+1}, \dots, v_n\}$ is linearly independent, this cannot be the case unless $\sum_{j=m+1}^{n} a_j v_j = 0$, so $a_{m+1} = \dots = a_n = 0$. Therefore, $\{v_{m+1} + W, \dots, v_n + W\}$ is a basis, so the dimension of V/W is $n - m$.

If $\dim_F(V) = \infty$ and $\dim_F(W) = \infty$, then we are done. Otherwise, if $\dim_F(V) = \infty$ and $\dim_F(W) < \infty$, take a basis $\{w_1, \dots, w_m\}$ of W. Pick $v_1 \in V, v_1 \notin W$. Put $v_1 + W$ in $\mathcal{B}$. Pick $v_2 \in V$, $v_2 \notin W \cup \text{span}_F\{v_1\}$, and put $v_2 + W$ into $\mathcal{B}$. Continue this process. Then, $\dim_F(V/W) = \infty$.

Corollary: Kernel of Linear Transformations and Subspaces

Let $T \in \text{Hom}_F(V, W)$. Then, $\ker T$ is a subspace of V, $T(V)$ is a subspace of W, and $\dim_F(V) = \dim_F \ker T + \dim_F T(v)$.

To prove this, we use something akin to the first isomorphism theorem.

Corollary: Linear Transformations between Vector Spaces of Identical Finite Dimension

Let $T \in \text{Hom}_F(V, W)$ with $\dim_F(V) = \dim_F(W) = n$. Then, the following are equivalent:

(i) T is an isomorphism;

(ii) T is injective;

(iii) T is surjective;

(iv) T sends a basis of V to a basis of W.

Field Extensions and Characteristics

Let K and F be fields. If $F \subseteq K$, then we say K is an extension field of F (note that K is also an F-vector space). Denote K as an extension field by K/F (yes, this is very bad notation).

Viewing K as an F-vector space, we say the degree of K over F means $\dim_F(K)$, written as $\deg(K/F)$. If $\deg(K/F) < \infty$,we say K is a finite extension of F. If $\deg(K/F) = \infty$, it is an infinite extension.

(1) For $F = \mathbb{R}$, $K = \mathbb{C}$, we have $\deg(K/F) = 2$.

(2) For $K = \mathbb{Q}(\sqrt{2})$, $\deg(K/\mathbb{Q}) = 2$.

(3) For $K = \mathbb{R}$ and $F = \mathbb{Q}$, then $\deg(\mathbb{R}/\mathbb{Q}) = \infty$.

For K a field, K has characteristic n if $n \cdot 1_R = 0_K$ and no smaller value of n satisfies this criterion. If there is no such n, then K has characteristic 0. For example, $\text{char}(\mathbb{Q}) = 0$ and $\text{char}(\mathbb{F}_p) = p$.

Since fields are integral domains, all characteristics must be 0 or prime.

Suppose K has characteristic zero. Then, the map

$$\begin{aligned}
f : Z &\hookrightarrow K \\
n &\mapsto \underbrace{1_K + \cdots + 1_K}_{k \text{ times}} \\
0 &\mapsto 0_K \\
-n &\mapsto \underbrace{-1_K - \cdots - 1_K}_{k \text{ times}} \\
&\vdots
\end{aligned}$$

implying that $\mathbb{Q} \hookrightarrow K$. Thus, if K has characteristic 0, it is automatically an extension field of $\mathbb{Q}$.

If K has characteristic p, then $\mathbb{Z} \xrightarrow{\varphi} K$ with $\ker \varphi \supseteq p\mathbb{Z}$ implies that $\ker \varphi = p\mathbb{Z}$. Thus, $\mathbb{Z}/p\mathbb{Z} \cong \text{im } \varphi$. Every field is an extension of either $\mathbb{Q}$ or $\mathbb{F}_p$.

Polynomial Division Algorithm

Let F be a field, $f(x), g(x) \in F[x]$, $g(x) \neq 0$. Then, there exist unique $q(x), r(x) \in F[x]$ with $r(x) = 0$ or $\deg r(x) < \deg g(x)$ such that $f(x) = g(x)q(x) + r(x)$.

We will use induction on $\deg f$. If $\deg(f) = 0$, then $f \in F$. If $g \notin F$, then $f = g \cdot 0 + f$. If $g \in F$, then $f = g \cdot \frac{f}{g} + 0$.

Assume the result holds for any polynomial with degree less than or equal to $n-1$. Let

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,\, a_n \neq 0\\ g(x) &= b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0,\, b_m \neq 0 \end{aligned}$$

If $m > n$, then $f = g \cdot 0 + f$. Suppose $m \leq n$. Consider the polynomial

$$\tilde{f}(x) = f(x) - \frac{a_n}{b_m}x^{n-m}g(x).$$

Since the leading term of $f(x)$ is $a_n x^n$, and the leading term of $-\frac{a_n}{b_m}x^{n-m}g(x)$ is

$$-\frac{a_n}{b_m}x^{n-m}\left(b_m x^m\right) = -a_n x^n,$$

we can apply the induction hypothesis to $\tilde{f}$, resulting in

$$\tilde{f}(x) = g(x)\tilde{q}(x) + \tilde{r}(x),$$

with $\tilde{q}(x), \tilde{r}(x) \in F[x]$ and $\deg \tilde{r}(x) < \deg g(x)$. Replacing $\tilde{f}(x)$, we find

$$\begin{aligned} f(x) - \frac{a_n}{b_m}x^{n-m}g(x) &= g(x)\tilde{q}(x) + \tilde{r}(x)\\ f(x) &= g(x)\left(\tilde{q}(x) + \frac{a_n}{b_m}x^{n-m}\right) + \tilde{r}(x), \end{aligned}$$

Setting $q(x) = \left(\tilde{q}(x) + \frac{a_n}{b_m}x^{n-m}\right)$ and $r(x) = \tilde{r}(x)$, we see that we have satisfied the existence condition.

Corollary to Polynomial Division: Principal Ideal Domain

Let F be a field. Every ideal in $F[x]$ is principal.

Let $I \subseteq F[x]$ be an ideal. If $a \in I$ for some $a \in F$, then $I = \langle 1_F \rangle = F[x]$. Assume every nonzero element of I has positive degree. Let $\mathcal{I} \in \{n \in \mathbb{Z}_{\geq 1} \mid n = \deg f \text{ for some } f \in I\}$. By the well-ordering principle, $\mathcal{I}$ has a smallest element, n_0. Let $f_0 \in I$ be the polynomial with degree n_0.

We claim that $I = \langle f_0 \rangle$. Let $g(x) \in I$. Write $g(x) = f_0(x)q(x) + r(x)$ with $q(x), r(x) \in F[x]$, $r(x) = 0$ or $\deg r(x) < \deg f(x)$. Since I is an ideal, and $f_0(x), g(x) \in I$, we have $r(x) = g(x) - f_0(x)q(x) \in I$. If $r(x) \neq 0$, then $\deg r(x) < n_0$. Thus $r(x) = 0$ and $f_0(x)|g(x)$.

Irreducible Polynomials

Let $f(x) \in F[x]$. We say $f(x)$ is irreducible if whenever $f(x) = g(x)h(x)$ for some $g(x), h(x) \in F[x]$, then $g(x)$ or $h(x)$ is in F.

Corollary: Irreducible Polynomials and Maximal Ideals

Let $f(x) \in F[x]$. Then, $\langle f(x) \rangle$ is a maximal ideal.

Suppose $\langle f(x) \rangle \subseteq I \subseteq F[x]$. We have $I = \langle g(x) \rangle$ for some $g(x) \in F[x]$ (by the previous result). Since $\langle f(x) \rangle \subseteq \langle g(x) \rangle$, we know $g(x)|f(x)$. In particular, $f(x) = g(x)h(x)$ for some $h(x) \in F[x]$. Since f is irreducible, we must have either $g(x) \in F$ or $h(x) \in F$. If $g(x) \in F$, then $I = F$, and if $g(x) = f(x)h(x)^{-1}$, so $f(x)|g(x)$, and $I = \langle f(x) \rangle$.

Field Extensions for Roots of Irreducible Polynomials

Let $f(x) \in F[x]$ be irreducible. There is a field K containing a root of f and an isomorphic copy of F.

We let $K = F[x]/\langle f(x) \rangle$. Then K is a field since $\langle f(x) \rangle$ is maximal. We have

$$\begin{aligned} \pi : F[x] &\to F[x]/\langle f(x) \rangle\\ g(x) &\mapsto g(x) + \langle f(x) \rangle. \end{aligned}$$

Note that

$$\begin{aligned}\pi|_F : F &\to F[x]/\langle f(x)\rangle\\ a &\mapsto a + \langle f(x)\rangle\end{aligned}$$

meaning $1_F \mapsto 1_F + \langle f(x)\rangle \neq 0 + \langle f(x)\rangle$, and

$$\ker(\pi|_F) = 0.$$

Thus, $\pi|_F$ is an injection, so $F \cong \pi|_F(F)$. Set $\theta = \pi(x) = x + \langle f(x)\rangle$. Then, $f(\theta) = f(x + \langle f(x)\rangle) = f(x) + \langle f(x)\rangle = 0 + \langle f(x)\rangle$, so θ is a root of f in K.

Roots of Irreducible Polynomials

Let $f(x) \in F[x]$ be irreducible with deg $f = n$. Set $K = F[x]/\langle f(x)\rangle$ and $\theta = x + \langle f(x)\rangle \in K$. Then, $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ forms a basis for K as an F-vector space.

Let $g(x) + \langle f(x)\rangle \in K$. Write $g(x) = f(x)q(x) + r(x)$. Then,

$$\begin{aligned}g(\theta) &= f(\theta)q(\theta) + r(\theta)\\ &= r(\theta)\\ &\in \operatorname{span}\{1, \theta, \theta^2, \dots, \theta^{n-1}\}\end{aligned}$$

since $r(x) = 0$ or deg $r(x) < n$.

If $a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} = 0$, then $g(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ satisfies $g(\theta) = 0$, so $f(x)|g(x)$, so $g(x) = 0$ since f is irreducible.

(1) Set $F = \mathbb{R}$, $f(x) = x^2 + 1$. Then, $K = F[x]/\langle x^2 + 1\rangle$, with elements of K looking like $a + b\theta$. Let $a(\theta) = 1 + 3\theta$ and $b(\theta) = 2 - 7\theta$. Note $a(\theta) + b(\theta) = 3 - 4\theta$. However,

$$\begin{aligned}a(\theta)b(\theta) &= (1 + 3\theta)(2 - 7\theta)\\ &= 2 - \theta - 21\theta^2\end{aligned}$$

Notice that $\theta^2 + 1 = f(\theta) = 0$. Therefore, $\theta^2 = -1$.

$$= 23 - \theta$$

In $F[x]$, we have

$$\begin{aligned}a(x)b(x) &= 2 - x - 21x^2\\ &= -21x^2 - x + 2,\end{aligned}$$

and by long division, we have

$$\begin{aligned} &= (-21)(x^2 + 1) + (-x + 23)\\ a(\theta)b(\theta) &= 23 - \theta\end{aligned}$$

Proposition: Irreducibility and Roots

Let $f(x) \in F[x]$. If deg $f(x) = 2$ or 3, then $f(x)$ is irreducible in $K[x]$ for K/F an extension if and only if f does not have a root.

The proof is effectively what has been said.

Proposition: Polynomial over Integers

Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$. If $r/s \in \mathbb{Q}$, $\gcd(r, s) = 1$, and $f(r/s) = 0$, then $r|a_0$ and $s|a_n$. In particular, if f is monic, the only possible roots of f in $\mathbb{Q}$ are roots in $\mathbb{Z}$ that divide a_0.

Suppose $f(r/s) = 0$. Then,

$$\begin{aligned} 0 &= a_n\left(\frac{r}{s}\right)^n + \cdots + a_1\frac{r}{s} + a_0 \\ &= a_nr^n + a_{n-1}r^{n-1}s + \cdots + a_1rs^{n-1} + a_0s^n \\ 0 &= r\left(a_nr^{n-1} + \cdots + a_1s^{n-1}\right) + a_0s^n \end{aligned}$$

Therefore, $r|a_0s^n$, meaning $r|a_0$ (as $\gcd(r, s) = 1$). Similarly,

$$0 = a_nr^n + s\left(a_{n-1}r^{n-1} + \cdots + a_0s^{n-1}\right)$$

so $s|a_nr^n$, meaning $s|a_n$.

Proposition: Irreducible Polynomials over Integral Domains

Let $I \subset R$ with R an integral domain. Let $p(x)$ be a non-constant monic polynomial in $R[x]$. If $\overline{p}(x)$, the image of $p(x)$ in $(R/I)[x]$, cannot be factored into two polynomials of smaller degree in $(R/I)[x]$, then $p(x)$ is irreducible.

Suppose $p(x)$ is reducible. Since p is monic, we can write $p(x) = a(x)b(x)$ with $a(x), b(x)$ monic, irreducible polynomials of smaller degree. But then, $\overline{p}(x) = \overline{a}(x)\overline{b}(x)$, which contradicts $\overline{p}(x)$ as irreducible.

Eisenstein's Criterion

Let R be an integral domain, $\mathcal{P} \in \operatorname{Spec}(R)$, and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be a non-constant polynomial. Suppose $a_0, \dots, a_{n-1} \in \mathcal{P}$, but $a_0 \notin \mathcal{P}^2$. Then, f is irreducible.

Suppose $f(x) = b(x)c(x)$ in $R[x]$ with $b(x), c(x)$ non-constant. We have $x^n = \overline{b(x)c(x)}$, where $\overline{p(x)}$ denotes the image of the coefficients of $p(x)$ in $(R/\mathcal{P})[x]$. The constant terms gives that $b_0c_0 \equiv 0$ modulo $\mathcal{P}$. Since $R/\mathcal{P}$ is an integral domain, $b_0 \in \mathcal{P}$ or $c_0 \in \mathcal{P}$. Assume $b_0 \in \mathcal{P}$.

Now, consider the linear term. This implies $b_0c_1 + b_1c_0 \in \mathcal{P}$. However, $b_0 \in \mathcal{P}$, meaning $b_1c_0 \in \mathcal{P}$. Either $b_1 \in \mathcal{P}$ or $c_0 \in \mathcal{P}$. If $c_0 \in \mathcal{P}$, we have achieved our contradiction. Otherwise, assume $b_1 \in \mathcal{P}$.

In the quadratic term, we have that $b_2c_0 \in \mathcal{P}$, so either $b_2 \in \mathcal{P}$ or $c_0 \in \mathcal{P}$. Continuing the process, we either get that every $b_i \in \mathcal{P}$ or $c_0 \in \mathcal{P}$. If all $b_i \in \mathcal{P}$, then $\overline{b(x)} = x^m$, meaning

$$\begin{aligned} x^n &= x^m\overline{c(x)} \\ &= x^m\left(x^k + \overline{c_{k-1}}x^{k-1} + \cdots + \overline{c_1}x + \overline{c_0}\right) \\ &= x^n + \cdots + x^m\overline{c_0}. \end{aligned}$$

Thus, it must be the case that $c_0 \in \mathcal{P}$, meaning $a_0 = b_0c_0 \in \mathcal{P}^2$.

Gauss's Lemma

Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial. If $f(x)$ is irreducible in $\mathbb{Z}[x]$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Suppose $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbb{Q}[x]$. Set a to be the least common multiple of the denominators of coefficients of g. Similarly, set b to be the least common multiple denominator of coefficients of h.

Consider $abf(x) = G(x)H(x)$, where $G(x) = ag(x)$ and $H(x) = bh(x)$. Notice that $abf(x) = G(x)H(x)$ is an equation in $\mathbb{Z}[x]$. If $ab = 1$, we have a contradiction. Otherwise, let p be a prime such that $p|ab$. In $(\mathbb{Z}/p\mathbb{Z})[x]$, we have

$$0 = \overline{G(x)H(x)}$$

Since $(\mathbb{Z}/p\mathbb{Z})[x]$ is an integral domain, either $\overline{G(x)} = 0$ or $\overline{H(x)}$. Assume without loss of generality that $\overline{G(x)} = 0$. Then, p divides all the coefficients of $G(x)$. Thus,

$$\begin{aligned} abf(x) &= G(x)H(x) && \text{in } \mathbb{Z}[x] \\ \frac{ab}{p}f(x) &= f(x)\frac{1}{p}G(x)H(x) && \text{in } \mathbb{Z}[x]. \end{aligned}$$

We can do this for every prime, such that $f(x) = \tilde{G}(x)\tilde{H}(x)$ in $\mathbb{Z}[x]$.

Example: Applying Eisenstein's Criterion

(1) Let p be prime, with $n \geq 2$ an integer. Consider $f(x) = x^n - p$. We say f is an Eisenstein polynomial with prime p, so f is irreducible over $\mathbb{Z}[x]$. Thus, by Gauss's Lemma, $f(x) = x^n - p$ is irreducible in $\mathbb{Q}[x]$. This shows that $\sqrt[n]{p} \notin \mathbb{Q}$ for any prime p with $n \geq 2$. We can form $K = \mathbb{Q}[x]/\langle x^n - p\rangle$. This is a degree n field extension of $\mathbb{Q}$ that contains an nth root of p.

(2) Let p be prime. Consider the polynomial $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$. This is clearly a polynomial in $\mathbb{Z}[x]$. Note that this can also be written as $\frac{x^p - 1}{x-1}$. This means all roots of $\Phi_p(x)$ must be not equal to 1 but must be equal to 1 when raised to the power p. This polynomial is *not* Eisenstein. However, we can show that it is irreducible.

    Suppose $\Phi_p(x) = g(x)h(x)$ for some $g(x), h(x) \in \mathbb{Z}[x]$. This also gives $\Phi_p(x+1) = g(x+1)h(x+1)$. To show $\Phi_p(x)$ is irreducible, it is enough to show that $\Phi_p(x+1)$ is irreducible.

$$\begin{aligned} \Phi_p(x+1) &= \frac{(x+1)^p - 1}{(x+1-1)} \\ &= \frac{(x+1)^p - 1}{x} \\ &= \frac{1}{x}\left(\sum_{k=0}^{p}\binom{p}{k}x^k - 1\right) \\ &= x^{p-1} + px^{p-1} + \cdots + \frac{p(p-1)}{2}x + p. \end{aligned}$$

    This polynomial does satisfy the Eisenstein criterion, so it is irreducible, meaning $\Phi_p(x)$ is irreducible in $\mathbb{Q}[x]$ (upon application of Gauss's lemma).

    The polynomials $\Phi_p(x)$ are called cyclotomic polynomials. Note that $\mathbb{Q}[x]/\langle\Phi_p(x)\rangle$ is a polynomial of degree $p-1$ and contains a pth root of unity.

(3) Consider the ring $\mathbb{F}_p[t]$. Let $\mathbb{F}_p(t)$ denote the field of rational functions. In $\mathbb{F}_p[t]$, $\langle t\rangle$ is a prime ideal. In the polynomial ring $(\mathbb{F}_p[t])[x]$, the polynomial $f(x) = x^n - t$ is irreducible by the Eisenstein criterion.

    By a more general version of Gauss's lemma, we have $f(x)$ is irreducible in $(\mathbb{F}_p(t))[x]$. So, $(\mathbb{F}_p(t))[x]/\langle x^n - t\rangle$ is a degree n extension in $\mathbb{F}_p(t)$.

    For $n = 2$, elements of $(\mathbb{F}_p(t))[x]/\langle x^2 - t\rangle$ look like $a(t) + b(t)\theta$ where θ is a root of $x^2 - t$.

Simple Field Extensions

Let K/F be an extension of fields. Let $\alpha \in K$. We write $F(\alpha)$ for the smallest field that contains F and α. In other words,

$$F(\alpha) = \bigcap_{\substack{F \subseteq E \\ \alpha \in E}} E.$$

We refer to this as the extension of F by α. More generally, for $\{\alpha_i\}$ with $\alpha_i \in K$,

$$F(\{\alpha_i\}) = \bigcap_{\substack{F \subseteq E \\ \{\alpha_i\} \subseteq E}} E$$

If $K = F(\alpha)$, we say K is a simple extension and α is a primitive element.

Theorem: Constructing a Simple Field Extension

Let F be a field, $p(x) \in F[x]$ irreducible. Let K be an extension of F containing a root α of $p(x)$. Then, $F(\alpha) \cong F[x]/\langle p(x)\rangle$.

Define $\varphi : F[x] \to F(\alpha)$, $f(x) \mapsto f(\alpha)$. Since $f(\alpha)$ contains F and α, it must be the case that φ is a homomorphism. Note that $\varphi(p(x)) = p(\alpha) = 0$. Therefore, $\langle p(x)\rangle \subseteq \ker\varphi$. Since φ is not the zero map, and $p(x)$ is irreducible, $\langle p(x)\rangle = \ker\varphi$, as $\langle p(x)\rangle$ is maximal.

Then, $F[x]/\langle p(x)\rangle \xrightarrow{\psi} F(\alpha)$ is an injection (as it is not the zero map). Thus, $F[x]/\langle p(x)\rangle$ is isomorphic to its image in $F(\alpha)$. Note that $F \subseteq \operatorname{im}(\psi)$, and $\alpha \in \operatorname{im}(\psi)$. Since $\operatorname{im}(\psi)$ is a field that contains both F and α, $\operatorname{im}(\psi) = \alpha$. Thus, $F[x]/\langle p(x)\rangle \cong F(\alpha)$.

Example: Simple Field Extensions

(1) Let $F = \mathbb{Q}$, $p(x) = x^3 - p$. We know that $p(x)$ is irreducible by the Eisenstein criterion. Consider $K = \mathbb{R}$. Then, $\alpha = \sqrt[3]{p}$. We have $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{p}) \subseteq \mathbb{R}$. We know that $\mathbb{Q}(\sqrt[3]{p}) \cong \mathbb{Q}[x]/\langle x^3 - p\rangle$.

However, if $K = \mathbb{C}$, then we have α could be $\sqrt[3]{p}$, $\zeta_3\sqrt[3]{p}$ or $\zeta_3^2\sqrt[3]{p}$, where ζ_3 denotes the cubic roots of unity. Then, we have $\mathbb{Q}(\sqrt[3]{p})$, $\mathbb{Q}(\zeta_3\sqrt[3]{p})$, and $\mathbb{Q}(\zeta_3^2\sqrt[3]{p})$ as separate fields, each isomorphic to $\mathbb{Q}[x]/\langle x^3 - p\rangle$.

Theorem: Isomorphism between Field Extensions

Let F and E be fields, with $\varphi : F \xrightarrow{\simeq} E$. Let $p(x) \in F[x]$ be irreducible, and $q(x)$ be the polynomial created by applying φ to the coefficients of p. Let α be a root of $p(x)$ in some extension K/F, and β a root of $q(x)$ in some extension L/E. There exists an isomorphism $\Phi : F(\alpha) \to E(\alpha)$, with $\alpha \mapsto \beta$ and $\Phi|_F = \varphi$.

We can extend φ to an isomorphism $\tilde{\varphi} : F[x] \to E[x]$. We have $q(x) = \tilde{\varphi}(p(x))$. Since $\tilde{\varphi}$ is an isomorphism, we have $\langle p(x)\rangle$ maximal in $F[x]$, meaning $\langle q(x)\rangle$ is maximal in $E[x]$. In particular, $F[x]/\langle p(x)\rangle \cong E[x]/\langle q(x)\rangle$. Thus, $F(\alpha) \cong E(\alpha)$.

Algebraic and Transcendental Elements

An element $\alpha \in K$ is said to be algebraic over F if there is a polynomial $f(x) \in F[x]$ with $f(\alpha) = 0$. If α is not algebraic, we say α is transcendental over F. We say K/F is an algebraic extension if every element of K is algebraic over F.

(1) $\sqrt{2}$ is algebraic over $\mathbb{Q}$, since $f(\sqrt{2}) = 0$ where $f(x) = x^2 - 2$.

(2) π is transcendental over $\mathbb{Q}$. However, π is algebraic over $\mathbb{R}$, as $f(\pi) = 0$ where $f(x) = x - \pi$.

Proposition: Minimal Polynomials

Let α be algebraic over F. There is a unique monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ such that α is a root. Moreover, $f(x) \in F[x]$ has α as a root if and only if $m_{\alpha,F}(x)|f(x)$.

Let $g(x) \in F[x]$ have α as a root. Assume g has minimum degree among such polynomials. If g is not monic, scale g to be monic. Suppose $g(x) = a(x)b(x)$. Then, $0 = a(\alpha)b(\alpha)$. Then, $a(\alpha) = 0$ or $b(\alpha) = 0$. If $\deg(a(x)), \deg(b(x)) < \deg(g(x))$, then this is a contradiction to g with minimum degree. Thus, g is irreducible.

Suppose $f(x) \in F[x]$ with $f(\alpha) = 0$. We use the division algorithm to write $f(x) = g(x)q(x) + r(x)$ with $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$. Plugging in α, we get $f(\alpha) = g(\alpha)q(\alpha) + r(\alpha) = 0 + r(\alpha)$. Thus, $r(\alpha) = 0$ implies $r(x) = 0$ (or else r would be a polynomial with degree lower than g that has α as a root).

The polynomial $m_{\alpha,F}$ is called the minimal polynomial of α over F. If F is clear from context, we write m_α. We say α has a degree equal to the degree of $m_{\alpha,F}$.

Corollary: Minimal Polynomial over Field Extension

Let L/F be fields. If α is algebraic over L and F, then $m_{\alpha,L}(x) | m_{\alpha,F}(x)$ in $L[x]$.

Since L is an extension of F, $m_{\alpha,F}(x) \in L[x]$. Since $m_{\alpha,F}(\alpha) = 0$, the proposition gives $m_{\alpha,L} | m_{\alpha,F}$.

Corollary: Simple Field Extension of Minimal Polynomial

Let α be algebraic over F. Then, $F(\alpha) \cong F[x]/\langle m_{\alpha,F}(x)\rangle$. Thus, $\deg_F(\alpha) = \deg(m_{\alpha,F}(x)) = \dim_F(F(\alpha))$.

Proposition: Condition for Algebraic over Field

We have $\alpha \in K$ is algebraic over F if and only if $F(\alpha)/F$ is a finite extension. Specifically, if $\dim_F(K) = n$, then $\deg(m_{\alpha,F}(x)) \leq n$ for all $\alpha \in K$. We have $\deg(m_{\alpha,F}(x)) = n$ exactly when $K = F(\alpha)$.

Suppose $\alpha \in K$ is algebraic. Then, we have $F(\alpha) \cong F[x]/\langle m_{\alpha,F}(x)\rangle$, so $\dim_F(F(\alpha)) = \deg(m_{\alpha,F}(x))$.

Suppose $\dim_F(F(\alpha)) = n$. We must have $\{1, \alpha, \alpha^2, \dots, \alpha^n\}$ is linearly dependent. So, there exists $a_0, a_1, \dots, a_n \in F$ with $a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0$. Set $f(x) = a_nx^n + \cdots + a_1x + a_0$. Since $f(\alpha) = 0$, α is algebraic.

(1) Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $F_2 = \mathbb{Q}(\sqrt{2})$, and $F_3 = \mathbb{Q}(\sqrt{3})$. Then,

$$\begin{aligned} m_{\sqrt{2},\mathbb{Q}}(x) &= x^2 - 2 \\ m_{\sqrt{2},F_3}(x) &= x^2 - 2 \\ m_{\sqrt{2},F_2}(x) &= x - \sqrt{2}. \end{aligned}$$

Theorem: Dimensions of Field Extensions

Let $F \subseteq K \subseteq L$ be fields. Then, $\dim_F(L) = \dim_F(K) \cdot \dim_K(L)$.

Let $\{x_1, \dots, x_m\}$ be a basis for L/K, and $\{y_1, \dots, y_n\}$ be a basis for K/F. We claim that $\{x_iy_j\}$ is a basis for L/F.

Let $z \in L$. We can write $z = a_1x_1 + \cdots + a_mx_m$ for $a_i \in K$. For each i, write $a_i = b_{i,1}y_1 + \cdots + b_{i,n}y_n$ for some $b_{i,j} \in F$. Thus,

$$z = \left(\sum_{j=1}^{n} b_{1,j}y_j\right)x_1 + \cdots + \left(\sum_{j=1}^{n} b_{m,j}y_j\right)x_m,$$

meaning $z \in \operatorname{span}_F(\{x_iy_j\})$. Thus, we have $\{x_iy_j\}$ is spanning for L.

To show linear independence, suppose $\exists b_{i,j} \in F$ with

$$\begin{aligned} 0 &= \sum_{i=1}^{m}\sum_{j=1}^{n} b_{i,j}x_iy_j \\ &= \sum_{i=1}^{m}\left(\sum_{j=1}^{n} b_{i,j}y_j\right)x_i. \end{aligned}$$

Since $\{x_i\}$ is linearly independent over K, we must have that for each i,

$$0 = \sum_{j=1}^{n} b_{i,j}y_j.$$

Similarly, since $\{y_j\}$ is linearly independent over F, we must have that $b_{i,j} = 0$ for all i,j. Thus, $\{x_iy_j\}$ is linearly independent.

Thus, we have that for L/F fields, if $F \subseteq K \subseteq L$, then $\dim_F(K) | \dim_F(L)$.

Example: Applying Field Extension Dimensions

(1) Let ζ_{11} be a 11th root of unity with $\zeta_{11} \neq 1$. Therefore, ζ_{11} is a root of $\Phi_{11}(x) = \frac{x^{11}-1}{x-1} = x^{10} + x^9 + \cdots + x + 1$. We used the Eisenstein criterion to show this was an irreducible polynomial. Thus, $Q(\zeta_{11}) \cong \mathbb{Q}[x]/\langle \Phi_{11}(x) \rangle$. We have $m_{\zeta_{11},\mathbb{Q}}(x) = \Phi_{11}(x)$, meaning $\dim_{\mathbb{Q}}(\mathbb{Q}(\zeta_{11})) = 10$, and $\{1, \zeta_{11}, \dots, \zeta_{11}^9\}$ is a basis for $\mathbb{Q}(\zeta_{11})$ over $\mathbb{Q}$.

We claim that $\sqrt[3]{2} \notin \mathbb{Q}(\zeta_{11})$. Set $K = Q(\sqrt[3]{2})$. Then, we know that $m_{\sqrt[3]{2},\mathbb{Q}} = x^3 - 2$ by the Eisenstein criterion, meaning $\dim_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})) = 3$. If $\sqrt[3]{2} \in \mathbb{Q}(\zeta_{11})$, then $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\zeta_{11})$, which would give that $\dim_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})) | \dim_{\mathbb{Q}}(Q(\zeta_{11}))$, but 3 does not divide 10.

Note that this shows $m_{\sqrt[3]{2},\mathbb{Q}}(x) = x^3 - 2$.

(2) Let p be prime. We know that $f(x) = x^n - p$ is irreducible, so $\dim_{\mathbb{Q}}\left(\mathbb{Q}(\sqrt[n]{p})\right) = n$. Let $m|n$. Observe that $\left(\sqrt[n]{p}\right)^{n/m} = \sqrt[m]{p}$. So, $\sqrt[m]{p} \in \mathbb{Q}(\sqrt[n]{p})$. In particular, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[m]{p}) \subseteq \mathbb{Q}(\sqrt[n]{p})$.

Thus, $\dim_{\mathbb{Q}(\sqrt[m]{p})}\mathbb{Q}(\sqrt[n]{p}) = n/m$, and $\deg(m_{\sqrt[n]{p},\mathbb{Q}(\sqrt[m]{p})}) = n/m$. Set

$$f(x) = x^{n/m} - \sqrt[m]{p} \in \mathbb{Q}(\sqrt[m]{p})[x].$$

Then, $f(\sqrt[n]{p}) = 0$, and f is monic with $\deg(f) = n/m$. Thus, $m_{\sqrt[n]{p},\mathbb{Q}(\sqrt[m]{p})} = x^{n/m} - \sqrt[m]{p}$. Moreover, this gives $x^{n/m} - \sqrt[m]{p}$ is irreducible over $\mathbb{Q}(\sqrt[n]{p})$.

Theorem: Generated Field Extensions

The extension K/F is finite if and only if $K = F(\alpha_1, \dots, \alpha_r)$ for some $\alpha_1, \dots, \alpha_r$ algebraic over F. If α_i has degree n_i, then $\dim_F(K) \leq n_1 n_2 \cdots n_r$.

Suppose K/F is finite. Let $\alpha_1, \dots, \alpha_r$ be a basis for K/F, if $\dim_F(K) = r$. Then, $F \subseteq F(\alpha_i) \subseteq K$ for some α_i. Since K/F is finite, and $\dim_F(F(\alpha_i)) \mid \dim_F(K)$, so too must be $F(\alpha_i)/F$. Thus, α_i is algebraic.

Exercise: Show $\dim_F(F(\alpha_1, \dots, \alpha_r)) \leq n_1 n_2 \cdots n_r$. This can be done by inducting on r.

$$\dim_F(F(\alpha_1, \dots, \alpha_r)) = \dim_F(F(\alpha_1))\dim_{F(\alpha_1)}(F(\alpha_1, \dots, \alpha_n))$$
$$\vdots$$

Corollary: Operations on Algebraic Elements

Let α, β be algebraic over F. Then, $\alpha \pm \beta$, $\alpha\beta$, and α/β (provided $\beta \neq 0$) are algebraic over F.

We have that $\alpha \pm \beta$, $\alpha\beta$, and α/β ($\beta \neq 0$) are all elements of $F(\alpha, \beta)$. Since α, β are algebraic over F, $F(\alpha, \beta)/F$ is an algebraic extension.

Corollary: Extending Field Extensions

Let L/F be an extension. Let K be the set of elements algebraic over L. Then, K is a field extension.

Examples: More Field Extensions

(1) Let $L = \mathbb{C}$, $F = \mathbb{Q}$. Let $\overline{\mathbb{Q}} \subseteq \mathbb{C}$ be the subfield containing all complex numbers algebraic over $\mathbb{Q}$. We refer to this as the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. Note that $\sqrt[n]{2} \in \overline{\mathbb{Q}}$ for every n. Thus, we have

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[n]{2}) \subset \overline{\mathbb{Q}}.$$

Thus, we have $\dim_{\mathbb{Q}}(\overline{\mathbb{Q}}) \geq n$ for every $n \in \mathbb{Z}_{\geq 1}$. Thus, $\dim_{\mathbb{Q}}(\overline{\mathbb{Q}}) = \infty$.

Fixing a degree n, if $\alpha \in \overline{\mathbb{Q}}$ has degree n, then $\deg\left(m_{\alpha,\mathbb{Q}}(x)\right) = n$ and $m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Q}[x]$. For each such polynomial, there are n coefficients, each of which has countably many choices (from $\mathbb{Q}$). So, there are countably many elements of degree n. Thus, $\overline{\mathbb{Q}}$ is the countable union of these countable roots of countably many polynomials, so $\overline{\mathbb{Q}}$

is countable.

This means $\mathbb{R} \setminus (\mathbb{R} \cap \overline{\mathbb{Q}})$ is an uncountable set. These are the real transcendental numbers. Similarly, $\mathbb{C} \setminus \overline{\mathbb{Q}}$ is the complex transcendental numbers.

Theorem: Transitivity of Algebraic Extensions

Suppose K/F and L/K are algebraic extensions. Then, L/F is algebraic.

Let $\alpha \in L$. There exists a polynomial $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in K[x]$ such that $f(\alpha) = 0$. Consider $F(\alpha, a_0, \dots, a_n)$. We have that K/F is algebraic. Thus, $E = F(a_0, \dots, a_n)$ is a finite extension of F. Observe that $f(x) \in F(\alpha_0, \dots, \alpha_n)[x]$.

We have $\dim_F(E) = \dim_{F(\alpha_1,\dots,\alpha_n)}(E)\dim_F(F(\alpha_1, \dots, \alpha_n))$. Thus, E/F is finite, so α is algebraic over F. Thus, L/F is algebraic.

Definition: Compositum of Fields

Let K_1, K_2 be subfields of K. The compositum of K_1 and K_2, denoted K_1K_2 is the smallest subfield of K containing both K_1 and K_2.

Proposition: Degree of Compositum Extension

Let K_1 and K_2 be finite extensions of F, and let $K_1, K_2 \subseteq K$ for some field K. Then, $\deg(K_1K_2/F) \leq \deg(K_1/F)\deg(K_2/F)$. We have equality if and only if an F-basis for K_1 or K_2 remains linearly independent over the other field. If $\{x_1, \dots, x_n\}$ is a basis for K_1/F, and $\{y_1, \dots, y_m\}$ is a basis for K_2/F, then $\{x_i y_j\}$ spans K_1K_2/F.

We can see that $K_1K_2 = F(x_1, \dots, x_n, y_1, \dots, y_m)$. Since we know that $\{x_1, \dots, x_n\}$ is a basis for K_1/F, $x_j^k \in K_1$ can be written as $\sum a_i x_i$ for $a_i \in F$. Similarly, $y_j^k \in K_2$ can be written as $\sum b_i y_i$ for $b_i \in F$.

If we consider sums of the form $\sum a_{i,j} x_i y_j$, these sums are closed under addition and multiplication. Thus, $\{x_i y_j\}$ spans K_1K_2. This gives $\dim_F(K_1K_2) \leq \dim_F(K_1)\dim_{K_2}$. To find equality, we have

$$\begin{aligned} K_1K_2 &= F(x_1, \dots, x_n, y_1, \dots, y_m) \\ &= K_1(y_1, \dots, y_m), \end{aligned}$$

so $\{y_1, \dots, y_m\}$ spans K_1K_2 over K_1. Thus, $\dim_{K_1}(K_1K_2) \leq \dim_F(K_2)$, with equality if and only if $\{y_1, \dots, y_m\}$ is linearly independent over K_1. Thus,

$$\begin{aligned} \dim_F(K_1K_2) &= \dim_{K_1}(K_1K_2)\dim_F(K_1) \\ &= \dim_F(K_2)\dim_F(K_1) \end{aligned}$$

if and only if $\{y_1, \dots, y_m\}$ is linearly independent over K_1.

$$\begin{tikzcd}
 & K & \\
 & K_1K_2 \arrow[u, dash] & \\
K_1 \arrow[ur, dash, "\leq m"] & & K_2 \arrow[ul, dash, "\leq n"'] \\
 & F \arrow[ul, dash, "n"] \arrow[ur, dash, "m"'] &
\end{tikzcd}$$

Corollary: More Degree of Compositum Extensions

Let K_1, K_2 be finite extensions of F with $\dim_F(K_1) = n$ and $\dim_{K_2}(F) = m$. If $\gcd(m, n) = 1$, then $\dim_F(K_1K_2) = \dim_{K_1}(F)\dim_{K_2}(F)$.

We always have $\dim_F(K_1K_2) \leq \dim_{K_2}(F)\dim_{K_1}(F)$, and $F \subseteq K_1 \subseteq K_1K_2$, so $\dim_F(K_1)|\dim_F(K_1K_2)$, and similarly $\dim_F(K_2)|\dim_F(K_1K_2)$, so $\text{lcm}(m, n)|\dim_F(K_1K_2)$, so $mn|\dim_F(K_1K_2)$. Thus, $\dim_F(K_1K_2) = mn$.

Examples: Compositum Field Extensions

(1) Consider $K_1 = \mathbb{Q}(i)$ and $K_2 = \mathbb{Q}(\sqrt[3]{2})$. We know that $\dim_{\mathbb{Q}}(\mathbb{Q}(i)) = 2$, and $\dim_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})) = 3$. Thus, $[\mathbb{Q}(i)\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 6$ (where $[K : F] = \dim_F(K)$) with basis $\{1, i, \sqrt[3]{2}, \sqrt[3]{4}, i\sqrt[3]{2}, i\sqrt[3]{4}\}$. Moreover, $\mathbb{Q}(i, \sqrt[3]{2})$ contains $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt[3]{2})$, so it contains $\mathbb{Q}(i)\mathbb{Q}(\sqrt[3]{2})$, and since $i\sqrt[3]{2} \in \mathbb{Q}(i)\mathbb{Q}(\sqrt[3]{2})$, we have $\mathbb{Q}(i, \sqrt[3]{2}) \subseteq \mathbb{Q}(i)\mathbb{Q}(\sqrt[3]{2})$, meaning $\mathbb{Q}(i, \sqrt[3]{2}) = \mathbb{Q}(i)\mathbb{Q}(\sqrt[3]{2})$.

(2) Consider $K_1 = \mathbb{Q}(i)$ and $K_2 = \mathbb{Q}(\zeta_8)$, with $\zeta_8 = e^{2\pi i/8} = e^{\pi i/4}$. Therefore, $\zeta_8 = \sqrt{i}$. Let $f(x) = x^4 + 1$. Then, $f(\zeta_8) = 0$, and f is irreducible (examine $f(x+1)$ and find it is Eisenstein). Thus, $[Q(\zeta_8) : \mathbb{Q}] = 4$. The compositum $[\mathbb{Q}(i)\mathbb{Q}(\zeta_8) : \mathbb{Q}] \leq 8$, but since $\mathbb{Q} \subseteq \mathbb{Q}(i) \subseteq \mathbb{Q}(\zeta_8)$, so we do not have equality. Thus, $\mathbb{Q}(i)\mathbb{Q}(\zeta_8) = \mathbb{Q}(\zeta_8)$, so $[\mathbb{Q}(\zeta_8)\mathbb{Q}(i) : \mathbb{Q}] = 4$.

Classic Geometry Problems

We are going to be examining straightedge and compass constructions and the classic Greek problems in them.

(1) Doubling the cube: can we construct a cube with double the volume of a given cube?

(2) Trisecting an angle: given an angle, are we able to construct an angle 1/3 the size?

(3) Squaring the circle; can we construct a square with precisely the area of a given circle?

Start with a fixed distance, call this 1. We say a number is constructible if we can construct its length. We say a point $(x, y) \in \mathbb{R}^2$ is constructible if we can construct x and y.

The set of numbers in $\mathbb{R}$, along with their negatives, that can be constructed are called the constructible numbers. The following operations can be performed with compass and straightedge:

(1) We can connect any two points with a line.

(2) We can find a point of intersection of two lines.

(3) We can draw a circle with a given center and radius.

(4) We can find the intersection of a line with a circle, or an intersection between two circles.

Suppose a and b are constructible. Then, $a + b$ is constructible. Similarly, $a - b$ is constructible.

To construct ab, take a segment with length a, mark off 1 on said segment, and draw a segment with length b at an angle to the segment with length a. Draw a segment from the endpoint of b to the endpoint of 1, then one parallel to this segment at the endpoint of a. The intersection of the line with length b and this parallel line is a segment of length ab.

To construct a/b, mark off 1 from a segment of length b. Construct a segment of length a at an angle from the segment of length b. Draw a segment from the endpoint of b to the endpoint of a. The segment parallel to this one starting from 1 intersecting at a is of length a/b.

Thus, the set of constructible numbers is a subfield of $\mathbb{R}$. We see that we can construct $\mathbb{Q}$, but what else is constructible?

If a is constructible, then so too is $\sqrt{a}$. We form a circle of diameter $1 + a$ by appending a segment of length 1 to a segment of length a. We take the perpendicular at the endpoint of the segment of radius 1 inside the circle, intersecting the circle. The segment from the intersection of the circle to the diameter line is of length $\sqrt{a}$.

Therefore, $\sqrt{2}$ is constructible, and so the field of constructible numbers properly contains $\mathbb{Q}$.

Field of Constructible Numbers

We claim that addition, multiplication, subtraction, division, and square roots are the extent of the constructible numbers.

Note that we are allowed to intersect lines. A line defined over a field F is $ax + by - c = 0$ for $a, b, c \in F$. We see that intersecting two such lines gives another element of the field.

For an intersection between a line and a circle, we have that $(x-h)^2+(y-k)^2=r^2$ for $h,k,r\in F$ is the expression of a circle, and $ax+by-c=0$ with $a,b,c\in F$ is the line. Then, we have

$$x=\frac{c-by}{a}$$
$$\left(\frac{c-by}{a}-h\right)^2+(y-k)^2=r^2$$

is a quadratic equation in y and coefficients in F. The quadratic formula allows us to take square roots of elements in F, but nothing else.

For the intersection of two circles, we have $(x-h_1)^2+(y-k_1)^2=r_1^2$ and $(x-h_2)^2+(y-k_2)^2=r_2^2$. If we subtract the second equation from the first equation, we have

$$2(h_2-h_1)x+2(k_2-k_1)y=r_1^2-h_1^2-k_1^2-r_2^2+h_2^2+k_2^2.$$

Specifically, we see that this equation describes a line. Therefore, the intersection of the first equation and the second equation reduces to the intersection of the first equation and the above equation, meaning that we effectively are taking the intersection of a line with a circle, so we can take at most square roots.

Theorem: Degree of Constructible Numbers

Let $\alpha\in\mathbb{R}$ with α constructible. Then, $[\mathbb{Q}(\alpha):\mathbb{Q}]=2^k$ for some $k\in\mathbb{Z}_{\geq 0}$.

Theorem: Solution of the Greek Problems

We claim that none of the Greek problems are solvable by compass and straightedge.

(1) In order to double the cube, we would need to construct $\sqrt[3]{2}$ — however, $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3\neq 2^k$.

(2) Suppose θ can be constructed. Then, we can construct $\cos\theta$ and $\sin\theta$. Similarly, if we can construct $\cos\theta$ and $\sin\theta$, then we can construct θ. Constructing $\theta/3$ is equal to constructing $\cos(\theta/3)$. Let $\theta=\pi/3$. Then, $\cos\theta=1/2$. Using the triple angle formula, we find $\cos\theta=4\cos^3(\theta/3)-3\cos(\theta/3)$. When $\theta=\pi/3$, we set $\alpha=\cos(\pi/9)$. We find that $1/2=4\alpha^3-3\alpha$. In other words, $8\alpha^3-6\alpha-1=0$. Setting $\beta=2\alpha$, this is equal to finding $\beta^3-3\beta-1=0$, which is irreducible over $\mathbb{Q}$. Thus, $[\mathbb{Q}(\beta):\mathbb{Q}]=[\mathbb{Q}(\alpha):\mathbb{Q}]=3$.

(3) Constructing a circle of area π would involve constructing $\sqrt{\pi}$, but $[\mathbb{Q}(\sqrt{\pi}):\mathbb{Q}]=\infty$.

Splitting Field

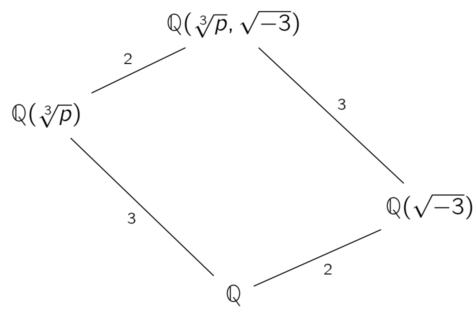
Let $f(x)\in F[x]$. We know there exists K/F so that f has a root in K. We have $f(x)=(x-\alpha)g(x)$ for some $g(x)\in K[x]$. We say K is a splitting field for f if $f(x)$ factors completely into linear factors over $K[x]$, and there is no smaller field than K for which this is true.

- Let $f(x)=x^2+1\in\mathbb{Q}[x]$. We know that $f(x)=(x-i)(x+i)$. Our splitting field, $\text{Spl}(f(x))=\mathbb{Q}(i)$.

- Consider $f(x)=x^3-p\in\mathbb{Q}[x]$ with p prime. We know that $\sqrt[3]{p}$ is a root of $f(x)$. Considering the field $\mathbb{Q}(\sqrt[3]{p})A$, we see that f does not split over $\mathbb{Q}(\sqrt[3]{p})$. The roots of f are $\sqrt[3]{p}$, $\zeta_3\sqrt[3]{p}$, and $\zeta_3^2\sqrt[3]{p}$, where $\zeta_3=e^{2\pi i/3}$.

  Assume $\text{Spl}(f(x))$ exists. If $\text{Spl}(f(x))$ exists, then $\sqrt[3]{p},\zeta_3\sqrt[3]{p},\zeta_3^2\sqrt[3]{p}\in\text{Spl}(f(x))$. Similarly, we get $\zeta_3=\frac{\zeta_3\sqrt[3]{p}}{\sqrt[3]{p}}\in\text{Spl}(f(x))$. We have that $\zeta_3=-1/2+\sqrt{-3}/2\in\text{Spl}(f(x))$. So, $\sqrt{-3}\in\text{Spl}(f(x))$.

  Thus, $\mathbb{Q}(\sqrt[3]{p},\sqrt{-3})\subseteq\text{Spl}(f(x))$. Similarly, we know that $\text{Spl}(f(x))\subseteq\mathbb{Q}(\sqrt[3]{p},\sqrt{-3})$. Thus, $\text{Spl}(f(x))=\mathbb{Q}(\sqrt[3]{p},\sqrt{-3})$.



Theorem: Splitting Field Existence

Let F be a field, $f(x) \in F[x]$. Then, a splitting field for $f(x)$ exists.

We use induction on the degree of $f(x)$. If f is of degree 1, then $\operatorname{Spl}_F(f(x)) = F$.

Assume the result holds for for all polynomials of degree $\leq n-1$. Given $f(x) \in F[x]$ with degree n, construct K/F with $\alpha \in K$ so that $f(\alpha) = 0$. We can write $f(x) = (x-\alpha)g(x)$ for some $g(x) \in K[x]$. We know that $\deg(g) = n-1$. Applying the induction hypothesis to g, we construct $\operatorname{Spl}_K(g(x))$. Note that this is the smallest extension of K that has all the roots of g. Since $K = F(\alpha) \subseteq \operatorname{Spl}_K(g(x))$, we know that all the roots of f are contained in $\operatorname{Spl}_K(g(x))$.

Suppose we have $L \subset \operatorname{Spl}_K(g(x))$ and L contains all the roots of $f(x)$. Since L contains all the roots of f, $F(\alpha) \subseteq L$. If L contains all the rest of the roots of f (i.e., the roots of g), then L is not a proper subfield of $\operatorname{Spl}_K(g(x))$. So, we must have $\operatorname{Spl}_F(f(x)) = \operatorname{Spl}_K(g(x))$.

Corollary: Degree of Splitting Field

Let $f(x) \in F[x]$ with $\deg(f) = n$. Then, $[\operatorname{Spl}_F(f(x)) : F] \leq n!$.

Write $f(x) = (x-\alpha_1)^{k_1} g_1(x)$. Then, we have $[F(\alpha_1) : F] \leq n$. We have g has degree $n - k_1$, and $f(x) = (x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2} g_2(x)$, with $[F(\alpha_1, \alpha_2) : F] = [F(\alpha_1, \alpha_2) : F(\alpha_1)][F(\alpha_1) : F] \leq n(n-1)$. Going down the line, we find that $[\operatorname{Spl}_F(f(x)) : F] \leq n!$.

Multiple Roots over Splitting Field

Let $f(x) \in F[x]$. Write $f(x) = (x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2} \cdots (x-\alpha_m)^{n_m}$ over $\operatorname{Spl}_F(f)$ with α_i distinct and $n_i \geq 1$. If $n_i \geq 2$, we say α_i is a multiple root, and n_i is the multiplicity of α_i. If $n_i = 1$, we say α_i is a simple root.

We say f is separable if f has no multiple roots. If f is not separable, we say f is inseparable.

(1) $f(x) = x^4 - 1 \in \mathbb{Q}[x]$ factors into $f(x) = (x-1)(x+1)(x-i)(x+i)$, meaning f is separable.

(2) Consider $f(x) = x^2 - t \in \mathbb{F}_2(t)[x]$. This polynomial is irreducible. However, it is not separable. We see that $f(x) = (x - \sqrt{t})(x + \sqrt{t}) = (x + \sqrt{t})^2$.

Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$. Define $D_x f(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + a_1$. We define this to be the formal derivative of $f(x)$. We can verify that D_x holds all the properties that we assume of derivatives.

Proposition: Existence of Multiple Roots

A polynomial $f(x)$ has a multiple root α if $(D_x f)(\alpha) = 0$. In particular, f is separable if and only if $\gcd(f(x), D_x f(x)) = 1$.

Suppose f has a multiple root. Write $f(x) = (x-\alpha)^n g(x)$ with $n \geq 2$. Then,

$$D_x f(x) = n(x-\alpha)^{n-1} g(x) + (x-\alpha)^n D_x g(x),$$

and since $n - 1 > 0$, we have

$$(D_x f)(\alpha) = 0.$$

Suppose $(D_x f)(\alpha) = 0$. We write $f(x) = (x-\alpha)g(x)$. Then, $D_x f(x) = g(x) + (x-\alpha)D_x g(x)$. So, $(D_x f)(\alpha) = 0 = g(\alpha)$, so $g(\alpha) = 0$, meaning $(x-\alpha)|g(x)$, so $(x-\alpha)^2|f(x)$.

(1) Let $f(x) = x^n - 1 \in F[x]$. We see that $D_x f(x) = nx^{n-1}$. If $\text{char}(F)$ does not divide n, or $\text{char}(F) = 0$, then the only root of $D_x f(x)$ is 0, meaning f is separable.

    In this case, there are n distinct nth roots of unity in $\text{Spl}_F(f(x))$.

(2) Let $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$. Note $D_x f(x) = p^n x^{p^n - 1} - 1 = -1$. Since $D_x f(x) \neq 0$ for all x, f is separable.

Irreducible Polynomials over Characteristic 0 Fields

If $f(x) \in F[x]$ is irreducible and $\text{char}(F) = 0$, then f is separable.

Suppose f has degree n. Then, $D_x f(x)$ has degree $n-1$. Since f is irreducible, $\gcd(f, D_x f) = 1$.

(1) Considering $f(x) = x^n - 1 \in \mathbb{Q}[x]$. We know that this has roots given by $1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}$, with $\zeta_n = e^{2\pi i/n}$.

    If K is any field that contains these roots, then $\{1, \zeta_n, \dots, \zeta_n^{n-1}\}$ forms a cyclic group of order n generated by ζ_n. We denote this as μ_n. If ζ_n^a generates μ_n for some a, we say ζ_n^a is a primitive nth root of unity. There are $\phi(n)$ (totient function) primitive nth roots of unity.

    We see that $\text{Spl}_{\mathbb{Q}}(x^n - 1) = \mathbb{Q}(\zeta_n)$. Our next question is to find $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$.

    If $n = p$, we can see that $m_{\zeta_p, \mathbb{Q}}(x) = \frac{x^n - 1}{x - 1} = x^{p-1} + \cdots + x + 1$, so $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$.

    Define the nth cyclotomic polynomial

$$\begin{aligned}\Phi_n(x) &= \prod_{\substack{\zeta \in \mu \\ \zeta \text{ primitive}}} (x - \zeta) \\ &= \prod_{\substack{1 \leq a < n \\ \gcd(a,n)=1}} (x - \zeta_n^a).\end{aligned}$$

    This polynomial has degree $\phi(n)$. We have that

$$\begin{aligned}x^n - 1 &= \prod_{\zeta \in \mu_n} (x - \zeta) \\ &= \prod_{d|n} \prod_{\substack{\zeta \in \mu_d \\ \zeta \text{ primitive}}} (x - \zeta) \\ &= \prod_{d|n} \Phi_d(x).\end{aligned}$$

    We can use this to compute $\Phi_n(x)$. For example, if $n = 4$, we have

$$\begin{aligned}x^4 - 1 &= \Phi_1(x)\Phi_2(x)\Phi_4(x) \\ &= (x-1)(x+1)\Phi_4(x)\end{aligned}$$

    meaning

$$\Phi_4(x) = x^2 + 1.$$

Lemma: Properties of $\Phi_n(x)$

For all $n \geq 1$, $\Phi_n(x)$ is monic, and lies in $\mathbb{Z}[x]$.

The proof that $\Phi_n(x)$ is monic by its definition. To show $\Phi_n(x) \in \mathbb{Z}[x]$, we use induction on n.

Base case is done. Assume $\Phi_d(x) \in \mathbb{Z}[x]$ for all $1 \leq d < n$. We have

$$\begin{aligned} x^n - 1 &= \prod_{d|n} \Phi_d(x) \\ &= \Phi_n(x) f(x), \end{aligned}$$

where

$$f(x) = \prod_{\substack{d|n \\ d<n}} \Phi_d(x) \in \mathbb{Z}[x] \qquad \text{by the induction hypothesis.}$$

Therefore, $f(x)|x^n - 1$ in $\mathbb{Q}(\zeta_n)[x]$. However, $f(x), x^n - 1 \in \mathbb{Z}[x]$ gives that the division is over $\mathbb{Q}[x]$ by the division algorithm. Applying Gauss's lemma, we find that the divisibility is over $\mathbb{Z}[x]$, meaning $\Phi_n(x) \in \mathbb{Z}[x]$.

Theorem: Irreducibility of Cyclotomic Polynomial

The polynomial $\Phi_n(x)$ is irreducible over $\mathbb{Z}[x]$.

Suppose toward contradiction that $\Phi_n(x) = f(x)g(x)$ for some $f(x), g(x) \in \mathbb{Z}[x]$ and $f(x)$ irreducible. Let ζ be a primitive nth root of unity. We can assume $f(\zeta) = 0$. Let p be a prime with p not dividing n. Then, ζ^p is a primitive nth root of unity. In particular, ζ^p is a root of $f(x)$ or $g(x)$, since $\Phi_n(\zeta^p) = 0$.

Suppose ζ^p is a root of g. Then, ζ is a root of $g(x^p)$ Since f is the minimal polynomial of ζ, $f(x)|g(x^p)$ We can write $g(x^p) = f(x)h(x)$ for some $h(x) \in \mathbb{Z}[x]$.

Reducing the equation modulo p, we have $\overline{g(x^p)} = \overline{f(x)h(x)}$ in $\mathbb{F}_p$, and $\overline{g(x^p)} = \overline{g(x)}^p$, meaning $\overline{g(x)}^p = \overline{f(x)h(x)}$ in $\mathbb{F}_p[x]$. Since $\mathbb{F}_p[x]$ is a unique factorization domain, $\overline{f(x)}$ and $\overline{g(x)}$ share a factor.

Going back to $\Phi_n(x) = f(x)g(x)$, and reducing modulo p, we have $\overline{\Phi_n(x)} = \overline{f(x)g(x)}$. Since $\overline{f(x)}$ and $\overline{g(x)}$ share a factor, they must share a root in the compositum of their splitting fields over $\mathbb{F}_p$. Thus, $\overline{\Phi_n(x)}$ has a multiple root in $K/\mathbb{F}_p$; in particular, $\overline{x^n - 1}$ has a multiple root in some extension of $K/\mathbb{F}_p$ for K a sufficiently large field.

However, we had seen earlier that $\overline{x^n - 1}$ has a multiple root only if $p|n$, which is a contradiction. This contradiction shows that we ζ^p is a root of g if p does not divide n. So, every ζ^p with p not dividing n is a root of f, meaning all the roots of Φ_n are roots of f, so $\Phi_n(x) = f(x)$. Since $f(x)$ was irreducible by assumption, thus too is $\Phi_n(x)$.

Thus, $\Phi_n(x)$ is the minimal polynomial of ζ_n over $\mathbb{Q}$, so $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.

Example: Cyclotomic Polynomials

Consider p and q primes, with $f(x) = x^p - q \in \mathbb{Q}[x]$. By Eisenstein, $f(x)$ is irreducible. We see that $\sqrt[p]{q}$ is a root, as well as $\zeta_p \sqrt[p]{q}, \dots, \zeta_p^{p-1} \sqrt[p]{q}$.

We can see that $\mathbb{Q}(\zeta_p, \sqrt[p]{q}) \subseteq \operatorname{Spl}_{\mathbb{Q}}(f(x))$. Similarly, $\operatorname{Spl}_{\mathbb{Q}}(f(x)) \subseteq \mathbb{Q}(\zeta_p, \sqrt[p]{q})$ contains all the roots of $f(x)$.

$$\begin{tikzcd}
& \mathbb{Q}(\zeta_p, \sqrt[p]{q}) \arrow[dl, dash, "p-1"'] \arrow[dr, dash, "p"] & \\
\mathbb{Q}(\sqrt[p]{q}) \arrow[dr, dash, "p"'] & & \mathbb{Q}(\zeta_p) \arrow[dl, dash, "p-1"] \\
& \mathbb{Q} &
\end{tikzcd}$$

Theorem: Uniqueness of Splitting Field

Let $\varphi : F \to \tilde{F}$ be an isomorphism. Let $f(x) \in F[x]$, and $\tilde{f}(x) \in \tilde{F}[x]$ under natural extension of φ to $F[x] \to \tilde{F}[x]$. Let $E = \text{Spl}_F(f(x))$ and $\tilde{E} = \text{Spl}_{\tilde{F}}(\tilde{f}(x))$. Then, φ extends to an isomorphism $\Phi : E \to \tilde{E}$ such that the following diagram commutes.

$$\begin{tikzcd} E \arrow[r, "\Phi"] \arrow[d, dash] & \tilde{E} \arrow[d, dash] \\ F \arrow[r, "\varphi"] & \tilde{F} \end{tikzcd}$$

In particular, $\varphi = \text{id}$ shows the splitting field is unique up to isomorphism.

We will use induction on the degree of f to prove this. Since $\varphi : F \to \tilde{F}$ is an isomorphism, $\varphi : F[x] \to \tilde{F}[x]$ is an isomorphism. Thus, $f(x)$ and $\tilde{f}(x)$ have corresponding factorizations.

In the base case, with $\deg(f) = 1$, then F is the splitting field of f, meaning $\tilde{f}$ has degree 1, so $\tilde{F} = \text{Spl}_{\tilde{F}}(\tilde{f}(x))$, so φ gives the isomorphism.

Assume the result is true for any K, isomorphism ψ, and polynomial $g(x)$ with $\deg(g(x)) < n$.Let $f(x) \in F[x]$ have degree $n \geq 1$. Let $p(x)$ be an irreducible factor of $f(x)$. We can assume $\deg(p(x)) \geq 2$. If $f(x) = (x - \alpha)^n$, then $\tilde{f}(x) = (x - \beta)^n$, meaning $\text{Spl}_F(f(x)) = F$ and $\text{Spl}_{\tilde{F}}(\tilde{f}(x)) = \tilde{F}$, and we are done.

Let α be a root of $p(x)$. Let β be a corresponding root of $\tilde{p}(x)$. We have that the following diagram commutes.

$$\begin{tikzcd} F(\alpha) \arrow[r, "\varphi'"] \arrow[d, dash] & \tilde{F}(\beta) \arrow[d, dash] \\ F \arrow[r] & \tilde{F} \end{tikzcd}$$

Let $F_1 = F(\alpha)$ and $\tilde{F}_1 = \tilde{F}(\beta)$, and $\varphi_1 = \varphi'$. We have $f(x) = (x - \alpha)f_1(x)$ in $F_1[x]$, and $\tilde{f}(x) = (x - \beta)\tilde{f}_1(x)$ in $\tilde{F}_1[x]$. We have that $\deg(f_1(x)) = \deg(\tilde{f}(x)) = n - 1$.

We have $E = \text{Spl}_{F_1}(f_1(x))$. Note that E contains all the roots of $f(x)$; in particular, it contains $F_1 = F(\alpha)$ and the roots of $f_1(x)$ as $f_1(x)|f(x)$. Suppose there were a smaller field extension of F_1 that contains all the roots of $f_1(x)$. Then, this is an extension of F that contains all the roots of f, so it would contain E. Similarly, for $\tilde{E}$, we have that $\tilde{E} = \text{Spl}_{\tilde{F}_1}(\tilde{f}_1(x))$.

$$\begin{tikzcd} \text{Spl}_{F_1}(f_1(x)) \arrow[r, "\Phi"] \arrow[d, dash] & \text{Spl}_{\tilde{F}_1}(\tilde{f}_1(x)) \arrow[d, dash] \\ F_1 \arrow[r, "\varphi_1"] \arrow[d, dash] & \tilde{F}_1 \arrow[d, dash] \\ F \arrow[r, "\varphi"] & \tilde{F} \end{tikzcd}$$

Thus, we have that splitting fields are unique up to isomorphism.

Separability in Finite Fields

Recall that $f(x) \in F[x]$ is separable if it has no repeated roots. Additionally, if $f(x)$ is irreducible and $\text{char}(F) = 0$, then f is separable, and if $\text{char}(F) = p$, it is possible for f to be irreducible and inseparable (such as $f(x) = x^2 - t \in \mathbb{F}_2(t)[x]$).

Let $\text{char}(F) = p$. The Frobenius map, given by $\text{Frob}_p : F \to F$, $\alpha \to \alpha^p$. We claim that Frob_p is an injective homomorphism. If F is finite, then Frob_p is an automorphism.

Let $a, b \in F$. Write $\varphi_p = \text{Frob}_p$. We have

$$\begin{aligned} \varphi_p(ab) &= (ab)^p \\ &= a^p b^p \\ &= \varphi_p(a)\varphi_p(b), \end{aligned}$$

and

$$\begin{aligned}\varphi_p(a+b) &= (a+b)^p\\ &= \sum_{k=0}^{p}\binom{p}{k}a^k b^{p-k}\\ &= a^p + b^p + \sum_{k=1}^{p-1}\binom{p}{k}a^k b^{p-k}\\ &= a^p + b^p.\end{aligned}$$

Thus, it is a homomorphism. To show injectivity, we know that $\ker\varphi_p$ is an ideal in F. Thus, $\ker\varphi_p = \{0\}$ or $\ker\varphi_p = F$. Since $\varphi_p(1) \neq 0$, it must be the case that $\ker\varphi_p = \{0\}$, meaning φ_p is injective.

Let F be a field with $\text{char}(F) = p$. If every element of F can be written as x^p for some x, then we say F is a perfect field. We also say characteristic 0 fields are perfect.

Irreducible Polynomials over Perfect Field

Every irreducible polynomial over a perfect field is separable.

We have shown this to be the case in a characteristic 0 field. We will restrict ourselves to $\text{char}(F) = p$. Assume that F is perfect. Let $f(x) \in F[x]$ be irreducible and inseparable (i.e., f has a multiple root).

If $D_x f(x) \neq 0$, then $f(x)$ and $D_x f(x)$ must be relatively prime because f is irreducible. This would contradict f being inseparable. We have that $D_x f(x) = 0$, meaning p divides the exponent of every term in $f(x)$. Thus, we can write $f(x) = g(x^p)$ for some $g(x)$. Set $g(x) = a_n x^n + \cdots + a_1 x + a_0$. Since $F^p = F$, we can write $a_j = c_j^p$ for some $c_j \in F$. Thus,

$$\begin{aligned}f(x) &= c_n^p x^{p^n} + \cdots + c_1^p x^p + c_0^p\\ &= (c_n x^n + \cdots + c_1 x + c_0)^p,\end{aligned}$$

which contradicts f being irreducible.

Corollary: Order of Finite Fields

For any $n > 0$ and prime p, there exists a unique field up to isomorphism with order p^n. We denote this field as $\mathbb{F}_{p^n}$.

Let $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$. We have that $D_x f(x) = p^n x^{p^n - 1} - 1 = -1$. Therefore, $\gcd(f(x), D_x f(x)) = 1$, so f is separable. Therefore, there are p^n distinct roots of f.

Let $\mathbb{F}$ be the roots of $f(x)$ inside $\text{Spl}_{\mathbb{F}_p}(f(x))$. Then, $\alpha \in \mathbb{F}$ if and only if $f(\alpha) = 0$, meaning $\alpha^{p^n} = \alpha$. Let $\alpha, \beta \in \mathbb{F}$. We have $\alpha\beta^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$, so $\alpha\beta \in \mathbb{F}$. Additionally, $\left(\alpha^{-1}\right)^{p^n} = \left(\alpha^{p^n}\right)^{-1} = \alpha^{-1}$, so $\alpha^{-1} \in \mathbb{F}$, and $(\alpha \pm \beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n} = \alpha \pm \beta$.

Thus, $\mathbb{F} \subseteq \text{Spl}_{\mathbb{F}_p}(f(x))$ is a subfield, and $\mathbb{F}$ contains all the roots of $f(x)$, so $\mathbb{F} = \text{Spl}_{\mathbb{F}_p}(f(x))$. So we get for any n a field $\mathbb{F}/\mathbb{F}_p$ of order p^n.

Let $\mathbb{F}$ be any field of order p^n. Specifically, $[\mathbb{F} : \mathbb{F}_p] = n$. If $\mathbb{F}$ has order p^n, then $\mathbb{F}^\times$ is cyclic with order $p^n - 1$. So, any element $\alpha \in \mathbb{F}^\times$ satisfies $\alpha^{p^n - 1} = 1$, meaning $\alpha^{p^n} = \alpha$, meaning every element of $\mathbb{F}$ is a root of $f(x) = x^{p^n} - x$. Thus, $\mathbb{F} = \text{Spl}_{\mathbb{F}_p}\left(x^{p^n} - x\right)$, since $\mathbb{F} \subseteq \text{Spl}_{\mathbb{F}_p}\left(x^{p^n} - x\right)$ and they both have size p^n.

Galois Theory

Automorphisms

Let K be a field. We have $\text{Aut}(K)$ is the collection of automorphisms of K. We have that $\text{Aut}(K)$ is a group.

Given $\sigma \in \text{Aut}(K)$, we say σ fixes $x \in K$ if $\sigma(x) = x$. Given $F \subseteq K$, we say F is fixed by σ if $\forall x \in F$, $\sigma(x) = x$. The automorphisms of K that fix F is denoted $\text{Aut}(K/F)$. We can show that $\text{Aut}(K/F)$ is a subgroup.

Proposition: Automorphism of Algebraic Extensions

Let K/F be an extension of fields, $\alpha \in K$ algebraic over F, with $m_{\alpha,F}(x)$ the minimal polynomial. Given $\sigma \in \operatorname{Aut}(K/F)$, $\sigma(\alpha)$ is a root of $m_{\alpha,F}(x)$ (i.e., $\operatorname{Aut}(K/F)$ permutes the roots of $m_{\alpha,F}(x)$).

Let $\sigma \in \operatorname{Aut}(K/F)$. Write $m_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in F[x]$. Thus,

$$\begin{aligned} m_\alpha(\sigma(\alpha)) &= (\sigma(\alpha))^n + a_{n-1}(\sigma(\alpha))^{n-1} + \cdots + a_1\sigma(\alpha) + a_0 \\ &= (\sigma(\alpha))^n + \sigma(a_{n-1})(\sigma(\alpha))^{n-1} + \cdots + \sigma(a_1)\sigma(\alpha) + \sigma(a_0) \\ &= \sigma\left(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0\right) \\ &= \sigma(m_\alpha(\alpha)) \\ &= \sigma(0) \\ &= 0. \end{aligned}$$

Examples: Automorphisms of Algebraic Extensions

(1) Let p be a prime, $f(x) = x^2 - p$. Then, we know $K = \mathbb{Q}(\sqrt{p}) = \mathbb{Q}[x]/\langle f(x)\rangle$. Considering $\operatorname{Aut}(K/\mathbb{Q})$, we know that for $\sigma \in \operatorname{Aut}(K/\mathbb{Q})$, then $\sigma(\sqrt{p})$ is a root of $f(x)$. Therefore, $\sigma(\sqrt{p}) = \pm\sqrt{p}$.

We also know that $K = \{a + b\sqrt{p} \mid a, b \in \mathbb{Q}\}$. We have that $\sigma(a + b\sqrt{p}) = a + b\sigma(\sqrt{p})$. Thus, we have $\operatorname{Aut}(K/\mathbb{Q}) = \{\sigma_0, \sigma_1\}$, with $\sigma_0(\sqrt{p}) = \sqrt{p}$ and $\sigma_1(\sqrt{p}) = -\sqrt{p}$.

(2) Let $K = \mathbb{Q}(\sqrt[3]{2})$. Looking at $\sigma \in \operatorname{Aut}(K/\mathbb{Q})$, we have that $\sigma(\sqrt[3]{2})$ maps to another root of $x^3 - 2$. Thus, we must have $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$, since there are no other roots of f in K. Thus, $\operatorname{Aut}(K/\mathbb{Q}) = \{\mathrm{id}\}$.

Proposition: Fixed Fields

Let K/F be an extension and $H \leq \operatorname{Aut}(K/F)$. The fixed field is given by $K^H := \{x \in K \mid \sigma(x) = x, \forall \sigma \in H\}$. For instance, $K^{\operatorname{Aut}(K/F)} = F$. We claim that for any such $H \leq \operatorname{Aut}(K/F)$, K^H is a field.

Let $x, y \in K^H$. Let $\sigma \in H$. We have

$$\begin{aligned} \sigma(x-y) &= \sigma(x) - \sigma(y) && \sigma \in \operatorname{Aut}(K/F) \\ &= x - y, \end{aligned}$$

so $x - y \in K^H$. Similarly,

$$\begin{aligned} \sigma(xy^{-1}) &= \sigma(x)\sigma(y^{-1}) \\ &= xy^{-1}. \end{aligned}$$

Thus, $xy^{-1} \in K^H$.

For any $H \leq \operatorname{Aut}(K/F)$, we have that $F \subseteq K^H \subseteq K$.

Corollary: Inclusion Reversing

(1) If we have $F_1 \subseteq F_2 \subseteq K$, then $\operatorname{Aut}(K/F_2) \subseteq \operatorname{Aut}(K/F_1)$.

(2) If $H_1 \leq H_2 \leq \operatorname{Aut}(K/F)$, then $K^{H_2} \subseteq K^{H_1}$.

Theorem: Splitting Field Automorphisms

Let $f(x) \in F[x]$. Let $K = \operatorname{Spl}_F(f(x))$. Then, $|\operatorname{Aut}(E/F)| \leq \deg(f(x)) = [E : F]$. Moreover, we have equality if f is separable.

Galois Extensions

Let K/F be a finite extension. We say K/F is Galois if $|\operatorname{Aut}(E/F)| = [E : F]$. If this is the case, we write $\operatorname{Gal}(K/F) = \operatorname{Aut}(K/F)$, and refer to it as the Galois group.

Corollary: Galois Extensions and Splitting Field Automorphisms

If K/F satisfies $K = \mathrm{Spl}_F(f(x))$, and $f(x)$ is separable, then K/F is Galois.

Examples: Examining Galois Groups

(1) For p prime, $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ is Galois. The Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt{p})/\mathbb{Q}) = \{\sigma_0, \sigma_1\} \cong \mathbb{Z}/2\mathbb{Z}$.

(2) Let p, q be distinct primes. Consider $K = \mathbb{Q}(\sqrt{p}, \sqrt{q})$. We have that $K = \mathrm{Spl}_{\mathbb{Q}}((x^2-p)(x^2-q))$. Thus, $K/\mathbb{Q}$ is separable, and a Galois extension.

Suppose $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Then, $\sigma(\sqrt{p}) = \pm\sqrt{p}$, because $\sigma(\sqrt{p})$ must be a root of $x^2 - p$. Similarly, $\sigma(\sqrt{q}) = \pm\sqrt{q}$, since $\sigma(\sqrt{q})$ must be a root of $x^2 - q$.

Recall that K has a basis of $\{1, \sqrt{p}, \sqrt{q}, \sqrt{pq}\}$. We have

$$\sigma(a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq}) = a + b\sigma(\sqrt{p}) + c\sigma(\sqrt{q}) + d\sigma(\sqrt{p})\sigma(\sqrt{q}).$$

Therefore, we have

$$\begin{aligned}
\sigma_0 &:= \sqrt{p} \mapsto \sqrt{p}, \sqrt{q} \mapsto \sqrt{q} \\
\sigma_1 &:= \sqrt{p} \mapsto -\sqrt{p}, \sqrt{q} \mapsto \sqrt{q} \\
\sigma_2 &:= \sqrt{p} \mapsto \sqrt{p}, \sqrt{q} \mapsto -\sqrt{q} \\
\sigma_3 &:= \sqrt{p} \mapsto -\sqrt{p}, \sqrt{q} \mapsto -\sqrt{q}.
\end{aligned}$$

We have that $\sigma_1^2 = \sigma_0$, $\sigma_2^2 = 0$, $\sigma_3^2 = 0$, implying that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

We also have $\langle\sigma_1\rangle, \langle\sigma_2\rangle, \langle\sigma_3\rangle$ are subgroups of order 2.

- $K^{\langle\sigma_1\rangle} = \{x = a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq} \mid a, b, c, d \in \mathbb{Q}, \sigma_1(x) = x\}$. We have $\sigma_1(x) = a - b\sqrt{p} + c\sqrt{q} - d\sqrt{pq} = a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq}$. Thus, we must have $b = d = 0$. Thus, we have $K^{\langle\sigma_1\rangle} = \mathbb{Q}(\sqrt{q})$.
- Using the same argument, we find $K^{\langle\sigma_2\rangle} = \mathbb{Q}(\sqrt{p})$.
- We see that $K^{\langle\sigma_3\rangle} = \mathbb{Q}(\sqrt{pq})$.
- Finally, $K^{\langle\sigma_1, \sigma_2\rangle} = \mathbb{Q}$, and $K^{\langle\sigma_0\rangle} = K$.

$$\begin{tikzcd}
 & K = \mathbb{Q}(\sqrt{p}, \sqrt{q}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{p}) \arrow[dr, dash, "2"'] & \mathbb{Q}(\sqrt{q}) \arrow[d, dash, "2"] & \mathbb{Q}(\sqrt{pq}) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \langle\sigma_0\rangle \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\langle\sigma_2\rangle \arrow[dr, dash] & \langle\sigma_1\rangle \arrow[d, dash] & \langle\sigma_3\rangle \arrow[dl, dash] \\
 & \langle\sigma_1, \sigma_2\rangle &
\end{tikzcd}$$

(3) Let $f(x) = x^3 - 2$. We saw that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, but $|\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = 1$, meaning $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois.

To find a Galois extension, we need to include the rest of the roots of $x^3 - 2$. In particular, we know that the roots are $\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}$. In particular, $\mathrm{Spl}_{\mathbb{Q}}(x^3 - 2) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. We know that ζ_3 is a root of $x^2 + x + 1$, and $\sqrt[3]{2}$ is a root of $x^3 - 2$.

We know that $[\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}] = 6$. We get $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}) \leq S_3$.

We have

$$\begin{aligned}
\sigma &: \begin{cases} \sqrt[3]{2} \mapsto \zeta_3\sqrt[3]{2} \\ \zeta_3 \mapsto \zeta_3 \end{cases} \\
\tau &: \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \zeta_3 \mapsto \zeta_3^2 \end{cases}.
\end{aligned}$$

Thus, our basis for $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$ is $\{1, \sqrt[3]{2}, \sqrt[3]{4}, \zeta_3, \zeta_3\sqrt[3]{2}, \zeta_3\sqrt[3]{4}\}$, and we have

$$\sigma : \begin{cases} 1 \mapsto 1 \\ \sqrt[3]{2} \mapsto \zeta_3\sqrt[3]{2} \\ \sqrt[3]{4} \mapsto \zeta_3^2\sqrt[3]{4} \\ \zeta_3 \mapsto \zeta_3 \\ \zeta_3\sqrt[3]{2} \mapsto \zeta_3^2\sqrt[3]{2} \\ \zeta_3\sqrt[3]{4} \mapsto \sqrt[3]{4} \end{cases}$$

$$\tau : \begin{cases} 1 \mapsto 1 \\ \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \sqrt[3]{4} \mapsto \sqrt[3]{4} \\ \zeta_3 \mapsto \zeta_3^2 \\ \zeta_3\sqrt[3]{2} \mapsto \zeta_3^2\sqrt[3]{2} \\ \zeta_3^2\sqrt[3]{2} \mapsto \zeta_3\sqrt[3]{2} \end{cases}$$

For our group, we have

$$\begin{aligned} e &= \text{id} \\ \sigma &= \begin{cases} \sqrt[3]{2} \mapsto \zeta_3\sqrt[3]{2} \\ \zeta_3 \mapsto \zeta_3 \end{cases} \\ \tau &= \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \zeta_3 \mapsto \zeta_3^2 \end{cases} \\ \tau^2 &= \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \zeta_3 \mapsto \zeta_3 \end{cases} \\ &= \text{id} \\ \sigma^2 &= \begin{cases} \sqrt[3]{2} \mapsto \zeta_3^2\sqrt[3]{2} \\ \zeta_3 \mapsto \zeta_3 \end{cases} \\ \sigma^3 &= \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \zeta_3 \mapsto \zeta_3 \end{cases} \\ &= \text{id} \\ \sigma\tau &= \begin{cases} \sqrt[3]{2} \overset{\sigma}{\mapsto} \zeta_3\sqrt[3]{2} \overset{\tau}{\mapsto} \zeta_3\sqrt[3]{2} \\ \zeta_3 \overset{\sigma}{\mapsto} \zeta_3 \overset{\tau}{\mapsto} \zeta_3^2 \end{cases} \\ \sigma^2\tau &= \begin{cases} \sqrt[3]{2} \overset{\sigma^2}{\longmapsto} \zeta_3^2\sqrt[3]{2} \overset{\tau}{\mapsto} \zeta_3^2\sqrt[3]{2} \\ \zeta_3 \overset{\sigma^2}{\longmapsto} \zeta_3 \overset{\tau}{\mapsto} \zeta_3^2 \end{cases} \end{aligned}$$

We can verify that $\tau\sigma = \sigma^2\tau$ and $\tau\sigma^2 = \sigma\tau$. Therefore, $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}) = \langle \sigma, \tau \rangle$.

Examining $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)^{\langle \tau \rangle}$, we have

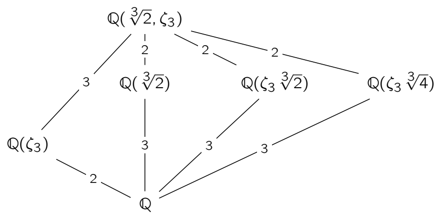
$$\tau : \begin{cases} 1 \mapsto 1 \\ \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \sqrt[3]{4} \mapsto \sqrt[3]{4} \\ \zeta_3 \mapsto \zeta_3^2 \\ \zeta_3\sqrt[3]{2} \mapsto \zeta_3^2\sqrt[3]{2} \\ \zeta_3\sqrt[3]{4} \mapsto \zeta_3^2\sqrt[3]{4} \end{cases},$$

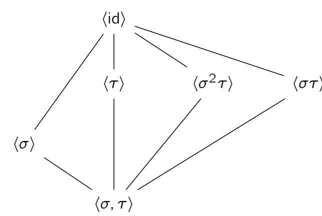
so we have $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)^{\langle \tau \rangle} = \mathbb{Q}(\sqrt[3]{2})$. Similarly, we find $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)^{\langle \sigma \rangle} = \mathbb{Q}(\zeta_3)$.

Examining $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)^{\langle \sigma\tau \rangle}$, we have

$$\sigma\tau : \begin{cases} 1 \mapsto 1 \\ \sqrt[3]{2} \mapsto \zeta_3 \sqrt[3]{2} \\ \sqrt[3]{4} \mapsto \zeta_3^2 \sqrt[3]{4} \\ \zeta_3 \mapsto \zeta_3^2 \\ \zeta_3 \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \zeta_3 \sqrt[3]{4} \mapsto \zeta_3 \sqrt[3]{4} \end{cases},$$

so $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)^{\langle \sigma\tau \rangle} = \mathbb{Q}(\zeta_3 \sqrt[3]{4})$.





Fundamental Theorem of Galois Theory

Let K/F be a Galois extension, with $G = \mathrm{Gal}(K/F)$. There is a bijection from the subfields $F \subseteq E \subseteq K$ to the subgroups $H \leq G$. The map from E to the elements of G that fix E and the map from H to K^H are inverses.

$$\begin{tikzcd} K \arrow[d, dash] & \{e\} \arrow[d, dash] \\ E \arrow[d, dash] & H \arrow[d, dash] \\ F & G \end{tikzcd}$$

(1) This is inclusion-reversing: if E_1, E_2 correspond to H_1, H_2, then $E_1 \subseteq E_2 \Leftrightarrow H_2 \leq H_1$.

(2) $[K : E] = |H|$ and $[E : F] = [G : H]$.

(3) K/E is always Galois. The first map in the bijection is $E \mapsto \mathrm{Gal}(K/E)$. Thus, $\mathrm{Gal}(K/K^H) = H$.

(4) E/F is Galois if and only if $H \trianglelefteq G$. In this case, $\mathrm{Gal}(E/F) \cong \mathrm{Gal}(K/F)/\mathrm{Gal}(K/E) \cong G/H$. More generally, even if H is not normal, the isomorphisms of E that fix F are in a one to one correspondence with the cosets $\{\sigma H\}_{\sigma \in G}$.

(5) If E_1, E_2 correspond to H_1, H_2, then $E_1 \cap E_2$ corresponds to $\langle H_1, H_2 \rangle$, and $E_1 E_2$ corresponds to $H_1 \cap H_2$. Therefore, the lattice of fields $F \subseteq E \subseteq X$ is dual to the lattice of subgroups $\{e_g\} \leq H \leq G$.

Propositions that follow from Fundamental Theorem

Theorem 7.10: Let K/F be an extension of fields, with $G \leq \mathrm{Aut}(K/F)$ and $F = K^G$. Then, $|G| = [K : F]$. The proof of the above depends on a result in character theory that we will not cover.

Corollary 7.11: if K/F is any finite extension, then $|\mathrm{Aut}(K/F)| \leq [K : F]$. We have equality if and only if $F = K^{\mathrm{Aut}(K/F)}$. We have that K/F is Galois if and only if $K^{\mathrm{Aut}(K/F)} = F$.

> Let $F_1 = K^{\mathrm{Aut}(K/F)}$. Then, we have $F \subseteq F_1 \subseteq K$. Theorem 7.10: gives $[K : F_1] = |\mathrm{Aut}(K/F)|$. Thus, $[K : F] = [K : F_1][F_1 : F] = |\mathrm{Aut}(K/F)|[F_1 : F]$. Thus, $|\mathrm{Aut}(K/F)| \leq [K : F]$, with equality if $[F_1 : F] = 1$, meaning $F = K^{\mathrm{Aut}(K/F)}$.

Corollary 7.12: let $G \leq \mathrm{Aut}(K)$, with $F = K^G$. Then, every automorphism of K that fixes F is in G; i.e., $G = \mathrm{Aut}(K/F)$. In particular, K/F is Galois, and $\mathrm{Gal}(K/F) = G$.

> We have $G \leq \mathrm{Aut}(K/F)$ by the definition of F. In particular, $|G| \leq |\mathrm{Aut}(K/F)|$. We know from the theorem that $|G| = [K : F]$. By Corollary 7.11, we get that $|\mathrm{Aut}(K/F)| \leq [K : F]$. Thus, we must have $|G| = |\mathrm{Aut}(K/F)|$, as both G and $\mathrm{Aut}(K/F)$ are equal.

Corollary 7.13: let G_1, G_2 be distinct finite subgroups of $\mathrm{Aut}(K)$. Then, $K^{G_1} \neq K^{G_2}$.

Let $F_i = K^{G_i}$. Suppose $F_1 = F_2$. Then, F_1 is fixed by G_2, meaning by Corollary 7.12, we have $G_1 \leq G_2$. By similar logic, we have $G_2 \leq G_1$, meaning $G_1 = G_2$.

Theorem 7.14: An extension K/F is Galois if and only if K is the splitting field of a separable polynomial over F. Further, if this is the case, then every irreducible polynomial in $F[x]$ is separable and has all its roots in K, meaning K/F as an extension is separable.

We have shown that if K is the splitting field of a separable polynomial over F, then K/F is Galois.

Let K/F be Galois and $f(x) \in F[x]$ be irreducible with a root $\alpha \in K$. Set $\mathrm{Gal}(K/F) = \{\sigma_1 = \mathrm{id}, \sigma_2, \dots, \sigma_n\}$. Since $\alpha \in K$, $\sigma_i(\alpha) \in K$. Let $\alpha_1, \dots, \alpha_r$ be the distinct elements in $A = \{\sigma_1(\alpha), \sigma_2(\alpha), \dots, \sigma_n(\alpha)\}$.

For any $\tau \in \mathrm{Gal}(K/F)$, $\tau\sigma_1, \tau\sigma_2, \dots, \tau\sigma_n$ are distinct elements, because if $\tau\sigma_i = \tau\sigma_j$, then $\sigma_i = \sigma_j$. If we apply τ to elements in A, we get a permutation, meaning $r = n$.

Set $g(x) = (x-\alpha_1)\cdots(x-\alpha_n)$. If $h(x) = a_nx^n + \cdots + a_1x + a_0$, then $h^\tau(x) = \tau(a_n)x^n + \cdots + \tau(a_1)x + \tau(a_0)$. Specifically,

$$\begin{aligned} g^\tau(x) &= \prod_{j=1}^{n}(x - \tau(\alpha_j)) \\ &= \prod_{k=1}^{n}(x - \alpha_k). \end{aligned}$$

Thus, τ leaves all the *coefficients* of g fixed. Since τ is arbitrary, we have that the coefficients of g must be in F. Therefore, $g(x) \in F[x]$, and splits over K.

We have $f(x)$ is irreducible, $f(\alpha) = 0$, so $f(x) = m_{\alpha,F}(x)$. However, $g(x) \in F[x]$ and $g(\alpha) = 0$. So, $f(x)|g(x)$. Additionally, we can see that all the roots of $g(x)$ are of the form $\sigma_j(\alpha)$, with α as a root in $f(x) \in F[x]$, and $\sigma_j \in \mathrm{Gal}(K/F)$, meaning $\sigma_j(\alpha)$ must be roots of $f(x)$ as well, meaning $g(x)|f(x)$. Thus, $g(x) = f(x)$, and $f(x)$ is separable with all its roots in K.

Let $x_1, \dots, x_n$ be a basis for K/F. Let $f_i(x) = m_{x_i,F}(x)$. Therefore, each f_i splits over K. Set $g(x)$ to be the polynomial resulting from removing all repeated factors of $\{f_i(x)\}$. So, the splitting field of $g(x)$ is the same as the splitting field of $f_1(x), \dots, f_n(x)$. Since $x_1, \dots, x_n$ is a basis for K/F, K is also a basis for $f_1(x), \dots, f_n(x)$. Since g is a separable polynomial, K is the splitting field for a single separable polynomial.

We know that K/F is Galois if it satisfies any of the following:

(i) K/F is the splitting field of a separable polynomial;

(ii) $F = K^{\mathrm{Aut}(K/F)}$;

(iii) $[K : F] = |\mathrm{Aut}(K/F)|$;

(iv) K/F is finite, normal and separable, where normal means any polynomial in $F[x]$ with a root in K fully splits over K.

Example: Galois Group of Polynomial over Finite Field

Let p be prime, $n \in \mathbb{Z}$. Recall that we constructed $\mathbb{F}_{p^n}$ as the splitting field of of $f(x) = x^{p^n} - x$. Since $f(x) \in \mathbb{F}_p[x]$ is separable, $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois.

We also saw that the Frobenius map $\phi_p : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}; x \mapsto x^p$ in $\mathbb{F}_{p^n}$ is an automorphism of $\mathbb{F}_{p^n}$, and the map fixes $\mathbb{F}_p$. Thus, $\phi_p \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

In particular, we can take $\langle \phi_p \rangle \leq \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. For $\alpha \in \mathbb{F}_{p^n}$, we see that $\phi_p^n(\alpha) = \alpha^{p^n} = \alpha$. Thus, $\phi_p^n = \mathrm{id}$. If $\phi_p^j = \mathrm{id}$ for some $0 < j < n$. Thus, $\alpha^{p^j} = \alpha$ for every $\alpha \in \mathbb{F}_{p^n}$. This would give p^n roots of $x^{p^j} - x$, but a polynomial cannot have any more roots than its degree.

Thus, $|\langle \phi_p \rangle| = n$, but $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$, so $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \phi_p \rangle \cong \mathbb{Z}/n\mathbb{Z}$.

The intermediate fields $\mathbb{F}_p \subseteq K \subseteq \mathbb{F}_{p^n}$ correspond to subgroups of $\mathbb{Z}/n\mathbb{Z}$. These subgroups are given by $\mathbb{Z}/d\mathbb{Z}$, where $d|n$. In particular, the subgroups of $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ are $\langle \phi_p^d \rangle$ with $d|n$. Thus, we get $\langle \phi_p^d \rangle \cong \mathbb{Z}/(n/d)\mathbb{Z}$, with fixed field $\mathbb{F}_{p^{n/d}}$.

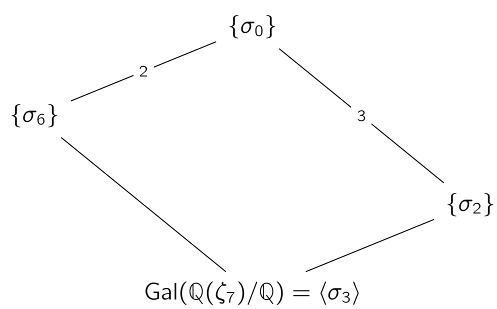
Example: Roots of Unity

Let $f(x) = x^n - 1$, and let $\mathbb{Q}(\zeta_n) = \mathrm{Spl}_{\mathbb{Q}}(f(x))$. Then, $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois (separating and splitting field). Note that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$, meaning $|\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.

We claim that $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. Define $\varphi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, $a \mapsto \left(\zeta_n \overset{\sigma_a}{\longmapsto} \zeta_n^a\right)$. We can verify that φ is a homomorphism. If $a \in \ker\varphi$, then $\varphi(a) = \zeta_n \overset{\sigma_a}{\longmapsto} \zeta_n$. We know that $\sigma_a(\zeta_n) = \zeta_n^a$, meaning $\zeta_n^a = \zeta_n$, meaning $a \equiv 1$ modulo n. Therefore, $\ker\varphi$ is trivial. Since the sets are finite, and φ is injective, it is an isomorphism.

Consider $\mathbb{Q}(\zeta_7)/\mathbb{Q}$. We know that $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z}$. We know that this is a cyclic group of order 6, meaning we have the trivial subgroup, a unique subgroup of order 2, and a unique subgroup of order 3 (unique due to cyclic group).

We can see that $|2| = 3$ in $(\mathbb{Z}/7\mathbb{Z})^\times$, meaning $\langle \sigma_2 \rangle$ has order 3 in $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$. Additionally, we see $|6| = 2$ in $(\mathbb{Z}/7\mathbb{Z})^\times$, so $\langle \sigma_6 \rangle$ has order 2 in $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$.

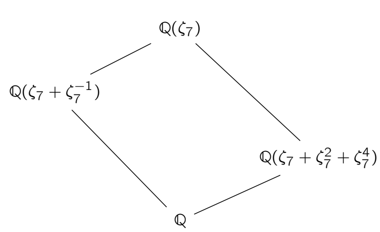


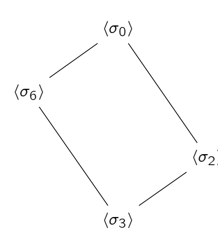
We want to calculate $\mathbb{Q}(\zeta_7)^{\langle \sigma_6 \rangle}$ and $\mathbb{Q}(\zeta_7)^{\langle \sigma_2 \rangle}$.

Let $\alpha = \zeta_7 + \zeta_7^{-1}$. Note that $\sigma_6^2 = \mathrm{id}$, then $\sigma_6(\zeta_7) = \zeta_7^{-1}$. So, $\sigma_6(\alpha) = \sigma_6(\zeta_7) + \sigma_6(\zeta_7^{-1}) = \zeta_7^{-1} + \zeta_7 = \alpha$. Therefore, $\mathbb{Q}(\zeta_7 + \zeta_7^{-1}) \subseteq \mathbb{Q}(\zeta_7)^{\langle \sigma_6 \rangle}$.

Let $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$, with $\tau \notin \langle \sigma_6 \rangle$. We have $\tau(\alpha)$ must be a linear combination of the basis elements $1, \zeta_7, \dots, \zeta_7^6$. If $\tau(\alpha) = \alpha$, then $\tau(\zeta_7) = \sigma(\zeta_7)$ for some $\sigma = \sigma_1, \sigma_6$, but $\tau \notin \langle \sigma_6 \rangle$. Thus, it must be that $\mathbb{Q}(\zeta_7 + \zeta_7^{-1}) = \mathbb{Q}(\zeta_7)^{\langle \sigma_6 \rangle}$.

Consider $\beta = \zeta_7 + \sigma_2(\zeta_7) + \sigma_2^2(\zeta_7)$. We can see that $\sigma_2(\beta) = \sigma_2(\zeta_7) + \sigma_2^2(\zeta_7) + \sigma_2^3(\zeta_7) = \beta$. We get that $\mathbb{Q}(\zeta_7 + \zeta_7^2 + \zeta_7^4) \subseteq \mathbb{Q}(\zeta_6)^{\langle \sigma_2 \rangle}$. With the same argument, we can show that if $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$ that fixes β, then $\tau \in \langle \sigma_2 \rangle$, meaning $\mathbb{Q}(\zeta_7 + \zeta_7^2 + \zeta_7^4) = \mathbb{Q}(\zeta_7)^{\langle \sigma_2 \rangle}$.





We have that $\mathbb{Q}(\zeta_7+\zeta_7^{-1})\subseteq\mathbb{R}$, and

$$\begin{aligned}[\mathbb{Q}(\zeta_7):\mathbb{Q}(\zeta_7+\zeta_7^{-1})] &= [\mathbb{Q}(\zeta_7):\mathbb{Q}(\zeta_7)^{\langle\sigma_6\rangle}]\\ &= |\sigma_6|\\ &= 2.\end{aligned}$$

Moreover, $\mathbb{Q}(\zeta_7)\not\subseteq\mathbb{R}$. Then, $\mathbb{Q}(\zeta_7)\cap\mathbb{R}$ is a subfield of $\mathbb{Q}(\zeta_7)$ and $\mathbb{R}$, so we have $\mathbb{Q}(\zeta_7)\supseteq\mathbb{Q}(\zeta_7)\cap\mathbb{R}\supseteq\mathbb{R}(\zeta_7+\zeta_7^{-1})$. Since $[\mathbb{Q}(\zeta_7):\mathbb{Q}(\zeta_7)\cap\mathbb{R}]\neq 1$ and $[\mathbb{Q}(\zeta_7):\mathbb{Q}(\zeta_7+\zeta_7^{-1})]=2$, we must have $\mathbb{Q}(\zeta_7+\zeta_7^{-1})=\mathbb{Q}(\zeta_7)\cap\mathbb{R}$.

Thus, $\mathbb{Q}(\zeta_7+\zeta_7^{-1})$ is the largest subfield of $\mathbb{Q}(\zeta_7)$ contained in $\mathbb{R}$; it is known as the maximal totally real subfield.

Propositions that follow from Fundamental Theorem, Cont'd

Proposition 7.15: Let K/F be Galois, and E/F be a field. Then, KE/E is Galois, and $\mathrm{Gal}(KE/E)\cong\mathrm{Gal}(K/K\cap E)$ — $\mathrm{Gal}(KE/E)$ is isomorphic to a subgroup of $\mathrm{Gal}(K/F)$.

$$\begin{tikzcd}
 & KE \arrow[dl, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash] \arrow[ddr, dash, bend right] & & E \arrow[dl, dash] \\
 & K\cap E \arrow[d, dash] & \\
 & F &
\end{tikzcd}$$

We know K/F is Galois, meaning K is the splitting field of some $f(x)\in F[x]$. We have $F\subset E$, so if we have $f(x)\in E[x]$, then $KE=\mathrm{Spl}_E(f(x))$.

This gives KE/E is Galois.

Define $\varphi:\mathrm{Gal}(KE/E)\to\mathrm{Gal}(K/F)$, with $\sigma\mapsto\sigma|_K$.

We have $\sigma|_K$ maps to K because $K=\mathrm{Spl}_F(f(x))$. Thus, since σ is an automorphism, it fixes F, meaning $\sigma(\alpha)\in K$ for any $\alpha\in K$. Thus φ is well-defined.

We can verify that φ is a homomorphism. We also have $\ker\varphi:\{\sigma\in\mathrm{Gal}(KE/E)\mid\sigma|_K=\mathrm{id}\}$. If $\sigma\in\ker\varphi$, $\sigma|_K=\mathrm{id}$ and $\sigma|_E=\mathrm{id}$ since it is in $\mathrm{Gal}(KE/E)$. But, if σ fixes K and fixes E, it fixes KE, meaning $\ker\varphi$ is trivial, and thus φ is injective.

Let $H\leq\mathrm{Gal}(K/F)$ be the image of φ. Consider the fixed field K^H. Let $\sigma\in\mathrm{Gal}(KE/E)$. We have σ fixes E, so it fixes $K\cap E$. We have $K\cap E\subset K$, so $\sigma|_K$ fixes $K\cap E$, meaning $\varphi(\sigma)$ fixes $K\cap E$, meaning $K\cap E\subseteq K^H$.

We have σ fixes E, and σ acts on K^H via restriction, so it fixes K^H and E, hence K^HE. Thus, $\sigma|_{K^HE}=\mathrm{id}$. Thus, $\mathrm{Gal}(KE/E)$ fixes K^HE. The Fundamental Theorem gives $K^HE=E$, implying $K^H\subseteq E$ In particular, $K^H\subseteq K\cap E$.

Combining, we have $K^H=K\cap E$. Thus, $\mathrm{Gal}(KE/E)\cong\mathrm{im}(\varphi)=\mathrm{Gal}(K/K^H)=\mathrm{Gal}(K/K\cap E)$.

Proposition: Intersection and Compositum of Galois Extensions

Let K_1/F and K_2/F be Galois. Then, we have the following results.

(1) $K_1\cap K_2/F$ is Galois.

(2) K_1K_2/F is Galois, and $\mathrm{Gal}(K_1K_2/F)$ is isomorphic to

$$H=\{(\sigma,\tau)\in\mathrm{Gal}(K_1/F)\times\mathrm{Gal}(K_2/F)\mid\sigma|_{K_1\cap K_2}=\tau|_{K_1\cap K_2}\}.$$

Let $\alpha \in K_1 \cap K_2$ with $f(x) = m_{\alpha,F}(x)$. In particular, $f(x)$ splits over K_1 since $\alpha \in K_1$ and $f(x)$ splits over K_2 as $\alpha \in K_2$. So, f splits over $K_1 \cap K_2$.

Let $K_1 = \mathrm{Spl}_F(f_1(x))$ and $K_2 = \mathrm{Spl}_F(f_2(x))$. Then, $K_1K_2 = \mathrm{Spl}_F(\overline{f_1(x)f_2(x)})$, where $\overline{f_1(x)f_2(x)}$ denotes the square-free part of $f_1(x)f_2(x)$. Since $\overline{f_1(x)f_2(x)}$ is separable, K_1K_2 is Galois.

Consider the map

$$\begin{aligned} \varphi : \mathrm{Gal}(K_1K_2/F) &\to \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F) \\ \sigma &\mapsto \left(\sigma|_{K_1}, \sigma|_{K_2}\right). \end{aligned}$$

We can verify that this is a homomorphism. Suppose $\sigma \in \ker\varphi$. Then, we have $\sigma|_{K_1} = \sigma|_{K_2} = \mathrm{id}$. Thus, $\sigma|_{K_1K_2} = \mathrm{id}$, meaning φ is injective. Thus, $\mathrm{Gal}(K_1K_2/F) \cong \mathrm{im}(\varphi)$.

Note that $\varphi(\sigma) = (\sigma|_{K_1}, \sigma|_{K_2})$. We have $\left(\sigma|_{K_1}\right)|_{K_1\cap K_2} = \sigma|_{K_1\cap K_2} = \left(\sigma|_{K_1\cap K_2}\right)|_{K_1}$. Thus, $\mathrm{im}(\varphi) \subseteq H$.

Set $G_1 = \mathrm{Gal}(K_1/F)$, $G_2 = \mathrm{Gal}(K_2/F)$, and $N = \mathrm{Gal}(K_2/K_1 \cap K_2)$.

$$\begin{tikzcd}
 & K_1K_2 \arrow[dl, dash] \arrow[dr, dash] & \\
K_1 \arrow[dr, dash] & & K_2 \arrow[dl, dash] \\
 & K_1 \cap K_2 \arrow[d, dash] & \\
 & F &
\end{tikzcd}$$

We want to determine the size of H, since we know $\mathrm{im}(\varphi) \subseteq H$ and $\mathrm{Gal}(K_1K_2/F) \cong \mathrm{im}(\varphi)$, so if we know the size of H, we can see that $\mathrm{im}(\varphi) = H$.

Let $\psi \in \mathrm{Gal}(K_1 \cap K_2/F) \cong G_2/N$. If we look at ψN, we see there are $|N|$ elements in the coset. Pick $\sigma \in G_1$, and set $\psi = \sigma|_{K_1\cap K_2}$. If $\psi N = \tau N$, then we have $\psi\tau^{-1} \in N$. This means $\psi\tau^{-1}$ fixes $K_1 \cap K_2$; in other words, $\psi\tau^{-1}(x) = x$ for every $x \in K_1 \cap K_2$, meaning $\psi(x) = \tau(x)$ for every $x \in K_1 \cap K_2$.

Therefore, $|H| = |G_1||N|$, or

$$\begin{aligned} |H| &= |G_1|\frac{|G_2|}{|\mathrm{Gal}(K_1 \cap K_2/F)|} \\ &= \frac{|\mathrm{Gal}(K_1/F)||\mathrm{Gal}(K_2/F)|}{|\mathrm{Gal}(K_1 \cap K_2/F)|}. \end{aligned}$$

On the other hand, we also have

$$\begin{aligned} \mathrm{im}(\varphi) = |\mathrm{Gal}(K_1K_2/F)| &= [K_1K_2 : F] \\ &= [K_1K_2 : K_2][K_2 : F] \\ &= [K_1 : K_1 \cap K_2][K_2 : F] \\ &= \frac{[K_1 : F]}{[K_1 \cap K_2 : F]}[K_2 : F] \\ &= \frac{|\mathrm{Gal}(K_1/F)||\mathrm{Gal}(K_2/F)|}{\mathrm{Gal}|(K_1 \cap K_2/F)|} = |H|. \end{aligned}$$

Corollary: Condition for Direct Product

Let K_1/F and K_2/F be Galois with $K_1 \cap K_2 = F$. Then, $\mathrm{Gal}(K_1K_2/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$. Conversely, if K/F is Galois and $\mathrm{Gal}(K/F) \cong G_1 \times G_2$, then K is the compositum of two Galois extensions.

We have $\mathrm{Gal}(K_1K_2/F) \cong \{(\sigma, \tau) \in \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F) \mid \sigma_{K_1\cap K_2} = \tau|_{K_1\cap K_2}\}$. Since $K_1 \cap K_2 = F$, and σ, τ are in Galois groups, we must have $\sigma|_F = \tau|_F$, meaning they are identity on F, so our set is equal to $\mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$.

Set $K_i = K^{G_i}$. Then, $K_1 \cap K_2 = K^{\langle G_1, G_2 \rangle} = K^{\mathrm{Gal}(K/F)} = F$. We also have

$$\begin{aligned} K_1K_2 &= K^{G_1 \cap G_2} \\ &= K^{\{e_G\}} \\ &= K. \end{aligned}$$

Example: Cyclotomic Fields and Compositum

Let $n = p_1^{e_1} \cdots p_k^{e_k}$. Note that $\zeta_n^{p_2^{e_2} \cdots p_r^{e_r}}$ is a primitive $p_1^{e_1}$ root of unity. Therefore, $\mathbb{Q}\left(\zeta_{p_j^{e_j}}\right) \subseteq \mathbb{Q}(\zeta_n)$ for $j = 1, \dots, r$. Set $K_j = \mathbb{Q}\left(\zeta_{p_j^{e_j}}\right)$. Then, $\mathbb{Q}(\zeta_n) = K_1K_2 \cdots K_r$.

Note that

$$\begin{aligned} [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n) &= \phi\left(p_1^{e_1}\right)\phi\left(p_2^{e_2}\right) \cdots \phi\left(p_r^{e_r}\right) \\ &= [K_1 : \mathbb{Q}][K_2 : \mathbb{Q}] \cdots [K_r : \mathbb{Q}]. \end{aligned}$$

So, we see that via a previous result and induction,

$$\begin{aligned} \mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right) &\cong \mathrm{Gal}(K_1/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(K_r/\mathbb{Q}) \\ &\cong (\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \times \cdots \times \left(\mathbb{Z}/\mathbb{Z}_{p_r^{e_r}}\right), \end{aligned}$$

and $K_i \cap K_j = \mathbb{Q}$ for $i \neq j$.

Abelian Extensions and the Kronecker–Weber Theorem

We say a Galois extension K/F is abelian if $\mathrm{Gal}(K/F)$ is an abelian group. The Kronecker–Weber theorem states that if $K/\mathbb{Q}$ is an abelian extension, then $K \subseteq \mathbb{Q}(\zeta_n)$ for some n.

There is a field called the Galois closure of any extension K/F with $F \subseteq K \subset \tilde{K}$, with $\tilde{K}/F$ Galois.

Galois Group of Polynomials

Let $f(x) \in F[x]$ be a separable polynomial. The Galois group of $f(x)$, denoted $\mathrm{Gal}(f(x))$ is $\mathrm{Gal}\left(\mathrm{Spl}_F(f(x))/F\right)$.

Example: Galois Group of Polynomials

(1) $\mathrm{Gal}(x^3 - 2) = \mathrm{Gal}\left(\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}\right) \cong S_3$

(2) $\mathrm{Gal}(x^n - 1) = \mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right) \cong (\mathbb{Z}/n\mathbb{Z})^{\times}$

Let $f(x) = F[x]$ be separable with degree n. Let $K = \mathrm{Spl}_F(f(x))$, $X = \{\alpha_1, \dots, \alpha_n\}$. If $\sigma \in \mathrm{Gal}(K/F)$, then $\sigma(\alpha_j) \in X$ for each j.

Moreover, $\mathrm{id}(\alpha_j) = \alpha_j$. We have $(\sigma\tau)(\alpha_j) = \sigma(\tau(\alpha_j))$ for all $\sigma, \tau \in \mathrm{Gal}(K/F)$. This is a group action of $\mathrm{Gal}(K/F)$ on X. In particular, we have $\mathrm{Gal}(K/F) \hookrightarrow S_n$.

Elementary Symmetric Functions and General Polynomials

Let $x_1, \dots, x_n$ be indeterminates. The elementary symmetric functions in $x_1, \dots, x_n$ are

$$\begin{aligned} s_1 &= x_1 + x_2 + \cdots + x_n \\ s_2 &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n \sum_{i \leq j} x_ix_j \\ &\vdots \\ s_n &= x_1x_2x_3 \cdots x_n \end{aligned}$$

The general polynomial of degree n is the polynomial $(x - x_1) \cdots (x - x_n)$.

Exercise: Use induction to show that

$$(x - x_1)\cdots(x - x_n) = x^n - s_1x^{n-1} + s_2x^{n-1} + \cdots + (-1)^n s_n.$$

The field $F(x_1, \dots, x_n)$ is the field of rational functions in $x_1, \dots, x_n$. Note that $F(s_1, \dots, s_n) \subseteq F(x_1, \dots, x_n)$. Moreover, $F(x_1, \dots, x_n)/F(s_1, \dots, s_n)$ is a Galois extension.

Given $\sigma \in S_n$, we have σ acts on $\{x_1, \dots, x_n\}$ with $\sigma(x_i) = x_{\sigma(i)}$. This gives $S_n \subseteq \operatorname{Aut}(F(x_1, \dots, x_n)/F(s_1, \dots, s_n))$, with:

- $S_n \subseteq \operatorname{Aut}(F(x_1, \dots, x_n))$ by mapping $x_i \mapsto x_{\sigma(i)}$, fixing elements of F.
- S_n fixes $F(s_1, \dots, s_n)$.

We see that $F(s_1, \dots, s_n) \subseteq F(x_1, \dots, x_n)^{S_n}$. Moreover, $[F(x_1, \dots, x_n) : F(x_1, \dots, x_n)^{S_n}] = |S_n| = n!$.

However, we also have $F(x_1, \dots, x_n)$ is the splitting field of $x^n - s_1x^{n-1} + \cdots + (-1)^n s_n$, meaning $[F(x_1, \dots, x_n) : F(s_1, \dots, s_n)] \leq n!$. Therefore, we have

$$\underbrace{F(s_1, \dots, s_n) \subseteq \overbrace{F(x_1, \dots, x_n)^{S_n} \subseteq F(x_1, \dots, x_n)}^{=n!}}_{\leq n!}$$

Thus, $\operatorname{Gal}(F(x_1, \dots, x_n)/F(s_1, \dots, s_n)) \cong S_n$.

Given a rational function $f(x_1, \dots, x_n) \in F(x_1, \dots, x_n)$, and $\sigma \in S_n$, we say $f^\sigma(x_1, \dots, x_n) = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$. We say $f(x_1, \dots, x_n)$ is symmetric if $f^\sigma = f$ for all $\sigma \in S_n$.

Corollary: Symmetric Functions and Rational Functions

Any symmetric function in $x_1, \dots, x_n$ is rational in $s_1, \dots, s_n$.

If $f^\sigma = f$ for every $\sigma \in S_n$, then f is fixed by $\operatorname{Gal}(F(x_1, \dots, x_n)/F(s_1, \dots, s_n))$.

So $f \in F(x_1, \dots, x_n)^{S_n} = F(s_1, \dots, s_n)$.

Theorem: Separability of General Polynomials

The general polynomial $f(x) = (x - x_1)\cdots(x - x_n)$ is separable over $F(s_1, \dots, s_n)$ with Galois group S_n.

Sovability in Terms of Radicals

(1) An element α that is algebraic over F can be solved for in terms of radicals if $\alpha \in K$, where K satisfies

$$F = K_0 \subset K_1 \subset \cdots \subset K_n = K,$$

where $K_{i+1} = K_i\left(\sqrt[n_i]{a_i}\right)$, for some $a_i \in K_i$, $n_i \in \mathbb{Z}_{\geq 2}$. We define $\sqrt[n_i]{a_i}$ as any root of $x^{n_i} - a_i = 0$.

We call such an extension K a root extension of F.

(2) We say a polynomial can be solved by radicals if all its roots can be solved in terms of radicals.

Proposition: Cyclic Extensions and Roots of Unity

An extension K/F is said to be cyclic if it is cyclic with cyclic Galois group.

Let F be a field with $\operatorname{char}(F) \nmid n$, and $\mu_n \subseteq F$, where μ_n denotes the nth roots of unity. Then, the extension $F(\sqrt[n]{a})/F$ is cyclic of degree dividing n, for any $a \in F$.

We see that $F(\sqrt[n]{a})/F$ is Galois, as $F(\sqrt[n]{a}) = \operatorname{Spl}_F(x^n - a)$, since $\mu_n \subseteq F$, and $x^n - a$ is separable, since $\operatorname{char}(F) \nmid n$.

Given any $\sigma \in \text{Gal}\left(F(\sqrt[n]{a})/F\right)$, we have $\sigma(\sqrt[n]{a})$ is another root of $x^n - a$. So, $\sigma(\sqrt[n]{a}) = \zeta_\sigma \sqrt[n]{a}$, for some $\zeta_\sigma \in \mu_n$.

This gives a map $\varphi : \text{Gal}\left(F(\sqrt[n]{a})/F\right) \to \mu_n$, $\sigma \mapsto \zeta_\sigma$. We have $\varphi(\sigma\tau) = \zeta_{\sigma\tau} = \zeta_\sigma\zeta_\tau$, meaning φ is a homomorphism. If $\varphi(\sigma) = 1$, then $\sigma(\sqrt[n]{a}) = 1\sqrt[n]{a}$, meaning $\sigma = \text{id}$, so φ is injective.

Therefore, $\text{Gal}\left(F(\sqrt[n]{a})/F\right) \hookrightarrow \mu_n$, and μ_n is cyclic, so $\text{Gal}\left(F(\sqrt[n]{a})/F\right)$ is cyclic.

Lagrange Resolvents

Let K/F be cyclic, $\text{Gal}(K/F) = \langle\sigma\rangle$, with $[K : F] = n$. Let $\mu_n \subseteq F$, and $\text{char}(F) \nmid n$. For $\alpha \in K$ and $\zeta \in \mu_n$, the Lagrange resolvent is given by $(\alpha, \zeta) \in K$, with

$$\begin{aligned}(\alpha,\zeta) &= \sum_{k=0}^{n-1} \zeta^k\sigma^k(\alpha)\\ &= \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha).\end{aligned}$$

Proposition 7.22: Let K/F be cyclic of degree n, $\mu_n \subseteq F$, and $\text{char}(F) \nmid n$, with $\text{Gal}(K/F) = \langle\sigma\rangle$. Then, $K = F\left(\sqrt[n]{\alpha}\right)$.

Apply σ to (α, ζ). Then,

$$\begin{aligned}\sigma\left(\alpha,\zeta\right) &= \sigma(\alpha) + \zeta\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^n(\alpha)\\ &= \sigma(\alpha) + \zeta\sigma^2(\alpha) + \cdots + \zeta^{n-1}\alpha\\ &= \zeta^{-1}\alpha + \sigma(\alpha) + \zeta\sigma^2(\alpha) + \cdots + \zeta^{n-2}\sigma^{n-1}(\alpha).\\ &= \zeta^{-1}\left(\alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha)\right)\\ &= \zeta^{-1}(\alpha,\zeta).\end{aligned}$$

Thus,

$$\begin{aligned}\sigma\left((\alpha,\zeta)^n\right) &= \left(\sigma(\alpha,\zeta)\right)^n\\ &= \left(\zeta^{-1}(\alpha,\zeta)\right)^n\\ &= \zeta^{-n}(\alpha,\zeta)^n\\ &= (\alpha,\zeta)^n,\end{aligned}$$

meaning $(\alpha, \zeta)^n \in F$ for any $\alpha \in K$ (as every element of $\text{Gal}(K/F)$ fixes $(\alpha, \zeta)^n$).

Recall that $\text{Gal}(K/F) = \{1, \sigma, \sigma^2, \dots, \sigma^{n-1}\}$. We want to show that these are linearly independent as functions. In other words,

$$a_1 + a_2\sigma + a_3\sigma^2 + \cdots + a_n\sigma^{n-1} = \mathbb{0}$$

if and only if a_i are identically 0. Let $\{\sigma_1, \sigma_2, \dots, \sigma_n\} = \{1, \sigma, \sigma^2, \dots, \sigma^{n-1}\}$.

Let $a_1\sigma_1 + a_2\sigma_2 + \cdots a_k\sigma_k = \mathbb{0}$ with the minimal number of a_i nonzero. For any $\beta \in K$,

$$a_1\sigma_1(\beta) + a_2\sigma_2(\beta) + \cdots + a_k\sigma_k(\beta) = 0. \tag{$*$}$$

Since $\sigma_k \neq \sigma_1$, there is some $\beta_0 \in K$ such that $\sigma_k(\beta_0) \neq \sigma_1(\beta_0)$. Applying to $\beta\beta_0$,

$$\begin{aligned}a_1\sigma_1(\beta\beta_0) + a_2\sigma_2(\beta\beta_0) + \cdots + a_k\sigma_k(\beta\beta_0) &= 0\\ a_1\sigma_1(\beta)\sigma_1(\beta_0) + a_2\sigma_2(\beta)\sigma_2(\beta_0) + \cdots + a_k\sigma_k(\beta)\sigma_k(\beta_0) &= 0.\end{aligned} \tag{$**$}$$

Multiply $(*)$ by $\sigma_k(\beta_0)$, and subtract from $(**)$. (I couldn't put the first step here because it caused margin difficulties.)

$$0 = \underbrace{a_1\left(\sigma_1(\beta_0) - \sigma_k(\beta_0)\right)\sigma_1(\beta)}_{\neq 0} + \cdots + a_{k-1}\left(\sigma_{k-1}(\beta_0) - \sigma_k(\beta_0)\right)\sigma_{k-1}(\beta).$$

Returning to (α, ζ), we see that since $1, \sigma, \sigma^2, \dots, \sigma^{n-1}$ are linearly independent, there is an $\alpha_0 \in K$ with $(\alpha_0, \zeta) \neq 0$. Note that $\sigma\left((\alpha_0, \zeta)^i\right) = \zeta^{-i}(\alpha_0, \zeta)$. As long as ζ is a primitive nth root of unity, then σ does not fix $(\alpha_0, \zeta)^i$ for $0 < i < n$, meaning $(\alpha_0, \zeta)^i \notin F$ for $0 < i < n$.

Thus, $[F((\alpha_0, \zeta)) : F] = [K : F] = n$, so $K = F((\alpha_0, \zeta))$. Set $a = (\alpha_0, \zeta)^n$, meaning $K = F(\sqrt[n]{a})$.

Lemma: Galois Root Extensions Let $F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = K$ be a root extension. For any $\alpha \in K$, α is contained in a root extension that is Galois over F, and each intermediate field is cyclic.

Theorem 7.24: The polynomials $f(x)$ can be solved in radicals if and only if its Galois group is solvable.

Solvable Group

A group G is said to be solvable if there is a chain of subgroups

$$1 = G_n \leq G_{n-1} \leq G_{n-2} \leq \cdots \leq G_0 = G$$

with G_i/G_{i+1} cyclic.

Fact: If $H \leq G$ and G/H are both solvable, then so is G.

Assume $f(x)$ is solvable by radicals. Every root of $f(x)$ is contained in a root extension of the form $F = K_1 \subseteq K_1 \subseteq \cdots \subseteq K_n = K$, with $\mathrm{Gal}(K_{i+1}/K_i)$ cyclic. Let $L = K_0K_1K_2\cdots K_n$.

This is also a root extension. Then, $F = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_m = L$, with $\mathrm{Gal}(L_{i+1}/L_i)$ cyclic. Set $G_i = \mathrm{Gal}(L/L_i)$ (the group that corresponds to L_i). From the fundamental theorem of Galois theory, $G_i/G_{i+1} \cong \mathrm{Gal}(L_{i+1}/L_i)$ is cyclic. This yields the chain of groups.

We have $\mathrm{Spl}_F(f(x)) \subset L$, meaning $\mathrm{Gal}(f(x))$ is a quotient of $\mathrm{Gal}(L/F)$, which is itself solvable.

Suppose $\mathrm{Gal}(f(x))$ is solvable. Let $K = \mathrm{Spl}_F(f(x))$. Set $1 = G_n \leq G_{n-1} \leq \cdots \leq G_0 = G$. Set $K_i = K^{G_i}$. This gives a chain

$$F = K_0 \subset K_1 \subset \cdots \subset K_n = K.$$

Each of K_{i+1}/K_i is cyclic of degree m_i. Set F' to be F adjoin the m_i roots of unity for $m_1, m_2, \ldots, m_n$.

Form $K_i' = F'K_i$. We now have a sequence

$$F \subset F' = F'K_0 \subset F'K_1 \subset \cdots \subset F'K_n = F'K.$$

$$\begin{tikzcd}
 & F'K_{i+1} \arrow[dl, dash, "\cong"'] \arrow[dr, dash] & \\
F'K_i \arrow[dr, dash] & & K_{i+1} \arrow[dl, dash, "\cong"] \\
 & K_{i+1} \cap F'K_i \arrow[d, dash] & \\
 & K_i \arrow[uur, dash, bend right, "\text{cyclic of degree } m_i"'] &
\end{tikzcd}$$

Therefore,

$$\begin{aligned}\mathrm{Gal}(F'K_{i+1}/F'K_i) &\cong \mathrm{Gal}(K_{i+1}/K_{i+1} \cap F'K_i)\\ &\subseteq \mathrm{Gal}(K_{i+1}/K_i),\end{aligned}$$

meaning it is cyclic of degree dividing m_i. Thus, we have $F'K_{i+1} = F'K_i(\sqrt[n_i]{a_i})$, with $n_i \in \mathbb{Z}_{\geq 2}$, $a_i \in F'K_i$.

Corollary: Solvability of the Quintic

The general polynomial of degree ≥ 5 cannot be solved by radicals. The general polynomial of degree ≤ 4 can be.

We know that the Galois group of the general polynomial is S_n. It is known that S_n for $n \geq 5$ is not a solvable group, and S_n for $n \leq 4$ is a solvable group.