Number Fields and Galois Theory

Xavier Choe and Garima Rastogi

Abstract

In this program, we began by studying number theory, then transitioned to abstract algebra (with a focus on number fields) and finally Galois theory. In this paper, we start by introducing basic abstract algebra concepts such as fields, and the build up to the idea of number fields. From there, we study Galois extensions and Galois groups of these number fields. We also discuss prime ideals and factorization of rings of integers.

1 Abstract Algebra Prerequisites

In this section, we will cover the basic abstract algebra definitions and theorems as a basis for the main topic of this paper.

1.1 Group Theory

We start with the most basic object in algebra: the group.

Definition 1.1. A **group** G is a set which, under a binary operation $*$, satisfies the following four properties:

- Closure: For any two elements $x, y \in G$, the element $x * y$ is also in G.
- Associativity: For any elements $x, y, z \in G$, the binary operation is associative, i.e. $(x * y) * z = x * (y * z)$.
- Identity: There is an element $e \in G$, known as the identity, such that for all elements $x \in G$, we have that $x * e = e * x = x$.
- Inverses: For every element $x \in G$, there exists an element $y \in G$ known as the inverse of x, such that $x * y = y * x = e$.

Example 1.2. Some common examples of groups under addition include the group of integers modulo n, denoted $\mathbb{Z}/n\mathbb{Z}$; the group of integers, denoted $\mathbb{Z}$; the group of reals, denoted $\mathbb{R}$; the group of rationals, $\mathbb{Q}$; and the group of complex numbers, denoted $\mathbb{C}$.

The notion of the size of a group, also known as the order of the group, follows naturally.

Definition 1.3. The **order** of a group G is the number of elements in G, denoted $|G|$.

In terms of order, there are two types of groups:

Definition 1.4. A group with finite order are known as **finite groups**. A group with infinite order are known as **infinite groups**.

Example 1.5. Some examples of groups with finite order include $\mathbb{Z}/n\mathbb{Z}$, since $|\mathbb{Z}/n\mathbb{Z}| = n$, and the nth symmetric group S_n, since $|S_n| = n!$.

Example 1.6. Some examples of groups with infinite order include $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, and $\mathbb{Z}$.

Another way to classify groups is based on the property of commutativity:

Definition 1.7. A group G is **abelian** if it satisfies the condition of commutativity: for any two elements $x, y \in G$, $x * y$ must equal $y * x$.

Example 1.8. The group $\mathbb{Z}/n\mathbb{Z}$ is abelian because addition is commutative.

Of course, not all groups are abelian.

Example 1.9. For example, the symmetric groups S_n are not abelian. Such groups are called **non-abelian groups**.

Example 1.10. As another example, consider the group of symmetries of an equilateral triangle $D_3 = \{e, r, r^2, b, rb, r^2b\}$, where r is a rotation by 120 degrees around the center of the triangle and b is a reflection along the vertical axis of symmetry. This group is non-abelian, because rb is not the same as br (a rotation followed by a reflection is not the same as a reflection followed by a rotation).

Now, we consider subsets of groups which are still groups in their own right.

Definition 1.11. Let $(G, *)$ be a group. The subset $H \subset G$ is a **subgroup** of G if it is a group under $*$. We write $H \leq G$ to denote that H is a subgroup of G. When $H \neq G$, we call H a **proper subgroup** of G, which we can denote by $H < G$.

Example 1.12. When $k|n$ for two positive integers k and n, then $\langle k \rangle \subseteq \mathbb{Z}/n\mathbb{Z}$ (the subgroup generated by k) is a subgroup of $\mathbb{Z}/n\mathbb{Z}$.

Example 1.13. Similar to Example 1.12, the groups $n\mathbb{Z}$ for $n \in \mathbb{Z}$ are all subgroups of $\mathbb{Z}$.

Subgroups have a property known as cosets:

Definition 1.14. Let G be a group with $H \leq G$. The set $aH = \{ah \mid h \in H\}$ for any $a \in G$ is a **left coset** of H in G. Similarly, the set $Ha = \{ha \mid h \in H\}$ for any $a \in G$ is a **right coset** of H in G.

Example 1.15. For example, consider $5\mathbb{Z} \subset \mathbb{Z}$. The left coset $2 + H$ is $2 + 5\mathbb{Z} = \{... - 3, 2, 7, ...\}$.

Definition 1.16. In some cases, where G is a group and $H \leq G$, the left cosets aH are equivalent to the respective right cosets Ha for all $a \in G$. Such subgroups H are called the **normal subgroups** of G, and are denoted by $H \lhd G$.

Remark 1.17. In other words, the subgroup H "commutes with" any element of G. Another way to define this property is that conjugation by any $g \in G$ leaves H intact. In particular, all subgroups of an abelian group G are normal.

Example 1.18. For example, since $\mathbb{Z}$ is abelian, all subgroups $n\mathbb{Z} \lhd \mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ are normal.

Example 1.19. Other examples of normal subgroups include $\{e, b\} \lhd D_3$, where b is the operation as defined in Example 1.10.

Non-example 1.20. The subset $H = \{e, (12)\}$ of S_3 is not a normal subgroup since $(13)H \neq H(13)$.

We can also look at the group of cosets for a normal subgroup:

Definition 1.21. Let $(G, *)$ be a group with $H \lhd G$. The **quotient group** G/H is the group of cosets of H in G, closed under $*$.

Example 1.22. For example, take the group $\mathbb{Z}$ and its subgroup $2\mathbb{Z}$. As per Remark 1.17, we know that $2\mathbb{Z} \lhd \mathbb{Z}$, so we can look at the quotient group $\mathbb{Z}/2\mathbb{Z} = \{2\mathbb{Z}, 1 + 2\mathbb{Z}\}$, which, modulo 2, is equivalent to $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$.

So far, we have focused on groups with one operation. For this next section, let's look at groups with two operations.

1.2 Rings

Definition 1.23. A **ring** $(R, +, *)$ consists of a set R such that $(R, +)$ is an abelian group, with a secondary operation $*$. For any three elements $a, b, c \in R$, the following additional properties are satisfied:

- Associative under $*$: $a * (b * c) = (a * b) * c$.
- Distributive property: $a * (b + c) = a * b + a * c$ and $(b + c) * a = b * a + c * a$.

Convention. From now on, we will refer to the secondary operation $*$ as multiplication.

We now briefly introduce the idea of a subring. We will refer back to this idea in the next section.

Definition 1.24. Consider a ring $(R, +, *)$. A subgroup $S \subseteq R$ is a **subring** of the ring R such that $(S, +, *)$ is itself also a ring.

Example 1.25. For example, $\mathbb{R}$ is a subring of $\mathbb{C}$ (under the standard operations of addition and multiplication).

Just as there are abelian and non-abelian groups, there are commutative and non-commutative rings.

Definition 1.26. A ring R is called a **commutative ring** if the multiplication operation is also commutative.

Example 1.27. For example, the integers $\mathbb{Z}$ and the rationals $\mathbb{Q}$ are commutative rings under addition and multiplication.

Non-example 1.28. The ring of $n \times n$ matrices (for $n > 1$) with rational entries is a non-commutative ring because matrix multiplication is not commutative.

Definition 1.29. We call a ring R **unital** if there exists a multiplicative identity 1 in R. The multiplicative identity satisfies $1 * r = r * 1 = r$ for all $r \in R$.

Example 1.30. Some examples of unital rings include $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$, and $\mathbb{R}$.

Non-example 1.31. The set of 3 dimensional vectors $\mathbb{R}^3$ under addition with the secondary operation as cross product, is not a unital ring because there is no identity element for multiplication within the ring. (It turns out not to be a ring at all: the cross product is not associative.)

Non-example 1.32. The ring $n\mathbb{Z}$ is not a ring for any integer $n > 1$ because $1 \notin n\mathbb{Z}$.

Definition 1.33. A **unit** of R is an element $u \in R$ such that there exists $v \in R$ with $uv = 1$. Units are also known as invertible elements.

An interesting way to generate groups naturally is by taking all units of a ring.

Definition 1.34. The **group of units**, denoted $R^\times$, are the elements of R which are units.

Example 1.35. For example, $U_8 \coloneqq (\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$, since these are the only elements within $\mathbb{Z}/8\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6, 7\}$ with an inverse: 1 has an inverse of 1, 3 has an inverse of 3, 5 has an inverse of 5, and 7 has an inverse of 7.

In general, not all elements in a unital ring have an inverse.

Example 1.36. Consider the ring $\mathbb{Z}$. We see that 2 doesn't have an inverse, but the ring is unital because $1 \in \mathbb{Z}$.

Convention. For the rest of this paper, we will assume that all rings are commutative and unital. We simply use the term *ring* to refer to a commutative unital ring. We will also assume that that the group operation is addition and that the secondary operation is multiplication (in the usual sense).

Not all elements have inverses, but there are varying degrees of non-invertibility. One of the worse types is called a zero-divisor.

Definition 1.37. Let R be a ring. A nonzero element $r \in R$ is a **zero-divisor** if there exists another nonzero element $s \in R$ such that $r \cdot s = 0$.

Example 1.38. Consider the ring $\mathbb{Z}/50\mathbb{Z}$. The element 15 is a zero-divisor in this ring since $15 \cdot 40 = 600 \equiv 0 \pmod{50}$.

Definition 1.39. Rings that do not have any zero-divisors are called **integral domains**.

Example 1.40. The ring $\mathbb{Q}$ is an integral domain.

Example 1.41. For all prime p, the rings $\mathbb{Z}/p\mathbb{Z}$ are integral domains.

Non-example 1.42. For composite n, the rings $\mathbb{Z}/n\mathbb{Z}$ are not integral domains because the elements k such that $\gcd(k, n) > 1$ are zero-divisors.

Remark 1.43. Integral domains are not required to consist solely of units, since those two definitions are somewhat independent. For example, $\mathbb{Z}$ has only two units, being 1 and -1, but is still an integral domain since it has no zero-divisors.

We now define the idea of cancellation:

Definition 1.44. Take an integral domain R. For any set of three elements $x, y, z \in R$ such that $x \neq 0$, the **cancellation** property states that if $xy = xz$, then $y = z$. For an arbitrary ring R, where R is not necessarily an integral domain, if the above property holds for $x, y, z \in R$, then we say that the element x is **cancellative**.

Example 1.45. For example, consider the nonzero element 5 from the integral domain $\mathbb{Z}$. Since $\mathbb{Z}$ is an integral domain, $5y = 5z$ for $y, z \in \mathbb{Z}$ implies $y = z$.

Example 1.46. The ring $\mathbb{Z}/8\mathbb{Z}$ is not an integral domain, but $3 \in U_8$ is a cancellative element. (Even better, 3 is a unit.)

Now that we have discussed the idea of cancellation, we claim the following:

Lemma 1.47. *The following are equivalent for a ring R:*

- *R is an integral domain.*
- *R has the cancellation property.*

Proof. Consider an integral domain R. Take the elements $x, y, z \in R$ where $x \neq 0$ with $xy = xz$. We want to show that $y = z$. Then $xy - xz = x(y - z) = 0$, meaning either $x = 0$ or $y - z = 0$. Since we assumed that $x \neq 0$, we must have $y - z = 0$, so $y = z$.

Conversely, assume that the cancellation property $xy = xz$ applies. Since integral domains do not have any zero-divisors, we want to show that $xy = 0$ (for $x \neq 0$) implies $y = 0$. Take $z = 0$. Then $xy = xz = 0$. By the cancellation property, since $x \neq 0$, we have $y = z = 0$. □

Now, let's look at a special type of ring that also happens to be an integral domain - a fact that we will prove soon.

1.3 Fields

Definition 1.48. A **field** F is a (commutative) ring where every non-zero element is a unit.

Example 1.49. For example, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all fields.

Example 1.50. The ring of integers $\mathbb{Z}$ is not a field since only 1 and -1 have multiplicative inverses.

Example 1.51. Finite fields, denoted $\mathbb{F}_q$ for some prime power $q = p^k$, are the (unique, up to isomorphism) field with q elements. In particular, for $q = p$ a prime, $\mathbb{F}_p$ is just $\mathbb{Z}/p\mathbb{Z}$. Furthermore, for any $q = p^k$, $1 \in \mathbb{F}_q$ generates a subfield isomorphic to $\mathbb{F}_p$, since the characteristic is p (these notions are discussed shortly).

Now that we have our basic definition down for this section, let's prove the following theorem:

Theorem 1.52. *Every field is an integral domain.*

Proof. Consider a field F. Take $x, y \in F$, where $x \neq 0$, and suppose $xy = 0$. Since x is a nonzero element of F, it has an inverse x^{-1}. Multiplying both sides of $xy = 0$ by x^{-1}, we get $x^{-1}xy = x^{-1}0$. Since $x^{-1}x = 1$, the equation reduces to simply $y = 0$, thus showing there are no zero divisors in a field. □

Every ring has an attribute called its *characteristic*, which is particularly important for fields:

Definition 1.53. The **characteristic** of a ring R, denoted by char R, is the least positive integer n such that $nx = 0$ for all x in R. If there is no such integer, then the characteristic is 0.

Remark 1.54. If the ring is unital, for example if it is a field, the characteristic can be found by checking just $x = 1$.

Example 1.55. For example, the ring $\mathbb{Z}/n\mathbb{Z}$ has characteristic n.

All integral domains, and thus all fields, have a characteristic of 0 or a prime number p, since they have no zero-divisors. Additionally, a field F is said to be *perfect* if its characteristic is 0, or if the characteristic is $p > 0$ such that the set of values a^p for all elements $a \in F$ is equivalent to the field F.

1.4 Extras with rings and fields

Let's now look at ideals, which are the ring analog for normal subgroups.

Definition 1.56. For a ring R, a subset $S \subseteq R$ is an ideal of R if, for every $r \in R$ and every $s \in S$, we have $rs \in S$. An ideal S is a **proper ideal** of R when $S \subsetneq R$.

Example 1.57. Every ring R is an ideal of itself.

Example 1.58. For every ring R, $\{0\}$ is an ideal, since $0 \cdot r = r \cdot 0 = 0$ for any $r \in R$. This ideal is also known as the **trivial ideal** of a ring.

Example 1.59. The only ideals of $\mathbb{Q}$ (or any field) are itself and the trivial ideal.

The ring analogy for quotient groups are *quotient rings*.

Definition 1.60. A **quotient ring**, also known as a **factor ring**, of a ring R is the ring of cosets $R/S = \{r + S | r \in R\}$ for an ideal S of the ring.

Another type of ideals, namely *prime ideals*, follow an idea similar to the well-known theorem stating that for a prime p and $a, b \in \mathbb{Z}$, if $p \mid ab$, then $p \mid a$ or $p \mid b$:

Definition 1.61. Consider a ring R. A **prime ideal** is a proper ideal $\mathfrak{p}$ of R such that, for any two elements $r, s \in R$, if $rs \in \mathfrak{p}$, then $r \in \mathfrak{p}$ or $s \in \mathfrak{p}$. Equivalently, $R/\mathfrak{p}$ is an integral domain.

Example 1.62. The prime ideals of $\mathbb{Z}$ are (0) and (p) for all prime integers p.

Example 1.63. The prime ideals of $\mathbb{C}[x]$ are $(x-a)$ for all $a \in \mathbb{C}$ and (0).

Non-example 1.64. The ideal $(3, x^2+11)$ of $\mathbb{Z}[x]$ is not prime since $x^2+11-3\cdot 4 = x^2-1 = (x-1)(x+1)$, but neither $x-1$ nor $x+1$ is in the ideal.

Another type of ideal that we will discuss is the *maximal ideal*.

Definition 1.65. Consider a ring R. An ideal $\mathfrak{m}$ is a **maximal ideal** if the only ideal properly containing $\mathfrak{m}$ is R itself. Equivalently, $R/\mathfrak{m}$ is a field.

Remark 1.66. Every maximal ideal is a prime ideal, but not all prime ideals are maximal ideals.

Example 1.67. The ring $n\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$ if and only if $n = p$ is prime.

Non-example 1.68. The zero ideal $\{0\}$ of $\mathbb{Z}$ is prime but not maximal.

Before moving on, let's define subfields and extension fields.

Definition 1.69. Consider a field $(F, +, *)$. A subset K of F is a **subfield** if $(K, +, *)$ is a field.

Example 1.70. The set of real numbers $\mathbb{R}$ is a subfield of $\mathbb{C}$, since both are fields under the operations of addition and multiplication.

Example 1.71. The set of numbers $a + bi$ where $a, b \in \mathbb{Q}$ is a subfield of $\mathbb{C}$, since it forms a field and all elements are contained in $\mathbb{C}$.

Non-example 1.72. For $a, b \in \mathbb{N}$, where $\mathbb{N}$ is the group of natural numbers, the set of numbers $a + bi$ is not a subfield of $\mathbb{C}$ since, even though all its elements are contained in $\mathbb{C}$, it does not form a field , or even a group under addition, due to lack of inverses.

An extension field is essentially the opposite of a subfield:

Definition 1.73. For two fields F and E, F is an **extension field** of E if E is a subfield of F.

Example 1.74. The set of complex numbers $\mathbb{C}$ is an extension field of $\mathbb{R}$ because $\mathbb{R} \subseteq \mathbb{C}$ and $\mathbb{C}$ is a field.

1.5 Vector Spaces

Definition 1.75. Let F be a field. A **vector space** V over F is an abelian group closed under addition equipped with a scalar multiplication map. The following properties hold, for all elements $x, y \in V$ and $a, b \in F$:

- $a(x+y) = ax + ay$.

- $(a+b)x = ax + bx$.
- $a(bx) = (ab)x$.
- $1v = v1 = v$.

For the rest of this section, we will use F to denote the base field, and V to denote the vector space over F.

Definition 1.76. A **subspace** of V over F is a subset U of V which is also a vector space over F.

Definition 1.77. A **basis** B of V over F is a subset of V of *linearly independent* vectors such that every element in V can be written (uniquely) as a linear combination of the elements in B.

Definition 1.78. The **dimension** of V is the size of the basis of V.

Remark 1.79. Vector spaces can have many different bases, but in each case, the size of the basis is always the same. Additionally, every finite dimensional vector space has a basis, and an infinite-dimensional vector space has a basis if we assume the axiom of choice.

Example 1.80. For example, $\mathbb{R}^n = \{(a_1, a_2, ..., a_n) \mid a_i \in \mathbb{R}\}$ is a vector space over $\mathbb{R}$ with dimension n.

Definition 1.81. Let F/E be a field extension; then E can be considered a vector space over F. The **degree** of E/F is the dimension of E.

Now, let's look at some types of group actions.

1.6 Homomorphisms

Definition 1.82. Consider two groups $(G, *_1)$. A **homomorphism** from G to another group $(H, *_2)$ is a function ϕ that maps G to H such that for all $a, b \in G$ we have $\phi(a *_1 b) = \phi(a) *_2 \phi(b)$ and $\phi(1_G) = 1_H$.

Example 1.83. Consider $G = H = \mathbb{Z}$, closed under addition. Define $\phi(x) = -x$ for all $x \in \mathbb{Z}$. Then, for $a, b \in \mathbb{Z}$, we have $\phi(a+b) = -a-b = (-a)+(-b) = \phi(a)+\phi(b)$, as desired.

Definition 1.84. The **kernel** of a homomorphism ϕ, denoted as $\ker \phi$, is the set of elements $x \in G$ such that $\phi(x) = e$, where e is the identity element in G.

Definition 1.85. A homomorphism ϕ that is bijective is called an **isomorphism**. For two groups G and H of the same order, an isomorphism from G onto H is denoted by $G \cong H$.

Definition 1.86. An **automorphism** is an isomorphism of a group to itself. In the case of E, an extension field of a field F, an automorphism of E is a ring isomorphism from E onto E. We say an automorphism α of E fixes F if, for all elements $f \in F$, $\alpha(f) = f$ is satisfied.

Homomorphisms, isomorphisms, and automorphisms are all defined for rings, fields, and vector spaces. The only additional statement in the case of rings, fields, and vector spaces is that the mapping function must respect both operations of the structure.

2 Number Fields

Definition 2.1. Algebraic number fields K, also known as **number fields**, are finite degree extension fields of $\mathbb{Q}$. In other words, the following conditions are satisfied:

- K is a field.
- $\mathbb{Q} \subseteq K$.
- K is a finite dimension vector space over $\mathbb{Q}$.

Example 2.2. For example, $\mathbb{Q}$, $\mathbb{Q}(i)$, and $\mathbb{Q}(\sqrt{d})$ are all number fields.

Example 2.3. The nth cyclotomic field $\mathbb{Q}(\zeta_n)$ consists of $\mathbb{Q}$-linear combinations of the n complex solutions to $x^n = 1$. The solutions to $x^n = 1$ are generated by the n powers of $\zeta_n = e^{\frac{2\pi i}{n}}$. Additionally, the dimension of $\mathbb{Q}(\zeta_n)$ as a vector space over $\mathbb{Q}$ is $\phi(n)$ (rather than n).

Non-example 2.4. The finite fields $\mathbb{F}_q$ are not number fields because they do not contain $\mathbb{Q}$.

Non-example 2.5. The fields $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Q}(\pi)$, or $\mathbb{Q}$ adjoin any transcendental number, are not number fields because they are infinite-dimensional vector spaces over $\mathbb{Q}$ (alternatively, infinite-degree extensions).

Non-example 2.6. The ring $\mathbb{Q}[x]/(x^2)$ is not a number field because it is not a field.

Minimal polynomials are an attribute of number fields:

Definition 2.7. Let F be a field and $a \in F$. The **minimal polynomial** of a (over F) is the minimum degree polynomial $f_a(x) \in F[x]$ satisfying the following properties:

- f_a is monic.
- f_a is irreducible over F.
- $f_a(a) = 0$.

Proposition 2.8. *Let $K \subset L$ be an extension of number fields and $\alpha \in L$. A minimal polynomial $f(x)$ satisfies the following properties:*

- *It has the lowest degree of any polynomial with α as a root.*
- *It is unique.*
- *It is irreducible in $K[x]$.*

Proposition 2.9. *Let $K \subset L$ be a finite extension of number fields. Then any $\alpha \in L$ is the root of some minimal polynomial $f(x) \in K[x]$.*

The following theorem, known as the Primitive Element Theorem, characterizes number fields:

Theorem 2.10 (Primitive Element Theorem)**.** *Every finite extension of* $\mathbb{Q}$ *is of the form* $\mathbb{Q}(\alpha)$*, where* α *is a root of some minimal polynomial* $f(x)$ *over* $\mathbb{Q}$*.*

This finite extension is often written as $\mathbb{Q}[x]/f(x)$, where $f(x)$ is the minimal polynomial for x over $\mathbb{Q}$. It turns out that $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/f(x)$, which suggests that α is only "distinguishable" up to its conjugates (the other roots of $f(x)$). This important observation is fundamental to the next section, which is Galois theory.

Definition 2.11. The algebraic integers $\overline{\mathbb{Z}}$ is the subset of $\mathbb{C}$ whose minimal polynomial over $\mathbb{Z}$ is monic.

Definition 2.12. The **ring of integers** of a number field K is $\mathcal{O}_K \coloneqq K \cap \overline{\mathbb{Z}}$.

One way to view the ring of integers is as the "integer" part of the field K. Just as $\mathbb{Z}$ is the "integer" part of $\mathbb{Q}$, we can try to determine which subring of K is the "integer" part of K; we find it is $\mathcal{O}_K$. Furthermore, K is the field of fractions of $\mathcal{O}_K$.

Note that $K \subset L$ implies that $\mathcal{O}_K \subset \mathcal{O}_L$. Since $K \subset L$, we have that the intersection of K with a set S is a subset of the intersection of L with a set S. In this case, $S = \overline{\mathbb{Z}}$, so $K \cap \overline{\mathbb{Z}} = \mathcal{O}_K \subset L \cap \overline{\mathbb{Z}} = \mathcal{O}_L$.

Proposition 2.13. *Let* K *be a number field. The ring of integers* $\mathcal{O}_K$ *is a Dedekind domain. That is, all prime ideals are maximal, and ideals factor uniquely into products of prime ideals.*

Example 2.14. The ring of integers of $\mathbb{Q}$ is $\mathbb{Z}$.

Example 2.15. The ring of integers of $\mathbb{Q}(i)$ is $\mathbb{Z}[i]$.

Example 2.16. The ring of integers of $\mathbb{Q}(\sqrt{2})$ is $\mathbb{Z}[\sqrt{2}]$.

Remark 2.17. The ring of integers of $\mathbb{Q}(\sqrt{d})$ is not always $\mathbb{Z}[\sqrt{d}]$. For example, the ring of integers of $\mathbb{Q}(\sqrt{d})$ for $d \equiv 1 \pmod 4$ (and d squarefree) is actually $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

Now, let's move onto Galois Theory.

3 Galois Theory

Galois theory understands the automorphisms of a field preserving a subfield. The relevant groups are called the *Galois group* field extension.

3.1 Motivation

Before we dive into the particulars of this branch of math, we will introduce the motivation behind Galois Theory.

One way to motivate Galois Theory is to consider $\sqrt{-1}$, or alternatively, solutions to the polynomial $x^2 + 1$. Since both i and $-i$ are solutions, we effectively cannot tell apart i and $-i$.

We can look at this in the context of automorphisms of $\mathbb{C}$ preserving $\mathbb{R}$. These automorphisms are $\{1, \sigma\}$, where 1 is the identity and σ is a complex conjugation. It turns out that this set of automorphisms forms a group, called a Galois Group.

Using Galois Groups and Galois Extensions, one of the aims of Galois Theory is to find a way to quantify this issue of i and $-i$. We can view $\mathbb{C}$ as $\mathbb{R}$ adjoin i or $-i$, and they give the same field.

To begin this topic, we will first define normal and separable, which are the two defining components of Galois extensions.

3.2 Normal and Separable Extensions

Definition 3.1. Let K be a field and $f(x) \in K[x]$ a polynomial. We define the **splitting field** of f (with respect to K) to be the minimal field extension of K such that f splits into linear factors in this field extension.

Example 3.2. Taking $K = \mathbb{Q}$, the splitting field of $f(x) = x^2 + 1$ is $\mathbb{Q}(i)$.

Example 3.3. Taking $K = \mathbb{Q}$, the splitting field of $f(x) = x^3 - 2$ is $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$.

Definition 3.4. A field extension $K \subset L$ is **normal** if every irreducible polynomial over K either has no roots in L or splits into linear factors over L.

Example 3.5. In particular, all splitting fields are normal extensions.

Example 3.6. The extension $\mathbb{C}/\mathbb{R}$ is normal since all the roots of every polynomial with coefficients in $\mathbb{R}$ are in $\mathbb{C}$.

Example 3.7. The extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is normal because it is the splitting field of $x^2 - 2$; it has no roots in $\mathbb{Q}$ but all roots are in $\mathbb{Q}(\sqrt{2})$.

Example 3.8. The extension $\mathbb{Q}(i)/\mathbb{Q}$ is normal because it is the splitting field of $x^2 + 1$, which has no roots in $\mathbb{Q}$ but all are in $\mathbb{Q}(i)$.

Non-example 3.9. The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal because the minimal polynomial of $\sqrt[3]{2}$ is $x^3 - 2$, which has no roots in $\mathbb{Q}$ but only one of its 3 roots (viewed inside $\mathbb{C}$) is in $\mathbb{Q}(\sqrt[3]{2})$.

Definition 3.10. A field extension $F \subset E$ is **separable** if for every $\alpha \in E$, the minimal polynomial of α over F has no repeated roots in any extension (equivalently, its formal derivative is nonzero).

Example 3.11. Any extension of a field of characteristic zero is automatically separable because the formal derivative of any (nonconstant) polynomial is nonzero. Since all number fields are extensions of $\mathbb{Q}$, extensions of number fields are always separable.

Non-example 3.12. Consider $(X^p - t)/\mathbb{F}_p(t) \subset \mathbb{F}_p(t)[X]$. The minimal polynomial of t has the root $t^{1/p}$ with multiplicity p. Another way to see this is that the formal derivative of the minimal polynomial of t, which is $X^p - t$, is $pX^{p-1} = 0$.

3.3 Galois Extensions

Definition 3.13. As mentioned in Section 3.1, a field extension is **Galois** if it is both normal and separable. Since we are working mainly with number fields, by Example 3.11, we only need to check if a number field is normal to determine whether it is Galois.

Example 3.14. A splitting field is normal (Example 3.5). If the base field has characteristic 0, then it is also separable, and therefore Galois.

In the case of a Galois extension, we can define the Galois group.

Definition 3.15. Let $F \subset E$ be a Galois extension. The **Galois group** of E/F, denoted as $G = \mathrm{Gal}(E/F)$, is the group of all automorphisms of E that map every element of F to itself.

Consider the Galois extension $F \subset E$ with Galois group G. It is known that not all elements - if any - have to map to themselves in any given automorphism. However, the set of all the elements which do map to themselves under all automorphisms in some subgroup $H \leq G$ are known as the **fixed field** of H. In fact, the fixed field of G's largest subgroup - itself - is the base field F. For this reason, a Galois group of an extension field E over F is also referred to as "the group of automorphisms of E over F preserving F."

Proposition 3.16. *Let E/F be a Galois extension. The only elements of E fixed by $\mathrm{Gal}(E/F)$ are F.*

Proposition 3.17. *If E/F is a Galois extension, then $[E : F] = |\mathrm{Gal}(E/F)|$.*

Now, let's look at some examples of Galois extensions.

Example 3.18. The extension $\mathbb{C}/\mathbb{R}$ is Galois. We showed it's normal in Example 3.6, and separable in Example 3.11.

Example 3.19. The extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is Galois. We showed it's normal in Example 3.7, and separable in Example 3.11.

Example 3.20. The extension $\mathbb{Q}(i)/\mathbb{Q}$ is Galois. We showed it's normal in Example 3.8, and separable in Example 3.11.

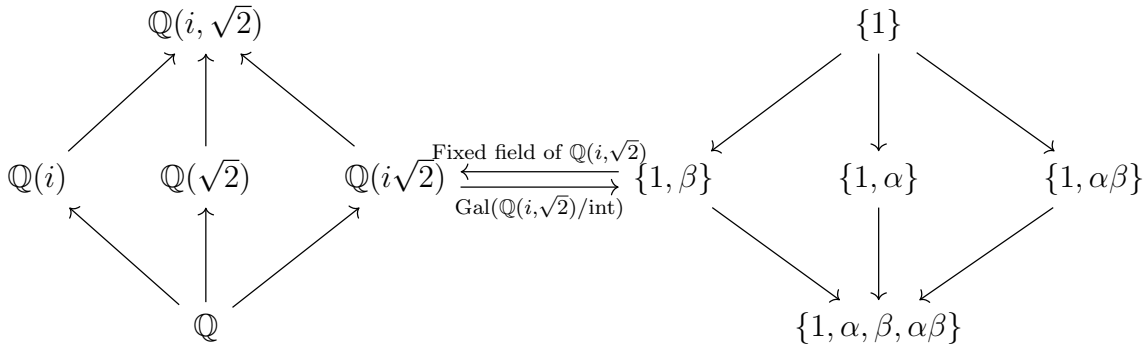
Example 3.21. The extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is separable because both fields are characteristic 0. It is also normal because it is the splitting field of $\Phi_n(x)$, the n^{th} cyclotomic polynomial (alternatively, $x^n - 1$ if we use non-irreducible polynomials). As a result, it is Galois. The roots of $\Phi_n(x)$ are precisely ζ_n^k for $\gcd(k, n) = 1$, so any automorphism is determined by $\zeta_n \mapsto \zeta_n^k$ for $\gcd(k, n) = 1$; this implies that the Galois group is in bijection with k with $\gcd(k, n) = 1$. Therefore the Galois group is $(\mathbb{Z}/n\mathbb{Z})^\times$.

Non-example 3.22. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal, and therefore not Galois. The only automorphism of $\mathbb{Q}(\sqrt[3]{2})$ fixing $\mathbb{Q}$ is the identity, so there is only one such automorphism, even though the degree of the extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ is 3 (violating Proposition 3.17).

3.4 The Galois Correspondence

Theorem 3.23. *Let L/K be a Galois extension. There is an inclusion-reversing bijection between subgroups of $\mathrm{Gal}(L/K)$ and intermediate fields $K \subset M \subset L$. The two (mutually inverse) directions are $G \supset H \mapsto L^H$ and $M \mapsto \mathrm{Gal}(L/M) \subset \mathrm{Gal}(L/K)$.*

Example 3.24. We can visualize the Galois Correspondence for $\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}$ as follows:



Here, α is the automorphism such that $\alpha(\sqrt{2}) = \sqrt{2}$ and $\alpha(i) = -i$, and β is the automorphism such that $\beta(\sqrt{2}) = -\sqrt{2}$ and $\beta(i) = i$. On the left of this visual is the Galois extension and its intermediate fields. On the right is the corresponding Galois Group and its subgroups. We can see from this visual that the fixed field of $\{1, \alpha, \beta, \alpha\beta\}$ is $\mathbb{Q}$, the fixed field of $\{1, \beta\}$ is $\mathbb{Q}(i)$ and the fixed field of $\{1\}$ is $\mathbb{Q}(i, \sqrt{2})$.

This correspondence between the intermediate fields of a Galois extension and the subgroups of the Galois group is the basis of the fundamental theorem of Galois theory.

4 Factorization of prime ideals

Section Notation 4.1. Let $K \subset L$ be an extension of number fields. Then $\mathcal{O}_K \subset \mathcal{O}_L$. Pick a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$. Then $\mathfrak{p}\mathcal{O}_L$ is an ideal, but not necessarily prime. In this section, we will understand its prime factorization into prime ideals.

Because $\mathfrak{p}\mathcal{O}_L$ is an ideal of $\mathcal{O}_L$, it factors uniquely into a product of prime ideals by Proposition 2.13, so $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{q}_i^{e_i}$ (where $\mathfrak{q}_i$ are prime ideals of $\mathcal{O}_L$).

Any $\mathfrak{q}_i \subset \mathcal{O}_L$ must contain $\mathfrak{p} \subset \mathcal{O}_K$, so we have the well-defined injection $\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{q}_i$ for every i. Because these are Dedekind domains, each of the quotients is a field, so we have an extension of (finite) fields. Denote $f_i \coloneqq [\mathcal{O}_L/\mathfrak{q}_i : \mathcal{O}_K/\mathfrak{p}]$.

Proposition 4.1. *Using Section Notation 4.1, we have*

$$[L : K] = \sum_{i=1}^{r} e_i f_i.$$

Proposition 4.2. *Under the assumptions of Section Notation 4.1, if $K \subset L$ is also Galois, then $e_1 = \cdots = e_r$ and $f_1 = \cdots = f_r$. Let $e \coloneqq e_1 = \cdots = e_r$ and $f \coloneqq f_1 = \cdots = f_r$. In particular, $[L : K] = ref$.*

In this case, $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{r} \mathfrak{q}_i^{e}$. The $\mathfrak{q}_i$ are related to each other via the Galois group:

Proposition 4.3. *Under the assumptions of Section Notation 4.1, the Galois group $\mathrm{Gal}(L/K)$ acts transitively on the set of primes lying above any prime ideal of $\mathcal{O}_K$. In the above notation, the Galois group acts transitively on the $\mathfrak{q}_i$.*

4.1 Computing the factorization concretely

Let's now work on determining the prime factorization under the assumption that the base field is $\mathbb{Q}$.

Let K be a number field. We have $\mathbb{Q} \subset K$, so on the ring of integers this restricts to an inclusion $\mathbb{Z} \subset \mathcal{O}_K$.

The prime ideals of $\mathbb{Z}$ are (p) for a prime p. We will compute the factorization of $p\mathcal{O}_K$ into prime ideals.

Theorem 4.4. *Let $\mathcal{O}_K = \mathbb{Z}[\alpha]$ where the minimal polynomial of α is $f(x) \in \mathbb{Z}[x]$. Consider the irreducible polynomials $g_i(x)$ in $\mathbb{Z}/p\mathbb{Z}$. We can write the prime factorization of $f(x) \pmod p$ as $f(x) \equiv \prod_{i=1}^{r} g_i(x)^{e_i} \pmod p$. For all but finitely many primes p, the ideal $p\mathcal{O}_K$ factors into $\prod_{i=1}^{r}(p, g_i(\alpha))^{e_i}$, and $f_i = \deg g_i$.*

Example 4.5. For $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, the minimal polynomial is $x^2 - 2$. We look at this modulo the primes $p = 2, 3, 5, 7, 11$:

(2) $x^2 - 2 \equiv 0 \pmod 2$ is $x^2 \equiv 0 \pmod 2$, so $x \equiv 0 \pmod 2$. So, the factorization of $2\mathcal{O}_{\mathbb{Q}(\sqrt{2})}$ is $(2, \sqrt{2})(2, \sqrt{2})$.

(3) $x^2 - 2 \equiv 0 \pmod 3$ is $x^2 \equiv 2 \pmod 3$. This equation has no real solutions, so the ideal $3\mathcal{O}_{\mathbb{Q}(\sqrt{2})}$ is prime.

(5) $x^2 - 2 \equiv 0 \pmod 5$ is $x^2 \equiv 2 \pmod 5$. This equation has no real solutions, thus the ideal $5\mathcal{O}_{\mathbb{Q}(\sqrt{2})}$ is prime.

(7) $x^2 - 2 \equiv 0 \pmod 7$ is $x^2 \equiv 9 \pmod 7$, with solutions $x \equiv 3, 4 \pmod 7$. So, the factorization of $7\mathcal{O}_{\mathbb{Q}(\sqrt{2})} = (7, \sqrt{2} - 3)(7, \sqrt{2} - 4)$.

(11) $x^2 - 2 \equiv 0 \pmod{11}$ is $x^2 \equiv 2 \pmod{11}$. This equation has no real solutions, thus the ideal $11\mathcal{O}_{\mathbb{Q}(\sqrt{2})}$ is prime.

In the final section, we will look at the case where the Galois extensions of a certain type exhibit a more predictable behavior.

5 Kronecker-Weber

Any Galois extension produces a Galois group. As discussed in Definition 1.7, abelian groups are groups which are often easier to work with. If the Galois group is abelian, we might expect to be able to deduce more of the structure of the extension. The Kronecker-Weber theorem describes abelian Galois extensions of $\mathbb{Q}$ in a very concrete way.

Theorem 5.1 (Kronecker-Weber)**.** *Every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field $\mathbb{Q}(\zeta_n)$.*

We know that the Galois group of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is $(\mathbb{Z}/n\mathbb{Z})^\times$, from Example 3.21. We might expect that every finite abelian group is also the Galois group of some extension of $\mathbb{Q}$, from Kronecker-Weber and knowing the Galois group of cyclotomic fields. Every finite abelian group is of the form $\mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_k\mathbb{Z}$ for positive integers n_i. In particular, $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^k})/\mathbb{Q}) \cong (\mathbb{Z}/p^k\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)p^{k-1}\mathbb{Z})$. This

group has a subgroup (generated by $p-1$) isomorphic to $\mathbb{Z}/p^{k-1}\mathbb{Z}$, which by the Galois correspondence, corresponds to a subfield of $\mathbb{Q}(\zeta_{p^k})$. Therefore intuitively, we might expect that we can find some sufficiently large n such that $\mathbb{Z}/n_1\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/n_k\mathbb{Z}$ is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$.

This turns out to be true.

Theorem 5.2 (Inverse Galois Problem for abelian groups)**.** *Every finite abelian group is the Galois group of an extension of* $\mathbb{Q}$*.*

Proof. Consider any finite abelian group $G \cong \mathbb{Z}/t_1\mathbb{Z} \times \cdots \times \mathbb{Z}/t_n\mathbb{Z}$ for positive integers t_i. By Dirichlet's theorem on arithmetic progressions, there exists (infinitely many, although we only need one) primes p_i such that $t_i | p_i - 1$. Then let $c = \prod p_i$. We have that

$$(\mathbb{Q}(\zeta_c)/\mathbb{Q}) \cong (\mathbb{Z}/c\mathbb{Z})^\times \cong \prod(\mathbb{Z}/p_i\mathbb{Z})^\times \cong \prod \mathbb{Z}/(p_i-1)\mathbb{Z},$$

and this contains the subgroup $H = \prod \frac{p_i-1}{t_i}\mathbb{Z}/(p_i-1)\mathbb{Z}$. Thus the field fixed by H has Galois group

$$(\mathbb{Q}(\zeta_c)^H/\mathbb{Q}) \cong (\mathbb{Q}(\zeta_c)/\mathbb{Q})/H \cong \prod \mathbb{Z}/t_i\mathbb{Z} \cong G.$$

□

Acknowledgments

We would like to thank the MIT Math Department for this opportunity, Dr. Haine for organizing PRIMES Circle, and our mentor Merrick for his guidance and encouragement throughout the program.