In the previous section, we have introduced some basics about group, ring and field theories. We start this section [1] by introducing field extension that is fundamental to understand number field. All things lead to the Galois group in the end, which is interesting in itself as well as gives insights of cyclotomic number field that is widely used across recent lattice-based cryptography and homomorphic encryption developments.

0.1 Field extension

The concept of field extensions is fundamental in solving polynomials, especially polynomials with rational coefficients, denoted by $\mathbb{Q}[x]$. The first attempt to solve these polynomials is to find their roots in the field of rationals $\mathbb{Q}$. For some rational (coefficient) polynomials, however, their roots only exist beyond $\mathbb{Q}$. For example, the polynomial $x^2 - 2$ has two irrational roots $\pm\sqrt{2}$. For this reason, we need to construct a field that is larger than $\mathbb{Q}$ so that it includes all roots of the polynomial $x^2 - 2$, but not too large that includes many unnecessary values. To achieve this goal, we first define extension fields.

Definition 0.1.1. *If a field F is contained in a field E, then E is called an* ***extension field*** *of F.*

Field extension

If E is an extension (field) of F, then F is a **subfield** of E. This pair of fields is called a **field extension** and denoted by E/F.

For the above example $x^2 - 2$, we can **adjoin** to $\mathbb{Q}$ the roots of this polynomial to get a larger field that includes all the roots of $x^2 - 2$, denoted by $\mathbb{Q}(\pm\sqrt{2}) := \{a \pm b\sqrt{2} \,:\, a, b \in \mathbb{Q}\}$. Note that since an extension field is also a field, it is sufficient to adjoin only $\sqrt{2}$. Being a field also implies the extension $Q(\sqrt{2})$ includes more elements such as $1 + \sqrt{2}$, $5\sqrt{2}$ and so on.

F-vector space

Given a field extension E/F, the larger field E forms a vector space over F, which is also known as an **F-vector space**. The larger field E consists of the "vectors" in the vector space and the smaller field F consists of the scalars for multiplying with the vectors. For example, $\mathbb{Q}(\sqrt{2})$ forms a $\mathbb{Q}$-vector space, because the extension $\mathbb{Q}(\sqrt{2})$ is closed under addition (satisfying commutativity, associativity, additive identity and inverse) and scalar multiplication with $\mathbb{Q}$ (satisfying compatibility, scalar identity in $\mathbb{Q}$, distributivity of scalar multiplication w.r.t. scalar addition in $\mathbb{Q}$ or addition in $\mathbb{Q}(\sqrt{2})$).

Field extension degree

Since an extension forms a vector space over the base field, it makes sense to talk about the degree of an extension.

Definition 0.1.2. *Give a field extension E/F, the* ***degree*** *of the extension field E, denoted by $[E : F]$, is the dimension of the vector space formed by E over F.*

An extension E is **finite** if its degree is finite. Otherwise, it is infinite. There are at least two ways of counting the dimension of an extension. One way is through the degree of the minimal polynomial of a primitive element that generates the extension. This will be discussed in more detail in subsequent subsections.

The other way of counting the dimension of the extension field is by counting the number of linearly independent vectors in its basis (same as for vector spaces in linear algebra). Hence, one could specify a basis of the extension over the base field in order to get the degree of the extension. For example, the degree $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$, $[\mathbb{C} : \mathbb{R}] = 2$ because the corresponding basis for each extension field is $\{1, \sqrt{2}\}$, $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$, $\{1, i\}$ respectively.

Similar to Lagrange's theorem in group theory, the degrees of extensions follow the "Tower Law".

Proposition 0.1.3. *(The Tower Law) If L/M and M/K are field extensions (finite or infinite), then the degrees of the extensions satisfy*

$$[L : K] = [L : M][M : K].$$

Intuitively, L forms a M-vector space and M forms a K-vector space, so L also forms a K-vector space. Each dimension in L over M is again a $[M : K]$-dimensional vector space.

The following subsections introduce some special types of field extensions that eventually lead to Galois extensions and Galois groups.

[1] This section is part of the work *A Tutorial Introduction to Lattice-based Cryptography and Homomorphic Encryption* by the authors Yang Li, Kee Siong Ng, Michael Purcell from the School of Computing, Australian National University @2022.

0.1.1 Algebraic extension

Historically, solving mathematical equations with rational coefficients was a natural but challenging task. This lead to the definition of algebraic numbers that are roots of non-zero rational polynomials. More formally,

Algebraic number

Definition 0.1.4. *A complex number is **algebraic** (over the rationals $\mathbb{Q}$) if it is a root of a non-zero polynomial whose coefficients are rational numbers. That is, $r \in \mathbb{C}$ is an algebraic number if it satisfies $f(r) = 0$ for some non-zero polynomial $f(x) \in \mathbb{Q}[x]$.*

All rational numbers are algebraic because they can be written in a linear equation $x - r$ for all $r \in \mathbb{Q}$. The irrational number $\sqrt{2}$ is algebraic because it is a root of $x^2 - 2$. The complex number i is also algebraic because it is a root of x^2+1. Complex numbers that are not algebraic are called **transcendental**. In other words, transcendental numbers are not roots of any rational coefficient polynomials. For example, the number π or e.

Almost all real numbers are not algebraic. The set of real numbers is uncountable, but the set of algebraic numbers are countable. That is, there is a one-to-one correspondence between all the algebraic numbers and the natural numbers.

When developing cryptosystems, we almost always work with integer (coefficient) polynomials $\mathbb{Z}[x]$. Within $\mathbb{Z}[x]$, monic polynomials are of special interest due to their computational efficiency. A polynomial is **monic** if the coefficient of its leading term (i.e., the term with the highest degree) is one. For example, when dividing polynomials, it is convenient to work with integer polynomials with leading coefficient one. In most cases, we work with polynomials defined over a field (e.g., $\mathbb{Z}_p[x]$ for prime p), so even if it is not monic, it can always made monic by dividing its coefficients with the leading term's coefficient.

Algebraic integer

Definition 0.1.5. *A complex number is an **algebraic integer** if it is a root of a monic polynomial with integer coefficients.*

Algebraic integers are generalization of ordinary integers which we call rational integers. Similar to numbers, field extensions can be algebraic or transcendental too.

Algebraic extension

Definition 0.1.6. *A field extension E/F is **algebraic** if every element in the extension field E is algebraic.*

Since all rational numbers are algebraic, a field extension $\mathbb{Q}(\alpha)$ is algebraic if all the additional elements are algebraic.

All transcendental extensions are of infinite degree. For example, the transcendental extension $Q(\pi)$ has a basis $\{1, \pi, \pi^2, \pi^3, \dots\}$ of infinite linearly independent vectors. The above statement also implies that all finite extensions are algebraic. This is also proved in the following proposition.

Proposition 0.1.7. *Every finite extension is algebraic.*

Proof. Let E be an extension over F with a finite degree $[E : F] = n$. For an element $x \in E$, the elements $1, x, x^2, \dots, x^n \in E$ because E is a field. These $n+1$ elements are also in the n-dimensional vector space over F, so must be linear dependent. Hence, there exists a set of non-zero coefficients $\{a_0, \dots, a_n\}$ such that $1 + a_1x + a_2x^2 + \cdots + a_nx^n = 0$. This implies that x is algebraic. □

Algebraic closed

Definition 0.1.8. *A field F is **algebraically closed** if for any polynomial $f(x) \in F[x]$, all of its roots are in the field F.*

Obviously $\mathbb{Q}$ and $\mathbb{R}$ are not algebraically closed, but $\mathbb{C}$ is. This is the **Fundamental Theorem of Algebra**. It implies that all polynomials can be completely solved or factored into linear factors in the complex field $\mathbb{C}$.

As mentioned earlier, given a field extension $\mathbb{Q}(r)/\mathbb{Q}$, another way of identifying the degree of the extension is by identifying the degree of the minimal polynomial of r over $\mathbb{Q}$. To finish off this subsection, we define what minimal polynomial is.

Irreducible polynomial

Definition 0.1.9. *A polynomial $f(x) \in F[x]$ is **reducible** over the field F if it can be factored into polynomials with smaller degrees. Otherwise, it is **irreducible**.*

Example 0.1.10. *Given the following polynomials over the field of rationals $\mathbb{Q}$:*

$$\begin{aligned}
f_1(x) &= x^2 + 4x + 4 = (x+2)(x+2),\\
f_2(x) &= x^2 - 4 = (x+2)(x-2),\\
f_3(x) &= 9x^2 - 3 = (3x+\sqrt{3})(3x-\sqrt{3}),\\
f_4(x) &= x^2 + 1 = (x+i)(x-i),
\end{aligned}$$

the polynomials $f_1(x)$ and $f_2(x)$ are reducible over $\mathbb{Q}$ whilst the other two are irreducible over $\mathbb{Q}$. The polynomials $f_3(x)$ and $f_4(x)$ are reducible over $\mathbb{R}$ and $\mathbb{C}$, respectively. The polynomial $f_4(x)$ is irreducible over $\mathbb{R}$.

Theorem 0.1.11. *Let p be a prime and $f(x) \in \mathbb{F}_p[x]$ be a monic irreducible polynomial of degree n. The quotient ring $\mathbb{F}_p[x]/f(x)$ is a field of order p^n. (Each polynomial in $\mathbb{F}_p[x]/f(x)$ has coefficients taken from the field $\mathbb{F}_p$ and the polynomial degree is at most $n-1$.)*

Proof. Each coset in the quotient ring $\mathbb{F}_p[x]/f(x)$ has the form $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$, where $a_i \in \mathbb{F}_p$. So there are p^n different cosets. The polynomial $f(x)$ is irreducible implies the quotient ring is also a field. □

Minimal polynomial

Definition 0.1.12. *Let E/F be a field extension. If r is algebraic over F, its **minimal polynomial** over F is the irreducible monic polynomial $f(x) \in F[x]$ of the least degree satisfying $f(r) = 0$.*

It is necessary for r to be algebraic, for otherwise it is not a root of any polynomial in $F[x]$.

Uniqueness

Note the minimal polynomial of an algebraic number over a base field is unique up to scalar multiplication. A simple argument is as the following. Let $J_r = \{f(x) \in F[x] \mid f(r) = 0\}$ be the set of all polynomials in $F[x]$ where r is a root, then J_r is an ideal of the polynomial ring $F[x]$ (easy to verify). Let $p, q \in J_r$ be two monic polynomials of least degree $n > 0$, then $p - q \in J_r$ because J_r is an ideal. Also $p - q$ has degree less than n because p, q are monic. This contradicts with p, q being least degree polynomials in J_r, unless $p = q$.

For different base fields, the minimal polynomial of a number could be different. Here is an example. Given the field extension $\mathbb{R}/\mathbb{Q}$, the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$ because this polynomial is monic, irreducible and has the least degree over the base field $\mathbb{Q}$ where $\sqrt{2}$ is a root. However, in the field extension $\mathbb{R}/\mathbb{R}$, the minimal polynomial for $\sqrt{2}$ is $x - \sqrt{2}$.

The degree of an extension $E = F(r)$ is the degree of the minimal polynomial of r over F. This is formally proved by Theorem 0.1.14 in the next subsection. In the above example, the degree $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, because the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$.

0.1.2 Simple extension

Simple extension

Definition 0.1.13. *An extension field E over F is **simple** if there exists an element $r \in E$ with $E = F(r)$.*

The simple extension $F(r)$ is the smallest extension over F that contains F and r. The number r can be either transcendental or algebraic, but we are only interested in algebraic simple extensions.

In the previous section, we mentioned that if r is an algebraic number over the base field F then its unique minimal polynomial $p(x)$ always exists. In addition, since $p(x)$ is irreducible over F, the principal ideal $\langle p(x)\rangle$ is also maximal in $F[x]$. This gives us a way of building the extension field $F(r)$ from the polynomial ring $F[x]$ using the principal ideal by Proposition **??** as stated in the following theorem.

Theorem 0.1.14. *Let E/F be a field extension and $r \in E$ be an algebraic number over F with minimal polynomial $p(x) \in F[x]$ of degree n, then*

1. *$F(r) \cong F[x]/\langle p(x)\rangle$.*

2. *$\{1, r, r^2, \ldots, r^{n-1}\}$ is a basis of the vector space $F(r)$ over F.*
3. *$[F(r) : F] = deg(p)$.*

The first part of Theorem 0.1.14 is a direct consequence of the First Isomorphism Theorem (Theorem **??**). An important observation as stated in the following corollary of the above theorem is that if two algebraic numbers have the same minimal polynomial, then the simple extensions generated by them are isomorphic. This tells us that simple algebraic extension of an algebraic number is unique.

Corollary 0.1.15. *Let E/F be a field extension. If two algebraic numbers $\alpha, \beta \in E$ over F have the same minimal polynomial in $F[x]$, then there is an isomorphism $\phi : F(\alpha) \to F(\beta)$ with $\phi|_F = I$.*

0.1.3 Splitting field

One way of building the smallest field extension for solving a polynomial is to look at the splitting field of the polynomial.

Solving a degree n polynomial $f(x) \in F[x]$ for its roots can be done by rewriting it as the product of linear factors in an appropriate extension field E. That is,

$$f(x) = c \prod_{i=1}^{n} (x - a_i),$$

where $c \in F$ is a constant and $x - a_i \in E[x]$ is a linear factor. This rewriting process is also known as **splitting** a polynomial.

Splitting field

Definition 0.1.16. *Let F be a field and $f(x) \in F[x]$ be a polynomial. The extension field E is a* ***splitting field*** *of $f(x)$ over F if*

- *$f(x)$ splits over E and*
- *if $F \subseteq L \subsetneq E$, then $f(x)$ does not split over L.*

By definition, a splitting field of $f(x)$ is the smallest extension that contains all the roots of $f(x)$. Alternatively, we say that the extension E is generated by the roots of $f(x)$. That is, if $r_1, \ldots, r_n$ are the roots of $f(x)$ and E is the splitting field of $f(x)$ then $E = F(r_1, \ldots, r_n)$. For example, the extension $\mathbb{Q}(\sqrt{2})$ is the splitting field of $x^2 - 2 \in \mathbb{Q}[x]$, because the polynomial splits into $(x + \sqrt{2})(x - \sqrt{2})$ in it. But $\mathbb{C}$ is not a splitting field of $x^2 - 2$, because it is not the smallest.

The following theorems state that the splitting field of a polynomial always exists and is unique up to isomorphism.

Existence

Theorem 0.1.17. *(Existence) Let F be a field and $f(x) \in F[x]$ be a polynomial of degree $n > 0$. Then there exists a splitting field K of $f(x)$ over F with degree $[K : F] \leq n!$.*

The construction of a splitting field can be done by taking the quotient of $F[x]$ with the principle ideal $\langle f(x) \rangle$ where $f(x)$ is irreducible. If it is reducible, we can factor it into irreducible factors and take the same process repeatedly until $f(x)$ splits.

Uniqueness

Theorem 0.1.18. *(Uniqueness) Let $\phi : F \to E$ be an isomorphism, $f(x) \in F[x]$ be a polynomial and $\phi(f(x)) \in E[x]$ be the corresponding polynomial in $E[x]$. If K and L are the splitting fields of $f(x)$ and $\phi(f(x))$ over F and E respectively, then ϕ extends to an isomorphism $K \cong L$.*

0.1.4 Normal extension

Sometimes we prefer to work with an algebraic extension that includes all the roots of a polynomial, so that we do not need to adjoin more roots to the extension. For this purpose, we define the following.

Normal extension

Definition 0.1.19. *An algebraic extension E over F is* ***normal*** *if whenever an irreducible polynomial over F has a root in E, then it splits in E.*

From splitting field, we know that an extension is normal if whenever it contains one root of a polynomial, it contains all roots of the polynomial. The most important result about normal extension is its connection with splitting field.

Normal iff splitting

Theorem 0.1.20. *A finite algebraic extension E over F is normal if and only if it is the splitting field of some polynomial $f(x) \in F[x]$.*

The theorem implies that if E is the splitting field of one polynomial over F, then it is the splitting field of every other polynomial over F with one root in E.

0.1.5 Separable extension

In addition to normal extensions, it is also convenient when a polynomial has distinct roots, so we do not need to worry about duplicated roots. This is especially the case when working with Galois groups that consist of automorphisms between polynomial roots. Before introducing separable extensions, we define what it means for a polynomial to be separable and how separability can be tested.

Separable polynomial

Definition 0.1.21. *A polynomial over a field F is* ***separable*** *if the number of its distinct roots in a splitting field is equal to the degree of the polynomial.*

Example 0.1.22. *The polynomial $x^2 - 2$ has two distinct roots $\pm\sqrt{2}$, so it is separable. The polynomial $(x^2 - 1)^2$ is not separable, because both roots ± 1 have multiplicity 2.*

Test separability

One way of testing separability is to check whether or not a polynomial is coprime with its *formal derivative*[2].

Lemma 0.1.23. *A polynomial $f(x) \in F[x]$ is separable if and only if* $\gcd(f, f') = 1$.

Proof. Let K be the splitting field of $f(x)$ and $r \in K$ is a root of $f(x)$. The re-write the polynomial as

$$f(x) = (x - r)^m g(x)$$

with $m \geq 1$ and $g(r) \neq 0$. Take the formal derivative, we get

$$f'(x) = m(x - r)^{m-1} g(x) + (x - r)^m g'(x) = (x - r)^{m-1}[mg(x) + (x - r)g'(x)].$$

Evaluating the second factor $mg(x) + (x - r)g'(x)$ at r gives $mg(r) + 0 = 0 \iff m = 0$ because $g(r) \neq 0$.

If $f(x)$ is separable, by definition $m = 1$ and $f'(x) = g(x) + (x - r)g'(x)$. So $f'(r) \neq 0$ and none of the two factors of $f(x)$ divides $f'(x)$. This implies they are coprime.

If $f(x)$ is not separable, then $m > 1$ and $f'(r) = 0$. Hence, $x - r$ is a common factor of f and f', so they are not coprime. □

Example 0.1.24. *In the examples above, $f(x) = x^2 - 2$ is separable, because its formal derivative $f(x)' = (x^2 - 2)' = 2x$ and $\gcd(f, f') = 1$. If $f(x) = (x^2 - 1)^2$, then its formal derivative $f'(x) = ((x^2 - 1)^2)' = 4x(x^2 - 1)$ and $\gcd(f, f') = x^2 - 1$, so the polynomial $(x^2 + 1)^2$ is not separable.*

Separable extension

Definition 0.1.25. *An algebraic extension E over F is* ***separable*** *if for every element $\alpha \in E$, its minimum polynomial over F is separable.*

The Fundamental Theorem of Galois Theory states a correspondence between intermediate field extensions and subgroups of a Galois group. Hence, we would like to know the separability of the intermediate field extensions between a base field and a separable extension.

Intermediate extensions are separable

Theorem 0.1.26. *Given field extensions $L/M/K$. If L/K is separable, then the intermediate extensions L/M and M/K are also separable.*

$char(F) = 0 \implies$ separable

In the previous section, we stated that a field characteristic is either 0 or a prime. The following results connect the characteristic of a polynomial to its separability.

Theorem 0.1.27. *Every irreducible polynomial over a field of characteristic zero is separable, and hence every algebraic extension is separable.*

[2] Formal derivative is similar to derivative in calculus, but for elements of a polynomial ring.

Proof. Let E/F be a field extension with $char(F) = 0$, and $f(x) \in F[x]$ be the minimal polynomial of $\alpha \in E$ over F. Assuming $f(x)$ is not separable. That is, without loss of generality, there is a root β with multiplicity 2. Then $f(\beta) = 0$ and its formal derivative $f'(\beta) = 0$, because $f(x)$ has a factor $(x - \beta)^2$, which becomes $2(x - \beta)$ in $f'(x)$.

However, $f'(x)$ does not have zero coefficients, because it is over a field of zero characteristic. The fact that $f(x)$ is a minimal polynomial implies it is irreducible, and $f'(x)$ has a lower degree than $f(x)$ imply that $\gcd(f, f') = 1$. Hence, there are $a, b \in F[x]$ such that $af(x) + bf'(x) = 1$. Substituting $x = \beta$, we get a contradiction, so $f(x)$ cannot be non-separable. Hence, every irreducible polynomial over F is separable. This implies every algebraic extension is separable and every finite extension is also separable because every finite extension is algebraic by Proposition 0.1.7. □

A similar but more general result is the following theorem.

Theorem 0.1.28. *Let $f \in F[x]$ be an irreducible polynomial of degree n. Then f is separable if either of the following conditions is satisfied:*

- *the field F has characteristic 0 or*
- *the field F has characteristic p where p is prime and $p \nmid n$.*

The same argument can be used here to prove the second condition. Since $f(x)$ is a degree n polynomial, its formal derivative $f'(x)$ much contain a term $na_n x^{n-1}$, in which the coefficient $na_n \neq 0$ in the field F as $char(F) = p$ is prime and $p \nmid n$. So $\gcd(f, f') = 1$ and the same contradiction can be reached is $f(x)$ is assumed to be non-separable.

The intuition behind both theorems is that if the characteristic of the field F does not satisfy either condition, then the coefficients of $f'(x)$ may be all zero. So $f'(x) = 0$ cannot lead to the same contradiction when assuming $f(x)$ non-separable.

0.2 Galois extension and Galois group

In the preceding subsections, we have defined different types of field extensions, finite, algebraic, simple, normal and separable. This section will connect some of these extensions to an important field extension, called *Galois extension* and will define the *Galois groups* of Galois extensions.

Group action

To start with, we introduce group action on a set. One way to define a group action on a set is by the following definition.

Definition 0.2.1. *A group $(G, *)$ **acts** on a set S if there is a map*

$$\mu : G \times S \to S$$

such that

- *for all $s \in S$, we have $\mu(e, s) = s$,*
- *for all $x, y \in G$ and $s \in S$, we have $\mu(x * y, s) = \mu(x, \mu(y, s))$.*

For simplicity, we write $\mu(x, s)$ as $x(s)$. Another way of defining group action is by a group homomorphism.

Definition 0.2.2. *A group G **acts** on a set S if there is a homomorphism*

$$\phi : G \to Sym(S)$$

from the group to the symmetric group (or the permutation group $Perm(S)$) of S.

In this case, we say ϕ is the group action of G on S. Each element of G is mapped to a certain permutation of the set S by the action. For example, when the Dihedral group

$$D_4 = \langle r, f \rangle = \{e, r, r^2, r^3, f, fr, fr^2, fr^3)$$

acts on itself, each element in D_4 is mapped to a certain permutation of the set $S = D_4$. For example, the elements *rotation* r and *reflection* f correspond to the following permutations of D_4

$$r : \{e, r, r^2, r^3, f, fr, fr^2, fr^3) \mapsto \{r, r^2, r^3, e, rf = fr^3, rfr = f, rfr^2 = fr, rfr^3 = fr^2)$$
$$f : \{e, r, r^2, r^3, f, fr, fr^2, fr^3) \mapsto \{f, fr, fr^2, fr^3, e, r, r^2, r^3).$$

The action of D_4 only gives rise to certain permutes of D_4. In other words, there are 8 elements in D_4 and the symmetric group has size $|Perm(D_4)| = 8!$, the homomorphism ϕ is injective, which we call faithful as stated next.

Faithful action

Definition 0.2.3. *A group action ϕ of G on a set S is **faithful** if ϕ is injective. That is, for every two distinct elements $g, h \in G$, there exists an element $s \in S$ such that $g(s) \neq h(s)$.*

If a group action is faithful, then we can think the group G embeds into the permutation group of S, as in the above example of D_4, where each element of $G = D_4$ corresponds to a certain permutation of the set $S = D_4$.

Similarly, we can define a group G acts on a ring R (or a field F). The difference is that a ring has more algebraic structures than a set, so simple permutations of the ring elements do not necessarily preserve the ring structure. For this reason, we replace permutations by automorphisms, which are bijective ring homomorphisms between R and itself. Let $\text{Aut}(R)$ be the **automorphism group** of R.

Definition 0.2.4. *An **action** of a group G on a ring R is a group homomorphism*

$$\phi : G \to Aut(R).$$

Fixed field

Some elements in the ring R or field F stay invariant under the action. They make up the fixed field.

Definition 0.2.5. *Given a field extension E/F and a group action of G on E, the **fixed field** of E under the action of G*

$$E^G = \{a \in E \mid g(a) = a, \forall g \in G\}.$$

is the set of elements in the extension field that are fixed point-wise by all automorphisms of R.

Automorphism group

Definition 0.2.6. *Let E/F be a field extension. The **automorphism group** of the field extension*

$$\begin{aligned} Aut(E/F) &= \{\alpha \in Aut(E) \mid \alpha(x) = x, \ \forall x \in F\} \\ &= \{\alpha \in Aut(E) \mid \alpha_F = Id_F\} \end{aligned}$$

is the set of automorphisms that fixes F when acting on E.

The automorphism group is a group with function composition as the group operator. It is a subgroup of the group of automorphisms of E, i.e., $Aut(E/F) \subseteq Aut(E)$. Now, we are ready to define the Galois group of a field extension.

Galois group

Definition 0.2.7. *The **Galois group** of a field extension E/F, denoted by $Gal(E/F)$, is the automorphism group of the field extension. That is,*

$$Gal(E/F) := Aut(E/F) = \{\alpha \in Aut(E) \mid \alpha_F = Id_F\}.$$

By definition, the Galois group is a subset of the automorphism group or permutation group (or symmetric group) of the extension E.

As explained in the previous section that an extension field can be viewed as a vector space over the base field, so when working with Galois groups, instead of thinking where all elements in the extension are mapped to, it is convenient to know where the basis vectors are mapped to by the automorphisms.

Let us work through some simple examples.

Example 0.2.8. *Let the field extension be $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. It is a 2-dimensional $\mathbb{Q}$-vector space with a basis $\{1, \sqrt{2}\}$. The Galois group must fix the base field, so it contains the identity map I. In addition, it should contain another automorphism σ that maps $\sqrt{2}$ to another element a in the extension whiling fixing $\mathbb{Q}$. Since σ is an automorphism, it must satisfy $a^2 = \sigma(\sqrt{2})^2 = \sigma((\sqrt{2})^2) = \sigma(2) = 2$. So whatever $\sigma(\sqrt{2}) = a$ is, it must satisfy $a^2 - 2 = 0$ in the extension, which means $a = \pm\sqrt{2}$. Since the identity map is already included, it entails $\sigma(\sqrt{2}) = -\sqrt{2}$. Hence, the Galois group $Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{I, \sigma : \sqrt{2} \mapsto -\sqrt{2}\} \cong C_2$ which is isomorphic to the cyclic group of order 2.*

Example 0.2.9. *Let the field extension be $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$. This is a 4-dimensional $\mathbb{Q}$-vector space with a basis $\{1, \sqrt{2}, i, \sqrt{2}i\}$. The minimal polynomials over $\mathbb{Q}$ for $\sqrt{2}$ and i are $x^2 - 2$ and $x^2 + 1$, respectively. The Galois group of the field extension contains all the automorphisms that fix $\mathbb{Q}$ while permuting roots in each minimal polynomial. That is, it contains a map τ that permutes $\{\sqrt{2}, -\sqrt{2}\}$ and a map σ that permutes $\{i, -i\}$. We can identify these automorphisms as shown in Table 1. The Galois group is isomorphic to the Klein four group $V_4 = C_2 \times C_2$.*

	1	$\sqrt{2}$	i	$\sqrt{2}i$
I	1	$\sqrt{2}$	i	$\sqrt{2}i$
σ	1	$\sqrt{2}$	$-i$	$-\sqrt{2}i$
τ	1	$-\sqrt{2}$	i	$-\sqrt{2}i$
$\sigma\tau$	1	$-\sqrt{2}$	$-i$	$\sqrt{2}i$

Table 1: The Galois group of the extension $\mathbb{Q}(\sqrt{2}, i)$. It is isomorphic to the Klein four group $V_4 = C_2 \times C_2$.

It is important to note that not all automorphisms (or permutations) that fix the base field are in the Galois group. From the above two examples, we can see that the Galois group only contains those automorphisms that permute roots of the same minimal polynomial while fixing the base field. In Example 0.2.9, $\sqrt{2}$ and $-\sqrt{2}$ come from the minimal polynomial $x^2 - 2$ in $\mathbb{Q}$ and i and $-i$ come from the minimal polynomial $x^2 + 1$ in $\mathbb{Q}$. Let us take a look at a counter example.

Example 0.2.10. *Let the field extension be $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. The permutation $\phi : \sqrt{2} \mapsto \sqrt{3}$ is not in the Galois group. Assuming it is, then $\phi(\sqrt{2}) = \sqrt{3}$ implies $\phi(\sqrt{2})^2 = 3$. By the definition of homomorphism, $\phi(\sqrt{2})^2 = \phi(\sqrt{2}^2) = \phi(2) = 2$ because ϕ fixes $\mathbb{Q}$. This implies $2 = 3$.*

Example 0.2.11. *A slightly more complicated example is with a field extension $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$. The roots $\sqrt[4]{2}$ and i have the minimal polynomials $x^4 - 2$ and $x^2 + 1$ over $\mathbb{Q}$, respectively. The polynomial $x^4 - 2$ has four roots $\pm\sqrt[4]{2}$ and $\pm i\sqrt[4]{2}$. The polynomial $x^2 + 1$ has two roots $\pm i$. The Galois group should contain automorphisms that permutes roots for each polynomial. The process of finding the automorphisms is more or less trial and error.*[3] *Let*

$$\begin{aligned} \sigma(\sqrt[4]{2}) &= i\sqrt[4]{2} \text{ and } \sigma(i) = i, \\ \tau(i) &= -i \text{ and } \tau(\sqrt[4]{2}) = \sqrt[4]{2}. \end{aligned}$$

Then we have

$$\begin{aligned} \sigma^2(\sqrt[4]{2}) &= -\sqrt[4]{2} \text{ and } \sigma^2(i) = i, \\ \sigma^3(\sqrt[4]{2}) &= -i\sqrt[4]{2} \text{ and } \sigma^3(i) = i, \\ \sigma^4(\sqrt[4]{2}) &= \sqrt[4]{2} \text{ and } \sigma^4(i) = i, \\ \tau^2(i) &= i \text{ and } \tau^2(\sqrt[4]{2}) = \sqrt[4]{2}. \end{aligned}$$

So the orders of σ and τ in the Galois group are 4 and 2, respectively. Hence, the Galois group is $\{I, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$.

Combining the definitions of fixed field and Galois group, we know that for a field extension E/F, the fixed field by the Galois group should at least contain the base field F. Because all automorphisms in the Galois group at least fix F, though they may fix more than F. Hence, we can define what it means for a field extension to be Galois.

Galois extension

Definition 0.2.12. *A field extension E/F is an* ***Galois extension*** *if the fixed field by the Galois group $Gal(E/F)$ is exactly F. That is, $E^{Gal(E/F)} = F$.*

In other words, the Galois group has to fix exactly the base field, nothing more nothing less. An important theorem that characterizes Galois extension using previously defined extension types is the following.

Normal and separable $\implies$ Galois

Theorem 0.2.13. *An algebraic field extension is a* ***Galois extension*** *if it is normal and separable.*

This theorem says that for an algebraic field extension to be a Galois extension, any polynomial that has a root in the extension must have all its roots in the extension and these roots must be all distinct. The requirement of being normal and separable is a sufficient condition for a field extension to be Galois.

[3] Perhaps there are better ways of finding the Galois group, but they are not in the scope of this material.

Example 0.2.14. *The Galois group $Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{I\}$ contains only the identity map. If $\phi(\sqrt[3]{2}) = a$ is another automorphism, then it must satisfy $a^3 - 2 = 0$. So ϕ must map $\sqrt[3]{2}$ to a root of the minimal polynomial $a^3 - 2 = 0$ in the extension. But the only root that is in the extension is $\sqrt[3]{2}$, because the other two roots are complex. So ϕ is the identity map. Given the Galois group contains only the identity map, the fixed field is $\mathbb{Q}(\sqrt[3]{2})$ not $\mathbb{Q}$, so the field extension is not Galois. By Theorem 0.2.13, the extension is not both normal and separable. In fact, this is true, because the extension does not contain the two complex roots of the minimal polynomial $x^3 - 2$.*

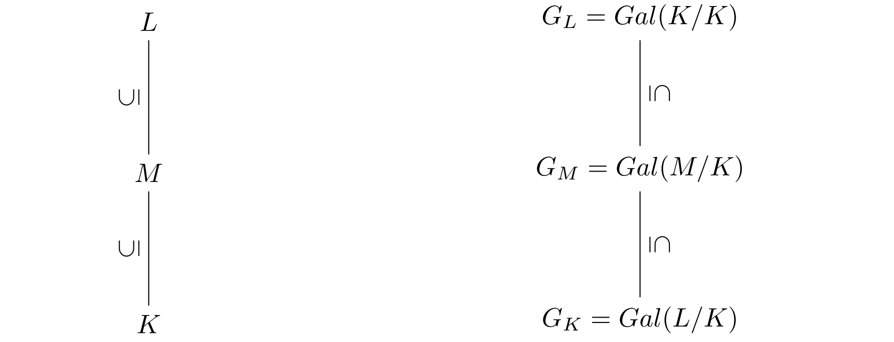
The example suggests that a field extension can have a Galois group, but it is not necessarily a Galois extension.

Since a Galois extension is normal and separable, we would expect the number of automorphisms in the Galois group to be related to the number of roots of a minimal polynomial. The next lemma connects the number of automorphisms in the Galois group to the degree of a Galois extension.

Lemma 0.2.15. *If a finite field extension E/F is Galois, then the number of elements in the Galois group is the degree of the field extension. That is, $|Gal(E/F)| = [E : F]$.*

For example, the field extension $Q(\sqrt{2}, i)/Q$ has degree 4 (as it is a 4 dimensional vector space over Q) and there are 4 automorphisms in the Galois group as stated in Table 1.

The next theorem is the most important theorem in Galois Theory. It builds a connection between subgroups of a Galois group and field extensions of a base field. The theorem is important in the sense that it provides a way of understanding field extensions from group's perspective, which is relatively well studied. In the most basic form, it states that if $L/M/K$ is a finite Galois extension, then there is a one-to-one correspondence between an intermediate extension and a subgroup of the Galois group $Gal(L/K)$. The next theorem explicitly defines what it means for a one-to-one correspondence between the two different algebraic structures.



(a) A finite Galois extension.

(b) Subgroups of the Galois group $G_K = Gal(L/K)$.

Figure 1: A finite Galois extension and the corresponding Galois groups.

Fundamental Theorem of Galois Theory

Theorem 0.2.16. *(Fundamental Theorem of Galois Theory) Suppose $L/M/K$ is a finite Galois extension with the corresponding Galois group $G_K = Gal(L/K)$.*

1. *There is an inclusion reversing correspondence between an intermediate field M of L/K and a subgroup $G_M \subseteq G_L$ given as follows:*

$$\begin{aligned} M &\to G_M = \{\phi \in Aut(L) \mid \phi_M = Id_M\} \\ G_M &\to L^{G_M} = M. \end{aligned}$$

2. *The degrees of the field extensions are given by*

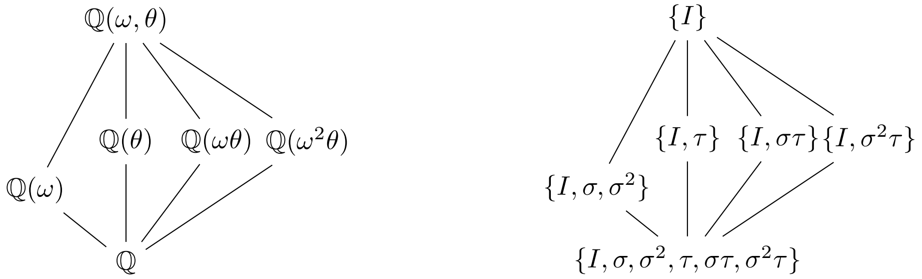
$$[L : M] = |G_M| \text{ and } [M : K] = \frac{|G_K|}{|G_M|}.$$

3. *The intermediate field extension M/K is Galois if and only if $G_M \lhd G_K$ is a normal subgroup. In this case, the corresponding Galois group is given by*

$$Gal(M/K) \cong G_K/G_M.$$

The first point of the theorem says that if M is an intermediate extension between L/K, then M corresponds to the set of automorphisms of L that fixes M. If $M = K$, then M corresponds to the set of automorphisms of L that fixes K, which is the entire $Gal(L/K)$. If $M = L$, then M corresponds to the set of automorphisms of L that fixes L, which is identity map.

The second point says the degree of the M-vector space L equals the number of automorphisms of L that fix M. If $M = K$ or $M = L$, then the degrees $[L : M] = [L : K] = |G_K| = Gal(L/K)$ or $[L : M] = [L : L] = |G_L| = 1$, respectively. Combining the two qualities, we get $[L : M][M : K] = |G_K| = [L : K]$ which is consistent with the Tower Law in Proposition 0.1.3.


$\mathbb{Q}(\omega, \theta)$
$\mathbb{Q}(\theta)$
$\mathbb{Q}(\omega\theta)$
$\mathbb{Q}(\omega^2\theta)$
$\mathbb{Q}(\omega)$
$\mathbb{Q}$
$\{I\}$
$\{I, \tau\}$
$\{I, \sigma\tau\}$
$\{I, \sigma^2\tau\}$
$\{I, \sigma, \sigma^2\}$
$\{I, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$

(a) A finite Galois extension and the intermediate extensions.

(b) Subgroups of the Galois group $Gal(\mathbb{Q}(\omega, \theta)/\mathbb{Q})$.

Figure 2: A finite Galois extension $\mathbb{Q}(\omega, \theta)/\mathbb{Q}$ and the corresponding Galois groups, where $\omega = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$ and $\theta = \sqrt[3]{2}$. Each structure is a lattice and there is a one-to-one correspondence between them.

Example 0.2.17. *Let the field extension be $\mathbb{Q}(\theta, \omega)/\mathbb{Q}$, where $\theta = \sqrt[3]{2}$ and $\omega = \frac{-1}{2} \pm i\frac{\sqrt{3}}{2}$. The extension is a 6-dimensional $\mathbb{Q}$-vector space with a basis $\{1, \theta, \theta^2, \omega, \theta\omega, \theta^2\omega\}$. Define the automorphisms*

$$\sigma(\theta) = \omega\theta \text{ and } \sigma(\omega) = \omega,$$
$$\tau(\theta) = \theta \text{ and } \tau(\omega) = \omega^2.$$

The two automorphisms in the Galois group have orders 3 and 2, respectively. It can be seen that they can make the entire Galois group $\{I, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$. The intermediate field extensions from $\mathbb{Q}$ to $\mathbb{Q}(\omega, \theta)$ are shown in Figure 1a. The extension $\mathbb{Q}(\omega)$ can be extended to $\mathbb{Q}(\omega, \theta)$ by adjoining θ and the other three extensions can be extended to $\mathbb{Q}(\omega, \theta)$ by adjoining ω. The corresponding subgroups of the Galois group are shown in Figure 1b.

The two structures are lattices. According to the Fundamental theorem of Galois Theory, they are in one-to-one correspondence. The automorphisms that fix $\mathbb{Q}(\omega)$ are $\{I, \sigma, \sigma^2\}$. The degree of the intermediate extension $\mathbb{Q}(\omega)$ is $[\mathbb{Q}(\omega, \theta) : \mathbb{Q}(\omega)] = 3$, because $\mathbb{Q}(\omega, \theta)$ has a basis $\{1, \theta, \theta^2\}$ over the field $\mathbb{Q}(\omega)$. Also, $[\mathbb{Q}(\omega, \theta) : \mathbb{Q}] = [\mathbb{Q}(\omega, \theta) : \mathbb{Q}(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}] = 3 \cdot 2 = 6$. The normal extensions are $\mathbb{Q}$, $\mathbb{Q}(\omega)$ and $\mathbb{Q}(\omega, \theta)$ because the corresponding subgroups $\{I, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$, $\{I, \sigma, \sigma^2\}$ and $\{I\}$ are normal subgroups of the Galois group $\{I, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$.

References