PMATH 348 Fields and Galois Theory - Lecture Notes

Instructor: Yu-Ru Liu
LaTeX'd by Daniel Horton

University of Waterloo - Winter 2024

Office Hours: Mondays 9:30 - 10:30 am in MC5316

Contents

1 Course Overview

1.1 Intro to Galois Theory

Definition 1.1 (Polynomial Equations)**:** A polynomial equation is an equation of the form

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = 0$$

where $a_n \neq 0$. n is called the degree of the equation.

Definition 1.2 (Radical Expressions and Solutions)**:** An algebraic expression that uses only $+, -, \times, \div, \sqrt[n]{}$ is called a radical expression. A radical solution is a radical expression which solves a given polynomial equation.

Example 1.1: Linear equations $ax+b=0$ and quadratic equations $ax^2+bx+c=0$ where $a \neq 0$ are degree 1 and degree 2 polynomial equations with radical solutions $x - \frac{b}{a}$ and $x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$.

Definition 1.3 (Cubic Equations)**:** A cubic equation is a degree 3 polynomial equation (i.e. $ax^3 + bx^2 + cx + d = 0$ with $a \neq 0$).

Note: One can prove that all cubic equations can be reduced to the form

$$x^3 + px + q = 0.$$

A radical solution to the above equation is

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{p^3}{2q} + \frac{q^2}{4}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{p^3}{2q} + \frac{q^2}{4}}}.$$

One can use this solution (along with polynomial division and the quadratic formula) to derive radical expressions for the other two solutions. Hence all cubic equations have radical solutions.

Definition 1.4 (Quartic Equations)**:** A quartic equation is a degree 4 polynomial equation (i.e. $ax^4 + bx^3 + cx^2 + dx + e$ with $a \neq 0$).

Note: There also exist radical solutions to all quartic equations (see bonus 1).

Definition 1.5 (Quintic Equations)**:** A quintic equation is a degree 5 polynomial equation (i.e. $ax^5 + bx^4 + cx^3 + dx^2 + ex + f$ with $a \neq 0$).

Naturally, we now ask the question:

Do all quintic equations have radical solutions?

To study this question, we consider what would happen if it were true. One might ask:

Suppose that a radical solution exists for a general quintic equation. How would this radical expression behave?

We can investigate this problem following the two main steps of Galois Theory:

1. Link a root of a quintic equation, say α, to $\mathbb{Q}(\alpha)$, smallest field containing all of $\mathbb{Q}$ and α.

   Our knowledge about fields at the moment is limited, but consider $\mathbb{Q}(\sqrt{2},\sqrt{3})$, the smallest field containing $\mathbb{Q}$, $\sqrt{2}$ and $\sqrt{3}$. Notice that there are many fields that lie *strictly* between $\mathbb{Q}(\sqrt{2},\sqrt{3})$ and $\mathbb{Q}$ (i.e. $\mathbb{Q} \subsetneq F \subsetneq \mathbb{Q}(\sqrt{2},\sqrt{3})$. For example:

   $$\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6}), \mathbb{Q}(\sqrt{2}+\sqrt{3}), \mathbb{Q}(\sqrt{2}-\sqrt{3}), \cdots \subsetneq \mathbb{Q}(\sqrt{2},\sqrt{3})$$

2. Link the field $\mathbb{Q}(\alpha)$ to a group. More precisely, we associate the field extension of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ to the group

   $$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha)) = \{\psi : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha), \psi \text{ is an isomorphism and } \psi\restriction_{\mathbb{Q}} = 1_{\mathbb{Q}}\}.$$

   - One can show that if α is "good", say "algebraic", $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ is finite.
   - There is a one-to-one correspondence between the intermediate fields of $\mathbb{Q}(\alpha)$ and the subgroups of $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$.

Galois theory is all about the interactions between field theory and finite group theory.

1.2 Review of Ring Theory

This subsection consisted of content from the rings section of PMATH347. A majority of chapters 8,9 and 10 of PMATH347 were given without proof, and will be used throughout this course. These results have been omitted here.

2 Integral Domains

2.1 Irreducibles and Primes

Definition 2.1 (Divisibility)**:** Let R be an integral domain and $a, b \in R$. We say that a divides b (denoted $a \mid b$) if there exists $c \in R$ such that $b = ca$.

Remark: Recall that in $\mathbb{Z}$ if $n \mid m$ and $m \mid n$ then $n = \pm m$ and $\langle n \rangle = \langle m \rangle$. Similarly, in $F[x]$ if $f(x) \mid g(x)$ and $g(x) \mid f(x)$ then $f(x) = cg(x)$ for some $c \in F^*$ and $\langle f(x) \rangle = \langle g(x) \rangle$. The following proposition generalizes this idea to any integral domain.

Proposition 2.1: Let R be an integral domain. For $a, b \in R$, the following are all equivalent:

1. $a \mid b$ and $b \mid a$
2. $a = ub$ for some unit $u \in R^*$
3. $\langle a \rangle = \langle b \rangle$

Proof.

- $(1 \implies 2)$: If $a \mid b$ and $b \mid a$ then write $a = ub$ and $b = va$ for some $u, v \in R$. Note that if $a = 0$ then $b = 0$, thus $a = 1 \cdot b$ so assume $a \neq 0$. This means that $a = u(va) = (uv)a$ so $uv = 1$ since R is an integral domain. Thus u is a unit.
- $(2 \implies 3)$: If $a = ub$ then $\langle a \rangle \subseteq \langle b \rangle$. Since u is a unit and $b = u^{-1}a$ we have $\langle b \rangle \subseteq \langle a \rangle$. It follows that $\langle a \rangle = \langle b \rangle$.
- $(3 \implies 1)$: If $\langle a \rangle = \langle b \rangle$ then since $a \in \langle a \rangle$, $a \in \langle b \rangle$. Hence $a = ub$ for some $u \in R$ and so $b \mid a$. A symmetric argument gives $a \mid b$.

□

Definition 2.2 (Associations)**:** Let R be an integral domain. For $a, b \in R$ we say that a is associated to b (denoted by $a \sim b$), if $a \mid b$ and $b \mid a$. By Proposition 2.1 $\sim$ is an equivalence relation in R.

Proposition 2.2 (Properties of Associations)**:** Let R be an integral domain and $a, a', b, b' \in R$.

1. If $a \sim a'$ and $b \sim b'$, then $ab \sim a'b'$.
2. If $a \sim a'$ and $b \sim b'$, then $a \mid b$ if and only if $a' \mid b'$.

Proof. This follows easily from Proposition 2.1. □

Example 2.1: Let $R = \mathbb{Z}[\sqrt{3}] = \{m + n\sqrt{3} : m, n \in \mathbb{Z}\}$, which is an integral domain. Note that $(2 + \sqrt{3})(2 - \sqrt{3}) = 1$. Thus $2 + \sqrt{3}$ is a unit in R. Since $3 + 2\sqrt{3} = (2 + \sqrt{3})\sqrt{3}$, we have $3 + 2\sqrt{3} \sim \sqrt{3}$.

Definition 2.3 (Reducibility)**:** Let R be an integral domain. We say $p \in R$ is reducible if $p \neq 0$, $p \notin R^*$ and there exist some $a, b \in R \setminus R^*$ such that $p = ab$. If $p \neq 0$ and $p \notin R^*$ but no such a, b exist then we say that p is irreducible.

Remark: By this definition, all non-zero non-unit elements of an integral domain must be either reducible or irreducible, while 0 and the units are neither reducible nor irreducible.

Proposition 2.3: Let R be an integral domain and let $p \in R$ with $p \neq 0$ and $p \notin R^*$. The following are all equivalent:

1. p is irreducible.
2. If $d \mid p$, then $d \sim 1$ or $d \sim p$.
3. If $p \sim ab$ in R, then $p \sim a$ or $p \sim b$.
4. If $p = ab$ in R, then $p \sim a$ or $p \sim b$.

Proof.

- $(1 \implies 2)$: If $p = ad$, then by (1), either d or a is a unit. Then $d \sim 1$ or $d \sim p$.
- $(2 \implies 3)$: If $p \sim ab$, then $b \mid p$. By (2), either $b \sim 1$ or $b \sim p$. In the first case, $a \sim p$.
- $(3 \implies 4)$: Trivial.
- $(4 \implies 1)$: If $p = ab$, then by (4), $p \sim a$ or $p \sim b$. If $p \sim a$, write $a = up$ for some unit u. Since R is associative we have $p = ab = (up)b = p(ub)$. Since R is an integral domain and $p \neq 0$, we have $1 = ub$. Thus b is a unit. Similarly, $p \sim b$ implies that a is a unit, so p is irreducible.

□

Definition 2.4: Let R be an integral domain and $p \in R$. We say p is prime if $p \neq 0$ and $p \notin R^*$ and if whenever $p \mid ab$ with $a, b \in R$ then either $p \mid a$ or $p \mid b$.

Note: One can show that if $p \sim q$ then p is prime if and only if q is prime.

Proposition 2.4: Let R be an integral domain and $p \in R$. If p is prime then p is irreducible.

Proof. Let $p \in R$ be prime. If $p = ab$, then $p \mid a$ or $p \mid b$. If $p \mid a$ then write $a = dp$ for some $d \in R$. Since R is commutative we have $a = dp = d(ab) = a(db)$. Since R is an integral domain and $a \neq 0$, we have $1 = db$. Thus b is a unit. Similarly, if $p \mid b$ then a is a unit. It follows that p is irreducible. □

Remark: The converse Proposition 2.4 is not true in general.

Example 2.2: $p = 1 + \sqrt{-5}$ is not prime in $\mathbb{Z}[\sqrt{-5}]$.

Proof. If it were prime then since

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3$$

we would have $p \mid 2$ or $p \mid 3$, neither of which are possible in $\mathbb{Z}[\sqrt{-5}]$. □

Question: In $\mathbb{Z}$, p is prime if and only if it is irreducible. Similarly, in $F[x]$ (F=field), a polynomial is irreducible if and only if it is also prime. What additional property does an integral domain need for primes and irreducibles to be equivalent?

2.2 Ascending Chain Conditions

Definition 2.5 (The ACCP)**:** An integral domain R is said to satisfy the ascending chain condition on principal ideals (ACCP for short) if for any ascending chain

$$\langle a_1\rangle \subseteq \langle a_2\rangle \subseteq \langle a_3\rangle \subseteq \cdots$$

of principal ideals there exists and $n \in \mathbb{N}$ such that

$$\langle a_n\rangle = \langle a_{n+1}\rangle = \langle a_{n+2}\rangle = \cdots .$$

Example 2.3: $\mathbb{Z}$ satisfies the ACCP.

Proof. If $\langle a_1\rangle \subseteq \langle a_2\rangle \subseteq \langle a_3\rangle \subseteq \cdots$ in $\mathbb{Z}$ then $a_2 \mid a_1$, $a_3 \mid a_2, \cdots$. Taking the absolute values we gives

$$|a_1| \geq |a_2| \geq |a_3| \geq \cdots .$$

Since each $|a_i| \geq 0$ is an integer, at some point we get

$$|a_n| = |a_{n+1}| = |a_{n+2}| = \cdots$$

for some $n \in \mathbb{N}$. Thus we also have

$$\langle a_n\rangle = \langle a_{n+1}\rangle = \langle a_{n+2}\rangle = \cdots$$

□

Example 2.4: Consider the set $R = \{n + xf : n \in \mathbb{Z}, f \in \mathbb{Q}[x]\}$, the set of polynomials in $\mathbb{Q}[x]$ whose constant term is in $\mathbb{Z}$. Then R is an integral domain (exercise) but

$$\langle x\rangle \subsetneq \left\langle \frac{1}{2}x \right\rangle \subsetneq \left\langle \frac{1}{4}x \right\rangle \subseteq \cdots$$

in R. Thus R does not satisfy the ACCP.

Theorem 2.5: Let R be an integral domain satisfying ACCP. If $a \in R$ with $a \neq 0$ and $a \notin R^*$ then a is a product of irreducible elements of R.

Proof. Let a satisfy the required conditions but for the sake of contradiction, suppose a is not a product of irreducible elements. Then a is reducible and so by Proposition 2.3 we can write $a = x_1a_1$ with $a \not\sim x_1$ and $a \not\sim a_1$. Note that at least one of x_1 and a_1 is not a product of irreducible elements.

Without loss of generality, suppose that a_1 is not a product of irreducible elements. Then as before we can write $a_1 = x_2a_2$ with $a_1 \not\sim x_2$ and $a_1 \not\sim a_2$. This process continues infinitely and we have an ascending chain of principal ideals

$$\langle a\rangle \subseteq \langle a_1\rangle \subseteq \langle a_2\rangle \subseteq \cdots$$

Since $a \not\sim a_1, a_1 \not\sim a_2, \cdots$ by Proposition 2.1, we have

$$\langle a\rangle \subsetneq \langle a_1\rangle \subsetneq \langle a_2\rangle \subsetneq \cdots$$

which contradicts the ACCP.

□

Theorem 2.6: If R is an integral domain satisfying the ACCP, so is $R[x]$.

Proof. Suppose that $R[x]$ does not satisfy the ACCP. Then there exists an infinite chain of principal ideals

$$\langle f_1 \rangle \subsetneq \langle f_2 \rangle \subsetneq \cdots$$

in $R[x]$. Thus $f_{i+1} \mid f_i$ for all $i \in \mathbb{N}$. Let a_i denote the leading coefficient of f_i for each i. Since $f_{i+1} \mid f_i$ we have $a_{i+1} \mid a_i$. Thus

$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \cdots .$$

Since R satisfies the ACCP, we have $\langle a_n \rangle = \langle a_{n+1} \rangle = \cdots$ for some $n \geq 1$ (i.e. $a_n \sim a_{n+1} \sim \cdots$). For $m \geq n$, let $f_m = g f_{m+1}$ for some $g(x) \in R[x]$. If b is the leading coefficient of $g(x)$, then $a_m = b a_{m+1}$. Since $a_m \sim a_{m+1}$, b is a unit in R. However, $g(x)$ is not a unit in $R[x]$ since $\langle f_m \rangle \neq \langle f_{m+1} \rangle$. Thus $g(x) \neq b$ and we have $\deg g \geq 1$. By the product formula for $R[x]$, this implies that

$$\deg(f_m) > \deg(f_{m+1})$$

for all $m \geq n$. Thus we have

$$\deg(f_n) > \deg(f_{n+1}) > \deg(f_{n+2}) > \cdots$$

which leads to a contradiction since $\deg(f_i) \geq 0$. Thus $R[x]$ satisfies the ACCP. □

Example 2.5: Since $\mathbb{Z}$ satisfies the ACCP, by Theorem 2.6 so does $\mathbb{Z}[x]$.

2.3 Unique Factorization Domains and Principal Ideal Domains

Definition 2.6: An integral domain R is a unique factorization domain (UFD) if it satisfies the following conditions:

1. If $a \in R$, $a \neq 0$ and $a \notin R^*$ then a is a product of irreducible elements in R.
2. If $p_1 p_2 \cdots p_r \sim q_1 q_2 \cdots q_s$ where $r, s \in \mathbb{N}$ and p_i, q_i are irreducible elements of R then $r = s$ and there exists a relabeling such that $p_i = q_i$ for all i.

Example 2.6:

- All fields are UFDs.
- $\mathbb{Z}$ and $F[x]$ (for any field F) are UFDs.

Proposition 2.7: Let R be a UFD and $p \in R$. If p is irreducible, then p is prime.

Proof. Let $p \in R$ be irreducible. If $p \mid ab$ with $a, b \in R$, write $ab = pd$ for some $d \in R$. Since R is a UFD, we can factor a, b and d into irreducible elements, say $a = p_1 p_2 \cdots p_k$ and $b = q_1 q_2 \cdots q_\ell$ and $d = r_1 r_2 \cdots r_m$. (where we allow k, ℓ, m to be 0 in the cases where a, b, d is are units). Since $pd = ab$, we have

$$p r_1 \cdots r_m = p_1 \cdots p_k q_1 \cdots q_\ell .$$

Since p is irreducible, it implies that $p \sim p_i$ for some i or $p \sim q_j$ for some j. Thus $p \mid a$ or $p \mid d$. □

Example 2.7: Since $\mathbb{Z}$ is a UFD, a prime $p \in \mathbb{Z}$ satisfies Euclid's lemma:

$$p \mid ab \implies p \mid a \text{ or } p \mid b$$

A similar statement holds if we replace $\mathbb{Z}$ by $F[x]$ for some field F.

Example 2.8: Consider $R = \mathbb{Z}[\sqrt{-5}]$ and $p = 1 + \sqrt{-5} \in R$. We have seen in Example 2.2 that p is irreducible but not prime. By Proposition 2.7 this means R is not a UFD. For example:

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3$$

Where $1 + \sqrt{-5}, 1 - \sqrt{-5}, 2$ and 3 are all irreducible. However $1 + \sqrt{-5} \not\sim 2, 3$.

Example 2.9: $R = \mathbb{Z}[\sqrt{-5}]$ satisfies the ACCP.

Proof. Recall Assignment 1 question 1 where we defined the norm function $N : R \to \mathbb{Z}$ by

$$N(a + b\sqrt{5}) = (a + b\sqrt{5})(a - b\sqrt{5}) = a^2 - db^2$$

and showed that $N(x) = \pm 1 \iff x \in R^*$. If

$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \cdots$$

in R, then $a_2 \mid a_1, a_3 \mid a_2, \cdots$. Taking their norms gives

$$N(a_1) \geq N(a_2) \geq \cdots$$

Since each $N(a_i) \geq 0$ is an integer, we get $N(a_n) = N(a_{n+1}) = \cdots$ for some $n \in \mathbb{N}$. Since $N(d) = \pm 1 \iff d \in R^*$, it follows that $a_{i+1} \sim a_i$ for all $i \geq n$. Thus $\langle a_i \rangle = \langle a_{i+1} \rangle$ for all $i \geq n$.

□

Definition 2.7: Let R be an integral domain and $a, b \in R$. We say $d \in R$ is a greatest common divisor of a, b, denoted by $\gcd(a, b)$ if it satisfies the following conditions:

1. $d \mid a$ and $d \mid b$.
2. If $e \in R$ with $e \mid a$ and $e \mid b$ then $e \mid d$.

Note: From this definition we see that if d_1 and d_2 are both GCDs of a and b then $d_1 \mid d_2$ and $d_2 \mid d_1$. Hence $d_1 \sim d_2$ and so GCDs are unique up to association.

Proposition 2.8: Let R be a UFD and $a, b \in R \setminus \{0\}$. If $p_1, p_2, \cdots, p_k$ are the non-associated primes dividing a and b, say

$$a \sim p_1^{\alpha_1} \cdots p_k^{\alpha_k} \quad \text{and} \quad b \sim p_1^{\beta_1} \cdots p_k^{\beta_k}$$

with $\alpha_i, \beta_i \in \mathbb{N} \cup \{0\}$. Then $\gcd(a, b) \sim p_1^{\min\{\alpha_1, \beta_1\}} \cdots p_k^{\min\{\alpha_k, \beta_k\}}$.

Proof. Omitted (exercise).

□

Corollary 2.8.1: If R is a UFD with $d, a_1, \cdots, a_m \in R$ then

$$\gcd(da_1, \cdots, da_m) \sim d \gcd(a_1, \cdots, a_m).$$

Proof. Omitted (exercise).

□

Theorem 2.9: Let R be an integral domain. The following are all equivalent:

1. R is a UFD.
2. R satisfies the ACCP and $\gcd(a, b)$ exists for all non-zero $a, b \in R$.
3. R satisfies the ACCP and every irreducible element in R is prime.

Proof.

- (1) $\implies$ (2): By Proposition 2.8, $\gcd(a, b)$ exists. Also, suppose that there exists

  $$\{0\} \neq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subseteq \cdots$$

  in R. Since $\langle a_1 \rangle \neq R$, a_1 is not a unit and $a_1 \neq 0$. Write $a_1 = p_1^{k_1} \cdots p_r^{k_r}$ where the p_i are non-associated primes and $k_i \in \mathbb{N}$. Since $a_i \mid a_1$ for all i, we have

  $$a_i \sim p_1^{d_{i,1}} \cdots p_r^{d_{i,r}}$$

  where $0 \leq d_{i,j} \leq k_j$. Thus there are only finitely many choices for a_i up to association and so there exist $m \neq n$ with $a_m \sim a_n$. This implies that $\langle a_m \rangle = \langle a_n \rangle$, a contradiction. Thus R satisfies the ACCP.

- (2) $\implies$ (3): Let $p \in R$ be irreducible and suppose $p \mid ab$. By (2) let $d = \gcd(a, p)$. Then $d \mid p$. Since p is irreducible, we have $d \sim p$ or $d \sim 1$.

  In the first case, since $d \sim p$ and $d \mid a$, we get $p \mid a$. In the second case, since $d = \gcd(a, p) \sim 1$, then $\gcd(ab, pb) \sim b$. Since $p \mid ab$ and $p \mid pb$, we have $p \mid \gcd(ab, pb) \sim b$ and so $p \mid b$.

- (3) $\implies$ (1): If R satisfies the ACCP, then by Theorem 2.5, for $a \in R$ with $a \neq 0$, non-unit, a is a product of irreducible elements of R. Thus is suffices to show such a factorization is unique.

  Suppose we have

  $$p_1 \cdots p_r \sim q_1 \cdots q_s$$

  where p_i and q_j are irreducible. Since p_1 is a prime, $p_1 \mid q_j$ for some j. Without loss of generality, reorder so that $p_1 \mid q_1$. By Proposition 2.3 we have $p_1 \sim q_1$. Since $p_1 \sim q_1$ and $p_1 \cdots p_r \sim q_1 \cdots q_s$, we have $p_2 \cdots p_r \sim q_2 \cdots q_s$. Repeating this argument finitely many times gives $r = s$ and $p_i \sim q_i$.

□

Definition 2.8 (Principal Ideal Domains)**:** An integral domain R is a principal ideal domain (PID) if every ideal in R is principal.

Example 2.10:

- Every field F is a PID since the only ideals are $\{0\} = \langle 0 \rangle$ and $F = \langle 1 \rangle$.
- We have previously proved that $\mathbb{Z}$ and $F[x]$ (where F is a field) are also PIDs.

Remark: It is possible for all ideals of a ring R to be principal, but R not be an integral domain and hence not a PID. For example, all ideals of $\mathbb{Z}_n$ are principal for all n, but $\mathbb{Z}_n$ is only an integral domain (and hece a PID) if n is prime.

Proposition 2.10: Let R be a PID and let $a_1, \cdots, a_n$ be non-zero elements of R. Then $\gcd(a_1, \cdots, a_n)$ exists and there exist $r_1, \cdots, r_n \in R$ such that:

$$\gcd(a_1, \cdots, a_n) = r_1 a_1 + \cdots + r_n a_n$$

Proof. Let $A = \langle a_1, \cdots a_n \rangle = \{r_1 a_1 + \cdots + r_n a_n : r_i \in R\}$ which is an ideal of R. Since R is a PID, there exists $d \in R$ such that $A = \langle d \rangle$. Thus $d = r_1 a_1 + \cdots + r_n a_n$ for some $r_1, \cdots, r_n \in R$.

Claim 2.10.1: $d \sim \gcd(a_1, \cdots, a_n)$

Proof. Since $A = \langle d \rangle$ and $a_i \in A$ for all i we have $d \,|\, a_i$ so $d \,|\, \gcd(a_1, \cdots, a_n)$. On the other hand $\gcd(a_1, \cdots, a_n) \,|\, a_i$ for each i and so there exist $b_1, \cdots, b_n$ such that $a_i = b_i \gcd(a_1, \cdots, a_n)$ and so

$$d = r_1 a_1 + \cdots + r_n a_n = (r_1 b_1 + \cdots + r_n b_n) \gcd(a_1, \cdots, a_n),$$

meaning we also have $\gcd(a_1, \cdots, a_n) \,|\, d$. We conclude that

$$d \sim \gcd(a_1, \cdots, a_n).$$

□

The result follows from this claim.

□

Theorem 2.11: Every PID is a UFD.

Proof. If R is a PID, by Proposition 2.10 and Theorem 2.9, it suffices to show that R satisfies the ACCP. If

$$\langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \cdots$$

in R, then define

$$A = \langle a_n \rangle \cup \langle a_2 \rangle \cup \cdots .$$

Note that A is an ideal (exercise). Since R is a PID, we can write $A = \langle a \rangle$. Furthermore, we must have $a \in \langle a_n \rangle$ for some n and hence

$$\langle a_n \rangle \subseteq \langle a_{n+1} \rangle \subseteq \cdots \subseteq A = \langle a \rangle.$$

Thus

$$\langle a_n \rangle = \langle a_{n+1} \rangle = \cdots = \langle a \rangle,$$

and so R satisfies the ACCP.

□

Theorem 2.12: Let R be a PID. If $p \in R$ with $p \neq 0$, and $p \notin R^*$ then the following are all equivalent:

1. p is a prime.
2. $R/\langle p \rangle$ is a field.
3. $R/\langle p \rangle$ is an integral domain.

Proof.

- (1) $\implies$ (2): Consider the coset $a + \langle p \rangle \neq 0 + \langle p \rangle$ in $R/\langle p \rangle$. Then $a \notin \langle p \rangle$ and thus $p \nmid a$. Consider
$$A = \{ra + sp : r, s \in R\}$$
which is an ideal in R. Since R is a PID, $A = \langle d \rangle$ for some $d \in R$. Since $p \in A$, we have $d \,|\, p$. Since p is prime and thus irreducible, we have $d \sim p$ or $d \sim 1$. If $d \sim p$, then we have $\langle p \rangle = \langle d \rangle = A$. Since $a \in A$, we have $p \,|\, a$ which is a contradiction. Thus we have $d \sim 1$. It follows that $A = \langle 1 \rangle = R$. In particular, $1 \in A$, say $1 = ba + cp$ for some $b, c \in R$. Then we have
$$(a + \langle p \rangle)(b + \langle p \rangle) = ab + \langle p \rangle = 1 - cp + \langle p \rangle = 1 + \langle p \rangle \in R/\langle p \rangle.$$
It follows that $R/\langle p \rangle$ is a field.
- (2) $\implies$ (3): Every field is an integral domain (proposition from PMATH347).
- (3) $\implies$ (1): Suppose $p \,|\, ab$ with $a, b \in R$. Then
$$(a + \langle p \rangle)(b + \langle p \rangle) = ab + \langle p \rangle = 0 + \langle p \rangle \in R/\langle p \rangle.$$
Since $R/\langle p \rangle$ is an integral domain this means that either $a + \langle p \rangle = 0 + \langle p \rangle$ or $b + \langle p \rangle = 0 + \langle p \rangle$. It follows that either $p \,|\, a$ or $p \,|\, b$, hence p is prime.

□

Corollary 2.12.1: In a PID, every non-zero prime ideal is maximal.

Proof. This follows directly from Theorem 2.12 and the final remark in subsection 9.2 of PMATH347. □

Example 2.11: $\mathbb{Z}[x]$ is not a PID.

Proof. Consider $A = \{2n + xf(x) : n \in \mathbb{Z}, f(x) \in \mathbb{Z}[x]\}$, which is an ideal of $\mathbb{Z}[x]$ (exercise). Suppose that $A = \langle g(x) \rangle$ for some $g(x) \in \mathbb{Z}[x]$. Then since $2 \in A$, we have $g(x) | 2$. It follows that $g(x) \sim 1$ or $g(x) \sim 2$. Thus $A = \mathbb{Z}[x]$ or $A = \langle 2 \rangle$, neither of which are the ideal we started with. □

Remark: So far we have shown:

$$\boxed{\text{Field} \Rightarrow \text{PID} \Rightarrow \text{UFD} \Rightarrow \text{ACCP} \Rightarrow \text{Integral Domain} \Rightarrow \text{Commutative Ring} \Rightarrow \text{Ring}}$$

Furthermore, we have counter-examples disproving the converses of all these implications except for PID $\Rightarrow$ UFD. In the following subsection we will find an example which proves that not all UFDs are PIDs.

As motivation for this, we make the following observation:

- In a PID
$$I \text{ is a maximal ideal} \iff I \text{ is a prime ideal}$$
while only the forwards direction is true in general.
- In a UFD
$$p \text{ is prime} \iff p \text{ is irreducible}$$
but again, only the forwards direction is true in general.

2.4 Gauss' Lemma

Example 2.12: Consider the polynomial $2x + 4$.

- It is irreducible in $\mathbb{Q}[x]$ since 2 is a unit of $\mathbb{Q}$.
- It is not irreducible in $\mathbb{Z}[x]$ since $2x + 4 = 2(x + 2)$.

Notice that $2 = \gcd(2, 4)$.

This motivates us to make the following definition:

Definition 2.9: If R is a UFD and $0 \neq f(x) \in R[x]$, a greatest common divisor of the nonzero coefficients of $f(x)$ is called a content of $f(x)$ and is denoted by $c(f)$. If $c(f) \sim 1$, we say that $f(x)$ is a primitive polynomial.

Lemma 2.13: Let R be a UFD and let $0 \neq f(x) \in R[x]$. We have:

1. $f(x)$ can be written as $f(x) = c(f)f_1(x)$, where $f_1(x)$ is primitive.
2. If $0 \neq b \in R$, then $c(bf) \sim b\, c(f)$.

Proof.

1. For $f(x) = a_m x^m + \cdots + a_0 \in R[x]$, let $c = c(f) \sim \gcd(a_0, \cdots, a_m)$. Write $a_i = cb_i$ for all i. Then $f(x) = c\, f_1(x)$ where $f_1(x) = b_m x^m + \cdots + b_0$. This gives:

$$c \sim \gcd(a_0, \cdots, a_m) \sim \gcd(cb_0, \cdots, cb_m) \sim c \gcd(b_0, \cdots, b_m)$$

   It follows that $\gcd(b_0, \cdots, b_m) \sim 1$, i.e. $c(f_1) = 1$ and so $f_1(x)$ is primitive.

2. This follows from Corollary 2.8.1.

□

Lemma 2.14: Let R be a UFD and $\ell(x) \in R[x]$ be irreducible with $\deg \ell \geq 1$. Then $c(\ell) \sim 1$.

Proof. By Lemma 2.13, write $\ell(x) = c(\ell)\ell_1(x)$ with $\ell_1(x)$ being primitive. Since $\ell(x)$ is irreducible, either $c(\ell)$ or $\ell_1(x)$ is a unit. Since $\deg(\ell_1) = \deg(\ell) \geq 1$, $\ell_1(x)$ is not a unit. Thus $c(\ell)$ is a unit and so $c(\ell) \sim 1$.

□

Lemma 2.15 (Gauss' Lemma)**:** Let R be a UFD. If $f \neq 0$ and $g \neq 0$ in $R[x]$, then:

$$c(fg) \sim c(f)c(g)$$

In particular, this implies that any product of primitive polynomials is primitive.

Proof. Let $f(x) = c(f)f_1(x)$ and $g(x) = c(g)g_1(x)$ where f_1, g_1 are primitive. Then by Lemma 2.13 we have

$$c(fg) = c(c(f)f_1c(g)g_1) = c(f)c(g)c(f_1g_1).$$

So it suffices to show that $f(x)g(x)$ is primitive when $f(x)$ and $g(x)$ are primitive.

For the sake of contradiction, suppose that $f(x)$ and $g(x)$ are primitive, but $f(x)g(x)$ is not primitive. Since R is a UFD, there exists a prime p dividing each coefficient of $f(x)g(x)$. Write $f(x) = a_0 + \cdots + a_m x^m$ and $g(x) = b_0 + \cdots + b_n x^n$. Since $f(x)$ and $g(x)$ are primitive, p does not divide all of the a_i's, or all of the b_j's. Thus there exists $k, s \in \{0, 1, 2, \cdots\}$ such that:

1. $p \nmid a_k$ but $p \mid a_i$ for all $0 \leq i < k$.
2. $p \nmid b_s$ but $p \mid b_j$ for all $0 \leq j < s$.

The coefficient of x^{k+s} in $f(x)g(x)$ is:

$$c_{k+s} = \sum_{i+j=k+s} a_i b_j$$

Notice that if $i < k$ then $p \mid a_i$ and so $p \mid a_i b_j$. Furthermore, if $i > k$ then $j < s$ so $p \mid b_j$ which again gives $p \mid a_i b_j$. As for the case where $i = s$ we get $j = k$ and so $p \nmid a_i b_j$. Thus all but one term of the sum is divisible by p, so c_{k+s} is not divisible by p which is a contradiction. We conclude that $f(x)g(x)$ is primitive when $f(x)$ and $g(x)$ are primitive, which completes the proof.

□

Theorem 2.16: Let R be a UFD whose field of fractions is F. Regard $R \subseteq F$ as a subring of F in the usual sense. If $\ell(x) \in R[x]$ is irreducible in $R[x]$, then $\ell(x)$ is irreducible in $F[x]$.

Proof. Let $\ell(x) \in R[x]$ be irreducible. Suppose $\ell(x) = g(x)h(x)$ for some $g(x), h(x) \in F[x]$. Let a and b be the product of the denominators of the coefficients of $g(x)$ and $h(x)$ and define $g_1(x), h_1(x) \in R[x]$ by $g_1(x) = ag(x)$ and $h_1(x) = bh(x)$. Note that this gives the factorization

$$ab\ell(x) = g_1(x)h_1(x) \in R[x].$$

Since $\ell(x)$ is irreducible in $R[x]$, by Lemma 2.14 $c(\ell) \sim 1$. By Gauss' Lemma 2.15 and Lemma 2.13 this gives

$$ab \sim abc(\ell) \sim c(ab\ell(x)) = c(g_1h_1) \sim c(g_1)c(h_1). \qquad (*)$$

Now write $g_1(x) = c(g_1)g_2(x)$ and $h_1(x) = c(h_1)h_2(x)$, where $g_2(x)$ and $h_2(x)$ are primitive in $R[x]$. Then

$$ab\ell(x) = g_1(x)h_1(x) = c(g_1)c(h_1)g_2(x)h_2(x)$$

and so by $(*)$ we have $\ell(x) \sim h_2(x)g_2(x)$ in $R[x]$. Since $\ell(x)$ is irreducible in $R[x]$, it follows that $h_2(x) \sim 1$ or $g_2(x) \sim 1$ in $R[x]$.

Suppose $g_2(x) \sim 1$ in $R[x]$. Since $ag(x) = g_1(x) = c(g_1)g_2(x)$ we have follows that

$$g(x) = a^{-1}c(g_1)g_2(x) \in F[x]$$

with $g_2(x) \sim 1$ in $R[x]$. So $g(x) \sim 1$ in $F[x]$ and hence it is a unit in $F[x]$. Similarly, if $h_2(s) \sim 1$ then $h(x)$ is a unit in $F[x]$.

Thus $\ell(x) = g(x)h(x)$ in $F[x]$ implies that either $g(x)$ or $h(x)$ is a unit in $F[x]$. It follows that $\ell(x)$ is irreducible in $F[x]$.

□

Remark: We see from the above proof that if $f(x) \in R[x]$ admits a factorization in $F[x]$ as $g(x)h(x)$, then by Gauss' Lemma 2.15, there exist $\tilde{g}(x), \tilde{h}(x) \in R[x]$ such that $f(x) = \tilde{g}(x)\tilde{h}(x) \in R[x]$.

Note: The converse of Theorem 2.16 is false. For example, $2x + 4$ is irreducible in $\mathbb{Q}[x]$, but $2x + 4 = 2(x + 2)$ is reducible in $\mathbb{Z}[x]$. Note that $2 = c(2x + 4)$.

Proposition 2.17: Let R be a UFD whose field of fractions is F. Regard $R \subseteq F$ as a subring of F in the usual sense. Let $f(x) \in R[x]$ with $\deg(f) \geq 1$. The following are equivalent:

1. $f(x)$ is irreducible in $R[x]$.
2. $f(x)$ is primitive and irreducible in $F[x]$.

Proof.

- (1) $\implies$ (2): This follows from Lemma 2.14 and Theorem 2.16.
- (2) $\implies$ (1): Suppose $f(x)$ is a primitive and irreducible polynomial in $F[x]$, but it is reducible in $R[x]$. Then a non-trivial factorization of $f(x)$ in $R[x]$ must be of the form $f(x) = dg(x)$ with $d \in R$ and $d \not\sim 1$ (if both factors had degree ≥ 1 then it would be a non-trivial factorization in $F[x]$). Since $d|f(x)$, $d \not\sim 1$ divides each coefficient of $f(x)$, which contradicts the fact that $f(x)$ is primitive. Thus $f(x)$ is irreducible in $R[x]$.

□

Theorem 2.18: If R is a UFD, then $R[x]$ is also a UFD.

Proof. The proof of this theorem is long an technical. For the sake of time it was omitted from lectures. □

Example 2.13: Since $\mathbb{Z}$ is a UFD it follows from Theorem 2.18 that $\mathbb{Z}[x]$ is a UFD. Since $\mathbb{Z}[x]$ is not a PID, we can now definitively say:

$$R \text{ is a UFD} \not\implies R \text{ is a PID}$$

Definition 2.10 (Multivariate Polynomial Rings)**:** Let R be a UFD and $x_1, \cdots, x_n$ be n commuting variables (i.e. $x_i x_j = x_j x_i$ for all $1 \leq i, j \leq n$). We define the multivariate polynomial ring $R[x_1, \cdots, x_n]$ of polynomials in n variables inductively by:

$$R[x_1, \cdots, x_n] = R[x_1, \cdots, x_{n-1}][x_n]$$

Corollary 2.18.1: If R is a UFD, then for all $n \in \mathbb{N}$, $R[x_1, \cdots, x_n]$ is also a UFD.

Proof. This follows directly from Theorem 2.18.

□

Theorem 2.19 (Eisenstein's Criterion for UFDs)**:** Let R be a UFD with the field of fractions F. Let $h(x) = c_n x^n + \cdots + c_1 x + c_0 \in R[x]$ with $n \geq 1$. Let $\ell \in R$ be an irreducibe element. If $\ell \nmid c_n$, $\ell | c_i$ for all i with $0 \leq i \leq (n-1)$ and $\ell^2 \nmid c_0$, then $h(x)$ is irreducible in $F[x]$.

Proof. We proceed by contradiction. Suppose that $h(x)$ is reducible in $F[x]$. By Gauss' Lemma 2.15 for UFDs, there exist $s(x), r(x) \in R[x]$ of degree at least 1 such that $h(x) = s(x)r(x)$. Write

$$s(x) = a_0 + a_1 x + \cdots + a_m x^m$$
$$r(x) = b_0 + b_1 x + \cdots + b_k x^k$$

where $1 \leq m, k < n$. Since $h(x) = s(x)r(x)$ we have:

$$\begin{aligned} c_0 &= a_0 b_0 \\ c_1 &= a_0 b_1 + a_1 b_0 \\ c_2 &= a_0 a_2 + a_1 b_1 + a_2 b_0 \\ &\vdots \end{aligned}$$

Consider the constant term. Since $\ell | c_0$, we have $\ell | a_0 b_0$. Since ℓ is irreducible and R is a UFD, we have $\ell | a_0$ or $\ell | b_0$. Without loss of generality, suppose $\ell | a_0$. Since $\ell^2 \nmid c_0$ we have $\ell \nmid b_0$.

Now consider the coefficient of x. Since $\ell | c_1$, we have $\ell | (a_0 b_1 + a_1 b_0)$. Since $\ell | a_0$, we have $\ell | a_1 b_0$. Since $\ell \nmid b_0$, we have $\ell | a_1$.

By repeating this argument, for conditions on the coefficients of $h(x)$ imply that $\ell | a_i$ for all $0 \leq i \leq (m-1)$ and $\ell \nmid a_m$ since $\ell \nmid c_n$. Consider the reduction $\overline{h}(x) = \overline{s}(x)\overline{r}(r) \in (R/\langle \ell \rangle)[x]$. By the assumption on the coefficients of h, $\overline{h}(x) = \overline{c}_n x^n$. However, since $\overline{s}(x) = \overline{a}_m x^m$ and $\ell \nmid b_0$, $\overline{s}(x)\overline{r}(x)$ contains the term $\overline{a}_m \overline{b}_0 x^m$, which leads to a contradiction.

□

Remark: It is easy to categorize the irreducible polynomials over fields like $\mathbb{R}$ or $\mathbb{C}$, however categorizing the irreducible polynomials in $\mathbb{Q}[x]$ can be quite difficult. Eisenstein's Criterion is useful in this regard.

Example 2.14: Let p be a prime and let

$$\zeta(p) = e^{2\pi i/p} = \cos\left(\frac{2\pi}{p}\right) + i \sin\left(\frac{2\pi}{p}\right)$$

be a p-th root of 1. It is a root of the p-th cyclotomic polynomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} \cdots + x + 1.$$

Note that Eisenstein's Criterion does not imply the irreducibility of $\Phi_p(x)$ immediately, however we can consider:

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{1} x^{p-2} + \binom{p}{2} x^{p-3} + \cdots + \binom{p}{p-2} x + \binom{p}{p-1} \in \mathbb{Z}[x]$$

Notice that Eisenstein's criterion does apply to $\Phi_p(x+1)$, so $\Phi_p(x+1)$ is irreducible in $\mathbb{Q}[x]$. This implies that $\Phi_p(x)$ is also irreducible in $\mathbb{Q}[x]$ since the map $x \mapsto x+1$ is a ring isomorphism in $\mathbb{Q}[x]$. Since $\Phi_p(x)$ is primitive, $\Phi_p(x)$ is also irreducible in $\mathbb{Z}[x]$.

3 Field Extensions

3.1 Degrees of Extensions

Definition 3.1 (Field Extensions)**:** If E is a field containing another field F, we say that E is a field extension of F, denoted by E/F.

Remark: The notation E/F is not used to denote a quotient ring here, as the field E has no ideals other that E and $\{0\}$.

Notation 3.2: If E/F is a field extension, we can view E as a vector space over F using the following operations.

1. **Addition**: For $e_1, e_2 \in E$:
$$\underbrace{e_1 + e_2}_{\substack{\text{vector space}\\ \text{addition}}} := \underbrace{e_1 + e_2}_{\substack{\text{field}\\ \text{addition}}}$$
2. **Scalar Multiplication**: For $c \in F$ and $e \in E$:
$$\underbrace{ce}_{\substack{\text{vector space}\\ \text{multiplication}}} := \underbrace{ce}_{\substack{\text{field}\\ \text{multiplication}}}$$

Definition 3.3 (Degrees of Extensions)**:** The dimension of E/F when viewed as a vector space is called the degree of E over F, denoted by $[E : F]$. If $[E : F] < \infty$, we say that E/F is a finite extension. Otherwise E/F is an infinite extension.

Example 3.1:

1. $[\mathbb{C} : \mathbb{R}] = 2$ is a finite extension since $C \cong \mathbb{R} + \mathbb{R}i$ where $i^2 = -1$.
2. Let F be a field. Define
$$F[x] = \{f(x) = a_0 + \cdots + a_n x^n, a_i \in F \text{ and } n \in \mathbb{N} \cup \{0\}\}$$
and
$$F(x) = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in F[x] \text{ and } g(x) \neq 0 \right\}.$$
Then $[F(x) : F] = \infty$ since $\{1, x, x^2, \cdots\}$ are linearly independent over F.

Theorem 3.1: If E/K and K/F are finite extensions, then E/F is a finite field extension and $[E : F] = [E : K][K : F]$. In-particular, if K is an intermediate field of a finite extension E/F, then $[K : F]|[E : F]$.

Proof. Suppose $[E : K] = m$ and $[K : F] = n$. Let $\{a_1, \cdots, a_m\}$ be a basis of E/K and $\{b_1, \cdots, b_n\}$ be a basis of K/F. It suffices to prove $\{a_i b_j : 1 \leq i \leq m \text{ and } 1 \leq j \leq n\}$ is a basis of E/F since this set has size nm.

Claim 3.1.1: Every element of E is a linear combination of $\{a_i b_j\}$ over F.

Proof. For $e \in E$, we have $e = \sum_{i=1}^{m} k_i a_i$ with $k_i \in K$. For $k_i \in K$, we have $k_i = \sum_{j=1}^{n} c_{ij} b_j$ with $c_{ij} \in F$. Thus

$$e = \sum_{i=1}^{m} \sum_{j=1}^{n} c_{ij} b_j a_i.$$

□

Claim 3.1.2: The set $\{a_i b_j : 1 \leq i \leq n \text{ and } 1 \leq j \leq n\}$ is linearly independent over F.

Proof. Suppose $\sum_{i=1}^{m} \sum_{j=1}^{n} c_{ij} b_j a_i = 0$ with $c_{ij} \in F$. Since $\sum_{j=1}^{n} c_{ij} b_j \in K$ and $\{a_1, \cdots, a_m\}$ is linearly independent over K, we have $\sum_{j=1}^{n} c_{ij} b_j = 0$. Since $\{b_1, \cdots, b_n\}$ is independent over F, we have $c_{ij} = 0$.

□

Combining these two claims we see that $\{a_i b_j : 1 \leq i \leq m \text{ and } 1 \leq j \leq n\}$ is a basis of E/F and so

$$[E : F] = mn = [E : K][K : F].$$

□

3.2 Algebraic and Transcendental Extensions

Definition 3.4 (Algebraic and Transcendental Elements)**:** Let E/F be a field extension and $\alpha \in E$. We say that α is algebraic over F if there exists $f(x) \in F[x] \setminus \{0\}$ with $f(\alpha) = 0$. Otherwise, α is transcendental over F.

Example 3.2: $\frac{c}{d} \in \mathbb{Q}$ (root of $dx - c$) and $\sqrt{2}$ (root of $x^2 = 2$) are algebraic over $\mathbb{Q}$. However e and π are transcendental over $\mathbb{Q}$.

Example 3.3: $\alpha = \sqrt{2} + \sqrt{3}$ is algebraic over $\mathbb{Q}$.

Proof. Writing $\alpha - \sqrt{2} = \sqrt{3}$ and squaring both sides gives:

$$\alpha^2 - 2\sqrt{2}\alpha + 2 = 3$$

It follows that $\alpha^2 - 1 = 2\sqrt{2}\alpha$ and so squaring both sides again gives:

$$\alpha^4 - 2\alpha^2 + 1 = 8\alpha^2 \implies \alpha^4 - 10\alpha^2 + 1 = 0$$

□

Notation 3.5: Let E/F be a field extension and $\alpha \in E$. We use $F[\alpha]$ to denote the smallest subring of E containing F and α and we use $F(\alpha)$ to denote the smallest subfield of E containing F and α. For $\alpha_1, \alpha_2, \cdots, \alpha_n \in F$, we define $F[\alpha_1, \alpha_2, \cdots, \alpha_n]$ and $F(\alpha_1, \alpha_2, \cdots, \alpha_n)$ similarly.

Theorem 3.2: Let E/F be a field extension and $\alpha \in E$. If α is transcendental over F, then

$$F[\alpha] \cong F[x]$$

and

$$F(\alpha) \cong F(x)$$

where $F(x)$ is the field of rational functions as defined in Example 3.1. In particular, this gives $F[\alpha] \neq F(\alpha)$.

Proof. Let $\psi : F(x) \to F(a)$ be the unique field homomorphism defined by $\psi(x) = \alpha$. Thus for $f(x), g(x) \in F[x]$ with $g(x) \neq 0$,

$$\psi\left(\frac{f(x)}{g(x)}\right) = \frac{f(\alpha)}{g(\alpha)} \in F(\alpha).$$

Note that since α is transcendental, we have $g(\alpha) \neq 0$. Thus the map is well defined.

Now, since $F(x)$ is a field and $\ker(\psi)$ is an ideal of $F(x)$, we have $\ker(\psi) = F(x)$ or $\ker(\psi) = \{0\}$. Since $\psi(x) = \alpha \neq 0$, $\ker(\psi) \neq F$, meaning $\ker(\psi) = 0$ and so ψ is injective. Also, since $F(x)$ is a field, $\mathrm{Im}(\psi)$ contains a field generated by F and α, i.e. $F(\alpha) \subseteq \mathrm{Im}(\psi)$. Thus $\mathrm{Im}(\phi) = F(\alpha)$ and ψ is surjective, making it an isomorphism. It follows that $F(x) \cong F(\alpha)$ and $F[x] \cong F[\alpha]$.

□

Theorem 3.3: Let E/F be a field extension and $\alpha \in E$. If α is algebraic over F, then there exists a unique monic irreducible polynomial $p(x) \in F[x]$ such that there exists a field isomorphism

$$\psi : F[x]/\langle p \rangle \to F[\alpha] \text{ with } \psi(x) = \alpha$$

from which we conclude $F[\alpha] = F(\alpha)$.

Proof. Consider the unique field homomorphism $\psi : F[x] \to F[\alpha]$ defined by $\psi(x) = \alpha$. Thus for $f(x) \in F[x]$, we have $\psi(f) = f(\alpha) \in F[\alpha]$. Since $F[x]$ is a ring, $\mathrm{Im}(\psi)$ contains a ring generated by F and α, i.e. $F[\alpha] \subseteq \mathrm{Im}(\psi)$. Thus $\mathrm{Im}(\psi) = F[\alpha]$.

Now, to consider the kernal let

$$I = \ker(\psi) = \{f(x) \in F[x], f(\alpha) = 0\}.$$

Since α is algebraic, $I \neq \{0\}$. By the first isomorphism theorem, we have

$$F[x]/I \cong \mathrm{Im}(\psi)$$

which is a subring of the field $F(\alpha)$. Thus $F[x]/I$ is an integral domain, and so I is a prime ideal. It follows that $I = \langle p(x) \rangle$, where $p(x)$ is irreducible. If we assume that $p(x)$ is monic then it is uniquely specified. It follows that

$$F[x]/\langle p(x) \rangle \cong F[\alpha].$$

Since $F[x]$ is a PID, the prime ideal $\langle p(x) \rangle$ is maximal. Thus $F[x]/\langle p(x) \rangle$ is a field. Since $F(\alpha)$ is the smallest field containing F and α, we have $F[\alpha] = F(\alpha)$.

□

Definition 3.6 (Minimal Polynomials)**:** If α is algebraic over F, then the unique monic irreducible polynomial $p(x)$ in Theorem 3.3 is called the minimal polynomial of α over F. From the proof of Theorem 3.3, we see that if $f(x) \in F[x]$ with $f(\alpha) = 0$, then $p(x) | f(x)$.

As a direct consequence of Theorems 3.2 and 3.3, we have:

Theorem 3.4: Let E/F be a field extension and $\alpha \in E$.

1. α is transcendental over $F \iff [F(\alpha) : F] = \infty$
2. α is algebraic over $F \iff [F(\alpha) : F] < \infty$

Moreover, if $p(x)$ is the minimal polynomial of α over F, we have $[F(\alpha) : F] = \deg(p)$ and $\{1, \alpha, \alpha^2, \cdots, \alpha^{\deg(p)-1}\}$ is a basis of $F(\alpha)/F$.

Proof. It suffices to prove $\implies$ in (1) and (2).

1. By Theorem 3.2, if α is transcendental over F, then $F(\alpha) = F(x)$. In $F(x)$, the elements $\{1, x, x^2, \cdots\}$ are linearly independent over F. Thus $[F(\alpha) : F] = \infty$.
2. From Theorem 3.3, if α is algebraic over F then
$$F(\alpha) \cong F[x]/\langle p(x)\rangle$$
with $x \mapsto \alpha$. Note that
$$F(x)/\langle p(x)\rangle \cong \{r(x) \in F[x], \deg(r) < \deg(p)\}$$
where p is the minimal polynomial of α. Thus $\{1, x, \cdots, x^{\deg(p)-1}\}$ forms a basis of $F[x]/\langle p(x)\rangle$. It follows that $[F(\alpha) : F] = \deg(p)$ and $\{1, \alpha, \cdots, \alpha^{\deg(p)-1}\}$ is a basis of $F(\alpha)$ over F.

□

Example 3.4: Let $p \in \mathbb{Z}$ be prime and $\zeta_p = e^{2\pi i/p}$ be a p-th root of 1. We have seen in chapter 2 that ζ_p is a root of the p-th cyclotomic polynomial $\Phi_p(x)$, which is irreducible. Thus by Theorem 3.4, $\Phi_p(x)$ is the minimal polynomial of ζ_p over $\mathbb{Q}$ and $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$. The field $\mathbb{Q}(3\zeta)$ is called the p-th cyclotomic extension of $\mathbb{Q}$.

Example 3.5: Let $\alpha = \sqrt{2} + \sqrt{3}$. In Example 3.3 we showed that α was a root of $x^4 - 10x^2 + 1$. One can show (exercise) that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Since $\sqrt{2}$ is a root of $x^2 - 2$, which is irreducible, we have $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Also, since $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ (exercise) we have $\alpha \notin \mathbb{Q}(\sqrt{2})$. Hence $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})] \geq 2$. Since α is a root of a polynomial of degree 4, it follows that:

$$4 \geq [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \geq 2 \cdot 2 = 4$$

Thus $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ and so $x^4 - 10x^2 + 1$ is the minimal polynomial of α over $\mathbb{Q}$.

Exercise: Can we instead use Eisenstein's criterion to prove that the polynomial in this example is irreducible?

Theorem 3.5: Let E/F be a field extension. If $[E : F] < \infty$, there exists $\alpha_1, \alpha_2, \cdots, \alpha_n \in E$ such that:
$$F \subsetneq F(\alpha_1) \subsetneq F(\alpha_1, \alpha_2) \subsetneq \cdots \subsetneq F(\alpha_1, \cdots, \alpha_n) = E$$

Proof. We proceed by induction on $[E : F]$. If $[E : F] = 1$, $E = F$ and we are done. Now suppose $[E : F] > 1$ and the statement holds for all field extensions E_1/F_1 with $[E_1 : F_1] < [E : F]$. Let $\alpha_1 \in E/F$, by Theorem 3.1 $[E : F] = [E : F(\alpha_1)][F(\alpha_1) : F]$. Since $F[(\alpha_1) : F] > 1$, we have $[E : F(\alpha_1)] < [E : F]$. By the hypothesis, there exist $\alpha_2, \cdots, \alpha_n$ such that:

$$F(\alpha_1) \subseteq F(\alpha_1)(\alpha_2) \subsetneq \cdots \subsetneq F(\alpha_1)(\alpha_2, \cdots, \alpha_n) = E = F(\alpha_1, \cdots, \alpha_n)$$

Thus the result holds since $F \subsetneq F(\alpha_1)$.

□

Remark: From Theorem 3.5 we see that to understand a finite extension, it suffices to understand a finite simple extension.

Definition 3.7 (Algebraic and Transcendental Field Extensions)**:** A field extension E/F is algebraic if every $\alpha \in E$ is algebraic over F. Otherwise, it is transcendental.

Theorem 3.6: Let E/F be a field extension. If $[E : F] < \infty$ then E/F is algebraic.

Proof. Suppose $[E : F] = n$. For $\alpha \in E$, the elements $\{1, \alpha, \alpha^2, \cdots, \alpha^n\}$ are not linearly independent over F. Thus there exist $c_i \in F$, not all zero, such that $\sum_{i=0}^{n} c_i \alpha^i = 0$. Thus α is a root of the polynomial $\sum_{i=0}^{n} c_i \alpha^i \in F[x]$ and so it is algebraic over F.

□

Remark: The converse of Theorem 3.6 is false (see Example 3.7).

Theorem 3.7: Let E/F be a field extension. Define $L = \{\alpha \in E : [F(\alpha) : F] < \infty\}$. Then L is an intermediate field of E/F.

Proof. If $\alpha, \beta \in L$ then we need to show that $\alpha \pm \beta$, $\alpha \cdot \beta$ and α/β (with $\beta \neq 0$) are in L. By the definition of L, we have $[F(\alpha) : F] < \infty$ and $[F(\beta) : F] < \infty$. Consider the field $F(\alpha, \beta)$. Since the minimal polynomial over $F(\beta)$ divides the minimal polynomial of α over F (the minimal polynomial of α over F, say $p(x) \in F[x]$, is also a polynomial over $F(\beta)$, i.e. $p(x) \in F(\beta)[x]$ with $p(\alpha) = 0$). We have $[F(\alpha, \beta) : F(\beta)] \leq [F(\alpha) : F]$. Combining this with Theorem 3.1, we have

$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\beta)][F(\beta) : F] \leq [F(\alpha) : F][F(\beta) : F] < \infty$$

Since $\alpha + \beta \in F(\alpha, \beta)$, it follows that

$$[F(\alpha + \beta) : F] \leq [F(\alpha, \beta) : F] < \infty$$

i.e. $\alpha + \beta \in L$. Similarly $\alpha - \beta$, $\alpha \cdot \beta$ and α/β ($\beta \neq 0$) are in L. Thus L is a field.

□

Definition 3.8 (Algebraic Closures)**:** Let E/F be a field extension. The set

$$L = \{\alpha \in E : [F(\alpha) : F] < \infty\}$$

is called the algebraic closure of F in E.

Example 3.6: By the fundamental theorem of algebra, $\mathbb{C}$ is algebraically closed. Moreover, $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$ in $\mathbb{C}$.

Example 3.7: Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. In other words $\overline{\mathbb{Q}}$ contains all the elements of $\mathbb{C}$ which are algebraic over $\mathbb{Q}$. Since $\zeta_p \in \overline{\mathbb{Q}}$, we have $[\overline{\mathbb{Q}} : \mathbb{Q}] \geq [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$. Since there are infinitely many primes we have $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$. Thus the converse of Theorem 3.6 is false.

4 Splitting Fields

4.1 Existence of Splitting Fields

Definition 4.1 (Splitting Polynomials)**:** Let E/F be a field extension. We say $f(x) \in F[x]$ splits over E if E contains all roots of $f(x)$, i.e. $f(x)$ is a product of linear factors in $E[x]$.

Definition 4.2: Let $\tilde{E}/F$ be a field extension, $f(x) \in F[x]$ and $F \subseteq E \subseteq \tilde{E}$. If:

1. $f(x)$ splits over E
2. There is no proper subfield of E that $f(x)$ splits over

then we say E is a splitting field of $f(x)$ in $\tilde{E}$.

Theorem 4.1: Let $p(x) \in F[x]$ be irreducible. The quotient ring $F[x]/\langle p(x)\rangle$ is a field containing F and a root of $p(x)$.

Proof. Since $p(x)$ is irreducible, the ideal $I = \langle p(x)\rangle$ is prime. Since $F[x]$ is a PID, I is maximal. Thus $E = F[x]/I$ is a field. Consider the coset map:

$$\psi : F \to E, \qquad a \mapsto a + I$$

Since F is a field and $\psi \neq 0$, ψ is injective. Thus by identifying F with $\psi(F)$, F can be viewed as a subfield of E.

Claim 4.1.1: Let $\alpha = x + I \in E$. Then α is a root of $p(x)$.

Proof. Write $p(x) = a_0 + a_1x + \cdots + a_nx^n$ where $a_i \in F$. We have:

$$p(x) = a_0 + a_1x + \cdots + a_nx^n = (a_0 + I) + (a_1 + I)x + \cdots + (a_n + I)x^n \in E[x]$$

This gives:

$$\begin{aligned} p(\alpha) &= (a_0 + I) + (a_1 + I)\alpha + \cdots + (a_n + I)\alpha^n \\ &= (a_0 + I) + (a_1 + I)(x + I) + \cdots + (a_n + I)(x + I)^n \\ &= (a_0 + I) + (a_1x + I) + \cdots + (a_nx^n + I) \\ &= (a_0 + a_1x + \cdots + a_nx^n) + I \\ &= p(x) + I = 0 + I \end{aligned}$$

Thus $\alpha = x + I \in E$ is a root of $p(x)$.

□

This completes the proof.

□

Theorem 4.2 (Kronecker)**:** Let $f(x) \in F[x]$. There exists a field E containing F such that $f(x)$ splits over E.

Proof. We proceed by induction on $\deg(f)$. If $\deg(f) = 1$, let $E = F$ and we are done. So suppose that $\deg(f) > 1$ and the statement holds for all $g(x)$ with $\deg(g) < \deg(f)$ ($g(x)$ is not necessarily in $F[x]$). Write $f(x) = p(x)h(x)$ where $p(x), h(x) \in F[x]$ and $p(x)$ is irreducible. By Theorem 4.1, there exists a field K such that $F \subseteq K$ and K contains a root of $p(x)$, say α. Thus $p(x) = (x - \alpha)q(x)$ and $f(x) = (x - \alpha)h(x)q(x)$ where $q(x) \in K[x]$. Since $\deg(hq) < \deg(f)$, by induction there exists a field E containing K over which $h(x)q(x)$ splits. It follows that $F[x]$ splits over E.

□

Theorem 4.3: Every $f(x) \in F[x]$ has a splitting field which is a finite extension of F.

Proof. For $f(x) \in F[x]$, by Theorem 4.2, there exists a field extension E/F over which $f(x)$ splits. Let $\alpha_1, \cdots, \alpha_n$ be the roots of $f(x)$ in E. Consider $F(\alpha_1, \cdots, \alpha_n)$. This is the smallest subfield of E containing all roots of $f(x)$. So $f(x)$ does not split over any proper subfield of it. Thus $F(\alpha_1, \cdots, \alpha_n)$ is the splitting field of $f(x)$ in E. In addition, since α_i are all algebraic, $F(\alpha_1, \cdots, \alpha_n)/F$ is finite. □

Remark: If $f(x)$ splits in E, i.e. $\alpha_1, \cdots, \alpha_n$ are roots in E, then $F(\alpha_1, \cdots, \alpha_n)$ is the splitting field of $f(x)$ in E.

Example 4.1: Consider $x^3 - 2 \in \mathbb{Q}[x]$. We have

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\zeta_3)(x - \sqrt[3]{2}\zeta_3^2)$$

where $\zeta_3 = e^{2\pi i/3}$. Hence the splitting field of $x^3 - 2$ over $\mathbb{Q}$ is

$$\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\zeta, \sqrt[3]{2}\zeta^2) = \mathbb{Q}(\sqrt[3]{2}\zeta).$$

4.2 Uniqueness of Splitting Fields

We have seen that for the field extension E/F, given $f(x) \in F[x]$ with roots $\alpha_1, \cdots \alpha_n$ the field $F(\alpha_1, \cdots, \alpha_n)$ in is the splitting field of $f(x)$ in E and it is unique within E.

Question: If we change E/F to a different field extension, say E_1/F, what's the relation between the splitting field of $f(x)$ in E and the one in E_1?

Definition 4.3 (Extensions of Ring Homomorphisms)**:** Let $\phi : R \to R_1$ be a ring homomorphism and $\Phi : R[x] \to R_1[x]$ be the unique ring homomorphism satisfying $\Phi\restriction_R = \phi$ and $\Phi(x) = x$. In this case we say Φ extends ϕ. More generally, if $R \subseteq S$, $R_1 \subseteq S_1$ and $\Phi : S \to S_1$ is a ring homomorphism with $\Phi\restriction_R = \phi$, we say Φ extends ϕ.

Theorem 4.4: Let $\phi : F \to F_1$ be an isomorphism of fields and $f(x) \in F[x]$. Let $\Phi : F[x] \to F_1[x]$ be the unique ring isomorphism which extends ϕ. Let $f_1(x) = \Phi(f(x))$ and E/F and E_1/F_1 be splitting fields of $f(x)$ and $f_1(x)$ respectively. Then there exists an isomorphism $\psi : E \to E_1$ which extends ϕ.

Proof. We proceed by induction on $[E : F]$. If $[E : F] = 1$ then $f(x)$ is a product of linear factors in $F[x]$ and so is $f_1(x) \in F_1[x]$. Thus $E = F$, $E_1 = F_1$ and if we take $\psi = \phi$ then we are done. So suppose $[E : F] > 1$ and the statement is true for all field extensions $\tilde{E}/\tilde{F}$ with $[\tilde{E} : \tilde{F}] < [E : F]$.

Let $p(x) \in F[x]$ be an irreducible factor of $f(x)$ with $\deg(p) \geq 2$ and let $p_1(x) = \Phi(p(x))$ (such $p(x)$ exists since if all irreducible factors of $f(x)$ were of degree 1, then $[E : F] = 1$).

Let $\alpha \in E$ and $\alpha_1 \in E_1$ be roots of $p(x)$ and $p_1(x)$ respectively. From Theorem 3.3, we have a field isomorphism $F(\alpha) \cong F[x]/\langle p(x)\rangle$, $\alpha \mapsto x + \langle p(x)\rangle$. Similarly, there is a field isomorphism $F_1(\alpha_1) \cong F_1[x]/\langle p_1(x)\rangle$, $\alpha_1 \mapsto x + \langle p_1(x)\rangle$.

Consider the isomorphism $\Phi : F[x] \to F_1[x]$ which extends ϕ. Since $p_1(x) = \Phi(p(x))$ there exists a field isomorphism $\tilde{\Phi} : F[x]/\langle p(x)\rangle \to F_1[x]/\langle p_1(x)\rangle$, $x + \langle p(x)\rangle \mapsto x + \langle p_1(x)\rangle$ which extends ϕ. It follows that there exists a field isomorphism $\tilde{\phi} : F(\alpha) \to F_1(\alpha)$, $\alpha \mapsto \alpha_1$ which extends ϕ.

Note that since $\deg(p) \geq 2$, $[E : F(\alpha)] < [E : F]$ since E (respectively, E_1) is the splitting field of $f(x) \in F(\alpha)[x]$ (respectively, $f_1(x) \in F_1(\alpha)[x]$) over $F(\alpha)$ (respectively, $F_1(\alpha_1)$). By induction, there exists $\psi : E \to E_1$ which extends $\tilde{\phi}$. Thus ψ also extends ϕ. □

Corollary 4.4.1: Any two splitting fields of $f(x) \in F[x]$ over F are F-isomorphic. Thus we can now say "the" splitting field of $f(x)$ over F.

Proof. Let $\phi : F \to F$ be the identity map and apply Theorem 4.4

□

4.3 Degrees of Splitting Fields

Theorem 4.5: Let F be a field and $f(x) \in F[x]$ with $\deg(f) = n \geq 1$. If E/F is the splitting field of $f(x)$, then $[E : F]|n!$.

Proof. We prove this theorem by induction on $\deg(f) = n$. If $\deg(f) = 1$ then we choose $E = F$ and we have $[E : F]|1!$.

So suppose that $\deg(f) = n > 1$ and the statement holds for all $g(x)$ with $\deg(g) < \deg(f)$.

- If $f(x) \in F[x]$ is irreducible and $\alpha \in E$ a root of $f(x)$, by Theorem 3.3 $F(\alpha) \cong F[x]/\langle f(x)\rangle$ and $[F(\alpha) : F] = \deg(f) = n$. Write $f(x) = (x - \alpha)g(x) \in F(\alpha)[x]$ with $g(x) \in F(\alpha)[x]$. Since E is the splitting field of $g(x)$ over $F(\alpha)$ and $\deg(g) = n - 1$, by induction, $[E : F(\alpha)]|(n - 1)!$. Since $[E : F] = [E : F(\alpha)][F(\alpha) : F]$, it follows that $[E : F]|n!$.
- If $f(x)$ is not irreducible, write $f(x) = g(x)h(x)$ with $g(x), h(x) \in F[x]$, $\deg(g) = m$, $\deg(h) = k$, $m + k = n$ and $1 \leq m, k < n$. Let k be the splitting field of $g(x)$ over F. Since $\deg(g) = m$, by induction $[K : F]|m!$. Since E is the splitting field of $h(x)$ over K and $\deg(h) = k$, by induction $[E : K]|k!$. Thus $[E : F]|m!k!$, which is a factor of $n!$ (by the binomial theorem since $m+k = n$).

□

5 More Field Theory

5.1 Prime Fields

Definition 5.1 (Prime Fields)**:** The prime field of a field F is the intersection of all subfields of F.

Theorem 5.1: If F is a field, then its prime field is isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}_p$ for some prime p.

Proof. Let F_1 be a subfield of F. Consider the ring map

$$\chi : \mathbb{Z} \to F_1, \quad n \mapsto n \cdot 1$$

where $1 \in F_1 \subseteq F$. Let $I = \ker(\chi)$ be the kernel of χ. Since $\mathbb{Z}/I \cong \operatorname{Im}\chi$, a subring of F_1, it is an integral domain. Thus I is a prime ideal. This gives two cases:

1. If $I = \langle 0 \rangle$, then $\mathbb{Z} \subseteq F_1$. Since F_1 is a field, $\mathbb{Q} = \operatorname{Frac}(\mathbb{Z}) \subseteq F_1$.
2. If $I = \langle p \rangle$, by the first isomorphism theorem, $\mathbb{Z}_p \cong \mathbb{Z}/\langle p \rangle \cong \operatorname{Im}\chi \subseteq F_1$.

□

Definition 5.2 (Field Characteristics)**:** Given a field F, if its prime field is isomorphic to $\mathbb{Q}$ we say F has characteristic 0. Otherwise, if the prime field of F is isomorphic to $\mathbb{Z}_p$ then we say that F has characteristic p. The characteristic of F is denoted $\operatorname{ch}(F)$.

Note: If $\operatorname{ch}(F) = p$, then for all $a, b \in F$,

$$\begin{aligned}(a+b)^p &= a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \cdots + \binom{p}{p-1}ab^{p-1} + b^p \\ &= a^p + b^p\end{aligned}$$

since all the coefficients $\binom{p}{i}$ for $1 < i < p$ are divisible by p and hence 0.

Proposition 5.2: Let F be a field with $\operatorname{ch}(F) = p$ and let $n \in \mathbb{N}$. Then the map $\psi : F \to F$ given by $u \mapsto u^{p^n}$ is an injective $\mathbb{Z}_p$ homomorphism of fields. Furthermore, if F is finite, then ψ is a $\mathbb{Z}_p$ isomorphism.

Proof. TODO - Proof missing

□

5.2 Formal Derivatives and Repeated Roots

Definition 5.3 (Formal Derivatives)**:** If F is a field then the monomials $\{1, x, x^2, x^3, \cdots\}$ form an F-basis for $F[x]$. Define the linear operator $D : F[x] \to F[x]$ by $D(1) = 0$ and $D(x^i) = ix^{i-1}$ $(i \in \mathbb{N})$. Thus for

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \qquad (a_i \in F)$$

we have

$$D(f)(x) = a_1 + 2a_2 x + 3a_3 x^2 + \cdots + n a_n x^{n-1}.$$

We call $f' := D(f)$ the formal derivative of f.

Note: Formal derivatives obey many of the properties we would expect from "normal" derivatives. Some examples are:

1. $D(f+g) = D(f) + D(g)$
2. $D(cf) = cD(f)$, $c \in F$
3. Leibniz Rule: $D(fg) = D(f)g + fD(g)$

Theorem 5.3: Let F be a field and $f(x) \in F[x]$.

1. If $\mathrm{ch}(F) = 0$, then $f'(x) = 0$ if and only if $f(x) = c$ for some $c \in F$.
2. If $\mathrm{ch}(F) = p$, then $f'(x) = 0$ if and only if $f(x) = g(x^p)$ for some $g(x) \in F[x]$.

Proof.

1. $\Longleftarrow$ This follows from the definition of f'.

   $\Longrightarrow$ If $f(x) = a_0 + a_1x + \cdots + a_nx^n$, then $f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1} = 0$ implies that $ia_i = 0$ for all $1 \le i \le n$. Since $\mathrm{ch}(F) = 0$, $i \neq 0$, thus $a_i = 0$ for all $i \ge 1$. Thus $f(x) = a_0 \in F$.

2. $\Longleftarrow$ Write $g(x) = b_0 + b_1x + \cdots + b_mx^m \in F[x]$. Then $f(x) = g(x^p) = b_0 + b_1x^p + \cdots + b_mx^{mp}$. Thus $f'(x) = pb_1x^{p-1} + \cdots + pmb_mx^{pm-1} = 0$ since $\mathrm{ch}(F) = p$.

   $\Longrightarrow$ For $f(x) = a_0 + a_1x + \cdots + a_n$, $f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1} = 0$ implies that $ia_i = 0$ for all $1 \le i \le n$. Since $\mathrm{ch}(F) = p$, $ia_i = 0$ implies that $a_i = 0$ unless $p \mid i$. Thus $f(x) = a_0 + a_px^p + a_{2p}x^{2p} + \cdots + a_{mp}x^{mp} = g(x^p)$ where $g(x) = a_0 + a_px + \cdots + a_{mp}x^m \in F[x]$.

□

Definition 5.4 (Repeated Roots)**:** Let E/F be a field extensions and $f(x) \in F[x]$. We say $\alpha \in E$ is a řepeated root of $f(x)$ if $f(x) = (x-\alpha)^2 g(x)$ for some $g(x) \in E[x]$.

Theorem 5.4: Let E/F be a field extension, $f(x) \in F[x]$ and $\alpha \in E$. Then α is a repeated root of $f(x)$ if and only if $(x-\alpha)$ divides both $f(x)$ and $f'(x)$ (i.e. $(x-\alpha) \mid \gcd(f, f')$.

Proof.

$\Longrightarrow$ Suppose $f(x) = (x-\alpha)^2 g(x)$. Then

$$f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x) = (x-\alpha)(2g(x) + (x-\alpha)g(x))$$

thus $(x-\alpha)$ divides both f and f'.

$\Longleftarrow$ Suppose that $(x-\alpha)$ divides both f and f'. Write $f(x) = (x-\alpha)h(x)$ where $h(x) \in E[x]$. Then

$$f'(x) = h(x) + (x-\alpha)h'(x)$$

and so, since $f'(\alpha) = 0$, we must have $h(\alpha) = 0$ and so $(x-\alpha) \mid h(x)$. Thus $(x-\alpha) \mid f'(x)$.

□

Definition 5.5 (Separable Polynomials)**:** Let F be a field and $f(x) \in F[x] \setminus \{0\}$. We say $f(x)$ is separable over F if it has no repeated root in any extension of F.

Corollary 5.4.1: $f(x) \in F[x]$ is separable if and only if $\gcd(f, f') = 1$.

Proof. Note that $\gcd(f, f') \neq 1$ if and only if $(x - \alpha) \mid \gcd(f, f')$ for α in some extensions of F. By Theorem 5.4 the result follows. □

Remark: Notice that the condition of repeated roots in the definition of separability depends on the extensions of F, while the equivalent $\gcd(f, f')$ condition in Corollary 5.4.1 involves only the field F.

Corollary 5.4.2: If $\mathrm{ch}(F) = 0$, then every irreducible $r(x) \in F[x]$ is separable.

Proof. Let $r(x) = F[x]$ be irreducible. Then:

$$\gcd(r, r') = \begin{cases} 1, & r' \neq 0 \\ r, & r' = 0 \end{cases}$$

Suppose that $r(x)$ is not separable. Then by Corollary 5.4.1 $\gcd(r, r') \neq 1$, thus $r' = 0$. Since $\mathrm{ch}(F) = 0$, from Theorem 5.3, $r'(x) = 0$ implies that $r(x) = c \in F$, a contradiction since $\deg(r) \geq 1$. Thus $r(x)$ is separable. □

Example 5.1: The p-th cyclotomic polynomial $\Phi_p(x) = x^{p-1} + \cdots + x + 1$ is irreducible over $\mathbb{Q}$ and hence separable. We recall that the roots of $\Phi_p(x)$ are $\zeta_p, \zeta_p^2, \cdots, \zeta_p^{p-1}$ which are all distinct.

5.3 Finite Fields

Notation 5.6: Given a field F, let $F^* = F \setminus \{0\}$ be the multiplicative group of non-zero elements of F.

Proposition 5.5: If F is a finite field, then $\mathrm{ch}(F) = p$ for some prime p and $|F| = p^n$ for some $n \in \mathbb{N}$.

Proof. Since F is a finite field, by Theorem 5.1, its prime field is $\mathbb{Z}_p$. Since F can be viewed as a finite dimensional vector space over $\mathbb{Z}_p$, we have $F \cong \mathbb{Z}_p^n$ and so $|F| = p^n$. □

Theorem 5.6: Let F be a field and G be a finite subgroup of F^*. Then G is a cyclic group. In-particular, if F is a finite field then F^* is a cyclic group.

Proof. Without loss of generality, we can assume $G \neq \{1\}$. Since G is a finite abelian group, using the fundamental theorem of finite abelian groups we have

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$

with $n_1 > 1$ and $n_1 \mid n_2, n_2 \mid n_3, \cdots n_{r-1} \mid n_r$. It follows that

$$n_r(\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}) = 0$$

and so for all $u \in G$, u is a root of $x^{n_r} - 1 \in F[x]$. Since this polynomial has at most n_r distinct roots in F, we have $r = 1$ and $G \cong \mathbb{Z}/n_r\mathbb{Z}$.

□

Corollary 5.6.1: If F is a finite field, then F is a simple extension of $\mathbb{Z}/p\mathbb{Z}$, i.e. $F = \mathbb{Z}/p\mathbb{Z}(u)$

Proof. This follows by taking u to be a generator of the multiplicative group F^*.

□

Theorem 5.7: Let p be a prime and $n \in \mathbb{N}$.

1. F is a field with $|F| = p^n$ if and only if F is a splitting field of $x^{p^n} - x$ over $\mathbb{Z}/p\mathbb{Z}$.
2. Let F be a finite field with $|F| = p^n$. Let $m \in \mathbb{N}$ with $m|n$. Then F contains unique subfield K with $|K| = p^m$.

Proof.

1. $\Longrightarrow$ If $|F| = p^n$, then $|F^*| = p^n - 1$. Then every $u \in F^*$ satisfies $u^{p^n-1} = 1$, and thus they are all roots of $x(x^{p^n-1} - 1) = x^{p^n} - x \in \mathbb{Z}/p\mathbb{Z}[x]$. Since $0 \in F$ is also a root of $x^{p^n} - x$ it has p^n distinct roots in F, i.e. it splits over F. Thus F is the splitting field of $x^{p^n} - x$ over $\mathbb{Z}/p\mathbb{Z}$.

   $\Longleftarrow$ Suppose F is the splitting field of $f(x) = x^{p^n} - x$ over $\mathbb{Z}/p\mathbb{Z}$. Since $\mathrm{ch}(F) = p$, we have $f'(x) = -1$. Since $\gcd(f, f') = 1$, by Corollary 5.4.1, $f(x)$ has p^n distinct roots in F. Let E be the set of all roots of $f(x)$ in F. Let $\phi : F \to F$ be given by $u \mapsto u^{p^n}$ for $u \in F$. u is a root of $f(x)$ if and only if $\phi(u) = u$. Since the condition is closed under addition, subtraction, multiplication and division, the set E is a subfield of F of order p^n, which contains $\mathbb{Z}/p\mathbb{Z}$ (since all $u \in \mathbb{Z}/p\mathbb{Z}$ satisfy $u^{p^n} = u$). Since F is the splitting field, it is generated over $\mathbb{Z}/p\mathbb{Z}$ by the roots of $f(x)$, i.e. the elements of E. Thus $F = \mathbb{Z}/p\mathbb{Z}(E) = E$.

2. We recall that
$$x^{ab} - 1 = (x^a - 1)(x^{ab-a} + x^{ab-2a} + \cdots + x^a + 1).$$
Thus if $n = mk$, we have
$$p^n - 1 = p^{mk} - 1 = (p^m - 1)(\cdots)$$
and so
$$x^{p^n} - x = x(x^{p^n-1} - 1) = x(x^{p^m-1} - 1)g(x) = (x^{p^m} - 1)g(x)$$
for some $g(x) \in \mathbb{Z}/p\mathbb{Z}[x]$. Since $x^{p^n} - x$ splits over F, so does $x^{p^m} - x$. Let $K = \{u \in F : u^{p^m} - u = 0\}$. Then $|K| = p^m$ since the roots of $x^{p^m} - x$ are distinct. Also, by (1) K is a field. Note that if $\tilde{K} \subseteq F$ is any subfield with $|\tilde{K}| = p^m$, then $\tilde{K} \subseteq K$ since all elements in $\tilde{K}$ satisfy $u^{p^m} = u$. It follows that $\tilde{K} = K$.

□

Corollary 5.7.1 (E. H. Moore)**:** Let p be a prime and $n \in \mathbb{N}$. Then any two finite fields of order p^n are isomorphic. We will denote such a field by $\mathbb{F}_{p^n}$.

Proof. This is a direct consequence of Theorem 5.7 and Corollary 4.4.1.

□

Corollary 5.7.2: Let F be a finite field with $\mathrm{ch}(F) = p$.

1. $F = F^p = \{x^p : x \in F\}$.
2. Every irreducible $r(x) \in F[x]$ is separable.

Proof.

1. Every finite field $F = \mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$ for some prime p and $n \in \mathbb{N}$. Then for every $a \in F$,
$$a = a^{p^n} = (a^{p^n-1})^p$$
since $a^{p^n-1} \in F$, $F = F^p$.

2. Let $r(x) \in F[x]$ be irreducible. Then
$$\gcd(r, r') = \begin{cases} 1 & \text{if } r' \neq 0 \\ r & \text{if } r' = 0 \end{cases}$$
Suppose $r(x)$ is not separable. Then by Corollary 5.4.1, $\gcd(r, r') \neq 1$. Thus $r'(x) = 0$. Since $\mathrm{ch}(F) = p$, from Theorem 5.3, $r'(x) = 0$ implies that
$$r(x) = a_0 + a_1 x^p + \cdots + a_m x^{mp}.$$
Since $F = F^p$, we can write $a_i = b_i^p$ with $b_i \in F$. Thus
$$r(x) = b_0^p + b_1^p x^p + \cdots + b_m^p x^{mp} = (b_0 + b_1 x + \cdots + b_m x^m)^p$$
a contradiction since $r(x)$ is irreducible. Thus $r(x)$ is separable.

□

Example 5.2: Let $\mathrm{ch}(F) = p$ and consider $f(x) = x^p - a$. Since $f'(x) = px^{p-1} = 0$ we have $\gcd(f, f') \neq 1$ and so by Corollary 5.4.1 $f(x)$ is not separable. Define $F^p = \{b^p : b \in F\}$ which is a subfield of F. The behaviour of $f(x)$ will depend on if $a \in F^p$.

1. If $a \in F^p$, say $a = b^p$ for some $b \in F$, then $f(x) = x^p - b^p = (x - b)^p \in F[x]$, which is not separable. Note that $f(x)$ is reducible in $F[x]$.

2. Suppose $a \notin F^p$. Let E/F be an extension where $x^p - a$ has a root, say $\beta \in E$. Hence we have $\beta^p - a = 0$. Note that since $a = \beta^p \notin F^p$, $\beta \notin F$ but we still have
$$f(x) = x^p - a = x^p - \beta^p = (x - \beta)^p$$
which is not separable.

Example 5.3: One can show that $f(x) = x^p - a$ is irreducible in $F[x]$.

Proof. Suppose we can write $x^p - a = g(x)h(x)$ where $g(x), h(x) \in F[x]$ are monic polynomials. We have seen in Example 5.2 that $x^p - a = (x - \beta)^p$. Thus $g(x) = (x - \beta)^r$ and $h(x) = (x - \beta)^s$ for some $r, s \in \mathbb{N} \cup \{0\}$ with $r + s = p$. Write
$$g(x) = (x - \beta)^r = x^r - r\beta x^{r-1} + \cdots + r\beta^{r-1}x + \beta^r.$$
Then, in-particular, $r\beta \in F$. Since $\beta \notin F$, as an element of F we have $r = 0$. Thus as an integer we have $r = 0$ or $r = p$. It follows that either $g(x) = 1$ or $h(x) = 1$ in $F[x]$. Thus $f(x)$ is irreducible in $F[x]$.

□

6 Solvable Groups and Automorphism Groups

All the way back in Chapter 1 we said that Galois theory is all about the interactions between field theory and finite group theory. At this point we've established the prerequisite field theory, so now it's time for the group theory.

6.1 Solvable Groups

Definition 6.1 (Solvable Groups)**:** A group G is solvable if there exists a tower

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_m = \{1\}$$

with $G_{i+1} \lhd G_i$ and G_i/G_{i+1} abelian for all $0 \leq i \leq m-1$.

Remark: G_{i+1} is not necessarily a normal subgroup of G. However, if G_{i+1} is a normal subgroup of G, we get $G_{i+1} \lhd G_i$ for free.

Example 6.1: Consider the symmetric group S_4. Let A_4 be the alternating group of S_4 and $K_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ be the Klein 4-group. Note that A_4 and K_4 are normal subgroups of S_4. We have

$$S_4 \supseteq A_4 \supseteq K_4 \supseteq \{1\}.$$

Since $S_4/A_4 \cong \mathbb{Z}/2\mathbb{Z}$ and $A_4/K_4 \cong \mathbb{Z}/3\mathbb{Z}$, S_4 is solvable.

We now recall the second and third isomorphism theorems for groups from PMATH347.

Theorem 6.1 (The Second Isomorphism Theorem)**:** Let H and K be subgroups of a group G with $K \lhd G$. Then HK is a subgroup of G, $K \lhd HK$, $H \cap K \lhd H$ and

$$\frac{HK}{K} \cong \frac{H}{H \cap K}.$$

Theorem 6.2 (Third Isomorphism Theorem)**:** Let $K \subseteq H \subseteq G$ be groups with $K \lhd G$ and $H \lhd G$. Then $H/K \lhd G/K$ and

$$\frac{G/K}{H/K} \cong \frac{G}{H}.$$

The proofs of these theorems were given in PMATH347 and will be omitted.

Theorem 6.3: Let G ba solvable group.

1. If H is a subgroup of G, then H is solvable.
2. Let N be a normal subgroup of G. Then the quotient group G/N is solvable.

Proof. Since G is a solvable group, there exists a tower

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_m = \{1\}$$

with $G_{i+1} \lhd G_i$ and G_i/G_{i+1} abelian for all $0 \leq i \leq m-1$.

1. Define $H_i = H \cap G_i$. Since $G_{i+1} \lhd G_i$ the tower
$$H = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_m = \{1\}$$
satisfies $H_{i+1} \lhd H_i$. Note that both H_i and G_{i+1} are subgroups of G_i and
$$H_{i+1} = H \cap G_{i+1} = H_i \cap G_{i+1}.$$
Applying the second isomorphism theorem to G_i, we have:
$$\frac{H_i}{H_{i+1}} = \frac{H_i}{H_i \cap G_{i+1}} \cong \frac{H_i G_{i+1}}{G_{i+1}} \subseteq \frac{G_i}{G_{i+1}}$$
Since G_i/G_{i+1} is abelian, we find that H_i/H_{i+1} is also abelian and so it follows that H is solvable.

2. Consider the towers
$$G = G_0 N \supseteq G_1 N \subseteq \cdots \supseteq G_m N = N$$
and
$$G/N = G_0 N/N \supseteq G_1 N/N \supseteq \cdots \supseteq G_m N/N = \{1\}.$$
Since $G_{i+1} \lhd G_i$ and $N \lhd G$, we have $G_{i+1}N \lhd G_i N$, which implies that $G_{i+1}N/N \lhd G_i N/N$. By the third isomorphism theorem,
$$\frac{G_i N/N}{G_{i+1}N/N} \cong \frac{G_i N}{G_{i+1}N}.$$
By the second isomorphism theorem,
$$\frac{G_i N}{G_{i+1}N} \cong \frac{G_i}{G_i \cap G_{i+1}N}.$$
Consider the natural quotient map $G_i \to G_i/(G_i \cap G_{i+1}N)$ which is a surjective homomorphism. Since $G_{i+1} \subseteq (G_i \cap G_{i+1}N)$, it induces a surjective homomorphism $G_i/G_{i+1} \to G_i/(G_i \cap G_{i+1}N)$. Since G_i/G_{i+1} is abelian, so is $G_i/(G_i \cap G_{i+1}N)$. Thus $\frac{G_i N/N}{G_{i+1}N/N}$ is abelian. It follows that G/N is solvable.

□

Theorem 6.4: Let N be a normal subgroup of G. If both N and G/N are solvable, then G is solvable. In particular, a direct product of finitely many solvable groups is solvable.

Proof. Since N is solvable, we have a tower
$$N = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_m = \{1\}$$
with $N_{i+1} \lhd N_i$ and N_i/N_{i+1} abelian for all i.

For any subgroup $H \subseteq G$ with $N \subseteq H$, we define $\overline{H} = H/N$. Since G/N is solvable, we have a tower
$$G/N = \overline{G} = \overline{G}_0 \supseteq \overline{G}_1 \supseteq \cdots \supseteq \overline{G}_r = N/N = \{1\}$$
with $\overline{G}_{i+1} \lhd \overline{G}_i$ and $\overline{G}_i/\overline{G}_{i+1}$ is abelian. Let $\mathrm{Sub}_N(G)$ denote the set of subgroups G which contain N. Consider the map
$$\sigma : \mathrm{Sub}_N(G) \to \mathrm{Sub}_N(G/N), \qquad H \mapsto H/N.$$
For all $i = 0, 1, \cdots, r$, define $G_i = \sigma^{-1}(\overline{G}_i)$. Since $N \lhd G$ and $\overline{G}_{i+1} \lhd \overline{G}_i$, we have $G_{i+1} \lhd G_i$. Also, by the third isomorphism theorem, $G_i/G_{i+1} \cong \overline{G}_i/\overline{G}_{i+1}$. It follows that
$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_r = N = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_m = \{1\}$$
with $G_{i+1} \lhd G_i$, $N_{i+1} \lhd N_i$, and G_i/G_{i+1}, N_i/N_{i+1} are all abelian. Thus G is solvable.

□

Example 6.2: S_4 contains subgroups isomorphic to S_3 and S_2. Since S_4 is solvable, by Theorem 6.3, S_3 and S_2 are solvable.

Definition 6.2 (Simple Groups)**:** A group G is simple if it is not trivial and has no normal subgroups except for $\{1\}$ and G.

Example 6.3: One can show that the alternating group A_5 is simple (see Bonus 4). Since $A_5 \supseteq \{1\}$ is the only tower and $A_5/\{1\}$ is not abelian, A_5 is not solvable. Thus by Theorem 6.3, S_5 is also not solvable. Moreover, since all S_n with $n \geq 5$ contain a subgroup isomorphic to S_5, which is not solvable, by Theorem 6.3, S_n is not solvable for all $n \geq 5$.

Corollary 6.4.1: Let G be a finite solvable group. Then there exists a tower

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_m = \{1\}$$

with $G_{i+1} \lhd G_i$ and G_i/G_{i+1} a cyclic group.

Proof. If G is solvable, there exists a tower

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_m = \{1\}$$

with $G_{i+1} \lhd G_i$ and G_i/G_{i+1} abelian. Consider $A = G_i/G_{i+1}$, a finite abelian group. We have

$$A \cong C_{k_1} \times C_{k_2} \times \cdots \times C_{k_r}$$

where C_k is a cyclic group of order k. Since each G_i/G_{i+1} can be rewritten as a product of cyclic groups, the result follows.

□

Remark: By the Chinese Remainder Theorem, we can further require the quotient G_i/G_{i+1} to be a cyclic group of prime order.

6.2 Automorphism Groups

Definition 6.3 (Automorphism Groups)**:** Let E/F be a field extension. If ψ is an automorphism of E, (i.e. $\psi : E \to E$ is an isomorphism) such that $\psi(1_F) = 1_F$, we say that ψ is an F-automorphism of E. By map compositions, the set

$$\{\psi : E \to E : \psi \text{ is an } F\text{-automorphism}\}$$

is a group which we call the automorphism group of E/F, denoted by $\mathrm{Aut}_F(E)$.

Lemma 6.5: Let E/F be a field extension, $f(x) \in F[x]$ and $\psi \in \mathrm{Aut}_F(E)$. If $\alpha \in E$ is a root of $f(x)$, then $\psi(\alpha)$ is also a root of $f(x)$.

Proof. Write $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$. We have:

$$\begin{aligned} f(\psi(\alpha)) &= a_0 + a_1\psi(\alpha) + \cdots + a_n(\psi(\alpha))^n \\ &= \psi(a_0) + \psi(a_1)\psi(\alpha) + \cdots + \psi(a_n)(\psi(\alpha)^n) \\ &= \psi(f(\alpha)) = \psi(0) = 0 \end{aligned}$$

Thus $\psi(\alpha)$ is a root of $f(x)$.

□

Lemma 6.6: Let $E = F(\alpha_1, \alpha_2, \cdots, \alpha_n)$ be a field extension of F. For $\psi_1, \psi_2 \in \mathrm{Aut}_F(E)$, if $\psi_1(\alpha_i) = \psi_2(\alpha_i)$ for all α_i then $\psi_1 = \psi_2$.

Proof. Note that for $\alpha \in E$, α is of the form

$$\alpha = \frac{f(\alpha_1, \cdots, \alpha_n)}{g(\alpha_1, \cdots, \alpha_n)}$$

where $f(x_1, \cdots, x_n), g(x_1, \cdots, x_n) \in F[x_1, \cdots, x_n]$ with $g \neq 0$. The result follows. □

Corollary 6.6.1: If E/F is a finite extension, then $\mathrm{Aut}_F(E)$ is a finite group.

Proof. Since E/F is a finite extension, by Theorem 3.6, $E = F(\alpha_1, \cdots, \alpha_n)$ where α_i $(1 \leq i \leq n)$ are algebraic over F. For $\psi \in \mathrm{Aut}_F(E)$, by Lemma 6.5, $\psi(\alpha_i)$ is a root of the minimal polynomial of α_i. Thus it has only finitely many choices. By Lemma 6.6, since $\psi \in \mathrm{Aut}_F(E)$ is completely determined by our choices of $\psi(\alpha_i)$ for each i, there are only finitely many choices for ψ and so $\mathrm{Aut}_F(E)$ is finite. □

Remark: The converse of the above corollary is false. For example, $\mathbb{R}/\mathbb{Q}$ is an infinite extension, but $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{R}) = \{1\}$. Indeed, one can show that $\mathrm{Aut}(\mathbb{R}) = \{1\}$ as $\psi \in \mathrm{Aut}(\mathbb{R})$ with $\psi(1) = 1$ will imply $\psi\restriction_{\mathbb{Q}}$ is the identity map (for more details see Assignment 6 question 3).

6.3 Automorphism Groups of Splitting Fields

Definition 6.4 (Automorphism Groups of Polynomials)**:** Let F be a field and $f(x) \in F[x]$. The automorphism group of $f(x)$ over F is defined to be $\mathrm{Aut}_F(E)$ where E is the splitting field of $f(x)$ over F.

Theorem 6.7: Let E/F be the splitting field of a non-zero polynomial $f(x) \in F[x]$. We have $|\mathrm{Aut}_F(E)| \leq [E : F]$ and equality holds if and only if every irreducible factor of $f(x)$ is separable.

Proof. This is a direct consequence of Theorem 4.4 and Assignment 4 question 2. □

Theorem 6.8: If $f(x) \in F[x]$ has n distinct roots in the splitting field E, then $\mathrm{Aut}_F(E)$ is isomorphic to a subgroup of S_n. In-particular, $|\mathrm{Aut}_F(E)|$ divides $n!$.

Proof. Let $X = \{\alpha_1, \cdots, \alpha_n\}$ be distinct roots of $f(x)$ in E. By Lemma 6.5, if $\psi \in \mathrm{Aut}_F(E)$, then $\psi(X) = X$. Let $\psi\restriction_X$ be the restriction of ψ in X and S_X be the permutation group of X. The map

$$\mathrm{Aut}_F(E) \to S_X \cong S_n, \qquad \psi \mapsto \psi\restriction_X$$

is a group homomorphism. Moreover, by Lemma 6.6 it is injective. Thus $\mathrm{Aut}_F(E)$ is isomorphic to a subgroup of S_n. □

Example 6.4: Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ and $E/\mathbb{Q}$ be the splitting field of $f(x)$. Then $E = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ and

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

Since $\mathrm{ch}(\mathbb{Q}) = 0$, $f(x)$ is separable. By Theorem 6.7, $|\operatorname{Aut}_{\mathbb{Q}}(E)| = [E : \mathbb{Q}] = 6$. Also, since $f(x)$ has three distinct roots in E, by Theorem 6.8, $\operatorname{Aut}_{\mathbb{Q}}(E)$ is a subgroup of S_3. Since the only subgroup of S_3 of order 6 is S_3 itself, we conclude that $\operatorname{Aut}_{\mathbb{Q}}(E) \cong S_3$.

Example 6.5: Let F be a field with $\mathrm{ch}(F) = p$ and $F^p \neq F$. Let $f(x) = x^p - a$ with $a \in F \setminus F^p$. Let E/F be the splitting field of $f(x)$. We have seen in Chapter 5 that $f(x)$ is irreducible in $F[x]$ and $f(x) = (x - \beta)^p$ for some $\beta \in E \setminus F$. Thus $E = F(\beta)$, and since β can only be mapped to β, $\operatorname{Aut}_F(E)$ is the trivial group. Note that in this case $|\operatorname{Aut}_F(E)| = 1$ while $[E : F] = \deg(f) = p$.

Definition 6.5 (Fixed Fields of Automorphisms)**:** Let E/F be a field extension and $\psi \in \operatorname{Aut}_F(E)$. Define

$$E^{\psi} = \{a \in E : \psi(a) = a\}$$

to be the set of all elements of E which are fixed points of ψ. Note that E^{ψ} is a subfield of E containing F. We call E^{ψ} the fixed field of ψ.

Definition 6.6 (Fixed Fields of Groups)**:** Let E/F be a field extension and G be a subgroup of $\operatorname{Aut}_F(E)$. The fixed field of G is defined by

$$E^G = \bigcap_{\psi \in G} E^{\psi} = \{a \in E : \psi(a) = a \text{ for all } \psi \in G\}.$$

Theorem 6.9: Let $f(x) \in F[x]$ be a polynomial in which every irreducible factor is separable. Let E/F be the splitting field of $f(x)$. If $G = \operatorname{Aut}_F(E)$, then $E^G = F$.

Proof. Set $L = E^G$. Since $F \subseteq E^{\psi}$ for all $\psi \in \operatorname{Aut}_F(E)$, $F \subseteq L$ and we have $\operatorname{Aut}_L(E) \subseteq \operatorname{Aut}_F(E)$. On the other hand, if $\psi \in \operatorname{Aut}_F(E)$ then by the definition of L for all $a \in L$ we have $\psi(a) = a$. This implies that $\psi \in \operatorname{Aut}_L(E)$ and so

$$\operatorname{Aut}_L(E) = \operatorname{Aut}_F(E).$$

Note that since $f(x)$ is separable over F and splits over E, $f(x)$ is also separable over L and has E as its splitting field over L and has E as its splitting field over L. Thus by Theorem 6.7 we have

$$|\operatorname{Aut}_F(E)| = [E : F] \text{ and } |\operatorname{Aut}_L(E)| = [E : L].$$

It follows that $[E : F] = [E : L]$. Since $[E : F] = [E : L][L : F]$ we have $[L : F] = 1$. Thus $L = F$ (i.e. $E^G = F$).

□

7 Separable Extensions and Normal Extensions

7.1 Separable Extensions

Definition 7.1: Let E/F be an algebraic field extension. For $\alpha \in E$, let $p(x) \in F[x]$ be the minimal polynomial of α. We say α is separable over F if its minimal polynomial $p(x)$ is separable. If α is separable for all $\alpha \in E$, then we say that the extension E is separable.

Example 7.1: If $\mathrm{ch}(F) = 0$, by Corollary 5.4.2 every irreducible polynomial $p(x) \in F[x]$ is separable. Thus if $\mathrm{ch}(F) = 0$ any algebraic extension E/F is separable.

Theorem 7.1: Let E/F be the splitting field of $f(x) \in F[x]$. If every irreducible factor of $f(x)$ is separable, then E/F is separable.

Proof. Let $\alpha \in E$ and $p(x) \in F[x]$ be the minimal polynomial of α. Let $\{\alpha = \alpha_1, \alpha_2, \cdots, \alpha_n\}$ be all of the distinct roots of $p(x)$ in E. Define

$$\tilde{p}(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

we aim to show that $\tilde{p}(x) = p(x)$.

Claim 7.1.1: $\tilde{p}(x) \in F[x]$

Proof. Let $G = \mathrm{Aut}_F(E)$ and $\psi \in G$. Since ψ is an automorphism, $\psi(\alpha_i) \neq \psi(\alpha_j)$ if $i \neq j$. By Lemma 6.5, ψ permutes $\alpha_1, \cdots, \alpha_n$. Thus by extending $\psi : E \to E$ uniquely to $\psi : E[x] \to E[x]$ with $x \mapsto x$, we have

$$\psi(\tilde{p}(x)) = (x - \psi(\alpha_1))(x - \psi(\alpha_2)) \cdots (x - \psi(\alpha_n)) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) = \tilde{p}(x).$$

It follows that $\tilde{p}(x) \in E^{\psi}[x]$ for all $\psi \in G$. Thus $\tilde{p}(x) \in E^{G}[x]$. Since E/F is the splitting field of $f(x)$ whose irreducible factors are separable, by Theorem 6.9, $\tilde{p}(x) \in F[x]$.

□

Thus we have $\tilde{p}(x) \in F[x]$ with $\tilde{p}(\alpha) = 0$. Since $p(x)$ is the minimal polynomial of α over F, we have $p(x) | \tilde{p}(x)$. Also, since $\alpha_1, \cdots, \alpha_n$ are all distinct roots of $p(x)$, we have $\tilde{p}(x) | p(x)$. Since both $p(x)$ and $\tilde{p}(x)$ are monic, we have $\tilde{p}(x) = p(x)$. It follows that $p(x)$ is separable.

□

Corollary 7.1.2: Let E/F be a finite extension and $E = F(\alpha_1, \cdots, \alpha_n)$. If each α_i is separable over F then E/F is separable.

Proof. Let $p_i(x) \in F[x]$ be the minimal polynomial of α_i $(1 \leq i \leq n)$. Let $f(x) = p_1(x) \cdots p_n(x)$ with each $p_i(x)$ being separable. Let L be the splitting field of $f(x)$ over F. By Theorem 7.1 L/F is separable. Since $E = F(\alpha_1, \cdots, \alpha_n)$ is a subfield of L, E is also separable.

□

Corollary 7.1.3: Let E/F be an algebraic extension and L be the set of all $\alpha \in E$ which are separable over F. Then L is a field.

Proof. Let $\alpha, \beta \in L$. Then $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ (assuming $\beta \neq 0$) are all elements of $F(\alpha, \beta)$. By Corollary 7.1.2, $F(\alpha, \beta)$ is separable, and hence it is contained in L. Thus these composite elements are also contained in L.

□

Definition 7.2 (Primitive Elements)**:** If $E = F(\gamma)$ is a simple extension, we say γ is a primitive element of E/F

Recall from Theorem 3.5 that any finite extension is a composition of simple extensions.

Theorem 7.2 (Primitive Element Theorem)**:** If E/F is a finite separable extension, then $E = F(\gamma)$ for some $\gamma \in E$. In-particular, by Corollary 5.4.2 if $\mathrm{ch}(F) = 0$, then any finite extension E/F is a simple extension.

Proof. We have seen in Corollary 5.6.1 that a finite extension of a finite field is always simple. Thus without loss of generality, we assume that F is an infinite field. Since $E = F(\alpha_1, \cdots, \alpha_n)$ for some $\alpha_1, \cdots, \alpha_n \in E$, it suffices to consider the case when $E = F(\alpha, \beta)$ and the general case can be done by induction. Let $E = F(\alpha, \beta)$ with $\alpha, \beta \notin F$.

Claim 7.2.1: There exists $\lambda \in F, \gamma \in E$ such that $\gamma = \alpha + \lambda\beta$ and $\beta \in F(\gamma)$.

Proof. Let $a(x)$ and $b(x)$ be the minimal polynomials of α and β over F respectively. Since $\beta \notin F$, $\deg(b) > 1$. Thus since E/F is separable there exists a root $\tilde{\beta}$ of $b(x)$ such that $\tilde{\beta} \neq \beta$. Choose $\lambda \in F$ such that $\lambda \neq \frac{\tilde{\alpha}-\alpha}{\beta-\tilde{\beta}}$ for all roots $\tilde{\alpha}$ of $a(x)$ and all roots $\tilde{\beta}$ of $b(x)$ with $\tilde{\beta} \neq \beta$ in some splitting field of $a(x)b(x)$ over F. The choice is possible since there are infinitely many elements in F, but only finitely many choices of $\tilde{\alpha}$ and $\tilde{\beta}$.

Now let $\gamma = \alpha + \lambda\beta$ and consider the polynomial $h(x) = a(\gamma - \lambda x) \in F(\gamma)[x]$. Notice that $h(\beta) = a(\gamma - \lambda\beta) = a(\alpha) = 0$. However, for any $\tilde{\beta} \neq \beta$, since

$$\gamma - \lambda\beta = \alpha + \lambda(\beta - \tilde{\beta}) \neq \tilde{\alpha}$$

we have $h(\tilde{\beta}) = a(\gamma - \lambda\tilde{\beta}) \neq 0$. Since the minimal polynomial of β in $F(\gamma)$ must divide both $h(x)$ and $b(x)$, and the only common root of these polynomials is β, we conclude the minimal polynomial of β in $F(\gamma)$ is $x - \beta$ and so $\beta \in F(\gamma)$.

□

It follows from this claim that $\alpha = \gamma - \lambda\beta \in F(\gamma)$, and so we have $F(\alpha, \beta) \subseteq F(\gamma)$. Also, since $\gamma = \alpha + \lambda\beta$, $F(\gamma) \subseteq F(\alpha, \beta)$. Thus $E = F(\alpha, \beta) = F(\gamma)$.

□

7.2 Normal Extensions

Definition 7.3 (Normal Extensions)**:** Let E/F be an algebraic extension. We say E/F is a normal extension if for any irreducible polynomial $p(x) \in F[x]$ either $p(x)$ has no root in E or $p(x)$ has all roots in E. In other words, if $p(x)$ has a root in E, $p(x)$ splits over E.

Example 7.2: Let $\alpha \in \mathbb{R}$ with $\alpha^4 = 5$. Since the roots of $x^4 - 5$ are $\pm\alpha$ and $\pm i\alpha$ and $\mathbb{Q}(\alpha)$ is real, $\mathbb{Q}(\alpha)/\mathbb{Q}$ is not normal.

So instead let's try $\beta = (1 + i)\alpha$. Notice that $\beta^2 = 2i\alpha^2, \beta^4 = -4\alpha^4 = -20$. Since $\pm\beta, \pm i\beta$ all satisfy $x^4 = -20$, to show that $\mathbb{Q}(\beta)$ is not normal it suffices to show that $i \notin \mathbb{Q}(\beta)$. Since the minimal polynomial of β over $\mathbb{Q}$ is $p(x) = x^4 + 20$, we have $[\mathbb{Q}(\beta) : \mathbb{Q}] = 4$. Also, the roots of $p(x)$ are $\pm\beta$, $\pm i\beta$. Since the minimal polynomial of α is $x^4 - 5$, we have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Note that if $\alpha \in \mathbb{Q}(\beta)$, since $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4 = [\mathbb{Q}(\beta) : \mathbb{Q}]$, it implies that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$, which is impossible since $\beta = \alpha + i\alpha \notin \mathbb{Q}(\alpha)$. Thus $\alpha \notin \mathbb{Q}(\beta)$, which implies $i \notin \mathbb{Q}(\beta)$. It follows that the factorization of $p(x)$ over $\mathbb{Q}(\beta)$ is

$$(x - \beta)(x + \beta)(x^2 + \beta^2).$$

Since $p(x)$ does not split over $\mathbb{Q}(\beta)$, $\mathbb{Q}(\beta)/\mathbb{Q}$ is not normal.

Theorem 7.3: A finite extension E/F is normal if and only if it is the splitting field of some $f(x) \in F[x]$.

Proof.

$\Longrightarrow$ Suppose that E/F is normal. Write $E = F(\alpha_1, \cdots, \alpha_n)$. Let $p_i(x) \in F[x]$ be the minimal polynomial of α_i. Set

$$f(x) = p_1(x)p_2(x)\cdots p_n(x).$$

Since E/F is normal, each $p_i(x)$ splits over E. Let $\alpha_i = \alpha_{i,1}, \alpha_{i,2}, \cdots, \alpha_{i,r_i}$ be the roots of $p_i(x)$ in E. Then

$$E = F(\alpha_{1,1}, \cdots, \alpha_{1,r_1}, \alpha_{2,1}, \cdots, \alpha_{2,r_2}, \cdots, \alpha_{n,1}, \cdots, \alpha_{n,r_n})$$

is the splitting field of $f(x)$ over F.

$\Longleftarrow$ Let E/F be the splitting field of $f(x) \in F[x]$. Let $p(x) \in F[x]$ be irreducible and have a root $\alpha \in E$. Let K/E be the splitting field of $p(x)$ over E. Write $p(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ where $0 \neq c \in F$, $\alpha = \alpha_1 \in E$, $\alpha_2, \cdots, \alpha_n \in K = E(\alpha_1, \cdots, \alpha_n)$.

Since $F(\alpha) \cong F[x]/\langle p(x)\rangle \cong F(\alpha_2)$, we have the F-isomorphism $\theta : F(\alpha) \to F(\alpha_2)$, $\theta(\alpha) = \alpha_2$. Note that $p(x)f(x) \in F[x] \subseteq F(\alpha)[x]$ and $p(x)f(x) \in F(\alpha_2)[x]$. Thus we can view K as the splitting field of $p(x)f(x)$ over $F(\alpha)$ and $F(\alpha_2)$ respectively. Thus by Theorem 4.4, there exists an isomorphism $\psi : K \to K$ which extends θ. In particular $\psi \in \mathrm{Aut}_F(K)$.

Since $\psi \in \mathrm{Aut}_F(K)$, ψ permutes the roots of $f(x)$. Since E is generated over F by the roots of $f(x)$, by Lemma 6.5, we have $\psi(E) = E$. It follows that for $\alpha \in E$, $\alpha_2 = \psi(\alpha) \in E$. Similarly, we can prove that $\alpha_i \in E$ for all $1 \leq i \leq n$. Thus $K = E$ and $p(x)$ splits over E. It follows that E/F is normal.

□

Example 7.3: Every quadratic extension is normal.

Proof. Let E/F be the field extension with $[E : F] = 2$. For $\alpha \in E \setminus F$, we have $E = F(\alpha)$. Let $p(x) = x^2 + bx + c$ be the minimal polynomial of α over F. If β is another root of $p(x)$ then

$$p(x) = (x-\alpha)(x-\beta) = x^2 - (\alpha+\beta)x + \alpha\beta.$$

Thus $\beta = -b - \alpha$ is the other root of $p(x)$ and $\beta \in E$. Hence E/F is normal. □

Example 7.4: The extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal since the irreducible polynomial $p(x) = x^4 - 2$ has a root in $\mathbb{Q}(\sqrt[4]{2})$, but $p(x)$ does not split over $\mathbb{Q}(\sqrt[4]{2})$.

Note that the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is made up of the two quadratic extensions $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, which are normal. Thus if E/K and K/F are normal extensions, then E/F is not always normal.

Proposition 7.4: If E/F is a normal extension and K is an intermediate field, then E/K is normal.

Proof. Let $p(x) \in K[x]$ be irreducible and have a root $\alpha \in E$. Let $f(x) \in F[x] \subseteq K[x]$ be the minimal polynomial of α over F. Then $p(x)|f(x)$. Since E/F is normal and $f(x)$ splits over E, so does $p(x)$. Thus E/K is a normal extension. □

Remark: In Proposition 7.4, K/F is not always normal. For example, let $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[4]{2})$ and $E = \mathbb{Q}(\sqrt[4]{2}, i)$. Then E/F is the splitting field of $x^4 - 2$ and hence normal. Also, E/K is normal but $K/\mathbb{Q}$ is not normal.

Proposition 7.5: Let E/F be a finite normal extension and $\alpha, \beta \in E$. The following are all equivalent:

1. There exists $\psi \in \mathrm{Aut}_F(E)$ such that $\psi(\alpha) = \beta$.
2. The minimal polynomials of α and β over F are the same.

Proof.

- $(1 \implies 2)$**:** Let $p(x)$ be the minimal polynomial of α over F and $\psi \in \mathrm{Aut}_F(E)$ with $\psi(\alpha) = \beta$. By Lemma 6.5, β is also a root of $p(x)$. Since $p(x)$ is monic and irreducible, it is the minimal polynomial of β over F. Hence α and β have the same minimal polynomials.
- $(2 \implies 1)$**:** Suppose that the minimal polynomial of α and β are the same, say $p(x)$. Since $F(\alpha) \cong F[x]/\langle p(x)\rangle \cong F(\beta)$, we have the F-isomorphism $\theta : F(\alpha) \to F(\beta)$ with $\theta(\alpha) = \beta$. Since E/F is a finite normal extension, by Theorem 7.3, E is the splitting field of some $f(x) \in F[x]$ over F. We can also view E as the splitting field of $f(x)$ over $F(\alpha)$ and $F(\beta)$ respectively. Thus by Theorem 4.4, there exists an isomorphism $\psi : E \to E$ which extends θ. It follows that $\psi \in \mathrm{Aut}_F(E)$ and $\psi(\alpha) = \beta$.

□

Notation 7.4: If $\alpha, \beta \in E$ satisfy either of the equivalent conditions in Proposition 7.5 we say that they are conjugate over F.

Example 7.5: Let complex numbers $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta_3$, $\sqrt[3]{2}\zeta^2$ are all conjugates over $\mathbb{Q}$ since they are roots of the irreducible polynomial $x^3 - 2 \in \mathbb{Q}[x]$.

Definition 7.5 (Normal Closures)**:** A normal closure of a finite extension E/F is a finite normal extension N/F satisfying the following properties:

1. E is a subfield of N.
2. Let L be an intermediate field of N/E. If L is normal over F, then $L = N$.

Example 7.6: Let normal closure of $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$.

Theorem 7.6: Every finite extension E/F has a normal closure N/F which is unique up to E-isomorphism.

Proof. Write $E = F(\alpha_1, \cdots, \alpha_n)$.

- **Existence:** Let $p_i(x)$ be the minimal polynomial of α_i over F. Write $f(x) = p_1(x) \cdots p_n(x)$ and let N/E be the splitting field of $f(x)$ over E. Since $\alpha_1, \cdots, \alpha_n$ are roots of $f(x)$, N is also the splitting field of $f(x)$ over F. By Theorem 7.3, N is normal over F. Let $L \subseteq N$ be a subfield containing E. Then L contains all α_i. If L is normal over F, each $p_i(x)$ splits over L. Thus $N \subseteq L$ and so $L = N$.

- **Uniqueness:** Let N/E be the splitting field of $f(x)$ over E defied as above. Let N_1/F be another normal closure of E/F. Since N_1 is normal over F and contains all α_i, N_1 must contain a splitting field $\tilde{N}$ of $f(x)$ over F. By Corollary 4.4.1, N and $\tilde{N}$ are E-isomorphic since $\tilde{N}$ is a splitting field of $f(x)$ over F.

□

8 Galois Correspondence

8.1 Galois Extensions

We recall that for finite extensions E/F we have proved the following two results:

1. E is the splitting field of some $f(x) \in F[x] \iff E/F$ is normal (Theorem 7.3).
2. If E is the splitting field of some polynomial $f(x) \in F[x]$ whose irreducible factors are all separable $\implies E/F$ is separable (Theorem 7.1).

We note that if E is the splitting field of some $f(x) \in F[x]$ then by (1) the backwards direction of (2) is also true. This motivates the following definition:

Definition 8.1 (Galois Extensions and Groups)**:** An algebraic extension E/F is a Galois extension if it is normal and separable. If E/F is a Galois extension then the Galois group of E/F (denoted $\mathrm{Gal}_F(E)$) is defined to be the automorphism group $\mathrm{Aut}_F(E)$.

Remark:

1. By Theorems 7.1 and 7.3 a finite extension E/F is a Galois extension if and only if it is the splitting field of a polynomial $f(x) \in F[x]$ whose irreducible factors are all separable.
2. If E/F is a finite Galois extension, by Theorem 6.7 $|\mathrm{Gal}_F(E)| = [E : F]$.
3. If E/F is the splitting field of a separable polynomial $f(x) \in F[x]$ with $\deg(f) = n$, then by Theorem 6.8, $\mathrm{Gal}_F(E)$ is a subgroup of S_n.

Example 8.1: Let E be the splitting field of $(x^2-2)(x^2-3)(x^2-5) \in \mathbb{Q}[x]$. Then $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ and $[E : \mathbb{Q}] = 8$ (see piazza exercise).

For $\psi \in \mathrm{Gal}_{\mathbb{Q}}(E)$ we have $\psi(\sqrt{2}) \in \{\pm\sqrt{2}\}, \psi(\sqrt{3}) \in \{\pm\sqrt{3}\}, \psi(\sqrt{5}) \in \{\pm\sqrt{5}\}$. Since $|\mathrm{Gal}_{\mathbb{Q}}(E)| = [E : \mathbb{Q}] = 8$, we have

$$\mathrm{Gal}_{\mathbb{Q}}(E) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Definition 8.2 (Elementary Symmetric Polynomials)**:** Let $t_1, t_2, \cdots, t_n$ be variables. We define the elementary symmetric polynomials in $t_1, \cdots, t_n$ as:

$$\begin{aligned} s_1 &= t_1 + t_2 + \cdots + t_n \\ s_2 &= \sum_{1 \le i < j \le n} t_i t_j \\ s_3 &= \sum_{1 \le i < j < k \le n} t_i t_j t_k \\ &\vdots \\ s_n &= t_1 t_2 \cdots t_n \end{aligned}$$

Remark: It follows from this definition that given $f(x) = (x - t_1)(x - t_2)\cdots(x - t_n)$ we have

$$f(x) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \cdots + (-1)^n s_n.$$

Theorem 8.1 (E. Artin)**:** Let E be a field and G a finite subgroup of $\mathrm{Aut}(E)$, the automorphism group of E. Let $E^G = \{\alpha \in E : \psi(\alpha) = \alpha, \forall \psi \in G\}$. Then E/E^G is a finite Galois extension and $\mathrm{Gal}_{E^G}(E) = G$. In-particular, $[E : E^G] = |G|$.

Proof. Let $n = |G|$ and $F = E^G$. For $\alpha \in E$, consider the G-orbit of α:

$$\{\psi(\alpha) : \psi \in G\} = \{\alpha = \alpha_1, \alpha_2, \cdots, \alpha_m\}$$

Note that $m \leq n$ since there may exist $\psi_1, \psi_2 \in G$ with $\psi_1 \neq \psi_2$ but $\psi_1(\alpha) = \psi_2(\alpha)$.

Let $f(x) = (x - \alpha_1) \cdots (x - \alpha_m)$. For any $\psi \in G$, ψ permutes the roots $\{\alpha_1, \cdots, \alpha_m\}$. Since the coefficients of $f(x)$ can be viewed as symmetric polynomials in $\alpha_1, \cdots, \alpha_m$ they are invariant under all $\psi \in G$. Thus $f(x) \in E^G[x] = F[x]$. To show that $f(x)$ is the minimal polynomial of α, consider a factor $g(x) \in F[x]$ of $f(x)$. Without loss of generality, we can write $g(x) = (x - \alpha_1) \cdots (x - \alpha_\ell)$ with $\ell \leq m$.

If $\ell < m$, since $\alpha_1, \cdots, \alpha_m$ are in the G-orbit of α, there exists $\psi \in G$ such that $\{\alpha_1, \cdots, \alpha_\ell\} \neq \{\psi(\alpha_1), \cdots, \psi(\alpha_\ell)\}$. It follows that $\psi(g(x)) = (x - \psi(\alpha_1)) \cdots (x - \psi(\alpha_\ell)) \neq g(x)$. Thus if $\ell < m$, $g(x) \notin F[x]$. It follows that $f(x)$ is the minimal polynomial of α over F. Since $f(x) \in F[x]$ is separable and splits over E, E/F is a Galois extension.

Claim 8.1.1: $[E : F] \leq n$

Proof. If $[E : F] > n = |G|$, we can choose $\beta_1, \cdots, \beta_n, \beta_{n+1} \in E$ which are linearly independent over F. Consider the system of n linear equations in the $n + 1$ variables $v_1, \cdots, v_{n+1}$

$$\psi(\beta_1)v_1 + \cdots + \psi(\beta_{n+1})v_{n+1} = 0, \quad \forall \psi \in G.$$

Thus it has a non-zero solution in E. Let $(\gamma_1, \cdots, \gamma_{n+1})$ be such a solution which has the minimal number of non-zero coordinates, say r. Clearly $r \geq 2$ (since we need at least two non-zero coordinates to get zero). Without loss of generality, we can assume $\gamma_1, \cdots, \gamma_r \neq 0$ and $\gamma_{r+1}, \cdots, \gamma_{n+1} = 0$. Thus

$$\psi(\beta_1)\gamma_1 + \cdots + \psi(\beta_r)\gamma_r = 0, \quad \forall \psi \in G. \tag{1}$$

By dividing the solution by γ_r, we can assume that $\gamma_r = 1$. Also, since $(\beta_1, \cdots, \beta_r)$ are linearly independent over F, and $\beta_1\gamma_1 + \cdots + \beta_r\gamma_r = 0$ there exists at least one $\gamma_i \notin F$. Since $r \geq 2$, without loss of generality we can assume that $\gamma_1 \notin F$. This means that we can choose $\phi \in G$ such that $\phi(\gamma_1) \neq \gamma_1$. Applying ϕ to (1) we get

$$(\phi \circ \psi)(\beta_1)\phi(\gamma_1) + \cdots + (\phi \circ \psi)(\beta_r)\phi(\gamma_r) = 0, \quad \forall \psi \in G.$$

Since ψ runs through all the elements of G, so does $\phi \circ \psi$. Thus we can rewrite the above equation as:

$$\psi(\beta_1)\phi(\gamma_1) + \cdots + \psi(\beta_r)\phi(\gamma_r) = 0, \quad \forall \psi \in G. \tag{2}$$

By subtracting (2) from (1), we get:

$$\psi(\beta_1)(\gamma_1 - \phi(\gamma_1)) + \cdots + \psi(\beta_r)(\gamma_{r-1} - \phi(\gamma_{r-1})) + \psi(\beta_r)(\gamma_r - \phi(\gamma_r)) = 0, \quad \forall \psi \in G$$

Note that since $\gamma_r = 1$, we must have $\phi(\gamma_r) = 1$ and so $\gamma_r - \phi(\gamma_r) = 0$. Also, since $\gamma_1 \notin F$ we have $\gamma_1 - \phi(\gamma_1) \neq 0$. Thus

$$\gamma_1 - \phi(\gamma_1), \cdots, \gamma_{r-1} - \phi(\gamma_{r-1}), 0, \cdots, 0$$

is a non-zero solution of the system that contains fewer non-zero coordinates than $\gamma_1, \cdots, \gamma_{n+1}$, which is a contradiction. Thus $[E : F] \leq n$.

□

Since we have shown that E/F is a finite Galois extension, E is the splitting field of some separable polynomial over F. Also, since

$$F = E^G = \{\alpha \in E : \psi(\alpha) = \alpha, \forall \psi \in G\}$$

G is a subgroup of $\mathrm{Gal}_F(E)$. By Theorem 6.7, we have

$$n = |G| \leq |\mathrm{Gal}_F(E)| = [E : F] \leq n$$

and so it follows that $[E : F] = n$ and thus $\mathrm{Gal}_F(E) = G$.

□

Remark: Let E be a field and G a finite subgroup of $\mathrm{Aut}(E)$. For $\alpha \in E$ let $\{\alpha = \alpha_1, \alpha_2, \cdots, \alpha_m\}$ be the G-orbit of α (i.e. the set of all conjugates of α). The we see from the proof of theorem 8.1 that the minimal polynomial of α over E^G is

$$(x - \alpha_1) \cdots (x - \alpha_m) \in E^G[x].$$

Example 8.2: Let $E = F(t_1, \cdots, t_n)$ be the rational function field in n variables $t_1, \cdots, t_n$ over a field F. Consider the symmetric group S_n as the subgroup of $\mathrm{Aut}(E)$ which permutes the variables $t_1, \cdots, t_n$ and fixes the field F. We claim that if we let $G = Sn$ then $E^{S_n} = E^G = F(s_1, \cdots, s_n)$ where $s_1, s_2, \cdots, s_n$ are the elementary symmetric polynomials in the variables $t_1, t_2, \cdots, t_n$.

Proof. From the proof of Theorem 8.1, the coefficients of the minimal polynomial of t_1 lie in E^G. Thus by considering the minimal polynomial of t_1, we can get some information about E^G.

The G-orbit of t_1 is $\{t_1, t_2, \cdots, t_n\}$. The minimal polynomial of t_1 over E^G is

$$f(x) = (x - t_1)(x - t_2) \cdots (x - t_n).$$

Let $s_1, s_2, \cdots, s_n$ be the elementary symmetric functions of $t_1, \cdots, t_n$ so we have

$$f(x) = x^n - s_1 x^{n-1} + s_2 x^{n-2} + \cdots + (-1)^n s_n \in L[x]$$

where $L = F(s_1, \cdots, s_n)$. Note that $L \subseteq E^G$ and E is the splitting field of $f(x)$ over L. Since $\deg(f) = n$, by Theorem 4.5, we have $[E : L] \leq n!$. On the other hand, by Theorem 8.1

$$E : E^G = |G| = |S_n| = n!.$$

Since $L \subseteq E^G$ we have

$$n! = [E : E^G] \leq [E : L] \leq n!$$

so we conclude $E^G = L$.

□

8.2 The Fundamental Theorem of Galois Theory

Theorem 8.2 (The Fundamental Theorem of Galois Theory)**:** Let E/F be a finite Galois extension and $G = \mathrm{Gal}_F(E)$. There is an order reversing bijection between the intermediate fields of E/F and the subgroups of G.

More precisely, let $\mathrm{Int}(E/F)$ denote the set of intermediate fields of E/F and $\mathrm{Sub}(G)$ the set of subgroups of G. Then the maps

$$\mathrm{Int}(E/F) \to \mathrm{Sub}(G), \qquad L \mapsto L^* := \mathrm{Gal}_L(E)$$

and

$$\mathrm{Sub}(G) \to \mathrm{Int}(E/F), \qquad H \mapsto H^* := E^H$$

are inverses of each other and reverse the set inclusion relation. In-particular, for $L_1, L_2 \in \mathrm{Int}(E/F)$ with $L_2 \subseteq L_1$, $H_1, H_2 \in \mathrm{Sub}(G)$ and $H_2 \subseteq H_1$ we have $[L_1 : L_2] = [L_2^* : L_1^*]$ and $[H_1 : H_2] = [H_2^* : H_1^*]$. These relations are outlined in the diagram below.

Figure 1: A Diagram of the Fundamental Theorem of Galois Theory

$$\begin{array}{ccc} E & \longleftrightarrow & \{1\} = \mathrm{Gal}_E(E) \\ \cup & & \cap \\ L_1 & \longleftrightarrow & L_1^* = \mathrm{Gal}_{L_1}(E) \\ \cup & & \cap \\ L_2 & \longleftrightarrow & L_2^* = \mathrm{Gal}_{L_2}(E) \\ \cup & & \cap \\ F & \longleftrightarrow & G = \mathrm{Gal}_F(E) \end{array}$$

Note: The $\cup$ and $\cap$ symbols here denote (strict) set inclusion relations up and down the diagram. The arrows $\leftrightarrow$ represent the invertible map $(\,\cdot\,)^*$.

Proof. Let $L \in \mathrm{Int}(E/F)$ and $H \in \mathrm{Sub}(G)$. We recall Theorem 6.9 which states that if $G_1 = \mathrm{Gal}_{F_1}(E_1)$, then $E_1^{G_1} = F_1$. Thus

$$(L^*)^* = (\mathrm{Gal}_L(E))^* = E^{\mathrm{Gal}_L(E)} = L$$

Also, by Theorem 8.1

$$(H^*)^* = (E^H)^* = \mathrm{Gal}_{E^H}(E) = H,$$

Thus we have $H \mapsto H^* \mapsto (H^*)^* = H$ and $L \mapsto L^* \mapsto (L^*)^* = L$. In-particular, the maps $L \mapsto L^*$ and $H \mapsto H^*$ are inverses of each other.

Let $L_1, L_2 \in \mathrm{Int}(E/F)$. Since E/F is the splitting field of $f(x) \in F[x]$ whose irreducible factors are separable E/L_1 and E/L_2 are also Galois extensions since E is the splitting field of $f(x)$ over L_1 and L_2 respectively. We have $L_2 \subseteq L_1 \implies \mathrm{Gal}_{L_1}(E) \subseteq \mathrm{Gal}_{L_2}(E)$, i.e. $L_1^* \subseteq L_2^*$. Also,

$$[L_1 : L_2] = \frac{[E : L_2]}{[E : L_1]} = \frac{|\,\mathrm{Gal}_{L_2}(E)|}{|\,\mathrm{Gal}_{L_1}(E)|} = \frac{|L_2^*|}{|L_1^*|} = [L_2^* : L_1^*].$$

On the other hand, for $H_1, H_2 \in \mathrm{Sub}(G)$,

$$H_2 \subseteq H_1 \implies E^{H_1} \subseteq E^{H_2},$$

i.e. $H_1^* \subseteq H_2^*$. This time we get

$$[H_1 : H_2] = \frac{|H_1|}{|H_2|} = \frac{|\,\mathrm{Gal}_{E^{H_1}}(E)|}{|\,\mathrm{Gal}_{E^{H_2}}(E)|} = \frac{[E : E^{H_1}]}{[E : E^{H_2}]} = [E^{H_2} : E^{H_1}].$$

□

Remark: Consider the intermediate fields between $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $F = \mathbb{Q}$. $\mathrm{Gal}_{\mathbb{Q}}(E) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has only finitely many subgroups, so there are only finitely many intermediate fields between E and F

We have seen that if E/F is a finite Galois extension and $L \in \mathrm{Int}(E/F)$ then L/F is not always Galois. For example, $E = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, $L = \mathbb{Q}(\sqrt[3]{2})$, $F = \mathbb{Q}$.

$$\begin{array}{ccc} E & \longleftrightarrow & \{1\} = \mathrm{Gal}_E(E) \\ \cup & & \cap \\ L & \longleftrightarrow & L^* = \mathrm{Gal}_L(E) \\ \cup & & \cap \\ F & \longleftrightarrow & G = \mathrm{Gal}_F(E) \end{array}$$

From this diagram we see that, if L/F is Galois, it corresponds to the group G/L^* which is well-defined only if $L^* \lhd G$. This observation inspires the next result.

Proposition 8.3: Let E/F be a finite Galois extension with $G = \mathrm{Gal}_F(E)$. Let L be an intermediate field. For $\psi \in G$,

$$\mathrm{Gal}_{\psi(L)}(E) = \psi \,\mathrm{Gal}_L(E)\psi^{-1}.$$

Proof. For $\alpha \in \psi(L)$, $\psi^{-1}(\alpha) \in L$, if $\psi \in \mathrm{Gal}_L(E)$ then we have

$$\phi(\psi^{-1}(\alpha)) = \psi^{-1}(\alpha),$$

thus $(\psi\phi\psi^{-1})(\alpha) = \alpha$ and so $\psi\phi\psi^{-1} \in \mathrm{Gal}_{\psi(L)}(E)$. Thus $\psi \,\mathrm{Gal}_L(E)\psi^{-1} \subseteq \mathrm{Gal}_{\psi(L)}(E)$. Since

$$|\psi \,\mathrm{Gal}_L(E)\psi^{-1}| = |\,\mathrm{Gal}_L(E)| = [E : L] = [E : \psi(L)] = ||Gal_{\psi(L)}(E)|$$

we conclude that $\mathrm{Gal}_{\psi(L)}(E) = \psi \,\mathrm{Gal}_L(E)\psi^{-1}$.

□

Theorem 8.4: Let E/F, L, L^* all be defined as in Fundamental Theorem 8.2. Then L/F is a Galois extension if and only if L^* is a normal subgroup of G. In this case we have

$$\mathrm{Gal}_F(L) \cong G/L^*.$$

Proof.

$$\begin{aligned}
L/F \text{ is normal} &\iff \psi(L) = L \\
&\iff \mathrm{Gal}_{\psi(L)}(E) = \mathrm{Gal}_L(E), \text{ for all } \psi \in \mathrm{Gal}_F(E) \\
&\iff \psi \,\mathrm{Gal}_L(E)\psi^{-1} = \mathrm{Gal}_L(E), \text{ for all } \psi \in \mathrm{Gal}_F(E) \qquad \text{(By Proposition 8.3)} \\
&\iff L^* = \mathrm{Gal}_L(E) \lhd G
\end{aligned}$$

If L/F is a Galois extension, then since it is normal the restriction $\psi\restriction_L$: $\mathrm{Gal}_F(E) \to \mathrm{Gal}_F(L)$ is well-defined. Moreover, it is surjective and its kernel is

$$\mathrm{Gal}_L(E) = L^*.$$

So by the first isomorphism theorem, $\mathrm{Gal}_F(L) \cong G/L^*$.

□

8.3 Characterization of Intermediate Fields

This section contains two examples in which we use the Fundamental Theorem of Galois Theory (Theorem 8.2) to characterize the intermediate fields of finite Galois extensions.

Example 8.3: Let p be a prime and $q = p^n$. To characterize the intermediate fields of $\mathbb{F}_q/\mathbb{F}_p$ we need to understand $\mathrm{Gal}_{\mathbb{F}_p}(\mathbb{F}_q)$. Recall from Assignment 4 the Frobenius automorphism of $\mathbb{F}_q$ defined by $\sigma_p : \mathbb{F}_q \to \mathbb{F}_q$ with $\sigma(\alpha) = \alpha^p$. For $\alpha \in \mathbb{F}_q$, we have $\sigma_p^n(\alpha) = \alpha^{p^n} = \alpha$. For $1 \le m < n$, we have $\sigma_p^m(\alpha) = \alpha^{p^m}$. Since the polynomial $x^{p^m} - x$ has at most p^m roots in $\mathbb{F}_q$, there exists $\alpha \in E$ such that $\alpha^{p^m} - \alpha \neq 0$. Thus $\sigma_p^m \neq 1$. Hence σ_p has order n. Let $G = \mathrm{Gal}_{\mathbb{F}_p}(\mathbb{F}_q)$, it follows that

$$n = |\langle\sigma_p\rangle| \le |G| = [\mathbb{F}_q : \mathbb{F}_p] = n$$

and so $G = \langle\sigma_p\rangle$ is a cyclic group of order n.

Now consider a subgroup H of G which of order d. Thus $d \,|\, n$ and $[G : H] = \frac{n}{d}$. By Theorem 8.2,

$$\frac{n}{d} = [G : H] = [H^* : G^*] = [\mathbb{F}_q^H : \mathbb{F}_q^G] = [\mathbb{F}_q^H : \mathbb{F}_p]$$

and thus $H^* = \mathbb{F}_q^H = \mathbb{F}_{p^{n/d}}$. These relations are outlined in following diagram.

$$\begin{array}{ccccc} \mathbb{F}_q & \longleftrightarrow & \{1\} & & \\ \cup & & \cap & & \\ H^* = \mathbb{F}_{p^{n/d}} & \longleftrightarrow & H & & |H| = d \\ \cup & & \cap & & \\ \mathbb{F}_p & \longleftrightarrow & G & & |G| = n \end{array}$$

Example 8.4: Let E be the splitting field of $x^5 - 7$ over $\mathbb{Q}$ in $\mathbb{C}$. Then $E : \mathbb{Q}(\alpha, \zeta_5)$ with $\alpha = \sqrt[5]{7}$ and $\zeta_5 e^{2\pi i/5}$. Note that the minimal polynomials of α and ζ_5 over $\mathbb{Q}$ are $x^5 - 7$ and $x^4 + x^3 + x^2 + x + 1$ respectively. In-fact, one can show (piazza exercise) that $[E : \mathbb{Q}] = 20$, and hence $G = \mathrm{Gal}_{\mathbb{Q}}(E)$ is a subgroup of S_5 of order 20.

By Lemma 6.6, given any $\psi \in G$ its action is entirely determined by $\psi(\alpha)$ and $\psi(\zeta_5)$. Let $\psi = \psi_{k,s}$ if $\psi(\alpha) = \alpha\zeta_5^k$ and $\psi(\zeta_5) = \zeta_5^s$ for $k \in \mathbb{Z}_5$ and $s \in \mathbb{Z}_5^*$.

Using this notation, Figure 2 gives a complete classification of all the subgroups of G that is proven below. From this we can then apply the Fundamental Theorem of Galois Theory to generate a complete classification of the intermediate fields between $\mathbb{Q}$ and E which is given in Figure 3.

Proof. Deriving the classification of the subgroups of G given in can be done by an application of Sylow theory learned in PMATH347. Recall that we have $|G| = 20 = 4 \cdot 5$. Let n_p be the number of Sylow p-subgroups of G. By the third Sylow theorem, $n_5 \mid 4$ and $n_5 \equiv 1 \bmod 5$, hence $n_5 = 1$. Also, $n_2 \mid 5$ and $n_2 \equiv 1 \bmod 2$. Hence $n_2 = 1$ or 5. If $n_2 = 1$, then $G \cong \mathbb{Z}_4 \times \mathbb{Z}_5$, which contradicts that G is not abelian, thus $n_2 = 5$. Similarly, one can also show that $n_5 = 1$.

If we define

$$\sigma = \psi_{1,1} = \begin{cases} \alpha \mapsto \alpha\zeta_5 \\ \zeta_5 \mapsto \zeta_5 \end{cases} \quad \text{and} \quad \tau = \sigma_{0,2} = \begin{cases} \alpha \mapsto \alpha \\ \zeta_5 \mapsto \zeta_5^2 \end{cases}$$

then G can be expressed as

$$G = \langle \sigma, \tau : \tau\sigma = \sigma^2\tau \rangle.$$

Since $\tau \in G$ is of order 4, the cyclic group $\langle \tau \rangle$ is a Sylow 2-subgroup and all other Sylow 2-subgroups are conjugate to it. Note that the elements of G are of the form $\sigma^a\tau^b$. Hence we have

$$\sigma^a\tau^b(\tau)\tau^{-b}\sigma^{-a} = \sigma^a\tau\sigma^{-a}$$

for all $a \in \{0, 1, 2, 3, 4\}$. Using the relation $\tau\sigma = \sigma^2\tau$ we have

$$\langle \sigma^4\tau\sigma^{-4} \rangle = \langle \sigma^{-1}\tau\sigma \rangle = \langle \sigma\tau \rangle = \langle \psi_{1,2} \rangle \qquad \text{(exercise)}$$

Using a similar argument, we find that the Sylow 2-groups are

$$\langle \psi_{0,2} \rangle, \langle \psi_{1,2} \rangle, \langle \psi_{2,2} \rangle, \langle \psi_{3,2} \rangle, \langle \psi_{4,2} \rangle \qquad (*4)$$

and so these are all the subgroups of order 4. Moreover, since all subgroups of G of order 2 are contained in a Sylow 2-subgroup and

$$\langle \psi_{0,2}^2 \rangle, \langle \psi_{1,2}^2 \rangle, \langle \psi_{2,2}^2 \rangle, \langle \psi_{3,2}^2 \rangle, \langle \psi_{4,2}^2 \rangle \qquad (*2)$$

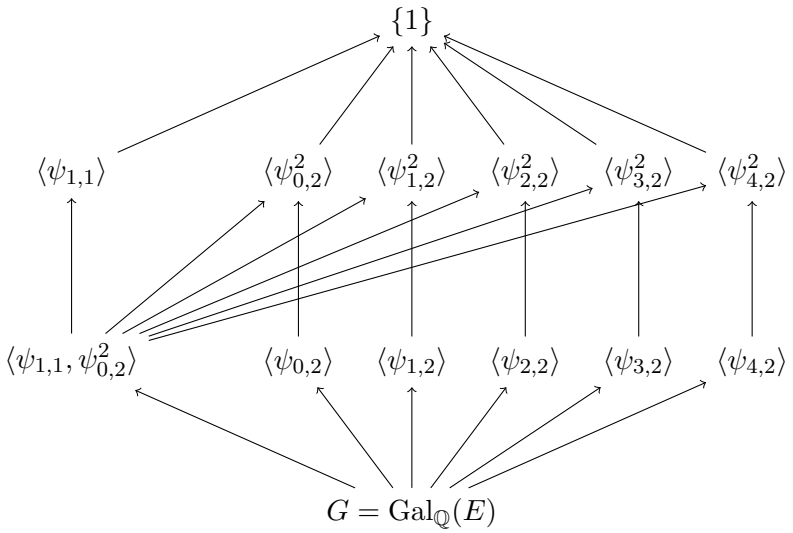
are all subgroups of order 2 that are contained groups $(*4)$ above, $(*2)$ are all the subgroups of order 2.

For a subgroup H of G to be of order 10, since there is only one subgroup of G of order 5, we must have $H \supseteq \langle \sigma \rangle$. Thus $\sigma^a\tau^b \in H$ if and only if $\tau^b \in H$.

Since the only divisors of 20 are 2,4,5 and 10, we have now found all the subgroups of G.

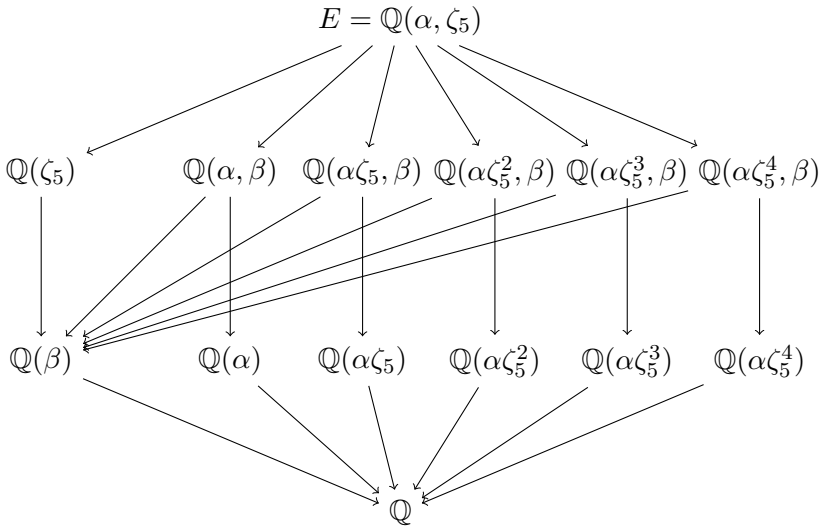
□

Figure 2: A Diagram of the Characterization of the Subgroups of G



Note: The arrows in this diagram represent a subgroup relation where $A \to B$ means $A \supseteq B$.

Figure 3: A Diagram of the Characterization of the Intermediate Fields of $E/\mathbb{Q}$



Note: The arrows in this diagram represent a subfield relation where $A \to B$ means $A \supseteq B$. This diagram uses $\alpha = \sqrt[5]{7}$ and $\beta = \zeta_5 + \zeta_5^{-1}$.

To go from Figure 2 above to a characterization of the intermediate fields of E/F we apply the Fundamental Theorem of Galois Theory (Theorem 8.2). For an intermediate field L of $E/\mathbb{Q}$, we consider $L^* = \mathrm{Gal}_L(E)$. For example, for $\mathbb{Q}(\zeta_5)$ note that $\psi_{1,1}(\zeta_5) = \zeta_5$. Thus $\mathbb{Q}(\zeta_5)^* \supseteq \langle \psi_{1,1} \rangle$. Since $|\langle \psi_{1,1} \rangle| = [\langle \psi_{1,1} \rangle : \{1\}] = 5$ and $5 = [E : \mathbb{Q}(\zeta_5)] = [\mathbb{Q}(\zeta_5)^* : \{1\}]$ we have $\mathbb{Q}(\zeta_5)^* = \langle \psi_{1,1} \rangle$.

Next, notice that $\psi_{1,2}(\alpha\zeta_5^r) = \alpha\zeta_5^{2r+1}$. If $\psi_{1,2}$ fixes $\alpha\zeta^r$, then $r \equiv 2r+1 \bmod 5$ and so $r \equiv 4 \bmod 5$. Thus $\mathbb{Q}(\alpha\zeta_5^4)^* \supseteq \langle \psi_{1,2} \rangle$. Since $|\langle \psi_{1,2} \rangle| = [\langle \psi_{1,2} \rangle : \{1\}] = 4$ and $[E : \mathbb{Q}(\alpha\zeta_5^4)] = 4$, we find $\mathbb{Q}(\alpha\zeta_5^4)^* = \langle \psi_{1,2} \rangle$. Using a similar argument we an get and expression for $\langle \psi_{r,2} \rangle^*$ for all $r \in \{0, 1, 2, 3, 4\}$ gives

Now consider $\beta = \zeta_5 + \zeta_5^{-1} \in \mathbb{R}$. We have

$$\beta^2 + \beta + 1 = \zeta_5^2 + 2 + \zeta_5^{-2} + \zeta_5 + \zeta_5^{-1} - 1 = 1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta)5^4 = 0.$$

Since $x^2 + x - 1 = 0$ has no rational roots, we have $[\mathbb{Q}(\beta) : \mathbb{Q}] = 2$. Similarly, $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = 2$. Altogether, this gives Figure 3 as a characterization of the intermediate fields of $E/\mathbb{Q}$.

9 Cyclic Extensions

Definition 9.1 (Cyclic, Abelian and Solvable Extensions)**:** A Galois extension E/F is called cyclic, abelian or solvable if the group $\mathrm{Gal}_F(E)$ has the corresponding property.

Lemma 9.1 (Dedekind's Lemma)**:** Let K and L be fields and let $\psi_i : L \to K$ be distinct non-zero homomorphisms $(1 \leq i \leq n)$. If $c_i \in K$ and

$$c_1\psi_1(\alpha) + c_2\psi_2(\alpha) + \cdots + c_n\psi_n(\alpha) = 0, \quad \forall \alpha \in L$$

then

$$c_1 = c_2 = \cdots = 0.$$

Proof. For the sake of contradiction suppose that the statement is false. Let $m \geq 2$ be the minimal positive integer such that

$$c_1\psi_1(\alpha) + \cdots + c_m\psi_m(\alpha) = 0, \quad \forall \alpha \in L \tag{1}$$

Sine m is minimal, we have $c_i \neq 0$ $(1 \leq i \leq m)$. Since $\psi_1 \neq \psi_2$, we can choose $\beta \in L$ such that $\psi_1(\beta) \neq \psi_2(\beta)$. Moreover, we can assume $\psi_1(\beta) \neq 0$. By (1), we have

$$c_1\psi_1(\alpha\beta) + \cdots + c_m\psi_m(\alpha\beta) = 0, \quad \forall \alpha \in L.$$

By dividing the above equation by $\psi_1(\beta)$, we have

$$c_1\psi_1(\alpha) + c_2\psi_2(\alpha)\frac{\psi_2(\beta)}{\psi_1(\beta)} + \cdots + c_m\psi_m(\alpha)\frac{\psi_m(\beta)}{\psi_1(\beta)} = 0, \quad \forall \alpha \in L \tag{2}$$

Consider the equation (1) − (2). After some rearrangement we obtain

$$c_2\left(1 - \frac{\psi_2(\beta)}{\psi_1(\beta)}\right)\psi_2(\alpha) + \cdots + c_m\left(1 - \frac{\psi_m(\beta)}{\psi_1(\beta)}\right)\psi_m(\alpha) = 0, \quad \forall \alpha \in L.$$

Since we chose $\psi_1(\beta) \neq \psi_2(\beta)$ we get $c_2(1 - \frac{\psi_2(\beta)}{\psi_1(\beta)}) \neq 0$, and so we have a contradiction with the minimal choice for m.

□

Theorem 9.2: Let F be a field and $n \in \mathbb{N}$. Suppose $\mathrm{ch}(F) = 0$ or $\mathrm{ch}(F) = p$ with $p \nmid n$. Assume also that $x^n - 1$ splits over F.

1. If the Galois extension E/F is cyclic with degree n, then $E = F(\alpha)$ for some $\alpha \in E$ with $\alpha^n \in F$. In-particular, $x^n - \alpha^n$ is the minimal polynomial of α over F.
2. If $E = F(\alpha)$ with $\alpha^n \in F$, then E/F is a cyclic extension of degree d with $d \mid n$ and $\alpha^d \in F$. In-particular, $x^d - \alpha^d$ is the minimal polynomial of α over F.

Proof. Let $\zeta_n \in F$ be a primitive n-th root of unity, i.e. $\zeta_n^n = 1$ and $\zeta_n^d \neq 1$ for any $1 \leq d < n$. Note that since $\mathrm{ch}(F) = 0$ or p with $p \nmid n$, the polynomial $x^n - 1$ is separable. Thus $1, \zeta_n, \zeta_n^2, \cdots, \zeta_n^{n-1}$ are all distinct.

1. Let $G = \mathrm{Gal}_F(E) = \langle\psi\rangle \cong C_n$, the cyclic group of order n. Apply Dedekind's Lemma 9.1 to $K = L = E$ where ψ_i are all the elements of G and $c_1 = 1, c_2 = \zeta_n^{-1}, \cdots, c_n = \zeta^{-(n-1)}$. Since $c_i \neq 0$ for all $1 \leq i \leq n$, there exists $u \in E$ such that

$$\alpha = u + \zeta_n^{-1}\psi(u) + \cdots + \zeta_n^{-(n-1)}\psi^{n-1}(u) \neq 0.$$

We have

$$\begin{aligned}
\psi^0(\alpha) &= \alpha \\
\psi^1(\alpha) &= \psi(u) + \zeta_n^{-1}\psi^2(u) + \cdots + \zeta_n^{-(n-1)}\psi^n(u) = \alpha\zeta_n \\
\psi^2(\alpha) &= \psi^2(u) + \zeta_n^{-1}\psi^3(u) + \cdots + \zeta_n^{-(n-1)}\psi^{n+1}(u) = \alpha\zeta_n^2 \\
&\vdots
\end{aligned}$$

or, in general, $\psi^k(\alpha) = \alpha\zeta_n^k$. Thus $\alpha, \alpha\zeta_n, \cdots, \alpha\zeta_n^{n-1}$ are conjugates to each other (in the sense of Notation 7.4), and so they all share the same minimal polynomial over F, say $p(x)$. Since $\alpha, \alpha\zeta_n, \cdots, \alpha\zeta_n^{n-1}$ are all distinct, it follows that $\deg(p) = n$. Also, since $p(x) \in F[x]$,

$$p(0) = \pm\alpha(\alpha\zeta_n)\cdots(\alpha\zeta_n^{n-1}) = \alpha^n\zeta_n^{\frac{n(n-1)}{2}} \in F.$$

Since $\zeta_n \in F$, $\alpha^n \in F$. Since α is a root of $x^n - \alpha^n \in F[x]$ and $\deg(p) = n$, we have $p(x) = x^n - \alpha^n$. Moreover, since $F(\alpha) \subseteq E$ and $[F(\alpha) : F] = \deg(p) = n = [E : F]$, we have $E = F(\alpha)$.

2. Suppose $\alpha^n \in F$. Let $p(x) \in F[x]$ be the minimal polynomial of α over F. Since α is a root of $x^n - \alpha^n \in F[x]$, $p(x) \mid (x^n - \alpha^n)$. Thus the roots of $p(x)$ are of the form $\alpha\zeta_n^i$ for some i and we have
$$p(0) = \pm\alpha^d\zeta^k$$
for some $k \in \mathbb{Z}$ and $d \in \mathbb{N}$ where d is the number of roots of $p(x) = \deg(p)$. Since $p(0) \in F$ and $\zeta_n \in F$, we have $\alpha^d \in F$. Since $x^d - \alpha^d \in F[x]$ has α as a root, $p(x) \mid (x^d - \alpha^d)$. Since $\deg(p) = d$ and $p(x)$ is monic, we have $p(x) = x^d - \alpha^d$.

Claim 9.2.1: $d \mid n$

Proof. For the sake of contradiction, suppose $d \nmid n$. Then set $n = qd + r$ for some $0 < r < d$. Since $\alpha^n, \alpha^d \in F$, we have $\alpha^r = \alpha^{n-qd} = \alpha^n(\alpha^d)^{-q} \in F$. Since $\alpha^r \in F$, α is a root of $x^r - \alpha^r \in F[x]$. It follows that $p(x) \mid (x^r - \alpha^r)$ which is a contradiction since $\deg(p) = d > r$. Thus $d \mid n$.

□

Now write $n = md$. Since $p(x) = x^d - \alpha^d$, the roots of $p(x)$ are

$$\alpha, \alpha\zeta_n^m, \alpha\zeta_n^{2m}, \cdots, \alpha\zeta_n^{(d-1)m}.$$

Since $\zeta_n \in F$, $E = F(\alpha)$ is the splitting field of the separable polynomial $p(x)$ over F, and thus is Galois. If $\psi \in G = \mathrm{Gal}_F(E)$ satisfies $\psi(\alpha) = \alpha\zeta_n^m$ then $G = \langle\psi\rangle \cong C_d$. Thus E/F is a cyclic extension of degree d.

□

Theorem 9.3: Let F be a field with $\mathrm{ch}(F) = p$ where p is a prime.

1. If $x^p - x - a \in F[x]$ is irreducible then its splitting field E/F is a cyclic extension of degree p.
2. If E/F is a cyclic extension of degree p then E/F is the splitting field of some irreducible polynomial $x^p - x - a \in F[x]$.

Proof.

1. Let $f(x) = x^p - x - a$ and α be a root of $f(x)$. Then since $\mathrm{ch}(F) = p$ we get

$$f(\alpha+1) = (\alpha+1)^p - (\alpha+1) - a = \alpha^p + 1 - \alpha - 1 - a = \alpha^p - \alpha - a = 0,$$

so $\alpha + 1$ is also a root of $f(x)$. Similarly, $\alpha + 2, \cdots, \alpha + (p-1)$ are also all roots of $f(x)$. Since $f(x)$ has at most p distinct roots, this means that

$$\alpha, \alpha + 1, \cdots, \alpha + (p-1)$$

are all roots of $f(x)$. It follows that $E = F(\alpha, \alpha+1, \cdots, \alpha+(p-1)) = F(\alpha)$ and $[E : F] = \deg(f) = p$. Since C_p is the only group of order p, we have $\mathrm{Gal}_F(E) \cong C_p$. Indeed, $\mathrm{Gal}_F(E) = \langle\psi\rangle$, where $\psi : E \to E$, $\psi\restriction_F = 1_F$, $\alpha \mapsto \alpha + 1$.

2. Let $G = \mathrm{Gal}_F(E) = \langle\psi\rangle \cong C_p$. Apply Dedekind's Lemma 9.1 to $K = L = E$ with ψ_i all elements of G and $c_1, \cdots, c_p = 1$. Since $c_i \neq 0$ there exists some $v \in E$ such that

$$\beta := v + \psi(v) + \psi^2(v) + \cdots + \psi^{p-1}(v) \neq 0.$$

Since $\psi^i(\beta) = \beta$ for all $\psi^i \in G$ with $0 \leq i \leq p-1$, we have $\beta \in F$. Setting $u = v/\beta$, this gives:

$$\begin{aligned} u + \psi(u) + \cdots + \psi^{p-1}(u) &= v/\beta + \psi(v/\beta) + \cdots + \psi^{p-1}(v/\beta) \\ &= \frac{v + \psi(v) + \cdots + \psi^{p-1}(v)}{\beta} \\ &= \frac{\beta}{\beta} = 1 \end{aligned}$$

If we now set $\alpha := 0 \cdot u - 1\psi(u) - 2\psi^2(u) - \cdots - (p-1)\psi^{p-1}(u)$ then:

$$\begin{aligned} \psi(\alpha) &= -\psi^2(u) - 2\psi^3(u) - \cdots - (p-1)\psi^p(u) \\ \psi(\alpha) - \alpha &= \psi(u) + \psi^2(u) + \cdots + \psi^{p-1}(u) + \psi^p(u) \\ \psi(\alpha) - \alpha &= 1 \\ \psi(\alpha) &= \alpha + 1 \end{aligned}$$

Since $\mathrm{ch}(F) = p$, we have

$$\psi(\alpha^p) = \psi(\alpha)^p = (\alpha+1)^p = \alpha^p + 1.$$

It follows that

$$\psi(\alpha^p - \alpha) = \psi(\alpha^p) - \psi(\alpha) = \alpha^p + 1 - (\alpha+1) = \alpha^p - \alpha.$$

Thus $\alpha^p - \alpha$ is fixed by ψ. Since $G = \langle\psi\rangle$, we have $a = \alpha^p - \alpha \in F$ and α is a root of $x^p - x - a \in F[x]$. Since $[E : F] = p$, $[F(\alpha) : F]$ is a factor of p. Since $\alpha \notin F$ (as $\psi(\alpha) = \alpha + 1 \neq \alpha$) and p is a prime, we have $[F(\alpha) : F] = p$ and $E = F(\alpha)$. Since $[F(\alpha) : F] = p$, it also follows that $x^p - x - a \in F[x]$ is the minimal polynomial of α.

□

10 Solvability by Radicals

10.1 Radical Extensions

Definition 10.1: A finite extension E/F is radical if there exists a tower of fields

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m = E$$

such that for each i, $F_i = F_{i-1}(\alpha_i)$ (where $\alpha_i \in F$) and $\alpha_i^{d_i} \in F_{i-1}$ for some $d_i \in \mathbb{N}$.

Lemma 10.1: If E/F is a finite separable radical extension, then its normal closure N/F is also radical.

Proof. Since E/F is a finite separable extension, by the Primitive Element Theorem 7.2, $E = F(\beta)$ for some $\beta \in E$. Since E/F is a radical extension, there is a tower

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m = E$$

such that $F_i = F_{i-1}(\alpha_i)$ and $\alpha_i^{d_i} \in F_{i-1}$ for some $d_i \in \mathbb{N}$. Let $p(x) \in F[x]$ be the minimal polynomial of β and let $\beta = \beta_1, \beta_2, \cdots, \beta_n$ be the roots of $p(x)$. By the definition of normal closure and Theorem 7.3,

$$N = E(\beta_2, \cdots, \beta_n) = F(\beta_1, \cdots, \beta_n).$$

Also, there exist F-isomorphisms

$$\sigma_j : F(\beta) \to F(\beta_j), \quad \beta \mapsto \beta_j, \quad \forall j = 2, 3, \cdots, n.$$

Since N can be viewed as the splitting field of $p(x)$ over $F(\beta)$ and $F(\beta_j)$ respectively, by Theorem 4.4 there exists $\psi_j : N \to N$ which extends σ_j. Thus $\psi_j \in \mathrm{Gal}_F(N)$ and $\psi_j(\beta) = \beta_j$. This gives the following tower of fields:

$$\begin{aligned} F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m = E &= F(\beta_1) = F(\beta_1)\psi_2(F_0) \\ &\subseteq F(\beta_1)\psi_2(F_1) \subseteq \cdots \subseteq F(\beta_1)\psi_2(F_m) = F(\beta_1, \beta_2) = F(\beta_1, \beta_2)\psi_2(F_0) \\ &\subseteq F(\beta_1, \beta_2)\psi_3(F_1) \subseteq \cdots \\ &\vdots \\ &\subseteq \cdots \subseteq F(\beta_1, \cdots, \beta_n) = N \end{aligned}$$

Note that since $F_i = F_{i-1}(\alpha_i)$ we have

$$F(\beta_1, \cdots, \beta_{j-1})\psi(F_i) = F(\beta_1, \cdots, \beta_{j-1})\psi_j(F_{i-1}(\alpha_i)) = (F(\beta_1, \cdots, \beta_{j-1})\psi_j(F_{i-1}))\,(\psi_j(\alpha_i)).$$

But $\alpha_i^{d_i} \in F_{i-1}$, so

$$(\psi_j(\alpha_i))^{d_i} = \psi_j(\alpha_i^{d_i}) \in \psi_j(F_{i-1}).$$

Thus N/F is a radical extension.

□

Remark: By Lemma 10.1, to consider a finite separable radical extension, we could instead consider its normal closure, which is Galois.

Definition 10.2 (Solvability by Radicals)**:** Let F be a field and $f(x) \in F[x]$. We say $f(x)$ is solvable by radicals if there exists a radical extension E/F such that $f(x)$ splits over E.

Remark: It is possible that $f(x) \in F[x]$ is solvable by radicals, but its splitting field is not a radical extension (see A10).

Remark: We recall that an expression involving only $+, -, \times, \div, \sqrt[n]{}$ is called a radical expression (this was Definition 1.2). Let F be a field and $f(x) \in F[x]$ be separable. If $f(x)$ is solvable by radicals, by the definition of radical extensions, $f(x)$ has a root given by a radical expression. We call this a radical root. Conversely, if $f(x)$ has a radical root, it must be in some radical extension E/F. By Lemma 10.1, the normal closure N of E/F is radical. Since $f(x)$ splits over N, $f(x)$ is solvable by radicals.

10.2 Radical Solutions

Lemma 10.2: Let E/F be a field extension and let K, L be intermediate fields of E/F. Suppose that K/F is a finite Galois extension. Then KL is a finite Galois extension of L and $\mathrm{Gal}_L(KL)$ is isomorphic to a subgroup of $\mathrm{Gal}_F(K)$.

Proof. Since K/F is a finite Galois extension, K is the splitting field of some $f(x) \in F[x]$ over F whose irreducible factors are separable. Since $F \subseteq L$, KL is the splitting field of $f(x)$ over L, thus Galois. Consider the map

$$\Gamma : \mathrm{Gal}_L(KL) \to \mathrm{Gal}_F(K), \qquad \psi \mapsto \psi\restriction_K .$$

Note that $\psi \in \mathrm{Gal}_L(KL)$ fixed L and thus F. Also, since K is a Galois extension, $\psi(K) = K$. Thus Γ is well-defined. Moreover, if $\psi\restriction_K = 1_K$ then ψ is trivial on K and L. Thus ψ is trivial on KL. This shows that Γ is an injection. Thus $\mathrm{Gal}_L(KL) \cong \mathrm{Im}\,\Gamma$, a subgroup of $\mathrm{Gal}_F(K)$.

□

Definition 10.3 (Galois Groups of Polynomials)**:** Let E/F be the splitting field of a polynomial $f(x) \in F[x]$ whose irreducible factors are separable. The Galois group of $f(x)$ is defined to be $\mathrm{Gal}_F(E)$, denoted by $\mathrm{Gal}(f)$.

Theorem 10.3: Let F be a field with $\mathrm{ch}(F) = 0$ and $f(x) \in F[x] \setminus \{0\}$. Then $f(x)$ is solvable by radicals if and only if its Galois group $\mathrm{Gal}(f)$ is solvable.

Proof.

$\Longleftarrow$ Suppose $G = \mathrm{Gal}(f)$ is solvable. Let E/F be the splitting field of $f(x)$ and $n = |G|$. Let L/E be the splitting field of $x^n - 1$ over E and $\zeta_n \in L$ be a primitive n-th root of unity. Set $K = F(\zeta_n)$ and we have $L = E(\zeta_n) = KE$. Since $L = KE$ and E/F is a finite Galois extension, by Lemma 10.2, L/K is a finite Galois extension and $H = \mathrm{Gal}_K(L)$ is isomorphic to a subgroup of G. By Theorem 6.3, H is solvable. Write

$$H = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_m = \{1\}$$

where $H_i \lhd H_{i-1}$ and $H_{i-1}/H_i \cong C_{d_i}$, a cyclic group of order d_i $(1 \le i \le m)$. Since H is a subgroup of G, we have $d_i \mid n$. Let $K_i = H_i^* = L^{H_i}$ for all $0 \le i \le m$. By Theorem 6.9, we have $\mathrm{Gal}_{K_i}(L) = H_i$ and so we get a tower of fields

$$F \subseteq F(\zeta_n) = K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_m = L = E(\zeta_n).$$

Since $H_i \lhd H_{i+1}$, by Theorem 8.4, K_i/K_{i-1} is Galois and $\mathrm{Gal}_{K_{i-1}}(K_i) \cong H_{i-1}/H_i \cong C_{d_i}$. Since ζ_n is in K_{i-1}, $\zeta_{d_i} = \zeta_n^{n/d_i}$ is in K_{i-1}, and by Theorem 9.2 there exists $\alpha_i \in K_i$ such that

$$K_i = K_{i-1}(\alpha_i) \text{ and } \alpha_i^{d_i} \in K_{i-1}.$$

Moreover, $K_0 = K(F(\zeta_n)$ and $\zeta_n^n = 1 \in F$. It follows that L/F is a radical extension. Since all roots of $f(x)$ are in E, and thus in L, we conclude that $f(x)$ is solvable by radicals.

$\Longrightarrow$ Suppose $f(x)$ is solvable by radicals, i.e. $f(x)$ splits over some extension E/F satisfying $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m = E$ with $F_i = F_{i-1}(\alpha_i)$ and $\alpha_i^{d_i} \in F_{i-1}$ for some $d_i \in \mathbb{N}$. By Lemma 10.1, without loss of generality we can assume E/F is Galois. Thus E/F is the splitting field of some $\tilde{f}(x) \in F[x]$. Let

$$n = \prod_{i=1}^{m} d_i,$$

let L/E be the splitting field of $x^n - 1$ over E and let $\zeta_n \in L$ be a primitive n-th root of unity. Set $K = F(\zeta_n)$ and we have $L = E(\zeta_n) = KE$. Define $K_i = KF_i = F_i(\zeta_n)$, then we have

$$F \subseteq F(\zeta_n) = K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m = F_m(\zeta_n) = L$$

since $F_i = F_{i-1}(\alpha_i)$, we have $K_i = K_{i-1}(\alpha_i)$. Since $\alpha_i^{d_i} \in F_{i-1} \subseteq K_{i-1}$ and $\zeta_{d_i} = \zeta_n^{n/d_i} \in K_{i-1}$, by Theorem 9.2, K_i/K_{i-1} is a cyclic Galois extension. Note that L is the splitting field of $\tilde{f}(x)(x^n - 1)$ over F (also over K_i). Hence L/F (also L/K_i) is Galois. We have

$$G = \mathrm{Gal}_F(L) \supseteq \mathrm{Gal}_{K_0}(L) \supseteq \mathrm{Gal}_{K_1}(L) \supseteq \cdots \supseteq \mathrm{Gal}_{K_m}(L) = \{1\}.$$

Since K_i/K_{i-1} is a Galos extension, by Theorem 8.4, $\mathrm{Gal}_{K_i}(L) \lhd \mathrm{Gal}_{K_{i-1}}(L)$ and we have

$$\mathrm{Gal}_{K_{i-1}}(L)/\mathrm{Gal}_{K_i}(L) \cong \mathrm{Gal}_{K_{i-1}}(K_i),$$

which is cyclic, thus abelian. Also,

$$\mathrm{Gal}_F(L)/\mathrm{Gal}_{K_0}(L) = \mathrm{Gal}_F(L)/\mathrm{Gal}_K(L) \cong \mathrm{Gal}_F(K) = (\mathbb{Z}/n\mathbb{Z})^*$$

is abelian (where in this case $(\mathbb{Z}/n\mathbb{Z})^*$ is the group of units modulo n, not the Galois correspondence). Thus $\mathrm{Gal}_F(L)$ is solvable.

Let $\tilde{E}$ be the splitting field of $f(x)$ which is a subfield of L. Since $\tilde{E}/F$ is a Galois extension, by Theorem 8.4 we have

$$\mathrm{Gal}(f) = \mathrm{Gal}_F(\tilde{E}) \cong \mathrm{Gal}_F(L)/\mathrm{Gal}_{\tilde{E}}(L).$$

Since $\mathrm{Gal}(f)$ isa quotient group of the solvable group $\mathrm{Gal}_F(L)$, by Theorem 6.3, $\mathrm{Gal}(f)$ is solvable.

□

Proposition 10.4: Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of prime degree p. If $f(x)$ contains precisely two normal roots in $\mathbb{C}$, then $\mathrm{Gal}(f) \cong S_p$.

Proof. We recall that the symmetric group S_n can be generated by the cycles $(1\,2)$ and $(1\,2\,3\,\cdots\,n)$. Thus to show $\mathrm{Gal}(f) \cong S_p$, it suffices to find a p-cycle and a 2-cycle in $\mathrm{Gal}(f)$. Since $\deg(f) = p$, by Theorem 6.8, $\mathrm{Gal}(f)$ is a subgroup of S_p. Let α be a root of $f(x)$. Since $f(x)$ is irreducible with degree p, we have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = p$. Thus $p \,|\, |\mathrm{Gal}(f)|$. By Cauchy's theorem this means that there exists an element of $\mathrm{Gal}(f)$ of order p, i.e. a p-cycle. Also, the complex conjugate map $\sigma(a + bi) = a - bi$ will interchange two non-real roots of $f(x)$ and fix all real roots so it is an element of order 2, i.e. a 2-cycle. By changing notation where necessary, we have $(1\,2), (1\,2\,\cdots\,n) \in \mathrm{Gal}(f)$. It follows that $\mathrm{Gal}(f) \cong S_p$. □

Example 10.1: Consider $f(x) = x^5 + 2x^3 - 24x - 2 \in \mathbb{Q}[x]$, which is irreducible by Eisenstein's criterion with $\ell = 2$. Since $f(-1) = 10$, $f(1) = -23$, $\lim_{x\to\infty} f(x) = \infty$ and $\lim_{x\to-\infty} f(x) = -\infty$, by the intermediate value theorem $f(x)$ has at least three real roots. Let $\alpha_1, \cdots, \alpha_5$ be the roots of $f(x)$. By considering the coefficients of x^4 and x^3 in $f(x)$ then we see that

$$\sum_{i=1}^{5} \alpha_i = 0 \text{ and } \sum_{i<j} \alpha_i\alpha_j = 2.$$

From the first sum we have

$$0 = \left(\sum_{i=1}^{5} \alpha_i\right)^2 = \sum_{i=1}^{5} \alpha_i^2 + 2\sum_{i<j} \alpha_i\alpha_j.$$

It follows that $\sum_{i=1}^{5} \alpha_i^2 = -4$. Thus not all the roots of $f(x)$ can be real. Since $f(x)$ has at least three real roots, we conclude that it has exactly three real roots and two non-real roots. By Proposition 10.4, $\mathrm{Gal}(f) \cong S_5$. Since S_5 is not solvable, by Theorem 10.3 the polynomial $x^5 - 2x^3 - 24x - 2$ over $\mathbb{Q}$ is not solvable by radicals.

From the above example, we see a polynomial of degree 5 is not always solvable by radicals. Since $S_5 \subseteq S_n$ for all $n \geq 5$, we get:

Theorem 10.5 (Abel-Ruffini Theorem)**:** A general polynomial $f(x)$ with $\deg(f) \geq 5$ is not solvable by radicals.

Proof. Since A_5 isn't solvable, S_5 isn't a solvable group. Since S_5 is a subgroup of S_n for all $n \geq 5$, S_n isn't solvable for all $n \geq 5$. It follows by Theorem 10.3 that not all polynomials of degree $n \geq 5$ are solvable by radicals in general.

□

Example 10.2: Consider the polynomial

$$x^7 - 2x^4 - 7x^3 + 14 = (x^3 - 2)(x^4 - 7).$$

Even though this polynomial has degree 7, it factors into degree 3 and 4 polynomials which are solvable. Hence it is solvable.

11 Examples of Applications of Galois Theory

11.1 Probabilistic Galois Theory

Theorem 10.5 tells us that not all polynomials of degree ≥ 5 are solvable by radicals. However, we know of many examples that are such cyclotomic polynomials or anything of a form similar to Example 10.2. A natural question then is to ask:

What fraction of the polynomials of degree n are solvable for $n \geq 5$?

Using probabilistic Galois theory (as well as some algebraic number theory) one can show:

"Almost all" polynomials $f(x)$ of degree n satisfy $\mathrm{Gal}(f) \cong S_n$.

More precisely, let

$$E_n(N) = \#\{f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x], |a_i| \leq N, \mathrm{Gal}(f) \subsetneq S_n\}$$

and

$$T_n(N) = \#\{f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x], |a_i| \leq N\}.$$

Then by using a result in algebraic number theory known as the large sieve, Gallagher proved that

$$\lim_{N\to\infty} \frac{E_n(N)}{T_n(N)} = 0.$$

Thus we conclude that for "almost all" (i.e. density 1) polynomials $f(x) \in \mathbb{Z}[x]$ with $\deg(f) = n$, $\mathrm{Gal}(f) \cong S_n$. This is an example of probabilistic Galois theory. It is conjectured that

$$E_n(N) \approx O((2N+1)^{n-1}).$$

11.2 Cyclotomic Extensions

For a prime p, we have seen that the p-th cyclotomic polynomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible in $\mathbb{Q}[x]$. However for a general $n \in \mathbb{N}$ with $n \geq 3$ this is not true. For example,

$$\Phi_4(x) = \frac{x^4 - 1}{x - 1} = (x^2 + 1)(x + 1).$$

Note that

$$\Phi_p(x) = (x - \zeta_p)(x - \zeta_p^2)\cdots(x - \zeta_p^{p-1})$$

where $\zeta_p = e^{2\pi i/p}$. For each $k = 1, 2, \cdots, p$, we have $\gcd(k, p) = 1$. So we can write

$$\Phi_p(x) = \prod_{\substack{1\leq k\leq p \\ \gcd(k,p)=1}} (x - \zeta_p^k).$$

Let $\zeta_n = e^{2\pi i/n}$. For a general $k \in \mathbb{Z}$, the order of ζ_n^k is $\frac{n}{\gcd(n,k)}$. Hence if $\gcd(n, k) = 1$, then the order of ζ_n^k is the same as the order of ζ_n if and only if $\gcd(n, k) = 1$.

Definition 11.1 (The n-th Cyclotomic Polynomial)**:** The n-th cyclotomic polynomial $\Phi_n(x)$ is defined by

$$\Phi_n(x) = \prod_{\substack{1\leq k\leq p \\ \gcd(k,p)=1}} (x - \zeta_n^k)$$

where $\zeta_n = e^{2\pi i/n}$.

Remark: As mentioned above this agrees with Example 2.14 in the case where $n = p$ is prime.

We have the following two theorem from Gauss which we won't prove here:

Theorem 11.1 (Gauss)**:** $\Phi_n(x) \in \mathbb{Z}[x]$ and is irreducible.

Theorem 11.2 (Gauss)**:** We have $\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n)) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

Definition 11.2 (Cyclotomic Extensions)**:** For $n \in \mathbb{N}$ and $k \in \mathbb{Z}$ with $\gcd(k, n) = 1$, the field $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_n^k)$ is called the n-th cyclotomic extension over $\mathbb{Q}$.

Theorem 11.3: Let A be a finite abelian group. Then there exists a Galois extension $E/\mathbb{Q}$ with $E \subseteq \mathbb{Q}(\zeta_n)$ and $\mathrm{Gal}_{\mathbb{Q}}(E) \cong A$.

From this we see that to understand general abelian extensions we can instead examine the cyclotomic extensions.

Lemma 11.4: Let p be a prime and $m \in \mathbb{N}$ with $p \nmid m$. Then for $a \in \mathbb{Z}$, p divides $\Phi_m(a)$ if and only if $p \nmid a$ and $a \pmod p$ has order m in $\mathbb{F}_p^*$, the multiplicative group of $\mathbb{F}_p$.

We recall Euclid's theorem, that there are infinitely many primes. Since there is only one even prime, this means that there are infinitely many odd primes (i.e. primes p of the form $p \equiv 1 \pmod p$).

How about primes of the form $p \equiv 1 \pmod 4$, or $p = 3 \pmod 4$? Are there infinitely many primes of either form?

Remark: The original proof of Euclid's theorem works for $p \equiv 3 \bmod 4$ but not for $p \equiv 1 \bmod 4$.

Question: For any positive integer m, let $k \in \mathbb{Z}$ with $\gcd(k, m) = 1$.
Are there infinitely many primes p of the form $p \equiv k \pmod m$?

Another way to formulate the question is to ask for $f(x) = mx + k$, is the set of prime divisors of the sequence $f(1), f(2), f(3) \cdots$ infinite?

Lemma 11.5: If $f(x) \in \mathbb{Z}[x]$ is monic and $\deg(f) \geq 1$, the set of prime divisors of the non-zero integers in the sequence $f(1), f(2), f(3), \cdots$ is infinite.

Theorem 11.6 (Dirichlet's Theorem)**:** For $m, k \in \mathbb{N}$ with $m \geq 2$ and $\gcd(k, m) = 1$, there are infinitely many primes p such that $p \equiv k \pmod m$.

Remark: It has been proved that $\pi(x) = \#\{p = \text{prime} : p \leq x\} \approx \frac{x}{\log(x)}$

Dirichlet also proved that for $\gcd(k, m) = 1$,

$$\pi(x, k, m) = \#\{p = \text{prime} : p \equiv k \pmod m\} \approx \frac{1}{\psi(m)}\pi(x)$$

where $\psi(m) = \#\{1 \leq k \leq m, \gcd(k, m) = 1\}$ is the Euler-ψ function.