2020/03/15

Contents

Definition 0.0.1.

1. 5 assignments
2. Midterm: Wed, Feb 12, in class
3. Final: Exame, 2.5 hours
4. Final Grades: $0.25Ass, 0.25Mid, 0.5final$

Chapter 1

I

凝視我，别再只看天花，我非你杯茶。
也可盡情地喝吧，别遺忘有人在，為你，聲沙

浮夸，陈奕迅

1.1 Intro

Remark 1.1.1 (Polynomial Equations). We begin with solutions of polynomial equations. Recall the solutions for linear equation $ax + b = 0$ is $x = -\frac{b}{a}$. The solution for quardratic equation $ax^2 + bx + c = 0$ is $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.

Definition 1.1.1. An expression involving any of $+, -, \times, /, \sqrt[n]{}$ is called a ***radical***.

Theorem (Tartaglia, del Fierro, Fontana(1535)). *All cubic equations can be reduced to the following equation*

$$x^3 + px = q$$

A solution of the above equation is of the form

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}$$

Theorem (Fierro). *There exists radical solutions of quartiz equations.*

Remark 1.1.2. In 1799, Ruffini gave a 516 pages proof about the insolvability of quintic equations. His proof was almost correct.

In 1824, Abel filled the gap in Ruffini's proof. His proof was later simplified by Kronecker in 1879.

Remark 1.1.3. However, even as we showed the insolvability of quintic equation, we know there exist quintic equations that has radical solutions.

Therefore, it is natural to ask, given a quintic equation, is it solvable by radicals? This is not a very good question, as we are trying to solve equations one by one.

The reverse question is more useful: Suppose that a radical solution exists, how does its associated quintic equations look like?

Remark 1.1.4 (Two main steps of Galois Theory)**.**

1. Link a root of a polynomial equation, say α, and the smallest field $\mathbb{Q}(\alpha)$ containing $\mathbb{Q}$ and α.
   Note $\mathbb{Q}(\alpha)$ is a field, so it has more structures to be played with than α.
   However, our knowledge about $\mathbb{Q}(\alpha)$ is still too little to answer the question. For example, we do not know how many intermediate field E between $\mathbb{Q}$ and $\mathbb{Q}(\alpha)$, i.e. $\mathbb{Q} \subseteq E \subseteq \mathbb{Q}(\alpha)$.
2. Link the field $\mathbb{Q}(\alpha)$ to a group. More precisely, we associate the field extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ to the group

$$Aut_{\mathbb{Q}}(\mathbb{Q}(\alpha)) = \{\phi : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha) : \phi \in Aut(\mathbb{Q}(\alpha)), \phi|_{\mathbb{Q}} = 1\}$$

   It can shown that if α is algebraic, then $Aut_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ is finite.
   If α is constructible, the order of $Aut_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ is in certain forms.

Moreover, there is a 1 to 1 correspondence between the intermediate fields of $\mathbb{Q}(\alpha)/\mathbb{Q}$ and the subgroups of $Aut_{\mathbb{Q}}(\mathbb{Q}(\alpha))$.

Remark 1.1.5 (Galois Theory)**.** The interplay between fields and groups.

Definition 1.1.2. A ***commutative ring*** with 1 (or ring) is a set R with addition and multiplication such that $(R, +)$ is an abelian group with identity 0. For multiplication, $(R, *)$ is commutative with identity 1 and associative. Also, $r(s+t) = rs+rt$ for all $r, s, t \in R$.

Remark 1.1.6. In this course, a ring is always commutative and unital.

Definition 1.1.3. Let R be a ring. An element $r \in R$ is a unit if it is invertible.

Definition 1.1.4. A ***field*** is a ring R in which every element is an unit.

Definition 1.1.5. A ring R is an ***integral domain*** if for all $a, b \in R$, $ab = 0 \Rightarrow a = 0 \vee b = 0$. Viz, it has no zero divisors.

Example 1.1.1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ are all fields.

Theorem. *Every subring of a field is an integral domain.*

Definition 1.1.6. An ***ideal*** of a ring R is a subset I containing 0 such that for all $a, b \in I$ and $r \in R$, we have $a - b \in I$ and $ra \in I$.

Example 1.1.2. The only ideals of a field is 0 and itself.

Definition 1.1.7. An integral domain R is a ***principle ideal domain*** (PID) if every ideal can be generated by one element.

Example 1.1.3. The set of integers $\mathbb{Z}$ is an integral domain. The units of $\mathbb{Z}$ are $\{1, -1\}$.

Remark 1.1.7 (Division Algorithm)**.** Recall from 145... Using this, we can show that an ideal of $\mathbb{Z}$ is of the form $\langle n \rangle$. Thus $\mathbb{Z}$ is a PID.

Remark 1.1.8. Consider all fields containing $\mathbb{Z}$. Their intersection (the smallest field containing $\mathbb{Z}$) is the set of rational numbers $\mathbb{Q}$.

Definition 1.1.8. We say a polynomial is monic if the leading coefficient is 1. We should know what the degree of a polynomial is... In this course, the degree of 0 is $-\infty$.

Example 1.1.4. Let F be a field, define $F[x]$ to be all of the polynomials in F. Then $F[x]$ is integral domain and PID. In addition, the units in $F[x]$ is $F^\times = F \backslash \{0\}$.

We remark that the intersection of all fields containing $F[x]$ is the set of rational (polynomial) functions:

$$F(x) = \left\{ \frac{f(x)}{g(x)} : f, g \in F[x], g \neq 0 \right\}$$

Definition 1.1.9. Recall what a quotient ring is...

Example 1.1.5. $\mathbb{Z}/\langle n \rangle \cong \mathbb{Z}_n$. $F[x]/\langle f(x) \rangle$ is the set of polynomials with degree less than $f(x)$.

Theorem. *Recall first isomorphism theorem for rings.*

Example 1.1.6. Let F be a field and S be a ring, consider homomorphism $\phi : F \to S$. Since the only ideals of F is 0 or F, ϕ is either 0 or injective.

Definition 1.1.10. An ideal I in a ring R is ***maximal*** if $I \neq R$ and there is no ideal J with $I \subsetneq J \subsetneq R$.

Definition 1.1.11. An ideal I is ***prime*** if $I \neq R$ and $ab \in I$ imply $a \in I$ or $b \in I$.

Remark 1.1.9. Every maximal ideal is prime. In PID, every prime is maximal. In (left) Artinian ring, every prime is maximal.

Example 1.1.7. In $\mathbb{Z}$, $\langle n \rangle$ is maximal (prime) iff n is prime.

In $F[x]$, $\langle f(x) \rangle$ is maximal(prime) iff $f(x)$ is irreducible.

Theorem. *I is maximal iff R/I is field. I is prime iff R/I is integral domain.*

Chapter 2

Field Theory

Penser l'impossible avant tout
Brûler nos prisons dorées
Oser l'utopie jusqu'au bout
Seuls les fous nous ont fait avancer

Penser l'impossible from Mozart
l'Opéra Rock

2.1 Intro

Definition 2.1.1. If E is a field containing field F, we say E is a ***field extension*** of F, denoted by E/F.

Remark 2.1.1. Note when we talk about fields, quotient rings are not very useful (F only have two ideals). So it should not cause confusion about quotients and field extensions.

Remark 2.1.2. If E/F is a field extension, we can view E as a vector space over F as follows:

1. $e_1, e_2 \in E$ then $e_1 + e_2 = e_1 + e_2$,
2. $k \in F, e_1 \in E$ then $ke_1 = ke_1$.

Definition 2.1.2. The ***degree*** of E/F is the dimension of E as vector space over F, denoted by $[E : F]$. Moreover, if $[E : F]$ is finite, we say E/F is a ***finite extension***, otherwise, we say it is an ***infinite extension***.

Example 2.1.1. We have

1. $[\mathbb{C} : \mathbb{R}] = 2$ is a finite extension,
2. $[\mathbb{R} : \mathbb{Q}]$ is a infinite extension,

3. Let F be a field, then $[F(x) : F]$ is an infinite extension as $\{x^i : i \in \mathbb{N}\}$ is linear independent.

Theorem 1 (Theorem 1). *If E/K and K/F are finite extensions, then E/F is finite extension and*

$$[E : F] = [E : K] \cdot [K : F]$$

In particular, if K is an intermediate field of a finite extension E/F, then $[K : F] \mid [E : F]$. We remark this also holds for infinite extension.

Proof. Suppose $[E : K] = m$ and $[K : F] = n$. Let $\{a_1, ..., a_m\}$ be a basis of E/K and $\{b_1, ..., b_n\}$ be a basis of K/F. It suffices to prove

$$\beta = \{a_i b_j : 1 \leq i \leq m, 1 \leq j \leq n\}$$

is a basis of E/F.

Claim: $span(\beta) = E$.

Note $E \supseteq span(\beta)$ is trivial. For $e \in E$, we have $e = \sum k_i a_i$ where $k_i \in K$. Thus each $k_i = \sum f_{ij} b_j$ and so $e \in span(\beta)$ as desired. Thus $E = span(\beta)$. This is the end of the claim.

Claim: β is linear independent.

Suppose

$$\sum_{i,j} c_{ij} a_i b_j = 0$$

where $c_{i,j} \in F$. Note $\sum_j c_{i,j} b_j \in K$ and since $a_1, ..., a_m$ are linear independent, we must have $\sum_j c_{i,j} b_j = 0$ for all $1 \leq i \leq m$.

Hence, each $c_{i,j} = 0$ as $b_1, ..., b_n$ are linear independent.

Thus β is indeed linear independent and so E/F is finite extension and in particular $[E : F] = m \cdot n = [E : K] \cdot [K : F]$ and the proof follows. ♡

Definition 2.1.3. Let E/F is a field extension and $\alpha \in E$. We say α is ***algebraic over*** F if there exists $f(x) \in F[x] \backslash \{0\}$ with $f(\alpha) = 0$. Otherwise, we say α is ***transcedental over*** F.

Example 2.1.2. We have $c/d \in \mathbb{Q}$, $\sqrt{2}$, $7 + 2i$ are algebraic over $\mathbb{Q}$. We have e, π are transcedental.

Definition 2.1.4. Let E/F be a field extension and $\alpha \in E$, let $F[\alpha]$ denote the smallest subring of E containing F and α. In addition, $F(\alpha)$ denote the smallest subfield of E containing F and α.

Similarly, we have $F[\alpha_1, ..., \alpha_n]$ and $F(\alpha_1, ..., \alpha_n)$ are defined the same way.

Definition 2.1.5. If $E = F(\alpha)$ for some $\alpha \in E$, then we say E is a ***simple extension*** of F.

Remark 2.1.3. The degree of the simple extension $F(\alpha)/F$ is either infinite or finite. In this section, we will show that this depends on if α is transcedental or algebraic.

2.2 Finite Extensions

Definition 2.2.1. Let R and R' be two rings which contain a field F. A ring homomorphism $\phi : R \to R'$ is said to be a ***F-homomorphism*** if $\phi|_F = 1_F$.

Theorem 2 (Theorem 2). *Let E/F be a field extension and $\alpha \in E$. If α is transcedental over F then $F[\alpha] \cong F[x]$ and $F(\alpha) \cong F(x)$. In particular, $F[\alpha] \ncong F(\alpha)$.*

Proof. Let $\psi : F(x) \to F(\alpha)$ be the unique F-homomorphism defined by $\psi(x) = \alpha$. Thus for $f(x), g(x) \in F[x]$ with $g(x) \neq 0$, we have $\psi(\frac{f}{g}) = \frac{f(\alpha)}{g(\alpha)}$. Note that α is transcedental so $g(\alpha) \neq 0$. Thus the map is well-defined. Note $Ker(\psi)$ is an ideal of a field, so it is either zero or the whole thing. However, $\psi(x) = \alpha$, so the kernel cannot be the whole thing. Thus ψ is injective. Also, since $F(x)$ is a field, $Im(\psi)$ contains a field generated by F and α, i.e. $F(\alpha) \leq Im(\psi)$, we have $Im(\psi) = F(\alpha)$ and ψ is surjective. It follows that ψ is an isomorphism and we have $F(\alpha) \cong F(x)$ and $F[\alpha] \cong F[x]$. ♡

Theorem 3 (Theorem 3). *Let E/F be a field extension and $\alpha \in E$. If α is algebraic over F, there exists a unique monic irreducible polynomial $p(x) \in F[x]$ such that there exists a F-isomorphism $\psi : F[x]/\langle p(x)\rangle \to F[\alpha]$ with $\psi(x) = \alpha$, from which we conclude $F[\alpha] = F(\alpha)$.*

Proof. Consider the unique homomorphism $\phi : F[x] \to F[\alpha]$ defined by $\phi(x) = \alpha$. Thus for $f(x) \in F[x]$, we have $\phi(f) = f(\alpha) \in F[\alpha]$. Since $F[x]$ is a ring, $Im(\phi)$ contains a ring generated by F and α, i.e. $F[\alpha] \subseteq Im(\phi)$. Thus $Im(\phi) = F[\alpha]$. Let $I = Ker(\phi)$, since α is algebraic, $I \neq \{0\}$. Then, we have $F[x]/I \cong Im(\phi)$, a subring of a field $F(\alpha)$. Thus $F[x]/I$ is an integral domain and I is a prime ideal. It follows that $I = \langle p(x)\rangle$ with $p(x)$ irreducible. If we assume $p(x)$ to be monic, then it is unique and it follows that $F[x]/\langle p(x)\rangle \cong F[\alpha]$.

Since $p(x)$ is irreducible, $F[x]/\langle p(x)\rangle$ is a field, thus $F[\alpha]$ is a field and hence $F[\alpha] \cong F(\alpha)$. ♡

Definition 2.2.2. If α is algebraic over a field F, the unique monic irreducible polynomial $p(x)$ in Thm 3 is called the ***minimal polynomial*** of α over F.

Remark 2.2.1. From the proof of theorem 3, we see that if $f(x) \in F[x]$ with $f(\alpha) = 0$, then $p(x) \mid f(x)$.

As a consequence of Thm 2 and 3, we have the following:

Theorem 4 (Theorem 4). *Let E/F be a field extension and $\alpha \in E$, then*

1. *α is transcedental over F iff $[F(\alpha):F]$ is infinity,*
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 $\{1,\alpha^1,...,\alpha^{deg(p)-1}\}$ is a basis of $F(\alpha)/F$.

Proof. It suffices to prove ($\Rightarrow$) for (1) and (2).

(1), ($\Rightarrow$): From Thm 2, if α is transcedental over F, $F(\alpha)\cong F(x)$. In $F(x)$, the elements $\{1,x,x^2,...\}$ are linearly independent over F, thus $[F(\alpha):F]$ is ∞.

(2), ($\Rightarrow$): From Thm 3, if α is algebraic over F, $F(\alpha)\cong F[x]/\langle p(x)\rangle$ with $x\mapsto\alpha$. Note that $F[x]/\langle p(x)\rangle=\{r(x)\in F[x]:deg(r)<deg(p)\}$. Thus $\{1,...,x^{deg(p)-1}\}$ is a basis of $F[x]/\langle p(x)\rangle$ and it follows that $[F(\alpha):F]$ is $deg(p)$ and $\{1,\alpha,...,\alpha^{deg(p)-1}\}$ is a basis of $F(\alpha)$ over F. ♡

Theorem 5 (Theorem 5). *Let E/F be a field extension with $[E:F]<\infty$. Then there exists $\alpha_1,...,\alpha_n\in E$ such that*

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

Proof. We use induction on $[E:F]$. If $[E:F]=1$, $E=F$ and we are done. Suppose it holds for all field extension with degree less than $[E:F]$. Let $\alpha\in E\backslash F$, by Thm 1, we have $[E:F]=[E:F(\alpha_1)]\cdot[F(\alpha_1):F]$. Since $[F(\alpha_1):F]>1$, we have $[E:F(\alpha_1)]<[E:F]$ as $[F(\alpha_1):F]>1$. Thus, by induction hypothesis, there exists $\alpha_2,...,\alpha_n$ such that $F(\alpha_1)\subsetneq ...\subsetneq F(\alpha_1,...,\alpha_n)=E$. Thus

$$F\subsetneq F(\alpha_1)\subsetneq ...\subsetneq E$$

♡

Definition 2.2.3. A field extension E/F is ***algebraic*** if every $\alpha\in E$ is algebraic over F. Otherwise, it is transcedental.

Theorem 6 (Theorem 6). *Let E/F be a field extension. If $[E:F]$ be finite, then E/F is algebraic.*

Proof. Suppose $[E:F]=n$. For $\alpha\in E$, the elements $\{1,\alpha,...,\alpha^n\}$ are not linear independent over F. Thus there exists $c_i\in F$, not all zero, that vanishes α^i, i.e.

$$\sum_{i=0}^{n}c_i\alpha^i=0$$

Thus α is root of the polynomial $f(x)=\sum_{i=0}^{n}c_ix^i\in F[x]$, thus algebraic over F. ♡

Theorem 7 (Theorem 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. We need to show it is a field. Let $\alpha, \beta \in L$, if we can show $\alpha \pm \beta, \alpha \cdot \beta, \alpha/\beta \in L$ where if the last case we assume $\beta \neq 0$.

By definition of L, we have $[F(\alpha) : F] < \infty$ and $[F(\beta) : F] < \infty$. Consider $F(\alpha, \beta)$, since the minimal polynomial of α 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. $p(x) \in F(\beta)[x]$ such that $p(\alpha) = 0$), we have $[F(\alpha, \beta) : F(\beta)] \leq [F(\alpha) : F]$, combining this with Thm 1,

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

Since $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in F(\alpha, \beta)$, they are in L. ♡

Definition 2.2.4. Let E/F be a field extension. The set

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

is called the ***algebraic closure*** of F over E.

Definition 2.2.5. A field F is ***algebraically closed*** if for any algebraic extension E/F, we have $E = F$.

Example 2.2.1. By the fundamental theorem of algebra, we have $\mathbb{C}$ is algebraically closed. Moreover, $[\mathbb{C} : \mathbb{R}] = 2$ with $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$ in $\mathbb{C}$.

2.3 Eisenstein's Criterion

Definition 2.3.1. Let $f(x) = \sum_{i=0}^{n} a_i x^n \in \mathbb{Z}[x]$, we say $f(x)$ is ***primitive*** if $a_n > 0$ and the coefficients have no common integer factor except for ± 1.

Lemma 2.3.1. *Every non-zero polynomial $f(x) \in \mathbb{Q}[x]$ can be written uniquely as a product $f(x) = cf_0(x)$ where $f_0(x)$ is primitive and $c \in \mathbb{Q}$. Moreover, $f(x) \in \mathbb{Z}[x]$ iff $c \in \mathbb{Z}$.*

Lemma 2.3.2 (Gauss's Lemma(Ez version))**.** *Let $f(x) \in \mathbb{Z}[x]$ be non-constant. If $f(x)$ is irreducible in $\mathbb{Z}$ then it is irreducible in $\mathbb{Q}$.*

Example 2.3.1. The converse of the above result is not true. Consider $2x + 8 = 2(x + 4)$, which is reducible in $\mathbb{Z}[x]$ but not in $\mathbb{Q}[x]$.

The constant 2 in the above example is the only obstruction between irreducibility of $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$. More precisely, $f(x) \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$ if and only if, either $f(x)$ is a prime integer or $f(x)$ is primitive and irreducibility in $\mathbb{Q}[x]$.

Definition 2.3.2. An integral domain R is a ***unique factorization domain*** (UFD) if every non-zero, non-unit can be uniquely written as a product of irreducibles in R, upto reordering and associates.

Example 2.3.2.

1. Let $R = \mathbb{Z}$, then $30 = 2 \cdot 3 \cdot 5 = 3 \cdot 5 \cdot 2 = (-3) \cdot 5 \cdot (-2)$.

2. Note field imply UFD.

Theorem. *Let R be UFD, every irreducible is prime.*

Proof. Let $p \in R$ be irreducible, thus, $0 \neq p$ and $p \notin R^\times$. Let $x, y \in R$ such that $p \mid xy$. Thus, $xy = pz$ for $z \in R$. By uniqueness in UFD, p must be an associate of an irreducible factor of x or y. Without lose of generality, say $p = uq$ where $u \in R^\times$ and q is an irreducible factor of x. Then $u^{-1}p = q$ which imply $p \mid q$ and since $q \mid x$, we have $p \mid x$. ♡

Definition 2.3.3. Let R be a ring, we say R is Noetherian if whenever $I_1 \subseteq I_2 \subseteq I_3 \subseteq ...$ is a chain of ideals of R, there exists $N \in \mathbb{N}$ such that $I_k = I_N$ for $k \geq N$.

Example 2.3.3. Consider the ring $R = \mathbb{C}[x_1, x_2, x_3, ...]$ be the collection of all finite polynomials with countable many variables. Then, we have $\langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset \langle x_1, x_2, x_3 \rangle ...$ and so R is not Noetherian.

Lemma 2.3.3. *Every PID is Noetherian.*

Proof. Suppose R is a PID, let $I_1 \subseteq I_2 \subseteq ...$ be a chain of ideals of R. Then, $\bigcup_{i=1}^{\infty} I_i = I$ is an ideal of R. Say $I = \langle a \rangle$ where $a \in R$ as R is PID. Thus, there exists $N \in \mathbb{N}$ such that $a \in I_n$, which imply $I \subseteq I_N$. Thus $I_k = I_N = I$ for all $k \geq N$. ♡

Theorem. *Every PID is UFD.*

Proof. Let R be a PID. Let $r \in R$ be non-zero such that $p \notin R^\times$.

We will show existence first. If r is irreducible then we are done. Otherwise, $r = r_1 r_2$ where $r_1, r_2 \notin R^\times$. If r_1 and r_2 are irreducible, we are done. Otherwise, we have r_1 or r_2 is not irreducible. Without lose of generality, r_1 is not irreducible. Thus $r_1 = r_{11} r_{12}$ where $r_{11}, r_{12} \notin R^\times$. Continuing in this way, $\langle r \rangle \subset \langle r_1 \rangle \subset \langle r_{11} \rangle \subset ...$ Since R is Noetherian, this process must terminate. Hence, we indeed have a factorization of irreducibles of p.

We then show uniqueness. We proceed by induction on the number of irreducible factors of r, say induction on n. Say $r = p_1 ... p_n = q_1 ... q_m$ where p_i, q_j are irreducibles. Since R is PID, p_1 is irreducible if and only if p_1 is prime. Thus $p_1 \mid q_1 ... q_m$. Without lose of generality, suppose $p_1 \mid q_1$, and thus $q_1 = p_1 u$ where $u \in R$. Since q_1 is irreducible and $p_1 \notin R^\times$, we have $u \in R^\times$. Hence, $r = p_1 ... p_n = u p_1 q_2 q_3 ... q_m$. Inductively, $p_2, ..., p_n$ and $q_2, ..., q_m$ must be the same up to ordering and associates. Moreover, since p_1 and q_1 are associates, we are done. ♡

Definition 2.3.4. Let R be an integral domain, let $X = \{(a, b) : a, b \in R, b \neq 0\}$. Define a relation on X by $(a, b) \sim (c, d)$ if and only if $ad = bc$. For each $(a, b) \in X$, let $\frac{a}{b} := \{x \in X : x \sim (a, b)\}$. Then let F denote the set of distinct sets of the form $\frac{a}{b}$, we obtained F is a field with the operation $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ and $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$, and is called ***field of fractions of R***.

Theorem (Gauss's lemma)**.** *Let R be UFD, let F be the field of fractions of R. Let $f(x) \in R[x]$. If $f(x) = A(x)B(x)$ for some non-constant $A(x), B(x) \in F[x]$, then there exists $a(x), b(x) \in R[x]$ such that*

1. *$deg(A) = deg(a), deg(B) = deg(b)$*
2. *and $f(x) = a(x)b(x)$.*

Proof. Suppose $f(x) = A(x)B(x)$ as in the theorem. Then, multiple through by a common denominator $0 \neq d \in R$ for all the coefficients of $A(x)$ and $B(x)$, we obtain $df(x) = \alpha(x)\beta(x)$ where $\alpha(x), \beta(x) \in R[x]$. If d is a unit in R, we are done as $a(x) = d^{-1}\alpha(x), b(x) = \beta(x)$ would be the claimed polynomials in $R[x]$. Thus, assume $d \notin R^\times$, then $d = p_1...p_n$ where $1 \leq i \leq n$ and p_i is irreducible as R is UFD. Note in UFD, we have irreducible imply prime, so $\langle p_i \rangle$ is prime ideal for $1 \leq i \leq n$. Thus, $(R/\langle p_i \rangle)[x]$ is integral domain as $R/\langle p_i \rangle$ is integral domain. Thus, mod $df(x) = \alpha(x)\beta(x)$ by p_i, we have $0 = \overline{\alpha(x)} \cdot \overline{\beta(x)}$ in $(R/\langle p_i \rangle)[x]$. Hence, we must have $p_i \mid \alpha(x)$ or $p_i \mid \beta(x)$ as $(R/\langle p_i \rangle)[x]$ is integral domain and we must have either $\overline{\alpha(x)} = 0$ or $\overline{\beta(x)} = 0$. Say $p_i \mid \alpha(x)$, then we can cancel p_i from both side of the equation $df(x) = \alpha(x)\beta(x)$ in $R[x]$. Start with 1 and continue this process, we can cancel all of the factors of d on the left hand side of $df(x) = \alpha(x)\beta(b)$ and so $f(x) = a(x)b(x)$ as desired. In particular, we note $a(x), b(x)$ are $F-$multiples of $A(x), B(x)$, respectively, i.e. $\exists u, v \in F$ so $a(x) = uA(x)$ and $b(x) = vB(x)$. ♡

Corollary. *Let R be UFD and F be the field of fraction of R.*

1. *If $f(x) \in R[x]$ is reducible over F then $f(x)$ is reducible over R.*
2. *If f is irreducible and non-constant in $R[x]$ then $f(x)$ is irreducible in $F[x]$.*

Theorem 8 (Theorem 8)**.** *Let $f(x) = a_n x^n + ... + a_0 \in \mathbb{Z}[x]$ and let p be a prime. Suppose that $p \nmid a_n$ and $p \mid a_i$ for $0 \leq i < n$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}[x]$.*

In particular, if $f(x)$ is primitive, then f is irreducible in $\mathbb{Z}[x]$.

Proof. Consider the map $\mathbb{Z}[x] \mapsto \mathbb{Z}_p[x]$ by $f(x) \mapsto \overline{f}(x) = \overline{a_n}x^n + ... + \overline{a_0} \pmod{p}$. Since $p \nmid a_n$ and $p \mid a_i$ for $0 \leq i \leq n-1$, we have $\overline{f(x)} = \overline{a_n}x^n$. If $f(x)$ is reducible in $\mathbb{Q}[x]$, then it can be factored in $\mathbb{Z}[x]$ into non-constant polynomials, say $f(x) = g(x)h(x)$. It follows $\overline{a_n}x^n = \overline{g}(x)\overline{h}(x)$. Since $\mathbb{Z}_p[x]$ is a UFD, from which we see that $\overline{g}(x) = bx^m$ and $\overline{h}(x) = cx^k$ for some $b, c \in \mathbb{Z}_p$. In other words, $\overline{g}$ and $\overline{h}$ have 0 constant in $\mathbb{Z}_p$.

Since the constant of both g and h are divisible by p, this implies that the constant of $f(x)$ is divides by p^2, which is a contradiction. ♡

Example 2.3.4.

1. The polynomial $2x^7 + 3x^4 + 6x^2 + 12$ is irreducible in $\mathbb{Q}[x]$.
2. Let p be a prime, let $\zeta_p = e^{\frac{2\pi i}{p}} = \cos(2\pi/p) + i \cdot \sin(2\pi/p)$ be a p-th root of 1. It is a root of the pth cyclotomic polynomial

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

Eisenstein's Criterion does not apply here. However, consider $\Phi_p(x+1) = x^{p-1} + \sum_{i=1}^{p-1} \binom{p}{i} x^{p-1-i} \in \mathbb{Z}[x]$. Since p is a prime, $p \nmid 1$ and $p \mid \binom{p}{i}$ and $p^2 \nmid \binom{p}{p-1}$. By Eisenstein's Criterion, we have $\Phi_p(x+1)$ is irreducible in $\mathbb{Q}[x]$ and this imply $\Phi_p(x)$ is also irreducible in $\mathbb{Q}[x]$. Since $\Phi_p(x)$ is primitive, $\Phi_p(x)$ is also irreducible in $\mathbb{Z}[x]$.

3. Let p be a prime and $\zeta_p = e^{\frac{2\pi i}{p}}$. Since ζ_p is a root of the p-th cyclotomic polynomial $\Phi_p(x)$, which is irreducible. Then by Thm 3 and 4, $\Phi_p(x)$ is the minimal polynomial of ζ_p and $[\mathbb{Q}[\zeta_p] : \mathbb{Q}] = p - 1$. The field $\mathbb{Q}(\zeta_p)$ is called ***p-th cyclotomic extension*** of $\mathbb{Q}$.
4. Let $\overline{Q}$ be the algebraic closure of $\mathbb{Q}$ over $\mathbb{C}$. Since $\zeta_p \in \overline{\mathbb{Q}}$, we have $[\overline{\mathbb{Q}} : \mathbb{Q}] \geq [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ and since $p \to \infty$, we have $[\mathbb{Q}(\zeta_p) : \mathbb{Q}]$ is infinite. We have seen in Thm 6 that if E/F is finite then E/F is algebraic, now we see the converse is not true.

Remark 2.3.1. Now, let R be a UFD and F be the field of fraction. Let $f(x) \in R[x]$ be non-constant, then $R[x]$ is a subring of $F[x]$ and Eisenstein's Criterion holds with R and F.

Theorem 9 (Eisenstein's Criterion)**.** *Let R be a UFD with field of fraction F. Let ℓ be an irreducible element of R. If $f(x) = a_n x^n + ... + a_0 \in R[x]$ with $n \geq 1$ and if $\ell \nmid a_n, \ell \mid a_i$ for $0 \leq i \leq n-1$ and $\ell^2 \nmid a_0$, then $f(x)$ is irreducible in $F[x]$.*

In particular, if $f(x)$ is primitive, then $f(x)$ is irreducible in $R[x]$.

2.4 Splitting Fields

Definition 2.4.1. Let E/F be a field extension, we say $f(x) \in F(x)$ ***splits over*** E if E contains all roots of $f(x)$. In another words, $f(x)$ is a product of linear factors in $E[x]$.

Definition 2.4.2. Let $\tilde{E}/F$ be a field extension, $f(x) \in F[x]$ and $F \subseteq E \subseteq \tilde{E}$. If $f(x)$ splits over E and there is no proper subfield of E such that $f(x)$ splits over, then we say E is a ***splitting field of*** $f(x) \in F[x]$ ***in*** $\tilde{E}$.

Theorem 10 (Theorem 10)**.** *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 maximal. Thus $E = F[x]/I$ is a field. Consider the homomorphism $\psi : F \to E$ via $a \mapsto a + I$. Since F is a field and ψ is not zero, ψ must be injective and hence identifying F with $\psi(F)$, we have F is a subfield of E.

We note $\alpha = x + I \in E$ will be a root of $p(x)$. Indeed, say $p(x) = \sum_{i=0}^{n} (a_i + I) x^i \in E[x]$, we have $p(\alpha) = (a_0 + I) + (a_1 + I)(x + I) + ... + (a_n + I)(x + I)^n = p(x) + I = 0$. ♡

Theorem 11 (Theorem 11(Kronecker))**.** *Let $f(x) \in F[x]$, there exists a field E containing F such that $f(x)$ splits over E.*

Proof. We use induction on degree of the polynomial. If $deg(f) = 1$ then just take $E = F$ and we are done. Assume it holds for all polynomials (not necessarily in $F[x]$) with degree less than n and $deg(f) = n > 1$.

Write $f(x) = p(x)h(x)$ where both $p(x), h(x) \in F[x]$ and $p(x)$ is irreducible. By Thm 10, 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 $f(x) = (x-\alpha)q(x)h(x)$ and since $deg(qh) < deg(f)$, by induction there exists a field E containing K which $h(x)q(x)$ splits. It follows that $f(x)$ splits over E. ♡

Theorem 12 (Theorem 12). *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 Thm 11, there exists a field extension E/F over which $f(x)$ splits. Say $\alpha_1, ..., \alpha_n$ are roots of $f(x)$ in E. Consider $F(\alpha_1, ..., \alpha_n)$, this field contains all roots of $f(x)$ and $f(x)$ does not split over any proper subfield of it. Thus $F(\alpha_1, ..., \alpha_n)$ is the splitting field of $f(x)$ in E. In addition, since α_i are all algebraic, $F(\alpha_1, ..., \alpha_n)/F$ is a finite extension. ♡

Remark 2.4.1. If we change E/F to a different field extension, say E_1/F, what is the relation between the splitting field of $f(x)$ in E and in E_1?

Definition 2.4.3. Let $\phi : R \to R_1$ be a ring homomorphism and $\Phi : R[x] \to R_1[x]$ be the unique homomorphism satisfying $\Phi|_R = \phi$ and $\Phi(x) = x$. In this case, we say Φ ***extends*** ϕ.

More generally, if $R \leq S$ and $R_1 \leq S_1$, and $\Phi : S \to S_1$ is a ring homomorphism with $\Phi|_R = \phi$, we say Φ extends ϕ.

Theorem 13 (Theorem 13). *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 the splitting field of $f(x)$ and f_1 respectively. Then, there exists an isomorphism $\psi : E \to E_1$ which extends ϕ.*

Proof. We prove this theorem by induction on the $[E : F]$. 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 $E = F$ and $E_1 = F_1$. Take $\phi = \Phi$ and we are done.

Suppose that $[E : F] > 1$ and the result holds for all field extension E'/F' with $[E' : F'] < [E : F]$.

Let $p(x) \in F[x]$ be an irreducible factor of $f(x)$ with degree $deg(p) \geq 2$ and let $p_1(x) = \Phi(p(x))$ (such $p(x)$ exists as if all irreducible factors of $f(x)$ are 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. By Thm3, we have an F-isomorphism $F(\alpha) \cong F[x]/\langle p(x)\rangle$ that sends α to $x + \langle p(x)\rangle$. Similarly, there is an F_1-isomorphism $F_1(\alpha_1) \cong F_1[x]/\langle p_1(x)\rangle$.

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 $\tilde{\Phi} : F[x]/\langle p(x)\rangle \to F_1[x]/\langle p_1(x)\rangle$ with $x + \langle p(x)\rangle \mapsto x + \langle p_1(x)\rangle$ which extends ϕ. It follows that there exists a field isomorphism $\tilde{\phi} : F(\alpha) \to F_1(\alpha_1)$ which extends ϕ with $\alpha \mapsto \alpha_1$. Note that since $deg(p) \geq 2$, we have $[E : F(\alpha)] < [E : F]$. Since E (respectively E_1) is the splitting field of $f(x) \in F(\alpha)[x]$ (respectively $f_1(x) \in F_1(\alpha_1)[x]$), by induction, there exists $\psi : E \to E_1$ which extends $\tilde{\phi}$. So, ψ extends ϕ. ♡

Corollary 14 (Corollary 14). *Two splitting fields of $f(x) \in F[x]$ over F are F-isomorphic. Thus we can say **the** splitting field of $f(x)$ over F.*

Proof. Let $\phi : F \to F$ be the identity map and apply Thm 13. ♡

Theorem 15 (Theorem 15). *Let F be a field and $f(x) \in F[x]$ with degree $deg(f) = n \geq 1$. If E/F is the splitting field of $f(x)$, then $[E : F] \mid n!$.*

Proof. We use induction on $deg(f)$. If $deg(f) = 1$, choose $E = F$ and $[E : F] \mid 1$.

Suppose $deg(f) > 1$ and the statement holds for all $g(x)$ with $deg(g) < deg(f)$. Note $g(x)$ is not necessarily in $F[x]$. Then consider two cases:

Case One: If $f(x) \in F[x]$ is irreducible and $\alpha \in E$ is a root of $f(x)$, then by Thm 3, $F(\alpha) \cong F[x]/\langle f(x)\rangle$ and $[F(\alpha) : F] = deg(f) = n$. Write $f(x) = (x-\alpha)g(x)$ 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 we have $[E : F(\alpha)] \mid (n-1)!$. Since $[E : F] = [E : F(\alpha)] \cdot [F(\alpha) : F]$, we have $[E : F] \mid n!$ as desired.

Case Two: If $f(x)$ is not irreducible, $f(x) = g(x)h(x)$ with $g(x), h(x) \in F[x]$. Say $deg(g) = m, deg(h) = k$ where $1 \leq m, k < n$ and $n = m + k$. Let K be the splitting field of $g(x)$ over F. Since $deg(g) = m < n$, by induction we have $[K : F] \mid m!$. Since E is the splitting field of $h(x)$ over K and $deg(h) = k < n$, by induction we have $[E : K] \mid k!$. Thus $[E : F] \mid k!m!$ where $m!k! \mid n!$ since $\frac{n!}{m!k!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}$ is an integer. ♡

2.5 Field Expert I

Definition 2.5.1. If F is a field, then the ***prime field*** of F is the intersection of all subfields of F.

Theorem 16 (Theorem 16). *If E is a field, then its prime field is isomorphic to $\mathbb{Q}$ or $\mathbb{Z}_p$ for some prime p.*

Proof. Consider $\chi : \mathbb{Z} \to F$ by $n \mapsto n$. Let $I = Ker(\chi)$ be the kernel of χ. Then $\mathbb{Z}/I \cong Im(\chi)$. Note $Im(\chi)$ is an integral domain as it is a subring of a field, we have I is a prime ideal. Now consider two cases.

Case One: If $I = \langle 0 \rangle$, then $\mathbb{Z} \subseteq F$ and since F is a field, $\mathbb{Q} = Frac(\mathbb{Z}) \subseteq F$.

Case Two: If $I = \langle p \rangle$, then $\mathbb{Z}_p = \mathbb{Z}/\langle p \rangle \cong Im(\chi) \subseteq F$. ♡

Definition 2.5.2. Given a field F, if it's prime field is isomorphic to $\mathbb{Q}$ (respectively $\mathbb{Z}$), we say F has characteristic 0 (respectively p), denoted by $char(F) = ch(F) = 0$ (respectively p).

Remark 2.5.1. Note if $char(F) = p$ then $p = 0$ in that field. Also, note if $char(F) = p$, then $(a + b)^p = a^p + b^p$.

Proposition 17 (Proposition 17). *Let F be a field with $ch(F) = p$ and let $n \in \mathbb{N}$. Then, the map $\phi : F \to F$ given by $v \mapsto v^p$ is an injective $\mathbb{Z}_p$-homomorphism of fields(when we think F as module of $\mathbb{Z}_p$). If F is finite, then ϕ is $\mathbb{Z}_p$-isomorphism of F.*

Definition 2.5.3. If F is a field, the monomials $\{1, x, x^2, ...\}$ for an F-basis of $F[x]$. Define a linear operator $D : F[x] \to F[x]$ by $D(1) = 0$ and $D(x^n) = nx^{n-1}$ for $n \in \mathbb{N}$, then extend by linearity. This is called the ***formal derivative***.

Remark 2.5.2. Note $D(f + g) = D(f) + D(g)$, $D(fg) = D(f)g + fD(g)$. We sometimes call $D(f)$ to be f'.

Theorem 18 (Theorem 18). *Let F be a field and $f(x) \in F[x]$:*

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

Proof. (1): ($\Leftarrow$) is clear.

(1): ($\Rightarrow$): Say $f(x) = \sum_{i=0}^{n} a_i x^i$, then $f'(x) = a_1 + 2a_2x + ... + na_nx^n = 0$ imply $ia_i = 0$ for $1 \leq i \leq n$. Since $ch(F) = 0$, we have $a_i = 0$ for all $1 \leq i \leq n$. Thus $f(x) = a_0$ for $a_0 \in F$.

(2): ($\Leftarrow$): Write $g(x) = b_0 + b_1x + ... + b_mg^m$. Then $f(x) = g(x^p)$ imply $f'(x) = pb_1x^1 + ... + mpb_mx^{pm-1}$ and since $ch(F) = p$, we have $f'(x) = 0$.

(2): ($\Rightarrow$): For $f(x) = \sum_{i=0}^{n} a_i x^i$, we have $f'(x) = \sum_{i=1}^{n} ia_ix^{i-1} = 0$ imply $ia_i = 0$ and so $a_i = 0$ unless $p \mid i$ for all $1 \leq i \leq n$. Thus $f(x) = a_0 + a_px^p + a_{2p}x^{2p} + ... + a_{mp}x^{mp}$ and if we define $g(x) = a_0 + a_px + a_{2p}x^2 + ... + a_{mp}x^m$ then we are done. ♡

Definition 2.5.4. Let E/F be a field extension and $f(x) \in F[x]$, we say $\alpha \in E$ is a repeated root of $f(x)$ if $f(x) = (x - \alpha)^2 \cdot g(x)$ for some $g(x) \in E[x]$.

Theorem 19 (Theorem 19). *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 nad f' (in the field extension E).*

Proof. ($\Rightarrow$): Suppose $f(x) = (x-\alpha)^2 g(x)$. Then $f'(x) = 2(x-\alpha)g(x)+(x-\alpha)^2 g'(x)$ and so α divides both f and f' as desired.

($\Leftarrow$): Suppose $(x-\alpha)$ divides both $f(x)$ and $f'(x)$. Write $f(x) = (x-\alpha)h(x)$, $h(x) \in E[x]$. Then $f'(x) = h(x) - (x-\alpha)h'(x)$. Since $f'(\alpha) = 0$ as $(x-\alpha)$ divides $f'(x)$, we have $h(\alpha) = 0$. Thus $(x-\alpha)$ is a factor of $h(x)$ and so $f(x) = (x-\alpha)^2 g(x)$ for some $g(x) \in E[x]$. ♡

Corollary 20 (Corollary 20). *Let F be a field, $f(x) \in F[x]$. Then $f(x)$ has no repeated root in any extension of F if and only if $gcd(f, f') = 1$.*

Proof. Note $gcd(f, f') \neq 1$ if and only if $(x-\alpha) \mid gcd(f, f')$ for some α in some extension of F. ♡

Remark 2.5.3. We remark that in Corollary 20, our condition of repeated roots depends on the extension of F while the gcd condition involves only F.

2.6 Field Expert II

Proposition 21 (Proposition 21). *If F is a finite field, then $ch(F) = p$ for some non-zero prime number p. Moreover, $|F| = p^n$ for some $n \in \mathbb{N}$.*

Proof. Since F is a finite field, by Thm 16, its prime field is $\mathbb{Z}_p$. Since F is a finite dimension vector space over $\mathbb{Z}_p$, we have $F \cong \mathbb{Z}_p^n$ for some $n \in \mathbb{N}$. Hence $|F| = p^n$. ♡

Theorem 22 (Theorem 22). *Let F be a field, let G be a finite subgroup of $F^\times := F\backslash\{0\}$. Then G is a cyclic group. In particular, if F is a finite field, then $F^\times$ is a cyclic group.*

Proof. WLOG, assume $G \neq \langle 1 \rangle$. Since G is finite abelian group, we have $G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \mathbb{Z}_{n_3} \times ... \times \mathbb{Z}_{n_r}$ where $n_1 > 1$ and $n_1 \mid n_2 \mid ... \mid n_r$. This follows from Fundamental Theorem of Finitely Generated Modules over PID (plz check my 446 notes QAQ).

Since $n_r(\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \mathbb{Z}_{n_3} \times ... \times \mathbb{Z}_{n_r}) = 0$, it follows that for every $v \in G$, is a root of $x^{n_r} - 1 = 0$.

Since the polynomial $x^{n_r} - 1$ has at most n_r distinct roots in F, this imply the size of the group G must be at most n_r, i.e. we have $r = 1$ and $G \cong \mathbb{Z}_{n_r}$. The proof follows. ♡

Corollary 23 (Corollary 23). *If F is a finite field, then F is a simple extension of $\mathbb{Z}_p$, i.e. $F = \mathbb{Z}_p(u)$.*

Proposition 24 (Proposition 24).

1. *Let p be a prime number and $n \in \mathbb{N}$, then F is a finite field with $|F| = p^n$ if and only if F is the splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$.*
2. *Let F be finite field with $|F| = p^n$ for some $n \in \mathbb{N}$. Let $m \in \mathbb{N}$ be such that $m \mid n$, then F contains a unique subfield K with $|K| = p^m$.*

Proof. (1): ($\Rightarrow$): Suppose $|F| = p^n$, then $|F^\times| = p^n - 1$. Thus every element in $F^\times$ satisfies $u^{p^n-1} - 1 = 0$, thus it is a root of $x(x^{p^n-1} - 1) = x^{p^n} - x$. Since $0 \in F$ is a root of $x^{p^n} - x$ as well, the polynomial $x^{p^n} - x$ has p^n distinct roots in F, i.e. F is the splitting field of $x^{p^n} - x$.

(1) : ($\Leftarrow$) : Suppose F is the splitting field of $f(x) = x^{n^p} - x$. Since $char(F) = p$ we have $f'(x) = -1$. Since $gcd(f, f') = 1$, by Corollary 20, $f(x)$ has p^n distinct roots in F. Let E be the set of all roots of $f(x)$ in F. Let $\phi : F \to F$ given by $\phi(u) = u^{p^n}$. For $u \in F$, u is a roto of $f(x)$ if and only if $\phi(u) = u$. Since the condition is closed under addition, subtraction, multiplication and division, E is a subfield of F of order p^n which contains $\mathbb{Z}_p$ (since all $u \in \mathbb{Z}_p$ satisfy $u^p = u$ and thus $u^{p^n} = u$).

Since F is the splitting field of $f(x)$, it is generated over $\mathbb{Z}_p$ by the roots of $f(x)$, i.e. the elements in E. Thus $F = \mathbb{Z}_p(E) = E$.

(2): Observe that $x^{ab} - 1 = (x^a - 1)(x^{ab-a} + x^{ab-2a} + ... + x^a + 1)$. Thus, if $n = mk$, then

$$\begin{aligned} x^{p^n} - x &= x(x^{p^n-1} - x) \\ &= x(x^{p^m-1} - 1)g(x) \\ &= (x^{p^m} - x)g(x) \end{aligned}$$

for some $g(x) \in \mathbb{Z}_p[x]$. Since $x^{p^n} - x$ splits over F, so does $x^{p^m} - x$. Let $K = \{v \in F : v^{p^m} - v = 0\}$, 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 of F with $|\tilde{K}| = p^m$ then $\tilde{K} \subseteq K$ (as $\tilde{K}$ will be the splitting field of $x^{p^m} - x$). Thus $\tilde{K} = K$. ♡

Corollary 25 (Corollary 25, E.H.Moore)**.** *Let p be a prime and $n \in \mathbb{N}$. Then any two finite field of order p^n are isomorphic. We denote such a field F by $\mathbb{F}_{p^n}$.*

Proof. Follows from Proposition 24 and Corollary 14. ♡

Definition 2.6.1. Let F be a field and $0 \neq f(x) \in F[x]$. If $f(x)$ is irreducible, we say $f(x)$ is ***separable over*** F if it has no repeated root in any extension of F. In general, we say $f(x)$ is separable over F if each irreducible factor of $f(x)$ is separable over F.

Example 2.6.1.

1. $f(x) = (x - 4)^9$ is separable in $\mathbb{Q}[x]$.
2. Consider $f(x) = x^n - a \in F[x]$ with $n \geq 2$. If $a = 0$, the only irreducible factor of $f(x)$ is x. Since $gcd(x, x') = 1$, we have $f(x)$ is separable. Now assume $a \neq 0$, then $f'(x) = nx^{n-1}$. Thus the only irreducible factor of $f'(x)$ is x, provided that $n \neq 0$.

Now, if $ch(F) = 0$, since $x \nmid f(x)$, we have $gcd(f, f') = 1$ and so $f(x)$ is separable.
If $ch(F) = p$ and $gcd(n, p) = 1$, since $x \nmid f(x)$, then $gcd(f, f') = 1$ and so $f(x)$ is separable.
If $ch(F) = p$ and $p \mid n$. In this case we consider $f(x) = x^p - a$. Since $f'(x) = 0$, we have $gcd(f, f') \neq 1$. However, it is still possible that all irreducible factors $l(x)$ of $f(x)$ has the property that $gcd(l, l') = 1$. To decide if $f(x)$ is separable, we need to find its irreducible factors.
First, define $F^p = \{b^p : b \in F\}$, which is a subfield of F. If $a \in F^p$, say $a = b^p$ for some $b \in F$, then $f(x) = x^p - b^p = (x - b)^p$, which is separable.
Suppose $a \notin F^p$, then we claim $f(x) = x^p - a$ is irreducible in $F[x]$.
Write $x^p - a = g(x)h(x)$ where $g(x), h(x)$ are monic polynomials. Let E/F be an extension where $x^p - a$ has a root, say $\beta \in E$, i.e. $\beta^p - a = 0$. Note $\beta \notin F$ since $a = \beta^p \notin F^p$. We have $x^p - a = x^p - \beta^p = (x - \beta)^p$, hence $g(x) = (x - \beta)^r$ and $h(x) = (x - \beta)^s$ for some $r, s \in \mathbb{N} \cup \{0\}$ and $r + s = p$. Write $g(x) = x^r - r\beta x^{r-1} + ...$, then $r\beta$ must be in F as $g(x) \in F[x]$. Since $\beta \notin F$, we must have $r = 0$. Thus, as an integer, we have either $r = 0$ or $r = p$. Hence, it follows that one of $g(x)$ or $h(x)$ must be equal to 1 in $F[x]$ and so $f(x)$ is irreducible as desired.
Since $f(x)$ is irreducible and $f(x) = (x-\beta)^p \in E[x]$, it is not separable. In this case, since all roots of $f(x)$ are the same, we say $f(x)$ is purely inseparable.

2.7 Perfect Field Expert

Definition 2.7.1. A field F is ***perfect*** if every irreducible polynomial $r(x) \in F[x]$ is separable over F.

Theorem 26. *Let F be a field,*

1. *If $ch(F) = 0$, then F is perfect,*
2. *if $ch(F) = p$ and $F^p = F$, then F is perfect.*

Proof. 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 for a contradiction. Then by Corollary 20, $gcd(r, r') \neq 1$. Thus $r'(x) = 0$.

If $ch(F) = 0$, from Theorem 18(1), $r'(x) = 0 \Leftrightarrow r(x) = c \in F$. A contradiction since $deg(r) \geq 1$. Thus $r(x)$ is separable and F is perfect.

If $ch(F) = p$, from Theorem 18(2), $r'(x) = 0$ imply that $r(x) = a_0 + a_1x^p + ... + a_mx^{pm} \in F[x]$. Since $F = F^p$, we can write $a_i = b_i^p$ with $b_i \in F$. Thus $r(x) = b_0^p + ... + b_m^p x^{pm} = (b_0 + b_1x + ... + b_mx^m)^p$. This is a contradiction as $r(x)$ is irreducible. Thus $r(x)$ is separable and F is perfect. ♡

Remark 2.7.1. Let $ch(F) = p$, and $F^p \neq F$, for example, $F = \mathbb{F}_p(x)$. If we take $a \in F \backslash F^p$, then $x^p - a$ is purely inseparable. Thus $ch(F) = p$, then F is perfect if and only if $F^p = F$.

Corollary 27. *Every finite field is perfect.*

Proof. Every finite field $F = \mathbb{F}_p$ is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$ for some priem p and $n \in \mathbb{N}$. Thus for every $a \in F$, we have $a = a^{p^n} = (a^{p^{n-1}})^p$ and since $a^{p^{n-1}} \in F$, we have $F = F^p$. Hence by Theorem 26 we have F is perfect. ♡

Chapter 3

Group Theory

始まってしまった物語に流して来た悲しみに
今終わりを告げるため命を懸けたクルセイダース
宿命のラストページにその怒りを叩きこめ
end of THE WORLD その血の記憶

ジョジョその血の記憶

3.1 The Sylow Theorem

Definition 3.1.1. An ***action*** of a group G on a set S is a function $G \times S \to S$ (usually denoted by $(g, x) \mapsto gx$) such that for all $x \in S$ and $g_1, g_2 \in G$, we have $ex = x$ and $(g_1 g_2)x = g_1(g_2 x)$.

Definition 3.1.2. Let G acts on S, for $x \in S$, we denote the ***orbit*** of x to be $\overline{X}$, i.e.

$$\overline{x} := \{gx : g \in G\}$$

Also, we denote G_x to be the ***stablizer*** of $x \in S$, i.e.

$$G_x := \{g \in G : gx = x\}$$

We denote $C_G(x)$ to be the ***centralizer*** of $x \in G$, i.e.

$$C_G(x) := \{g \in G : gxg^{-1} = x\}$$

We denote $Z(G)$ to be the ***center*** of G, i.e.

$$Z(G) := \{g \in G : \forall x \in G, gxg^{-1} = x\}$$

We denote $N_G(H)$, where $H \leq G$, to be the ***normalizer*** of H, i.e.

$$N_G(H) := \{g \in G : gHg^{-1} = H\}$$

In particular, the normalizer is always normal.

Remark 3.1.1. One should recall

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(x_i)]$$

where $x_i \in G \backslash Z(G)$ are distinct representatives, i.e. $\overline{x_i}$ are the distinct conjugacy classes of G with at least two elements.

Lemma 28. *Let H be a group of order p^n where p is prime, which acts on a finite set S. Let*

$$S_0 := \{x \in S : \forall h \in H, hx = x\}$$

Then we have $|S| \equiv |S_0| \pmod{p}$

Proof. For $x \in S$, $|\overline{x}| = 1$ if and only if $x \in S_0$. Thus S can be written as a disjoint union $S = S_0 \cup \overline{x_1} \cup ... \cup \overline{x_m}$ where $|\overline{x_i}| > 1$.

Thus

$$|S| = |S_0| + |\overline{x_1}| + ... + |\overline{x_m}|$$

Since $|\overline{x_i}| > 1$ and $|\overline{x_i}| = [H : Hx_i]$ divides $|H| = p^n$, we have $p \mid |\overline{x_i}|$ for each i. It follows that $|S| \equiv |S_0| \pmod{p}$. ♡

Theorem 29 (Cauchy). *Let p be a prime and G a finite group. If $p \mid |G|$, then G contains an element of order p.*

Proof. Define $S = \{(a_1, a_2, ..., a_p) : a_i \in G, a_1 a_2 ... a_p = e\}$. Since a_p is uniquely determined by $a_1, ..., a_{p-1}$, if $|G| = n$ we have $|S| = n^{p-1}$. Since $p \mid n$, we have $|S| \equiv 0 \pmod{p}$.

Let the group $\mathbb{Z}_p$ acts on S by cyclic permutation, i.e. for $k \in \mathbb{Z}_p$, we have

$$k(a_1, ..., a_p) = (a_{k+1}, a_{k+2}, ..., a_p, a_1, ..., a_k)$$

One should check this action is well-defined. Also, $(a_1, ..., a_p) \in S_0$ if and only if $a_1 = a_2 = ... = a_p$. Clearly $(e, e, ..., e) \in S_0$ and hence $|S_0| \geq 1$. By Lemma 28, we have $|S_0| \equiv |S| \equiv 0 \pmod{p}$.

Since $|S_0| \geq 1$ and $|S_0| \equiv 0 \pmod{p}$, we have $|S_0| \geq p$ and hence there exists $a \neq e$ such that $(a, ..., a) \in S_0$, which imply $a^p = e$. ♡

Definition 3.1.3. Let p be a prime. A group in which every element has order a non-negative power of p is called p-***group***.

Corollary 30. *A finite group G is a p-group if and only if $|G|$ is a power of p.*

Lemma 31. *The center $Z(G)$ of a non-trivial finite p-group G contains more than 1 elements.*

Proof. Since G is a p-group, hence $|G|$ is a power of p. Now, observe by class equation we have

$$|G| = |Z(G)| + \sum [G : C_G(x_i)]$$

with $[G : C_G(x_i)] > 1$. Since $|G|$ is a power of p, we have $[G : C_G(x_i)] \mid |G|$, i.e. $p \mid [G : C_G(x_i)]$. Therefore, we must have $p \mid |Z(G)|$ where $|Z(G)| \geq 1$, i.e. $Z(G) \geq p$. ♡

Remark 3.1.2 (Midterm)**.** Check the handout.

Lemma 32. *Let $H \leq G$. If H is a p-group by itself, then*

$$[N_G(H) : H] \equiv [G : H] \pmod{p}$$

Proof. Let S be a set of all left cosets of H in G and let H act on S by left multiplication. Then $|S| = [G : H]$.

For $x \in G$, we have

$$\begin{aligned} xH \in S_0 &\Leftrightarrow \forall h \in H, hxH = xH \\ &\Leftrightarrow \forall h \in H, x^{-1}hxH = H \\ &\Leftrightarrow x^{-1}Hx = H, \quad \text{as above equality holds for all } h \\ &\Leftrightarrow x \in N_G(H) \end{aligned}$$

Hence S_0 is the number of cosets xH with $x \in N_G(H)$, i.e. $|S_0| = [N_G(H) : H]$. By Lemma 28, we know

$$[N_G(H) : H] \equiv |S_0| \equiv |S| \equiv [G : H] \pmod{p}$$

♡

Corollary 33. *If H is a p-subgroup of a finite group G with $p \mid [G : H]$, then $N_G(H) \neq H$.*

Proof. Since $p \mid [G : H]$, by Lemma 32, we have $[N_G(H) : H] \equiv [G : H] \equiv 0 \pmod{p}$. Since $p \mid [N_G(H) : H]$ and $[N_G(H) : H] \geq 1$, we have $[N_G(H) : H] \geq p$. Hence $N_G(H) \neq H$. ♡

Theorem 34 (First Sylow Theorem)**.** *Let G be a group of order $p^n \cdot m$, where p is a prime, $n \geq 1$ and $gcd(p, m) = 1$. Then G contains a subgroup of order p^i for $1 \leq i \leq n$ and every subgroup of G of order p^i is normal in some subgroup of order p^{i+1} for $1 \leq i < n$.*

Proof. We prove this theorem by induction. For $i = 1$, since $p \mid |G|$, by Theorem 29 G has an element of order p. This asserts the base case.

Suppose it holds for all value less than or equal to i. Hence, there exists a subgroup of order p^i. Then $p \mid [G : H]$. We have seen in the proof of Corollary 33 that $p \mid [N_G(H) : H]$ and $[N_G(H) : H] \geq p$. Then by Thm 29, $N_G(H)/H$ contains a subgroup of order p.

Such a group is of the form H_1/H where H_1 is a subgroup of $N_G(H)$ containing H by correspondence theorem. Since $H \trianglelefteq N_G(H)$ we have $H \trianglelefteq H_1$. Finally, $|H_1| = |H| \cdot |H_1/H| = p^i \cdot p = p^{i+1}$. ♡

Definition 3.1.4. A subgroup P of a group G is said to be a ***Sylow p-subgroup*** if P is a maximal p-group of G, i.e. $P \subseteq H \subseteq G$ with H be a p-group, then $P = H$ or $H = G$.

Corollary 35. *Let G be a group of order $p^n m$ with p prime, $n \geq 1$ and $gcd(p, m) = 1$. Let H be a p-subgroup of G, then*

1. *H is a Sylow p-subgroup if and only if $|H| = p^n$*
2. *Every conjugate of a Sylow p-subgroup is a Sylow p-subgroup*
3. *If there is only one Sylow p-subgroup P then P is normal*

Theorem 36 (Second Sylow Theorem)**.** *If H is a p-subgroup of a finite group G and P is any Sylow p-subgroup of G, then there exists $g \in G$ such that $H \subseteq gPg^{-1}$. In particular, any two Sylow p-subgroup of G are conjugate.*

Proof. Let S be the set of all left coset of P in G and let H act on S be left multiplication. By Lemma 28, we have $|S_0| \equiv |S| \equiv [G : P] \pmod{p}$. Since $p \nmid [G : P]$, we have $|S_0| \neq 0$. Thus there exist $xP \in S_0$ for some $x \in G$. Note that $xP \in S_0$ if and only if $hxP = xP$ for all $h \in H$ if and only if $x^{-1}hxP = P$ for all $h \in H$ if and only if $x^{-1}Hx \subseteq P$ if and only if $H \subseteq xPx^{-1}$.

If H is a Sylow p-group, then $|H| = |P| = |xPx^{-1}|$. Thus $H = xPx^{-1}$. ♡

Theorem 37 (Third Sylow Theorem)**.** *If G is a finite group and p is a prime, then the number of Sylow p-group of G divides $|G|$ and is of the form $kp + 1$ for some $k \in \mathbb{Z}_{\geq 0}$.*

Proof. By Thm 36, the number of Sylow p-subgroup of G is the number of conjugate of any one of them, say P. This number is $[G : N_G(P)]$, which is a divisor of $|G|$.

Let S be the set of all Sylow p-subgroups of G and let P act on S by conjugation. Then $Q \in S_0$ if and only if $xQx^{-1} = Q$ for all $x \in P$. The latter condition holds if

and only if $P \subseteq N_G(Q)$. Both P and Q are Sylow p-subgroup of G and hence they are Sylow p-subgroup of $N_G(Q)$ as well.

Thus by Corollary 35, they are conjugate in $N_G(Q)$. Since $Q \trianglelefteq N_G(Q)$, this can only occur if $Q = P$. Thus $S_0 = \{P\}$ and by Lemma 28, $|S| \equiv |S_0| \equiv 1 \pmod{p}$ and so $|S| = kp + 1$. ♡

Remark 3.1.3. Suppose G is a group with $|G| = p^n m$ and $gcd(p, m) = 1$. Let n_p be the number of Sylow p-subgroups of G. By the Third Sylow Theorem (Thm 37) we have $n_p \mid p^n m$ and $n_m \equiv 1 \pmod{p}$. Since $p \nmid n_p$ we have $n_p \mid m$.

Example 3.1.1. We claim every group of order 15 is cyclic.

Let G be a group of order $15 = 3 \cdot 5$, let n_p be the number of Sylow p-group of G. By the third Sylow theorem, we have $n_3 \mid 5$ and $n_3 \equiv 1 \pmod{3}$, i.e. $n_3 = 1$. Similarly, we have $n_5 \mid 3$ and $n_5 \equiv 1 \pmod{5}$. Thus $n_5 = 1$.

It follows that there is only one Sylow 3-subgroup and Sylow 5-subgroup of G, say P_3 and P_5 respectively. Then $P_3 \trianglelefteq G$ and $P_5 \trianglelefteq G$. Consider $|P_3 \cap P_5|$, which divides 3 and 5. Thus $|P_3 \cap P_5| = 1$, also $|P_3 P_5| = 15 = |G|$, it follows

$$G \cong P_3 \times P_5 \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$$

Example 3.1.2. There are two isomorphism classes of group of order 21.

Let G be a group of order $21 = 3 \cdot 7$. Let n_p be the number of Sylow p-group of G. By the third Sylow theorem, we have $n_3 \mid 7$ and $n_3 \equiv 1 \pmod{3}$. Thus $n_3 = 1$ or 7. Also $n_7 \mid 3$ and $n_7 \equiv 1 \pmod{7}$. Thus $n_7 = 1$. It follows that G has a unique Sylow 7-group. Say P_7.

Note $P_7 \trianglelefteq G$ and P_7 is cyclic, say $P_7 = \langle x \rangle$ with $x^7 = 1$. Let H be a Sylow 3-group. Since $|H| = 3$, H is cyclic and $|H| = \langle y \rangle$ with $y^3 = 1$.

Since $P_7 \trianglelefteq G$, we have $yxy^{-1} = x^i$ for some $0 \leq i \leq 6$. It follows that $x = y^3 x y^{-3} = y^2 x^i y^{-1} = x^{i^3}$. Since $x^7 = 1$ we have $1 \equiv i^3 \pmod{7}$. Since $0 \leq i \leq 6$ we have $i = 1, 2, 4$. Now we need to consider three cases.

If $i = 1$, then $yxy^{-1} = x \Rightarrow xy = yx$. Thus G is abelian and hence $G \cong \mathbb{Z}/\langle 21 \rangle$.

If $i = 2$ then $yxy^{-1} = x^2$. Hence $G = \{x^i y^j : 0 \leq i \leq 6, 0 \leq j \leq 2, yxy^{-1} = x^2\}$. Note this group is $\mathbb{Z}_7 \rtimes \mathbb{Z}_3$ and it is the smallest non-abelian group of odd order.

If $i = 4$ then $yxy^{-1} = x^4$. Note that $y^2 x y^{-2} = y x^4 y^{-1} = x^{16} = x^2$. Note that y^2 is also a generator of H, thus by replacing y by y^2 we are back to case 2.

It follows there are only two classes of group of order 21.

3.2 Solvable Groups

Definition 3.2.1. A group G is ***solvable*** if there exists a tower

$$G = G_0 \geq G_1 \geq ... \geq G_m = \{1\}$$

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

Remark 3.2.1. Note G_{i+1} is not necessarily a normal subgroup of G.

Example 3.2.1. Consider S_4. Let A_4 be the alternating subgroup of S_4 and $V = \mathbb{Z}_2 \times \mathbb{Z}_2$ be the Klein 4 group. Then, we have

$$S_4 \geq A_4 \geq V \geq \{1\}$$

and satisfying the solvable condition.

Theorem (Second Isomorphism Theorem)**.** *If H and N are subgroups of G with $N \trianglelefteq G$, then*

$$H/(N \cap H) \cong NH/N$$

Theorem. *If H and N are both normal subgroups of G such that $N \subseteq H$, then $H/N \trianglelefteq G$ and*

$$(G/N) \Big/ (H/N) \cong G/H$$

Theorem 38.

1. *If G is solvable then every subgroup and every quotient group of G are solvable.*
2. *If N is a normal subgroup of G and both N and G/N are solvable then G is solvable. In particular, a direct product of finitely many solvable groups is solvable.*

Proof. (1): Suppose that G is a solvable group with a tower $G = G_0 \geq G_1 \geq G_2 \geq ... \geq G_m = \{1\}$ where $G_{i+1} \trianglelefteq G_i$ and G_i/G_{i+1} is abelian.

Claim (1.1): Let H be a subgroup of G, then H is solvable.

Define $H_i = H \cap G_i$. Since $G_{i+1} \trianglelefteq G_i$, we have a tower

$$H = H_0 \geq H_1 \geq ... \geq H_m = \{1\}$$

with $H_{i+1} \trianglelefteq H_i$. Note that both H_i and G_{i+1} are subgroups of G_i and $H_{i+1} = H \cap G_{i+1} = H_i \cap G_{i+1}$. Now, apply the second isomorphism theorem to G_i, we have $H_i/H_{i+1} = H_i/(H_i \cap G_{i+1}) \cong H_iG_{i+1}/G_{i+1}$ where H_iG_{i+1}/G_{i+1} is a subgroup of G_i/G_{i+1}, hence abelian. Viz, H is solvable. The proof of the claim follows.

Claim (1.2): Let N be normal subgroup of G, then G/N is solvable.

Consider the tower

$$G = G_0N \geq G_1N \geq ... \geq G_mN = N$$

Then we have

$$G/N = G_0N/N \geq G_1N/N \geq ... \geq G_mN/N = \{1\}$$

Since $G_{i+1} \trianglelefteq G_i$ and $N \trianglelefteq G$, we have $G_{i+1}N \trianglelefteq G_iN$ which imply $G_{i+1}N/N \trianglelefteq G_iN/N$. By third isomorphism theorem, we have

$$G_iN/N \Big/ G_{i+1}N/N \cong G_iN/G_{i+1}N$$

By the second isomorphism theorem, we have

$$G_iN/G_{i+1}N \cong G_i/(G_i \cap G_{i+1}N)$$

However, note $G_{i+1} \subseteq (G_i \cap G_{i+1}N)$, there is a natural injection $G_i/(G_i \cap G_{i+1}N) \to G_i/G_{i+1}$ given by $g + (G_i \cap G_{i+1}N) \mapsto g + G_{i+1}$. Since G_i/G_{i+1} is abelian, so is $G_i/(G_i \cap G_{i+1}N)$. Thus $(G_iN/N)/(G_{i+1}N/N)$ is abelian and so G/N is solvable. The proof of the claim follows.

(2): Since N is solvable we have a tower $N = N_0 \geq N_1 \geq ... \geq N_m = \{1\}$ with $N_{i+1} \trianglelefteq N_i$ and N_i/N_{i+1} is abelian. For a subgroup $H \subseteq G$ with $N \subseteq H$, we denote $\overline{H} = H/N$. Since G/N is solvable, we have a tower $G/N = \overline{G} = \overline{G_0} \geq \overline{G_1} \geq \overline{G_2} \geq ... \geq \overline{G_r} = N/N = \{\overline{1}\}$ with $\overline{G_{i+1}} \trianglelefteq \overline{G_i}$ and $\overline{G_{i+1}}/\overline{G_i}$ is abelian.

Let $Sub_N(G)$ denote the subgroup of G containing N. Consider the map $\sigma : Sub_N(G) \to Sub_{\langle\overline{1}\rangle}(G/N)$ via $H \mapsto H/N$.

For $i = 0, 1, ..., r$, define $G_i = \sigma^{-1}(\overline{G_i})$. Since $N \trianglelefteq G$ and $\overline{G_{i+1}} \trianglelefteq \overline{G_i}$ we have $G_{i+1} \trianglelefteq G_i$.(Exercise)

Moreover, by the 3rd isomorphism theorem we have $G_i/G_{i+1} \cong \overline{G_i}/\overline{G_{i+1}}$. It follows that we have a tower $G = G_0 \geq G_1 \geq ... \geq G_r = N = N_0 \geq N_1 \geq ... \geq N_m = \{1\}$ with $G_{i+1} \trianglelefteq G_i$, $N_{i+1} \trianglelefteq N_i$ and G_i/G_{i+1}, N_i/N_{i+1} all abelian. Thus G is solvable. ♡

Example 3.2.2. We have S_4 contains subgroups isomorphic to S_3 and S_2. Since S_4 is solvable, we have S_3 and S_2 are.

Definition 3.2.2. A group G is ***simple*** if it is not trivial and has no normal subgroup except G and $\{1\}$.

Example 3.2.3. One can show that A_5 is simple. Since $A_5 \geq 1$ is the only tower and $A_5/\{1\}$ is not abelian, A_5 is not solvable. Thus by Thm 38, S_5 is also not solvable. Moreover, since for $n \geq 5$, all S_n contains S_5 we have S_n is not solvable for $n \geq 5$.

Corollary 39. *G is finite solvable group iff there exists a tower $G = G_0 \geq G_1 \geq ... \geq G_m = \{1\}$ with $G_{i+1} \trianglelefteq G_i$ and G_i/G_{i+1} is a cyclic group of prime order for each i.*

3.3 Automorphism Groups

Definition 3.3.1. Let E/F be a field extension. If ψ is an automorphism of E and $\psi|_F = 1_F$, we say ψ is an ***F-automorphism of*** E.

Remark 3.3.1. We see F-automorphism of E forms a subgroup of automorphism group of E.

Definition 3.3.2. We call the group $Aut_F(E) := \{F\text{-Automorphism of } E\}$ to be the ***automorphism group of*** E/F.

Lemma 40. *Let E/F be a field extension, $f(x) \in F[x]$ and $\psi \in Aut_F(E)$. If $\alpha \in E$ is a root of $f(x)$ then $\psi(\alpha)$ is a root of $f(x)$.*

Proof. Say $f = \sum_{i=0}^{n} a_i x^i$. We have

$$f(\psi(\alpha)) = \sum a_i \psi(\alpha)^i = \sum \psi(a_i \alpha^i) = \psi(\sum a_i \alpha^i) = \psi(0) = 0$$

♡

Lemma 41. *Let $E = F(\alpha_1, ..., \alpha_n)$, for $\phi_1, \phi_2 \in Aut_F(E)$, if $\phi_1(\alpha_i) = \phi_2(\alpha_i)$ then $\phi_1 = \phi_2$.*

Proof. Note for $\alpha \in E$, we have

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

where $f, g \in F[x_1, ..., x_n]$. Thus the lemma follows. ♡

Corollary 42. *If E/F is a finite extension then $Aut_F(E)$ is finite.*

Proof. Since E/F is a finite extension, by Thm 5 we have $E = F(\alpha_1, ..., \alpha_n)$ where α_i are algebraic over F. For $\phi \in Aut_F(E)$, by Lemma 40, we must have $\phi(\alpha_i)$ is a root of the minimal polynomial of α_i.

Thus it has only finitely many choices. By Lemma 41, since $\phi \in Aut_F(E)$ is completely determined by $\phi(\alpha_i)$, there are only finitely many choices of ϕ and $|Aut_F(E)| < \infty$. ♡

Remark 3.3.2. The converse of the above corollary is false. For example, $\mathbb{R}/\mathbb{Q}$ is an infinite extension but one can show $Aut_{\mathbb{Q}}(\mathbb{R}) = \{1\}$ as $\mathbb{Q}$ is dense in $\mathbb{R}$.

Definition 3.3.3. Let F be a field and $f \in F[x]$. The ***automorphism group of*** $f(x)$ ***over*** F is $Aut_F(E)$ where E is the splitting field of F.

Remark 3.3.3. Recall that

Theorem 43. *Let $0 \neq f \in F[x]$ and E be splitting field of f. We have $|Aut_F(E)| \leq [E : F]$ and equality holds iff $f(x)$ is separable.*

Proof. Immediate by assignment. ♡

Example 3.3.1. Let F be a field with $ch(F) = p$ and $F^p \neq F$. Let $f(x) = x^p - a$ with $a \in F \backslash F^p$. Let E/F be the splitting field of $f(x)$, we have seen before that $f(x) = (x-b)^p$ for some $b \in E/F$. Thus $E = F(b)$. Since b can only map to b, we have $Aut_F(E)$ is trivial while $|Aut_F(E)| = 1 \neq [E : F] = p$.

Theorem 44. *If $f(x) \in F[x]$ has n distinct roots in the splitting field E, then $Aut_F(E)$ is isomorphic to a subgroup of the Symmetric group S_n. In particular, $|Aut_F(E)|$ divides $n!$.*

Proof. Let $X = \{\alpha_1, ..., \alpha_n\}$ be distinct roots of $f(x)$ in E. By Lemma 40, if $\phi \in Aut_F(E)$ then $\phi(X) = X$. Let $\phi|_X$ be the restriction of ϕ to X and S_X be the permutation of X. Then, the map $\phi \mapsto \phi|_X$ is a group homomorphism. Moreover, by Lemma 41, this homomorphism is injective and so $Aut_F(E)$ is a subgroup of $S_X \cong S_n$. ♡

Example 3.3.2. Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ and $E/\mathbb{Q}$ be the splitting field of $f(x)$. Thus, $E = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ and $[E : F] = 6$. Since $ch(\mathbb{Q}) = 0$ we have $f(x)$ is separable and hence $|Aut_F(E)| = 6$. However, since $f(x)$ has three distinct roots, by Thm 44, we have $Aut_F(E)$ is a subgroup of S_3.

There is only one subgroup of S_3 with order 6, hence $Aut_F(E) = S_3$.

Definition 3.3.4. Let E/F be a field extension and $\phi \in Aut_F(E)$. Define

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

which is a subfield of E containing F. This is called the ***fixed field of*** ϕ.

Definition 3.3.5. If $G \leq Aut_F(E)$, then the ***fixed field of*** G is defined to be

$$E^G = \bigcap_{g \in G} E^g$$

Theorem 45. *Let $f(x) \in F[x]$ be a separable polynomial and E/F its splitting field. If $G = Aut_F(E)$ then $E^G = F$.*

Proof. Let $L = E^G$. Since $F \subseteq L$ we have $Aut_L(E) \subseteq Aut_F(E)$. On the other hand, if $\phi \in Aut_F(E)$ then $\phi(a) = a$ for all $a \in L$ and so $\phi \in Aut_L(E)$. Viz, $Aut_F(E) \subseteq Aut_L(E)$. Hence we get $Aut_L(E) = Aut_F(E)$.

Note that since $f(x)$ is separable over F and splits over E, we have $f(x)$ is separable over L and has E as its splitting field over L. Hence, by Thm 43 we have $|Aut_L(E)| = [E : L]$ and $|Aut_F(E)| = [E : F]$ and since those two are equal, we have $[E : F] = [E : L]$. However, $[E : F] = [E : L][L : F]$ and so $[L : F = 1$, i.e. $L = E^G = F$. ♡

Chapter 4

Galois Theory

期盼明月，期盼朝阳，期盼春风浴。
可逆风不解，挟雨伴雪，催梅折枝去。
凤凰于飞，翔翔其羽，远去无痕迹。
听梧桐细雨，瑟瑟其叶，随风摇记忆

凤凰于飞，刘欢

4.1 Separable Extensions

Definition 4.1.1. Let E/F be 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 $p(x)$ is separable. If for all $\alpha \in E$ we have α is separable, we say E/F is ***separable***.

Example 4.1.1. If $ch(F) = 0$, by Thm 26, F is perfect, i.e. every polynomial $f(x) \in F[x]$ is separable. Thus if $ch(F) = 0$, any algebraic extension is separable.

Theorem 46. *Let E/F be the splitting field of $f(x) \in F[x]$. If $f(x)$ 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 $\{\alpha_1, ..., \alpha_n\}$ be distinct roots of $p(x)$ in E.

We claim $P(x) = (x-\alpha_1)...(x-\alpha_n) \in F[x]$. Let $G = Aut_F(E)$ and $\phi \in G$. Since ϕ is an automorphism, $\phi(\alpha_i) \neq \phi(\alpha_j)$ if $i \neq j$. Thus by lemma 40, ϕ permutes $\alpha_1, ..., \alpha_n$. Thus we have $\phi(P) = P$, i.e. $P \in E^{\phi}[X]$. However, since $\phi \in G$ is arbitrary, we have $P \in E^G[x]$. Since E/F is the splitting field of the separable polynomial $f(x)$, by Thm 45 we have $E^G = F$ and so $P \in F[x]$.

Thus we have $P \in F[x]$ which has α as a root. Thus $p \mid P$ as p is the minimal polynomial of α. On the other hand, since P contains all roots of p, we must have $P \mid p$. This means $P = p$ and so p is indeed separable. ♡

Corollary 47. *Let E/F be finite extension and $E = F(\alpha_1, ..., \alpha_n)$. 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. Let $f(x) = p_1(x)...p_n(x)$. Since each p_i is separable, we have $f(x)$ is separable.

Let L be the splitting field of $f(x)$ over F. Then by Thm 46, L/F is separable. Since $E = F(\alpha_1, ..., \alpha_n)$ is subfield of L, E is separable. ♡

Corollary 48. *Let E/F be an algebraic extension and L the set of all $\alpha \in E$ such that α is separable. Then L is an intermediate field between E/F.*

Proof. Let $\alpha, \beta \in L$. Then $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in F(\alpha, \beta)$. By Cor 47, $F(\alpha, \beta)$ is separable and hence it is contained in L. Thus L is indeed a field. ♡

Remark 4.1.1. The converse of Theorem 46 is also true.

Definition 4.1.2. If $E = F(\alpha)$ is a simple extension, we say α is ***primitive element*** of E/F.

Theorem 49 (Primitive Element Theorem)**.** *If E/F is finite separable extension, then $E = F(\gamma)$ for some $\gamma \in E$. In particular, if $ch(F) = 0$, then any finite extension E/F is a simple extension.*

Proof. We have seen in Cor 23 that a finite extension of a finite field is always simple. Thus we are done the finite field case.

Thus, WLOG we may assume F is an infinite field.

Since $E = F(\alpha_1, ..., \alpha_n)$ for some $\alpha_1, ..., \alpha_n \in E$, it suffice to consider the case when $E = F(\alpha, \beta)$ and the general case can be done by induction.

Let $E = F(\alpha, \beta)$ with $\alpha, \beta \notin F$. We claim there exists $\lambda \in F$ such that $\gamma = \alpha + \lambda\beta$ and $\beta \in F(\gamma)$. If the claim holds, then $F(\alpha, \beta) \subseteq F(\gamma)$ and $F(\gamma) \subseteq F(\alpha, \beta)$ and the proof follows.

Let $a(x), b(x)$ be the minimal polynomial of α and β over F, respectively. Since $\beta \notin F$ we have $deg(b) > 1$. Thus there exists a root $\tilde{\beta}$ of $b(x)$ such that $\tilde{\beta} \neq \beta$. Choose any $\lambda \in F$ such that $\lambda \neq \frac{\tilde{\alpha}-\alpha}{\beta-\tilde{\beta}}$ for all roots $\tilde{\alpha}$ of $a(x)$ and for all roots $\tilde{\beta}$ of $b(x)$ with $\tilde{\beta} = \beta$ 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 $\tilde{\beta}$.

Let $\gamma = \alpha + \lambda\beta$, consider $h(x) = a(\gamma - \lambda x) \in F(\gamma)[x]$. Then $h(\beta) = a(\gamma - \lambda\beta) = a(\alpha) = 0$. However, for any $\tilde{\beta} \neq \beta$, since $\gamma - \lambda\tilde{\beta} = \alpha + \lambda(\beta - \tilde{\beta}) \neq \alpha$ by the choice of λ. We have $h(\tilde{\beta}) = a(\gamma - \lambda\tilde{\beta}) \neq 0$.

Thus $h(x)$ and $b(x)$ have β as a common root, but no other common root in any extension of $F(\gamma)$. Let $b_1(x)$ be the minimal polynomial of β over $F(\gamma)$. Then $b_1(x)$ divide both $h(x)$ and $b(x)$. Since E/F is separable and $b(x) \in F[x]$ is irreducible, $b(x)$ has distinct roots and so does $b_1(x)$. The roots of $b_1(x)$ are also common to $h(x)$ and $b(x)$. Since $h(x)$ and $b(x)$ has only β as a common root, $b_1(x) = x - \beta$. Since $b_1(x) \in F(\gamma)[x]$, we have $\beta \in F(\gamma)$ as required. ♡

4.2 Normal Extensions

Definition 4.2.1. 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 $p(x)$ splits over E, i.e. have all the rotos in E.

Example 4.2.1. Let $\alpha \in \mathbb{R}$ with $\alpha^4 = 5$. Then since the roots of $x^4 - 5$ are $\pm\alpha, \pm i\alpha$ and $\mathbb{Q}(\alpha)$ is real, we have $\mathbb{Q}(\alpha)/\mathbb{Q}$ is not normal.

On the other hand, let $\beta = (1 + i)\alpha$, we claim $\mathbb{Q}(\beta)/\mathbb{Q}$ is still not normal. Note $\beta^2 = 2i\alpha^2$ and $\beta^4 = -4\alpha^4 = -20$. Hence, the minimal polynomial for 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 $\alpha \in \mathbb{Q}(\beta)$ we would have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4 = [\mathbb{Q}(\beta) : \mathbb{Q}]$. This would imply that $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$, which is not possible as $\mathbb{Q}(\alpha) \subset \mathbb{R}$ while $\mathbb{Q}(\beta)$ contains the element $\alpha + i\alpha$.

Therefore, $\alpha \notin \mathbb{Q}(\beta)$ and it imply that $i \notin \mathbb{Q}(\beta)$ since $\alpha = \frac{\beta}{i+1}$. Hence $\pm i\beta$ are not in $\mathbb{Q}(\beta)$ and so it is not normal.

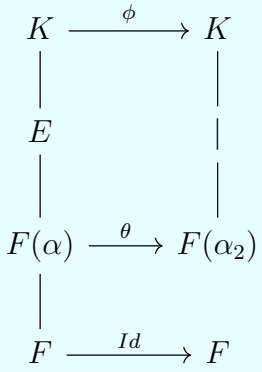
Theorem 50. *A finite extension E/F is normal if and only if it is the splitting field of some $f(x) \in F[x]$.*

Proof. ($\Rightarrow$): Say $E = F(\alpha_1, ..., \alpha_n)$, then $f(x) = p_1(x)p_2(x)...p_n(x)$ would suffice where $p_i(x) \in F[x]$ is the minimal polynomial of α_i. Indeed, since E/F is normal we have each $p_i(x)$ splits over E, we have E contains all roots of each p_i and so E is the splitting field of $f \in F[x]$.

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

Since $F(\alpha) \cong F[x]/\langle p(x)\rangle \cong F(\alpha_2)$, we have an F-isomorphism $\theta : F(\alpha) \to F(\alpha_2)$ such that $\theta(\alpha) = \alpha_2$. 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 Thm 13 there exists an isomorphism $\phi : K \to K$ which extends θ

and in particular note $\phi \in Aut_F(K)$. Viz, we have the following diagram



Since $\phi \in Aut_F(K)$, ϕ permutes the roots of $f(x)$. Since E is generated over F by the roots of $f(x)$, by Lemma 40, we have $\phi(E) = E$. It follows that for $\alpha \in E$, $\alpha_2 = \phi(\alpha) \in E$. Similarly we have $\alpha_i \in E$ for $3 \leq i \leq n$. Thus $K = E$ and so $p(x)$ splits over E. It follows that E/F is normal. ♡

Example 4.2.2. We claim that every quardratic extension is normal.

Let E/F be a field extension with $[E : F] = 2$. For $\alpha \in E \backslash F$, we have $E = F(\alpha)$. Let $p(x) = x^2 + ax + b$ be the minimal polynomial of α over F. If β is another roots of $p(x)$, then $p(x) = (x-\alpha)(x-\beta) = x^2 - (\alpha+\beta)x + \alpha\beta$. Thus $\beta = b/\alpha$ (or $\beta = -a-\alpha$) is the other root of $p(x)$ and the splitting field of $p(x)$ is $F(\alpha, b/\alpha) = F(\alpha) = E$. Since E/F is the splitting field of $p(x)$ over F, by Thm 50, it is normal.

Example 4.2.3. The extension $\mathbb{Q}(4\sqrt{2})/\mathbb{Q}$ is not normal since the irreducible polynomial $x^4 - 2$ has a root in $\mathbb{Q}(4\sqrt{2})$, but $p(x)$ does not split over $\mathbb{Q}(4\sqrt{2})$. Note that the extension $\mathbb{Q}(4\sqrt{2})/\mathbb{Q}$ is made up of two quardratic extension $\mathbb{Q}(4\sqrt{2})/\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, which are normal. Thus if E/K and K/F are normal, then E/F is not necessarily normal.

Proposition 51. *If E/F is normal extension and K is an intermediate field, then E/K is normal.*

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

Example 4.2.4. Take $F = \mathbb{Q}$, $K = \mathbb{Q}(4\sqrt{2})$ and $E = \mathbb{Q}(4\sqrt{2}, i)$. Then E/F is normal so is E/K. However, K/F is not normal.

Proposition 52. *Let E/F be a finite normal extension and $\alpha, \beta \in E$, then the following are equivalent:*

1. *There exists $\phi \in Aut_F(E)$ such that $\phi(\alpha) = \beta$.*
2. *The minimal polynomial of α and β over F are the same.*

In this case, we say α and β are conjugate over F.

Proof. (1) $\Rightarrow$ (2): Let $p(x)$ be the minimal polynomial of α over F and $\phi \in AUt_F(E)$ with $\phi(\alpha) = \beta$. By Lemma 40, β is also a root of $p(x)$. Since $p(x)$ is monic and irreducible, it is the minimal polynomial of β over F. Thus α and β have the same minimal polynomial.

(2) $\Rightarrow$ (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 Thm 50, 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 Thm 13, there exists an isomorphism $\phi : E \to E$ which extends θ. It follows that $\phi \in Aut_F(E)$ and $\phi(\alpha) = \beta$. ♡

Example 4.2.5. The complex numbers $\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2$ where $\zeta_3 = e^{2\pi i/3}$ are all conjugates over $\mathbb{Q}$ since they are roots of the irreducible polynomial $x^3 - 2 \in \mathbb{Q}[x]$.

Definition 4.2.2. A ***normal closure*** of a finite extension E/F is a finite normal extension N/F satisfying the following property:

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 4.2.6. The normal closure of $\mathbb{Q}(3\sqrt{2})/\mathbb{Q}$ is $\mathbb{Q}(3\sqrt{2}, \zeta_3)/\mathbb{Q}$.

Theorem 53. *Every finite extension E/F has a normal closure N/F which is unique up to E-isomorphism.*

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

(Existence): Let $p_i(x)$ be the minimal polynomial of α_i over F. Write $f(x) = p_1(x)...p_n(x)$ and let N/F be the splitting field of $f(x)$ over E. Since $\alpha_1, ..., \alpha_n$ are roots of $f(x)$, N is also the splitting field of $f(x)$ over F. By Thm 50, N is normal over F. Now let $L \subseteq N$ be an intermediate field containing E. Then L contains all α_i. If L is normal over F, each $p_i(x)$ splits over F and thus $N \subseteq L$ and so $N = L$.

(Uniqueness): Let N/E be the splitting field of $f(x)$ over E defined as above. Let N_1/E 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 N' of $f(x)$ over F, thus over E. By Corollary 14, N and N' are E-isomorphic. Sine N' is a splitting field of $f(x)$ over F, by Thm 50, N' is normal over F. Thus by definition of normal closure we have $N_1 = N'$. It follows that N and N' are E-isomophic. ♡

4.3 Galois Extension

Definition 4.3.1. An algebraic extension E/F is ***Galois extension*** if it is normal and separable. If E/F is a Galois extension we say the automorphism gorup $Aut_F(E)$ is the ***Galois group*** E/F and is denoted by $Gal_F(E)$.

Definition 4.3.2. A Galois extension E/F is called ***abelian***, ***cyclic*** or ***solvable*** if the Galois group $Gal_F(E)$ is abelian, cyclic or solvable.

Remark 4.3.1.

1. By Theorem 46 and Theorem 50, a finite Galois extension E/F is the equivalent to the splitting field of a separable polynomial $f(x) \in F[x]$.
2. If E/F is a finite Galois extension, by Theorem 43, we know $|Gal_F(E)| = [E : F]$
3. If E/F is the splitting field of a separable polynomial $f(x) \in f[x]$ with degree n, then by Theorem 44, $Gal_F(E)$ is a subgroup of S_n.

Example 4.3.1. 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 $[E : \mathbb{Q}] = 8$. For $\psi \in Gal_{\mathbb{Q}}(E)$ we have $\psi(\sqrt{2}) \in \{\sqrt{2}, -\sqrt{2}\}$, $\psi(\sqrt{3}) \in \{\sqrt{3}, -\sqrt{3}\}$ and $\psi(\sqrt{5}) \in \{\sqrt{5}, -\sqrt{5}\}$. Since $[E : \mathbb{Q}] = |Gal_{\mathbb{Q}}(E)| = 8$, we have the above are all the possibilities and so

$$Gal_{\mathbb{Q}}(E) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

Theorem 54 (E. Artin). *Let E be a field and G is a finite subgroup of $Aut(E)$, the automorphism group of E. Let $E^G := \{\alpha \in E : \forall \psi \in G, \psi(\alpha) = \alpha\}$ be a subfield of E. Then E/E^G is a finite Galois extension and $Gal_{E^G}(E) = G$. In particular, we have $|E : E^G| = |G|$.*

Proof. Let $n = |G|$ and $F = E^G$. We can check easily that F is a field. For $\alpha \in F$, consider the G-orbit of α, i.e. $Orb(\alpha) = \{\phi(\alpha) : \alpha \in G\} = \{\alpha_1, ..., \alpha_m\}$ where α_i's are distinct. Note that $m \leq n$. Let $f(x) := (x - \alpha_1)(x - \alpha_2)...(x - \alpha_m)$. For any $\phi \in G$, we have ϕ permutes the list $\{\alpha_1, ..., \alpha_m\}$. Since the coefficients of $f(x)$ are symmetric with respect to α_i for $1 \leq i \leq m$, they are fixed by all $\phi \in G$. Hence $f(x) \in E^G[x] = F[x]$.

Now, we want to show $f(x)$ is the minimal polynomial of α over F. Let $g(x)$ be a factor of $f(x)$, WLOG, we can write $g(x) = (x - \alpha_1)...(x - \alpha_l)$. If $l \neq m$ then since α_i for $1 \leq i \leq m$ are in the G-orbit of α, there exists $\phi \in G$ such that $\{\alpha_1, ..., \alpha_l\} \neq \{\phi(\alpha_1), ..., \phi(\alpha_l)\}$. It follows $\phi(g(x)) \neq g(x)$ and so $g \notin F[x]$, i.e. a contradiction. Thus $l = m$ and so $f(x)$ is irreducible and $f(x)$ is minimal as desired.

Since $f(x) \in F[x]$ is separable and splits over E, we see E/F is the splitting field of $f(x)$ and hence Galois. Next, we only need to show $Aut_F(E) = G$.

Claim: $[E : F] \leq n$. We will do a proof by contradiction. If $[E : F] > n = |G|$, then we can choose $\beta_1, ..., \beta_{n+1} \in E$ which is linearly independent over F. Consider the system of n equations

$$\forall \phi \in G, \phi(\beta_1)v_1 + ... + \phi(\beta_{n+1})v_{n+1} = 0 \tag{4.1}$$

Note we have $n + 1$ variables and so we get a non-trivial solution $(\gamma_1, ..., \gamma_{n+1})$ in E with minimal number of non-zero coordinates. Say we have $r > 1$ many non-zero coordinates in $(\gamma_1, ..., \gamma_{n+1})$. WLOG, say $\gamma_1, ..., \gamma_r$ are non-zero. Thus $\phi(\beta_1)\gamma_1 + ... + \phi(\beta_r)\gamma_r = 0$ for all $\phi \in G$. Then, by dividing γ_r in each equation, we can assume $\gamma_r = 1$. Since $\beta_1, ..., \beta_r$ are linearly independent over F, we know $\beta_1\gamma_1 + ... + \beta_r\gamma_r = 0$. There must be at least one γ_i that is not in F, because if all γ_i are in F we would contradict the linear independence of β_i's.

WLOG, we can assume $\gamma_1 \notin F$. Choose $\psi \in G$ such that $\psi(\gamma_1) \neq \gamma_1$. Apply ψ to the system of equations (4.1), we get

$$\forall \phi \in G, \phi(\beta_1)\psi(\gamma_1) + ... + \phi(\beta_r)\psi(\gamma_r) = 0 \tag{4.2}$$

Thus, by subtract equation (4.2) from (4.1), we get

$$\forall \phi \in G, \sum_{i=1}^{r} \phi(\beta_i)(\gamma_i - \psi(\gamma_i)) = 0$$

Since $\gamma_r = 1$ we have $\gamma_r - \psi(\gamma_r) = 0$. Also, since $\gamma_1 \notin F$, we have $\gamma_1 - \psi(\gamma_1) \neq 0$. Thus, $(\gamma_1 - \psi(\gamma_1), ..., \gamma_r - \psi(\gamma_r))$ is a nonzero solution of the system $\forall \phi \in G, \phi(\beta_1)v_1 + ... + \phi(\beta_{n+1})v_{n+1} = 0$. This contradict the choice of $(\gamma_1, ..., \gamma_{n+1})$.

Thus $[E : F] \leq n$ as claimed.

We have proved $[E : F]$ is a finite Galois extension. Thus E is the splitting field of some separable polynomial over F. Also, since $F = E^G = \{\alpha \in E : \forall \phi \in G, \phi(\alpha) = \alpha\}$ we have G is a subgroup of $Aut_F(E)$. By Theorem 43, we have $n = |G| \leq |Gal_F(E)| = [E : F] \leq n$. It follows $[E : F] = n$ and $Gal_F(E) = G$. ♡

Remark 4.3.2. Let E/E^G be a Galois extension with the Galois group G. For $\alpha \in E$, let $\{\alpha_1, ..., \alpha_m\}$ be the G-orbit of α. Then we see from the proof of Thm 54 that the minimal polynomial of α over E^G is $(x - \alpha_1)...(x - \alpha_m) \in E^G[x]$.

Example 4.3.2 (Fundamental Theorem of Symmetric polynomials)**.** Let $E = F(t_1, ..., t_n)$ be the function field in n variables $t_1, ..., t_n$.

Consider the symmetric group S_n as the subgroup of $Aut(E)$ which permutes the variables. We want to find $E^{S_n} = E^G$ with $G = S_n$.

The G-orbit of t_1 is $\{t_1, ..., t_n\}$. By the Remark, we see that $f(x) = (x - t_1)...(x - t_n)$ is the minimal polynomial of t_1 over E^G. Define the ***elementary symmetric functions*** in $t_1, ..., t_n$ as

$$S_1 = t_1 + ... + t_n$$
$$S_k = \sum_{1 \leq i_1 < i_2 < ... < i_k \leq n} t_{i_1}...t_{i_k}$$
$$S_n = t_1...t_n$$

Thus $f(x) = x^n - S_1x^{n-1} + S_2x^{n-2} + ... + (-1)^nS_n \in L[x]$ where $L = F(s_1, ..., s_n) \subseteq E^G$.

We claim $L = E^G$. Observe $L \subseteq E^G$ trivially. Note that E is the splitting field of $f(x)$ over L. Since $deg(f) = n$, by Thm 15, we have $[E : F] \leq n!$. On the other hand, by Thm 54, $[E : E^G] = |G| = |S_n| = n!$. SInce $L \leq E^G$, it follows that $n! = [E : E^G] \leq [E : L] \leq n!$ and hence $E^G = L$.

4.4 Fundamental Theorem of Galois Theory

Theorem 55 (Fundamental Theorem of Galois Theory)**.** *Let E/F be a fintie Galois extension and $G = Gal_F(E)$. There is an order reversing bijection between the intermediate field of E/F and the subgroups of G. More precisely, let $Int(E/F)$ denote the set of intermediate fields of E/F and $Sub(G)$ the set of subgroups of G. Then the map*

$$\begin{aligned} Int(E/F) &\to Sub(G) \\ L &\mapsto L^* := Gal_L(E) \end{aligned}$$

and

$$\begin{aligned} Sub(G) &\to Int(E/F) \\ H &\mapsto H^* := E^H \end{aligned}$$

are inverse of each other and reverse the inclusion relation.

In particular, for $L_1, L_2 \in Int(E/F)$ with $L_2 \subseteq L_1$, we have $[L_1 : L_2] = [L_2^* : L_1^*]$. For $H_1, H_2 \in Sub(G)$ with $H_2 \subseteq H_1$, we have $[H_1 : H_2] = [H_2^* : H_1^*]$.

Proof. Let $L \in Int(E/F)$ and $H \in Sub(G)$, we recall Thm 45 which states that if $G_1 = Gal_{F_1}(E_1)$ then $E^{G_1} = F_1$. Thus we have $(L^*)^* = (Gal_L(E))^* = E^{Gal_L(E)} = L$. Also, by Thm 54 we have $G_1 \leq Aut(E_1)$ then $Gal_{E_1^{G_1}}(E_1) = G_1$. Thus we have $(H^*)^* = (E^H)^* = Gal_{E^H}(E) = H$.

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 inverse of each other.

FOr $L_1, L_2 \in Int(E/F)$, by Prop 51, E/L_1 and E/L_2 are also Galois extensions. We have $L_2 \subseteq L_1$, we have $Gal_{L_1}(E) \subseteq Gal_{L_2}(E)$, i.e. $L_1^* \subseteq L_2^*$. Also, we have $[L_1 : L_2] = \frac{[E:L_2]}{[E:L_1]} = \frac{|Gal_{L_2}(E)|}{|Gal_{L_1}(E)|} = [L_2^* : L_1^*]$.

For $H_1, H_2 \in Sub(G)$, we have $H_2 \subseteq H_1 \Rightarrow E^{H_1} \subseteq E^{H_2}$, i.e. $H_1^* \subseteq H_2^*$. Hence similarly we get $[H_1 : H_2] = [H_2^* : H_1^*]$. ♡

Remark 4.4.1. From Thm 55 we see that $Int(E/F)$ are in 1 to 1 correspondence with $Sub(G)$ and since $Sub(G)$ is finite, there are only finitely many intermediate fields.

Proposition 56. *Let E/F be a fintie Galois extension with $G = Gal_F(E)$. Let L be an intermediate field. For $\psi \in G$, we have $Gal_{\psi(L)}(E) = \psi \cdot Gal_L(E) \cdot \psi^{-1}$.*

Proof. For any $\alpha \in \psi(L)$, we have $\psi^{-1}(\alpha) \in L$. If $\phi \in Gal_L(E)$ we have $\phi \circ \psi^{-1}(\alpha) = \psi^{-1}(\alpha)$, thus $\psi \circ \phi \circ \psi^{-1}(\alpha) = \alpha$. It follows that $\psi \circ \phi \circ \psi^{-1} \in Gal_{\psi(L)}(E)$ for all $\phi \in Gal_L(E)$. Thus $\psi Gal_L(E)\psi^{-1} \subseteq Gal_{\psi(L)}(E)$. Since $|\psi Gal_L(E)\psi^{-1}| = |Gal_L(E)| = [E : L] = [E : \psi(L)] = |Gal_{\psi(L)}(E)|$. We have $Gal_{\psi(L)}(E) = \psi Gal_L(E)\psi^{-1}$. ♡

Theorem 57. *Let E/F, L, L^* be defined in Thm 55. Then L/F is a Galois extension if and only if L^* is a normal subgroup of G. In this case, $Gal_F(L) \cong G/L^*$.*

Proof. Note that L/F is normal if and only if $\psi(L) = L$ for all $\psi \in Gal_F(E)$ if and only if $\psi Gal_L(E)\psi^{-1} = Gal_L(E)$ for all $\psi \in Gal_F(E)$ by Prop 56 if and only if $L^* = Gal_L(E)$ is a normal subgroup of G.

If L/F is a Galois extension, the restriction map $G = Gal_F(E) \to Gal_F(L)$ given by $\psi \mapsto \psi|_L$ is well-defined. Moreover, it is surjective and its kernel is $Gal_L(E) = L^*$. Thus $Gal_F(L) \cong G/L^*$. ♡

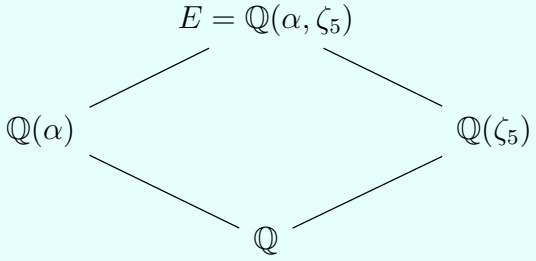
Example 4.4.1. For a prime p, let $q = p^n$. Consider the finite field $\mathbb{F}_q$ of q elements which is an extension of $\mathbb{F}_p$ of degree n. The ***Frobenius automorphism*** of $\mathbb{F}_q$ is defined by (recall Assignment 2) $\sigma_p : \mathbb{F}_q \mapsto \mathbb{F}_q$, $\sigma_p(\alpha) = \alpha^p$.

For $\alpha \in \mathbb{F}_q$, we have $\sigma_p^n(\alpha) = \alpha^{p^n} = \alpha$. Thus $\sigma_p^n = 1$. For $1 \leq m < n$, 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 $G = Gal_{\mathbb{F}_p}(\mathbb{F}_q)$.

It follows that $n = |\sigma_p| \leq |G| = [\mathbb{F}_q : \mathbb{F}_p] = n$. Thus $G = \langle \sigma_p \rangle$ is a cyclic group of order n. Consider a subgroup H of G of order d. Thus $d \mid n$ and $[G : H] = \frac{n}{d}$. By Thm 55, we have $\frac{n}{d} = [G : H] = [H^* : G^*] = [\mathbb{F}_q^H : \mathbb{F}_q^G] = [\mathbb{F}_q^H : \mathbb{F}_q]$. Thus $H^* = \mathbb{F}_q^H = \mathbb{F}_q^{\frac{n}{d}}$.

Example 4.4.2. Let E be the splitting field of $x^5 - 7$ over $\mathbb{Q}$ in $\mathbb{C}$. Then $E = \mathbb{Q}(\alpha, \zeta_5)$ where $\alpha = \sqrt[5]{7}$ and $\zeta_5 = e^{2\pi i/5}$. The minimal polynomial of α and ζ_5 over $\mathbb{Q}$ are $x^5 - 7$ and $(x^4 + x^3 + x^2 + x + 1)$ respectively.

We have



Since $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$ and $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$ are divisors of $[E : \mathbb{Q}]$, we must have $[E : \mathbb{Q}]$ is divisible by 20. Thus $[E : \mathbb{Q}(\zeta_5)] \geq 5$. Also, $E = \mathbb{Q}(\alpha, \zeta_5) = \mathbb{Q}(\zeta_5)(\alpha)$ and the minimal polynomial of α over $\mathbb{Q}(\zeta_5)$ divides $x^5 - 7$. Thus $[E : \mathbb{Q}(\zeta_5)] \leq 5$. It follows that $[E : \mathbb{Q}_5] = 5 \Rightarrow [E : \mathbb{Q}] = 20$.

For each $\psi \in G = Gal_{\mathbb{Q}}(E)$, its action is determined by $\psi(\alpha)$ and $\psi(\zeta_5)$. We write $\psi = \psi_{k,s}$ if $\psi(\alpha) = \alpha\zeta_5^k$ and $\psi(\zeta_5) = \zeta_5^s$ where $k \in \mathbb{Z}_5$ and $s \in \mathbb{Z}_5^\times$. Then, define $\sigma = \psi_{1,1}$ and $\tau = \psi_{0,2}$. It can be checked that $\tau\sigma = \sigma^2\tau$ and we have

$$G = \langle \sigma, \tau : \sigma^5 = 1 = \tau^4, \tau\sigma = \sigma^2\tau \rangle$$

Thus it follows

$$G = \{\sigma^i\tau^j : 0 \leq i \leq 5, 0 \leq j \leq 4\}$$

Since $|G| = 20$, by Lagrange's Theorem the possible subgroups of G are of order $1, 2, 4, 5, 10, 20$. We have $|G| = 20 = 2^2 \cdot 5$. Let n_p be the number of Sylow p-subgroup

of G and by the third Sylow's theorem we have $n_2 \mid 5$ and $n_2 \equiv 1 \pmod 2$. Hence we must have n_2 equal 1 or 5. Also, we have $n_5 \mid 4$ and $n_5 \equiv 1 \pmod 5$. Thus $n_5 = 1$ and we have one unique Sylow 5-group, P_5, which is order 5. Since $\langle\sigma\rangle$ is a subgroup of order 5, we have P_5 is isomorphic to $\mathbb{Z}_5$. Note that by the 2nd Sylow theorem, we have $P_5 \trianglelefteq G$.

Note that if $n_2 = 1$ then there is on ly one Sylow 2-group, say $P_2 = \langle\tau\rangle \cong \mathbb{Z}_4$ then $P_2 \trianglelefteq G$. Since $|P_2 \cap P_5| = 1$ it follows $G = P_2 \times P_5 \cong \mathbb{Z}_4 \times \mathbb{Z}_5$ and we must have G is abelian. This is a contradiction to the fact that G is not abelian as $\tau\sigma = \sigma^2\tau$.

Hence, we must have 5 Sylow 2-groups and they are cyclic since they are conjugate to $\langle\tau\rangle$. We have seen that τ has order 4 and thus $\langle\tau\rangle$ is a Sylow 2-group and all other Sylow 2-groups are conjugate to it. Note that since all elements of G are of the form $\sigma^a\tau^b$, we have $\sigma^a\tau^b\tau\tau^{-b}\sigma^{-a} = \sigma^a\tau\sigma^{-a}$ where $a \in \{0, 1, ..., 4\}$. Now using relation that $\tau\sigma = \sigma^2\tau$ we have $\langle\sigma^4\tau\sigma^{-4}\rangle = \langle\sigma^{-1}\tau\sigma\rangle = \langle\sigma\tau\rangle = \langle\psi_{1,2}\rangle$. Using the same argument, we see that the Sylow 2-groups are

$$\langle\psi_{0,2}\rangle, \langle\psi_{1,2}\rangle, \langle\psi_{2,2}\rangle, \langle\psi_{3,2}\rangle, \langle\psi_{4,2}\rangle$$

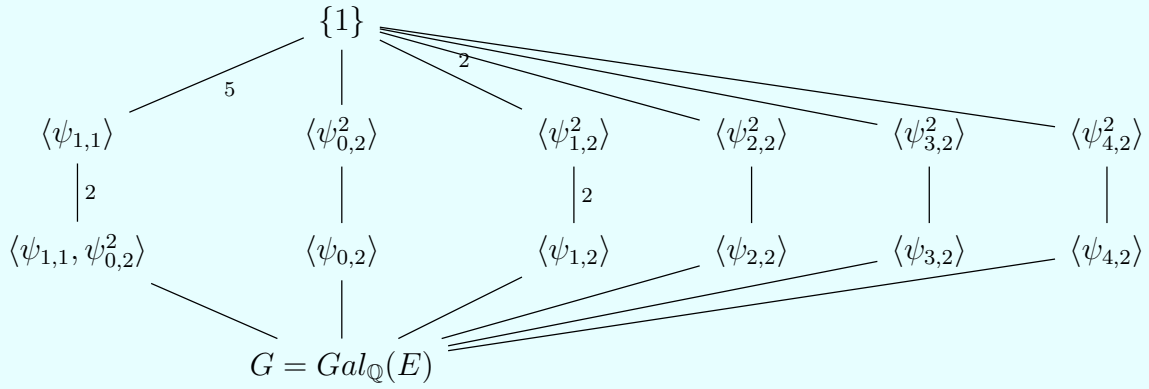
Moreover, since a subgroup of G of order 2 are contained in a Sylow 2-group. Observe

$$\langle\psi_{0,2}^2\rangle, \langle\psi_{1,2}^2\rangle, \langle\psi_{2,2}^2\rangle, \langle\psi_{3,2}^2\rangle, \langle\psi_{4,2}^2\rangle$$

are all the subgroups of order 2.

For a subgroup H of G of order 10, since P_5 is the only subgroup of G of order 5. $H \geq P_5 = \langle\sigma\rangle$. Thus $\sigma^a\tau^b \in H$ if and only if $\tau^b \in H$. The only element of the form τ^b which is of order 2 is σ^2 and thus $H = \langle\sigma, \tau^2\rangle$.

Thus, we have



For an intermediate field L of $E/\mathbb{Q}$, we consider $L^* = Gal_L(E)$. 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 $|\langle\psi_{1,1}\rangle| = [\langle\psi_{1,1}\rangle : \langle 1\rangle] = 5$ and $5 = [E : \mathbb{Q}(\zeta_5)] = [\mathbb{Q}(\zeta_5)^* : \langle 1\rangle]$ and we have $\mathbb{Q}(\zeta_5)^* = \langle\psi_{1,1}\rangle$.

Also, $\psi_{1,2}(\alpha\zeta_5^r) = \alpha\zeta_5\zeta_5^{2r} = \alpha\zeta_5^{2r+1}$. If $\psi_{1,2}$ fixed $\alpha\zeta_5^r$ then $r \equiv 2r + 1 \pmod 5$, i.e. $r \equiv 4 \pmod 5$. Thus we have $\mathbb{Q}(\alpha\zeta_5^4) \supseteq \langle\psi_{1,2}\rangle$. Since $|\langle\psi_{1,2}\rangle| = [\langle\psi_{1,2}\rangle : \{1\}] = 4$ and $[E : \mathbb{Q}(\alpha\zeta_5^4)] = 4$. Thus $\mathbb{Q}(\alpha\zeta_5^4) = \langle\psi_{1,2}\rangle$.

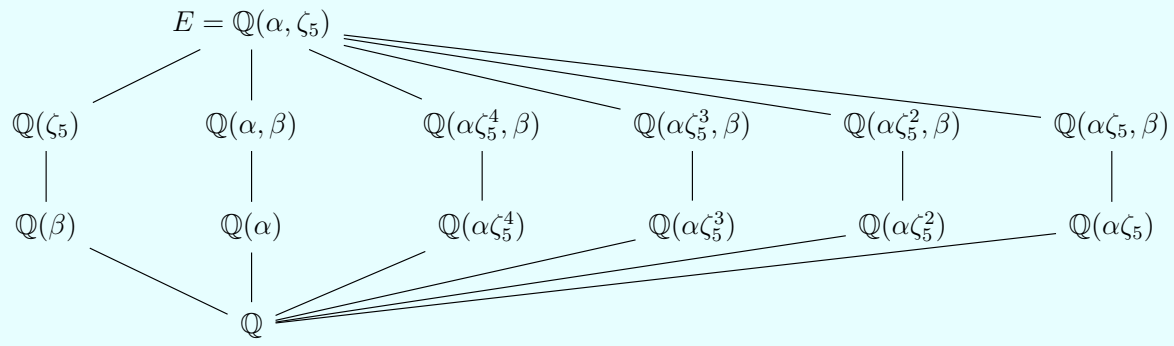
Using the same argument we can get $\langle \psi_{r,2} \rangle^*$ for $0, 1, 2, 3, 4$.

Consider $\beta = \zeta_5 + \zeta_5^{-1}$, we have

$$\begin{aligned} \beta^2 + \beta - 1 &= (\zeta_5 + \zeta_5^{-1})^2 + (\zeta_5 + \zeta_5^{-1}) - 1 \\ &= \zeta_5^2 + 2 + \zeta_5^{-2} + \zeta_5 + \zeta_5^{-1} - 1 \\ &= \zeta_5^4 + \zeta_5^3 + \zeta_5^2 + \zeta_5^1 + 1 \\ &= 0 \end{aligned}$$

Since $x^2 + x - 1$ has no rational roots, we have $[\mathbb{Q}(\beta) : \mathbb{Q}] = 2$.

Consider the following diagram



Chapter 5

Application

土生木酿水中火，金樽玉液小乾坤。
文痴武客三点血，江湖相见半盏春。
一白忘忧再消愁，三碗同天竞风流
浮云苍狗烂柯泥，唯此醪糟诚不欺

大汎歌，洛天依/戴荃

5.1 Solvability by Radicals

Example 5.1.1 (Cardano Formula).

We recall quardratic formula as $x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$ with $char(F) \neq 2$. This is called a radical solution.

Now consider the cubic equation $x^3 + Ax^2 + Bx + C = 0$ with $a, b, c \in F$ where $char(F) \neq 2, 3$. By replacing x by $x - \frac{A}{3}$, it suffice to find the roots for the equation $x^3 + bx + c = 0$.

Set $x = u + v$ where u, v are indeterminate. We obtain

$$\begin{aligned} x^3 + bx + c &= (u+v)^3 + b(u+v) + c \\ &= u^3 + v^3 + (3uv + b)(u+v) + c = 0 \end{aligned}$$

By imposing the condition $uv = \frac{-b}{3}$, the equation is reduced to

$$u^3 + v^3 = -c$$

Let $\alpha = u^3$ and $\beta = v^3$, we have

$$\alpha + \beta = -c, \text{ and } \alpha\beta = u^3v^3 = (\frac{-b}{3})^3$$

Thus α and β are solutions of $y^2 + cy - (\frac{b}{3})^3 = 0$ and so

$$\alpha, \beta = \frac{-c \pm \sqrt{c^2 + 4(\frac{b}{3})^3}}{2} = -\frac{c}{2} \pm \sqrt{\frac{c^2}{4} + \frac{b^3}{27}}$$

Since $\alpha = u^3$ and $\beta = v^3$ there are three choices for u and three for v. However, the condition $uv = -\frac{b}{3}$ forces that there are only three choices for u, v.

Theorem 58 (Tartaglia, del Fierro, Fontana)**.** *The solutions for $x^3 + bx + c = 0$ are of the form, if we let*

$$A = -\frac{c}{2} + \sqrt{\frac{c^2}{4} + \frac{b^3}{27}}, B = -\frac{c}{2} - \sqrt{\frac{c^2}{4} + \frac{b^3}{27}}$$

then the roots are:

$$A^{1/3} + B^{1/3}, \zeta_3(A)^{1/3} + \zeta_3^2(B)^{1/3}, \zeta_3^2(A)^{1/3} + \zeta_3(B)^{1/3}$$

where the cubic roots are chosen properly such that $A^{1/3}B^{1/3} = -\frac{b}{3}$.

Example 5.1.2. Now we consider the quartiz equation $x^4+Ax^3+Bx^2+Cx+D = 0$. By replacing x with $x - A/4$, it suffice to consider $x^3 + bx^2 + cx + d = 0$. Suppose $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ are the solutions, then $\sum_i \alpha_i = 0$. Also, we define the ***resolvent cubic*** of $x^4 + bx^2 + cx + d$ to be $g(x) = x^3 - bx^2 - 4dx + 4db - c^2$ whose roots are $u = \alpha_1\alpha_2 + \alpha_3\alpha_4$, $v = \alpha_1\alpha_3 + \alpha_2\alpha_4$ and $w = \alpha_1\alpha_4 + \alpha_2\alpha_3$. Apply Thm 58, we get

$$u + v = -(\alpha_1 + \alpha_4)^2, v + w = -(\alpha_1 + \alpha_2)^2, w + u = -(\alpha_1 + \alpha_3)^2$$

Consequently, we have $\alpha_1 + \alpha_4 = \pm\sqrt{-u - v}, \alpha_1 + \alpha_2 = \pm\sqrt{-v - w}$ and $\alpha_1 + \alpha_3 = \pm\sqrt{-w - u}$.

In particular, observe

$$(\alpha_1 + \alpha_4) + (\alpha_1 + \alpha_2) + (\alpha_1 + \alpha_3) = 3\alpha_1 + (\alpha_2 + \alpha_3 + \alpha_4) = 2\alpha_1$$

Therefore we get

$$(\alpha_1 + \alpha_4) + (\alpha_1 + \alpha_2) + (\alpha_1 + \alpha_3) = \pm\sqrt{-u - v} \pm \sqrt{-v - w} \pm \sqrt{-w - u}$$

It appears that there are 8 choices for α. However, since

$$\begin{aligned}(\alpha_1 + \alpha_4)(\alpha_1 + \alpha_2)(\alpha_1 + \alpha_3) &= \alpha_1^2(\sum_{i=1}^{4} \alpha_i) + (\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4) \\ &= 0 + (-c) = -c\end{aligned}$$

This cuts down the choices for α_1 to 4. ALso, once α_1 is chosen, i.e. these $\pm$ signs are chosen, then $\alpha_2, \alpha_3, \alpha_4$ are fixed.

Theorem 59 (Ferrari)**.** *The solutions for $x^4 + bx^2 + cx + d = 0$ are of the form, if we let $A = (-u - v)^{1/2}$, $B = (-v - w)^{1/2}$ and $C = (-w - u)^{1/2}$ then,*

$$\frac{1}{2}(A + B + C), \frac{1}{2}(-A - B + C), \frac{1}{2}(-A + B - C), \frac{1}{2}(A - B - C)$$

where the square roots (it can be any square root) are chosen properly such that

$$ABC = -c$$

5.2 Cyclic Extensions

Lemma 60 (Dedekind's lemma)**.** *Let K and L be fields and $\phi_i : L \to K$ be all the distinct homomorphisms ($1 \leq i \leq n$). If $c_i \in K$ and*

$$\forall \alpha \in L, \sum_{i=1}^{n} c_i \phi_i(\alpha) = 0$$

then $c_1 = ... = c_n = 0$.

Proof. Suppose the statement is false, i.e. there exists $c_1, ..., c_n \in K$, not all zero, such that $\forall \alpha \in L, \sum c_i \phi_i(\alpha) = 0$. Rearrange if necessary, let $m \geq 2$ be the minimal positive integer such that

$$\forall \alpha \in L, \sum_{i=1}^{m} c_i \phi_i(\alpha) = 0 \tag{5.1}$$

and $c_i \neq 0$ for $1 \leq i \leq m$. Choose $\beta \in L$ so that $\phi_1(\beta) \neq \phi_2(\beta)$ and $\phi_1(\beta) \neq 0$ (such β exists because $\phi_1 \neq \phi_2$ and ϕ_1 is embedding so kernel is trivial). We have

$$\forall \alpha \in L, \sum_{i=1}^{m} c_i \phi_i(\alpha\beta) = 0$$

By dividing the above equation by $\phi_1(\beta)$, we get

$$\forall \alpha \in L, c_1 \phi_1(\alpha) + \sum_{i=2}^{m} c_i \phi_i(\alpha) \frac{\phi_i(\beta)}{\phi_1(\beta)} = 0 \tag{5.2}$$

Now subtract equation (5.1) by equation (5.2), we obtain

$$\forall \alpha \in L, \sum_{i=2}^{m} c_i (1 - \frac{\phi_i(\beta)}{\phi_1(\beta)}) \phi_i(\alpha) = 0$$

Note $c_2(1 - \frac{\phi_2(\beta)}{\phi_1(\beta)}) \neq 0$, we have a contradiction with the minimal choice for m. Thus such $c_1, ..., c_m$ does not exist and the lemma holds. ♡

Theorem 61. *Let F be a field and $n \in \mathbb{N}$. Suppose $ch(F) = 0$ or p with $p \nmid n$. Assume $x^n - 1$ splits over F. Then*

1. *If the Galois extension E/F is cyclic of degree n, then $E = F(\alpha)$ for some $\alpha \in E$ such that $\alpha^n \in F$. In particular, $x^n - \alpha^n$ is the minimal polynomial of α over F.*
2. *Conversely, if $E = F(\alpha)$ and $\alpha^n \in F$. 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 ζ_n be the 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 $char(F) = 0$ or p not dividing n, we have $x^n - 1$ is separable and so $1, \zeta_1, ..., \zeta_n^{n-1}$ are all distinct.

Assertion (1): Let $G = Gal_F(E) = \langle \phi \rangle \cong C_n$, the cyclic group of order n. Apply Dedekind's lemma to $K = L = E$, ϕ^i all elements of G, and $c_1 = 1, c_2\zeta_n^{-1}, ..., c_n = \zeta_n^{-(n-1)}$. Since $c_i \neq 0$ for all $1 \leq i \leq n$ we have $u \in E$ such that

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

Then, we have

$$1(\alpha) = \alpha, \phi(\alpha) = \alpha\zeta_n, \phi^2(\alpha) = \alpha\zeta_n^2, ..., \phi^{n-1}(\alpha) = \alpha\zeta_n^{n-1}$$

Thus $\alpha, \alpha\zeta_n, ..., \alpha\zeta_n^{n-1}$ are conjugates to each other, i.e. they have the same minimal polynomial over F, say $p(x)$. Since $\alpha, \alpha\zeta_n, ..., \alpha\zeta_n^{n-1}$ are all distinct, it follows that $deg(p) = n$. Also, since $p(x) \in F[x]$ we have

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

since $\zeta_n \in F, \alpha^n \in F$.

Now, because 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 $E = F(\alpha)$.

Assertion (2): ♡