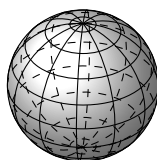


UNIVERSITY OF WATERLOO



PMATH 348 FIELDS AND GALOIS THEORY

PROF. YU-RU LIU • WINTER 2018

Contents

1	INTRODUCTION	1
1.1	Polynomial Equations	1
1.2	Cubic Equations	1
1.3	Quartic Equations	1
1.4	Quintic Equations	1
2	FIELD EXTENSIONS	3
2.1	Degree of Extensions	3
2.2	Algebraic and Transcendental Extensions	4
2.3	Eisenstein's Criterion	7
3	SPLITTING FIELDS	9
3.1	Existence of Splitting Fields	9
3.2	Uniqueness of Splitting Fields	10
3.3	Degree of Splitting Fields	11
4	FINITE FIELDS	12
4.1	Prime Fields	12
4.2	Formal Derivatives and Repeated Roots	12
4.3	Finite Fields	13
4.4	Separable Polynomials	14
5	THE SYLOW THEOREMS	17
5.1	The Sylow Theorems	18
6	SOLVABLE GROUPS	21

1 Introduction

1.1 Polynomial Equations

Consider the quadratic equation. Let $ax^2 + bx + c = 0$ with the leading coefficient $a \neq 0$, then we have that,

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

We notice immediately that there are a couple of operations that are involved in this equation.

Definition 1.1.1. An expression involving only addition, subtraction, multiplication, division and radicals is called a radical. These operations are denoted by $+$, $-$, \times , \div and $\sqrt[n]{}$.

The natural question that is raised is the extension to higher dimensions.

1.2 Cubic Equations

All cubic equations can be reduced to the following equation,

$$x^3 + px = q$$

for some $p, q \in \mathbb{C}$. A solution to the above equation is of the form

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} \quad (\text{Cardano's Formula})$$

1.3 Quartic Equations

A radical solution can be obtained by reducing a quartic to a cubic equation.

1.4 Quintic Equations

- General radical solutions were attempted by Euler, Bézout and Lagrange without success
- In 1799, Ruffini gave a 516 page proof about the unsolvability of quintic equations. His Proof was “almost right”
- In 1824, Abel filled the gap in Ruffini’s proof.

We can now ask ourselves, given a quintic equation, is it solvable by radicals? This question seems to be too hard, so we ask, suppose that a radical solution exists. How does its associated quintic equation look like?

Two main steps in Galois Theory

1. Link a root of a quintic equation, say α to $\mathbb{Q}(\alpha)$, the smallest field containing \mathbb{Q} and α . $\mathbb{Q}(\alpha)$ is a field. So it has more structures to be played with than α ; however, our knowledge of $\mathbb{Q}(\alpha)$ is still too little to answer the question. For example, we do not know how many intermediate fields, E between \mathbb{Q} and $\mathbb{Q}(\alpha)$. What we mean is how many fields E satisfy

$$\mathbb{Q} \subseteq E \subseteq \mathbb{Q}(\alpha).$$

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

$$\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha)) = \left\{ \Psi : \mathbb{Q}(\alpha) \rightarrow \mathbb{Q}(\alpha) \text{ an isomorphism and } \Psi|_{\mathbb{Q}} = 1_{\mathbb{Q}} \right\}$$

It can be shown that if α is “good”, say algebraic, $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ is finite. If α is “very good”, say constructable, the order of $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ is in certain forms. Moreover, there is a one-to-one correspondence between the intermediate fields between $\mathbb{Q}(\alpha)$ and \mathbb{Q} and the subgroups of $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$.

It follows that given some “good” α , we have that the intermediate fields of $\mathbb{Q}(\alpha)$ and \mathbb{Q} are indeed finitely many. This introduces Galois Theory; the interplay between fields and groups.

2 Field Extensions

2.1 Degree of Extensions

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

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

1. Addition: For $e_1, e_2 \in E$, $e_1 + e_2 := e_1 + e_2$ (addition in E)
2. Scalar Multiplication: For $c \in F, e \in E$, $c \cdot e := ce$ (multiplication in E)

Definition 2.1.2. The dimension of E over F (viewed as a vector space) called the degree of E over F , denoted by $[E : F]$. If $[E : F] < \infty$, we say E/F is a finite extension. Otherwise, E/F is an infinite extension.

Example 2.1.3. $[\mathbb{C} : \mathbb{R}] = 2$ is a finite extension since $\mathbb{C} \cong \mathbb{R} + \mathbb{R}i$, with $i^2 = -1$.

Example 2.1.4. Let F be a field. Then $[F(x) : F]$ is ∞ since $\{1, x, x^2, \dots\}$ are linearly independent over F .

Remark. $F[x] = \{f(x) = a_0 + a_1x + \dots + a_nx^n : a_i \in F, n \in \mathbb{N} \cup \{0\}\}$, the polynomial ring of F .

Remark. $F(x) = \{\frac{f(x)}{g(x)} : f(x), g(x) \in F[x]\}$, the fraction field of the polynomial ring of F .

Theorem 1. If E/K and K/F are finite field extensions, then E/F is a finite field extension and

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

In particular, K is an intermediate field of an field extension E/F , then $[K : F] \mid [E : F]$.

Proof. Suppose $[E : K] = m$ and $[K : F] = n$. Let $\{a_i, \dots, a_m\}$ be a basis of E/K and $\{b_1, \dots, b_n\}$ be a basis of K/F . It suffices to show $\{a_i b_j : 1 \leq i \leq m, 1 \leq j \leq n\}$ is a basis of E/F .

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

For $e \in E$, we have

$$e = \sum_{i=1}^m k_i a_i$$

with $k_i \in K$. Also, for each $k_i \in K$, we have

$$k_i = \sum_{j=1}^n c_{ij} b_j$$

with $c_{ij} \in F$. Thus,

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

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

Suppose that

$$\sum_{i=1}^m \sum_{j=1}^n c_{ij} b_j a_i = 0$$

with $c_{ij} \in F$. Since $\sum_{j=1}^n c_{ij} b_j \in K$ and $\{a_1, \dots, a_m\}$ are independent over K . We have

$$\sum_{j=1}^n c_{ij} b_j = 0.$$

Since $\{b_1, \dots, b_n\}$ are independent over F , we have $c_{ij} = 0$.

Combining both claims, we see that $\{a_i b_j, 1 \leq i \leq m, 1 \leq j \leq n\}$ is a basis of E/F and we have $[E : F] = [E : K][K : F]$. \square

2.2 Algebraic and Transcendental Extensions

Definition 2.2.1. Let E/F be a field extension and $\alpha \in E$. We say α is algebraic over F if there exists $f(x) \in F[x] \setminus \{0\}$ with $f(\alpha) = 0$. Otherwise, α is transcendental over F .

Example 2.2.2. $\frac{e}{d} \in \mathbb{Q}$, $\sqrt{2}$, $\sqrt[3]{7} + 2i$ are algebraic over \mathbb{Q} (see Assignment 1) but e (Hermite, 1873) and π (Lindemann, 1882) are transcendental over \mathbb{Q} .

Let E/F be a field extension and $\alpha \in E$. Let $F[\alpha]$ denote the smallest subfield of E containing F and α . For $\alpha, \beta \in E$, we define $F[\alpha, \beta]$ and $F(\alpha, \beta)$ similarly.

Definition 2.2.3. If $F = F(\alpha)$ for some $\alpha \in E$, we say E is a simple extension of F .

Definition 2.2.4. Let R_1 and R_2 be two rings which contain a field F . A ring homomorphism $\Psi : R_1 \rightarrow R_2$ is said to be a F -homomorphism if $\Psi|_F = 1_F$.

Theorem 2. Let E/F be a field extension and $\alpha \in E$. If α is transcendental over F , then

$$F[\alpha] \cong F[x] \quad \text{and} \quad F(\alpha) \cong F(x)$$

In particular, $F[\alpha] \neq F(\alpha)$.

Remark. In fact, if α is algebraic, indeed $F[\alpha] = F(\alpha)$.

Proof. Let $\Psi : F(x) \rightarrow F(\alpha)$ be the unique F -homomorphism defined by $\Psi(x) = \alpha$. Thus, for $f(x), g(x) \in F[x]$, $g(x) \neq 0$,

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

Notice that this is indeed a well-defined map as $g(x) \neq 0$ implies $g(\alpha) \neq 0$ since α is transcendental. Since $F(x)$ is a field and $\ker(\Psi)$ is an ideal of $F(x)$, we have $\ker(\Psi) = F(x)$ or trivial. Thus $\Psi = 0$ or Ψ is injective. Since $\Psi(x) = \alpha \neq 0$, Ψ must be injective. Also, since $F(x)$ is a field, $\text{im}(\Psi)$ contains a field generated by F and α , in other words, $F(\alpha) \subseteq \text{im}(\Psi)$. Thus, $\text{im}(\Psi) = F(\alpha)$ and Ψ is surjective. It follows that Ψ is an isomorphism and we have

$$F[\alpha] \cong F[x] \quad \text{and} \quad F(\alpha) \cong F(x).$$

\square

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 -homomorphism

$$\Psi : F[x]_{\langle p(x) \rangle} \rightarrow F[\alpha] \quad \text{with } \Psi(x) = \alpha$$

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

Proof. Consider the unique F -homomorphism $\Psi : F[x] \rightarrow F[\alpha]$ defined by $\Psi(x) = \alpha$. Thus, for $f(x) \in F[x]$, we have $\Psi(f) = f(\alpha)$. Since $F[x]$ is a ring, $\text{im}(\Psi)$ contains a ring generated by F and α , in other words, $F[\alpha] \subseteq \text{im}(\Psi)$. Thus, $\text{im}(\Psi) = F[\alpha]$.

Let

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

Since α is algebraic, $I \neq \{0\}$. We have $F[x]_I \cong \text{im}(\Psi) = F[\alpha] \subseteq F(\alpha)$, a subring of a field $F(\alpha)$. Thus, $F[x]_I$ is an integral domain so I is a prime ideal. It follows that $I = \langle p(x) \rangle$, where $p(x)$ is irreducible. If we assume $p(x)$ is monic, then it is unique. 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. So $F[\alpha]$ is a field. It follows that $F[\alpha] = F(\alpha)$. \square

Definition 2.2.5. If α is algebraic over a field F , the unique monic polynomial irreducible polynomial $p(x)$ in Theorem 3 is called the minimal polynomial of α over F .

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

Theorem 4. Let E/F be a field extension and $\alpha \in E$.

1. α is transcendental over F if and only if $[F(\alpha) : F]$ is ∞ .
2. α is algebraic over F if and only if $[F(\alpha) : F] < \infty$.

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

Proof. It suffices to prove the forward direction for each statement as the inverse direction implies the other statement.

(1) **Forwards:** From Theorem 2, if α is transcendental over F , then $F(x) \cong F(\alpha)$. In $F(x)$, the elements $\{1, x, x^2, \dots\}$ are linearly independent over F . Thus, $[F(\alpha) : F]$ is ∞ .

(2) **Forwards:** From Theorem 3, if α is algebraic over F , $F[x]_{\langle p(x) \rangle} \cong F(x)$ with the map $x \mapsto \alpha$. Note that,

$$F[x]_{\langle p(x) \rangle} \cong \{r(x) \in F[x] : \deg(r) < \deg(p)\} \quad (\deg(0) = -\infty)$$

Thus, $\{1, x, x^2, \dots, x^{\deg(p)-1}\}$ forms a basis for $F[x]_{\langle p(x) \rangle}$. It follows that $[F(\alpha) : F] = \deg(p)$ and $\{1, \alpha, \alpha^2, \dots, \alpha^{\deg(p)-1}\}$ is a basis of $F(\alpha)/F$. \square

Theorem 5. Let E/F be a field extension. If $[E : F] < \infty$, then there exists $\alpha_1, \dots, \alpha_n \in E$ such that

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

Proof. We proceed with induction on $[E : F]$. If $[E : F] = 1$, $E = F$. Suppose that $[E : F] > 1$ and the statement holds for any field extension \tilde{E}/\tilde{F} with $[\tilde{E} : \tilde{F}] < [E : F]$. Let $\alpha_1 \in E/F$. By Theorem 1,

$$[E : F] = [E : F(\alpha_1)][F(\alpha_1) : F].$$

Since $[F(\alpha) : F] > 1$, we have $[E : F] > [E : F(\alpha_1)]$. By induction hypothesis, there exists $\alpha_2, \dots, \alpha_n$ such that

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

Thus, we have

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

as desired. \square

Definition 2.2.6. A field extension E/F is algebraic if every $\alpha \in E$ is algebraic over F . Otherwise, it is transcendental.

Theorem 6. Let E/F be a field extension. If $[E : F] < \infty$, then E/F is algebraic.

Proof. Suppose $[E : F] = n$. For $\alpha \in E$, the elements $\{1, \alpha, \dots, \alpha^n\}$ are not linearly independent over F . Thus, there exists $c_i \in F$ for all $i = 0, \dots, n$, not all 0, such that

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

Thus, α is a root of the polynomial $\sum_{i=0}^n c_i \alpha^i \in F[x]$ so it is algebraic over F . \square

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. If $\alpha, \beta \in L$ with $\beta \neq 0$, we need to show that $\alpha \pm \beta, \alpha\beta, \frac{\alpha}{\beta} \in L$. By definition of L , we have $[F(\alpha) : F] < \infty$ and $[F(\beta) : F] < \infty$. Consider the field $F(\alpha, \beta)$. 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 $F(\beta)$). In other words, $p(x) \in F(\beta)[x]$ such that $p(\alpha) = 0$, we have

$$[F(\alpha, \beta) : F(\beta)] \leq [F(\alpha) : F].$$

Combining this with Theorem 1, we have

$$\begin{aligned} [F(\alpha, \beta) : F] &= [F(\alpha, \beta) : F(\beta)][F(\beta) : F] \\ &\leq [F(\alpha) : F][F(\beta) : F] \end{aligned}$$

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

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

so $a + b \in L$. We can follow a similar line to show $\alpha - \beta, \alpha\beta, \frac{\alpha}{\beta} \in L$. So L is a field. \square

Definition 2.2.7. Let E/F be a field extension. The set,

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

is called the algebraic closure of F in E .

Definition 2.2.8. A field F is algebraically closed if for any algebraic extension E/F , we have $E = F$.

Example 2.2.9. By the Fundamental Theorem of Algebra, \mathbb{C} is algebraically closed.

2.3 Eisenstein's Criterion

Definition 2.3.1. Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. We say $f(x)$ is primitive if $a_n > 0$ and $\gcd(a_0, \dots, a_n) = 1$.

Lemma. Every non-zero polynomial $f(x) \in \mathbb{Q}[x]$ can be written uniquely as a product $F(x) = c f_0(x)$ where $c \in \mathbb{Q}$ and $f_0(x)$ is a primitive polynomial on $\mathbb{Z}[x]$. Moreover, $f(x) \in \mathbb{Z}[x]$ if and only if $c \in \mathbb{Z}$. If so, then $|c|$ is the greatest common divisor of the coefficients of $f(x)$ and the sign of c is the sign of the leading coefficient of $f(x)$.

Theorem (Gauss' Lemma for $\mathbb{Z}[x]$). Let $f(x) \in \mathbb{Z}[x]$ be non-constant. If $f(x)$ is irreducible in $\mathbb{Z}[x]$, then it is irreducible in $\mathbb{Q}[x]$.

Example 2.3.2. The converse of Section 2.3 is not true. Consider the polynomial $2x + 8$ is irreducible in $\mathbb{Q}[x]$, but $2x + 8 = 2(x + 4)$ is reducible in $\mathbb{Z}[x]$.

Remark. $f(x) \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$ if and only if either

1. $f(x)$ is a prime integer
2. $f(x)$ is a primitive polynomial which is irreducible in $\mathbb{Q}[x]$

Theorem 8 (Eisenstein's Criterion for $\mathbb{Z}[x]$). Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ and let p be a prime integer. Suppose that $p \nmid a_n$, $p \mid a_i$ for all $0 \leq i \leq (n-1)$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$. In particular, if $f(x)$ is primitive, then it is irreducible in $\mathbb{Z}[x]$.

Proof. Consider the map $f : \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x]$ defined by

$$f(x) \mapsto \bar{f}(x) = \bar{a}_n x^n + \cdots + \bar{a}_1 x + \bar{a}_0$$

where $\bar{a}_i = a_i \pmod{p} \in \mathbb{Z}_p$. Since $p \nmid a_n$ and $p \mid a_i$ for all $0 \leq i \leq (n-1)$, we have $\bar{f}(x) = \bar{a}_n x^n$ with $\bar{a}_n \neq 0$. If $f(x)$ is reducible in $\mathbb{Q}[x]$, then it can be factored in $\mathbb{Z}[x]$ into polynomials of positive degree, say $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbb{Z}[x]$ and $\deg(g), \deg(h) \geq 1$. It follows that $\bar{a}_n x^n = \bar{g}(x)\bar{h}(x)$ from which we see that $\bar{g}(x)$ and $\bar{h}(x)$ have no constant terms in $\mathbb{Z}_p[x]$, as $\mathbb{Z}_p[x]$ is a UFD. Since the constants of both $g(x)$ and $h(x)$ are divisible by p , this implies that the constant of $f(x)$ is divisible by p^2 , which leads to a contradiction. So, $f(x)$ is irreducible in $\mathbb{Q}[x]$ \square

Example 2.3.3. The polynomial $2x^7 + 3x^4 + 6x^2 + 12$ is irreducible in $\mathbb{Q}[x]$ by applying Eisenstein's Criterion with $p = 3$.

Example 2.3.4. Consider the n^{th} cyclotomic polynomial defined by

$$\Phi_n(x) = \sum_{\substack{1 \leq k \leq n \\ \gcd(k, n) = 1}} \left(x - e^{2i\pi \frac{k}{n}} \right).$$

If $n = p$ where p is a prime number, then $\xi_p = e^{\frac{2i\pi}{p}} = \cos \frac{2\pi}{p} + i \sin \frac{2\pi}{p}$ (the p^{th} root of 1) is a root of the p^{th} cyclotomic polynomial. Notice here, since p is co-prime with all $1 \leq k \leq p$, we have

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

Eisenstein's Criterion does not imply the irreducibility of $\Phi_p(x)$ immediately; however, consider

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

with the Binomial Theorem. Since p is prime, $p \nmid 1$, $p \mid \binom{p}{i}, \forall i \in \{1, \dots, p-1\}$ and $p^2 \nmid \binom{p}{p-1}$. Here, Eisenstein's Criterion gives that $\Phi_p(x+1)$ is irreducible in $\mathbb{Q}[x]$, but if $\Phi_p(x) = g(x)f(x)$, then $\Phi_p(x+1) = g(x+1)h(x+1)$ gives a factorization for $\Phi_p(x+1)$, so $\Phi_p(x)$ must be irreducible in $\mathbb{Q}[x]$ as well. Furthermore, since $\Phi_p(x)$ is primitive, $\Phi_p(x)$ is also irreducible in $\mathbb{Z}[x]$.

Example 2.3.5. Let p be prime and $\xi_p = e^{\frac{2i\pi}{p}}$. Since it is a root of $\Phi_p(x)$, which is irreducible, by Theorem 4,

$$[\mathbb{Q}(\xi_p) : \mathbb{Q}] = \deg(\Phi_p(x)) = p - 1.$$

The field $\mathbb{Q}(\xi_p)$ is called the p^{th} cyclotomic extension on \mathbb{Q} .

Example 2.3.6. Let $\bar{\mathbb{Q}}$ be the algebraic closure of \mathbb{Q} in \mathbb{C} . Since $\xi_p \in \mathbb{Q}$, we have

$$[\bar{\mathbb{Q}} : \mathbb{Q}] \geq [\mathbb{Q}(\xi_p) : \mathbb{Q}] = p - 1.$$

Since $p \rightarrow \infty$, we have $[\bar{\mathbb{Q}} : \mathbb{Q}]$ is ∞ . We have seen in Theorem 6 that if E/F is finite, then E/F is algebraic. However, this example shows that the converse is false.



Now, let R be any unique factorization domain and let F be its fraction field. Then $R[x]$ is a subring of $F[x]$.

Lemma (Gauss' Lemma). *Let R be a UFD with the fraction field F . Let $f(x) \in R[x]$ be non-constant. If $f(x)$ is irreducible in $R[x]$, then it is irreducible in $F[x]$.*

Theorem 9 (Eisenstein's Criterion). *Let R be a UFD with the fraction field F . Let ℓ be an irreducible element of R . If $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$ with $n \geq 1$, $\ell \nmid a_n$, $\ell \mid a_i$, for all $0 \leq i \leq n-1$ and $\ell^2 \nmid a_0$, then $f(x)$ is irreducible in $F[x]$.*

3 Splitting Fields

Definition 3.0.1. Let E/F be a field extension. We say $f(x) \in R[x]$ splits over E if E contains all roots of $f(x)$. In other words, $f(x)$ is a product of linear factors in $E[x]$.

Definition 3.0.2. Let \tilde{E}/F , $f(x) \in F[x]$ and $F \subseteq E \subseteq \tilde{E}$. If

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

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

3.1 Existence of Splitting Fields

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 map

$$\Psi : F \rightarrow E, \quad a \mapsto a + I$$

Since F is a field and $\Psi \neq 0$, Ψ is injective. Thus, by identifying F with $\Psi(F)$, F is a subfield of E .

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

Notice,

$$\begin{aligned} p(x) &= a_0 + a_1x + \cdots + a_nx^n \\ &= (a_0 + I) + (a_1 + I)x + \cdots + (a_n + I)x^n \\ &\in E[x]. \end{aligned}$$

Thus, we have

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

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

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 proceed with induction on $\deg(f)$. If $\deg(f) = 1$, let $E = F$ and we are done. Suppose $\deg(f) > 1$ and the statement holds for all $g(x)$ with $\deg(g) < \deg(f)$ ($g(x)$ need not to be in $F[x]$). We write $f(x) = p(x)h(x)$, where $p(x), h(x) \in F[x]$ and $p(x)$ is irreducible. By Theorem 10, there exists a field K such that $F \subseteq K$ and K containing a root of $p(x)$, say α . Thus, $p(x) = (x - \alpha)q(x)$ and $f(x) = (x - \alpha)g(x)h(x)$ where $q(x) \in K[x]$. Since $\deg(hq) < \deg(f)$, by induction, there exists a field E containing K over which $h(x)q(x)$ splits. It follows that $f(x)$ splits over E . □

Theorem 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 Theorem 11, there exists a field extension E/F over which $f(x)$ splits, say $\alpha_1, \alpha_2, \dots, \alpha_n$ are roots of $f(x) \in E$. Consider $F(\alpha_1, \dots, \alpha_n)$. The field contains all the roots of $f(x)$ and $f(x)$ does not split over any proper subfield of it. Thus, $F(\alpha_1, \dots, \alpha_n)$ is the splitting field of $f(x)$ in E . In addition, since α_i are all algebraic, $F(\alpha_1, \dots, \alpha_n)/F$ is finite. \square

3.2 Uniqueness of Splitting Fields

We have seen from Theorem 12 that for a field extension \tilde{E}/F , a splitting field of $f(x) \in F[x]$ in E is of the form $F(\alpha_1, \dots, \alpha_n)$ where α_i are roots of $f(x)$ in \tilde{E} . Thus, it is unique within \tilde{E} .

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

Definition 3.2.1. Let $\phi : R \rightarrow R'$ be a ring homomorphism, and $\Phi : R[x] \rightarrow R'[x]$ be the unique ring homomorphism satisfying $\Phi|_R = \phi$ and $\Phi(x) = x$. In this case, we say Φ extends ϕ . More generally, if $R \subseteq S$, $R' \subseteq S'$, and $\Phi : S \rightarrow S'$ is a ring homomorphism with $\Phi|_R = \phi$, we say Φ extends ϕ .

Theorem 13. Let $\phi : F \rightarrow F'$ be an isomorphism of fields and $f(x) \in F[x]$. Let $\Phi : F[x] \rightarrow F'[x]$ be the unique ring homomorphism which extends ϕ . Let $f'(x) = \Phi(f(x))$ and E/F and E'/F' be splitting fields of $f(x)$ and $f'(x)$ respectively. Then there exists an isomorphism $\Psi : E \rightarrow E'$.

Proof. We proceed with induction on $[E : F]$. If $[E : F] = 1$, then $f(x)$ is a product of linear factors in $F[x]$, and so is $f'(x)$ in $F'[x]$. Thus, $E = F$ and $E' = F'$ so take $\Psi = \phi$ and we are done. Now, suppose $[E : F] < \infty$ and the statement is true for all field extensions \tilde{E}/\tilde{F} with $[\tilde{E} : \tilde{F}] < [E : F]$. Let $p(x) \in F[x]$ be an irreducible factor of $f(x)$ with $\deg(p) > 1$ and let $p'(x) = \Phi(p(x))$ (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 $\alpha' \in E'$ be roots of $p(x)$ and $p'(x)$ respectively. From Theorem 3, we have an F -isomorphism,

$$F(\alpha) \cong F[x]/\langle p(x) \rangle, \quad \alpha \mapsto x + \langle p(x) \rangle$$

Similarly, there is an F' -isomorphism,

$$F'(\alpha') \cong F'[x]/\langle p'(x) \rangle, \quad \alpha' \mapsto x + \langle p'(x) \rangle$$

Consider the isomorphism $\Phi : F[x] \rightarrow F'[x]$ which extends ϕ . Since $p'(x) = \Phi(p(x))$, there exists a field isomorphism,

$$\tilde{\Phi} : F[x]/\langle p(x) \rangle \rightarrow F'[x]/\langle p'(x) \rangle, \quad x + \langle p(x) \rangle \mapsto x + \langle p'(x) \rangle$$

which extends ϕ . It follows that there exists a field isomorphism,

$$\tilde{\phi} : F(\alpha) \rightarrow F'(\alpha'), \quad \alpha \mapsto \alpha'$$

which extends ϕ . Note that since $\deg(p) > 1$, $[E : F(\alpha)] < [E : F]$. Since E (respectively E') is the splitting field of $f(x) \in F(\alpha)[x]$ (respectively $f(x) \in F(\alpha')[x]$) over $F(\alpha)$ (respectively $F(\alpha')$), by induction, there exists $\Psi : E \rightarrow E'$ which extends $\tilde{\phi}$. Thus, Ψ extends ϕ . \square

Corollary 14. Any two splitting fields of $f(x) \in F[x]$ over F are F -isomorphic. Thus, we say “the” splitting field of $f(x)$ over F .

Proof. Let $\phi : F \rightarrow F$ be the identity map and apply Theorem 13 \square

3.3 Degree of Splitting Fields

Theorem 15. *If E/F is the splitting field of $f(x)$, then $[E : F] \mid \deg(f)!$.*

Proof. We proceed by induction on $\deg(f)$. If $\deg(f) = 1$, choose $E = F$ and we have $[E : F] \mid 1$. Suppose $\deg(f) > 1$ and the statement holds for all $g(x)$ with $\deg(g) < \deg(f)$. We break this down into 2 cases.

Case 1: If $f(x) \in F[x]$ is irreducible and $\alpha \in E$ is a root of $f(x)$, by Theorem 13,

$$F(\alpha) \cong F[x]/\langle f(x) \rangle \quad \text{and} \quad [F(\alpha) : F] = \deg(f) = n.$$

We write $f(x) = (x - \alpha)g(x) \in F(\alpha)[x]$ with $g(x) \in F(\alpha)[x]$. Since E is the splitting field of $g(x)$ over $F(\alpha)$ and $\deg(g) = n - 1$, by induction hypothesis, $[E : F(\alpha)] \mid (n - 1)!$. Since $[E : F] = [E : F(\alpha)][F(\alpha) : F]$, it follows that $[E : F] \mid n!$.

Case 2: If $f(x)$ is not irreducible, write $f(x) = g(x)h(x)$ with $g(x), h(x) \in F[x]$, $\deg(g) = m$, $\deg(h) = k$, $1 \leq m, k < n$ and $m + k = n$. Let K be the splitting field of $g(x)$ over F . Since $\deg(g) = m$, by induction, $[K : F] \mid m!$. Since E is the splitting field of $h(x)$ over K and $\deg(h) = k$, by induction hypothesis, $[E : K] \mid k!$. Thus, $[E : F] \mid m!k!$, which is a factor of $n!$ as

$$\frac{n!}{m!k!} = \binom{n}{m} \in \mathbb{Z}$$

□

4 Finite Fields

4.1 Prime Fields

Definition 4.1.1. The prime field of a field F is the intersection of all subfields of F .

Theorem 16. If F is a field, then its prime field is isomorphic to either \mathbb{Q} or $\mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$ for some prime p .

Proof. Consider the ring map $\chi : \mathbb{Z} \rightarrow F$ defined by

$$\chi(n) = n \cdot 1 = \underbrace{1 + \cdots + 1}_{n \text{ times}}$$

Let $I = \ker(\chi)$, the kernel of χ . Since $\mathbb{Z}/I \cong \text{im}(\chi)$, a subring of F , it is an integral domain. Thus, I is a prime ideal. We break this down to two cases.

Case 1: If $I = \langle 0 \rangle$, then $\mathbb{Z} \subseteq F$. Since F is a field, $\mathbb{Q} = \text{Frac}(\mathbb{Z}) \subseteq F$.

Case 2: If $I = \langle p \rangle$, then

$$\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} \cong \text{im } \chi \subseteq F$$

□

Definition 4.1.2. Given a field F , if its prime field is isomorphic to \mathbb{Q} (respectively \mathbb{Z}_p), we say F has characteristic 0 (respectively characteristic p) denoted by $\text{ch}(F) = 0$ (respectively $\text{ch}(F) = p$).

Remark. Note that if $\text{ch}(F) = p$, for $a, b \in F$,

$$(a + b)^p = a^p + b^p.$$

Using this property, the following proposition follows.

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

4.2 Formal Derivatives and Repeated Roots

Definition 4.2.1. If F is a field, the monomials $\{1, x, x^2, \dots\}$ for a F -basis of $F[x]$. Define the linear operator

$$D : F[x] \rightarrow F[x]$$

by $D(1) = 0$ and $D(x^i) = ix^{i-1}$ for all $i \in \mathbb{N}$. Thus for

$$f(x) = a_0 + a_1x + \cdots + a_nx^n, a_i \in F$$

we have

$$D(f)(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}.$$

Note that

1. D is linear: $D(f + g) = D(f) + D(g)$
2. D respects the Leibniz Rule: $D(fg) = (D(f))g + f(D(g))$.

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

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

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

Proof. 1. Backwards is trivial. Suppose we have $f(x) = a_0 + a_1x + \cdots + a_nx^n$, then $f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1} = 0$. This implies that $ia_i = 0$ for all $1 \leq i \leq n$. Since $\text{ch}(F) = 0$, $i \neq 0$. Thus, $a_i = 0$ for all $i \geq 1$. This, $f(x) = a_0 \in F$.

2. Forwards. For $f(x) = a_0 + a_1x + \cdots + a_nx^n$, $f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1} = 0$ implies that $ia_i = 0$ for all $1 \leq i \leq n$. Since $\text{ch}(F) = p$, $ia_i = 0$ implies that $ia_i = 0$ implies that $a_i = 0$ unless $p \mid i$. Thus,

$$f(x) = a_0 + a_px^p + \cdots + a_{mp}x^{mp} = g(x^p)$$

where $g(x) = a_0 + a_px^p + \cdots + a_{mp}x^{mp} \in F[x]$.

Backwards. Write $g(x) = b_0 + b_1x + \cdots + b_mx^m \in F[x]$. Then,

$$f(x) = g(x^p) = b_0 + b_1x^p + \cdots + b_mx^{mp}.$$

Thus, $f'(x) = pb_1x^{p-1} + 2pb_2x^{2p-1} + \cdots + mpb_mx^{pm-1}$. Since $\text{ch}(F) = p$, we have $f'(x) = 0$. □

Definition 4.2.2. Let E/F is a field extension and $f(x) \in F[x]$. We say $\alpha \in E$ is a repeated root of $f(x)$ if $f(x) = (x - \alpha)^2g(x)$ for some $g(x) \in E[x]$.

Theorem 19. Let E/F is a field extension and $f(x) \in F[x]$. Then α is a repeated root of $f(x)$ if and only if $(x - \alpha)$ divides both f and f' . In other words, $(x - \alpha) \mid \gcd(f, f')$.

Proof. Forwards. Suppose $f(x) = (x - \alpha)^2g(x)$. Then,

$$\begin{aligned} f'(x) &= 2(x - \alpha)g(x) + (x - \alpha)^2g'(x) \\ &= (x - \alpha)(2g(x) + (x - \alpha)g'(x)) \end{aligned}$$

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

Backwards. Suppose $(x - \alpha)$ divides both f and f' . We write $f(x) = (x - \alpha)h(x)$ where $h(x) \in E[x]$. Then, $f'(x) = h(x) + (x - \alpha)h'(x)$. Since $f'(\alpha) = 0$, we have $h(\alpha) = 0$. Thus, $(x - \alpha)$ is a factor of $h(x)$ and $f(x) = (x - \alpha)^2g(x)$ for some $g(x) \in E[x]$. □

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

4.3 Finite Fields

Proposition 21. If F is a finite field, then $\text{ch}(F) = p \neq 0$ for some prime p and $|F| = p^n$ for some $n \in \mathbb{N}$.

Proof. Since F is a finite field, by Theorem 16, its prime field is \mathbb{Z}_p . Since F is a finite dimensional vector space over \mathbb{Z}_p , we have

$$F \cong \underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n \text{ summands}}.$$

Thus $|F| = p^n$. □

Theorem 22. *Let F be a field and $F^* = F \setminus \{0\}$, multiplicative group of nonzero elements of F . Let G be a finite subgroup of F^* , then G is a cyclic group. In particular, if F is a finite field, then F^* is a cyclic group.*

Proof. If $G = \langle 1 \rangle$, the result follows immediately. Otherwise, since G is a finite abelian group,

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

where $n_i > 1$ and $n_1 \mid \cdots \mid n_r$. Since $n_r \left(\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z} \right) = 0$, it follows that every $u \in G$ is a root of $x^{n_r} - 1 \in F[x]$. Since the polynomial has at most n_r distinct roots in F , we have $r = 1$ and $G \cong \mathbb{Z}/n_r\mathbb{Z}$. \square

By taking u to be a generator of the multiplicative group F^* , we have the following corollary.

Corollary 23. *If F is a finite field, then F is a simple extension of \mathbb{Z}_p . In other words, $F = \mathbb{Z}_p(u)$ for some $u \in F$.*

Proposition 24. *Let p be prime and $n \in \mathbb{N}$. Then F is a finite field with $|F| = p^n$ if and only if F is a splitting field of $x^{p^n} - x$ over \mathbb{Z}_p .*

Proof. Forwards: If $|F| = p^n$, then $|F^*| = p^n - 1$. Thus, every $u \in F$ satisfies $u^{p^n-1} = 1$ and thus is a root of $x(x^{p^n-1} - 1) = x^{p^n} - x \in \mathbb{Z}_p[x]$. Since $0 \in F$ is also a root of $x^{p^n} - x$, the polynomial $x^{p^n} - x$ has distinct p^n distinct roots in F . In other words, it splits over F . Thus F is a splitting field of $x^{p^n} - x$ over \mathbb{Z}_p .

Backwards: Suppose F is a splitting field of $f(x) = x^{p^n} - x$ over \mathbb{Z}_p . Since $\text{ch}(F) = p$, we have

$$\begin{aligned} f'(x) &= p^n x^{p^n-1} - 1 \\ &\equiv -1 \pmod{p}. \end{aligned}$$

Now, since $\gcd(f, f') = 1$, by Corollary 20, $f(x)$ has p^n distinct roots in F . Let E be the set of the roots of $f(x)$ in F . Let $\varphi : F \rightarrow F$ be given by $u \mapsto u^{p^n}$. For $u \in F$, u is a root of $f(x)$ if and only if $\varphi(u) = u$. Thus, the set E is a subfield of F of order p^n which contains \mathbb{Z}_p . Since F is a splitting field, it is generated over \mathbb{Z}_p by the roots of $f(x)$, in other words, the elements of E . Thus, $F = \mathbb{Z}_p(E) = E$. \square

As a direct consequence of Proposition 24 and Corollary 14, we have the following corollary.

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.*

4.4 Separable Polynomials

Definition 4.4.1. Let F be a field and $f(x) \in F[x]$, $f \neq 0$. If $f(x)$ is irreducible, we say $f(x)$ is separable over F if it has no repeated root in any extension E of F . In the general case, we say $f(x)$ is separable over F if each irreducible factor of f is separable over F .

Example 4.4.2. $f(x) = (x - 2)^2$ is separable over \mathbb{Q} .

Example 4.4.3. Consider the polynomial $f(x) = x^n - a \in F[x]$ with $n \geq 2$. We recall that if $\gcd(f, f') = 1$, then $f(x)$ has no repeated root in any extension of F . In other words, $f(x)$ is separable. Note that if $a = 0$, the only irreducible factor of $f(x)$ is x and $\gcd(x, 1) = 1$. Thus, $f(x)$ is separable. Now, assume $a \neq 0$. Note that $f'(x) = nx^{n-1}$.

(1) If $\text{ch}(F) = 0$, we have $\gcd(f, f') = 1$ since

$$\begin{aligned} 1 &= \frac{x}{na} nx^{n-1} - \frac{1}{a}(x^n - a) \\ &= \frac{x}{na} f' - \frac{1}{a} f \end{aligned}$$

Thus, f is separable.

(2) If $\text{ch}(F) = p$ and $\gcd(n, p)$, then by Fermat's Little Theorem, $f(x) = x^n - a$ and $f'(x) = nx^{n-1} = 1$ so $\gcd(f, f') = 1$ and $f(x)$ is separable.

(3) If $\text{ch}(F) = p$ and $\gcd(n, p) \neq 1$, consider $f(x) = x^p - a$. Since $f'(x) = px^{p-1} = 0$, we have $\gcd(f, f') \neq 1$. However, it is still possible that all irreducible factors $\ell(x)$ of $f(x)$ has the property that $\gcd(\ell, \ell') = 1$. 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 .

(3.1) If $a \in F^p$, say $a = b^p$ for some $b \in F$, then

$$f(x) = x^p - b^p = (x - b)^p \quad (\text{by Binomial Theorem})$$

which is irreducible. Since each irreducible factor of $f(x)$ is linear, thus separable. Thus, $f(x)$ is separable.

(3.2) Suppose $a \notin F^p$

Claim. $f(x) = x^p - a$ is irreducible in $F[x]$.

We write $x^p - a = g(x)h(x)$ where $g(x), h(x) \in F[x]$ 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 that $\beta \notin F$, otherwise $a = b^p \in F^p$. We have

$$x^p - a = x^p - \beta^p = (x - \beta)^p. \quad (\text{by Binomial Theorem})$$

Thus, $g(x) = (x - \beta)^r$ and $h(x) = (x - \beta)^s$ for some $r, s \in \mathbb{N} \cup \{0\}$ and $r + s = p$. We write,

$$g(x) = x^r - r\beta x^{r-1} + \dots$$

then $r\beta \in F$. Since $\beta \notin F$, as an element of F , we have $r = 0$. Thus, as an integer, we have $r = 0$ or $r = p$. It follows that wither $g(x) = 1$ or $h(x) = 1$ in $F[x]$. Thus, $f(x)$ is irreducible.

Since $f(x)$ is irreducible and $f(x) = (x - \beta)^p \in E[x]$, it is not separable. This type of polynomial is called a purely inseparable polynomial.

Definition 4.4.4. 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 $\text{ch}(F) = 0$, then F is perfect.

2. If $\text{ch}(F) = p$ and $F = F^p$, then F is perfect.

Proof. Let $r(x) \in F[x]$ be irreducible. Then

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

Suppose $r(x)$ is not separable. Then by Corollary 20, $\gcd(r, r') \neq 1$, so it must be that $\gcd(r, r') = 0$.

1. If $\text{ch}(F) = 0$, from Theorem 18, $r'(x) = 0$ implies that $r(x) = c \in F$, which is a contradiction since $\deg(r) \geq 1$. Thus, $r(x)$ is separable and F is perfect.
2. If $\text{ch} = p$, from Theorem 18, $r'(x) = 0$ implies that

$$r(x) = a_0 + a_1x^p + a_2x^{2p} + \cdots + a_mx^{mp}, a_i \in F$$

Since $F = F^p$, we can write $a_i = b_i^p$ with $b_i \in F$. Thus,

$$\begin{aligned} r(x) &= b_0^p + b_1^p x^p + b_2^p x^{2p} + \cdots + b_m^p x^{mp} \\ &= (b_0 + b_1x + b_2x^2 + \cdots + b_mx^m)^p \end{aligned}$$

which raises a contradiction since $r(x)$ is irreducible. Thus, $r(x)$ must be separable and F is perfect. □

Remark. Let $\text{ch}(F) = p$ and $F \neq F^p$ (e.g. $F = \mathbb{F}_p(x)$). If we take $a \in F/F_p$, then the polynomial $x^p - a$ is not separable. Thus, if $\text{ch}(F) = p$, F is perfect if and only if $F^p = F$.

Corollary 27. *Every finite field is perfect.*

Proof. Every finite field F with $|F| = p^n$ is the splitting field of $x^{p^n} - x$ over \mathbb{Z}_p for some prime p and $n \in \mathbb{N}$. Thus, for every $a \in F$, $a = a^{p^n} = (a^{p^{n-1}})^p$. Since $a^{p^{n-1}} \in F$, $F = F^p$. Thus, by Theorem 26, F is perfect. □

Remark. It is possible that $F^p = F$ and F is an infinite field, say $F = \overline{\mathbb{F}_p}$.

5 The Sylow Theorems

Recall the following definitions and theorems from Group Theory:

Theorem (Lagrange's Theorem). *If H is a subgroup of a group G , then $|G| = [G : H]|H|$. In particular, if G is finite, and $g \in G$, then $|\langle g \rangle|$ divides $|G|$.*

We can ask the reverse question; if a positive integer m divides the order of a group G , does G have a subgroup of order m ?

Definition 5.0.1. An action of a group G on a set S is a function $G \times S \rightarrow S$ (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 $(g_1g_2)x = g_1(g_2x)$). We say G acts on S by a group action.

Definition 5.0.2. If G acts on S , for $x \in S$, we define the orbit of x by $\bar{x} := \{gx : g \in G\}$.

Definition 5.0.3. If G acts on S , for $x \in S$, we define the stabilizer of x by $G_x := \{g \in G : gx = x\}$. G_x is a subgroup of G and $|\bar{x}| = [G : G_x]$.

Definition 5.0.4. Let G be a group acting on itself by conjugation. Then, for $x \in G$, we define the centralizer of x by $C_G(x) := G_x = \{g \in G : gxg^{-1} = x\}$.

Definition 5.0.5. Let S be all subgroups of G and let G act on S by conjugation. Then, for $K \in S$, we define the normalizer of K by $N_G(K) := G_K = \{g \in G : gKg^{-1} = K\}$.

Definition 5.0.6. Let G be a group. Then we define the center of G by $C(G) := \{g \in G : gxg^{-1} = x, \forall x \in G\}$.

Theorem (Class Equation of a Group). *Suppose G is a finite group acting on itself by conjugation, $C(G)$ is the center of G , and C_1, C_2, \dots, C_r are all the conjugacy classes in G comprising the elements outside the center. Let g_i be an element in C_i for each $1 \leq i \leq r$. Then, we have*

$$|G| = |C(G)| + \sum_{i=1}^r |G : C_G(g_i)|.$$

Lemma 28. *Let H be a group of order p^n for some prime p , which acts on a finite set S . Let $S_0 = \{x \in S : hx = x, \forall h \in H\}$. Then, we have $|S| \equiv |S_0| \pmod{p}$.*

Proof. For $x \in S$, $|\bar{x}| = 1$ if and only if $x \in S_0$. Thus, S can be written as a disjoint union $S = S_0 \cup \bar{x}_1 \cup \dots \cup \bar{x}_n$. Thus,

$$|S| = |S_0| + \sum_{i=1}^n |\bar{x}_i|.$$

Since $|\bar{x}_i| > 1$ and $|\bar{x}_i| = [H : H_{x_i}]$ divides $|H| = p^n$, we have $p \mid |\bar{x}_i|$ for all i . It follows that $|S| \equiv |S_0| \pmod{p}$. \square

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

Proof. Consider the set,

$$S = \{(a_1, \dots, a_p) : a_i \in G, a_1 \cdots a_p = e\}.$$

Since a_p is uniquely determined and $|G| = n$, we have $|S| = n^{p-1}$. Since $p \mid n$, we have $|S| \equiv 0 \pmod{p}$. Let the group \mathbb{Z}_p act on S by cyclic permutation, in other words, for $k \in \mathbb{Z}_p, k(a_1, \dots, a_p) = (a_{k+1}, a_{k+2}, \dots, a_p, a_1, \dots, a_k)$. Since $(a_1, \dots, a_p) \in S_0$ if and only if $a_1 = \dots = a_p$. Clearly, $(e, \dots, e) \in S_0$, so $|S_0| \geq 1$. By Lemma 28, we have $|S_0| \equiv |S| \equiv 0 \pmod{p}$. So $|S_0| \geq p$. Thus, there exists $a \neq e$ such that $(a, \dots, a) \in S_0$ which implies that $a^p = e$. Since p is prime, the order of a is p . \square

5.1 The Sylow Theorems

Definition 5.1.1. Let p be a prime. A group in which the order of every element is a non-negative power of p is called a p -group.

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

Proof. This is a direct consequence of Theorem 29. □

Lemma 31. The center $C(G)$ of a nontrivial finite p -group G contains more than 1 element.

Proof. Since G is a p -group by Corollary 30, $|G|$ is a power of p . Recall the class equation:

$$|G| = |C(G)| + \sum_{i=1}^n [G : C_G(x_i)], \quad \text{where } [G : C_G(x_i)] \geq 1.$$

Since $|G|$ is a power of p , $[G : C_G(x_i)] \mid |G|$, and $[G : C_G(x_i)] > 1$. We see that $p \mid [G : C_G(x_i)]$. It follows that $p \mid |C(G)|$ since $|C(G)| \geq 1$ so $C(G)$ has at least p elements. □

Definition 5.1.2. If H is a subgroup of a group G , then the normalizer of H is defined by

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

In particular, $H \triangleleft N_G(H)$.

Lemma 32. If p is prime and H is a p -subgroup of a finite group G , then $[N_G(H) : H] \equiv [G : H] \pmod{p}$.

Proof. Let S be the set of all left cosets of H in G and let H act on S by left translation, $G \times S \rightarrow S$ defined by,

$$h \cdot xH \mapsto (hx)H$$

which fixes on coset to another. Then, $|S| = [G : H]$. For some fixed $x \in G$, consider the set S_0 defined by $xH \in S_0 \iff hxH = xH$ for all $h \in H$. In other words, all elements of S_0 are fixed by the group action. Now, we have,

$$\begin{aligned} xH \in S_0 &\iff hxH = xH \\ &\iff x^{-1}hxH = H \\ &\iff x^{-1}Hx = H \\ &\iff x \in N_G(H) \end{aligned}$$

So, $|S_0| = [N_G(H) : H]$. By Lemma 28,

$$\begin{aligned} [N_G(H) : H] &= |S_0| \\ &\equiv |S| \pmod{p} \\ &= [G : H]. \end{aligned}$$

□

Corollary 33. If H is a p -subgroup of a finite group G such that $p \mid [G : H]$, 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 $[N_G(H) : H] \geq p$, so $N_G(H) \neq H$. □

Theorem 34 (First Sylow Theorem). *Let G be a group with order $p^n m$ with p prime, $n \geq 1$, $\gcd(p, m) = 1$. Then G contains a subgroup of order p^i for all $1 \leq i \leq n$ which is normal under some subgroup of order p^{i+1} .*

Proof. We proceed with induction on i . For $i = 1$, since $p \mid |G|$, we have by Theorem 29 that G contains an element a of order p , so $|\langle a \rangle| = p$. Suppose that the statement holds for some $1 \leq i \leq n$, say H is a subgroup of order p^i . Now, from Corollary 33, we have $p \mid [N_G(H) : H]$ and $[N_G(H) : H] \geq p$, since $H \triangleleft N_G(H)$. Then, by Theorem 29, $N_G(H)/H$ contains a subgroup of order p . Such a group is of the form H'/H where H' is a subgroup of $N_G(H)$ containing H . Since $H \triangleleft N_G(H)$, we have $H \triangleleft H'$. Finally, $|H'| = |H| \left| \frac{H'}{H} \right| = p^{i+1}$. \square

Definition 5.1.3. A subgroup P of a group G is said to be a Sylow p -subgroup if P is a maximal p -subgroup of G . In other words, if $P \subseteq H \subseteq G$ with H a p -subgroup of G , then $P = H$.

Corollary 35. *Let G be a group of order $p^n m$ where p is a prime, $n \geq 1$, $\gcd(p, m) = 1$. Let H be a p -subgroup of G . Then, all the following hold:*

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 $P \triangleleft G$.

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 -subgroups of G are conjugate.*

Proof. Let S be the set of all left cosets of P in G , and let H act on S by left multiplication. By Lemma 28, we have $|S_0| \equiv |S| = [G : P] \pmod{p}$. Since $p \nmid [G : P]$, we have $|S_0| \neq 0$. There exists $xP \in S_0$ for some $x \in G$. Note that

$$\begin{aligned} xP \in S_0 &\iff hxP = xP, \quad \forall h \in H \\ &\iff x^{-1}hxP = P, \quad \forall h \in H \\ &\iff x^{-1}Hx \subseteq P \\ &\iff H \subseteq xPx^{-1}. \end{aligned}$$

In particular, if H is a Sylow p -subgroup, then $|H| = |P| = |xPx^{-1}|$. Thus, $H = xPx^{-1}$. \square

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

Proof. By Theorem 36, the number of Sylow p -subgroups of G is the number of conjugates 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 -subgroups of G and hence of $N_G(Q)$. Thus, by Corollary 35, they are conjugate in $N_G(Q)$. Since $Q \triangleleft N_G(Q)$, this can only occur if $Q = P$. Thus, $S_0 = \{P\}$ and by Lemma 28, $|S| \equiv |S_0| \equiv 1 \pmod{p}$. Thus, $|S| = kp + 1$ for some $k \in \mathbb{N} \cup \{0\}$. \square

Example 5.1.4. 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 -subgroups of G . By Theorem 37, we have $n_3 \mid 15$ and $n_3 \equiv 1 \pmod{3}$. Thus, $n_3 = 1$. Similarly, since $n_5 \mid 15$ and $n_5 \equiv 1 \pmod{5}$, $n_5 = 1$. It follows that there is only one Sylow 3-subgroup and one Sylow 5-subgroup in G , say P_3 and P_5 respectively. Thus, $P_3 \triangleleft G$ and $P_5 \triangleleft G$. 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 that

$$G \cong P_3 \times P_5 \cong \mathbb{Z}/\langle 3 \rangle \times \mathbb{Z}/\langle 5 \rangle \cong \mathbb{Z}/\langle 15 \rangle.$$

Example 5.1.5. There are exactly two isomorphism classes of groups of order 21.

Let G be a group of order $21 = 7 \cdot 3$. Let n_p be the number of Sylow p -subgroups of G . By Theorem 37, we have $n_3 \mid 21$ and $n_3 \equiv 1 \pmod{3}$. Thus, $n_3 = 1$ or 7. Similarly, we have $n_7 \mid 21$ and $n_7 \equiv 1 \pmod{7}$. Thus, $n_7 = 1$. It follows that G has a unique Sylow 7-subgroup, say P_7 and note that $P_7 \triangleleft G$ and P_7 is cyclic, say $P_7 = \langle x \rangle$ with $x^7 = 1$. Let H be a Sylow 3-subgroup. Since $|H| = 3$, H is cyclic and $H = \langle y \rangle$ with $y^3 = 1$. Since $P_7 \triangleleft G$, we have $xyx^{-1} = x^i$ for some power $i \in [0, 6]$. It follows that

$$\begin{aligned} x &= y^3 x y^{-3} \\ &= y^2 y x y^{-1} y^{-2} \\ &= y^2 x^i y^{-2} \\ &= y x^{i^2} y^{-1} \\ &= x^{i^3}. \end{aligned}$$

Since $x^{i^3} = x$ and $x^7 = 1$, we have $i^3 - 1 \equiv 0 \pmod{7}$. Then, it must be that $i = 1, 2, 4$.

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

2. If $i = 2$, then $xyx^{-1} = x^2$. Thus,

$$G = \{x^i y^j : 0 \leq i \leq 6, 0 \leq j \leq 2, yxy^{-1} = x^2\}$$

which has 21 distinct elements. Here, G is generated by x and y .

3. If $i = 4$, then $xyx^{-1} = x^4$. 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 get back to case (2).

6 Solvable Groups

Definition 6.0.1. A group G is solvable if there exists a tower of subgroups

$$\{1\} = G_0 < G_1 < \cdots < G_k = G$$

such that $G_i \triangleright G_{i+1}$ and G_i/G_{i+1} is abelian.

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

Example 6.0.2. Consider the symmetric group S_4 . Let A_4 be the alternating subgroup of S_4 and $V \cong \mathbb{Z}/\langle 2 \rangle \times \mathbb{Z}/\langle 2 \rangle$ the Klein 4 group. Note that A_4 and V are normal subgroups of S_4 . We have

$$S_4 > A_4 > V > \{1\}.$$

Since $S_4/A_4 \cong \mathbb{Z}/\langle 2 \rangle$ and $A_4/V \cong \mathbb{Z}/\langle 3 \rangle$, we see that S_4 is solvable.

Theorem 38 (Second Isomorphism Theorem). *If H and N are subgroups of a group G with $N \triangleleft G$, then $H/H \cap N \cong NH/N$.*

Theorem 39 (Third Isomorphism Theorem). *If H and N are normal subgroups of a group G such that $N \subseteq H$, then H/N is a normal subgroup of G/N and $(G/N)/(H/N) \cong G/(NH)$.*

Theorem 40.

1. *If G is a solvable group, every subgroup and every quotient group of G is solvable*
2. *Conversely, if N is a normal subgroup of a group 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

$$\{1\} = G_0 < G_1 < \cdots < G_k = G$$

with $G_i \triangleright G_{i+1}$ and G_i/G_{i+1} is abelian.

Claim. *Let H be a subgroup of G . Then, H is solvable.*

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

$$\{1\} = H_0 < H_1 < \cdots < H_k = H$$

with $H_{i+1} \triangleleft H_i$. Note that both H_i and G_{i+1} are subgroups of G_i and $H_{i+1} = H \cap G_{i+1} = H_i \cap G_{i+1}$. Applying Theorem 38 to G_i , we have

$$H_i/H_{i+1} = H_i/H_i \cap G_{i+1} \cong H_i G_{i+1}/G_{i+1} \subset G_i/G_{i+1}.$$

Since G_i/G_{i+1} is abelian, so is H_i/H_{i+1} . So H is solvable.

Claim. *Let N be a normal subgroup of G . Then G/N is solvable.*

Consider the towers

$$N = G_0N < G_1N < \cdots < G_kN = G$$

and

$$\{1\} = G_0N/N < G_1N/N < \cdots < G_kN/N = G/N.$$

Since $G_{i+1} \triangleleft G_i$ and $N \triangleleft G$, we have $G_{i+1}N \triangleleft G_iN$, which implies that $G_{i+1}N/N \triangleleft G_iN/N$. By Theorem 39,

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

By Theorem 38, we have

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

Since $G_{i+1} \subseteq (G_i \cap G_{i+1}N)$, there is a natural injection $G_i/G_i \cap G_{i+1}N \rightarrow G_i/G_i + 1$ defined 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. It follows that G/N is solvable.

Both these claims together show the first part of this theorem.

2. Suppose that N is a normal subgroup of a group G and both N and G/N are solvable.

□