University of Waterloo

PMATH 348

Fields and Galois Theory

Prof. Yu-Ru Liu • Winter 2018

Contents

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 $\sqrt[n]{\cdot}$

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

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

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 insolvability 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

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

   It can be shown that if α is "good", say algebraic, $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ is finite. If α is "very good", say constructable, the order of $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ 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 $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$.

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 <u>Galois Theory</u>; 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 ${}^{E}\!/_{F}$ if a field extension, we can view E as a vector space over F.

1. Addition: For $e_1, e_2 \in E$, $e_1 + e_2 \coloneqq e_1 + e_2$ (addition in E)
2. Scalar Multiplication: For $c \in F, e \in E$, $c \cdot e \coloneqq ce$ (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. $F[x] = \{f(x) = a_0 + a_1x + \cdots + a_nx^n : a_i \in F, n \in \mathbb{N} \cup \{0\}\}$, 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 $\{a_ib_j : 1 \le i \le m, 1 \le j \le n\}$ is a basis of ${}^{E}\!/_{F}$.

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

For $e \in E$, we have

$$e = \sum_{i=1}^{m} k_ia_i$$

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,

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

Claim. *The set $\{a_ib_j : 1 \le i \le m, 1 \le j \le n\}$ 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 $\{a_1, \ldots, a_m\}$ are independent over K. We have

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

Since $\{b_1, \ldots, b_n\}$ 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 $[E : F] = [E : K][K : F]$. □

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. $\frac{c}{d} \in \mathbb{Q}$, $\sqrt{2}\ \sqrt[3]{7} + 2i$ 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 $\Psi : R_1 \to R_2$ 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*

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

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

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

Proof. Let $\Psi : F(x) \to F(\alpha)$ 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, $\mathrm{im}(\Psi)$ contains a field generated by F and α, in other words, $F(\alpha) \subseteq \mathrm{im}(\Psi)$. Thus, $\mathrm{im}(\Psi) = F(\alpha)$ and Ψ is surjective. It follows that Ψ is an isomorphism and we have

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

□

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*

$$\Psi : {}^{F[x]}\!/_{\langle p(x) \rangle} \to F[\alpha] \quad \textit{with } \Psi(x) = \alpha$$

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

Proof. Consider the unique F-homomorphism $\Psi : F[x] \to F[\alpha]$ defined by $\Psi(x) = \alpha$. Thus, for $f(x) \in F[x]$, we have $\Psi(f) = f(\alpha)$. 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 $F[\alpha] = F(\alpha)$. □

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 $p(x) \big| f(x)$.

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 $\{1, \alpha, \alpha^2, \ldots, \alpha^{\deg(p)-1}\}$ 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 $\{1, x, x^2, \ldots\}$ 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,

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

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

Theorem 5. *Let ${}^{E}\!/_{F}$ be a field extension. If $[E : F] < \infty$, then there exists $\alpha_1, \ldots, \alpha_n \in E$ such that*

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

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 ${}^{\widetilde{E}}\!/_{\widetilde{F}}$ with $[\widetilde{E} : \widetilde{F}] < [E : F]$. 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

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

Thus, we have

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

as desired. □

Definition 2.2.6. A field extension ${}^{E}\!/_{F}$ is <u>algebraic</u> if every $\alpha \in E$ is algebraic over F. Otherwise, it is <u>transcendental</u>.

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. □

Theorem 7. *Let ${}^{E}\!/_{F}$ be a field extension. Define,*

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

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 $[F(\alpha)] < \infty$ 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 α over F, say $p(x) \in F[x]$, is also a polynomial over $F(\beta)$. In otherwords, $p(x) \in F(\beta)[x]$ 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. □

Definition 2.2.7. Let ${}^{E}\!/_{F}$ be a field extension. The set,

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

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 $\gcd(a_0, \ldots, a_n) = 1$.

Lemma. *Every non-zero polynomial $f(x) \in \mathbb{Q}[x]$ can be written uniquely as a product $F(x) = cf_0(x)$ 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 $f : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ 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 $0 \leq i(n-1)$, 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 $\mathbb{Q}[x]$ ∎

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

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

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, $p \nmid 1$, $p \mid \binom{p}{i}, \forall i \in \{1, \ldots, p-1\}$ 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 $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. Since $\xi_p \in \mathbb{Q}$, we have

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

Since $p \to \infty$, we have $[\overline{\mathbb{Q}} : \mathbb{Q}]$ 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 it's 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 $0 \leq i \neq (n-1)$ and $\ell^2 \nmid a_0$, then $f(x)$ is irreducible in $F[x]$.*

3 Splitting Fields

Definition 3.0.1. Let ${}^{E}\!\diagup_{F}$ 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 ${}^{\widetilde{E}}\!\diagup_{F}$, $f(x) \in F[x]$ and $F \subseteq E \subseteq \widetilde{E}$. 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 $\widetilde{E}$.

3.1 Existence of Splitting Fields

Theorem 10. *Let $p(x) \in F[x]$ be irreducible. The quotient ring ${}^{F[x]}\!\diagup_{\langle p(x)\rangle}$ 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, $E = {}^{F[x]}\!\diagup_{I}$ is a field. Consider the map

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

Since F is a field and $\Psi \neq 0$, Ψ is injective. Thus, be 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,

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

Thus, we have

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

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 $\alpha_1, \alpha_2, \dots, a_n$ 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 ${}^{\widetilde{E}}\!/\!_{F}$, 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 $\widetilde{E}$. Thus, it is unique within $\widetilde{E}$.

If we change ${}^{E}\!/\!_{F}$ to a different field extension, sat ${}^{E'}\!/\!_{F}$, what is the relation between the splitting field of $f(x)$ in E and the one in E'?

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

Theorem 13. *Let $\phi : F \to F'$ be an isomorphism of fields and $f(x) \in F[x]$. Let $\Phi : F[x] \to F'[x]$ 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 $\Psi : E \to E'$.*

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 $[E : F] < 1$ and the statement is true for all field extensions ${}^{\widetilde{E}}\!/\!_{\widetilde{F}}$ with $[\widetilde{E} : \widetilde{F}] < [E : F]$. Let $p(x) \in F[x]$ be an irreducible factor of $f(x)$ with $\deg(p) > 1$ and let $p'(x) = \Phi(f(x))$ (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,

$$F'(\alpha) \cong {}^{F'[x]}\!/\!_{\left\langle p'(x)\right\rangle}, \quad \alpha \mapsto x + \left\langle p'(x)\right\rangle$$

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

$$\widetilde{\Phi} : {}^{F[x]}\!/\!_{\langle p(x)\rangle} \to {}^{F'[x]}\!/\!_{\left\langle p'(x)\right\rangle}, \quad x + \langle p(x)\rangle \mapsto x + \left\langle p'(x)\right\rangle$$

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

$$\widetilde{\phi} : F(\alpha) \to F'(\alpha), \quad \alpha \mapsto \alpha'$$

which extends ϕ. Note that since $\deg(p) > 2$, $[E : F[\alpha]] < [E : F]$. 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 $\Psi : E \to E'$ which extends $\widetilde{\phi}$. Thus, Ψ extends ϕ. $\square$

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

Proof. Let $\phi : F \to F$ 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.
<u>Case 1</u>: If $f(x) \in F[x]$ is irreducible and $\alpha \in E$ is a root of $f(x)$, by Theorem 13,

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

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 $\deg(g) = n$, by induction hypothesis, $[E : F(\alpha)] \mid (n-1)\,!$. Since $[E : F] = [E : F(\alpha)][F(\alpha) : F]$, it follows that $[E : F] \mid n\,!$.
<u>Case 2</u>: 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

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

$\square$

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 $\chi : \mathbb{Z} \to F$ defined by

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

Let $I = \ker(\chi)$, the kernel of χ. Since $\mathbb{Z}/I \cong \operatorname{im}(\chi)$, 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, $\mathbb{Q} = \operatorname{Frac}(\mathbb{Z}) \subseteq F$.
Case 2: If $I = \langle p \rangle$, then

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

□

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 $\operatorname{ch}(F) = 0$ (respectively $\operatorname{ch}(F) = p$).

Remark. Note that if $\operatorname{ch}(F) = p$, 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 $\operatorname{ch}(F) = p$ and let $n \in \mathbb{N}$. Then, the map $\phi : F \to F$ given by $u \mapsto u^{p^n}$ is an injective $\mathbb{Z}_p$-homomorphism of fields. If F is finite, then phi 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

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

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: $D(fg) = \big(D(f)\big)g + f\big(D(g)\big)$.

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

Proof. 1. 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 $1 \le i \le n$, Since $\mathrm{ch}(F) = 0$, $i \ne 0$. Thus, $a_i = 0$ for all $i \ge 1$. This, $f(x) = a_0 \in F$.

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

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

where $g(x) = a_0 + a_p + \cdots + a_{mp}x^m \in F[x]$.
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, $g'(x) = pb_1x^{p-1} + 2pb_2x^{2p-1} + \cdots + mpb_m^{pm-1}$. Since $ch(F) = p$, we have $f'(x) = 0$. $\square$

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

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

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 $f(x) = (x-\alpha)^2 g(x)$ for some $g(x) \in E[x]$. $\square$

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