Notes on Commutative Algebra

Apiros3

First Version : Mar 19, 2025
Last Update : Jan 29, 2025

Contents

1 Introduction

2 Properties about Commutative Rings

Definition 2.0.1. *For any ring R, there is a unique ring map (homomorphism) $\phi : \mathbb{Z} \to R$ such that*

$$\phi(n) = \overbrace{1 + \cdots + 1}^{n \text{ times}}$$

Define the ***characteristic*** *written* $\mathrm{char}(R)$ *to be the unique $r \geq 0$ such that $(r) = \ker(\phi)$*

Note that if R is a domain, then $\mathrm{char}(R)$ is either 0 or a prime number.

2.1 Fields

Proposition 2.1.1. *Let R be a domain. Then there is a field F and an injective ring map $\phi : R \to F$ such that if*

$$\phi : R \to F_1$$

is a ring map into a field F_1, then there is a unique ring map $\lambda : F \to F_1$ such that $\phi_1 = \lambda \circ \phi$.

Proof. TODO!! □

Definition 2.1.2. *As a consequence of the above proposition, F is determined uniquely up to isomorphism. We call F the* ***field of fractions****, and write* $\mathrm{Frac}(F)$*.*

Note that $\mathrm{Frac}(R) = R_{R \setminus \{0\}}$

Lemma 2.1.3. *Let K be a field and $I \subseteq K$ be an ideal. Then $I = (0)$ or $I = K$.*

Proof. Immediate (any non-zero element has an inverse, thus generates K). □

Lemma 2.1.4. *Let K, L be fields and $\phi : K \to L$ be a ring map. Then ϕ is injective.*

Proof. Consider the kernel of ϕ. This is an ideal, thus is either (0) or K. In the former ϕ is injective (by the First Isomorphism Theorem), in the latter K and L are both zero-rings, so it follows. □

2.2 Polynomial Rings

Definition 2.2.1. *Let R be a ring. Write $R[x]$ to be the ring of polynomials in the variable x and coefficients in R (with standard operations). If $r \geq 0$ is an integer, $K[x_1, \ldots, x_r] := K$ if $r = 0$ and*

$$K[x_1, \ldots, x_r] := K[x_1][x_2] \ldots [x_r]$$

Given $P(x) = a_d x^d + \cdots + a_1 x + a_0 \in R[x]$ with $a_d \neq 0$, $P(x)$ is ***monic*** *if $a_d = 1$ (and $\deg(0) = -\infty$). We define the* ***degree*** *of $P(x)$ written $\deg(P) := d$.*

An element $t \in R$ is a ***root*** *of $P(x)$ if $P(t) = 0$.*

Lemma 2.2.2. *If R is a domain, then $R[x]$ is also a domain.*

Proof. TODO!!! □

Proposition 2.2.3. *If K is a field, $K[x]$ is a euclidian domain.*

Proof. TODO!! □

Consequently, $K[x]$ is a PID.

Definition 2.2.4. *A **unique factorization domain** (UFD) is a domain R such that for any $r \in R\backslash\{0\}$, there is a sequence $r_1, \dots, r_k \in R$ such that*

1. *r_i is irreducible for all i*
2. *$(r) = (r_1 \cdots r_k)$*
3. *if $r'_1, \dots, r'_{k'}$ is another such sequence with the above properties, $k = k'$ and there is a permutation $\sigma \in S_n$ such that $(r_i) = (r'_{\sigma(i)})$ for all $i \in \{1, \dots, k\}$*

Proposition 2.2.5. *Any PID is a UFD.*

Definition 2.2.6. *Write $\gcd(P_1, \dots, P_k)$ for the unique monic generator of the ideal $(P_1(x), \dots, P_k(x))$.*

Lemma 2.2.7. *Suppose that R is a UFD. An element $f \in R\backslash\{0\}$ is irreducible if and only if (f) is a prime ideal.*

Proof. The forward direction is immediate, noting that if $f|p_1p_2$, $f|p_1$ or $f|p_2$, from the fact that f is irreducible and p_1, p_2 can be split into irreducible components.

On the other hand, if (f) is a prime ideal and f is not irreducible, then $f = f_1f_2$ for some non-units. But as f is prime, $f|f_1$ or $f|f_2$. Without loss of generality, taking $f|f_1$, we have $f_1f_2|f_1$, meaning f_2 is a unit, a contradiction. $\square$

Lemma 2.2.8. *Let R be a PID. Let $I \triangleleft R$ be a nonzero prime ideal. Then I is a maximal ideal.*

Proof. Suppose not. Then we can find an element $r \in R$ such that $r \notin I$ and $([r]_I)$ is not R/I. Also, $([r]_I) = [(r, I)]_I$, and $(r, I) \neq R$ and $I \subsetneq (r, I)$. As we are in a PID, we can find $g, h \in R$ such that $(g) = (r, I)$ and $(h) = I$. Then, $g|h$ but $h \not| g$ (thus h is reducible). But h is irreducible as I is prime and R is a UFD, a contradiction. $\square$

Proposition 2.2.9. *Let K be a field and $f \in K[x], a \in K$. Then,*

1. *a is a root of f if and only if $(x - a)|f$*
2. *there is a polynomial $g \in K[x]$ with no roots and a decomposition*

$$f(x) = g(x) \prod_{i=1}^{k} (x - a_i)^{m_i}$$

where $k \geq 0$ and $m_i \geq 1$ and $a_i \in K$.

Proof. Immediate. For the forward case in (i), we use euclidian division on $(x - a)$ and show the remainder is 0. $\square$

Proposition 2.2.10 (Eisenstein Criterion)**.** *Let*

$$f = x^d + \sum_{i=1}^{d-1} a_i x^k \in \mathbb{Z}[x]$$

Let $p > 0$ be a prime number. Suppose $p|a_i$ and $p^2 \not| a_0$. Then f is irreducible in $\mathbb{Z}[x]$.

Proof. Sketch. The idea is that viewing this polynomial in $\mathbb{F}_p[x]$ gives x^d, and we show that if this is reducible, they are x^n and x^{d-n} in the same field. This contradicts with the assumption $p|a_0$. (Need some algebraic manipulation to show the first statement) □

Lemma 2.2.11. *Let $f \in \mathbb{Z}[x]$ be monic. Let $p > 0$ and $f \pmod p \in \mathbb{F}_p[x]$ is irreducible. Then f is irreducible in $\mathbb{Z}[x]$.*

Proof. TODO!!! □

Lemma 2.2.12 (Gauss Lemma)**.** *Let $f \in \mathbb{Z}[x]$. Then f is irreducible in $\mathbb{Z}[x]$ if and only if it is irreducible in $\mathbb{Q}[x]$.*

Proof. TODO!! □

2.3 Action of Groups on Rings

Definition 2.3.1. *Let S be a set and G be a group. Write $\mathrm{Aut}_{\mathrm{Sets}}(S)$ for the group of bijective maps $a : S \to S$ (where the group operator works by composition). An **action** of G on S is a group homomorphism*

$$\phi : G \to \mathrm{Aut}_{\mathrm{Sets}}(S)$$

Notation 2.3.2. *Given $\gamma \in G$ and $s \in S$, we write*

$$\gamma(s) := \phi(\gamma)(s)$$

or γs for $\gamma(s)$.

Definition 2.3.3. *The set of invariants of S under the action of G is written*

$$S^G := \{s \in S \mid \gamma(s) = s \ \forall \gamma \in G\}$$

If $s \in S$,

$$\mathrm{Orb}(G, s) := \{\gamma(s) \mid \gamma \in G\}$$

*is the **orbit** of s under G, and*

$$\mathrm{Stab}(G, s) := \{\gamma \in G \mid \gamma(s) = s\}$$

*is the **stabiliser** of s. We omit G when it is clear.*

Definition 2.3.4. *The action of G on a ring R is **compatible** with the ring structure of R, or G acts on a ring R if the image of ϕ lies in the subgroup*

$$\mathrm{Aut}_{\mathrm{Rings}}(R) \subseteq \mathrm{Aut}_{\mathrm{Sets}}(R)$$

where $\mathrm{Aut}_{\mathrm{Rings}}(R)$ is the group of bijective maps $R \to R$ which respects the ring structure.

Intuitively, each group element is mapped to a endomorphism which has some structure.

Lemma 2.3.5. *Let G act on a ring R.*

1. *R^G is a subring of R.*
2. *If R is a field, R^G is a field.*

Proof. The first case is immediate by noting $\gamma(ab) = \gamma(a)\gamma(b) = ab$ and $\gamma(a+b) = \gamma(a)+\gamma(b) = a+b$. The second follows from the fact that $1 = \gamma(aa^{-1}) = \gamma(a)\gamma(a^{-1}) = a\gamma(a^{-1})$. $\square$

Definition 2.3.6. *Let R be a ring and $n \geq 1$. There is a natural action of S_n on the ring $R[x_1, \dots, x_n]$ by*

$$\sigma(P(x_1, \dots, x_n)) = P(x_{\sigma(1)}, \dots, x_{\sigma(n)})$$

Define a ***symmetric polynomial*** *with coefficients in R to be an element in $R[x_1, \dots, x_n]^{S_n}$.*

Example 2.3.7. *For any $k \in \{1, \dots, n\}$, the polynomial*

$$s_k := \sum_{i_1 < i_2 < \cdots < i_k} \prod_{j=1}^{k} x_{i_j} \in \mathbb{Z}[x_1, \dots, x_n]$$

is symmetric. We call this the k-th elementary symmetric function (in n variables), and this satisfies

$$(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_d) = x^d - s_1(\alpha_1, \dots, \alpha_d)x^{d-1} + \cdots + (-1)^d s_d(\alpha_1, \dots, \alpha_d)$$

Theorem 2.3.8 (Fundamental Theorem of the Theory of Symmetric Functions)**.** *Let $\phi : R[x_1, \dots, x_n] \to R[x_1, \dots, x_n]$ be the map of rings which sends x_k to s_k and constants to themselves. Then,*

1. *$R[x_1, \dots, x_n]^{S_n}$ is the image of ϕ*
2. *ϕ is injective*

Then, by the first isomorphism theorem, we have $R[x_1, \dots, x_n]^{S_n} = R[s_1, \dots, s_n]$.

Proof. For the first case, we show that every symmetric polynomial can be expressed as a polynomial in s_i. Define lexicographic ordering on monomials

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} \leq x_1^{\beta_1} \cdots x_n^{\beta_n}$$

By $\alpha_1 < \beta_1$ or $\alpha_1 = \beta_1$ and $x_2^{\alpha_2} \cdots x_n^{\alpha_n} \leq x_2^{\beta_2} \cdots x_n^{\beta_n}$. Fix any symmetric polynomial f. Let $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ be the largest monomial in f. We need $\alpha_1 \geq \cdots \geq \alpha_n$, as any permutation of the powers must also be in f. Also, the largest monomial in $s_1^{\alpha_1 - \alpha_2} s_2^{\alpha_2 - \alpha_3} \cdots s_n^{\alpha_n}$ is also $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. Thus, there exists a $c \in R$ such that all monomials in $f - c \cdot s_1^{\alpha_1 - \alpha_2} s_2^{\alpha_2 - \alpha_3} \cdots s_n^{\alpha_n}$ are strictly smaller than $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. By repeating, we can write f as a polynomial in s_i.

To show (ii), we can show that s_i are algebraicly independent, and therefore that the kernel is 0. TODO!!! $\square$

Definition 2.3.9. *Define,*

1. *$\Delta(x_1, \dots, x_n) := \prod_{i<j}(x_i - x_j)^2 \in \mathbb{Z}[x_1, \dots, x_n]^{S_n}$*
2. *$\delta(x_1, \dots, x_n) := \prod_{i<j}(x_i - x_j) \in \mathbb{Z}[x_1, \dots, x_n]^{A_n}$*
3. *If $\sigma \in S_n$, $\delta(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \mathrm{sign}(\sigma) \cdot \delta(x_1, \dots, x_n)$.*

where sign $: S_n \to \{-1, 1\}$ *gives the* ***sign*** *of the permutation, and $A_n := \ker(sign)$ is called the* ***alternating group****. We call $\Delta(x_1, \dots, x_n)$ the* ***discriminant****.*

Note the third point follows from the fact that any permutation can be written as a product of transpositions, and $\mathrm{sign}(\sigma) = -1$ if σ is a transposition. The $\in$ in the second point follows from this.

3 Field Extensions

3.1 Field extension

Definition 3.1.1. *Let K be a field. A* ***field extension*** *of K, or K-extension is an injection*

$$K \hookrightarrow M$$

of fields. This injection gives M the structure of a K-vector space. We write $M|K$ for the field extension of K to M.

A map from the K extension $M|K$ to $M'|K$ is a ring map $M \to M'$ that is compatible with the injections $K \hookrightarrow M$ and $K \hookrightarrow M'$. Alternatively, it is a map that makes the following commute.

$$\begin{tikzcd}
K \arrow[d, hook] \arrow[dr, hook] & \\
M \arrow[r] & M'
\end{tikzcd}$$

Given $M|K$ is a field extension, we write $\mathrm{Aut}_{\mathrm{K}}(M)$ for the group of bijective maps of K-extensions from M to M, where the group law is the composition of maps. This is the subgroup of $\mathrm{Aut}_{\mathrm{Rings}}(M)$ which are compatible with the K-extension structure of M. We say that the field extension is **finite** if $\dim_K(M) < \infty$.

If M is a finite extension of K, then by rank nullity, any ring map from M to M is a bijection.

Example 3.1.2. *If M is not a finite extension of K, then endomorphisms on M need not be bijective. Consider $\phi : \mathbb{Q}(t) \to \mathbb{Q}(t)$ which sends $t \mapsto t^2$. Consequently, $\dim_M(M)$ need not be 1, depending on the structure of the extension.*

Proposition 3.1.3 (Tower Law)**.** *If $L|M$ and $M|K$ are finite field extensions, we have*

$$[M : K] \cdot [L : M] = [L : K]$$

Specificaly, if $m_1, \dots, m_s$ is a basis of M as a K-vector space and $l_1, \dots, l_t$ is a basis of L as a M vector space, (as vector spaces induced by the field extensions), then $\{m_i l_j\}$ is a basis for L as a K-vector space (as the composition of extensions).

Proof. TODO!!! □

Definition 3.1.4. *Let $M|K$ be a field extension and $a \in M$. Define*

$$\mathrm{Ann}(a) := \{P(x) \in K[x] \mid P(a) = 0\}$$

We have $\mathrm{Ann}(a) \subseteq K[x]$ is an ideal.

We say that a is ***transcendental*** *over K if $\mathrm{Ann}(a) = (0)$ and* ***algebraic*** *if $\mathrm{Ann}(a) \neq (0)$. If a is algebraic over K, then the* ***minimal polynomial*** *m_a is the unique monic polynomial that generates $\mathrm{Ann}(a)$.*

Alternatively the annihalator is the kernel of the map from $K[x]$ to L.

$$\begin{tikzcd}
K \arrow[d] \arrow[dr, hook, "\phi"] & \\
K[x] \arrow[r, "e_a"'] & M
\end{tikzcd}$$

Consequently, there is a injection $K[x]/\mathrm{Ann}(a) \hookrightarrow M$ where M is a domain. Thus, $\mathrm{Ann}(a)$ is prime. If a is algebraic over K, m_a is irreducible (as (m_a) is a prime ideal in a UFD). Thus a monic irreducible polynomial that annihalates a is the minimal polynomial. Prime ideals in a PID are maximal, so $\mathrm{Ann}(a)$ is maximal.

Definition 3.1.5. *We say that a field extension $M|K$ is **algebraic** if for all $m \in M$, the element m is algebraic over K. Else, we say that the field extension is **transcendental**.*

Lemma 3.1.6. *If $M|K$ is finite, then $M|K$ is algebraic.*

Proof. Let $m \in M$. If m is transcendental over K, there is an injection of a K-vector space $K[x] \hookrightarrow M$. $K[x]$ is infinite dimensional, but this contradicts the fact M is a finite-dimensional vector space over K. □

3.2 Separability

Let K be a field. Let $P(x) \in K[x]$, and suppose

$$P(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$$

Define $P'(x) = \frac{\mathrm{d}}{\mathrm{dx}}P(x) := da_d x^{d-1} + (d-1)a_{d-1}x^{d-2} + \cdots + a_1$, where $d-i$ is $1_K + \cdots + 1_K$ $(d-i)$-times. This is a K-linear map from $K[x]$ to $K[x]$ and satisfies

$$\frac{\mathrm{d}}{\mathrm{dx}}(P(x)Q(x)) = \frac{\mathrm{d}}{\mathrm{dx}}(P(x))Q(x) + P(x)\frac{\mathrm{d}}{\mathrm{dx}}(Q(x))$$

Definition 3.2.1. *$P(x)$ has **multiple roots** if $(P(x), P'(x)) = (1)$. Equivalently, we have that $\gcd(P(x), P'(x)) = 1$ (by Bézout's Lemma).*

Given

$$P(x) = (x-\rho_1)(x-\rho_2)\cdots(x-\rho_d)$$

we see that $P(x)$ has multiple roots if and only if there are $i \neq j$ such that $\rho_i = \rho_j$.

Lemma 3.2.2. *Let $L|K$ be a field extension, $P(x), Q(x) \in K[x]$. Write $\gcd_L(P(x), Q(x))$ for the greatest common divisor of $P(x)$ and $Q(x)$ viewed as polynomials with coefficients in L. Then,*

$$\gcd(P(x), Q(x)) = \gcd_L(P(x), Q(x))$$

Proof. We use the fact that a generator of $(P(x), Q(x))$ can be computed using Euclidian division. We note that the sequence in which we get this by euclidian algorithm is unique and is invariant of the field. □

In particular, the definition of multiple roots captures roots that may not yet be in the base field.

Remark 3.2.3. *Let K be a field and $P(x) \in K[x]$. Let $L|K$ be a field extension. Then, $P(x)$ has multiple roots as a polynomial with coefficients in K if and only if it has multiple roots as a polynomial with coefficients in L.*

Lemma 3.2.4. *Let $P(x), Q(x) \in K[x]$ and suppose $Q(x)|P(x)$. If $P(x)$ has no multiple roots, $Q(x)$ also has no multiple roots.*

Proof. Let $T(x) \in K[x]$ be such that $Q(x)T(x) = P(x)$. By the Leibniz rule,

$$(P, P') = (QT, Q'T + QT')$$

If Q and Q' were both divisible by some polynomial W with positive degree, it also divides $Q'T+QT'$ and QT, thus 1 would be divisible by W, a contradiction. □

Lemma 3.2.5. *Suppose that K is a field and that $P(x) \in K[x] \backslash \{0\}$. Suppose that $\operatorname{char}(K)$ does not divide $\deg(P)$ and that $P(x)$ is irreducible. Then $(P, P') = (1)$.*

Proof. Let

$$P(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$$

where $a_d \neq 0$. First note that $d = 0_K$ in K as $\operatorname{char}(K)$ does not divide d. Thus, $P'(x) \neq 0$. As P is irreducible, any common divisor of P and P' is a non-zero constant or P times a non zero constant. It is not the latter as $\deg(P') < \deg(P)$. Thus, it must be a non-zero constant. In other words, $(P, P') = (1)$. □

Noting the proof, if $P' \neq 0$, and P is irreducible, the same result follows.

Definition 3.2.6. *Let K be a field. We say that $P(x) \in K[x] \backslash \{0\}$ is **separable** if all the irreducible factors of $P(x)$ have no multiple roots.*

Note that by Remark 3.2.3 and Lemma 3.2.4, this notion is invariant under field extensions. Also, by Lemma 3.2.5, irreducible polynomials with coefficients in K whose degree is prime to the characteristic of K is separable. Specificaly, if $\operatorname{char}(K) = 0$, any irreducible polynomial with coefficients in K is separable.

Definition 3.2.7. *Let $L|K$ be an algebraic field extension. We say that $L|K$ is **separable** if the minimal polynomial over K of any element of L is separable.*

Noting the previous paragraph, if K is a field and $\operatorname{char}(K) = 0$, all algebraic extensions of K are separable (noting that minimal polynomials are irreducible in $K[x]$).

Lemma 3.2.8. *Let $M|L$ and $L|K$ be algebraic field extensions. Suppose $M|K$ is separable. Then, $M|L$ and $L|K$ are both separable.*

Proof. By definition, $L|K$ is separable. Let $m \in M$ and let $P(x) \in K[x]$ be the minimal polynomial over K. Let $Q(x)$ be the minimal polynomial of m over L. By assumption, $Q(x)|P(x)$. By assumption, $P(x)$ has no multiple roots over K thus also over L by Remark 3.2.3. By Lemma 3.2.4, $Q(x)$ also has no multipe roots over L, thus is separable. □

Example 3.2.9. *Finite extensions need not be separable. Noting the proof in Lemma 3.2.5, we at least want to find a polynomial P such that $P' = 0$.*

Consider $K := \mathbb{F}_2(t)$ where $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Let $P(x) := x^2 - t$. As $P(x)$ is of degree 2 and has no roots in K (by considering degrees), it is irreducible.

Define $L := K[x]/(P(x))$. As $P(x)$ is irreducible, $(P(x))$ is prime, thus maximal in $K[x]$, meaning L is a field. However, $P'(x) = 0$, thus $(P', P) = (P) \neq (1)$. As $P(x)$ is the minimal polynomial of $x \in L$, $L|K$ is not separable.

3.3 Simple Extensions

Definition 3.3.1. *Let $\iota : K \hookrightarrow M$ be a field extension and $S \subseteq M$ be a subset. Define*

$$K(S) := \bigcap_{\text{field } L, L \subseteq M, L \supseteq S, L \supseteq \iota(K)} L$$

*This is a subfield of M and is called the **field generated by** S **over** K, and the elements of S are called **generators** of $K(S)$. The field extensions $M|K$ is the composition of the natural field extensions $K(S)|K$ and $M|K(S)$.*

Note also that if $S = \{s_1, \ldots, s_k\}$, then

$$K(S) = K(s_1)\ldots(s_k)$$

We also say that $M|K$ is a **simple extension** if there is a $m \in M$ such that $M = K(m)$.

Example 3.3.2. *Some examples of simple extensions:*

- *Let $K = \mathbb{Q}$ and $M = \mathbb{Q}(i, \sqrt(2))$ be a field generated by i and $\sqrt{2}$ in $\mathbb{C}$. Then M is a simple algebraic extension of K generated by $i + \sqrt{2}$.*
- *Let $M = \mathbb{Q}(x) = \mathrm{Frac}(\mathbb{Q}[x])$ and let $K = \mathbb{Q}$. Then M is a simple transcendental extension of K, generated by x.*

Proposition 3.3.3. *Let $M = K(\alpha)|K$ be a simple algebraic extension. Let $P(x)$ be the minimal polynomial of α over K. Then, there is a natural isomorphism of K-extensions*

$$K[x]/(P(x)) \simeq M$$

which sends x to α.

Proof. We first note that there is a natural map from $K[x]/(P(x))$ to M by evaluation. As $P(x) \neq 0$, we have $(P(x))$ is a maximal ideal. Thus, the image of $K[x]/(P(x))$ in M is a field. By definition, this is the entirety of M. ☐

Remark 3.3.4. *Noting the above proposition, we can note that $[M : K] = \deg(P)$. Then, the set $\{1, x, \ldots, x^{\deg(P)-1}\}$ is a basis. Also as a consequence, a finitely generated algebraic extension is a finite extension.*

Corollary 3.3.5. *Let $M = K(\alpha)|K$ be a simple algebraic extension. Let $K \hookrightarrow L$ be an extension of fields. Let $P(x)$ be the minimal polynomial of α over K. There is a bijective correspondence with the roots of $P(x)$ in L and the maps of K-extensions $M \hookrightarrow L$.*

Proof. The corresponding map is given by the unique map extended from sending α to the root of $P(x)$ in L. ☐

Example 3.3.6. *Let $M := \mathbb{Q}(i) \subseteq \mathbb{C}$ and let $K = \mathbb{Q}$, and $L = \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{C}$. There is no map of K-extensions $M \hookrightarrow L$ because the roots of $x^2 + 1$ do not lie in $L \subseteq \mathbb{R}$. If we change $L = \mathbb{C}$, then there are two maps of K-extensions $M \hookrightarrow L$ corresponding to the function extended by sending $i \mapsto i$ and $i \mapsto -i$.*

3.4 Splitting Fields

Definition 3.4.1. *Let K be a field. Let $P(x) \in K[x]$. We say that $P(x)$* ***splits*** *in K if for some $c \in K$ and sequence of $\{a_i \in K\}$, we have*

$$P(x) = c \cdot \prod_{i=1}^{k} (x - a_i)$$

We call a field ***algebraicly closed*** *if any polynomial with coefficients with L splits in L.*

If $P(x) \in K[x]$ is irreducible and $\deg(P) > 1$, $P(x)$ has no roots in K and thus does not split in K.

Definition 3.4.2. *A field extension $M|K$ is a* ***splitting extension*** *for $P(x) \in K[x]$ if*

1. *$P(x)$ splits in M*
2. *M is generated over K by the roots of $P(x)$ in M.*

Theorem 3.4.3. *Let $P(x) \in K[x]$. Then,*

- *There exists a field extension $M|K$ which is a splitting extension for $P(x)$*
- *If $L|K$ is a splitting extension for $P(x)$, then L and M are isomorphic as K-extensions*
- *Let $L|K$ be a splitting extension for $P(x)$ and $J|K$ be any K-extension. Then, the images of all the maps of K-extensions $L \hookrightarrow J$ coincide.*

Proof. (i) We work by induction on $\deg(P)$. If $\deg(P) = 1$, then $K|K$ is a splitting extension for $P(x)$. Suppose that $\deg(P) > 1$. Let P_1 be an irreducible factor of $P(x)$. Consider $M_1 := K[x]/(P_1(x))$. M_1 is a field, and there is a natural map of rings $K \hookrightarrow M_1$.

By definition, $P(x)$ has a root a in M_1 (which is just x in the presentation $M_1 = K[x]/(P_1(x))$). Let M be a splitting field for $P(x)/(x-a) \in M_1[x]$ over M_1, which exists by the inductive hypothesis. By construction, $P(x)$ splits in M. Let $a_2, \ldots, a_k$ be roots of $P(x)/(x-a)$ in M. By Proposition 3.3.3, $M = K(a)(a_2)\ldots(a_k) = K(a, a_2, \ldots, a_k)$ and thus M is generated over K by roots in M. Consequently, M is a splitting field of $P(x)$ over K.

(ii) We work by induction on $\deg(P)$. If $\deg(P) = 1$, we are done. Suppose $\deg(P) > 1$. Let $a \in M$ be a root of $P(x)$ in M and $Q(x) \in K[x]$ be its minimal polynomial. As $Q(x)|P(x)$, $Q(x)$ splits in M and also in L.

Now let a_1 be a root of $Q(x)$ in L. Note from before that $M|K(a)$ is a splitting extension of $P(x)/(x-a) \in K(a)$. Similarly, $L|K(a_1)$ is a splitting extension of $P(x)/(x-a_1) \in K(a_1)$. Define $J := K[x]/(Q(x))$. This is a field as $Q(x)$ is irreducible, and there are natural isomorphisms $J \simeq K(a)$ and $J \simeq K(a_1)$ of K-extensions. Considering the J-extensions $M|J$ and $L|J$ from these isomorphisms, the inductive hypothesis shows the two are isomorphic as J extensions. By construction, this gives an isomorphism of K-extensions.

(iii) If there are no maps of K-extensions $L \hookrightarrow J$, we are done. Else, suppose there is a map $\phi : L \hookrightarrow J$ of K-extensions. As L is generated over the roots of $P(x)$, the image of ϕ are generated over K by the image of these roots in J under ϕ. We claim these images are the roots of $P(x)$ in J.

To prove the above claim, let $\alpha_1, \ldots, \alpha_d$ be roots of $P(x)$ in L with multiplicities. Then,

$$P(x) = x^d - \sigma_1(\alpha_1, \ldots, \alpha_d)x^{d-1} + \cdots + (-1)^d \sigma_d(\alpha_1, \ldots, \alpha_d)$$

Thus, the elements of $\phi(\alpha_1), \ldots, \phi(\alpha_d)$ are the roots of

$$\begin{aligned} &x^d - \sigma_1(\phi(\alpha_1), \ldots, \phi(\alpha_d))x^{d-1} + \cdots + (-1)^d \sigma_d(\phi(\alpha_1), \ldots, \phi(\alpha_d)) \\ = &x^d - \phi(\sigma_1(\alpha_1, \ldots, \alpha_d))x^{d-1} + \cdots + (-1)^d \phi(\sigma_d(\alpha_1, \ldots, \alpha_d)) \end{aligned}$$

Now the set of roots of $P(x)$ in J does not depend on ϕ, and so the claim follows. (TODO!!! (understand invariance better)) $\square$

Remark 3.4.4. *Let K be a field and $P(x) \in K[x]$. Suppose that there is a field extension $K \hookrightarrow L$, where L is algebraicly closed. Let $S \subseteq L$ be the roots of $P(x) \in L$. Then $K(S) \subseteq L$ is a splitting field for $P(x)$. This follows from the fact $P(x)$ splits in $K(S)$ as L is algebraicly closed, and that $K(S)$ is generated by the roots of $P(x)$ by construction.*

As a specific example, we can generate a splitting field for any polynomial in $\mathbb{Q}[x]$ by considering $L = \mathbb{C}$.

Remark 3.4.5. *Any field K has an algebraic field extension $K \hookrightarrow K'$ such that K' is algebraicly closed. This is unique up to isomorphism and is called the **algebraic closure** of K.*

3.5 Normal Extensions

Definition 3.5.1. *An algebraic extension $L|K$ is called **normal** if the minimal polynomial over K of any element of L splits in L.*

Note that a splitting extension (field) is by definition a normal extension (field).

Example 3.5.2. *Some examples of extensions are*

- *$\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ is not normal, as the minimal polynomial for $\sqrt[3]{2}$, namely $x^3 + 2$, does not split.*
- *$\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ is normal, noting that as $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, any minimal polynomial in $\mathbb{Q}(\sqrt{2})$ has degree at most 2, which if it has a root, splits.*

Lemma 3.5.3. *Let $M = K(\alpha_1, \ldots, \alpha_k)|K$ be an algebraic field extension. Let $J|K$ be an extension in which the polynomial $\prod_{i=1}^k m_{\alpha_i} \in K[x]$ splits. Then the set of maps of K-extensions $M \to J$ is finite and non-empty. If m_{α_i} are all separable, there are $[M : K]$ such maps.*

Proof. We first prove that this set is finite and non-empty. By Corollary 3.3.5, there is an extension of the map $K \hookrightarrow J$ to $K(\alpha_1)$, and only finitely many choices for such extension. The minimal polynomial of α_2 over $K(\alpha_1)$ divides m_{α_2} and has a root in J as m_{α_2} splits in J. Thus, again, there is an extension from the ring map $K(\alpha_1) \hookrightarrow J$ to $K(\alpha_1)(\alpha_2) = K(\alpha_1, \alpha_2) \hookrightarrow J$, and only finitely many such. Repearing shows the same is the case for $K(\alpha_1, \ldots, \alpha_k) = M \hookrightarrow J$.

For the cardinality of the set, we note that there are $[K(\alpha_1) : K] = \deg(m_{\alpha_1})$ extensions of maps $K \hookrightarrow J$ to $K(\alpha_1)$. Continuting, for any ring map $K(\alpha_1) \hookrightarrow J$, there are $[K(\alpha_1, \alpha_2) : K(\alpha_1)]$ extensions of this map to a map $K(\alpha_1, \alpha_2) \hookrightarrow J$. By the tower law, there are

$$[K(\alpha_1) : K][K(\alpha_1, \alpha_2) : K(\alpha_1)] = [K(\alpha_1, \alpha_2) : K]$$

extensions of the map $K \hookrightarrow J$ to a ring map $K(\alpha_1, \alpha_2) \hookrightarrow J$. Continuting,

$$[K(\alpha_1) : K] \cdots [M : K(\alpha_1, \ldots, \alpha_{k-1})] = [M : K]$$

extensions of the map $K \hookrightarrow J$ to a ring map $M \hookrightarrow J$. $\square$

Theorem 3.5.4. *A finite field extension $L|K$ is normal if and only if it is a splitting extension for a polynomial with coefficients in K.*

Proof. ($\Rightarrow$) Suppose that $L|K$ is finite and normal. Let $\alpha_1, \ldots, \alpha_k$ be generators for L over K (as a K-basis). Define

$$P(x) := \prod_{i=1}^{k} m_{\alpha_i}(x)$$

where $m_{\alpha_i}(x)$ is the minimal polynomial for α_i over K. Then, by assumption, $P(x)$ splits in L and the roots of $P(x)$ generate L, so L is a splitting field for $P(x)$.

($\Leftarrow$) Suppose that L is a splitting field of a polynomial in $K[x]$. Let $\alpha \in L$ and $\beta_1, \ldots, \beta_k \in L$ be such that $L = K(\alpha, \beta_1, \ldots, \beta_k)$. Let J be a splitting field of the products of the minimal polynomials over K over the elements $\alpha, \beta_1, \ldots, \beta_k$. Choosing a root ρ in J of the minimal polynomial $Q(x)$ of α over K. By Corollary 3.3.5, there is an extension of the map $K \hookrightarrow J$ to a ring map $\mu : K(\alpha) \hookrightarrow J$ such that $\mu(\alpha) = \rho$. By Lemma 3.5.3, there is an extension of μ to a ring map $\lambda : L \hookrightarrow J$. By Theorem 3.4.3, the image of λ on L in J is independent of λ and thus of μ. Consequently, as we have not fixed ρ, the image of λ with L in J contains all the roots of $Q(x)$. Thus, $Q(x)$ splits in the image of λ. As $Q(x)$ has coefficients in K and λ gives an isomorphism between L and the image of λ, $Q(x)$ splits in L. $\square$

Theorem 3.5.5. *Let $L|K$ be a splitting field of a separable polynomial over K. Then we have* $\#\mathrm{Aut}_K(L) = [L : K]$.

Proof. Apply Lemma 3.5.3 with $L = M = J$. $\square$

Theorem 3.5.6. *Let $\iota : K \hookrightarrow L$ be a finite field extension. Then* $\mathrm{Aut}_K(L)$ *is finite. Furthermore, the following are equivalent :*

1. $\iota(K) = L^{\mathrm{Aut}_K(L)}$
2. *$L|K$ is normal and separable*
3. *$L|K$ is a splitting extension for a separable polynomial with coefficients in K.*

Proof. We first note that if $\mathrm{Aut}_K(L)$ were infinite, we can obtain infinitely many maps of K extensions $L \hookrightarrow J$ by composing any map $L \hookrightarrow J$ with elements of $\mathrm{Aut}_K(L)$, which contradicts the result from Lemma 3.5.3.

$(i) \Rightarrow (ii)$ Let $P(x)$ be the minimal polynomial of some element $\alpha \in L$. We have to show that $P(x)$ splits and is separable. Define

$$Q(x) := \prod_{\beta \in \mathrm{Orb}(\mathrm{Aut}_K(L), \alpha)} (x - \beta)$$

By definition, $Q(x)$ is separable. Let $d := \#\mathrm{Orb}(\mathrm{Aut}_K(L), \alpha)$. Let $\beta_1, \ldots, \beta_d$ be the elements of $\mathrm{Orb}(\mathrm{Aut}_K(L), \alpha)$. Note that

$$Q(x) = x^d - s_1(\beta_1, \ldots, \beta_d)x^{d-1} + \cdots + (-1)^d s_d(\beta_1, \ldots, \beta_d)$$

For any $\gamma \in \mathrm{Aut}_K(L)$ and for any $i \in \{1, \ldots, d\}$ we have

$$\gamma(s_i(\beta_1, \ldots, \beta_d)) = s_i(\gamma(\beta_1), \ldots, \gamma(\beta_d))$$

Noting that s_i is a symmetric function and γ permutes elements of $\mathrm{Orb}(\mathrm{Aut}_K(L), \alpha)$ (by composition), we have

$$s_i(\gamma(\beta_1), \ldots, \gamma(\beta_n)) = s_i(\beta_1, \ldots, \beta_n)$$

As γ was arbitrary, we see that $s_i(\beta_1, \ldots, \beta_d) \in L^{\mathrm{Aut}_K(L)} = \iota(K)$. Thus, $Q(x) \in \iota(K)[x]$. We can therefore identify $Q(x)$ with a polynomial in $K[x]$ with ι.

However, $\alpha \in \mathrm{Orb}(\mathrm{Aut}_K(L), \alpha)$, so $Q(\alpha) = 0$. By definition of $P(x)$, $P(x)|Q(x)$, so $P(x)$ splits in L and has no multiple roots and therefore is separable.

(ii) $\Rightarrow$ *(iii)* Let $\alpha_1, \ldots, \alpha_k$ be generators of L over K. Let $P(x) := \prod_{i=1}^k m_{\alpha_i}(x)$, where $m_{\alpha_i}(x)$ is the minimal polynomial of α_i over K. Then, $P(x)$ is a separable polynomial by construction and L is also a splitting extension for $P(x)$.

(iii) $\Rightarrow$ *(i)* Note first that by construction, $\iota(K) \subseteq L^{\mathrm{Aut}_K(L)}$ as any element of $\mathrm{Aut}_K(L)$ fixes the image of K in L by definition. So, $L|K$ is the composition of extensions $L^{\mathrm{Aut}_K(L)}|K$ and $L|L^{\mathrm{Aut}_K(L)}$. Note that $L|L^{\mathrm{Aut}_K(L)}$ is also the splitting field of a separable polynomial over $L^{\mathrm{Aut}_K(L)}$ (by taking the same polynomial for $L|K$). Also note the identity $\mathrm{Aut}_{L^{\mathrm{Aut}_K(L)}}(L) = \mathrm{Aut}_K(L)$

Now, by Theorem 3.5.5, we have

$$[L : L^{\mathrm{Aut}_K(L)}] = \#\mathrm{Aut}_{L^{\mathrm{Aut}_K(L)}}(L)$$

and

$$[L : K] = \#\mathrm{Aut}_K(L)$$

giving $[L : L^{\mathrm{Aut}_K(L)}] = [L : K]$. The tower law shows that $[L^{\mathrm{Aut}_K(L)} : K] = 1$, or equivalently, $L^{\mathrm{Aut}_K(L)} = \iota(K)$. $\square$

Corollary 3.5.7. *Let $L|K$ be an algebraic field extension. Suppose that L is generated by $\alpha_1, \ldots, \alpha_k \in M$ and the minimal polynomial of each α_i is separable. Then, $L|K$ is separable.*

Proof. By Lemma 3.5.3 and Theorem 3.4.3, there is an extension $M|L$ such that $M|K$ is the splitting field of a separable polynomial (the product of the minimal polynomials). By 3.5.6, the extension $M|K$ is separable. Thus, the extension $L|K$ is also separable. $\square$

4 Main Ideas in GT - No definitions

The concept of multiple roots (on $P(x) \in K[x]$) is invariant under

- field extension. (Pf. ED algorithm is unique in computing a generator)
- polynomials $Q(x)$ such that $Q(x)|P(x)$

The gcd of P, Q is the generator of (P, Q)
If $P' \neq 0$ and P is irreducible, it has no multiple roots.
Extension of maps :

$$\begin{tikzcd}
K \arrow[r, hook] \arrow[d] & L \\
K(\alpha) \arrow[ur, hook, dashed] &
\end{tikzcd}$$

is determined by sending α to the roots of m_α in L, where m_α is the minimal polynomial of α with coefficients in K. So the cardinality of maps is the number of roots of m_α in L. This is a consequence of the fact $K(\alpha) \simeq K[x]/m_\alpha$.