Algebra II - Lecture Note

Lectures by Jae-Hoon Kwon
Notes by Byeongsu Yu

December 18, 2016

Abstract

dfjdkfjdkdjfkThis note is based on the course, Algebra II given by professor Jae-hoon Kwon on Fall 2016 at Seoul National University. Much part of this note was TEX-ed after class. Every blemish on this note is Byeongsu's own.

Contents

Without specific instruction, use R as a commutative ring, $\mathfrak{S}_n$ be symmetric n-group, and $\mathfrak{a}$ be an (left) ideal.

1 Tensors

Thanks to **Hobin Jeong** for constructing concrete categories in this section, and to **See-Hak Seong** for investigating errors and revising the definition of Algebra and the claim 1.0.3.

Definition 1.0.1 (Algebra)**.** *Let R be a commutative ring with identity, then, A is an algebra if*

- *A is ring*
- *$(A, +)$ is an unitary (left) $R-$module.*
- *$r(ab) = (ra)b = a(rb)$, $\forall r \in R$, $\forall a, b \in A$.*

Especially, if A which , as a ring, is division ring, is called division algebra.

Note that unitary R-module is an R-module M satisfying that $\forall a \in M$, $1_R \cdot a = a$, where 1_R is identity in R. This definition follows Hungerford's definition in [2][p.227]. Note that if R is a field, then algebra is always a vector space.

Example 1.0.2.
1. *Every ring is an additive abelian group, so it is $\mathbb{Z}$-module, therefore, it is $\mathbb{Z}$-algebra.*
2. *Polynomial ring with R, then it has R-module structure, so it is algebra.*
3. *Let G be a multiplicative group and R is a commutative ring with identity. Then group ring $R(G) = \sum_{v \in G} R = \{$ assign R on each element in $G\}$, with natural addition and multiplication. Then it has R-module structure given by $r(\sum r_{g_i} g_i) = \sum (r r_{g_i} g_i)$, so it is R-algebra.*

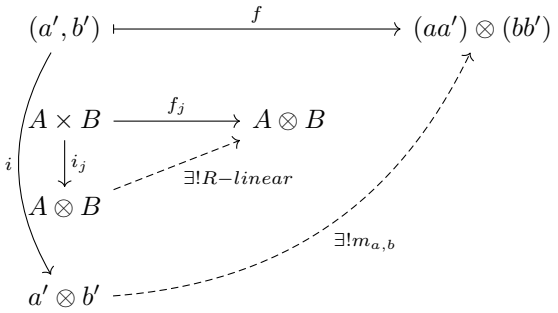
Now we can see much things on tensor product of R-algebra. Let A, B be R-algebras, and define its tensor product $(A \otimes_R B, \cdot)$, where $\cdot((a_1 \otimes b_1), (a_2 \otimes b_2)) = (a_1 a_2) \otimes (b_1 b_2)$. Now check its well-definedness.

Claim 1.0.3. *$(A \otimes_R B, \cdot)$ is well-defined as R-algebra homomorphism.*

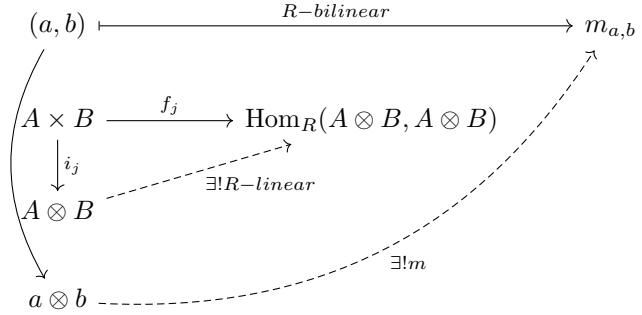
Proof. Given $a \in A, b \in B$, consdier the map $f : A \times B \to A \otimes_R B$ by $(a', b') \mapsto (aa' \otimes bb')$. First of all, $\forall b' \in B$, $a' \mapsto f(a', b)$ is R-module homomorphism by checking below;

$$\begin{aligned} ra' \mapsto f(ra', b') &= a(ra') \otimes bb' = r(aa') \otimes bb' = r(aa' \otimes bb') = rf(a, b) \\ a'_1 + a'_2 \mapsto f(a'_1 + a'_2, b') &= a(a'_1 + a'_2) \otimes bb' = a'_1 a \otimes bb' + a'_2 a \otimes bb' = f(a'_1, b') + f(a'_2, b'). \end{aligned}$$

Similarly, $\forall a' \in A$, $b' \mapsto f(a', b')$ is R-module homomorphism. Therefore, it is bilinear.



(a) Map $m_{a,b}$.



(b) Map m.

Figure 1: Define multiplication on $A \otimes B$.

Then, by universal mapping property stated in theorem 5.6 of [2][p.211] in case of tensor product, we can get unique R-linear map $m_{a,b}$, in figure 1(a). Since a, b are arbitrary, we can get a map $A \times B \to \mathrm{Hom}_R(A \otimes B, A \otimes B)$ by $(a, b) \mapsto m_{a,b}$. This map is bilinear, because

$$m_{ra,b} = rm_{a,b}, m_{a_1+a_2,b} = m_{a_1,b} + m_{a_2,b}, \text{ and } m_{a,b_1+b_2} = m_{a,b_1} + m_{a,b_2},$$

from tensor's linearity. By universal mapping property of tensor product, we can get unique map m in figure 1(b). So, $m \in \mathrm{Hom}_R(A \otimes B, \mathrm{Hom}_R(A \otimes B, A \otimes B)) \cong \mathrm{Hom}_R((A \otimes B) \otimes (A \otimes B), A \otimes B)$, from theorem 5.10 of Hungerford. In other words, adjointness between Hom and $\otimes$ gives the desired isomorphism. Therefore, m is binary operator. To check that it acts as multiplication without disturbing R-algebra structure, check below equation.

$$\forall a \otimes b, a' \otimes b' \in A \otimes B, rm(a \otimes b, a' \otimes b') = r(aa' \otimes bb') = raa' \otimes bb' = a(ra') \otimes bb'.$$

Thus, $A \otimes B$ becomes an R-algebra with respect to m, □

Since this universal mapping property of quotient object is used often, so I'll mention it as a theorem. For any algebraic object I deal with in this article, this universal property holds and you can easily prove them by the similar way. I'll call it **universal mapping property** throughout this article. If you find a comment as "using universal (mapping) property" without any proof throughout this article, You can check the universal mapping property like below.

Theorem 1.0.4 (Universal mapping property of tensor product)**.** *Tensor product is an initial object of certain category.*

Proof. Actually this is proof of theorem 5.6 of [2][p.209 212]. Construct a category $\mathscr{C}$ such that

- Object : (f, C) where $f : A \times B \to C$ is bilinear R-module homomorphism for $A, B, C \in R$-mod, where R is a commutative ring with identity.
- Morphism: $\phi_{21} : C_2 \to C_1$ such that for $(f_1, C_1), (f_2, C_2) \in obj\mathscr{C}, \phi_{21}$ is an R-module homomorphism such that $\phi_{21} f_2 = f_1$.

Since 1_C is identity morphism of (f, C), ϕ_{21} is an equivalence in $\mathscr{C}$ if and only if ϕ_{21} is isomorphism of R-module homomorphism. Hence $\mathscr{C}$ is well-defined. Note that $i : A \times B \to A \otimes_R B$ given by $(a, b) \mapsto a \otimes_R b$ defined in [2][p.209] is bilinear.

Now it suffices to show that $(i, A \otimes_R B)$ is initial obect. Let $(g, D) \in Obj\mathscr{C}$. Then, define F, K in [2][p.208] where F is free abelian group on the set $A \times B$ and K is subgroup of F generated by some forms defined in [2], which gives $A \otimes_R B = F/K$. From these, we can define $g_1 : F \to D$ by $(a, b) \mapsto g(a, b) \in C$ determines a unique homomorphism by theorem 2.1 (iv) in [2][p.181]. Also note that $K \subset ker g_1$ since g is bilinear. Hence we have quotient map $\bar{g} : F/K = A \otimes_R B \to C$ such that $\bar{g}[(a, b) + K] = g_1[(a, b)] = g(a, b)$. (Check that it is R-module homomorphism.) Since $(a, b) + K = a \otimes_R b$, and the map is homomorphism, $\bar{g}$ is homomorphism such that $\bar{g} i = g$.

To show uniqueness of $\bar{g}$, suppose $h : A \otimes_R B \to C$ is any R-module homomorphism such that $hi = g$. Then, for any generator $a \otimes b \in A \otimes_R B$,

$$h(a \otimes_R b) = hi(a, b) = g(a, b) = \bar{g} i(a, b) = \bar{g}(a \otimes_R b).$$

Since h and $\bar{g}$ agree on generator of $A \otimes_R B$, so it agrees on $A \otimes_R B$. So $h = \bar{g}$.

Hence $\bar{g}$ is unique R-module homomorphism from $A \otimes_R B$ to D, so $(i, A \otimes_R B)$ is initial object. □

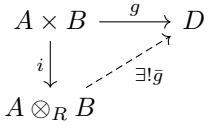


Figure 2: Universal Property of a quotient object.

There are three concrete example, such as, tensor algebra, symmetric algebra, and exterior algebra. These are from [1][XVI, 6,7,8, XIX, 7]

1.1 Tensor Algebra

Let E be an R-module. Then, let $T^r := \underbrace{E \otimes \cdots \otimes E}_{r \text{ times}} = E^{\otimes r}$ with $T^0(E) := R$. These are R-module, since it is tensor product of R-module. Then define

$$T(E) = \oplus_{r \geq 0} T^r(E),$$

a direct sum of R-modules. Also, define multiplication; for $r, s \geq 0$, $T^r(E) \times T^s(E) \to T^{r+s}(E)$ as $(x_1, x_2) \mapsto x_1 \otimes x_2$ or $x_1 x_2$ when $r = 0$ or $s = 0$. Then, $T(E)$ becomes an R-algebra with 1.

Definition 1.1.1. *T(E) is called the "tensor algebra generated by E over R."*

Proof. Note that direct sum of R-module is also R-module, since category of R-module has product and coproduct(direct sum). And, it has ring structure equipped with above multiplication; from direct sum, addition is naturally defined and it satisfy additive axioms of ring because R is commutative. Also, multiplicative identity exists, and associative. Also distribution law holds from that of tensor product. And scalar multiplication with ring R is already defined since T^0 is in $T(E)$. □

Remark 1.1.2. *1. T can be regarded as a functor; define it as $E \xrightarrow{f} E'$ with $T(E) \xrightarrow{T(f)} T(E')$. Then, if $f : E \to F$, $g : F \to G$ a linear map, then $T(f) = \oplus_{r\geq 0} T(\underbrace{f, \cdots, f}_{r})$, then $T(id_E) = id_{T(E)}$, $T(g \circ f) = T(g) \circ T(f)$ by definition. Note that $T(\underbrace{f, \cdots, f}_{r})$ is a map induced from tensor product. This is from commutativity of tensor product map with product map.*

2. If E is free over R with basis $\{v_1 \cdots, v_n\}$, then $B_r = \{v_{i_1} \otimes \cdots \otimes v_{i_r} : \{i_1, \cdots, i_r\} \subset \{1, 2, \cdots, n\}\}$ is R-basis of $T^r(E)$, with $B_0 = \{1\}$. So, $B = \sqcup_{r\geq 0} B_r$ is R-basis of $T(E)$.

Let A be an R-algebra generated by $\{s_1, \cdots, s_n\} \subset A$. Then, $\exists \phi : T(E) \to A$, an R-algebra homomorphism such that $\phi(v_i) = s_i$ for $i = 1, \cdots, n$.

Proof. For $0 \leq r \leq n$, we can get below diagram from direct sum.

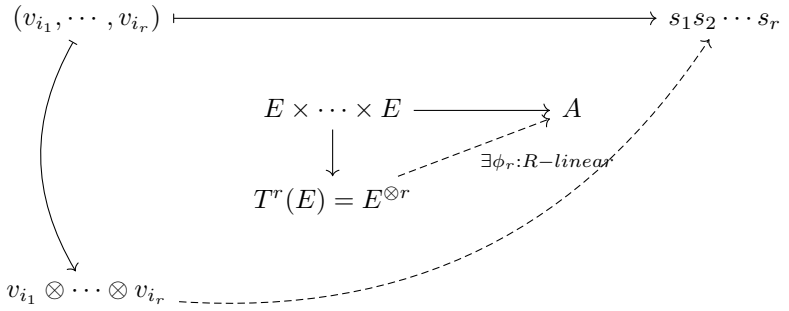
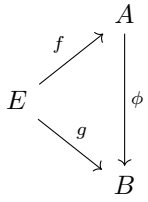


Figure 3: Commutative diagram for T(E)

From this, the R-linear map $\phi : T(E) \to A$ with $\phi = \oplus_{r\geq 0} \phi_r$, which preserves multiplication exists. □

Remark 1.1.3. *If E is a free module on $\{v_1, \cdots, v_n\}$, $T(E)$ can be viewed as a universal object in a certain category of R-algebra. So $T(E)$ is also called a "free non-commutative algebra generated by $\{v_1, \cdots, v_n\}$.", since $v_i \otimes v_j \neq v_j \otimes v_i$ if $i \neq j$.*

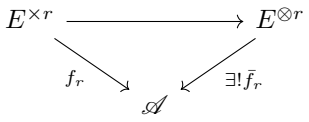
Proof. Define a category $\mathscr{C}$ with object $(\mathscr{A}, E \xrightarrow{f} \mathscr{A})$ where $\mathscr{A}$ is R-algebra, and f is R-linear map, with morphism $\phi : \mathscr{A} \to \mathscr{B}$ where ϕ is R-algebra homomorphism such that for $(\mathscr{A}, E \xrightarrow{f} \mathscr{A})$ and $(\mathscr{B}, E \xrightarrow{g} \mathscr{B})$, below figure commute. commute. In this category, $(T(E), E \xrightarrow{f} T(E))$ with $x \mapsto (0, x, 0, \cdots)$ exists, since f is R-linear.
It suffices to show that existence and uniqueness of morphism from $T(E)$ to every other object.



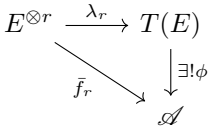
Let $(\mathscr{A}, f)$ be an arbitrary object in $\mathscr{C}$. Define $f_r : E^{\times r} \to \mathscr{A}$ by $f_r(v_1, \cdots, v_r) = f(v_1) \cdots f(v_r)$. Then f_r is R-multilinear map since for any $1 \geq i \geq r$,

$$\begin{aligned} f_r(v_1, \cdots v_{i-1}, av_i + w_i, v_{i+1}, \cdots, v_r) &= f(v_1) \cdots f(v_{i-1}) f(av_i + w_i) f(v_{i+1}) \cdots f(v_r) \\ &= af(v_1) \cdots f(v_r) + f(v_1) \cdots f(v_{i-1}) f(w_i) f(v_{i+1}) \cdots f(v_r). \end{aligned}$$

So, from the definition of tensor product as an universal object of a category of multilinear maps of a fixed multiset of modules $\{\underbrace{E, \cdots E}_{r}\}$, [1] [p.602-603], we can get unique $\bar{f}_r : E^{\otimes r} \to \mathscr{A}$, making below diagram commute.



By the universal property of a direct sum, $\exists! \phi : T(E) \to \mathscr{A}$ s.t. below diagram commutes. (λ_r

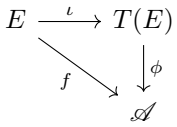


is natural injection.)
So, if we check that ϕ is R-algebra homomorphism and commute with R-linear map, we are done. Since E is free module on $\{v_1, \cdots, v_n\}$, it suffices to check that ϕ preserves multiplication for tensor products from the set. Now take $v_{i_1} \otimes \cdots \otimes v_{i_r}, v_{j_1} \otimes \cdots \otimes v_{j_s} \in T(E)$. Then,

$$\begin{aligned} & \phi((v_{i_1} \otimes \cdots \otimes v_{i_r}) \cdot (v_{j_1} \otimes \cdots \otimes v_{j_s})) \\ = \ & \phi(v_{i_1} \otimes \cdots \otimes v_{i_r} \otimes v_{j_1} \otimes \cdots \otimes v_{j_s}) \\ = \ & \bar{f}_{r+s}(v_{i_1} \otimes \cdots \otimes v_{i_r} \otimes v_{j_1} \otimes \cdots \otimes v_{j_s}) \\ = \ & f(v_{i_1}) \cdots f(v_{i_r}) f(v_{j_1}) \cdots f(v_{j_s}) \\ = \ & \bar{f}_r(v_{i_1} \otimes \cdots \otimes v_{i_r}) \cdot \bar{f}_s(v_{j_1} \otimes \cdots \otimes v_{j_s}) \\ = \ & \phi(v_{i_1} \otimes \cdots \otimes v_{i_r}) \cdot \phi(v_{j_1} \otimes \cdots \otimes v_{j_s}) \end{aligned}$$

So it is R-algebra homomorphism, and since $\forall v \in E$, $\phi(v) = f_1(v) = f(v)$, so following diagram commutes. □

Also note that even if E is not finite ranked, the above discussion still hold, without change the argument.



1.2 Symmetric Algebra

Definition 1.2.1. *A R-linear map $f : E^r \to F$ is symmetric if $f(x_1, \cdots x_r) = f(x_{\sigma(1)}, \cdots x_{\sigma(r)})$ for any $\sigma \in S_r$.*

Motivation is to remedy non-commutativeness of $T(E)$. For $r \geq 0$, I_r is R-submodule of $T^r(E)$ spanned by $x_1 \otimes \cdots \otimes x_r - x_{\sigma(1)} \otimes \cdots \otimes x_{\sigma(r)}$, for $x_i \in E, \sigma \in S_r$, a symmetric group with r.

Example 1.2.2. *If $r = 2$, $I_r =< x_1 \otimes x_2 - x_2 \otimes x_1 >$.*

Define $S^r := T^r(E)/I_r$, and $S(E) := \oplus_{r\geq 0} S^r(E)$. Denote the element $x_1 \otimes \bar{\cdots} \otimes x_r \in S^r(E)$ as $x_1 \cdots x_r$. Note that $S(E)$ is still R-module. Now define multiplication on $S(E)$ by

$$(x_1 \cdots x_p) \cdot (x'_1, \cdots, x'_q) = x_1 \cdots x_p x'_1 \cdots x'_q.$$

Proof. This multiplication is well-defined since for any $\sigma \in S_p$,

$$\begin{aligned}(x_{\sigma(1)} \cdots x_{\sigma(p)}) \cdot (x'_1, \cdots, x'_q) &= x_{\sigma(1)} \cdots x_{\sigma(p)} x'_1 \cdots x'_q \\ &= x_{\tau(\sigma(1))} \cdots x_{\tau(\sigma(p))} x'_{\tau(p+1)} \cdots x'_{\tau(p+q)} \\ &= x_1 \cdots x_p x'_1 \cdots x'_q \\ &= (x_1 \cdots x_p) \cdot (x'_1, \cdots, x'_q),\end{aligned}$$

where $\tau(k) = \sigma^{-1}(k)$ if $k \in [p]$, $\tau(k) = k - p$ if $k \in [q+p] \setminus [p]$. Note that $\tau \in S_{p+q}$. □

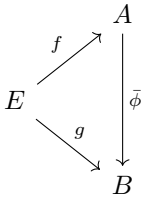
So $S(E)$ becomes an R-algebra, as the same arguments on $T(E)$.

Definition 1.2.3. *$S(E)$ is called the "symmetric algebra generated by E."*

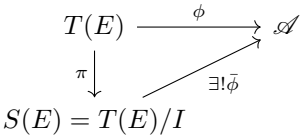
Remark 1.2.4. *1. $I = \oplus_{r\geq 2} I_r$, a two sided ideal in $T(E)$. (I_0, I_1 are empty.) Then, $S \cong T(E)/I$, from the argument that direct sum of quotient module is isomorphic to a quotient module of two direct sums.*

2. Suppose E is free over R with basis $\{v_1, \cdots, v_n\}$. Then $S(E)$ satisfies the universal mapping property, i.e., for commutative R-algebra generated by $\{s_1, \cdots, s_n\}$, say A, $\exists! \bar{\phi} : S(E) \to A$, an R- algebra homomorphism such that $\bar{\phi}(v_i) = s_i$ for $i = 1, \cdots, n$. So, $S(E)$ is called a free commutative algebra generated by $\{v_1, \cdots, v_n\}$.

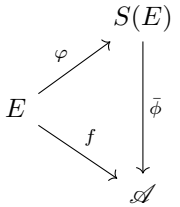
Proof of 1.9.2. Define a subcategory $\mathscr{D}$ of $\mathscr{C}$, with object $(\mathscr{A}, E \xrightarrow{f} \mathscr{A})$ where $\mathscr{A}$ is commutative R-algebra generated by n-elements, and f is symmetric R-linear map, with morphism $\bar{\phi} : \mathscr{A} \to \mathscr{B}$ where ϕ is R-algebra homomorphism such that for $(\mathscr{A}, E \xrightarrow{f} \mathscr{A})$ and $(\mathscr{B}, E \xrightarrow{g} \mathscr{B})$, below figure commute.
It is not an empty category, since $(S(E), E \xrightarrow{\varphi} S(E))$ with $f(x) = (0, x, 0, \cdots)$ is an object, since $S(E)$ is commutative and f is symmetric and linear. Now, it suffices to show that there exists unique R-algebra homomorphism from $S(E)$ to arbitrary object in $\mathscr{D}$. Take arbitrary commutative algebra $(\mathscr{A}, E \xrightarrow{f} S(E))$ in $\mathscr{D}$, where $\mathscr{A}$ is generated by $\{s_1, \cdots, s_n\}$. Since it is



also object in $\mathscr{C}$, $\exists!\phi : T(E) \to \mathscr{A}$. which is R-algebra homomorphism, which translate v_i in each elements to s_i for $i = 1, \cdots, n$. Also, canonical projection map (R-algebra homomorphism) from $T(E) \xrightarrow{\pi} S(E) = T(E)/I$ exists, since it preserves multiplication on $T(E)$. Then, by universal mapping property of quotients module $T(E)/I$, we can get unique $\bar{\phi} : S(E) \to \mathscr{A}$, which makes below diagram commutes.



Note that $\bar{\phi}$ is also R-algebra homomorphism since it is induced from category $\mathscr{C}$. So we should check that it is symmetric, since if it is symmetric, then $\bar{\phi}$ is unique morphism from $(S(E), \varphi) \to (\mathscr{A}, f)$ which commutes the diagram below, so we are done.



Since $\mathscr{A}$ is commutative, kernel of $\phi : T(E) \to \mathscr{A}$ contain terms such as $x_1 \cdots x_k - x_{\sigma(1)} \cdots x_{\sigma(k)}$ for any $k \in \mathbb{N}$ and any $\sigma \in S_k$. This implies that $I \subset \ker \phi$. Thus, ϕ is symmetric, therefore, $\bar{\phi}$ is also symmetric. So, $\bar{\phi}$ is unique symmetric R-algebra homomorphism, so $S(E)$ is universal. □

Note 1.2.5. *Check the "universal property of quotient module $T(E)/I$" in exact sense.*

Proof. Let's construct such category for some quotient module E/I. (X, f) be an objects in this category, where X is R-algebra, $f : E \to X$ be R-algebra homomorphism, and $I \subseteq \ker(f)$. Also define morphism $(X_0, f_0) \to (X_1, f_0)$ if $\exists g : X_0 \to X_1$ be R-algebra homomorphism such that $g \circ f_0 = f_1$. It is category, you can trivially checks. Then, $(E/I, \pi)$ is in this category, and let (X, f) be arbitrary object. Then, take $g : E/I \to X$ by $a + I \mapsto f(a)$. Then, it is well-defined since if $a + I = b + I$, then $f(b - a) = 0$ since $b - a \in I$, so $f(b) = f(a)$ since f is R-algebra homomorphism, so $g(a+I) = g(b+I)$. Also, $g(r(a+I)) = g(ra+I) = f(ra) = rf(a) = rg(a+I)$, and $g((a+I)+(b+I)) = f(a+b) = f(a)+f(b) = g(a+I)+g(b+I)$, and $g((a+I)\cdot(b+I)) = g(ab+I) = g(ab) = f(a)f(b) = g(a+I)\cdot g(b+I)$, where $(a+I)\cdot(b+I) = ab+I$ is from R-algebra's axiom. Therefore, g is R-algebra homomorphism, and it is unique since if g, h are such R-algebra homomorphism, then $g(a+I) = f(a) = h(a+I)$ for all $a \in E$, so $g = h$. □

Proposition 1.2.6 (Proposition 8.1 in Lang)**.** *Suppose E is free over R with basis $\{v_1, \cdots, v_n\}$. Then, $S(E) \cong R[x_1, \cdots, x_n]$ as an R-algebra, where $x_i's$ are indeterminate.*

Proof. Note that $(R[x_1, \cdots, x_n], E \xrightarrow{f} R[x_1, \cdots, x_n])$ with $f(v_i) = x_i$ is an object of $\mathscr{D}$, therefore $\exists! \bar{\phi} : S(E) \to R[x_1, \cdots, x_n]$, from universal mapping property. And by definition of f, $\bar{\phi}$ maps $\sum c_{i_1 \cdots i_r} v_{i_1} \cdots v_{i_r}$ with $(1 \leq i_1 \leq \cdots \leq i_r \leq n)$ to $\sum c_{i_1 \cdots i_r} x_{i_1} \cdots x_{i_r}$.
Suppose $\bar{v} = \sum c_{i_1 \cdots i_r} v_{i_1} \cdots v_{i_r} = 0$, then $\bar{\phi}(\bar{v}) = \sum c_{i_1 \cdots i_r} x_{i_1} \cdots x_{i_r} = 0$. Then, from linear independence, each $c_{i_1 \cdots i_r}$ in the sum is zero, therefore, $\bar{v}'s$ coefficients are zero. To recap, for any $r \geq 1$, $\{v_{i_1}, \cdots, v_{i_r} : 1 \leq i_1 \leq \cdots \leq i_r \leq n\}$ is linearly independent since $\{x_{i_1}, \cdots x_{i_r} : 1 \leq i_1 \leq \cdots \leq i_r \leq n\}$ is linearly independent in $R[x_1, \cdots, x_n]$. Therefore, with the fact that $\bar{\phi}$ maps basis to basis, it is one-to-one as show, and onto, since for any monomial $cx_{i_1} \cdots x_{i_r}$, there exists $cv_{i_1} \cdots x_{i_r}$ such that $\bar{\phi}(cv_{i_1} \cdots x_{i_r}) = cx_{i_1} \cdots x_{i_r}$. So, it is bijective R-algebra homomorphism, so isomorphism as R-algebra. □

Also note that for any monomial $f \in R[x_1, \cdots, x_n]$, we can identify it as a function from $\mathbb{Z}^n_{\geq 0} \to R$ such that if $f = ax_1^{m_1} \cdots x_n^{m_n}$, then $f(m_1, \cdots, m_n) = a$, otherwise $f(\cdot) = 0$. Then any element in the polynomial ring can be written by linear combination of those functions.

Corollary 1.2.7. *For $r \geq 1$, $\{v_{i_1} \cdots v_{i_r} : 1 \leq i_1 \leq \cdots \leq i_r \leq n\}$ is an R-basis of $S^r(E)$.*

Proof. We already proved it on the above statements. □

Proposition 1.2.8 (Proposition 8.2 in Lang)**.** *Let E, E' be free R-module of finite rank, with basis $B = \{v_1, \cdots, v_n\}, C = \{v_{n+1}, \cdots, v_{n+m}\}$ respectively. Then*

1. *$S^r(E \oplus E') \cong \oplus_{p+q=r} S^p(E) \otimes S^q(E)$*
2. *$S(E \oplus E') \cong S(E) \otimes S(E')$ as algebra.*

Proof. Let $f_E : E \to E \oplus E'$, $f_{E'} : E' \to E \oplus E'$, a canonical injection. Then we can define linear map

$$T : S(E) \otimes S(E') \to S(E \oplus E')$$

by

$$T(\overline{(v_{i_1} \otimes \cdots \otimes v_{i_r})}, \overline{(v_{i_{n+1}} \otimes \cdots \otimes v_{i_{n+s}})}) = \overline{(v_{i_1} \otimes \cdots \otimes v_{i_r} \otimes v_{i_{n+1}} \otimes \cdots \otimes v_{i_{n+s}})}.$$

for any monomial in $S(E)$. From the corollary above, it suffices to show that 1) $A := \{x \otimes y : x \in R\text{-basis of } S(E), y \in R\text{-basis of S(E') }\}$ is R-basis of $S(E) \otimes S(E')$, and 2) T is bijection of basis map, so that T is one-to-one and onto, and 3) T is homomorphism.
1) is easy, since for any element in $S(E) \otimes S(E')$ can be written by using their R-basis, so A spans $S(E) \otimes S(E')$, and A is linearly independent since for distinct $x_1 \otimes y_1, \cdots, x_k \otimes y_k$ with $k \in \mathbb{N}$, $\sum_{i=1}^k c_i x_i \otimes y_i = 0$ implies $c_i = 0$, since no two distinct elements are cancellable from linearly independence of B, C. (Suppose it is, then $(x_j + cx_l) \otimes (y_j + cy_l) = 0$ for some constant c, which implies $x_j = -cx_l$ or $y_j = -cy_l$, a contradiction.)
2) Is also easy but tedious; since every monomial in $S(E \oplus E')$ can be denoted as form

$$\overline{v_{i_1} \otimes \cdots \otimes v_{i_r} \otimes v_{i_{n+1}} \otimes \cdots \otimes v_{i_{n+s}}},$$

which is equal to

$$\overline{v_{i_1} \otimes \cdots \otimes v_{i_r}} \otimes \overline{v_{i_{n+1}} \otimes \cdots \otimes v_{i_{n+s}}},$$

which shows that T is onto. Also, if $T(\bar{x} \otimes \bar{y}) = 0$, then $\overline{x \otimes y} = 0$, implies every coefficients in the linear combination of basis representing $x \otimes y$ is zero, so that $\bar{x} \otimes \bar{y} = 0$, implies coefficients in

the its linear combination of basis representing $x \otimes y$ is zero, so $\bar{x} \otimes \bar{y} = 0$. This shows one-to-one. 3) is also tedious; Let $x \otimes y$, $x' \otimes y' \in S(E) \otimes S(E')$. Then,

$$\begin{aligned} T(x \otimes y \cdot x' \otimes y') &= T(x \otimes x' \otimes y \otimes y') \text{ from commutativity of } S(E) \otimes S(E') \\ &= \overline{x \otimes x' \otimes y \otimes y'} \text{ by definition of } T \\ &= \overline{x \otimes y \otimes x' \otimes y'} \text{ by commutativity of } S(E \oplus E') \\ &= \overline{x \otimes y'} \otimes \overline{y \otimes y'} \text{ by definition of product in } S(E \oplus E') \\ &= T(x \otimes y) \cdot T(x' \otimes y') \text{by definition of } T. \end{aligned}$$

Thus, T is an isomorphism. And first statement is deduced from T, since $S^r(E \oplus E')$ should be also mapped on elements which spanned by monomials with r elements, a direct sum above. □

Example 1.2.9. *Belows are deduced from second statement of proposition 8.2.*

1. $R[x] \otimes R[y] \cong R[x, y]$ *with* $x^m \otimes y^n \mapsto x^m y^n$.
2. *Let k be a field, and K is an extension of k as a ring, which implies as a vector space over k, then $K \otimes_k k[x] \cong K[x]$ as K-algebra.*

1.3 Exterior Algebra

It is also called **alternating algebra** or **Grassmann algebra**. Let J_r be the R-submodule of $T^r(E)$ generated by $x_1 \otimes \cdots \otimes x_r - sgn(\sigma) x_{\sigma(1)} \otimes \cdots \otimes x_{\sigma(r)} = 0$, for $x_i \in E, \sigma \in S_r$. Define $\bigwedge^r(E) = T^r(E)/J_r$, and $\bigwedge(E) = \oplus_{r \geq 0} \bigwedge^r(E)$. And denote $x_1 \otimes \cdots \otimes x_r + J_r \in \bigwedge^r(E)$ as $x_1 \wedge \cdots \wedge x_r$, call it wedge product. Then $\bigwedge(E)$ is an R-algebra with respect to $(x_1 \wedge \cdots \wedge x_r) \cdot (y_1 \wedge \cdots \wedge y_r) = x_1 \wedge \cdots \wedge x_r \wedge y_1 \wedge \cdots \wedge y_r$.

Definition 1.3.1. *$\bigwedge(E)$ is called the exterior algebra generated by E.*

Remark 1.3.2. *Suppose E is free over R with basis $\{v_1, \cdots, v_n\}$. Then, for $r = 0$, $\bigwedge^r(E) = T^0(E) = R$, for $r = 1$, $\bigwedge^1(E) = T^1(E) = E$, for $1 < r < n$, $\bigwedge^r(E) =$span $\{v_{i_1} \wedge \cdots \wedge v_{i_r} : 1 \leq i_1 < \cdots < i_r \leq n\}$, for $r = n$, $\bigwedge^r(E) = Rv_1 \wedge \cdots \wedge v_n$, and $\bigwedge^r(E) = 0$ for $r > n$.*
Also, if $w_j = \sum_{i=1} a_{ij} v_i$ for $j \in [n]$, $w_1 \wedge \cdots \wedge w_n = \det(a_{ij}) v_1 \wedge \cdots \wedge v_n$, since only terms choosing all of v_i left up to sign, and definition of determinant, $detA = \sum_{\sigma \in S_n} sgn(\sigma) a_{1,\sigma(1)} \cdots a_{n,\sigma(n)}$ covers all such elements.

Note that alternating n-linear form has linearity, and sign is changed when we permute its input.

Proposition 1.3.3 (Proposition 1.1 on Lang)**.** *Let E be such free group. Then, for $1 \leq r \leq n$, $\{v_{i_1} \wedge \cdots \wedge v_{i_r} : 1 \leq i_1 < \cdots < i_r \leq n\}$ are R-basis of $\bigwedge^r(E)$.*

Proof. First of all, we should show that $\forall a \in R, \exists!$ alternating n-form F such that $F(v_1, \cdots, v_n) = a$. To show this, let F be arbitrary alternating n-form. Then, for $(w_1, w_2, \cdots, w_n)$ where

$w_i = \sum_{j_i=1}^{n} a_{i,j_i} v_{j_i}$,

$$\begin{aligned}
F(w_1, w_2, \cdots, w_n) &= \sum_{j_1} \cdots \sum_{j_n} \prod_{k=1}^{n} a_{k,j_k} F(v_{j_1}, \cdots, v_{j_n}) \text{ by linearity,} \\
&= \sum_{f \in [n]^{[n]}} \prod_{k=1}^{n} a_{k,j_k} F(v_{f(1)}, \cdots, v_{f(n)}) \text{ just consider all possible functions,} \\
&= \sum_{\sigma \in \mathfrak{S}_n} \prod_{k=1}^{n} a_{k,j_k} F(v_{\sigma(1)}, \cdots, v_{\sigma(n)}) \text{ since only bijections (permutations) are nonzero,} \\
&= \sum_{\sigma \in \mathfrak{S}_n} sgn(\sigma) \prod_{k=1}^{n} a_{k,j_k} F(v_1, \cdots, v_n) \text{ from alternating property,} \\
&= \det(a_{i,j_i}) F(v_1, \cdots, v_n) \text{ by definition of determinant.}
\end{aligned}$$

Actually this argument proves the latter part of above remark. Also, the argument shows that every alternating n-linear form is determined when we fix its value on $(v_1, \cdots, v_n)$. So for any two alternating form having the same value a on $(v_1, \cdots, v_n)$ is equivalent, therefore, $Alt_n(E) \cong R$, where $Alt_n(E)$ is the set of alternating R-multilinear map. Also, we get projection $\pi = \pi_{J_r} \circ \pi' : E^{\times n} \to T^r(E) = E^{\otimes n} \to E^r/J_r = \bigwedge^n E$ as follow; first of all, as we shown in remark 1.6, for the morphism $E^{\times} \xrightarrow{f} R$, with projection map $\pi' : E^{\times n} \to T^n$ defined in the remark 1.6, we get unique map $\varphi : T^n(E) \to R$, from universal property of $T^n(E)$. Also, using this φ, and a canonical projection map ϕ_{J_r}, we can get unique G by the universal mapping property, since $J_r \subset \ker \varphi$. So, we get the universal property in Figure 4.

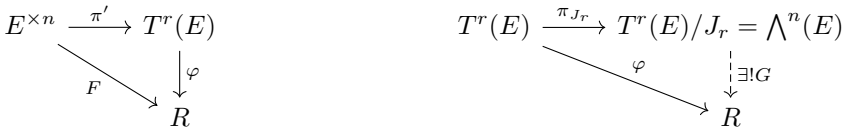


Figure 4: Two commutative maps for π', π_{J_r}.

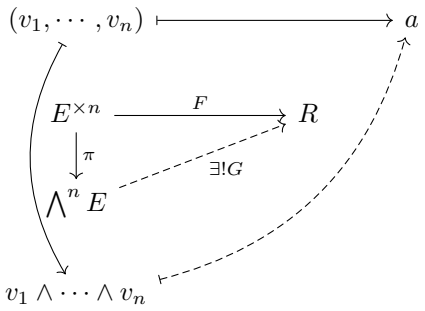


Figure 5: Universal property of alternating mulitilinear map.

In short, we have a universal property of $\bigwedge^n(E)$ with respect to R-linear alternating maps. Also, note that every R-algebra homomorphism from $\bigwedge^n E$ to R is can be induced by R-linear alternating map F since for any $\phi \in \mathrm{Hom}_R(\bigwedge^n(E), R)$, $\phi(rv_1 \wedge \cdots \wedge v_n) = r\phi(v_1 \wedge \cdots \wedge v_n)$,

therefore it is induced by F whose value on $(v_1, \cdots, v_n)$ is equal to $\phi(v_1 \wedge \cdots \wedge v_n)$. So, $Alt_n(E) \cong \mathrm{Hom}_R(\bigwedge^n(E), R)$. Next, It is clear that $v_1 \wedge \cdots \wedge v_n$ generates $\bigwedge^n E$. However, it may be not linearly independent, for example, 1 generate $\mathbb{Z}/3\mathbb{Z}$ but $\{1\}$ is not linearly independent when we see $\mathbb{Z}/3\mathbb{Z}$ as $\mathbb{Z}$-module, since $3 \cdot 1 = 0$. So we should check linear independence. Let $v = v_1 \wedge \cdots \wedge v_n$, with $rv = 0$. Then, for any $G \in \mathrm{Hom}_R(\bigwedge^n(E), R)$, $G(rv) = rG(v) = 0$. Now, take G such that $G(v) = 1$, then $r = 0$, so it is linearly independent as R-module. Hence $\bigwedge^n(E)$ has a basis $\{v_1 \wedge \cdots \wedge v_n\}$, so it is free over R. □

Proof of remark. For $\bigwedge^r E$ with $1 \leq r < n$, we also show that linear independence of $\mathscr{B}_r = \{v_{i_1} \wedge \cdots \wedge v_{i_r} : 1 \leq i_1 < \cdots < i_r \leq n\}$. (Actually, $\bigwedge^r E$ =span $\mathscr{B}_r$ is trivial.) Let $0 = \sum a_{i_1, \cdots, i_r} v_{i_1} \wedge \cdots \wedge v_{i_r}$, with $i_1 < \cdots < i_r$. Then, choose particular $(i_1, \cdots i_r)$, say $(i'_1, \cdots i'_r)$ let $w = j_{r+1} \wedge \cdots \wedge j_n$ be wedge products where $j's$ terems are not in $\{i'_1, \cdots, i'_r\}$. Then,

$$0 = \left(\sum a_{i_1, \cdots, i_r} v_{i_1} \wedge \cdots \wedge v_{i_r}\right) \wedge w = (a_{i'_1, \cdots, i'_r}) v_{i'_1} \wedge \cdots v_{i'_r} \wedge v_{j_{r+1}} \wedge \cdots \wedge v_{j_n} = (sgn(\sigma) a_{i'_1, \cdots, i'_r}) v_1 \wedge \cdots \wedge v_n$$

where $\sigma = (i'_1, \cdots, i_r, j_{r+1}, \cdots, j_n)^{-1} \in \mathfrak{S}_n$. Note that the second equality holds since all other terms vanishes by above wedge product since they contain at least one elements among $v_{j+1}, \cdots v_n$. Since $\bigwedge^n$ has basis $v_1 \wedge \cdots \wedge v_n$, $a_{i'_1, \cdots, i'_r} = 0$. Since $(i_1, \cdots i_r)$ was arbitrarily chosen, all coefficients are zero. □

2 Polynomial Ring

This is from [1][Ch4]

2.1 Basic Properties for polynomials over a field

Theorem 2.1.1 (Euclidean Algorithm)**.** *A is a commutative ring. $f(x), g(x) \in A[x] \setminus \{0\}$ where the leading coefficient of $g(x)$ is a unit. Then, $\exists! q(x), r(x) \in A[x]$ s.t. $f(x) = g(x)q(x) + r(x)$ where $\deg r(x) < \deg g(x)$.*

Proof. Let $f(X) = a_n X^n + \cdots + a_0$, $g(X) = b_n X^d + \cdots + b_0$, where $n = \deg f$, $d = \deg g$ so that $a_n, b_d \neq 0$ and b_d is a unit in A. Use induction;

- If $n = 0$, and $d > n$, take $q = 0, r = f$. if $d = n = 0$, then $r = 0$, $q = a_n b_d^{-1}$
- Suppose it is proved for $n < m$, with $m > 0$. Assume $d \leq n$ (otherwise, take $q = 0$, $r = f$.) Then,
$$f(X) = a_n b_d^{-1} X^{n-d} g(X) + f_1(X),$$
where $\deg f_1 < n$. So by inductive hypothesis, $\exists! q_1, r$ such that
$$f(X) = a_n b_d^{-1} X^{n-d} g(X) + q_1(X) g(X) + r(X)$$
Take $q(X) = a_n b_d^{-1} X^{n-d} + q_1(X)$

so existence is proved.

As for uniqueness, let $f = q_1 g + r_1 = q_2 g + r_2$. with $\deg r_1, \deg r_2 < \deg g$. Then $(q_1 - q_2)g = r_2 - r_1$. Since the leading coefficient of g is unit (so none of coefficients of $q_1 - q_2$ are zero when proceeds product),

$$\deg(q_1 - q_2)g = \deg(q_1 - q_2) + \deg g.$$

But $\deg(r_2 - r_1) < \deg g$, $q_1 - q_2 = 0$, $r_1 - r_2 = 0$ are only solution. □

Suppose k is a field.

Remark 2.1.2. *Let $f(x) \in k[x] \setminus \{0\}$. Then*

- *$f(x)$ is unit in $k[x]$ if and only if $f(x) \in k^*$ or $\deg f(x) = 0$, where $k^* = k \setminus \{0\}$.*
- *$f(x)$ is irreducible if and only if $f(x)$ is not of the form $f(x) = g_1(x)g_2(x)$ with $\deg g_i(x) > 0$ for $i = 1, 2$.*

Proof. ($\Leftarrow$) is easy since $1 \in k$ is also $1 \in k[x]$, so k^* is still unit in $k[x]$. Also, if $f(x)$ is nonzero degree zero polynomial, it is in k^*. So it is unit.
($\Rightarrow$) Suppose $f(x)$ is nonzero polynomial with degree > 0. Then its the leading coefficient is unit, so none of elements in k^* make it zero by product, therefore f(x)g(x) cannot be 1 for any nonzero $g(x)$. Hence $\deg f = 0$, so $f \in k^*$

A polynomial is **irreducible** if it has degree ≥ 1, and if one cannot write $f(x)$ as a product with $f(X) = g(X)h(X)$ with $g, h \in k[X]$, and both $g, h \notin k$. So, by definition, above statement holds. □

Recall 2.1.3. *If $f(x) = (x-a)^m g(x)$ for some $a \in k$, $m \geq 1$ with $g(a) \neq 0$, then a is a **root** of $f(x)$, with **multiplicity** m.*

Applications of theorem 2.1 are below;

- $k[x]$ is principal, hence factorial.
- If $f(x) \in k[x]$ with $\deg f = n \geq 0$, $f(x)$ has at most n roots in k.

Proof. Those are theorem 1.2, 1.3, and 1.4 in [1][IV, §1]. Suppose $\mathfrak{a}$ is an ideal of $k[x]$, assume $\mathfrak{a} \neq 0$. Let $g \in \mathfrak{a}$ of a smallest degree ≥ 0. Let $f \in \mathfrak{a}$ with $f \neq 0$. Then by Euclidean algorithm, $\exists! q, r$ such that $f = qg + r$. With $\deg r < \deg g$. But $r = f - qg \in \mathfrak{a}$, this contradicts the minimality of degree of g if $r \neq 0$. So $r = 0$, hence $\mathfrak{a} =< g >$. From principal ideal ring $\Rightarrow$ unique factorization ring in [1][II, §2, Theorem 5.2], $k[X]$ is factorial. (Factorial means unique factorization.)

For the second part, suppose $f(a) = 0$, then $\exists! q, r$ s.t. $f(x) = q(x)(x-a) + r(x)$, with $\deg r < 1$. So, $0 = f(a) = r(a)$, implies $r = 0$. Hence $f(x) = (x-a)q(x)$, with $\deg q = n - 1$. From induction that for $n = 0$, it is true, and for any n degree polynomial, the last argument show that q has at most $n-1$ roots, therefore f has at most n roots. □

Theorem 2.1.4 (Theorem 1.9 in [1][IV, §1)**.** *Suppose u be a finite multiplicative subset of k. Then u is a cyclic group of k^**

Proof. Note that u is group, since for arbitrary $g \in u$, $g^1, g^2, \cdots g^k \cdots \in u$, however u is a finite, so $\exists n, m \in \mathbb{N}$ such that $n \neq m$, $g^n = g^m$. Hence $g^{n-m} = 1$, so u has inverse, associativity and identity.
Also u is abelian since it is subgroup of a field. Hence, by the fundamental theorem of finite abelian group (Every finite abelian group is an internal group direct product of cyclic groups whose orders are prime powers.),

$$u = \prod_{p:prime} u(p)$$

where $u(p)$ is a p-group, i.e., finite group whose order is p^r for some $r \in \mathbb{N}$. Fix p, and let $p^r = \max\{|a| : a \in u(p)\}$. Then $\forall a \in u(p)$, $a^{p^r} = 1$. Hence all elements in $u(p)$ is a root of $X^{p^r} - 1$. And by letting a' be element having maximal order in $u(p)$, then $< a >$ has p^r elements. If $u(p)$ is not equal to $< a >$, then $X^{p^r} - 1$ has more then p^r roots, contradiction. Hence $u(p) =< a >$. Since orders in $\prod u(p)$ are relatively prime, by theorem 4.3(v) in [1][I,§4], u is cyclic. □

Example 2.1.5. *$n \geq 1$, $\mu_n = \{\xi : \xi^n = 1\}$, cyclic of order n. Then $\mu_n =< \xi_n >$, where ξ_n is n-th primitive root.*

Corollary 2.1.6 (Corollary 1.10 in [1][IV,§1)**.** *Let k is finite field, then k^* is cyclic.*

This is deduced directly from the above theorem.

Definition 2.1.7. *For $f(x) = an_x^n + \cdots + a_1 x + a_0 \in k[x]$, let $D(\cdot) : k[x] \to k[x]$ such that*

$$Df(x) = na_n x^{n-1} + \cdots + a_1$$

D is k-linear (this is proved at basic calculus course). It is called ***a formal derivative****.*

Note that $D(fg) = D(f)g + fD(g)$, and $a_l = D^l f(0)$ for $l \geq 0$.

Proposition 2.1.8 (Proposition 1.11 in [1][IV,§1)**.** *Let a be a multiple root of $f(x) \iff f(a) = f'(a) = 0$.*

Proof. If a is a multiple root of $f(x)$, then by definition, $f(x) = (x-a)^m g(x)$for some $m > 1$, $g(x) \in k[x]$. Therefore, by Leibniz rule, $f'(x) = m(x-a)^{m-1}g(x) + (x-a)^m g'(x)$, so $f'(a) = 0$. Conversely, if $m = 1$, then $f'(x) = (x-a)g'(x) + g(x)$, so $f'(a) = g(a) \neq 0$. So, we must have $m > 1$ if $f'(a) = 0$. □

Proposition 2.1.9 (Proposition 1.12 in [1][IV,§1)**.** *Let $f(x) \in k[x]$, with $\deg f(x) \geq 1$. Then if ch $k = 0$, then $f'(x) \neq 0$, if ch $k = p$, then $f(x) = g(x^p)$ for some $g(x) \in k[x]$ if and only if $f'(x) = 0$.*

Proof. For the first part, from $\deg(f) = n \geq 1$, f has x^n term with nonzero coefficient. Hence its derivative contain nx^{n-1} with nonzero coefficients.
For the second part, if $f(x) = \sum_{i=0}^n a_i x^i$, suppose $f'(x) = 0$. Then, for any nonzero a_m, $1 \leq m \leq n$, $p|m$; because $f'(x)$ has coefficients ma_m for each x^{m-1}, so $ma_m = 0$ implies that. Hence, we can represent each x^m having nonzero coefficients as $(x^p)^r$ for some r. So, take $g(x)$ consists of $a_m x^r$ for such m. Then, $g(x^p) = f(x)$. □

Remark 2.1.10 (Frobenius Homomorphism)**.** *Let $\sigma_p : k \to k$ by $x \mapsto x^p$an injective ring homomorphism, where k is a field with characteristic p. Check that it is ring homomorphism below;*

$$\begin{aligned} \sigma_p(a+b) &= (a+b)^p = a^p + b^p = \sigma_p(a) + \sigma_p(b) \text{ by freshman's dream.} \\ \sigma_p(ab) &= a^p b^p = \sigma_p(a)\sigma_p(b) \\ \sigma_p(a) = 0 &\implies a^p = 0, \text{ so } a = 0. \end{aligned}$$

Hence, if k is finite field, then it is isomorphism, hence automorphism.

In proposition 1.12, if $f \in k[x]$ and $f'(x) = 0$, then $f(x) = h(x)^p$ for some $h(x) \in k[x]$, since from $f'(x) = 0$, $f(x) = \sum_{i=1}^k a_{pn_i} x^{pn_i}$, as shown above. Also, each a_{pn_i} has a b_{n_i} such that $\sigma_p(b_{n_i} = a_{pn_i}$, since σ_p is automorphism. Therefore, let $h(x) = \sum_{i=1}^k b_{pn_i} x^{n_i}$. Then,

$$(h(x))^p = \left(\sum_{i=1}^k b_{pn_i} x^{n_i}\right)^p = \sum_{i=1}^k (b_{pn_i})^p (x^{n_i})^p = \sum_{i=1}^k a_{pn_i} x^{pn_i} = f(x)$$

by freshman's dream.
For example, $x^{p^r} - c$ has a root in k, say α, then $\alpha^{p^r} = c$, so $x^{p^r} - \alpha^{p^r} = (x-\alpha)^{p^r}$.

2.2 Polynomials over a factorial ring

Let A be a factorial ring, i.e., A is entire (integral domain) and every nonzero elements have a unique factorization by irreducible elements. k be the quotient field of A.

Remark 2.2.1. *$p \in A$ is prime $\iff$ p is irreducible.*

Proof. To show that prime implies irreducible, suppose $p = ab$, where p is prime but not irreducible, hence $\exists a, b$ where a, b is nonzero nonunit. Then, $p|ab$, hence $p|a$ or $p|b$ by definition of prime. Without loss of generality, let $a = pc$ for some $c \in A$. Then, $p = pcb$, which implies $cb = 1$ since A is integral domain, hence b is unit, contradiction.
Conversely, suppose p is irreducible. Then, p is non unit. Take $ab \in (p) \setminus 0$. Then, $ab = cp$ for some $c \in A$. Since A is factorial, we have unique factorization of a, b, c. Then, from unique factorization, at least one element in such factorization of ab contain p. Hence $p|a$ or $p|b$. □

Suppose $a \in k^* = K \setminus \{0\}$. Then, $a = p^r \frac{b_1}{b_2}$ for unique $r \in \mathbb{Z}$ and $b_1, b_2 \in A$ such that $p \neq b_1, b_2$. (If there is another $r' \in \mathbb{Z}$ with $\frac{b_1'}{b_2'}$ such that $\frac{b_1'}{b_2'} = \frac{b_1}{b_2}$, then from unique factorization, so either $p|b_1'$ or $p|b_2'$, therefore $b_1 b_2' = b_1' b_2$, so by unique factorization, $p|b_1$ or $p|b_2$, contradiction.) Hence we can define such unique number r as order;

Definition 2.2.2. *For $a \in k^*$, we can represent a as $p^r \frac{b_1}{b_2}$ for unique $r \in \mathbb{Z}$. Say r as "the order of a at p," and write $r = ord_p(a)$.*

Note that

$$ord_p(aa') = ord_p(a) + ord_p(a')$$

Extend this definition to polynomial;

Definition 2.2.3. *Let $f(x) = \sum_{i=0}^n a_i x^i$. Then, $\forall p \in A$, where p is prime,*

$$ord_p(f) := \min_{a_i \neq 0, \forall i} \{ord_p(a_i)\}.$$

Also, define "the content of f" as

$$cont(f) := \prod_{p, prime} p^{ord_p(f)}.$$

*And if $cont(f) = 1$, then f is called **primitive**.*

Remark 2.2.4. *1. $f(x)$ is primitive, then $f(x) \in A[x]$, since*

$$cont(f) = 1 \implies \forall p, ord_p(f) = 0 \implies \forall p, \min_i ord_p(a_i) \geq 0 \implies a \in A.$$

2. $cont(cf(x)) = c \cdot cont(f)$ for any $c \in k^*$

3. $f(x) = cont(f(x)) f_1(x)$ where $f_1(x)$ is primitive, and $f_1(x) \in A[x]$.

4. If $\forall f(x) = \sum_{i=0}^n a_i x^i \in A[x] \setminus \{0\}$, then $cont(f) = g.c.d(a_1, \cdots, a_n$.
Here, we assume that $cont(f) = \infty$ if $f = 0$.

Theorem 2.2.5 (Gauss Lemma)**.** *Let $f, g \in k[x]$. Then $cont(fg) = cont(f) \cdot cont(g)$.*

Proof. Assume $fg \neq 0$. Then, $f = cont(f)f_1$, $g = cont(g)g_1$ where $f_1, g_1 \in A[x]$, with $f_1 = \sum_i a_i x^i$, $g_1 = \sum_j b_j x^j$. It suffices to show that $cont(f_1 g_1) = 1$, which means that $\forall p$, prime, $ord_p(f_1 g_1) = 0$.
Let p be arbitrary prime. Choose maximal $r, s \geq 0$, such that $p \not| a_r$, $p \not| b_s$. (Since $cont(f_1) = cont(g_1) = 1$, at least one of coefficients in $f_1 and g_1$ cannot be divisible by p.) Then coefficient of $x^{r+s} \in f_1 g_1$, say c, is

$$\begin{aligned} c = a_r b_s \quad + \quad & a_{r-1} b_{s+1} + \cdots \\ & a_{r+1} b_{s-1} + \cdots . \end{aligned}$$

Then except $a_r b_s$, all other terms in the righthandside of c is divisible by p, so c is not divisible by p. Since p was arbitrary, $c \not\equiv 0 \bmod p$. So $ord_p(f_1 g_1) = 0$ for all p. □

Theorem 2.2.6 (Theorem 2.3 in [1] IV. §2)**.** *Given A, k, $A[x]$ is factorial, and the set of primes in $A[x]$ is $\{p : prime\ in\ A\} \cup \{f(x) : f(x)\ is\ irreducible\ in\ k[x]\ and\ f\ is\ primitive\ \}$.*

Corollary 2.2.7. *If $x_1, \cdots, x_n$ are indeterminate, then $A[x_1, \cdots, x_n]$ is factorial.*

Lemma 2.2.8. *If k is a field, then $k[x]$ is euclidean domain.*

Proof. Since all nonzero elements in k is unit, we can use euclid algortihm and deg function as euclidean function. □

Note that deg function is not euclid function in general integral domain, since we cannot use euclid alorithm for a polynomial with nonunit coefficient.

Proof of the theorem. Let $f(x) \in A[x] \setminus \{0\}$, and assume $\deg(f) \geq 1$. (Otherwise, it has unique factorization from A.) Note that $k[x]$ is factorial since $k[x]$ is euclidean domain. So, $f(x) = p_1(x) \cdots p_r(x)$ for some irreducible $p_i(x) \in k[x]$. Now let $p_i(x) = c_i q_i(x)$ where $c_i = cont(p_i(x)), q_i(x) \in A[x]$, which is primitive. Then,

$$f(x) = \left(\prod_{i=1}^{r} c_i \right) q_1(x) \cdots q_r(x)$$

and note that $(\prod_{i=1}^{r} c_i) \in A$ since $(\prod_{i=1}^{r} c_i) = cont(f(x))$ by the Gauss Lemma and $q_1 \cdots q_r$ is primitive. Also note that $q_i(x)$ is irreducible in $k[x]$, since it is the same as $p_i(x)$ up to unit. Now it suffices to show that $q_i(x)$ is irreducible in $A[x]$ and that such factorization is unique.
Suppose not. Then $q_i(x) = r_i(x)s_i(x)$ for some nonzero nonunit $r_i, s_i \in A[x]$. Then, $cont(q_i) = cont(r_i)cont(s_i) = 1$. So, if one of r_i, s_i has degree zero, then that degree zero polynomial is unit, a contradiction. Hence $\deg(r_i) > 0, \deg(s_i) > 0$. However, in this case, r_i, s_i is also nonzero nonunit in $k[x]$, so $q_i(x)$ is reducible in $k[x]$, a contradiction. Hence $q_i(x)$ is irreducible in $A[x]$.
To show uniqueness, suppose there are another factorization such that

$$f(x) = cq_1(x) \cdots q_r(x) = d\tilde{q_1}(x) \cdots \tilde{q_s}(x).$$

where $q_i, \tilde{q_j} \in A[x]$ are primitive and their degree are at least 1. By comparing content of the equation, $c = d$. Since $k[x]$ is factorial, $r = s$, $q_i = u_i \tilde{q_i}$ for some $u_i \in K$ up to some permutation. So, $u_i = \frac{a_i}{b_i}, a_i, b_i \in A$. Hence $b_i q_i(x) = a_i \tilde{q_i}(x)$. Since content of lefthandside and that of righthandside is equal and $cont(q_i) = cont(\tilde{(q_i)}) = 1$, so $cont(b_i) = cont(a_i)$, therefore u_i contain only unit elements in its factorization, otherwise above equality cannot hold. So $q_i = u_i \tilde{q_i}$ for some $u_i \in A$, done.
The second statement is follows from construction of factorial ring $A[x]$ from $k[x]$; suppose f is

prime element such that $f|gh$ for some $g, h \in A[x]$. Then $f|g$ or $f|h$, which implies f is contained in factorization of g or that of h, so f should be primitive and irreducible in $k[x]$, since we construct factorization from $k[x]$. □

Remark 2.2.9. *Let $f(x) \in A[x]$, primitive, degree ≥ 1. Then $f(x)$ is irreducible in $A[x] \iff$ $f(x)$ is irreducible in $k[x]$.*

Proof. If f is irreducible in $A[x]$ then it is prime in $A[x]$ since $A[x]$ is factorial, so by the above theorem, f is irreducible. Conversely, if f is irreducible in $k[x]$, and having content 1, then the above theorem tells that f is prime in $A[x]$, so f is irreducible. □

2.3 Criteria for irreducibility

Theorem 2.3.1 (Eisenstein Criterion)**.** *Let A be factorial ring, k be the quotient field of A, and $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in A[x]$ of degree $n \geq 1$. If $\exists p$, prime in A, such that $a_n \not\equiv 0$ (mod p), $a_i \equiv 0$ (mod p) for $0 \leq i < n$, and $a_0 \not\equiv 0$ (mod p^2). Then f is irreducible in $k[x]$.*

Proof. Assume $cont(f) = 1$. (Otherwise, get g.c.d. out of f). Suppose $f(x) = g(x)h(x)$ for some $g(x), h(x) \in k[x]$ of degree at least 1, where g, h are nonzero nonunit. By the gauss lemma, g, h are primitive, so $g, h \in A[x]$. Let $g(x) = b_r x^r + \cdots + b_0$, $h(x) = c_s x^s + \cdots + c_0$. Then, $b_i, c_j \in A$, and $p \not| a_n = b_r c_s$, and $p|b_0 c_0$ but $p^2 \not| b_0 c_0$. Without loss of generality, $p|c_0$ but $p \not| b_0$. Take the smallest t such that $p \not| c_t$. Then, since all terms except the first term is divisible by p but $p \not| b_0 c_t$ implies $p \not| a_t = b_0 c_t + b_1 c_{t-1} + \cdots$. So $a_t \not\equiv 0 \pmod{p}$, a contradiction. □

Lemma 2.3.2. *Let D be integral domain, $c \in D$. Then $f(x) \in D[x]$ is nonunit if and only if $f(x - c)$ is nonunit. Also, $f(x) \in D[x]$ is nonzero if and only if $f(x - c)$ is nonzero.*

Proof. For the first statement, it suffices to show that $f(x)$ is unit if and only if $f(x - c)$ is unit. Suppose $f(x)$ is unit in $D[x]$. Then $\exists g \in D[x]$ such that $fg = 1$. By theorem 6.1.(iii), $0 = \deg(1) = \deg(fg) = \deg(f) + \deg(g)$. So, $\deg(f) = \deg(g) = 0$, hence $f, g \in D$. So, $f(x) = f(x-c), g(x) = g(x-c)$. Conversely, if $f(x-c)$ is a unit, the same argument shows that $f(x-c) \in D$, so $f(x) = f(x-c)$.
For the second statement, let $f(x)$ be nonzero in D. If $\deg(f) = 0$, then $f(x) = f(x - c)$ so done. If $\deg(f) \geq 1$, then $f(x) = a_0 + \sum_{i=1}^{n} a_n x^n$ for some $n \geq 1$, with $a_n \neq 0$.Then $f(x - c) = a_0 + \sum_{i=1}^{n} a_n (x-c)^n$ is nonzero polynomial since its unique form from linear combination of the power of x is nonzero, since $a_n x^n$ is contained in $f(x - c)$ with $a_n \neq 0$. □

Lemma 2.3.3 (Exercise III. 6. 10 in [2])**.** *Let D be integral domain. Then, $f(x) \in D[x]$ is irreducible $\iff$ $f(x - c)$ is irreducible for some $c \in D$.*

Proof. Now suppose $f(x)$ is reducible. Then there exists $g(x), h(x) \in D[x]$ such that $f(x) = g(x)h(x)$, where $g(x), h(x)$ are nonzero and nonunit. Then, by replacing x^i to $(x - c)^i$ for all monomials in the lefthandside and the righthandside of equation, $f(x-c) = g(x-c)h(x-c)$. Since $g(x-c), h(x-c)$ are also nonzero, nonunit by above lemma, $f(x-c)$ is also reducible. Conversely, $f(x - c)$ be reducible. Then there exists $g(x), h(x) \in D[x]$ such that $f(x - c) = g(x)h(x)$. By the exercise III. 6. 2. proved above, for each g, h, with respect to $(x - c)$ we can get a unique polynomials having degree lower than $1 = \deg(x - c)$, representing g, h by linear combination of power of $(x - c)$, respectively. Since degrees are lower than 1, they are in D, so we can get $g'(x-c), h'(x-c)$ such that $g'(x-c) = g(x), h'(x-c) = h(x)$. Hence, $f(x-c) = g'(x-c)h'(x-c)$,so by replacing x to $x - c$ in both sides, $f(x) = g'(x)h'(x)$. Since $g'(x), h'(x)$ are also nonunit and nonzero by the lemma, $f(x)$ is reducible. □

Example 2.3.4.

- *For $a \in \mathbb{Z} \setminus \{\pm 1\}$ such that a is squarefree, $x^n - a$ is irreducible in $Q[x]$.*
- *For $f(x) = \frac{x^p-1}{x-1} \in \mathbb{Z}[x]$, with prime p, let*

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

  satisfy the Eisenstein criterion, so it is irreducible in $\mathbb{Q}[x]$. And by the above lemma, $f(x)$ is irreducible in $\mathbb{Q}[x]$.

- *Let t be indeterminate, k be a field. Then, let $A = k[t], K$ be the quotient field of A. Then, $x^n - t \in K[x]$. Also, t is prime in A as factorial ring, by the theorem 2.3 in [1][IV. §2]. So, by the Eisenstein criterion, $x^n - t$ is irreducible in $K[x]$. Since $x^n - t$ is primitive, it is irreducible in $A[x] = k[t, x]$, so it is irreducible in $k[t, x]$.*
- *$x^3y^2 + x^3 + xy^2 + y \in k[x, y]$. It is factorial ring, so think the polynomial as*

$$(y^2 + 1)x^3 + y^2x + y.$$

  Then, $y^2 + 1 \not\equiv 0$ mod y, $y|y^2$, but $y^2 \not| y$, so this polynomial satisfies the Eisenstein criterion, hence it is irreducible in $k[x][y] = k[x, y]$.

Theorem 2.3.5 (Reduction Criterion)**.** *Suppose A, B are entire ring, K, L are the quotient field of A, B respectively, and $\phi : A \to B$ be a ring homomorphism. (So we can extend it as homomorphism for $A[x] \to B[x]$. If $f(x) \in A[x]$ such that $\deg(\phi f) = \deg(f) = n \geq 1$ and ϕf is irreducible in $L[x]$, then $f(x)$ does not have a factorization $f(x) = g(x)h(x)$ with $g, h \in A[x]$ and $\deg(g), \deg(h) \geq 1$.*

Proof. Suppose f has a factorization. Then, $\phi(f) = \phi(g)\phi(h)$. Since $\deg(\phi(g)) \leq \deg(g)$ and $\deg(\phi(h)) \leq \deg(h)$, our hypothesis implies that equality holds on these inequalities. So, from the irreducibility in $L[x]$, g or h is an element in A, as desired. □

Example 2.3.6. *In the reduction criterion, if A is factorial, then $f(x)$ is irreducible in $K[x]$.*

Proof. If f is reducible in $K[x]$, then $f = gh$ for some $g, h \in K[x]$, so $f = cont(gh)g_1h_1$ for some $g_1, h_1 \in A[x]$, which gives contradiction; since $f(x)$ is not product of polynomials in $A[x]$ of degree greater then 1. □

Note that factoriality is needed since this proof use the Gauss lemma.

Example 2.3.7. *In particular, let $A = \mathbb{Z}$, $B = \mathbb{Z}/p\mathbb{Z}$, $f \in \mathbb{Z}[x]$ is monic, and $\phi(f) = \overline{f(x)} \in \mathbb{Z}/p\mathbb{Z}[x]$ is irreducible. Then, $f(x)$ is irreducible in $\mathbb{Z}[x]$ by reduction criterion.*
For example, since $x^p - x - 1 \in \mathbb{Z}/p\mathbb{Z}[x]$ is irreducible (check that x^p and $-x - 1$ are distinct with respect to even and odd criterion), it is irreducible in $\mathbb{Z}[x]$ by the reduction criterion.

Proposition 2.3.8 (Integral root test)**.** *Suppose A, k as above. Let $f(x) = a_nx^n + \cdots + a_1x + a_0 \in A[x]$. If $\alpha \in k$ is a root of f, with $\alpha = \frac{b}{d}$, where $b, d \in A$ and g.c.d$(b, d) = 1$. Then, $b|a_0$, $d|a_n$. In particular, if $a_n = 1$, then $\alpha \in A$ and $\alpha|a_0$.*

Proof. See $d^n f(\frac{b}{d}) - a_0d^n = -a_0d^n$. □

Note that $k[x_1, \cdots, x_n]$ is not a principal ideal domain if $n \geq 2$. Algebraic geometry concerns on ideal on $k[x_1, \cdots, x_n]$ since it deals with surface, which can be represented as polynomial.

3 Algebraic Extensions

The Galois theory is important since it shows a connection between the (undergraduate) group theory and the field theory, which seems distinct at glance. Also, the theory deals with classical problem of solving higher degree polynomial. Maybe finding connection between two irrelevant field is still important now.

3.1 Finite and algebraic extensions

From now on, k, E, F, L, K denote "fields." Let E be an **extension of** F if $F \subset E$ is subfield. We denote it by below figure; and write it E/F. So E is F-module, which implies a vector space over F. Also denote E/F be finite when $\dim_F E < \infty$, and infinite otherwise.

$$\begin{array}{c} E \\ | \\ F \end{array}$$

Figure 6: Notation for field extension.

Definition 3.1.1. *$\alpha \in E$ be algebraic over F if $f(\alpha) = 0$ for some $f \in F[x] \setminus \{0\}$.*

Remark 3.1.2. *Let $\alpha \in E$ be algebraic $/F$. Then, $\phi_\alpha(f) = f(\alpha) \in E$ is ring homomorphism. Also, since $F[x]$ is a free commutative F-algebra and E is also F-algebra, it is F-algebra homomorphism. $\ker \phi_\alpha =< p(x) >$ since it is ideal and $F[x]$ is PID. So, $p(x)$ is irreducible, and is unique up to scalar multiplication, so take monic polynomial.*

Definition 3.1.3. *$irr(\alpha, F, x) = p(x)$*

If the context is clear, we can omit F in the left hand side.

Note 3.1.4. *$Im\phi_\alpha = \phi_\alpha(F[x]) =: F[\alpha] = \{f(\alpha) : f(x) \in F[x]\} \subset E$.*

Definition 3.1.5. *E/F is algebraic extension if $\forall \alpha \in E$, α is algebraic $/F$. In this case, denote $[E : F] = \dim_F E$*

Proposition 3.1.6 (Proposition 1.2 in [1] V. §1)**.** *For $k \subset F \subset E$, $[E : k] = [E : F][F : k]$*

Proof. Tedious; Let $\{x_i\}_{i\in I}$ be a basis for F over k, and $\{y_j\}_{j\in J}$ be a basis for E over F. Then, for any $z \in E$, $z = \sum_{j\in J} \alpha_j y_j = \sum_{j\in J}\sum_{i\in I} \beta i x_i y_j$ for some $\alpha_j \in F$ having representation, $\alpha_j = \sum_{i\in I} \beta_i x_i$ for some $\beta_i \in k$. Thus, $\{x_i y_j\}_{i\in I, j\in J}$ is a family of generator for E over k. Also, it is linearly independent, since $\sum_j \sum_i c_{ij} x_i y_j = \sum_j (\sum_i c_{ij} x_i) y_j = 0 \implies \forall j, \sum_i c_{ij} x_i = 0$ since $\{y_j\}_{j\in J}$ is basis, which implies $\forall i, \forall j, c_{ij} = 0$ since $\{x_i\}_{i\in I}$ is basis. Hence $\{x_i y_j\}_{(i,j)\in I\times J}$ is basis of E over k. □

Corollary 3.1.7 (Corollary 1.3 in [1] V. §1)**.** *E/k is finite extension $\iff$ E/F, F/k are finite extension.*

Remark 3.1.8. *For $\alpha \in E$, $k(\alpha) = \{\frac{f(\alpha)}{g(\alpha)} : f(x), g(x) \in k[x], g(\alpha) \neq 0\} \subset E$ is the smallest subfield including k and α.*

Proposition 3.1.9 (Proposition 1.4 in [1] V. §1)**.** *Let α be algebraic over k. Then, $k[\alpha] = k(\alpha)$, and $[k(\alpha) : k] = \deg irr(\alpha, k, x)$.*

Proof. For the first part, note that $k[\alpha] \cong k[x]/ < p(x) >$ where $p(x) = irr(\alpha, k, x)$, since for all $f(x) \in k[x]$, $f(\alpha) = q(\alpha)p(\alpha) + r(\alpha) = r(\alpha)$ for some unique $q, r \in k[x]$ by euclid algorithm. Also, $< p(x) >$ is maximal ideal, since for any $g \in k[x] \backslash < p(x) >$, $p \not| g$, this implies p, g are relatively prime, so $\exists a, b \in k[x]$ such that $ap + bg = 1$, which implies $< p, g >= k[x]$. Hence $k[\alpha]$ is a field, and $k[\alpha] \subset k(\alpha)$ by definition. Therefore, from the definition that $k(\alpha)$ is the smallest subfield containing k and α, $k[\alpha] = k(\alpha)$.
For the second part, suppose $\deg(p(x)) = d$. Then, it suffices to show that $\{1, \alpha, \alpha^2, \cdots, \alpha^{d-1}\}$ forms a k-basis. Firstly, they span $k(\alpha)$, since any α^n with $n > d$ can be replaced by $x^d = -irr(\alpha, k, x) + x^d$. Also, it is linearly independent, if not, we have another irreducible polynomial having α as root, and degree is lower than $irr(\alpha, k, x)$, contradiction. Hence$[k(\alpha) : k] = \deg(irr(\alpha, k, x))$. □

Definition 3.1.10. *Let L be a filed containing E, F as subfield. Then, denote EF be the smallest subfield of L including E and F, called compositum of E and F in L. One can define the compositum of a family of subfield E_i, $i \in I$. So,*

$$EF = \left\{ \frac{\sum_{finite} a_i b_i}{\sum_{finite} a_j b_j} : a_i, a_j \in E, b_i, b_j \in F, \sum_{finite} a_j b_j \neq 0 \right\},$$

and

$$\prod_{i \in I} E = \left\{ \frac{\sum_{finite} \prod_{i \in I} a_i}{\sum_{finite} \prod_{j \in I} a_j} : a_i, a_j \in E_i, \sum_{finite} \prod_{j \in I} a_j \neq 0 \right\}.$$

Remark 3.1.11 (Remark and definition)**.**

- *Let $k \subset E$, $\alpha_1, \cdots, \alpha_n \in E$, then $k(\alpha_1, \cdots, \alpha_n)$ is the smallest subfield of E including α_i's and k, which means that*

$$k(\alpha_1, \cdots, \alpha_n) = \left\{ \frac{f(\alpha_1, \cdots, \alpha_n)}{g(\alpha_1, \cdots, \alpha_n} \right\} = k(\alpha_1) \cdots k(\alpha_n).$$

- *If $E = k(\alpha_1, \cdots, \alpha_n)$, then E is called "finitely generated over k." Similarly, let $S = \{\alpha_1, \cdots, \alpha_n\} \subset E$ be finite set. Then, $k(S) := k(\alpha_1, \cdots, \alpha_n)$. Extending this definition, for $S \subset E$ arbitrary subset, define $k(S) = \cup_{S' \subset S S' \text{ is finite}} k(S')$, the smallest subfield containing k, S, and is called "subfield generated by S over k." This is, namely, compositum of $\{k(S') : S' \subset S \text{ finite }\}$. For example, $EF = \cup_{S \subset E S is finite} F(S)$.*
- *Think about such subfield; If $E = k(\alpha_1, \cdots, \alpha_n)$,*

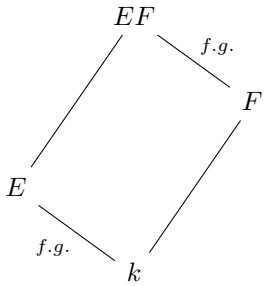


Figure 7: Extension of E, F, EF over k; "f.g." means "finitely generated."

$$\text{then, } EF = FE := F(k(\alpha_1, \cdots, \alpha_n)) = F(\alpha_1, \cdots, \alpha_n).$$

Proposition 3.1.12 (Proposition 1.5 in [1]V. §1)**.** *E/k : finite $\implies$ E/k : f.g.*

Proof. Let $\{\alpha_1, \cdots, \alpha_n\}$ be a k-basis of E. Then, $k(\alpha_1, \cdots, \alpha_n) = E$, implies finitely generated. □

Example 3.1.13. *Let x be indeterminate. Then, $k(x)/k$ is finitely generated extension but have infinite dimension.*

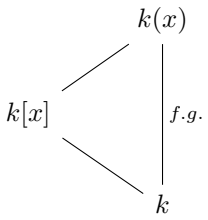


Figure 8: Example of finitely generated extension having infinite dimension.

Remark 3.1.14 (Miscellaneous notation)**.** *We define a **tower** of fields to be a sequence $F_1 \subset F_2 \subset \cdots \subset F_n$ of extension fields. The tower is called **finite** if and only if each step is finite. Think about figure 7. In this case, EF/F is called the **translation** of E to F, or the **lifting** of E to F.*

Proposition 3.1.15 (Proposition 1.6 in [1] V §1)**.** *$E = k(\alpha_1 \cdots, \alpha_n)$ f.g. over k, where α_i :alg. $/k$. $\implies$ E/k :finite.*

Proof.

$$k \subset k(\alpha_1) \subset \underset{\substack{\| \\ k(\alpha_1,\alpha_2)}}{k(\alpha_1)(\alpha_2)} \subset \cdots \subset \underset{\substack{\| \\ E}}{k(\alpha_1, \cdots, \alpha_n)}$$

Then, $k(\alpha_1, \cdots, \alpha_i)/k(\alpha_1, \cdots, \alpha_{i+1})$ is finite for all $i = 1, 2, \cdots, n-1$. Hence E/k is finite, algebraic over k by corollary 1.3. □

Definition 3.1.16 (Distinguished Class)**.** *Let $\mathscr{C}$ be a class of extensions $F \subset E$. Then $\mathscr{C}$ is called "**distinguished**" if following conditions hold.*

1. *E/F, $F/k \in \mathscr{C} \iff E/k \in \mathscr{C}$.*
2. *$E/k \in \mathscr{C}$ with the following figure. Then $EF/F \in \mathscr{C}$.*

Note that third condition suggested in [1] is automatically holds when 1,2 condition hold. Third condition is this; if $F/k, E/k \in \mathscr{C}$, and F, E are subfield of a common field, then $k \subset EF \in \mathscr{C}$. It is deduced by following argument; From 2, $EF/F \in \mathscr{C}$, and think tower $EF/F/k$.

Proposition 3.1.17 (Proposition 1.7 in [1] V §1)**.** *The class of algebraic extensions and the class of finite extensions are distinguished.*

Proof. In case of finite extension, condition 1 is done by the proposition 1.2. on [1]. For condition 2, since $E = k(\alpha_1, \cdots, \alpha_n)/k$ are finite, $F(\alpha_1, \cdots, \alpha_n) = EF/F$ is also finite; this is due to the fact that $\deg(irr(\alpha_i, F, x)) \leq \deg(irr(\alpha_i, k, x))$ for all i.
In case of algebraic extension, suppose E/k algebraic. Then, E/F, F/k is algebraic since $\forall \alpha \in$

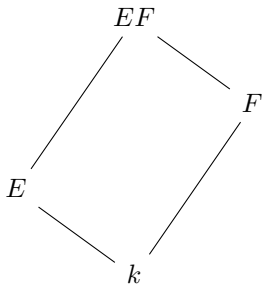


Figure 9: Condition 2 of distinguished class

$E, irr(\alpha, k, x) \in k[x] \subset F[x]$ and $\forall \alpha \in F \implies \alpha \in E$. Suppose $E/F, F/k$ are algebraic. Then, $\forall \alpha \in E$, $a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0$ for some $a_0, \cdots, a_n \in F$. (Note that not all a_i are zero.) Then, let $k_0 = k(a_0, \cdots, a_n)$ and it is algebraic over k_0. Then,

$$k_0(\alpha) \supset k_0 \supset k(a_0, \cdots, a_{n-1} \supset \cdots \supset k(a_0) \supset k$$

is tower of algebraic simple extension, which implies finite extension. Hence, from distinguishness of finite extension, $k_0(\alpha)/k$ is finite, So α is algebraic over k by the proposition 1.6. Now, suppose E/k is algebraic extension. Then, $EF = \cup_{S \subset E \text{finite}} F(S)$. And since $F(S)/F$ is finite because each element in S is algebraic in F so $F(S)$ is tower of simple algebraic extension. So $F(S)/F$ is algebraic by proposition 1.6, hence EF/F is algebraic. □

Remark 3.1.18. *For any set S, $K(S) = \cup_{S' \subset S S' \text{ is finite}} K(S')$. If $S \subset E$, where E is algebraic extension over K, then $K(S)$ is also algebraic extension.*

3.2 Algebraic Closure

Definition 3.2.1. *Let $E/F, L$ be fields, and let $\sigma : E \to L$ is called **embedding** of F, into L, if it is an injective homomorphism. Let $\tau : E \to L$ is embedding. Then,*

- *τ is **over** σ, or τ **extends** σ if $\tau|_F = \sigma$.*
- *τ is called embedding of E **over** F if σ is identity, i.e., $\tau|_F = id_F$.*

Note 3.2.2. *If x is transcendental, we can take $\sigma : x \mapsto x^2$ to show that there exists embedding which fix k but cannot fix polynomial.*

$$\begin{array}{ccc} k(x) & \xrightarrow{\sigma: x \mapsto x^2} & k(x) \\ \uparrow & & \uparrow \\ k & \xrightarrow{\cong} & k \end{array}$$

Figure 10: Example of embedding fix k but cannot fix its polynomial

Lemma 3.2.3 (Lemma 2.1 in [1] V. §2)**.** *E/k algebraic extension. $\sigma : E \to E$ is embedding $/k$. Then, $\sigma(E) = E$.*

Proof. It suffices to show σ is surjective. Let $\alpha \in E$, $p(x) = irr(\alpha, x, k)$. Then, let $E' = k(\alpha_1, \cdots, \alpha_n)$ where $\alpha_1, \cdots, \alpha_n$ are the set of roots of $p(x)$ in E. Then,

$$\sigma(E') = k(\sigma\alpha_1, \cdots, \sigma\alpha_n).$$

So, for any $i \in [n]$, $\sigma\alpha_i$ is also a root of $p(x)$, since $\sigma(p(\alpha_i)) = p(\sigma\alpha_i) = 0$. Hence, $\sigma(E') = E'$, which implies $\alpha in \sigma(E') \subseteq \sigma(E)$. □

Lemma 3.2.4 (Lemma 2.2 in [1] V. §2)**.** *Let $k \subset E_1, E_2 \subset E$ field, and $\sigma : E \to L$ is embedding of E in some field L. Then, $\sigma(E_1E_2) = \sigma(E_1)\sigma(E_2)$.*

Proof.

$$\sigma\left(\frac{\sum_{\text{finite}} a_ib_i}{\sum_{\text{finite}} a'_jb'_j}\right) = \frac{\sum_{\text{finite}} \sigma(a_i)\sigma(b_i)}{\sum_{\text{finite}} \sigma(a'_j)\sigma(b'_j)}$$

□

Remark 3.2.5. *The Lemma 2.2 holds for the composition of arbitrary family of subfield E_is of E.*

Proposition 3.2.6 (Proposition 2.3 in [1] V. §2)**.** *Let $f(x) \in k[x]$. If $\deg f \geq 1$, then $\exists E/k$ such that $f(x)$ has a root in E.*

Proof. Assume that $f(x) = \sum_{i\geq 0} a_ix^i$ is irreducible. Consider a canonica homomorphism $\sigma : k[x] \to k[x]/ < f(x) >$. Then σ induces homomorphism on k, and it has trivial kernel, since every nonzero element of k is invertible in k, generated the unit ideal, and $1 \notin \ker\sigma$. Hence $\sigma|_k k \to k[x]/ < f(x) >$ is an embedding.
Put $\xi = \sigma(x)$. Then, $f^\sigma := \sum_{i\geq 0} \sigma(a_i)x^i \in \sigma(k)[x]$, so

$$f^\sigma(\xi) = f^\sigma(\sigma(x)) = \sigma(f(x)) = 0.$$

Put $F = k[x]/ < f(x) >$. Let S be a set such that $|S| = |F - \sigma(k)|$ and $S \cap k = \emptyset$. Now define $E := k \cup S$. We want to extend σ as bijection, to make field structure on E. First of all, extend $\sigma|_k$ to E, say $\tilde{\sigma} : E \to F$, bijection. Then, give field structure as below; For $x, y \in E$,

- $x + y := \tilde{\sigma}^{-1}(\tilde{\sigma}(x) + \tilde{\sigma}(y))$
- $xy := \tilde{\sigma}^{-1}(\tilde{\sigma}(x) \cdot \tilde{\sigma}(y))$.

Therefore, E is an extension of k since it is a field containing k. Now let $\alpha := \tilde{\sigma}^{-1}(\xi)$, then α is a root of $f(x)$, done. □

Definition 3.2.7. *A field K is called "algebraically closed" if (1) $\forall f(x) \in K[x]$ has a root in K.*

Equivalently, if (2)$\forall f(x) \in K[x]$ splits into linear factors in $K[x]$, or (3) no proper algebraic extensions of K exists, then K is also said algebraically closed.

Proof. (2) $\implies$ (3) is easy; there are no irreducible polynomial having degree at least 2, since all polynomials splits into linear factors.
(3) $\implies$ (1): Suppose there are no proper algebraic extension of K, and take $f(x) \in K[x]$, irreducible. If at least one of root is not in K, then f should have degree at least 2, so we can extend K using f, say M. Then $[M : K] > 1$, which implies there is a proper algebraic extension over K, contradiction.
(1) $\implies$ (2): For any $f(x) \in K[x]$ with $\deg f = n \in \mathbb{N}$, it has root, say $u_1 \in K$, so $f = (x - u_1)g$ for some $g \in K[x]$. By repeating this, f splits into linear factors in $K[x]$. □

Theorem 3.2.8 (Theorem 2.5 in [1] V. §2)**.** *Let k be a field. Then, $\exists$ an extension of k, which is algebraically closed.*

Corollary 3.2.9 (Corollary 2.6 in [1] V. §2)**.** *Let k be a field. Then $\exists k^a$ which is algebraically closed and algebraic over k.*

Proof of the corollary. Let $k \subset E$, algebraically closed. Put $k^a := \cup_{K \subset F \subset E} F$, where F/k is algebraic. Then, k^a is also algebraic over k. Now it suffices to show that k^a is algebraically closed field. I will show that there are no proper algebraic extension over k^a. Suppose $\alpha \in E$ which is algebraic over k^a. Then, by distinguishness of algebraic extension, with the fact that $k^a(\alpha)/k^a, k^a/k$ are algebraic, so α is algebraic over k. Hence, $k(\alpha) \subset E$ is also algebraic extension over k, so $k(\alpha) \subset k^a$, implying $\alpha \in k^a$. Hence k^a is an algebraic closed. (Picking in E contain all possible algebraic elements in k since all polynomials in $k[x]$ is also in $E[x]$, and E contain every solution of its polynomial, which means every possible algebraic elements of k.) □

Proof of the theorem. 1. **Construct an extension in which every polynomial in $k[x]$ of degree ≥ 1 has a root.** For each $f \in k[x]$ of degree ≥ 1, assigns a letter X_f and let S be a set of such letter. So, S has bijection with the set of polynomial having degree ≥ 1. Now construct $k[S]$, a polynomial ring.

Lemma 3.2.10. *For any such f in $k[x]$, an ideal generated by all the polynomials $f(X_f) \in k[S]$ is not the unit ideal*

Proof. Suppose not. Then, $\exists$ a finite linear combination of elements in the ieal such that

$$g_1 f_1(X_{f_1}) + \cdots + g_n f_n(X_{f_n}) = 1$$

for some $g_i \in k[S], f_i \in k[x]$ having degree ≥ 1, $i \in [n]$. Now let $X_i := X_{f_i}$ for all $i \in [n]$. Then, for all g_i, only finitely many indeterminate are involved in all g_is. Say $X_1, \cdots X_N$ be such indeterminates. Then,

$$\sum_{i=1}^{n} g_i(X_1, \cdots, X_N) f_i(X_i) = 1.$$

Let F be a finite extension, having roots of each polynomial $f_1, \cdots, f_n$, say α_i is a root of f_i in F, for $i \in [n]$. Let $\alpha_i = 0$ for $i > n$. Then, by substituting X_i to α_i, we get $0 = 1$, a contradiction. □

So, we can construct the maximal ideal m containing all such $f(X_f)$ above. Then, $k[S]/m$ is a field, and we can get canonical projection $\sigma : k[S] \to k[S]/m$. For any $f \in k[x]$ havind degree ≥ 1, f^σ has a root in $k[S]/m$ by $\sigma(X_f)$. Also, $k[S]/m$ is an extension of σk. By constructing a set T having cardinals with $|k[S]/m - \sigma k|$ and $T \cap k = \emptyset$, and gives operations to make fields, like the proof of proposition 2.3. Then, we can get $E_1 = T \cup k$ be a field containing k and every polynomials of $k[x]$ having degree ≥ 1 has a root in E_1.

2. **Use mathematical induction.** Inductively, we can form a sequence

$$E_1 \subset E_2 \subset \cdots \subset E_n \subset \cdots .$$

such that every polynomials in $E_n[x]$ of degree ≥ 1 has a root in E_{n+1}. Let $E = \cup_{n=1}^{\infty} E_n$.

Lemma 3.2.11. *E is a field.*

Proof. For any $x, y \in E$, there exists $n \in \mathbb{N}$ such that $x, y \in E_n$, so we can use its field structure to define $x + y, xy$. □

Now, take $f \in E[x]$. Then $\exists E_n$ such that every coefficients of f lies on, so f has a root in $E_{n+1} \subset E$, hence f has a root in E. So E is algebraically closed, containing k.

□

Proposition 3.2.12. *Let $\sigma : k \to k^a$, embedding over k. Let $E = k(\alpha)$ for some algebraic element α, and $p(x) = irr(\alpha, k)$. Then # of extensions of σ to E = # of distinct roots of $p(x)$ in k^a.*

Proof. Let $X = \{$ extensions of σ to $E\}, Y = \{$ the roots of $p(x)$ in $k^a\}$. It suffices to show that $|X| = |Y|$. Let $\tau \in X$, so $p(\tau(\alpha)) = \tau(p(\alpha)) = 0 \implies \tau(\alpha) \in Y$. And τ is completely determined by $\tau(\alpha)$, i.e., if $\tau' \in X$ such that $\tau'(\alpha) = \tau(\alpha)$, then $\tau = \tau'$, since every elements in E can be represented by linear combination of power of α^n, $n \in \mathbb{N} \cup \{0\}$.
Conversely, given $\beta \in Y$, let $\tau = \phi_\beta \circ \phi_\alpha^{-1}$ where ϕ_β evaluates $\bar{f} \in k[x]/ < p(x) >$ to $f(\beta)$. This is isomorphism, as shown in [1][p.224]. So, $\tau|_k = id_k$. Hence $\tau \in X$.

$$k(\alpha) \xleftarrow{\cong} k[x]/ < p(x) > \xrightarrow{\cong} k(\beta)$$

$$f(\alpha) \xleftarrow{\phi_\alpha} \overline{f(x)} \xrightarrow{\phi_\beta} f(\beta)$$

Therefore, there exists bijection $X \to Y$ as $\tau \mapsto \tau(\alpha)$. This is bijection since by fixing α, all $\tau \in X$ have a form $\tau_\beta = \phi_\beta \circ \phi_\alpha^{-1}$ so that $\tau_\beta(\alpha) = \beta$ for any $\beta \in Y$, which implies $|X| = |Y|$. □

Remark 3.2.13. *We can extend this argument on arbitrary finitely generated extension.*

Proof. Let K/k be finitely generated algebraic extension. Then we can get a tower of algebraic simple extension, and apply the proposition 2.7 on each extensions, and sum all of it. □

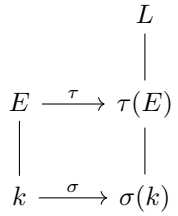
Theorem 3.2.14 (Theorem 2.8 in [1] V. §2)**.** *Let E/k be algebraic extension, $\sigma : k \to L$ be embedding of k, where L is algebraically closed field. Then, 1) $\exists \tau : E \to L$ which is extension of σ. 2)If E is algebraically closed, and $L/\sigma k$ is algebraic, then τ is isomorphism.*

Proof. 1. For 1) we use standard zorn's lemma argument. Let $S = \{(F, \tau) : E/F/k, \tau :$ extension of σ to an embedding of $F \in L\}$. Give an order $(F, \tau) \leq (F', \tau')$ if $F \subset F', \tau'|_F = \tau$. Then, $(k, \sigma) \in S$, so $S \neq \emptyset$. Then, for some totally ordered set $\{(F_i, \tau_i)\}$, define $F = \cup F_i$, $\tau(x) = \tau_i(x)$ for some $x \in F_i \subset F$. Then, $(F, \tau) \in S$, so it is upper bound for the totally ordered set. So, by Zorn's lemma, $\exists (K, \lambda)$ which is maximal. Then, $\lambda|_k = \sigma$. Now it suffices to show that $K = E$. Otherwise, $\exists \alpha \in E$ such that $\alpha \notin K$. Then, $(K(\alpha), \lambda(\alpha) \geq (K, \lambda)$, contradicting maximality of (K, λ). So there exists extension of σ, say $\tau : E \to L$.

2. For 2), see the picture. Then $\tau(E)$ is also algebraic closed; otherwise, $\exists$ irreducible polynomial in $\tau(E)[x]$ of degree ≥ 1. This polynomial is irreducible in $E(x)$, otherwise it is reducible, so contradiction. However, $L/\sigma k$ is algebraic $\implies L/\tau(E)$ is algebraic by distinguishness of algebraic extension, so $L = \tau(E)$ since algebraic closed field have no proper extension. Hence τ is isomorphism.

□

Remark 3.2.15. *Any algebraic extension of k which is algebraic closed is unique up to isomorphism. We call it "the algebraic closure" of k. This is what corollary 2.9 in [1] V. §2 says.*



Remark 3.2.16. *Lang's comment; in category theoretical aspect, $Aut(A)$ operates $Iso(A, B)$.*

Exercise 3.2.17. *If k is a field which is not finite, then any algebraic extension of k has the same cardinality.*

Proof. Note that $k[x]$ has infinite basis, say $\{1, x, x^2, \cdots\}$. So, $|k[x]| = |\cup_{n\in\mathbb{N}} k^n|$. However, for any n, $|k^n| = |k|$, furthermore, $|\cup_{n\in\mathbb{N}} k^n| = |k$ by invoking axiom of choice twice. Now, for any extension of E/k

$$\sigma : E \to k[x] \text{ by } \alpha \mapsto irr(\alpha, k, x).$$

Since $\sigma(k) = \{x - a : a \in k\}$, so $|\sigma(E)| \geq |\sigma(k)| = |k|$. Also, $|\sigma(E)| \leq |k[x]| = |k|$. So, $|\sigma(E)| = |k|$. Since fibers of σ, i.e., for any $f(x) \in \sigma(E)$, $\infty > |\sigma^{-1}(f)| > 0$, which implies $|E| = |\sigma(E)| = |k|$. □

3.3 Splitting fields and normal extension

Definition 3.3.1. *Let $f(x) \in k[x]$ of degree ≥ 1. Then, K/k is called **splitting field** of $f(x)$ if 1) $f(x)$ splits into linear factors in $k[x]$ (i.e., $f(x) = c(x - \alpha_1)\cdots(x - \alpha_n)$ with $c \in k$) and 2) $K = k(\alpha_1, \cdots, \alpha_n)$.*

Theorem 3.3.2 (Theorem 3.1 in [1] V. §3)**.** *Let K, E be splitting field of $f(x)$. Then,*

1. *$\exists\sigma : E \to K$ is isomorphism such that $\sigma|_k = id_k$.*
2. *If $k \subset K \subset k^a$, then for all $\sigma : E \to k^a$, which is embeding over E, $\sigma(E) = K$.*

Proof. 1. Take algebraic closure containing K, and use the result below;

2. By theorem 2.8 1), $\exists\sigma : E \to L$, which is embedding over k. Then, let $f(x) = c(x - \beta_1)\cdots(x - \beta_n)$ for some $\beta_i \in E$. Then, $f^\sigma(x) = c(x - \sigma\beta_1)\cdots(x - \sigma\beta_n)$. Since $f(x)$ has a unique factorization $f(x) = c(x - \alpha_1)\cdots(x - \alpha_n) \in k^a[x]$, $\{\sigma\beta_i\}_{i=1}^n = \{\alpha_i\}_{i=1}^n$, so they differ up to permutation. So $\{\sigma\beta_i\}_{i=1}^n \subset K$, which implies $\sigma(E) \subset K$. However, $K = k(\alpha_1, \cdots, \alpha_n) = k(\sigma\beta_1, \cdots, \sigma\beta_n) = \sigma(k(\beta_1, \cdots, \beta_n)) = \sigma(E)$. Hence σ is isomorphism, since it is both injective and surjective.

□

Remark 3.3.3. *For K/k algebraic, we may assume $K^a = k^a$ since $\exists\tau : K \to k^a$ by theorem 3.1, such that $\tau(K) \cong K$, so we can assume $k^a/K/k$.*

Remark 3.3.4. *$S = \{f_i(x) : i \in I\} \subset k[x]$, one can define a splitting field of S in the same way. $\forall i \in I$, k_i is a splittinf field of f_i. Then, $K = K(\cup_i S_i)$, the compositum of $K_i's$.*

Corollary 3.3.5. *Let K, E the splitting field of $\{f_i\}_{i\in I}$. Then $\exists\sigma : E \to K$ is isomorphism with $\sigma|_k = id_k$.*

Proof. By theorem 2.8, $\exists\sigma : E \to K$ is embedding $/k$. Then, E is compositum of E_is, and K is compositum of K_is. So, define $\sigma_i = \sigma|_{E_i}$, then, by the same argument in proof of theorem 3.1, σ_i induces isomorphism as $\sigma_i(E_i) = K_i$, so $\sigma(E) = \sigma(\prod_{i\in I} E_i) = \prod_{i\in I}\sigma(E_i) = K$, where the third equality is from lemma 2.2. Hence σ induces isomorphism, since it is already injective homomorphism. □

Remark 3.3.6. *In general, $\sigma(E) \neq E$, even if isomorphism. But it is equal when E is a splitting field.*

Example 3.3.7 (General Case)**.** *Let $f(x) = x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2}w)(x - \sqrt[3]{2}w^2)$ where $w = \frac{-1+\sqrt{-3}}{2}$. Then,*

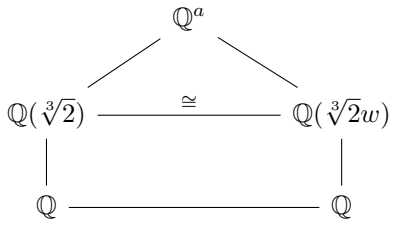


Figure 11: Extension of $f(x) = x^3 - 2$.

So $\sigma(\mathbb{Q}(\sqrt[3]{2})) \neq \mathbb{Q}(\sqrt[3]{2})$.

Theorem 3.3.8. *Let $k \subset K \subset k^a$. The following are equivalent.*

1. *$\forall\sigma : K \to k^a$, embedding $/k$, $\sigma(K) = K$.*
2. *K is the splitting field of some $\{f_i : i \in I\}$.*
3. *Let $f(x) \in k[x]$ such that f is irreducible and having a root in K. Then, f splits into linear factors in K.*

Proof. 1. 1. $\implies$ 3. : Given $\alpha, \beta \in K$, which are roots of $irr(\alpha, k, x)$, there exists isomorphism $k(\alpha) \cong k(\beta)$ by mapping α on β. (This is isomorphism since it preserves k, and clearly injective and surjective, and has inverse, and it is homomorphism.) Now extend this isomorphism to an embedding of K into k^a. This extension is from below; apply theorem 2.8 on the $K/k(\alpha)$ and $\sigma : k(\alpha) \to k(\beta) \subset k^a$. Then by condition 1., $\tau(K) = K$. So $\beta \in K$.

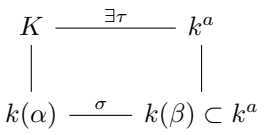


Figure 12: How to get extension of τ.

Since β was arbitrary, K have all root of f, so f splits into linear factors on K.

2. 1. $\implies$ 2. : Let $X = irr(\alpha, x, k) : \alpha \in K\}$, and $\tilde{K}$ is a splitting field of X. Then it suffices to show that $K = \tilde{K}$. By the above argument, for any $\alpha \in K$, every conjugate of α is in K, which condition 3. says. Hence $\tilde{K} \subset K$, which implies $K = \tilde{K}$.

3. 2. $\implies$ 1. : Let $X = \{f_i\}_{i \in I}$ is a family of polynomials in $k[x]$ such that K is splitting field of X. Then, if $\alpha \in K$ is root of some f_i, then $\forall \sigma : K \to k^a$ embedding over k, we know $\sigma(\alpha)$ is also root of f_i, so $\sigma(\alpha) \in K$. Since K is generated by all such roots, σ maps K to itself. Hence, $\sigma(K) = K$.

4. 3. $\implies$ 1. : Let $\sigma : K \to k^a$ embedding over k. Then, for all $\alpha \in K, \sigma(\alpha)$ is also root of $irr(\alpha, x, k)$, which implies $\sigma(\alpha) \in K$ since $irr(\alpha, x, K)$ splits into linear factors in K, which implies K has all roots. Hence $\sigma(K) \subset K$, which implies $\sigma(K) = K$ by the lemma 2.1, saying that every embedding of field into itself is automorphism.

□

Definition 3.3.9 (Normal Extension)**.** *K/k is called **normal** extension, if it satisfies one of the conditions in theorem 3.3.*

Theorem 3.3.10 (Theorem 3.4 in [1] V. §3)**.** *Below two figures, 13 and 14, hold.*

(a) K/k normal $\implies$ KF/F normal. (b) K/k normal $\implies$ K/E normal.

Figure 13: Lifting (Top) and Above subextension (Bottom) are normal.

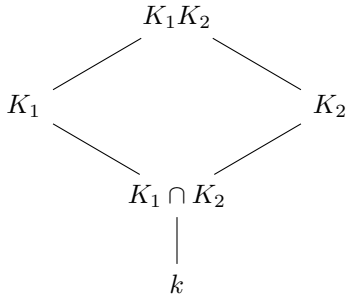


Figure 14: Composition and intersection are normal

Proof. 1. Assume $K \subset F^a$. Then, $KF \subset F^a$. So by theorem 2.8, $\exists \sigma : KF \to F^a$ embedding over F. which is extension of id_F. Then $\sigma|_k = k$, so

$$\sigma(KF) = \sigma(K)\sigma(F) = KF.$$

where first equality comes from the lemma 2.1 and the second equality comes from condition 1 of normal extension, and $\sigma|_F = id_F$. Hence KF/F is normal.

2. Suppose K/k is normal and take σ be embedding of K into k^a over E. Then, it is also embedding of K into k^a over k, so it is automorphism, Hence K/E satisfy condition 1 of normal extension.

3. Take k^a which contain both K_1, K_2. (This construction is possible by constructing algebraic closure of K_1K_2.) Then, for any $\sigma : K_1K_2 \to k^a$, embedding over k, $\sigma|_{K_i} \to k^a$ is also embedding over k, so $\sigma(K_i) = K_i$ for $i \in [2]$, so $\sigma(K_1K_2) = \sigma(K_1)\sigma(K_2) = K_1K_2$ with the lemma 2.1. Also, $\sigma(K_1 \cap K_2) = \sigma(K_1) \cap \sigma(K_2) = K_1 \cap K_2$.

□

Remark 3.3.11. *Normal extension do not form a distinguished class.*

Example 3.3.12. *Note that $\mathbb{Q}(\sqrt[3]{2}, w)$ is normal extension of $\mathbb{Q}$. However, for $\mathbb{Q}(\sqrt[3]{2}, w)/\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal. Also, in $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, each subextension is normal but $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal; since $x^2 - \sqrt{2}$ is irreducible in $\mathbb{Q}(\sqrt{2})$ but it is not in $\mathbb{Q}[x]$.*

In general, if $[K : k] = 2$ then K/k is normal, which implies $K = k(\alpha)$ for some α such that $irr(\alpha, k) = (x - \alpha)(x - \beta)$ implies $\beta \in K$.

Proof. If $[K : k] = 2$, then it is finitely generated algebraic extension by proposition 1.5. Then $K = k(\alpha_1, \cdots, \alpha_n)$ for some $n \in N$, but $[k(\alpha_1) : k] > 1$ implies K is simple extension. Say $K = k(\alpha)$. Then, $irr(\alpha, k)$ has degree 2. Denote β be its conjugate, then $irr(\alpha, k) = (x-\alpha)(x-\beta) = x^2 - (\alpha+\beta)x + \alpha\beta$, so $\alpha + \beta \in k$ implies $(\alpha + \beta) - \alpha = \beta \in K$. □

3.4 Separable extension

Definition 3.4.1. *Let E/F algebraic, $\sigma : F \to L$ embedding into L, which is algebraically closed. Then, for any extension of σ to E, the image of E is algebraic over σF. Let $[E : F]_s$ be the cardinality of $\{\tau | \tau : E \to L\}$, the set of embeddings of E. It is called* ***separable degree*** *of E/F.*

First of all, we should check it is well-defined.

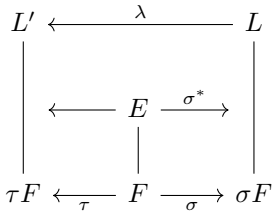


Figure 15: Separable extension

Proof. Let $S_\sigma = \{\phi : E \to L : \phi$ is extension of the embedding $\sigma : F \to L\}$, L' be another algebraic closed field, and $\tau : F \to L'$ be an embedding. Then, L' is algebraic closure of τF, so we can apply theorem 2.8 on $\tau \circ \sigma^{-1} : \sigma F \to \tau F \subset L'$ with L as algebraic extension of σF, so we can get $\lambda : L \to L'$. Since L is algebraically closed, λ is isomorphism. Let $S_\tau = \{\phi : E \to L' : \phi$ is extension of the embedding $\tau : F \to L'\}$.
Now it suffices to show that $|S_\sigma| = |S_\tau|$. Let $\sigma^* \in S_\sigma$. Then

$$\lambda \circ \sigma^*|_F = (\tau \circ \sigma^{-1}) \circ \sigma = \tau.$$

So λ induces mapping from S_σ to S_τ, and also λ^{-1} induces mapping vice versa. Hence there is bijection between S_σ and S_τ, so we are done. □

Theorem 3.4.2 (Theorem 4.1 in [1] V. §4)**.** *$E/F/k$ algebraic extension. Then 1) $[E:k]_s = [E:F]_s[F:k]_s$. Also, if E/k is finite, then $[E:k]_s \leq [E:k] < \infty$.*

Proof. Let $A = \{\sigma_i | \sigma_i : F \to L$ be extension of $\sigma : k \to L$ embedding of k into algebraically closed field L for $i \in I\}$. Then, $|A| = |I|$. Given $i \in I$, $\exists \sigma_{ij} : E \to k^a$, which is extension of σ_{ij} for some $j \in J$. The existence of σ_{ij} comes from the fact that $[E:F]_s$ is well-defined, so constructing set like A and take extensions. Then, $|J_i| = |J_{i'}|$ for all $i, i' \in I$ since each σ_i has precisely $[E:F]_s$ extensions of embedding of E into L, therefore, $\{\sigma_{ij}\}$ contain $[E:F]_s[F:k]_s$ extensions of embedding of F into L, since $\{\sigma_i\}$ has precisely $[F:k]_s$ elements, by definition of separable degree. (Think of S_{σ_i} and $S_{\sigma_{ij}}$ in the definition of separable degree.)
Then, since any embedding of E into L over σ must be one of the σ_{ij}, since its restriction on F is one of σ_i. So cardinality of the family of distinct embedding of E into L over σ is the same as $\{\sigma_{ij}\}_{(i,j)\in I\times J}$, done.
Now, suppose E/k is finite. Then, $E = k(\alpha_1, \cdots, \alpha_n)$ finitely generated algebraic extension, by the proposition 1.5., for some $\alpha_i \in L, i \in [n]$. Then make tower of simple algebraic extensions,

$$k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \cdots \subset k(\alpha_1, \cdots, \alpha_n) = E.$$

Then, $[k(\alpha_1, \cdots, \alpha_i) : k(\alpha_1, \cdots, \alpha_{i-1})]_s$ is number of distinct root of $irr(\alpha_i, k(\alpha_1, \cdots, \alpha_{i-1}))$, hence it is less than or equal to degree of $irr(\alpha_i, k(\alpha_1, \cdots, \alpha_{i-1})) = [k(\alpha_1, \cdots, \alpha_i) : k(\alpha_1, \cdots, \alpha_{i-1})]$.
Hence, by multiplicativity, we can say that $[E:k]_s \leq [E:k]$. □

Note that for some indeterminate t, let $E = k(t)/F = k(t^p)/k$. Then, let $t = \alpha$. So α is a root of $x^p - t^p = 0$, which is the same as $(x-t)^p = 0$, so t is transcendental over k but algebraic over t^p.

Corollary 3.4.3 (Cororally 4.2 in [1] V. §4)**.** *$[E:k]_s = [E:k]$ holds $\iff$ each step of the tower of simple algebraic extension is separable.*

Proof. Derived in the proof. □

Remark 3.4.4.
1. *For any finite extension E/k, denote E/k is **separable** if $[E:k]_s = [E:k]$.*
2. *Let α is algebraic over k. Then α is called **separable over** k if $k(\alpha)/k$ is separable.*
3. *Let $f(x) \in k[x]$. Then $f(x)$ is called **separable** if $f(x)$ has no multiple roots in k^a.*

Remark 3.4.5. *α is algebraic and separable $\iff$ $irr(\alpha, k)$ is separable $\iff$ all the roots of $irr(\alpha, k)$ are distinct.*

Proof. The second $\iff$ is just definition of separability of polynomial. Suppose α is separable over k. Then $k(\alpha)$ is separable, so $[k(\alpha):k]_s = [k(\alpha):k]$. Hence $k(\alpha)$ has $[k(\alpha):k]$ distinct embedding of $k(\alpha) \to k^a$ over k. If $irr(\alpha, k)$ doesn't have $[k(\alpha):k]$ distinct roots, then by principle of pigeon hole, there exists two maps which maps α to the same algebraic elements, which implies two maps are equal, contradiction. Hence $irr(\alpha, k)$ has $[k(\alpha):k]$ distinct roots, and since $[k(\alpha):k] = \deg(irr(\alpha, k))$, $irr(\alpha, k)$ has no multiple roots. Conversely, if all roots are distinct, we can make $[k(\alpha):k]$ embeddings which maps α to either other distinct root or itself. So $[k(\alpha):k] = [k(\alpha):k]_s$. □

Theorem 3.4.6 (Theorem 4.3 in [1] V. §4)**.** *E/k finite. Then E/k is separable $\iff$ $\forall \alpha \in E$, α is separable over k.*

Proof. Suppose E/k separable. Then

$$[E : k(\alpha)]_s[k(\alpha) : K]_s = [E : k]_s = [E : k] = [E : k(\alpha)][k(\alpha) : K].$$

Since $[E : k(\alpha)]_s \leq [E : k(\alpha)]$, $[k(\alpha) : K]_s \leq [k(\alpha) : K]$, this implies equality for each subinequality. Hence $[k(\alpha) : K]_s = [k(\alpha) : K]$, so α is separable.
Conversely, Let all elemetns in E is separable over k. Since E is finite extension, so it is finitely generated algebraic extension by the proposition 1.5. So $E = k(\alpha_1, \cdots, \alpha_n)$ for some $\alpha_1, \cdots \alpha_n \in E$. So we can get the tower of algebraic simple extensions,

$$k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \cdots \subset k(\alpha_1, \cdots, \alpha_n) = E.$$

Note that each α_i is separable over $k(\alpha_1, \cdots, \alpha_{i-1})$; since irreducible polynomial of α_i, $irr(\alpha_i, k(\alpha_1, \cdots, \alpha_{i-1}), x)$ can divide $irr(\alpha_i, k, x)$, and the latter have no multiple roots, so do the former. Hence $[k(\alpha_1, \cdots, \alpha_i) : k(\alpha_1, \cdots, \alpha_{i-1})]_s = [k(\alpha_1, \cdots, \alpha_i) : k(\alpha_1, \cdots, \alpha_{i-1})]$, so the conclusion can be derived. □

By this theorem, we have another definition of separability of E/k for infinite dimensional extension;

Definition 3.4.7. *For E/k algebraic with arbitrary dimension. Then E/k is separable iff $\forall \alpha \in E$, α is separable over k. This is equivalent to say that $[E : k]_s = [E : k]$, the original definition when dimension is finite.*

Theorem 3.4.8 (Theorem 4.4 in [1] V. §4)**.** *Let E/k algebraic. $E = k(S)$ for $S = \{\alpha_i\}_{i \in S}$. If $\forall i \in I, \alpha_i$ is separable over k, then E/k is separable.*

Proof. Note that $E = k(S) = \cup_{S' \subset S S' \text{ is finite}}$. Note that $k(S')/k$ is separable by the argument in the proof of theorem 4.3. (Make tower of simple algebraic extension, and each element is separable over middle extension, so that separable dimension is equal to general dimension.) Hence $k(S')/k$ is separable. So $\forall \alpha \in E$, $\exists S'$ which is finite, so that $\alpha \in k(S')$. So α is separable. □

Theorem 3.4.9 (Theorem 4.5 in [1] V. §4)**.** *Separable extensions form a distinguished class.*

Proof. 1. (Condition 1) Let $E/F/k$ and $E/F, F/k$ are separable. Then take arbitrary $\alpha \in E$, let $irr(\alpha, F) = a_0 + a_1 x + \cdots a_n x^n$. Now let $k_0 = k(a_0, \cdots, a_n)$. Then α is separable over k_0, since $irr(\alpha, k_0)$ is divisible by $irr(\alpha, F)$, which has no multiple roots by given condition, implying so does $irr(\alpha, k_0)$. And $k_0(\alpha)/k_0$ is finite and separable extension. Also, k_0/k is finite separable extension since k_0 is generated by separable elements in F over k. Hence

$$[k_0(\alpha) : k]_s = [k_0(\alpha) : k_0]_s[k_0 : k]_s = [k_0(\alpha) : k_0][k_0 : k] = [k_0(\alpha) : k],$$

by theorem 4.1 and proposition 1.1. Hence $k_0(\alpha)$ is separable over k. So by theorem 4.3 α is separable over k. Since α is arbitrary, E/k is separable.
Conversely, let E/k is separable. Then, F/k is also separable since every element in F is also in E, which implies they are separable over k. Now it suffices to show that E/F is separable. Let $\alpha \in E$. Then $irr(\alpha, F)$ can divides $irr(\alpha, k)$ but $irr(\alpha, k)$ have no multiple roots since E/k is separable. Hence $irr(\alpha, F)$ also have no multiple roots. Therefore α is separable over F.

2. (Condition 2) Let $E = \cup_{S \subset E, \text{finite}} k(S)$. Then $EF = F(\cup_{S \subset E, \text{finite}} k(S)) = \cup_{S \subset E, \text{finite}} F(S)$ since F contain k already. Since each S is separable over k, so it is separable over F by the same argument using divisibility of irreducible polynomial and its linear factors in algebraic closure.

□

Remark 3.4.10. *Let E/k be finite, $E \subset k^a$. Let $K = \cap_{E \subset K'} K'$ where K' is any normal extension over k containing E is normal extension over k, by theorem 3.4. This is the smallest normal extension of k containing E, by definition.*
Alternatively, let $\sigma' : K \to k^a$ be any embedding over k, and let σ be extension of σ' to K' for each K'. Then, since K' is normal, $\sigma(K') = K'$. Hence

$$\sigma(K) = \cap_{K' \supset E} \sigma(K') = \cap_{K' \supset E} K' = K$$

So we can check K is normal by this way.
Consider $A = \{\sigma_1, \cdots, \sigma_n : \sigma_i : E \to k^a$ is embedding over $k\}$. And let $K'' = \sigma_1 E \cdots \sigma_n E \subset k^a$. Then, we want to show that K''/k is normal. Let $\tau : K'' \to k^a$ be any embedding over k. Then, this can be extended as isomorphism $\tau : k^a \to k^a$ by theorem 2.8. Then, $\{\tau\sigma_1, \cdots \tau\sigma_n\} = \{\sigma_1, \cdots, \sigma_n\}$ since $\tau\sigma_i$ is also embedding of E into k^a over k, so it is in A, and each $\tau\sigma_i$ is distinct. Therefore, $\tau(K'') = \tau(\sigma_1 E \cdots \sigma_n E) = \tau\sigma_1 E \cdots \tau\sigma_n E = K''$.
Now note that $K \subset K''$ since K, K'' are normal but K is the smallest normal extension. Also, $K'' \subset K$ since $\forall i \in [n], \sigma_i E \subset K$ because $\sigma_i E \in K'$ for any normal extension of k containing E. Hence $K = K''$
This implies that the smallest normal extension of k containing E is equal to $\sigma_1 E \cdots \sigma_n E$.
In particular, if E/k is separable, then K/k is separable since each $\sigma_i E$ is separable over k since σ cannot change its irreducible polynomial, which implies all element has irreducible polynomial having no multiple roots. Hence by condition 2 of distinguishedness, $K = \sigma_1 E \cdots \sigma_n E$ is separable over k.

Theorem 3.4.11 (Primitive Element Theorem)**.** *E/k finite.*

1. *$E = k(\alpha)$ for some $\alpha \in E \iff \exists$ finitely many F such that $E/F/k$.*
2. *E/k separable. $\implies E = k(\alpha)$ for some $\alpha \in E$.*

Proof. 1. (1.,$\Leftarrow$) If k is finite field, then the multiplicative group of E, say $E^* =< \alpha >$ for some $\alpha \in E$, which implies $E = k(\alpha)$. Suppose k is infinite. Given $\alpha, \beta \in E$, consider $k(\alpha + c\beta)$ for some $c \in k$. Then the number of such form is infinite but they are all subfield of E containing k, so actual field must be finitely many. Hence,

$$k_0 = k(\alpha + c_1\beta) = k(\alpha + c_2\beta)$$

for some $c_1 \neq c_2$. This implies $(c_1 - c_2)\beta \in k_0$, which implies $\beta \in k_0$, so $\alpha in k_0$. Hence $k(\alpha, \beta) \subset k(\alpha + c\beta)$, this implies $k(\alpha, \beta) = k(\alpha + c\beta)$ since other inclusion is obvious. So, since E/k finite, $E = k(\alpha_1, \cdots, \alpha_n)$ for some α_i by the proposition 1.5, hence it suffices to show that $E = k(c_1\alpha_1 + \cdots c_n\alpha_n)$. If $n = 2$, then we done. Suppose $n > 3$. Then, $\exists k(c_2\alpha_2 + \cdots + c_n\alpha_n) = k(d_2\alpha_2 + \cdots + d_n\alpha_n)$ which contain all $\alpha_2, \cdots, \alpha_n$ by inductive hypothesis. This implies $k(\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n)$ contain α_1 by $\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n - (c_2\alpha_2 + \cdots + c_n\alpha_n) = \alpha_1 \in k(\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n)$. So $E = k(c_1\alpha_1 + \cdots + c_n\alpha_n)$, done.

2. (1.,$\Rightarrow$) Let $E = k(\alpha)$. Let $f(x) = irr(\alpha, k)$. Given $E/F/k$, consider $g_F(x) = irr(\alpha, F)$. Then f is divisible by g_F. Let $\{g_F(x) : E/F/k\}$. Then it is a finite set by thinking that all possible factorization in algebraic closure is finite. Now, let $F_0 = k(C)$ where C is the set of coefficients of $g_F(x)$. Then $F_0 \subset F$, and g_F is irreducible on F_0. So, $[F_0(\alpha) : F_0] = [F(\alpha) : F]$, but $F_0(\alpha) = k(C \cup \alpha) = k(\alpha)$ since $C \subset k(\alpha)$ and $F(\alpha) = k(\alpha)$ since $F \subset k(\alpha)$. So $F_0(\alpha) = F(\alpha)$, hence $F_0 = F$. Therefore, $\{F : E/F/k\}$ has a bijection with $\{g_F : E/F/k\}$. Since the latter is finite, so does the former.

3. (2.) Let E/k be finite and separable. Assume that k is infinite field. Given $\alpha, \beta \in E$, we claim that $k(\alpha, \beta) = k(\gamma)$ for some $\gamma \in E$, by assuming $E = k(\alpha, \beta)$. (If $E = k(\alpha_1, \cdots, \alpha_n)$ for some $n > 2$, We can apply this argument inductively, on the tower of simple algebraic extension;

$$\begin{aligned} k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \cdots &\subset E \\ k \subset k(\alpha') \subset k(\alpha', \alpha_3) \subset \cdots &\subset E \\ k \subset k(\alpha'') \subset k(\alpha'', \alpha_4) \subset \cdots &\subset E \\ &\cdots \\ k \subset k(\alpha^{[n]}) &\subset E = k(\alpha^{[n]}, \beta) \\ k \subset k(\gamma) &= E. \end{aligned}$$

Let $\sigma_1, \cdots, \sigma_n$ be distinct embeddings of $k(\alpha, \beta)$ in k^a over k. Let

$$p(x) = \prod_{i \neq j} (\sigma_i \alpha - \sigma_j \alpha + (\sigma_i \beta - \sigma_j \beta)x).$$

Then $p(x)$ is nonzero since each term $(\sigma_i \alpha - \sigma_j \alpha + (\sigma_i \beta - \sigma_j \beta)x) = (\sigma_i(\alpha - X\beta) - \sigma_j(\alpha - x\beta)) \neq 0$ if $\alpha - x\beta \neq 0$. Hence $\exists c \in k$ such that $p(C) \neq 0$. Then, $\sigma_i(\alpha + c\beta)$ are distinct for each $i \in [n]$, so

$$[k(\alpha, \beta) : k] \geq [k(\alpha + c\beta) : k] \geq n = [k(\alpha, \beta) : k]_s = [k(\alpha, \beta) : k].$$

This implies $k(\alpha, \beta) = k(\alpha + c\beta)$.

□

Remark 3.4.12. *If $E = k(\alpha)$ for separable extension E, then α is called **primitive element**.*

Remark 3.4.13. *An example of finite extension which is not simple is in [2][p.289] Exercise 15. Let F/k with $F = k(u, v)$, $char\, k = p \neq 0$, where $u^p, v^p \in k$ and $[F : k] = p^2$. Then F/k is not a simple extension of k, since it contains infinitely many intermediate fields. This is the same as exercise 24 in [1][p.255]*

Proof. Suppose it has only finitely many intermediate fields. Then, since $[F : k] < \infty$ means F/k is finite, we can use the primitive element theorem to conclude that $F = k(\alpha)$. Now take the frobenius map $\phi : F \to F$ by $x \mapsto \phi(x) = x^p$. Then $\phi(\alpha) = \alpha^p \in k(u^p, v^p)$ since α can be represented by linear combination of powers of u and v. However, $k(u^p, v^p) = k$, which implies $\alpha^p \in k$, so $x^p - \alpha^p \in k[x]$ is a polynomial having α as a root. However, $\deg(irr(\alpha, k)) = [F : k] = p^2$ by given condition, which contradicts the fact that $x^p - \alpha^p$ is also a polynomial in $k[x]$ having α as roots but its degree is p. □

Definition 3.4.14. *Let k^{sep} be the compositum of all separable extensions of a field k in a given algebraic closure k^a. This is a separable extension since $\forall \alpha \in k^{sep}$, α can be represetned by finite elements which are from distinct separable extensions, so $\alpha \in k_1 \cdots k_r$ where k_i/k is separable, for $i \in [r]$ some $r \in \mathbb{N}$. Then, $k_1 \cdots k_r(\alpha)/k_1 \cdots k_r/k$ is a tower with $k_1 \cdots k_r(\alpha)/k_1 \cdots k_r$ and $k_1 \cdots k_r/k$ are separable, so α is separable over k, by condition 1 of distinguishness. So*

$$k^{sep} = \{x : x \in k^a, x \text{ is separable over } k\}.$$

Actually the left inclusion is trivial since such x should be in k^{sep}. To show right inclusion holds, since $\forall x \in k^{sep}$ is separable over k as shown above, so k^{sep} is subset of the right hand side.

Remark 3.4.15. *And for E/k algebraic, $\sigma : E \to k^a$ embedding over k, then we call σE is **conjugate** of E in k^a. By above remark, the smallest normal extension of k containing E is the compositumm of all the conjugates of E in E^a. Also, for any α, algebraic, and $\{\sigma_i\}_{i\in[sep\deg\alpha]}$ are a set of distinct embedding of $k(\alpha) \to k^a$ over k. Then $\sigma_i\alpha$ is called the **conjugates** of α in k^a. The smallest normal extension of k containing one of these conjugates is simply $k(\{\sigma_i\alpha\}_{i\in[sep\deg\alpha]})$.*

Remark 3.4.16. *Let E/k finite, separable and noraml. Then, $[E:k] = [E:k]_s = |Aut(E/k)|$. where $Aut(E/k) = \{\phi|\phi : E \to E$ is isomorphism, $\phi|_k = id_k\}$. The third inequality comes from the fact that normal extension implies every embedding into algebraic closed field is automorphism.*

3.5 Finite Field

In this section we want to classify all finite fields. Let p be prime, and $\mathbb{Z}/p\mathbb{Z} := \mathbb{F}_p$. If E is any extension of $\mathbb{F}_p$, then $E \cong \mathbb{F}_p \oplus \cdots \oplus \mathbb{F}_p$ as abelian group. So $|E| = p^n$. However this is necessary condition of order of extension of $\mathbb{F}_p$. We don't know that there exists such field. If $f(x) \in \mathbb{F}_p[x]$ is irreducible with degree n, then take its root on $\mathbb{F}_p^a$, say α, and $\mathbb{F}_p(\alpha)$ is such fields. We want to generalize this.

Theorem 3.5.1 (Theorem 5.1 in [1] V. §5)**.** *Let p be prime, $n \geq 1$. Then*

1. *$\exists!$ finite field of order p^n in $\mathbb{F}_p^a$. So write it $\mathbb{F}_{p^n}$.*
2. *$\mathbb{F}_{p^n}$ = the splitting field of $x^{p^n} - x$ in $\mathbb{F}_p^a = \{\alpha : \alpha^{p^n} - \alpha = 0, \alpha \in \mathbb{F}_p^a\}$.*
3. *Every finite field is isomorphic to $\mathbb{F}_p^n$ for some $p, n \geq 1$.*

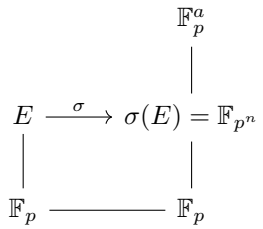
Proof. Let $S = \{\alpha : \alpha^{p^n} - \alpha = 0\}$, and let $f(x) = x^{p^n} - x$. Then $f'(x) = p^n x^{p^n-1} - 1 = -1 \neq 0$, so f has no multiple roots since $f(\alpha) = -1 \neq 0$ for any root α for f. Hence we know that $|S| = p^n$. Let E be the splitting field of $f(x)$ in $\mathbb{F}_p^a$.

Claim 3.5.2. *E=S.*

Proof. $S \subset E$ is clear since S is a set of roots of f, with the fact that splitting fields must contain all roots. Conversely, given $\alpha, \beta \in S$, $(\alpha \pm \beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n}$, and $(\alpha\beta)^{p^n} = \alpha^{p^n}(\beta)^{p^n}$. Also $0, 1 \in S$, and for any $0 \neq \beta \in S$, $(\beta^{-1})^{p^n} - \beta^{-1} = 0$, and $(-\beta)^{p^n} - (-\beta) = (-1)^{p^n}\beta^{p^n} + \beta = 0$ in any prime p. So S form a splitting field of f, which makes $E = S$. □

To show uniqueness, suppose E' be another finite field of order p^n in $\mathbb{F}_p^a$. Then $|(E')^*| = p^n - 1$, so $\forall\alpha \in (E')^*$, $\alpha^{p^n-1} = 1 \implies \alpha^{p^n} = \alpha$. Hence $E' \subset S$ and $|E'| = |S| \implies E' = S = E$.

To show third statement, let E be a finite field. Then $|E| = p^n$ for some $p, n \geq 1$. By theorem 2.8, there exists embedding into $\mathbb{F}_p^a$, say σ. Then, $\sigma(E)$ has order p^n in $\mathbb{F}_p^a$. From uniqueness of



a finite field of order p^n in $\mathbb{F}_p^a$, $\sigma(E) = \mathbb{F}_p^a$. Hence $E \cong \mathbb{F}_p$ □

Remark 3.5.3. $\mathbb{F}_{p^n}/\mathbb{F}_p$ *is simple, normal and separable.*

Proof. If $\alpha \in \mathbb{F}_{p^n}$ such that $<\alpha>=(\mathbb{F}_{p^n})^*$, $\mathbb{F}_p(\alpha)=\mathbb{F}_{p^n}$. Since $(\mathbb{F}_{p^n})^*$ is cyclic as shown in theorem 5.3, such element exists. Also, third statement of theorem 5.1 shows that $\mathbb{F}_{p^n}$ satisfy condition 1 of normal extension. And it is separable extension since every element is a root of irreducible polynomial, $f(x)=x^{p^n}-x$ which have no multiple roots. □

Theorem 3.5.4 (Theorem 5.3 in [1] V. §5)**.** *Let k be finite field. Then k^* is cyclic.*

Proof. Let $k=\mathbb{F}_{p^n}$, by theorem 5.1. Suppose (k^*) is not cyclic. Then,

$$k^* \cong \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_r}$$

for some $n \geq 2, q_i < p^n-1, \prod_{i\in[r]} q_i = p^n$ for some $i \in [r]$. This implies that

$$\forall \alpha \in k^*, \alpha^q = 1 \text{ where } q = l.c.m(q_1, \cdots, q_r) < p^n - 1$$

But this contradicts the fact that x^q-1 has only $q<p^n$ elements as roots. So (k^*) is cyclic. (If $q=p^n$, then q_is are mutually prime, then by chinese remainder theorem, it is cyclic.) □

Definition 3.5.5 (Frobenius map)**.** *Let $q=p^n$. Then define $\phi : \mathbb{F}_q \to \mathbb{F}_q$ by $\alpha \mapsto \alpha^p$. Call it the* ***Frobenius map****.*

Proposition 3.5.6. *ϕ is isomorphism.*

Proof. It is homomorphism by freshman's dream. The kernel of ϕ is 0, which implies injective. Since $\mathbb{F}_q$ is finite, injectivity implies surjectivity. □

Theorem 3.5.7 (Theorem 5.4 in [1] V. §5)**.** $Aut(\mathbb{F}_q) =< \phi >$.

Proof. Note that $|Aut(\mathbb{F}_q)| = n$ since $\mathbb{F}_q$ is separable and $[\mathbb{F}_q : \mathbb{F}_p] = n = [\mathbb{F}_q : \mathbb{F}_p]_s$. So it suffices to show that $|<\phi>| = n$ Note that $\phi^n(\alpha) = \alpha^{p^n} = \alpha$ so $\phi^n = id_{\mathbb{F}_q}$. If $\phi^m = id_{\mathbb{F}_q}$ for some $m < n$, then

$$\forall \alpha \in \mathbb{F}_{p^n}, \phi^m(\alpha) = \alpha^{p^m} = \alpha.$$

So $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$, which is impossible since $|\mathbb{F}_{p^n}| > |\mathbb{F}_{p^m}|$. So $|<\phi>| = n$, we are done. □

Theorem 3.5.8 (Theorem 5.5 in [1] V. §5)**.** *Let $m, n \geq 1$.*

1. $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m} \iff n|m$.
2. *For $m = nd$, $\mathbb{F}_{p^m}/\mathbb{F}_{p^n}$ is separable and normal. So $Aut(\mathbb{F}_{p^m}/\mathbb{F}_{p^n}) =< \phi^n >$.*

Proof. 1. (First Statement) Suppose $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$. Then, $Aut(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is subgroup of $Aut(\mathbb{F}_{p^m}/\mathbb{F}_p)$. By the Lagrange's theorem, $m = |Aut(\mathbb{F}_{p^m}/\mathbb{F}_p)|$ is divisible by $n = Aut(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Conversely, let $\alpha \in \mathbb{F}_{p^n}$. It suffices to show that $\alpha^{p^m} = \alpha$. We know that $\alpha^{p^n} = \alpha$. So

$$\alpha^{p^m} = \alpha^{p^{nd}} = \alpha^{p^n \cdots p^n} = \cdots = \alpha^{p^n p^n} = \alpha^{p^n} = \alpha.$$

2. Note that $[\mathbb{F}_{p^m} : \mathbb{F}_{p^n}] = d = |Aut(\mathbb{F}_{p^m}/\mathbb{F}_{p^n})|$ since $\phi^m|_{\mathbb{F}_{p^n}} = id_{\mathbb{F}_p} \implies \phi^n \in Aut(\mathbb{F}_{p^m}/\mathbb{F}_{p^n})$. And $|\phi^n| = d = \frac{m}{n}$ since $|\phi| = m$. So $<\phi^n>$ is subgroup of $Aut(\mathbb{F}_{p^m}/\mathbb{F}_{p^n})$. Two groups have the same order d, so they are equal.

□

3.6 Inseparable Extension

Proposition 3.6.1 (Theorem 6.1 in [1] V. §6)**.** *Let $\alpha \in k^a$, $f(x) = irr(\alpha, k)$.*

1. *$chK = 0 \implies \alpha$ is separable (have multiplicity 1).*
2. *$chK = p \implies \exists \mu \geq 0$ such that all the roots of $f(X)$ have the same multiplicity p^μ. So we have $[k(\alpha) : k] = p^\mu [k(\alpha) : k]_s$. Also, α^{p^μ} is separable over k.*

Before proving the proposition, we claim some fact;

Claim 3.6.2. *All the roots of $f(x)$ in k^a have the same multiplicity.*

Proof. Suppose $f(x) = (x-\alpha_1)^{m_1} \cdots (x-\alpha_n)^{m_n} \in k^a[x]$. Now let $\phi : k(\alpha_1) \to k(\alpha_i)$ embedding over k by $\phi(\alpha_1) = \alpha_i$ for some $i \in [n]$. Then, this is isomorphism by standard argument. Now, since $k(\alpha_1), k(\alpha_n)$ are subfield of k^a, we can extend this map as automorphism of k^a. Then, $\phi(f(x)) = f(x)$, which implies $f(x) = (x-\alpha_i)^{m_1} \cdots (x-\alpha_1)^{m_i} \cdots (x-\alpha_n)^{m_n}$. Since $k^a[x]$ is factorial, $m_1 = m_i$. Since i was arbitrary, $m_1 = \cdots = m_n$. □

Proof of 6.1. Suppose that $f(x)$ is not separable. Then, α is multiple root of $f(x)$. Hence $f(\alpha) = f'(\alpha) = 0$. Since $f = irr(\alpha, k)$, $f'(x)$ should be identically zero, otherwise $f'(x)$ is a polynomial having α as a root with lower degree than $f(x)$, contradiction.

1. (If $chK = 0$)
$$chK = 0 \implies f'(x) \neq 0 \implies f'(x) \in k[x] \setminus \{0\}.$$
Since $\deg f'(x) < \deg f(x)$, it contradicts that $f(x) = irr(\alpha, k)$.

2. (If $chK = p > 0$) Then, $f'(x) = 0$ is possible. By proposition 1.12 in [1][Ch 4], $f(x) = g_1(x^p)$ for some $g_1(x) \in k[x]$. Hence α^p is a root of $g_1(x)$. If $g_1(x)$ is not separable, then $g_1'(x)$ is also identically zero, then by the same argument. So we can take $g_2(x)$ such that $g_2(x^p) = g_1(x)$. Hence $g_2(x)$ has α^{p^2} as a root.
Repeat this step until we have α^{p^n} is separable over k for some $\mu \geq 1$, i.e., $f(x) = g_\mu(x^{p^\mu})$ where $g_\mu(x)$ is separable. (Since $\deg f$ is finite, this process should stop at some point. And the stop implies the g_μ is separable.) Now we can say that
$$\#\text{ of distinct roots of } f(x) = \#\text{ of distinct roots of } g_\mu(x),$$
since $LHS \leq RHS$ because g_μ has all p^μ power of roots of f as root of g_μ, and $LHS \geq RHS$ because if there exists $\beta_1, \cdots \beta_n$ as g's distinct root then Frobenius map assures that $\exists \alpha_i$ such that $\alpha_i^{p^\mu} = \beta_i$ in k^a. This implies
$$[k(\alpha) : k]_s = [k(\alpha^{p^\mu}) : k]_s.$$
By comparing degree of f, g_1, we can conclude that $[k(\alpha) : k(\alpha^p)] = p$. since $\deg f = p \deg g$ by putting x^p on g's leading term and $\deg f = [k(\alpha) : k] = [k(\alpha) : k(\alpha^p)][k(\alpha^p) : k] = p \deg g_1$ (If $g_1(x) \neq irr(\alpha^p, k)$ up to constant, then $\exists h \in k[x]$ such that $h(\alpha^p) = 0$ but $\deg h < \deg g$, which implies $h(x^p) \in k[x]$ such that $h(x^p)$ has α as a root, so $\deg h(x^p) = p \deg h < p \deg g_1 = \deg f$, contradict the fact that $f = irr(\alpha, k)$.) Applying this argument inductively on $g_1, \cdots g_\mu$, we can get
$$[k(\alpha) : k(\alpha^{p^\mu})] = p^\mu.$$
Since g_μ has root of multiplicity 1, we know $[k(\alpha^{p^\mu}) : k]_s = [k(\alpha^{p^\mu}) : k]$. Also, since the number of distinct roots of $f(x)$ is equal to the number of distinct roots of g_μ,
$$[k(\alpha) : k] = [k(\alpha) : k(\alpha^{p^\mu})][k(\alpha^{p^\mu}) : k] = p^\mu [k(\alpha^{p^\mu}) : k] = p^\mu [k(\alpha^{p^\mu}) : k]_s = p^\mu [k(\alpha) : k]_s.$$

□

Remark 3.6.3. *In the second case of the proof, $k(\alpha^{p^\mu})/k$ is separable, and $x^{p^\mu} - \alpha^{p^\mu} = (x - \alpha)^{p^\mu} \in k(\alpha^{p^\mu})[x]$.*

Corollary 3.6.4 (Corollary 6.2. in [1] V. §6)**.** *Let E/k be finite. Then $[E : k]_s | [E : k]$ and $\frac{[E:k]}{[E:k]_s} = \begin{cases} 1, & \text{if } chk = 0 \\ p^\mu, & \text{for some } \mu \geq 0 \text{ if } chk = p > 0 \end{cases}$*

Proof. Let $E = k(\alpha_1, \cdots, \alpha_n)$ by proposition 1.5 in [1]. Then, we can think a tower of simple algebraic extension. and $[\_ : \_], [\_ : \_]_s$ are transitive under multiplication. □

Definition 3.6.5. *Let E/k finite. Then denote $[E : k]_i = [E : k]/[E : k]_s$, and call it **inseparable degree** of E/k.*

Remark 3.6.6. *$[E : k]_i = [E : F]_i [F : k]_i$ for any intermedate field F.*

Definition 3.6.7. *Let $\alpha \in k^a, chk = p > 0$. Then, α is called **purely inseparable** over k if $\alpha^{p^\mu} \in k$ for some $\mu \geq 0$.*

Remark 3.6.8.

$$\alpha \text{is p. ins} \iff \#\text{ of distinct root of } irr(\alpha, k) = 1 \iff [k(\alpha) : k]_s = 1.$$

Proof. If α is purely inseparable, then $\exists n \in \mathbb{N}$ such that $\alpha^{p^n} \in k$, so $x^{p^n} - (\alpha^{p^n}) \in k[x]$. Since it has α as a root, and $x^{p^n} - (\alpha^{p^n}) = (x - \alpha)^{p^n}$ in $k^a[x]$, so the number of distinct root is 1. Conversely, suppose the number of distinct roots of $irr(\alpha, k)$ is 1. Then, $irr(\alpha, k) = (x - \alpha)^n$. If $n \neq p^\mu$ for some $\mu \in \mathbb{N} \cup \{0\}$, then $\alpha \in k$ since $irr(\alpha, k) = x^n - n \cdot \alpha x^{n-1} + \cdots \in k[x]$, so $n \neq 0$ if $n \neq lp$ for some $l \in \mathbb{N}$, and if $n = lp$ but $n \neq p^\mu$, then the coefficient of x^{n-p} is $\binom{lp}{p} = \frac{(lp)!}{((l-1)p)!p!}$, which include no p in irreducible term, so nonzero, implies $\alpha^{n-p} \in k$, so $\deg irr(\alpha, k) = n - p$, contradiction.
Second $\iff$ is from definition of $[\_ : \_]_s$. □

Proposition 3.6.9. *Let E/k algebraic, $chk = p$. Then the followings are equivalent.*

1. *$[E : k]_s = 1$*
2. *$\forall \alpha \in E$, α is purely inseparable.*
3. *$\forall \alpha \in E$, $irr(\alpha, k) = x^{p^\mu} - a$ for some $\mu \geq 0, a \in k$.*
4. *$E = k(S)$ for some $S = \{\alpha_i\}_{i \in I}$ such that α_i is purely inseparable over k.*

Definition 3.6.10. *E/k algebraic, call E/k be **purely inseparable** if one of the above four conditions holds.*

For example, α is purely inseparable over k and $\alpha^\mu \in k$, then $k(\alpha)/k(\alpha^\mu)$ is purely inseparable extension and $k(\alpha^\mu)/k$ is separable extension.

Proof. • (1 $\implies$ 2) Let $\alpha \in E$. Since $[E : k]_s = [E : k(\alpha)]_s [k(\alpha) : k]_s$ by theorem 4.1, $[k(\alpha) : k]_s = 1$. Then $irr(\alpha, k)$ has only one root, α. Hence $irr(\alpha, k) = (x - \alpha)^m \in k^a[x]$ for some $m \in \mathbb{N}$. If $m \neq p^\mu$ for some $\mu \in \mathbb{N} \cup \{0\}$, then $\alpha \in k$ since $irr(\alpha, k) = x^m - m \cdot \alpha x^{m-1} + \cdots \in k[x]$, so $m \neq 0$ if $n \neq lp$ for some $l \in \mathbb{N}$, and if $m = lp$ but $m \neq p^\mu$, then the coefficient of x^{m-p} is $\binom{lp}{p} = \frac{(lp)!}{((l-1)p)!p!}$, which include no p in irreducible term, so nonzero, implies $\alpha^{m-p} \in k$, so $\deg irr(\alpha, k) = n - p$, contradiction. Hence $m = p^\mu$, therefore $\alpha^{p^\mu} \in k$. Hence α is purely inseparable.

- ($2 \implies 3$) Let $\alpha \in E$. Since it is purely inseparable, $\exists \mu \in \mathbb{N}$ such that $\alpha^{p^\mu} \in k$ for some $\mu \geq 0$. Let $a = \alpha^{p^\mu}$. Then,

$$irr(\alpha, k) | x^{p^\mu} - a = (x - \alpha)^{p^\mu}.$$

So, $irr(\alpha, k) = (x - \alpha)^l$ for some $l \in \mathbb{N}$. Let $l = mp^\nu$, with $g.c.d(m, p) = 1$. Then,

$$(x-\alpha)^l = \left((x-\alpha)^{p^\nu}\right)^m = \left(x^{p^\nu} - \alpha^{p^\nu}\right)^m = x^{p^\nu} - \binom{m}{1}\alpha^{p^\nu} x^{p^\nu(m-1)} + \cdots \in k[x]$$

Hence $m\alpha^{p^\nu} \in k$. Since $g.c.d(m, p) = 1$, $\alpha^{p^\nu} \in k$. However, since $(x - \alpha)^l = irr(\alpha, k)$, so $l \leq p^\nu$. Therefore,

$$p^\nu \leq mp^\nu = l \leq p^\nu.$$

This implies $m = 1$, so $n = p^\nu$ for some ν.

- ($3 \implies 2$) trivial; just definition of purely inseparable element.
- ($3 \implies 4$) Take $S = E$. Then by $3 \iff 2$, $k(S) = E$.
- ($4 \implies 1$) Let $\sigma : E = k(S) \to k^a$ embedding over k. Then, $\sigma(a_i) = a_i$ for all $i \in I$, since a_i is purely inseparable, implies $irr(\alpha, k) | x^{p^\mu} - \alpha^{p^\mu}$ for some $\mu \in \mathbb{N}$, thus $irr(\alpha, k)$ has only one root. Hence σ is identity on each a_i. Therefore, σ is identity on E. Since σ was arbitrary, any embedding of E over k into k^a is identity. Therefore, $[E : k]_s = 1$.

□

Proposition 3.6.11. *A class of Purely Inseparable extensions form a distinguished class.*

Proof. 1. (First condition) Suppose $E/F/k$ with E/F, F/k are purely inseparable extension. Then, $[E : k]_s = [E : F]_s[F : k]_s = 1$ by theorem 4.1, implies E/k is purely inseparable. Conversely, if E/k is purely inseparable, then theorem 4.1 tells that $[E : F]_s = 1, [F : k]_s = 1$.

2. (Second condition) Suppose E/k is purely inseparable. Then, by condition 3 of purely inseparable extension, $E = k(S)$ for some $S = \{\alpha_i\}_{i \in I}$ such that α_i is purely inseparable over k. Then $EF = k(S)F = F(S)$ for any F/k. Since any element in S is also purely inseparable on F, since its power of p^μ is in $k \subset F$. Therefore, by condition 4 of purely inseparable extension, EF/F is purely inseparable extension.

□

Proposition 3.6.12 (Theorem 6.6 in [1] V. §6)**.** *E/k is algebraic, char $k = p$. Let E_0 be the compositum of all F such that $E/F/k$ where F/k is separable extension. Then, E/E_0 is purely inseparable, and E_0/k is separable.*

Proof. Let $\alpha \in E$. By the proposition 6.1.2, $\exists \mu \geq 0$ such that α^{p^μ} is separable over E_0. By definition of E_0, with the fact that $k(\alpha^{p^\mu})/k$ is separable, $\alpha^{p^\mu} \in E_0$. Hence α is purely inseparable over E_0.
E_0/k is separable, since separable extensions form a distinguished class and $E_0 = E_0F/F$ is separable for any F/k is separable, by condition 2 of distinguished class, which implies E_0/k is separable, by condition 1 of distinguished class. □

Remark 3.6.13. *For $k^a/k^{sep}/k$, k^a/k^{sep} is purely inseparable, k^{sep}/k is separable, by above proposition.*

Corollary 3.6.14 (Corollary 6.7 in [1] V. §6)**.** *E/k algebraic, and separable and also purely inseparable. Then $E = k$.*

Proof. Since E is purely inseparable, $[E : k]_s = 1$. Since E is separable, $[E : k]_s = [E : k]$. Hence $E = k$. □

Corollary 3.6.15 (Corollary 6.8 in [1] V. §6)**.** *Let K/k is normal, K_0 is the maximal separable subextension of K/k. Then K_0/k is normal.*

Proof. Let $\sigma : K_0 \to k^a$ be embedding of K_0 over k. Existence of σ is solved when we make $(K_0)^a$, which is actually isomorphic to k^a therefore at least one such σ exists. Then, by theorem 2.8, $\exists\tau : K \to k^a$ which is extension of σ. Then since K/k is normal, $\tau \in Aut(K/k)$, so $\tau(K_0) = \sigma(K_0) \subset K$. And also note that $\sigma(K_0)/k$ is separable since $\forall\alpha \in K_0$, $\sigma(\alpha)$ is another root of $irr(\alpha, k)$, which implies $\sigma(\alpha)$ is also separable. (Note that $\sigma(irr(\alpha, k)) = irr(\alpha, k)$ since it has no multiple roots.) Therefore, $\sigma(K_0) \subset K_0$ since K_0 is maximal separable extension. Then by the lemma 2.1, $\sigma(K_0) = K_0$. Since σ was arbitrary, K_0/k is normal. □

Corollary 3.6.16 (Corollary 6.9 in [1] V. §6)**.** *Let $E/k, F/k$ be finite, and E/k is separable, F/k is purely inseparable, and $\exists L$, a field such that $E \subset L$, $F \subset L$. Then, below figure holds; so $[EF : F] = [E : k] = [EF : k]_s$, $[EF : E] = [F : k] = [EF : k]_i$.*

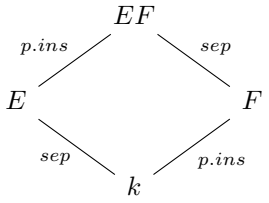


Figure 16: Corollary 6.9

Proof. The figure 16 holds by condition 2 of distinguished class and the fact that separable exensions and purely inseparable extensions form distinguished classes respectively. Then,

$$[EF : F] = [EF : F]_s = [EF : k]_s = [E : k]_s = [E : k]$$

where first equality comes from EF/F is separable, the second equality comes from $[F : k]_s = 1$, and the third equality comes from $[EF : k]_s = [EF : E]_s[E : k]_s = 1 \cdot [E : k]_s$, and the last equality comes from E/k is separable. Similarly,

$$[EF : E] = [EF : E]_i = [EF : k]_i = [F : k]_i = [F : k]$$

where first equality comes from EF/E is purely inseparable, the second equality comes from $[E : k]_i = 1$, and the third equality comes from $[EF : k]_i = [EF : F]_i[F : k]_i = 1 \cdot [F : k]_i$, and the last equality comes from F/k is purely inseparable. □

Corollary 3.6.17 (Corollary 6.10 in [1] V. §6)**.** *Let E/k finite, and $E^p = \{x^p : x \in E\}$. Then*

$$E/k \text{ separable} \iff E^p k = E \iff E^{p^n} k = E \forall n \geq 1.$$

Proof. Third statement contain the case of the second statement. If second statement holds, then

$$E = E^p k = (E^p k)^p k = E^{p^2}(k^p k) = E^{p^2} k,$$

where last equality comes from the fact that $k^p \cong k$ since $\mathrm{char}\, k = p$ and $x \mapsto x^p$ is the Frobenius map which induces isomorphism. By applying inductively, we can conclude that $E = E^{p^n} k$ for any $n \in \mathbb{N}$.
Suppose the second statement. Then, $E = k(\alpha_1, \cdots, \alpha_n)$ by the proposition 1.5. Then $\exists m$ such that $\alpha_i^{p^m}$ is separable over k for all i, by theorem 6.1. Hence $\alpha_i^{p^m} \in E_0$ which is maximal separable extension between E and k. Take the maximal m for all $1 \le i \le m$. Then $E = E^{p^m} k \subset E_0$ implies $E = E_0$. Conversely, suppose E/k be separable. Then, $E/E^p k$ is separable since still $irr(\alpha, E^p k)$ contain all distinct roots. Also, $E/E^p k$ is purely inseparable since $\forall \alpha \in E$, $\alpha^p \in E^p k$. Therefore, $E^p k = E$, by the corollary 6.7. □

Remark 3.6.18. *Let $\alpha \in E$. Then α is separable over $k \iff k(\alpha) = k(\alpha^{p^n}), \forall n \ge 1$.*

Proof. Put $E = k(\alpha)$, then $E^{p^n} k = k(\alpha^{p^n})$ □

Proposition 3.6.19 (Proposition 6.11 in [1] V. §6)**.** *K/k be normal. $G = Aut(K/k)$. Let $K^G = \{a \in K : \sigma a = a, \forall \sigma \in G\}$, K_0 be maximal separable extension of k in K. Then, the below figure holds.*

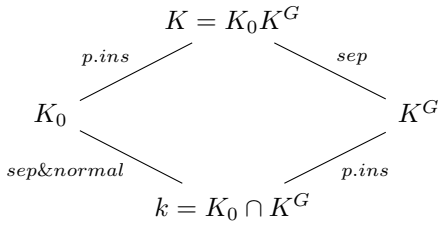


Figure 17: Proposition 6.11

Proof.

- (K^G/k is purely inseparable oveer k) Let $\alpha \in K^G$. Then, let $\sigma : k(\alpha) \to k^a$ be embedding. Then, take τ be extension of σ of K. Then, since K/k is normal, $\tau \in Aut(K/k) = G$, and $\tau|_{k(\alpha)} = \sigma$. Hence $\sigma(\alpha) = \tau(\alpha) = \alpha$. So σ is identity. Hence $[K(\alpha) : k]_s = 1$. Since α was arbitrary, K^G/K is inseparable.
- ($K_0 \cap K = k$) Note that $K_0 \cap K/k$ is purely inseparable and separable, hence $K_0 \cap K = k$ by corollary 6.7.
- (K/K^G is separable.) We should divides two casees.
  1. (K/k is finite.) Let $\alpha \in K$, and let $G\alpha := \{\sigma(\alpha) : \sigma \in G\}$. Since G is finite by theorem 4.1, so $G\alpha$ is finite, and take $\sigma_1, \cdots \sigma_r \in G$ such that $\sigma_i(\alpha) \ne \sigma_j(\alpha)$ for any two pair $(i, j) \in [r] \times [r]$, i.e., $G\alpha = \{\sigma_1(\alpha), \cdots \sigma_r(\alpha)\}$. Then, since K is normal, $G\alpha \subset K$. Now construct

$$f(x) = \prod_{i=1}^{r} (x - \sigma_i \alpha) \in k[x].$$

Then for any $\sigma \in G$,

$$\sigma f(x) = \prod_{i=1}^{r}(x - \sigma\sigma_i\alpha) = \prod_{i=1}^{r}(x - \sigma_i\alpha) = f(x).$$

since σ is just a permutation. (If $\sigma\sigma_i(\alpha) = \sigma\sigma_j(\alpha)$ with $i \neq j$, then $\sigma(\sigma_i(\alpha) - \sigma_j(\alpha)) = 0$, which implies σ is not injective, contradiction. Hence $\{\sigma\sigma_i(\alpha)\}_{i\in[r]} = G\alpha$.) Hence $f(x) \in K^G[x]$, hence $f(x)$ has no multiple roots, so α is also separable over K^G. Since α was arbitrary, K/K^G is separable.

2. (K/K^G is infinite.) Let $\alpha \in K$. Then take splitting field of α over K^G, call it L_α. Since L_α/K^G is normal and finite, we can conclude that L_α/K^G is separable. Since $K = \cup_{\alpha\in K} L_\alpha$, so it is also separable, by the definition that every finitely generated subextension is separable.

- ($K = K_0K^G$.) Since K/K_0 is purely inseparable and $K/K_0K^G/K_0$, K/K_0K^G is purely inseparable by condition 1 of distinguished class of purely inseparable extension. Also, since K/K^G is separable and $K/K_0K^G/K^G$, K/K_0K^G is separable by condition 1 of distinguished class of separable extension. Hence, by corollary 6.7, $K = K_0K^G$.
- (K_0/k is normal.) This is from corollary 6.8.

□

Corollary 3.6.20 (Corollary 6.12 in [1] V. §6)**.** *Let $k = k^p$, called **perfect**, E/k be algebraic extension. Then E/k is separable.*

Proof. Suppose $K/E/k$ for some K/k normal extension. (Note that such K exists, by just taking $K = k^a$.) Let $\alpha \in K^G$, then, since K^G/k is purely inseparable by the above theorem, $\alpha^{p^m} \in k = k^{p^m}$ for some m, since $k = k^p \implies k = k^p = k^{p^2} = \cdots$. So, $\alpha^{p^m} = a^{p^m}$ for some $a \in k$. Hence $\alpha = a$ by injectivity of frobenius map. Hence K/k is separable, which implies E/k separable by distinguished class of separable extensions. □

4 Galois Theory

Every number of theorem comes from Lang's book.

4.1 Galois Extensions

Definition 4.1.1. *Let K be a field, G a group of automorphism of K. Then,*

$$K^G := \{a \in K : \sigma a = a \text{ for } \sigma \in G\}$$

is called fixed field of G.

Definition 4.1.2. *For field k and its extension K, K/k is called Galois extension if it is separable and normal. Then, $G(K/k) := Gal(K/k) := Aut(K/k)$ is the galois group of K/k.*

Theorem 4.1.3. *Let K/k be finite Galois. Then,*

1.

$$\begin{array}{rcl} \mathscr{F} := \{E : k \subset E \subset K\} & \overset{bijective}{\longleftrightarrow} & \mathscr{G} := \{H : H \leq G(K/k)\} \\ E & \mapsto & G(K/E) \\ K^H & \hookleftarrow & H \end{array}$$

2. *For $E \in \mathscr{F}$, E/k is Galois $\iff$ $G(K/E) \trianglelefteq G(K/k)$. In this case, $G(E/k) \cong G(K/k)/G(K/E)$*

Remark 4.1.4. *For $E \in \mathscr{F}$, $[K : E] = |G(K/E)|$, and $[E : K] = (G(K/k) : G(K/E))$.*

Proof of the theorem will be given by step by step with other theorems.

Theorem 4.1.5. *Let K/k be Galois, and let $G = G(K/k)$. Then,*

1. *$K^G = k$*
2. *If $k \subset E \subset K$, then K/E is Galois.*
3. *$E \mapsto G(K/E)$ is injective.*

Proof. For the first assertion, let $\alpha \in K^G$, and think about $k(\alpha)$. Let σ be any embedding of $k(\alpha)$ in K^a, so that $\sigma|_k = 1_k$. Using theorem 2.8, we extend this map to an embeding of K into K^a by theorem 2.8. and say σ too. Then, σ is automorphism from theorem 3.3's normality condition 1. Thus, $\sigma \in G$, by definition of Galois group. Since $\alpha \in K^G$, $\sigma(\alpha) = \alpha$. Also, σ fixes k by definition. Thus, σ fixes $k(\alpha)$. Since σ was arbitrary,

$$[k(\alpha) : k]_s = 1.$$

Since α is separable over k by Galois condition of K, $k(\alpha) = k$, which implies $\alpha \in k$. Thus $K^G = k$.

For the second assertion, K is normal over E by theorem 3.4, and separable over E by theorem 4.5. Hence K/E is Galois. From the first assertion, $E = K^{G(K/E)}$.

It suffices to show that $E \mapsto G(K/E)$ is injective. If E, E' are intermediate fields such that $G(K/E) = G(K/E')$, then $E = K^{G(K/E)} = K^{G(K/E')} = E'$, done. □

Corollary 4.1.6.
1. *$G(K/F) \cap G(K/F') = G(K/FF')$*
2. *$F \cap F' = K^{G(K/F) \vee G(K/F')}$ where $\vee$ is join.*
3. *$F \subset F' \iff G(K/F) > G(K/F')$.*
4. *If K is finite Galois, $\exists$ only finitely many E's such that $k \subset E \subset K$.*

Proof. For any $\sigma \in G(K/F) \cap G(K/F')$, σ fixes FF', and for any $\tau \in G(K/FF')$ fixes F, F' too. Hence $G(K/F) \cap G(K/F') = G(K/FF')$.

Also, join implies the smallest subgroup containing each $G(K/F), G(K/F')$ respectively. Thus, for any element in the join, it can be represented by product of elements from $G(K/F), G(K/F')$. Since such product fixes $F \cap F'$, it is obvious.

Third thing is also obvious; If $\sigma \in G(K/F')$, then it fix F too. Thus $\sigma \in G(K/F)$. This implies $G(K/F) > G(K/F')$. If $G(K/F') < G(K/F)$, then $\sigma \in G(K/F')$ fixes F for any σ. Hence $F \subset F'$.

Since $|Gal(K/k)| < \infty$, so that the number of its fixed field is finite. □

Theorem 4.1.7 (Artin)**.** *Let K be a field and let $G = Aut(K)$ with $|G| = n$. Then, K/K^G is finite and Galois, and $G(K/K^G) = G$, $[K : K^G] = n$.*

Proof. Let $\alpha \in K$. Choose $\sigma_1, \cdots, \sigma_r \in G$ maximal such that $\sigma_1(\alpha), \cdots, \sigma_r(\alpha)$ are distinct. Thus, for any $\tau \in G$, $\{\sigma_1(\alpha), \cdots, \sigma_r(\alpha)\} = \{\tau\sigma_1(\alpha), \cdots, \tau\sigma_r(\alpha)\}$ by maximality and injectivity of τ. Hence,

$$f(x) = \prod_{i=1}^{r} (x - \sigma_i \alpha)$$

has α as a root, and $f^\tau = f \implies f \in K^G[x]$. Futhermore, f is separable by definition. Since $irr(\alpha, K^G)$ is a product of linear factors $x - \sigma_i\alpha$ in $K[x]$, $irr(\alpha, K^G)$ splits in $K[x]$. Since α was arbitrary, K is normal for K^G. Thus, K/K^G is Galois.

For any $\alpha \in K$,

$$[K^G(\alpha) : K^G] \leq n \implies [K : K^G] \leq n.$$

and, K/K^G is finite by lemma 1.7. And by theorem 4.1 of chapter V., $G(K/K^G)$ has order less than n. Since $|G| = |G(K/K^G)|$ and $G \leq G(K/K^G)$, $G(K/K^G) = G$. □

Lemma 4.1.8 (Lemma 1.7)**.** *Let E/k algebraic separable extension. Suppose $[k(\alpha) : k] \leq n$ for any $\alpha \in E$ and some n. Then, E/k finite, and $[E : k] \leq n$.*

Proof. Let α be an element such that $[k(\alpha) : k] = m \leq n$ is maximal. It suffices to show that $k(\alpha) = E$. Otherwise, $\exists\beta \in E$ such that $\beta \notin k(\alpha)$. From the primitive element theorem, $\exists\gamma \in k(\alpha, \beta)$ such that $k(\alpha, \beta) = k(\gamma)$. However,

$$k \subset k(\alpha) \subset k(\alpha, \beta) \implies [k(\alpha, \beta) : k] > m \implies [k(\gamma) : k] > m$$

contradiction. □

Corollary 4.1.9 (Corollary 1.9)**.** *Let K/k be finite and Galois. Then, $G(K/K^H) = H$ for $H \leq G(K/k)$.*

Proof. Apply Artin's theorem on H and K^H. □

Proof of theorem 1.1, first part. Note that $\tau : H \mapsto K^H$ is injection by theorem 1.1.5.3. Also, corollary 1.9 gives bijection between $Im\tau \cong \mathscr{G}$. Now it suffices to show that $Im\tau = \mathscr{F}$. For arbitrary $k \subset E \subset K$, K/E is Galois by theorem 1.1.5.2. And from Corollary 1.1.6.3, $G(K/k) > G(K/E)$. Hence let $H = G(K/E)$, then $H < G(K/k)$, which implies $\tau(H) = E$, so it is surjective. □

Theorem 4.1.10 (Theorem 1.10)**.** *Let K/k be Galois with $G = G(K/k)$, and let $k \subset F \subset K, H = G(K/F)$. Then,*

1. *F is normal over $k \iff H \triangleleft G$*
2. *If F/k is normal, then $G \xrightarrow{\phi} G(F/k)$ by $\sigma \mapsto \sigma|_F$ is a surjective group homomorphism with $ker\phi = H$. So, $G(K/k)/G(K/F) \cong G(F/k)$.*

Proof. Suppose F is normal over k. Pick arbitrary $\tau \in G$. Then, $\tau H\tau^{-1} = \{\tau\sigma\tau^{-1} : \sigma \in H\}$. Since F/k is normal, $\tau(F) = F$ by Normality condition 1. (Think it as embeding of K^a. Nor 1 gives automorphism.) Then, for any $\sigma \in H$, $\alpha \in F$,

$$\tau\sigma\tau^{-1}(\alpha) = \tau\sigma(\tau^{-1}(\alpha)) = \tau\tau^{-1}\alpha = \alpha$$

since $\tau^{-1}\alpha \in F$. Thus, $\tau\sigma\tau^{-1} \in H$ Since σ was arbitrary, $\tau H\tau^{-1} = H$. Hence $H \triangleleft G$.

Suppose $H \triangleleft G$. Let $\tau : F \to K^a$ be an embedding over k. Extend $\tilde{\tau} \in G$. Since $\tilde{\tau}H\tilde{\tau}^{-1} = H$, and $H = G(K/F)$ as defined above,

$$G(K/\tilde{\tau}F) = G(\tilde{\tau}K/\tilde{\tau}F) = \tilde{\tau}G(K/F)\tilde{\tau}^{-1} = G(K/F).$$

Hence $\tilde{\tau}F = F$. So F/k satisfy normality condition 1.

For second part, define $\phi : G \to G(F/k)$ by $\phi(\sigma) = \sigma|_F$. Then ϕ is well-defined. Hence ϕ is surjective from theorem 2.8 of chapter V, since any automorphism in $G(F/k)$ can be extended to be in $G(K/k)$, and any automorphism in $G(K/k)$ can be restricted to be in $G(F/k)$. Also, $\ker\phi = H$. □

Proof of theorem 1.1, second part. If E/k is Galois, E is normal, so that $G(K/E) \trianglelefteq G(K/k)$ by theorem 1.10 first part. Also, $G(E/k) \cong G(K/k)/G(K/E)$ by theorem 1.10 second part. □

Theorem 4.1.11 (Theorem 1.12)**.** *Let K/k be finite and Galois, and let F be an extension of k. Then, KF/F is Galois and $G(KF/F) \cong G(K/K \cap F)$ where the isomorphism is given by $\sigma \mapsto \sigma|_K$.*

Proof. KF/F is Galois from theorem 3.4 and distinguishness of separable extension. Consider the map $G(KF/F) \xrightarrow{\phi} G(K/K \cap F)$ defined by $\sigma \mapsto \sigma|_K$. Then, ϕ is injective, since $\sigma|_K = id_{K\cap F}$ implies $\sigma = id|_{KF}$. Surjectivity comes from below argument. Let $H = im\phi$. Then, $K^H \supset K \cap F$. Conversely, $\forall \alpha \in K^H, \forall \sigma \in G(K/K \cap F)$, $\sigma\alpha = \alpha$ since α is fixed by every element in H, which implies $\alpha \in F$, so that $\alpha \in K \cap F$. Thus $K^H \subset K \cap F$, so $K^H = K \cap F$. Hence $H = G(K/K \cap F)$ by Artin's theorem. □

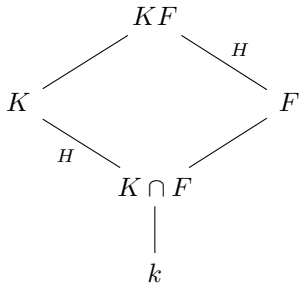


Figure 18: Theorem 1.12

It is suggestive to think of the opposite sides of a parallelogram as being equal.

Corollary 4.1.12 (Corollary 1.13)**.** *Let K/k be finite, Galois and let F/k be arbitrary extension. Then, $[KF : F] | [K : k]$. In particular, $[KF : F] = [K : k] \iff K \cap F = k$.*

Proof. From order of H divides order of G, with remark 1.1.4, our assertion follows. □

Theorem 4.1.13 (Theorem 1.14)**.** *Let K_1/k, K_2/k be Galois. ($K_1, K_2 \subset k^a$). Then,*

1. *K_1K_2/k is Galois*
2. *The map $G(K_1K_2/k) \xrightarrow{\phi} G(K_1/k) \times G(K_2/k)$ by $\sigma \mapsto (\sigma|_{K_1}, \sigma|_{K_2})$ where $\phi_1(\sigma) = \sigma|_{K_1}, \phi_2(\sigma) = \sigma_{K_2}$ is a well-defined injective group homomorphism. If $K_1 \cap K_2 = k$, then ϕ is isomorphism.*

For example,
In this case, $G(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Proof. First assertion is obvious from theorem 3.4 of chapter V and distinguishness of separability.

For the second assertion, since K_1, K_2 are normal over k, ϕ is well-defined; namely, restriction is also automorphism. Also, ϕ is a group homomorphism from trivial but tedious calculation. If $\sigma \in G(K_1K_2/k)$ such that $\sigma|_{K_1} = id|_{K_1}, \sigma|_{K_2} = id|_{K_2}$, then, $\sigma = id_{K_1K_2}$. So ϕ is injective.
Suppose $K_1 \cap K_2 = k$. Then, $\phi_1(G(K_1K_2/K_2)) = G(K_1/K_1 \cap K_2) = G(K_1/k)$ by theorem 1.12. Similarly, $\phi_2(G(K_1K_2/K_1)) = G(K_2/k)$. Thus, ϕ is surjective. □

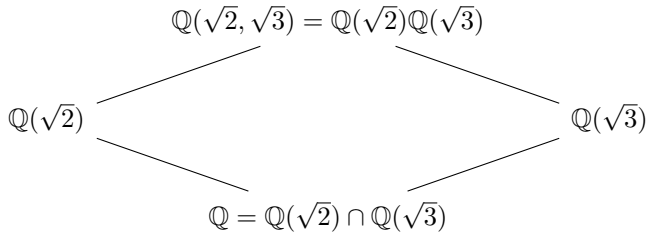


Figure 19: Example of theorem 1.14

Corollary 4.1.14. *1. Let $K_1, \cdots, K_n \subset k^a$ and let $K_1/k, \cdots, K_n/k$ be Galois. Assume that $K_{i+1} \cap (K_1 \cdots K_i) = k$ for each $i = 1, \cdots, n-1$. Then, $G(K_1 \cdots K_n/k) \cong G(K_1/k) \times \cdots \times G(K_n/k)$.*

2. Let K/k be Galois and let $G = G(K/k) = G_1 \times \cdots \times G_n$. Put $\tilde{G}_i = G_1 \times \cdots \{e\} \times \cdots \times G_n$ and $K_i = K^{\tilde{G}_i}$ for $i = 1, \cdots, n$, where $\{e\}$ in middle is i-th component. Then, K_i/k is Galois for $i = 1, \cdots, n$ with $G(K_i/k) \cong G_i$ and $K_{i+1} \cap (K_1 \cdots K_i) = k$ for $i = 1, \cdots, n-1$, and $K = K_1 \cdots K_n$.

Proof. For the first assertion, Inductively apply theorem 1.14.

For the second assertion, since $\tilde{G}_i \triangleleft G$, K_i/k is Galois by theorem 1.1 and $G(K_i/k) = G/\tilde{G}_i \cong G_i$ by theorem 1.1. Hence,

$$G(K/K_{i+1} \cap (K_1 \cdots K_i)) = G(K/K_{i+1}) \vee G(K/K_1 \cdots K_i) = \tilde{G_{i+1}} \vee (\tilde{G}_1 \cap \cdots \cap \tilde{G}_i) = G = G(K/k)$$

by corollary 1.1.6. Thus, $K_{i+1} \cap (K_1 \cdots K_i) = k$. Also,

$$G(K/K_1 \cdots K_n) = \tilde{G}_1 \cap \cdots \cap \tilde{G}_n = \{e\} = G(K/K).$$

Hence, $K_1 \cdots K_n = K$. □

Remark 4.1.15. *A Galois extension K/k is said to be **abelian** (resp. **cyclic**) if its Galois group G is abelian (resp. cyclic). Also, k^{ab} denote composite of all abelian extensions of k in a given algebraic closure . It is called maximal abelian extension of k.*

Remark 4.1.16 (Related theorems for abelian extension)**.** *1. (Cor 1.11) Let K/k be abelian. Then for any intermediate field E, E/k is abelian.*

2. (Thm 1.17) Assume all fields are contained in some common field.

(a) $K/k, L/k$ abelian $\implies$ KL/k abelian.

(b) K/k abelian, E/k any extension, $\implies$ KE/E abelian

(c) K/k abelian, E be intermediate field of K/k, then $E/k, K/E$ are abelian.

Proofs come from 1.12 and 1.14.

4.2 Examples and applications

Let $f(x) \in k[x]$ be separable, E be the splitting field of $f(x)$ over k. Hence E/k is Galois. Let $G(E/k)$ be Galois group of f.

Example 4.2.1 (Example 1, quadratic extensions)**.** *Let $a \in k$. If a is not square in k, $x^2 - a$ is irreducible. Suppose chark $\neq 2$. Then, polynomial is separable because $2 \neq 0$, and if α is root, then $k(\alpha)$ is the splitting field, Galois, and cyclic.*

Conversely, given an extension K/k of degree 2, $\exists a \in k$ such that $k(\alpha) = K, \alpha^2 = a$. This comes from by taking $\alpha \in K \setminus k$, and its order must be 2. Since sum of other root of $irr(\alpha, k)$ and product of roots are in k, the other root should be conjugation of α. Hence, its square must be in k. (Tedious calculation must be needed.)

Example 4.2.2 (Example 2, cubic extensions)**.** *Let $f(x) \in k[x]$ be separable, and let $\alpha_1, \cdots, \alpha_n$ be roots of $f(x)$. Define $\delta(f) = \prod_{i<j}(\alpha_i - \alpha_j), \Delta(f) = \delta(f)^2 = \prod_{i<j}(\alpha_i - \alpha_j)^2$; which is called* ***discriminant*** *of f.*

If $n = 2$, then, $\Delta(f) = (\alpha_1 - \alpha_2)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = a^2 - 4b$ where $f(x) = x^2 + ax + b \in k[x]$.

We may assume $G(E/k) < S_n$ since $G(E/k) \hookrightarrow S_n$ because $\{\sigma\alpha_1, \cdots, \sigma_{\alpha_n}\} = \{\alpha_1, \cdots, \alpha_n\}$, so that σ is permutation on $\{\alpha_1, \cdots, \alpha_n\}$. Then, for any $\sigma \in G(E/k)$,

$$\sigma(\delta(f)) = \pm\delta(f) \implies \sigma\Delta = \Delta \implies \Delta \in E^{G(E/k)} = k$$

. We can check that $\sigma\delta = \delta \iff \sigma$ is even, by checking for transposition cases.

Assume char $k \neq 3$. Consider $f(x) = x^3 + ax^2 + bx + c \in k[x]$ irreducible, separable, G be Galois group of f. So that $G < S_3$. Also, $|G| \geq 3$ since at least three ways of permuting roots does always exist. Hence, $G = A_3$ or S_3. Note that

$$G = A_3 \iff \sigma\delta = \delta, \forall\sigma \in G \iff \forall\sigma \in G, \sigma \text{ is even.} \iff \delta \in k$$

or

$$G = S_3 \iff \sigma\delta = -\delta, \text{ for some } \sigma \in G \iff \text{ Some } \sigma \text{ is odd.} \iff \delta \in K.$$

In particular, if $a = 0$, then $\Delta(f) = -4b^3 - 27c^2$. In general,

$$g(x) = f(x - \frac{a}{3}) = x^3 + px + q$$

for some $p, q \in K$. (cf. Hungerford Ch.V. Prop 4.8.) For example, $f(x) = x^3 - 2 \in \mathbb{Q}[x]$, $\Delta(f) = -27 \cdot 4 = -108$ (not square). Thus, Galois group of $f(x) = S_3$

Example 4.2.3. *$f(x) = x^4 - 2 \in \mathbb{Q}[x]$ irreducible by Eisenstein criterion. Then, $\{\alpha, -\alpha, i\alpha, -i\alpha\}$ where $\alpha = \sqrt[4]{2}$ are roots of f. So, let $K := \mathbb{Q}(\alpha, i)$. Then, $|G(K/\mathbb{Q})| = 8$ since below diagram.*

Note that $D_4 =< \sigma, \tau : \sigma^4 = \tau^2 = 1, \tau\sigma\tau\sigma = 1 >$. Let $\sigma \in G(K/\mathbb{Q}(i))$ such that $\sigma(\alpha) = i\alpha$. Then $|\sigma| = 4$. Let $\tau \in G(K/\mathbb{Q}(\alpha))$ such that $\tau(i) = -i$. Then $|\tau| = 2$, and $\tau \notin < \sigma >$. Hence $\tau\sigma\tau\sigma(\alpha) = \alpha$, $\tau\sigma\tau\sigma(i) = i$. Hence $\tau\sigma\tau\sigma = id_K$. Thus, $D_4 \cong G(K/\mathbb{Q})$.

Example 4.2.4. *Let $t_1, \cdots, t_n$ be indeterminates, and let $k[t_1, \cdots, t_n] \subset k(t_1, \cdots, t_n)$. Suppose that S_n acts on $k[t_1, \cdots, t_n]$ by $\sigma f(t_1, \cdots, t_n) = f(t_{\sigma(1)}, \cdots, t_{\sigma(n)})$. Let $K := k(t_1, \cdots, t_n), G = S_n$. Then, $G \leq AutK$.*

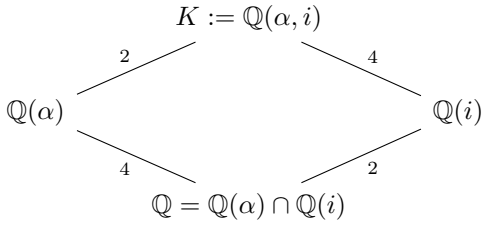


Figure 20: Lattice for K

Consider K/K^G. For $1 \leq m \leq n, s_m(t_1, \cdots, t_n) = \sum_{1 \leq i_1 < \cdots < i_m \leq n} t_{i_1} \cdots t_{i_m} \in K^G$, called (elementary) symmetric polynomial. s_m is a coefficient of $(-1)^m t^{n-m}$ in $\prod_{i=1}^n (x - t_i) \in K^G[x]$. Hence $k(s_1, \cdots, s_n) \subset K^G$. Also, $K/k(s_1, \cdots, s_n)$ is normal since K is a splitting field of $\prod_{i=1}^n (x - t_i)$ over $k(s_1, \cdots, s_n)$. Also K/K^G is Galois and $G(K/K^G) = G$ by Artin's theorem Also, from $\deg f = n$,

$$[K : k(s_1, \cdots, s_n)] \leq n! = |G|.$$

Since $[K : K^G] = |G| = n!$, $K^G = k(s_1, \cdots, s_n)$.

Example 4.2.5 (Example 5, $\mathbb{C}$ is algebraically closed. Not in notes.)**.** *First, for any $a, b \in \mathbb{R}$, $a + bi$ has square roots in $\mathbb{R}(i)$. (Tedious calculation.)*

Next, every finite extension of $\mathbb{R}$ is separable. Since every polynomial in $\mathbb{R}[x]$ having odd degrees must have a root in $\mathbb{R}$, we should consider polynomial of order 2.

Let K be union of all possible finite extension of $\mathbb{R}(i)$. Then, K is algebraic separable extension, and for any element $\alpha \in K$, $[\mathbb{R}(i)(\alpha) : \mathbb{R}(i)] \leq 2$, since every odd polynomial has a root in $\mathbb{R}$, and every even polynomial can be reduced as quadratic polynomial using quadratic formula. Hence, using lemma 1.7, $[K : \mathbb{R}(i)] \leq 2$, and $K/\mathbb{R}(i)$ is finite. Also, $K/\mathbb{R}$ is Galois since it is normal and separable.

Now, it suffices to show that $K = \mathbb{R}(i)$. Let $G = G(K/\mathbb{R})$, $H \leq G$ be a 2-Sylow subgroup of G. Let $F = K^H$. Since $|G/H|$ is odd, $[F : \mathbb{R}]$ is also odd. By the primitive element theorem, $\exists \alpha \in F$ such that $F = \mathbb{R}(\alpha)$. Then $irr(\alpha, \mathbb{R})$ has degree 1, since every odd degree polynomial has solution on $\mathbb{R}$. Thus $G = H$. G is a 2-group. Thus, $K/\mathbb{R}(i)$ is Galois, by Artin's theorem.

Let $G_1 = G(K/\mathbb{R}(i))$. Since G_1 is a p-group, $p = 2$, G_1 should have a subgroup G_2 with index 2, if G_1 is not trivial, by Sylow's theorem. Let $E = K^{G_2}$. Then, $[E : \mathbb{R}(i)] = 2$. However, $\mathbb{R}(i)$ has no quadratic extension since it has all roots of quadratic polynomial. Hence G_1 is trivial, thus $K = \mathbb{R}(i)$.

Example 4.2.6 (Example 6)**.** *Let p be prime and let $f(x)$ be irreducible in $\mathbb{Q}[x]$ of degree p. Suppose $f(x)$ has exactly two complex roots. Let $G = G(f)$. We may assume that $G < S_p$. Let $\tau \in G$ such that $\tau(a) = \bar{a}$, conjugation. Then, $\tau = (1 \quad 2)$, and $p||G|$, since* $\deg f = p$*. Then,*

$$\exists \sigma \in G s.t. |\sigma| = p,$$

i.e., σ is a p-cycle. Since $\sigma, \tau \in G$, and they can generate S_p, $G = S_p$.

So conclusion; Let $f(X)$ be an irreducible polynomial with rational coefficients and of degree p prime. If f has precisely two nonreal roots in the complex numbers, then the Galois group of f is S_p.

Example 4.2.7 (Example 7 - not in notes)**.** *Let $f(X) \in \mathbb{Z}[X]$ be a polynomial with integral coefficients, and leading coefficient 1. Let p be a prime number. Let $\bar{f}(X) = f(X) \bmod p$ be the polynomial obtained by reducing the coefficients mod p. Assume that f has no multiple roots in an algebraic closure of F_p. Then there exists a bijection*

$$(\alpha_1, \cdots, \alpha_n) \mapsto (\bar{\alpha_1}, \cdots, \bar{\alpha_n})$$

of the roots of f onto those of $\bar{f}$ and an embedding of the $G(\bar{f}) \hookrightarrow G(f)$. which gives an isomorphism of the action of those groups on the set of roots.

For example, $f(x) = x^5 - x - 1 \in \mathbb{Z}[x]$. By mod $p = 5$, it is irreducible. By mod 2, $f(x) = (x^2 + x + 1)(x^3 + x^2 + 1)$, so that $G(f)$ contain one 5-cycle and a product of 2-cycle and 3-cycle. Since the third power of the latter element has order 2, so $G(f) = S_5$.

4.3 Roots of unity

For $n \geq 1$, ξ is a primitive n-th root of unity in k^a if $< \xi >= \{\alpha : \alpha^n = 1\} \subset (k^a)^*$. Consider $k(\xi)/k$ when (char $k, n) = 1$. Then, $k(\xi)/k$ is Galois, since $x^n - 1$ is separable on $k[x]$ and it is the splitting field of $x^n - 1$. When $k = \mathbb{Q}$, $\mathbb{Q}(\xi)/\mathbb{Q}$ is called as n-th cyclotomic extension of $\mathbb{Q}$.

Theorem 4.3.1 (Theorem 3.1)**.** *Under the above hypothesis, $[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n)$, $G(\mathbb{Q}(\xi)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.*

Proof. Given $\sigma \in G := G(\mathbb{Q}(\xi)/\mathbb{Q})$, $\sigma(\xi) = \xi^i$ for some $i \in (\mathbb{Z}/n\mathbb{Z})^*$. Then the map $G \to (\mathbb{Z}/n\mathbb{Z})^*$ by $\sigma \mapsto i(\sigma)$ where $i(\sigma) = i$, is well defined. The map is a group homomorphism and injective, by checking some tedious calculation. Hence

$$|G| = [\mathbb{Q}(\xi) : \mathbb{Q}] | \varphi(n).$$

Put $f(x) = irr(\xi, \mathbb{Q})$. Now I claim that

$$f(x) = \prod_{1 \leq m < n, (m,n)=1} (x - \xi^m).$$

To show this claim, it is enough to show that ξ^p is a root of $f(x)$ for each prime $p \not| n$. Suppose not, ξ^p is not a root of $f(x)$. Then, $x^n - 1 = f(x)g(x)$ for some $g(x) \in \mathbb{Z}[x]$, and ξ^p is root of $g(x)$, since it is root of $x^n - 1$. Hence ξ is a root of $g(x^p)$. Now, since $f(x)$ is irreducible polynomial of ξ, $g(x^p) = f(x)h(x)$ for some $h(x) \in \mathbb{Z}[x]$. By reducing the coefficients to $\mathbb{Z}/p\mathbb{Z}$,

$$\bar{g}(x^p) = \bar{g}(x)^p = \bar{f}(x)\bar{h}(x) \text{ in } \mathbb{Z}/p\mathbb{Z}[x].$$

From above, we can conclude that $\bar{f}, \bar{g}$ has common factor. Hence,

$$x^n - \bar{1} = \bar{f}(x)\bar{g}(x) \in \mathbb{Z}/p\mathbb{Z}[x].$$

and $x^n - \bar{1}$ have multiple roots in $\mathbb{Z}/p\mathbb{Z}$. However, by differentiation and (char$k, n) = 1$, we know that it cannot have multiple roots, contradiction. Hence the claim holds, so $[\mathbb{Q}(\xi) : \mathbb{Q}] := \deg f(x) = \varphi(n)$, thus $G(\mathbb{Q}(\xi)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$. □

Corollary 4.3.2 (Corollary 3.2)**.** *If $(m, n) = 1$, and ξ_n, ξ_m are primitive n, mth root of 1, then $\mathbb{Q}(\xi_n) \cap \mathbb{Q}(\xi_m) = \mathbb{Q}$.*

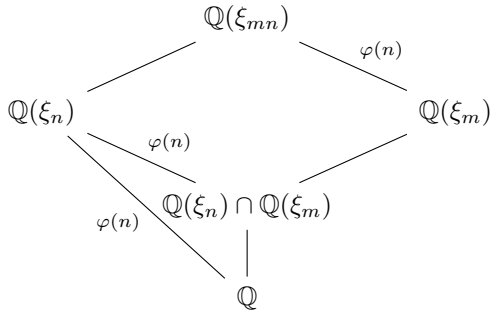


Figure 21: Structure of $\mathbb{Q}(\xi_{mn})$

Proof. If $(m,n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$ by homework. Also note that $\mathbb{Q}(\xi_m)\mathbb{Q}(\xi_n) = \mathbb{Q}(\xi_{mn})$, since $\xi_m\xi_n$ is primitive mn-th root of unity and ξ_m, ξ_n both are contained in $\mathbb{Q}(\xi_{mn})$. Consider below diagram;

From distinguishness of finite extension, $[\mathbb{Q}(\xi_{mn}) : \mathbb{Q}(\xi_m)] = [\mathbb{Q}(\xi_n) : \mathbb{Q}(\xi_n) \cap \mathbb{Q}(\xi_m)] = \varphi(n) = [\mathbb{Q}(\xi_n) : \mathbb{Q}]$. This implies $\mathbb{Q}(\xi_m) \cap \mathbb{Q}(\xi_n) = \mathbb{Q}$. □

Definition 4.3.3. *For $n \geq 1$, let ξ is primitive n-th root of unity. Then, define*

$$\Phi_n(x) := \prod_{1 \leq m \leq n, (m,n)=1} (x - \xi^m)$$

be n-th cyclotomic polynomial.

Remark 4.3.4. *Below facts were proven in exercise problems.*

1. $x^n - 1 = \prod_{d|n} \Phi_d(x)$. *If $n = p$, then* $\Phi_p(x) = x^{p-1} + \cdots + x + 1$.
2. *Let p be prime. Then,* $\Phi_{pn}(x) = \begin{cases} \frac{\Phi_n(x^p)}{\Phi_n(x)} & \text{if } p \nmid n \\ \Phi_n(x^p) & \text{if } p|n. \end{cases}$
3. *For $n \geq 1$,* $\Phi_n(x) = \prod_{d|n}(x^{n/d} - 1)^{\mu(d)}$ *where μ is the Möbius function such that*

$$\mu(d) = \begin{cases} 1 \text{ if } d = 1 \\ (-1)^r \text{ if } d > 2, d = p_1 \cdots p_r, \text{ squarefree} \\ 0 \text{ otherwise.} \end{cases}$$

Proof. 1. For all $d|n$, $\Phi_d(x)|x^n - 1$ and $\sum_{d|n} \varphi(d) = n$.

2. Note that if $p \nmid n$,

$$\deg(\Phi_n(x)\Phi_{pn}(x)) = \varphi(n) + \varphi(pn) = p\varphi(n) = \deg(\Phi_n(x^p)).$$

To prove this, first show that it hold for n is also prime. If this holds for n is prime, then it holds for $n = p^n$. Then it holds for any n, by induction. First of all, if $n = q$, some prime, then

$$x^{pq} - 1 = \Phi_1(x)\Phi_p(x)\Phi_q(x)\Phi_{pq}(x).$$

Also, by thinking x^p as one variable,

$$(x^p)^q - 1 = \Phi_1(x^p)\Phi_q(x^p).$$

Since $\Phi_1(x^p) = x^p - 1 = \Phi_1(x)\Phi_p(x)$, this formula holds. Suppose it holds for $n = q^{k-1}$ where k is some natural number. Then,

$$(x^p)^{q^k} - 1 = \Phi_1(x^p)\Phi_q(x^p)\cdots\Phi_{q^{k-1}}(x^p)\Phi_{q^k}(x^p).$$

By inductive hypothesis, $\Phi_1(x^p) = \Phi_1(x)\Phi_p(x)$ and $\Phi_{q^i}(x^p) = \Phi_{pq^i}(x)\Phi_{q^i}(x)$. And,

$$x^{pq^k} - 1 = (\Phi_1(x)\Phi_p(x)) \cdot \left(\prod_{i=1}^{k-1} \left(\Phi_{pq^i}(x)\Phi_{q^i}(x)\right)\right) \cdot \Phi_{pq^k}(x)\Phi_{q^k}(x).$$

So by removing each terms, we get the conclusion that this statement holds for $n = q^k$. Now suppose $n = mq^k$ with inductive hypothesis that it holds for any divisor of m and holds for k, where $k \in \mathbb{N}$. Then, using the same argument, it holds for n.

If $p|n$, then $n = p^k m$ for some $k, m \in \mathbb{N}$, hence

$$\deg(\Phi_{pn}(x)) = \varphi(p^{k+1}m) = \varphi(p^{k+1})\varphi(m) = p^k(p-1)\varphi(m) = p\varphi(p^k)\varphi(m) = p\varphi(n) = \deg(\Phi_n(x^p)).$$

Thus it suffices to show that $\Phi_n(x^p)|\Phi_{pn}(x)$ or vice versa. Let α be arbitrary solution of $\Phi_{pn}(x) = 0$. Then, $\alpha^{pn} = 1$ but $\alpha^k \neq 1$ if $k < np$. Thus, $(\alpha^p)^n = 1$ and $(\alpha^p)^m \neq 1$ if $m < n$. So α^p is a primitive n-th root of unity, hence α is also solution of $\Phi_n(x^p)$. Thus, two polynomial, having the same degreee, share the same roots. Therefore, they are the same polynomial.

3. Note that Möbius inversion formular is this; for some $F, G : \mathbb{Z} \to X$,

$$F(n) = \sum_{d|n} G(d) \implies G(n) = \sum_{d|n} \mu(d)F(n/d).$$

Now let $F(n) = \log(x^n - 1)$, $G(n) = \log \Phi_n(x)$. Then,

$$F(n) = \log(x^n - 1) = \sum_{d|n} \log \Phi_d(x) = \sum_{d|n} G(d).$$

Thus,

$$\log \Phi_n(x) = \sum_{d|n} \mu(d) \log(x^{n/d} - 1),$$

from the formula. By taking exponential, we get desired result.

□

4.4 Linear independence of characters

Definition 4.4.1. *Let K be a field and let G be a monoid (Unlike group, inverse may not exists).*

1. *A map $\chi : G \to K^*$ is called a character of G if $\chi(g_1g_2) = \chi(g_1)\chi(g_2)$ for any $g_1, g_2 \in G$.*
2. *Let $\{\chi_1, \cdots, \chi_n\}$ be a set of characters. $\{\chi_1, \cdots, \chi_n\}$ is linearly independent if*

$$\sum_{i=1}^{n} a_i\chi_i = 0 \text{ for some } a_i \in K \implies a_1 = \cdots a_n = 0.$$

Example 4.4.2. *Let $\sigma : K \to K^a$ be an embedding, $G = K^*$. Then, σ is a character of G, since σ preserves product as an embedding.*

Theorem 4.4.3 (Theorem 4.1, Artin)**.** *Let $X := \{\chi_1, \cdots, \chi_n\}$ be a set of distinct characters. Then, X is linearly independent.*

Proof. Suppose that $a_1\chi_1 + \cdots + a_n\chi_n = 0$ for some $a_i \in K$. Use induction on n. If $n = 1$, clear. Assume any non-empty proper subset of X is linearly independent. Then, $\exists z \in G$ such that $\chi_1(z) \neq \chi_2(z)$. Then, for any $g \in G$,

$$\begin{aligned}
& a_1\chi_1(zg) + \cdots + a_n\chi_n(zg) && = 0 \\
\implies \quad & a_1\chi_1(z)\chi_1(g) + \cdots + a_n\chi_n(z)\chi_n(g) && = 0 \\
\implies \quad & a_1\chi_1(g) + a_2\tfrac{\chi_2(z)}{\chi_1(z)}\chi_2(g) + \cdots + a_n\tfrac{\chi_n(z)}{\chi_1(z)}\chi_n(g) && = 0 \\
\implies \quad & a_2\left(1 - \tfrac{\chi_2(z)}{\chi_1(z)}\right)\chi_2(g) + \cdots + a_n\left(1 - \tfrac{\chi_n(z)}{\chi_1(z)}\right)\chi_n(g) && = 0
\end{aligned}$$

From inductive hypothesis with the fact that $1 - \frac{\chi_2(z)}{\chi_1(z)} \neq 0$, $a_2 = 0$. Now, by inductive hypothesis for $X - \{\chi_2\}$, $a_1 = a_3 = \cdots = a_n = 0$. □

Corollary 4.4.4. *Let $\alpha_1, \cdots, \alpha_n$ be distinct elements in K^*. If $a_1\alpha_1^k + \cdots a_n\alpha_n^k = 0$ for all $k \geq 0$, then, $a_1 = \cdots = a_n = 0$.*

Proof. Put $\chi_i(k) = \alpha_i^k$. Then, $\chi_i : \mathbb{Z}_{\geq 0} \to K^*$ is character. □

4.5 The norm and trace

Let E/k be finite with $r = [E : k]_s$ and let $\{\sigma_1, \cdots, \sigma_r\}$ be the set of distinct embeddings of E into k^a. For $\alpha \in E$, define

$$Tr_{E/k}(\alpha) := [E : k]_i \sum_{i=1}^{r} \sigma_i(\alpha), N_{E/k}(\alpha) := \left(\prod_{i=1}^{r} \sigma_i(\alpha)\right)^{[E:k]_i}.$$

Remark 4.5.1. *If E/k is separable, then*

$$Tr_{E/k}(\alpha) = \sum_{i=1}^{r} \sigma_i(\alpha), N_{E/k}(\alpha) = \prod_{i=1}^{r} \sigma_i(\alpha).$$

If E/k is Galois then,

$$Tr_{E/k}(\alpha) = \sum_{\sigma \in G(E/k)} \sigma_i(\alpha), N_{E/k}(\alpha) = \prod_{\sigma \in G(E/k)} \sigma_i(\alpha).$$

Theorem 4.5.2. *Let E/k be finite. Then,*

1. *$N_{E/k}(\alpha), Tr_{E/k}(\alpha) \in K$.*
2. *$N_{E/k} : E^* \to K^*$, $Tr_{E/k} : E \to K$ are group homomorphism, multiplicative and additive resp.*
3. *For $k \subset F \subset E$, $N_{E/k} = N_{F/k} \circ N_{E/F}$, $Tr_{E/k} = Tr_{F/k} \circ Tr_{E/F}$.*

Proof. Assume char $k = p$ and $[E : k]_i = p^\mu$ for some $\mu \geq 0$. Given $\alpha \in E$, α^{p^ν} is separable over k for some $0 \leq \nu \leq \mu$. Thus, α^{p^μ} is separable over k. Then, for an embedding of E into k^a, called σ,

$$\sigma\left(\prod_{i=1}^{r} \sigma_i(\alpha^{p^\mu})\right) = \prod_{i=1}^{r} \sigma_i(\alpha^{p^\mu}) \in K.$$

Since $\prod_{i=1}^r \sigma_i(\alpha^{p^\mu}) = (\prod_{i=1}^r \sigma_i(\alpha))^{p^\mu} = N_{E/k}(\alpha)$, $N_{E/k}(\alpha) \in K$.
In case of trace, if $[E : k]_i > 1$, the statement trivially holds. Otherwise, α is separable, so that

$$\sigma\left(\sum_{i=1}^{r} \sigma_i(\alpha)\right) = \sum_{i=1}^{r} \sigma_i(\alpha) = Tr_{E/k}(\alpha) \in K.$$

If char $k = 0$, the proof is similar.

For the second part, just check homomorphism.

For the third part, let F be intermediate field. Consider $\{\varphi_1, \cdots \varphi_p\}$ and $\{\tau_1, \cdots, \tau_q\}$ are distinct embedding of E in k^a over F, of F in k^a over k respectively. (Without loss of genrality, by copy of field argument, we can think that $E \subset k^a$.) Then, if σ is an embedding of E in k^a over k, then $\sigma|_F = \tau_j$ for some $j \in [q]$, thus $\tau_j^{-1}\sigma$ fixes F. Hence, $\tau_j^{-1}\sigma = \varphi_i$ for some i. Thus, $\{\varphi_i\tau_j\}_{i\in[p],j\in[q]}$ are all distinct embeddings of E in k^a over k. Thus, we get desired conclusion. □

Example 4.5.3. *Consider the case when $E/k(\alpha)/k$ is finite and $k(\alpha)/k$ is separable and $E/k(\alpha)$ is inseparable, with*

$$f(x) = irr(\alpha, k) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0.$$

Since any embeddings of E into k^a over $k(\alpha)$ fixes α,

$$N_{E/k(\alpha)}(\alpha) = \prod_{i}^{[E:k(\alpha)]_s} \sigma_i(\alpha)^{[E:k(\alpha)]_i} = \alpha^{[E:k(\alpha)]_s[E:k(\alpha)]_i} = \alpha^{[E:k(\alpha)]}.$$

Also,

$$Tr_{E/k(\alpha)}(\alpha) = [E : k(\alpha)]_i \sum_{i}^{[E:k(\alpha)]_s} \sigma_i(\alpha) = [E : k(\alpha)]_s[E : k(\alpha)]_i\alpha = [E : k(\alpha)]\alpha.$$

Thus,

$$N_{E/k} = N_{k(\alpha)/k} \circ N_{E/k(\alpha)}(\alpha) = N_{k(\alpha)/k}(\alpha^{[E:k(\alpha)]}) = N_{k(\alpha)/k}(\alpha)^{[E:k(\alpha)]} = ((-1)^d a_0)^{[E:k(\alpha)]}.$$

and

$$Tr_{E/k} = Tr_{k(\alpha)/k} \circ Tr_{E/k(\alpha)}(\alpha) = Tr_{k(\alpha)/k}([E : k(\alpha)]\alpha) = [E : k(\alpha)](-a_{n-1}).$$

4.6 Cyclic extensions

Let K/k be finite abelian, i.e., $G(K/k)$ is a finite abelian group, such that

$$G(K/k) \cong G_1 \times \cdots \times G_r$$

where G_i is cyclic.

Theorem 4.6.1 (Hilbert Theorem 90)**.** *Let K/k be cyclic with $G(K/k) =< \sigma >$ of order n. Then, For $\beta \in K$,*

$$N_{K/k}(\beta) = 1 \iff \beta = \frac{\alpha}{\sigma\alpha} \text{ for some } \alpha \in K.$$

Proof. If $\beta = \frac{\alpha}{\sigma\alpha}$,

$$N(\beta) = N(\alpha/\sigma\alpha) = N(\alpha)/N(\sigma\alpha) = 1.$$

Suppose $\beta \in K$ with $N(\beta) = 1$. Note that $G(K/k)$ is character, by thinking $G = K^*$. Then, define τ as

$$\tau := 1 + \sum_{i=1}^{n-1} \left(\left(\prod_{j=0}^{i-1} \sigma^j(\beta) \right) \sigma^i \right) = 1 + \beta\sigma + \beta\sigma(\beta)\sigma^2 + \cdots + \beta\sigma(\beta)\sigma^2(\beta)\cdots\sigma^{n-2}(\beta)\sigma^{n-1}.$$

By Artin's theorem on character, $\tau \neq 0$. Hence $\exists\theta \in K^*$ such that $\tau(\theta) \neq 0$. Also note that

$$\sigma(\tau) = \sigma + \sum_{i=2}^{n} \left(\left(\prod_{j=1}^{i-1} \sigma^j(\beta) \right) \sigma^i \right) = \sigma + \sigma(\beta)\sigma^2 + \sigma(\beta)\sigma^2(\beta)\sigma^3 + \cdots + \sigma(\beta)\sigma^2(\beta)\sigma^3(\beta)\cdots\sigma^{n-1}(\beta)\sigma^n.$$

Thus,

$$\beta\sigma(\alpha) = \beta\sigma(\theta) + \sum_{i=2}^{n} \left(\left(\prod_{j=0}^{i-1} \theta^j(\beta) \right) \sigma^i(\theta) \right) = \sum_{i=1}^{n-1} \left(\left(\prod_{j=0}^{i-1} \sigma^j(\beta) \right) \sigma^i(\theta) \right) + N_{K/k}(\beta)\sigma^n(\theta).$$

Since $N_{K/k}(\beta) = 1, \sigma^n = 1$,

$$\beta\sigma(\alpha) = \theta + \sum_{i=1}^{n} \left(\left(\prod_{j=0}^{i-1} \sigma^j(\beta) \right) \sigma^i(\theta) \right) = \alpha.$$

Thus, $\beta = \frac{\alpha}{\sigma(\alpha)}$ □

Example 4.6.2. *Let $\sigma \in G(\mathbb{Q}(i)/\mathbb{Q})$ be complex conjugation, and $z = a + bi \in \mathbb{Q}(i)$. Then, $N_{\mathbb{Q}(i)/\mathbb{Q}} = z\sigma(z) = a^2 + b^2$. If $a^2 + b^2 = 1$, then $z = \frac{w}{\sigma(w)} = \frac{c+di}{c-di} = \frac{c^2-d^2}{c^2+d^2} + \frac{2cd}{c^2+d^2}i$, where $c, d \in \mathbb{Z}$. Hence, $(c^2 - d^2)^2 + (2cd)^2 = (c^2 + d^2)^2$.*

Theorem 4.6.3 (Theorem 6.2)**.** *Let $n \geq 1$, char $k \nmid n$. Suppose that k has a primitive nth root of unity, say ξ. Then,*

1. *If K/k is cyclic of degree n, then $\exists\alpha \in K$ such that $K = k(\alpha)$ and α is a root of $x^n - a$ for some $a \in k$.*
2. *Let $a \in k$, and let α be a root of $x^n - a$. Then, $k(\alpha)/k$ is cyclic of degree $d|n$ and $\alpha^d \in k$.*

Proof. For the first part, let $G(K/k) =< \sigma >$. Then, $N_{K/k}(\xi^{-1}) = (\xi^{-1})^n = 1$, since $\xi \in k$ so that ξ is fixed by any σ. Thus, by Hilberth Theorem 90, $\xi^{-1} = \alpha/\sigma(\alpha)$ for some α. Hence, $\sigma(\alpha) = \xi\alpha$. Thus, $\sigma^i(\alpha) = \xi^i\alpha$ for $0 \leq i \leq n$, are mutually distinct. Thus, $\xi^i\alpha$ are n distinct conjugation of α over k. Therefore,

$$n \leq [k(\alpha) : k] \leq [K : k] = n.$$

Thus, $K = k(\alpha)$. And, $N_{K/k(\alpha)} = \xi^{\frac{n(n-1)}{2}}\alpha^n \in k \implies \alpha^n \in k$. Thus, $\alpha^n \in k$, and since $\xi^i\alpha$ are all roots of $x^n - \alpha^n = 0$, we are done.

For the second part, note that α is separable over k, since $x^n - a$ has all distinct roots. Thus, $\{\xi^i\alpha : 0 \leq i < n\}$ is the set of roots of $x^n - a$. By given assumption that $\xi \in k$, $k(\alpha)$ is the splitting field of $x^n - a$. Thus, $k(\alpha)/k$ is Galois. Let $G = G(k(\alpha)/k)$ and $H = \{c : c \in k, c^n = 1\} \subset k^*$. Call H be a group of cyclic of order n. (Check that group axiom holds.) Given $\sigma \in G$, $\sigma(\alpha) = \xi^i\alpha$ for some i. Write $\xi^i = \xi_\sigma$. Then, the map $G \to H$ by $\sigma \mapsto \xi_\sigma$ is an injective group homomorphism. Hence, G is cyclic of degree $d|n$ for some d. □

Theorem 4.6.4 (Hilbert Theorem 90 Additive form)**.** *Let K/k be cyclic with $G(K/k) =< \sigma >$ of order n. For $\beta \in K$,*

$$Tr_{K/k}(\beta) = 0 \iff \beta = \alpha - \sigma(\alpha)$$

for some $\alpha \in K$.

Proof. From right to left, obvious. Assume that $Tr_{K/k}(\beta) = 0$. Then, by linear independence of characters, $\exists\theta \in K$ such that $Tr_{K/k}(\theta) \neq 0$. Put

$$\alpha = \frac{1}{Tr(\theta)}\left[\sum_{i=0}^{n-1}\left(\sum_{j=0}^{i-1}\sigma^j(\beta)\right)\sigma^i(\theta)\right] = \frac{1}{Tr(\theta)}\left[\beta\sigma(\theta) + (\beta + \sigma(\beta))\sigma^2(\theta) + \cdots(\beta + \sigma(\beta) + \cdots + \sigma^{n-2}(\beta))\sigma^{n-1}(\theta)\right].$$

Note that

$$\beta = \frac{1}{Tr(\theta)}\left(\sum_{i=0}^{n-1}\beta\sigma^i(\theta)\right)$$

Thus,

$$\beta + \sigma(\alpha) = \frac{1}{Tr(\theta)}\left[\sum_{i=0}^{n-1}\left(\sum_{j=0}^{i-1}\sigma^j(\beta)\right)\sigma^i(\theta)\right] = \alpha.$$

□

Theorem 4.6.5 (Theorem 6.4, Artin-Schreier)**.** *Let k be a field of characteristic p. Then,*

1. *If K/k cyclic of degree p, then $\exists\alpha \in K$ such that $K = k(\alpha)$ and α is a root of $x^p - x - a$ for some $a \in k$.*
2. *For $a \in k$, the polynomial $x^p - x - a$ satisfies are of the following.*
   (a) *$x^p - x - a$ has a root in k. In this case, it splits in $k[x]$.*
   (b) *$x^p - x - a$ is irreducible. In this case, if α is a root of $x^p - x - a$, then $k(\alpha)/k$ is cyclic of degree p.*

Proof. 1. Assume that $G(K/k) =< \sigma >$. Since $Tr_{K/k}(-1) = p \cdot (-1) = 0$ since char $k = p$, $-1 = \alpha - \sigma(\alpha)$ for some $\alpha \in K$ by Hilbert Theorem 90's additive form. Thus, $\sigma(\alpha) = \alpha + 1$, $\sigma^i(\alpha) = \alpha + i$ for $0 \leq i < p$. Hence $K = k(\alpha)$. Also, $\sigma(\alpha^p - \alpha) = (\alpha+1)^p - (\alpha+1) = \alpha^p - \alpha$. Hence $a = \alpha^p - \alpha \in k$.

2. Let α be a root of $x^p - x - a$ in k^a. Then, $\{\alpha + i : 0 \leq i < p\}$ is the set of roots of $x^p - x - a$. If $\alpha \in k$, then $\alpha + i \in k$ for all i. Suppose that $\alpha \notin k$, (i.e., k has no roots in $x^p - x - a$)

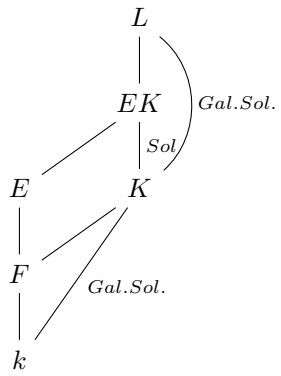


Figure 22: Solvability in subextensions implies that of all extensions

and $f(x)$ is reducible. Then, $f(x) = g(x)h(x)$ for some $g(x), h(x) \in k[x]$ of degree ≥ 1. Note that

$$f(x) = \prod_{i=1}^{p}(x - \alpha - i) \in K[x]$$

Thus, g is a product over certain i. If $r = \deg g$, then the coefficient of x^{r-1} term of g is sum of terms $-(\alpha+i)$, so that it can be expressed as $-r\alpha+j$ for some integer j. But $r \neq 0$ implies $r\alpha \in k$, which implies $\alpha \in k$, contradiction. Hence $f(x)$ is irreducible. Note that α is separable and $k(\alpha)$ is the splitting field of $x^p - x - a$. Hence $k(\alpha)/k$ is cyclic of degree p. □

4.7 Solvable and Radical extensions

Definition 4.7.1. *Let E/k be finite and separable. E/k is solvable if $\exists L/k$, finite and Galois such that $L \supset E$ and $G(L/k)$ is solvable.*

Remark 4.7.2. *One may replace L with the smallest Galois extension K of k containing E, with $G(K/k)$ is solvable. In this case, $G(L/k) \twoheadrightarrow G(K/k)$ surjective.*

Remark and definition is equivalent; if remark holds, then definition holds by taking $L = K$. If definition holds, $G(L/K)$ is normal for $G(L/k)$, and $G(K/k) \cong G(L/k)/G(L/K)$ is also solvable by property of solvability.

Proposition 4.7.3 (Proposition 7.1)**.** *Solvable extensions form a distinguished class.*

Proof. Suppose E/k be solvable. Then, $\exists K/k$ Galois, with solvable $G(K/k)$. Thus, KF/F is Galois, since lifting of Galois extension is also Galois. Hence $G(KF/F) \xrightarrow{\cong} G(K/K \cap F) < G(K/k)$ by theorem 1.12 in chpater VI. Hence $G(KF/F)$ is solvable, because subgroup of solvable group is solvable, so that $G(KF/F)$ is solvable. Since $EF \subset KF$, $G(EF/F)$ is solvable.

For the second part, let $k \subset F \subset E \subset K$. If E/k is solvable, then F/k, E/F are solvable by just taking K and match them with definition. Now suppose E/F, F/k are solvable. (See figure 5.) Since F/k is solvable, $\exists K/k$ is Galois, solvable. Thus, $\exists L/K$ is Galois, solvable. Let σ be an embedding of L into k^a. Then, $\sigma(K) = K$. So, $\sigma L/K$ is also Galois and solvable. Put $M = \sigma_1 L \cdots \sigma_n L$ where $\sigma_1, \cdots, \sigma_n$ are all distinct embeddings of L into k^a. Then, M/k is Galois by thoerem 1.14. And since K/k is Galois, M/K is also Galois, by Artin's theorem. Note that

1. $G(M/K) \subset G(\sigma_1 L/K) \times \cdots G(\sigma_n L/K)$ by corollary 1.16,
2. $G(M/k)/G(M/K) \cong G(K/k)$ by Artin's theorem.

Thus, $G(M/K)$ is solvable, since quotient group is solvable if and only if its original group is solvable. Thus E/k is solvable.

□

Definition 4.7.4. *Let F/k be finite and separable. F/k is called **solvable by radicals** if $\exists$ a sequence of finite extensions $k = E_0 \subset E_1 \subset \cdots E_m = E$ such that $E \supset F$ and E_{i+1} is obtained from E_i by adjoining one of the followings:*

1. *a root of unity*
2. *a root of $x^n - a$ where $a \in E_i$ and chark $\not| n$.*
3. *a root of $x^p - x - a$ where $a \in E_i$ if char $k = p$.*

Remark 4.7.5. *The extensions which are solvable by radicals form a distinguished class. (Subextensions are obvious. For lifting, adjoin lifting field for each E_i.)*

Remark 4.7.6. *Let char $k \not| n$, and let ξ be a primitive nth root of unity. Then, $k(\xi)/k$ is abelian Galois and $[k(\xi) : k] | \varphi(n)$.*

Proof. First comes from that $\varphi : G(k(\xi)/k) \to (\mathbb{Z}/\mathbb{Z}_n)^*$ by $\xi \mapsto a_\sigma \bmod n$ where a_σ is integer such that $\xi^{a_\sigma} = \sigma(\xi)$ is injective homomorphism. Let $\sigma, \tau \in G(k(\xi)/k)$. Then,

$$(\sigma\tau)(\xi) = \sigma(\tau(\xi)) = \sigma(\xi^{a_\tau} = \xi^{a_\sigma a_\tau}.$$

Also, since $(\sigma\tau)(\xi) = \xi^{a_{\sigma\tau}}$, $a_{\sigma\tau} \cong a_\sigma a_\tau \bmod n$. Hence φ is a homomorphism. Also, if $\sigma \in ker\varphi$, then $a_\sigma = 1$, so a_σ fix ξ, hence it fixes all element of $k(\xi)$. Thus, $\sigma = id \in G(k(\xi)/k)$. Thus it is injective.

The second is comes from $|(\mathbb{Z}/\mathbb{Z}_n)^*| = \varphi(n)$. □

Theorem 4.7.7. *Let E/k be finite separable. E/k is solvable by radicals $\iff$ E/k is solvable.*

Proof. Assume that E/k is solvable. Then, $\exists K/k$ is Galois, solvable such that $K \supset E$. Put

$$m = \prod_{\substack{q | [K:k] \\ q \text{ is prime} \\ q \neq \text{char } k}} q.$$

Let ξ be a primitive mth root of unity, and $F = k(\xi)$. Note that KF/F is Galois and solvable, by distinguishness of solvability and lifting property of Galois extensions. Thus, there exists tower of groups such that

$$\{e\} = G_0 < G_1 < \cdots < G_n = G(KF/F)$$

such that $G_i \triangleleft G_{i+1}$ and G_{i+1}/G_i is cyclic of prime order, by solvbaility of $G(KF/F)$. Then, we have

$$F = (KF)^{G_n} < (KF)^{G_{n-1}} < \cdots < (KF)^{G_0} = KF$$

where $(KF)^{G_i}/(KF)^{G_{i+1}}$ are type 2 or 3 by theorem 6.2. and 6.4. Thus, KF/F is solvable by radicals. Since F/k is also solvable by radical by definition, KF/k is solvable by radicals. Hence E/k is solvable by radicals.

Conversely, assume that E/k is solvable by radicals. Let σ be an embedding of E into k^a. Then, $\sigma E/k$ is solvable by radicals, by putting tower of fields for E on σ. Let K be the smallest Galois extension of K containing E. So $K = \sigma_1 E \cdots \sigma_n E$ for all distinct embeddings σ_i, $i \in [n]$. Then, K/k is also solvable by radicals, since it is compositum of all solvable by radical extensions. Put

$$m = \prod_{\substack{q|[K:k] \\ q \text{ is prime} \\ q \neq \text{char } k}} q.$$

Let ξ be a primitive mth root of unity, and $F = k(\xi)$. Then, F/k is solvable since it is abelian by above remark, and the fact that all abelian group is solvable. Note that KF/F is solvable by radical since it is lifting from K/k, which is solvable by radical. And KF/F is Galois since K/k is Galois. Thus, we have some tower of fields such that

$$F = L_0 \subset L_1 \subset \cdots \subset L_l$$

where $L_l \supset KF$ and L_{i+1}/L_i is of type 1,2, or 3. If L_{i+1}/L_i is of type 1, then it is abelian extension, by remark. If L_{i+1}/L_i is of type 2 or 3, then it is cyclic extension, by theorem 6.2 or 6.4. Thus, $Gal(L_l/F)$ is solvable. Since $Gal(KF/F)$ is homomorphic image of $Gal(L_l/F)$, $Gal(KF/F)$ is solvable. □

Remark 4.7.8. *Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial, and $G = Gal(f)$.*

1. *If $\deg f = 3$ or 4, then $G \leq S_3$ or S_4, with tower $\{e\} < A_3 < S_4$ or $\{e\} < V_4 < A_4 < S_4$ where V_4 is klein four group. Thus, the splitting field of f is solvable by radical.*
2. *If $\deg f = 5$, then $G \leq S_5$. It would be solvable or not. For example, If $Gal(f) = S_5$, then it is not solvable by radicals.*

For example, $f(x) = 2x^5 - 5x^4 + 5$. Then, $f'(x) = 10x^3(x-2)$. It has two nonreal roots.

Example 4.7.9. *If $A = \{t_i\}_{i=1}^n$ is a set of indeterminates, $B = \{s_i\}_{i=1}^n$ is a set of elementary symmetric polynomials from A, and $E = k(A)$, $K = k(B)$ for some field k. Then, $G(E/k) \cong S_n$, as shown above.*

Example 4.7.10. *Let $f(x) = x^4 - 4x^2 + 2 = (x^2 - (2-\sqrt{2}))(x^2 - (2+\sqrt{2}))$. Then, $x = \pm\sqrt{2-\sqrt{2}}, \pm\sqrt{2+\sqrt{2}}$. Let $K = k(f)$. Then,$K = \mathbb{Q}(\sqrt{2-\sqrt{2}})$, since $\sqrt{2-\sqrt{2}}\sqrt{2+\sqrt{2}} = \sqrt{2} \in \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2-\sqrt{2}})$. Thus, $K/\mathbb{Q}(\sqrt{2})/k$, therefore, $|Gal(f)| = 4$, which implies $Gal(f) = \mathbb{Z}_4$.*

5 Semisimplicity

See also §14. Representations of one Endomorphism.

5.1 Matrices and linear maps over non-commutative rings

Remark 5.1.1. *We use below facts.*

Let K be a ring.

$$Mat_n(K) = \{(a_{ij})_{1 \leq i,j \leq n} : a_{ij} \in K\}$$

is a ring under usual $+, \cdot$ of matrices.

1. *Let K be a division ring, i.e., $\forall a \in K \setminus \{0\}$ is a unit. Then, every K-module has a basis and any two bases have the same cardinality.*

2. *Let R be a ring and $E = E_1 \oplus \cdots \oplus E_n$, $F = F_1 \oplus \cdots \oplus F_m$ be R-module. (E_i, F_j are submodules.) Let $\varphi : E \to F$ be a R-linear map. For $1 \le i \le m$, $1 \le j \le n$, $\varphi_{ij} = \pi_i \circ \varphi \circ \iota_j$ where $\iota_j : E_j \to E$, $\pi_i : F \to F_i$ is a R-linear map from E_j to F_i. So $\varphi_{ij} \in \mathrm{Hom}_R(E_j, F_i)$.*

Sketch of proof. First one is the same as linear algebra; we do not use commutativity. Second one is related to proposition 2.1.3 below. See Lang's book, p.642∼643. □

Define $M(\varphi) := (\varphi_{ij})_{1 \le i \le m, 1 \le j \le n}$, a matrix.

Definition 5.1.2. *Let k be commutative ring, E be module. Then, $End_k(E)$ denotes the ring of k-endomorphisms of E, i.e., the ring of k-linear maps of E into itself.*

Proposition 5.1.3. *Let E be an R-module. Denote $E^{(n)} = \overbrace{E \oplus \cdots \oplus E}^{n}$ for $n \ge 1$. Then, $End_R(E^{(n)}) \cong Mat_n(K)$ as a ring, where $K = End_R(E)$.*

Proof. Note that $\varphi_{ij} \in End_R(E)$, and $\varphi \mapsto M(\varphi)$ is a ring isomorphism, since every ϕ has unique $M(\phi)$ and for every matrix in $Mat_n(K)$, this gives $End_R(E^{(n)})$. □

Proposition 5.1.4 (Proposition 1.1, Schur's Lemma)**.** *Let E, F be **simple** R-modules, i.e., there are no proper nontrivial submodules in E, F. If $f \in \mathrm{Hom}_R(E, F) \setminus \{0\}$, then f is an isomorphism. Thus, $End_R(E)$ is a division ring.*

Proof. $\{0\} \neq Imf \subset F$. Hence $Imf = F$, since F has no proper nontrivial submodule. Also, $kerf \subsetneq E$ since $f \neq 0$. Hence $\ker f = \{0\}$, since E has no proper nontrivial submodule. Thus, f is isomorphism. By letting $F = E$, we can conclude that any nonzero $f \in \mathrm{Hom}_R(E, E) = End_R(E)$ is unit. □

Remark 5.1.5. *Let R be a k-algebra, with k a field, and let E be a simple R-module. Then, since R is simple as an R-module, the Schur's lemma holds for E. In particular, if k is algebraically closed, then $End_R(E) \cong k$.*

Proof. Take $\sigma, \tau \in End_R(E)$. Then, if σ, τ has the same eigenvalue λ, then $\sigma = \lambda I = \tau$; this is from the fact that $ker(\sigma - \lambda I), ker(\tau - \lambda I)$ is nontrivial in E, so that $ker(\sigma - \lambda I) = E = ker(\tau - \lambda I)$. Thus we have the map $End_R(E) \to k^a = k$ by $\sigma \mapsto \lambda_\sigma$, where λ_σ is eigenvalue of σ, since λ_σ comes from any algebraic elements of k. Also any endomorphism can be represented by λI, so the map is bijective. Since ring homomorphism holds trivially, it is isomorphism as a ring. (So as a field.) □

Proposition 5.1.6 (Proposition 1.2)**.** *Let E be an R-module. Suppose $E = E_1^{(n_1)} \oplus \cdots \oplus E_r^{(n_r)}$ where E_i is simple, $E_i \ncong E_j$ for $i \neq j$, $n_i \ge 1$. Then, $\{E_1, \cdots, E_r\}$ and $n_1, \cdots, n_r$ are uniquely determined, and $End_R(E) \cong Mat_{n_1}(K_1) \times \cdots \times Mat_{n_r}(K_r)$ as rings where $K_i = End_R(E_i)$.*

Proof. Suppose that $E = F_1^{(m_1} \oplus \cdots \oplus F_s^{(m_s)}$ where F_i is simple, $F_i \ncong F_j$ for $i \neq j$, $m_i \ge 1$. Consider $E_j \xrightarrow{\iota_j} E \xrightarrow{\pi_i} F_i$. This map is R-linear since each ι_j, π_i is R-linear. Thus, by Schur's lemma,

$$\forall j, \exists i, s.t., E_j \xrightarrow{\iota_j} E \xrightarrow{\pi_i} F_i \text{ is isomorphism,}$$

otherwise this map is always zero, which means ι_j is zero, contradiction. Hence,

$$\{E_1, \cdots, E_r\} \subset \{F_1, \cdots, F_s\}.$$

Mutadis mutandi,

$$\{E_1, \cdots, E_r\} \supset \{F_1, \cdots, F_s\}.$$

Hence two set is equal, and by renumbering, we can say that $E_i \cong F_i$ for all i, and $r = s$.

Now the above isomorphism induces the fact that $E_i^{n_i} \to E \to F_i^{m_i}$ is isomorphism. Thus, it suffices to show that if $E^{(n)} \to E^{(m)}$ isomorphism exists for simple module E, then $n = m$. If such isomorphism exists, $End_R(E^{(n)}) \cong End_R(E^{(m)})$, and by proposition 2.1.3, $Mat_n(K) \cong Mat_m(K)$ as K-module, for $K = End_R(E)$. This implies $m = n$, so done. □

So such decomposition is unique up to renumbering. Hence, when E admits a (finite) direct sum decomposition of simple submodules, the number of times that a simple module of a given isomorphism class occurs in a decomposition will be called the **multiplicity** of the simple module (or of the isomorphism class of the simple module). Furthermore, sum of all multiplicity is called **length** of E.

5.2 Conditions defining semisimplicity

Let R be a ring and let E be an R-module.

Theorem 5.2.1. *The following are equivalent.*

1. *E is a sum of simple submodules, i.e., $E = \sum_{i \in I} E_i$, where E_is are simple submodules.*
2. *E is a direct sum of simple submodules, i.e., $E = \oplus_{i \in I} E_i$, where E_is are simple submodules.*
3. *For any submodule F of E, $\exists$ submodule F' such that $E = F \oplus F'$.*

Definition 5.2.2. *E is called semisimple if one of $1, 2, 3$ is satisfied.*

1 $\implies$ 2. Let J be a maximal subset of I such that the sum $\sum_{j \in J} E_j$ is a direct sum. For any $i \in I$, $E_i \cap \sum_{j \in J} E_j = 0$ or E_i. But if it is zero, then $E_i + (\sum_{j \in J} E_j)$ is also direct sum, so J is not maximal, contradiction. Hence every E_i is contained in $\sum_{j \in J} E_j = \oplus_{j \in J} E_j$. Thus, $E \subseteq \oplus_{j \in J} E_j$, so $E = \oplus_{j \in J} E_j$. □

2 $\implies$ 3. Let $F \subsetneq E$. Let J' be a maximal subset of J such that $F + (\oplus_{j \in J'} E_j)$ is a direct sum. Let $F' = \oplus_{j \in J'} E_j$. If such J' doesn't exists, $F = E$, contradiction. If $F \oplus F' \subsetneq E$, then, $\exists x \in E \setminus F'$, so $\exists i \in J$ such that $x \in E_i$, so $F + E_i \oplus F'$ is also direct sum. However, this contradicts maximality of J'. Thus, $E = F \oplus F'$. □

3 $\implies$ 1. First, claim that every submodule of E contains a simple submodule. Let $v \in E$, $v \neq 0$. Then, Rv is a principal R-module (and a left submodule of E), and $\pi : R \to Rv$ by $r \mapsto rv$ is R-linear homomorphism. Thus, $ker\pi$ is a left ideal in R. Let M be a maximal left ideal in R, containing $ker\pi$, using Zorn's lemma. By the first isomorphism theorem of the left R-module,

$$M/ker\pi \hookrightarrow R/ker\pi \xrightarrow{\cong} Rv.$$

Thus, image of this map, Mv, is a maximal submodule of Rv, by the isomorphism above. Thus, $E = Mv \oplus M'$ by the hypothesis 3. Then,

$$Rv = Mv \oplus (M' \cap Rv),$$

since for any $w \in Rv$, $\exists! w_1 \in Mv, w_2 \in M'$ where $w = w_1 + w_2$ from $E = Mv \oplus M'$, so $w_1 \in Mv \subset Rv$, and $w_2 \in M' \cap Rv$ since $w_2 = w - w_1 \in Rv$ from $w_1 \in Rv$. Thus,

$$M' \cap Rv \cong Rv/Mv \cong (R/ker\pi)/(M/ker\pi) \cong R/M.$$

Thus, $M' \cap Rv$ is simple, as desired. So the claim that every submodule of E contains a simple submodule holds.

Now, let E_0 be the sum of all simple submodules of E. If $E_0 \neq E$, then $E = E_0 \oplus E_0'$ with $E_0' \neq 0$, by the hypothesis 3. Thus, E_0' have also simple submodule by above claim, say F. Hence $E_0 \oplus F$ is also sum of simple submodules of E, contradicting the maximality of E_0. □

Proposition 5.2.3 (Proposition 2.2)**.** *Let E be semisimple R-module. A factor module of E and a submodule of E are semisimple.*

Proof. Let $E = \sum_{i \in I} E_i$, E_i be simple. Let F be factor module or submodule of E. In any case, $\exists f : E \to F$, which is R-linear. Hence, $Imf = \sum_{i \in I} f(E_i)$. And schur's lemma assures that $f(E_i)$ is zero module or simple module. □

Note 5.2.4. *Let $E' \subset E$ be submodule, and E is semisimple. Then,*

$$E = E' \oplus E'' \xrightarrow{\pi} E',$$

and π is R-linear. From the proposition 2.2, E' is also semisimple.

Remark 5.2.5. *The same is true for module over k-algebra.*

Note that left R-submodule of R is called left ideal.

Example 5.2.6. *1. Let k be a field. Think about E_{ij} in $R = Mat_n(k)$. Then, let (E_{ij}) be an left ideal in R. Thus, it is R-submodule. Also, $(E_{ij}) = (E_{i'j})$ since $E_{i'j}E_{ij} = E_{i'j} \in (E_{ij})$. Thus,*

$$R = \oplus_{j=1}^{n} (E_{1j}).$$

Note that (E_{ij}) is simple; if it has nontrivial submodule, then it contains $rE_{ij} = \begin{pmatrix} \vec{0} & \vec{r_i} & \vec{0} \end{pmatrix}$ for some $r \in R$, with $\vec{r_1}$ is its i-th column, so by taking $r' = \frac{1}{r_{ii}} E_{ij}$, we can see that $r'rE_{ij} = E_{ij}$ in the submodule. So it is nonproper. Hence R is semisimple R-module. Since each $(E_{ij}) \cong k^n$, $R \cong k^n \oplus \cdots \oplus k^n$.

2.

$$k[x]/ < (x-1)(x-2) > \cong k[x]/ < x-1 > \times k[x]/ < x-2 >,$$

by chinese remainder theorem. And since $k[x]/ < x-1 >$, $k[x]/ < x-2 >$ are simple, with generated by $\bar{f}(x) = f(1)$ and $\bar{f}(x) = f(2)$ respectively, $k[x]/ < (x-1)(x-2) >$ is semisimple.

Remark 5.2.7 (Counterexample)**.** *$k[x]/ < (x-1)^2(x-2) >$ is counter example. It is not semisimple.*

Proof. $k[x]/ < (x-1)^2(x-2) > \cong k[x]/ < (x-1)^2 > \times k[x]/ < (x-2) >$ from decomposition of PID. Note that $R/ < p^n >$ is indecomposable for p, prime, with R, PID. Since $(x-1)$ is prime $k[x]/ < (x-1)^2 >$ is indecomposable, and if $n > 2$, it has proper submodule $< p^i > / < p^n >$. Thus, $k[x]/ < (x-1)^2 >$ is not simple.

To show that $R/ < p^n >$ is indecomposable, let M be ideal on $R/ < p^n >$. Then, $\pi^{-1}(M) \subset R$ is ideal, so $\pi^{-1}(M) =< a >$ for some $a \in R$ from PID. Since $< a >$ contain $< p^n >$, $am = p^n$ for some $m \in R$, so $a | p^n$. Since PID is UFD, $a = p^l$ for some $l \leq n$. Thus, $M =< p^l > / < p^n >$. If it is decomposable, $< p^{l_1} > / < p^n > \oplus < p^{l_2} > / < p^n >$, for some $1 \leq l_1 \leq l_2 < l$. However, since $p^{l_2} \in < p^{l_1} >$, $< p^{l_1} > / < p^n > \cap < p^{l_2} > / < p^n > =< p^{l_1} > / < p^n >$, so it cannot be direct sum, contradiction. Thus, only $n = 0$ or 1 makes the submodule simple. □

5.3 The density theorem

Let R be a ring, E be semisimple R-module. Let $f \in R' = End_R(E) \subset End(E)$. We call R' as **commutant** of R. Then, E can be viewed as a R'-module with the product operation of R' on E being given by $(f, x) \mapsto f(x)$ for $f \in R'$, $x \in E$. Also note that each $r \in R$ induces R'-homomorphism $\lambda_r : E \to E$ by $\lambda_r(x) = rx$.

Similarly, take $R'' = End_{R'}(E) \subset End(E)$. Then it is called **bicommutant**. We get a ring homomorphism

$$\lambda : R \to R'', r \mapsto \lambda_r.$$

The density theorem states that the image of this homomorphism is quite big.

Example 5.3.1. *For some field k, $Mat_n(k)$ is a vector space, as well as a ring, since it has multiplication. Let $\{x_j\}_{j=1}^{i}$ be generator of $Mat_n(k)$. Questions; what is minimal i? Answer; $i = 2$. Take E_{11} and a permutation matrix.*

Definition 5.3.2. *Let E be R-module. Then, E is called **faithful** of $r \in R$ such that $rE = \{0\}$ implies $r = 0$.*

Faithfulness implies that $R \to R'' \subset End(E)$ by $r \mapsto \lambda_r$ is injective.

Lemma 5.3.3. *Let E be semisimple R-module. For $f \in R''$, $x \in E$, $f(x) = \alpha x$. for some $\alpha \in R$.*

Proof. Since E is semisimple, $E = Rx \oplus E'$ with some submodule E'. Let $\pi : E \to Rx$ be projection. Then,

$$Rx \hookrightarrow E \xrightarrow{\pi} Rx$$

is R-linear. Hence,

$$\pi \circ f(Rx) = f(\pi(Rx)) = f(Rx) \implies f(Rx) = Rx.$$

where first equality comes from $\pi \in R'$, and regard Rx as a submodule of R'-module E, with R'-scalar π. Since $f \in R''$ implies f is R'-linear, such equality holds.

Hence $f(x) \in Rx$, so $\exists \alpha \in R$ such that $f(x) = \alpha x$, as desired. □

Theorem 5.3.4 (Theorem 3.2, Jacobson Density Theorem)**.** *Let E be semisimple R-module. For $x_1, \cdots, x_n \in E$, $f \in R''$, $\exists \alpha \in R$ such that $f(x_i) = \alpha x_i$ for $1 \leq i \leq n$. In particular, if E is a finitely generated R'-module, then $\lambda : R \to R''$ by $r \mapsto \lambda_r$ is surjective.*

Proof. Assume that E is a simple module. Then, $E^{(n)}$ is also R-module, and define $R'_n := End_R(E^{(n)}) \cong Mat_n(R')$.

Consider $f^{(n)} : E^{(n)} \to E^{(n)}$ by $(y_1, \cdots, y_n) \mapsto (f(y_1), \cdots, f(y_n))$. Then, $f^{(n)} \in R''_n = End_{R'_n}(E^{(n)})$. And, its matrix form is

$$f^{(n)}(y_1, \cdots, y_n) = \begin{pmatrix} f & & \\ & \cdots & \\ & & f \end{pmatrix} \begin{pmatrix} y_1 \\ \cdots \\ y_n \end{pmatrix}.$$

So it is diagonal as a matrix form. Hence $f^{(n)}$ commutes with any element in $End_{R'_n}(E^{(n)})$. Thus, using the lemma 3.1, $\exists \alpha \in R$ such that $(\alpha y_1, \cdots, \alpha y_n) = (f(y_1), \cdots, f(y_n))$.

Now E is not simple, suppose that E is equal to a finite direct sum of simple submodules E_i (non-isomorphic), with multiplicities n_i. Then

$$E = \oplus_{i=1}^{r} E_i^{n_i}.$$

The matrices representing the ring of endomorphisms splits according to blocks corresponding to the non-isomorphic simple components in our direct sum decomposition. So we can apply the same argument above on those part.

If E is finitely generated R' module, then $f \in R''$ is determined by its value on a finite number of elements of E, thus $R \to R''$ is surjective. □

Note 5.3.5. *"Noetherian" module is related to commutative ring, and used for algebraic geometry. On the other hand, Linear algebra is related to semisimple rings and modules.*

Corollary 5.3.6 (Corollary 3.3, Burnside's theorem)**.** *Let k-algebraically closed, E be k-vector space with finite dimension, $R \subset End_k(E)$ be subalgebra. If E is a simple R-module, then $R' = k$ and $R = End_{R'}(E) = End_k(E)$.*

Proof. First of all, we want to show $R' = k$. Since E is simple R-module, by Schur's lemma, $R' = End_R(E)$ is division ring. And it contain k in its center, since $R' \supset \{cI_n : c \in k\} \cong k$ as a field. Let $\alpha \in R'$. Then, $k(\alpha)$ is also a field. Since R' is also finite dimensional k-space (think that space of linear transformation for finite dimensional vector space is also finite dimensional vector space.), so is $k(\alpha)$. Since k is algebraically closed, $k(\alpha) = k$. Since α is arbitrary, $R' = k$.

Thus, E is finitely generated R'-module since E is finite dimensional k-vector space, i.e., $k = R'$-module.

Thus By Jacobson density theorem, $\lambda : R \to R''$ is surjective. Also, this map is injective since $\lambda_\alpha(x) = 0$ iff $\alpha = 0$. Also, $R \subset End_k(E) = End_{R'}(E) = R''$ since $R' = k$. Thus, $R \subset R''$. With λ, bijective map, $R = R''$.

□

Remark 5.3.7 (Proof of $k \cong End_R(E)$, where E is simple.)**.** *Let $f \in End_R(E)$. $\exists\lambda$, an eigenvalue of f over k. Then, $f(v) = \lambda v$ for some $v \neq 0$. So consider $f - \lambda I \in R'$. Then, $0 \neq ker(f - \lambda I) \subset E \implies ker(f - \lambda I) = E$. So $f = \lambda I$. Hence take map $End_R(E) \to k$ by $f \mapsto \lambda$, we get desired result.*

Example 5.3.8. *Let k be a field. $Mat_n(k) = End_k(k^n)$ from above argument. Then let R be the subalgebra generated by $X = \sum_{i=1}^{n-1} E_{i,i+1}$ and $Y = X^t$. Note that k^n is a simple R-module. (If it has proper submodule, this contain e_i for some i. Using X, we can get all e_j with $j < i$, and using Y, we can get all e_j with $j > i$. So k^n is simple R-module.)*

Thus, Burnside theorem tells that $R = End_k(k^n) = Mat_n(k)$.

Remark 5.3.9. *In general, if R is k-algebra, with k is algebraically closed field, and E is simple R-module with $dim_k E < \infty$, with simple faithful $\rho : R \to End_k(E)$, by definition of R-module, then $\rho(R) = End_k(E)$.*

Why? If $\tilde{R} := \rho(R)$, E can be viewed as $\tilde{R}$-module. Since E is simple R-module, it is also simple $\tilde{R}$-module. Now apply Burnside's theorem. □

Theorem 5.3.10 (Theorem 3.7)**.** *Let k be field, R be k-algebra. Let $V_1, \cdots, V_n$ be simple R-modules such that $dim_k V_i < \infty$ for all $i \in [n]$. Also assume that $V_i \ncong V_j$ for $i \neq j$. Then, $\forall i \in [n]$, $\exists e_i \in R$ such that*

1. *e_i acts on V_i as an identity*
2. *$e_i V_j = 0$ for $j \neq i$.*

Proof. Let $E = V_1 \oplus \cdots \oplus V_n, \pi_i : E \to V_i$, projection. Then, $\forall f \in R' = End_R(E)$, $f(V_i) \subset V_i, \forall i \in [n]$, from simplicity and nonisomorphic condition on V_is. Thus, $\pi_i \circ f = f \circ \pi_i, \forall i \in [n]$. Thus, $\pi_i \in R''$.

Using jacobson theorem, $\exists e_i$ such that $\lambda(e_i) = \pi_i$. Thus e_is satisfy all desired conditions. □

Corollary 5.3.11 (Corollary 3.8, Bourbaki)**.** *Let k be a field, $chk = 0$, R be a k-algebra. Let E, F be semisimple R-modules, with $dim_k E < \infty, dim_k F < \infty$. If $tr(\alpha_E) = tr(\alpha_F)$ for all $\alpha \in R$, where α_E, α_F are the corresponding k-endomorphism on E,F resp., then $E \cong F$ as R-module.*

Proof. Let V be simple R-module. Then,

$$E = V^{(m)} \oplus E', F = V^{(n)} \oplus F'$$

for some $m, n \geq 0$, and F', E' submodules such that $F' \cap V = \{0\} = E' \cap V$. By theorem 3.7, $\exists e_v \in R$ such that e_v acts on V as identity and $e_v W = 0$ for any simple R-module $W \ncong V$. Then,

$$tr(e_E) = m \cdot dim_k V, tr(e_F) = n \cdot dim_k V.$$

(To see this, think it as a matrices; every nondiagonal term is zero, and every diagonal term which is not related to V is zero, and the number of diagonal term related to V should be $n \cdot dim_k V$, and the value on the position is 1. Similar to case of F.) Thus, $n = m$. Since V was arbitrary, $E \cong F$ as R-module. □

5.4 Semisimple rings

Definition 5.4.1. *Let R be a ring. Define R be semisimple if it is semisimple as a left R-module with respect to multiplication.*

Proposition 5.4.2 (Proposition 4.1)**.** *Let R be semisimple ring. Then, every R-module is semisimple.*

Proof. Let M be R-module. Then, $\exists F = \sum_{m \in M} Rm$, and a surjective map $F \twoheadrightarrow M$ as natural map. Since F is direct sum of Rm for any $m \in M$, and $Rm \cong R$ as a R-module, and R is semisimple. Hence M, a homomorphic image of F is semisimple by theorem 2.2. □

Remark 5.4.3. *Let $L \subset R$ be a R-submodule. Then, L is a left ideal of R. (Converse is also true.) Call L is **simple** if it is a simple as a R-submodule. So,*

$$R\text{: semisimple} \implies R = \sum_{L: simple left ideal} L.$$

Example 5.4.4. *Let $R = Mat_n(k)$, where k is a field. Then, by above argument, $R = \overbrace{k^n \oplus \cdots \oplus k^n}^{n}$, and since k^n is (semi)simple as shown above, R is also semisimple.*

Example 5.4.5. *Let G be a finite group. Then, let $k[G]$ be the group ring of G over k. By definition of $k[G]$, it is k-vector space with basis G and with multiplication defined distributively using the given multiplication of G. So, $k[G] = \oplus_{g \in G} k v_g$, with $v_g \cdot v_h = v_{gh}$ for any $g, h \in G$. Since scalar multiplication and associative law also hold, we can also view this as a k-algebra.*

Now let X be a set such that G acts on X. Then, we can also think G acts on $V = \oplus_{x \in X} k v_x$ by $g \mapsto \phi(g) \in End(V)$, where $\phi(g)$ is a map $x \mapsto gx$. Like this, take map $\rho : k[G] \to End(V)$ by $\sum c_g v_g \mapsto \sum c_g \phi_g$. By checking ρ is faithful by thinking $End(V) \cong Mat_{|G|}(K)$, we can think it as a $k[G]$-module. By below theorem, $k[G]$ is semisimple.

Theorem 5.4.6 (Mashcke, proof is not given)**.** *Let char $k \nmid |G|$. Then, $k[G]$ is semisimple. In particular, if char $k = 0$, $k[G]$ is always semisimple.*

For example of example, let $C_n =< \sigma >= \{e, \sigma, \cdots, \sigma^{n-1}\}$ a cyclic group of order n. Then, let

$$\mathbb{C}[C_n] = \mathbb{C}v_e \oplus \mathbb{C}v_\sigma \oplus \cdots \oplus \mathbb{C}v_{\sigma^{n-1}} = \mathbb{C}1 \oplus \mathbb{C}\sigma \oplus \cdots \oplus \mathbb{C}\sigma^{n-1}.$$

Note that last sum is just notational abuse. Then, using distributive law with the fact that $\sigma^{i+j} \cong \sigma^{i+j} \bmod \sigma^n = 1$, we can define multiplication well. Thus, we can show that

$$\mathbb{C}[C_n] = \mathbb{C}[x]/ < x^n - 1 > .$$

This is because $x^n - 1 = \prod_{k=0}^{n-1}(x - \xi^k)$, where ξ is primitive n-th root of unity and think C_n as a group of primitive n-th root of unity, and think about natural map from x to ξ. Then, since $\mathbb{C}$ is algebraically closed field, we can use the chinese remainder theorem to show that

$$\mathbb{C}[C_n] = \mathbb{C}[x]/ < x^n - 1 >= \mathbb{C}[x]/ < x - 1 > \times \mathbb{C}[x]/ < x - \xi > \times \cdots \times \mathbb{C}[x]/ < x - \xi^{n-1} > .$$

For fixed $i \in [n-1] \cup \{0\}$, $\mathbb{C}[x]/ < x - \xi^i > \cong k$ but $\bar{x} \cdot \bar{1} = \xi^i$. Hence, each factor is isomorphic to k, which is 1-dimensional vector space, so it is simple left ideal. However, they are nonisomorphic to each other as a left R-module, since they have $\bar{x} \cdot \bar{1}$ with different order.

Example 5.4.7.

$$\mathbb{C}[C_m \times C_n] \cong \mathbb{C}[C_m] \otimes \mathbb{C}[C_n]$$

To show this, use the map from vector spaces, and check that it is actually algebra isomorphism. In general, if G is a finite abelian group, then $\mathbb{C}[G]$ is tensor product of group rings from abelian groups which are component of G by the fundamental theorem of finitely generated abelian group.

Lemma 5.4.8 (Lemma 4.2)**.** *Let R be semisimple, L be simple left ideal, E be simple R-module. If $L \ncong E$, then $LE = 0$.*

Proof. Note that LE is also submodule of E since $R(LE) \subset (RL)E \subset RE = E$. Since E is simple module, so $LE = 0$ or E. If $LE = E$, then take $y \in E$ such that $Ly \neq 0$. Then, Ly is nontrivial submodule contained in E so $Ly = E$. Then, the map

$$\tau : L \to Ly = E \text{ by } r \mapsto ry$$

is surjective, so nonzero. From Schur's lemma, it is isomorphism. However, it contradicts $L \ncong E$, given condition. so $LE = 0$. □

Now let R be semisimple, and let $\mathscr{L} = \{L_i\}_{i \in I}$ be the set of simple left ideals such that $L_i \ncong L_j$ for $i \neq j$. Then, for all $i \in I$,

$$R_i = \sum_{L \cong L_i, L \subset R} L,$$

since there are more left ideals which are isomorphic to L_i.

Remark 5.4.9. *Now we can check followings;*

1. *$R_i R_j = 0$ for $i \neq j$. This comes from the lemma directly.*
2. *$R_i R_i = R_i$ since $R_i \subset RR_i = R_i R_i \subset R_i$., the first inclusion because R contains a unit element, and the last because R_i is a left ideal. From this conclusion, we can say that R_i is also a right ideal, so it is a two sided ideal.*

3. *$R = \sum_{i\in I} R_i$, since R is semisimple so that it is sum of simple left ideals, which is equivalent as simple left R-submodule.*

4. *$1 \in R = \sum_{i\in I} R_i$, so $1 = \sum_{j=1}^{s} e_{i_j}$ for some $i_j \in I$ and $s \in \mathbb{N}$. By renumbering we can say that $1 = \sum_{j=1}^{s} e_j$.*

5. *Thus, $e_i e_j = 0$ for $i \neq j$, since $R_i R_j = 0$ for $i \neq j$.*

6. *Also, $e_i^2 = e_i$ since $\forall x \in R$,*

$$x = x \cdot 1 = xe_1 + \cdots + xe_s,$$

and take $x = e_i$.

7. *Also note that $R_i = Re_i = e_i R$, since e_i is identity in R_i by remark 6.*

From remark 6, $R = R_1 \oplus \cdots \oplus R_s$ a direct sum. And since e_i is unit element of R_i, so it is equal as a ring. By remark 4, it is in fact that R is a direct product of R_i. This argument is capped on theorem 4.3. below.

Theorem 5.4.10 (Theorem 4.3)**.** *There exists only finitely many simple left ideals up to isomorphism. In Lang's textbook, above remark and conclusions are summarized in this part.*

Theorem 5.4.11 (Theorem 4.4)**.** *Let R be semisimple, E be nontrivial R-module. Then,*

$$E = \oplus_{i=1}^{s} R_i E = \oplus_{i=1}^{s} e_i E$$

where $e_i E = \oplus_{E' \subset E, E' \cong L_i} L_i$ is from theorem 4.3's argument.

Proof. For any simple submodule E' in E, $L_i E' = E'$ for some i, since $RE' = E'$. Thus, by lemma 4.2, $E' \cong L_i$. Hence E is direct sum of $E_i = e_i E$, and note that $R_i E = e_i E$. □

Corollary 5.4.12 (Corollary 4.5)**.** *Every simple R-module is isomorphic to L_i for some $i = 1, \cdots, s$, where s, L_i are from argument for theorem 4.3.*

Definition 5.4.13. *A ring is **simple** if it is semisimple and has only one simple left ideals up to isomorphism.*

Corollary 5.4.14 (Corollary 4.6)**.** *A simple ring has exactly one simple module, up to isomorphism.*

Proposition 5.4.15 (Proposition 4.7)**.** *Let k be a field, E be a finite dimensional k-vector space, R be a sub-algebra of $End_k(E)$. Then, R is semisimple $\iff$ E is semisimple R-module.*

Proof. If R is semisimple, then E is semisimple by proposition 4.1. So does $E^{\oplus \dim E}$, since it can be also represented by direct sum of simple modules.

Let $\{y_1, \cdots y_m\}$ be k-basis of E and consider $\phi : End_k(E) \to E^{(\dim E)}$ by $r \mapsto (ry_1, \cdots, ry_m)$. Then,$\phi$ is a $End_k(E)$-module isomorphism, thus not only $End_k(E)$ linear but also R-linear. If $(ry_1, \cdots, ry_m) = 0$, then r makes every basis be zero, so r is trivial. Hence ϕ is injective. Also, from linear algebra argument that there exists unique linear transformation from basis to any set of vectors having the same cardinality with basis, surjectivity holds. Thus,

$$R \subset End_k(E) \xrightarrow{\cong} E^{(\dim E)}.$$

Therefore, R is isomorphic to some submodule of semisimple module. Hence it is semisimple by proposition 2.2.

□

(Thanks **Hobin Jung** for giving detailed proof of below example.)

Example 5.4.16. *Let $k = \mathbb{R}$, $E = \mathbb{R}^3$. Let R be a subalgebra of $Mat_3(\mathbb{R}) = End_R(E)$ generated by permutation matrices. Note that permutation matrices in $Mat_3(\mathbb{R})$ are*

$$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}, \begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}, \begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}, \begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}, \begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}, \begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix},$$

and the set have actually group structure, isomorphic to S_3. Thus, $R \cong \mathbb{R}[S_3]$; this can be showed by just checking that algebra structure gives group ring structure.

Now I claim that R is semisimple. It is enough to show that E is semisimple R-module by proposition 4.7. For example, take $V_1 = \mathbb{R}(1,1,1)$ and $V_2 = \{(x,y,z) : x+y+z = 0\}$, a hyperplane orthogonal to V_1. Then, trivially, $E = V_1 + V_2$. We know that V_1 is simple since it is 1-dimension.

I claim that V_2 is simple. Let M be nontrivial submodule of V_2. Then, $0 \neq (l, m, -l-m) \in M$. From action of $(1,3)$ and $(2,3)$ in S_3, we can get $(-l-m, m, l)$ and $(l, -l-m, m)$ in M. By addition, we can get $(-m, 2m, -m)$ and $(2l, -l, -l)$. By scalar multiplication as $\mathbb{R}$-module, we can get $(-1, 2, -1)$ and $(2, -1, -1)$. From this, we can get

$$(1,-1,0) = \frac{1}{3}(2,-1,-1) + \frac{1}{3}(1,-2,1),$$

and,

$$(0,1,-1) = \frac{1}{3}(2,-1,-1) - \frac{2}{3}(1,-2,1).$$

Since $\{(1,-1,0),(0,1,-1)\}$ forms a basis of V_2, M is nonproper. Thus, V_2 is also simple. Since $V_1 \cap V_2 = \{0\}$, $E = V_1 \oplus V_2$, hence E is semisimple by definition.

5.5 Simple rings

Let R be semisimple ring. Then $R = \oplus_{i \in I} R_i$ for some R_i. We just call R_i as **simple ring**.

Lemma 5.5.1. *Let R be a ring. Then, $R^{opp} \cong End_R(R)$, a set of homomorphism of R into itself, viewd as R-module, isomorphic as a ring where R^{opp} is $(R^{opp}, +, \cdot)$ with $a \cdot b = ba$ for $a, b \in R$.*

Proof. Define $R^{opp} \xrightarrow{\rho} End_R(R)$ by $\alpha \mapsto \rho_\alpha : x \mapsto x\alpha$. Then,

$$\rho_{\alpha\cdot\beta}(x) = x(\alpha \cdot \beta) = (x\beta)\alpha = \rho_\alpha \circ \rho_\beta(x).$$

Since $ker\rho = \{0\}$, ρ is one-to-one. Also, for some $f \in End_R(R)$ such that $\alpha = f(1)$, for any $x \in R$,

$$f(x) = f(x \cdot 1) = xf(1) = x\alpha = \rho_\alpha(x)$$

where second equality comes from R-linearity of f. Since α was arbitrary, ρ is onto. So ρ is isomorphism, as desired. □

Theorem 5.5.2 (Theorem 5.2)**.** *Let R be simple. Then,*

1. *R is a finite direct sum of simple left ideals.*
2. *Suppose L, M be simple left ideals of R. Then, $\exists \alpha \in R$ such that $L\alpha = M$.*

3. There is no proper nonzero two-sided ideal of R.

Proof. 1. $1 \in R = \oplus_{i\in I} L_i$ from semisimplicity of R. Thus, $1 = x_{i_1} + \cdots + x_{i_s}$ for some $i_1, \cdots, i_s \in I$. Thus, $R \subset \oplus_{j=1}^{s} L_{i_j}$. Hence,

$$R = R \cdot 1 = \oplus_{j=1}^{s} R x_{i_j} = \oplus_{j=1}^{s} L_{i_j}.$$

2. From definition of semisimplicity, $R = L \oplus L'$ for some given L and some other submodule L'. Then, $\exists \sigma : L \to M \subset R$, which is R-linear isomorphism, from the lemma 4.2's argument. Then,

$$R \xrightarrow{\pi} L \xrightarrow{\sigma} M \subset R$$

is R-linear map. So, $\sigma \circ \pi \in End_R(R)$. By the lemma 5.1, $\sigma \circ \phi = \rho_\alpha$ for some $\alpha \in R$. Thus, $\rho_\alpha|_L$ is nonzero homomorphism from L to M, thus isomorphism by Schur's lemma.

3. Let I be nonzero two sided ideal. Then we can think it as a left R-module. Thus, I is a sum of left ideals. However, by second assertion, $IR = R$ since for any simple left ideals, $L\alpha = M$ so that LR is sum of all simple left ideals in R, thus $LR = R$. Hence take any L, left ideal in R. Then,

$$R = LR = R = IR = I.$$

Thus $I = R$

□

Theorem 5.5.3 (Theorem 5.4, Rieffel)**.** *Let R be simple ring, and L be a nonzero left ideal. Then, $\lambda : R \xrightarrow{\cong} R''$, where R', R'' are commutant and bicommutant.*

Proof. Note that $ker\lambda$ is two sided ideal, from linearity of λ. Hence, $ker\lambda = \{0\}$, by theorem 5.2. Hence it is injective. Now consider LR, a nonzero twosided ideal. Then from theorem 5.2, $LR = R$.

For $f \in R''$, $x, y \in L$,

$$f \circ \lambda_x(y) = f(xy) = f \circ \rho_y(x) = \rho_y \circ f(x) = f(x) \cdot y = \lambda_{f(x)}(y)$$

where third equality comes from the fact that $\rho \in R'$ and regard x is in a submodule of R'-module L, we argued in Lemma 3.1. Thus, $f \circ \lambda_x = \lambda_{f(x)}$. Hence, $\lambda(L)$ is a left ideal of R'', since above equation shows $R''\lambda(L) = \lambda(L)$. Finally,

$$R'' = R''\lambda(R) = R''\lambda(LR) = R''\lambda(L)\lambda(R) = \lambda(L)\lambda(R) = \lambda(LR) = \lambda(R).$$

So, λ is an isomorphism. □

Remark 5.5.4. *If L is simple, then $R \cong End_D(L) \cong Mat_n(D)$, where $n = dim_D L = n$, $D = End_R(L)$ is division ring by Schur's lemma.*

Theorem 5.5.5 (Theorem 5.5)**.** *Let D be division ring. E be D-module with $dim_D E < \infty$. Let $R = End_D(E)$. Then,*

1. *R is simple.*
2. *E is simple R-module.*
3. *$D = End_R(E)$.*

Proof. For the first assertion, let $B = \{v_1, \cdots, v_n\}$ be basis of E over D. Then, $\tau : R \to Mat_n D$ by $f \mapsto M(f)$ is ring isomorphism and $E \cong D^n = \overbrace{D \oplus \cdots \oplus D}^{n}$ as an R-module, by argument in proposition 2.1.3. of this note. We have D^n is simple $Mat_n(D)$-module, as shown in proposition 2.1.3. Hence $Mat_n(D) \cong D^n \oplus \cdots \oplus D^n$ as a $Mat_n(D)$-module. Thus, R is simple, and $E \cong D^n$ with τ is simple R-module.

For the second assertion, recall that $R = D'$. And E is finitely generated R-module, so finitely generated D'-module. Also, from conclusion 2, E is (semi)simple R-module. Hence by jacobson density theorem, $\lambda : D \to D''$ by $r \mapsto \lambda_r$ is surjective. Since this map is also injective from definition, it is isomorphism. So, $D = D'' = End_R(E)$. □

Remark 5.5.6. *1.*

$$R \text{ is semisimple} \iff R \cong End_{D_1}(E_1) \times \cdots \times End_{D_s}(E_s)$$

for some division rings D_i and D_i-module E_i, $i \in [s]$.

2. 1 is true when R is a k-algebra for a field k. This is from chapter 9 of Hungerford.

5.6 The Jacobson radical

Definition 5.6.1. *Let R be a ring. Denote $Rad(R) = \cap_{M:\substack{maximal\\left\ ideal}} M$. Call it jacobson radical.*

Theorem 5.6.2 (Theorem 6.1)**.** *Let $N = Rad(R)$. Then,*

1. *$NE = 0$ for all simple left R-module.*
2. *N is two sided ideal. N contain any two sided nilpotent ideals of R.*
3. *If R is finite dimensional k-algebra, then*

$$R \text{ is semisimple} \iff N = 0.$$

4. *if R is finite dimensional k-algebra, then N is nilpotent, i.e., $N^r = 0$ for some positive integer r.*

Proof. 1. It suffices to show that $N = B$ where $B = \{a \in R : aS = 0 \text{ for any simple } R\text{-module } S\}$. To show $N \supseteq B$, suppose $a \in B$. Take a maximal ideal of R, then R/M is simple R-module, thus $a(R/M) = 0$. Thus, $a \cdot 1 + M = 0 + M$, so $a \in M \subset N$.

To show $N \subseteq B$, suppose not; then $B \subsetneq N$. Then there exists simple module S such that $NS \neq 0$. Pick $s \in S$ such that $Ns \neq 0$. However, Ns is a submodule of S, and since S is simple, $Ns = S$. Thus, $xs = s$ for some $x \in N$. So $(x-1)s = 0$. Thus, $(x-1) \in Ann(s)$, annihilator of s, and since $Ann(s) \neq R$ (otherwise, $NS = 0$.) $Ann(s) \subseteq M \subset R$ for some maximal ideal M. Hence $(1-x) \in N$, so $(1-x) + x = 1 \in N$, contradiction.

2. Note that B is two sided ideal; for any $r \in R$, $a \in B$, $arS = a(rS) = 0, raS = r(aS) = r0 = 0$.

Let J be an arbitrary two sided nilpotent ideal. It suffices to show that J is contained in every maximal left ideal M of R. Note that for any maximal left ideal M, $M + J$ is also a left ideal of R containing M. If $M + J = M, J \subset M$. Otherwise, $M + J = R$, so $1 = x + y$ for $x \in M, y \in J$. From nilpotentness of J, $y^k = 0$ for some $k \in \mathbb{N}$. Thus,

$$(1 + y + y^2 + \cdots + y^{k-1})x = (1 + y + y^2 + \cdots + y^{k-1})(1 - y) = 1 - y^k = 1.$$

Thus, $1 \in M$, contradiction. Thus, $J \subset M$.

3. Suppose R is semisimple. Then, R is direct sum of simple left R-modules, say $R = \sum_{i\in I} L_i$, L_i is simple left ideal. However, by conclusion 1, $NL_i = 0$ for all $i \in I$. Thus, $NR = 0$. Since $1 \in R$, this implies $N = 0$.

   Suppose $N = 0$. Let M_1 be a maximal left ideal of R. If $M_1 \neq 0$, since $N = 0$, $\exists M_2$, a maximal left ideal of R such that $M_1 \cap M_2 \neq M_1$. Since $N = 0$, $\exists M_3$, a maximal left ideal of R such that $M_1 \cap M_2 \cap M_3 \neq M_1 \cap M_2$. From this, we have tower of left ideals such that

$$M_1 \supset M_1 \cap M_2 \supset M_1 \cap M_2 \cap M_3 \supset \cdots .$$

   Note that the related inclusion is proper inclusion. Since R is finite dimensional k-algebra, so M must be a subalgebra with some nonzero degree, so this sequence must be finite. Hence we can find some finitely many maximal left ideals, say $M_1, \cdots M_k$, with $M_1 \cap \cdots \cap M_k = 0$ for some $k \in \mathbb{N}$. Now, take R-module homomorphism

$$R \to \oplus_{i=1}^{n} R/M_i \text{ by } x \mapsto (x + M_1, \cdots, x + M_n).$$

   The kernel is $M_1 \cap \cdots \cap M_n = 0$. So the map is injective. Since R/M_i is simple, because of maximality of M, for any i, the RHS is semisimple. Since R can be viewed as submodule of this module by image of the map, R is semisimple by proposition 2.2.

4. Since R is finite k-algebra, the tower

$$N \supset N^2 \supset N^3 \supset \cdots$$

   must be stabilized, i.e., $\exists r \in \mathbb{N}$ such that $N^k = N^r$ for any $k \geq r$. Suppose that N is not nilpotent, i.e., $N^r \neq 0$. Then, let $A = \{L, \text{ left ideal} : N^r L \neq 0\}$. Then, since $R \in A$, so A is nonempty. Since R is finite dimensional k-algebra, there exists some left ideal with minimal dimension. Say it L. Then, since $N^r L \neq 0$, $\exists l \in L$ such that $N^r l \neq 0$. Thus, $N^r l$ is also a left ideal, and $N^r N^r l = N^r l \neq 0$. Hence $N^r l \in A$. Since L has the minimal dimension and $N^r l \in L$, $: L = N^r l$. Since L is also finitely generated, and generated by x since $L = N^r x$, $N^r L = L$. Thus, using Nakayama lemma, $L = 0$, contradiction. Hence, $N^r = 0$.

□

Example 5.6.3. *$u := \{A : A$ is upper triangular $n \times n$ matrices $\} \subset Mat_n(k)$. Then $N := \{B : B$ is strictly upper triangular matrices $\}$. And, $u/N \cong \overbrace{k \times \cdots \times k}^{n}$.*

Remark 5.6.4. *R is a ring, $R' := R/Rad(R)$. Then, $Rad(R') = 0$. If R is finite dimensional k-algebra, then R' is semisimple.*

Lemma 5.6.5 (Nakayama Lemma, module version)**.** *Let R be any ring and M a finitely generated module. Let $N = Rad(R)$. If $NM = M$, then $M = 0$.*

Proof. Let $w_1, \cdots, w_n$ be generator of M. Then, since $NM = M$,

$$w_1 = a_1 w_1 + \cdots + a_n w_n$$

for some $a_1, \cdots a_n \in N$. Thus,

$$(1 - a_1) w_1 = a_2 w_2 + \cdots + a_n w_n.$$

If $(1 - a_1)$ is not a unit in R, then $(1 - a_1)$ is contained in some maximal ideal I. Since $N \subset I$, $a_1 \in I$, so $(1 - a_1) + a_1 = 1 \in I$, contradiction. Thus, $(1 - a_1)$ is unit. Hence, $w_1 = \frac{a_2}{(1-a_1)} w_2 + \cdots + \frac{a_n}{(1-a_1)} w_n$, contradiction. Thus, $M = 0$ is only possibility for $NM = M$. □

References

[1] Serge Lang, *Algebra, revised third edition*. Springer, 2002

[2] Thomas, W. Hungerford *Algebra*. Springer, 1974