ALGEBRA II LECTURE NOTES

ERIC ALBERS

Contents

1. Fields and Galois Theory

In this first section we start with the general theory of field extensions denoted F/K, which is a field field F with subfield K. We will investigate various properties of field extensions, namely finiteness, algebraicity, normality, separability, and culiminating in the Galois property. We use this to transition to Galois theory in part 2. Fixing terminology, given field extensions $F/K, E/F$, we refer to $K \subseteq F \subseteq E$ as a *tower of fields*. We will say a property $\mathscr{P}$ is *well behaved in towers* if E/K has the property $\mathscr{P}$ if and only if both F/K and E/F have the same property.

1.1. **Finite & Algebraic Extensions.**

Throughout F/K is a field extension. Recall that F can be viewed as an K-vector space with scalar multiplication by K defined by multplication in the field F. The *degree* of an extension $|F : K|$ is simply the dimension of F as a K-vector space and F/K is called *finite* if its degree is finite.

Lemma 1.1. *Degrees are multiplicative in towers. Explicitly given a tower of fields $K \subseteq F \subseteq E$ one has*

$$|E : K| = |E : F||F : K|,$$

where we allow for infinite cardinal arithmetic if necessary.

Proof. Fix an F-basis for E, $(e_i)_{i\in I}$ and a K-basis for F, $(f_j)_{j\in J}$. Then the set of elements $(e_i f_j)_{(i,j)\in I\times J}$ is plainly seen to be a basis for E/K. □

An element $\alpha \in F$ is said to be *algebraic over* K if there is a non-zero polynomial $f \in K[x]$ such that $f(\alpha) = 0$ and is otherwise *transcendental*. The extension F/K is *algebraic* if every element therein is algebraic. For example, all finite field extensions are algebraic: For any extension of degree $|F : K| = n$, $\alpha \in F$, the list of elements $1, \alpha, \alpha^2, \dots \alpha^n$ is necessarily linearly dependent. Hence there exist a collection $(\xi_i)_{i\in[n]}$, not all zero, such that

$$\sum_{i=0}^{n} \xi_i \alpha^i = 0.$$

Then α is a root of the polynomial $f(x) = \sum_{i=0}^{n} \xi_i x^i$.

Given any element $\alpha \in F$ consider the map $\mathrm{ev}_\alpha : K[x] \to F$ defined by

$$f(x) \mapsto f(\alpha).$$

Evidently α is algebraic over K if and only if the above map has non-trivial kernel. In this case, since $K[x]$ is a principal ideal domain, there exists a unique monic generator f such that $\mathrm{Ker}(\mathrm{ev}_\alpha) = (f)$. f is said to be the *minimal polymonial of f over K* and is often denoted $m_{\alpha,K}$. Note that all minimal polynomials are irreducible since the image of ev_α is an integral domain giving the ideal (f) is prime. In PIDs primality of (f) is identical to irreducibility of f. Moreover for any polynomial $g \in K[x]$ having α as a root, the above implies that $f|g$.

Observe that $m_{\sqrt[n]{p},\mathbb{Q}} = x^n - p$ for any prime $p \in \mathbb{Z}$. This is because this polynomial certainly has the root $\sqrt[n]{p}$ and is irreducible in $\mathbb{Q}$ by Eisenstein's criterion. For another example, we see that $m_{e^{2\pi i/n},\mathbb{Q}} = \Phi_n$ since Φ_n is irreducible for every n.

Given a subset $\Omega \subseteq F$, the intersection of all subfields of F containing both Ω and K is again such a subfield, and evidently the smallest one. This field is reffered to as the *field generated by Ω and K* and is denoted by $K(\Omega)$. In that case that $\Omega = \{\alpha\}$ one writes $K(\alpha)$ omitting the set brackets. To investigate fields of the form $K(\alpha)$ we must consider two cases. In the first case, suppose $\alpha \in F$ is algebraic over K. Then via the evaluation at α map we see

$$\mathrm{ev}_\alpha(K[x]) = \left\{ \sum_{i=0}^{d} \xi_i \alpha^i | \xi_i \in K \right\} \cong K(\alpha),$$

where d is one less than the degree of m_α.

If instead we suppose α is transcendental, the evaluation map is injective and thus

$$\mathrm{ev}_\alpha(K[x]) = \left\{ \sum_{i=0}^{\infty} \xi_i \alpha^i | \xi_i \in K \right\}.$$

The above is not a field (it is isomorphic to $K[x]$), however every non-zero polynomial in $K[x]$ maps to a unit in F via this map. Hence the by the universal property of localizaiton, the evaluation map extends to a map from the field of fractions of $K[x]$, which we denote by $K(x)$. This is the field of rational functions in K and is easilly seen to be isomorphic to $K(\alpha)$.

Lemma 1.2. *For any field extension F/K one has the following.*

a) An element $\alpha \in F$ is algebraic if and only if $|K(\alpha) : K|$ is finite. In this case $|K(\alpha) : K| = deg(m_\alpha)$.

b) If $\alpha_1, \ldots, \alpha_s \in F$ are algebraic then $|K(\alpha_1, \ldots, \alpha_s) : K| \leq \prod_{i=1}^{s} deg(m_{\alpha_i})$.

Proof. a) $\Leftarrow$: We have already observed that the finiteness of the extension guarantees that all elements of $K(\alpha)$ are algebraic. In particular, α is algebraic.

$\Rightarrow$: By the above

$$K(\alpha) \cong K[x]/(m_\alpha).$$

Thus the set $1, \alpha, \ldots, \alpha^{n-1}$ for $n = \deg m_\alpha$ is clearly a spanning set and linearly independent by minimality of the polynomial m. This establishes *a).*

b) We proceed via induction, noting the case $n = 1$ is given by the preceeding. By Lemma 1.1 we see

$$|K(\alpha_1, \ldots, \alpha_s) : K| = |K(\alpha_1, \ldots, \alpha_s) : K(\alpha_1, \ldots, \alpha_{s-1})||K(\alpha_1, \ldots, \alpha_{s-1}) : K|.$$

By induction $|K(\alpha_1, \ldots, \alpha_{s-1}) : K| \leq \prod_{i=1}^{s-1} \deg(m_{\alpha_i})$. For brevity, define $F' := K(\alpha_1, \ldots, \alpha_{s-1})$. Then $K(\alpha_1, \ldots, \alpha_s) = F'(\alpha_s)$ and by *a*, $|F'(\alpha_s) : F'| = \deg m_{\alpha_s, F'}$. To conlude, simply note that since $m_{\alpha_s, K} \in F'[x]$ and has α_s as a root, $m_{\alpha_s, F'} | m_{\alpha_s, K}$. In particular $\deg m_{\alpha_s, F'} \leq \deg m_{\alpha_s, K}$, establishing the result. □

Proposition 1.3. *For any field extension F/K, the set*

$$\overline{K} := \{\alpha \in F | \alpha \text{ algebraic } \}.$$

is a subfield of F containing K. This is often coined the algebraic closure of F in K.

Proof. Trivially any element $\alpha \in K$, is algebraic over K as it satisfies the polynomial $x - \alpha \in K[x]$. We must still show for any two elements $\alpha, \beta \in \overline{K}$ the elements $\alpha - \beta, \alpha\beta, \beta^{-1} \in \overline{K}$. To see this note the algebraic extension $K[\alpha, \beta]$ contains all such elements, establishing the result. □

Theorem 1.4. *The following are equivalent for a field extension F/K.*

i) F/K is algebraic.

ii) $K(\alpha)/K$ is finite for any $\alpha \in F$.

iii) $K(\alpha_1, \ldots, \alpha_n)/K$ is finite for any collection $(\alpha_i)_{[n]} \subseteq F$.

Moreover algebraicity is well behaved in towers.

Proof. We omit the proof of the equivalences as it has all been justified by previous lemmas. Let $K \subseteq F \subseteq E$ be a tower of fields and suppose that E/K is algebraic. Then trivially F/K is algebraic and E/F is algebraic since $K[x] \subseteq F[x]$.

Conversely suppose both $E/F, F/K$ are algebraic. Let $\alpha \in E$. Then there exists a polynomial

$$f = \sum_{i=0}^{d} a_i x^i,$$

such that all $a_i \in F$ and $f(\alpha) = 0$. Consider then the extension $F' = K[a_0, \ldots, a_d]$. Then α is algebraic over F', and the extension F'/K is algebraic since F/K is an algebraic extension. Therefore by 1.1 we get that $F'(\alpha)/K$ is finite with intermediate extension $K(\alpha)/K$ which must then be finite. □

1.2. **Algebraic Closures.**

We define a field K to be *algebraically closed* if any the following equivalent statements hold.

i) Every non-constant polynomial $f \in K[x]$, splits completely into linear factors.
ii) Every non-constant polynomial $f \in K[x]$ has a root in K.
iii) If F/K is an algebraic extension then $F = K$.

We provide a brief justification of the equivalence of these statements.

i) ⇒ iii) Let F/K be algebraic. Let $\alpha \in F$. Then the minimal polynomial of α in K splits into linear factors. Since minimal polynomials are irreducible this gives that it is a linear polynomial itself and hence $\alpha \in K$.

iii) ⇒ ii) Consider the polynomial $f \in K[x]$. By formal adjunction of roots there exists an extension F/K such that f has a root. Moreover this field is finite and thus algebraic, giving that $F = K$, giving that the root is an element of K as desired.

ii) ⇒ i) This is trivially true via induction.

We remark here that algebraically closed fields are necessarily infinite since for any finite field $\mathbb{F}_n$ the polynomial

$$\prod_{\alpha \in \mathbb{F}_n} (x - \alpha) + 1,$$

has no roots. Additionally we remark that for any infinte field K, any algebraic extension F/K necessarily has the same cardinality as K. This is almost entirely a result of set theory and we omit the proof in favor of a few standard examples. The field

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \,|\, \alpha \text{ algebraic over } \mathbb{Q}\}.$$

is therefore countable as it is an algebraic extension of the countable field $\mathbb{Q}$. $\overline{\mathbb{Q}}$ is often referred to as the field of algebraic numbers. For our final remark, $\mathbb{C}$ is an algebraically closed field, the best proof of which uses Liouville's Theorem from complex analysis. At this point we have defined both what the algebraic closure of a field extension, and what it means for a field to be algebraically closed. We can similarly define the *algebraic closure* of a field K. An extension field $\overline{K}$ of K is an algebraic closure if both of the following hold:

a) $\overline{K}$ is algebraic.
b) Every non-constant polynomial $f \in K[x]$ splits into linear factors in $\overline{K}$.

With this definition in mind we can connect algebraic closures of fields to algebraic closures of extensions via the following lemma.

Lemma 1.5. *The following are equivalent for an extension F/K.*

i) F is an algebraic closure of the base field K.
ii) F/K is algebraic and F is algebraically closed.
iii) F/K is algebraic but E/K is not algebraic for any proper extension $F \subsetneq E$.

Proof. ii) $\Rightarrow$ i) This is trivial as F being algebraically closed is much stronger than the second condition in the above definition. The fact that all polynomials in $F[x]$ split gives that surely all polynomials in $K[x]$ split.

i) $\Rightarrow$ iii) Consider an algebraic extension E/K. Let $\alpha \in E$. Then the minimal polynomail $m_{\alpha,K}$ splits into linear factors in F. In particular since minimal polynomials are irreducible we must have $m_{\alpha,K} = x - \alpha$, giving $\alpha \in F$ as desired.

iii) $\Rightarrow$ ii) Let E/F be an algebraic extension. Then E/K is algebraic, by well-behavedness of algebraicity, giving that $E = F$, hence F is algebraically closed. □

There is the natural question as to whether or not algebraic closures exist for all fields. We present two methods to proof that such constructions are possible. First, for most intents and purposes the field one is working with is a subfield of the complex numbers $\mathbb{C}$ or some other algebraically closed field.

Proposition 1.6. *Let $K \subseteq F$ be fields, F algebraically closed. Then the intermediate field*

$$\overline{K} = \{\alpha \in K | \alpha \text{ algebraic over } K\},$$

is an algebraic closure of K.

Proof. Clearly $\overline{K}$ is by definition an algebraic extension of K. Now consider a polynomial $f \in K[x]$. In the algebraically closed field $F[x]$ we have

$$f = (x - \alpha_1) \dots (x - \alpha_d).$$

Now each α_i is algebraic over K, thus each $\alpha_i \in \overline{K}$ and hence the factorization above is in $\overline{K}[x]$. □

Thus, as described previously the field $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$. Ideally one would be able to construct an algebraic closure of any base field K, from only the field itself, independent of an algebraically closed extension field, which need not, a priori, exist. That leads to the following theorem, which is attributed to Ernst Steinitz, the proof we present is Emil Artin's.

Theorem 1.7. *Every field had an algebraic closure $\overline{K}/K$. Moreover this field is unique up to K-isomorphism.*

Proof. Set $\mathscr{S} = K[x] \setminus K$. Form the polynomial ring $R = K[x_f | f \in \mathscr{S}]$. Every $r \in R$ is a finite K-linear combination of finite products of the variables x_f. Set $I = (f(x_f) | f \in \mathscr{S})$. We claim I is a proper ideal and prove this via contradiction. Supposing otherwise, we'd then have

$$1 = r_1 f_1(x_1) + \dots r_t f_t(x_t),$$

for some $r_i \in R$ and some collection $f_1, \dots, f_t \in \mathscr{S}$. For each f_i there exists a field which has a root of f_i, α_i. Finding this fields iteratively we get a field F that has the roots $\alpha_1, \dots, \alpha_t$ for $f_1, \dots, f_t$. Now consider the following evaluation K-homomorphism $\epsilon : R \to F$ which maps $x_i \mapsto \alpha_i$ for each $i \in [t]$ and maps all other variables to 0. Then applying this map to the above equation we see

$$1 = \epsilon(r_1) f(\alpha_1) + \dots \epsilon(r_t) f(\alpha_t) = 0,$$

the desired contradiction.

Now, fix a maximal ideal $M \subseteq R$ containing I, and define $K' = R/M$. K' is a field generated over K by the residue classes $\alpha_f = x_f + M$, which all satisfy $f(\alpha_f) = 0$. Then K'/K is thus algebraic and each $f \in K[x]$ has a root in K'. We now recursively define an infinite tower of fields by

$$K_0 = K, \quad K_{i+1} = K_i',$$

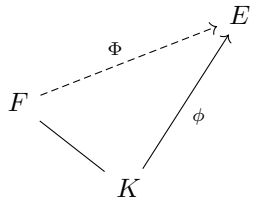
where K_i' is the construction as above. Then

$$\overline{K} = \bigcup_{i>0} K_i,$$

is a field which is algebraic over K. Now we claim $\overline{K}$ is algebraically closed, which will complete the proof of existence. Let $f \in \overline{K}[x]$. Then $f \in K_i[x]$ for some i and has a root in K_{i+1}, giving every polynomial in $\overline{K}[x]$ has at least one root. Hence $\overline{K}$ is algebraicailly closed, establishing existence of an algebraic closure.

For uniqueness we consider the following lemma.

Lemma 1.8. *Let $\phi : K \to E$ be a field homomorphism with E an algebraically closed field. Then for any algebraic extension F/K there exists a homomorphism $\Phi : F \to E$, such that $\Phi|_K = \phi$. This can be visualized by the following diagram*



Granting the proof for the time being, we prove uniqueness. Suppose the fields $\overline{K}, \widetilde{K}$ are algebraic closures of K. Then for $\phi : K \hookrightarrow \overline{K}$, we obtain a map $\Phi : \widetilde{K} \to \overline{K}$, which is injective since it is not the trivial homomorphism. Thus we have the tower of fields $K \subseteq \Phi(\widetilde{K}) \subseteq \overline{K}$. Since $\overline{K}/K$ is algebraic, $\overline{K}/\Phi(\widetilde{K})$ is algebraic. But since algebraic closures have no nontrivial algebraic extensions we get $\Phi(\widetilde{K}) = \overline{K}$ giving $\overline{K} \cong \widetilde{K}$, as desired.

The proof of lemma 8 can be a bit involved with only the present tools we have developed. Thus we postpone the proof til after we develop the notion of the tensor product. □

1.3. **Splitting Fields & Normal Extensions.**

Given some collection of non-constant polynomials $\mathscr{S} \subseteq K[x] \setminus K$, we define the *splitting field of* $\mathscr{S}$ to be the minimal such extension F/K in which all polynomials in $\mathscr{S}$ split completely. We say a field extension is *normal* if it is the splitting field for some collection $\mathscr{S} \subseteq K[x] \setminus K$. Note that if $\mathscr{S} = \{f_1, \ldots, f_n\}$, then a splitting field for $\mathscr{S}$ is the same as the splitting field for the collection

$$\mathscr{S}' = \left\{ \prod_{i=1}^{n} f_i \right\}.$$

We also claim that all normal extensions must be algebraic. Say F/K is the splitting field for some collection of non-constant polynomials $\mathscr{S} \subseteq K[x] \setminus K$. Then

each $f \in \mathscr{S}$ factors in F as

$$f = \mathrm{LC}(f)(x - \alpha_{f,1}) \dots (x - \alpha_{f,d_f}).$$

where $\mathrm{LC}(f)$ denotes the leading coefficient of f and $\alpha_{f,i} \in F$. Then we see $F = K[\alpha_{f,i} | f \in \mathscr{S}]$. Considering the tower

$$K \subseteq \overline{F} \subseteq F,$$

where $\overline{F} = \{\alpha \in F | \alpha \text{ algebriac over } F\}$ as in Proposition 1.6, we see that each $\alpha_{f,i} \in \overline{F}$ and thus we must have equality.

Proposition 1.9. *There exists a splitting field, F, for any given collection $\mathscr{S} \subseteq K[x] \setminus K$. Moreover F is unique up to K-isomorphism and if $\mathscr{S} = \{f\}$ with $deg f = n$, then $[F : K] \leq n!$.*

Proof. For existence, let $\overline{K}/K$ be an algebraic closure for K. In $\overline{K}$ each $f \in \mathscr{S}$ factors as

$$f = \mathrm{LC}(f)(x - \alpha_{f,1}) \dots (x - \alpha_{f,d_f}).$$

Then it is easy to see that $F = K[\alpha_{f,i} | f \in]$ is a desired splitting field.

For uniqueness let F' be another splitting field for the collection $\mathscr{S}$. Then by Lemma 1.8 the inclusion map $K \hookrightarrow \overline{K}$ extends to a homomorphism $\Phi : F' \to \overline{K}$ which is the identity when restricted to K. All f split completely over F' and hence split completely over $\Phi(F') \subseteq \overline{K}$. Therefore $F \subseteq \Phi(F')$.

In the case where $\mathscr{S} = \{f\}$ with $\deg f = n$, we prove the bound by induction on n with the base case being trivial. Now let $\alpha \in F$ be a root of f. Then $f = (x - \alpha)g$ for some $g \in E_f[x]$. By induction, the polynomial g has some splitting field E_g with $[E_g : K] \leq (n-1)!$. Consider the following tower of fields $F \subseteq E_g \subseteq E_f$ Then since $E_f = E_g[\alpha]$ and $m_{\alpha,E_g} | f$ we see $[E_f : E_g] \leq n$. Therefore by multiplicativity of field degrees in towers we get

$$[E_f : K] = [E_f : E_g][E_g : K] \leq n!.$$

□

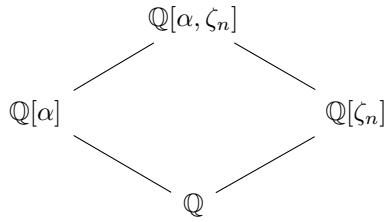
Extensions of degree two are always normal. This is because if $F = K + K\alpha = K[\alpha]$ then $[F : K] = 2$, giving the minimal polynomial of α in K has degree two. Then in F we get

$$m_{\alpha,K} = (x - \alpha)(x - \beta),$$

and thus F is the splitting field for $m_{\alpha,K}$. For $\zeta_n = e^{2\pi i/n}$, the field $\mathbb{Q}[\zeta_n]$ is the splitting field for Φ_n and for $x^n - 1$.

Consider the polynomial $f = x^n - a \in \mathbb{Q}[x]$ with $n \geq 2$ and $a \in \mathbb{Z}_{>0}$. The roots of f in $\mathbb{C}$ are $\alpha\zeta_n^j$ for $\alpha = \sqrt[n]{a}, \zeta_n$ as defined above and $j \in \{0, \dots, n-1\}$. It is then easy to see that the splitting field for f is given by $\mathbb{Q}[\alpha, \zeta_n]$. We now consider further the subcase where $(n, \varphi(n)) = 1$ and there exists a prime $p \in \mathbb{Z}$ such that $p | a, p^2 \nmid a$. These assumption give that $x^n - a$ is irreducible by Eisenstein's criterion.

We then get the following field diagram



By assumption $x^n - a$ is the minimal polynomial for α giving $[\mathbb{Q}[\alpha] : \mathbb{Q}] = n$ and we know $[\mathbb{Q}[\zeta_n] : \mathbb{Q}] = \varphi(n)$. Moreover since $(n, \varphi(n)) = 1$ we get that $\mathbb{Q}[\alpha, \zeta_n] = n\varphi(n)$.

Proposition 1.10. *The following are equivalent for a field extension F/K.*

i) F/K is normal.
ii) F/K is algebraic and for each $\alpha \in F$, the minimal polynomial for α in $K[x]$ splits completely in $F[x]$.
iii) F/K is algebraic and for each irreducible polynomial $f \in K[x]$, if f has a root in F, it splits completely in $F[x]$.

Proof. iii) $\Rightarrow$ ii): This is trivial as all minimal polynomials have a root.

ii) $\Rightarrow$ i): If *ii)* holds then F is clearly seen to be the splitting field of the collection of all minimal polynomials for $\alpha \in F$.

i) $\Rightarrow$ iii): Supposing F/K is normal, then by previous observation, F/K is algebraic. Let $f \in K[x]$ be a monic irreducible polynomial with $\alpha \in F$ satisfying $f(\alpha) = 0$. Consider the tower of fields $K \subseteq F \subseteq \overline{F}$ where $\overline{F}$ is an algebraic closure of F. In $\overline{F}$, the polynomial f splits completely as

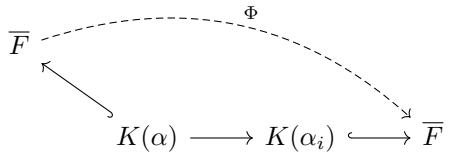
$$f = (x - \alpha)(x - \alpha_2) \dots (x - \alpha_d),$$

where $\alpha_i \in \overline{F}$. We then claim there exists a unique K-isomorphism $K(\alpha) \to K(\alpha_i)$ for any i. To see this, we have the following isomorphisms

$$K(\alpha) \cong K[x]/(f) \cong K(\alpha_i),$$

given explicity by the assignments $\alpha \mapsto x \mapsto \alpha_i$. Moreover since any K-isomoprhism of $K(\alpha)$ is completely determined by where it sends α we see this assignment is unique.

We now apply Lemma 1.8 to the following diagram



to get a map K-homomorphism $\Phi : \overline{F} \to \overline{F}$. Moreover, since K-homomorphisms send roots of polynomials to roots of polynomials, we see that it is enough to show that $\Phi(F) \subseteq F$. To this end, recall that F is the splitting field of some collection $\mathscr{S} \subseteq K[x] \setminus K$ with $F = K(\alpha_{i,g} | \alpha_i \text{ is a root } g \in \mathscr{S})$. Hence it is enough to show that $\Phi(\alpha_{i,g}) \in F$ for any $g \in \mathscr{S}$. But, since Φ is a K-homomorphism, it sends roots of g to roots of g for any $g \in \mathscr{S}$ and hence $\Phi(\alpha_{i,g}) \in F$, completing the proof. $\square$

1.4. **Separability.**

Throughout K is a field. A polynomial $f \in K[x]$ is said to be *separable* if f has no multiple roots in its splitting field.

Lemma 1.11. *The following are equivalent for $f \in K[x]$.*

i) f is separable.
ii) f and its formal derivative f' have no common root.
iii) The ideal $(f, f') = K[x]$. That is, these polynomials are relatively prime.

Moreover, in the case where f is an irreducible polynomial, then f is separable if and only if $f' \neq 0$.

Proof. Let $F = \overline{K}$ be an algebraic closure for K.
i) $\Leftrightarrow$ ii): Suppose f, f' share the root $\alpha \in \overline{K}$. Then

$$f = (x - \alpha)g$$
$$f' = (x - \alpha)h$$

for some $g, h \in F[x]$. Then applying the product rule of formal differentiation

$$f' = g + (x - \alpha)g' = (x - \alpha)h,$$

and thus $(x - \alpha)|g$ and hence α is a double root for f. Moreover if $(x - \alpha)^2|f$ then $(x - \alpha)|f'$ and we see that f, f' share the root α. This gives both implications.

ii) $\Rightarrow$ iii): Suppose, by way of contradiction that f, f' do not share a common root and $(f, f') \subsetneqq K[x]$. Then since $K[x]$ is a PID, $(f, f') = (g)$ for some non-constant $g \in K[x]$. Then any roots of g is a root of both f, f' contradicting the assumption that they shared no roots.

iii) $\Rightarrow$ii): If $(f, f') = K[x]$, then in particular we have the existence of some $g, h \in K[x]$ such that

$$1 = fg + f'h.$$

Any common root of f, f' would then be a root of the constant polynomial 1 and hence f, f' share no common roots.

Finally, if f is irreducible, then (f) is maximal. Then, since $\deg f' = \deg f - 1$, we see f is separable if and only if $f' \notin (f)$ which happens precisely when $f' \neq 0$. $\square$

There is also a notion of separability for field extensions. An extension F/K is said to be *separable* if for any $\alpha \in F$, the minimal polynomial of α over K is separable. Similarly an element is separable if its minimal polynomial is separable. We say a field K is *perfect* is every algebraic extension over K, is separable. We note this definition is equivalent to asking all irreducible polynomials $f \in K[x]$, be separable which by Lemma 1.11 is equivalent to each irreducible polynomial having non-zero deriviative.

Theorem 1.12. *The field K is perfect if and only if $charK = 0$ or $charK = p > 0$ and $K^p = K$.*

Proof. First, assume $\mathrm{char}K = 0$ and $f \in K[x]$ is irreducible. Then since f is not constant, $f' \neq 0$ and hence f is separable. Therefore K is perfect.

Now suppose $\mathrm{char}K = p > 0$. We aim to show K is perfect if and only is the Frobenius map $\Phi : K \to K$ given by $\zeta \mapsto \zeta^p$ is onto. First assume the Frobenius is

onto. Suppose, by way of contradiction, that there exists some irreducible $f \in K[x]$ such that $f' = 0$. Write

$$f(x) = \sum_{i=0}^{n} a_i x^i.$$

Then

$$f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}.$$

Since $f' = 0$, for $i \not\equiv 0 \pmod{p}$ we must have $a_i = 0$. Hence

$$f(x) = a_0 + a_p x^p + \dots,$$

and since the Frobenius is onto we can write $a_{ip} = \beta_i^p$ for each i. Then

$$\begin{aligned} f(x) &= \beta_0^p + \beta_1 x^p + \dots \\ &= \left(\sum_{i=0}^{n} \beta_i x^{ip} \right)^p \end{aligned}$$

and clearly this polynomial is not irreducible, reaching the desired contradiction.

Suppose now K is perfect and let $\alpha \in K$. Consider the polynomial $f(x) = x^p - a \in K[x]$. We see $f' = 0$ and hence this polynomial is not irreducible by Lemma 1.11. In an algebraic closure $\overline{K}$ there exists a root β of f and therfore $\beta^p = \alpha$. In $\overline{K}[x]$, $f = (x - \beta)^p$. But since f is not irreducible in $K[x]$ we get the existence of non-constant poylnomials $g, h \in K[x]$ such that

$$gh = f = (x - \beta)^p.$$

Thus by unique factorization in $\overline{K}[x]$ we see some power $(x - \beta)^r \in K[x]$. The coefficient of x^{r-1} in this polynomial is $-r\beta$ and thus $\beta \in K$. Hence the Frobenius map is onto. □

We remark here that all finite fields are perfect since the Frobenius map is an injective field homomorphism from finite sets of the same order and hence an automorphism of F.

1.5. **An Application: The Structure of Finite Fields.**

Let F be a finite field, say $|F| = q$. We now $q = p^r$ for some prime p, $r \geq 0$, Also for any $\alpha \in F$, $\alpha^q = \alpha$. Then the polynomial $x^q - x$ has solutions all elements of F. That is,

$$x^q - x = \prod_{\alpha \in F} (x - \alpha).$$

Thus $F = \{\text{roots of } x^q - x\}$ and is also the splitting field of $x^q - x \in \mathbb{F}_p[x]$. In particular the extension $F/\mathbb{F}_p$ is normal and separable since all finite fields are separable.

Given some $q = p^r$ with p, prime, $r > 0$, there is the question on the existence of a finite field of order q. Taking influence from the above, we conjecture that the splitting field of $x^q - x \in \mathbb{F}_p[x]$ is such a field. Let F denote this field. F is clearly finite as it is a finite extension of a finite deimensional vector space. Consider the

subfield

$$\begin{aligned} K &= \{\alpha \in F | \alpha \text{ is a root of } x^q - x\} \\ &= \{\alpha \in F | \alpha^q = \alpha\} \\ &= K^{\Phi^r} \end{aligned}$$

where Φ denotes the Frobenius and K^{Φ^r} denotes the fixed field of Φ^r. Hence K is subfield of F containing all roots of the polynomial $x^q - x$. But by minimality of the splitting field, this means $F \subseteq K$ and hence $F = K$. Thus the extension F is precisely the field of all roots of $x^q - x$ and since the formal derivative of $x^q - x$ is -1, it is separable, giving $|F| = q$, as desired. We summarize the results of the above paragraphs in the following theorem.

Theorem 1.13. *Given $q = p^r$ for some prime p, $r \in \mathbb{Z}_{\geq 0}$, there exists a field F of size q and F is unique up to isomorphism as the splitting field of $x^q - x$ over $\mathbb{F}_p[x]$.*

To conclude this study of finite fields we present the following lemma.

Lemma 1.14. *The multiplicative group of any finite field $\mathbb{F}_q$ is C_{q-1}. More generally, for any field K, $G \leq K^\times$, with G finite, G is cyclic.*

Proof. Since G is finite, abelian, it is a finite nilpotent group and thus

$$G \cong P_1 \times \cdots \times P_r,$$

where P_i denote the distinct Sylow subgroups of G. Thus it suffices to show each P_i is cyclic, since the direct product of cyclic groups of coprime order is cyclic. Hence we may restrict ourselves to the case where $|G| = p^n$. Let p^m be the largest order of any element in G. Then

$$\alpha^{p^m} = 1,$$

for all $\alpha \in G$. Hence all elements of G are roots of the polynomial

$$x^{p^m} - 1,$$

There are at most p^m such roots of this polynomial giving $|G| \leq p^m$. Thus it must hold that $n = m$, and hence G has ane element of order of p^n and is therefore cyclic. □

1.6. **More on Separability.**

The paragraphs of this section will be spent proving the following theorem, which summarizes the important facts on separability.

Theorem 1.15.

a) Separability is well behaved in towers.

b) Given any field extension F/K, the set

$$\widetilde{K} = \{\alpha \in F | \alpha \text{ is separable over } K\},$$

defines a subfield of F.

c) Let F/K be algebraic and let $\widetilde{K}$ be as defined in b. Then the extension $F/\widetilde{K}$ is purely inseparable. That is, for any $\alpha \in F$, the minimal polynomial of α over $\widetilde{K}$ has precisely one root.

Proof. Before developing further theory on separability, we are currently capable of proving one direction of *a)*. Let $K \subseteq F \subseteq E$ be a tower of fields and suppose E/K is separable. Then certainly the extension F/K is separable as $F \subseteq E$. E/F

is also separable since for any $\alpha \in E$, $m_{\alpha,F}|m_{\alpha,K}$ and since $m_{\alpha,K}$ has no repeated roots, this gives $m_{\alpha,F}$ has no repeated roots.

For the other direction of *a)* we must first develop the notion of the *separable degree*. For an algebraic field extension F/K, separable degree is defined as

$$[F:K]_S = |\{\text{all } K\text{-homomorphisms } \sigma : F \to \overline{K}\}|,$$

where $\overline{K}$ is an algebraic closure for K. By 1.8 the standard embedding $K \hookrightarrow F$ extends to a map $F \to \overline{K}$ and thus $[F:K]_S \geq 0$. The utility of the separable degree is made evident via the following proposition.

Proposition 1.16.

a) Separable degrees are multiplicative in towers.
b) If F/K is finite, then

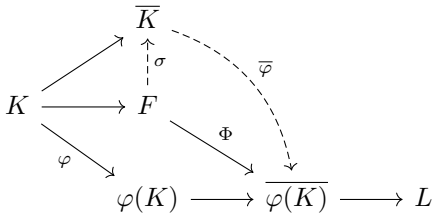
$$[F:K]_S \leq [F:K],$$

with equality if and only if the extension is separable.

Proof. To begin the proof of the proposition, we reformulate the definition of the separable degree. We claim, for some homomorphism $\varphi : K \to L$ with L algebraically closed, then

$$[F:K]_S = |\{\Phi : F \to L | \Phi|_K = \varphi\}|.$$

To see this, consider the following diagram



where $\overline{\varphi(K)} = \{\alpha \in L | \alpha \text{ algebraic over } \phi(K)\}$. By 1.8 the map $\varphi : K \to L$ extends to the map denoted $\overline{\varphi} : \overline{K} \to L$. Moreover since $\overline{K}/K$ is algebraic and K any the root of any polynomial in $f \in K[x]$ is mapped to a root of $\varphi(f)$, we get that $\overline{\varphi}$ is in fact a map $\overline{K} \to \overline{\varphi(K)}$. Moreover, the extension $\overline{\varphi(K)}/\overline{\varphi}(\overline{K})$ is algebraic and hence $\overline{K} \cong \overline{\varphi(K)}$. Therefore we get a bijection of maps

$$\{K - \text{homomorphisms } F \to \overline{K}\} \leftrightarrow \{\Phi : F \to L | \Phi|_K = \varphi\},$$

given by the assignments

$$\sigma \mapsto \overline{\varphi} \circ \sigma \circ \overline{\varphi}^{-1},$$
$$\Phi \mapsto \overline{\varphi}^{-1} \circ \Phi \circ \overline{\varphi}.$$

This establishes our reformulation of the separable degree.

With this in mind, we can now prove the proposition. For *a)*, let $K \subseteq F \subseteq E$ be a tower of algebraic extensions and let $\varphi : K \to L$ be a given homomorphism into the algebraically closed field L. Let $\{\Phi_i\}_{i \in I}$ be the collection of distinct extensions $F \to L$. By the above claim we see $|I| = [F:K]_S$. Then, for each Φ_i, let $\{\Phi_{i,j}\}_{j \in J}$ be the distinct extensions of Φ_i, $E \to L$. Again, by the claim, $|J| = [E:K]_S$. Thus we have construction $[E:F]_S[F:K]_S$ extensions of φ, $E \to L$. Moreover, all such

extensions arise in this manner, since any such extension restricted to F must be one of the Φ_i. Thus we achieve

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

proving *a)*.

In order to prove *b)* we first restrict ourselves to the case of simple algebraic extensions. Let $F = K(\alpha)$ be a simple algebraic extension of K. Then we claim

$$[K(\alpha) : K]_S = |\{\text{distinct roots of } m_{\alpha,K}\}|.$$

This is because any K-homomorphism of K must send roots of $m_{\alpha,K}$ to roots of $m_{\alpha,K}$. Moreover for any other roots α_i of $m_{\alpha,K}$ we have the K-isomorphism

$$K(\alpha) \cong K(\alpha_i),$$

which uniquely extends to K-homomorphism $K(\alpha) \to \overline{K}$ since any K-homomorphism of $K(\alpha)$ is uniquely determined by what it does to α. In particular we see

$$[K(\alpha) : K] = \deg(m_{\alpha,K}) \geq |\{\text{distinct roots of } m_{\alpha,K}\}| = [K(\alpha) : K]_S,$$

with equality if and only if $m_{\alpha,K}$ is separable.

We now prove *b)* by induction of $[F : K]$ with the base case $[F : K] = 1$ being trivial. Proceeding inductively, let $\alpha \in F \setminus K$. Considering the field tower $K \subseteq K(\alpha) \subseteq F$, by part *a)*,

$$[F : K]_S = [F : K(\alpha)]_S[K(\alpha) : K]_S \leq [F : K(\alpha)][K(\alpha) : K] = [F : K],$$

where $[K(\alpha) : K]_S \leq [K(\alpha) : K]$ from our examination of the case of simple extensions above, and the other inequality via induction. We note here that equality holds if and only if $[K(\alpha) : K]_S = [K(\alpha) : K], [F : K(\alpha)]_S = [F : K(\alpha)]$. Again, by our analysis of the case of simple extensions, the equality $[K(\alpha) : K]_S = [K(\alpha) : K]$ implies α is separable and since our choice of α was arbitrary, we see $[F : K]_S = [F : K]$ implies separability of F/K. For the other direction, note that by the already proven direction of separability behaving well in towers, F/K separable implies $F/K(\alpha), K(\alpha)/K$ are both separable. Then by induction on degrees we get eqaulity. This completes the proof of the proposition. □

Having proved Proposition 1.16, we now have the tools to complete the proof of Theorem 1.15. We first prove the other direction of separability being well-behaved in towers. Let $K \subseteq F \subseteq E$ be a tower of fields and suppose the extensions $F/K, E/F$ are separable. We aim to show for any $\alpha \in E$, $m_{\alpha,K}$ is separable. Since E/F is separable we have

$$m_{\alpha,F} = \sum_{i=1}^{d} \varphi_i x^i,$$

is separable. Consider the subfields $F' = K(\varphi_i | \text{ all } i)$, $E' = F'(\alpha)$. We then have the tower of fields $K \subseteq F' \subseteq E'$ where $E'/F', F'K$ is finite. Moreover, F'/F is a subextension of F/K and therefore separable. Moreover α is separable over F' since α is separable over F and $m_{\alpha,F} = m_{\alpha,F'}$.

Now, consider the tower $K \subseteq F' \subseteq F'(\alpha)$. Then we have

$$\begin{aligned} |F'(\alpha) : K| &= |F'(\alpha) : F'|F' : K|, \\ &= |F'(\alpha) : F'|_S|F' : K|_S, \\ &= |F'(\alpha) : K|_S. \end{aligned}$$

If we also consider the tower $K \subseteq K(\alpha) \subseteq F'(\alpha)$, since the above gives $|F'(\alpha) : K| = |F'(\alpha) : K|_S$, we then must have

$$|K(\alpha) : K| = |K(\alpha) : K|_S.$$

Therefore α is separable over K.

For *b)*, let $\alpha, \beta \in \widetilde{K}$. Then consider the tower of fields

$$K \subseteq K(\alpha) \subseteq K(\alpha, \beta).$$

Both $K(\alpha)/K, K(\alpha, \beta)/K(\alpha)$ are separable and by *a)* we get $K(\alpha, \beta)/K$ is separable. Hence $\alpha\beta, \alpha^{-1}, \alpha \pm \beta$ are all separable over K. This establishes *b)*.

Let $\alpha \in F$, $m_{\alpha,\widetilde{K}}$ be its minimal polynomial. In characteristic 0, all algebraic extensions are separable, hence F/K is a separable extension, giving $\widetilde{K} = F$.

Thus, we assume $\mathrm{char}K = p > 0$. We then claim that for every $\alpha \in F$ there exists some $n \geq 0$ such that $\alpha^{p^n} \in \widetilde{K}$. This will establish the result since then α will be a root of $x^{p^n} - \alpha^{p^n} \in K[x]$ and thus

$$m_{\alpha,\widetilde{K}} | x^{p^n} - \alpha^{p^n} = (x - \alpha)^{p^n},$$

giving α is the only root of $m_{\alpha,\widetilde{K}}$.

For $\alpha \in \widetilde{K}$ we may simply take $n = 0$. Thus, assume $\alpha \notin \widetilde{K}$ and induct on $\deg m_{\alpha,K} = |K(\alpha) : K|$. Since $\alpha \notin \widetilde{K}$, α is not separable over K and thereofre $m'_{\alpha,K} = 0$. Hence

$$m_{\alpha,K} = a_0 + a_1 x^p + \ldots,$$

or $m_{\alpha,K} = f(x^p)$ for some $f \in K[x]$. Then $f(\alpha^p) = 0$ and since $\deg f < \deg m_{\alpha,K}$, we get

$$\deg m_{\alpha^p,K} < \deg m.$$

Thus, by induction, α^p has a p^m power in $\widetilde{K}$ and we therefore have $\alpha^{p^{m+1}} \in \widetilde{K}$, as desired. □

In analogue with the definitions of algebraic closures for a field extension and algebraic closures for a single base field, we have a notion of the *separable closure* for a given field K. If we denote by K^{alg} the algebraic closure for K, then we define the separable closure of K to be

$$K^{\mathrm{sep}} = \{\alpha \in K^{\mathrm{alg}} | \alpha \text{ is separable over } K\}.$$

Proposition 1.17. *Given a field K, K^{sep} is a separable algebraic extension, and K^{sep} is separably closed: If F/K^{sep} is a separable algebraic extension, $F = K^{sep}$. Moreover, K^{sep} is uniquely determined up to K-isomorphism.*

Proof. Evidently K^{sep}/K is a separable algebraic extension. Let F/K^{sep} be a separable algebraic extension. By Lemma 1.8, applied to the standard embedding $\varphi : K^{\mathrm{sep}} \hookrightarrow K^{\mathrm{alg}}$ we get a K^{sep}-homomorphism $\overline{\varphi} : F \to K^{\mathrm{alg}}$. Set $F' = \overline{\varphi}(F)$. Then we have the tower of fields

$$K^{\mathrm{sep}} \subseteq F' \subseteq K^{\mathrm{alg}}.$$

Observe that F'/K^{sep} is a separable extension since $m_{\overline{\varphi}(\alpha),K^{\mathrm{sep}}} = m_{\alpha,K^{\mathrm{sep}}}$ and F/K^{sep} is a separable extension. Thus F'/K is separable by Theorem 1.15 *a)* and hence $F' \subseteq K^{\mathrm{sep}}$, as desired.

Uniqueness is an exercise on homework assignment 3. □

We remark here that K^{sep}/K is a normal extension. To show this, we need the following lemma.

Lemma 1.18. *Let F/K be normal extensions and set*

$$F_S = \{\alpha \in F | \alpha \text{ is separable over } K\}.$$

Then F_S/K is also normal.

Proof. Let $\alpha \in F_S$. By assumption $m_{\alpha,K}$ splits completely in F. Hence we can write

$$m_{\alpha,K} = \prod_{i=1}^{d}(x - \alpha_i),$$

where evidently all α_i are distinct in F. Thus each $\alpha_i \in F_S$, in particular $\alpha \in F_S$ as desired. □

Clearly our above claim follows from the lemma.

1.7. **Galois Extensions.**

Throughout F is a field. The set of field automorphisms of F, denoted $\text{Aut}(F)$ forms a group under composition and is called the *automorphism group* of F. More generally, given a field extensions F/K the set

$$\text{Aut}(F/K) := \{\sigma \in \text{Aut}(F) | \sigma|_K = \text{Id}_K\} \leq \text{Aut}(F),$$

is the *automorphism group of* F over K. We note here that any automorphism of F is an automorphism fixing its prime subfield $F_0 \subseteq F$. Then we can say $\text{Aut}(F) = \text{Aut}(F/F_0)$

We now work through the common examples. For the first example, we claim

$$\text{Aut}(\mathbb{R}) = \text{Aut}(\mathbb{R}\,/\,\mathbb{Q}) = \{1\}.$$

To that end, let $\varphi \in \text{Aut}(\mathbb{R}), \alpha \in \mathbb{R}$. Observe that if $\alpha > 0$ then $\varphi(\alpha) > 0$. This is because $\alpha = \beta^2$ for some $\beta \in \mathbb{R}$ and thus we can write $\varphi(\alpha) = \varphi(\beta)^2 > 0$. We therefore have that φ is order preserving. Now, suppose $\varphi(\alpha) \neq \alpha$ and suppose $\varphi(\alpha) > \alpha$. Then there exists some rational $q \in (\alpha, \varphi(\alpha))$ and we have the inequailities

$$\alpha < q < \varphi(\alpha).$$

Applying φ to $\alpha < q$ we get $\varphi(\alpha) < q$, a contradiction.

Next, observe $\text{Aut}(\mathbb{C}\,/\,\mathbb{R}) = C_2$, consisting of identity and complex conjugation. To see this, let $a + bi \in \mathbb{C}$. Any map $\varphi \in \text{Aut}(\mathbb{C}\,/\,\mathbb{R})$ is thus determined by where it maps i. Then since roots of polynomials over $\mathbb{R}$ must be sent to roots of the same polynomial, we see i can only be sent to $\pm i$, the two roots of $x^2 + 1$.

For any finite field $\mathbb{F}_q$, $q = p^r$.

$$\text{Aut}(\mathbb{F}_q) = \langle \Phi \rangle \cong C_r,$$

where Φ denotes the Frobenius automorphism. To see this, we first prove that $\Phi \in \text{Aut}(\mathbb{F}_q)$ has order r. By Fermat's Little theorem, $\Phi^r = \text{Id}_{\mathbb{F}_q}$. Moreover, if for some $0 < s < r$, $\Phi^s = \text{Id}$, we'd then have all elements of $\mathbb{F}_q$ would be roots of the polynomial

$$x^{p^s} - x,$$

a contradiction. Hence $\langle \Phi \rangle \cong C_r$.

By a similar argument

$$\begin{aligned}\mathbb{F}_q^{\Phi} &= \{\alpha \in \mathbb{F}_q \,|\Phi(\alpha) = \alpha\},\\ &= \{\alpha \in \mathbb{F}_q \,|\alpha^p = \alpha\},\\ &= \mathbb{F}_p\,.\end{aligned}$$

since surely $\mathbb{F}_p \subseteq \mathbb{F}_q^{\Phi}$ and there can be at most p roots of the polynomial $x^p - x$. Also, recall that $\mathbb{F}_q^{\times} \cong C_{q-1}$ by Lemma 1.14.

Thus, let $\varphi \in \mathrm{Aut}(\mathbb{F}_q), \alpha \in \mathbb{F}_q$. Consider the polynomial

$$f = \prod_{i=0}^{r-1}(x - \Phi^i(\alpha)).$$

Written in this form, we see f is fixed under the map applying Φ to the coefficients of f. Therefore $f \in \mathbb{F}_p[x]$. Thus since φ is the identity on $\mathbb{F}_p$, φ must send roots of f to roots of f. Hence $\varphi(\alpha) = \Phi^i(\alpha)$ for some i, as desired.

For the final example, we show the failure of automorphism groups in examining inseparable extensions. Let F/K be an algebraic extension, F_S be as denoted in Lemma 1.18. Then we claim $\mathrm{Aut}(F/F_S) = \{1\}$. If $\mathrm{char}K = 0$, then all algebraic extensions are separable, and hence $F = F_S$. Thus we may assume $\mathrm{char}K = p > 0$. Then via the claim in the proof of Theorem 1.15 *c)*, for any $\alpha \in F$ there exists some $n \geq 0$ such that $\alpha^{p^n} \in F_S$. Let $\varphi \in \mathrm{Aut}F/F_S$. Then $\varphi(\alpha^{p^n}) = \alpha^{p^n}$. Thus we see

$$0 = \varphi(\alpha)^{p^n} - \alpha^{p^n} = (\varphi(\alpha) - \alpha)^{p^n},$$

and hence $\varphi(\alpha) = \alpha$.

For any subgroup $G \leq \mathrm{Aut}(F)$ we define the *fixed field of* G to be

$$F^G := \{\alpha \in F | \sigma(\alpha) = \alpha \text{ for all } \sigma \in G\}.$$

This is plainly seen to be the intersection of the fixed field of all elements of G and thus, as the intersection of subfields, is itself a subfield of F. There is no necessity that G be a group in the above definition to obtain a subfield. However, note for any subset $S \subseteq \mathrm{Aut})(F)$, $F^S = F^{\langle S\rangle}$. Thus we have the correspondence

$$\{\text{intermediate fields } K \subseteq E \subseteq F\} \leftrightarrow \{\text{subgroups } G \leq \mathrm{Aut(F/K)}\},$$

given by the assignments

$$\begin{aligned}E &\mapsto \mathrm{Aut}(F/E),\\ F^G &\mapsto G.\end{aligned}$$

In general these assignments do not define a bijection, but we will go on to show in the case of normal separable (Galois) extensions, this does in fact define a bijection. Without any assumptions on F/K, both maps are inclusion reversing, and we have

$$\begin{aligned}E &\subseteq F^{\mathrm{Aut}(F/E)},\\ G &\subseteq \mathrm{Aut}(F/F^G).\end{aligned}$$

There is also a G action on both of the above sets. G acts on its subgroup via conjugation, that is

$$\sigma.H = \sigma H \sigma^{-1},$$

for any $\sigma \in G, H \leq G$. G also naturally acts on the set of interemediate fields via

$$\sigma.E = \sigma(E).$$

Moreover these actions are easilly seen to be equivariant.

Let K be a field, K^{alg}, and set $G_K := \text{Aut}(K^{\text{alg}}/K)$. G_K is determined by K up to isomorphism: If $\overline{K}$ is another algebraic closure then we have a K-isomorphism $\varphi : \overline{K} \to K^{\text{alg}}$. We then get an isomorphism $G_K \to G_{K'} = \text{Aut}(\overline{K}/K)$ given by the assignment

$$\sigma \mapsto \varphi \circ \sigma \circ \varphi^{-1}.$$

Now let F/K be an algebraic extension. Fix an algebraic closure F^{alg}, which is also seen to be an algebraic closure for the base field K. Then we have the following

$$G_F = \text{Aut}(F^{\text{alg}}/F) = \text{Aut}(K^{\text{alg}}/F) \leq \text{Aut}(K^{\text{alg}}/K) = G_K.$$

Also, for each $\sigma \in G_K$ we have the intermediate field $K \subseteq \sigma(F) \subseteq K^{\text{alg}}$.

Lemma 1.19. *Let F/K be a field extensions. Then F/K is a normal extension if and only if F/K is algebraic and $\sigma(F) = F$ for all $\sigma \in G_K$. In this case $G_F \trianglelefteq G_K$ and*

$$G_K/G_F \cong \mathit{Aut}(F/K),$$

via the restriction homomorphism.

Proof. Suppose F/K is a normal extension. Then it is algebraic and F is the splitting field for some collection $\mathscr{S} \subseteq K[x] \setminus K$. Thus $F = K($ all roots of all $f \in \mathscr{S})$. Any $\sigma \in G_K$, permutes the roots of any $f \in \mathscr{S}$, (σ is a K-homomorphism). Hence $\sigma(F) \subseteq F$. Moreover, since σ is a bijection we can get the other inclusion by taking σ^{-1}. Therefore $F = \sigma(F)$.

For the other direction, suppose F/K is algebraic and $\sigma(F) = F$ for all $\sigma \in G_K$. Let $\alpha \in F$. We aim to show that $m_{\alpha,K}$ splits completely in F, which will show normality by Proposition 1.10 To that end, let $\beta \in K^{\text{alg}}$ be a root of $m_{\alpha,K}$. We then obtain a K-isomorphism $K(\alpha) \to K(\beta)$. Then by applying Lemma 1.8 to the following diagram,

$$\begin{array}{ccc} K^{\text{alg}} & \overset{\Phi}{\dashrightarrow} & K^{\text{alg}} \\ \big| & & \big| \\ K(\alpha) & \longrightarrow & K(\beta) \end{array}$$

we get an automorphism of K^{alg} which fixes K pointwise and sends α to β. Hence $\Phi \in G_K$, and since $\Phi(F) = F$ by assumption we get that $\beta \in F$, as desired.

Now, suppose F/K is a normal extension. Then consider the map $G_K \xrightarrow{\phi} \text{Aut}(F/K)$ given by the assignment

$$\sigma \mapsto \sigma|_F.$$

By the foregoing, this is a well-defined group homomorphism and clearly has kernel G_F. Hence, we need only show ϕ is a surjection in order to have the desired isomorphism. Surjectivity follows via 1.8 since any K-homomorphism $F \to F$ extends to a map $K^{\text{alg}} \to K^{\text{alg}}$. □

Theorem 1.20. *The following are equivalent for a field extension F/K.*

1. *F/K is algebraic and $F^{Aut(F/K)} = K$.*
2. *F/K is normal and separable.*
3. *F is the splitting field of a collection of separable polynomials $\mathscr{S} \subseteq K[x] \setminus K$.*

If any of the following hold the extension F/K is said to be *Galois*. In this case, the group $\mathrm{Aut}(F/K)$ is the *Galois group* and denoted by $\mathrm{Gal}(F/K)$.

Before proceeding with the proof we sketch a few examples. First, note that $\mathbb{F}_q \,/\, \mathbb{F}_p$ is Galois with Galois group $\langle \Phi \rangle \cong C_r$ where $q = p^r$. Also, the extension $\mathbb{C} \,/\, \mathbb{R}$ is Galois with Galois group C_2. However, for any proper subfield $F \subseteq \mathbb{R}$, $\mathbb{R} \,/F$ is not Galois. We already know $\mathrm{Aut}(\mathbb{R} \,/\, \mathbb{Q}) = \{1\}$, and since $\mathrm{Aut}(\mathbb{R} \,/F) \subseteq \mathrm{Aut}(\mathbb{R} \,/\, \mathbb{Q})$ we see $\mathrm{Aut}(\mathbb{R} \,/F) = \{1\}$. Then clearly

$$F^{\mathrm{Aut}(\mathbb{R} \,/F)} = \mathbb{R} \neq F,$$

giving the extension is not Galois.

We now introduce the notion of the absolute Galois group. For any field K, the extension K^{sep}/K is Galois. It is clearly separable and we showed in Lemma 1.18 that this extension is normal. Now, applying Lemma 1.19 with $F = K^{\mathrm{sep}}$ we see that we have a surjective group homomorphism

$$G_K \twoheadrightarrow \mathrm{Aut}(K^{\mathrm{sep}}/K),$$

given via restriction. Moreover the kernel of this map is $G_{K^{\mathrm{sep}}} = \mathrm{Aut}(K^{\mathrm{alg}}/K^{\mathrm{sep}}) = \{1\}$ by our final example on page 15 of these notes. Therefore $\mathrm{Gal}(K^{\mathrm{sep}}/K) \cong G_K$. The group $\mathrm{Gal}(K^{\mathrm{sep}}/K) = G_K$ is coined the *absolute Galois group* of the field K. We now provide the proof of Theorem 1.20.

Proof. For brevity, fix $G = \mathrm{Aut}(F/K)$.

i) $\Rightarrow$ iii): Assume F/K is algebraic with $F^G = K$. We then claim that for any $\alpha \in F$,

$$m_{\alpha,K} = \prod_{\sigma \in G/G_\alpha} (x - \sigma(\alpha)) = \prod_{\beta \in G.\alpha} (x - \beta),$$

where G_α is the point stabilizer of the canonical action of G on F given by $\sigma.\alpha = \sigma(\alpha)$. Granting the claim we then have all $m_{\alpha,K}$ are separable in $F[x]$. Then F/K is easilly seen to be the splitting fields for the collection of all minimal polynomials for all $\alpha \in F$.

To prove the claim, recall that any $\sigma \in G$ must send a root of $m_{\alpha,K}$ to a root of $m_{\alpha,K}$. Hence $(x - \sigma(\alpha))$ is an irreducible factor of $m_{\alpha,K}$ in $F[x]$, from which we conclude

$$m := \prod_{\sigma \in G/G_\alpha} (x - \sigma(\alpha)) \Big| m_{\alpha,K},$$

in $F[x]$. Note also by applying σ to the coefficients of m, we see

$$\sigma(m) = \prod_{\beta \in G.\alpha} (x - \sigma(\beta)) = m,$$

since the orbits of this action partition F. Hence the coefficients of m are fixed by G and therefore belong to $F^G = K$. Thus, by irreducibility of $m_{\alpha,K}$, we see $m = m_{\alpha,K}$ as desired.

iii) $\Rightarrow$ ii): Assume F is the splitting field for some collection of separable polynomials $\mathscr{S} \subseteq K[x] \setminus K$. Normality of this extension is trivial. To see separability, consider the subextension $F_S = \{\alpha \in F | \alpha \text{ is separable over } K\}$. F is precicsely given by

$$K(\text{ all roots of all } f \in \mathscr{S}).$$

Moreover for each α that is the root of some polynomial $f \in \mathscr{S}$, it is separable by assumption and hence $\alpha \in F_S$. Thus we achieve the containment $F \subseteq F_S$, giving these fields are equal and the extension is separable.

ii) $\Rightarrow$ i): Assume F/K is normal and separable. Then clearing the extension is algebraic, since normal extensions are algebraic. Lemma 1.19 provides us with a short exact sequence of groups

$$1 \to G_F \xrightarrow{i} G_K \xrightarrow{\cdot|_F} \mathrm{Aut}(F/K) \to 1.$$

In particular $\sigma(F) = F$ for all $\sigma \in G$. Now, let $\alpha \in F$ be such that $\sigma(\alpha) = \alpha$ for all $\sigma \in G$. By the above σ is restrictiong of some $\varphi \in G_K$, and hence $\varphi(\alpha) = \alpha$ for all $\varphi \in G_K$. Moreover, by separability, $|K(\alpha) : K|_S = |K(\alpha) : K|$ and the separable degree is precisely the number of distinct K-homomorphisms $K(\alpha) \to K^{\mathrm{alg}}$. By Lemma 1.8 each K-homomorphism $\phi : K(\alpha) \to K$ extends to an element $\varphi \in G_K$ Since $\varphi(\alpha) = \alpha$ for all $\varphi \in G_K$, we must have that ϕ is the identity on $K(\alpha)$ since it is uniquely determined by what it does to α. Therefore $|K(\alpha) : K| = 1$ and thus $\alpha \in K$, as desired. □

Given an extension F/K it is natural to ask whether F is contained in some larger field E which is Galois over K. Since separability is well-behaved in towers, this can only happen if the extension is separable. This necessary condition is, in fact, sufficient: Fix an algebraic closure K^{alg}. Then we have the tower of fields

$$K \subseteq F \subseteq K^{\mathrm{sep}} = F^{\mathrm{sep}} \subseteq K^{\mathrm{alg}}.$$

Define E to be the subfield of K^{alg} generated by $\sigma(F)$ for all $\sigma \in G_K$. The extension E/K is easilly seen to be separable. Furthermore, we claim E/K is normal. To see this, note $\sigma(E)$ contains all $\sigma(F)$ for any $\sigma \in G_K$, and hence $E \subseteq \sigma(E)$. Since σ is an automorphism we then also have $\sigma(E) \subseteq E$ for any $\sigma \in G_K$ and hence by Lemma 1.19, E is normal. E is said to be the *Galois closure* of the separable extension F/K.

Recall our definition of the absolute Galois group of a field K to be $\mathrm{Aut}(K^{\mathrm{sep}}/K)$. If F/K is some Galois extension then, after applying Lemma 8, we may assume $F \subseteq K^{\mathrm{sep}}$. Then, Lemma 1.19 gives an epimorphism

$$G_K \twoheadrightarrow \mathrm{Gal}\, FK,$$

via restriction. Hence the galois group of any Galois extension F/K is a homomorphic image of G_K.

We now restrict ourselves to the case of finite Galois extensions. Recall that for any set X and any field F we have the F-vector space

$$F^X = \{\text{all functions } X \to F\}.$$

Lemma 1.21. *Any family of distinct elements of Aut(F) is linearly independent in F^F.*

Proof. Suppose, by way of contradiction, there exists some $\lambda_i \in F$ not all 0 such that

$$\sum_{i=1}^{m} \lambda_i \sigma_i = 0,$$

with m above chosen minimally to have such a non-trivial linear relation. Then $m \neq 1$ and $\lambda_i \neq 0$ for all i. Choose $x \in F^\times$ such that $\sigma_1(x) \neq \sigma_m(x)$. Then we see

for any $y \in F^\times$,

$$0 = \sum_{i=1}^{m} \lambda_i \sigma_i(xy) = \sum_{i=1}^{m} \lambda_i \sigma_i(x)\sigma_i(y)$$

$$0 = \sigma_1(x) \sum_{i=1}^{m} \lambda_i \sigma_i(y)$$

Subtracting both equations gives

$$0 = \sum_{i=1}^{m} \lambda_i (\sigma_i(x) - \sigma_1(x))\sigma_i(y),$$

contradicting the minimality of m. □

Theorem 1.22. *Let $G \leq \mathrm{Aut}(F)$, $K = F^G$. Then $[F : K] = |G|$, with both being potentially infinite.*

Proof. We begin by proving $|G| \leq [F : K]$. In this case we may assume $[F : K] = n < \infty$ and fix a basis $\alpha_1, \ldots, \alpha_n$ of F over K. Suppose, by way of contradiction there exists $\sigma_1, \ldots, \sigma_m$ distinct elements of G with $m > n$. Consider the following system of linear equations over F:

$$\sum_{j=1}^{m} \sigma_j(\alpha_i) x_j = 0,$$

for each α_i. This is a system of n equations in m-unknowns and hence there exists a non-trivial solution $(\lambda_1, \ldots, \lambda_m) \in F^m$ such that

$$\sum_{j=1}^{m} \lambda_j \sigma_j(\alpha_i) = 0,$$

for all α_i. Since $\alpha_1, \ldots, \alpha_n$ form a K-basis for F this gives that

$$\sum_{j=1}^{m} \lambda_j \sigma_j = 0,$$

contradicting Dedekin's lemma (Lemma 1.21).

On the other hand, we now prove $[F : K] \leq |G|$. Again, we may assume $|G| = n < \infty$. Suppose there exists a collection $\alpha_1, \ldots, \alpha_m$ of K-linearly independent elements of F with $m > n$. Then consider the system of F-linear equations

$$\sum_{i=1}^{m} \sigma(\alpha_i) x_i,$$

for all $\sigma \in G$. Again, this is a system of n equations in m unknowns and thus there exists a non-trivial solution $(\lambda_1, \ldots, \lambda_m) \in F^m$ such that

$$\sum_{i=1}^{m} \lambda_i \sigma(\alpha_i) = 0,$$

for all $\sigma \in G$. We may choose our solution $(\lambda_1, \ldots, \lambda_m)$ with a minimal number of non-zero elements and after rescaling we may assume $\lambda_1 = 1$. We therefore have

$$\sigma(\alpha_1) + \sum_{i=2}^{m} \lambda_i \sigma(\alpha_i), \tag{1}$$

for all $\sigma \in G$. In particular, taking $\sigma = 1$, we get

$$\alpha_1 = -\sum_{i=2}^{m} \lambda_i \alpha_i.$$

By K-linear independence of the α_i's we see that at least one $\lambda_i \in F \setminus K$. Without loss of generality we may assume $\lambda_m \notin K$. Since K is the fixed field of G, we may fix an element $\tau \in G$ such that $\tau(\lambda_m) \neq \lambda_m$. Applying τ to Equation 1 we see

$$\tau(\sigma(\alpha_1)) + \sum_{i=2}^{m} \tau(\lambda_i)\tau(\sigma(\alpha_i)) = 0,$$

for all $\sigma \in G$, or equivalently,

$$\sigma(\alpha_1) + \sum_{i=2}^{m} \tau(\lambda_i)\sigma(\alpha_i) = 0, \tag{2}$$

since $\{\tau\sigma | \sigma \in G\} = G$. Subtraction Equation 1 from Equation 2, we obtain

$$\sum_{i=2}^{m} (\tau(\lambda_i) - \lambda_i)\sigma(\alpha_i) = 0,$$

and since we are guaranteed $\tau(\lambda_m) - \lambda_m \neq 0$, the above contradicts the assumption that are chosen solution minimized the number of non-zero entries. □

Corollary 1.23.

a) Let F/K be a finite field extension. Then

$$|\operatorname{Aut}(F/K)| \Big| [F : K],$$

with equality if and only if the extension is Galois.

b) Let F be a field, $G \leq \operatorname{Aut}(F)$ be finite and set $K = F^G$. Then F/K is Galois and $G = \operatorname{Gal}(F/K)$.

Proof. a): Let $G = \operatorname{Aut}(F/K)$. Then $K \subseteq F^G$ and by multiplicativity of field degree

$$[F : K] = [F : F^G][F^G : K].$$

Moreover, by Theorem 1.22, $[F : F^G] = |\operatorname{Aut}(F/K)|$ and we have equality if and only if $[F^G : K] = 1$, which is equivalent to F/K being Galois.

b): By the above along with Theorem 1.22, we have

$$|\operatorname{Aut}(F/K)| \Big| |G| = [F : K].$$

On the other hand, $G \leq \operatorname{Aut}(F/K)$ and hence $G = \operatorname{Aut}(F/K)$. In particular, F/K is Galois since by part *a)* and hence $G = \operatorname{Gal}(F/K)$. □

Before moving on to the fundamental theorem of Galois theory we recall a few examples from previous sections. Set $F = \mathbb{F}_q$ with $q = p^r$ and take $G = \langle \Phi \rangle$. Then

$$F^G = \{\alpha \in F | \alpha^p = p\} = \mathbb{F}_p \,.$$

Thus by Corollary 1.23 we see $\mathbb{F}_q \,/\, \mathbb{F}_p$ is Galois with Galois group C_r.

Let $\zeta_n = e^{2\pi i/n} \in \mathbb{C}^\times$. Then $\mathbb{Q}(\zeta_n)$ is the splitting field of $x^n - 1$ (or of Φ_n) and hence the extension is Galois over $\mathbb{Q}$. Let $G = \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\,\mathbb{Q})$. We know via Corollary 1.23 that

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

Moreover for any $\sigma \in G$, $\sigma(\zeta_n)$ is a primitive nth root of unity and hence $\sigma(\zeta_n) = \zeta_n^k$ for some k such that $(k, n) = 1$. Hence we get an isomorphism

$$G \equiv (\mathbb{Z}/n\mathbb{Z})^\times,$$

since all maps of the aforementioned form must define the distinct $\mathbb{Q}$-automorphisms by considering the order of G.

Theorem 1.24. *Let F/K be a finite Galois extension, $G = \mathrm{Gal}(F/K)$. Then*

a) The maps between $\mathscr{F} = \{$intermediate fields of $F/K\}, \mathscr{G} = \{$subgroups of $G\}$, given by

$$K \subseteq E \subseteq F \mapsto \mathrm{Aut}(F/E) = \mathrm{Gal}(F/E)$$
$$H \leq G \mapsto F^H$$

define bijections which are inverse to one another.

b) Via the above correspondence, if $E \leftrightarrow H$, then

$$|H| = [F : E]$$
$$|G : H| = [E : K]$$

c) The extension E/K is normal if and only if $H = \mathrm{Aut}(F/E) \trianglelefteq G$. In this case $\mathrm{Gal}(E/K) \cong G/H$.

Proof. a): Let $E \in \mathscr{F}$. We need only show $F^{\mathrm{Aut}(F/E)} \subseteq E$. But we know the extension F/E is Galois so $F^{\mathrm{Aut}(F/E)} = E$, as desired. Conversely, let $H \leq G$. By Corollary 1.23 we have that $\mathrm{Aut}(F/F^H) = H$ since H is finite.

b): Let $E \leftrightarrow H$ via the above correspondence. Then by Corollary 1.23 we see $|H| = [F : E]$. Moreover,

$$\begin{aligned} |G| = [F : K] &= [F : E][E : K], \\ &= |H|[E : K], \end{aligned}$$

giving $[E : K] = \frac{|G|}{|H|} = [G : H]$.

c): Note E/K is Galois if and only if E/K is normal and by Lemma 1.19 this is the case if and only if $\sigma(E) = E$ for all $\sigma \in \mathrm{Aut}(K^{\mathrm{alg}}/K)$. Moreover, in this case

$$\mathrm{Gal}(E/K) \cong \mathrm{Gal}(K^{\mathrm{sep}}/K)/\mathrm{Gal}(K^{\mathrm{sep}}/E).$$

But since F/K is Galois we have an surjective homomorphism $G_K \twoheadrightarrow \mathrm{Gal}(F/K)$ via restriction. Thus E/K is normal if and only if $\sigma(E) = E$ for all $\sigma \in \mathrm{Gal}(F/K)$ which by G-equivariance is equivalent to $H \trianglelefteq G$. Hence we get a surjective homomorphism $\mathrm{Gal}(F/K) \twoheadrightarrow \mathrm{Gal}(E/K)$ given by restriction and the kernel is precisely $\mathrm{Gal}(F/E)$, giving the isomorphism

$$\mathrm{Gal}(E/K) \cong G/H.$$

□

1.8. **Galois Theory of Polynomials.**

Fix a field K, $f \in K[x]$, be separable, F be the splitting field of f, and $n = \deg f$. The purpose of this section in general is to understand the roots of f. We define the *Galois group of* f, denoted $\mathrm{Gal}(f)$ to be $\mathrm{Gal}(F/K)$. For example, given $x^q - x \in \mathbb{F}_p[x]$, with $q = p^r$, we see $\mathrm{Gal}(f) = \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) = C_r$. Also, $\mathrm{Gal}(\Phi_n) = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

We now consider the Galois group of the polynomial $f := x^4 - a$ for $a \in \mathbb{Z}$ such that there exists some prime $p \in \mathbb{Z}$ satisfying $p|a, p^2 \nmid a$. This setup gives that

f is irreducible by Eisenstein's criterion. The splitting field of f is $\mathbb{Q}(\sqrt[4]{a}, i)$. By examining the tower

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{a}) \subseteq \mathbb{Q}(\sqrt[4]{a}, i),$$

we see $[\mathbb{Q}(\sqrt[4]{i}, i) : \mathbb{Q}] = 8$. Setting $G = \mathrm{Gal}(f)$, we therefore obtain $|G| = 8$. Also, any $\sigma \in G$ is uniquely determined by where it maps $\sqrt[4]{a}, i$, and since these elements must me mapped to roots of their correpsonding minimal polynomials, we see

$$\sigma(\sqrt[4]{a}) \in \{\pm\sqrt[4]{a}, \pm\sqrt[4]{a}i\}, \quad \sigma(i) \in \{\pm i\}.$$

Thus the 8 possibilities above must all be elements of G. Define $\sigma \in G$, by $i \mapsto -i, \alpha \mapsto \alpha$, and $\tau \in G$, by $i \mapsto i, \alpha \mapsto i\alpha$. Then $|\sigma| = 2, |\tau| = 4$ and one verifiably sees $\tau\sigma = \sigma\tau^3$. Thus we get an onto group homomorphism $D_4 \twoheadrightarrow G$, and by examining orders we see $D_4 \cong G$.

Given a separable polynomial $f \in K[x]$, $\alpha_1, \ldots, \alpha_n$ its distinct roots in K^{alg}, since any $\sigma \in G$ permutes the α_i's, we get an embedding

$$G \hookrightarrow S_n.$$

We obtain an injective group homomorphism since the action must be faithful as any group homomorphism $F \to F$ is uniquely determined by its action on $\alpha_1, \ldots, \alpha_n$. Moreover, we claim this action is transitive if and only if f is irreducible. To see this, note by the proof of Theorem 1.20, for any $\alpha = \alpha_i$,

$$f = \mathrm{LC}(f) m_{\alpha_i, K} = \mathrm{LC}(f) \prod_{\alpha_j \in G.\alpha_i} (x - \alpha_j)$$

Hence $G.\alpha_i = \{\alpha_1, \ldots, \alpha_n\}$. Since $G \hookrightarrow S_n$, it is a natural question to ask when $G \hookrightarrow A_n$. Answering this question requires a brief intermezzo on symmetric polynomials.

Let $R = K[x_1, \ldots, x_n]$ be the polynomial algebra in n variables over some commutative ring K. Then S_n naturally acts on R via

$$\sigma.f(x_1, \ldots, x_n) \mapsto f(x_{\sigma(1)}, \ldots, f_{\sigma(n)}).$$

The set of polynomials fixed by this action is a sub-algebra of R, and is known as the sub-algebra of *symmetric polynomials*. For example, the power sums given by

$$p_k = x_1^k + \cdots + x_n^k,$$

are symmetric polynomials for any $k \geq 1$. Also, the elementary symmetric polynomials are defined by

$$e_k = \sum_{\substack{I \subseteq [n] \\ |I| = k}} \left(\prod_{i \in I} x_i \right).$$

We provide without proof the funademtal theorem of symmetric polynomials which states

$$K[x_1, \ldots, x_n]^{S_n} = K[e_1, \ldots, e_n].$$

With symmetric polynomials in mind, we can now define the discriminant of a polynomial and thus classify precisely when $G \hookrightarrow S_n$. Given a polynomial $f \in K[x], \deg f = n, \alpha_1, \ldots, \alpha_n$ its (not necessarily distinct) roots, we may write

$$f = \sum_{i=0}^{n} a_i x^i = \prod_{i=1}^{n} (x - \alpha_j),$$

in some splitting field of f. By expanding the product, we achieve

$$a_i = (-1)^{n-i} e_{n-i}(\alpha_1, \ldots, \alpha_n), \tag{3}$$

and hence the coefficients of f can be expressed in terms of its roots. Define $D, \Delta \in K[x_1, \ldots, x_n]$ via

$$D(x_1, \ldots, x_n) = \prod_{i<j} (x_i - x_j)^2,$$
$$\Delta(x_1, \ldots, x_n) = \prod_{i<j} (x_i - x_j).$$

Then we say the *discriminant of* f is given by $D(f) := D(\alpha_1, \ldots, \alpha_n)$. Hence $D(f) = \Delta(f)^2$. Note that D is a symmetric polynomial, while

$$\sigma.\Delta = \operatorname{sgn}(\sigma)\Delta.$$

By Equation 3, along with the fundamental theorem of symmetric polynomials,

$$D_f \in K[\alpha_1, \ldots, \alpha_n]^{S_n} = K[e_1(\alpha_1, \ldots, \alpha_n), \ldots, e_n(\alpha_1, \ldots, \alpha_n)],$$

and hence D_f is a polynomial expression in terms of the coefficents of f and therefore is an element of K.

With this in mind, we claim $G \hookrightarrow A_n$ if and only if D_f is a square in K, assuming the characteristic of K is not 2. To see this, note G embeds in A_n, if and only if every $\sigma \in G$ is an even permuation of $\alpha_1, \ldots, \alpha_n$. This is equivalent to requiring $\sigma(\Delta_f) = \Delta_f$ for every $\sigma \in G$. Thus, since $F^G = K$ this happends precisely when $\Delta_f \in K$ giving the claim.

Now, assume $K \subseteq R$, and let $f \in K[x]$ be irreducible, $\deg f = p$ for some prime $p \in \mathbb{Z}$. We then claim if f has exactly two non-real roots in $\mathbb{C}$, $G(f) = S_p$. Let $F = K(\alpha_1, \ldots, \alpha_p)$, where $\alpha_1, \ldots, \alpha_p$ denotes the distinct roots of $f \in \mathbb{C}$. Since f is irreducible, G_f is a transitive subgroup of S_p and thus via the orbit stabilizer theorem $|G : G_\alpha| = p$ for any $\alpha \in \{\alpha_i\}_{i \in [p]}$. By Cauchy's Theorem, there exists an elements $\sigma \in G$ with order p. Then σ must be a p-cycle, and after reordering the roots we may assume $\sigma = (1, 2, \ldots, p)$. Let τ be complex conjugation restricted to F. Then $\tau \in G$, and without loss of generality we may assume $(1, 2) = \tau$. To conclude simple note $\langle \tau, \sigma \rangle = S_p$, since conjugating τ by powers of σ will yield all coxeter generators.

1.9. **Solvability by Radicals.**

Throughout let $f \in K[x], F$ be its splitting field. f is said to be *solvable by radicals* if F is contained in some field E that is a root extension. That is, there exists a chain a fields

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t = E = K(\rho_1, \ldots, \rho_t),$$

with each $K_i = K_{i-1}(\rho_i)$ and $\rho_i^{e_i} \in K_{i-1}$ for some $e_i > 0$. For example, given $f = ax^2 + bx + c$, its roots are precisely

$$\alpha_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a},$$

and hence $F = K(\sqrt{b^2 - 4ac})$.

Theorem 1.25. *Let K be a field of characteristic 0. Then f is solvable by radicals if and only if $G(f)$ is a solvable group.*

Proof. Begin by supposing f is solvable by radicals. Fixing F to be the splitting field for f over K, we thus have a root extension E such that

$$K \subseteq F \subseteq E.$$

We claim we may assume E/K is Galois and there exists $\zeta_e \in K^\times$ such that $|\zeta| = e$ for $e = \operatorname{lcm}(e_i)_{i=1}^t$. Granting this for now, we complete this direction of the proof. Set $\mathscr{G} = \operatorname{Gal}(E/K)$. Then since F/K is Galois, we obtain a surjective group homormorphism

$$\mathscr{G} \twoheadrightarrow G,$$

via restriction. Thus, since homomorphic images of solvable groups are solvable, it is enough to show $\mathscr{G}$ is solvable.

Observe that K_i is the splitting field of $g = x^{e_i} - \rho_i^{e_i} \in K_{i-1}[x]$ and hence K_i/K_{i-1} is Galois: Defining $\zeta_i = \zeta^{e/e_i} \in K_i^\times$ we see that the roots of g are precisely $\rho_i\zeta_i^l$ for $l = 0, 1, \ldots, e_i - 1$. All roots then evidently belong to K_i and hence K_i/K_{i-1} is normal.

Furthermore, we claim $\operatorname{Gal}(K_i/K_{i-1})$ is abelian. Let $\sigma, \tau \in \operatorname{Gal}(K_i/K_{i-1})$. Then we see $\sigma(\rho_i) = \zeta_i^l\rho_i$, for some $l = 0, 1, \ldots, e_i - 1$, and similarly for τ. From this, commutativity easilly follows.

To conclude, the fundamental theorem of Galois theory gives rise to the dual chains

$$K = K_0 \subseteq \cdots \subseteq K_{i-1} \subseteq K_i \subseteq \cdots \subseteq K_t = E,$$
$$\mathcal{G} \geq \cdots \geq H_{i-1} \geq H_i \geq \cdots \geq \{1\}.$$

Moreover since K_i/K_{i-1} is normal, $H_i \trianglelefteq H_{i-1}$ and $\operatorname{Gal}(K_i/K_{i-1}) \cong H_{i-1}/H_i$ and thus $\mathscr{G}$ is evidently solvable.

It remains to justify the previous assumptions. First we justify that we may assume E/K to be Galois. In short, we will do this by replacing E by its Galois closure $\widetilde{E}$. Then we see $\widetilde{E}/K$ is a finite Galois extension since

$$|\{\sigma|_E = E | \sigma \in G_K\}| \leq |\{K\text{-hom. } E \to K^{\mathrm{alg}}\}| = [E : K] < \infty,$$

as Lemma 1.8 gives that all K-homomorphisms $E \to K^{\mathrm{alg}}$ extend to an element of G_K. Set $\operatorname{Gal}(\widetilde{E}/K) = \widetilde{G}$. Then by construction of the Galois closure we see

$$\widetilde{E} = K(\rho_i, \sigma(\rho_i) | i = 1, \ldots, t, \sigma \in \widetilde{G}).$$

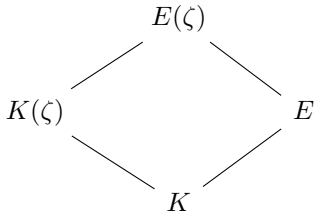
In particular, we obtain a new chain of extensions

$$K = \widetilde{K_0} \subseteq \cdots \subseteq \widetilde{K_i} = \widetilde{K}_{i-1}(\rho_i, \sigma(\rho_i) | \sigma \in \widetilde{G}) \subseteq \cdots \subseteq \widetilde{K_t} = \widetilde{E}.$$

Moreover each $\widetilde{K_i}$ is stable under the action by $\widetilde{G}$ and from this we see for any i, $\sigma(\rho_i)^{e_i} = \sigma(\rho_i^{e_i}) \in \widetilde{K}_{i-1}$. Thus by refining the above chain by adjoining each $\sigma(\rho_i)$ one at a time, we obtain a chain of simple root extensions up to $\widetilde{E}$. This justifies the first assumption.

To conclude this direction of the proof, we must show the existence of some $\zeta \in K^\times$ such that $|\zeta| = e := \operatorname{lcm}(e_i)_{i=1}^t$. In short, if there is no such element, we simply adjoin one to K. Fix a primitive eth root of unity, $\zeta \in E^{\mathrm{alg}}$ and consider

the following diagram of fields,



By the previous, E/K is a Galois extension, and $K(\zeta)/K$ is Galois as the splitting field of $x^e - 1$. Moreover one easilly sees that $\mathrm{Gal}(K(\zeta)/K) \cong (\mathbb{Z}/e\,\mathbb{Z})^\times$. Thus $EK(\zeta) = E(\zeta)/K$ is Galois, giving $E(\zeta)/K(\zeta)$ is Galois. Moreover, via the argument above it now follows that $\mathrm{Gal}(E(\zeta)/K(\zeta))$ is solvable. The fundamental theorem applied to the above diagram then gives the following isomorphisms:

$$\mathrm{Gal}(K(\zeta)/K) \cong \mathrm{Gal}(E(\zeta)/K)/\,\mathrm{Gal}(E(\zeta)/K(\zeta)),$$
$$\mathrm{Gal}(E/K) \cong \mathrm{Gal}(E(\zeta)/K)/\,\mathrm{Gal}(E(\zeta)/E).$$

From the first isomorphism, we conclude $\mathrm{Gal}(E(\zeta)/K)$ is solvable and from this the second isomorphism gives $\mathrm{Gal}(E/K)$ is solvable. This justifies the second assumption and concludes the first direction of the proof.

Now, suppose G is a solvable group. By hypothesis there exists a chain

$$1 = G_s \trianglelefteq G_{s-1} \trianglelefteq \ldots \trianglelefteq G_0 = G,$$

with each G_i/G_{i+1} abelian (and finite). We will later prove a more general statement of the structure theorem for finite abelian groups, from which we will see that we can refine the above tower so that each quotient is cyclic. That is,

$$G_i/G_{i+1} \cong C_{e_i},$$

for some $e_i \in \mathbb{Z}_{>0}$. The fundamental theorem then gives a correpsonding tower of fields

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_s = F,$$

with each K_{i+1}/K_i Galois for each i and $\mathrm{Gal}(K_{i+1}/K_i) \cong C_{e_i}$. Again we fix some $\zeta \in (F^{\mathrm{alg}})^\times$ such that $|\zeta| = e := \mathrm{lcm}(e_i)_{i=1}^t$, and consider the corresponding tower

$$K \subseteq \widetilde{K_0} \subseteq \widetilde{K_1} \subseteq \cdots \subseteq \widetilde{K_s} := E,$$

with $\widetilde{K_i} = K_i(\zeta)$. We then claim $\widetilde{K}_{i+1}/\widetilde{K_i}$ is still Galois with Galois group C_{m_i} for some $m_i | e_i$. Moreover we claim $\widetilde{K}_{i+1} = \widetilde{K}(\rho_i)$ for some ρ such that $\rho^{m_i} \in \widetilde{K_i}$. From this we will conclude that F/K is solvable by radicals. For the first claim, we prove a more general lemma.

Lemma 1.26. *Let F, K' be extensions of some base field K, that are contained in some common extension L. If F/K is Galois, then both $F/F \cap K', FK'/K'$ are Galois and*

$$\mathrm{Gal}(F/F \cap K') \cong \mathrm{Gal}(FK'/K').$$

Proof. Trivially $F/F \cap K'$ is Galois since $F \cap K'$ is an intermediate field of F/K. Moreover, since F is the splitting field for some $\mathscr{S} \subseteq K[x] \setminus K$, we obtain that FK' is the splitting field for $\mathscr{S} \subseteq K'[x] \setminus K'$. For brevity fix $G' = \mathrm{Gal}(FK'/K'), G =$

$\mathrm{Gal}(F/K)$. Since the extension F/K is normal and any $\sigma \in \mathrm{Gal}(FK'/K')$ extends to an element of G_K, we have a group homomorphism $G' \to G$ given by

$$\sigma \mapsto \sigma|_F$$

. The kernel of the map is precisely given by $\sigma \in G'$ that are the identity on both F and K' and hence the identity on FK'. Therefore the map is injective. Let H denote the image of this map. The fixed field of H is given by

$$F^H = (FK')^{G'} \cap F = K' \cap F.$$

Hence $H = \mathrm{Gal}(F/K' \cap F)$, giving the lemma. □

Applying this to our first claim, take $K = K_i, F = K_{i+1}, K' = K(\zeta), FK' = K_{i+1}(\zeta)$. Then as previously noted $\mathrm{Gal}(F/K) \cong C_{e_i}$ and thus the lemma gives

$$\mathrm{Gal}(FK'/K') \leq C_{e_i},$$

which justifies the claim.

To justify the second claim we use another lemma.

Lemma 1.27. *Let F/K be a Galois extension with cyclic Galois group $G \cong C_m$. Then, if there exists $\zeta \in K^\times$ such that $|\zeta| = m$, $F = K(\rho)$ for some ρ such that $\rho^m \in K$.*

We note before proving the lemma that this setup gives the second claim and thus completes the proof.

Proof. Fix a generator for $G = \langle\sigma\rangle$, $|\sigma| = m$. For any $\alpha \in F$ define the element

$$\rho_\alpha := \sum_{i=0}^{m-1} \zeta^i \sigma^i(\alpha).$$

Note that for any α

$$\sigma(\rho_\alpha) = \zeta^{-1}\rho_\alpha.$$

From this we obtain that $\sigma(\rho_\alpha^m) = \zeta^{-m}\rho_\alpha^m = \rho_\alpha^m$. Hence $\rho_\alpha^m \in K$. By Lemma 1.21, the map defined by

$$\sum_{i=0}^{m-1} \zeta^i \sigma^i \neq 0,$$

and hence there exists an $\alpha \in F$ such that $\rho_\alpha \neq 0$. Thus for $0 < i < m$, $\sigma^i(\rho_\alpha) = \zeta^{-i}\rho_\alpha \neq \rho_\alpha$ and hence ρ_α does not belong to the fixed field of any subgroup of G. Hence $F = K(\rho_\alpha)$. □

Having justfieid our claims, the proof of Theorem 1.25 is complete. □

1.10. **Three Theorems on Fields.**

To conclude the chapter on Fields and Galois Theory, we state two important theorems in Field Theory as well as state and prove the Fundamental Theorem of Algebra. First we present what is known as the primitive element theorem.

Theorem 1.28. *Any finite separable extension F/K is a simple algebraic extension. That is, there exists some $\alpha \in F$ such that $F = K(\alpha)$.*

The proof of this theorem is presented in Algebraic Number Theory Lecture notes and in *Dummitt & Foote* on pages 594-595. This theorem can be thought of as providing an explicit basis for F/K that is of the form $\{1, \alpha, \ldots, \alpha^{d-1}\}$ for some $\alpha \in F$. In a similar vein, one has the normal basis theorem.

Theorem 1.29. *Let F/K be a finite Galois extension with Galois group G. Then there exists some $\alpha \in F$ such that the elements $\{\sigma(\alpha)|\sigma \in G\}$ form a K-basis for F.*

The proof of this theorem is not presented in *Dummitt & Foote*. Finally, we conclude the chapter with the Fundamental Theorem of Algebra.

Theorem 1.30. *$\mathbb{C}$ is an algebraically closed field.*

Proof. Recall that every non-negative $\alpha \in \mathbb{R}$ has a square-root in $\mathbb{R}$. From this we obtain that every complex number has a square-root in $\mathbb{C}$. In terms of fields, this implies that $\mathbb{C}$ has no degree two extensions. Also, the intermediate value theorem gives that every odd-degree polynomial $f \in \mathbb{R}[x]$ has a root in $\mathbb{R}$. Again, in terms of fields, this implies that $\mathbb{R}$ has no proper odd degree extensions.

To prove the theorem, it suffices to show every finite extension $F/\mathbb{C}$ is such that $F = \mathbb{C}$. Enlarging F if necessary, we may assume $F/\mathbb{R}$ (and hence $F/\mathbb{C}$ is also Galois). Set $G = \mathrm{Gal}(F/\mathbb{R}), H = \mathrm{Gal}(F/\mathbb{C})$. We claim G is a 2-group. Since $[\mathbb{C} : \mathbb{R}] = 2$, it is clear that $2||G|$. Now, let $P \in \mathrm{Syl}_2(G)$ and consider the field tower

$$\mathbb{R} = F^G \subseteq F^P \subseteq F.$$

Then $[F^P : \mathbb{R}] = |G : P|$ which is odd and by the observation that $\mathbb{R}$ has no proper odd degree extensions we obtain $|G : P| = 1$ and hence G is a 2-group. Therefore H is also a 2-group. Assuming $H \neq \{1\}$, by Sylow's theorem, there exists a subgroup $D \leq H$ such that $|H : D| = 2$. Then we have the tower

$$\mathbb{C} = F^H \subseteq F^D \subseteq F,$$

and by the same argument as above see $[F^D : \mathbb{C}] = 2$, contradicting the fact that $\mathbb{C}$ has no degree two extensions. Thus $H = 1$ and hence $F = \mathbb{C}$, as desired. □

2. Rings and Modules

Throughout R will denote a (not necessarily commutative) ring. We denote the category of left R-modules by ${}_R\mathbf{Mod}$ and similarly $\mathbf{Mod}_R$ denotes the category of right R-modules.

2.1. Free and Projective Modules.

We define a module ${}_RM$ to be *free* if M has a *basis*. That is, a collection of elements $(m_i)_{i\in I}$ such that every $m \in M$ can be uniquely written as a finite sum

$$\sum_{i\in I} r_i m_i.$$

By finite, we mean that all but finitely many r_i above are 0. Note that direct sums of free modules are free. If $F_j \cong R^{(I_j)}$ for some $j \in J$, then we see

$$\bigoplus_{j\in J} F_j \cong R^I,$$

where $I = \bigsqcup_{j\in J} I_j$. Moreover any module is a homomorphic image of some free module. To see this let $M \in {}_R\mathbf{Mod}$, and $(m_i)_{i\in I}$ be a generating family for M. Then the map $R^{(I)} \to M$ given by

$$(r_i)_{i\in I} \mapsto \sum_{i\in I} r_i m_i,$$

is plainly seen to be an epimorphism.

Lemma 2.1. *All left R-modules are free if and only if R is a skew field.*

Proof. If R is a skew field, any R-module inherits all properties of a vector space, except for commutativity of scalars. Thus since all vector spaces have a basis, all R-modules have a basis.

In particular, the standard Zorn's Lemma argument applies since all singleton's form linearly independent sets over a skew field. Since singleton's are not necessarily linearly independent in a general module, one cannot guarantee the collection of linearly independent sets is non-empty.

Conversely, suppose all left R-modules are free and let L be a maximal left ideal of R. Then $M = R/L$ is a left R-module and therefore free by hypothesis. By maximality of L, this module has exactly two submodules, namely 0 and M, i.e. it is irreducible. We know $M \cong R^{(I)}$ for some I and by irreducibility $|I| = 1$. That is, M is the left regular R-module. Hence for any non-zero $x \in R$, $Rx = R$ and hence there exists some $y \in R$ such that $yx = 1$. Similarly there exists some $z \in R$ such that $zy = 1$, from which we see

$$z = z1 = z(yx) = (zy)x = 1x = x,$$

and hence y is the desired inverse for x. □

2.2. **Intermezzo: The Tensor Product.**

Let ${}_RM \in \mathbf{Mod}_R, N_R \in {}_R\mathbf{Mod}$. The *tensor product* of M, N is the abelian group defined by

$$M \otimes_R N := \mathbb{Z}^{M\times N}/\mathcal{R},$$

where $\mathbb{Z}^{M\times N}$ is the free abelian group on $M \times N$, and $\mathcal{R}$ is the subgroup generated by the elements

$$(m + m', n) - (m, n) - (m', n),$$
$$(m, n + n') - (m, n) - (m, n'),$$
$$(rm, n) - (m, rn).$$

The standard notation is to write $(m, n) + \mathcal{R} := m \otimes n$. These are the so-called simple tensors and they generate $M \otimes_R N$ as an abelian group (justified below).

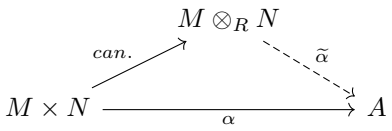
There is a canonical map $M \times N \to M \otimes_R N$ given by the assignment

$$(m, n) \mapsto m \otimes n.$$

This map is generally not a group homomorphism however it is R-balanced. That is, the following criteria are satisfied:

$$(m + m') \otimes n = (m \otimes n) + (m' \otimes n),$$
$$m \otimes (n + n') = (m \otimes n) + (m \otimes n'),$$
$$rm \otimes n = m \otimes rn.$$

This leads us to discuss a universal property of tensor products. Given an abelian group A and any R-balanced map $\alpha : M \times N \to A$, there exists a unique group homomorphism $\widetilde{\alpha} : M \otimes_R N \to A$ such that the diagram below commutes.



That is $\widetilde{\alpha}(m \otimes n) = \alpha(m,n)$. For a proof, note that α gives rise to a unique map $\mathbb{Z}^{M\times N} \to A$ given by $\widetilde{\alpha}(m,n) = \alpha(m,n)$. Moreover since α is R-balanced, this map vanishes on $\mathcal{R}$ and hence passing to the quotient gives the desired map $M \otimes_R N \to A$.

It follows from the universal property that the simple tensors generate $M \otimes_R N$. To see this, set $A := M \otimes_R N/\langle m \otimes n | m \in M, n \in N\rangle$. Consider the map $\alpha : M \otimes_R N \to A$ given by the zero map. This map is trivially R-balanced and hence we get a unique map $\widetilde{\alpha} : M \otimes_R N \to A$. But note that the canonical epimorphism π also satsifies $\pi(m \otimes n) = 0$ for all $m \in M, n \in N$ and hence by uniqueness $\pi = 0$. That is $A = 0$, as desired.

The universal properties gives a bijection between all R-balanced maps $M \times N \to A$, and group homomorphisms $M \otimes_R N \to A$. In other words, group homomorphisms $M \otimes_R N \to$ lift to $M \times N$ through the canonical map. In the interest of making these ideas more concrete, we explicitly compute the tensor product for the ring $R = \mathbb{Z}$ and modules $M = \mathbb{Z}/(m), N = \mathbb{Z}/(n)$. Note that for any $\overline{x} \in M, \overline{y} \in N$,

$$\overline{x} \otimes \overline{y} = x(1 \otimes \overline{y}) = xy(1 \otimes 1).$$

Hence $\langle 1 \otimes 1\rangle = M \otimes_R N$. Then for $d = (m,n)$ we know there exists $a, b \in \mathbb{Z}$ such that $am + bn = d$. Thus

$$d(1 \otimes 1) = (\overline{am} \otimes 1) + (1 \otimes \overline{bn}) = 0,$$

whence we conclude $|1 \otimes 1| \Big| d$. On the other hand, we have the map $\mu : M \times N \to \mathbb{Z}/(d)^2 \to \mathbb{Z}/(d)$, given by the assignments

$$(\overline{x}, \overline{y}) \mapsto (\overline{x}, \overline{y}) \mapsto \overline{xy}.$$

This map is $\mathbb{Z}$-balanced and hence extends to a group homomorphism $\widetilde{\mu} : M \otimes_{\mathbb{Z}} N \to \mathbb{Z}/(d)$. $\widetilde{\mu}(1 \otimes 1) = 1$ and hence the order of $1 \otimes 1$ cannot be smaller than d. Thus we have shown

$$\mathbb{Z}/(m) \otimes_{\mathbb{Z}} \mathbb{Z}/(n) \cong C_{(m,n)}.$$

As another example, consider the regular left and right modules ${}_RR, R_R$. We then claim that for any $M \in \mathbf{Mod}_R, N \in {}_R\mathbf{Mod}$,

$$M \otimes_R R \cong M,$$
$$R \otimes_R N \cong N.$$

To see this, consider the map $M \times R \to M$ given by $(m,r) \mapsto mr$. This map is R-balanced and hence extends to a map $M \otimes_R R \to M$ given by $m \otimes r \mapsto mr$. On the other hand we have the map $M \to M \otimes_R R$ given by $m \mapsto m \otimes 1$. One easilly checks that these maps are inverses, establishing the isomorphism.

We now discuss some categorical properties of the tensor product, the first of which being bifunctoriality. That is, the map $\cdot \otimes_R \cdot : \mathbf{Mod}_R \times {}_R\mathbf{Mod} \to \mathbf{AbGrps}$ is a functor in each of its components. Given a fixed $N \in {}_R\mathbf{Mod}$, $\cdot \otimes_R N$ acts on objects as expected, mapping $M \mapsto M \otimes_R N$. Also, given a map $f : M \to M'$, $f \otimes_R N$ correponds to the map $M \otimes_R N \to M' \otimes_R N$ given by

$$m \otimes n \mapsto f(m) \otimes n.$$

Since elements of the tensor product are tnot uniquely expressed in terms of simple tensors we must verify $f \otimes_R N$ is well-defined. To see this, consider the map $M \times N \to M' \otimes_R N$ given by $(m,n) \mapsto f(m) \otimes n$. This map is R-balanced since f is a module homomorphism and hence this extends to a map $M \otimes_R N \to M' \otimes_R N$, such that $(m,n) \mapsto f(m) \otimes n$ establishing well-definedness of the homomorphism.

Next we discuss a property known as right-exactness. Fix a left module ${}_RN$ and consider an exact sequence of right modules

$$M \xrightarrow{f} M' \xrightarrow{f'} M'' \to 0.$$

Then the corresponding sequence

$$M \otimes_R N \xrightarrow{f\otimes_R N} M' \otimes_R N \xrightarrow{f'\otimes_R N} M'' \otimes_R N \to 0,$$

is also exact. We omit the proof, although note that typically exact sequences have an extra zero on the far-left, which makes the map f necessarily injective. Injectivity is in general not preserved under the action of the functor $\cdot \otimes_R N$ and as such it is left out of the above. Thus one says the $\cdot \otimes_R N$ is *right-exact* and if a full exact sequence was preserved we'd say the functor is exact. For an example where injectivity is not preserved, let $R = \mathbb{Z}, M = M' = \mathbb{Z}, N = \mathbb{Z}/(2)$. Let the map $f : M \to M'$ be defined by $m \mapsto 2m$. Then

$$f \otimes_{\mathbb{Z}} \mathbb{Z}/(2) : \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/(2) \to \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/(2),$$

is the zero map.

Let I be a left ideal of the ring R. Then we have an exact sequence of left R-modules given by

$$(0 \to) I \xrightarrow{i} R \xrightarrow{\pi} R/I \to 0.$$

Upon tensoring with an arbitrary $M \in \mathbf{Mod}_R$, we get the exact sequence

$$M \otimes_R I \xrightarrow{M\otimes_R i} M \otimes_R R \xrightarrow{M\otimes_R \pi} M \otimes_R R/I \to 0.$$

Moreover, since $M \otimes_R R \cong M$ via the assignment $m \otimes r \mapsto mr$ and $M \otimes_R \pi$ is an epimorphism we obtain

$$M \otimes_R (R/I) \cong M/MI,$$

where $MI = (M \otimes_R i)(M \otimes_R I) = \{mi | m \in M, i \in I\}$.

Another property of the tensor product is the fact that it commutes with direct sums. That, for a collection $(M_i)_{i\in I} \subset \mathbf{Mod}_R, (N_j)_{j\in J} \subset_R \mathbf{Mod}$, one has

$$\left(\bigoplus_{i\in I} M_i\right) \otimes_R \left(\bigoplus_{j\in J} N_j\right) \cong \bigoplus_{(i,j)\in I\times J} (M_i \otimes_R N_j).$$

To justify this it is enough to show

$$M \otimes_R \left(\bigoplus_{j\in J} N_j\right) \cong \bigoplus_{j\in J} (M \otimes_R N_j),$$

as the argument for fixed $N \in \mathbf{Mod}_R$ is identical. To that end, consider the map $\mu_j : N_j \to N := \oplus_{j\in J} N_j$, given by the standard inclusion. We also have the standard projection map $\pi_j : N \to N_j$, and it is clear $\pi_j \circ \mu_j = \mathrm{Id}_{N_j}$, and

$$\sum_{j\in J} (\mu_j \circ \pi_j)(n) = n.$$

Then upon tensoring we see the maps we

$$M \otimes_R N \rightleftarrows \bigoplus_{j\in J}(M \otimes_R N_j)$$
$$m \otimes n \mapsto (m \otimes \pi_j(n))_{j\in J}$$
$$\sum_{j\in J}(m \otimes \mu_j(n)) \hookleftarrow (m \otimes n)_{j\in J}$$

define group homomorphisms which are inverses.

Some of the above isomorphisms seem to imply the tensor product inherits more structure than just that of an abelian group. To investigate this structure we first introduce the bimodule. Given two rings R, S an (R, S)-*bimodule* is an abelian group M that is both a left R-module and a right S-module. Fixing notation we write ${}_RM_S \in {}_R\mathbf{Mod}_S$. For example, given a ring homomorphism $f : R \to S$, we get the bimodule ${}_RS_S$ where the R action is defined by $r.s = f(r)s$.

Now, given $M_R, {}_RN_S$ the tensor product

$$M \otimes_R N,$$

inherits the structure of a right S-module via $(m \otimes n)s = m \otimes ns$. One must check that this action is well-defined since there is no uniqueness of representation in $M \otimes_R N$. But simply note that map $\varphi_s : M \times N \to M \times N \to M \otimes_R N$ defined by

$$(m, n) \mapsto (m, ns) \mapsto m \otimes ns,$$

is R-balanced and hence extends to a group homomorphism

$$\widetilde{\varphi_s} : M \otimes_R N \to M \otimes N,$$

defined by $m \otimes n \mapsto m \otimes ns$. This establishes well-definedness.

Using the example above, given a ring homomorphism $f : R \to S$, we can view S as an (R, S) bimodule. The we get a functor $\cdot \otimes_R S : \mathbf{Mod}_R \to \mathbf{Mod}_S$ given by

$$M \mapsto M \otimes_R S.$$

This concludes our intermezzo on the tensor product, and as such we return to our discussion of free modules. Given a free-module ${}_RM$, ideally one could speak on the size of its basis in the same way one talks about the dimension of vector space. Unfortunately over abitrary rings, free modules can have bases of varying sizes. Nevertheless we can develop the notion of the rank of the module under certain circumstances. Let R be a ring such that there exists a ring homomorphism $f : R \to D$, where D is some skew field. Then we define the *rank* of M to be given by

$$\operatorname{rank}(M) := \dim_D(D \otimes_D M).$$

This is, in fact, independent on the choice of f.

Lemma 2.2. *Let $(m_j)_{j\in J}$ be any generating family of M. Then*

$$|J| \geq \operatorname{rank}(M),$$

and if $(m_j)_{j\in J}$ is a basis, equality holds.

Proof. We have the standard epimorphism $\pi R^{(J)} \twoheadrightarrow M$ given by

$$(r_j)_{j\in J} \mapsto \sum_{j\in J} r_j m_j.$$

Then considering the functor $D \otimes_R \cdot : {}_R\mathbf{Mod} \to {}_D\mathbf{Mod}$ we see

$$\begin{array}{ccc} M & & D \otimes_R M \\ {\scriptstyle\pi}\uparrow\!\!\uparrow & & \uparrow\!\!\uparrow{\scriptstyle D\otimes_R \pi} \\ R^{(J)} & & D \otimes_R R^{(J)} \end{array}$$

gives rise to the map $D \otimes_R \pi : D \otimes_R R^{(J)} \to D \otimes_R M$, which is onto by right-exactness. Moreover

$$D \otimes_R R^{(J)} \cong (D \otimes_R R)^{(J)} \cong D^{(J)},$$

and hence by linear algebra, the above epimorphism gives that

$$\dim_D(D^{(J)}) = |J| \geq \dim_D(D \otimes_R M) = \operatorname{rank}(M).$$

□

We now move on to discussing projective modules. A module M is said to be *projective* if it is the direct summand of some free module F. That is, $F = M' \oplus N$, with $M' \cong M$. Thus, free modules are evidently projective however the converse is not true. As an example take $R = M_2(\mathbb{R}), F =_R R$. We have the left ideal of R given by

$$M = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} | a, b \in \mathbb{R} \right\},$$

which is plainly seen to be projective. However if $M \cong R^{(I)}$ then we'd have

$$\dim_{\mathbb{R}}(M) = 2 = |I| \dim_{\mathbb{R}}(R) = 4|I|,$$

a contradiction. Thus M is projective but not free. Moreover it is easilly seen that direct summands of projective modules are projective, althought evidently direct summands of free modules are not free. Also note that is again easy to see that direct sums of projective modules are projective.

Theorem 2.3. *The following are equivalent for $P \in {}_R\mathbf{Mod}$.*

i) P is projective.

ii) Given a diagram in ${}_R\mathbf{Mod}$,

$$\begin{array}{ccc} & & P \\ & {\scriptstyle\gamma}\swarrow & \downarrow{\scriptstyle\alpha} \\ M & \xrightarrow[\beta]{} & N \end{array},$$

we have the existence of γ such that $\beta \circ \gamma = \alpha$.

iii) Every epimorphism $\pi : M \twoheadrightarrow P$ splits. That is, there exists a map $\sigma : P \to M$ such that $\pi \circ \sigma = Id_P$.

Proof. ii) $\Rightarrow$ iii): Let π be an epimorphism $\pi : M \twoheadrightarrow P$ and consider the diagram below,

$$\begin{array}{ccc} & & P \\ & {\scriptstyle\gamma}\swarrow & \downarrow{\scriptstyle \mathrm{id}} \\ M & \xrightarrow[\pi]{} & P \end{array}$$

By *ii)* we have $\gamma \circ \pi = \mathrm{id}_P$, and hence the epimorphism splits.

iii) $\Rightarrow$ *i):* We have the existence of a free module F together with an epimorphism $\pi : F \twoheadrightarrow P$. By hypothesis this map splits, so there exists a map $\sigma : P \to F$ such that $\pi \circ \sigma = \mathrm{id}_P$. From our homework problem we conclude

$$F = \sigma(P) \oplus \mathrm{Ker}\pi.$$

σ has a left inverse and is therefore injective, hence $\sigma(P) \cong P$ and we conclude P is projective.

i) $\Rightarrow$ *ii):* Suppose there is some free module $F \in_R \mathbf{Mod}$ such that $F = P' \oplus N$, where $P' \cong P$. Then we have maps in ${}_R\mathbf{Mod}$ given by

$$\pi : F \twoheadrightarrow P' \xrightarrow{\sim} P,$$
$$\mu : P \xrightarrow{\sim} P \hookrightarrow F.$$

As such we can add to the diagram as in *ii)* thusly.

$$\begin{array}{ccc} & & F \\ & & {\scriptstyle\mu}\uparrow \quad \downarrow{\scriptstyle\pi} \\ & & P \\ & & \downarrow{\scriptstyle\alpha} \\ M & \xrightarrow[\beta]{} & N \end{array}$$

Then define $\varphi : F \to M$ as follows. Choose some basis $(f_i)_{i\in I}$ for f and choose elements $m_i \in M$ such that

$$\beta(m_i) = \alpha \circ \pi(f_i),$$

and set $\varphi(f_i) = \beta(m_i)$. Then note $\beta \circ \varphi = \alpha \circ \pi$ and therefore setting $\gamma := \varphi \circ \mu$ we get

$$\beta \circ \gamma = \beta \circ \varphi \circ \mu = \alpha \circ \pi \circ \mu = \alpha,$$

as desired. □

Theorem 2.4. *Let R be a ring such that every left ideal of R is projective as an R-module. Then every submodule of a free left R-module is isomorphic to a direct sum of left ideal of R (and consequently projective).*

Note that any commutative PID satisfies the hypothesis in Theorem 2.4. This is because all left ideals are principal and hence free of rank 1. The conclusion of the theorem then implies that all submodules of a free left R-module are in fact free. In general, rings that satisfy the hypothesis of the theorem are the so-called *left-hereditary* domains. For commutative rings, it turns out the class of hereditary domains is precisely the class of *Dedekind domains*.

Proof. Let $F \in_R \mathbf{Mod}$ be free and $M \subseteq F$ be a submodule. Fix a basis $(x_i)_{i\in I}$ of F so that any $x \in F$ can be written

$$x = \sum_{i\in I} c_i(x)x_i,$$

uniquely such that only finitely many $c_i(x) \neq 0$. For each $i \in I$, we have the left R-module homomorphism $c_i : F \to R$ given by $x \mapsto c_i(x)$. Define a well-ordering on I, i.e. a total order $\leq$ such that every subset of I has a smallest element. The

existence of such a well-ordering is guaranteed by the axiom of choice. Then for any $i \in I$, set

$$F_i := \sum_{j \leq i} Rx_j.$$
$$F_i^- := \sum_{j<i} Rx_j = \bigcup_{j<i} F_j.$$

Then each element $x \in F_i$ can uniquely be written in the form

$$x = x^- + c_i(x_i),$$

for some $x^- \in F_i^-$.

Now, consider $M \cap F_i := F_i$ along with the restriction $c_i|_{M_i} : M_i \to R$, for each i. By hypothesis, the image of this restriction $L_i := c_i|_{M_i}(M_i)$ is a projective R-module. Trivially this map is surjective and therefore Theorem 2.3 gives that $c_i|_{M_i}$ splits. That is, there exists some $s_i : L_i \to M_i$ such that $c_i|_{M_i} \circ s_i = \mathrm{Id}_{L_i}$, and by Homework this means

$$M_i = \mathrm{Ker}(c_i|_{M_i}) \oplus s_i(L_i).$$

For brevity we write $s_i(L_i) = N_i \cong L_i$ and also we note that

$$\mathrm{Ker}(c_i|_{M_i}) = M_i \cap F_i^- = M \cap F_i^- = \bigcup_{j<i} M_j. \tag{4}$$

Therefore, it is enough to show that $M = \bigoplus_{i \in I} N_i$, since each N_i is an isomorphic image of an ideal of R.

We first show the sum in $\sum_{i \in I} N_i := S$ is direct. Assume that

$$n_1 + \cdots + n_t = 0,$$

with each $n_j \in N_{i_j}$ for some $j \in I$. Note then that $n_t \in N_{i_t} \cap (M_{i_t} \cap F_{i_t}^-)$. By Equation 4 this must imply $n_t = 0$. Continuing inductively, we then see all $n_{i_j} = 0$ and so the sum is direct.

We conclude by showing $S = M$. Clearly $M = \cup_{i \in I} M_i$ and therefore $S \subseteq M$. Suppose $S \subsetneq M$. Then some $M_k \not\subseteq S$, and by the well ordering on I we can choose the minimal such k where this holds. Let $x \in M_k \setminus S$. Using Equation 4 we have that

$$x = x^- + n_k,$$

with $x^- \in \cup_{j<k} M_j, n_k \in N_k$. By choice of k all $M_j \subseteq S$, and since $N_k \subseteq S$ we have $x \in S$, a contradiction. Thus

$$M = \bigoplus_{i \in I} N_i,$$

completing the proof. □

2.3. **Completely Reducible Modules.**

Recall that a module M is said to be *irreducible* if the only submodules of M are 0 and M. For example, any diviision ring D is a irreducible D-module (and also a 1-dimensional D vector space). Taking inspiration from vector spaces, we note that any D-vector space can be written as a direct sum of irreducible modules. In general, a module $M \in_R \mathbf{Mod}$ that can be written as a direct sum of irreducble modules is said to be *completely reducible.*

Theorem 2.5. *The following are equivalent for a module M.*

i) M is completely reducible.
ii) M is a sum of irreducible submodules.
iii) Every submodule $N \subseteq M$ has a complement. That is, there exists $C \subseteq M$ such that

$$M = N \oplus C.$$

Proof. The implication *i) ⇒ ii)* is trivial so we begin by showing *ii) ⇒ iii)*. To that end, suppose $M = \sum_{i \in I} S_i$, with all $S_i \subseteq M$ irreducible. We claim given any submodule N, there exists some $J \subseteq I$, such that

$$M = N \oplus \bigoplus_{j \in J} S_j.$$

Clearly this will justify the result. To see this, let $N \subseteq M$ and using Zorn's Lemma let $J \subseteq I$ be maximal such that the following sum is direct:

$$M' := N \oplus \bigoplus_{j \in J} S_j.$$

If $M' \neq M$, then there exists some $k \in I$, such that $S_k \not\subseteq M'$. By irreducibility of S_k it must then hold that $S_k \cap M' = 0$. Hence the following sum is direct

$$M' + S_k = N \oplus \bigoplus_{j \in J} S_j \oplus S_k,$$

contradicting maximality of the chosen $J \subseteq I$. Also note, that taking $N = 0$, we see that the assumptions of *ii)* also imply *i)*

We conclude by showing *iii) ⇒ ii)*. Let S denote the sum of all irreducible submodules of M. We remark that S could be 0, for instance the regular $\mathbb{Z}$ module has no irreducible submodules. Suppose $M \neq S$. Then by assumption there exists a complement $C \subseteq M$ such that

$$M = S \oplus C.$$

It is enough to show that every non-zero submodule contains an irreducible submodule, as this would contradict directness of the above sum. To see this, let $0 \neq c \in C$ and replace C by $Rc \subseteq C$. This way we may assume C to be finitely generated. By Zorn's Lemma, C has a maximal submodule, say $D \subsetneq C$, and by hypothesis D has a complement , say

$$M = D \oplus E.$$

It follows that

$$C = D \oplus (E \cap C).$$

Thus

$$E \cap C \cong C/D,$$

and since D is maximal, by submodule correspondence, $E \cap C$ must be irreducible. □

Corollary 2.6.

a) Submodules and homomorphic images of completely reducible modules are again completely reducible.
b) If ${}_R R$ is completely reducible then all R-modules are completely reducible.

Proof. Let M be a completely reducible module, say $M = \sum_{i\in I} S_i$, with each S_i irreducible, with $f : M \twoheadrightarrow M'$ a module epimorphism. Then simply note

$$M' = f(M) = \sum_{i\in I} f(S_i) = \sum_{\substack{i\in I \\ f(S_i)\neq 0}} f(S_i) \cong \sum_{\substack{i\in I \\ f(S_i)\neq 0}} S_i,$$

since if $f(S_i) \neq 0$, by irreducibility it must then hold that $\mathrm{Ker} f|_{S_i} = 0$. In representation theory, this simply observation is known as *Schur's Lemma*.

Say $N \subseteq M$ is a submodule of some completely reducible module. Then there exists a complement $C \subseteq M$, such that

$$M = N \oplus C.$$

Projecting onto N we see that N is simply a homomorphic image of M, whence completely reducible by the above.

Say ${}_R R$ is completely reducible. Then in particular all free R-modules are completely reducible this complete reducibility is preserved under direct sums. To conclude simply note that any R-module is a homomorphic image of a free module, whence completely reducible. □

Rings as in *b)* in Corollary 2.6 are said to the *semi-simple*. A well-known theorem known as the Wedderburn Structure Theorem says that the semi-simple rings are precisely rings R such that

$$R \cong M_{n_1}(D_1) \times \cdots \times M_{n_t}(D_t),$$

for some $D_1, \ldots, D_t$, all division rings.

2.4. **Modules over Principal Ideal Domains.**

Throughout R is a commutative PID unless otherwise stated. In particular this means R is Noetherian, and from Algebra Lecture Notes we recall that this implies all finitely generated left R-modules are also Noetherian. Also, Theorem 2.4 gives that all submodules of a free R-module are again free. Finally, Lemma 2.2 says that all free R-modules have a well-defined rank as the cardinality of a set which forms a basis. The following theorem is workhorse that will make subsequent results in this section easy to prove. The proof of the theorem however, is a bit laborious and as such we provide a mere sketch of the proof, omitting the cumbersome details.

Theorem 2.7. *Let F be a finitely generated free R-module of finite rank s over a principal ideal domain. Let $M \subseteq F$ be a submodule. Then there exists a basis $(x_i)_1^s$ of F and a family of elements $(a_i)_1^t$ of R such that*

- $t < s$,
- $a_1 | a_2 | \ldots | a_t$,
- $(a_i x_i)_1^t$ *forms a basis for* M.

In particular, $t = \mathrm{rank}\, M \leq s = \mathrm{rank}\, F$.

Proof. We begin first with a generality, namely dual modules. Given an arbitrary $M \in_R \mathbf{Mod}$, (here R can be any commutative ring) put $M^* = \mathrm{Hom}_R(M, R)$. M^* is again an R-module as follows under pointwise addition and scalar multiplication of maps. In fact for any $M, N \in_R \mathbf{Mod}, \mathrm{Hom}_R(M, N)$ is similarly an R-module and thus are all objectives in the category of R-modules themselves.

We now proceed with the proof of the theorem. Clearly, we may assume $M \neq 0$, and for any $x \in F$, define

$$c(x) := \{\lambda(x) | \lambda \in F^*\}.$$

This defines an ideal in R, known as the *content of* x, and is thus generated by one element, say $c(x) = (c_x)$ for each $x \in F$. We now make the following claims, the proof of some we omit:

a) If $x \neq 0$, then $c_x \neq 0$, and there exists a unique $f_x \in F$ such that $x = c_x f_x$.
b) Choose $x \in M$ such that $c(x)$ is maximal among all contents. (Such a choice is guaranteed by R being Noetherian.) Pick $\lambda \in F^*$ with $\lambda(x) = c_x$. Then

$$F = Rf_x \oplus \mathrm{Ker}\lambda,$$

and

$$M = Rx \oplus \mathrm{Ker}\lambda|_M.$$

c) For all $\mu \in F^*$, $\mu(M) \subseteq (c_x)$ with x as in *b*.

Before proving parts of the above, we complete the proof granting the claims. We argue by induction on $\operatorname{rank} F$. Since $F' := \mathrm{Ker}\lambda, M' := \mathrm{Ker}\lambda|_M \subseteq F$, they are also free with

$$\operatorname{rank} F' = \operatorname{rank} F - 1 = s - 1,$$
$$\operatorname{rank} M' = \operatorname{rank} M - 1 = t - 1.$$

By induction, there is a basis of F', say $(x_i)_2^s$ and a family of elements $(a_i)_2^t$, of R such that $t \leq s$, $a_2|a_3|\ldots|a_t$, with $(a_i x_i)_2^t$ a basis for M'. Per claim *b)*, setting $x_1 = f_x$ and $a_1 = c_x$ we obtain $(x_i)_1^s$ is a basis for F and since $a_1 x_1 = x$, we see $(a_i x_i)_1^t$ form a basis for M.

To conclude, we need only show $a_1|a_2$. Define $\mu \in F^*$ by $\mu(x_2) = 1, \mu(x_i) = 0$, for all $i \neq 2$. Then we see

$$a_2 = \mu(a_2 x_2) \in \mu(M) \subseteq (a_1),$$

giving $a_1|a_2$.

Having proved the result granting the three claims above, we now justify only *a)* above, omitting the proof of the other two claims. Let $(b_i)_1^s$ be any basis of F and define $b^i \in F^*$ by $b^i(b_j) = \delta_{ij}$. Then for any $x \in F$, write

$$x = \sum_{i \in I} r_i b_i,$$

for $r_i \in R$, to get $b^i(x) = r_i \in c(x) = (c_x)$. Thus, if $x \neq 0$, then some $r_i \neq 0$, and hence $c_x \neq 0$. In general, $c_x | r_i$, and so $r_i = c_x r_i'$ for some $r_i' \in R$. Then we have

$$x = c_x \left(\sum_{i \in I} r_i' b_i \right),$$

and hence $f_x = \sum_{i \in I} r_i' b_i$ gives the result. For uniqueness, simply observe that F is torsion-free. $\square$

Corollary 2.8. *Given $A \in M_{m\times n}(R)$, there exists $S \in \mathrm{GL}_m(R), T \in \mathrm{GL}_n(R)$, such that*

$$SAT = \begin{pmatrix} a_1 & & & & & \\ & \ddots & & & & \\ & & a_t & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix},$$

with $a_1|a_2|\dots|a_t$.

Proof. Recall some basic facts about matrices over any commutative ring R. Given ${}_RF$, ${}_RG$ free R-modules with fixed bases $(f_i)_1^m, (g_j)_1^n$, we have the standard bijection $\mathrm{Hom}_R(G,F) \xrightarrow{\sim} M_{m\times n}(R)$, where $\alpha \mapsto (a_{ij})$, with $\alpha(g_j) = \sum_{i=1}^m a_{ij} f_j$. Moreover composition of homomorphisms corresponds to matrix multiplication (when defined) under this map. Also, module isomorphisms correpond to invertible matrices, which by multiplicativity of the determinant are precisely matrices $A \in M_n(R)$ such that $\det(A) \in R^\times$.

For the proof of the corollary, let $\alpha : G \to F$ be the map corresponding to the matrix A. Set $M = \alpha(G)$ and choose elements as in Theorem 2.7 such that $(x_i)_1^t$ is a basis for F, $(a_i)_1^t$ are elements in R such that $(a_i x_i)_1^t$ form a basis for M. Moreover $\alpha : G \twoheadrightarrow M$, is an epimorphism onto M and therefore splits. Hence there exists $\sigma : M \to G$ such that $\alpha \circ \beta = \mathrm{Id}_M$. Thus we have

$$G = \mathrm{Ker}\alpha \oplus \beta(M),$$

and for brevity fix $M' := \beta(M)$. Set $y_i = \beta(a_i x_i)$ to get a basis $(y_i)_1^t$ of M' and let $(y_i)_{t+1}^n$ be any basis of $\mathrm{Ker}\alpha$, to obtain the basis $(y_i)_1^s$ of G. Define $\tau : G \xrightarrow{\sim} G$ by $\tau(g_j) = y_j$, and $\sigma : F \xrightarrow{\sim} F$ by $\sigma(x_i) = f_i$. Then

$$\beta\alpha\tau(g_j) = \beta\alpha(y_j) = \begin{cases} a_j f_j & j \le t, \\ 0 & j > t \end{cases}.$$

To conclude simply note that with respect the original bases, the matrix for $\beta\alpha\tau$ is precisely the desired matrix. □

A *lattice* is a free abelian group (i.e. $\mathbb{Z}$-module) of finite rank. Given a lattice L or rank r, an endomorphism $\alpha \in \mathrm{End}_{\mathbb{Z}}(L)$ corresponds uniquely to a matrix $A \in M_r(\mathbb{Z})$.

Corollary 2.9. *Let L be a lattice and let $\alpha \in \mathrm{End}_{\mathbb{Z}}(L)$ be such that $\det\alpha \neq 0$. Then*

$$|\det\alpha| = |L : \alpha(L)|.$$

Proof. Fix a basis $(l_i)_1^r$ of L. By Corollary 2.8 there are isomorphisms $\sigma, \tau : L \xrightarrow{\sim} L$, such that the matrix of $\sigma\alpha\tau$ with respect to $(l_i)_1^r$, is of the form

$$\begin{pmatrix} a_1 & & & & & \\ & \ddots & & & & \\ & & a_t & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix},$$

such that $a_1|a_2|\dots|a_t$. By multiplicativity of the determinant, along with the fact that invertible matrices in $\mathbb{Z}$ have determinant ± 1, we see

$$\det(\sigma\alpha\tau) = \pm\det(\alpha) \neq 0,$$

and hence $t = r$. In fact the above equation implies $|\det\alpha| = |a_1 a_2 \dots a_r|$. Moreover note that

$$L/\alpha(L) = L/\alpha(\tau(L)) \cong L/\sigma(\alpha(\tau(L))) = \left(\bigoplus_{i=1}^{r} \mathbb{Z}\, l_i\right) / \left(\bigoplus_{i=1}^{r} \mathbb{Z}\, a_i l_i\right),$$

giving $|L : \alpha(L)| = |a_1 \dots a_r|$, as desired. □

Given any commutative domain R, $M \in_R \mathbf{Mod}$, the we define

$$\operatorname{Tor} M := \{m \in M | rm = 0 \text{ for some } r \in R\}.$$

This is easilly seen to be a submodule of M and is referred to as the *torsion submodule* of M. If $\operatorname{Tor} M = 0$, M is said to be *torsion-free*. If $R = \mathbb{Z}$, then $\operatorname{Tor} M$ is plainly seen to be the collection of all elements of finite order. We also remark here that for any module M, $\operatorname{Tor}(M/\operatorname{Tor} M) = 0$. Also, any submodule of a free module must be torsion-free.

Theorem 2.10. *Let R be a PID, $M \in_R \mathbf{Mod}$ be finitely generated. Then*

a) $M = F \oplus \operatorname{Tor} M$, with $F \cong R^r$ for some finite r.
b) $\operatorname{Tor} M \cong R/(a_1) \oplus \cdots \oplus R/(a_t)$, where all a_i are non-zero non-units such that $a_1|a_2|\dots|a_t$.

Before proceeding with the proof we provide a few preliminary remarks. First the ideals in the theorem above are known as the *invariant factors* of M and we will see later that they are uniquely determined. In the case where $R = \mathbb{Z}$, the theorem says that any finite abelian group G can be written

$$G \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_t\mathbb{Z},$$

such that $m_1|m_2|\dots m_t$.

Finally, we remark that with r, t as in the statement of the theorem, $r + t$ is uniquely determined as the minimal number of generators of M. Say M is generated by $(m_i)_1^g$. Then we have the canonical epimorphism $\pi : R^g \twoheadrightarrow M = F \oplus \operatorname{Tor} M$. Tensoring this map by $R/(a_1)$ we then get an epimorphism

$$(R/(a_1))^g \twoheadrightarrow (R/(a_1))^s \oplus \bigoplus_{i=1}^{t} (R/(a_1) \otimes_R R/(a_t)).$$

Moreover since $(a_1) + (a_i) = (a_1)$ for any $i = 1, \dots, t$, this is an epimorphism

$$(R/(a_1))^g \twoheadrightarrow (R/(a_1))^{r+t},$$

from which we see $r + t \leq g$.

Proof. We now provide the proof of Theorem 2.10. Let $(m_i)_1^s$ be a generating family of M of minimal size. We have the usual epimorphism $\pi : R^s \twoheadrightarrow M$, with $\mathrm{Ker}\pi \subseteq R^s$. Using Theorem 2.7 there exists a basis of $(x_i)_1^s$ of R^s and a familty $(a_i)_1^t \subseteq R$, such that $(a_i x_i)_1^t$ is a basis of $\mathrm{Ker}\pi$, and $a_1|a_2|\dots|a_t$. We claim all $a_i \notin R^\times$, for if some $a_i \in R^\times$, we'd then have

$$0 = \pi(a_i x_i) = a_i \pi(x_i),$$

implying $\pi(x_i) = 0$, contradicting minimality of the generating set. Then we have

$$M \cong R^s/\mathrm{Ker}\pi \cong \left(\bigoplus_{i=1}^{s} Rx_i\right) / \left(\bigoplus_{i=1}^{t} Ra_i x_i\right) \cong R^{s-t} \oplus \bigoplus_{i=1}^{t} R/(a_i).$$

Defining $F := R^{s-t}, T := \bigoplus_{i=1}^t R/(a_i)$, it remains only to show $T = \mathrm{Tor}\, M$. To that end, note that for any $i = 1, \dots, t$,

$$(a_t)R/(a_i) = (a_i) + (a_t)/(a_i) = 0,$$

since $(a_t) \subseteq (a_i)$. Hence $T \subseteq \mathrm{Tor}\, M$. Moreover since free modules are torsion-free and M/T is evidently free, we have that $\mathrm{Tor}\, M \subseteq T$, establishing the result. □

For the second structure theorem, we require a general result from ring theory known as the Chinese Remainder Theorem

Theorem 2.11. *Let A be a ring, $I_1, \dots, I_s \trianglelefteq A$ be ideals that are pairwise comaximal. Then*

$$A/\bigcap_{j=1}^{s} I_j \cong A/I_1 \times \cdots \times A/I_s.$$

Moreover, if A is commutative $\bigcap_{j=1}^s I_j = \prod_{j=1}^s I_j$.

Proof. The proof simply amounts to showing the map $A \to A/I_1 \times \cdots \times A/I_s$ given by the assignment

$$a \mapsto (a + I_j)_1^s,$$

is surjective, as its kernel is clearly $\bigcap_{j=1}^s I_j$. To that end, it is enough to show the result for two ideals, I, J and conclude via induction. Since I, J are comaximal, we may choose $x \in I, y \in J$, such that $x + y = 1$. Then given arbitrary $a, b \in A$, we see

$$\begin{aligned} ay + bx &\mapsto (ay + bx + I, ay + bx + J), \\ &= (ay + I, bx + J), \\ &= (ay + ax + I, bx + by + J), \\ &= (a + I, b + J). \end{aligned}$$

For the last assertion note that we certainly have $I \cap J \supseteq IJ + JI$. Then if $a \in I \cap J$,

$$a = a(x + y) = ax + ay \in IJ + JI.$$

□

Theorem 2.12. *Let R be a PID, $M \in_R \mathbf{Mod}$ be finitely generated. Then*

a) $M = F \oplus \mathrm{Tor}\, M$ for some free $F \cong R^r$.

b) $\operatorname{Tor} M \cong \bigoplus_{i=1^s} R/(p_i^{\alpha_i})$ *where all* $p_i \in R$ *are not necessarily distrinct irreducible elements and each* $\alpha_i \geq 1$.

Proof. In view of Theorem 2.10 we need only show that for some invariant factor a,

$$R/(a) \cong \bigoplus_{i=1}^{\ell} R/(p_i^{\alpha_i}).$$

To that end, since R is a UFD, write

$$a = p_1^{\alpha_1} \dots p_\ell^{\ell},$$

Then by the chinese remainder theorem

$$R/(a) \cong \bigoplus_{i=1}^{\ell} R/(p_i^{\alpha_i}),$$

as desired. □

Before continuing on to the next section, we make a few remarks on the usefulness of this structure theorem (which is often to referred as the elementary divisors theorem). Note that each summand in the elementary divisor decomposition is an indecomposable R-module. That is, $R/(p_i^{\alpha_i})$ cannot be written as a direct sum of non-zero submodules.

2.5. **Normal Forms of Matrices.**

With the theory of modules over PIDs above, we now focus on the special case where $R = F[x]$, the polynomial ring over a field F. First, we provide some background from linear algebra. There is an equivalence a categories between ${}_{F[x]}\mathbf{Mod}$ and F-vector spaces together with an endomorphism $T : V \to V$. The correspondence is as follows: Given a module M over $F[x]$, M is in particular an F-vector space via the action of the constant polynomials. Moreover the action of the polynomial x is given by

$$x.v = T(v),$$

for some $T \in \operatorname{End}(V)$ by the axioms of modules. On the other hand, given an F-vector space V and $T \in \operatorname{End}(V)$, define the action of x by $x.v = T(v)$, and the action of the constant polynomials to be the the action of the scalars on V. In summary we have a ring homomorphism $\operatorname{ev}_T : F[x] \to \operatorname{End}_F(V)$ given by $f \mapsto f(T)$ and hence we may define the $F[x]$ action via

$$f.v = f(T)(v).$$

Let V_T denote an $F[x]$-module whose action by x is defined by $T : V \to V$. Then in particular we have defined a functor between the two categories whose action on objects is defined by

$$V_T \leftrightarrow (V, T).$$

Given two F-vector spaces V, V' and $T \in \operatorname{End}(V), T' \in \operatorname{End}(V)$ we define the morphisms in the category of vector spaces with an endomorphism to be those maps $f : V \to V'$, such that

$$f \circ T = T' \circ f.$$

Given an $F[x]$ module homomorphism $f : V_T \to V'_{T'}$ it correponds to the natural F-linear map, $V \to V'$. Moreover by the properties of module homomorphism

$$f(x.v) = x.f(v),$$

which by the equivalence of categories is the same as the requirement that

$$(f \circ T)(v) = (T' \circ f)(v).$$

Moreover if f is an isomorphism we see the above implies

$$T = f^{-1} \circ T \circ f.$$

Consider the case where $\dim_F(V) = n$ for some finite natural number n. Fixing a basis we obtain an isomorphism $V \cong F^n$, and $\mathrm{End}_F(V) = M_n(F)$. Thus given an $F[x]$-module, V_T, T correponds to some matrix $A \in M_n(F)$. If V_T can be written as a direct sum or $F[x]$-modules

$$V_T = V_1 \oplus \cdots \oplus V_s,$$

then since each V_i is an $F[x]$-module the action of x on V_T, restricts to an action of x on V_i. Via the equivalence of categories, that is to say the endomorphism T restricts to an endomorphism of V_i for each i. Thus, assmebling a basis of V_T via bases of the V_i, the matrix A with respect to this basis is block diagonal where the $i$ith block is the matrix of $T|_{V_i}$.

In order to discuss normal forms of matrices we recall the notion of the minimal and characteristic polynomials of a linear transformation from basic linear algebra. Let V be a finite dimensional F-vector space, whose dimension we denote by n, with $T \in \mathrm{End}(V)$. The map $\mathrm{ev}_T : F[x] \to \mathrm{End}_F(V)$, given by $f \mapsto f(T)$, is evidently not injective, since as F-vector spaces

$$\dim_F(F[x]) = \infty, \quad \dim_F(\mathrm{End}_F(V)) = n^2.$$

Hence this map has non-trivial kernel and since $F[x]$ is a PID, we may write $\mathrm{Ker}(\mathrm{ev}_T) = (m_T)$ for a unique monic polynomial m_T. m_T is the *minimal polynomial* of the transformation T, so-called as it is the polynomial of least degree such that $m_T(T) = 0_V$. The *characteristic polynomial* of T is defined by

$$c_T(x) = \det(x\,\mathrm{Id}_V - T) \in F[x].$$

We recall in the case where $n = 2$ if T has associated matrix

$$A = \begin{pmatrix} a & -b \\ -c & d \end{pmatrix},$$

then the characteristic polynomial is given by

$$c_T = c_A = x^2 - (a+d)x + ad - bc = x^2 - \mathrm{tr}(T) + \det(T).$$

The following theorem is what is known as the *rational canonical form* for a linear transformation $T \in \mathrm{End}(V)$.

Theorem 2.13. *Given $T \in \mathrm{End}_F(V)$, V a finite dimensional vector space, there exists non-constant polynomials $a_1, \ldots, a_t \in F[x]$, such that*

i) $a_1 | a_2 | \ldots | a_t$,

ii) The matrix of T with respect to a suitable basis of V is block diagonal with blocks of the form

$$c_{a_i} = \begin{pmatrix} 0 & & & -\alpha_0 \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & \\ & & 1 & -\alpha_{d-1} \end{pmatrix},$$

where $a_i = x^d - \alpha_{d-1}x^{d-1} + \cdots + \alpha_0$.

iii) The minimial polynomial of T *is precisely* a_t*, and the characteristic polynomial is* $a_1 a_2 \dots a_t$.

Proof. Consider the $F[x]$ vector space V_T. Since $F[x]$ is a PID we may apply Theorem 2.10 to see that

$$V_T \cong \bigoplus_{i=1}^{t} F[x]/(a_i),$$

for non-constant monic polynomials $a_i \in F[x]$ such that $a_1|a_2|\dots|a_t$. V_T has no free part above since as an F-vector space, V has finite dimension and $F[x]$ is an infinite dimensional F vector space. Assembling a basis for V_T from bases of all summands above, the resulting matrix of T will be block diagonal for each summand. A careful choice of this basis will lead to the desired forms of the blocks. Write each $a = a_i = x^d + \alpha_{d-1}x^{d-1} + \cdots + \alpha_0$, and pick the standard basis of $F[x]/(a_i)$ $\{1, x, \dots, x^{d-1}\}$. Thus our basis for each summand is precisely $v_i = x^i + (a)$. Then $T(v_i) = x(x^i + (a)) = x^{i+1} + (a)$, and hence the block has the desired form.

For the characteristic and minimal polynomial, note that $f.V_T = 0$ if and only if $f.F[x]/(a_i) = 0$ for each i. This is equivalent to $a_i|f$ for each i and thus equivalent to $a_t|f$. Since m_T is the polynomial of smallest degree such that $m_T(T) = 0$, which is equivalent to $m_T.V_T = 0$, we see that $m_T = a_t$. The characteristic polynomial result is a simple determinant calculation using the fact that determinants of block diagonal matrices is the product of each block's determinant and hence we omit the calculation. □

Corollary 2.14. *With notation as above,*

i) $c_T(T) = 0$*, or equivalently* $m_T|c_T$.

ii) $c_T|m_T^t$.

Proof. $m_T = a_t|c_T = a_1 a_2 \dots a_t|a_t^t = m_T^t$. □

The above is known as the Cayley-Hamilton Theorem. It follows from this theorem that m_T and c_T have the same irreducible factors and hence the same roots in F^{alg}. These roots are precisely the eigenvalues of T:

$$\begin{aligned} c_T(\lambda) = 0 &\Leftrightarrow \det(\lambda \operatorname{Id}_V - T) = 0, \\ &\Leftrightarrow (\lambda \operatorname{Id}_V - T)(v) = 0 \text{ for some } v \neq 0, \\ &\Leftrightarrow T(v) = \lambda v. \end{aligned}$$

The following theorem is what is known as the *Jordan canonical form* for a linear transformation $T \in \operatorname{End}(V)$.

Theorem 2.15. *Let* V *be a finite dimensional* F*-vector space,* $T \in \operatorname{End}(V)$*. Furthermore assume all eigenvalues of* T *belong to* F*. Then*

(1) there is a basis of V *such that the matrix of* T *has block diagonal form with blocks of the form*

$$J_{\lambda,i} = \begin{pmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{pmatrix}_{n_{\lambda,i} \times n_{\lambda,i}}.$$

(2) The minimal polynomial of T is given by

$$m_T(x) = \prod_{\lambda} (x-\lambda)^{max\{n_{\lambda,i}\}},$$

and the characteristic polynomial is given by

$$c_T(x) = \prod_{\lambda} (x-\lambda)^{\sum n_{\lambda,i}}.$$

Proof. This time we apply the elementary divisor decomposition (Theorem 2.12) to the the $F[x]$ module V_T. Hence we may write

$$V_T \cong \bigoplus_{p \in \mathscr{P}} \left(\bigoplus_{i}^{fin.} F[x]/(p^{\alpha_i(p)}) \right),$$

where $\mathscr{P}$ denotes the collection of all monic irreducibles in $F[x]$. Assembling a basis of V_T from bases of the above direct sum, we again see the matrix corresponding to the transformation T is block diagonal. Exactly as in the proof of Theorem 2.13 the minimal polynomial is seen to be

$$m_T = \prod_{p} p^{\max\{\alpha_i(p)\}},$$

and

$$c_T = \prod_{p} p^{\sum \alpha_i(p)}.$$

From this observation the roots of all p with $\alpha_i(p) \neq 0$ for some i, are precisely the roots of m_T and thus the eigenvalues of T. By assumption on F we therefore obtain that each p must be irreducible of degree 1, i.e. of the form $x - \lambda$ for some $\lambda \in F$. Writing $\alpha_i(p) = n_{\lambda,i}$ the formulations for the characteristic polynomial and the minimal polynomial are then obtained.

It remains to justify the form of the blocks. Fix a summand $W := F[x]/(x-\lambda)^n$. Choose the following basis for W,

$$b_i = (x-\lambda)^{n-i}.$$

To see that this is indeed a basis simply note that $F[x] \cong F[x-\lambda]$ and since $1, x, x^2, \ldots, x^{n-1}$ is a basis in $F[x]/(x^n)$, the image under the isomorphism is a basis for $F[x-\lambda]/(x-\lambda^n) \cong F[x]/(x-\lambda)^n$. Then applying T to each basis element we get

$$\begin{aligned} T(b_i) = x.b_i &= \overline{x(x-\lambda)}^{n-i}, \\ &= (x-\lambda)(x-\lambda)^{n-i} + \lambda(x-\lambda)^{n-i}, \\ &= (x-\lambda)^{n-i+1} + \lambda(x-\lambda)^{n-i}. \end{aligned}$$

Thus for $i = 1$, get $T(b_1) = \lambda b_1$, and for all greater i $T(b_i) = b_{i-1} + \lambda b_i$, as desired. □

2.6. **Some Concluding Topics.**

This section addresses a few ancilliary topics before continuing on to discuss the beginnings of multilinear algebra. We first discuss the Cayley Hamilton Theorem for modules over commutative rings. Let $A = (a_{ij}) \in M_n(R)$, for some commutative ring R. We have the usual definition of the determinant of A given by

$$\det A = \sum_{\sigma \in S_n} \left(\operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)} \right).$$

Forming the matrix $x \operatorname{Id} - A \in M_n(R[x])$, we then define the characteristic polynomial of A to be

$$c_A(x) = \det(x \operatorname{Id} - A) \in R[x].$$

We then claim $c_A(A) = 0$ in $M_n(R)$. In the case where $R \subseteq F$ for some field F, one can simply view A as a matrix over F, and apply the traditional Cayley-Hamilton Theorem. In general, not all rings are contained in some field, and there are proofs that work for any commutative ring. Alternatively, we may argue as follows. Let R_A be the subring generated by the entries of A. Then evidently $A \in M_n(R_A), \det A \in R_A, c_A(x) \in R_A[x], c_A(A) \in M_n(R_A)$. Let $x_{ij}, i, j = 1, \ldots, n$ be variables and consider the generic matrix

$$X := (x_{ij}) \in M_n(R_X),$$

where $R_X = \mathbb{Z}[x_{11}, \ldots, x_{nn}]$. $R_X \subseteq F := Q(x_{11}, \ldots, x_{nn}) = Q(R_X)$, and hence applying the Cayley Hamilton Theorem (Corolary 2.14) we see that $C_X(X) = 0$. Consider the ring homomorphism $\alpha : R_X \to \mathbb{Z}[a_1 1, \ldots, a_n n] = R_A$, given by the assignment $x_{ij} \mapsto a_{ij}$. This yields a ring a homomorphism $M_n(\alpha) : M_n(R_X) \to M_n(R_A)$ with $M_n(\alpha)(X) = A$. We also have the ring homomorphism $\alpha[x] : R_X[x] \to R_A[x]$ with

$$\alpha[x](c_X(x)) \mapsto c_A(x).$$

Finally, $M_n(\alpha)\left(c_X(X)\right) = 0$ and

$$M_n(\alpha)\left(c_X(X)\right) = \left(\alpha[x]\left(c_X(x)\right)\right)\left(M_n(\alpha)(X)\right) = c_A(A),$$

establishing the result.

We next talk about using the tensor product in a context known sometimes referred to as *extending* the base field. Given a field extensions F/K we have the usual functor

$$F \otimes_K \cdot : {}_K\mathbf{Mod} \to {}_F\mathbf{Mod}.$$

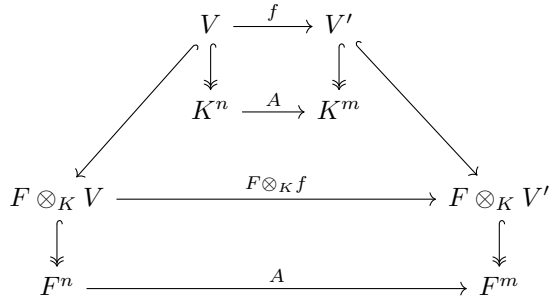
While this was covered in much more generality while discussing bimodules, in this case a more explicit description can be given. Let $V \in {}_K\mathbf{Mod}$ and fix an isomorphism $V \cong K^{(I)}$. Then we know

$$F \otimes_K V \cong (F \otimes_K K)^{(I)} \cong F^{(I)}.$$

Moreover the map $v \mapsto 1 \otimes v$, defines an embedding of K-vector spaces $V \hookrightarrow F \otimes_K V$ and any K-basis for V becomes an F-basis for $F \otimes_K V$ via the embedding.

Let $f : V \to V'$ be a map in ${}_K\mathbf{Mod}$. Via the functor discussed above, we also have the map $F \otimes_K f : F \otimes_K V \to F \otimes_K V'$. Assuming V, V' are finite dimensional of dimensions n, m respectively, the map f corresponds to a unique

matrix $A \in M_{m\times n}(K)$. Via our above discussion on the basis for $F \otimes_K V$ together with the diagram



we see that the matrix corresponding to $F \otimes_K f$ is simply A viewed in $M_{m\times n}(F)$. Thus altogether we see that in this case, the tensor product is a formal way to discuss extending the matrix A over K to a matrix over the larger field F.

Another important notion we have yet to discuss is that of similarity of matrices. Recall the equivalence of categories between $K[x]$ modules and K-vector spaces together with an endomoprhism $T : K \to K$. Moreover, two such $K[x]$ modules $V_T, V'_{T'}$ are isomorphic if and only if there exists an isomorphism of vector spaces $f : V \xrightarrow{\sim} V'$ such that

$$T = f^{-1} \circ T' \circ f.$$

In the special case where $V = V'$, the map f belongs to $\mathrm{GL}(V)$. Altogether $\mathrm{GL}(V)$ acts on $\mathrm{End}(V)$ by conjugation, that is

$$g.T = g \circ T \circ g^{-1}.$$

Two endomorphisms T, T' are said to be *similar* if they belong to the same orbit by the above action. Thus in the case of $K[x]$-modules, $V_T \cong V_{T'}$ if and only the matrices T, T' are similar.

Before moving onto part three of these notes we remark that the data in the structure theorems is uniquely determined by the module M.

Proposition 2.16. *Let $M \in {}_R\mathbf{Mod}$ be such that*

$$M \cong R^r \oplus \bigoplus_{i=1}^{t} R/(a_i) \cong R^s \oplus \bigoplus_{i=1}^{u} R/(b_i),$$

where $a_1|a_2|\dots|a_t, b_1|b_2|\dots b_u$. Then $r = s, t = u$ and up to reording $(a_i) = (b_i)$ for all i.

Proof. For brevity, let N denote the left sum above and N' the right sum. Let $F = Q(R)$ and consider the functor

$$F \otimes_R \cdot : {}_R\mathbf{Mod} \to {}_F\mathbf{Mod}.$$

Since tensoring commuters with direct sums, we see

$$F \otimes_R \left(R^r \oplus \bigoplus_{i=1}^{t} R/(a_i) \right) \cong F^r \oplus \bigoplus_{i=1}^{r} (F \otimes_R R/(a_i)) \cong F^r,$$

since $F \otimes_R R/(a_i) = F/F(a_i) = 0$. Thus we see $F^r \cong F^s$ from which we conclude $r = s$. With the tools of multilinear algebra, we will complete the remaining pieces of the proof in the next section. □

3. Multiliner Algebra

3.1. A Brief Review of Tensor Products.

Let R, S be rings and M be an (S, R)-bimodule. Previously we have discussed the functor

$$M \otimes_R \cdot : {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$$

which is right exact and commutes with direct sums. An important special case of bimodules arise as follows. Given a ring homomorphism $f : R \to S$, we obtain the natural bimodule ${}_SS_R$ where $s.r = sf(r)$. Recall for any ideal $I \trianglelefteq R$, for $S = R/I$ we have the canonical epimorhpism $R \twoheadrightarrow R/I$ and hence for any $V \in {}_R\mathbf{Mod}$,

$$R/I \otimes_R V \cong V/IV,$$

in ${}_{R/I}\mathbf{Mod}$ (or in ${}_R\mathbf{Mod}$ by inflation).

We now discuss another general property of the tensor product, namely associativity. Given bimodules ${}_SM_R$, ${}_RN_T$, and a module ${}_TV$ then we have the following isomorphism in ${}_S\mathbf{Mod}$

$$(M \otimes_R N) \otimes_T V \cong M \otimes_R (N \otimes_V T).$$

We spare the reader the proof of this property which can be on page 371 of *Dummit & Foote*.

While uniqueness of representation is always an issue when working with tensor products, in the case where one of the modules being tensored is free this is not an issue. Let $M_R \in \mathbf{Mod}_R$ be free with fixed basis $(m_i)_{i\in I}$ and $N \in {}_R\mathbf{Mod}$ be arbitrary. Then every element in $M \otimes_R N$ has the form

$$\sum_{i\in I} m_i \otimes n_i,$$

with each $n_i \in N$ unique. To justify this we have the chain of isomorphisms

$$M \otimes_R N \cong R^{(I)} \otimes_R N \cong (R \otimes_R N)^{(I)} \cong N^{(I)},$$

and tracking elements from right to left under these maps we get

$$(n_i)_{i\in I} \leftrightarrow (1 \otimes_R n_i)_{i\in I} \leftrightarrow \sum_{i\in I} e_i \otimes n_i \leftrightarrow m_i \otimes n_i.$$

From uniqueness of expression in $N^{(I)}$ we conclude uniqueness of expression of elements in $M \otimes_R N$ of the aforementioned form.

From now on, unless otherwise noted, R will be a commutative ring. Any $M \in {}_R\mathbf{Mod}$ can bew viewed as a right R-module (and so an (R, R)-bimodule) by defining the action

$$mr := rm.$$

One easilly checks this action satisfies the associative law for modules. We then write R-$\mathbf{Mod}$ for the category of (R, R) bimodules where the left and right action of R is precisely as defined above. With this in mind, the general theory of tensor products gives a bifunctor

$$\cdot \otimes_R \cdot : R\text{-}\mathbf{Mod} \times R\text{-}\mathbf{Mod} \to R\text{-}\mathbf{Mod},$$

with the usual properties (right-exactness in each argument etc.) Similarly if M, N are both free with $(m_i)_{i\in I}, (n_j)_{j\in J}$ respective bases we see that $M \otimes_R N$ is also free with basis $(m_i \otimes n_j)_{i,j\in I\times J}$. Thus

$$\operatorname{rank}(M \otimes_R N) = \operatorname{rank} M \operatorname{rank} N.$$

Given $M, N, L \in R$-**Mod** a map $\beta : M \times N \to L$ is called R-bilinear if the maps

$$\beta(\cdot, n) : M \to L,$$
$$\beta(m, \cdot) : N \to L$$

are R-linear maps for all $m \in M, n \in N$. In particular, β is R-balanced since

$$\beta(mr, n) = r\beta(m, n) = \beta(m, rn).$$

Thus the unversal property of the tensor product gives a group map $\widetilde{\beta} : M \otimes_R N \to L$ defined by

$$\widetilde{\beta}(m \otimes n) = \beta(m, n).$$

One easily checks that $\widetilde{\beta}$ is a map in R-**Mod** and the canonical map can. : $M \times N \to M \otimes_R N$ is a bilinear map. In this way we obtain bijections,

$$\mathrm{BiLin}(M \times N, L) \xrightarrow{\sim} \mathrm{Hom}_R(M \otimes_R N, L)$$
$$\beta \mapsto \widetilde{\beta}$$
$$\varphi \circ \text{can.} \hookleftarrow \varphi$$

Recall that earlier in these notes, we defined an R-algebra to be a a ring A equipped with a map $R \to Z(A)$. For example given a ring R, $M_n(R)$ is an R-algebra via the map $r \mapsto r\,\mathrm{Id}_n$. Also $R[x]$ is an algebra with the map $r \mapsto r$ where on the right r denotes the constant poylnomial $r \in R[x]$. In particular given two R-algebras A, B, they are both R-modules via the scalara map and hence $A \otimes_R B \in R$-**Mod**. Explicitly, we may consider the following scalar map $R \to A \otimes_R B$:

$$r \mapsto r(1 \otimes 1) = r \otimes 1 = 1 \otimes r = (1 \otimes 1)r.$$

Moreover there is a multiplication in $A \otimes_R B$ defined by

$$(a \otimes b)(a' \otimes b') = aa' \otimes bb'.$$

It is a straightforward computation using the universal property to see that this map is well-defined. Via this multiplication we see that $A \otimes_R B$ is in fact an R-algebra. As an example we claim

$$A \otimes_R R[x] \cong A[x].$$

To see this, consider the map $A \times R[x] \to A[x]$ given by $(a, f) \mapsto af$. This map is R-balanced and hence extends to a group map $A \otimes_R R[x] \to A[x]$. The action of A is preserved by this map and hence this is a map of A-modules. Multiplicativity of this map is easy to check and therefore this is a map of A-algebras. To see this map is bijective, note that as an A-module $A \otimes_R R[x]$ has basis $(1 \otimes x^i)$ which maps to the basis of $A[x]$ given by x^i.

In the following paragraph, we provide a short digression on a more modern definition of algebras. We say an R-algebra is an object $A \in R$-**Mod** together with two R-linear maps, $u : R \to A, m : A \otimes_R A \to A$, such that the following two diagrams commute

$$\begin{array}{ccc} A \otimes_R A \otimes_R A & \xrightarrow{m \otimes \mathrm{Id}_A} & A \otimes_R A \\ {\scriptstyle \mathrm{Id}_A \otimes m}\downarrow & & \downarrow{\scriptstyle m} \\ A \otimes_R A & \xrightarrow{\quad m \quad} & A \end{array} \qquad \begin{array}{ccccc} & & A \otimes_R A & & \\ & {\scriptstyle u \otimes \mathrm{Id}_A}\nearrow & & \nwarrow{\scriptstyle u \otimes \mathrm{Id}_A} & \\ R \otimes_R A & & \downarrow{\scriptstyle m} & & A \otimes_R R \\ & \searrow & & \swarrow & \\ & & A & & \end{array}$$

The diagram on the left is the associative law of the map m which is often referred to as multiplication. The diagram on the right stipulates that $u(1_R) := 1_A$ is an identity element in the algebra A. While this is certainly a more involved definition of an R-algebra, one use of this definition is the way it helps on define coalgebras. Coalgebras are also objects in R-**Mod** together with maps u, m going in the opposite direction of the maps defining an algebra such that the diagrams above, with all arrows reversed, also commute. Following this definition we define R-algebra homomorphisms to be R-linear maps $f : A \to B$, such that the following diagrams commute:

$$\begin{array}{ccc} A \otimes_R A & \xrightarrow{f\otimes f} & B \otimes_R B \\ {\scriptstyle m}\downarrow & & \downarrow{\scriptstyle m} \\ A & \xrightarrow{f} & B \end{array} \qquad \begin{array}{ccc} A & \xrightarrow{\quad f \quad} & B \\ & {\scriptstyle u}\nwarrow \quad \nearrow{\scriptstyle u} & \\ & R & \end{array}$$

The diagram on the left corresponds to multiplicativity of the map and the diagram on the right corresponds to the identity element mapping to identity element.

For concreteness, we work through determining the structure of the $\mathbb{R}$-algebra $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$. It is easilly seen to be a commutative 4-dimensional $\mathbb{R}$-algebra and since $\mathbb{C} = \mathbb{R}[x]/(x^2+1)$ we note

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}[x]/(x^2+1).$$

Since $\mathbb{C}$ is a free $\mathbb{R}$-module upon tensoring with $\mathbb{C}$, the exact sequence

$$0 \to (x^2+1) \to \mathbb{R}[x] \to \mathbb{R}[x]/(x^2+1) \to 0,$$

becomes the exact sequence

$$0 \to \mathbb{C} \otimes_{\mathbb{R}} (x^2+1) \to \mathbb{C}[x] \to \mathbb{C}[x]/\,\mathbb{C}[x] \otimes_{\mathbb{R}} (x^2+1) \to 0.$$

Hence viewing (x^2+1) as an ideal in $\mathbb{C}[x]$ we see that

$$\mathbb{C}[x]/\,\mathbb{C}[x] \otimes_{\mathbb{R}} (x^2+1) \cong \mathbb{C}[x]/(x^2+1) \cong \mathbb{C} \times \mathbb{C},$$

where we use the Chinese Remainder Theorem for the final isomorphism.

3.2. **Tensor, Symmetric, and Exterior Algebras.**

Given $V_1, \ldots, V_n \in R$-**Mod**, define inductively

$$V_1 \otimes_R \cdots \otimes_R V_n := (V_1 \otimes_R \cdots \otimes_R V_{n-1}) \otimes V_n,$$

recalling that a different bracketing would result in isomorphic results by associativity of the tensor product. We then have the canonical map can. : $V_1 \times \cdots \times V_n \to V_1 \otimes_R \cdots \otimes_R V_n$ defined by

$$(v_1, \ldots, v_n) \mapsto v_1 \otimes \cdots \otimes v_n := (v_1 \otimes \cdots \otimes v_{n-1}) \otimes v_n.$$

This map is *R-mulitlinear*: for each $i = 1, \ldots, n$ the map

$$\text{can.}(v_1, \ldots, v_{i-1}, \cdot, v_{i+1}, \ldots, v_n) : V_i \to V_1 \otimes_R \cdots \otimes_R V_n,$$

is R-linear for any choice of $v_j \in V_j$ for $j \neq i$. Our earlier observations about bilinearity together with induction yield a natural bijection for any $W \in R$-**Mod**.

$$\begin{aligned} \text{MultiLin}(V_1 \times \cdots \times V_n, W) &\xrightarrow{\sim} \text{Hom}_R(V_1 \otimes_R \cdots \otimes_R V_n, R) \\ \beta &\mapsto \widetilde{\beta} \\ \varphi \circ \text{can.} &\mapsfrom \varphi \end{aligned}$$

In the specific case where $V_1 = V_2 = \cdots = V_n := V$, we define

$$V^{\otimes n} = \begin{cases} R & n = 0 \\ V \otimes_R \cdots \otimes_R V & n > 0 \end{cases}.$$

From basic principles of the tensor product we have the two equations

$$V^{\otimes n} \otimes_R R \cong V^{\otimes n} \cong R \otimes_R V^{\otimes n},$$
$$V^{\otimes n} \otimes_R V^{\otimes m} = V^{\otimes (n+m)}.$$

For any given module $V \in R$-**Mod** we define the *tensor algebra* to be

$$T(V) := \bigoplus_{n \geq 0} V^{\otimes n} \in R\text{-}\mathbf{Mod},$$

together with the unit map $u : R \to V^{\otimes 0} \hookrightarrow T(V)$ and multiplication $m : T(V) \otimes_R T(V) \to T(V)$ which we define as follows. By linearity it suffices to define multlplication on $V^{\otimes n} \otimes_R V^{\otimes m} \cong V^{\otimes (n+m)}$ which we define by

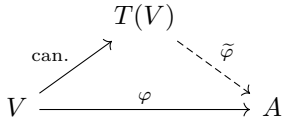
$$(v_1 \otimes \cdots \otimes v_n)(v_{n+1} \otimes \cdots \otimes v_{n+m}) = v_1 \otimes \cdots \otimes v_{n+m}.$$

It is then straightforward to check that these definitions satisfy the algebra axioms.

We now discuss the universal property of the tensor algebra. Trivially the map

$$V \xrightarrow{=} V^{\otimes 1} \hookrightarrow T(V)|_{R\text{-}\mathbf{Mod}},$$

is a map in R-**Mod**. Moreover given any map $\varphi : V \to A|_{R\text{-}\mathbf{Mod}}$ for some R-algebra A, there is a unique lift $\widetilde{\varphi}$ making the following diagram commute.



Explicitly, this map is given by $\widetilde{\varphi}(v_1 \otimes \ldots v_n) = \varphi(v_1) \ldots \varphi(v_n)$. In short given an algebraic $A \in R$-**Alg** and $V \in R$-**Mod**, there is a natural bijection

$$\mathrm{Hom}_R(V, A|_{R\text{-}\mathbf{Mod}}) \xrightarrow{\sim} \mathrm{Hom}_{R\text{-}\mathbf{Alg}}(T(V), A).$$

I.e. T and $\cdot|_{R\text{-}\mathbf{Mod}}$ are adjoint functors.

Earlier in these notes we developed the notion of a free group from a given set X. Given such a set we can similarly define the free algebra on X. Recall that given any set X the set

$$R^{(X)} = \{\text{all functions } f : X \to R \text{ with finite support}\},$$

is an R-module with basis $f_x(y) = \delta_{x,y}$. This basis is in bijection with X via $f_x \mapsto x$. Writing x instead of f_x, one obtains the module RX of formal R-linear combinations of X, the free module over R with basis X. We define the tensor algebra

$$T(RX) := R\langle X \rangle,$$

and refer to it as the *free R-algebra* generated by X. We have the functor $R\cdot : \mathbf{Sets} \to R$-**Mod** given by $X \mapsto RX$ and we easilly have the bijection

$$\mathrm{Hom}_{\mathbf{Sets}}(X, V|_{\mathbf{Sets}}) \xrightarrow{\sim} \mathrm{Hom}_R(RX, V),$$

for any $V \in R$-**Mod**. Thus given any $X \in \mathbf{Sets}, A \in R$-**Alg** via the above along with the universal property of the tensor algebra we see

$$\mathrm{Hom}_{\mathbf{Sets}}(X, V|_{\mathbf{Sets}}) \xrightarrow{\sim} \mathrm{Hom}_R(RX, V) \xrightarrow{\sim} \mathrm{Hom}_{R\text{-}\mathbf{Alg}}(R\langle X \rangle, A).$$

4. Some Outstanding Topics from Other Sources

4.1. **Nullstellensatz and an Introduction to Algebraic Geometry.** In this section we work towards proving Hilbert's Nullstellensatz which says that given a field extension F/k, if F is a finitely generated k-algebra then it is a finietely generated k-module. En route to proving this theorem we will also prove an important result known as the Noether Normalization lemma. Recall that an extension of rings B/A is said to be integral if any $b \in B$ is the root of a monic polynomial $f \in A[x]$.

Proposition 4.1.

a) If B is module finite over A, then B is integral over A.
b) Let $A \subseteq B \subseteq C$ be a tower of rings. If C is module finite over B and B is module finite over A, then C is module finite over A.
c) If $b \in B$ is integral over A, then $A[b]$ is module finite over A.

Proof. The proof of b is identical to the one used to show degrees of extensions multiply in towers. Thus we prove c and use this to prove a. Suppose $b \in B$ is integral over A, that is there exists, $a_0, \ldots, a_{n-1}$ such that

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0.$$

Hence $b^n = -a_{n-1}b^{n-1} - \cdots - a_0$, from which it follows that

$$A[b] = A + Ab + \cdots + Ab^{n-1}.$$

Assume B is generated by $b_1, \ldots, b_n$ as an A-module. For any $b \in B$, we have the multiplication by b maps $B \to B$ which is an A-module map, which if

$$bb_i = \sum_{j=1}^{n} a_{ij}b_j,$$

for $i = 1, \ldots, n$, has matrix representation (a_{ij}). Thus we have the equation,

$$b \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = (a_{ij}) \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}.$$

Upon multiplying by the adjoint of $bI_n - (a_{ij})$ we obtain that for all i,

$$\det(bI_n - (a_{ij}))b_i = 0.$$

Thus

$$\det(bI_n - (a_{ij}))b = 0,$$

for all $b \in B$ giving $\det(bI_n - (a_{ij})) = 0$. The determinant is a monic polynomial in b giving b is algebraic over A. □

We now state and prove the Noether Normalization Lemma for infinite fields, but remark that the result holds true for all fields.

Lemma 4.2 (Noether Normalization)**.** *Let k be an (infinite) field and A be a finite k-algebra, say $A = k[x_1, \ldots, x_n]/I$. Then there exists $y_1, \ldots, y_m \in A$ such that $n \leq m$, the y_i are algebraically independent and A is module finite over $k[y_1, \ldots, y_m]$.*

To prove this we require the following lemma.

Lemma 4.3. *Suppose $f \in k[x_1, \dots, x_n]$ is such that $\deg f = d \geq 1$. Then there exists a change of variable $x_i' = x_i - \alpha_i x_n$ for $i = 1, \dots, n-1$, such that*

$$f(x_1' + \alpha_i x_n, \dots, x_{n-1}' + \alpha_{n-1} x_n, x_n) \in k[x_1', \dots, x_{n-1}', x_n],$$

is a monic polynomial in x_n with coefficients in $k[x_1', \dots, x_{n-1}']$.

Proof. Break f into the sum of two polynomials, one of which is homogenous of degree d, $f = f_d + g$. Then,

$$\begin{aligned} f(x_1' + \alpha_1, \dots, x_{n-1} + \alpha_{n-1} x_n, x_n) &= f_d(x_1' + \alpha_1, \dots) + g(x_1' + \alpha_1, \dots), \\ &= f_d(\alpha_1, \dots, \alpha_{n-1}, 1) x_n^d + \text{lower degree terms.} \end{aligned}$$

Since k is infinite we may find α_i so that $f_d(\alpha_1, \dots, \alpha_{n-1}, 1) \neq 0$. □

We now proceed with the proof of Noether Normalization.

Proof of Lemma 4.2. Note that if $I = (0)$ then the result is trivial so we assume that $I \neq 0$ and proceed via induction on n. If $n = 1$, then $A = k[x_1]/I$ for some $I \neq 0$. For any $f \in I$, we obtain a surjection,

$$k[x_1]/(f) \twoheadrightarrow k[x_1]/I.$$

Since $k[x_1]/(f)$ is a finitely generated A-module, it follows that so too is A as the quotient of a finitely generated A module.

Now assume the result holds for $n-1$. Again take $f \in (I)$, and as in Lemma 4.3 perform a change of variables so that $f(x_1' + \alpha_1 x_n, \dots, x_n)$ is monic in x_n with coefficients in $k[x_1', \dots, x_{n-1}']$. Letting $a_1, \dots, a_{n-1}$ denote the class of $x_1', \dots, x_{n-1}'$ in A respectively, set $A' = k[a_1, \dots, a_{n-1}] \subseteq A$. Then f becomes monic in $A'[x_n]$ and we have a surjection,

$$A'[x_n]/(f) \twoheadrightarrow A'[x_n]/I = A,$$

giving A is module finite over A'. By assumption A' is module finite over some $k[y_1, \dots, y_m]$ and hence A is module fintie $k[y_1, \dots, y_m]$ completing the proof. □

Recall, without proof that if B/A is integral with B a field, then A is a field. We now prove Nullstellensatz using this fact.

Theorem 4.4. *Let F/k be a field extension such that F is of finite type over k. Then $[F : k] < \infty$.*

Proof. Via Noether Normalization, there exists $y_1, \dots, y_m \in F$ such that F is module finite over $k[y_1, \dots, y_m]$. Hence F is integral over $k[y_1, \dots, y_m]$ via Proposition 4.1 and via the remark this implies $k[y_1, \dots, y_m]$ is a field. This must imply $m = 0$ since the $y_1, \dots, y_m$ are algebraically independent over k. □