NOTES FOR ABSTRACT ALGEBRA

Based on lectures provided by Dima Arinkin on MATH 742 2025 SPRING

Author
Wells Guan

Contents

1 Rings and Ideals

1.1 Rings

Definiton 1.1.1. (Ring)

A ring R is an abelian group with an associative multiplication distributive over the addition. (We always assume a ring has a multiplicative identity and commutative if not marked)

A unit is an element u with a reciprocal $1/u$ such that $u \cdot 1/u = 1$, which is also denoted u^{-1} and called a numtiplicative inverse and the units form a multiplicative group, denoted $R^{\times}$.

Definiton 1.1.2. (Homomorphism)

A ring homomorphism is a ring map $\phi : R \to R'$ which preserving sums, products and 1. If $R' = R$ we call ϕ an endomorphism and if it is also bijective we call it an automorphism.

Definiton 1.1.3. (Subring)

A subset $R'' \subset R$ is a buting if R'' is a ring and the inclusion $R'' \hookleftarrow R$ is a ring map. We call R a extension of R'' and the inclusion an extension.

Definiton 1.1.4. (Algebra)

An R-algebra is a ring R' that comes equipped with a ring homomorphism $\phi : R \to R'$ called the structure map. An R-algebta homormorphism $R' \to R''$ is a ring homomorphism between R-algebtas compatible with structure maps.

Definiton 1.1.5. (Group action)

A group G is said to act on R if there is a homomorphism given from G into the group of automorphisms of R. The ring of invariants R^G is the subring defined by

$$R^G := \{x \in R | gx = g \text{ for all } g \in G\}$$

Definiton 1.1.6. (Boolean)

A ring B is called Boolean if $f^2 = f$ for all $f \in B$, then $2f = 0$ since

$$2f = (f + f)^2 = 4f$$

Definiton 1.1.7. (Polynomial rings)

Let R be a ring, $P := R[X_1, \cdots, X_n]$ the polynomial ring in n variables. P has the Universal Mapping Property (UMP), i.e. given a ring homomorphism $\phi : R \to R'$ and given an element x_i of R' for each i, there is a unique ring map $\pi : P \to R'$ with $\pi|_R = \phi$ and $\pi(X_i) = x_i$.

Similarly, let $X := \{X_\lambda\}_{\lambda \in \Lambda}$ be any set of variables. Set $P' := R[X]$ the elements of P' are the polynomials in any finitely many of X.

Definiton 1.1.8. (Ideals)

Let R be a ring. An ideal I is a subset containing 0 of R such that $xa \in I$ for any $x \in R, a \in I$ and closed under addition.

For a subset $S \subset R$, $\langle S \rangle$ means the smallest ideal containing S.

Given a single element a, we say that the ideal $\langle a \rangle$ is principal. For a number of ideals I_λ, the sum $\sum I_\lambda$ mean the set of all finite linear combinations $\sum x_\lambda a_\lambda$ for $x_\lambda \in R, a_\lambda \in I_\lambda$. If

Λ is finite, then the product $\prod I_\lambda$ means the ideal generated by all products $\prod a_\lambda, a_\lambda \in I_\lambda$.

For two ideals I and J, the transporter of J into I mean the set

$$(I : J) := \{x \in R | xJ \subset I\}$$

If $I \subset J$ a subsring such that $I \neq J$, then we call I proper.

For a ring homomorphism $\phi : R \to R'$, $I \subset R$ a subring, denote by IR' or I^e the ideal of R' generated by $\phi(I)$ can we call it the extension of I.

Given an ideal J of R' and its preimage $\phi^{-1}(J)$ is an ideal of R and we call ti the contraction of J denoted with J^c.

Definiton 1.1.9. (Residue Rings)

Let I be an ideal of R and the cosets of I

$$R/I := \{x + I | x \in R\}$$

have a ring structure and it will be called the residue ring or quotient ring or factor ring of R modulo I and the quotient map:

$$\kappa : R \to R/I, \quad \kappa(x) = x + I$$

and κx is called the residue of x.

Proposition 1.1.1.

For $I \subset R$ a subring and a ring homomorphism from R to R', then $\ker(\phi) \supset I$ implies that is a ring homomorphism $\psi : R/I \to R'$ with $\psi\kappa = \phi$.

ψ is surjective iff ϕ is surjective. ψ is injective iff $I = \ker(\phi)$.

Corollary 1.1.2. $R/\ker(\phi) \cong Im(\phi)$

Proposition 1.1.3.

R/I is universal among R-algebras R' such that $IR' = 0$, i.e. for $\phi : R \to R'$ such that $\phi(I) = 0$, there is a unique ring homomorphism $\psi : R/I \to R'$ such that $\psi\kappa = \phi$.

Definiton 1.1.10. The UMP serves to determine R/I up to unique isomorphism, i.e. if R' equipped with $\phi : R \to R'$ has the UMP too, then R' is isomorphic to R/I.

Proof.

If R' has the UMP among the R-algebras R'' such that $IR'' = 0$, then $\phi(I) = 0$ and hence there is a unique $\psi : R/I \to R'$ such that $\psi\kappa = \phi$ and since $\kappa I = 0$, we know there exists unique ψ' such that $\psi'\phi = \kappa$ and then $(\psi'\psi)\kappa = \kappa$ and hence $\psi'\psi = 1$ and we are done by the uniqueness.

Proposition 1.1.4. Let R be a ring, $P := R[X]$ the polynomial ring in one variable, $a \in R$ and $\pi : P \to R$ the R-algebra mao define by $\pi(X) := a$, then

- $\ker \pi = \{F(X) \in P | F(a) = 0\} = \langle X - a \rangle$
- $P/\langle X - a \rangle \cong R$

Definiton 1.1.11. (Order of a polynomial)

Let R be a ring, P the polynomial ring in variables X_λ for $\lambda \in \Lambda$ and $(x_\lambda) \in R^\Lambda$ a vector. Let $\phi_{(x_\lambda)} P \to P$ denote the R-algebra homomorphism defined by $\phi_{(x_\lambda)} X_\mu := X_\mu + x_\mu$.

The order of F at the vector (x_λ) is defined as the smallest degree of monomials M in $(\phi_{(x_\lambda)}F)$.

We know $\mathrm{ord}_{(x_\lambda)}F = 0$ iff $F(x_\lambda) \neq 0$.

Definiton 1.1.12. Let R be a ring, I an ideal and κ the quotient map. Given an ideal $J \supset I$ then the cosets

$$J/I := \{b + I | b \in J\} = \kappa(J)$$

and then J/I is an ideal of R/I and also $J/I = J(R/I)$.

Proposition 1.1.5. Given $J \supset I$ and we know

$$\phi : R \to R/I \to (R/I)/(J/I)$$

then we have the commutative diagram:

$$\begin{tikzcd} R \arrow[r] \arrow[d] & R/J \arrow[d, "\cong"] \\ R/I \arrow[r] & (R/I)/(J/I) \end{tikzcd}$$

Proof.

Since $\phi(J) = 0$, so there exists unique $\psi : R/J \to (R/I)/(J/I)$ such that $\psi\kappa_J = \phi$ and since $\kappa_J(I) = 0$ and there exists p such that $p\kappa_I = \kappa_J$ and consider $p(J/I) = 0$ and there exists h such that $h\kappa_{(J/I)} = p$ and it is easy to check $h\psi = 1$ by uniqueness and we are done.

Definiton 1.1.13. Let R be a ring. Let $e \in R$ be an idempotent, i.e. $e^2 = e$ then Re is a ring with e as multiplication unit, but Re is not a subring unless $e = 1$.

Let $e' := 1 - e$, then e' is idempotent and $ee' = 0$ and we call them complementary idempotents.

Denote $\mathrm{Idem}(R)$ the set of all idempotents, which is close under a ring homomorphism.

Proposition 1.1.6. If $e_1, e_2 \in R$ such that $e_1 + e_2 = 1$ and $e_1e_2 = 0$, then they are complementary idempotents.

Definiton 1.1.14. Let $R : R' \times R''$ be a product of two rings with componentwise operations.

Proposition 1.1.7. Let R be a ring and e', e'' complementary idempotents. Set $R' := Re'$ and $R'' = Re''$. Define $\phi : R \to R' \times R''$ by $\phi(x) = (xe', xe'')$ and then ϕ is a ring isomorphism. $R' = R/Re''$ and $R'' = R/Re'$.

Proof.

Check ϕ is surjective and injective.

There is a natrual isomorphism between $I = \{(0, xe'')\} \subset R' \times R''$ and R'', and consider the diagram

$$\begin{tikzcd} R \arrow[r, leftrightarrow] \arrow[d] & R' \times R'' \arrow[d] \\ R/R'' & R' \times R''/I \end{tikzcd}$$

and use the UMP.

1.2 Prime Ideals

Definiton 1.2.1. (Zerodivisors)

Let R be a ring. An element x iscalled a zerodivisor if there is a nonzero y such that $xy = 0$; otherwise, x is called a nonzerodivisor. Denote the set of zerodivisors by z.div(R) and the nonzerodivisors by S_0.

Definiton 1.2.2. (Multiplicative subsets, prime ideals)

Let R be a ring. A subset S is called multipliccative if $1 \in S$ and $x, y \in S$ implies $xy \in S$.

An ideal P is called prime if its complement $R - p$ is multiplicative, or equivalentely, if $1 \neq P$ and $xy \in P$ implies $x \in P$ or $y \in P$.

Definiton 1.2.3. (Fields,domains)

A ring is called a field if $1 \neq 0$ and if every nonzero element is a unit.

A ring is called an integral domain, or a domain if $\langle 0 \rangle$ or equivalently, if R is nonzero and has no nonzero zerodivisors.

Every domain R is a subring of its fraction field $\mathrm{Frac}(R) := \{x/y, x, y \in R \text{ and } y \neq 0\}$.

Proposition 1.2.1. Any subring R of a field K is a domain, and for a domain R, Frac(R) has the UMP: the inclusion of R into any field L extends uniquely to an inclusion of Frac(R) into L.

Proof.

For any subring R of a field, $a, b \in R$, if $ab = 0$, and a nonzero, then $b = 0$ and we are done.

If $\phi : R \hookrightarrow L$, then $\phi(x/y) = \phi(x)\phi(y)^{-1}$ is well-defined and obviously a ring homomorphism and we are done.

Definiton 1.2.4. (Polynomials over a domain)

Let R be a domain, X a set of variable. $P := R[X]$ and then P is a domain, and Frac(P) is called the rational functions.

Definiton 1.2.5. (Unique factorization)

Let R be a domain, p a nonzero nonunit. We call p prime if $p|xy$ implies $p|x$ or $p|y$, which is equivalent with $\langle p \rangle$ is prime.

For $x, y \in R$, we call $d \in R$ their gcd if $d|x$ and $d|y$ and if $c|x, c|y$ then $c|d$.

p is irreducible if $p = yz$ implies y or z is a unit. We call R is a UFG if every nonzero nonunit factors into a product of irreducibles and the facrtotization is unique to order and units.

Proposition 1.2.2. If every nonzero nonunit factors have a factorization of a product of irreducible elements, then the factorization is unique up to order and units iff every irreducible element is prime.

Proof.

Lemma 1.2.3. Let $\phi : R \to R'$ be a ring homomorphism, and $T \subset R'$ a subset. If T is multiplicative, then $\phi^{-1}T$ is multiplicative; the converse holds if ϕ is surjective.

Proof.

Proposition 1.2.4. Let $\phi : R \to R'$ be a ring map, and $J \subset R'$ an ideal. Set $I := \phi^{-1}J$. If J is prime, then I is prime; the converse holds if ϕ is surjective.

Corollary 1.2.5. Let R be a ring, I an ideal. Then I is prime iff R/I is a domain.

Proof.

Consider

$$\kappa : R \to R/I$$

the quotient map and I prime implies $\langle 0 \rangle$ is prime in R/I and hence R/I is a domain.

Definiton 1.2.6. (Maximal ideal)

Let R be a ring. An ideal I is sai to be maximal if I is proper and there is no proper ideal J such that $I \subset J, I \neq J$.

Proposition 1.2.6. A ring R is a field iff $\langle 0 \rangle$ is a maximal ideal.

Corollary 1.2.7. Let R be a ring, I an ideal. Then I is maximal iff R/I is a field.

Proof.

Only need to check $\langle 0 \rangle$ is maximal in R/I.

Corollary 1.2.8. In a ring, every maximal ideal is prime.

Definiton 1.2.7. (Coprime)

Let R be a ring, and $x, y \in R$. We say x and y are coprime if their ideals $\langle x \rangle$ and $\langle y$ are comaximal.

x and y are coprime if and only if there are $a, b \in R$ such that $ax + by = 1$.

Definiton 1.2.8. A domain R is called a Principal Ideal Domain if every ideal is principal. A PID is a UFD.

Theorem 1.2.9. Let R be a PID. Let $P := R[X]$ be the polynomial ring in one variable X, and I a nonzero prime ideal of P. Then $P = \langle F \rangle$ with F prime, or P is maximal. Assume P is maximal. Then either $P = \langle F \rangle$ with F prime, or $P = \langle p, G \rangle$ with $p \in R$ prime, $pR = P \cap R$ and $G \in P$ prime with iamge $G' \in (R/pR)[X]$ prime.

Theorem 1.2.10. Every proper ideal I is contained in some maximal ideal.

Corollary 1.2.11. Let R be a ring, $x \in R$. Then x is a unit iff x belongs to non maximal ideal.

1.3 Radicals

Definiton 1.3.1. (Radical)

Let R be a ring. Its radical $\mathrm{rad}(R)$ is defined to be the intersection of all its maximal ideals.

Proposition 1.3.1. Let R be a ring, I an ideal, $x \in R$ and $u \in R^\times$. Then $x \in \mathrm{rad}(R)$ iff $u - xy \in R^\times$ for all $y \in R$. In particular, the sum of an element of $\mathrm{rad}(R)$ and a unit is a unit, and $I \subset \mathrm{rad}(R)$ if $1 - I \subset R^\times$.

Proof.

For a maximal ideal J, if $u - xy \in J$, then $u \in J$ which is a contradiction and hence $u - xy$ is a unit. Conversely, if there exists J maximal such that $x \in J$, then $\langle x \rangle + J = R$ and hence there exists $m \in J$ such that $u - xy = m$ for some unit u, which is a contradiction.

Corollary 1.3.2. Let R be a ring, I an ideal, $\kappa : R \to R/I$ the quotient map. Assume $I \subset \mathrm{rad}(R)$, then κ is injective on $\mathrm{Idem}(R)$.

Proof.

For $e, e' \in \mathrm{Idem}(R)$ and $x = e - e'$, if $\kappa(x) = 0$, then $x^3 = x$ and hence $x(1 - x^2) = 0$, so $1 - x^2$ is a unit and hence x is 0 and we are done.

Definiton 1.3.2. (Local ring)

A ring is called local if it has exactly one maximal ideal, and semilocal if it has at least one and at most finitely many.

By the residue field of a local ring A, we mean the field A/M where M is the maximal ideal of A.

Lemma 1.3.3. Let A be a ring, N the set of nonunits. Then A is local iff N is an ideal, if so, then N is the maximal idal.

Proof.

Only need to check the sufficiency, if A is local, then we know M is contained in N, and if there is $y \in M - N$, then $\langle y \rangle$ is a proper ideal and hence $y \in N$, which is a contradiction and hence $M = N$ and we are done.

Proposition 1.3.4. Let R be a ring, S a multiplicative subset, and I an ideal with $I \cap S = \emptyset$. Set $\mathcal{S} := \{J, J \supset I, J \cap S = \emptyset\}$, then $\mathcal{S}$ has a maximal element P and every such P is prime.

Proof.

By Zorn's lemma, their is a maximal element P in S, for $x, y \in R - P$, there exists $p, q \in P, a, b \in R$ such that $p + ax \in S, q + by \in S$ and hence $pq + pby + qax + abxy \in S$, and hence $xy \notin P$ and we are done.

Definiton 1.3.3. (Saturated multiplicative subsets)

Let R be a ring, and S a multiplicative subset. We say S is saturated if for $x, y \in R, xy \in S$, then $x, y \in S$.

Lemma 1.3.5. Let R be a ring, I a subset of R that is stable under addition and multiplication, and $P_1, \cdots, P_n$ ideals such that $P_3, \cdots, P_n$ are prime. If I is not contained in P_j for all j, then there is an $x \in I$ such that $x \in P_j$ for j or equivalently, if $I \subset \bigcup_{i=1}^n P_i$, then $I \subset I_i$ for some i.

Proof.

If $n = 1$ then we are done. We may use the induction, assume that $n \geq 2$, then by induction, for each i, there is $x_i \in I$ such that x_i is not in $P_j, i \neq j$ and $x_i \in P_i$, so then $x_1 + x_2 \notin P_2$ if $n = 2$. For other n, we will know $(x_1 \cdots, x_{n-1}) \notin P_j$ for all j.

Definiton 1.3.4. Let R be a ring, S a subset, its radical $\sqrt{S}$ is the set

$$\sqrt{S} := \{x \in R | x^n \in S \text{ for some } n\}$$

If I is an ideal and $I = \sqrt{I}$, then call I to be radical.

We call $\sqrt{0}$ is the nilradical and denoted as $\mathrm{nil}(R)$. We call $x \in R$ nilpotent if $x \in \mathrm{nil}(0)$, we call an ideal I nilpotent if $a^n = 0$ for some $n \geq 1$.

Theorem 1.3.6. Let R be a ring, I an ideal, then

$$\sqrt{I} = \cap_{P \supset I, P \text{ prime}} P$$

Proof.

For $x \notin \sqrt{I}$, let S contains all the expotents of x and S is multiplicative, then $I \cap S = \emptyset$ and then there is an P prime containing I with not containing x and hence $\sqrt{a}$ contains the union.

Converse direction is easy.

Proposition 1.3.7. Let R be a ring, I an ideal. Then $\sqrt{I}$ is an ideal.

Definiton 1.3.5. (Minimal primes)

Let R be a ring, I an ideal and P prime. We call P a minimal prime of I if P is minimal in the set of primes containing I, we all P a minimal prime of R if P is a minimal prime of $\langle 0 \rangle$.

Proposition 1.3.8. A ring R is reduced, i.e. 0 is the only nilpotent, and has only one minial prime iff R is a domain.

Proof.

Converse direction is obvious. If 0 is the only nilpotent elements, Q is a minimal prime ideal, then $Q = 0$ since 0 is the intersection of all the minimal primes, and we are done.

1.4 Modules

Definiton 1.4.1. (Modules)

Let R be a ring. An R-module M is an abelian group with a scalar multiplication $R \times M \to M$ which is

- $x(m + n) = xm + xn$ and $(x + y)m = xm + ym$
- $x(ym) = (xy)m$
- $1m = m$

A submodule N of M closed under scalar multiplication.

Given $m \in M$, its annihilator

$$\mathrm{Ann}(m) := \{x \in R | xm = 0\}$$

and the annilhilator of M is

$$\mathrm{Ann}(M) := \{x \in R | xm = 0 \text{ for all } m \in M\}$$

We call the intersection of all maximal ideals containing $Ann(M)$ the radical of M, denoted as $\mathrm{rad}(M)$.

Proposition 1.4.1. There is a bijection between the maximal ideals containing $\mathrm{Ann}(M)$ and the maximal ideals of $R/\mathrm{Ann}(M)$, and hence

$$\mathrm{rad}(R/\mathrm{Ann}(M)) = \mathrm{rad}(M)/\mathrm{Ann}(M)$$

Proposition 1.4.2. Given a submodule N of M, and then $\mathrm{Ann}(M) \subset \mathrm{Ann}(N)$ and we also have $\mathrm{Ann}(M) \subset \mathrm{Ann}(M/N)$.

Definiton 1.4.2. (Semilocal)

We call M semilocal if there are only finitely many maximal ideals containing $\mathrm{Ann}(M)$. If R is semilocal, so is M and we will know M is semilocal iff $R/\mathrm{Ann}(M)$ is a semilocal ring.

Definiton 1.4.3. (Polynomials)

The sets of polynomials

$$M[X] := \{\sum_{i=0}^{n} m_i M_i, M_i \text{ monomials}\}$$

and then $M[X]$ is an $R[X]-module$.

Definiton 1.4.4. (Homomorphisms)

Let R be aring, M and N modules. A R-linear map is a map $\alpha : M \to N$ such that

$$\alpha(xm + yn) = x\alpha m + y\alpha n$$

Let $\iota : \ker\alpha \to M$ be the inclusion and then $\ker\alpha$ has the UMP: $\alpha\iota = 0$ and for a homomorphism $\beta : K \to M$ with $\alpha\beta = 0$, there is a unique homomorphism $\gamma : K \to \ker\alpha$ with $\iota\gamma = \gamma$ as shown below

$$\begin{tikzcd}
\ker\alpha \arrow[r, "\iota"] & M \arrow[r, "\alpha"] & N \\
& K \arrow[ul, "\gamma"] \arrow[u, "\beta"] \arrow[ur, "0"'] &
\end{tikzcd}$$

Definiton 1.4.5. (Endomorphism)

An endomorphism of M a self-homomorphism denoted as $\mathrm{End}_R(M) \subset \mathrm{End}_{\mathbb{Z}}(M)$.

For $x \in R$, let μ_x the self map of multiplication by x and then $x \mapsto \mu_x$ denoted as

$$\mu_R : R \to \mathrm{End}_R(M)$$

and note that $\ker\mu_R = \mathrm{Ann}(M)$. We call M faithful if μ_R is injective.

Definiton 1.4.6. For two rings R and R', suppose R' is an R-algebra and M' an R'-module, then M' is also an R-module by $xm := \phi(x)m$.

A subalgebra R'' of R' is a subring such that the structure map owning image in R''. The subalgebra generated by $x_\lambda \in R'$ for $\lambda \in \Lambda$ is the smallest R-subalgebra containing x_λ and we denote it by $R[\{x_\lambda\}]$ and we call x_λ the generators.

We say R' is a finitely generated R-algebra if there exists $x_i, 1 \leq i \leq n$ such that $R' = R[x_1, \cdots, x_n]$.

Definiton 1.4.7. (Residue modules)

Let R be a ring, Ma module and $M' \subset M$ a submodule. Then

$$M/M' := \{m + M' | m \in M\}$$

which is the residue module or M modulo M', form the quotien map

$$\kappa : M \to M/M', \quad m \mapsto m + M'$$

Definiton 1.4.8. (Cyclic Modules)

Let R be a ring. A module M is said to be cyclic if there exists $m \in M$ such that $m = Rm$, then $\alpha : x \mapsto xm$ induces an isomorphism $R/\mathrm{Ann}(m) \cong M$.

Definiton 1.4.9. (Noether Isomorphisms)

Let R be a ring, N a module, and L and M submodules.

Assume $L \subset M$, and

$$\alpha : N \to N/L \to (N/L)/(M/L)$$

and we may know $\ker \alpha = M$. then α factors through the isomorphism β in $N \to N/M \to (N/L)/(M/L)$ since α is surjective and $\ker \alpha = M$, so

$$\begin{tikzcd}
N \arrow[r] \arrow[d] & N/M \arrow[d, "\beta"] \\
N/L \arrow[r] & (N/L)/(M/L)
\end{tikzcd}$$

Assume L not in M and

$$L + M := \{l + m, l \in L, m \in M\}$$

and it will be a submodule, then similarly

$$\begin{tikzcd}
L \arrow[r] \arrow[d] & L/(L \cap M) \arrow[d, "\beta"] \\
L + M \arrow[r] & (L+M)/M
\end{tikzcd}$$

Definiton 1.4.10. (Cokernels, coimages)

Let R be a ring, $\alpha : M \to N$ linear. Associated to α there are its cokernel and its coimage

$$\mathrm{Coker}(\alpha) := N/\mathrm{Im}(\alpha) \quad \mathrm{Coim}(\alpha) := M/\ker \alpha$$

Definiton 1.4.11. (Generators, free modules)

Let R be a ring, M a module. Given some submodules N_λ, by the sum $\sum N_\lambda$, we mean the set of all finite linear combinations $\sum x_\lambda m_\lambda, m_\lambda \in N_\lambda$.

Elements m_λ are said to be free of linearly independent if the linear combination equals to zero implies zero coefficients. If m_λ are said to be form a (free) basis of M, then they are free and generate M and we say M is free on m_λ.

We say M is finitely generated if it has a finite set of generators and M is free if it has a free basis.

Theorem 1.4.3. Let R be a PID, E a free module with e_λ a basis, and F a submodule, then F is free and has a basis indexed by a subset of λ.

Definiton 1.4.12. Let R be a ring, Λ a set, M_λ a module for $\lambda \in \Lambda$. The direct product of M_λ is the set of any vectors

$$\prod M_\lambda := \{(m_{m_\lambda})\}$$

which is a module under componentwise addition and scalar multiplication.

The direct sum of M_λ is the subset of restricted vectors:

$$\bigoplus M_\lambda := \{(m_\lambda), m_\lambda \text{ nonzero for only finite elements}\}$$

Proposition 1.4.4. $\prod M_\lambda$ has the UMP, for R-homomorphism $\alpha_\kappa : L \to M_\kappa$, there is a unique R-homomorphism $L \to \prod M_\lambda$ such that $\pi_\kappa \alpha = \alpha_\kappa$, in other words, π_λ induce a bijection of

$$\mathrm{Hom}(L, \prod M_\lambda) \cong \prod \mathrm{Hom}(L, M_\lambda)$$

Similarly, the direct sum comes equipped with injections

$$\iota_\kappa \to \bigoplus M_\lambda$$

and it has the UMP: given $\beta_\kappa : M_\kappa \to N$, there is a unique R-homomorphism $\beta : \bigoplus M_\lambda \to N$ such that $\beta \iota_\kappa = \beta_\kappa$ and ι_κ induce the bijection:

$$\mathrm{Hom}(\bigoplus, N) \to \bigoplus \mathrm{Hom}(M_{\lambda,N})$$

1.5 Exact Sequences

Definiton 1.5.1. (Exact)

A sequence of module homomorphisms

$$\cdots \to M_{k-1} \overset{\alpha_{k-1}}{\to} M_k \overset{\alpha_k}{\to} M_{k+1} \to \cdots$$

is said to be exact at M_k if $\ker \alpha_k = \mathrm{Im}(\alpha_k)$. The sequence is said to be exact if it is exact at every M_k, except an initial source of final target.

Definiton 1.5.2. (Short exact sequences)

A sequence $0 \to L \overset{\alpha}{\to} M \overset{\beta}{\to} N \to 0$ is exact if and only if α is injective and $N \cong \mathrm{Coker}\alpha$ or dually if and only if β is surjective and $L = \ker \beta$. Then the sequence is called short exact and we often regard L as a submodule of M and N the quotient M/L.

Proof.

Proposition 1.5.1. For $\lambda \in \Lambda$, let $M'_\lambda \to M_\lambda \to M''_\lambda$ be sequence of module homomorphisms. If every sequence is exact, then so are the two induced sequences

$$\bigoplus M'_\lambda \to \bigoplus M_\lambda \to \bigoplus M''_\lambda, \quad \prod M'_\lambda \to \prod M_\lambda \to \prod M''_\lambda$$

Conversely, if either induced sequence is exact then so is every original one.

Proof.

Proposition 1.5.2. Let $0 \to M' \overset{\alpha}{\to} M \overset{\beta}{\to} M'' \to 0$ be a short exact sequence, and $N \subset M$ a submodule. Set $N' := \alpha^{-1}(N)$ and $N'' := \beta(N)$. Then the induced sequence $0 \to N' \to N \to N'' \to 0$ is short exact.

Definiton 1.5.3. (Retraction, section, splits)

A linear map $\rho : M \to M'$ is a retraction of another $\alpha : M' \to M$ if $\rho\alpha = 1_{M'}$, then α is injective and ρ is surjective.

Dually, we call $\sigma : M'' \to M$ a section of another $\beta : M \to M''$ if $\beta\sigma = 1_{M''}$, then β is surjective and σ is injective.

We call a 3-term exact sequence $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$ splits if there is an isomorphism $\phi : M \cong M' \oplus M''$ with $\phi\alpha = \iota_{M'}$ and $\beta = \pi_{M''}\phi$.

Proposition 1.5.3. Let $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$ be a 3-term exact sequence. Then the following conditions are equivalent

- The sequence splits
- There exists a retraction $\rho : M \to M'$ of α and β is surjective.
- There exists a section $\sigma : M'' \to M$ of β and α is injective

Proof.

Assume the sequence is splits, then we have the commuting diagram

$$\begin{tikzcd}
M' \arrow[r, "\alpha"] \arrow[dr, "\iota_{M'}"'] & M \arrow[r, "\beta"] \arrow[d, "\phi(\cong)"] & M'' \\
& M' \oplus M'' \arrow[ur, "\pi_{M''}"'] &
\end{tikzcd}$$

then let $\rho = \pi_{M'}\phi$, then $\rho\alpha = \pi_{M'}\phi\phi^{-1}\iota_{M'} = 1_{M'}$. Let $\sigma = \phi^{-1}\iota_{M''}$ and then $\beta\sigma = \pi_{M''}\phi\phi^{-1}\iota_{M''} = 1_{M''}$ and then β is surjective and α is injective.

Now assume there is such a retraction ρ and β is surjective, then define $\sigma = 1_M - \alpha\rho$ and $\phi : M \to M' \oplus M''$ by $m \mapsto (\rho(m), \beta\sigma(m))$., if $\phi(m) = 0$, then $\rho(m) = 0$ and $\sigma(m) = m$, which means $\beta(m) = 0$. There exists $a \in M'$ such that $m = \alpha(a)$ and hence $a = 0$ which means $m = 0$, so $\ker\phi = 0$. For $(a, b) \in M' \oplus M''$, assume $\beta(m) = b$, then $\phi(\alpha(a)+\sigma(m)) = (a+\rho(m-\alpha\rho(m)), \beta(\alpha(a))+\beta(\sigma(m))) = (a, b)$ and hence ϕ is surjective. And $\phi\alpha(a) = (a, \beta\sigma\alpha(a)) = (a, 0)$ and $\pi_{M''}\phi(m) = \beta(\sigma(m)) = \beta(m)$ and we are done.

Lemma 1.5.4. Consider this commutative diagram with exact rows:

$$\begin{tikzcd}
& M' \arrow[r, "\alpha"] \arrow[d, "\gamma'"] & M \arrow[r, "\beta"] \arrow[d, "\gamma"] & M'' \arrow[r] \arrow[d, "\gamma''"] & 0 \\
0 \arrow[r] & N' \arrow[r, "\alpha'"] & N \arrow[r, "\beta'"] & N'' &
\end{tikzcd}$$

It yields the following exact sequence:

$$\ker\gamma' \xrightarrow{\varphi} \ker\gamma \xrightarrow{\psi} \ker\gamma'' \xrightarrow{\partial} \mathrm{coker}\gamma' \xrightarrow{\varphi'} \mathrm{coker}\gamma \xrightarrow{\psi'} \mathrm{coker}\gamma''$$

Moreover, if α is injective, then so is φ; dually, if β' is surjective, then so is ψ'.

Proof.

Notice $\alpha'\gamma' = \gamma\alpha, \beta'\gamma = \gamma''\beta$ and let $\varphi = \alpha|_{\ker\gamma'}, \psi = \beta|_{\ker\gamma}$ and we know $\varphi(\ker\gamma') \subset \ker\gamma, \psi(\ker\gamma) \subset \ker\gamma''$. Obviously, $\mathrm{Im}(\varphi) \subset \ker\psi$ and for any $b \in \ker\psi$, it is in $\ker\gamma \cap \mathrm{Im}\alpha$, since α' is injective and hence its preimage has to be contained in $\ker\gamma'$ and hence it is in $\mathrm{Im}(\varphi)$.

α', β' will induce natural φ', ψ' on $\mathrm{coker}\gamma', \mathrm{coker}\gamma$ by defining $n' + \mathrm{Im}\gamma' \mapsto \alpha'(n') + \mathrm{Im}\gamma, n + \mathrm{Im}\gamma \mapsto \beta'(n) + \mathrm{Im}\gamma''$, which is well-defined since $\alpha'(\mathrm{Im}\gamma') \subset \mathrm{Im}\gamma, \beta'(\mathrm{Im}\gamma) \subset \mathrm{Im}\gamma''$ and the exactness is similarly checked.

Define ∂ by the following, if $\gamma'' m'' = 0$, consider m is one of preimage of m'' and let a to be the preimage of $\gamma(m)$, then let $\partial m'' = a + \mathrm{Im}\gamma'$. It is well-defined since if $\beta m = \beta n = m''$, then $m - n \in \ker \beta$, which means the preiamges of $\gamma m, \gamma n$ are in the same coset. For $m \in \ker \gamma$, $\partial(\psi(m)) = \alpha'^{-1}\gamma(m) + \mathrm{Im}\gamma' = 0$ and if $\partial(m'') = 0$, then assume $\beta m = m''$ and we know $\alpha^{-1}\gamma(m) \in \mathrm{Im}\gamma'$ and hence there exists $x \in M'$ such that $\gamma \alpha x = \gamma m$ and we know $\beta(m - \alpha(x)) = m''$ and $\gamma(m - \alpha x) = 0$, which means $\ker \partial = \mathrm{Im}\psi$. If $a = \alpha'^{-1}(\gamma(m))$ with $m'' = \beta m \in \ker \gamma''$, then $\varphi'(a + \mathrm{Im}(\gamma')) = \alpha' a + \mathrm{Im}\gamma = 0$ and if $\varphi'(a + \mathrm{Im}(\gamma')) = 0$, then there exists m such that $\alpha'(a) = \gamma m$ and then $\partial(\beta(m)) = a + \mathrm{Im}\gamma'$ and we are done.

Theorem 1.5.5. (Left exactness of Hom)

- Let $M' \to M \to M'' \to 0$ be a sequence of linear maps. Then it is exact iff for all modules N, the following induced sequence is exact

$$0 \to \hom(M'', N) \to \hom(M, N) \to \hom(M', N)$$

- Let $0 \to N' \to N \to N''$ be as sequence of linear maps. Then it is exact iff for all modules M, the following induced sequence is exact.

$$0 \to \hom(M, N') \to \hom(M, N) \to \hom(M, N'')$$

Proof.

Assume $M' \xrightarrow{\phi} M \xrightarrow{\psi} M''$ and then the induced map will be $\tilde{\psi} : f \mapsto f \circ \psi$ and $\tilde{\phi} : g \mapsto g \circ \phi$. If ψ is surjective, then $\tilde{\psi}$ will be an injective since $f \circ \psi = 0$ implies $f = 0$, and if $g \circ \phi = 0$, then $\ker \psi = \mathrm{Im}\phi \subset \ker g$ and hence there will be $g' : M'' \cong M/\ker \psi \to N$ such that $g'\psi = g$ by the UMP and we are done. We know for $g : M \to N, g \circ \phi = 0$, equivalently $\mathrm{Im}\phi \subset \ker g$ iff there exists unique $g' : M'' \to N$ such that $g' \circ \psi = g$, which means $M'' \cong \mathrm{coker}\phi$ and the diagram

$$\begin{tikzcd}
M' \arrow[r, "\phi"] & M \arrow[r, "\psi"] \arrow[dr, "\kappa"] & M'' \arrow[r] \arrow[d, leftrightarrow] & 0 \\
 & & \mathrm{coker}\phi \arrow[ur] &
\end{tikzcd}$$

commutes and we are done.

Similarly assume that $N' \xrightarrow{\phi} N \xrightarrow{\psi} N''$, then $\tilde{\phi} : f \mapsto \phi \circ f$ and $\tilde{\psi} : g \mapsto \psi \circ g$, which means $\ker \psi = N' \hookrightarrow N$. It is easy to check $\ker \tilde{\phi} = 0$ and $\mathrm{Im}\tilde{\phi} \subset \ker \tilde{\psi}$. For $g \in \ker \tilde{\psi}$, since $\mathrm{Im}g \subset \ker \psi = \mathrm{Im}\phi$, then let $g' = g|_N$ will satisfy that $\phi \circ g' = g$. For the converse direction, we know for any $g : M \to N$, $\mathrm{Im}g \subset \ker \psi$ iff there exists a unique $g' : M \to N'$ such that

$\phi \circ g' = g$, then we may, which is

$$\begin{tikzcd} 0 \arrow[r] \arrow[dr] & N' \arrow[r, "\phi"] & N \arrow[r, "\psi"] & N'' \\ & \ker\psi \arrow[ur, hook] & & \end{tikzcd}$$

Definiton 1.5.4. (Presentation)

A (free) presentation of a module M is an exact sequence

$$G \to F \to M \to 0$$

with G and F free. If G and F are free of finite rank, then the presentation is called finite. If M has a finite presentation, then call M finitely presented.

Proposition 1.5.6. Let R be a ring, M a module, m_λ generators. Then there is an exact sequence $0 \to K \to R^{\oplus\Lambda} \overset{\alpha}{\to} M \to 0$ with $\alpha e_\lambda = m_\lambda$ where e_λ the standard basis and there is a presentation.

Remark.

Choose $K = \ker\alpha$ and $k_\sigma, \sigma \in \Sigma$ to be generators of K, then

$$R^{\oplus\Sigma} \to R^{\oplus\Lambda} \to M \to 0$$

is a presentation.

Definiton 1.5.5. (Projective Module)

A module P is called projective if given any surjective linear map $\beta : M \to N$, every linear map $\alpha : P \to N$ lifts to one $\gamma : P \to M$, i.e. $\alpha = \beta\gamma$.

Theorem 1.5.7. The following conditions on an R-module P are equivalent

- The module P is projective
- Every short exact sequence $0 \to K \to M \to P \to 0$ splits
- There is a module K such that $K \oplus P$ is free
- Every exact sequence $N' \to N \to N''$ induces an exact sequence

$$\hom(P, N) \to \hom(P, N) \to \hom(P, N'')$$

- Every surjective homomophism $\beta : M \to N$ induces a surjection

$$\hom(P, \beta) : \hom(P, M) \to \hom(P, N)$$

Proof.

By considering the $P \cong M/\ker\phi$ it will induce a section of $\psi : M \to P$ and obviously $\phi : K \to M$ is injective and we are done for (1) implies (2). Use proposition 1.5.6. and we will know there exists K such that $K \oplus P \cong R^{\oplus\Lambda}$ which is free, which is for (2) implies (3).

Assume (3), then there exists Λ such that $K \oplus P \cong R^{\oplus\Lambda}$. Also notice that we will have

$$\prod N'_\lambda \to \prod N_\lambda \to \prod N''_\lambda$$

is exact, which implies that

$$\hom(R^{\oplus\Lambda}, N') \to \hom(R^{\oplus\Lambda}, N) \to \hom(R^{\oplus\Lambda}, N'')$$

is exact since $\hom(R^{\oplus\Lambda}, N) \cong \prod N_\lambda$ and hence

$$\hom(K \oplus P, N') \to \hom(K \oplus P, N) \to \hom(K \oplus P, N'')$$

which implies

$$\hom(K, N') \oplus \hom(P, N') \to \hom(K, N) \oplus \hom(P, N) \to \hom(K, N'') \oplus \hom(P, N'')$$

by isomorphism and hence the conclusion goes.

Assume (4), we know $M \to N \to 0$ is exact and we are done.

Assume (5), which is exactly the definition of projective module.

Lemma 1.5.8. (Schanuel)

Any two short exact sequences

$$0 \to L \overset{i}{\to} P \overset{\alpha}{\to} M \to 0, \quad 0 \to L' \overset{i'}{\to} P' \overset{\alpha'}{\to} M \to 0$$

with P and P' projective are essentially isomorphic; i.e. there is the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & L \oplus P' \arrow[r, "i\oplus 1_{P'}"] \arrow[d, "\cong\ \beta"] & P \oplus P' \arrow[r, "\alpha\oplus 0"] \arrow[d, "\cong\ \gamma"] & M \arrow[r] \arrow[d, "="] & 0 \\
0 \arrow[r] & P \oplus L' \arrow[r, "1_P\oplus i'"] & P \oplus P' \arrow[r, "0\oplus\alpha'"] & M \arrow[r] & 0
\end{tikzcd}$$

Proof.

Firstly, it is easy to check the two exact sequences are exact. Then consider

$$0 \to K := \ker(\alpha \oplus \alpha') \to P \oplus P' \to M \to 0$$

which is exact, there exists $\pi : P' \to P$ such that $\alpha\pi = \alpha'$, so we may define $\phi : P \oplus P' \to P \oplus P'$ by $\begin{pmatrix} 1_P & \pi \\ 0 & 1'_P \end{pmatrix}$ which means $(p, p') \mapsto (p + \pi p', p')$ and then $\alpha p + \alpha' p' = (\alpha \oplus 0)\phi(p, p') = (\alpha \oplus \alpha')(p, p')$ where the inverse of ϕ will be $\begin{pmatrix} 1_P & -\pi \\ 0 & 1'_P \end{pmatrix}$ and hence ϕ is an automorphism.

Notice L is $\ker\alpha$, and for $(p, p') \in L \oplus P'$, denoted $\psi : L \oplus P' \to K$ the induced map by ϕ^{-1} and then $\psi(p, p') = (p - \pi p', p')$ which is in $\ker(\alpha \oplus \alpha')$ and it has inverse obviously, and hence $L \oplus P' \cong K$, and use the similar construction to $P \oplus L'$ and we are done.

Proposition 1.5.9. Let R be a ring, and $0 \to M \to N \to M' \to 0$ an exact sequence. Prove M, M' are finitely generated implies N is finitely generated.

Proposition 1.5.10. Let R be a ring, and $0 \to L \to R^n \to M \to 0$ an exact sequence. Prove M is finitely generated iff L is finitely presented.

Proposition 1.5.11. Let $0 \to L \overset{\alpha}{\to} M \overset{\beta}{\to} N \to 0$ be a short exact sequence with L finitely generated and M finitely presented. Then N is finitely presented.

Proof.

There exists $G \to F \to M \to 0$ exact with G, F free of finite rank. Let $\mu : R^m \to M$ any surjection and $\nu := \beta\mu$, let$K = \ker \nu$ and $\lambda = \mu|_K$, then the diagram

$$\begin{tikzcd} 0 \arrow[r] & K \arrow[r] \arrow[d, "\lambda"] & R^m \arrow[r, "\nu"] \arrow[d, "\mu"] & N \arrow[r] \arrow[d, "1_N"] & 0 \\ 0 \arrow[r] & L \arrow[r, "\alpha"] & M \arrow[r, "\beta"] & N \arrow[r] & 0 \end{tikzcd}$$

commutes and the snake lemma ensure that $\ker \lambda \cong \ker \mu$, however $\ker \mu$ is finitely generated and hence $\ker \lambda$ is finitely generated, and snake lemma ensured that $\text{coker}\lambda = 0$ and hence $0 \to \ker \lambda \to K \to L \to 0$ is exact and hence K is finitely generated and hence N is finitely presented.

Proposition 1.5.12. Let $0 \to L \overset{\alpha}{\to} M \overset{\beta}{\to} N \to 0$ be a short exact sequence with L, N finitely presented. Then M is finitely presented.

Proof.

Let $\lambda : R^l \to L, \nu : R^n \to N$ any two surjections and define $\gamma := \alpha\lambda$ and since R^n is projective, then define $\delta : R^n \to M$ by lifting ν and $\mu : R^l \oplus R^n \to M$ by $\gamma + \delta$ and the diagram

$$\begin{tikzcd} 0 \arrow[r] & R^l \arrow[r] \arrow[d, "\lambda"] & R^l \oplus R^n \arrow[r, "\nu"] \arrow[d, "\mu"] & R^n \arrow[r] \arrow[d, "\nu"] & 0 \\ 0 \arrow[r] & L \arrow[r, "\alpha"] & M \arrow[r, "\beta"] & N \arrow[r] & 0 \end{tikzcd}$$

commutes, and the snake lemma yields that

$$0 \to \ker \lambda \to \ker \mu \to \ker \nu \to 0$$

exact and $\text{coker}\mu = 0$ and $\ker \lambda, \ker \mu$ are finitely generated and hence $\ker \mu$ is ginitely generated and hence M is finitely presented.

1.6 Direct Limits

Definiton 1.6.1. (Categories)

A category $\mathcal{C}$ is a collection of elements, called objects. Each pair of objects A, B is equipped with a set $\hom_{\mathcal{C}}(A, B)$ called maps or morphisms. For objects A, B, C, there is a composition law

$$\hom_{\mathcal{C}}(A, B) \times \hom_{\mathcal{C}}(B, C) \to \hom_{\mathcal{C}}(A, C), \quad (a, \beta) \to \beta\alpha$$

and there is a distinguished map $1_B \in \hom_{\mathcal{C}}(B,B)$ such that

$$\gamma(\beta\alpha) = (\gamma\beta)\alpha \text{ for any } \gamma : C \to D, \quad \text{ and } 1_B\alpha = \alpha, \beta 1_B = \beta$$

and we say α is an isomorphism with inverse $\beta : B \to A$ such that $\alpha\beta = 1_B$ and $\beta\alpha = 1_A$.

Definiton 1.6.2. (Functors)

A map of categories is known as a functor. Namely, given categories $\mathcal{C}$ and $\mathcal{C}'$, a functor $F : C \to \mathcal{C}'$ is a rule that assigns to each object A of $\mathcal{C}$ and $F(A)$ of $\mathcal{C}'$ and to each map α such that $F(\alpha) : F(A) \to F(B)$

$$F(\beta\alpha) = F(\beta)F(\alpha), \quad F(1_A) = 1_{F(A)}$$

A map of functors is known as a matural transformation. Given two functors $F, F' : \mathcal{C} \to \mathcal{C}'$, a natrual transformation $\theta : F \to F'$ is a collection of maps $\theta(A) : F(A) \to F'(A)$ such that $\theta(B)F(\alpha) = F'(\alpha)\theta(A)$ for any α and $1_{F(A)}$ trvially form a natrual transformation 1_F. We call F and F' isomorphic if there are natural transformation $\theta : F \to F'$ and $\theta' : F' \to F$ such that $\theta'\theta = 1_F$ and $\theta\theta' = 1_{F'}$.

A contravariant functor G from C to C' is a rule similar to F but $G(\alpha) : G(B) \to G(A)$ with analogous properties with functors.

Definiton 1.6.3. (Adjoint)

Let $F : \mathcal{C} \to \mathcal{C}'$ and $F' : \mathcal{C}' \to \mathcal{C}$ be functors. We call (F, F') an adjoint pair , F the left adjoint of F' and F' the right-adjoint of F if for any $A \in \mathcal{C}$ and $A' \in \mathcal{C}'$, there is given a natural bijection

$$\hom_{\mathcal{C}'}(F(A), A') \cong \hom_{\mathcal{C}}(A, F'(A'))$$

here natural means that maps $B \to A$ and $A' \to B'$ induce a commutative diagram:

$$\begin{tikzcd}
\hom_{\mathcal{C}'}(F(A), A') \arrow[r, "\cong"] \arrow[d] & \hom_{\mathcal{C}}(A, F'(A')) \arrow[d] \\
\hom_{\mathcal{C}'}(F(B), B') \arrow[r, "\cong"] & \hom_{\mathcal{C}}(B, F'(B'))
\end{tikzcd}$$

Proposition 1.6.1. Naturality serves to determine an adjoint up to canonical isomorphism. Namely, let F and G be two left adjoints of F' and then F and G are isomorphic.

Proof.

Define $\theta(A) : G(A) \to F(A)$ by the image of $1_{F(A)}$ under the isomorphism

$$\hom(F(A), F(A)) \cong \hom(A, F'F(A)) \cong \hom(G(A), F(A))$$

for $\alpha : A \to B$ it will induce the commutative diagram

$$\begin{tikzcd}
\hom_{\mathcal{C}'}(F(A), F(A)) \arrow[r, "\cong"] \arrow[d] & \hom_{\mathcal{C}}(A, F'F(A)) \arrow[r, "\cong"] \arrow[d] & \hom_{\mathcal{C}'}(G(A), F(A)) \arrow[d] \\
\hom_{\mathcal{C}'}(F(A), F(B)) \arrow[r, "\cong"] & \hom_{\mathcal{C}}(A, F'F(B)) \arrow[r, "\cong"] & \hom_{\mathcal{C}'}(G(A), F(B)) \\
\hom_{\mathcal{C}'}(F(B), F(B)) \arrow[r, "\cong"] \arrow[u] & \hom_{\mathcal{C}}(B, F'F(B)) \arrow[r, "\cong"] \arrow[u] & \hom_{\mathcal{C}'}(G(B), F(B)) \arrow[u]
\end{tikzcd}$$

where we may know $\theta(B)G(\alpha) = F(\alpha)\theta_A$ and hence θ is a natural transformation, similarly, define $\theta' : F \to G$ and we will have

$$\begin{array}{ccccc} \hom_{\mathcal{C}'}(F(A), F(A)) & \xrightarrow{\cong} & \hom_{\mathcal{C}}(A, F'F(A)) & \xrightarrow{\cong} & \hom_{\mathcal{C}'}(G(A), F(A)) \\ \downarrow & & \downarrow & & \downarrow \\ \hom_{\mathcal{C}'}(F(A), G(A)) & \xrightarrow{\cong} & \hom_{\mathcal{C}}(A, F'G(A)) & \xrightarrow{\cong} & \hom_{\mathcal{C}'}(G(A), G(A)) \end{array}$$

which is induced by $\theta'(A)$ and then $\theta'(A)\theta(A) = 1_G(A)$ and we are done.

Definiton 1.6.4. (Direct limits)

Let $\Lambda, \mathcal{C}$ categories and Λ is small, i.e. its objects form a set. Given a functor $\lambda \mapsto M_\lambda$ from Λ to $\mathcal{C}$, its direct limit denoted with $\varinjlim M_\lambda$ is defined to be the object of $\mathcal{C}$ universal among objects P equipped with maps $\beta_\mu : M_\mu \to P$ what are compatible with the transition map $\alpha_\mu^\kappa : M_\kappa \to M_\mu$, i.e. there is a unique map β such that all the diagrams

$$\begin{array}{ccccc} M_\kappa & \xrightarrow{\alpha_\mu^\kappa} & M_\mu & \xrightarrow{\alpha_\mu} & \varinjlim M_\lambda \\ \downarrow{\scriptstyle \beta_\kappa} & & \downarrow{\scriptstyle \beta_\mu} & & \downarrow{\scriptstyle \beta} \\ P & \xrightarrow{1_P} & P & \xrightarrow{1_P} & P \end{array}$$

where $\lambda \mapsto M_\lambda$ is often called a direct system. We know the limit is determined up to unique isomorphism.

We say $\mathcal{C}$ has direct limits indexed by Λ if for every functor $\lambda \mapsto M_\lambda$, the direct limit exists. We say that $\mathcal{C}$ has direct limits if it has direct limites indexed by every small category.

Given a functor $F : C \to C'$, note that a functor $\lambda \mapsto M_\lambda$ from Λ to $\mathbb{C}$ yields a functor from Λ to $\mathcal{C}'$. Furthermore, whenever the corresponding two direct limits exist, the maps $F(\alpha_\mu) : F(M_\mu) \to F(\varinjlim M_\lambda)$ induce a canonical map

$$\phi_F : \varinjlim F(M_\lambda) \to F(\varinjlim M_\lambda)$$

If ϕ_F is always an isomorphism, we say F preserves direct limits.

Proposition 1.6.2. Assume $\mathcal{C}$ has direct limits indexed by Λ. Then, given a natural transformation from $\lambda \mapsto M_\lambda$ to $\lambda \mapsto N_\lambda$, universality yields unique commutative diagrams

$$\begin{array}{ccc} M_\mu & \longrightarrow & \varinjlim M_\lambda \\ \downarrow & & \downarrow \\ N_\mu & \longrightarrow & \varinjlim N_\lambda \end{array}$$

Proof.

We know

$$\theta(\mu) : M_\mu \to N_\mu, \theta(\mu)\alpha_\mu^\lambda = \beta_\mu^\lambda \theta(\lambda)$$

and hence consider

$$\begin{array}{ccccc}
M_\lambda & \longrightarrow & M_\mu & \longrightarrow & \varinjlim M_\lambda \\
\downarrow & & \downarrow & & \downarrow{\scriptstyle\alpha} \\
N_\lambda & \longrightarrow & N_\mu & \longrightarrow & \varinjlim N_\lambda \\
\downarrow & & \downarrow & & \\
P & \xrightarrow{=} & P & \xrightarrow{=} & P
\end{array}$$

Definiton 1.6.5. (Functor category)

The functor category $\mathcal{C}^\Lambda$, i.e. a category with objects to be the functors from Λ to $\mathcal{C}$ and the maps are the natrual transformation, then $\varinjlim$ yields a functor from C^Λ to C.

The direct limit functor is the left adjoint of the diagonal function $\Delta : \mathcal{C} \to \mathcal{C}^\Lambda$ which send M to the constant functor ΔM which has the same value M at every Λ and 1_M at every map of Λ; for $\gamma : M \to N$ it caarries γ to $\Delta\gamma : \Delta M \to \Delta N$ which has the same value γ at every λ.

Proof.

By proposition 1.6.2. we assume $\lambda \mapsto M_\lambda, \lambda \mapsto N_\lambda$ and θ a natural transformation, then

$$\varinjlim(\theta) : \varinjlim M_\lambda \to \varinjlim N_\lambda$$

which is uniquely determined.

Notice

$$\varinjlim : \mathcal{C}^\Lambda \to \mathcal{C}, \quad \Delta : \mathcal{C} \to \mathcal{C}^\Lambda$$

and we want to check

$$\hom(\varinjlim(\lambda \mapsto M_\lambda), N) \cong \hom(\lambda \mapsto M_\lambda, \Delta N)$$

assume $\gamma : \varinjlim(\lambda \mapsto M_\lambda) \to N$ and then we would like $\gamma \mapsto \Delta\gamma$ is an isomorphism, which is obviously an injection and assume $\delta : \lambda \mapsto M_\lambda \to \Delta N$ where we know $\delta(\lambda) : M_\lambda \to N$ which satisfies some commutative diagram and hence there exists a unique $\gamma : \varinjlim(\lambda \mapsto M_\lambda) \to N$.

Definiton 1.6.6. (Coproduct)

Let $\mathcal{C}$ be a category, Λ a set and M_λ an object for each $\lambda \in \Lambda$. The coproduct $\coprod_{\lambda\in\Lambda} M_\lambda$ is defined as the object of $\mathcal{C}$ universal among objects P equipped with a map $\beta_\mu : M_\mu \to P$ and the maps $\iota_\lambda : M_\lambda \to \coprod M_\lambda$ is call the inclusions.

If Λ is empty then B is an object with a unique map β to other P and such B is called an initial object.

Definiton 1.6.7. (Coequalizers)

Let $\alpha, \alpha' : M \to N$ their coequalizer is the object universal among P with $\eta : N \to P$ such that $\eta\alpha = \eta\alpha'$.

Lemma 1.6.3. A category has direct limits iff it has coproducts and coqualizers. If a category has direct limits, then a functor preserves them iff it preserves coproduct and coequalizers.

Proof.

Let $\Lambda \mapsto M_\lambda$ where $\hom(\mu,\nu)$ is empty for any $\mu \neq \nu$ and then the corresponding direct limit is the coproduct. For $M, N \in \mathcal{C}$ and two morphsims, then the inclusion of them two is a small category and the direct limit will be the coequalizer. If F preserves direct limits, since we have shown that coproduct and coequalizer is special direct limits and we are done.

Conversely, if $\mathcal{C}$ has coproducts and coequalizers. Assume Λ a small category and $\lambda \mapsto M_\lambda$ a functor, let Σ all transition maps and for each $\sigma = \alpha_\mu^\lambda \in \Sigma$, set $M_\Sigma := M_\lambda$ and let $M := \coprod M_\sigma$ and $N = \coprod M_\lambda$, for each σ, there are two maps $M_\sigma \to N$ which is ι_λ and the composition $\iota_\mu \alpha_\mu^\lambda$, then let C be the coequalizer of corresponding maps $\alpha, \alpha' : M \to N$ aand $\eta : N \to C$ the insertion. So if $\beta_\lambda : M_\lambda \to P$ compatible with the transition maps, then there is a unique $\beta : N \to P$ such that $\beta\iota_\lambda = \beta_\lambda$ and hence $\beta\alpha = \beta\alpha'$ and we are done.

If F preserves coproduct and coeqqualizers, then F preserves the construction and we are done.

Theorem 1.6.4. The categories R-module and sets have direct limits.

Theorem 1.6.5. Every left adjoint $F : \mathcal{C} \to \mathcal{C}'$ preserves direct limits.

Proposition 1.6.6. Let $\mathcal{C}$ be a category, Λ and Σ small categories. Assume $\mathcal{C}$ has direct limits indexed by Σ. Then the functor category $\mathcal{C}^\Lambda$ does too.

Theorem 1.6.7. Let $\mathcal{C}$ be a category with direct limits indexed by small categories Σ and Λ. Let $\sigma \mapsto (\lambda \mapsto M_{\sigma\lambda})$ be a functor from Σ to $\mathcal{C}^\Lambda$. Then

$$\varinjlim_\sigma \varinjlim_\lambda M_{\sigma\lambda} = \varinjlim_\lambda \varinjlim_\sigma M_{\sigma\lambda}$$

Corollary 1.6.8. Let Λ be a small category, R a ring, and $\mathcal{C}$ is sets or R-modules. Then functor $\varinjlim : \mathcal{C}^\Lambda \to \mathcal{C}$ preserves coproduces and coequalizers.

1.7 Tensor Products

Definiton 1.7.1. (Bilinear maps)

Let R be a ring and M, N, P modules. We call a map $\alpha : M \times N \to P$ bilinear if it is lienarin each variable. Denote the set of all these maps by $\mathrm{Bil}_R(M, N; P)$, it is clearly an R-module with sum and scalar multiplication performed valuewise.

Definiton 1.7.2. (Tensor product)

Let R be a ring and M, N modules. Their tensor product denoted $M \otimes_R N$ is constructed as the quotient of the free module $R^{\oplus(M\times N)}$ modulo the submodule generated by the following elemants, where (m, n) stands for the standard basis element $e_{(m,n)}$:

$$(m + m', n) - (m, n) - (m', n), (m, n + n') - (m, n) - (m, n'), (xm, n), (m, xn) - x(m, n)$$

and the above construction yields a canonical bilinear map

$$\beta : M \times N \to M \otimes N$$

and set $m \otimes n := \beta(m, n)$

Theorem 1.7.1. (UMP of tensor product)

Let R be a ring, M, N modules. Then $\beta : M \times N \to M \otimes N$ is the universal bilinear map with source $M \times N$; in fact, β induces a module isomorphism

$$\theta : \hom_R(M \otimes_R N, P) \cong \mathrm{Bil}_R(M, N; P)$$

Corollary 1.7.2. (Bifunctoriality)

Let R be a ring, $\alpha : M \to M'$ and $\alpha' : N \to N'$ module homomorphisms. Then there is a canonical commutative diagram:

$$\begin{tikzcd}
M \times N \arrow[r, "\alpha\times\alpha'"] \arrow[d, "\beta"] & M' \times N' \arrow[d, "\beta'"] \\
M \otimes N \arrow[r, "\alpha\otimes\alpha'"] & M' \otimes N'
\end{tikzcd}$$

Proof.

Notice

$$(\alpha \otimes \alpha')(m \otimes n) = \alpha m \otimes \alpha' n$$

Proposition 1.7.3. Let R be a ring, M and N modules,

- Then the switch map $(m, n) \mapsto (n, m)$ induces an isomorphism

$$M \otimes_R N = N \otimes_R M$$

- The multiplication on M indcues an isomorphism

$$R \otimes_R M = M$$

Proof.

The switch map induces an isomorphism between $M \otimes_R N = N \otimes_R M$.

Define $\beta : R \times M \to M$ by $\beta(x, m) := xm$, then β is bilinear and we have for any $\alpha : R \times M \to P$, define $\gamma : M \to P$ by $\gamma(m) = \alpha(1, m)$ and then $\alpha = \gamma\beta$, where γ is unique since β surjective and hence $M \cong R \otimes M$ since

$$\begin{tikzcd}
R \times M \arrow[r, "\beta'"] \arrow[d] \arrow[dr, "\beta''"] & P \\
R \otimes M \arrow[ur, "\beta"'] & M \arrow[u, "\gamma"']
\end{tikzcd}$$

let P be M and $R \otimes M$ and we are done.

Definiton 1.7.3. Let R and R' be rings. An abelian group N is an (R, R')-bimoudle if it is both an R-module and an R'-module if $x(x'n) = x'(xn)$ for all $x \in R, x' \in R'$ and $n \in N$.

1.8 Flatness

Lemma 1.8.1. Let R be a ring, $\alpha : M \to N$ a homomorphism of modules. Then there is a commutative diagram with two short exacct sequences involving N'

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r] & M \arrow[rr, "\alpha"] \arrow[dr, "\alpha'"] & & N \arrow[r] & N'' \arrow[r] & 0 \\
& & 0 \arrow[r] & N' \arrow[r] \arrow[ur, "\alpha''"] & 0 & &
\end{tikzcd}$$

iff $M' = \ker\alpha$ and $N' = \mathrm{Im}\alpha$ and $N'' = \mathrm{Coker}\alpha$.

Definiton 1.8.1. (Exact Functors)

Let R be a ring , R' an algebra, F a linear functor from $((R\text{-mod}))$ to $((R'\text{-mod}))$. Call F faithful if the associated map

$$\hom_R(M, N) \to \hom_{R'}(FM, FN)$$

is injective, or equivalently, if $F\alpha = 0$ implies $\alpha = 0$. Call F exact if it preserves exact sequences, left exact if it preserves kernels and right exact if it preserves cokernels.

Proposition 1.8.2. Let R be a ring, R' an algebra, F an R-linear functor from $((R\text{-mod}))$ to $((R'\text{-mod}))$. Then the following conditions are equivalente

- F is exact
- F preserves short exact sequences
- F preserves kernels and surjections.
- F preserves cokernels and injections
- F preserves kernels and images

Proof.

(1) implies (2),(3),(4) is trivial. (3) implies (2) and (4) implies (2) are trivial. (2) implies (5) by lemma and assume (5), let $M' \to M \to M''$ exact, then $\ker(\beta) = \mathrm{Im}(\alpha)$ and then $\ker(F(\beta)) = F(\ker(\beta)) = F(\mathrm{Im}(\alpha)) = \mathrm{Im}F\alpha$ and we are done.

Definiton 1.8.2. (Flatness)

We say an R-module M is flat over R or is R-flat if $M \otimes_R \cdot$ is exact. It is equivalent with that $M \otimes_R \cdot$ preserve injection since it preserves cokernels.

We say M is faithfully if $M \otimes_R \cdot$ is exact and faithful.

We say an R-algebra is falt or faithfully flat if it is so as an R-module.

1.9 Cayley-Hamilton Theorem

Theorem 1.9.1. (Cayley-Hamilton Theorem)

Let R be a ring, and $M := (a_{i,j})$ with $a_{i,j} \in R$, Then characteristic polynomial of M is

$$P_M(T) := T^n + a_1T^{n-1} + \cdots + a_n := \det(TI_n - M)$$

Let A be an ideal. If $a_{ij} \in A$ for all i, j, then $a_k \in A^k$ for all k.

The Cayley-Hamilton Theorem asserts that in the ring of matrices,

$$P_M(M) = 0$$

1.10 Localization

Definiton 1.10.1. (Localization)

Let R be a ring, and S a multiplicative subset. Define a relation on $R \times S$ by $(x, s) \sim (y, t)$ if there is a $u \in S$ such that $xtu = ysu$, which is an quivalence relation. Denote $S^{-1}R$ the set of equivalence classes, and by x/s the class of (x, s) and defined $x/s \cdot y/t := xy/st$ and $x/s + y/t = (tx + sy)/st$, and then $S^{-1}R$ wil be a ring, which is called the localization at S. $\phi_S : R \to S^{-1}R$ by $\phi_S(x) := x/1$.

2 Fields and Galois Theory

2.1 Definitions and Results

Definiton 2.1.1. A field is a set F with binary operations $+$ and $\cdot$ such that

- $(F, +)$ is a commutative group
- $(F^\times, \cdot)$ where $F^\times = F - \{0\}$ is a commutative group
- the distributive law holds

Lemma 2.1.1. A nonzero commutative ring R is a field iff it has no ideals other than (0) and R.

Definiton 2.1.2. An F-algebra for a field F is finite if it is a finite-dimensional F-vector space.

Definiton 2.1.3. (Characteristic of a Field)

Consider $Z \to F$ by $n \mapsto n1_F$, if the kernel of this map is (0), then there exists $Q \hookrightarrow F$ and we say it has characteristic zero.

If the kernel is not zero, then the smallest integer in the kernel has to be a prime p and we know $F_p \hookrightarrow F$ and we call it has caracteristic p. A field isomorphic to F_p or Q is called a prime field.

Definiton 2.1.4. (Frobenius endomorphism)

Assume R a commutative ring has characteristic p if it contains a prime field of characteristic p as a subring, then the prime field is unique and contains 1_R, it is easy to qcheck that $(a+b)^p = a^p + b^p$ for any $a, b \in R$ if p is nonzero and hence $a \mapsto a^p$ us a homomorphism and it is called the frobenius endomorphism of R. The charaacteristic exponent of a field F is 1 if F has characteristic 0 and p if F has characteristic $p \neq 0$.

Proposition 2.1.2. (Gauss's Lemma)

Let $f(X) \in \mathbb{Z}[X]$. If $f(X)$ factors nontrivially in $\mathbb{Q}[\mathbb{X}]$, then it factors nontrivially in $\mathbb{Z}[X]$.

Proposition 2.1.3. If $f \in \mathbb{Z}[X]$ is monic, then every monic factor of f in $\mathbb{Q}[X]$ lies in $\mathbb{Z}[X]$.

Proposition 2.1.4. (Eisenstein's Criterion)

Let $f = a_m X^m + a_{m-1} X^{m-1} + \cdots + a_0, a_i \in \mathbb{Z}$ suppose that there is a prime number p such that

- p does not divide a_m
- p divides $a_{m-1}, \cdots, a_0$
- p^2 does not divide a_0

then f is irreducible in $\mathbb{Q}[X]$.

2.1.1 Extensions

Definiton 2.1.5. (Extensions)

Let F be a field. An **extension** of F is field containing F as a subfield. An extension E of F is an F-vector space, whose dimension is called the **degree** $[E : F]$ of E over F. An extension is said to be finite if its degree is finite.

When E and E' are extensions of F, an F-homomorphism $E \to E'$ is a homomorphism $\phi : E \to E'$ such that $\phi|_F \circ id|_F = id_F$ and an F-isomorphism is a bijective F-homomorphism.

Proposition 2.1.5. Consider fields $F \supset E \supset F$. Then L/F is of finite degree if and only if L/E and E/F are both of finite degree, in which case

$$[L : F] = [L : E][E : F]$$

Proof.

To see the sufficiency, obviously $[L : F] \geq [L : E]$ and assume $\{l_i\}_{i=1}^m$ a basis of L as an F-vector space and then E as an F-vector space will satisfy that $[E : F] \leq [L : F]$. Assume $\{e_i\}_{i=1}^k$ and $\{l'_j\}_{j=1}^r$ are relatively bases of E as an F-vector space and L as an E-space. Then we may know that $\{e_i l'_j\}$ will generate L and will become a basis since if

$$\sum_{1 \leq i \leq k, 1 \leq j \leq r} f_{ij} e_i l'_j = 0$$

will implies that $\sum_{i=1}^k f_{ij} e_i = 0$ for each $j, 1 \leq j \leq r$ and then $f_{ij} = 0$ for any i, j and we are done.

Definiton 2.1.6. (Generated subring)

Let F be a subfield of a field E and S a subset of E. The intersection of all subrings of E containing F and S is called the subring of E **generated by** F and S and denoted by $F[S]$.

Lemma 2.1.6. The ring $F[S]$ consists of the elements of E that can be expressed as F-linear combanation of finite product of elements in S (including 0 elements, i.e. 1_F).

Lemma 2.1.7. Let R be a finite F-algebra. If R is an integral domain, then it is a field.

Proof.

Let $\alpha \in R$ nonzero, and consider $x \to \alpha x$ which is an injective linear map and hence surjective since $R \to R$ finite-dimensional and we are done.

Definiton 2.1.7. (Generated subfield)

Let F be a subfield of a field E and S a subset of E. The intersection of all subfields of E containing F and S is called the subfield of E **generated by** F and S and denoted by $F(S)$,which is the field of fractions of $F[S]$.

Definiton 2.1.8. (Simple extension and composite)

An extension E of F is said to be **simple** if $E = F(\alpha)$ for some $\alpha \in E$. Let F and F' be subfields of a field E. We call the intersection of subfields of E containing both F and F' as the **composite** of F and F' in E.

Proposition 2.1.8. For a monic irreducible polynomial $f(X)$ of degree m in $F[X]$, then $F[x] := F[X]/(f)$ is a field of degree m over F.

Definiton 2.1.9. (Stem fields)

Let f be a monic irreducible polynomial in $F[X]$. A pair (E, α) cconsisting of an extension E of F and an $\alpha \in E$ is called a **stem field** for f if $E = F[\alpha]$ and $f(\alpha) = 0$, which is F-isomorphic to $(F[X]/(f), x)$.

2.1.2 Algebraic and Transcendental Elements

Definiton 2.1.10. (Algebraic and Transcendental Elements)

Let F be a field and E an integral domain containing F as a subring. An element α of E defines a homomorphism $f(X) \mapsto f(\alpha) : F[X] \to E$.

If the kernel of the map is zero, then we call α **transcendental** over F.

If the kernel is nonzero, then we say α is **algebraic** over F. We call the monic, irreducible polynomial f generating the kernel the **minimal polynomial** of α over F, and then $F[\alpha]$ is a stem field for f.

Definiton 2.1.11. (Algebraic extension)

An extension E of F is said to be **algebraic** if every element of E is algebraic over F, otherwise it is said to be **transcendental**.

Proposition 2.1.9. Let $E \supset F$ be fields. If E/F is finite, then E is algebraic and finitely generated over F; conversely, if E is generated over F by a finite set of algebraic elements, then it is of finite degree over F.

Proof.

If α is transcendental over F, then we know $1, \alpha, \alpha^2, \cdots$ are linearly independent over F, which is a contradiction. And if $E = F$, then E is generated by the empty set. Or there is an element in $E - F$ and we will have

$$[F[\alpha_1] : F] < [F[\alpha_1, \alpha_2] : F] < \cdots < [E : F]$$

which means $E = F[\alpha_1.\alpha_2, \cdots, \alpha_n]$ for some integer n and $\alpha_i \in E$.

Notice $F[\alpha_1]$ is finite generated since α_1 is algebraic and hence $F[\alpha_1] = F(\alpha_1)$, which means $F(\alpha_1)/F$ is finite. Then notice α_2 is algebraic over $F(\alpha_1)$ and repeating the argument.

Corollary 2.1.10. Consider fields $L \supset E \supset F$. If L is algebraic over E and E is algebraic over F, then L is algebraic over F.

Proof.

Consider $l \in L$ is a root of $\sum_{i=0}^{m} a_i X^i$ and then $F[a_0, \cdots, a_m]$ is finite over F and $F[a_0, \cdots, a_m, l]$ is finite over F and hence l is algebraic oveer F.

Proposition 2.1.11. Let F be a field and R an integral domain containing F as a subring. If R is generated as an F-algebra by elements algebraic over F, then it is a field algebraic over F.

Proof.

For any $r \in R$, there exists $\{\alpha_i\}_{i=1}^m$ such that $r \in F[\alpha_1, \cdots, \alpha_m]$ (as a fraction) and then since for any α_i, there exists $a_j \in F$ such that $\alpha_i^m = a_0 + a_1\alpha_i + \cdots + a_m\alpha_i^{m-1}$ and we may know that $F[\alpha_1, \cdots, \alpha_m]$ is finite and hence algebraic, which means r is algebraic over F.

2.1.3 Algebraically Closed Fields

Definiton 2.1.12. Let F be a field. A polynomial is said to **split** in $F[X]$ if it is a product of polynomials of degree at most 1 in $F[X]$.

Proposition 2.1.12. For a field Ω, the following statemetns are equivalent:

- Every nonconstant polynomial in $\Omega[X]$ splits in $\Omega[X]$
- Every nonconstant polynomial in $\Omega[X]$ has at least one root in Ω
- The irreducible polynomials in $\Omega[X]$ are those of degree 1
- Every field of finite degree over Ω equals Ω.

Proof.

(a) to (b) to (c) are obvious.

(c) to (a) by UFD. (c) to (d), consider E a finite extension and hence algebraic, for $\alpha \in E$ the minimal polynomial of α has degree 1 and we are done.

(d) to (c) consider $\Omega[X]/(f)$ and its degree has to be 1 and we are done.

Definiton 2.1.13. (Algebraic Closure)

A field Ω is **algebraically closed** if it satisfies the equivalent statements above. A field Ω is an **algebraic closure** of a subfield F if it is algebraically closed and algebraic over F.

Proposition 2.1.13. If Ω is algebraic over F and every polynomial f splits in $\Omega[X]$, then Ω is algebraically closed.

Proof.

Let $f \in \Omega[X]$ and we want to show f has a root in Ω. Since f has a root α insome finite extension Ω' of Ω and consider

$$F \subset F[a_0, \cdots, a_n] \subset [a_0, \cdots, a_n, \alpha]$$

which is finite since they are all generated by finite algebraic elements and hence α is algebraic over F and hence it is a root of some polynomial in F and then $\alpha \in \Omega$ and we are done.

Proposition 2.1.14. Let F be a field and Ω an integral domain containing F as a subring. Then $\bar{F} := \{\alpha \in \Omega, \alpha \text{ algebraic over } F\}$ is a field, which is called the algebraic closure of F in Ω.

Proof.

Notice $F[\alpha, \beta]$ is finite over F.

Corollary 2.1.15. Let Ω be an algebraically closed field. For any subfield F of Ω, the algebraic closure E of F in Ω is an algebraic closure of F.

Proof.

For $f \in F[X]$ we know it splits in $\Omega[X]$ and is has its roots in E, so splits in $E[X]$ and we are done.

2.2 Splitting Fields; Multiple Roots

Proposition 2.2.1. Let $F(\alpha)$ be a simple extension of F and Ω a second extension of F.

- Suppose α is transcendental over F. For every F-homomorphism $\phi : F(\alpha) \to \Omega$, $\phi(\alpha)$ is transcendental over F, and the map $\phi \mapsto \phi(\alpha)$ defines a one-to-one correspondence

$$\{F\text{-homomorphisms } F(\alpha) \to \Omega\} \leftrightarrow \{\text{elements of } \Omega \text{ transcendental over } F\}$$

- Suppose α is algebraic over F, and let $f(X)$ be its minimal polynomial. For every F-homomorphism $\phi : F[\alpha] \to \Omega$, $\phi(\alpha)$ is a root of $f(X)$ in Ω, and the map $\phi \mapsto \phi(\alpha)$ defines a one-to-one correspondence

$$\{F\text{-homomorphisms } F(\alpha) \to \Omega\} \leftrightarrow \{\text{roots of } f \text{ in } \Omega\}$$

  In particular, the number of such maps is the number of distinct roots of f in Ω.

Proof.

(a) For an F-homomorphism, since $F[\alpha]$ is isomorphic to the polynomial ring with symbol α, then consider $\phi(\alpha) = \gamma$ and since ϕ is defined on $F(\alpha)$, which implies that γ is transcendental over F. By the way, only notice that $\phi(\alpha) = \gamma$ transcendental will extend to a unique homomophism $F(\alpha) \to \Omega$.

(b) Only need to check the necessity, if $\gamma \in \Omega$ a root of $f(X)$, then consider $F[X] \to \Omega : g(X) \mapsto g(\gamma)$, which factors through $F[X]/(f(X))$ which is isomorphic to $F[\alpha]$ and hence ϕ sends α to γ.

Proposition 2.2.2. Let $F(\alpha)$ be a simple extension of F and $\phi_0 : F \to \Omega$ a homomorphism from F into a second field Ω.

(a) If α is transcendental over F, then the map $\phi \mapsto \phi(\alpha)$ defines a one-to-one correspondence

$$\{\text{extensions } \phi : F(\alpha) \to \Omega \text{ of } \phi_0\} \leftrightarrow \{\text{elements of } \Omega \text{ transcendental over } \phi_0(F)\}$$

(b) If α algebraic over F, with minimal polynomial $f(X)$, then the map $\phi \mapsto \phi(\alpha)$ defines a one-to-one correspondence

$$\{\text{extensions } \phi : F[\alpha] \to \Omega \text{ of } \phi_0\} \leftrightarrow \{\text{roots of } \phi_0 f \text{ in } \Omega\}$$

In particular, the number of such maps is the number of distinct roots of $\phi_0 f$ in Ω.

Definiton 2.2.1. Let f be a polynomial with coefficients in F. A field E containing F is said to **split** f if f splits in $E[X]$ and we call E a **splitting** or **root field** for f if it is generated by the roots of f.

Proposition 2.2.3. Every polynomial $f \in F[X]$ has a splitting field E_f and $[E_f : F] \leq (\deg f)!$.

Proof.

Let $F_1 = F[\alpha_1]$ be a stem field for some monic irreducible factor of f in $F[X]$ and let $F_2 = F_1[\alpha_2]$ be a stem field for some monic irreducible factor of $f(X)/(X - \alpha_1)$ and continuing, we will have a splliting field E_f where $[F_{k+1} : F_k] \leq n - k, F_0 = F$ and we are done.

Proposition 2.2.4. Let $f \in F[X]$. Let E be an extension of F generated by the roots of f in E and Ω an extension of F splitting f. There exists an F-homomorphism $\phi : E \to \Omega$ and the number of such homomorphisms is at most $[E : F]$ an equivalents $[E : F]$ if f has distinct roots in Ω.

Proof.

Suppose f monic. Assume $f = \prod(X - \beta_i) \in \Omega[X]$ and L a subfield of Ω containing F, g a monic factor if f in $L[X]$. We know $g|f$ in $\Omega[X]$ and hence a product of some $X - \beta_i$, which means g splits in Ω and has distinct roots if f does.

$E = F[\alpha_1, \cdots, \alpha_m]$ with $\alpha_i \in E$ roots of f and we know the minimal polynomial of α_1 is an irreducible $f_1|f$. Then we know f_1 splits in Ω by letting $L = F$ with distinct roots if f have. Then we know the number of F-homomorphism $\phi_1 : F[\alpha_1] \to \Omega$ is the number of distinct roots of f_1, whose degree is $[F[\alpha_1] : F]$ with equality when f has distinct roots in Ω. The minimal polynomial of α_2 over $F[\alpha_1]$ is an irreducible f_2 in $F[\alpha_1][X]$, then let $L = \phi_1 F[\alpha_1]$ and $g = \phi_1 f_2$ which splits in Ω and its roots are distinct if the roots of f are and each ϕ_1 extends to a homomorphism $\phi_2 : F[\alpha_1, \alpha_2] \to \Omega$ with at most $[F[\alpha_1, \alpha_2] : F[\alpha_1]]$ with equality when f has distinct roots and continuing, we are done.

Corollary 2.2.5. If E_1 and E_2 are both spliiting field for f, then every F-homomorphism $E_1 \to E_2$ is an isomorphism. In particular, any two splitting fields for f are F-isomorphic.

Proof.

Notice that every F-homomorphism $E_1 \to E_2$ is injective, which is since it is a field homomorphism and then we know $[E_1 : F] \leq [E_2 : F]$ and hence $[E_1 : F] = [E_2 : F]$ which means that $E_1 \cong E_2$ for each homomorphism.

Corollary 2.2.6. Let E and L be extension of F, with E finite over F. The number of F-homomorphisms $E \to L$ is at most $[E : F]$.

Proof.

Let $E = F[\alpha_1, \cdots, \alpha_m]$ and let $f \in F[X]$ be the product of the minimal polynomials (which has to exist) of α_i and hence E is generated over F by roots of F. Let Ω be a splitting field for f as an element of $L[X]$. Then there exists an F-homomorphism $E \to \Omega$ and the number of such homomorphisms is at most $[E : F]$. For an F-homomorphism $E \to L$, it has to be able to regarded as an F-homophism since Ω is an L extension.

Proposition 2.2.7. Let f and g be polynomials in $F[X]$ and let Ω be an extension of F. If $r(X)$ is the gcd of f and g computed in $F[X]$, then it is also the gcd of f and g in $\Omega[X]$. In particular, distict monic irreducible polynomials in $F[X]$ do not acquire a common root in any extension of F.

Proof.

Notice $r_F(X)|r_\Omega(X)$ and use the Euclid.

Definiton 2.2.2. (Multiplicity)

Let $f \in F[X]$ and f splits into linear factors

$$f(X) = a\prod_{i=1}^{r}(X-\alpha_i)^{m_i}, \quad a \in F, \quad \alpha_i \text{ distinct}, \quad m_i \geq 1$$

in $E[X]$ for some extension of F and we say α_i is a root of f of **multiplicity** m_i in E, where $\{m_i\}$ is independent with the extension. We say f **has a multiple root** when at least one $m_i > 1$ and f **has only simple roots** when $m_i = 1$.

Proof.

Consider E and its subfield $F[\alpha_1, \cdots, \alpha_r]$, where $\{m_i\}$ keep unchanged and we may consider E, E' all splitting fields of f and then we know they are F-isomorphic.

Definiton 2.2.3. (Derivative)

The **derivative** of a polynomial $f(X) = \sum a_i X^i$ is defined to be $f'(X) = \sum i a_i X^{i-1}$.

Lemma 2.2.8. A root of f is multiple if and only if it is also a root of f'.

Proposition 2.2.9. For a nonconstant irreducible polynomial f in $F[X]$, the following are equivalent

- f has a multiple root
- $gcd(f, f') \neq 1$
- F has nonzero characteristic p and f is a polynomial in X^p
- all the roots of f are multiple.

Proof.

(d) to (a), (a) to (b) trivial. For (b) to (c), as f is irreducible and $\deg f' < \deg f$, then $gcd(f, f') \neq 1$ implies that $f' = 0$ and hence $f = a_0 + \cdots + a_d X^d$ implies that $f' = a_1 + \cdots + i a_i X^{i-1} + \cdots + d a_d X^{d-1}$ which is zero iff F has characteristic $p \neq 0$ and $a_i = 0$ for all i not divisible by p. (c) to (d) consider $f(X) = g(X^p)$ which implies $g = \prod(X - a_i)^{m_i}$ for some p^{th} power a_i and then $f(X) = g(X^p) = \prod(X^p - a_i)^{m_i} = \prod(X - \alpha_i)^{pm_i}$ for some α_i.

Proposition 2.2.10. The following conditions on a nonzero polynomial $f \in F[X]$ are equivalent:

- $gcd(f, f') = 1$ in $F[X]$
- f has only simple roots.

Definiton 2.2.4. (Separable)

A polynomial is **separable** if it is nonzero and satisfies the equivalent conditions above.

Definiton 2.2.5. A field F is **perfect** if it has characteristic zero or it has characteristic p and every element of F is a p^{th} power.

Proposition 2.2.11. A field F is perfect if and only if every irreducible polynomial in $F[X]$ is separable.

Proof.

If F has characteristic zero, the statement is obvious. If F has a nonzero characteristic, and A is not a p^{th} power, then $X^p - a$ is irreducible but not separable. Conversely, if every element of F is a p^{th} power, then every polynomial in X^p is a p^{th} power in $F[X]$ and hence not irreducible.

To see $X^p - a$ is irreducible, consider α a root of $X^p - a$ in some extension, then we know $X^p - a = (X - \alpha)^p$ in the extension, and hence $(X - \alpha)^d$ is in $F[X]$ for some d, which means $d\alpha \in F$ and hence $\alpha \in F$, which is a contradiction.

2.3 The Fundamental Theorem of Galois Theory

2.3.1 Galois Group

Definiton 2.3.1. (Automorphism)

Consider fields $E \supset F$. An F-isomorphism $E \to E$ is called an F-automorphism of E. The F-automorphisms of E form a group, which we denote $\mathrm{Aut}(E/F)$.

Proposition 2.3.1. Let E be a splitting field of a separable polynomial f in $F[X]$; then $\mathrm{Aut}(E/F)$ has order $[E : F]$.

Proof.

As f separable, it has $\deg f$ distinct roots in E and hence then we know that the number of F-homomorphisms $E \to E$ is $[E : F]$ and we are done.

Definiton 2.3.2. (Fixed field)

When G is a group of automorphisms of a field E, we set

$$E^G = \mathrm{Inv}(G) = \{\alpha \in E | \sigma\alpha = \alpha, \text{ for all } \sigma \in G\}$$

which will be a subfield of E and hence called the **fixed field** of G.

Theorem 2.3.2. Let G be a finite group of automorphisms of a field E, then

$$[E : E^G] \leq (G : 1) := |G|$$

Proof.

Let $F = E^G$ and let $G = \{\sigma_1, \cdots, \sigma_m\}$ with σ_1 identity. It suffices to show that every set $\{\alpha_1, \cdots, \alpha_n\}$ of elements of E with $n > m$ is linearly dependent. Consider

$$\sigma_i(\alpha_1)X_1 + \cdots \sigma_i(\alpha_n)X_n = 0$$

will have nontrivial solutions in E and hence we choose $(c_1, \cdots, c_n)$ with fewest possible nonzero elements and WLOG $c_1 \in E^G$ nonzero. If not all c_i are in F, then $\sigma_k(c_i) \neq c_i$ for some $k \neq 1$ and then we will find $(c_1, , \sigma_k(c_2), \cdots, \sigma_k(c_i), \cdots)$ is a solution and then we will obtain a solution with lest nonzero elements. So $c_1, \cdots, c_n \in E^G$ and we are done.

Corollary 2.3.3. Let G be a fintie group of automorphisms of a field E, then $G = \mathrm{Aut}(E/E^G)$.

Proof.

As $G \subset \text{Aut}(E/E^G)$ and

$$[E : E^G] \leq |G| \leq |\text{Aut}(E/E^G)| \leq [E : E^G]$$

and hence $G = \text{Aut}(E/E^G)$.

Definiton 2.3.3. (Separable Extension)

An algebraic extension E/F is **separable** if the mininal polynomial of every element is separable; other wise, it is **inseparable**.

Proposition 2.3.4. An algebraic extension E/F is separable if every irreducible polynomial in $F[X]$ having a root in E is separable, and it is inseparable if F is nonperfect and there is an element α of E whose minimal polynomial is of the form $g(X^p)$ with p the characteristic of F.

Definiton 2.3.4. (Normal Extension)

An algebraic extension E/F is **normal** if it is algebraic and the minimal polynomial of every element of E splits in $E[X]$.

Here is an extra useful proposition.

Proposition 2.3.5. Let Ω/F be an extension of fields. If Ω is algebraic over F and every nonconstant polynomial in $F[X]$ has a root in Ω, then Ω is algebraically closeds.

Proposition 2.3.6. An algebraic extension E/F is normal if every irreducible polynomial in $F[X]$ having one root in E will split in $E[X]$.

Proposition 2.3.7. Let E be an algebraic extension of F, and let f a monic irreducible polynomial in $F[X]$. If f has a root in E, then E/F is normal and separable iff every irreducible polynomial in $F[X]$ having a root in E has $\deg f$ distinct roots in E.

Definiton 2.3.5. (Galois Group)

An extension E/F of fields is **Galois** if it is finite, normal and separable. Then $\text{Aut}(E/F)$ is called the **Galois group** of E over F, and denoted by $\text{Gal}(E/F)$.

Theorem 2.3.8. For an extension E/F, the following statements are equivalent

- E is the splitting field of a separable polynomial $f \in F[X]$
- E is finite over F and $F = E^{\text{Aut}(E/F)}$
- $F = E^G$ for some finite group G of automorphisms of E
- E is Galois over F

Proof.

(a) to (b), we know E is finite over F since it is generated by finite algebraic elements. Let $F' = E^{\text{Aut}(E/F)} \supset F$ and it suffices to show $F' = F$. Notice f can be viewed as a polynomial in $F'[X]$ and hence

$$|\text{Aut}(E/F')| = [E : F'] \leq [E : F] = |\text{Aut}(E/F)|$$

and notice the equality of terms on both sides and hence $[E : F] = [E : F]$, which means $F' = F$. (b) to (c) trivial.

(c) to (d), we know E/F is finite by Artin's theorem. Let $\alpha \in E$ and f the minimal polynomial of α, and consider α_i the orbit of α under G on E with $\alpha_1 = 1$ and let $g(X) = \prod(X - \alpha_i)$ and it is easy to check $G \in F[X]$ and hence $f|g$. Conversely we will know that $g|f$ by use $\sigma \in G$ on f and we know $f(\alpha_i) = 0$ and hence $f = g$ and we are done.

(d) to (a), assume $E = F[\alpha_1, \cdots, \alpha_m], \alpha_i \in E$ and let f_i the minimal polynomial of α_i and f the product of distinct f_i. E normal implies that f_i splits in E and hence E is the splitting field of f. E separable means that f_i separable and hence f separable since f_i will be coprime.

Corollary 2.3.9. Let G be a finite groups of automorphisms of a field E, and let $F = E^G$. Then E is a Galois extension of F with Galois group G, and $[E : F] = |G|$.

Proof.

E is Galois by the theorem, and G is the Galois group by corollary 2.3.3., and $[E : F] = |\mathrm{Aut}(E/F)| = |G|$.

Corollary 2.3.10. Every finite separable extension E of F is contained in a Galois extension.

Proof.

Let $E = F[\alpha_1, \cdots, \alpha_m]$ and f_i the minimal polynomial of α_i, the the product of the distinct f_i is a separable polynomial in $F[X]$ whose splitting field is a Galois extension of F containing E.

Corollary 2.3.11. Let $E \supset M \supset F$, if E is Galois over F, then it is Galois over M.

Proof.

E is the splitting field of some separable $f \in F[X]$ which is also a separable polynomial in $M[X]$.

Definiton 2.3.6. (Special Galois Groups)

An extension E of F is **cyclic/abelian/solvable** if it is a Galois extension of F with cyclic/abelian/solvable Galois group.

2.3.2 Main Theorem

Definiton 2.3.7. (Subextension)

Let E be an extension of F. A **subextension** of E/F is an extension M/F with $M \subset E$, i.e. a field M with $F \subset M \subset E$.

Theorem 2.3.12. (Fundamental Theorem of Galois Theory)

Let E be a Galois extension of F with Galois group G. The map $H \mapsto E^H$ is a bijection from the set of subgroups of G to the set of subextensions of E/F,

$$\{\text{subgroups } H \text{ of } G\} \leftrightarrow \{\text{subextensions } F \subset M \subset E\}$$

with inverse $M \mapsto \mathrm{Gal}(E/M)$. Moreover, we have

- $H_1 \supset H_2 \Leftrightarrow E^{H_1} \subset E^{H_2}$
- $(H_1 : H_2) = [E^{H_2} : E^{H_1}]$
- $\sigma H \sigma^{-1} \leftrightarrow \sigma M$, i.e.

$$E^{\sigma H \sigma^{-1}} = \sigma(E^H), \quad \mathrm{Gal}(E/\sigma M) = \sigma \mathrm{Gal}(E/M)\sigma^{-1}$$

- H is normal in $G \Leftrightarrow E^H$ is normal over F, in which case $\mathrm{Gal}(E^H/F) \cong G/H$.

Proof.

Let H a subgroup of G, then we know $\mathrm{Gal}(E/E^H) = H$ and if M/F a subextension, then E is Galois over M and $E^{\mathrm{Gal(E/M)}} = M$ and hence they are inverse maps.

(a) $H_1 \supset H_2$ implies $E^{H_1} \subset E^{H_2}$ implies $\mathrm{Gal}(E/E^{H_1}) \supset \mathrm{Gal}(E/E^{H_2})$ and hence $H_1 \supset H_2$.

(b) For H subgroup, we know $|\mathrm{Gal}(E/E^H)| = [E : E^H]$ and hence the conclusion is true for $H_2 = 1$. For general we know $(H_1 : 1) = (H_1 : H_2)(H_2 : 1)$ and $[E : E^{H_1}] = [E : E^{H_2}][E^{H_2} : E^{H_1}]$ and we are done.

(c)For $\tau \in G, \alpha \in E$, $\tau\alpha = \alpha \Leftrightarrow \sigma\tau^{-1}\sigma\alpha = \sigma\alpha$ and hence τ fixes M iff $\sigma\tau\sigma^{-1}$ fixed σM and so $\mathrm{Gal}(E/\sigma M) = \sigma \mathrm{Gal}(E/M)\sigma^{-1}$ and hence $E^{\sigma H \sigma^{-1}} = \sigma E^H$ and use the theorem 3.8.

(d) Assume H normal, then we know $\sigma E^H = E^H$ for all $\sigma \in G$ and hence consider $\sigma \mapsto \sigma|_{E^H} : G \to \mathrm{Aut}(E^H/F)$ whose kernel is H and notice $(E^H)^{\mathrm{Aut}(E^H/F)} = F$ and hence E^H is Galois oevr F since $\mathrm{Aut}(E^H/F) \cong G/H$ and we are done.

Suppose M normal and $\alpha_1. \cdots, \alpha_m$ generate M over F. For $\sigma \in G$, $\sigma\alpha_i$ is a root of the minimal polynomial of α_i over F and hence in M, which means $\sigma M = M$ and this implies that $\sigma H \sigma^{-1} = H$ and we are done.

Proposition 2.3.13. Let E and L be extensions of F contained in some common field. If E/F is Galois, then EL/L and $E/E \cap L$ are Galois and the map

$$\sigma \mapsto \sigma|_E : \mathrm{Gal}(EL/L) \to \mathrm{Gal}(E/E \cap L)$$

is an isomorphism.

Proof.

If E is Galois over F, it is the splitting field of a separable polynomial $f \in F[X] \subset L[X]$ and hence EL is the splitting field of f and E is Galois over $E \cap L$ by $F \subset E \cap L$. Every automorphism σ of EL fixing the elements of L maps roots of f to roots of f and hence $\sigma E = E$ and hence $\sigma \mapsto \sigma E : \mathrm{Gal}(EL/L) \to \mathrm{Gal}(E/E \cap L)$.

If $\sigma \in \mathrm{Gal}(EL/L)$ fiexes the elements of E, then it fixes the elements of EL and hence $\sigma \mapsto \sigma|_E$ is injective. If $\alpha \in E$ is fixed by all $\sigma \in \mathrm{Gal}(EL/L)$, then $\alpha \in E \cap L$ and hence $\sigma \mapsto \sigma|_E$ is surjective.

Corollary 2.3.14. Suppose that L is finite over F. Then

$$[EL : F] = \frac{[E : F][L : F]}{[E \cap L : F]}$$

Proof.

We have

$$[EL : F] = [EL : L][L : F] = [E : E \cap L][L : F] = \frac{[E : F][L : F]}{[E \cap L : F]}$$

Proposition 2.3.15. Let E_1 and E_2 be extensions of F contained in some common field. If E_1 and E_2 are Galois over F, then E_1E_2 and $E_1 \cap E_2$ are Galois over F and the map

$$\sigma \mapsto (\sigma|_{E_1}, \sigma|_{E_2}) : \mathrm{Gal}(E_1E_2/F) \to \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F)$$

is an isomorphism of $\mathrm{Gal}(E_1E_2/F)$ onto the subgroup $H = \{(\sigma_1, \sigma_2) | \sigma|_{E_1 \cap E_2} = \sigma_2|_{E_1 \cap E_2}\}$ of $\mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F)$

Proof.

Let $a \in E_1 \cap E_2$ and f its minimal polynomial over F. Then f has $\deg f$ distinct roots in E_1 and also in E_2, since it can have at most f roots in E_1E_2 and the roots have to be in $E_1 \cap E_2$, which means $E_1 \cap E_2$ is normal separable and hence Galois. Also E_1E_2 is a splitting fields for some polynomial in $F[X]$ by E_1, E_2. The map $\sigma \mapsto (\sigma|_{E_1}, \sigma)$ is obviously injective, and its image is in H.

We know

$$\mathrm{Gal}(E_2/F)/\mathrm{Gal}(E_2/E_1 \cap E_2) \cong \mathrm{Gal}(E_1 \cap E_2/F)$$

and so, for $\sigma_1 \in \mathrm{Gal}(E_1/F)$, $\sigma_1|_{E_1 \cap E_2}$ has exactly $[E_2 : E_1 \cap E_2]$ to an element of $\mathrm{Gal}(E_2/F)$ and hence

$$|H| = [E_1 : F][E_2 : E_1 \cap E_2] = \frac{[E_1 : F][E_2 : F]}{[E_1 \cap E_2 : F]} = [E_1E_2 : F]$$

Definiton 2.3.8. (Galois Group of a Polynomial)

If a polynomial $f \in F[X]$ is separable, then its splitting field F_f is Galois over F and we call $\mathrm{Gal}(F_f/F)$ the Galois group G_f of f.

Proposition 2.3.16. For a separable polynomial $f \in F[X]$, we have $[F_f] | (\deg f)!$.

Proof.

We know G_f is consisted by the permutations σ of the roots of f such that for $P \in F[X_1, \cdots, X_{\deg f}]$, $P(\alpha_1, \cdots, \alpha_{\deg f}) = 0$ implies that $P(\sigma\alpha_1, \cdots, \sigma\alpha_{\deg f}) = 0$ because of the dimension and we are done.