Notes on Serge Lang's Algebra

Amanuel Tewodros

October 4, 2025

Contents

Chapter 1

Groups

Theorem 1 (Sylow Theorems)**.** *Let G be a finite group with p divides $|G|$, where p is a prime. Then*

1. *There exists a Sylow p-subgroup of G.*
2. *The number of Sylow p-subgroups of G is congruent to 1 modulo p and divides $|G|$.*
3. *All Sylow p-subgroups of G are conjugate.*

Proof. If $H \leq G$ with $[G : H]$ coprime with p, then by induction H and therefore G contains a Sylow p-group. Otherwise, by the class equation,

$$|G| = |Z(G)| + \sum_x [G : N_x(G)],$$

it follows $Z(G)$ is divisible by p and thus $\langle g \rangle \leq Z(G)$ for some $g \in Z(G)$ with exponenet = p. Inducting on the order of G, $G/\langle g \rangle$ contains a Sylow p-subgroup, say $S/\langle g \rangle$ that is the image of $S \leq G$ that is a Sylow p-subgroup of G.

Let $P, Q \in \mathrm{Syl}_p(G)$. P does not normalize Q because otherwise $PQ \leq G$ and $p^m = |PQ| > |P|$, a contradiction. Let $S = \{P_1, \ldots, P_k\}$ be the conjugates of P and let $\mathcal{O}_i$ be the orbit of P_i by the action P on the set S by conjugation. Then $|\mathcal{O}_i| = [P : N_P(P_i)] = [P : N_G(P_i) \cap P] = [P : P_i \cap P] \implies k = 1 \mod p$.

If $P, Q \in \mathrm{Syl}_p(G)$ are not conjugates, then Q is not conjugate with conjugates of P. Consider the action of the elements of Q on the set $\{gPg^{-1} : g \in G\} = \{P_1, \ldots, P_m\}$. Then

$$|\mathcal{O}_{P_i}| = [Q : N_Q(P_i)] = [Q : P_i \cap Q],$$

where the latter equality follows because $P_i(N_G(P_i) \cap Q)$ is a p-group that contains P_i with order $\leq |P_i|$(a Sylow p-group) and thus $N_G(P_i) \cap Q \leq P_i$. Since Q is not a conjugate of P, $[Q : Q \cap P_i] = p^k, k > 0$ and $\mathcal{O}_{P_i}$ is divisible by p and the number of conjugates of P which is $\sum_i |\mathcal{O}_{P_i}| = 0 \mod p$, a contradiction. $\square$

Theorem 2. *If $|G| = pq$ for primes $p < q$, then $G = \mathbb{Z}/pq\mathbb{Z}$ if $p \nmid q - 1$ else $G = \mathbb{Z}/pq\mathbb{Z}$ of $G = \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ for some non-trvial semi-direct product.*

Proof. If $q > p$, $n_q = 1$ and thus $Q \in \mathrm{Syl}_q(G)$ is normal. $|\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})| = q-1$, therefore, there is a nontrivial map $\phi : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ if $p \mid q-1$ $\square$

Theorem 3 (Fundamental Theorem of Finitely Generated Abelian Groups)**.** *Let A be a finite abelian group and let $A(p)$ be the subgroup of all elements with order that is a power of p. Then*

$$\prod_{A(p)\neq\{1\}} A(p) = A.$$

Proof. Clearly the map $\phi : \prod_p A(p) \to A$ defined by $\phi((x_p)) = \prod_p x_p$ is an endomorphism. We show that ϕ is injective and surjective. Let $\phi((x_p)) = 1$ for some $x = (x_p) \in \prod_p A(p)$. Let q be a prime with $A(q) \neq \{1\}$. Then

$$x_q = \prod_{p\neq q} x_p^{-1}.$$

Let m be the least common multiple of the primes powers on the right hand side, i.e. powers of $p \neq q$. Then $x_q^m = 1$. But, $x_q^{q^r} = 1$ too. Consequently, $x_q^{(m,q^r)} = x_q^1 = x_q = 1$. Thus $\prod_p x_p = 1$ iff all $x_p = 1$ and $\ker\phi = \{1\}$.

To prove surjectivity, let $x \in A$ with $x^m = 1$ such that $m = \prod p_i^{r_i}$. By Euclidean algorithm, $1 = \sum_i u_i \prod_{j\neq i} p_j^{r_j}$ and thus $x = \prod_i x^{u_i \prod_{j\neq i} p_j^{r_j}}$ with $x^{u_i \prod_{j\neq i} p_j^{r_j}} \in A(p_i)$. $\square$

Why nilpotence and the existence of normal Sylow sub-groups are equivalent?: If $P, Q \in \mathrm{Syl}_p(G)$ then $N_P(Q) = P \cap Q < P, Q$ and thus $Z(G)$ is always $< G$. Thus $P = Q \iff G$ nilpotent.

The number of ways G acts on H: = # of homomorphisms from G to $\mathrm{Aut}(H)$ = # subgroups of order $|G|/|H^*|$.

Theorem 4. *If $n \geq 5$ then S_n is not solvable.*

Proof. Let S_n decompose as $S_n = H_m \supset \cdots \supset H_0 = \{1\}$. Clearly, S_n contains all 3-cycles. We also know since H_n/H_{n-1} is abelian $(abc)(ade)(acb)(aed) = (adebc)(aedcb) = (abd) \in H_{m-1}$. By induction all 3 cycles are in $\{1\}$, a contradiction. $\square$

Theorem 5. *A_n is simple for all $n \geq 5$.*

A priori: A_n can be generated by 3-cycles and 3-cycles are conjugates.

Proof. Let $N \trianglelefteq A_n$. Let $\sigma \in N$. We show that σ is a 3-cycle or $\sigma = \mathrm{id}$. The former implies $N = A_n$ and the latter implies N is the trivial subgroup. Let σ have the maximal number of fixed points in N.

Lrt all σ's orbits have size 2 and it does not fix elements i, j. If σ is (ijk) for some k, we are done. Otherwise, $\langle\sigma\rangle > \langle(ij)(rs)\rangle$ for some r, s because σ is an even permutation and not a 3-cycle. Let $\tau = (rsk)$ for some k. Then $\tau' = \tau\sigma\tau^{-1}\sigma^{-1} \in N$. But $\tau' = (i,j)\sigma$ contradicting σ fixes the maximal number of points. Thus at least one σ's orbit has more than 2 elements.

Therefore, $\sigma = (ijk)(rs)\theta$ where θ is possible identity permutation. By similar argumenta as above picking $\tau' = (rsk)$, σ can not be the element of N with maximal fixed points unless it contains all of A_n. $\square$

Properties of Common Non-Abelian Groups

- *Dihedral Group*: D_{2n}
  - $\cong \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ acting by inversion
  - $= \{a, b | a^n, b^2, baba\}$
- *Binary Dihedral Group/ Dicyclic Group*: $\mathrm{DiC}(4n)$
  - $\cong \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ acting by inversion
  - $= \{a, b | a^n, b^4, baba\}$
- *Generalized Quaternions*: $Q_{2^{n+2}}$
  - $\cong \mathbb{Z}/2^n\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ acting by inversion
  - $= \{a, b | a^{2^n}, b^4, baba\}$
- *Holomorph Group*: $\mathrm{Hol}(G)$
  - $\cong G \rtimes \mathrm{Aut}(G)$
  - if G is $\mathbb{Z}/p\mathbb{Z}$, p prime, $\mathrm{Hol}(G)$ is isomorphic to the *generalized affine group*

Notes on Category Theory

- A category $\mathcal{C}$ is a collection of **objects** $\mathrm{Ob}(\mathcal{C})$, along with a set of maps, called **morphisms** between any two objects $A, B \in \mathrm{Ob}(\mathcal{C})$ denoted by $\mathrm{Mor}(A, B)$.
- Morphisms follow the law of composition.
- Three axioms
  1. **CAT 1** $\mathrm{Mor}(A, B)$ and $\mathrm{Mor}(A', B')$ are disjoint unless $(A, B) = (A', B')$, in which case they are equal.
  2. **CAT 2** For every $A \in \mathrm{Ob}(\mathcal{C})$, there exists a morphism, id_A in $\mathrm{Mor}(A, A)$ that acts as a left and right identity for the elements of $\mathrm{Mor}(A, B)$ and $\mathrm{Mor}(B, A)$ resp. for all B.
  3. **CAT 3** The law of composition of morphisms is associative.
- The **operation** of a group G on an object $A \in \mathrm{Ob}(\mathcal{C})$ is a homomorphism from G to $\mathrm{Aut}(A)$. It is also called a **representation.**

- Given a category $\mathcal{C}$, we can construct a new category $\mathcal{D}$ where the objects are the morphisms of $\mathcal{C}$ and the morphisms between two objects f, f' are defined by a pair of momorphism (ϕ, ψ) that make the following diagram commute:

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\phi"'] & B \arrow[d, "\psi"] \\ A' \arrow[r, "f'"'] & B' \end{tikzcd}$$

- An object P of a category $\mathcal{C}$ is called **universally attracting** (resp. **universally repelling**) if there is exists a *unique* morphism from (resp. to) every object to(resp. from) P. If it is both, it is called **universal object**.

Chapter 2

Rings

Proposition 6. *For two ideals $\mathfrak{a}, \mathfrak{b}$ of a ring A, if $\mathfrak{a} + \mathfrak{b} = A$, then $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$.*

Proof. Clearly, $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$. Thus, it suffices to prove the contra-positive relation. Since $1 = a + b$ for some $a \in \mathfrak{a}, b \in \mathfrak{b}$, $c = c \cdot a + c \cdot b$ for all $c \in A$. Of course, if $c \in \mathfrak{a} \cap \mathfrak{b}$, $c \cdot a + c \cdot b \in \mathfrak{a}\mathfrak{b}$. □

Let A be a ring and let $\lambda : \mathbb{Z} \to A$ given by

$$\lambda(n) = \underbrace{1_A + \cdots + 1_A}_{n \text{ times}}.$$

Then $\ker \lambda = \langle n \rangle$ for some $n \geq 0$. If $\langle n \rangle$ is a prime ideal, then we say A has characteristic n.

Proposition 7. *If S is a set with more than two elements and A is a ring with $1_A \neq 0_A$, then $\mathrm{Map}(S, A)$ is not an integral domain.*

Proof. Let $\{\} \neq T \subset S$

$$f(x) = \begin{cases} 1_A \text{ if } x \in T \\ 0_A \text{ if } x \in S - T \end{cases} \qquad \text{and } g(x) = 1_A - f(x).$$

$fg = 0_{\mathrm{Map}(S,A)}$. □

If $\mathfrak{p}$ is a prime ideal in a ring A, then it means

1. $A/\mathfrak{p}$ is an integral domain.

2. $xy \in \mathfrak{p} \implies x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

The ideal $\{0_A\}$ is a prime ideal of A iff A is an integral domain.

Proof. ($\implies$) $A/\{0_A\} \cong A$, thus A should be an integral domain.

($\impliedby$). If A is an integral domain, then $xy \in \{0_A\} \implies x = \{0_A\}$ or $y \in \{0_A\}$. □

Theorem 8 (Chinese Remainder Theorem). *Let $\mathfrak{a}_1, \dots \mathfrak{a}_n$ be ideals of a ring A such that $\mathfrak{a}_i + \mathfrak{a}_j = A$ for any $i \neq j$. Let x_i be elements of A. Then there is an element $x \in A$ such that $x \equiv x_i \mod \mathfrak{a}_i$.*

Proof. If $n = 2$, $A = \mathfrak{a}_1 + \mathfrak{a}_2$, and thus $1_A = a_1 + a_2$ for some $a_i \in \mathfrak{a}_i$. Then $x = x_1 a_1 + x_2 a_2$ satisfies the statement.

If $n > 2$, then $a_i + b_i = 1_A$ for some $a_i \in \mathfrak{a}_1$ and $b_i \in \mathfrak{a}_{j>1}$. Thus the product $\prod_i (a_i + b_i) = 1_A$. In other words,

$$A = \mathfrak{a}_1 + \prod_{i=2}^{n} \mathfrak{a}_i.$$

By the case for $n = 2$, there is an element y_1 such that,

$$y_1 \equiv 1_A \mod \mathfrak{a}_1 \text{ and } y_1 \equiv 0_A \mod \Big(\prod_{i=2}^{n} \mathfrak{a}_i\Big)$$

Since $\prod_{i=2}^{n} \mathfrak{a}_i \subseteq \bigcap_{i=2}^{n} \mathfrak{a}_i$, it follows that $y_1 \in \mathfrak{a}_i$ for all $i > 1$ and therefore, $y \equiv 0_A \mod \mathfrak{a}_i$ for $i > 1$. Carrying out the same procedure in similar fashion to obtain $y_2, \dots, y_n$ such that

$$y_i \equiv 1_A \mod \mathfrak{a}_i \text{ and } y_i \equiv 0_A \mod \mathfrak{a}_j, j \neq i,$$

we see that $x = \sum_{i=1}^{n} x_i y_i$ satisfies the statement of the theorem. □

A non-zero polynomial f of degree d over a commutitive ring A is homogenous iff for every set of $n+1$ algebraically independent elements $u, t_1, \dots, t_n$ over A,

$$f(ut_1, \dots, ut_n) = u^d f(t_1, \dots, t_n).$$

Proof. Let $f(X) = \sum_{(v)} a_{(v)} X_1^{v_1} \cdots X_n^{v_n}$. If f is homogenous of degree d, $v_1 + \cdots + v_n = d$ for all $a_{(v)} \neq 0$. $f(ut_1, \dots, ut_n) = \sum_{(v)} a_{(v)} (ut_1)^{v_1} \cdots (ut_n)^{v_n}$. Since A is commutitive, this is equal to $\sum_{(v)} a_{(v)} u^{v_1 + \cdots + v_n} t_1^{v_1} \cdots t_n^{v_n}$.

On the other hand, if $f(ut_1, \dots, ut_n) = u^d f(t_1, \dots, t_n)$m, then $\sum_{(v)} a_{(v)} u^{v_1 + \cdots + v_n} = f(u1_A, \dots, u1_A) = u^d f(1_A, \dots, 1_A) = u^d \sum_{(v)} a_{(v)}$. This is a polynomial in u over A and equality is assured iff $u^d = u^{v_1 + \cdots v_n}$.

□

Let G be a monid and let $A[G]$ be the set of all mappings $\alpha : G \to A$ such that $\alpha(x) = 0$ for almost all $x \in G$. Addition is defined ordinarily and multiplication is defined as

$$\alpha\beta(z) = \sum_{xy=z} \alpha(x)\beta(y).$$

Then $A[G]$ is a ring. A more convenient notation can be acheived if we define $a \cdot x$ as

$$a \cdot x(z) = \begin{cases} a \text{ if } z = x \\ 0 \text{ if otherwise.} \end{cases}$$

This way we can define, $\alpha = \sum_{x \in G} \alpha(x) \cdot x$, and

$$\left(\sum_{x \in G} a_x \cdot x\right)\left(\sum_{y \in G} b_y \cdot y\right) = \left(\sum_{x,y} a_x b_y \cdot xy\right)$$

$$\left(\sum_{x \in G} a_x \cdot x\right) + \left(\sum_{x \in G} b_x \cdot y\right) = \left(\sum_{x \in G} (a_x + b_x) \cdot x\right),$$

where $\{a_z\}_{z \in G}$, $\{b_z\}_{z \in G}$ are the elements of A, most of them equal to 0.

The injective homomorphisms $x \mapsto 1_A \cdot x$ and $a \mapsto a \cdot e$ show that G and A are embedded in $A[G]$.

Let A be a communtative ring and S be a multiplicative subset [1]. *For $a, a' \in A$ and $s, s' \in S$, we say*

$$(a, s) \sim (a', s')$$

if there is $s_1 \in S$ such that

$$s_1(as' - sa') = 0.$$

$\sim$ is an equivalance relation.

Proof. Symmetry and Reflexitvness are trivial. Transitivity can be verified as follows. Let $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then for some $s_1, s_2 \in S$, we have

$$s_1 ad = s_1 bc$$

$$s_2 de = s_2 cf$$

Multiplying both sides of first and the second equation by $s_2 f$ and $s_1 b$, it follows that $(s_1 s_2 d)(af - be) = 0$. $\square$

This construction of ring is called **ring of fraction of A by S**, $S^{-1}A$. The homomorphism $A \mapsto S^{-1}A$ defined by $a \mapsto a/1_A$ is a universal object (See 1). If A is an integral domain, then $S^{-1}A$ is the field of fractions.

If A has a unique maximal ideal, it is called **a local ring.** An intersting example is $A_\mathfrak{p} = S^{-1}A$,where S is the multiplicative subset $A - \mathfrak{p}$.

Principal Ideal Domains and Unique Factorization

Let A be an prinicipal integral domain. We say a divides b if $b = ac$ for some $c \in A$

Definition 9. d is called the greatest common divisor of a and b if and only if $c|a$ and $c|b \implies c|d$.

Proposition 10. *If $d = \gcd(a, b)$, then $ar + bs = d$ for some $r, s \in A$.*

[1] A subset containting 1_A and closed under multiplication

Proof. Let $a = dx$ and $b = dy$. Because d is a gcd of a and b, for $c \notin A^*$ $c \mid x \implies c \nmid y$ and vice versa, thus $\gcd(x, y)$ is a unit in A.

Now, $A \subseteqq \langle x, y \rangle$. To show that, let $\langle z \rangle = \langle x, y \rangle$. Since $x, y \in \langle x, y \rangle$, $x = w_1 z$ and $y = w_2 z$. But then z should be a unit in A and thus $1_A \in \langle x, y \rangle$. The proposition follows directly. $\square$

The proof also shows if $\langle a, b \rangle = \langle c \rangle$, then $c = \gcd(a, b)$.

Definition 11. We call $p \in A$ **irreducible** if $p = ab$ for some $a, b \in A$, then $\{a, b\} \cap A^* \neq \emptyset$. If $c \in A$ can be written as a product of a unit in A and a product of some irreducibles in A, we call the product **a factorization** of c. If every non-zero element of A has a unique factorization (upto commutitivity) we call A a **unique factorization domain (UFD)** or **factorial ring**.

Theorem 12. *If A is a principal ideal domain, then A is a UFD.*

Proof. Existence: Let S be the set of ideals of A generated by elements a_i that don't have factorization. Let $S \neq \emptyset$. Then $\langle a_1 \rangle \in S$.. Consider the chain,

$$\langle a_1 \rangle \subsetneqq \langle a_2 \rangle \subsetneqq \cdots \subsetneqq \langle a_n \rangle \subsetneqq \cdots$$

Because, A is a principal ideal domain $\cup_i \langle a_i \rangle = \langle a \rangle$ for some $a \in A$. However, $\langle a_i \rangle \subset \langle a_{i+1} \rangle$, $a \in \langle a_n \rangle$ for some n and the chain is finite. Thus if $\langle a \rangle \subsetneqq \langle b \rangle$, then b admits factorization.

Remark 13. The fact that A is a principal ideal domain is important in constructing the chain. Consider the following chain if $A = \mathbb{Q}$, for example

$$\langle 1/2 \rangle \subsetneqq \langle 1/4 \rangle \subsetneqq \cdots \subsetneqq \langle 1/2^n \rangle \subsetneqq \cdots$$

The union of these ideals = $\mathbb{Q}$ which is not a principal ideal.

Now, consider a. Clearly, a is not an irreducible. Thus Assume $a = bc$. But $\langle a \rangle \subsetneqq \langle b \rangle$. Thus b (and also c) admits factorization and by induction a does making S empty.

Uniqueness First, we prove that irreducibility implies primality. Let p be irreducible and let $p \mid ab$. If $p \nmid a$ then $\gcd(a, p) = 1_A$ and $1_A = ax + py \implies b = abx + pby = p(c'x + by)$ for some c.

If

$$a = up_1 \cdots p_r = vq_1 \cdots q_s,$$

$p_1 \mid q_1 \cdots q_s$ and WLOG, $q_1 = u_1 p_1$. Thus $up_2 \cdots p_r = vu_1 q_2 \cdots q_s$. The argument completes by induction. $\square$

Chapter 3

Modules

The concept of rings is motivated by the properties of a set of *endomorphims* on an (additive) abelian group. Left R-modules are the abelian groups M such thaat there is a ring homomorphism $R \to \text{End}(M)$.

Example: If J is an ideal of a ring A, then we can define an operation of an element $a, b \in A$ on A/J as $a \cdot (x + J) \mapsto ax + J$. This mapping is an endomorphim of A/J because $a \cdot (x + y + J) = a \cdot (x + J) + a \cdot (y + J)$. We can define the a ring homomorphism from $A \to \text{End}(A/J)$ trivially. Therefore, A defines a module structure over A/J.

To show a group M is A-module, it suffieces to show that for $a, b \in A$, $x, y \in M$

$$a(x + y) = ax + ay \text{ and } (a + b)x = ax + by,$$

These conditions are equivalent to showing there is a ring homomorphism from the actions of elements of A on M to $\text{End}(M)$.

Some basic constructions from the companion. Let M be an A-module.

1. For $N \subseteqq M$, $\{r \in A : rN = 0\}$ forms an left ideal in A.
2. For $N \leqq M$, $\{r \in A : rM \subseteqq N\}$ forms a right ideal of A.
3. For $N \leqq M$, $\{r \in A : rN \subseteqq N\}$ forms a subring.
4. If N is a submodule, then the ideals in 1 and 2 are 2-sided. Here, it is important to point out that when N is a submodule, then closure of the actions of A on N is maintained.

If $x \in M$, then $Rx \cong R/I$, where I is the annhilator ideal of $\{x\}$ as in 1.

Every ideal (left, right and 2-sided) and subring of A can be constructed in the above way

---

Definition 14. A **module-homomorphism** is an additive group homomorphism $f : M \to M'$ from modules M to module M' and such that $f(ax) = af(x)$.

If f is module-homomorphism from M to M' then the kernel and the image of f are submodules of M and M' respectively.

Proof. Clearly, $\ker f \leqq M$ because f is a group homomorphism. Let $a \in A$ and $x \in \ker f$. $f(ax) = af(x) = 0$. Hence, the kernel of f is a submodule of M.

Again, $\operatorname{Im} f \leqq M'$. $af(x) = f(ax) \in \operatorname{Im} f$.

□

$M'/f(M)$ is a universal(inital) among the modules N with homomorphism $g : M' \to N$ such that $g \circ f = 0$. That is the following diagram commutes and $\hat{g}$ is unique:

$$\begin{tikzcd} M \arrow[r, "f"] & M' \arrow[r, "g"] \arrow[d, "c"] & N \\ & M'/f(M) \arrow[ur, "\hat{g}"] & \end{tikzcd}$$

This is dual with the kernel of f which is a terminal object among modules N with homomorphism $g : N \to M$ such that $f \circ g = 0$. Thus, it is called the **cokernel** of f.

Definition 15. A **monomorphism** is a module-homomorphism $u : N \to M$ characterized by the exact sequence $0 \to N \xrightarrow{u} M$. Similarly, an **epimorphism** is characterized by dual exact sequence $N \xrightarrow{u} M \to 0$.

These definitions concide with the definitions of one-to-one homomorphisms and surjective homomorphism in the category of modules over a ring R.

Definition 16. For a commutitive[1] ring A, we say K is an A-algebra, if K is a module with E a **A-bilinear map** $g : E \times E \to E$.

In the companion, the following remark is left.

Let A be a commutative ring. Then

associative, unital A-algebra $R \equiv$ Ring R with a homomorphism $f : A \to Z(R)$.

[1]the concept of algebras does not make much sense with non-commutative rings

f is a way of endcoding the bilinear operator, and why it's into the center of R is mainly because we require $a \cdot xy = (a \cdot x)y = x(a \cdot y) := f(a)xy = (f(a)x)y = xf(a)y$

Another intersting remark is that algebras are abstractions of the natural structure of A-module-endomorphims of a module M, $\mathrm{End}_A(M)$, just like rings abstract the endomorphims of an abelian group.

A sequence $\cdots \to A \xrightarrow{f} B \xrightarrow{g} C \to \cdots$ is called exact if $\mathrm{Im}\, f = \ker g$. We denote the group of of A-homomorphisms from A-module X to Y by $\mathrm{Hom}_A(X, Y)$.

Proposition 17. *Let X, X', X'' and Y be A-modules. Then the short sequence*

$$X' \xrightarrow{\lambda} X \xrightarrow{\mu} X'' \to 0$$

is exact if and only if

$$\mathrm{Hom}_A(X', Y) \xleftarrow{\lambda'} \mathrm{Hom}_A(X, Y) \xleftarrow{\mu'} \mathrm{Hom}_A(X'', Y) \leftarrow 0$$

is exact for all Y.

Remark 18. This proposition is analogous to the duality of linear maps in vector spaces.

Proof. Suppose the first sequence is exact. Then the following statements hold:

(i) $\mathrm{Im}\, \lambda = \ker \mu$

(ii) $\mathrm{Im}\, \mu = X''$.

Let $g \mapsto g \circ \lambda = 0$. Since $\mathrm{Im}\, \lambda \subseteqq \ker g$, g factors through $X/\mathrm{Im}\, \lambda$. By i and ii, $X/\mathrm{Im}\, \lambda \cong \mathrm{Im}\, \mu = X''$ which implies $g = f \circ \mu$ for some $f \in \mathrm{Hom}(X'', Y)$. This shows $\ker \lambda' \subseteqq \mathrm{Im}\, \mu'$. Similarly, let $h \circ \mu \in \mathrm{Im}\, \mu'$. By i, the composition of this with λ, $h \circ \mu \circ \lambda = 0$, implying $\mathrm{Im}\, \mu' \subseteqq \ker \lambda'$ (thus $\mathrm{Im}\, \mu' = \ker \lambda'$). The first implication of the proposition follows from the fact that if $f \mapsto f \circ \mu = 0$ for some $f : X'' \to Y$, then $f = 0$ by ii.

The proof of the converse is an easy application of the following common technique: **To study the consequences of a condition holding for all morphisms of a given sort, consider a universal example.**

Suppose the second sequence is exact, i.e.,

(i) $\ker \lambda' = \mathrm{Im}\, \mu'$

(ii) $\ker \mu' = 0$.

By i, $\ker \lambda' \supseteqq \mathrm{Im}\, \mu'$. That is, for every Y and $f : X'' \to Y$ $f \circ \mu \circ \lambda = 0$. Now, consider the universal example for all fs, i.e., the category of morphisms from X'' which is id, the identity morphisms. $\mathrm{id} \circ \mu \circ \lambda = \mu \circ \lambda = 0$ implies $\ker \mu \supseteqq \mathrm{Im}\, \lambda$.

Similarly, the condition $\ker \lambda' \subseteqq \mathrm{Im}\, \mu'$ implies for every Y, a map $g : X \to Y$ such that $g \circ \lambda = 0$ can be factored through X''. The universal object of all morphisms from

$X \to Y$ which are 0 at $\mathrm{Im}\,\lambda$ is the canonical homomorphism $q : X \to X/\mathrm{Im}\,\lambda$. Hence $q = f \circ \mu$ which is obviously 0 on $\mathrm{Im}\,\lambda$ and thus $\ker q = \mathrm{Im}\,\lambda \supseteqq \ker \mu$.

Finally, the universal object of morphisms from $X'' \to Y$ annihilated by $\mathrm{Im}\,\mu$ is the canonical morphism $p : X'' \to X''/\mathrm{Im}\,\mu$. However, ii implies $p = 0$ and $X'' \cong \mathrm{Im}\,\mu$ which completes the proof. $\square$

Let $\{M\}_{i\in I}$ be a family of submodules of M. Then we have the induced homomorphism

$$\lambda_* : \bigoplus_{i\in I} M_i \to M$$

defind by $\lambda_*((x_i)) = \sum x_i$. If λ_* is isomporphism, then we call the family $\{M\}_{i\in I}$, **direct sum decomposition** of M as we have

$$\bigoplus M_i = M.$$

Otherwise, if λ_* is only surjective, we can write

$$M = \sum M_i$$

Remark 19. This notion is analogous to linear independece and direct sums in linear algebra.

Let M_1, M_2, N be modules. Then we have the following isomorphism of abelian groups

$$\mathrm{Hom}(M_1 \oplus M_2, N) \cong \mathrm{Hom}(M_1, N) \times \mathrm{Hom}(M_2, N)$$
$$\mathrm{Hom}(N, M_1 \times M_2) \cong \mathrm{Hom}(N, M_1) \times \mathrm{Hom}(N, M_2)$$

The first isomorphism follows from the association $f \mapsto (f_1, f_2)$ where f is an element of the LHS group and $f_i : M_i \to N$ are the homomorphisms defined by $f_i = f \circ I_i$. The second one follows with similar associations.

Proposition 20. *Let the following sequence of modules be exact:*

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

The following conditions are equivalent

1. *There is a homomorphism $\varphi : M'' \to M$ such that $id = g \circ \varphi$.*

2. *There is a homomorphism $\psi : M \to M'$ such that $id = \psi \circ f$.*

If these conditions are satisfied, then we have the following isomporphisms:

$$M = \ker g \oplus \mathrm{Im}\,\varphi = \ker \psi \oplus \mathrm{Im}\,f \cong M' \oplus M''.$$

The general idea is the exactness of the sequence makes M factorize into $M' \times M/M'$ in group theory terms.

Proof. Let $x \in M$. Then $x - \varphi(g(x)) \in \ker g$ by definition. Thus $x = (x - \varphi(g(x))) + \varphi(g(x)) \in \ker g + \operatorname{Im} \varphi$. This sum is direct because $\ker g \cap \operatorname{Im} \varphi = 0$. The others isomorphisms follow immediately. □

Definition 21. A **free module** is an A-module that admits a basis.

Proposition 22. *Let M be a free module with basis $\{x_i\}_{i \in I}$ and let $\mathfrak{a}$ be a two-sided ideal of A. Then*

1. *$\mathfrak{a}M$ is also a submodule of M that is also $\mathfrak{a}$-module.*

2. *Each $\mathfrak{a}x_i$ a submodule of Ax_i.*

3. *We have the module isomorphism*

$$M/\mathfrak{a}M \cong \bigoplus_{i \in I} Ax_i/\mathfrak{a}x_i.$$

4. *$Ax_i/\mathfrak{a}x_i$ is isomorphic to $A/\mathfrak{a}$ as A-module*

5. *Suppose A is commutative. Then $A/\mathfrak{a}$ is a ring. Furthermore $M/\mathfrak{a}M$ is a free over $A/\mathfrak{a}$ and $Ax_i/\mathfrak{a}x_i$ is a free over $A/\mathfrak{a}$. If $\overline{x_i}$ is the image of x_i under the canonical homomorphism $Ax_i \to Ax_i/\mathfrak{a}x_i$, then $\overline{x_i}$ is the basis of $Ax_i/\mathfrak{a}x_i$.*

Proof. We go through the statements one by one:

1. Let $x \in M$. Then $x = \sum_{i \in I} a_i x_i$ uniquely for $\{a_i\}_{i \in I} \subseteqq A$. By definition, $\mathfrak{a}M = \{\sum yx : y \in \mathfrak{a}, x \in M\}$. But $yx = \sum_i y a_i x_i = \sum_i y_i x_i \in M$ where $y_i \in \mathfrak{a}$ because $\mathfrak{a}$ is two-sided ideal.

2. Clearly, $\mathfrak{a}x_i \subseteqq Ax_i$. Let $a', b' \in \mathfrak{a}$ and $a, b, c \in A$. Ax_i is a A-module because $(a+b)cx_i = (ac+bc)x_i = acx_i + bcx_i$ and $c(a'x_i + b'x_i) = c(a+b)x_i = (ca+cb)x_i = cax_i + cbx_i$. The statement follows from $A\mathfrak{a}x_i \subseteqq \mathfrak{a}x_i$

3. By definition, $M = \bigoplus_{i \in I} Ax_i$. Consider the isomprohism

$$\sum_{i \in I} a_i x_i \mapsto (a_i x_i)_{i \in I}$$

   which induces the isomorphism

$$\sum_{i \in I} a_i x_i + \mathfrak{a}M \mapsto (a_i x_i + \mathfrak{a}M)_{i \in I}.$$

   Since $\mathfrak{a}M$ is a $\mathfrak{a}$-module and $a_i x_i + \mathfrak{a}M = a_i x_i + \mathfrak{a}x_i$, and $Ax_i/\mathfrak{a}x_i$ is an $A/\mathfrak{a}$-module, the statement is true.

4. Consider the isomoprhism $1_A \mapsto x_i$.

5. $A/\mathfrak{a}$ is a ring of cosets of $\mathfrak{a}$. $M/\mathfrak{a}M$ is free as the basis $\{x_i\}_{i \in I}$, serves as a basis for $M/\mathfrak{a}M$ over $A/\mathfrak{a}$.

□

We say an exact sequence of abelian groups

$$0 \to A \to B \to C \to 0$$

splits if $B \cong A \oplus C$.
For Example: The sequence

$$0 \to \mathbb{Z}/2\mathbb{Z} \overset{x \mapsto x}{\to} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \overset{-1}{\to} \mathbb{Z}/2\mathbb{Z} \to 0$$

splits but

$$0 \to \mathbb{Z}/2\mathbb{Z} \overset{x \mapsto 2x}{\to} \mathbb{Z}/4\mathbb{Z} \overset{\text{mod } 2}{\to} \mathbb{Z}/2\mathbb{Z} \to 0$$

does not split.

Proposition 23. *Every surjective module-homomorphism from a A-module, M to a **free** a A-module F splits.*

Proof. Let $\phi : M \to F$ be a surjective homomorphism. By the first isomorphism theorem, $F \cong M/\ker\phi$. Let $\{x_i + \ker\phi\}_{i \in I}$ form the basis of $M/\ker\phi$. Define $\psi : M/\ker\phi \to M$ as

$$\psi\left(\sum_{i \in I} a_i x_i + \ker\phi\right) = \sum_{i \in I} a_i x_i.$$

Clearly $\phi \circ \psi = \text{id}$ □

F need not be a free module for $A \to F$ to split. Modules that admit splitting like the above are called **projective**. Here are four equivalent conditions that are satisfied by a projective module P:

1. Given a homomorphism $f : P \to M$ and a subjective homomorphism $g : M' \to M$, there exists a homomorphism $h : P \to M'$ that makes the following diagram commute:

$$\begin{tikzcd} & P \arrow[dl, "h"'] \arrow[d, "f"] & \\ M' \arrow[r, "g"'] & M \arrow[r] & 0 \end{tikzcd}$$

2. The exact sequence $0 \to M' \to M \to P \to 0$ splits

3. There exists a module M such that $P \oplus M$ is free.

4. The functor $M \mapsto \text{Hom}_A(P, M)$ is exact.

Proof. We only leave the proof of $(4) \implies (1)$ as the rest is found in the book. Consider (4) is true, i.e, if $0 \to M'' \to M' \overset{g}{\to} M \to 0$ is exact, $0 \to \text{Hom}_A(P, M'') \to \text{Hom}_A(P, M') \overset{\lambda}{\to} \text{Hom}_A(P, M) \to 0$ is also exact. Since λ is surjective, for any $f \in \text{Hom}_A(P, M)$, we can find $h \in \text{Hom}_A(P, M')$ such that $\lambda(h) = g \circ h = f$. □

Proposition 24. *Let V be a vector space. Let Γ be the set of generators of V and S be a set of any linearly independent elements. Then, there is a basis $\mathfrak{B}$ such that $S \subseteqq \mathfrak{B} \subseteqq \Gamma$.*

Proof. Let $\mathfrak{I}$ be the sets $T \supseteqq S$ that are linearly independent. Assuming $V \neq \{0\}$, $\mathfrak{I}$ is non-empty. Clearly $\mathfrak{I}$ is a poset by ascending inclusion. Since if $T_i \subseteqq T_{i+1} \in \mathfrak{I}$ then $T_i \cup T_{i+1}$ is linearly independent making $\mathfrak{I}$ an inductively orderd set. By zorns lemma, there is a maximal element of $\mathfrak{I}$. Let's call that $\mathfrak{B}$ and let $\langle B \rangle = W$. If $W \neq V$, then there is $x \in V$ such that $x \neq \sum_{y \in \mathfrak{B}} a_y y$ making $\mathfrak{B} \cup x$ linearly independent and contradictng maximality of $\mathfrak{B}$. Thus $V = W$. $\square$

Proposition 25. *Let V, U be vector spaces over field K and let $V \xrightarrow{f} U$ be homomorphism. Then we have*

$$\dim_K V = \dim_K \ker f + \dim_K \operatorname{Im} f.$$

Proof. Let $\{w_i\}_{i \in I}$ and $\{u_i\}_{i \in I}$ be the basis of $\ker f$ and $\operatorname{Im} f$ resp. Let $\{v_i\}_{i \in I}$ be a family of elements such that $f(v_i) = u_i$. Let $x \in V$. Then we have,

$$f(x) = \sum_{i \in I} a_i u_i,$$

where $\{a_i\}_{i \in I}$ is a family in K such that all except finit of them are 0. This implies,

$$y = x - \sum_{i \in I} a_i v_i \in \ker f.$$

However, $\ker f$ is a vector field and $y = \sum_i b_i w_i$. This implies

$$x = \sum_{i \in I} a_i v_i + \sum_{j \in I} b_j w_j.$$

Proving $\{v_i, w_i\}_{i \in I}$ generates V. It remains to show that this generator is linearly indepenendent.

Let $0 = \sum_{i \in I} a_i v_i + \sum_{j \in I} b_j w_j$. Then $f(\sum_{i \in I} a_i v_i + \sum_{j \in I} b_j w_j) = 0 + \sum_{i \in I} a_i f(v_i) + 0 = \sum_{i \in I} a_i u_i = 0 \implies a_i = 0 \implies b_j = 0$. $\square$

An important insight from the companion: *A free left R-module with rank n is isomorphic to a standard*[2] *module R^n*. This helps us derive the following facts about modules over non-field ring:

- *If $R \xrightarrow{f} S$ is a homomorphism and m, n are positive integers such that $R^m \cong R^n$, then $S^m \cong S^n$.*

  If $\mathcal{M}$ is a (isomorphic) transformation from $R^m \to R^n$, then is $f(\mathcal{M})$ is too from $S^m \to S^n$.

- *If there is a homomorphism onto a field (division ring), then all left R-modules have a fixed number of elements in their basis.*

  This follows by taking $f = R \mapsto R/I$ where I is a maximal ideal.

Warning: Modules over non-commutative rings do not necessarily have unique ranks.

[2] By standard, we mean where the action of R is trivial as in linear algebra

Dual Space and Dual Module

Let E be a free module over a commutitive ring A. We denote the **dual module**, $\mathrm{Hom}_A(E, A)$, of E by $E^\vee$ and we call the elements of $E^\vee$ as **functionals.**

If $x \in E$, then x induces a map $\langle x, - \rangle$ from $E^\vee$ to itself defined by $\langle x, f \rangle = f(x)$.

The map $\theta : E \to E^{\vee\vee}$ is not surjective for the following reason. In infinite-dimensional modules over a field A, $E^{\vee\vee}$ is also infinite dimensional. However, x can be expressed as a linear combination of the basis of E and so is $\theta(x)$.

Proposition 26. *If E is free, so is $E^\vee$. Moreover,* $\mathrm{rank}E = \mathrm{rank}E^\vee$

Theorem 27. *Let E be finite dimensional. The map $x \xrightarrow{\phi} (f \mapsto \langle x, f \rangle)$ is an isomorphism from E to $E^{\vee\vee}$.*

Theorem 28. *Let U, V, W be finite-dimensional free modules over commutative ring A. If the sequence*

$$0 \to W \to V \to U \to 0$$

is exact, then so is

$$0 \to U^\vee \to V^\vee \to W^\vee.$$

Why it is called a sequence splits? A short sequence

$$0 \to C \to C \oplus B \xrightarrow{g} B \to A$$

is **splits** into

$$0 \to C \to C \to 0 \to 0$$

$$0 \to 0 \to B \to B \to 0$$

We require a right inverse map g',i.e., that satisfies $\mathrm{id} = g \circ g' : B \to C \oplus B$, to say so, the action of this map on C would be 0 and the action on B would be g^{-1}

Modules over Principal Ideal Domains

Theorem 29. *Let R be a principal ideal domain and let F be a free R-module. If M is a submodule of F, then M is free with rank less than or equal to* $\mathrm{rank}F$*.*

sketch. Let M_i be the submodule of M generated by the basis subset $\{x_1, \dots, x_i\}$. Let $\mathfrak{a}_{i+1}$ denote the set of coffecients of x_{i+1} in $M - M_i$. If $\mathfrak{a}_{i+1} = 0$, we are done. If not, observe that $RM_i \subsetneqq M_i$ and $\mathfrak{a}_{i+1} = \langle a_{i+1} \rangle$ for some $a_{i+1} \in R$. Let $w := \sum_{j \leqq i} b_j x_j + a_{i+1} x_{i+1}$. Then $M_{i+1} = M_i + Rw$. $\square$

Remark 30. The PID nature of R permits the constructions of *generators* w_i of M corresponsing to the generators x_i

NB: Finitely generated modules are factor modules of a free module.

Definition 31. An R-module M is called a **torsion** module if for some $x \in M$, there is an element $a \in R$ such that $ax = 0$. We denote the module that contain all torsion elements by M_{tor}.

Theorem 32. *Let E be finitely generated. The factor module E/E_{tor} is free and there is a free submodule F of E such that*

$$E = E_{\text{tor}} \oplus F.$$

Modules ove PID exhibit similar characterstics as abelian groups. For example, the cyclic p-groups are analogous to a moule generated by an element x modulo a prime ideal, i.e $Rx/(p)x$. We call a module of type $(r_1, \ldots, r_k)$ if is a product of modules isomorphic to $R/(p^{r_i})$. The following two theorems support the similarity even more by stating the equivalent statements to the fundamental theorem of abelian groups.

Theorem 33. *Let R be a princial ideal domain and let E be a finitely generated torsion module over R. Let $E(p)$ denote all elements of E with exponent*[3] *that is a power of a prime element $p \in R$. Then E has the decomposition*

$$E = \bigoplus_p E(p),$$

where the direct sum is over p such that $E(p) \neq 0$. Moreover, for each p, we have

$$E(p) = R/(p^{v_1}) \oplus \cdots \oplus R/(p^{v_r})$$

with $1 \leqq v_1 \leqq \cdots \leqq v_r$ that are determined uniquely.

$E_m :=$ the kernel of the map $x \mapsto mx$ in E.

Proof. Let a be an exponent of E. Consider the map $x \mapsto ax$. Let $a = bc$ with $(b, c) = (1)$. Let $xb + yc = 1$. Then $v = vxb + vyc$ where $vxb \in E_c$ and $vyc \in E_b$. Moreover, $E_b \cap E_c = 0$. Thus $E_a = E_b \oplus E_c$. By induction, the stated decomposition of E follows.

Next, we show that $E(p)$ is a direct sum as stated.

The intuition for such decomposition of $E(p)$ comes from boxing all elements of $E(p)$ with the same period[4] into a direct summand.

We will use induction. Consider the canonical map from $E(p) \to E(p)/(x)$ where x is an element of $E(p)$ with maximal period, p^r. Suppose $\{\overline{y_1}, \ldots, \overline{y_m}\}$ are independent[5] elements of $E(p)/(x)$ with representatives $\{y_1, \ldots, y_m\}$ in $E(p)$. If p^{n_i} is the period of $\overline{y_i}$, then $p^{n_i} y_i = p^s cx$ for some $c \in R$, $p \nmid c$. By assumption, $r \geqq s$, thus $p^{n_i - s + r} =$

[3] An exponent of a module M (an element of a module x resp.) is an element m of R such that mE (resp. mx) is 0.

[4] A period T of an element x is an element of R such that the kernel of the mao $a \mapsto ax$ equals $\langle T \rangle$

[5] We call a family of elements $\{y_i\}$ of a module M independent if $\sum_i a_i y_i = 0 \iff a_i y_i = 0 \,\forall i$

$0 \implies n_i - s + r \leqq r \implies n_i \leqq s$. Therefore the element $y_i - p^{s-n}cx$ is well-defined and has period equal to that of $\overline{y_i}$.

Moreover the set $\{x, y_1, \ldots, y_m\}$ is independent because if $bx + \sum_i a_i y_i = 0$, then $\sum_i a_i \overline{y_i} = 0$ which can not happen unless $a_i \overline{y_i} = 0$ for all i. But by previous part of the proof, this implies all period $c_i \mid a_i \implies a_i y_i = 0$ and $bx = 0$.

Thus, $E(p)$ has $m+1$ independent elements $x, y_1 \ldots, y_m$. It is clear that $(x, y_1, \ldots, y_m) = (x) \oplus (y_1) \oplus \cdots \oplus (y_m)$ by independece. Note that if $w \in E$ has period t, then $(w) \cong R/\langle t \rangle$. This proves the existence of such decomposition.

Uniquness of the decomposition follows as following. Let $(s_1, \ldots, s_m)$ and $(r_1, \ldots, r_n)$ be two types of $E(p)$ with $s_i \leqq s_{i+1}$ and $r_i \leqq r_{i+1}$. WLOG, let $s_i < r_i$ be the first different entries. Clearly, there is an element $x \in E(p)$ with period p^{s_i}. However, no such element exist in $R/(p^{r_i}) \oplus \cdots \oplus R/(p^{r_n})$. Thus $s_i = r_i$. $\square$

Remark 34. The proof of theorem 7.8 on the book utilizes a trick to select a basis set with particular property. The trick relies (generally speaking) on the fact that functionals capture the properties of basis.
For example: The dimenstion of a free module M is equal to $\max_{\lambda \in M^\vee} \dim \lambda(M)$.

Direct and Inverse Limits

Let I be a directed set. Let $\{A_i\}_{i \in I}$ be a family of A-modules and let$\{f_{i,j} : A_i \to A_j\}$ be a family of A-homomorphism satisfying

$$f_{i,i} = \mathrm{id}$$

$$f_{i,k} = f_{j,k} \circ f_{i,j} \text{ if } i < j.$$

We call this family of morphisms, **a directed family of morphisms**. When we have a family like $\{A_i\}$, we want to study their properties together. The **direct limit** has the required algebraic properties to do so and it's defined as follows.

Consturct a category $\mathcal{C}$ by defining $\mathrm{Ob}(\mathcal{C})$ as the pair (A, f_i) with A in the family of modules and $f_i : A_i \to A$ that makes the following diagram commute

$$\begin{tikzcd}
A_i \arrow[rr, "f_i"] \arrow[dr, "f_{i,j}"'] & & A \\
& A_j \arrow[ur, "f_j"'] &
\end{tikzcd}$$

where the morphisms are f_i themselves. The direct limit $(B = \varinjlim A_i, h_i)$ is the universal object of this category, i.e., for every (C, g_i) in this cateory there is a unique homomorphism t that makes the following diagram commute

Chapter 4

Polynomials

Proposition 35. *If k is a field and $k[X_1, \dots, X_m]$ is the ring of polynomials over the variables $X_1, \dots, X_n$. Let $f \in k[X_1, \cdots, X_m]$ and $S_1, \cdots, S_m$ be infinites subsets of the field k such that $f(a_1, \cdots, a_n)$ for all $a_i \in S_i$. Then $f = 0$.*

Proof. For $m = 1$, the propostion is trivial. For $m > 1$, note that

$$k[X_1, \cdots, X_m] = k[X_1, \cdots, X_{m-1}][X_m].$$

For fixed $a_1, \dots, a_{m-1}$, $f(a_1, \cdots a_{m-1}, X_n)$ is then $\in k[X_n]$ and thus $f(a_1, \cdots, a_{m-1}, X_n) = 0$ obtainig the result by symmetry and induction.

□

Theorem 36. *Let k be a field and let U be a finite multiplicative subgroup k. Then U is cyclic.*

Proof. Let $U = \prod_p U(p)$ where $U(p)$ is a p-group for each prime p. Let $a \in U(p)$ be an element with maximal power say p^r. Then for all $b \in U(p)$, $b^{p^r} - 1 = 0$ making $|U(p)| \leq p^r$. Hence each $U(p)$ is cyclic.

□

Remark 37. Generally, certain polyonmials over fields like $X^{p^r} - 1$ in the above proof, help us enumerate elements of the field with certain characterstics by measns of their roots.

Definition 38 (Algebraic Closure)**.** A field k is called algebaically closed if all polyonmials in $k[X]$ of degree ≥ 1 have all their roots in k.

Definition 39 (Frobenius Map)**.** If k is a field with characteristic p, we call the map

$$x \mapsto x^{p^r}$$

the frobenius map or frobenius endomorphism

Polynomials over a Factorial Ring

Let A be a factorial ring and K be its field of fraction.

Definition 40 (Order)**.** If $a \in K$ and $p \in A$ be a prime element.

$$\mathrm{ord}_p : K \to \mathbb{Z},$$

$$\mathrm{ord}_p(a) := r : a = p^r x/y, p \nmid x, p \nmid y.$$

If $f \in K[X]$, $f(X) = \sum a_i x^i$, we extend the above definition as

$$\mathrm{ord}_p f = \min_p \mathrm{ord}_p(a_i),$$

where the minimum is taken over all primes p of A.

Definition 41 (p-content, content)**.** We say the element $up^{\mathrm{ord}_p f}$, a p-content for f for any unit u. Then the content of f, denoted by $\mathrm{cont}(f)$ is defined as

$$\prod_p p^{\mathrm{ord}_p f},$$

over all primes p, upto multiplication by a unit.

Remark 42. Content is a generalization of the concept of gcd for fractions. For instance, $\mathrm{cont}(p) = p$, $\mathrm{cont}(px+q) = 1$, $\mathrm{cont}(px+p) = p$ for prime p, q.

Theorem 43 (Gauss Lemma)**.** *For any two $f, g \in K[X]$, we have*

$$\mathrm{cont}(fg) = \mathrm{cont}(f)\mathrm{cont}(g).$$

Sketch 1.: If both f and g are primitive, then fg is primitive. This can be shown by noting that for any prime p, if we can not extract p from both f and g, then there is a coefficient in fg namely $c = \sum_{i+j=r+s} a_i b_j$ where r and s are the largest integers (resp) such that a_r and b_s are indivisible by p and c is thus indivisible by p.
Sketch 2. Considering the reduction modulo a prime p of two polynomials f, g, say $\bar{f}$ and $\bar{g}$, we have

$$\bar{fg} = \bar{f}\bar{g}.$$

Since $A/(p)$ is an integral domain, $\overline{fg} = 0 \iff \overline{f} = \overline{g} = 0$.

Theorem 44. *$A[X]$ is factorial and the primes are primes of A or irreducible polynomials of $K[X]$ with content of* 1.

Proof. Let f factorize as follows in $K[X]$

$$f(X) = c\prod_i p_i(X),$$

such that $\mathrm{cont}(p_i) = 1$. Since $\mathrm{cont}(f) = c$, $c \in A$ and there exists a factorization of f in $A[X]$. Uniqueness follows from uniqueness of factorization in $K[X]$ upto multiplication by units and unitary content of irreducibles in A. ☐

Critera of Irreducibility

Theorem 45 (Eisenstein's Criterion of Irreducibility)**.** *Let A be a factorial ring and let $f \in A[X]$ such that*

$$f(X) = a_0 + a_1 x + \cdots a_n x^n.$$

Let p be a prime in A. If we have

$$a_n \not\equiv 0 \mod p \quad a_i \equiv 0 \mod p \quad i < n$$
$$a_0 \not\equiv 0 \mod p^2$$

then f is irreducible in $A[X]$ (thus $K[X]$).

Sketch: If f were reducible to g, h such that $[X^n]g = b_n$, $[X^n]h = c_n$ and $\deg g = m$, $\deg h = n$ then neither of b_m and c_n are divisible by p. Moreover, WLOG, there is greaterst index r such that all of $c_i, i > r$ are divisible by p, then

$$[X^r]f = b_0 c_r + \cdots$$

is not divisible by p.

Theorem 46 (Reduction Criterion)**.** *Let A, B be entire rings and let $\phi : A \to B$ be a homomorphism. Let K, L be the quotient fields of A, B resp. Assume for $f \in A[X]$, $\phi f \neq 0$ and $\deg \phi f = \deg f$. If ϕf is irreducible in $L[X]$, then f does not factorize to $g, h \in A[X]$ such that both $\deg g$, $\deg h \geq 1$.*

Proof. Since $\phi f = (\phi g)(\phi h)$, by irreduciblity of ϕf, one of the two factors on the right should have degree 0. But $\deg \phi f = \deg \phi g + \deg \phi h$ by assumption, thus $f = c \cdot h$ for some $c \in A$. $\square$

Remark 47. This theorem is powerful test to check irreducibility. Eg. $X^p - X - 1$ is irreducibile over the field $\mathbb{Z}/p\mathbb{Z}$ thus irreducible over $\mathbb{Q}$.

Hilbert's Theorem

Theorem 48 (Hilbert's Theorem)**.** *If A is commutitive and Noetherian, so is $A[X]$.*

Sketch Take an ideal of $A[X]$, $\mathfrak{U} = \oplus \mathfrak{a}_i X^i$. By ACC, there is r such that $\mathfrak{a}_r = \mathfrak{a}_{r+s}$. Since $\mathfrak{a}_i$ is finitely generated, say by a^i_j, for $0 \leq i \leq r$, there are polynomials $f_{ij}(X) = a^i_j X^i + g(X)$, $g \in \mathfrak{U}$, $\deg g < i$, that generate $A[X]$ and the number of f_{ij} is finite.

Partial Fractions

Theorem 49. *Let A be a principal entire ring and let $K = \operatorname{frac}(A)$. Let $\alpha \in K$ and P be the set of representatives of the irreducibles of A, i.e, unique upto multiplication by units of A. For each $p \in P$, there exists an element α_p and non-negative integer $j(p)$ with $\gcd(p^{j(p)}, \alpha_p) = 1$ that satisfies*

$$\alpha = \sum_{p \in P} \frac{\alpha_p}{p^{j(p)}}$$

with $j(p) = 0$ for all but finite elements of P. Moreover, this expression is unique upto the condition $\alpha_p \equiv \alpha'_p \mod p^{j(p)}$.

Theorem 50. *Let k be a field and $k[X]$ be the ring of polynomials over k. Let $f, g \in k[X]$ such that $\deg g \geq 1$. There exists a unique sequence of polyonmials $f_0, \dots, f_d$ with $\deg f_i < \deg g$ such that*

$$f = f_0 + f_1 g + \cdots f_d g^d.$$

The expresion of f as such is called the g-**adic expansion** of f

Symmetric Polynomials

Define the monomials s_i as follows:

$$\prod_{i=1}^{n}(X + t_i) = \sum_{i=0}^{n} s_i X^{n-i}$$

Theorem 51. *Let $f(t) \in A[t_1, \dots, t_n]$ be a symmetric polyomial with degree d. Then There is polynomial g of weight $\leq d$ such that $f(t_1, \dots, t_n) = g(s_1, \dots, s_n)$.*

Mason-Stothers Theorem and The *abc* Conjecture

Let $n_0(f)$ be the number of distinct roots of the polynomisl $f \in K[X]$.

Theorem 52 (Mason-Stothers)**.** *If $a, b \in K[t]$ are relatively prime polyonmials in an algebraically closed field K, then*

$$\max(\deg(a, b)) \leq n_o(ab(a + b)) - 1.$$

Conjecture 53 (*abc* conjecture)**.** *For a given $\epsilon > 0$, relatively prime integers a, b and their sum c, and a constant factor $C(\epsilon)$ depending only on ϵ,*

$$\max(|a|, |b|, |c|) \leq C(\epsilon) N_0(abc)^{1+\epsilon},$$

where $N_0(x)$ is the product of distinct prime divisors of x, called radical of x.

The Resultant

Let $v = (v_0, \dots, v_n)$ and $w = (w_0, \dots, w_m)$ be algebraically independent over a commutitive ring A. Let

$$f_v(X) = \sum_{i=0^n} v_i X^i, \quad g_w = \sum_{i=0}^{m} w_i X^i$$

$$\mathrm{Res}(f_v, g_w) = \det \begin{bmatrix} v_0 & v_1 & \cdots & v_n & 0 & \cdots & 0 \\ 0 & v_0 & v_1 & \cdots & v_n & \cdots & 0 \\ \vdots & & \ddots & & & \ddots & \vdots \\ 0 & \cdots & 0 & v_0 & v_1 & \cdots & v_n \\ w_0 & w_1 & \cdots & w_m & 0 & \cdots & 0 \\ 0 & w_0 & w_1 & \cdots & w_m & \cdots & 0 \\ \vdots & & \ddots & & & \ddots & \vdots \\ 0 & \cdots & 0 & w_0 & w_1 & \cdots & w_m \end{bmatrix}$$

Denote $R(v, w) = \mathrm{Res}(f_v, g_w)$. Then for any z, we have $R(zv, w) = z^n R(v, w), \quad R(v, zw) = z^m R(v, w)$. Hence, R is homogenous in v and w. We also have,

$$[v_0^m w_m^n] R(v, w) = 1.$$

One can also show there exists $\phi_{v,w}, \psi_{v,w} \in Z[v, w][X]$ such that

$$R(v, w) = \phi_{v,w} f_v + \psi_{v,w} g_w.$$

This relation serves as an 'invariant' (i.e. not depending on X). For example:

Proposition 54. *For a subfield K of L and $f_a, g_b \in K[X]$ having a common root η, then $R(a, b) = 0$.*

Proposition 55. *Let*

$$f_v(X) = v_0 \prod_{i=1}^{n} (X - t_i) = \sum_{i=0}^{n} v_i X^i,$$

$$g_w(X) = w_0 \prod_{i=1}^{n} (X - u_i) = \sum_{i=0}^{m} w_i X^i.$$

Then

$$\mathrm{Res}(f_v, g_w) = v_0^m w_0^n \prod_{i=1}^{m} \prod_{j=1}^{n} (t_i - u_j).$$

Power Series

The formal power series $A[[X]]$ in one variable is formally defined as the ring of morphisms from G to A where G is the multiplicative monioid of mappings from $\{X\} \to \mathbb{N}$. We denote an element f as

$$f(X) = \sum_{n=0}^{\infty} a_n X^n$$

where f maps $(X^n : X \mapsto n)$ to $a_n \in A$.

We define power series in n variables $A[[X_1, \ldots, X_n]]$ inductively. If k is a field then $k[[X_1, \cdots, X_n]]$ is a complete local ring where a sequence $\{a_n\}$ is considered Cauchy if there exist N such that for all $n, m \geq N$, $a_n - a_m \in I^v$ for a given power v and ideal I.

Here it's worth to consider what complete local ring means in other terms. A convergence point a by the above notion is an element a such that $a - a_k \in I^v$ for all $k \geq N(v)$ for any power v. This translates to an element $x = (x_0, \dots)$ in the projective limit $\varprojlim_n R/I^n$ such that $x_j = a_i \mod I^j$ for all $i \geq N(v)$ and $j \leq v$. Therefore, an element x in the projective limit defines a convergence points for some Cauchy sequence and thus a ring is complete if R is equal to the projective limit.

Locality, on the otherhand, implies R has only one maximal ideal and anything outside the a given maximal ideal is invertible.

Theorem 56. *Let $\mathfrak{o}$ be a complete local ring with maximal ideal $\mathfrak{m}$. Let $f(X) \in \mathfrak{o}[[X]]$ be given by*

$$f(X) = \sum_{i=0}^{\infty} a_i X^i$$

such that not all a_i lie in $\mathfrak{m}$. Suppose $a_0, \dots, a_{n-1} \in \mathfrak{m}$ and $a_n \in \mathfrak{o}^*$ is a unit. Then given $g \in \mathfrak{o}[[X]]$ one can solve the equation

$$g = qf + r$$

uniquely where $q \in \mathfrak{o}[[X]]$ and $r \in \mathfrak{o}[X]$, $\deg r \leq n-1$.

Remark 57. If a_0 is a unit and all the other a_i are non-units, f is invertible and and one can always solve $g = qf$ by mutliplying inverse of f to both sides. The theorem states a general case where $a_i \leq n-1$ are non-units, in which case one will have to make for the first $n-1$ terms of g by adding polynomial r.

Example: Let $\mathfrak{o} = \mathbb{Z}$, and $f(X) = 2 + X + 2X^2 + 4X^3 + \cdots$. Let $g(X) = \sum_{n=0}^{\infty} 2^n X^n$. $f(X) = 1 + Xg(X) \implies (1-2X)f(X) = 1 - X \implies (1 + X + X^2 + \cdots)f(X) = g(X)$.

The integrer n is called **Weierstrass Degree** of f and denoted $\deg_W(f)$.

Theorem 58 (Weierstrass Preparation)**.** *Let f be a polynomial in a complete local ring $\mathfrak{o}$ with $\deg_W(f) = n$. Then we can solve the following equation uniquely*

$$(X^n + b_{n-1}X^{n-1} + \cdots + b_0)u = f(X),$$

where u is a unit in $\mathfrak{o}[[X]]$ and $b_i \in \mathfrak{m}$.

Theorem 59. *If k is a field, then $k[[X_1, \dots, X_n]]$ is a UFD.*