Chapter 1 Algebraic Foundations

1.1 Groups

设 S 是一个集合，考虑运算 $S \times S$ 表示一个二元组 (s,t), 其中 $s \in S, t \in S$. 那么一个 $S \times S$ 到 S 上的映射被称为 S 上的二元运算**(binary operation)**.

如果 $S \times S$ 的像仍然在 S 内，我们称 S 具有封闭性. **(closure property)**

Definition 1.1 Group

考虑集合 G 和运算 $*$. 如果满足以下三条性质，那么 $(G,*)$ 就是一个群.

(1) 结合律**(associative)**，对于 $a,b,c \in G$, 有 $a*(b*c)=(a*b)*c$.

(2) 存在单位元 **(identity)**. 即存在一个元素 $e \in G$, 使得对于任意 $a \in G$, 都有 $a*e=e*a=a$.

(3) 每个元素都有逆元**(inverse element)**. 即对于每个元素 $a \in G$, 都存在一个元素 $a^{-1} \in G$, 使得 $a*a^{-1}=a^{-1}*a=e$.

如果对于任意的 $a,b \in G$, 都有 $a*b=b*a$ 的话，那这个群则成为交换群 **(commutative group)**.

这个符号是任意的，也可以用 "+" 或者其他符号来表示.

Example 1.2

比如，整数集 $\mathbb{Z}$ 对于加法是一个群，它满足结合律，存在单位元 0, 每个元素都有其相反数作为逆元；同时它满足交换律，所以它也是一个交换群.

Definition 1.3 Cyclic Group and Generator

考虑乘法群 $(G,*)$, 如果存在一个元素 $a \in G$ 使得对于所有的 $b \in G$ 都存在正整数 j 使得 $b=a^j$, 那么这个乘法群是循环群.

这样的元素 a 被称为生成元，群 G 可以记为 $G=<a>$.

Discussion 1.3 Equivalence Relation

设 R 是 $S \times S$ 的一个子集， R 是 S 上的等价关系，当且仅当 S 满足下面三条性质：

(1) 自反性 **(Reflexivity)**: 对于任意的 $s \in S$ 有 $(s,s) \in R$.

(2) 对称性 **(Symmetry)**: 如果 $(s,t) \in R$, 那么 $(t,s) \in R$.

(3) 传递性 **(Transitivity)**: 如果 $(s,t),(t,u) \in R$, 那么 $(s,u) \in R$.

根据等价关系，可以对集合进行划分. 也就是说集合 S 等于若干个非空且相互不交的 R 的并集.

选取每个等价类**(Equivalence class)** 的代表元 s, 等价类可以记为 $[s] = \{t \in S : (s,t) \in R\}$

Definition 1.4 Congruent

对于任意整数 a, b 和正整数 n, 如果 $a-b$ 是 n 的倍数，即存在某个整数 k 使得 $a = b + kn$, 那么称 a 与 b 同余，记做 $a \equiv b \mod n$.

可以发现同余关系是整数集 $\mathbb{Z}$ 上的一个等价关系.

定义

$$[a] + [b] = [a+b] \tag{1.1}$$

即两个等价类的和等于两个等价类代表元的和.

Definition 1.5 Group of Integers Module N

由集合 $\{[0],[1],\ldots,[n-1]\}$ 构成的关于运算 (1.1) 的群记做 $\mathbb{Z}_n$.

Definition 1.6 Finite Group and Order

如果一个群里的元素是有限的，那就称这个群是有限群，元素个数被称为这个群的阶. 对于有限群 G，它的阶被记为 $|G|$.

Example 1.7

凯莱图，用表来表示有限群，过于简单，此处略.

Definition 1.8 Subgroup

群 G 的一个子集 H 是 G 的子群，当 H 对于 G 上的运算也构成群时.

平凡子群 **(Trivial Subgroups)** 是 G 本身和 e. 其余的叫做非平凡子群 **(Nontrivial Subgroups)**.

Definition 1.9 Generated Subgroup

如果一个群 G 的子群包含了所有某个 G 中元素 a 的所有幂次，那么称这个子群是循环子群，记做 $< a >$

这个子群一定是循环群. 如果这个群是有限群，那么它的阶就是 a 的阶；否则元素 a 是一个阶为无穷的元素.

一个元素 a 的阶为 k 意味着 k 是满足 $a^k = e$ 的最小正整数. 对于其它 m 满足 $a^m = e$, 则一定有 $k \mid m$.

设 S 是 G 的一个非空子集，如果 G 的子群 H 包括了 S 中所有有限阶元素的幂次，就称子群 H 由 S 生成，记为 $H =< S >$.

例如整数集上的同余关系就是一个这样的生成关系. 它定义了一个整数集上的等价关系.

Theorem 1.10 Cosets

设 H 是 G 的子群，那么 G 上的关系 $R_H : (a, b) \in R_H$ 是等价关系，当且仅当存在 $h \in H$ 使得 $a = bh$.

这样的子群可以把 G 分为若干个非空且互不相交的集合，这些集合被称为 G 模 H 的左陪集，记做

$$aH = \{ah : h \in H\}$$

右陪集同理.

如果群是交换群，那么左陪集和右陪集相等，统称为陪集.

Example 1.11

设 $G = \mathbb{Z}_{12}, H = \{[0], [3], [6], [9]\}$, 那么所有 G 模 H 的陪集就是：

$[0] + H = \{[0], [3], [6], [9]\}$

$[1] + H = \{[1], [4], [7], [10]\}$

$[2] + H = \{[2], [5], [8], [11]\}$

Theorem 1.12

设 H 是 G 的一个有限子群，那么每个 G 模 H 的陪集中的元素都和 H 中的元素个数相等.

Definition 1.13 Index

如果 G 的子群 H 只在 G 上产生有限多个 G 模 H 的陪集，陪集的个数被称为 H 在 G 中的指数. 在下面记做 $index(H)$.

Theorem 1.14

群 G 的阶等于其任意一个子群 H 的阶乘以 H 在 G 上的指数. 即：

$$|G| = |H| \times index(H)$$

也就是说，群 H 的阶可以整除群 G 的阶，任意元素 $a \in G$ 的阶整除 G 的阶.

Theorem 1.15

(i) 循环群的子群仍然是循环群.

(ii) 一个阶为 m 的有限循环群 $< a >$, 元素 a^k 可以生成一个阶为 $m/gcd(k,m)$ 的子群.

(iii) 一个阶为 m 的有限循环群 $< a >$, 设 d 是 m 的一个正因子，那么 $< a >$ 中恰好会有一个指数为 d 的子群. 对于每个 m 的正因子 f, $< a >$ 中恰有一个阶为 f 的子群.

(iv) 一个阶为 m 的有限循环子群 $< a >$, 设 f 是 m 的一个正因子. 那么 $< a >$ 中有 $\phi(f)$ 个阶为 f 的元素.

(v) 一个阶为 m 的有限循环群 $< a >$ 有 $\phi(m)$ 个生成元. 生成元 a^r 满足 $gcd(r,m) = 1$.

证明：

(i) 设 H 是循环群 $< a >$ 的子群且 $H \neq \{e\}$. 如果 $a^n \in H$, 那么就有 $a^{-n} \in H$.

设 d 是满足 $a^d \in H$ 的最小正整数，并令 $a^s \in H$. 那么就有 $s = qd + r, 0 \leq r < d, q, r \in \mathbb{Z}$.

所以就有 $a^s(a^{-d})^q = a^r \in H$, 这与 d 的最小性矛盾. 所以 $r = 0$. 因此所有在 H 中的元素 a 的幂次都整除 d. 即 $H =< a^d >$.

(ii) 令 $d = gcd(k,m)$. 群 $< a^k >$ 的阶是满足 $a^{kn} = e$ 的最小正整数 n. 所以 $m \mid kn$, 即 $m/d \mid n$. 满足这个式子的最小的 n 就是 m/d.

(iii) 根据 (ii), 给定 d, 那么 $< a^d >$ 的阶是 m/d, 指数是 d. 如果 $< a^k >$ 是另一个指数为 d 的子群，它的阶是 m/d. 因此可以得到 $d = gcd(k,m)$.

特别的, $d \mid k$, 所以 $a^k \in < a^d >$, $< a^k >$ 是 $< a^d >$ 的子群. 但是它们的阶是相等的，所以它们相等.

定理 (iii) 的后半部分也显然，因为阶为 f 的子群就是指数为 m/f 的子群.

(iv) 令 $|< a >| = m, m = df$. 根据 (ii) 元素 a^k 的阶是 f 当且仅当 $gcd(k,m) = d$. 所以阶为 f 的元素个数就是满足 $1 \leq k \leq m$ 且 $gcd(k,m) = d$ 的正整数 k 的个数.

令 $k = dh, 1 \leq h \leq f$, 那么等价于求满足 $gcd(h,f) = 1$ 的 h 的个数. 所以 h 的个数就是 $\phi(f)$.

(v) 由于 $< a >$ 的生成元的阶是 m，所以前半部分等价于 (iv), 后半部分等价于 (ii)

Definition 1.16 Homomorphism and Isomorphic

考虑映射 $f : G \to H$, 这个映射是 G 到 H 的同态映射，当且仅当 f 保存了 G 上的运算. 也就是说，设 G 和 H 上的运算分别是 $\times$ 和 $\cdot$, 那么当

$$f(a \times b) = f(a) \cdot f(b)$$

的时候，这个映射是同态映射. 如果 f 是满射的，则 f 是一个满同台， H 是 G 的一个满同态像.

一个 G 到 G 的同态被称为自同态.

如果 f 是一个一一映射，那么 f 是一个同构映射，称 G 和 H 同构. 一个 G 到 G 的同构被称为自同构.

同构的群具有相同的性质和结构.

例如，考虑 $f:\mathbb{Z}\to\mathbb{Z}_n$, 即 $f(a)=[a]$, 那么

$$f(a+b)=[a+b]=[a]+[b]=f(a)+f(b), a,b\in\mathbb{Z}$$

那么 f 就是一个同态映射.

设 e 是 G 的单位元， f 是 G 到 H 的同态映射. 由于 $ee=e$, 所以 $f(e)f(e)=f(e)$, 所以 $f(e)=e'$, 是 H 中的单位元.

由于 $aa^{-1}=e$, 所以 $f(a^{-1})=(f(a))^{-1}$, 这对于任意 $a\in G$ 都成立.

下面考虑一个自同构. 对于给定的 $a\in G$, 定义 f_a 为 $f_a(b)=aba^{-1}$, 其中 $b\in G$. 那么 f_a 是 G 上的一个内自同构. 让 a 遍历 G 中的每一个元素，就可以得到所有的 G 的内自同构.

元素 b 和 aba^{-1} 的关系称为共轭关系，对于 G 的一个非空子集 S, 集合 $aSa^{-1}=\{asa^{-1}:s\in S\}$ 与集合 S 共轭.

因此， S 的共轭只是 S 在不同的 G 的自同构中的像.

Definition 1.17 Kernel

同态 $f:G\to H$ 的核定义为:

$$kerf=\{a\in G:f(a)=e'\}$$

其中 e' 是 H 中的单位元

可以发现这个集合就是单位元的原像集.

Example 1.18

考虑 $f:\mathbb{Z}\to\mathbb{Z}_n$, 即 $f(a)=[a]$, $kerf$ 就是满足 $[a]=[0]$ 的所有的 a, 也就是说 $kerf=<n>$.

可以发现 $kerf$ 一定是 G 的子群. 此外，对于任意 $a\in G, b\in kerf$, 都有 $aba^{-1}\in kerf$.

Definition 1.19 Normal Subgroup

群 G 的子群 H 如果满足对于任意的 $a\in G, h\in H$ 都有 $aha^{-1}\in H$ 成立，则称 H 是 G 的正规子群.

显然所有交换群的子群都是正规子群.

Theorem 1.20 How to Check Normal Subgroup

(i) 子群 H 是 G 的正规子群，当且仅当 H 与其共轭相等

(ii) 子群 H 是 G 的正规子群，当且仅当对于每一个 $a \in G$, 都有左陪集 aH 和右陪集 Ha 相等.

Theorem 1.21

如果子群 H 是 G 的正规子群，那么子群上的陪集 aH 关于运算 $(aH)(bH) = (ab)H$ 形成群.

Definition 1.22 Factor Group

对于 G 的正规子群 H, G 模 H 在 **Theorem 1.21** 中的运算下的陪集被称作商集. 记做 G/H.

如果商集是有限集，那么它的阶等于子群 H 在 G 中的指数. 即

$$|G/H| = \frac{|G|}{|H|}$$

每一个 G 的正规子群都确定了一个 G 的同态.

Theorem 1.23 Homomorphism Theorem

设 $f : G \to f(G) = G_1$ 是一个 G 到 G_1 的同态映射，那么 $kerf$ 是 G 的正规子群，且 G_1 与商集 $G/kerf$ 同构.

反过来，如果 H 是 G 的任意一个正规子群，定义映射 $\phi : G \to G/H$ 为 $\phi(a) = aH, a \in G$, 那么这个映射是一个 G 到 G/H 的同态映射，其中 $ker\phi = H$.

Definition 1.24 Normalizer

设 S 是群 G 的一个非空子集. S 在 G 中的正规化子被定义为 $N(S) = \{a \in G : aSa^{-1} = S\}$

Theorem 1.25

对于群 G 的任意一个非空子集 S, $N(S)$ 是 G 的子群，且 G 模 $N(S)$ 的陪集和 S 的不同共轭 aSa^{-1} 间存在一一对应关系.

证明： 因为 $e \in N(S)$, 如果 $a, b \in N(S)$, 那么根据定义 a^{-1}, ab 也在 $N(S)$ 内，所以 $N(S)$ 是 G 的一个子群.

那么

$$\begin{aligned} aSa^{-1} = bSb^{-1} \Leftrightarrow S = a^{-1}bSb^{-1}a = (a^{-1}b)S(a^{-1}b)^{-1} \\ \Leftrightarrow a^{-1}b \in N(S) \Leftrightarrow b \in aN(S) \end{aligned}$$

因此可以知道不同的共轭相等，当且仅当这两个元素属于同一个陪集，所以命题得证.

Definition 1.26 Center

对于任意群 G, G 的中心被定义为集合 $C = \{c \in G : ac = ca\}, \forall a \in G$.

显然群的中心是群的一个正规子群. G 是交换群当且仅当 $C = G$.

Theorem 1.27 Class Equation

设 G 是一个有限群，C 是群的中心，那么

$$|G| = |C| + \sum_{i=1}^{k} n_i$$

其中，n_i 是 $|G|$ 的大于等于 2 的因子. 事实上，$n_1, n_2, \ldots, n_k$ 就是每个超过一个元素的共轭类中的元素个数.

证明：

由于共轭关系是一个等价关系，那么不同的共轭类构成了一个 G 的划分. 因此 $|G|$ 等于所有共轭类的元素个数之和.

而群总共有 $|C|$ 个等价类只含有一个元素，$n_1, n_2, \ldots, n_k$ 就是每个超过一个元素的共轭类中的元素个数，所以得到上面等式.

要证明每一个 n_i 都整除 $|G|$, 只需要注意到 n_i 是某元素 $a \in G$ 的共轭的个数，所以根据 Theorem 1.25 可以知道它等于 G 模 $N(\{a\})$ 的左陪集的个数，所以命题得证.

1.2 Rings and Fields

Definition 1.28 Rings

设集合 R, 两个二元运算 $+$ 和 $\cdot$. 那么 $(R,+,\cdot)$ 是环，当：

（1） R 对于 $+$ 是交换群

（2）$\cdot$ 运算有交换律

（3） $\cdot$ 运算有分配律

下面用 0 来表示加法的单位元，用 $-a$ 表示 a 的加法逆元，$a+(-b)$ 简写为 $a-b$, $a\cdot b$ 简写成 ab.

Definition 1.29 Special Rings and Fields

(1) 含幺环：如果环对于乘法有单位元，即存在元素 e 对于所有 $a\in R$ 都有 $ae=ea=a$, 那么这个环是含幺环.

(2) 交换环：如果环对于乘法满足交换律，那么这个环是交换环.

(3) 整环：如果一个环是交换环，其单位元 $e\neq 0$, 即 $ab=0$ 可以推出 $a=0$ 或 $b=0$, 那么这个环是整环. （没有零因子）

(4) 除环：如果每一个 R 上的非零元素关于乘法形成了群，那么这个环就是除环.

(5) 域：一个交换除环是域.

总结：域对于加法是交换群，对于乘法，非零元形成交换群，且对于乘法有分配律、交换律和结合律.

乘法单位元下面用 1 来表示.

域一定是整环，但是整环不一定是域；在元素个数有限的时候，整环是域.

Example 1.30

整数集是一个整环，但不是域（乘法没有逆元）

Theorem 1.31

每个有限整环都是域.

证明： 设这个整环 R 上的元素为 $a_1,a_2,\dots,a_n$. 对于 某个确定的非零元 $a\in R$, 考虑 $aa_1,aa_2,\dots,aa_n$.

它们是两两不同的，因为如果 $aa_i=aa_j$, 那么 $a(a_i-a_j)=0$, 由于 $a\neq 0$, 所以 $a_i=a_j$.

所以 R 中元素可以写成 aa_i 的形式，其中存在 $1\leq i\leq n$ 使得 $e=aa_i$. 由于 R 是交换环，所以 $a_ia=e$, 所以 a_i 是 a 的逆元.

所以所有 R 中的非零元形成了交换群，所以 R 是交换除环，所以 R 是一个域.

Definition 1.32 Subring

环 R 的子集 S 被称为 R 的子环，如果 S 在 R 的两个运算下也形成群.

Definition 1.33 Ideal

环 R 的子集 J 被称为 R 的理想，当 J 是 R 的子环且对于所有的 $a \in J, r \in R$ 都有 $ar \in J$ 和 $ra \in J$.

Example 1.34

设 $R = \mathbb{Q}$. 那么 $\mathbb{Z}$ 是 $\mathbb{Q}$ 的子环，但不是 $\mathbb{Q}$ 的理想. 这是因为对于 $1 \in \mathbb{Z}, 0.5 \in \mathbb{Q}, 1 \times 0.5 = 0.5 \notin \mathbb{Z}$.

设 R 是一个交换环，那么它的最小的包含 $a \in R$ 的理想是 $(a) = \{ra + na : r \in R, n \in \mathbb{Z}\}$. 如果 R 有单位元，那么 $(a) = \{ra : r \in R\}$.

Definition 1.35 Principal Ideal

设 R 是一个交换环. J 是 R 的理想. 如果存在 $a \in R$ 使得 $J = (a)$, 那么 J 是 R 的主理想. J 被称为由 a 生成的主理想.

理想构成了环 R 的划分，被称为模 J 的剩余类，包含元素 a 的模 J 剩余类可以记做 $[a] = a + J$.

可以发现环 R 上的不同的模 J 剩余类对于下列运算形成群

$$(a + J) + (b + J) = (a + b) + J$$
$$(a + J)(b + J) = ab + J$$

Definition 1.36 Residue Class Ring (Factor Ring)

环 R 模 J 形成的满足上面两个运算形成的剩余类的环被称为剩余类环，记做 R/J.

Example 1.37

考虑环 $\mathbb{Z}/(n)$.

元素有 $[0] = 0 + (n), [1] = 1 + (n), \ldots, [n-1] = n - 1 + (n)$.

Theorem 1.38

整数集模一个由素数生成的主理想所形成的环是一个域. 即 $\mathbb{Z}/(p)$ 是一个域，其中 p 是素数.

证明： 元素的有限性显然，由 **Theorem 1.31** 只需要证明 $\mathbb{Z}/(p)$ 是一个整环.

可以发现 $[1]$ 是这个环的单位元，$[a][b] = [ab] = [0]$ 当且仅当存在整数 k 使得 $ab = kp$.

但是 p 是素数，所以 $p \mid ab$ 当且仅当 p 整除 a, b 的任意一个因子. 所以就有 $[a] = [0]$ 或者 $[b] = [0]$, 所以 $\mathbb{Z}/(p)$ 无零因子.

所以其是一个整环，也就是一个域.

Discussion 1.39 Homomorphism, Kernel and Isomorphism

例子是同 Example 1.7 的卡莱图 过于简单，此处省略. 例子是对 $\mathbb{Z}/(3)$ 的一个列举.

根据上面的 **Theorem 1.38** 可以知道 $\mathbb{Z}/(3)$ 是一个有限域.

环的同态和群类似，考虑映射 $\phi : R \to S$, 其中 R, S 都是环，如果对于任意 $a, b \in R$ 都有

$$\phi(a+b) = \phi(a) + \phi(b)$$
$$\phi(ab) = \phi(a)\phi(b)$$

那么这个映射就是一个同态映射.

核被定义为集合

$$ker\phi = \{a \in R : \phi(a) = 0 \in S\}$$

是加法单位元的原像集.

如果 ϕ 是一一映射，那么 ϕ 就是一个同构映射，环 R 和 S 同构.

Theorem 1.40 Homomorphism Theorem for Rings

如果 ϕ 是 R 到 S 的同态映射，那么 $ker\phi$ 是 R 和 S 的一个理想，且同构于 $R/ker\phi$.

反过来，如果 J 是环 R 的理想，那么映射 $\phi : R \to R/J, \phi(a) = a + J, a \in R$ 是一个 R 到 R/J 的同态映射，它的核是 J.

Definition 1.41 Finite Field

对于素数 p, 令 $\mathbb{F}_p$ 表示整数集合 $\{0, 1, \ldots, p-1\}$. 令 $\phi : \mathbb{Z}/(p) \to \mathbb{F}_p, \phi([a]) = a, a = 0, 1, \ldots, p-1$.

那么这个 $\mathbb{F}_p$ 就是一个有限域，被称为阶为 p 的伽罗瓦域.

可以发现这个域和 $\mathbb{Z}/(p)$ 是同构的.

Example 1.42

考虑 $\mathbb{Z}/(2)$.

+	**0**	**1**
0	0	1
1	1	0

·	**0**	**1**
0	0	0

·	**0**	**1**
1	0	1

Definition 1.43 Characteristic of Rings

设 R 是一个环，如果存在一个正整数 n 使得对于所有的 $r \in R$ 都有 $nr = 0$.

那么满足这个条件的最小正整数 n 就被称为环 R 的特征，R 有特征 n.

如果这样的正整数 n 不存在，那么 R 的特征就是 0.

Theorem 1.44

如果一个环 $R \neq \{0\}$, 它的特征为正，有单位元且没有零因子，那么这个环的特征是素数.

证明： 设环的特征为 n.

由于环含有非零的元素，所以 $n \geq 2$. 假设它不是一个素数，那么 $n = km, k, m \in \mathbb{Z}, 1 < k, m < n$. 那么就有 $0 = ne = (km)e = (ke)(me)$, 由于 R 无零因子，所以 $ke = 0$ 或 $me = 0$.

所以 $kr = (ke)r = 0$ 或 $mr = (me)r = 0$ 对于所有 $r \in R$ 成立，这和特征 n 的定义矛盾. 所以假设不成立，n 是素数.

Corollary 1.45

有限域的特征是素数.

证明： 由 **Theorem 1.44** 只需要证明有限域的特征为正. 考虑单位元的倍数 $e, 2e, 3e \ldots$. 由于 F 只含有有限个元素，那么必然存在两个整数 $k, m, 1 \leq k < m$ 满足 $ke = me$, 即 $(m - k)e = 0$.

所以 F 的特征是正数. 所以特征是素数.

有限域 $\mathbb{Z}/(p)$ 的特征是 p.

特别的，当 $p = 2$ 时，有 $2a = 0 = a + a$, 所以 $a = -a$ 对于 $a \in \mathbb{Z}/(2)$ 恒成立.

Theorem 1.46

设 R 是一个交换环，特征是素数 p. 那么对于任意的 $a, b \in R, n \in \mathbb{N}$ 都有

$$(a + b)^{p^n} = a^{p^n} + b^{p^n}$$
$$(a - b)^{p^n} = a^{p^n} - b^{p^n}$$

证明由二项式定理展开显然.

下面给出一些概念：

因子(divisor)： $a \in R$ 是 $b \in R$ 的因子，如果存在 $c \in R$ 使得 $ac = b$.

单位(unit)： 单位元的因子.

相伴(associate): 两个元素 $a, b \in R$ 相关，如果存在 R 的一个单位 ϵ 使得 $a = b\epsilon$.

素元(prime element): 一个元素 $c \in R$ 是素元，如果这个元素不是单位，且它只有 R 的单位和与 c 相伴的两个因子.

Discussion 1.46 Prime Ideal, Maximal Ideal and Principal Ideal Domain

一个理想 $P \neq R$ 是环 R 的素理想，如果对于任意的 $a, b \in R$, 有 $ab \in P$ 当且仅当 $a \in P$ 或者 $b \in P$.

一个理想 $M \neq R$ 是环 R 的极大理想，如果对于 R 的所有理想 J, $M \subseteq J$ 可以推出 $J = R$ 或 $J = M$.

环 R 被称为主理想环，如果 R 是一个整环，且每一个 R 的理想 J 都是 R 的主理想. 即存在一个 J 的生成元 a 使得 $J = (a) = \{ra : r \in R\}$.

Theorem 1.47

(i) 一个理想 M 是 R 的极大理想，当且仅当 R/M 是一个域.

(ii) 一个理想 P 是 R 的素理想，当且仅当 R/P 是一个整环.

(iii) 每个 R 的极大理想都是一个素理想.

(iv) 如果 R 是一个主理想环，那么 $R/(c)$ 是一个域，当且仅当 c 是环 R 上的素元.

证明：

(i)

（1）设 M 是 R 的极大理想。

那么对于 $a \notin M, a \in R$, 集合 $J = \{ar + m : r \in R, m \in M\}$ 是 R 的一个真包含 M 的理想，所以 $J = R$.

记 1 为环 R 的乘法单位元，那么就存在 $r \in R, m \in M$ 使得 $ar + m = 1$. 也就是说，如果 $a + M \neq 0 + M$ 是一个 R/M 中非零的元素，那么它就有乘法逆元，这是因为 $(a + M)(r + M) = ar + M = (1 - m) + M = 1 + M$.

因此 R/M 是一个域.

（2）反过来，设 R/M 是一个域，设 $J \supseteq M, J \neq M$ 是 R 的一个理想. 那么对于 $a \in J, a \notin M$, 剩余类 $a + M$ 有乘法逆元，所以存在 $r \in R$ 使得 $(a + M)(r + M) = 1$.

因此就存在 $m \in M$ 使得 $ar + m = 1$. 又因为 J 是一个理想，所以有 $1 \in J$, 所以 $(1) = R \subseteq J$, 所以 $J = R$.

因此 M 是 R 的极大理想.

(ii)

（1）设 P 是 R 的素理想. 那么 R/P 是一个交换环，单位元 $1 + P \neq 0 + P$. 令 $(a + P)(b + P) = 0 + P$, 则有 $ab \in P$.

因为 P 是素理想，所以有 $a \in P$ 或者 $b \in P$, 即 $a+P=0+P$ 或 $b+P=0+P$. 所以 R/P 没有零因子，是一个整环.

（2）逆命题同理.

(iii) 由于每个域都是整环，所以此条根据 (i) (ii) 显然.

(iv)

（1）设 $c \in R$. 如果 c 是一个单位，那么 $(c)=R$, 那么环 $R/(c)$ 只有一个元素，不是域.

（2）如果 c 不是一个单位，也不是素元，那么它就有因子 $a \in R$, 这个因子不是一个单位，也不和 c 相伴.

注意到 $a \neq 0$. 因为如果 $a=0$ 那么就有 $c=0$ 从而就可以得到 a 和 c 相伴，矛盾. 所以可以将 c 写成 $c=ab$, 其中 $b \in R$.

下面要证明 $a \notin (c)$.

如果 $a \in (c)$ 那么就存在 $d \in R$ 使得 $a=cd=abd$, 即 $a(1-bd)=0$. 由于 $a \neq 0$, 所以 $bd=1$. 所以 d 是一个单位，得到 a 和 c 相伴，矛盾.

因此 $(c) \subsetneqq (a) \subsetneqq R$, 所以根据 (i), $R/(c)$ 就不是一个域.

（3）如果 c 是一个素元，那么由于 c 不是一个单位，那么 $(c) \neq R$.

又因为 R 是一个主理想环，所以对于 R 的一个理想 $J \supseteq (c)$, 那就存在 $a \in R$ 使得 $J=(a)$.

因此 $c \in (a)$, 因此 a 是 c 的因子. 所以 a 要么与 c 相伴，要么是一个单位. 所以要么 $J=R$, 要么 $J=(c)$.

因此 (c) 是 R 的极大理想，根据 (i) 可以知道 $R/(c)$ 是一个域.

下面考虑这个定理的一个应用. 令 $R=\mathbb{Z}$. $\mathbb{Z}$ 是一个主理想整环. p 为素数.

那么根据该定理的 (iv) 可以知道 $\mathbb{Z}/(p)$ 是一个域. (p) 是 $\mathbb{Z}$ 的极大理想，也是素理想.

对于合数 n 来说，理想 (n) 并不是 $\mathbb{Z}$ 的主理想，所以 $\mathbb{Z}/(n)$ 也不是整环,

1.3 Polynomials

考虑环 R 上的多项式，它由下面的形式表示

$$f(x)=\sum_{i=0}^{n}a_ix^i=a_0+a_1x+\ldots+a_nx^n$$

其中 n 是非负整数，系数 a_i 是 R 上的元素，x 是未定元. 两个多项式相等当且仅当所有对应幂次的系数相等.

设:

$$f(x)=\sum_{i=0}^{n}a_ix^i\quad g(x)=\sum_{i=0}^{n}b_ix^i$$

那么加法定义为:

$$f(x)+g(x)=\sum_{i=0}^{n}(a_i+b_i)x^i$$

设:

$$f(x)=\sum_{i=0}^{n}a_ix^i\quad g(x)=\sum_{j=0}^{m}b_ix^i$$

那么乘法定义为:

$$f(x)g(x)=\sum_{k=0}^{n+m}c_kx^k$$

其中

$$c_k=\sum_{i+j=k,0\leq i\leq n,0\leq j\leq m}a_ib_j$$

Definition 1.48 Polynomial Ring

由 R 上的多项式所形成的，由上面的加法和乘法所定义的环被称为 R 上的多项式环，记做 $R[x]$.

这个环的零元是零多项式，记为 0.

Definition 1.49 Degree and Monic Polynomial

设 $f(x)=\sum_{i=0}^{n}a_ix^i$ 是 R 上的多项式，且不是零多项式，$a_n\neq 0$. 那么 a_n 被称为首项系数, a_0 为常数项, n 被称为多项式的次数，记做 $n=deg(f(x))=deg(f)$. 特别地，定义 $deg(0)=-\infty$.

如果一个多项式的次数小于等于 0, 那这个多项式是常数多项式.

如果 R 有单位元 1 且 $f(x)$ 的首项系数是 1, 那么 $f(x)$ 是首一多项式.

Theorem 1.50

设 $f, g \in R[x]$, 那么:

$$deg(f+g) \leq max(deg(f), deg(g))$$
$$deg(fg) \leq deg(f) + deg(g)$$

如果 R 是一个整环，那么:

$$deg(fg) = deg(f) + deg(g)$$

Theorem 1.51

设 R 是一个环，那么:

(i) $R[x]$ 是交换环当且仅当 R 是交换环.

(ii) $R[x]$ 是有单位元的环，当且仅当 R 有单位元.

(iii) $R[x]$ 是整环，当且仅当 R 是整环.

Theorem 1.52 Division Algorithm

设 $g \neq 0$ 是 $F[x]$ 上的多项式. 那么对于任意的 $f \in F[x]$ 都存在多项式 $q, r \in F[x]$ 使得

$$f = qg + r$$

其中 $deg(r) < deg(g)$.

Example 1.53 Long Division

长除法过程略. 考虑 $f(x) = 2x^5 + x^4 + 4x + 3, g(x) = 3x^2 + 1$, $f(x), g(x) \in \mathbb{F}_5[x]$.

那么根据长除法求 $q, r \in \mathbb{F}_5[x]$ 使得 $f = qg + r$ 可以得到 $q(x) = 4x^3 + 2x^2 + 2x + 1, r(x) = 2x + 2$.

Theorem 1.54

$F[x]$ 是一个主理想整环. F 是一个域.

事实上，对于每个 $F[x]$ 的理想 $J \neq (0)$ 都存在唯一的首一多项式 $g \in F[x]$ 满足 $J = (g)$.

证明:

1. **存在性:**

首先根据 **Theorem 1.51** 可知 $F[x]$ 是一个整环. 设 $J \neq (0)$ 是 $F[x]$ 的一个理想. 令 $h(x)$ 是一个 J 中的最低次非零多项式.

设 b 是 $h(x)$ 的首项系数，令 $g(x) = b^{-1}h(x)$. 那么就有 $g \in J$ 且为首一多项式.

2. **唯一性:**

设 $f(x)$ 是一个任意多项式，那么根据 **Theorem 1.52** 可知，存在 $q, r \in F[x]$, 使得 $f = qg + r$ 且 $deg(r) < deg(g) = deg(h)$

由于 J 是一个理想，那么就有 $f - qg = r \in J$, 根据 $h(x)$ 的定义可以知道 $r = 0$. 因此 f 是 g 的倍数，所以 $f = (g)$.

如果 $g_1 \in F[x]$ 是另一个满足 $J = (g_1)$ 的首一多项式，那么 $g = c_1 g_1$, $g_1 = c_2 g$, $c_1, c_2 \in F[x]$.

所以就有 $g = c_1 c_2 g$, 所以 $c_1 c_2 = 1$, c_1, c_2 都是常数多项式.

又因为 g 和 g_1 都是首一的，所以 $g = g_1$.

Theorem 1.55

设 $f_1, f_2, \ldots, f_n$ 是 $F[x]$ 上的多项式，不全为 0. 那就存在唯一的首一多项式 $d \in F[x]$ 满足：

(i) d 整除每个 $f_j, 1 \leq j \leq n$.

(ii) 可以整除每个 $f_j, 1 \leq j \leq n$ 的多项式 $c \in F[x]$ 都整除 d.

此外， d 可以表示为：

$$d = b_1 f_1 + \ldots + b_n f_n, b_1, \ldots, b_n \in F[x] \tag{1.2}$$

证明：

1. **存在性：**

设集合 J 是形如 $c_1 f_1 + \ldots + c_n f_n, c_1, \ldots, c_n \in F[x]$ 的所有多项式，那么显然 J 是 $F[x]$ 的一个理想.

由于 f_j 不全为零，所以 $J \neq (0)$. 所以根据 **Theorem 1.54** 可知存在首一多项式 $d \in F[x]$ 使得 $J = (d)$.

所以由 (1.2) 的形式可以知道存在性得证.

2. **唯一性：**

设 d_1 是另一个 $F[x]$ 上满足题设条件的首一多项式，那么根据性质可以知道 d 和 d_1 互相整除，所以 $(d) = (d_1)$.

那么根据 Theorem 1.54 中唯一性的证明过程，可以知道 $d = d_1$. 所以唯一性得证.

Example 1.56 Euclideam algorithm

两个多项式也可以进行和整数一样的欧几里得算法. 设 $f(x) = 2x^6 + x^3 + x^2 + 2, g(x) = x^4 + x^2 + 2x, f, g \in \mathbb{F}_3[x]$.

那么：

$$\begin{aligned} 2x^6 + x^3 + x^2 + 2 &= (2x^2 + 1)(x^4 + x^2 + 2x) + x + 2 \\ x^4 + x^2 + 2x &= (x^3 + x^2 + 2x + 1)(x + 2) + 1 \\ x + 2 &= (x + 2)1 \end{aligned}$$

所以就有 $gcd(f, g) = 1$.

求最小公倍数 (lcm) 的时候则有：

$$a^{-1}fg = lcm(f,g)gcd(f,g)$$

其中 a 是 fg 的首项系数.

同时有

$$gcd(f_1,f_2,\dots,f_n) = gcd(f_1, gcd(f_2,\dots,f_n)) = \dots$$
$$lcm(f_1,f_2,\dots,f_n) = lcm(f_1, lcm(f_2,\dots,f_n)) = \dots$$

Definition 1.57 Irreducible Polynomial

如果多项式 $p \in F[x]$ 满足 p 的次数为正且 $p = bc, b, c \in F[x]$ 意味着 b 或 c 是一个常数多项式，那么称 p 在 $F[x]$ 上不可约.

例如多项式 $x^2 - 2$ 在 $\mathbb{Q}$ 上不可约，但是在 $\mathbb{R}$ 上可约，因为 $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$

因为环上的多项式可以写成一系列不可约多项式的形式，所以不可约多项式的研究是构造环的基础.

Lemma 1.58

如果不可约多项式 $p \in F[x]$ 可以整除 $f_1 \dots f_m \in F[x]$, 那么 p 至少可以整除 f_1 到 f_m 中的其中一个多项式.

证明：

因为 p 整除 $f_1 \dots f_m$, 所以 $(f_1 + (p)) \dots (f_m + (p)) = 0 + (p)$ 是商环 $F[x]/p$ 的单位元.

根据 **Theorem 1.47(iv)** 可以知道这个商环是一个域，所以如果对于某个 j 满足 $f_j + (p) = 0 + (p)$, 那么就有 p 整除 f_j.

Theorem 1.59 Unique Factorization in F[x]

每个正系数多项式 $f \in F[x]$ 都可以写成

$$f = ap_1^{e_1} \dots p_k^{e_k} \tag{1.3}$$

其中 $a \in F, p_1, \dots, p_k$ 是 $F[x]$ 上的不同的首一不可约多项式, $e_1, \dots, e_k$ 是正整数. 且这个分解是唯一的.

证明：

1. 存在性：

将 $f(x)$ 表示为式 (1.3) 的形式. 下面由数学归纳法证明.

如果 $deg(f) = 1$ 结论显然，其本身就是 F 上的不可约多项式.

假设对于 $deg(f) < n$ 的时候结论都成立.

当 $deg(f) = n$ 时，如果 f 本身在 F 上不可约，那么 $f = a(a^{-1}f)$, 其中 a 是首项系数，$a^{-1}f$ 是首一不可约多项式.

如果 f 可约，那么设 $f = gh, 1 \le deg(g) < n, 1 \le deg(h) < n, g, h \in F[x]$. 根据归纳假设，$g, h$ 都可以写成式 (1.3) 的形式，所以 f 也可以写成这样的形式.

2. 唯一性：

假设存在两种不一样的分解形式，即

$$f = ap_1^{e_1} \dots p_k^{e_k} = bq_1^{d_1} \dots q_r^{d_r} \tag{1.4}$$

通过对比系数可以知道 $a = b$. 可以知道不可约多项式 p_1 整除式 (1.4) 的右侧，所以根据 **Lemma 1.58** 可以知道存在一个 $j, 1 \leq j \leq r$ 使得 p_1 整除 q_j. 但是 q_j 也是不可约多项式，那么就有 $q_j = cp_1$, 其中 c 是一个常数多项式.

由于 q_j 和 p_1 都是首一多项式，所以就有 $q_j = p_1$. 所以就可以对两侧进行约分.

重复这一步骤就可以去掉所有因子了. 所以唯一性得证.

Example 1.60

找出 $\mathbb{F}_2$ 上所有次数为 4 的不可约多项式.

解： 总共有 16 个 $\mathbb{F}_2$ 上的次数为 4 的多项式，一个 $\mathbb{F}_2$ 上的多项式可约，当且仅当它有一个次数为 1 或 2 的因子.

所以可以枚举所有 $(a_0 + a_1x + a_2x^2 + x^3)(b_0 + x)$ 和 $(a_0 + a_1x + x^2)(b_0 + b_1x + x^2)$, 其中 $a_i, b_j \in \mathbb{F}_2$

比较结果和所有的 16 个多项式可以得到以下三个多项式是在 $\mathbb{F}_2$ 上不可约的.

$$f_1(x) = x^4 + x + 1$$
$$f_2(x) = x^4 + x^3 + 1$$
$$f_3(x) = x^4 + x^3 + x^2 + x + 1$$

Theorem 1.61

对于每个 $f \in F[x]$, 剩余类环 $F[x]/f$ 是域，当且仅当 f 在 F 上不可约.

Example 1.62

(1) 设 $f(x) = x \in \mathbb{F}_2[x]$. 那么就有 $p^n = 2^1$ 个次数小于 1 的多项式，它们组成了所有 $\mathbb{F}_2[x]/(x)$ 的剩余类

因此 $\mathbb{F}_2[x]/(x)$ 包含了剩余类 $[0]$ 和 $[1]$ 并同构于 $\mathbb{F}_2$.

(2) 考虑 $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$. 那么 $\mathbb{F}_2[x]/f$ 就有 $p^n = 2^2$ 个元素 $[0]$, $[1]$, $[x]$, $[x + 1]$. 所以运算规则如下.

+	**[0]**	**[1]**	**[x]**	**[x+1]**
[0]	[0]	[1]	[x]	[x+1]
[1]	[1]	[0]	[x+1]	[x]
[x]	[x]	[x+1]	[0]	[1]
[x+1]	[x+1]	[x]	[1]	[0]

×	**[0]**	**[1]**	**[x]**	**[x+1]**
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[x]	[x+1]
[x]	[0]	[x]	[x+1]	[1]
[x+1]	[0]	[x+1]	[1]	[x]

这些运算都是模 $f = x^2 + x + 1$ 之后的结果.

Definition 1.63 Root

$b \in F$ 是多项式 $f \in F[x]$ 的一个根，如果 $f(b) = 0$.

Theorem 1.64

一个元素 $b \in F$ 是多项式 $f \in F[x]$ 的根，当且仅当 $x - b$ 整除 $f(x)$.

证明：

根据 **Theorem 1.52** 可以知道 $f(x) = q(x)(x - b) + c, q \in F[x], c \in F$. 令 $x = b$ 可以得到 $f(b) = c$.

因此 $f(x) = q(x)(x - b) + f(b)$. 所以当且仅当 $f(b) = 0$ 时 $(x - b) \mid f(x)$.

Definition 1.65 Multiplicity, Simple Root and Multiple Root

设 $b \in F$ 是多项式 $f \in F[x]$ 的根. 如果 k 满足多项式可以被 $(x - b)^k$ 整除但不可以被 $(x - b)^{k+1}$ 整除，那么这个 k 叫做根 b 的重数.

如果 $k = 1$ 那么 b 是 $f(x)$ 的单根，如果 $k \geq 2$ 那么 b 是 $f(x)$ 的重根.

Theorem 1.66

设 $f \in F[x]$, 次数为 $n, n \geq 0$. 如果 $b_1, \ldots, b_m \in F$ 是 f 的不同根，重数分别为 $k_1, \ldots, k_m$, 那么就有 $(x - b_1)^{k_1} \ldots (x - b_m)^{k_m}$ 整除 $f(x)$. 同时 $k_1 + \ldots + k_m \leq n$, f 在 F 上最多有 n 个不同的根.

证明：容易发现对于所有的 $x - b_j, 1 \leq j \leq m$ 它们都是 F 上的不可约多项式，所以 $(x - b_j)^{k_j}$ 就是 f 的标准分解的一个因子.

同理，$(x - b_1)^{k_1} \ldots (x - b_m)^{k_m}$ 都是 f 标准分解的一个因子，比较次数可知 $k_1 + \ldots + k_m \leq n$.

Definition 1.67 Derivative

设 $f(x)=a_0+a_1x+a_2x^2+\ldots+a_nx^n\in F[x]$, 那么 $f(x)$ 的导数定义为 $f'=f'(x)=a_1+2a_2x+\ldots+na_nx^{n-1}\in F[x]$.

Theorem 1.68

$b\in F$ 是 $f\in F[x]$ 的重根，当且仅当 b 同时为 f 和 f' 的根.

Theorem 1.69

次数为 2 或者 3 的多项式 $f\in F[x]$ 在 $F[x]$ 上不可约，当且仅当 f 在 F 上没有根.

证明： 正向显然.

如果 f 在 F 上没有根且在 $F[x]$ 上可约，那么 $f=gh, g,h\in F[x], 1\leq deg(g)\leq deg(h)$.

但是 $deg(g)+deg(h)=deg(f)\leq 3$, 所以 $deg(g)=1$. 所以 $g(x)=ax+b, a,b\in F, a\neq 0$.

所以 $g(x)$ 有一个根 $-ba^{-1}$, 也是 $f(x)$ 的根，这和 f 在 F 上没有根矛盾. 所以 f 在 $F[x]$ 上不可约.

Example 1.70

考虑 $\mathbb{F}_2[x]$ 上的次数为 2 和 3 的多项式，可以发现不可约多项式只有 $f(x)=x^2+x+1$, $f(x)=x^3+x+1$ 和 $f(x)=x^3+x^2+1$.

Theorem 1.71 Lagrange Interpolation Formula

设 $n\geq 0, a_0,\ldots,a_n$ 是 F 中的不同的 $n+1$ 个元素，$b_0,\ldots,b_n$ 是 F 上的任意的 $n+1$ 个元素. 那么存在唯一一个多项式 $f\in F[x]$, 它的次数为 n, 且对于 $i=0,\ldots,n$ 有 $f(a_i)=b_i$. 这个多项式是：

$$f(x)=\sum_{i=0}^{n}b_i\prod_{k=0,k\neq i}^{n}(a_i-a_k)^{-1}(x-a_k)$$

Definition 1.72 Degree, Term and Homogeneous

设 $f\in R[x_1,\ldots,x_n]$ 定义为

$$f(x_1,\ldots,x_n)=\sum a_{i_1\ldots i_n}x_1^{i_1}\ldots x_n^{i_n}$$

如果 $a_{i_1\ldots i_n}\neq 0$, 那么 $a_{i_1\ldots i_n}x_1^{i_1}\ldots x_n^{i_n}$ 被称为 f 的项，$i_1+\ldots+i_n$ 被称为这个项的次数.

对于 $f\neq 0$ 定义多项式 f 的次数为最大项的次数，记作 $\deg(f)$. 对于 $f=0$ 记 $\deg(f)=-\infty$.

如果 $f=0$ 或 f 的每一项次数都相同，则称 f 是齐次式.

每个多项式 $f\in R[x_1,\ldots,x_n]$ 都可以写成有限个齐次多项式的和. $R[x_1,\ldots,x_n]$ 中的多项式的次数满足 **Theorem 1.50**.

如果 R 是整环，那么对应的 $R[x_1,\ldots,x_n]$ 也是整环；如果 F 是一个域，那么 $F[x_1,\ldots,x_n]$ 上的正次数多项式可以被唯一分解成一个常数和若干个首一多项式的乘积. 但是当 $n\geq 2$ 时，不存在类似带余除法的表示，且 $F[x_1,\ldots,x_n]$ 不是主理想整环.

Definition 1.73 Symmetric

多项式 $f\in R[x_1,\ldots,x_n]$ 是对称的，如果 $f(x_{i_1},\ldots,x_{i_n})=f(x_1,\ldots,x_n)$ 对于所有的关于整数 $1,\ldots,n$ 的排列 $i_1,\ldots,i_n$ 都成立.

Example 1.74

设 $z\in R[x_1,\ldots,x_n]$ 是一个未定元，令 $g(z)=(z-x_1)(z-x_2)\ldots(z-x_n)$, 那么

$$g(z)=z^n-\sigma_1 z^{n-1}+\sigma_2 z^{n-2}+\ldots+(-1)^n\sigma_n$$

其中

$$\sigma_k=\sigma_k(x_1,\ldots,x_n)=\sum_{1\leq i_1<\ldots<i_k\leq n}x_{i_1}\ldots x_{i_n}(k=1,2,\ldots,n)$$

因此

$$\begin{gathered}\sigma_1=x_1+x_2+\ldots+x_n\\ \sigma_2=x_1x_2+x_1x_3+\ldots+x_1x_n+x_2x_3+\ldots+x_2x_n+\ldots+x_{n-1}x_n\\ \vdots\\ \sigma_n=x_1x_2\ldots x_n\end{gathered}$$

因为 g 在任意的 x_i 的排列下保持不变，所以所有的 σ_n 都是对称多项式，也都是齐次式

$\sigma_k=\sigma_k(x_1,\ldots,x_n)\in R[x_1,\ldots,x_n]$ 被称为 $k-$初等对称多项式.

Theorem 1.75 Newton's Formula

设 $\sigma_1,\ldots,\sigma_n$ 是关于 $x_1,\ldots,x_n$ 的在 R 上的初等对称多项式。

令 $s_0=n\in\mathbb{Z}$ 且对于 $k\geq 1$ 有 $s_k=s_k(x_1,\ldots,x_n)=x_1^k+\ldots+x_n^k\in R[x_1,\ldots,x_n]$. 那么对于 $k\geq 1$ 有

$$s_k-s_{k-1}\sigma_1+s_{k-2}\sigma_2+\ldots+(-1)^{m-1}s_{k-m+1}\sigma_{m-1}+(-1)^m\frac{m}{n}s_{k-m}\sigma_m=0$$

其中 $m=\min(k,n)$.

Theorem 1.76 Waring's Formula

在 **Theorem 1.75** 的条件和记号下，对于 $k\geq 1$ 有

$$s_k=\sum(-1)^{i_2+i_4+i_6\ldots}\frac{(i_1+i_2+\ldots+i_n-1)!k}{i_1!i_2!\ldots i_n!}\sigma_1^{i_1}\sigma_2^{i_2}\ldots\sigma_n^{i_n}$$

其中 $i_1+2i_2+\ldots+ni_n=k$.

$\sigma_1^{i_1}\sigma_2^{i_2}\dots\sigma_n^{i_n}$ 的系数一定是整数.

1.4 Field Extensions

设 F 是一个域，K 是 F 的一个子集，如果 K 在 F 的运算下也是一个域，那么 K 就是 F 的子域. F 是 K 的一个域扩张.

如果 $K \neq F$ 就称 K 是 F 的一个真子域.

Definition 1.77 Prime Field

一个不包含任何真子域的域叫做素域.

Theorem 1.78 Properties of Prime Field

一个域 F 的素域同构于 $\mathbb{F}_p$ 或者 $\mathbb{Q}$. 因为 F 的特征是一个素数 p 或者 0.

Definition 1.79 Simple Extension and Defining Element

设 K 是 F 的子域，M 是 F 的子集。定义：域 $K(M)$ 为所有包含 K 和 M 的域 F 的子域的交，$K(M)$ 被称为 K 的通过 M 中元素邻接得到的域扩张.

对于有限集 $M = \{\theta_1, \ldots, \theta_n\}$, 将其写作 $K(M) = (\theta_1, \ldots, \theta_n)$.

如果 M 由一个元素 $\theta \in F$ 组成，则称 $L = K(\theta)$ 为 K 的单扩张；θ 是 L 在 K 上的定义元.

Definition 1.80 Algebraic Extension

设 K 是 F 的子域， $\theta \in F$. 如果 θ 满足

$$a_n\theta^n + \ldots + a_1\theta + a_0 = 0$$

其中 $a_i \in K$ 不全为 0, 则称 θ 在 K 上是代数的(algebraic over K).

如果某个扩张域 L 中的每个元素都在 K 上是代数的，则称 L 是 K 的代数扩张。

Definition 1.81 Minimal Polynimial

设 $\theta \in F$ 在 K 上是代数元，$g \in K[x]$ 是满足 $g(\theta) = 0$ 的最低次首一多项式. 则称 g 为 θ 在 K 上的极小多项式(也称为不可约多项式).

θ 在 K 上的次数等于 g 的次数.

Theorem 1.82 Properties of Minimal Polynomial

设 $\theta \in F$ 在 K 上是代数的，那么其在 K 上的极小多项式 g 满足：

(i) g 在 $K[x]$ 上不可约.

(ii) 对于 $f \in K[x]$, $f(\theta) = 0$ 当且仅当 $g|f$.

(iii) g 是 $K[x]$ 上次数最小的以 θ 为根的首一多项式.

证明：

(i) 和 (ii) 都在定义中体现。

对于 (iii), 可以发现所有以 θ 为根的 $K[x]$ 上的多项式都必须是 g 的倍数，所以这个多项式要么是 g, 要么次数就会超过 g.

Definition 1.83 Finite Extension and Degree

设 L 是域 K 的扩张. 考虑 L 是 K 上的一个有限维数的向量空间，则称 L 是 K 的一个有限扩张.

线性空间 L 的维数被称为 L 在 K 上的次数，记为 $[L : K]$.

Theorem 1.84

设 L 是 K 的域扩张，M 是 L 的一个有限扩张，那么 M 也是 K 的一个有限扩张，且：

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

证明： 设 $[M : L] = m, [L : K] = n$, 设 $\{a_1, \ldots, a_m\}$ 是 M 在 L 上的一组基，设 $\{b_1, \ldots, b_m\}$ 是 L 在 K 上的一组基.

那么对于每个 $a \in M$ 都是一个线性组合，$a = a_1c_1 + \ldots + a_mc_m, c_i \in L, 1 \leq i \leq m$. 将 c_i 用 b_j 表示可以得到：

$$a = \sum_{i=1}^{m} a_i c_i = \sum_{i=1}^{m} (\sum_{j=1}^{n} r_{ij} b_j) a_i = \sum_{i=1}^{m} \sum_{j=1}^{n} r_{ij} b_j a_i$$

其中 $r_{ij} \in K$. 下面只需要证明这 mn 个元素 $b_j a_i, 1 \leq i \leq m, 1 \leq j \leq n$ 在 K 上线性无关. 假设有

$$\sum_{i=1}^{m} \sum_{j=1}^{n} s_{ij} b_j a_i = 0$$

其中系数 $s_{ij} \in K$, 那么

$$\sum_{i=1}^{m} (\sum_{j=1}^{n} s_{ij} b_j) a_i = 0$$

由于 a_i 是线性无关的，所以

$$\sum_{j=1}^{n} s_{ij} b_j = 0, 1 \leq i \leq m$$

但是由于 b_j 也是线性无关的，所以只能有 $s_{ij} = 0$. 即这 mn 个元素是线性无关的. 所以原式得证.

Theorem 1.85

每个 K 的有限扩张都是代数扩张.

证明： 设 L 是 K 的域扩张，$[L:K]=m$. 对于 $\theta\in L, m+1$ 个元素 $1,\theta,\dots,\theta^m$ 在 K 上是线性相关的.

所以就有 $a_0+a_1\theta+\dots+a_m\theta^m=0$, 其中 $a_i\in K$ 且不全为零.

也就是说 θ 是 K 上的代数元. 所以 L 是代数扩张.

Theorem 1.86

设 $\theta\in F$ 在 K 上是代数的，次数为 n, 设 g 是 K 上关于 θ 的极小多项式，则有：

(i) $K(\theta)$ 和 $K[x]/(g)$ 同构.

(ii) $[K(\theta):K]=n$, 且 $\{1,\theta,\dots,\theta^{n-1}\}$ 是 $K(\theta)$ 在 K 上的一组基.

(iii) 每个 $\alpha\in K(\theta)$ 都是在 K 上代数的；它们在 K 上的次数都是 n 的因子.

证明：

(i) 考虑映射 $h:K[x]\to K(\theta)$, 其中 $h(f)=f(\theta), f\in K[x]$, 显然这是一个环同态.

根据极小多项式的定义，核 $kerh=\{f\in K[x]:f(\theta)=0\}=(g)$.

设 S 是 h 的像，即 S 是关于 θ 的多项式的集合，系数都在 K 内，那么根据环同态理论 **Theorem 1.40** 可以得到 S 同构于 $K[x]/(g)$. 但是根据 **Theorem 1.82(i)** 和 **Thorem 1.61** 可以知道 $K[x]/(g)$ 是一个域，所以 S 是一个域.

因为 $K\subseteq S\subseteq K(\theta), \theta\in S$, 那么根据 $K(\theta)$ 的定义，可以知道 $S=K(\theta)$, 所以 $K(\theta)$ 同构于 $K[x]/(g)$.

(ii) 因为 $S=K(\theta)$, 所以每个给定的 $a\in K(\theta)$ 都可以写成 $a=f(\theta)$, 其中 $f\in K[x]$. 而 f 可以写成 $f=qg+r, q,r\in K[x], deg(r)<deg(g)=n$. 所以 $a=f(\theta)=q(\theta)g(\theta)+r(\theta)$, 因此 a 是 $1,\theta,\dots,\theta^{n-1}$ 的一个线性组合，系数都在 K 内.

另一方面，如果存在确定的 $a_i\in K$ 使得 $a_0+a_1\theta+\dots+a_{n-1}\theta^{n-1}=0$, 那么 $h(x)=a_0+a_1x+\dots+a_{n-1}x^{n-1}\in K[x]$ 就有根 θ, 根据 Theorem 1.82(ii) 可以知道 h 是 g 的倍数.

又因为 $deg(h)<n=deg(g)$, 所以 $h=0$, 那么所有的 $a_i=0$. 因此 $1,\theta,\dots,\theta^{n-1}$ 在 K 上线性无关，是一组基.

(iii) 根据 (ii) 可以知道 $K(\theta)$ 是 K 的域扩张，根据 Theorem 1.85 可以得到 $a\in K(\theta)$ 在 K 上是代数的. 所以 $K(a)$ 是 $K(\theta)$ 的子域.

设 d 是 a 在 K 上的次数，那么 $n=[K(\theta):K]=[K(\theta):K(a)][K(a):K]=[K(\theta):K(a)]d$, 因此 $d\mid n$.

Theorem 1.87

设多项式 $f \in K[x]$ 在域 K 上不可约，那么存在一个 K 的代数单扩张，定义元是 f 的一个根.

证明： 考虑剩余类环 $L = K(x)/f$, 根据 **Theorem 1.61** 由于 f 不可约，所以 $K(x)/f$ 是一个域.

环 L 的元素是 $[h] = h + (f), h \in K[x]$. 对于每个 $a \in K$ 都一个构造出由常多项式 a 决定的剩余类 $[a]$. 由于 f 的次数为正，所以如果 $a, b \in K$ 不同，那么 $[a] \neq [b]$.

考虑映射 $a \to [a]$. 这是一个从 K 到 L 的子域 K' 的同构映射，那么 K' 和 K 相同. 对于每一个 $h(x) = a_0 + a_1x + \ldots + a_mx^m \in K[x]$,

都有 $[h] = [a_0 + a_1x + \ldots + a_mx^m] = [a_0] + [a_1][x] + \ldots + [a_m][x^m] = a_0 + a_1[x] + \ldots + a_m[x^m]$.

因此，每一个 L 中的元素都可以写成关于 $[x]$ 的多项式形式，系数都在 K 中.

因为每个包含 K 和 $[x]$ 的域中都包含这些多项式， 所以 L 是 K 的加入 $[x]$ 形成的单扩张.

如果 $f(x) = b_0 + b_1x + \ldots + b_nx^n$, 那么 $f([x]) = b_0 + b_1[x] + \ldots + b_n[x^n] = [b_0 + b_1x + \ldots + b_nx^n] = [f] = [0]$, 所以 $[x]$ 是 f 的一个根，而且 L 是 K 的代数单扩张.

Example 1.88

考虑素域 $\mathbb{F}_3$ 和不可约多项式 $f(x) = x^2 + x + 2 \in \mathbb{F}_3[x]$.

设 θ 是 f 的一个根，即是 $L = \mathbb{F}_3[x]/(f)$ 中的一个剩余类 $x + (f)$. 因为 $f(2\theta + 2) = (2\theta + 2)^2 + (2\theta + 2) + 2 = \theta^2 + \theta + 2 = 0$, 所以 $2\theta + 2$ 也是 f 的一个根.

那么，根据 **Theorem 1.86(ii)**, 单代数扩张 $L = \mathbb{F}_3(\theta)$ 包含了 9 个元素：$0, 1, 2, \theta, \theta + 1, \theta + 2, 2\theta, 2\theta + 1, 2\theta + 2$. 这是一组基.

Theorem 1.89

设 a, b 是不可约多项式 $f \in K[x]$ 的两个根，那么 $K(a), K(b)$ 在 a 到 b 的同构映射下同构，且 K 中的元素保持不变.

Definition 1.90 Splitting Field

设 $f \in K[x]$ 的次数为正， F 是 K 的一个域扩张。

如果 f 可以被写成若干个 F 上一次因子的乘积，即存在 $a_1, a_2, \ldots, a_n \in F$ 满足：

$$f(x) = a(x - a_1)(x - a_2)\ldots(x - a_n)$$

则称 f 在 F 上可分裂 (split in).

如果 f 在 F 上可分裂且 $F = K(a_1, a_2, \ldots a_n)$, 则称 F 是 f 在 K 上的分裂域.

显然， F 是包含所有 f 的根的最小的域.

Theorem 1.91 Existence and Uniqueness of Splitting Field

如果 K 是一个域，f 是 $K[x]$ 上的一个正次数多项式，那么存在一个 f 在 K 上的分裂域.

任意两个 f 在 K 上的分裂域在一个保持 K 中元素不变且让 f 的根映射到 f 的根的同构映射下，保持同构.

Definition 1.92 Discriminant

设 $f \in K[x]$ 是一个次数 $n \geq 2$ 的多项式，设 $f(x) = a_0(x-a_1)\dots(x-a_n)$, 其中 a_i 是 f 在 K 上的分裂域中的元素.

那么 f 的判别式 $D(f)$ 被定义为：

$$D(f) = a_0^{2n-2} \prod_{1 \leq i < j \leq n} (a_i - a_j)^2$$

根据定义，当且仅当 $D(f) = 0$ 的时候，f 有重根. $D(f)$ 也是 K 中的一个元素.

例如 $n = 2, f(x) = ax^2 + bx + c = a(x-a_1)(x-a_2)$, 那么 $D(f) = a^2(a_1 - a_2)^2 = a^2((a_1+a_2)^2 - 4a_1a_2) = a^2(b^2a^{-2} - 4ca^{-1})$.

化简得到 $D(f) = b^2 - 4ac$.

设多项式 $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$ 那么称 n 为 $f(x)$ 的形式次数，显然这个值一定大于等于 $deg(f)$. 这里的 a_n 可以为零.

Definition 1.93 Resultant

设 $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n \in K[x], g(x) = b_0x^m + b_1x^{m-1} + \dots + b_m \in K[x]$. 它们的形式次数分别为 $n, m \in \mathbb{N}$.

那么结式 $R(f,g)$ 被定义为行列式

$$R(f,g) = \begin{vmatrix} a_0 & a_1 & \dots & a_n & 0 & & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_n & 0 & \dots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \dots & 0 & a_0 & a_1 & & \dots & a_n \\ b_0 & b_1 & \dots & & b_m & 0 & \dots & 0 \\ 0 & b_0 & b_1 & \dots & & b_m & \dots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \dots & 0 & b_0 & b_1 & & \dots & b_m \end{vmatrix}$$

行列式的阶为 $m+n$.

如果 $deg(f) = n$ 且 $f(x) = a_0(x-\alpha_1)\dots(x-\alpha_n)$ 并在 f 在 K 的分裂域上，那么 $R(f,g)$ 可以表示为

$$R(f,g) = a_0^m \prod_{i=1}^{n} g(\alpha_i)$$

显然，$R(f,g) = 0$ 当且仅当 f 和 g 有相同的根.

Theorem 1.68 提到 $b \in F$ 是 $f \in F[x]$ 的重根，当且仅当 b 同时为 f 和 f' 的根. 这可以得到判别式 $D(f)$ 和结式 $R(f,f')$ 之间的关系。

设 $f \in K[x], deg(f) = n \geq 2$, 首项系数为 a_0，那么

$$D(f) = (-1)^{n(n-1)/2} a_0^{-1} R(f, f')$$

总之，可以通过计算一个阶为 $2n-1$ 的关于 K 中元素的判别式来获得 $D(f)$ 的值.