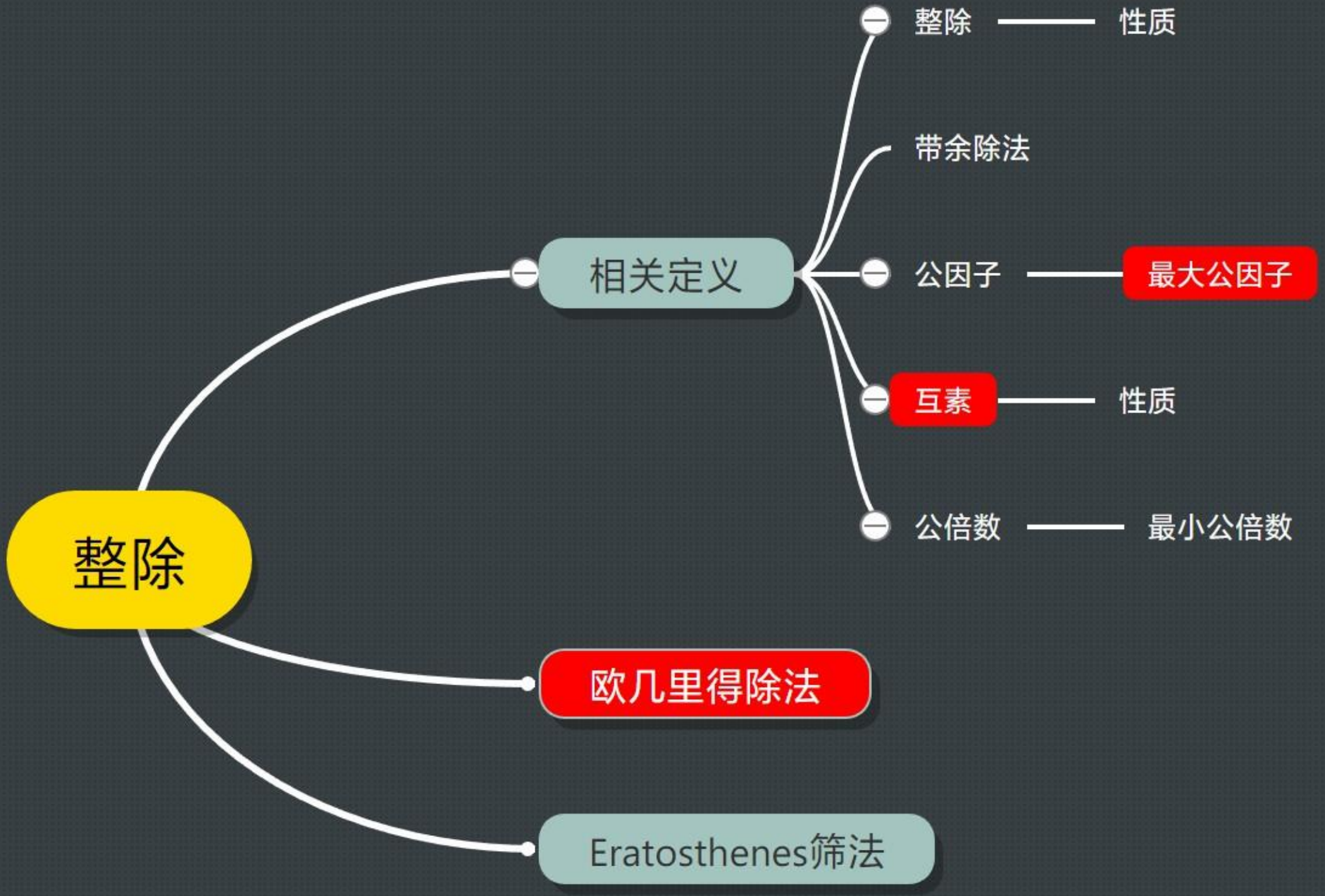

整除
相关定义
整除
性质
带余除法
公因子
最大公因子
互素
性质
公倍数
最小公倍数
欧几里得除法
Eratosthenes筛法

群

群

相关定义

- 群
- 推广
- 交换群
- 阶
- 幂

群的等价

- 方程组有解

群的判别

1. 封闭
2. 结合律
3.
   - 群的等价
   - 消去律

子群

相关定义

- 子群
- 平凡子群
- 真子群

判定定理

- 群的定义
- 带逆元封闭
- 有限
  - 封闭

映像

相关定义

- 像
- 原像
- 单射
- 满射
- 变换

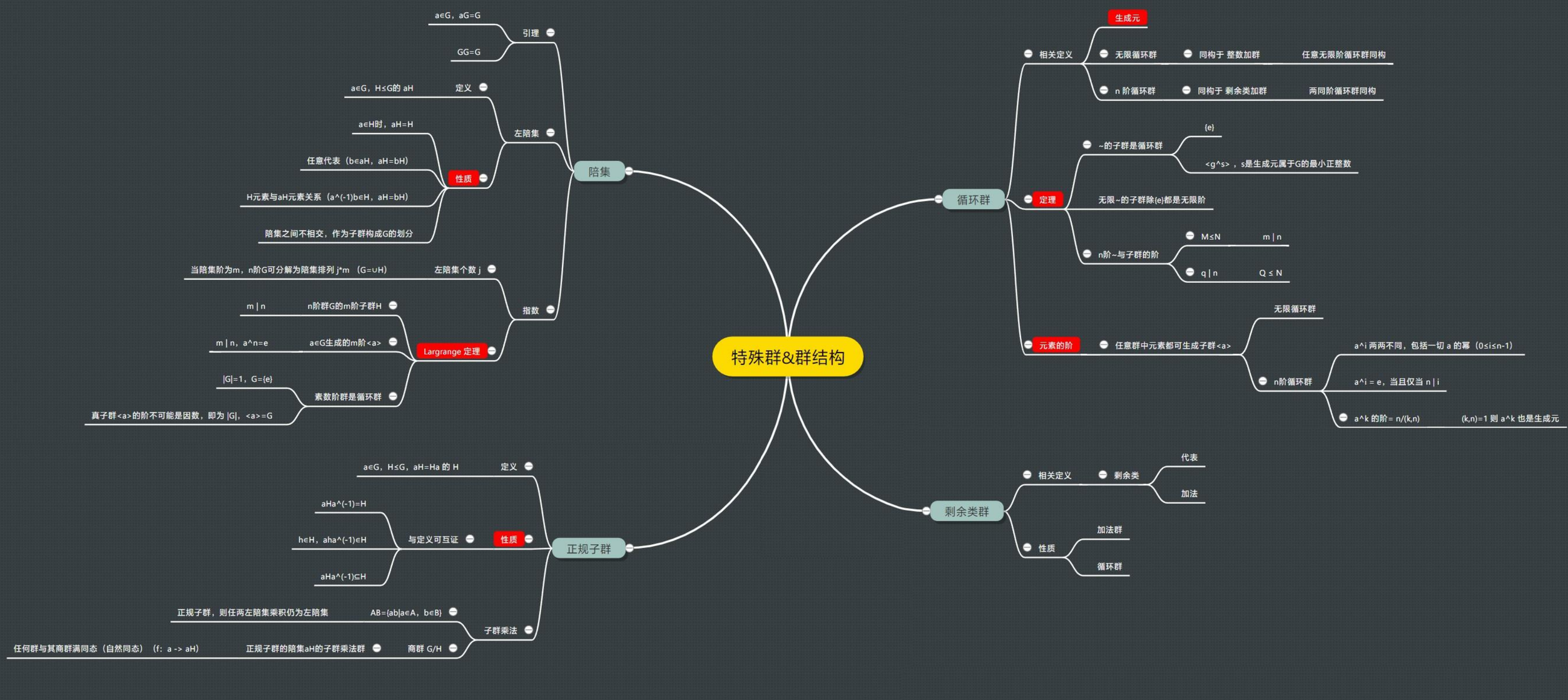
同态

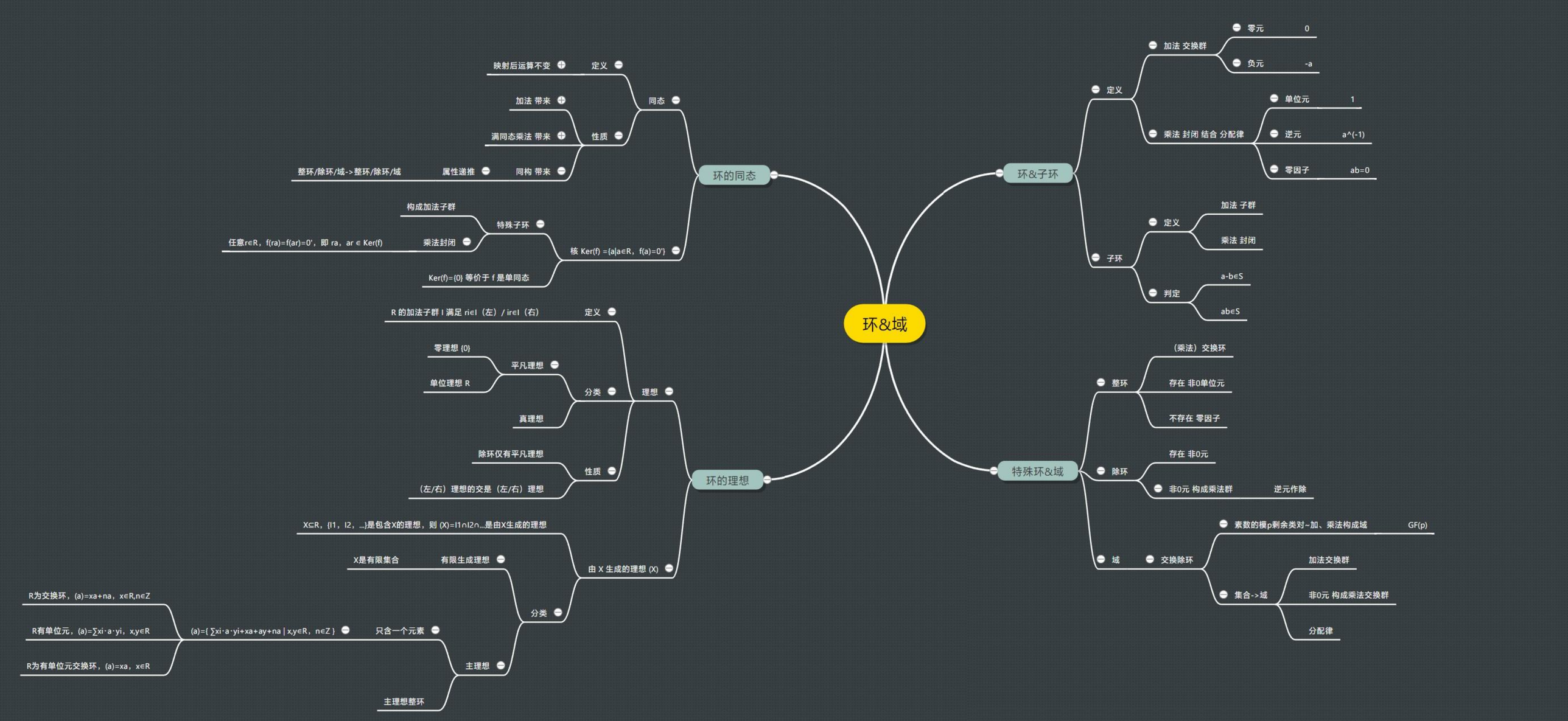
同构

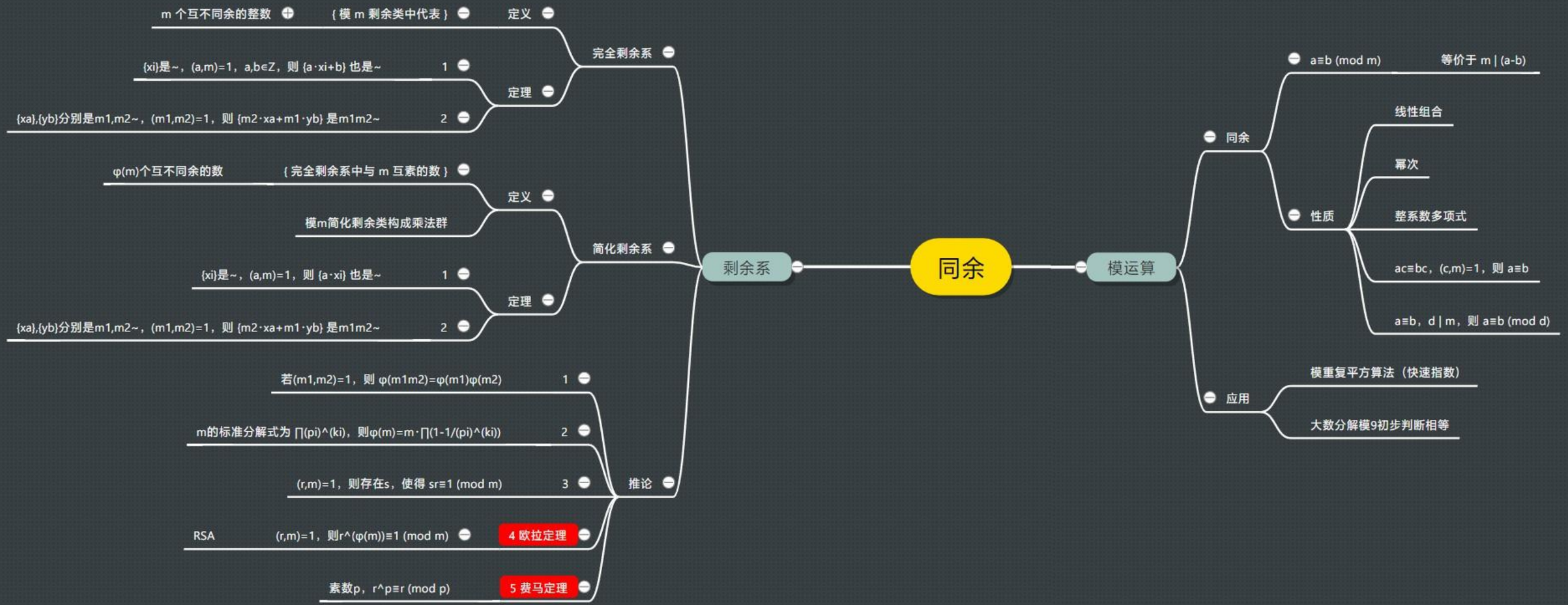
完全反像

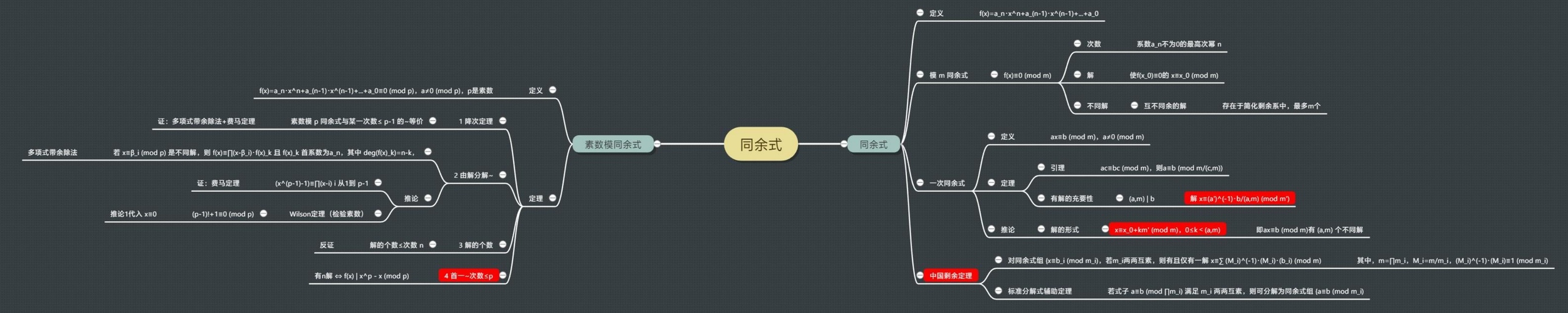
定理

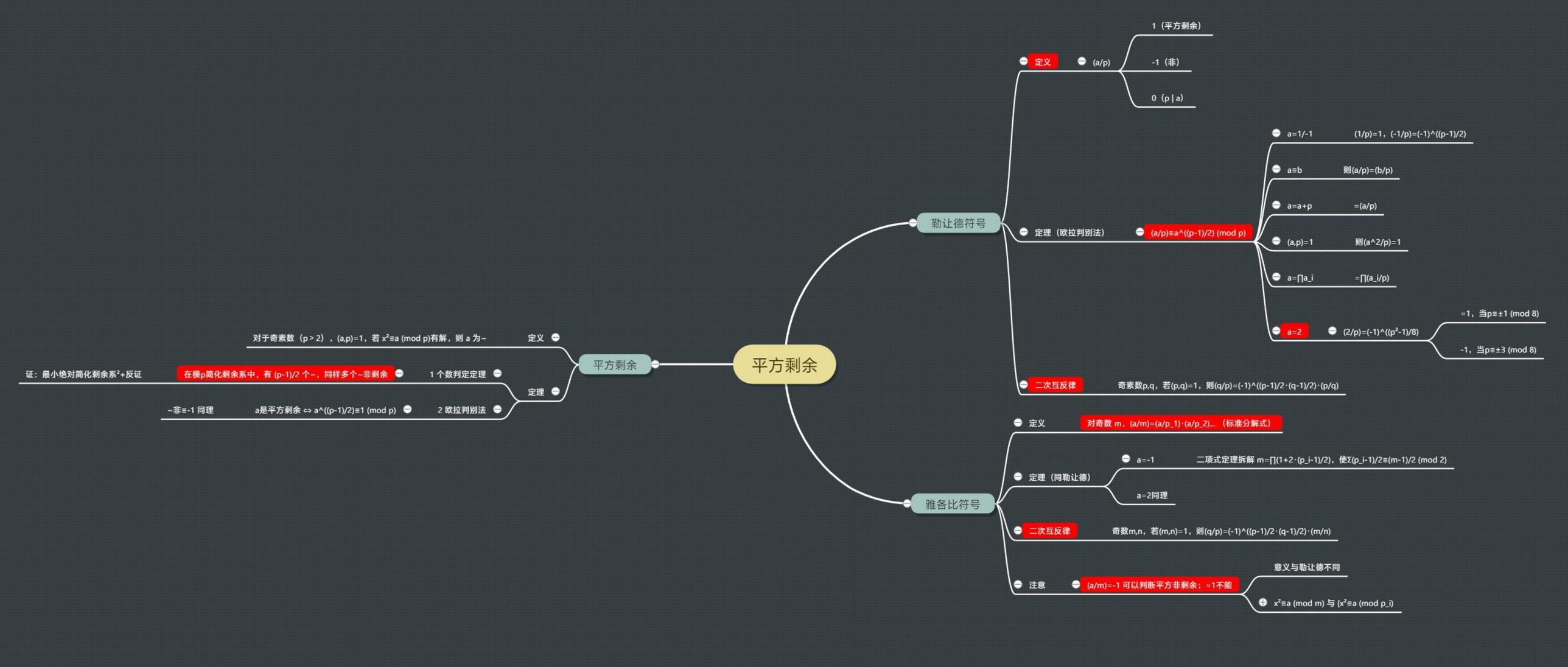
- 核

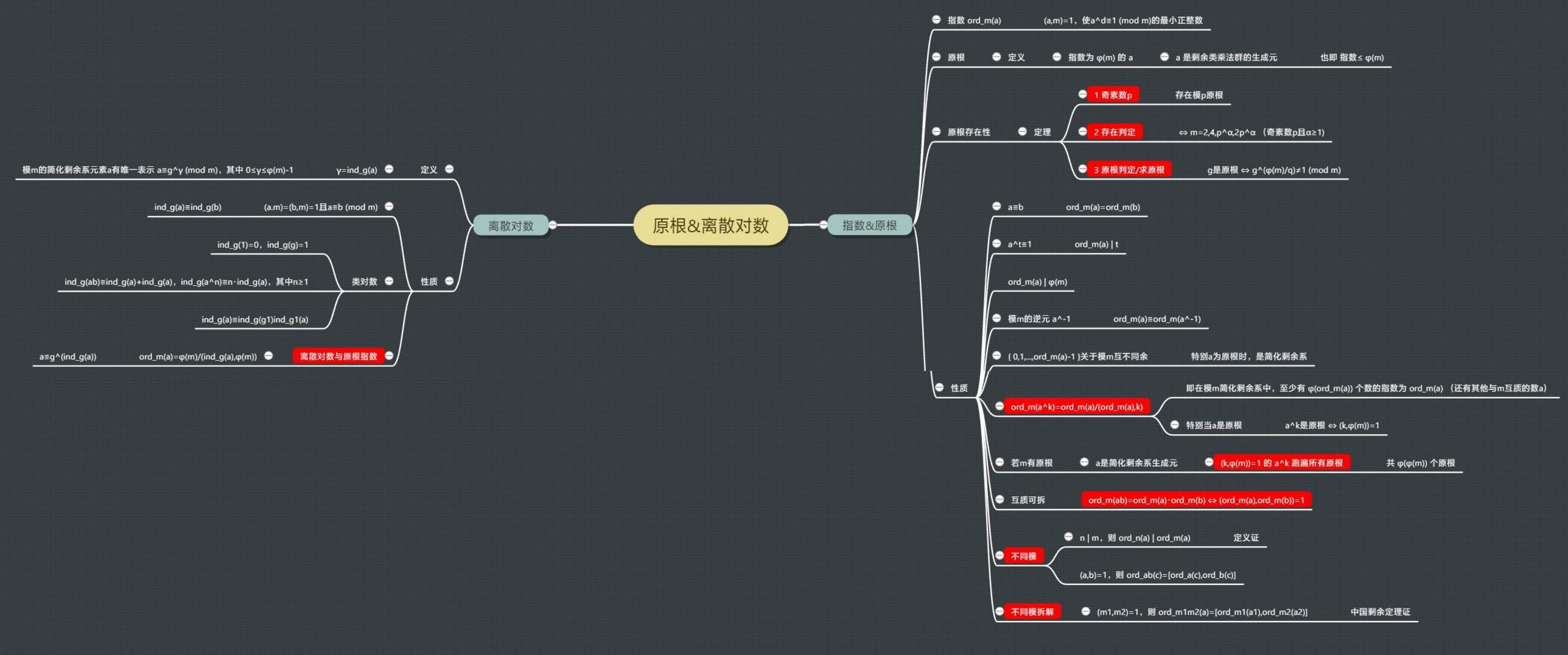

特殊群&群结构
陪集
引理
a∈G，aG=G
GG=G
左陪集
定义
a∈G，H≤G的 aH
性质
a∈H时，aH=H
任意代表（b∈aH，aH=bH）
H元素与aH元素关系（a^(-1)b∈H，aH=bH）
陪集之间不相交，作为子群构成G的划分
指数
左陪集个数 j
当陪集阶为m，n阶G可分解为陪集排列 j*m （G=∪H）
Largrange 定理
n阶群G的m阶子群H
m | n
a∈G生成的m阶<a>
m | n，a^n=e
素数阶群是循环群
|G|=1，G={e}
真子群<a>的阶不可能是因数，即为 |G|，<a>=G
循环群
相关定义
生成元
无限循环群
同构于 整数加群
任意无限阶循环群同构
n 阶循环群
同构于 剩余类加群
两同阶循环群同构
定理
~的子群是循环群
{e}
<g^s> ，s是生成元属于G的最小正整数
无限~的子群除{e}都是无限阶
n阶~与子群的阶
M≤N
m | n
q | n
Q ≤ N
元素的阶
任意群中元素都可生成子群<a>
无限循环群
n阶循环群
a^i 两两不同，包括一切 a 的幂（0≤i≤n-1）
a^i = e，当且仅当 n | i
a^k 的阶= n/(k,n)
(k,n)=1 则 a^k 也是生成元
剩余类群
相关定义
剩余类
代表
加法
性质
加法群
循环群
正规子群
定义
a∈G，H≤G，aH=Ha 的 H
性质
与定义可互证
aHa^(-1)=H
h∈H，aha^(-1)∈H
aHa^(-1)⊆H
子群乘法
AB={ab|a∈A，b∈B}
正规子群，则任两左陪集乘积仍为左陪集
商群 G/H
正规子群的陪集aH的子群乘法群
任何群与其商群满同态（自然同态） （f：a -> aH）


环&域
环的同态
同态
定义
映射后运算不变
性质
加法 带来
满同态乘法 带来
同构 带来
属性递推
整环/除环/域->整环/除环/域
核 Ker(f) ={a|a∈R，f(a)=0'}
特殊子环
构成加法子群
乘法封闭
任意r∈R，f(ra)=f(ar)=0'，即 ra，ar ∈ Ker(f)
Ker(f)={0} 等价于 f 是单同态
环的理想
理想
定义
R 的加法子群 I 满足 ri∈I（左）/ ir∈I（右）
分类
平凡理想
零理想 {0}
单位理想 R
真理想
性质
除环仅有平凡理想
（左/右）理想的交是（左/右）理想
由 X 生成的理想 (X)
X⊆R，{I1，I2，...}是包含X的理想，则 (X)=I1∩I2∩...是由X生成的理想
分类
有限生成理想
X是有限集合
主理想
只含一个元素
(a)={ ∑xi·a·yi+xa+ay+na | x,y∈R，n∈Z }
R为交换环，(a)=xa+na，x∈R,n∈Z
R有单位元，(a)=∑xi·a·yi，x,y∈R
R为有单位元交换环，(a)=xa，x∈R
主理想整环
环&子环
定义
加法 交换群
零元 0
负元 -a
乘法 封闭 结合 分配律
单位元 1
逆元 a^(-1)
零因子 ab=0
子环
定义
加法 子群
乘法 封闭
判定
a-b∈S
ab∈S
特殊环&域
整环
（乘法）交换环
存在 非0单位元
不存在 零因子
除环
存在 非0元
非0元 构成乘法群
逆元作除
域
交换除环
素数的模p剩余类对~加、乘法构成域
GF(p)
集合->域
加法交换群
非0元 构成乘法交换群
分配律


同余
剩余系
完全剩余系
定义
m 个互不同余的整数
{ 模 m 剩余类中代表 }
定理
1
{xi}是~，(a,m)=1，a,b∈Z，则 {a·xi+b} 也是~
2
{xa},{yb}分别是m1,m2~，(m1,m2)=1，则 {m2·xa+m1·yb} 是m1m2~
简化剩余系
定义
φ(m)个互不同余的数
{ 完全剩余系中与 m 互素的数 }
模m简化剩余类构成乘法群
定理
1
{xi}是~，(a,m)=1，则 {a·xi} 也是~
2
{xa},{yb}分别是m1,m2~，(m1,m2)=1，则 {m2·xa+m1·yb} 是m1m2~
推论
1
若(m1,m2)=1，则 φ(m1m2)=φ(m1)φ(m2)
2
m的标准分解式为 ∏(pi)^(ki)，则φ(m)=m·∏(1-1/(pi)^(ki))
3
(r,m)=1，则存在s，使得 sr≡1 (mod m)
4 欧拉定理
RSA
(r,m)=1，则r^(φ(m))≡1 (mod m)
5 费马定理
素数p，r^p≡r (mod p)
模运算
同余
a≡b (mod m)
等价于 m | (a-b)
性质
线性组合
幂次
整系数多项式
ac≡bc，(c,m)=1，则 a≡b
a≡b，d | m，则 a≡b (mod d)
应用
模重复平方算法（快速指数）
大数分解模9初步判断相等


同余式
同余式
定义
f(x)=a_n·x^n+a_(n-1)·x^(n-1)+…+a_0
模 m 同余式
f(x)≡0 (mod m)
次数
系数a_n不为0的最高次幂 n
解
使f(x_0)≡0的 x≡x_0 (mod m)
不同解
互不同余的解
存在于简化剩余系中，最多m个
一次同余式
定义
ax≡b (mod m)，a≠0 (mod m)
定理
引理
ac≡bc (mod m)，则a≡b (mod m/(c,m))
有解的充要性
(a,m) | b
解 x≡(a')^(-1)·b/(a,m) (mod m')
推论
解的形式
x≡x_0+km' (mod m)，0≤k < (a,m)
即ax≡b (mod m)有 (a,m) 个不同解
中国剩余定理
对同余式组 {x≡b_i (mod m_i)，若m_i两两互素，则有且仅有一解 x≡∑ (M_i)^(-1)·(M_i)·(b_i) (mod m)
其中，m=∏m_i，M_i=m/m_i，(M_i)^(-1)·(M_i)≡1 (mod m_i)
标准分解式辅助定理
若式子 a≡b (mod ∏m_i) 满足 m_i 两两互素，则可分解为同余式组 {a≡b (mod m_i)
素数模同余式
定义
f(x)=a_n·x^n+a_(n-1)·x^(n-1)+…+a_0≡0 (mod p)，a≠0 (mod p)，p是素数
定理
1 降次定理
素数模 p 同余式与某一次数≤ p-1 的~等价
证：多项式带余除法+费马定理
2 由解分解~
若 x≡β_i (mod p) 是不同解，则 f(x)≡∏(x-β_i)·f(x)_k 且 f(x)_k 首系数为a_n，其中 deg(f(x)_k)=n-k，
多项式带余除法
推论
(x^(p-1)-1)≡∏(x-i) i 从1到 p-1
证：费马定理
(p-1)!+1≡0 (mod p)
Wilson定理（检验素数）
推论1代入 x≡0
3 解的个数
解的个数≤次数 n
反证
4 首一~次数≤p
有n解 ⇔ f(x) | x^p - x (mod p)


平方剩余
勒让德符号
定义
(a/p)
1（平方剩余）
-1（非）
0（p | a）
定理（欧拉判别法）
(a/p)≡a^((p-1)/2) (mod p)
a=1/-1
(1/p)=1，(-1/p)=(-1)^((p-1)/2)
a≡b
则(a/p)=(b/p)
a=a+p
=(a/p)
(a,p)=1
则(a^2/p)=1
a=∏a_i
=∏(a_i/p)
a=2
(2/p)=(-1)^((p²-1)/8)
=1，当p≡±1 (mod 8)
-1，当p≡±3 (mod 8)
二次互反律
奇素数p,q，若(p,q)=1，则(q/p)=(-1)^((p-1)/2·(q-1)/2)·(p/q)
雅各比符号
定义
对奇数 m，(a/m)=(a/p_1)·(a/p_2)…（标准分解式）
定理（同勒让德）
a=-1
二项式定理拆解 m=∏(1+2·(p_i-1)/2)，使Σ(p_i-1)/2≡(m-1)/2 (mod 2)
a=2同理
二次互反律
奇数m,n，若(m,n)=1，则(q/p)=(-1)^((p-1)/2·(q-1)/2)·(m/n)
注意
(a/m)=-1 可以判断平方非剩余；=1不能
意义与勒让德不同
x²≡a (mod m) 与 {x²≡a (mod p_i)
平方剩余
定义
对于奇素数（p > 2），(a,p)=1，若 x²≡a (mod p)有解，则 a 为~
定理
1 个数判定定理
在模p简化剩余系中，有 (p-1)/2 个~，同样多个~非剩余
证：最小绝对简化剩余系²+反证
2 欧拉判别法
a是平方剩余 ⇔ a^((p-1)/2)≡1 (mod p)
~非≡-1 同理


原根&离散对数
指数&原根
指数 ord_m(a)
(a,m)=1，使a^d≡1 (mod m)的最小正整数
原根
定义
指数为 φ(m) 的 a
a 是剩余类乘法群的生成元
也即 指数≤ φ(m)
原根存在性
定理
1 奇素数p
存在模p原根
2 存在判定
⇔ m=2,4,p^α,2p^α （奇素数p且α≥1）
3 原根判定/求原根
g是原根 ⇔ g^(φ(m)/q)≠1 (mod m)
性质
a≡b
ord_m(a)=ord_m(b)
a^t≡1
ord_m(a) | t
ord_m(a) | φ(m)
模m的逆元 a^-1
ord_m(a)≡ord_m(a^-1)
{ 0,1,...,ord_m(a)-1 }关于模m互不同余
特别a为原根时，是简化剩余系
ord_m(a^k)=ord_m(a)/(ord_m(a),k)
即在模m简化剩余系中，至少有 φ(ord_m(a)) 个数的指数为 ord_m(a) （还有其他与m互质的数a）
特别当a是原根
a^k是原根 ⇔ (k,φ(m))=1
若m有原根
a是简化剩余系生成元
(k,φ(m))=1 的 a^k 跑遍所有原根
共 φ(φ(m)) 个原根
互质可拆
ord_m(ab)=ord_m(a)·ord_m(b) ⇔ (ord_m(a),ord_m(b))=1
不同模
n | m，则 ord_n(a) | ord_m(a)
定义证
(a,b)=1，则 ord_ab(c)=[ord_a(c),ord_b(c)]
不同模拆解
(m1,m2)=1，则 ord_m1m2(a)=[ord_m1(a1),ord_m2(a2)]
中国剩余定理证
离散对数
定义
模m的简化剩余系元素a有唯一表示 a≡g^γ (mod m)，其中 0≤γ≤φ(m)-1
γ=ind_g(a)
性质
ind_g(a)≡ind_g(b)
(a.m)=(b,m)=1且a≡b (mod m)
类对数
ind_g(1)=0，ind_g(g)=1
ind_g(ab)≡ind_g(a)+ind_g(a)，ind_g(a^n)≡n·ind_g(a)，其中n≥1
ind_g(a)≡ind_g(g1)ind_g1(a)
离散对数与原根指数
a≡g^(ind_g(a))
ord_m(a)=φ(m)/(ind_g(a),φ(m))