课程复习 -整数的可除性

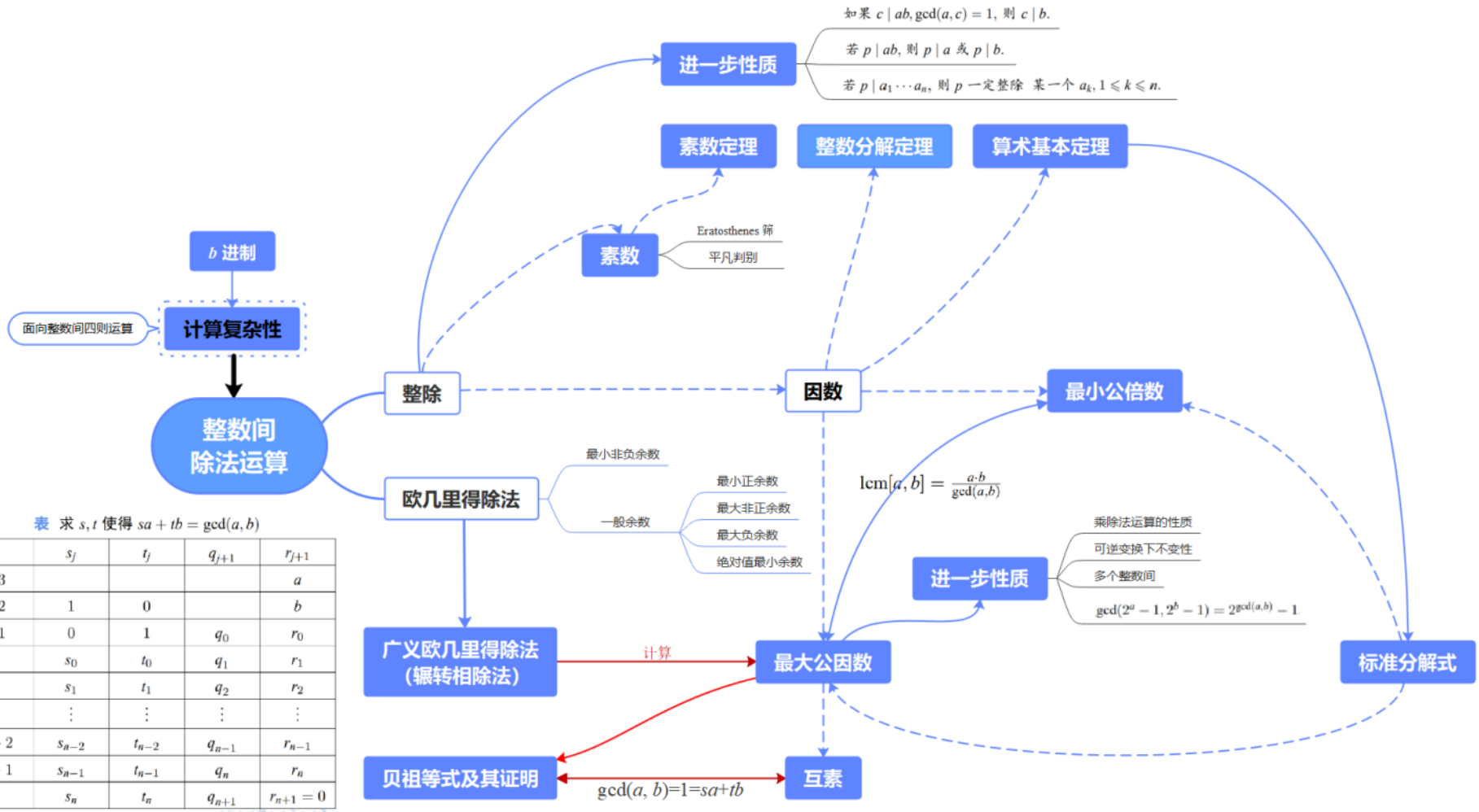
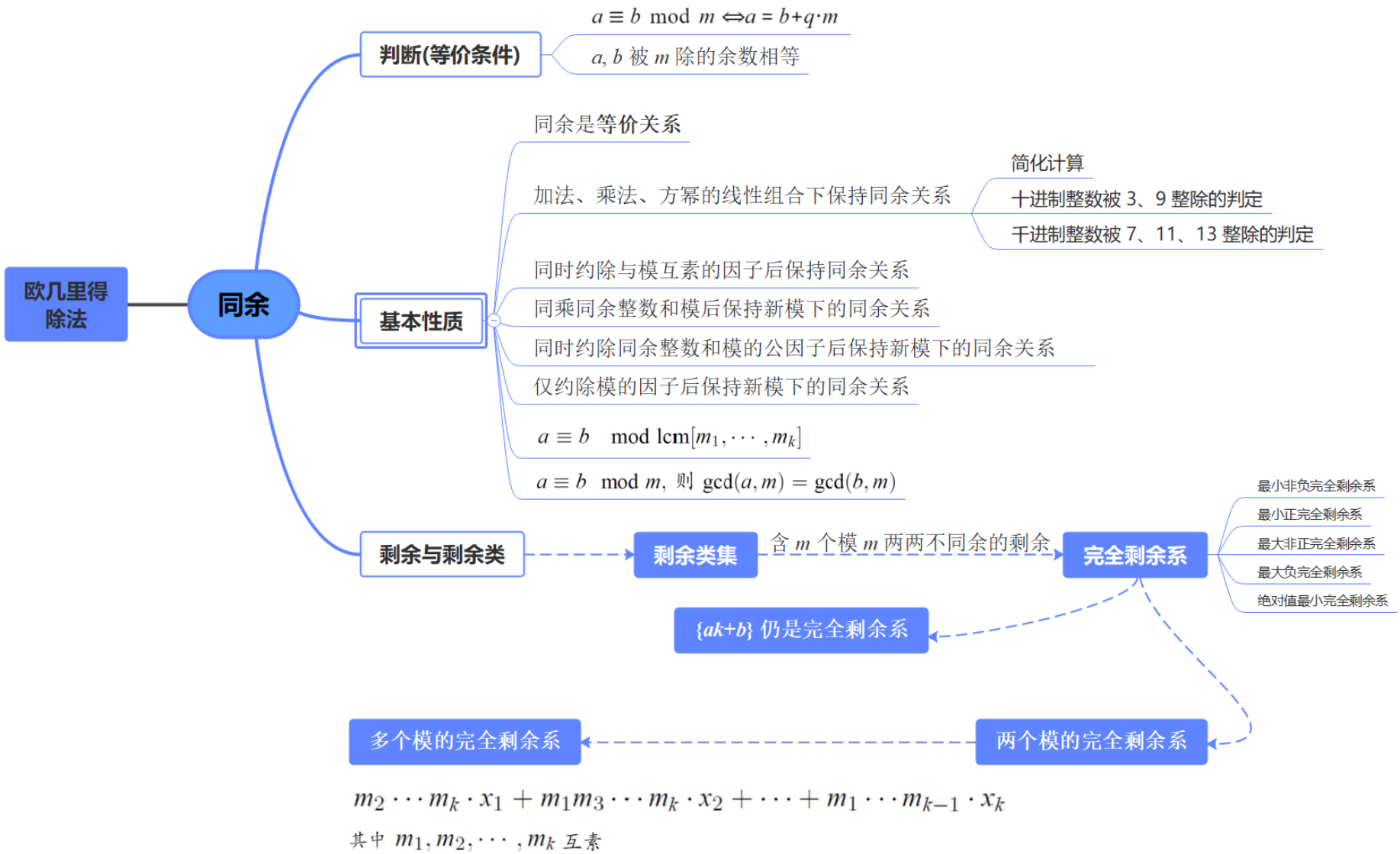


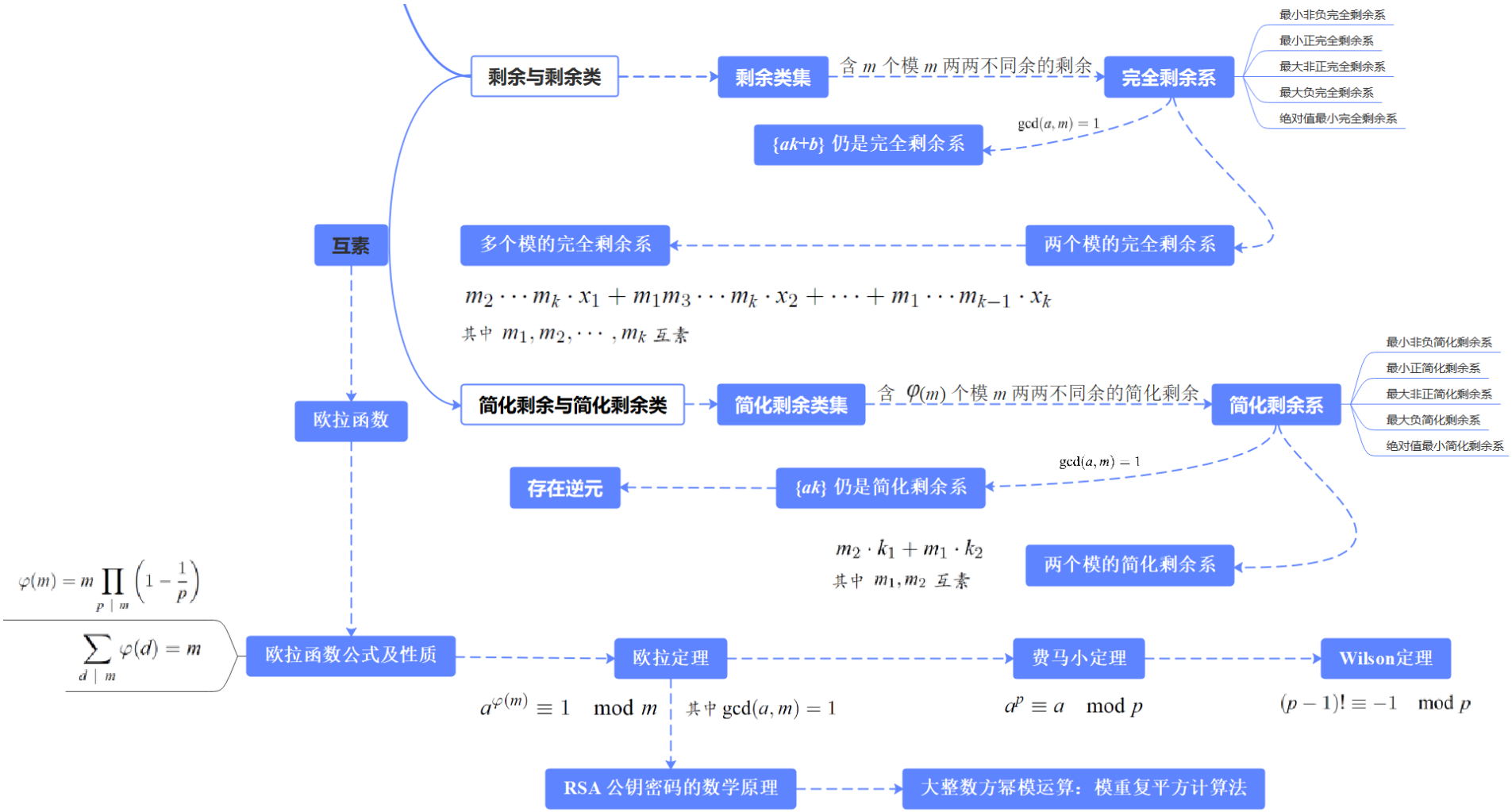
表 求 s,t 使得 $sa+tb=\gcd(a,b)$

j	s_j	t_j	q_{j+1}	r_{j+1}
-3				a
-2	1	0		b
-1	0	1	q_0	r_0
0	s_0	t_0	q_1	r_1
1	s_1	t_1	q_2	r_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$n-2$	s_{n-2}	t_{n-2}	q_{n-1}	r_{n-1}
$n-1$	s_{n-1}	t_{n-1}	q_n	r_n
n	s_n	t_n	q_{n+1}	$r_{n+1}=0$

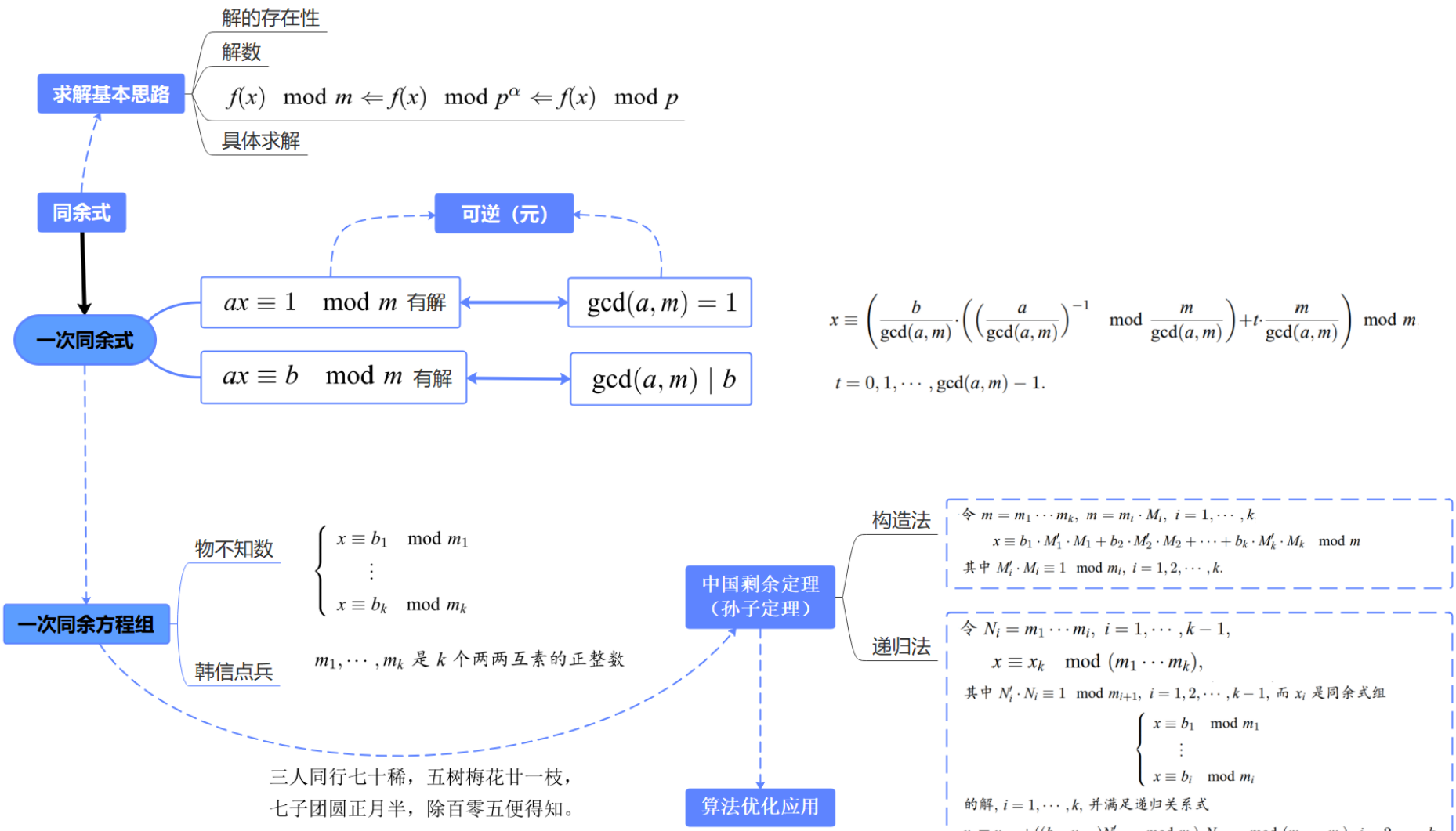
课程复习 -同余 (1)


欧几里得除法
同余
判断(等价条件)
$a \equiv b \mod m \Leftrightarrow a = b+q\cdot m$
a, b 被 m 除的余数相等
基本性质
同余是等价关系
加法、乘法、方幂的线性组合下保持同余关系
简化计算
十进制整数被 3、9 整除的判定
千进制整数被 7、11、13 整除的判定
同时约除与模互素的因子后保持同余关系
同乘同余整数和模后保持新模下的同余关系
同时约除同余整数和模的公因子后保持新模下的同余关系
仅约除模的因子后保持新模下的同余关系
$a \equiv b \mod \mathrm{lcm}[m_1, \cdots, m_k]$
$a \equiv b \mod m$, 则 $\gcd(a, m) = \gcd(b, m)$
剩余与剩余类
剩余类集
含 m 个模 m 两两不同余的剩余
完全剩余系
最小非负完全剩余系
最小正完全剩余系
最大非正完全剩余系
最大负完全剩余系
绝对值最小完全剩余系
$\{ak+b\}$ 仍是完全剩余系
多个模的完全剩余系
两个模的完全剩余系
$m_2 \cdots m_k \cdot x_1 + m_1 m_3 \cdots m_k \cdot x_2 + \cdots + m_1 \cdots m_{k-1} \cdot x_k$
其中 $m_1, m_2, \cdots, m_k$ 互素

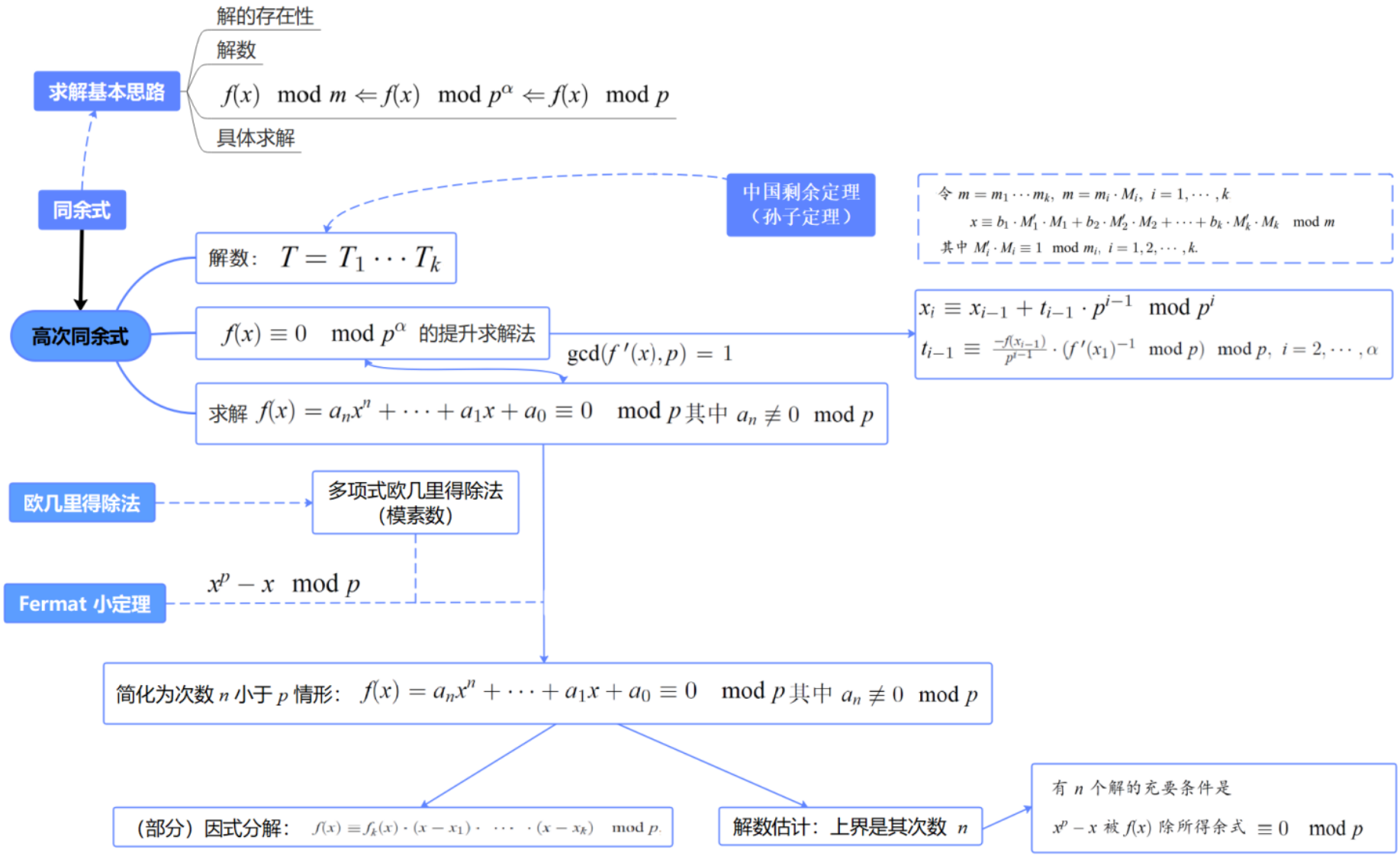
课程复习 -同余 (2)


剩余与剩余类
剩余类集
含 m 个模 m 两两不同余的剩余
完全剩余系
最小非负完全剩余系
最小正完全剩余系
最大非正完全剩余系
最大负完全剩余系
绝对值最小完全剩余系
$\gcd(a,m)=1$
$\{ak+b\}$ 仍是完全剩余系
互素
多个模的完全剩余系
两个模的完全剩余系
$m_2\cdots m_k\cdot x_1+m_1m_3\cdots m_k\cdot x_2+\cdots+m_1\cdots m_{k-1}\cdot x_k$
其中 $m_1,m_2,\cdots,m_k$ 互素
简化剩余与简化剩余类
简化剩余类集
含 $\varphi(m)$ 个模 m 两两不同余的简化剩余
简化剩余系
最小非负简化剩余系
最小正简化剩余系
最大非正简化剩余系
最大负简化剩余系
绝对值最小简化剩余系
欧拉函数
$\gcd(a,m)=1$
存在逆元
$\{ak\}$ 仍是简化剩余系
$m_2\cdot k_1+m_1\cdot k_2$
其中 m_1,m_2 互素
两个模的简化剩余系
$\varphi(m)=m\prod_{p\mid m}\left(1-\frac{1}{p}\right)$
$\sum_{d\mid m}\varphi(d)=m$
欧拉函数公式及性质
欧拉定理
费马小定理
Wilson定理
$a^{\varphi(m)}\equiv 1 \mod m$
其中 $\gcd(a,m)=1$
$a^p\equiv a \mod p$
$(p-1)!\equiv -1 \mod p$
RSA 公钥密码的数学原理
大整数方幂模运算：模重复平方计算法

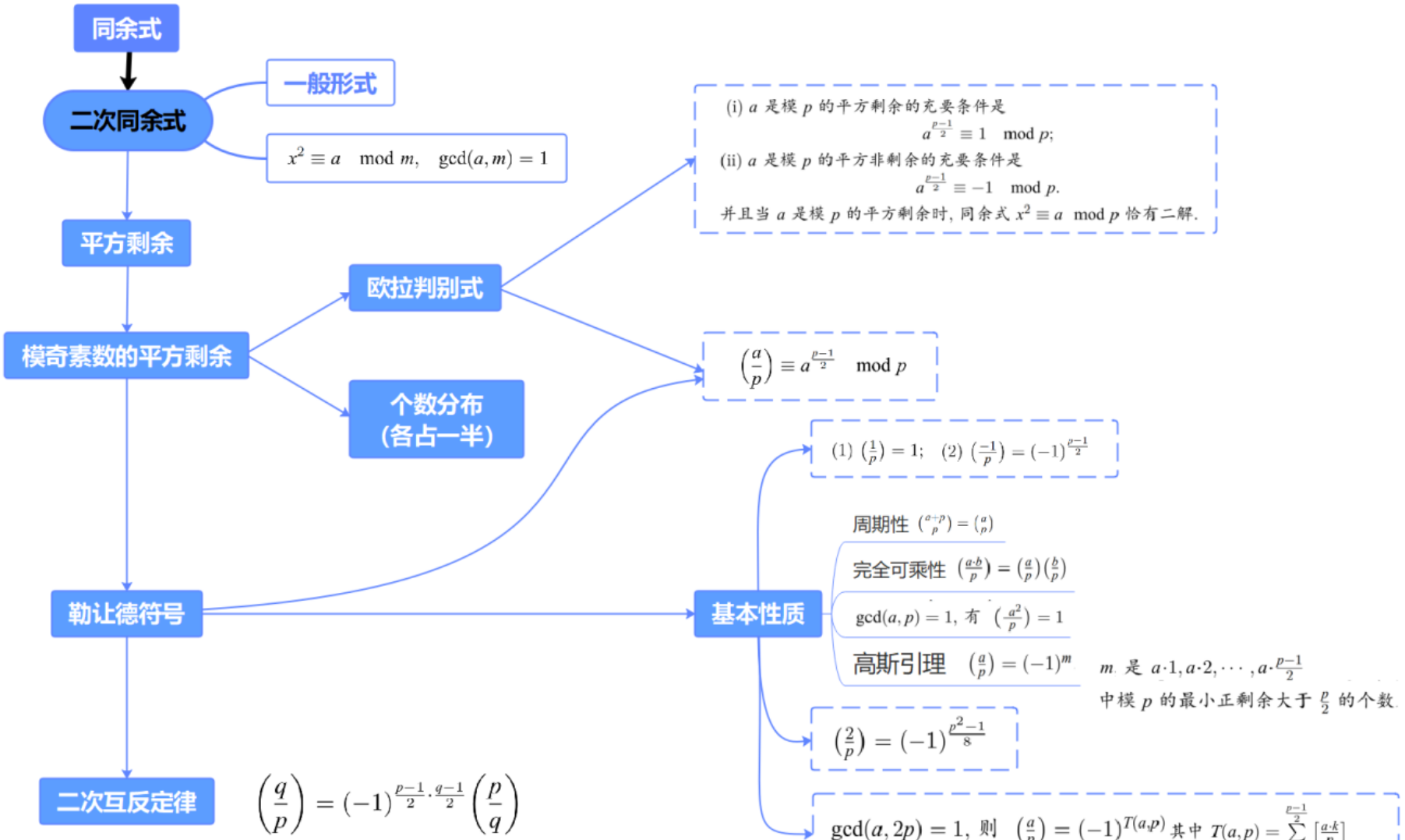
课程复习 -同余式 (1)


求解基本思路
解的存在性
解数
$f(x) \mod m \Leftarrow f(x) \mod p^{\alpha} \Leftarrow f(x) \mod p$
具体求解
同余式
可逆（元）
一次同余式
$ax \equiv 1 \mod m$ 有解
$\gcd(a,m)=1$
$ax \equiv b \mod m$ 有解
$\gcd(a,m) \mid b$
$x \equiv \left(\frac{b}{\gcd(a,m)} \cdot \left(\left(\frac{a}{\gcd(a,m)}\right)^{-1} \mod \frac{m}{\gcd(a,m)}\right) + t \cdot \frac{m}{\gcd(a,m)}\right) \mod m$
$t = 0, 1, \cdots, \gcd(a,m) - 1.$
一次同余方程组
物不知数
韩信点兵
$\begin{cases} x \equiv b_1 \mod m_1 \\ \vdots \\ x \equiv b_k \mod m_k \end{cases}$
$m_1, \cdots, m_k$ 是 k 个两两互素的正整数
三人同行七十稀，五树梅花廿一枝，
七子团圆正月半，除百零五便得知。
中国剩余定理（孙子定理）
构造法
令 $m = m_1 \cdots m_k$, $m = m_i \cdot M_i$, $i = 1, \cdots, k$
$x \equiv b_1 \cdot M_1' \cdot M_1 + b_2 \cdot M_2' \cdot M_2 + \cdots + b_k \cdot M_k' \cdot M_k \mod m$
其中 $M_i' \cdot M_i \equiv 1 \mod m_i$, $i = 1, 2, \cdots, k$.
递归法
令 $N_i = m_1 \cdots m_i$, $i = 1, \cdots, k-1$,
$x \equiv x_k \mod (m_1 \cdots m_k)$,
其中 $N_i' \cdot N_i \equiv 1 \mod m_{i+1}$, $i = 1, 2, \cdots, k-1$, 而 x_i 是同余式组
$\begin{cases} x \equiv b_1 \mod m_1 \\ \vdots \\ x \equiv b_i \mod m_i \end{cases}$
的解, $i = 1, \cdots, k$, 并满足递归关系式
$x_i \equiv x_{i-1} + ((b_i - x_{i-1}) N_{i-1}' \mod m_i) \cdot N_{i-1} \mod (m_1 \cdots m_i)$, $i = 2, \cdots, k$.
算法优化应用

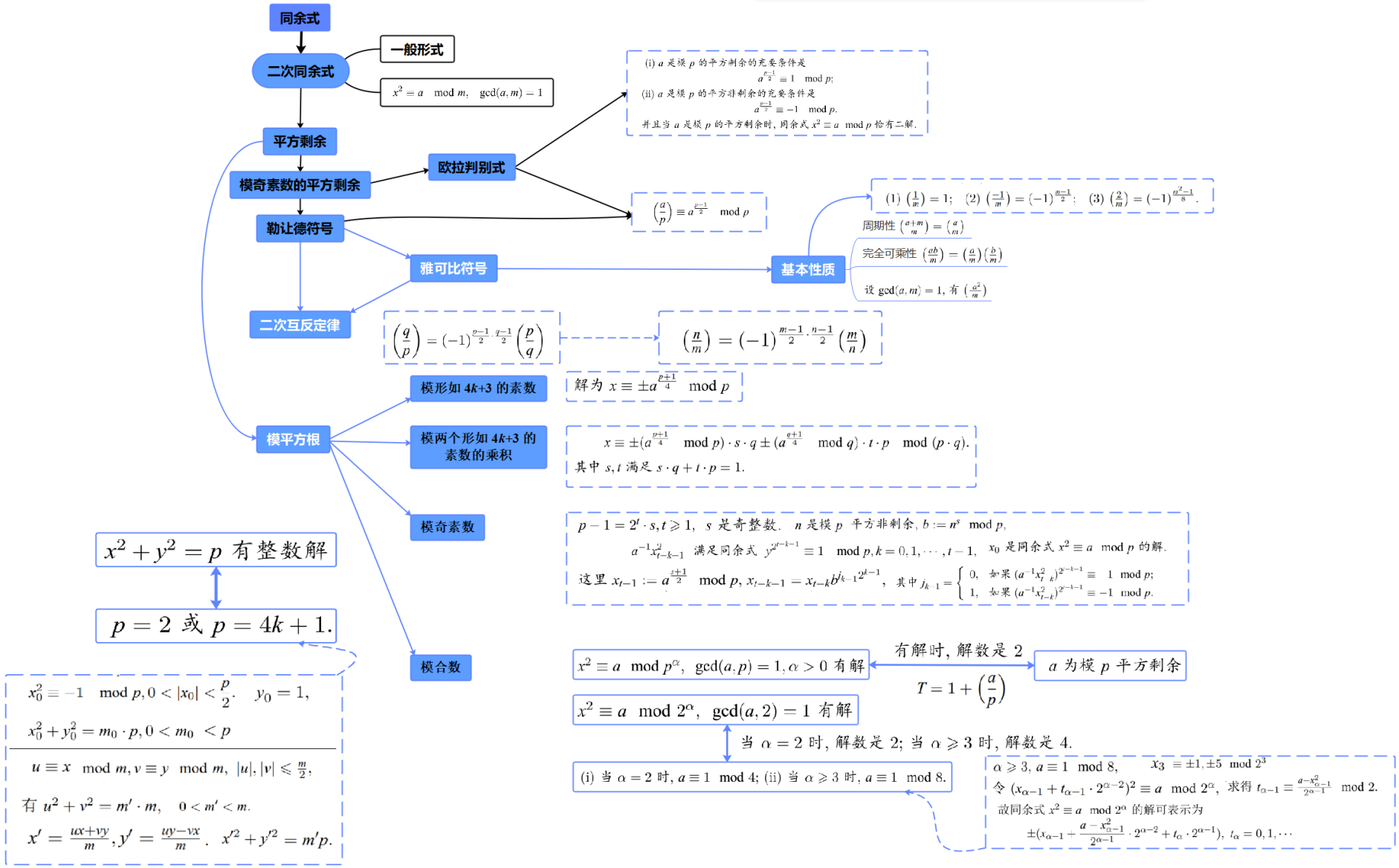
课程复习 -同余式 (2)


求解基本思路
解的存在性
解数
$f(x) \mod m \Leftarrow f(x) \mod p^\alpha \Leftarrow f(x) \mod p$
具体求解
同余式
高次同余式
中国剩余定理
（孙子定理）
令 $m = m_1 \cdots m_k$, $m = m_i \cdot M_i$, $i = 1, \cdots, k$
$x \equiv b_1 \cdot M_1' \cdot M_1 + b_2 \cdot M_2' \cdot M_2 + \cdots + b_k \cdot M_k' \cdot M_k \mod m$
其中 $M_i' \cdot M_i \equiv 1 \mod m_i$, $i = 1, 2, \cdots, k$.
解数：$T = T_1 \cdots T_k$
$f(x) \equiv 0 \mod p^\alpha$ 的提升求解法
$\gcd(f'(x), p) = 1$
$x_i \equiv x_{i-1} + t_{i-1} \cdot p^{i-1} \mod p^i$
$t_{i-1} \equiv \frac{-f(x_{i-1})}{p^{i-1}} \cdot (f'(x_1)^{-1} \mod p) \mod p$, $i = 2, \cdots, \alpha$
求解 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \mod p$ 其中 $a_n \not\equiv 0 \mod p$
欧几里得除法
多项式欧几里得除法
（模素数）
Fermat 小定理
$x^p - x \mod p$
简化为次数 n 小于 p 情形：$f(x) = a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \mod p$ 其中 $a_n \not\equiv 0 \mod p$
（部分）因式分解：$f(x) \equiv f_k(x) \cdot (x - x_1) \cdot \cdots \cdot (x - x_k) \mod p$.
解数估计：上界是其次数 n
有 n 个解的充要条件是
$x^p - x$ 被 $f(x)$ 除所得余式 $\equiv 0 \mod p$

课程复习 -二次同余式与平方剩余 (1)



课程复习 -二次同余式与平方剩余 (2)



课程复习 -原根与指标 (1)

指数（阶）

最小正整数 e，使得 $a^e \equiv 1 \mod m$

$\mathrm{ord}_m(a) = \varphi(m)$

原根

基本性质

$a^d \equiv 1 \mod m \iff \mathrm{ord}_m(a) \mid d$

若 $b \equiv a \mod m$，则 $\mathrm{ord}_m(b) = \mathrm{ord}_m(a)$.

$\mathrm{ord}_m(a^{-1}) = \mathrm{ord}_m(a)$

$\mathrm{ord}_m(a) = \varphi(m)$ 时，$1 = a^0, a, \cdots, a^{\varphi(m)-1}$ 组成模 m 的简化剩余系.

$a^d \equiv a^k \mod m \iff d \equiv k \mod \mathrm{ord}_m(a)$

$$\mathrm{ord}_m(a^d) = \frac{\mathrm{ord}_m(a)}{\gcd(d, \mathrm{ord}_m(a))}$$

模 m 有 $\varphi(\varphi(m))$ 个不同的原根.

模 m 原根的概率是 $\frac{\varphi(\varphi(m))}{\varphi(m)} = \prod_{i=1}^{s}(1 - \frac{1}{p_i})$.

求解原根

- 模 p

$p-1$ 的所有不同素因数是 $q_1, \cdots, q_s$

$g^{\frac{p-1}{q_i}} \not\equiv 1 \mod p, \quad i = 1, \cdots, s.$

- 模 p^α

g 或者 $g+p$ 是模 p^2 原根 $\Rightarrow$ 是模 p^α 的原根.

g 是模 p^α 原根，则 g 与 $g+p^\alpha$ 中的奇数是模 $2p^\alpha$ 的原根.

- 模 2^α 指数

$\alpha \geqslant 3,$

$a^{\frac{\varphi(2^\alpha)}{2}} \equiv a^{2^{\alpha-2}} \equiv 1 \mod 2^\alpha$

$\mathrm{ord}_{2^\alpha}(5) = \frac{\varphi(2^\alpha)}{2} = 2^{\alpha-2}$

模 m 的原根存在 $\iff m = 2, 4, p^\alpha, 2p^\alpha$

大指数构造

$\gcd(\mathrm{ord}_m(a), \mathrm{ord}_m(b)) = 1 \iff \mathrm{ord}_m(a \cdot b) = \mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b)$

若 $n \mid m$，则 $\mathrm{ord}_n(a) \mid \mathrm{ord}_m(a)$.

若 $\gcd(m, n) = 1$，则 $\mathrm{ord}_{mn}(a) = \mathrm{lcm}[\mathrm{ord}_m(a), \mathrm{ord}_n(a)]$.

$m = 2^n \cdot p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ 时 $\mathrm{ord}_m(a) = \mathrm{lcm}[\mathrm{ord}_{2^n}(a), \mathrm{ord}_{p_1^{\alpha_1}}(a), \cdots, \mathrm{ord}_{p_k^{\alpha_k}}(a)]$.

$\gcd(m, n) = 1$ 对与 mn 互素的 a_1, a_2，存在整数 a 使得 $\mathrm{ord}_{mn}(a) = \mathrm{lcm}[\mathrm{ord}_m(a_1), \mathrm{ord}_n(a_2)]$.

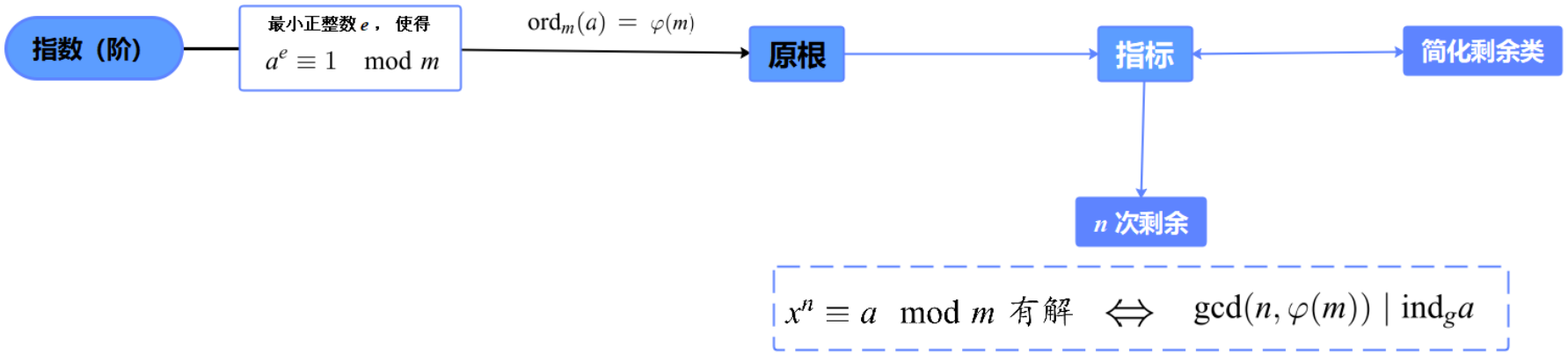
对与 m 互素的任意整数 a, b，存在整数 c 使得 $\mathrm{ord}_m(c) = \mathrm{lcm}[\mathrm{ord}_m(a), \mathrm{ord}_m(b)]$.

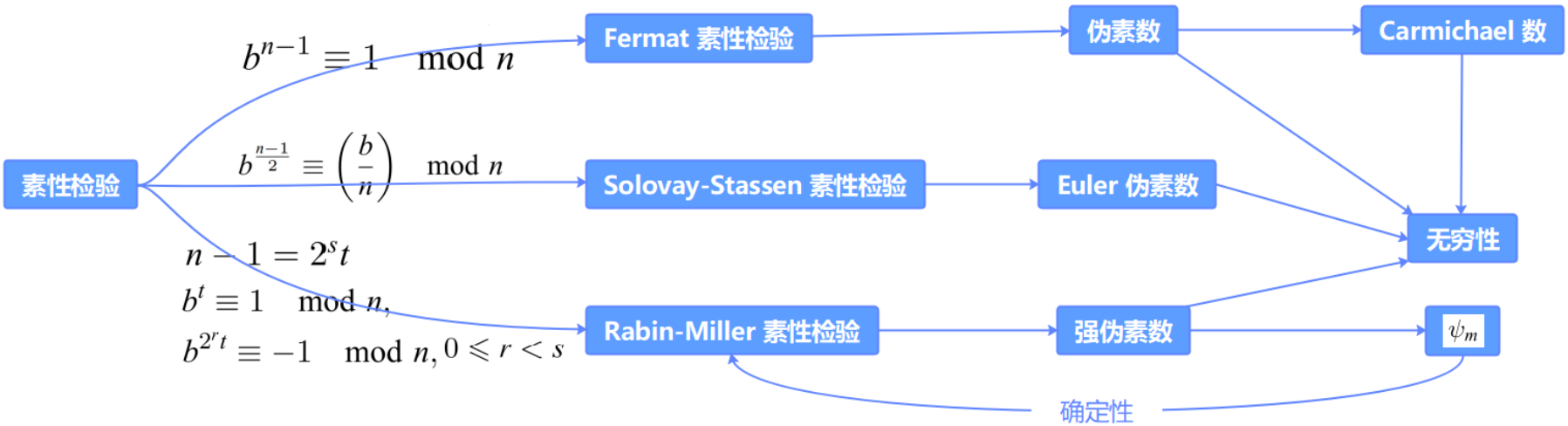
设 $m > 1$ 是整数，$a_1, a_2, \cdots, a_{\varphi(m)}$ 是模 m 的简化剩余系，e 是使得 $a_k^e \equiv 1 \mod m$，$1 \leqslant k \leqslant \varphi(m)$ 成立的最小正整数，则存在整数 a 使得

$e = \mathrm{ord}_m(a) = \mathrm{lcm}[\mathrm{ord}_m(a_1), \mathrm{ord}_m(a_2), \cdots, \mathrm{ord}_m(a_{\varphi(m)})]$.

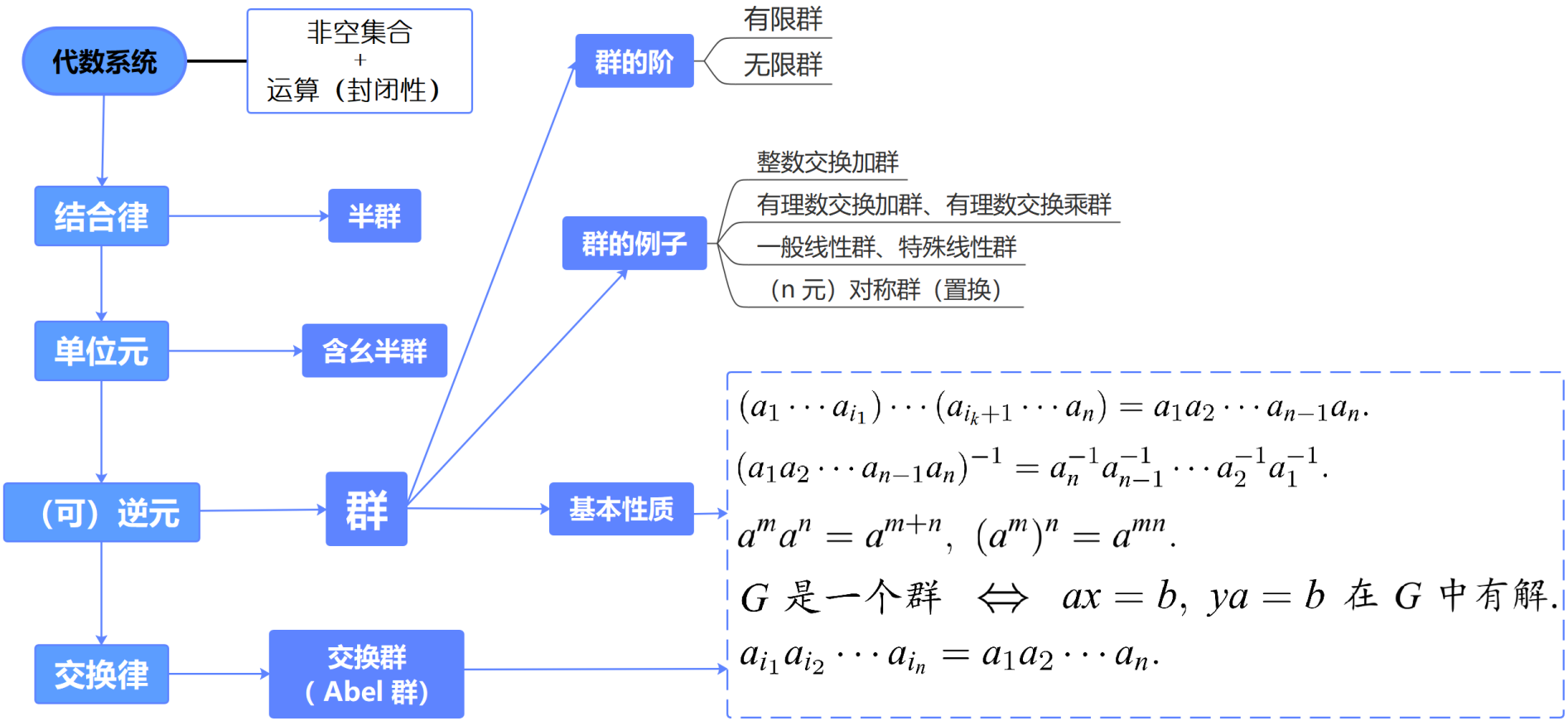
$\Rightarrow$ **简化剩余系指数**

课程复习 -原根与指标 (2) & 素性检验

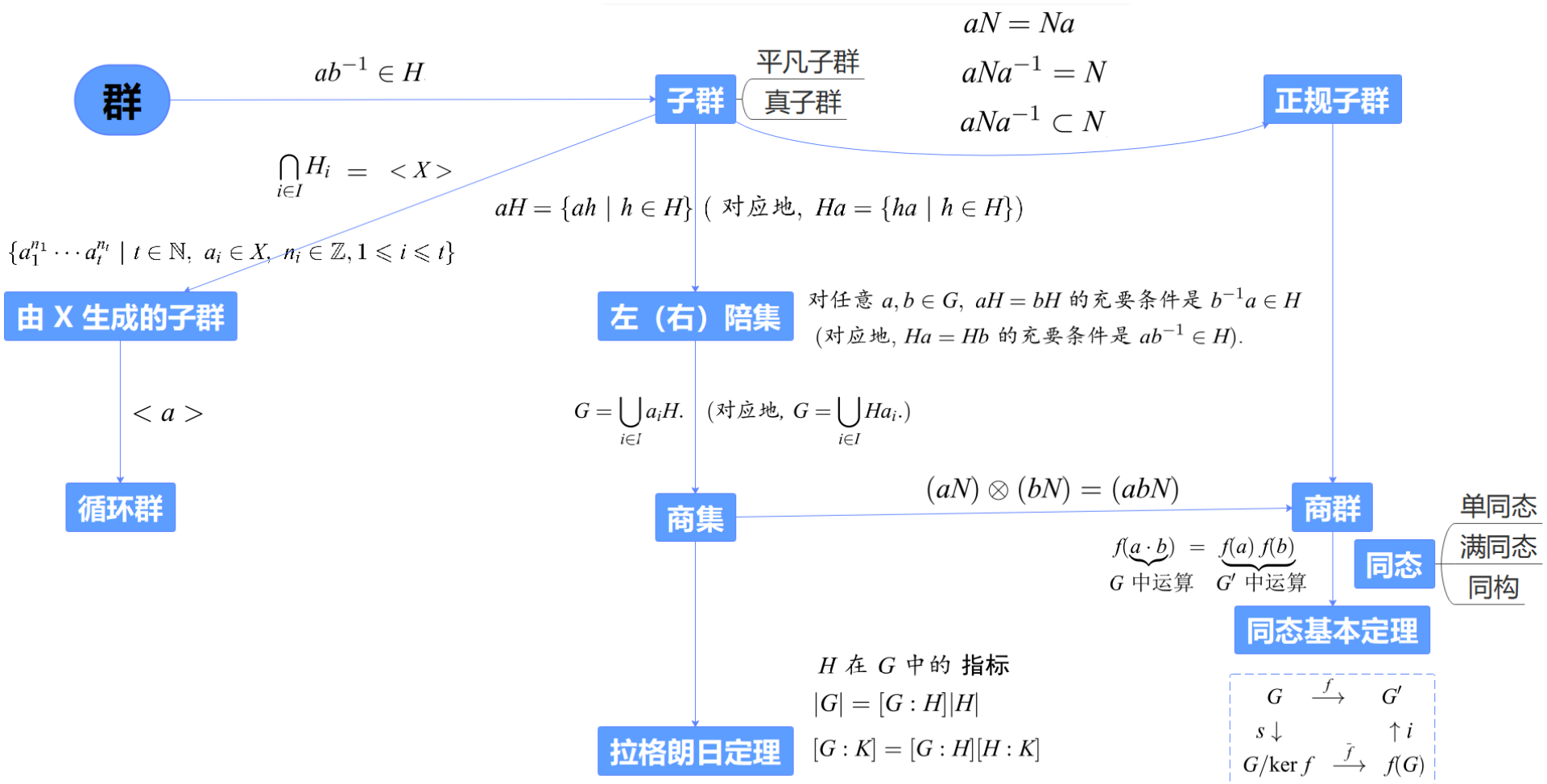




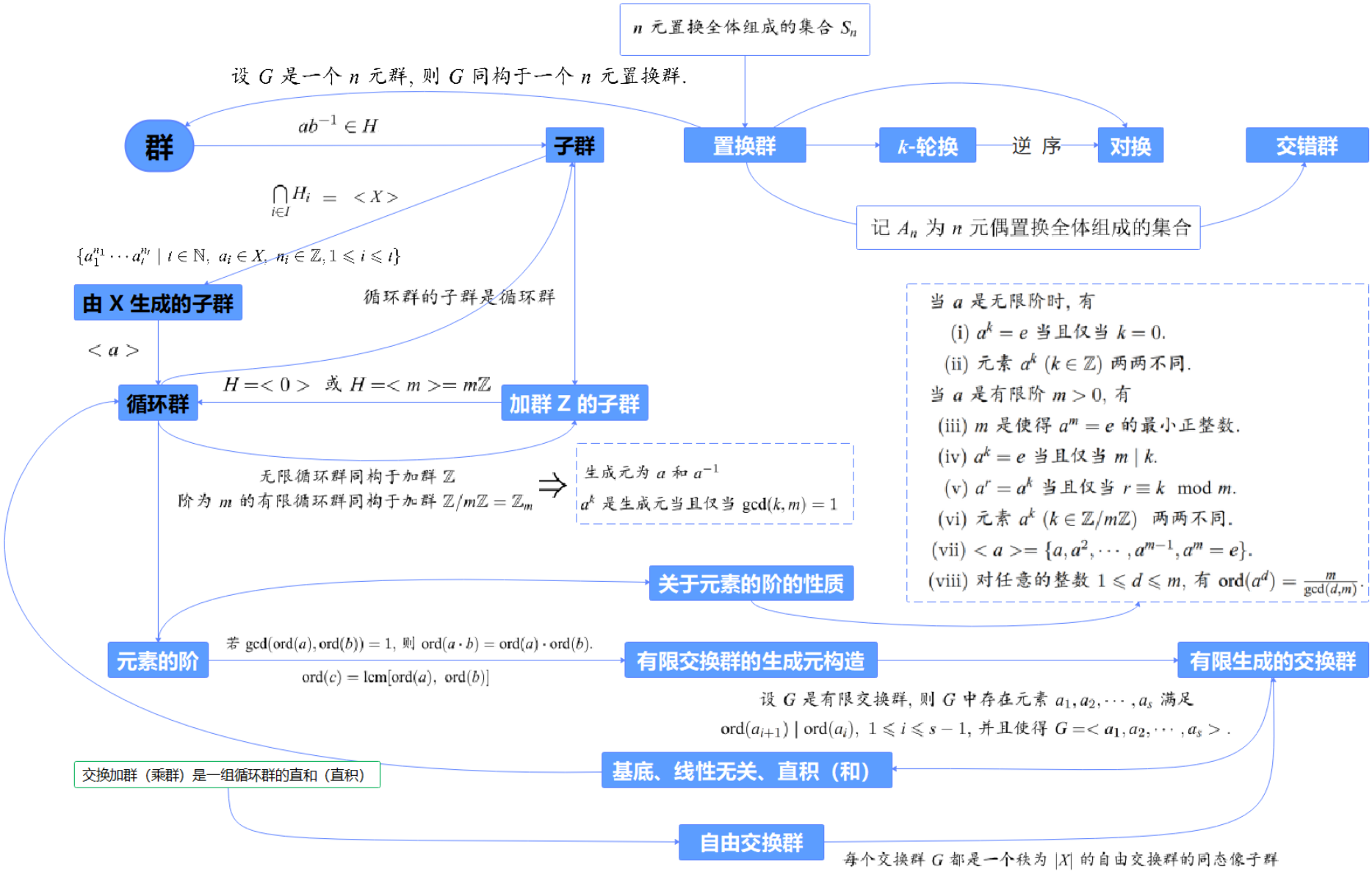
课程复习 -群 (1)


代数系统
非空集合
+
运算（封闭性）
结合律
半群
单位元
含幺半群
（可）逆元
群
交换律
交换群
(Abel 群)
群的阶
有限群
无限群
群的例子
整数交换加群
有理数交换加群、有理数交换乘群
一般线性群、特殊线性群
（n 元）对称群（置换）
基本性质
$(a_1 \cdots a_{i_1}) \cdots (a_{i_k+1} \cdots a_n) = a_1 a_2 \cdots a_{n-1} a_n.$
$(a_1 a_2 \cdots a_{n-1} a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_2^{-1} a_1^{-1}.$
$a^m a^n = a^{m+n},\ (a^m)^n = a^{mn}.$
G 是一个群 $\Leftrightarrow$ $ax = b,\ ya = b$ 在 G 中有解.
$a_{i_1} a_{i_2} \cdots a_{i_n} = a_1 a_2 \cdots a_n.$

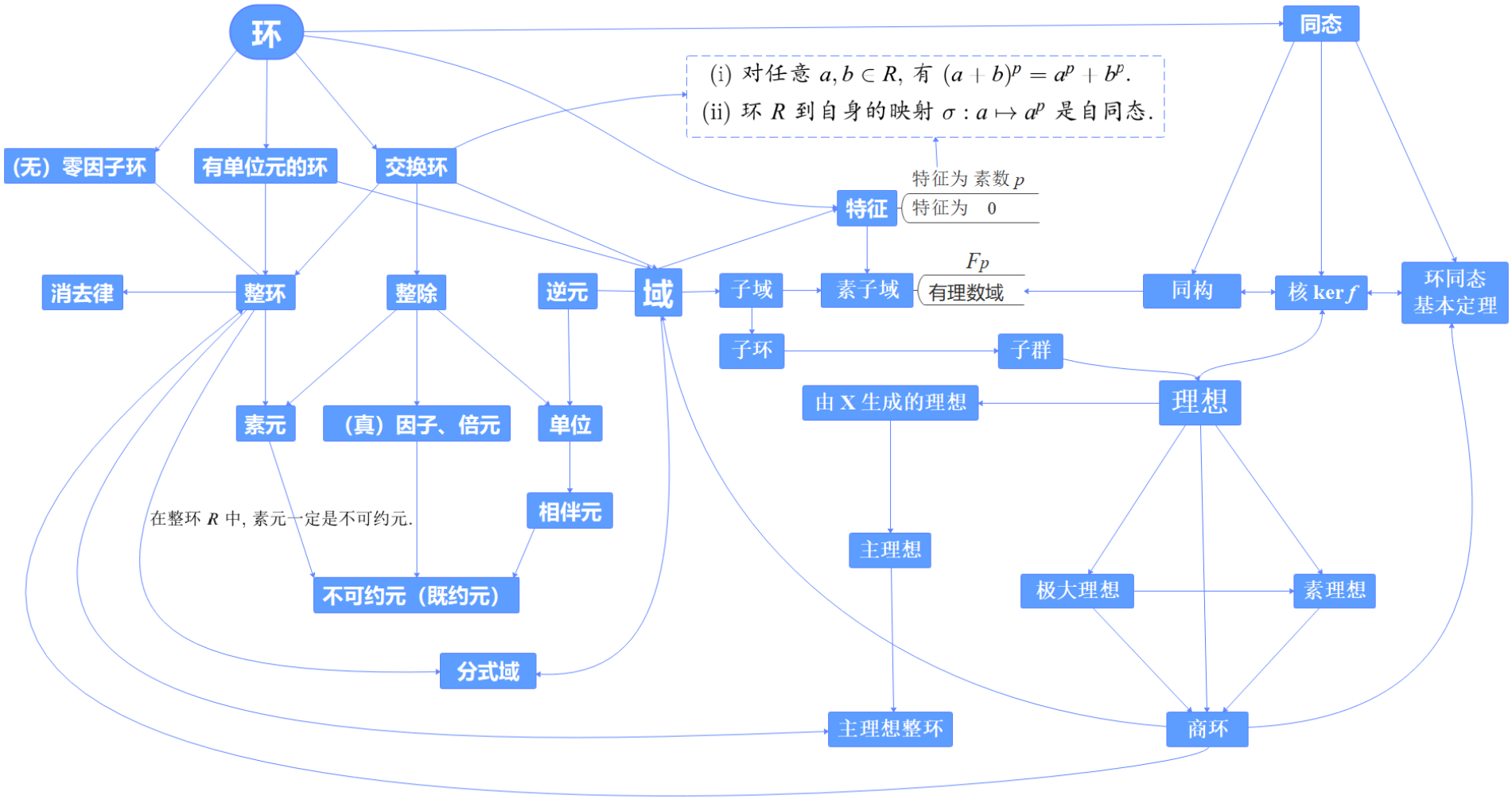
课程复习 -群 (2)


群
$ab^{-1} \in H$
子群
平凡子群
真子群
$aN = Na$
$aNa^{-1} = N$
$aNa^{-1} \subset N$
正规子群
$\bigcap_{i\in I} H_i = \langle X \rangle$
$aH = \{ah \mid h \in H\}$ (对应地, $Ha = \{ha \mid h \in H\}$)
$\{a_1^{n_1} \cdots a_t^{n_t} \mid t \in \mathbb{N},\ a_i \in X,\ n_i \in \mathbb{Z}, 1 \leqslant i \leqslant t\}$
由 X 生成的子群
左（右）陪集
对任意 $a, b \in G$, $aH = bH$ 的充要条件是 $b^{-1}a \in H$
(对应地, $Ha = Hb$ 的充要条件是 $ab^{-1} \in H$).
$\langle a \rangle$
$G = \bigcup_{i\in I} a_i H.$ (对应地, $G = \bigcup_{i\in I} Ha_i.$)
循环群
商集
$(aN) \otimes (bN) = (abN)$
商群
$f(\underbrace{a \cdot b}_{G \text{ 中运算}}) = \underbrace{f(a)\, f(b)}_{G' \text{ 中运算}}$
同态
单同态
满同态
同构
同态基本定理
H 在 G 中的 指标
$|G| = [G : H]|H|$
$[G : K] = [G : H][H : K]$
拉格朗日定理
$G \xrightarrow{f} G'$
$s \downarrow \quad \uparrow i$
$G/\ker f \xrightarrow{\bar{f}} f(G)$

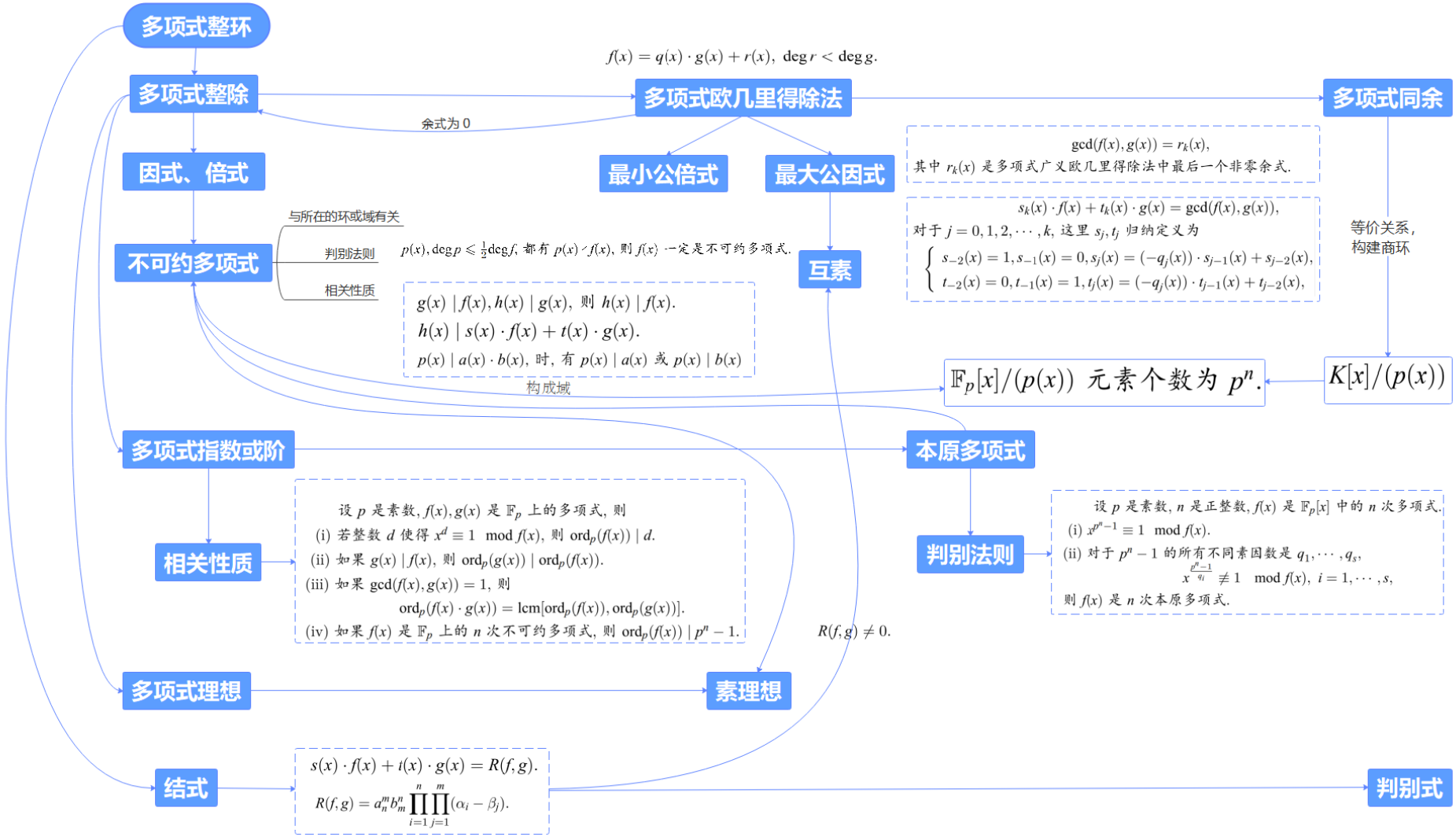
课程复习 -群的结构


n 元置换全体组成的集合 S_n
设 G 是一个 n 元群, 则 G 同构于一个 n 元置换群.
群
$ab^{-1} \in H$
子群
置换群
k-轮换
逆 序
对换
交错群
$\bigcap_{i\in I} H_i = < X >$
记 A_n 为 n 元偶置换全体组成的集合
$\{a_1^{n_1} \cdots a_t^{n_t} \mid t \in \mathbb{N},\ a_i \in X,\ n_i \in \mathbb{Z}, 1 \leqslant i \leqslant t\}$
由 X 生成的子群
循环群的子群是循环群
$< a >$
$H =< 0 >$ 或 $H =< m >= m\mathbb{Z}$
循环群
加群 Z 的子群
当 a 是无限阶时, 有
(i) $a^k = e$ 当且仅当 $k = 0$.
(ii) 元素 a^k $(k \in \mathbb{Z})$ 两两不同.
当 a 是有限阶 $m > 0$, 有
(iii) m 是使得 $a^m = e$ 的最小正整数.
(iv) $a^k = e$ 当且仅当 $m \mid k$.
(v) $a^r = a^k$ 当且仅当 $r \equiv k \mod m$.
(vi) 元素 a^k $(k \in \mathbb{Z}/m\mathbb{Z})$ 两两不同.
(vii) $< a >= \{a, a^2, \cdots, a^{m-1}, a^m = e\}$.
(viii) 对任意的整数 $1 \leqslant d \leqslant m$, 有 $\mathrm{ord}(a^d) = \frac{m}{\gcd(d,m)}$.
无限循环群同构于加群 $\mathbb{Z}$
阶为 m 的有限循环群同构于加群 $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$
⇒
生成元为 a 和 a^{-1}
a^k 是生成元当且仅当 $\gcd(k, m) = 1$
关于元素的阶的性质
元素的阶
若 $\gcd(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$, 则 $\mathrm{ord}(a \cdot b) = \mathrm{ord}(a) \cdot \mathrm{ord}(b)$.
$\mathrm{ord}(c) = \mathrm{lcm}[\mathrm{ord}(a),\ \mathrm{ord}(b)]$
有限交换群的生成元构造
有限生成的交换群
设 G 是有限交换群, 则 G 中存在元素 $a_1, a_2, \cdots, a_s$ 满足
$\mathrm{ord}(a_{i+1}) \mid \mathrm{ord}(a_i)$, $1 \leqslant i \leqslant s-1$, 并且使得 $G =< a_1, a_2, \cdots, a_s >$.
交换加群（乘群）是一组循环群的直和（直积）
基底、线性无关、直积（和）
自由交换群
每个交换群 G 都是一个秩为 $|X|$ 的自由交换群的同态像子群

课程复习 -环与理想


环
同态
(i) 对任意 $a,b \subset R$, 有 $(a+b)^p = a^p + b^p$.
(ii) 环 R 到自身的映射 $\sigma : a \mapsto a^p$ 是自同态.
(无) 零因子环
有单位元的环
交换环
特征为 素数 p
特征为 0
特征
消去律
整环
整除
逆元
域
子域
素子域
F_p
有理数域
同构
核 $\ker f$
环同态基本定理
子环
子群
理想
由 X 生成的理想
素元
(真) 因子、倍元
单位
在整环 R 中, 素元一定是不可约元.
相伴元
主理想
极大理想
素理想
不可约元 (既约元)
分式域
主理想整环
商环

课程复习 -多项式环


多项式整环
多项式整除
$f(x)=q(x)\cdot g(x)+r(x),\ \deg r<\deg g.$
多项式欧几里得除法
余式为 0
多项式同余
因式、倍式
最小公倍式
最大公因式
$\gcd(f(x),g(x))=r_k(x),$
其中 $r_k(x)$ 是多项式广义欧几里得除法中最后一个非零余式.
$s_k(x)\cdot f(x)+t_k(x)\cdot g(x)=\gcd(f(x),g(x)),$
对于 $j=0,1,2,\cdots,k$, 这里 s_j,t_j 归纳定义为
$\begin{cases} s_{-2}(x)=1, s_{-1}(x)=0, s_j(x)=(-q_j(x))\cdot s_{j-1}(x)+s_{j-2}(x), \\ t_{-2}(x)=0, t_{-1}(x)=1, t_j(x)=(-q_j(x))\cdot t_{j-1}(x)+t_{j-2}(x), \end{cases}$
等价关系,
构建商环
不可约多项式
与所在的环或域有关
判别法则
相关性质
$p(x),\deg p\leqslant\frac{1}{2}\deg f,$ 都有 $p(x)\nmid f(x)$, 则 $f(x)$ 一定是不可约多项式.
互素
$g(x)\mid f(x),h(x)\mid g(x)$, 则 $h(x)\mid f(x)$.
$h(x)\mid s(x)\cdot f(x)+t(x)\cdot g(x)$.
$p(x)\mid a(x)\cdot b(x)$, 时, 有 $p(x)\mid a(x)$ 或 $p(x)\mid b(x)$
构成域
$\mathbb{F}_p[x]/(p(x))$ 元素个数为 p^n.
$K[x]/(p(x))$
多项式指数或阶
本原多项式
相关性质
设 p 是素数, $f(x),g(x)$ 是 $\mathbb{F}_p$ 上的多项式, 则
(i) 若整数 d 使得 $x^d\equiv 1 \mod f(x)$, 则 $\mathrm{ord}_p(f(x))\mid d$.
(ii) 如果 $g(x)\mid f(x)$, 则 $\mathrm{ord}_p(g(x))\mid\mathrm{ord}_p(f(x))$.
(iii) 如果 $\gcd(f(x),g(x))=1$, 则
$\mathrm{ord}_p(f(x)\cdot g(x))=\mathrm{lcm}[\mathrm{ord}_p(f(x)),\mathrm{ord}_p(g(x))]$.
(iv) 如果 $f(x)$ 是 $\mathbb{F}_p$ 上的 n 次不可约多项式, 则 $\mathrm{ord}_p(f(x))\mid p^n-1$.
判别法则
设 p 是素数, n 是正整数, $f(x)$ 是 $\mathbb{F}_p[x]$ 中的 n 次多项式.
(i) $x^{p^n-1}\equiv 1 \mod f(x)$.
(ii) 对于 p^n-1 的所有不同素因数是 $q_1,\cdots,q_s$,
$x^{\frac{p^n-1}{q_i}}\not\equiv 1 \mod f(x),\ i=1,\cdots,s,$
则 $f(x)$ 是 n 次本原多项式.
$R(f,g)\neq 0.$
多项式理想
素理想
结式
$s(x)\cdot f(x)+t(x)\cdot g(x)=R(f,g).$
$R(f,g)=a_n^m b_m^n\prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i-\beta_j).$
判别式

课程复习 -域和 Galois 理论、域的结构