



离散数学

Discrete Mathematics

第十三讲：子群与群的分解

吴楠

南京大学计算机科学与技术系

	R0	M2	R1	D2	R2	M1	R3	D1
R0								
M2								
D2								
R2								
M1								
R3								
D1								

2021 年 11 月 18 日



前情提要



- 对称的代数
- 半群
- **Monoid**
- 群
- 群论公理
- 群的性质





●	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	●	3	2	5	4	7	6	9	8	11	10	13	12	15	14	17	16	19	18	21	20	23	22
2	4	●	5	1	3	8	10	6	11	7	9	14	16	12	17	13	15	20	22	18	23	19	21
3	5	1	4	●	2	9	11	7	10	6	8	15	17	13	16	12	14	21	23	19	22	18	20
4	2	5	●	3	1	10	8	11	6	9	7	16	14	17	12	15	13	22	20	23	18	21	19
5	3	4	1	2	●	11	9	10	7	8	6	17	15	16	13	14	12	23	21	22	19	20	18
6	7	12	13	18	19	●	1	14	15	20	21	2	3	8	9	22	23	4	5	10	11	16	17
7	6	13	12	19	18	1	●	15	14	21	20	3	2	9	8	23	22	5	4	11	10	17	16
8	10	14	16	20	22	2	4	12	17	18	23	●	5	6	11	19	21	1	3	7	9	13	15
9	11	15	17	21	23	3	5	13	16	19	22	1	4	7	10	18	20	●	2	6	8	12	14
10	8	16	14	22	20	4	2	17	12	23	18	5	●	11	6	21	19	3	1	9	7	15	13
11	9	17	15	23	21	5	3	16	13	22	19	4	1	10	7	20	18	2	●	8	6	14	12
12	18	6	19	7	13	14	20	●	21	1	15	8	22	2	23	3	9	10	16	4	17	5	11
13	19	7	18	6	12	15	21	1	20	●	14	9	23	3	22	2	8	11	17	5	16	4	10
14	20	8	22	10	16	12	18	2	23	4	17	6	19	●	21	5	11	7	13	1	15	3	9
15	21	9	23	11	17	13	19	3	22	5	16	7	18	1	20	4	10	6	12	●	14	2	8
16	22	10	20	8	14	17	23	4	18	2	12	11	21	5	19	●	6	9	15	3	13	1	7
17	23	11	21	9	15	16	22	5	19	3	13	10	20	4	18	1	7	8	14	2	12	●	6
18	12	19	6	13	7	20	14	21	●	15	1	22	8	23	2	9	3	16	10	17	4	11	5
19	13	18	7	12	6	21	15	20	1	14	●	23	9	22	3	8	2	17	11	16	5	10	4
20	14	22	8	16	10	18	12	23	2	17	4	19	6	21	●	11	5	13	7	15	1	9	3
21	15	23	9	17	11	19	13	22	3	16	5	18	7	20	1	10	4	12	6	14	●	8	2
22	16	20	10	14	8	23	17	18	4	12	2	21	11	19	5	6	●	15	9	13	3	7	1
23	17	21	11	15	9	22	16	19	5	13	3	20	10	18	4	7	1	14	8	12	2	6	●



子群



■ 子群是群的子代数 (subalgebra)

■ 定义 (子群) :

设 $\langle G, *, e, {}^{-1} \rangle$ 为群, $H \subseteq G$, 若:

(1) $(\forall x, y \in H)(x * y \in H)$ (运算封闭性)

(2) $e \in H$ (单位元封闭性)

(3) $(\forall x \in H)(x^{-1} \in H)$ (逆元封闭性)

则称 $\langle H, * \rangle$ 为 $\langle G, * \rangle$ 的子群 (subgroup), 记为 $\langle H, * \rangle \leq \langle G, * \rangle$,

若 $H \subset G$, 称 $\langle H, * \rangle$ 为 $\langle G, * \rangle$ 的真子群, 记为 $\langle H, * \rangle < \langle G, * \rangle$



子群 (续)



- 设 $\langle G, *, e, {}^{-1} \rangle$ 为群，则 $\langle \{e\}, * \rangle \leq \langle G, * \rangle$ 和 $\langle G, * \rangle \leq \langle G, * \rangle$ 称为 G 的平凡子群 (trivial subgroup)
- 子群的例子：
 - $\langle \mathbb{Z}, + \rangle \leq \langle \mathbb{R}, + \rangle$
 - $\langle b\mathbb{Z}, + \rangle \leq \langle \mathbb{Z}, + \rangle, b \in \mathbb{Z}$

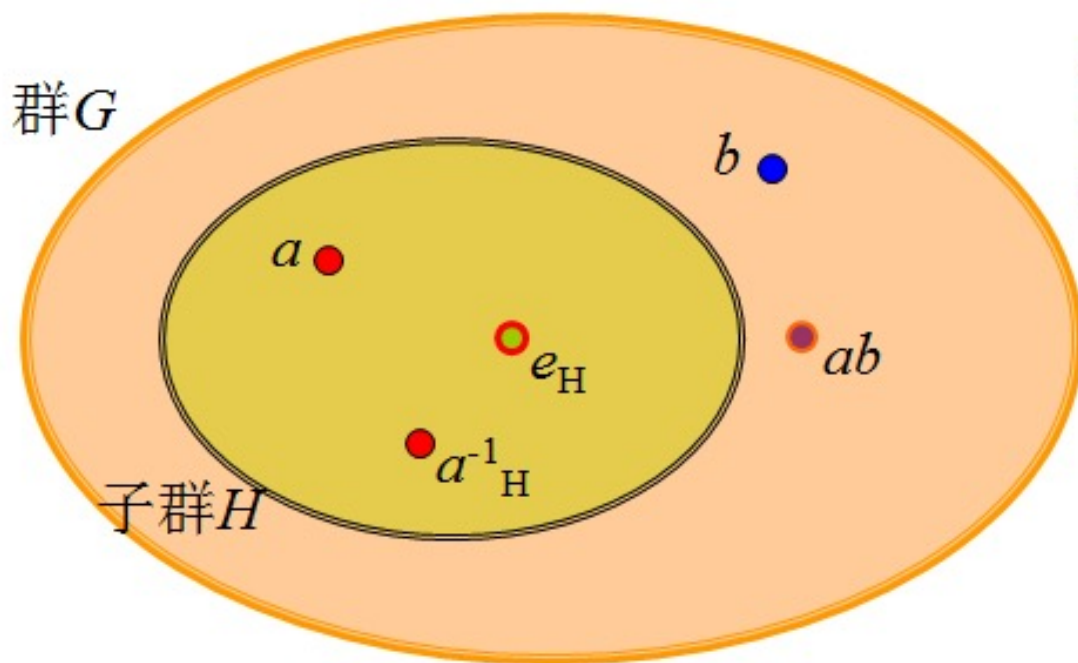


子群的判定定理



■ 考虑子群的存在条件：

问题1: ab 应该在哪儿?



问题2:
 e_H 是否一定是 e_G ?



子群的判定定理 (续)



■ 定理 (子群判定定理) :

设 $\langle G, *, e, {}^{-1} \rangle$ 为群, $H \subseteq G$, 以下四点等价:

(a) $\langle H, * \rangle \leq \langle G, * \rangle$

(b) $\langle H, *, e, {}^{-1} \rangle$ 为群

(c) (c.1) $H \neq \emptyset$

(c.2) $(\forall a, b \in H)(ab \in H)$

(c.3) $(\forall a \in H)(a^{-1} \in H)$

(d) (d.1) $H \neq \emptyset$ (d.2) $(\forall a, b \in H)(ab^{-1} \in H)$



子群的判定定理 (续)



证明: (a) \Rightarrow (b): 设 $\langle H, * \rangle \leq \langle G, * \rangle$, 由子群定义易得 $\langle H, *, e, {}^{-1} \rangle$ 为群。

(b) \Rightarrow (c): 设 $\langle H, *, e, {}^{-1} \rangle$ 为群

$$\because e \in H$$

\therefore (c.1) $H \neq \emptyset$ 成立。(c.2)与(c.3)易见。

(c) \Rightarrow (d): $\forall a, b \in H$, 由(c.3)知 $b^{-1} \in H$,

又由(c.2)得 $ab^{-1} \in H$ 。

(d) \Rightarrow (a): 由(d.1)知, $H \neq \emptyset$, 取 $b \in H$,

从而由(d.2)知 $bb^{-1} = e \in H$,

从而 $\forall a \in H$, 由(d.2)得 $ea^{-1} \in H$, 即 $a^{-1} \in H$ 。

又 $\forall a, b \in H$, 我们有 $a, b^{-1} \in H$,

由(d.2)知, $a(b^{-1})^{-1} = ab \in H$ 。

我们在验证 $\langle H, * \rangle$ 是否为 $\langle G, * \rangle$ 子群时, 只需验证 H 非空且运算 $*$, ${}^{-1}$ 对 H 封闭。



有限子群的判定定理



■ 定理（有限子群判定定理）：

设 G 为群， H 是 G 的非空有穷子集，则 H 是

G 的子群当且仅当： $\forall a, b \in H, ab \in H$



有限子群的判定定理 (续)



■ 证明:

必要性: 显然;

充分性: 只需要证明对 $a \in H, a^{-1} \in H$: 任取 $a \in H$, 若 $a = e$ 则 $a^{-1} = e \in H$; 若 $a \neq e$, 令 $S = \{a, a^2, a^3, \dots\}$, 则 $S \subseteq H$ 。因为 H 是有穷集, 必有 $a^i = a^j$; 不妨设正整数 $i < j$, 根据消去律, 有 $a^{j-i} = e$, 由于 $a \neq e$, 故 $j-i > 1$, 由此可得: $a^{j-i-1}a = e$ 且 $aa^{j-i-1} = e$ 。从而 $a^{-1} = a^{j-i-1} \in H$ 。

□



群中元素的阶



■ 定义（元素的阶）：

设 $\langle G, * \rangle$ 为群， $n \in \mathbb{Z}$, $a \in G$ ，以下定义 a^n ：

若 $n \geq 0$ ，则 a^n 已在上讲定义。

若 $n < 0$ ，则 $a^n = (a^{-n})^{-1}$ 。

若 $(\exists n \in \mathbb{N}^+)(a^n = e)$ ，则称 a 的阶(order)是有穷的且记 a 的阶 $|a| = \min\{n > 0 \mid a^n = e\}$ 。

若 $\neg (\exists n \in \mathbb{N}^+)(a^n = e)$ ，则称 a 的阶是无穷的，且记 a 的阶 $|a| = \infty$ 。

性质：

$$a^m a^n = a^{m+n}$$

$$(a^n)^m = a^{nm}$$



群中元素的阶 (续)



■ 例：

在 Klein 四元群 $\langle V, * \rangle$ 中, $|e| = 1$, 当 $a \neq e$ 时, $|a| = 2$ 。

在 $\langle \mathbb{Z}_7, \oplus_7 \rangle$ 中, $|0| = 1$, $a \neq 0$, $|a| = 7$ 。

在 $\langle \mathbb{Z}_6, \oplus_6 \rangle$ 中, 各元素的阶如下:

元素	0	1	2	3	4	5
阶	1	6	3	2	3	6

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e



群中元素的阶 (续)



■ 定理 (元素的阶的性质) :

设 $\langle G, * \rangle$, $a, b \in G$, $|a|, |b|$ 为有穷

$$(1) \text{ 对 } k \in \mathbb{Z}^+, a^k = e \Leftrightarrow |a| \mid k$$

$$(2) |a| = |a^{-1}|$$

$$(3) |ab| = |ba|$$

$$(4) |b^{-1}ab| = |a|$$



群中元素的阶 (续)



■ (1) 对 $k \in \mathbb{Z}^+$, $a^k = e \Leftrightarrow |a| \mid k$

证明: (1) “ \Rightarrow ” , 设 $|a| = m > 0$, $m = \min\{k \mid a^k = e \wedge k > 0\}$

故 $k \geq m$, 从而 $k = q \times m + r$, 这里 $0 \leq r < m$

$$\therefore a^k = a^{qm} * a^r = (a^m)^q * a^r = e^q * a^r = a^r$$

$$\therefore a^r = e$$

$$\therefore r < m$$

$$\therefore r = 0, \text{ 从而 } k = q \times m, \text{ 故 } m \mid k.$$

“ \Leftarrow ” , 设 $|a| = r$

$$|a| \mid k \rightarrow r \mid k \rightarrow k = n \times r \rightarrow a^k = a^{n \times r} = (a^r)^n = e^n = e$$



群中元素的阶 (续)



(2) 令 $|a| = r$

$$(2) \quad |b^{-1}ab| = |abb^{-1}| = |ae| = |a|$$

$$\because (a^{-1})^r = (a^r)^{-1} = e^{-1} = e$$

$$\therefore |a^{-1}| \mid |a|, \text{ 同理 } |a| \mid |a^{-1}|, \text{ 故 } |a^{-1}| = |a|.$$

$$(3) (ab)^{n+1} = abab \cdots ab = a(ba)^n b$$

Case 1: ab 的阶有穷, 设为 r

$$\text{从而 } (ab)^{r+1} = a(ba)^r b$$

$$\text{从而 } ab = a(ba)^r b, \text{ 故 } (ba)^r = e$$

故 ba 的阶有穷, 设为 r' , 由(1)知 $r' \mid r$

同理 $|ba| = r'$ 时有 $|ab|$ 有穷, 若为 r , 则 $r \mid r'$

因此 $|ab| = |ba|$. (4) 由(3)可知, $|b^{-1}ab| = |abb^{-1}| = |ae| = |a|$



群中元素的阶 (续)



- **例题**：设 $\langle G, * \rangle$ 为群，试证明：若 $|G| = n$ ，则
 G 中阶大于2的元素有**偶数个**

证明：

对于 $a \in G$ ，若 $|a| > 2$ ，则 $a \neq a^{-1}$ ，若不然，则 $a = a^{-1}$ ，从而 $a^2 = e$ ，故 $|a| \leq 2$ 与 $|a| > 2$ 矛盾！因此我们有 $|a| > 2 \rightarrow a \neq a^{-1}$ ，故 G 中阶 > 2 的元素 a 与其逆 a^{-1} 成对出现，因此 G 有偶数个阶 > 2 的元素。



陪集与群的分解



- 以下讨论群论中一个深远的问题：

子群将群分解为陪集 (coset)

- 定义 (陪集) : 设 $\langle H, * \rangle \leq \langle G, * \rangle$, $a \in G$, 令 :

$$Ha = \{ha | h \in H\}, \quad aH = \{ah | h \in H\}$$

称 Ha (或 aH) 为子群 H 在 G 中的右 (或左) 陪集,
 H 在 G 中右 (或左) 陪集的个数称为 H 在 G 中的指数 (index), 记为 $[G:H]$



陪集 (续)



- **例 1** : 令 $H = \{2n | n \in \mathbb{Z}\}$, $\langle H, + \rangle \leq \langle \mathbb{Z}, + \rangle$, $a \in \mathbb{Z}$, $Ha = \{2n + a | n \in \mathbb{Z}\}$, \because 对 $k \in \mathbb{Z}$, $H(2k + 1) = \mathbb{Z} - H$, $H(2k) = H$, $\therefore [\mathbb{Z} : H] = 2$, 此例中 $aH = Ha$
- **例 2** : $\langle \mathbb{Z}_6, \oplus_6 \rangle$ 为群, 令 $H = \{0, 3\}$, 则 $\langle H, \oplus_6 \rangle \leq \langle \mathbb{Z}_6, \oplus_6 \rangle$, 且 $H0 = H$, $H1 = \{1, 4\}$, $H2 = \{2, 5\}$
 $H3 = \{3, 0\} = H$, $H4 = \{4, 1\} = H1$, $H5 = \{5, 2\} = H2$,
因此 $[\mathbb{Z}_6 : H] = 3$, 易见 $\bigcup \{Ha | a \in \mathbb{Z}_6\} = \mathbb{Z}_6$



陪集与划分



■ **定理（陪集与划分）** : 设 $\langle H, * \rangle \leq \langle G, * \rangle$,

(1) $He = H$

(2) $(\forall a \in G)(a \in Ha)$ 从而 $\cup\{Ha|a \in G\} = G$

(3) $(\forall a, b \in G)(Ha = Hb \vee Ha \cap Hb = \emptyset)$

(4) $\{Ha|a \in G\}$ 为 G 之划分



证 (1) 易见 (2) $\{Ha \mid a \in G\} = \{Hb \mid b \in G\}$ 且 $Hb \cap Ha = \{e\}$ 故 $Hb \cap Ha = \{e\} = G$

(2) $\because a = ea$ 而 $e \in H \therefore a \in Ha$ 从而 $\cup\{Ha \mid a \in G\} = G$

(3) 任给 $a, b \in H$, 欲证 $Ha = Hb \vee Ha \cap Hb = \emptyset$, 只需证

$Ha \cap Hb \neq \emptyset \rightarrow Ha = Hb$. 设 $Ha \cap Hb \neq \emptyset$, 则有 $h_1, h_2 \in H$

使 $h_1a = h_2b$, 从而任给 $h \in H$, $ha = hh_1^{-1}h_2b \in Hb$

故 $Ha \subseteq Hb$ 同理 $Ha \supseteq Hb$, 因此 $Ha = Hb$.

(4) 由(1),(2),(3)即得



陪集等价关系



- 定义 “右陪集关系” : 设 $\langle H, * \rangle \leq \langle G, * \rangle$, 定义 G 上的二元关系 R :

$$(\forall a, b \in G) aRb \Leftrightarrow ab^{-1} \in H$$

则 R 是 G 上的等价关系, 且 $[a]_R = Ha$

- 相应地, 可以定义 “左陪集关系” R' :

$$(\forall a, b \in G) aR'b \Leftrightarrow b^{-1}a \in H$$



陪集等价关系 (续)



■ **引理 (陪集相等的判定)** : 设 $\langle H, * \rangle \leq \langle G, * \rangle$,

则 $\forall a, b \in G$:

$$a \in Hb \Leftrightarrow ab^{-1} \in H \Leftrightarrow Ha = Hb$$

证明:

见[屈婉玲] p.188 定理 10.8 的证明部分



陪集等价关系 (续)



- **证明 (右陪集关系是等价关系)** : 对于群 G 的子群 H ,
 $(a, b) \in R \Leftrightarrow ab^{-1} \in H$, 则二元关系 R 满足:
 - **自反性**: $\forall a \in G, aa^{-1} = e \in H \Leftrightarrow (a, a) \in R$;
 - **对称性**: $\forall a, b \in G, (a, b) \in R \Rightarrow ab^{-1} \in H \Rightarrow (ab^{-1})^{-1} \in H \Rightarrow ba^{-1} \in H \Rightarrow (b, a) \in R$;
 - **传递性**: $\forall a, b, c \in G, (a, b) \in R \wedge (b, c) \in R \Rightarrow ab^{-1} \in H \wedge bc^{-1} \in H \Rightarrow (ab^{-1})(bc^{-1}) = a(b^{-1}b)c^{-1} = ac^{-1} \in H \Rightarrow (a, c) \in R$.

因此关系 R 是等价关系。下面证明 $\forall a \in G, [a]_R = Ha$:
 $\forall b \in G, b \in [a]_R \Leftrightarrow (a, b) \in R \Leftrightarrow ab^{-1} \in H \Leftrightarrow Ha = Hb \Leftrightarrow b \in Ha$ (由引理及 $b \in Hb$). \square



陪集与群的分解



- 事实上，对群 $\langle G, * \rangle$ 和 $\langle H, * \rangle \leq \langle G, * \rangle$ ，若 $a, b \in G$ ，以下5个命题等价：

(1) $a \in Hb$

(2) $b \in Ha$

.....陪集元素

(3) $ab^{-1} \in H$

(4) $ba^{-1} \in H$

.....等价关系

(5) $Ha = Hb$

.....等价类
(i.e.划分块)



Lagrange 定理



■ 引理（陪集的势）：

设 $\langle H, * \rangle \leq \langle G, * \rangle$, $a \in G$, 则 $H \approx Ha \approx aH$

■ 证明：

令 $\tau: H \rightarrow Ha$ 为 $\tau(h) = ha$, $\sigma: H \rightarrow aH$ 为 $\sigma(h) = ah$, 由消去律可知 τ, σ 为 1-1, 易见 τ, σ 亦为 onto, 故 $H \approx Ha$, $H \approx aH$



Lagrange 定理 (续)



- 由上面的讨论可知，右陪集构成群的元素的一个划分，每个元素恰属某个右陪集；对于有限群，即可得到以下具有重要地位的经典结果：

- 定理(Lagrange, 1771)：设 $\langle G, * \rangle$ 为有限群， $\langle H, * \rangle \leq \langle G, * \rangle$ ，则 $|G| = |H| \cdot [G:H]$





Lagrange 定理 (续)



- **Lagrange定理**：设 $\langle G, * \rangle$ 为有限群， $\langle H, * \rangle \leq \langle G, * \rangle$ ，则 $|G| = |H| \cdot [G:H]$
- **证明**：由于 $|G|$ 有穷，故 $[G:H]$ 有穷，设其为 N ，从而有 $a_1, \dots, a_N \in G$ 使 $\{Ha_i | 1 \leq i \leq N\}$ 为 G 之划分，故 $G = \bigcup_{i=1}^N Ha_i$ ；由引理，对任意 i, j ： $|Ha_i| = |Ha_j| = |H|$ ， $\therefore |G| = |H| \cdot N$ 即 $|G| = |H| \cdot [G:H]$. \square



Lagrange 定理 (续)



- **推论1**：设 $\langle G, * \rangle$ 为**有限群**， $a \in G$ ，则 $|a|$ 为 $|G|$ 的因子
- **证明***：设 $|a| = r$ ，因为 $\langle \langle a \rangle, * \rangle \leq \langle G, * \rangle$ ^[注]，由Lagrange定理， $|\langle a \rangle|$ 为 $|G|$ 的因子，又由于 $|a|$ 有穷， $\langle a \rangle = \{a^0 = e, a^1, a^2, \dots, a^{r-1}\}$ ，故 $|\langle a \rangle| = |a|$ ，故 $|a|$ 为 $|G|$ 的因子。 □
- **注**： $\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$ ， $\langle \langle a \rangle, * \rangle$ 称元素 a 的**生成子群**，将在第20讲详述



Lagrange 定理 (续)



■ **推论2***：设 $\langle G, * \rangle$ 为 p 阶群，若 p 为质数，则

$$(\exists a \in G)(\langle a \rangle = G)$$

证：设 $|G| = p$ 为素数，可以取 $a \neq e, a \in G$, 由上推论知

$$|\langle a \rangle| \text{ 为 } |G| \text{ 的因子, } \because |\langle a \rangle| \geq 2 \therefore |\langle a \rangle| = p$$

$$\text{故 } G = \langle a \rangle$$



Lagrange 定理 (续)



命题：如果群 G 只含 1 阶和 2 阶元，则 G 是 Abel 群.

证 设 a 为 G 中任意元素，有 $a^{-1} = a$. 任取 $x, y \in G$ ，则

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx,$$

因此 G 是 Abel 群.

例 证明 6 阶群中必含有 3 阶元.

证 设 G 是 6 阶群，则 G 中元素只能是 1 阶、2 阶、3 阶或 6 阶.

若 G 中含有 6 阶元，设 6 阶元是 a ，则 a^2 是 3 阶元.

若 G 中不含 6 阶元，下面证明 G 中必含有 3 阶元.

如若不然， G 中只含 1 阶和 2 阶元，即 $\forall a \in G$ ，有 $a^2 = e$ ，

由命题知 G 是 Abel 群. 取 G 中 2 阶元 a 和 b ， $a \neq b$ ，令

$$H = \{e, a, b, ab\}$$

则 $H \leq G$ ，但 $|H| = 4$ ， $|G| = 6$ ，与拉格朗日定理矛盾.



本次课后作业



- 教材内容：[屈婉玲] 10.2 节
- 课后习题：
 - Problem Set 13
- 提交时间：11月30日（期中考试当日）



伽罗瓦(1811-1832)的遗书



我请求我的爱国同胞们，我的朋友们，不要指责我不是为我的国家而死。

我是作为一个不名誉的风骚女人和她的两个受骗者的牺牲品而死的。我将在可耻的诽谤中结束我的生命。噢！为什么要为这么微不足道的，这么可鄙的事去死呢？我恳求苍天为我作证，只有武力和强迫才使我在我曾想方设法避开的挑衅中倒下。

我亲爱的朋友：

我已经得到分析学方面的一些新发现……

在我一生中，我常常敢于预言当时我还不十分有把握的一些命题。但是我在这里写下的这一切已经清清楚楚地在我的脑海里一年多了，我不愿意使人怀疑我宣布了自己未完全证明的定理。

请公开请求雅可比或高斯就这些定理的重要性（不是就定理的正确与否）发表他们的看法。然后，我希望有人会发现将这一堆东西整理清楚会是很有益处的一件事。

热烈地拥抱你，

—— 伽罗瓦



期中测验通知



- **时间地点**：11月30日 14:00—16:00 @**仙II-311、仙II-312**
- **内容**：自开学到第13讲（子群与群的分解）课程所有内容（*标记的内容除外）
- **形式**：闭卷，题型均为解答题
- **占总评成绩比例**：20%
- **习题与复习课时间地点**：11月28日（周日）18:30 @ 计算机科学技术楼111会议室（第三领域咖啡馆内），复习课和习题课由助教主持，自愿参加；主要内容包括：课程内容回顾、作业错误总结、典型习题练习和助教现场答疑等