子群及其陪集

回顾

- 问题1：什么是代数系统?
  - 非空集合+封闭的(二元)运算
- 问题2：代数系统相关性质?
  - 封闭性、结合性、交换性、分配性；单位元、零元、逆元；同态同构
- 问题3：什么是群?
  - 封闭 + 结合律 + 单位元 + 逆元
- 问题4：群具有哪些性质?
  - 元素的阶、群的阶

本节提要

- 问题1：什么是子群，如何判别之?
- 问题2：子群一定存在么，若存在则满足什么性质?

子群的定义

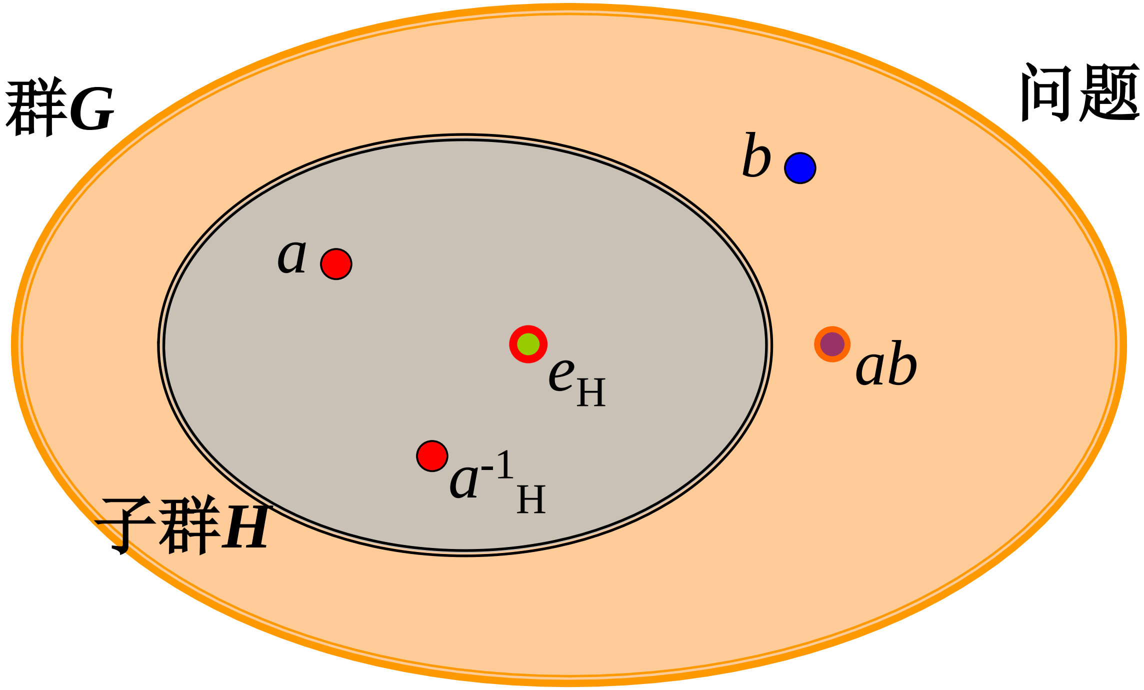
- 设(G, ∘)是群，H是G的非空子集，如果H关于G中的运算构成群，即(H, ∘)也是群，则H是G的子群。
  - 记作(H, ∘) ≤ (G, ∘), 简记为 H≤G。
- 例子：偶数加系统是整数加群的子群
- 平凡子群　(G, ∘)，　({e}, ∘)

注意：结合律在G的子集上均成立。

关于子群定义的进一步思考

问题1：e_H是否一定是e_G?　　$e_H\, e_H = e_H \rightarrow e_H = e_G$

问题2：ab应该在哪儿？



子群的判定：判定定理一

- G是群，H是G的非空子集。H是G的子群当且仅当：
  - $\forall a,b\in$H, $ab\in$H, 并且
  - $\forall a\in$H, $a^{-1}\in$H

  （注意：这里a^{-1}是a在G中的逆元，当H确定为群后，它也是a在H中的逆元）
- 证明
  - 必要性显然
  - 充分性：只须证明G中的单位元也一定在H中，它即是H的单位元。

子群的判定：判定定理二

- G是群，H是G的非空子集。H是G的子群当且仅当：

  $\forall a,b\in H,\ ab^{-1}\in H$

- 证明
  - 必要性易见
  - 充分性：
    - 单位元素：因为H非空，任取$a\in H$, $e=aa^{-1}\in H$
    - 逆元素： $\forall a\in H$, 因为$e\in H$, 所以 $a^{-1}=ea^{-1}\in H$
    - 封闭性： $\forall a,b\in H$, 已证$b^{-1}\in H$，所以$ab=a(b^{-1})^{-1}\in H$

子群的判定：判定定理三

- G是群，H是G的非空有限子集。H是G的子群当且仅当：

$$\forall a,b \in H,\ ab \in H$$

- 证明. 必要性显然. 下证充分性，只须证明逆元存在性
  - 若H中只含G的单位元，H显然是子群。
  - 否则，任取H中异于单位元的元素a, 考虑序列

$$a,\ a^2,\ a^3,\ \ldots$$

注意：该序列中各项均为有限集合H中的元素，因此，必有正整数i, j(j>i+1), 满足：$a^i=a^j$,由消去率有$e=a^{j-i}$, 因此：

$$a^{-1}=a^{j-i-1} \in H$$

本节提要

- 问题1：什么是子群，如何判别之?
  - 非空子集 + 封闭、结合律、单位元、逆元
  - 判定：根据定义或三个判定定理
- 问题2：子群一定存在么，若存在则满足什么性质?

生成子群

- 设G是群，$a\in$G，构造G的子集H如下：

$$H = \{a^k \mid k\text{是整数}\}$$

  则H构成G的子群，称为a生成的子群$\langle a\rangle$

- 证明：
  - H非空：a在H中
  - 利用判定定理二：

$$\forall a^m, a^n \in H,\ a^m(a^n)^{-1} = a^{m-n} \in H$$

非平凡子群一定存在么？

左(右)陪集

- 若H是群G的一个子群，a是G中的任意一个元素，定义：$a\mathrm{H} = \{ ah \mid h \in \mathrm{H} \}$
- aH称为H的一个左陪集
  - 由群的封闭性可知，aH也是G的子集
  - $\forall h \in \mathrm{H}.\ ah \in \mathrm{H}$ *iff* $a \in \mathrm{H}$ (陪集不一定是子群)
- 类似可定义右陪集

陪集与划分

- 设H是群G的子群，则H的所有左陪集构成G的划分
  - G中任意元素a一定在某个左陪集中：$a \in a\mathrm{H}$
  - $\forall a,b \in \mathrm{G}$, $a\mathrm{H}=b\mathrm{H}$或者$a\mathrm{H} \cap b\mathrm{H}=\varnothing$
    - 假设$a\mathrm{H} \cap b\mathrm{H} \neq \varnothing$, 即存在$c \in a\mathrm{H} \cap b\mathrm{H}$, 令$c=ah_1=bh_2$
    - 则$a=bh_2h_1^{-1}$, 从而$a\mathrm{H} \subseteq b\mathrm{H}$
    - 同理可得： $b\mathrm{H} \subseteq a\mathrm{H}$. 所以 $a\mathrm{H}=b\mathrm{H}$
- 注：a, b属于同一左陪集

  iff $a \in b\mathrm{H}$

  iff $b^{-1}a \in \mathrm{H}$

例

- 令$H=\{2n|n\in\mathbb{Z}\}$，$\langle H,+\rangle<\langle\mathbb{Z},+\rangle$，$a\in\mathbb{Z}$，$aH=\{2n+a|n\in\mathbb{Z}\}$，$(2k)H=H$，$(2k+1)H=\mathbb{Z}-H$，$\{0H,1H\}\mathbb{Z}$的一个划分。
- $\langle\mathbb{Z}_6,\oplus_6\rangle$为群，令$H=\{0,3\}$，$\langle H,\oplus_6\rangle<\langle\mathbb{Z}_6,\oplus_6\rangle$，$H0=H$，$H1=\{1,4\}$，$H2=\{2,5\}$

  $H3=H,H4=\{4,1\}=H1,H5=\{5,2\}=H2$

  $\{H0,H1,H2\}$是$\mathbb{Z}_6$的一个划分。

例：左陪集关系

- 设H是群G的子群，定义G上的二元关系R如下：$\forall a,b\in G$, $(a,b)\in R$当且仅当$b^{-1}a\in H$。证明R是G上的等价关系，并给出R的等价类。

- R是G上的等价关系
  - 自反性：$\forall a\in G$, $a^{-1}a=e$
  - 对称性：注意$a^{-1}b=(b^{-1}a)^{-1}$
  - 传递性：如果$b^{-1}a\in H$, $c^{-1}b\in H$, 则

$$c^{-1}a=c^{-1}(bb^{-1})a=(c^{-1}b)(b^{-1}a)\in H$$

- $[a]_R=aH$：$x\in[a]_R \Leftrightarrow aRx \Leftrightarrow x^{-1}a=h\in H \Leftrightarrow x=ah^{-1}\in aH$

例：正规子群

- **H是群G的一个子群，*a*是G中的任意一个元素，H称为G的正规子群 *iff*：*a*H = H*a***
  - 即：对任意的$h_i \in H$, $a \in G$，一定存在$h_j \in H$使得$h_i a = a h_j$
  - 注：h_i与h_j不一定相等
- 证明：子群**N**是**G**的正规子群当且仅当对于任意的$g \in G$, $n \in N$ 有 $gng^{-1} \in N$。
  - $\Rightarrow$ 存在$n_1 \in N$ 使得$gn = n_1 g$, 即$gng^{-1} = n_1 \in N$;
  - $\Leftarrow$ 先证$gN \subseteq Ng$: 对于任意的$gn \in gN$, 因$gng^{-1} \in N$，定义$gng^{-1} = n_1$，则有$gn = n_1 g \in Ng$；同理有$Ng \subseteq gN$。

例：正规子群的左陪集关系

- N是G的正规子群，左陪集关系为$(a,b)\in R$当且仅当$b^{-1}a\in N$。如果$p^{-1}a\in N$, $q^{-1}b\in N$, 则有$(pq)^{-1}(ab)\in N$。
  - 证明：令$p^{-1}a=n_1$, $q^{-1}b=n_2$ $(n_1,n_2\in N)$

    则有$(pq)^{-1}(ab) = q^{-1}p^{-1}ab = q^{-1}n_1b = n_3q^{-1}b$ (正规子群)

    $=n_3n_2 \in N$
- 同余关系：
  - 若(S,*)为一个半群，S上的等价关系R如满足：
    aRa' and bRb' imply $(a * b)R(a' * b')$，则称R为同余关系。

Lagrange 定理

- 引理（陪集的势）

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

- 证明：

令$\sigma: H \to aH$为$\sigma(h) = ah$，由消去律可知

σ为1-1，易见σ亦为满射，故$H \approx aH$。

同理可证$H \approx Ha$。

Lagrange 定理（续）

- $\{aH|\ a\in G\}$ 是G的一个划分。
- 对有限群G，每个陪集元素个数有限且相同，并等于$|H|$, 于是$|G|=k|H|$, k是左（右）陪集的个数，称为H在G中的指数，记为$[G:H]$

Lagrange 定理（续）

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

- **证明：** 由于$|G|$有穷，故$[G:H]$有穷且设为N，从而有$a_1,\cdots,a_N \in G$使$\{a_iH|1 < i \leq N\}$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*：$\because \langle \langle a \rangle, * \rangle \leq \langle G, * \rangle \therefore |\langle a \rangle|$为$|G|$的因子，又由于$|a|$有穷，故$|\langle a \rangle| = |a|$，故$|a|$为$|G|$的因子. $\square$

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

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

故$G = \langle a\rangle$

拉格朗日定理的应用

- **6阶群G必含3阶子群**
- 证明
  - 如果G中有6阶元素a, 则$b=aa$是3阶元素，因此$\langle b\rangle$是3阶子群
  - 如果G中没有6阶元素，则根据拉格朗日定理的推论，G中元素的阶只可能是1,2或3。
    - 如果没有3阶元素，即$\forall x\in G$, $x^2=e$, 那么$\forall x, y\in G$, $xy=(yx)^2(xy)=yx$, 即G是交换群。
    - 因此，易证$\{e,a,b,ab\}$构成4阶子群，但4不能整除6，矛盾。
  - 所以G中必含3阶元素a, 即由a生成的子群是3阶子群。

本节小结

- 问题1：什么叫做群的子群，如何判别之?
  - 非空子集 + 封闭、结合律、单位元、逆元
  - 判定：根据定义或三个判定定理
- 问题2：子群一定存在么，若存在则满足什么性质?
  - 一定存在平凡子群
  - 子群**H**的所有陪集构成母群**G**的一个划分
  - 拉格朗日定理及其推论：有限群的子群阶是母群阶的因子、有限质数阶群没有非平凡子群、有限质数阶群一定是循环群

作业

- 见课程主页