第四讲子群、生成子群

陈建文

February 14, 2023

定义1. 设S为群G的非空子集，如果G的运算在S中封闭且S对此运算也构成一个群，则称S为G的一个子群。如果$S \neq G$，则称S为G的真子群。

定理1. 设G为一个群，则$\{e\}$为G的子群，G为G的子群。

例. $(Z,+)$为$(Q,+)$的子群，$(Q,+)$为$(R,+)$的子群，$(R,+)$为$(C,+)$的子群；$(Q^*,\times)$为$(R^*,\times)$的子群，$(R^*,\times)$为$(C^*,\times)$的子群。这里Q^*, R^*和C^*本别代表非零有理数集合、非零实数集合和非零复数集合。集合$\{1,-1\}$对通常的乘法构成一个群，但它不是$(Q,+)$的子群，因为它们的运算不一样。

定理2. 设G_1为G的子群，则G_1的单位元必为G的单位元；G_1的元素a在G_1中的逆元素也是a在G中的逆元素。

证明. 设G_1的单位元为e_1，G的单位元为e，则$e_1e_1 = e_1e$，由消去律得$e_1 = e$。

设b为a在G_1中的逆元，则$ba = e$，该式在G中也成立，于是b也是a在G中的逆元。 □

定理3. 群G的任意多个子群的交还是G的子群。

证明. 设H为G的一些子群的交，则$e \in H$，从而$H \neq \phi$。其次，$\forall a, b \in H$，ab在每个参加交运算的子群中，从而$ab \in H$。所以，G的运算在H中封闭。最后，$\forall a \in H$，由a在每个参加交运算的子群中知a^{-1}在每个参加交运算的子群中，故$a^{-1} \in H$。因此，H为G的子群。 □

定理4. 任一群不能是其两个真子群的并。

证明. 用反证法。设G_1和G_2为G的两个真子群，且$G_1 \cup G_2 = G$。由于G_1和G_2为G的真子群，所以$\exists a, b \in G$，$a \notin G_1$，$b \notin G_2$。于是$a \in G_2$，$b \in G_1$，从而$ab \in G$，但$ab \notin G_1$且$ab \notin G_2$，这与$G = G_1 \cup G_2$矛盾。 □

定理5. 群G的非空子集S为G的子群的充分必要条件是

（1） $\forall a, b \in S, ab \in S$且

（2） $\forall a \in S, a^{-1} \in S$。

证明. $\Rightarrow$ 显然。

$\Leftarrow$ 运算的封闭性显然成立；运算的结合律显然成立；由S非空知$\exists a \in S$，从而$a^{-1} \in S$，于是$e = a^{-1}a \in S$。 □

定理6. 群G的非空子集S为G的子群的充分必要条件是$\forall a, b \in S, ab^{-1} \in S$。

证明. $\Rightarrow$ 显然。

$\Leftarrow$ 由S非空知$\exists a\in S$，从而$e=aa^{-1}\in S$;

$\forall g\in S$，$g^{-1}=eg^{-1}\in S$;

$\forall a,b\in S$，$b^{-1}\in S$，从而$ab=a(b^{-1})^{-1}\in S$。 □

定理7. 群G的有限非空子集F为G的子群的充分必要条件是$\forall a,b\in F,ab\in F$。

$\forall A,B\in 2^G$，定义$AB=\{ab|a\in A,b\in B\}$，则以上定理可以写成

定理8. 群G的有限非空子集F为G的子群的充分必要条件是$FF\subseteq F$。

定义2. 群G的元素a称为G的中心元素，如果a与G的每个元素可交换，即$\forall x\in G,ax=xa$。G的所有中心元素构成的集合C称为G的中心。

定理9. 群G的中心C是G的可交换子群。

证明. $\forall x\in G,ex=xe=x$，所以$e\in C$，故$C\neq\phi$。

$\forall a,b\in C$，$\forall x\in G$，$(ab)x=a(bx)=a(xb)=(ax)b=(xa)b=x(ab)$，从而$ab\in C$。

$\forall a\in C$，$\forall x\in G$，由$ax=xa$可得$xa^{-1}=a^{-1}x$，从而$a^{-1}\in G$。

故C为G的子群。C显然是可交换的。 □

例. 设G为一个群，$a\in G$，$\{\cdots,a^{-2},a^{-1},e,a,a^2,\cdots\}$为$G$的一个子群。

例. 设G为一个有限群，$a\in G$，$\{e,a,a^2,\cdots\}$为G的一个子群。

例. 设G为一个交换群，$a,b\in G$，则$\{a^mb^n|m,n\in Z\}$为G的一个子群。

定义3. 设M为G的一个非空子集，G的包含M的所有子群的交称为由M生成的子群，记为(M)。

$(\{a\})$简写为(a)，$(a)=\{\cdots,a^{-2},a^{-1},e,a,a^2,\cdots\}$。

$(\{a,b\})$简写为(a,b)。如果G为一个交换群，$a,b\in G$，则$(a,b)=\{a^mb^n|m,n\in Z\}$。

$(M)=\{m_1m_2\cdots m_r|r\in Z^+,m_i\in M\vee m_i^{-1}\in M,i=1,2,\ldots,r\}$。

课后作业题:

练习1. 举例说明两个子群的并可以不是子群。

解. $S_6=\{[0],[1],[2],[3],[4],[5]\}$,

$\{[0],[2],[4]\}$和$\{[0],[3]\}$为S_6的两个子群，但$\{[0],[2],[4]\}\cup\{[0],[3]\}=\{[0],[2],[3],[4]\}$不是$S_6$的子群，因为$[2]+[3]=[5]\notin\{[0],[2],[3],[4]\}$。 □

练习2. 设G_1和G_2为群G的两个真子群，证明：$G_1\cup G_2$为G的子群的充分必要条件是$G_1\subseteq G_2$或者$G_2\subseteq G_1$。

证明. 如果$G_1\subseteq G_2$或者$G_2\subseteq G_1$，则$G_1\cup G_2=G_2$或G_1，此时显然$G_1\cup G_2$为G的子群。

如果$G_1\cup G_2$为G的子群，以下用反证法证明$G_1\subseteq G_2$或者$G_2\subseteq G_1$。假设$G_1\nsubseteq G_2$并且$G_2\nsubseteq G_1$，则存在$g_2\in G_2$，但是$g_2\notin G_1$，同时存在$g_1\in G_1$，但是$g_1\notin G_2$。于是G_1为$G_1\cup G_2$的真子集，G_2为$G_1\cup G_2$的真子集，易得G_1和G_2为$G_1\cup G_2$的真子群，由于任一群不能是两个真子群的并，矛盾。 □

练习3. 设$(G_1, \circ)$和$(G_2, *)$都是群，$\phi : G_1 \to G_2$，$\forall a, b \in G_1$，$\phi(a \circ b) = \phi(a) * \phi(b)$，证明：$\phi^{-1}(e_2)$为$G_1$的子群，其中$e_2$为$G_2$的单位元素。

证明. 设e_1为G_1的单位元，则$\phi(e_1) = \phi(e_1 \circ e_1) = \phi(e_1) * \phi(e_1)$，两边同时左乘$\phi(e_1)^{-1}$，得$\phi(e_1) = e_2$，从而$e_1 \in \phi^{-1}(e_2)$，所以$\phi^{-1}(e_2)$非空。

$\forall x, y \in \phi^{-1}(e_2)$，$\phi(x) = \phi(y) = e_2$，从而$\phi(x \circ y) = \phi(x) * \phi(y) = e_2 * e_2 = e_2$，故$x \circ y \in \phi^{-1}(e_2)$，于是$G$中的乘法在$\phi^{-1}(e_2)$中封闭。

$\forall x \in \phi^{-1}(e_2)$，$e_2 = \phi(e_1) = \phi(x^{-1} \circ x) = \phi(x^{-1}) * \phi(x) = \phi(x^{-1}) * e_2 = \phi(x^{-1})$，从而$x^{-1} \in \phi^{-1}(e_2)$。

以上证明了$\phi^{-1}(e_2)$为G_1的子群。 □

练习4. 找出3次对称群的所有子群。

解. (1)，$\{(1), (1, 2)\}$，$\{(1), (1, 3)\}$，$\{(1), (2, 3)\}$，$\{(1), (123), (132)\}$，S_3。 □

练习5. 令$P = \{(12), (123)\} \subseteq S_3$。写出由$P$生成的$S_3$的子群$(P)$。

解. $(P) = S_3$。

显然$(1) \in (P), (12) \in (P), (123) \in (P)$。

其他元素可以由以下计算得到：

$(12)(123) = (13)$，$(123)(12) = (23)$，$(123)(123) = (132)$。 □