1 群论

1.1 群的原始定义和一些性质

1.1.1 群的原始定义

设G是一个非空集合，$*$是G上的乘法运算，如果它们满足以下性质：

①运算封闭：$\forall a, b \in G, a * b \in G$；

②满足结合律：$\forall a, b, c \in G, (a * b) * c = a * (b * c)$；

③有单位元：$\forall a \in G, \exists e \in G, s.t. a * e = e * a = a$；

④有逆元：$\forall a \in G, \exists a' \in G, s.t. a * a' = a' * a = e$；

则连同$G, *$称为一个群，记为$< G, * >$，有时为了方便也直接说G是一个群。

1.1.2 群的附加定义

（1）若只满足①②，称$< G, * >$为半群。

（2）若只满足①②③，称$< G, * >$为带1半群。

（3）若群还满足交换律，称$< G, * >$为交换群（Abel群）。

1.1.3 群的简单性质

（1）可定义方幂：$a^k = a * a * \cdots * a$(k个)

（2）左消去律、右消去律成立：$\forall a, b, c \in G, a * c = b * c \Rightarrow a = b$；（左消去律类似）

> c有逆元c'对吧，两边右乘就可以证明。

（3）在乘法群中，$a * x = b$有唯一解$a' * b$。（$y * a = b$类似）

> 假设有两个不同解，利用消去律可以证明这两个解相等，矛盾。

（4）群G中单位元和某元素的逆元都是唯一的。

（5）$(a')' = a$；

（6）$(a * b)' = b' * a'$；

1.1.4 群的衍生定义

（1）在群G中，G若为有限集合，则称G是有限群，其**阶数**记为$|G|$；

（2）在群G中，对于某个元素a，如果存在满足$a^n=e$的最小正整数n，则称元素a是n阶的，否则称之为无限阶的；

（3）类似数论中的阶，如果对于a有$a^m=e$，设a是n阶元，则一定有$n|m$；

1.1.4.1 举例

在群G中，有m阶元a，有n阶元b，(m, n)=1，如果$a*b=b*a$，则$a*b$是mn阶元；

> 设$a*b$的阶为k；
>
> $(a*b)^{mn}=(a^m)^n*(b^n)^m=e$（第二个等号用到交换性），故$k|mn$；
>
> $e=(a*b)^{km}=(a^m)^k*b^{km}=b^{km}$，故$n|km$，又因为$(m,n)=1$，则$n|k$，同理$m|k$，故$[m,n]|k$，也即$mn|k$。

1.2 群的等价定义

1.2.1 削弱条件的群定义

设G是一个非空集合，$*$是G上的乘法运算，如果它们满足以下性质：

①运算封闭：$\forall a,b\in G,a*b\in G$；

②满足结合律：$\forall a,b,c\in G,(a*b)*c=a*(b*c)$；

③有右单位元：$\forall a\in G,\exists e_r\in G,s.t.a*e_r=a$；

④有右逆元：$\forall a\in G,\exists a'\in G,s.t.a*a'=e_r$；

则$<G,*>$为群。

> 【1】先证右逆一定是左逆。
>
> $a*a'=e_r$，设a'的右逆是a''，则$a'*a''=e_r$，我们要证明$a'*a=e_r$。
>
> $a'*a=(a'*a)*e_r=(a'*a)*(a'*a'')=a'*a''=e_r$。
>
> 【2】再证右单位元一定是左单位元。
>
> $e_r*a=(a*a')*a=a*e_r=a$。

1.2.2 替换条件的群定义

设G是一个非空集合，$*$是G上的乘法运算，如果它们满足以下性质：

①运算封闭：$\forall a, b \in G, a * b \in G$；

②满足结合律：$\forall a, b, c \in G, (a * b) * c = a * (b * c)$；

③$\forall a, b \in G$，方程$ax = b, ya = b$在G中都有解。

则$< G, * >$为群。

> 【1】先证有右单位元。
>
> 因为方程$ax = a$有解，设其中一个是e_r；方程$ya = b$有解，其中一个是c，则$c * a = b$
>
> $b * e_r = (c * a) * e_r = c * a = b$，由于b的任意性，知道$e_r$就是我们要找的右单位元；
>
> 【2】再证有右逆。
>
> 现在我们知道$a * x = e_r$一定有解，所以$x = a'$就是右逆。

1.3 有限群

1.3.1 有限群的定义

设G是一个非空<u>有限</u>集合，$*$是G上的乘法运算，如果它们满足以下性质：

①运算封闭：$\forall a, b \in G, a * b \in G$；

②满足结合律：$\forall a, b, c \in G, (a * b) * c = a * (b * c)$；

③左消去律、右消去律都成立。

则$< G, * >$为群。

> 令$G = \{a_1, a_2, \cdots, a_n\}$，任取$G$中的某个元素记为$a$，与G中每个元素左乘，得到集合$G' = \{a * a_1, a * a_2, \cdots, a * a_n\}$。
>
> 由①知道$a * a_i \in G$，所以$G' \subseteq G$；
>
> 由于消去律成立，当$i \neq j$时，一定有$a * a_i \neq a * a_j$，所以$|G| = |G'| = n$；
>
> 所以有$G' = G$；
>
> 任取$a, b \in G$,一定有某个$x \in G$，使$a * x = b$。y的情况类似。

1.3.2 乘法表

有限群的乘法可以用乘法表来表示。

（1）有一行(列)与边栏元素一致，因为存在单位元；

（2）全体元素必在每行出现一次、在每列出现一次，因为消去律成立。

下面所示的是K$_4$群，$C_4 = \{e, a, a^2, a^3\}, K_4 = \{e, a, b, c\}$

$$\begin{array}{c|cccc} * & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & e & c & b \\ b & b & c & e & a \\ c & c & b & a & e \end{array} \tag{1}$$

1.3.3 有限群的一些性质

设G是有限群，则G的每个元素的阶都是有限的。

> 任取G的一个元素a，用a和e生成一个列：$e, a, a^2, \ldots, a^n, \ldots,$
>
> 这样的序列不能无限进行下去，一定有某个$i \neq j$，$a^i = a^j$，则$a^{i-j} = e$，这表示a是有限阶的。

1.4 子群

1.4.1 子群的定义

G是群，H是G的非空子集，如果

①$\forall a, b \in H, a * b \in H$；

②$\forall a \in H, a' \in H$；

则称H是G的子群，记为$H \leq G$。

1.4.2 子群的性质

（1）H是G的子群，则H也是群。

> 再验证结合律、$h * h' = e \in H$

（2）若H是G的有限非空子集，只要满足封闭性，就可以断言H是G的子群。

> 任取G的一个元素a，用a和e生成一个列：$e, a, a^2, \ldots, a^n, \ldots,$
>
> 这样的序列不能无限进行下去，一定有某个$i \neq j$，$a^i = a^j$，则$a^{i-j} = e$。
>
> 则$a * a^{i-j-1} = e$，定义后者为逆元即可。

（3）设$H_1 \subseteq H_2 \subseteq \ldots \subseteq H_n \subseteq \ldots$是群G的子群升链，令$H=\bigcup_i H_i$，则$H \leq G$。

（4）若S是群G的一个非空子集，集合$A=\{H|H \leq G且S \subseteq H\}$，即所有包含S构成的子群的集合，设$K=\bigcap_{H\in A} H$，则$K \leq G$。

> 用定义验证，并且对于（4）还可以做如下讨论：
>
> K 记 作 S 生 成 的 子 群 ， 记 为 $<S>$ ， 可 以 验 证 $\{a_1^{e_1} * a_2^{e_2} * \ldots * a_n^{e_n} | a_i \in S, e_i = \pm 1, n = 1, 2, \ldots\} =< S >$
>
> 这就是S生成的子群的构造。

1.5 循环群

1.5.1 定义

这样一类群，它的每一个元素都可以写成某个固定元素的幂次a^i或a^{-i}。

1.5.2 生成元

这样的g，使得$G=\{g^n|n\in\mathbb{Z}\}$。记$G=< g >$。

1.5.3 循环群的性质

（1）设元素g是群G中的k阶元，由g和e生成的群$\{g^n|n\in\mathbb{Z}\}$是$<G,*>$的一个k阶子群，即$H=\{g^0,g^1,\ldots,g^{k-1}\}$。

> 证明：$\forall g^r, g^s \in H, g^r * g^s = g^{r+s} \in H$，且任意元素$g^j$有逆元$g^{-j}$，所以H是子群。因为我们知道$g$是一个k阶元，那么$e, g, g^2, \ldots, g^{k-1}$应当是互不相同的元素，其余元素都与之中的某个相等。
>
> 特别：若G是n阶群，G中有n阶元g，则G=$< g >$。

（2）循环群的子群必是循环群。

> 令$G=< a >$，$H=\{e\}$时显然正确，
>
> 当$H\neq\{e\}$时，一定有$b\in H, b\neq e$，由于b也是G中的元素，存在一个标号$n, b=a^n$。
>
> 因为我们要了解H的结构，并且知道了H包含a的某个幂次，所以我们假设一个标号m，它是满足$a^m\in H$的最小正标号，于是设$n=mu+v, 0\leq v<m$，
>
> 则$b=a^n=a^{mu+v}=(a^m)^u * a^v$，则$a^v=a^{-mu} * a^n$，显然$a^v\in H$，若v>0，这与假设m是最小的正标号矛盾，故v=0，即$b=(a^m)^u$，由于m是与b无关的，则H中每个元素都可以表示成a^m的幂次，于是H是循环群。

（3）G是n阶循环群，$G=\langle a\rangle$且$|G|=n$，H是G的一个子群，$H=\langle b\rangle,b=a^s$。则$|H|=\dfrac{n}{(n,s)}$。

> 设H是一个m阶子群，m是b的阶（1得来），则$b^m=a^{sm}=e$（1中“特别”得来）
>
> a是n阶元，故$n|sm$，设$(n,s)=d$，$n=n_0d,s=s_0d$，且$(n_0,s_0)=1$，
>
> 所以$n_0|s_0m$，故$n_0|m$，m是满足这个式子的最小正整数，因此$m=n_0=\frac{n}{(n,s)}$。

1.6 置换群

1.6.1 用置换定义对称群

n元集合$A=\{1,2,\cdots,n\}$上的全体置换构成集合S_n，其在**合成运算**下构成一个群，称之为n次对称群，阶数为n!。

【命题】S_3是最小的非交换的对称群，与K_4同构。它可以表示为

$S_3=\left\{1,x,y,x^2,xy,x^2y\mid x^3=1,y^2=1,yx=x^2y\right\}$

这种表示方法的优点是写起来简单，所以运算方便。通过这个集合的约束条件我们也容易看出x,y代表这个集合的什么元素。另一方面也说明了，通过取一个群的部分元素进行不断的运算，是**可以表示出**这个完整的群的。这个思想也在之后的陪集相关概念中得到了验证。

1.6.2 用映射定义对称群

集合A上的**双射全体**对于映射的合成运算构成群，该群叫做对称群。

1.6.3 置换群

（1）对称群的子群叫置换群。

（2）置换群通常是非交换群。

1.6.4 置换群中性质

（1）$S_n=<(1\ 2),(1\ 3),\ldots,(1\ n))>$。

> 【1】证明$<(1\ 2),(1\ 3),\ldots,(1\ n))>\subseteq S_n$。
>
> 由S生成的子群的构造，$<(1\ 2),(1\ 3),\ldots,(1\ n))>=\{\sigma_1\sigma_2\cdots\sigma_n|\sigma_i=(1\ j),1\leq i,j\leq n,n=1,2,\ldots\}$
>
> （注意到$(1\ j)'=(1\ j)$）显然成立命题。
>
> 【2】证明$S_n\subseteq<(1\ 2),(1\ 3),\ldots,(1\ n))>$。
>
> 只要证明任意一个n元置换都能写成那些基本元素的乘积就可以了。

> 下面对n进行归纳，n=2时显然成立，假设对n=k时也成立，当n=k+1时，
>
> $\sigma = \begin{pmatrix} 1 & 2 & \cdots & k & k+1 \\ \sigma(1) & \sigma(2) & & \sigma(k) & \sigma(k+1) \end{pmatrix}$有两种情况，
>
> 一是$\sigma(k+1) = k+1$，此时σ本身是k元置换，命题显然成立。
>
> 二是不等于，那么前k个元素里一定有一个是k+1，用一个置换把它换到k+1的位置上即可。
>
> （注意到$(i\ j) = (1\ i)(1\ j)(1\ i)$）

1.7 群的同构

1.7.1 定义

$< G_1, *>, < G_2, \cdot >$是两个群，如果存在从$G_1$到$G_2$的双射$\phi$，使得对于任何$a, b \in G_1$，都有$\phi(a * b) = \phi(a) \cdot \phi(b)$，称两个群同构，记为$G_1 \cong G_2$，$\phi$称为同构映射。

1.7.2 同构的群满足的性质

（1）单位元满足：$\phi(e_1) = e_2$；

（2）逆元满足：$\phi(a') = \phi'(a)$。

> （1）$\phi(a) = \phi(a * e_1) = \phi(a) \cdot \phi(e_1)$，同时左乘$\phi'(a)$，所以$e_2 = e_2 \cdot \phi(e_1) = \phi(e_1)$
>
> （2）$\phi'(a) = \phi'(a) \cdot \phi(e_1) = \phi'(a) \cdot \phi(a) \cdot \phi(a') = \phi(a')$

1.7.3 举例

（1）同构的意义下循环群$G =< a >$只有两类：

①若a是无限阶元，则$G \cong< \mathbb{Z}, + >$；（取$f(a^m) = m$）

②若a是n阶元，则$G \cong \mathbb{Z}_n$。（取$f(a^i) = [i]$）

（2）任意一个群都与一个置换群同构。

> 这个置换群是$G' = \{f_a | a \in G, f_a : G \to G, f_a(x) = a * x\}$
>
> 同构映射为$G \to G' : h(a) = f_a$

（3）与n阶循环群同构的置换群是$< (a^0, a^1, \dots, a^{n-1}) >$。

（4）如果仅知道群$< G, * >$和一个双射f，这双射满足$f(a * b) = f(a) \cdot f(b)$，令$G' = \{f(a) | a \in G\}$，可以推出$< G', \cdot >$也是群。