第 7 章 群论

第七章中我们介绍了近世代数的一些基本概念，有了这些初步的准备，这一章我们来介绍群这个含有一个代数运算的重要的代数系统.

§1 群的定义

群是含有一种代数运算，这个代数运算一般用符号$\circ$或$\bullet$来表示，有时为了方便也可能直接用普通加法或乘法符号来表示，或者省略运算符号，仅写为ab，所以有时就把代数运算叫做乘法．请大家注意区分它和普通乘法的不同.

定义 1 设G是一个非空集合，在G上的一个二元运算$\circ$，若$\circ$满足结合律，则称G为一个**半群.**

引入半群的目的是为了更方便的介绍群的概念， 下面先介绍几个名词.

定义 2 设G为一个半群，如果存在元素$e_L \in G$， 对于任意的$g \in G$，都有

$$e_L \circ g = g，$$

那么就称e_L为G的一个**左单位元**；如果存在元素$e_R \in G$，对于任意的$g \in G$，都有

$$g \circ e_R = g .$$

那么就称e_R为G的一个**右单位元**；若e既为G的一个左单位元，又为G的一个右单位元，则称e为G的一个**单位元.**

注 半群既可以没有左单位元，又可以没有右单位元或者仅有左单位元或右单位元. 但是，若两者都存在，则一定相等，即为单位元．因为

$$e_L \circ e_R = e_L = e_R = e .$$

定义 3 $(G, \circ)$是含右单位元e的半群，称G中元素g是**右可逆**，如果存在$g' \in G$，使

$$g \circ g' = e，$$

称g'为g的**右逆元**；称G中元素g是**左可逆**，如果存在 $g'' \in G$，使

$$g'' \circ g = e，$$

称g''为g的**左逆元**；称G中元素g是**可逆元**，如果存在$g^{-1} \in G$，使

$$g \circ g^{-1} = g^{-1} \circ g = e,$$

称 g^{-1} 为 g 的**逆元**.

显然，若 $g \in G$， g 既有左逆元，又有右逆元，则两者必定相等，并为 G 中元素 g 得逆元.

有了半群、单位元、逆元的概念，即可引入群的定义.

定义 4 一个有单位元的半群 $(G, \circ)$，叫做一个**群**，如果 G 的每一个元都为可逆元．换言之，一个非空集合 G，给定 G 上的一个二元运算$\circ$，若以下条件满足

（1）任意 $a,b \in G,$ 则 $a \circ b \in G$；

（2）结合律成立：对任意的 $a,b,c \in G$ 有

$$(a \circ b) \circ c = a \circ (b \circ c);$$

（3） G 中存在唯一的单位元 $e \in G$，对任意的 $g \in G$ 都有

$$e \circ g = g \circ e = g;$$

（4） G 中任意元素 g，存在 $g^{-1} \in G$ 使

$$g \circ g^{-1} = g^{-1} \circ g = e.$$

则称 $(G,\circ)$ 为一个**群**.

在群的定义中，（1）是多余的，因为已知$\circ$是集合 G 上的一个二元运算，当然任意两个元素的运算结果仍在 G 中，此处只是强调一下 G 对$\circ$是封闭的.

定义了群之后，来看几个群的例子.

例 1 G 只包含一个元素 g，二元运算定义为 $g \circ g = g$，则 G 对于这个二元运算来说做成一个群.

（1） 结合律满足;

（2）存在单位元 g；

（3）对 G 中元素 g，存在逆元 g.

例 2 全体不等于零的有理数对于普通乘法来说做成一个群．结合律成立．单位元为 1． a 的逆元为 $\dfrac{1}{a}$.

例 3 $n \in Z$ ，模 n 剩余类

$$Z_n = \{[k] \mid k \in Z\} = \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\},$$

二元运算定义为模 n 加法，则 $(Z_n, +)$ 构成一个群.

（1）结合律成立；

（2）单位元为 $\bar{0}$；

（3）$\bar{0}$ 的逆元为 $\bar{0}$，$\bar{1}$ 的逆元为 $\overline{n-1}$，以此类推.

例 4 模 m 的简化剩余系 Z_m^* 对于模 m 乘法运算构成一个群.

证明 (1) 对任意的 $a, b \in Z_m^*$, 都有 $(a, m) = 1,\quad (b, m) = 1,$ 所以

$$(ab, m) = 1,\quad ab \in Z_m^*.$$

（2）对于模 m 乘法，结合律显然成立.

（3）单位元为 1.

（4）对任意的 $a \in Z^*{}_m$，存在唯一的 a^{-1}，使 $a \cdot a^{-1} = 1(\bmod m)$，故 Z_m^* 中每一个元素都有逆元.

以上三个例子中，例 1，例 3 ，例 4 的非空集合元素个数为有限多个，例 2 元素个数为无限多个.

定义 5 假如一个群的元的个数是一个有限整数，这个群叫做**有限群**，否则，这个群叫做**无限群**．一个有限群的元的个数叫做这个**群的阶**．记为 $|G|$.

从群得定义我们知道群满足结合律，而对于交换律，则不一定成立.

定义 6 一个群 $(G, \circ)$，假如对任意的 $a, b \in G$，都有 $a \circ b = b \circ a$. 则这个群叫做**交换群**（也叫 **Abel 群**）.

还有一个重要概念是利用单位元 e 来定义的.

定义 7 若群 G 的一个元 g，能够使得 $g^m = e$ 的最小的正整数 m 叫做 g 的**阶**（或**周期**）. 若这样的 m 不存在，则称 g 的阶为无限.

此处定义的 g 的阶类似于初等数论中定义 g 的指数 $\delta_m(g)$，在前面的介绍中我们知道指数满足如下性质：

对任给的整数 d，如果 $g^d \equiv 1(\bmod m)$，则 $\delta_m(g) \mid d$.

在此处元素的阶也有类似的性质.

定理 1 设 a 的周期为 m，当且仅当 $m\mid n$ 时，$a^n=e$.

证明 设 $m\mid n$，则存在整数 k，使得 $n=mk$. 于是

$$a^n=a^{mk}=(a^m)^k=e^k=e.$$

反之，设 $a^n=e$，但 $m\nmid n$，则 $n=mk+r$，$1\le r<m$. 于是

$$e=a^n=a^{mk+r}=ea^r=a^r,$$

与 m 是 a 的周期矛盾.

实际上，群中元素的阶的定义与模的既约剩余系中元素的指数定义是一致的，所不同的是，在模的既约剩余系中，当时我们并没有提到群的概念. 而在本质上，模的既约剩余系关于剩余类的乘法运算就构成一个有限群，元素的指数即为元素的阶（群中）.

最后我们来证明群的一个等价的定义.

定义 4′ 设 $(G,\circ)$ 是一个半群，如果对于 G 中任意 $a,b,$ 方程

$$a\circ x=b,\quad y\circ a=b$$

在 G 中都有解，则 G 为一个群.

证明 （1）先证 G 中有单位元 e.

令 $y\circ b=b$ 的一个解为 e_L，则 $e_L\circ b=b$. 对任意的 $a\in G,$ 因为 $b\circ x=a$ 有解 c，于是，

$$e_L\circ a=e_L\circ(b\circ c)=(e_L\circ b)\circ c=b\circ c=a,$$

e_L 为 G 的左单位元. 同样可以证明 $b\circ y=b$ 的解 e_R 为 G 的右单位元. 所以 $e_L=e_R=e$ 为 G 的单位元.

（2） 下证对任意的 $a\in G$，逆元 a^{-1} 存在.

显然 $y\circ a=e$ 的解 a' 为 a 的左逆元，而 $a\circ y=e$ 的解 a'' 为 a 的右逆元，

$$a'=a'e=a'aa''=ea''=a''.$$

故两者相等为 a 的逆元，所以 G 为一个群.

从群的等价定义 4′ 可以知道，在群中，一元一次方程有解且解唯一.

例 5 设 a,b 是群 G 的元素，a 的阶为 p，b 的阶为 q，（$p<q$ 为不同的素数)，且 $ab=ba$，则 ab 的阶为 pq.

证明　设ab的阶为r，由题设知

$$(ab)^{pq}=a^{pq}b^{pq}=e,$$

故$r\mid pq$．所以　$r=1,\ p,\ q,$ 或 $p\,q$中的一个．$r=1$显然是不可能的，

若$r=p$，则

$$(ab)^{p}=e=a^{p}b^{p}=b^{p},$$

因为$p<q$，所以与b的周期为q矛盾．

若$r=q$，则

$$(ab)^{q}=e=a^{q}b^{q}=a^{q}$$

从而$p\mid q$，此与q为素数矛盾．所以$r=pq$．

§2 循环群

在上一节中给出了群的定义，这一节中，我们介绍一种很重要的群—循环群，并重点研究循环群的结构．研究群的结构是群论的主要目的．到目前为止，仅有少数几类群的结构完全被大家所了解．而对于多数群的结构，目前还有待继续研究．

值得说明的是，本节中我们将代数运算通称为乘法．

定义 1 若一个群G的每一个元都是某一固定元a的乘方，$G=\{a^n\mid n\in Z\}$，则称G为**循环群**，我们也说，G是由元a所生成的，记为$G=(a)$，a叫做G的一个**生成元．**

我们先举两个循环群的例子．

例 1 $G=(Z,+)$是一个循环群，因为$G=(1)$．

例 2 G包含模n的n个剩余类,代数运算定义为模n加法.剩余类的每一个元可以写成$\bar{i}$，$0\le i\le n-1$．显然，$\bar{1}$是G的一个生成元．

这两个例子具有一定的代表性，例 1 中的群$(Z,+)$通常叫做整数加群，生成元1是无限阶的．例 2 中的群$(Z_n,+)$通常叫做模n的剩余类加群，生成元$\bar{1}$的阶为n．

例 3 前面我们证明了模m的简化剩余系Z_m^*构成一个群，当模m有原根g时，则g为Z_m^*

的生成元，且任给 i ，满足 $(i,\phi(m))=1$ ，则 g^{i} 亦为 Z_{m}^{*} 的生成元，并由此可看出， Z_{m}^{*} 的生成元共有 $\phi(\phi(m))$ 个.

通过下列定理可以知道，所有的循环群只有两类．而例 1 与例 2 中两个具体的群即为两类循环群的代表.

定理 1　假定 G 是一个由元 a 所生成的循环群，当 a 的阶无限时，那么 G 与整数加群同构；若 a 的阶是一个有限整数 n ，那么 G 与模 n 的剩余类加群同构.

证明 令

$$\phi : a^{k} \mapsto k$$

首先证明 ϕ 为 G 到 $(Z,+)$ 的映射：即证明

$$a^{h}=a^{k} \Rightarrow h=k\ .$$

反证法：若

$$a^{h}=a^{k}$$

而 $h \neq k$ ，假定 $h>k$ ，则得到

$$a^{h-k}=e\ ,$$

与 a 的阶无限矛盾．所以 ϕ 为 G 与整数加群 $(Z,+)$ 间的映射.

又因为

$$a^{h} \neq a^{k} \Rightarrow h \neq k\ ,$$

所以 ϕ 为单射．显然 ϕ 为满射，所以 ϕ 为一一映射.

又因为

$$\phi(a^{h}a^{k})=\phi(a^{h+k})=h+k=\phi(a^{h})\phi(a^{k})\ .$$

因此 ϕ 为同构映射．故 G 与整数加群同构.

（2） a 的阶是一个有限整数 n ，令

$$\varphi : a^{h} \mapsto \overline{h}$$

下证 φ 为 G 到 $(Z_{n},+)$ 的群同构映射.

由第 1 节定理及初等数论中剩余类的性质知：

$$a^h = a^k \Leftrightarrow a^{h-k} = e \Leftrightarrow n|h-k \Leftrightarrow \bar{h} = \bar{k}\,,$$

所以φ映射并且为单射．显然φ为满射，所以φ为一一映射．

又因为

$$\varphi(a^h a^k) = \varphi(a^{h+k}) = \overline{h+k} = \bar{h} + \bar{k}\ .$$

所以φ为G与模n的剩余类加群的同构映射．得证．

至此，我们对循环群的存在及构造问题就完全掌握了．但是一般的群构造极其复杂，很难得到象循环群类这样的完美结果．

§3 变换群、置换群

在前面介绍的群的例子中，集合上的二元运算都是一些具体的普通加法或乘法运算，本节讨论变换群，它的元素不再是普通的数，二元运算也不再是我们通常的四则运算．变换群虽然是一类具体的群，但从同构的概念上，任何抽象群都可以在这类群中找到同构的群．因此通过对变换群的研究，有助于帮助了解抽象群．

首先我们再回顾一下以前介绍过的集合A上的变换．

定义 1 A是给定的集合，我们称A到A的一个映射

$$\phi : A \to A$$

为集合A上的一个变换．A到A的一个一一映射称为A上的一个一一变换．A到A的恒等映射称为A上的恒等变换．

考虑集合A上的所有变换的全体，记为集合S，规定变换的合成$\circ$为S上的代数运算，显然恒等变换为S的单位元，由第 6 章的基本概念知$\circ$满足结合律．因此$(S,\circ)$是一个含有单位元的半群．通常$(S,\circ)$并不能构成一个群．但S的子集G对于上述运算却有可能构成一个群．下面定理说明了$(G,\circ)$构成群的一个必要条件．

定理 1 假如G是集合A的若干个变换所作成的集合，并且包含恒等变换ε，若是对于变换的合成来说G作成一个群，那么G只包含A的一一变换．

证明 若G关于变换的合成构成群．则对于任意的G的元素ϕ，一定存在ϕ^{-1}，使

$$\phi\phi^{-1} = \phi^{-1}\phi = \varepsilon\ .$$

下证ϕ为A 上的一一变换．任给$a \in A$，

$$\phi\phi^{-1}(a)=\phi(\phi^{-1}(a))=\varepsilon(a)=a\text{，}$$

所以ϕ为满射．若$\phi(a)=\phi(b)$，则

$$a=\phi^{-1}\phi(a)=\phi^{-1}(\phi(a))=\phi^{-1}(\phi(b))=\phi^{-1}\phi(b)=b\,.$$

所以ϕ为单射．定理得证．

定义 2 一个集合A的若干个一一变换对于变换的合成作成的群，叫做A的一个**变换群．**

我们给出了变换群的定义，但是是否存在变换群，即能否找到若干个一一变换作成变换群呢？我们来看如下定理．

定理 2 一个集合A的所有一一变换作成一个变换群G．

证明 （1）首先证明集合G对合成运算封闭．若ϕ_1,ϕ_2为一一变换，则$\phi_1\phi_2$也是A上的一一变换．

先证$\phi_1\phi_2$为满射：对任意$a\in A$，因为ϕ_1,ϕ_2为一一变换，所以存在$a',a''\in A$，使得

$$\phi_2(a')=a\text{，}\ \phi_1(a'')=a'\text{，}$$

故存在$a''\in A$，使$\phi_1\phi_2(a'')=a$．

再证$\phi_1\phi_2$为单射：若$a\neq b$，则

$$\phi_2(a)\neq\phi_2(b)\text{，}\ \phi_1[\phi_2(a)]\neq\phi_1[\phi_2(b)]\,.$$

因此$\phi_1\phi_2$也是A上的一一变换．

2） 结合律显然成立．

3） 恒同变换ε为一一变换，即为单位元．

4）若是ϕ一个一一变换，那么有一个A上变换ϕ'，对任意$a\in A$，定义

$$\phi':\phi(a)\mapsto a$$

容易证明ϕ'满足

$$\phi'\phi=\phi\phi'=\varepsilon\,.$$

所以$\phi'=\phi^{-1}$．定理得证．

在证明任意抽象群同构于一个变换群之前，首先需要证明以下结论．

定理 3 $(G,\circ)$ 是一个群，G' 是定义了一个二元运算$\bullet$的非空集合，如果存在一个G 到 G' 的同态满射，对任意的$a, b\in G$ 有

$$\phi(a\circ b)=\phi(a)\bullet\phi(b),$$

则$(G',\bullet)$ 也是一个群.

证明 因为ϕ是G 到G' 的同态满射，G 的二元运算$\circ$适合结合律，由第 6 章的定理知，G' 的二元运算$\bullet$也适合结合律.

若e是G 的单位元，

$$\phi(e)=e',$$

下证e'是G'的单位元，任意的$x'\in G'$，存在$x\in G$，使得

$$\phi(x)=x'$$

故

$$\phi(e\circ x)=\phi(x\circ e)=\phi(x)\Rightarrow\phi(e)\bullet\phi(x)=\phi(x)\bullet\phi(e)=\phi(x).$$

从而

$$e'\bullet x'=x'\bullet e'=x',$$

即e'是G'的单位元.

任取$a'\in G'$，存在$a\in G$,

$$\phi(a)=a'$$

同理

$$\phi(a\circ a^{-1})=\phi(a^{-1}\circ a)=\phi(e)\Rightarrow\phi(a)\bullet\phi(a^{-1})=\phi(a^{-1})\bullet\phi(a)=e'.$$

可知$\phi(a^{-1})\in G'$为a'在G'中的逆元．从而$(G',\bullet)$也是一个群.

下面定理在群的理论上是一个非常重要的结果. 它使任何一个抽象的群跟一个具体的变换群联系在一起.

定理 4 （Cayley 定理）任意群都与一个变换群同构.

证明 对于任意的$g\in G$，作集合G 的下述变换

$$\tau_g: x\mapsto gx$$

则 τ_g 是 G 的一一变换.

事实上，因

$$gx = b$$

在 G 中有解，故对任意 $b \in G$, 存在 $x \in G$ 使

$$\tau_g(x) = b ,$$

即 τ_g 是 G 到 G 的一个满射．又因为

$$x_1 \neq x_2 \Rightarrow gx_1 \neq gx_2 ,$$

故 τ_g 是 G 到 G 的一个单射．从而 τ_g 是 G 到 G 的一个一一变换．由于

$$\tau_g \bullet \tau_h(x) = \tau_g(\tau_h(x)) = \tau_g(hx) = g(hx) = (gh)x = \tau_{gh}(x),$$

故对任意的 $g, h \in G$ 都有

$$\tau_g \bullet \tau_h = \tau_{gh},$$

即 $G' = \{\tau_g \mid g \in G\}$ 关于映射的合成是封闭的.

令 $\phi: g \mapsto \tau_g$．显然 ϕ 为 G 到 G' 的满射，

设 $g \neq h$，则存在 $x \in G$,

$$gx \neq hx \Rightarrow \tau_g(x) \neq \tau_h(x) ,$$

即 $\tau_g \neq \tau_h$，所以 ϕ 是 G 到 G' 的一一映射．又因为

$$\phi(gh) = \tau_{gh} = \tau_g \bullet \tau_h = \phi(g) \bullet \phi(h) ,$$

由定理 3 知 G' 是一个群，且 $G \cong G'$．即 G 同构于集合 G 上的一个变换群.

从定理 4 知，从同构的角度，任意抽象群对应一个变换群．也就是说，如果对于抽象群的研究也可以转换成变换群研究．由此即可看出变换群在群论中的特殊地位，但往往变换群的结构并不比抽象群更容易.

下面我们讨论一类简单的变换群，即有限集合 A 上的一一变换群．一般一个有限集合的一个一一变换叫做一个**置换**．所以我们得到置换群的定义.

定义 3 一个有限集合的若干个置换作成的群叫做一个**置换群**.

置换群是变换群的特例，在高等代数中都介绍过，在此我们将一些主要结论简单回忆一下．

我们知道，n 个元的置换有 $n!$ 个，这 $n!$ 个 n 次置换关于置换合成作成的群叫做 n 次**对称群**，用 S_n 表示．故 n 次对称群 S_n 的阶为 $n!$．

现在我们规定一个新符号．

定义 4 S_n 的把 a_{i_1} 变到 a_{i_2}， a_{i_2} 变到 $a_{i_3},\cdots,a_{i_k}$ 变到 a_{i_1} ，而使其余元（假如还有的话）不变的置换，叫做一个 **k －循环置换**．我们用符号 $\left(i_1 i_2 \cdots i_k\right)$ 来表示．特别地，当 $k=2$ 时，称 $\left(i_1 i_2\right)$ 为一个对换．

每一个 n 个元的置换 π 都可以写成若干个互不相交的循环置换的乘积，而每一个循环置换可以表示成对换的乘积．虽然每个置换表示成对换的乘积时，表示法不唯一，但奇偶性不变．通常将表示成偶数个对换的置换为**偶置换**，表示成奇数个对换的置换为**奇置换**．$n!$ 个 n 次置换中奇偶置换各占一半．所有的偶置换构成一个置换群，称为 n 次交代群．

最后我们描述在有限群下的 Cayley 定理．

定理 5 每一个有限群都与一个置换群同构．

定理 5 说明了，每一个有限群都可以在置换群中找到例子．置换群是一种比较容易计算的例子．因此利用定理 5 寻找有限群的例子是一种较好的方法．

例 1 设 $G=(a)$ 是 n 阶循环群，则 G 与置换群 G' 同构，求 G'．

解 由于 G 是 n 阶循环群，故 G' 也是 n 阶循环群．为了找到 G'，只要找到 G' 的生成元即可．

$G \cong G'$，故 G 的生成元的象即为 a 的象．由 Cayley 定理的证明知

$$a \mapsto f_n： x \mapsto ax$$

$$f_n=\begin{pmatrix} e & a & a^2 & \cdots & a^{n-1} \\ a & a^2 & a^3 & \cdots & e \end{pmatrix}=\left(1 \quad 2 \quad \cdots \quad n\right),$$

即 $G'=\left(\left(1 \quad 2 \quad \cdots \quad n\right)\right)$．

例 2 证明：S_4 有生成元$\{(1 \quad 2),(1 \quad 3),(1 \quad 4)\}$．

证明 因为任一置换可表示成对换的乘积．S_4 中不同的对换为

$$\{(1 \quad 2),(1 \quad 3),(1 \quad 4),(2 \quad 3),(2 \quad 4),(3 \quad 4)\}$$

只需证明由 $(1 \quad 2),(1 \quad 3),(1 \quad 4)$ 可生成 $(2 \quad 3),(2 \quad 4),(3 \quad 4)$ 即可．

$$(1\quad 2)(1\quad 3)=(1\quad 3\quad 2)\,,\qquad (1\quad 4)(1\quad 3)=(1\quad 3\quad 4)\,,$$

$$(1\quad 2)(1\quad 4)=(1\quad 4\quad 2)\,,\qquad (1\quad 3)(1\quad 4)=(1\quad 4\quad 3)\,,$$

$$(1\quad 3)(1\quad 2)=(1\quad 2\quad 3)\,,\qquad (1\quad 4)(1\quad 2)=(1\quad 2\quad 4)\,,$$

$$(1\quad 2)(1\quad 3\quad 2)(1\quad 3\quad 4)=(1\quad 2)(1\quad 2)(3\quad 4)=(3\quad 4)\,,$$

$$(1\quad 4)(1\quad 4\quad 2)(1\quad 4\quad 3)=(1\quad 4)(1\quad 4)(2\quad 3)=(2\quad 3)\,,$$

$$(1\quad 3)(1\quad 2\quad 3)(1\quad 2\quad 4)=(1\quad 3)(1\quad 3)(2\quad 4)=(2\quad 4)\,,$$

所以由$S=\{(1\quad 2),(1\quad 3),(1\quad 4)\}$可生成$S_4$.

例 3 证明：S_3不是交换群.

证明 S_3有 6 个元．这 6 个元可以写成

$$I\,,\ (12)\,,\ (13)\,,\ (23)\,,\ (123)\,,\ (132)$$

因为

$$(12)(23)=(123)\neq(23)(12)=(132)$$

所以S_3不是交换群.

§4 子群 子群的陪集

集合论中我们学了子集的概念，在群论中，集合G的非空子集合H对于G上的二元运算是否也可构成一个群．我们规定

定义 1 群$(G,\circ)$非空子集H，若对于G的运算作成群，则说H是G的一个**子群**．我们用符号$H\le G$表示.

给定一个任意群G，则G至少有两个子群G和$\{e\}$，称之为平凡子群；其它的子群，称为G的真子群.

例 1 设

$$G=\{x \mid x^n=1, x\in C^*, n\in Z\},$$

C^*表示除去零元素以外的复数域，对于某个固定的n，

$$H=\{x \mid x^n=1, x\in C^*\}$$

构成G的子群.

因为任取$x_1,x_2\in H$，$(x_1x_2)^n=1$，故$x_1x_2\in H$．G中的元素满足结合律，所以H中的元素也满足结合律．$1^n=1,$　所以H中有单位元.

$$x^n=1\Rightarrow (x^{-1})^n=(x^n)^{-1}=1\Rightarrow x^{-1}\in H,$$

即H是一个子群.

例 2 模4的剩余类加群$(Z_4,+)=\{\bar{0},\bar{1},\bar{2},\bar{3}\}$，$Z_4$和$\{\bar{0}\}$为其平凡子群．$H=\{\bar{0},\bar{2}\}$为其真子群.

子群的定义给出了子群的判定方法，以下介绍一个更简单的判定方法，而不需要每次验证子集合H是否符合群的所有条件.

定理 1 H为群G的非空子集，H作成G的一个子群的充分必要条件是

⑴ $a,b\in H\Rightarrow ab\in H$；

⑵ $a\in H\Rightarrow a^{-1}\in H$.

证明 充分性：因为由⑴可知H是闭的．结合律在G中成立，在H中也成立．又因为H中至少有一个元a，由⑵知H中含有a^{-1}，所以由⑴得

$$aa^{-1}=e\in H.$$

故H中存在单位元．因此H构成一个群.

反过来，若H作成一个群，则⑴显然成立．下证（2）成立．因为H是一个群，H有单位元e'．任意的$a\in H$，

$$e'a=ae'=a.$$

由于$a,e'\in G$，所以e'是

$$ya=a$$

在G的解．但这个方程在G里只有一个解，就是G的单位元e，所以$e'=e\in H$．因为H是一个群，方程

$$ya=e$$

在 H 中有解 a'， a' 也是这个方程在 G 里的解，而方程在 G 里有且只有一个解 a^{-1}，所以，

$a' = a^{-1} \in H$． 证毕．

推论 1 H 为群 G 的非空子集， H 作成 G 的一个子群的充分必要条件是

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

有了子群的概念，我们讨论循环群的子群的结构．

定理 2 循环群的子群仍为循环群。

证明 若 H 只有唯一元，则 H 当然是循环群．若 $H \neq \{e\}$，由于 H 非空，故存在 $a^k \in H$，$k > 0$，从而 H 含有 a 的某些幂．令

$$A = \{k \mid k \geq 1, k \in Z, a^k \in H\},$$

则 A 不空，从而有最小者，设为 r．于是 $H = (a^r)$．否则任取 $a^l \in H$，若 $r \nmid l$，则 $l = qr + s$，$0 < s < r$． 由

$$a^l = (a^r)^q a^s$$

推出 $a^s \in H$，$s \in A$，这与 r 是 A 中最小者矛盾．从而对任何 $a^l \in H$，有 $r \mid l$，即 $H = (a^r)$．

定理 3 若 $G = (a)$ 为 n 阶循环群，任给 $a^i \in G, 0 \leq i \leq n-1$，循环子群 $H = (a^i)$ 的阶为 $\dfrac{n}{(n,i)}$．

例 3 若 $G = (a)$ 为 n 阶循环群，生成元的个数为 $\phi(n)$．

例 4 设 $H_i, i \in I$（一个有限或无限的指标集），都是群 G 的子群，则 $H = \bigcap_{i \in I} H_i$ 也是群 G 的子群．

证明 因为对任意 $i \in I$，有 $e \in H_i$，故 H 不会是空集．任取 $a, b \in H$，则对任意 $i \in I$，有 $a, b \in H_i$．因为每个 H_i 是子群，故 ab, a^{-1} 都在 H_i 中，即 $ab, a^{-1} \in H$．故 H 是一个子群．

任取群 G 的一个子集合 M，设 $H_i, i \in I$ 是群 G 中含有 M 的所有子群，则我们可证明 $H = \bigcap_{i \in I} H_i$ 是含 M 的最小子群．我们把这样得到的 H 叫做 M 的**生成子群**，用符号 $< M >$ 来表示．假如 M 是只含一个元的子集，那么， $H =< M >$ 是一个循环子群．

下面我们引入陪集的概念.

定义 2 若 H 是 G 的子群，任意 $a\in G$，称

$$aH=\{ah\mid h\in H\}$$

为子群 H 的一个**左陪集**；同理，称

$$Ha=\{ha\mid h\in H\}$$

为子群 H 的一个**右陪集.**

例 5 $(Z,+)$ 为整数加群，$H=\{nk\mid k\in Z\}$ 为它的一个子群，则 $a\in Z$

$$aH=\{a+b\mid b\in H\}=\{a+nk\mid k\in Z\},$$

为其左陪集，构成模 n 剩余类元 $[a]$.

定理 4 设 H 为 G 的子群，任给 H 的左陪集 aH,bH，则要么 $aH=bH$，要么 $aH\cap bH=\phi$.

证明 若存在 $x\in aH\cap bH$, 则存在 $h_1,h_2\in H$，使

$$x=ah_1=bh_2.$$

则任意 $ah\in aH$，有

$$ah=ah_1h_1^{-1}h=bh_2h_1^{-1}h=bh'\in bH,$$

故 $aH\subseteq bH$. 同理可证 $aH\supseteq bH$，所以 $aH=bH$. 定理得证.

例6 模 6 的剩余类加群

$$(Z_6,+)=\{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4},\overline{5}\},$$

它的两个子群为

$$H_2=\{\overline{0},\overline{2},\overline{4}\},\quad H_3=\{\overline{0},\overline{3}\}.$$

H_2 的陪集：

$$\overline{0}H_2=\overline{2}H_2=\overline{4}H_2=H_2=\{\overline{0},\overline{2},\overline{4}\},$$

$$\overline{1}H_2=\overline{3}H_2=\overline{5}H_2=\{\overline{1},\overline{3},\overline{5}\}.$$

H_3 的陪集：

$$\overline{0}H_3=\overline{3}H_3=\{\overline{0},\overline{3}\},$$

$$\overline{1}H_3=\overline{4}H_3=\{\overline{1},\overline{4}\},$$

$$\overline{2}H_3=\overline{5}H_3=\{\overline{2},\overline{5}\}.$$

定理 5 H 是 G 的子群，则 G 关于子群 H 的左陪集和右陪集的个数一定相等.

证明 设左陪集作成的集合为 S_L，右陪集作成的集合为 S_R，作 S_R 到 S_L 的映射

$$\phi: Ha \mapsto a^{-1}H$$

这是一个 S_R 到 S_L 的一一映射．因为

⑴ ϕ 是映射，即相同元素的象相同.

$$Ha=Hb \Rightarrow ab^{-1}\in H \Rightarrow (ab^{-1})^{-1}=ba^{-1}\in H \Rightarrow a^{-1}H=b^{-1}H .$$

⑵ S_L 的任意元 aH 是 S_R 的元 Ha^{-1} 的象，所以 ϕ 是一个满射.

(3)　由于

$$Ha\neq Hb \Rightarrow ab^{-1}\notin H \Rightarrow (ab^{-1})^{-1}=ba^{-1}\notin H \Rightarrow a^{-1}H\neq b^{-1}H,$$

所以 ϕ 是一个单射.

从而 ϕ 为 S_R 到 S_L 的一一映射存在．定理得证.

由定理 4 子群 G 可以划分成两两不同的左陪集的并，这就给出了群 G 的一个划分．容易证明该划分确定了 G 上的如下等价关系

$$\forall a,b\in G,\quad a \backsim b \Leftrightarrow a^{-1}b\in H .$$

定义 3　一个群 G 的一个子群 H 的右陪集（或左陪集）的个数叫做 H 在 G 里的**指数**，记为 $[G:H]$．其中 $[G:1]$ 表示 G 的阶.

定理 6（Lagrange 定理） 若 H 是一个有限群 G 的子群，则

$$[G:1]=[G:H][H:1\}$$

证明 G 的元被分成 $[G:H]$ 个互不相交的左陪集，并且每个左陪集的个数等于 $[H:1\}$．所以结论成立.

定理 7 一个有限群 G 的任一个元 a 的阶 n 都整除 G 的阶.

证明 a 生成一个阶是 n 的子群，由以上定理，n 整除 G 的阶．证毕．

例 7 设 G 是 n 阶循环群，且 $d \mid n$，则存在且仅存在一个阶数为 d 的子群．

证明 设 $G=(a)$, 因为 $d \mid n$，可令 $n=dr$，则 a^r 的周期为 d．这是因为

$$(a^r)^d = e,$$

故 a^r 的周期至多为 d．假定 a^r 的周期 $k<d$，则

$$a^{rk}=e,$$

而 $rk<rd=n,$ 与 a 的周期为 n 矛盾．故 a^r 的周期为 d，即 (a^r) 是 G 的阶数 d 的子群．

假定 H 是 G 的任一阶数 d 的子群，由于循环群的子群仍是循环群，故可设 $H=(a^t)$，若 $t=r$，则 $H=(a^r)$．若 $t\neq r$ 则

$$t=rq+s, 0\le s<r \Rightarrow td=trq+sd \Rightarrow a^{td}=a^{sd}=e.$$

而 $sd<rd=n \Rightarrow s=0,$ 即 $t=rq$．从而

$$a^t=(a^r)^q \in (a^r) \Rightarrow H \subseteq (a^r).$$

但 H 含有 d 个元，(a^r) 也含有 d 个元，故 $H=(a^r)$．即 G 只有一个阶数为 d 的子群 (a^r)．

§5 同态基本定理

上一节我们介绍了左右陪集，对于 G 的任意子群 H，左陪集 aH 未必等于右陪集 Ha，但是有一类 G 的特殊子群，其左陪集等于右陪集，我们给这类子群起一个特殊名字．

定义 1 设 H 是 G 的一个子群，如果任意 $a\in G, aH=Ha$，那么就说 H 是 G 的一个**不变子群（或正规子群）.**

例1 一个任意群 G 的子群 G 和 e 总是不变子群，因为对于任意 G 的元 a 来说，

$$Ga=aG=G$$
$$ea=ae=a$$

例 2 设 $G = S_3, H = \{(1), (123), (132)\}$. 这时

$$(1)H = H = H(1),$$

$$(12)H = \{(12),(23),(13)\},$$

$$H(12) = \{(12),(23),(13)\},$$

即对任意 $a \in G$，都有 $aH = Ha$，故 H 是 G 的一个不变子群.

判断 G 的一个子群 H 是不变子群的方法，除了定义外，还有以下几种方法.

定理 1 设 H 是 G 的子群，则下面四个条件等价

（1） H 是 G 的不变子群;

（2） $aHa^{-1} = H, \forall a \in G$；

（3） $aHa^{-1} \subseteq H, \forall a \in G$；

（4） $aha^{-1} \in H, \forall a \in G, \forall h \in H$.

证明 我们按照下面的证明途径：$(1) \Rightarrow (2) \Rightarrow (3) \Rightarrow (4) \Rightarrow (1)$，从而证明四个条件等价.

$(1) \Rightarrow (2)$ 因 H 是不变子群，故对于任意 $a \in G$，有 $aH = Ha$，于是

$$aHa^{-1} = (aH)a^{-1} = (Ha)a^{-1} = H(aa^{-1}) = He = H .$$

即 (2) 成立.

$(2) \Rightarrow (3)$ 任意 $a \in G, aHa^{-1} = H \Rightarrow aHa^{-1} \subseteq H$.

$(3) \Rightarrow (4)$ 由于 $aHa^{-1} \subseteq H$，故任意的 $a \in G,\ \ h \in H,$ 有 $aha^{-1} \in H$.

$(4) \Rightarrow (1)$ 因为 $aHa^{-1} \in H$，故对任意 h，存在 $h_1 \in H$ 使

$$aha^{-1} = h_1 \Rightarrow ah = h_1 a \Rightarrow aH \subseteq Ha.$$

另一方面，任取 $ha \in Ha$，因 $a^{-1}ha \in H,$ 故存在 $h_1 \in H$，使

$$a^{-1}ha = h_1 \Rightarrow ha = ah_1 \Rightarrow ha \in aH \Rightarrow Ha \subseteq aH,$$

即对任意的 $a \in G$ 有

$$aH = Ha,$$

从而 H 是 G 的不变子群.

若 H 是 G 的不变子群，$G/H = \{aH \mid a \in G\}$ 表示 G 关于 H 的所有陪集的集合，我们定义 G/H 上得一个二元运算$\circ$.

$$aH \circ bH = (a \cdot b)H \tag{1}$$

下证$\circ$为二元运算：若

$$(aH, bH) = (a'H, b'H),$$

则存在 $h_1, h_2, h_3, h_4 \in H$ 使得

$$ah_1 = a'h_2, h_3b = h_4b'.$$

所以

$$(a')^{-1}ab(b')^{-1} = h_2(h_1)^{-1}h_3(h_4)^{-1} \in H,$$

由不变子群的性质知：存在 $h \in H, ab = a'hb' = a'b'(h')^{-1}$，所以 $abH = a'b'H$，得证.

例 3 整数加群 $(Z, +)$，$H = \{nk \mid k \in Z\}$ 为不变子群，H 的陪集

$$aH = \{a + nk \mid k \in Z\} = [a]$$

作成模 n 剩余类加群.

例 4 设 H 是 G 的一个子群，则 H 的任意两个左陪集的乘积仍是一个左陪集当且仅当 H 是 G 的一个不变子群.

证明　充分性显然，下证必要性．我们先证

$$aHbH = (ab)H.$$

由题设，$aHbH$ 是一个左陪集，设为 cH．由

$$ab = ae \circ be \in aH \circ bH,$$

故

$$ab \in cH \Rightarrow abH = cH.$$

任取 $h \in H$，则任意的 $a \in G,$

$$aha^{-1}h \in aH \circ a^{-1}H = (aa^{-1})H = H \Rightarrow aha^{-1} \in H, \forall a \in G,$$

于是 H 是 G 的不变子群.

我们得到下面重要定理.

定理 2 一个不变子群的陪集对于（1）定义的乘法作成一个群.

证明 设 H 是群 G 的不变子群，对任意 $x, y, z \in G$，我们有

I. $(xHyH)zH = [(xy)H]zH = (xyz)H$

$xH(yHzH) = xH[(yz)H] = (xyz)H$.

II. $eHxH = (ex)H = xH$.

III. $x^{-1}HxH = (x^{-1}x)H = eH$.

这正是构成群的条件.

定义 2 一个群的不变子群的陪集对于（1）所作成的群叫做一个**商群**，记作 G/H .

例 5 设 H 是 G 的一个子群，$[G:H]=2$，则 H 是 G 的不变子群.

证明 因为任取 $a \in G$，则 $aH = Ha$. 若 $a \notin H,$ 则 aH, H 是 G 的两个不同的左陪集，由题设 $[G:H]=2$，故 $G = H \cup aH$. 同理有 $G = H \cup Ha$，即

$$H \cap aH = \phi = H \cap Ha ,$$

故

$$aH = G \setminus H = Ha ,$$

即对于任意 $a \in G,$ 均有 $aH = Ha$，H 是 G 的不变子群.

例 6 设 A, B 是 G 的子群，且 A 是不变子群，则 AB 是 G 的子群.

证明 因 A 是不变子群，对任意 $x \in G,$ 有 $xA = Ax$；从而对任意 $a \in A,$ 存在 $a' \in A$，使 $xa = a'x$，于是任取 $ab, a_1b_1 \in AB,$ 有

$$(ab)\cdot(a_1b_1) = a(ba_1)b_1 = a(a_1'b)b_1 = (aa_1')(bb_1) \in AB .$$

又

$$(ab)^{-1} = b^{-1}a^{-1} = a''b^{-1} \in AB ,$$

即 AB 是 G 的一个子群.

我们知道，同态映射是研究群的一个重要工具，不变子群，商群与同态映射之间也存在着重要的联系.

定理 3 一个群G同它的每一个商群G/H同态.

证明 作一个映射

$$\phi : a \mapsto aH，(a \in G)，$$

这显然是G到G/N的一个满射．且对任意的$a, b \in G$，

$$ab \mapsto abH = (aH)(bH)，$$

所以它是一个同态满射．证毕.

在某种意义下，此定理的逆定理也成立．为此先给出定义.

定义 3 ϕ是群G到群G'的同态满射，G'的单位元e'在ϕ的逆象为G的子集，称为同态满射ϕ的核，记作$Ker\phi$.

定理 4 若ϕ是群G到群G'的同态满射，那么$Ker\phi$是G的不变子群.

证明 令$Ker\phi = K$．则对任意$a,b \in K$，有

$$a \mapsto e', \quad b \mapsto e'.$$

因此

$$ab^{-1} \mapsto e'e'^{-1} = e'，$$

即K是一个群．对任意的$a \in G, k \in K$

$$a \mapsto a', k \mapsto e'，$$

有

$$aka^{-1} \mapsto a'e'a'^{-1} = e'$$

这就是说，对于任意$a \in G, k \in K \Rightarrow aka^{-1} \in K$，$K$是$G$的不变子群.

定理 5 若ϕ是群G到群G'的同态满射，则

$$G/Ker\phi \cong G'.$$

证明 作一个映射：

$$\varphi : aK \mapsto a' = \phi(a)，(a \in G)，$$

则这是一个G/K到G的同构映射.

1) $aK=bK\Rightarrow ab^{-1}\in K\Rightarrow b^{-1}a\in K\Rightarrow b'^{-1}a'=e'\Rightarrow a'=b'$，说明$\varphi$映射下$G/K$的元素有唯一确定的象.

2) 给定G'的一个任意元a'，在G里至少有一个元a满足$\phi(a)=a'$，由φ的定义，对给定的G'的一个任意元a'，aK为其在G/K的原象．所以φ是G/K到G的满射.

3) $aK\neq bK\Rightarrow b^{-1}a\notin K\Rightarrow b'^{-1}a'\neq e'\Rightarrow a'\neq b'$，所以$\varphi$是$G/K$到$G$的单射.

4) 在φ之下，

$$\varphi(aK\circ bK)=\varphi(abK)=\phi(a)\phi(b)=\varphi(aK)\cdot\varphi(bK),$$

所以φ是G/K到G的同态映射．因而

$$G/Ker\phi\cong G.$$

前一个定理只说与它的商群同态，其商群的性质并不一定与G相同，而这个定理中，我们可找到一个商群与之同构，即具有相同性质．这体现了不变子群与商群的重要性.

由定理 3 和定理 5 我们可以得到下面这个重要定理.

定理 6 （**同态基本定理**）设G是一个群，则G的任意商群都是G的同态象．反之，若G'是G的同态象$G'=f(G)$，则$G'\cong G/\ker f$.

最后我们引入同态满射的一个性质，读者可以自己证明.

定理 7 若ϕ是群G到群G'的同态满射，那么在这个映射下

（1）子群H的象H'是G'的一个子群；

（2）含有$\ker\phi$的不变子群N的象N'是G'的一个不变子群；

（3）G'的一个子群H'的逆象H是G的一个含$\ker\phi$的子群；

（4）G'的一个不变子群N'的逆象N是G的一个含有$\ker\phi$的不变子群.

由上面定理我们可以看到在同态映射意义下，含有$\ker\phi$的不变子群是一一对应的.

例 1 设f是G到G'的满同态，H'是G'的不变子群，

$$H = f^{-1}(H') = \{a \mid a \in G,\ f(a) \in H'\},$$

则H是G的不变子群，且$G/H \cong G'/H'$.

证明 由同态基本定理，

$$\phi: \ G' \sim G'/H',$$

ϕ是自然同态，又因为

$$f: G \sim G',$$

故

$$\varphi: G \sim G' \sim G'/H'$$

是G到G'/H'的满同态．若能证明$\ker\varphi = H$，则由同态基本定理就可推出所要结论．对任意的$a \in G$

$$\varphi(a) = (\phi \circ f)(a) = \phi(f(a)) = f(a)H',$$

设$a \in f^{-1}(H')$，则

$$f(a) \in H' \Rightarrow f(a)H' = H' \Rightarrow \varphi(a) = H',$$

即$a \in \ker\varphi$，亦即

$$f^{-1}(H') \subseteq \ker\varphi.$$

反之，设$a \in \ker\varphi$，则

$$\varphi(a) = f(a)H' = H' \Rightarrow f(a) \in H' \Rightarrow a \in f^{-1}(H'),$$

即

$$f^{-1}(H') \supseteq \ker\varphi,$$

从而$\ker\varphi = H$为G的不变子群．由同态基本定理得证$G/H \cong G'/H'$.

例 2 设G, G'分别是阶数m, n的循环群，证明：当且仅当$n \mid m$时，$G \sim G'$.

证明 设f是G到G'的同态映射，由同态基本定理，

$$G' \cong G/\ker f\ .$$

由于G'的阶数为n,故$G/\ker f$的阶数也是n，即G含有子群$\ker f$满足

$$[G:\ker f]=n\ ,$$

由

$$[G：1]=[G：\ker f][\ker f：1],$$

知$n\,|\,m$.

反之，设$n\,|\,m, G=(a), G'=(b)$, 命

$$f：\ a^k \mapsto b^k\ ,$$

则f是G到G'的映射，因为

$$a^k = a^l \Rightarrow a^{k-l} = e \Rightarrow m\,|\,k-l \Rightarrow n\,|\,k-l \Rightarrow b^k = b^l\ ,$$

即对G中的每一元，不论其表法如何，在f下确有唯一的象，故f是G到G'的映射．任取

$x' = b^l \in G'$，则$f(a^l) = b^l$，故f是G到G'的满射，

$$f(a^i a^j) = f(a^{i+j \bmod m}) = b^{i+j \bmod n} = b^{i \bmod n} b^{j \bmod n} = f(a^{i \bmod m}) f(a^{j \bmod m})$$

易见f是G到G'的同态映射，从而$G \sim G'$.

§6 有限群的实例

这一节重点结合密码学中的应用介绍两个具体的有限交换群的例子.

首先，我们看一下有限群Z_n^*及其子群Z_p^*，p为素数，且$p\,|\,n$.

定理 1 Z_n^*表示模n的既约剩余类集合, 任意$\overline{a},\overline{b} \in Z_n^*$，定义其上的乘法

$$\overline{a} \times \overline{b} = \overline{a \times b}$$

则$(Z_n^*, \times)$构成一个交换乘群且Z_n^*的阶为$\phi(n)$.

证明 （1）首先证明：若$\overline{a}=\overline{a'}$，$\overline{b}=\overline{b'}$，则$\overline{a\times b}=\overline{a'\times b'}$.

因为

$$\overline{a}=\overline{a'}\Rightarrow n\mid a-a'\text{，}\ \overline{b}=\overline{b'}\Rightarrow n\mid b-b'\text{，}$$

所以

$$n\mid(a-a')\times b+a'\times(b-b')=a\times b-a'\times b'\text{，}$$

即

$$\overline{a\times b}=\overline{a'\times b'}.$$

（2）显然Z_n^* 对运算“×”封闭，且满足结合律.

（3）任给$a\in Z_n^*$，$\overline{1}\times\overline{a}=\overline{1\times a}=\overline{a\times 1}=\overline{a}\times\overline{1}=\overline{a}$，则$\overline{1}$为单位元.

（4）由数论中同余的性质知每个元素$a\in Z_n^*$都存在逆元$\overline{a}\times\overline{a^{-1}}=\overline{1}$，$a^{-1}\in Z_n^*$.

由以上证明知$(Z_n^*,\times)$构成一个乘群.

（5）由乘法的定义可得

$$\overline{a}\times\overline{b}=\overline{a\times b}=\overline{b\times a}=\overline{b}\times\overline{a}\text{，}\ \forall\overline{a},\overline{b}\in Z_n^*.$$

故$(Z_n^*,\times)$为有限交换群.

$(Z_n^*,\times)$的元素个数为$\phi(n)$，即Z_n^*的阶为$\phi(n)$.

有限群中元素a的周期一定为$|G|$的因子，故有$a^{|G|}=e$，因此可通过群的理论推出 Euler 定理，群$(Z_n^*,\times)$中的任何元素a满足$a^{\phi(n)}\equiv 1(\bmod n)$.

例 1 p为素数且$p\mid n$，设模p的原根为g，则模p的既约剩余系可表示为

$$Z_P^*=\{g^0,g^1,\cdots,g^{p-1}\}=<g>\text{，}$$

$(Z_p^*,\times)$构成乘群，并且$Z_p^*\in Z_n^*$，所以$(Z_p^*,\times)$构成$(Z_n^*,\times)$的子群，容易验证$(Z_p^*,\times)$的阶$p-1\mid\phi(n)$.

定义 1 椭圆曲线E是由标准形式的三次曲线

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6,$$

（系数a_i属于数域K）的所有解$(x,y)\in K^2$的集合，以及一个无穷远点O组成.

对于一般的域K，如果$a_2\neq 0$，则可对椭圆曲线作如下变形

$$y^2+(a_1x+a_3)y=x^3+a_2x^2+a_4x+a_6,$$

则

$$y^2+(a_1x+a_3)y+\frac{(a_1x+a_3)^2}{4}-\frac{(a_1x+a_3)^2}{4}=(y-\frac{(a_1x+a_3)}{2})^2-\frac{(a_1x+a_3)^2}{4}$$

所以只需讨论

$$y^2=f(x)=x^3+ax+b$$

形式的椭圆曲线.

定义 3 在形如（1）的椭圆曲线E上定义加法运算“+”：设$P=(x_1,y_1)\in K$，$Q=(x_2,y_2)\in K$，则

（1）$P+O=P$；

（2）若$x_1=x_2, y_1=-y_2$，则$P+Q=O$；

（3）若$x_1\neq x_2$，$P+Q=(x_3,y_3)$，其中

$$x_3=\lambda^2-x_1-x_2 \pmod p,$$

$$y_3=\lambda(x_1-x_3)-y_1 \pmod p,$$

$$\lambda=\begin{cases}\dfrac{y_2-y_1}{x_2-x_1} \pmod p，\text{如果} P\neq Q,\\ \dfrac{3x_1^2+a}{2y_1} \pmod p，\text{如果} P=Q.\end{cases}$$

一般情况，将$\underbrace{P+P+\cdots+P}_{n\text{次}}$记为$nP$，且$0P=O$.

以上定义的加法运算具有鲜明的几何意义.

（1）若$x_1=x_2, y_1=-y_2$，此时它们的连线与x轴垂直相交，并

与椭圆曲线交于无穷远点O，所以$P+Q=O$.

（2）若$x_1 \neq x_2$，它们的连线与椭圆曲线交于第三个点

$R=(x_3, y_3)$，那么$P+Q+R=O$；

（3）若求$2P$，只需画出P点的切线，与椭圆曲线的另一个交点即为所求R，$P+P+R=O$.

定理 2 椭圆曲线上的有理点集合G关于加法运算构成交换群.

证明 显然P，Q为有理点时，由上述加法定义知$P+Q$仍为椭圆曲线上的有理点，因此G对于加法封闭．另外

（1） 对$\forall P, Q, R \in E$，容易验证有$(P+Q)+R=P+(Q+R)$成立.

（2） 对$\forall P \in E$，都有$P+O=O+P=P$，即无穷远点O为单位元.

（3） 对$\forall P \in E$，存在元素$\forall Q \in E$，使得$P+Q=O$，即Q为其逆元.

（4） $\forall P, Q \in E$，$Q+P=P+Q$.

因此，椭圆曲线上的有理点关于加法运算构成交换群.

例 2 椭圆曲线E（数域K定义为有理数域）由下列方程定义

$$y^2+y=x^3-x^2$$

设$P=(1,-1) \in E$，证明$\{P, 2P, 3P, 4P, 5P=O\}$构成E上的一个有理点群.

解：配方化简方程

$$(y+1/2)^2=(x-1/3)^3-x/3+1/27+1/4.$$

令$y'=y+1/2$，$x'=x-1/3$则方程化为

$$y'^2=x'^3-x'/3+25/108.$$

$P=(x_1, y_1)=(1,-1)$相应于化简后的方程中的点$P'=(2/3,-1/2)$，

$$\lambda=\frac{3\times(4/9)-1/3}{2\times(-1/2)}=-1.$$

所以

$$x_2 = (-1)^2 - 2x_1 = -1/3，\quad y_2 = -1/2，$$

$$2P' = (x_2, y_2) = 2(2/3,-1/2) = (-1/3,-1/2)；$$

$$\lambda = \frac{-1/2+1/2}{2/3+1/3} = 0 .$$

故

$$x_3 = -2/3+1/3 = -1/3，\quad y_3 = 1/2，$$

$$3P' = 3(2/3\,,-1/2) = (2/3,\,-1/2)+(-1/3,\,-1/2)，$$

$$5P' = 5(2/3,\,-1/2) = 3(2/3,\,-1/2)+2(2/3,\,-1/2) = (-1/3,1/2)+(-1/3,\,-1/2) = O$$

下面我们验证 $4P' \neq O$.

$$4P' = 4(2/3,\,-1/2) = 3(2/3,\,-1/2)+(2/3,\,-1/2) = (-1/3,1/2)+(2/3,\,-1/2)$$

其中

$$\lambda = \frac{1/2+1/2}{-1/3-2/3} = 1，\quad x_4 = 1+1/3-2/3 = 2/3，\quad y_4 = 1/2 .$$

故 $4P' \neq O$. 因此 $\{P,2P,3P,4P,5P = O\}$ 构成 E 上的一个有理点群.

习题

1．证明：一个非空集合 G 及它上面的乘法运算如果满足

（1）乘法在 G 中封闭;

（2）结合律成立，即对 G 中任意三个 a,b,c 都有

$$a(bc) = (ab)c；$$

（3） G 中至少存在一个左单位元 e，使得对任意 $a \in G$，

$$ea = a$$

成立;

（4）对任意 $a \in G$， G 中至少存在一个左逆元 a^{-1}，使得

$$a^{-1}a = e .$$

那么集合G对于乘法构成一个群（群的等价定义）.

2．设G是一个群，G不是交换群，$[G:1]>2$，证明：G中存在a,b满足$ab=ba$，且a,b都不是单位元.

3．$G=\{A\mid A\in(Q)_n,|A|\neq 0\}$，则$G$关于方阵乘法作成一个群.

4．设G是一个群，u是在G中取定的元，在G中规定运算“$\circ$”

$$a\circ b=au^{-1}b,$$

证明：　$(G,\circ)$是一个群.

5．设U_n表示n次单位根所成的集合，n是取定的自然数，即

$U_n=\{e^{2k\pi i/n},k=0,1,\cdots,n-1\}$，则$U_n$关于数的乘法做成一个循环群.

6．设G表示Q到Q的一切形如

$$f(x)=ax+b,a\neq 0,a,b\in Q$$

的变换所成集合，则G关于变换的合成作成一个群.

7．命$Z'_n=\{\overline{a}\mid\overline{a}\in Z_n,(a,n)=1\}$, 证明$Z'_n$关于运算$\overline{a}\cdot\overline{b}=\overline{ab}$作成一个群.

8．设 $\begin{matrix} f:a\mapsto(123),a^2\mapsto(132),e\mapsto(1), \\ b\mapsto(12),ab\mapsto(13),a^{2b}\mapsto(23)\end{matrix}$ 是G到S_3的映射，写出G的乘法表.

9．设$H\lhd G$，且$[G:H]=m$则对任意$x\in G$，均有$x^m\in H$.

１０．证明：阶数为$p^2(p$素数$)$的群是可换群.

１１．设H是G的子群，$a,b\in G$．证明：以下六个条件是等价的

1）$b^{-1}a\in H$，　　2）$a^{-1}b\in H$，

3）$b\in aH$，　　4）$a\in bH$，

5）$aH=bH$，　　6）$aH\cap bH\neq\phi$.

１２．设S是群G的一个子集，令

$$C(S)=\{a\mid a\in G,\forall x\in S:ax=xa\}.$$

则$C(S)$是G的一个子群.

１３．设G是循环群，生成元为a，即$G=(a)$，证明：

（1）若a的周期无限，则$G\cong Z$.

（2）若a的周期为n，则$G\cong U_n$.

１４．证明　无限循环群的子群除$\{e\}$外均为无限循环群.

１５．设$H\le K\le G$，证明

$$[G:H]=[G:K][K:H].$$

１６．设G是循环群，A,B,C是G的子群，证明：

$$A\cap((B\cup C))=((A\cap B)\cup(A\cup C)),$$

即A与$B\cup C$生成的子群的交等于$A\cap B, A\cap C$所生成的子群.

１７．设p,q是互异素数，$|G|=pq$，G是可换群，证明：G是循环群.

１８．设A, B是群G的两个有限子群，则

$$|AB|=\frac{|A||B|}{|A\cap B|}.$$

１９．设A, B是G的子群，则AB是G的子群的充分必要条件是

$AB=BA$.

２０．证明：f：$x\mapsto x^{-1}$是G的一个自同构的充要条件是G是可换群.

２１．设A是G的不变子群，B是G的不变子群，则$A\cap B, AB$都是G的不变子群.

２２．设G是一个群，S是G的子群，命

$$N(S)=\{x\mid x\in G,\forall a\in S: xax^{-1}\in S\},$$

则$N(S)$是G的子群．$N(S)$叫做S的正规化子.

２３．设$G\sim G',\ker f=K,H$是G的子群，证明：$f^{-1}(f(H))=HK$.

２４．设n是取定的自然数，$n>1$，命

$$M_n = \{[a, b] \mid a, b \in Z, (a, n) = 1\}$$

规定$[a, b] \circ [c, d] = [ac, bc + d]$，证明：$M_n$作成群.

命φ：$[a,b] \mapsto [\overline{a}]$，证明：$\varphi$是$M_n$到$Z_n'$的满同态，求$\ker\varphi$.

２５．设H, K 是G的子群，且K是$H \cup K$生成子群的不变子群，证明：

（1） $(H \cup U) = HK$；

（2）$H \cap K$是H的不变子群；

（3）命$\varphi : aK \mapsto a(H \cap K)$，则$\varphi$是$HK/K$到$H/H \cap K$的同构映射.

２６．设H, K是G的不变子群，且$H \supset K$, 则

$$G/H \cong {}^{G/K}\big/_{H/K}.$$

２７．设$H = \{(1), (12)(34), (13)(24), (14)(32)\}$，则

$$S_4/H \cong S_3$$

G/H中零元是什么？G/H中运算是怎样的？

２８．设U表示一切单位根作成的乘群，证明：Q/Z与U同构.

２９．设G是一个群，G的子群只有有限多个．f是G到自身的一个满同态.

证明：f是G的一个自同构.

３０．设G是一个群，$a, b \in G$, 符号$[a, b]$表示G中的元素$a^{-1}b^{-1}ab$，称之为G的换位元，证明：

1）G的一切有限个换位元的乘积所成集合G'是G的一个不变子群；

2）G/G'是可换群；

3）若N是G的不变子群，且G/N可换，则$N \geq G'$.

３１．设p, q是互异素数，$|G| = pq$，G是可换群，证明：G是循环群.

３２．设$H < G, |H| = n$, 且G的阶数为n的子群仅有一个，则H是G的

不变子群.

３３．设G是有限可换群，$|G|=n, p$是素数，$p\mid n$，则G中存在周期为p的素数.

３４．设p,q是互异素数，$|G|=pq, p<q$，证明：G的q元子群是不变子群.

３５．设$A_1\subseteq A_2\subseteq\cdots\subseteq A_n\subseteq\cdots$是$G$的不变子群的链，证明：$A=\bigcup_{i=1}^{\infty}A_i$是$G$的不变子群.

３６．$H<G,K<G,D=H\cap K$，证明：

（１）若$k_1,k_2\in K,$且k_1,k_2属于D的两个不同右陪集，则$Hk_1\cap Hk_2=\phi$.

（２）H,K是G的有限子群，$[K:D]=d,$且$K=\bigcup_{i=1}^{d}Dk_i$，则$HK=\bigcup_{i=1}^{d}Hk_i$.

３７．设G是可换群，证明：G中所有有限阶元素所成集合T是G的一个子群，并且G/T除单位元外不含有限阶元素.

３８．椭圆曲线E（数域K定义为有理数域）由下列方程定义

$$y^2+y-xy=x^3.$$

设$P=(1,1)\in E$，证明：$\{P,2P,3P,4P,5P,6P=O\}$构成E上的一个有理群.