目　录

第一章 整 数

本章介绍“数论”中一些最基本的事实，就是说，研究整数的一些最基本的性质．本课从整数的性质讲起，一方面由于这些性质本身是重要的，一方面是为以后较抽象的理论作准备，因为后面三章内的理论很多都可以在数论中找到根源和实例．

我们知道任意两个整数可以相加相减相乘，结果仍是整数．但两个整数不一定可以在整数的范围内相除，这是整数系统的特点，和有理数系统实数系统等不一样．既然如此，研究整数就必须针对这一个特点加以分析，这说明为什么研究整数的性质基本上就是要研究整除性因数分解等问题以及和这些事情有关的问题．

§1. 最 高 公 因

设 a,b 是两个整数，如果有整数 c 存在使 $a=bc$．则我们说 a 是 b 的**倍数**，b 是 a 的**因数**，或说 b **整除** a．b 整除 a 记为 $b|a$．例如，任意整数整除 0，而 ±1 整除任意整数．

由整除的定义，立刻可以证明下面几个简单的事实：

1° 若 $a|b$，$b|c$，则 $a|c$．

证．因为 $a|b$，$b|c$，故有整数 a,e 使 $b=ad$，$c=be$．因之 $c=a(de)$．但 de 为整数，所以 $a|c$．

2° 若 $a|b$，则 $a|bc$．

证．由定义，$b|bc$，今 $a|b$，$b|bc$，故由 1°，$a|bc$．

3° 若 $a|b$，$a|c$，则 $a|b\pm c$．

证．因为 $a|b$，$a|c$，故有整数 d,e 使 $b=ad$，$c=ae$，因之 $b\pm c=a(d\pm e)$．但 $d\pm e$ 为整数，所以 $a|b\pm c$．

4° 若在一等式中，除某项外，其余各项都是 a 的倍数，则此项也是 a 的倍数．

证．设在等式 $b-c=-d+e+f$ 中，b,c,d,f 都是 a 的倍数，求证 e 也是 a 的倍数．解出 e 得 $e=b-c+d-f$．由3°，$b-c+d-f$ 是 a 的倍数，故 e 是 a 的倍数．

5° 若 $a|b$，$b|a$，则 $b=\pm a$．

证．若 $a=b=0$，则自然 $b=\pm a$ 是对的．设 $a\neq0$，因为 $a|b$，$b|a$，故有整数 d,e 使 $b=ad$，$a=be$，于是 $a=ade$，消去 a 得 $1=de$．今 d,e 是整数而相乘得 1，故 d 和 e 都等于 ±1，因而 $b=\pm a$．

若 d 是 a,b 的公因数而 a,b 的任意公因数整除 d，则 d 说是 a,b 的**最高公因**．

这个定义只是说如果有那样的 d，则 d 叫做 a,b 的最高公因．对于任意 a,b，是

否一定有那样的 d 呢？现在还不知道，下面再研究．不过，有一点是容易说明的：如果 a,b 有最高公因，则最高公因除符号外唯一确定．事实上，若 d 和 d' 都是 a,b 的最高公因，则 $d|d', d'|d$，因而由 5°，$d'=\pm d$．

现在我们来看，是否任意 a,b 有最高公因．若 a,b 中有一个是 0，则其余一个就是最高公因，这由定义是显然的．设 $a\neq 0$，$b\neq 0$，若 $b|a$，则 b 就是 a,b 的最高公因．若 $b\nmid a$，则以 b 除 a 得一个商 q 和一个余数 r 而

$$a=qb+r,\quad 0<r<|b|. \tag{1}$$

观察(1)式我们发现，若 d 是 b,r 的公因数，则由4°，d 也是 a 的因数，因而是 a,b 的公因数．反之，若 d 是 a,b 的公因数，则由 4°，d 是 r 的因数，因而是 b,r 的公因数．可见 a,b 的公因数和 b,r 的公因数完全是相同的，求 a,b 的最高公因，只要求 b,r 的最高公因就成了．这就是说，我们把关于 a,b 的问题换成了关于 b,r 的问题，因为 b,r 的第二个数 r 小于 a,b 的第二个数 b（的绝对值），这样一换是有好处的．若 $r|b$，则 r 就是 b,r 的最高公因，因而也就是 a,b 的最高公因；若 $r\nmid b$，则以 r 除 b 得商及余数而照样推理．如此类推，因为所得的余数一直减小，所以一直作下去必然停止，这就是所谓辗转相除法．设辗转相除中得下列各式：

$$\begin{aligned}
&a=q_1b+r_1,\\
&b=q_2r_1+r_2,\\
&\cdots\cdots,\\
&r_{k-2}=q_kr_{k-1}+r_k,\\
&\cdots\cdots,\\
&r_{n-2}=q_nr_{n-1}+r_n,\\
&r_{n-1}=q_{n+1}r_n.
\end{aligned}\tag{2}$$

由以上的推理我们知道 a,b 的公因数和 r_1,r_2 的公因数相同，…，和 r_{n-1}，r_n 的公因数相同，但由(2)的最后一式，$r_n|r_{n-1}$，故 r_n 是 r_{n-1}，r_n 的最高公因，因而也是 a,b 的最高公因．这样，我们就证明了下面的定理：

定理 1．任意整数 a,b 有一个最高公因．

为了下面的应用我们证明

定理 2．a,b 的最高公因 d 可以表为下面的形式：

$$d=sa+tb, \tag{3}$$

其中 s,t 都是整数．

证．由(2)中第一式知

$$\begin{pmatrix}a\\b\end{pmatrix}=\begin{pmatrix}q_1 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}b\\r_1\end{pmatrix}.$$

又由第二式知

$$\begin{pmatrix}b\\r_1\end{pmatrix}=\begin{pmatrix}q_2 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}r_1\\r_2\end{pmatrix},$$

故

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} r_1 \\ r_2 \end{pmatrix},$$

由此类推可见

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} r_{k-1} \\ r_k \end{pmatrix}.$$

命

$$\begin{pmatrix} T_k & V_k \\ S_k & U_k \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix},$$

则

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} T_k & V_k \\ S_k & U_k \end{pmatrix}\begin{pmatrix} r_{k-1} \\ r_k \end{pmatrix}.$$

今 $\begin{vmatrix} q_1 & 1 \\ 1 & 0 \end{vmatrix} = \cdots = \begin{vmatrix} q_k & 1 \\ 1 & 0 \end{vmatrix} = -1$，故 $\begin{vmatrix} T_k & V_k \\ S_k & U_k \end{vmatrix} = (-1)^k$，而

$$\begin{pmatrix} T_k & V_k \\ S_k & U_k \end{pmatrix}^{-1} = \begin{pmatrix} \dfrac{U_k}{(-1)_k} & \dfrac{-V_k}{(-1)^k} \\ \dfrac{-S_k}{(-1)^k} & \dfrac{T_k}{(-1)^k} \end{pmatrix} = \begin{pmatrix} (-1)^k U_k & (-1)^{k-1}V_k \\ (-1)^k S_k & (-1)^k T_k \end{pmatrix}.$$

因之，

$$\begin{pmatrix} r_{k-1} \\ r_k \end{pmatrix} = \begin{pmatrix} T_k & V_k \\ S_k & U_k \end{pmatrix}^{-1}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} (-1)^k U_k & (-1)^{k-1}V_k \\ (-1)^{k-1}S_k & (-1)^k T_k \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix}.$$

特别，我们得到

$$r_k = (-1)^{k-1}S_k a + (-1)^k T_k b. \tag{4}$$

取 $k=n$，则得 $d = r_n = (-1)^{n-1}S_n a + (-1)^n T_n b$，即(3)式形式.

为了后面的应用，我们说明怎样简便地计算 S_k 和 T_k. 今

$$\begin{pmatrix} T_k & V_k \\ S_k & U_k \end{pmatrix} = \begin{pmatrix} T_{k-1} & V_{k-1} \\ S_{k-1} & U_{k-1} \end{pmatrix}\begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} q_k T_{k-1} + V_{k-1} & T_{k-1} \\ q_k S_{k-1} + U_{k-1} & S_{k-1} \end{pmatrix},$$

比较前后两个方阵的第二行知 $U_k = S_{k-1}$，$V_k = T_{k-1}$，故 $U_{k-1} = S_{k-2}$，$V_{k-1} = T_{k-2}$. 再比较方阵的第一行，则得

$$\begin{cases} S_k = q_k S_{k-1} + S_{k-2}, \\ T_k = q_k T_{k-1} + T_{k-2}. \end{cases} \tag{5}$$

此二式在 $k>2$ 时成立. 若命 $S_0 = U_1 = 0$，$T_0 = V_1 = 1$，则 $k=2$ 时亦成立. 今知 $S_0 = 0$，$S_1 = 1$，$T_0 = 1$，$T_1 = q_1$，故累用(5)式即可求出任意 S_k，T_k.

例. 求 301 和 133 的最高公因并表为 $301s + 133t$ 的形式，

解. 用辗转相除法求出最高公因为 7 而所得之商依次为 2，3，1，4. 求 S_k，T_k 如下：

$k=$	0	1	2	3
$q_k=$		2	3	1
$S_k=$	0	1	3	4
$T_k=$	1	2	7	9

故 $7 = (-1)^2 4\cdot 301 + (-1)^3 9\cdot 133 = 4\cdot 301 + (-9)133$.

若 a,b 的最高公因为 1，则我们说 a 和 b **互质**。例如 1 和任意整数互质。

定理 3。若 a,b 互质而 $a|bc$，则 $a|c$。

证。因为 a,b 互质，故有 s,t 使 $1=sa+tb$，因而 $c=sac+tbc$。但 $a|sac$，$a|tbc$，故 $a|c$。

习　　题

1. 求 1331 和 5709 的最高公因并表为 $1331s+5709t$ 的形式，

2. 记 T_k 为 $[q_1,q_2,\cdots,q_k]$，求证

$$S_k=[q_2,\cdots,q_k].$$

3. 求证 $[q_1,q_2,\cdots,q_k]=[q_k,\cdots,q_2,q_1]$。

4. 若 a 和 b 互质并和 c 互质，求证 a 和 bc 互质。用数学归纳法推广！

5. 分数 $\frac{m}{n}$ 叫做一个既约分数，如果 m 和 n 互质，证明任意分数可以化为一个既约分数而且只能等于一个既约分数。

6. 界说两数的最低公倍，证明若 d 是 a,b 的最高公因则 $\frac{ab}{d}$ 是 a,b 的最低公倍。

§2. 质　　数

一个正整数 $(\neq 1)$ 叫做一个**质数**，如果除了自己和 1 以外，没有其他正因数。

定理 1。若 p 为质数而 $p|a_1\cdots a_n$，则 p 必整除 $a_1,\cdots,a_n$ 之一。

证。若 $p|a_n$，则定理已证。设 $p\nmid a_n$。因为 p 只有 p 和 1 两个正因数，而 p 不是 a_n 的因数，故 p 和 a_n 的最高公因等于 1，即 p 和 a_n 互质。今 $p|(a_1\cdots a_{n-1})a_n$。故由上节定理 3，$p|a_1\cdots a_{n-1}$。同样，若 $p|a_{n-1}$ 则定理已证，否则 p 必整除 $a_1\cdots a_{n-2}$，如此类推，必可找到 $a_n,a_{n-1},\cdots,a_2$ 中的一个为 p 整除。

定理 3（算术的基本定理）。任意正整数 $n(\neq 1)$ 恰有一法写成质数的乘积。

证。先证 n 可以写成质数的乘积。$n=2$ 时这话显然对，因为 2 是质数，算是已经写成了质数的乘积。今用数学归纳法，假定 $n<a$ 时 n 可以写成质数的乘积，试证 $n=a$ 时也可以这样写。若 a 是质数，则 a 算是已经写成了质数的乘积，设 a 不是质数，则 a 有因数 b，$1<b<a$。因之，$a=bc$，$1<c<a$，既然 b 和 c 都 $<a$，故由归纳法假定，b 和 c 都可以写成质数的乘积。但 $a=bc$，所以只要把这两个乘积并起来就得到一个质数的乘积等于 a，归纳法已经作完，故任意正整数 $n(\neq 1)$ 可以写成质数的乘积。

再证 n 只有一法可以写成质数的乘积，换句话说，如果

$$n=p_1\cdots p_h=q_1\cdots q_k, \tag{1}$$

而 $p_1,\cdots,p_h,q_1,\cdots,q_k$ 都是质数，则 $h=k$ 而且 $p_1,\cdots,p_k$ 和 $q_1,\cdots,q_k$ 完全一样最多次序不同。由 (1)，$p_1(p_2\cdots p_h)=q_1\cdots q_k$，故 $p_1|q_1\cdots q_k$。由定理 1，p_1 应整除 $q_1,\cdots,q_k$ 之一，比方，$p_1|q_1$。今 q_1 是质数，只有 q_1 和 1 两个正因数，而 $p_1\neq 1$，故 p_1 必 $=q_1$。由 (1) 消去 p_1 而得 $p_2\cdots p_h=q_2\cdots q_k$，而由此式同上可证 p_2 必等于 $q_2,\cdots,q_k$ 之一，如

此类推，可见 $q_1,\cdots,q_k$ 和 $p_1,\cdots,p_h$ 完全相同最多次序不一样。

推论1．任意整数($\neq 0$，± 1)恰有一法写成下面的形式

$$\pm p_1\cdots p_k,$$

其中 $p_1,\cdots,p_k$ 都是质数，

推论1的 $p_1,\cdots,p_k$ 中，可能有的质数重复出现，若把相同的质数归在一起，则有

推论2．任意整数($\neq 0$，± 1)恰有一法写成下面的形式

$$\pm p_1^{r_1}\cdots p_n^{r_n}, \tag{2}$$

其中 $p_1,\cdots,p_n$ 是不相同的质数，$r_1,\cdots,r_n$ 是正整数。

现在我们谈一些关于质数的简单事实。

定理3．质数无穷多。

证．用欧几里得的方法，假定质数只有有限个，命为 $p_1,\cdots,p_n$。试看 $N=p_1p_2\cdots p_n+1$，因为 $p_1,p_2,\cdots,p_n$ 都不能整除 N，故 N 无质因数，此不可能。

质数既无穷多，自然无法求出所有质数，但用所谓“筛法”可以求小于某数的所有质数。

例．求30以内的质数。

解，把2到30的各数按次序写下，从3起隔一数去一数便把2的倍数筛去，从4起隔两数去一数便把3的倍数筛去，如此继续，剩下的便是质数：

2，3，4，5，6，7，8，9，10，11，12，13，14，15，16，17，18，19，20，21，22，23，24，25，26，27，28，29，30。

现在最大的质数表列出来了10000000以内的所有质数，而现在知道的较大质数例如有

$$2^{127}-1=170141183460469231731687303715884105727.$$

质数虽不能完全知道，但未尝不可有一种不太繁的算法，用它可以求出任意多的质数，比方，找些算式 $f(n)$，对于任意自然数 n，其值为质数，这样的算式现在还没有。Fermat 猜想 $2^{2^n}+1$ 永远代表质数，$n=0,1,2,3,4$ 时，$2^{2^n}+1=3,5,17,257,65537$ 果然都是质数，可惜后来有人发现 $2^{2^5}+1=641\times 6700417$。

习　　题

1．说明任意有理数($\neq 0,\pm 1$)恰有一法写成下面的形式

$$\pm p_1^{r_1}\cdots p_n^{r_n},$$

其中 $p_1,\cdots,p_n$ 是不同的质数，$r_1,\cdots,r_n$ 是非0整数。

2．设整数 a 写成了推论2中(2)的形式，a 有多少个因数？

3．设 $a=\pm p_1^{r_1}\cdots p_n^{r_n}$，$b=p_1^{s_1}\cdots p_n^{s_n}$，其中 $p_1,\cdots,p_n$ 是不同的质数，$r_1,\cdots,r_n$，$s_1,\cdots,s_n$ 是非负整数（事实上任意两个非0整数 a,b 一定可以写成这样，因为总可以在 a,b 的分解式中添上一些质数的0次方而把两个分解式中出现的质数凑成都是 $p_1,\cdots,p_n$）。问：a,b 的最高公因和最低公倍是什么？

4. 按照下列提示，不借助于最高公因的理论直接用数学归纳法证明算术的基本定理（Zermelo证法）：设定理对于所有小于 a 的数成立，试证对于 a 成立。取 a 的大于1的最小的因数 p，易证 p 是质数，因之，$a=pb$，由此易证 a 可以分为质因数的乘积。假定 a 尚有另一种分法，此分法中必不包含 p，因为 b 的分法唯一，设 q 是其中的一个质因数，则 $a=qc$。试看

$$a_0=a-pc=p(b-c)=(q-p)c.$$

$a_0, b-c, q-p, c$ 都是小于 a 的正数，故分法唯一，如此，则由上式不难推出矛盾。

5. 求证等差级数

$$7, 11, 15, \cdots$$

中有无穷多个质数。提示：先证任意多个形为 $4n+1$ 的数相乘仍是 $4n+1$ 的形式；假定上面等差级数中只有有限个质数 $p_1, \cdots, p_m$，试看 $N=4p_1\cdots p_m+3$。

§3. 合　　同

设 m 是任意正整数，a 为 m 整除时，我们也说 a **合同**于0模 m：

$$a\equiv 0 \pmod m.$$

一般说来，若 $a-b$ 为 m 整除，则我们说 a **合同**于 b 模 m：

$$a\equiv b \pmod m.$$

设 $a=q_1m+r_1$，$b=q_2m+r_2$，$0\leqslant r_1<m$，$0\leqslant r_2<m$。于是

$$a-b=(q_1-q_2)m+(r_1-r_2).$$

由§1的4°，$m\mid a-b$ 必要而且只要 $m\mid r_1-r_2$。但 $|r_1-r_2|<m$，故 $m\mid r_1-r_2$ 必要而且只要 $r_1-r_2=0$。因之，$a\equiv b \pmod m$ 必要而且只要以 m 除 a 和 b 所得余数相同。

所谓合同不过整除性的一种表达方法，但这种说法是有好处的，因为以下可以看出来，“合同”和“相同”，其性质是很类似的。

因为模 m 合同等于说以 m 除所得余数相同，所以下面的简单事实成立 $(\mathrm{mod}\ m)$：

1° $a\equiv a$，

2° 若 $a\equiv b$，则 $b\equiv a$。

3° 若 $a\equiv b$，$b\equiv c$，则 $a\equiv c$。

这些都和“相等”的性质相同，这些性质依次叫反身性，对称性，传递性。

4° 若 $a\equiv b$，$c\equiv d$，则 $a\pm c\equiv b\pm d$，$ac\equiv bd$。

证。因为 $a\equiv b$，$c\equiv d$，故有 r, s 使 $a-b=rm$，$c-d=sm$，故 $(a\pm c)-(b\pm d)=(r\pm s)m$，因而 $a\pm c\equiv b\pm d$。其次，$ac=(b+rm)(d+sm)=bd+rdm+bsm+rsm^2\equiv bd+0+0+0=bd$，故 $ac\equiv bd$。

由4°，在一个合同式中可以移项，比方，设 $a+b\equiv c \pmod m$。则可以推出 $a\equiv c-b \pmod m$。因为，由 $a+b=c$，$-b\equiv -b$ 得 $a+b-b\equiv c-b$，即 $a\equiv c-b$。同样，可以用同数乘合同式的两边，例如由 $a\equiv b \pmod m$ 可以推出 $ac\equiv bc \pmod m$。

这些都和相等的性质相同，但对于数的相等，我们还有消去律，即若 $c\neq 0$ 而 $ac=$

bc 则 $a=b$，这在合同并不普遍成立，例如

$$8\equiv 14 \pmod 6,\quad 4\not\equiv 7 \pmod 6.$$

但下列两个事实成立：

5° 若 $c\neq 0$ 而 $ac\equiv bc \pmod{mc}$，则 $a\equiv b \pmod m$.

证. 因为 $ac\equiv bc \pmod{mc}$，故 $ac-bc=qmc$，q 为整数；于是 $a-b=qm$，因而 $a\equiv b \pmod m$.

6° 若 c 和 m 互质，则由 $ac\equiv bc \pmod m$ 可以推出 $a\equiv b \pmod m$.

证. 由于 $ac\equiv bc \pmod m$，故 $m\mid (a-b)c$，但 c 和 m 互质，所以 $m\mid a-b$，即 $a\equiv b \pmod m$.

对于质数模 p，则有和相等完全类似的消去律：

7° 若 $c\not\equiv 0 \pmod p$ 而 $ac\equiv bc \pmod p$，则 $a\equiv b \pmod p$.

证. 因为 p 是质数，$c\not\equiv 0 \pmod p$ 就表示 c 和 p 互质，因而 7° 不过是 6° 的推论.

试模 m 来看所有整数，把模 m 合同的数归在一类，这样我们便把所有整数分成许多组，每一组叫一个**剩余类**. 因为以 m 除任意整数，可能得到的余数只有 $0,1,\cdots,m-1$ 这 m 个数，所以模 m 共有 m 个剩余类. 从每个类中取出一个数作为代表所得的 m 个数 $r_1,\cdots,r_m$ 说是作为一个**完全剩余系**，任意整数模 m 恰合同于 $r_1,\cdots,r_m$ 之一. 例如 $0,1,\cdots,m-1$ 便是这样一个完全剩余系，比方，模 3，三个数 0，1，2 作成一个完全剩余系，$-1,0,1$ 也是一样；模 2 有两个剩余类，可以用 0，1 作为代表，0 代表所有偶数，1 代表所有奇数.

定理. 若 a 和 m 互质而 b 任意，则模 m 恰有一个数 x 使 $ax\equiv b \pmod m$.

证一，设 $r_1,\cdots,r_m$ 是模 m 的一个完全剩余系，试看 $ar_1,\cdots,ar_m$，我们说，$i\neq j$ 时，$ar_i\not\equiv ar_j \pmod m$，因否则由 6° 将有 $r_i\equiv r_j \pmod m$. 因之，模 m，$ar_1,\cdots,ar_m$ 两两互不合同，今模 m 共有 m 个剩余类，可见 $ar_1,\cdots,ar_m$ 也作成一个完全剩余系，故 b 必合同于某一个 ar_i，取 $x=r_i$ 乃有 $ax\equiv b \pmod m$. 所谓模 m 只有一个这样的 x 意思是说若 $ax\equiv b$，$ay\equiv b$，则 $x\equiv y$. 这很容易说明，因为由 $ax\equiv b$，$ay\equiv b$ 得 $ax\equiv ay$，消去 a 乃得 $x\equiv y$.

证二，因为 a 和 m 互质，故有 s，t 使 $as+mt=1$，于是 $asb+mtb=b$，但 $mtb\equiv 0 \pmod m$，故 $asb\equiv b \pmod m$，取 $x=sb$ 乃有 $ax\equiv b \pmod m$. 唯一性的证明同上.

证一比较直观，使我们明白定理成立的所以然，证二给出求 x 的一个简便的方法（参看 1§ 中求 S_k,T_k 的方法）.

推论. 设 p 为质数，若 $a\not\equiv 0 \pmod p$ 而 b 任意，则模 p 恰有一个数 x 使 $ax\equiv b \pmod p$.

习　　题

1. 若 a 是一个奇数，说明 $a^2\equiv 1 \pmod 8$.

2. 解合同式 $35x\equiv 1 \pmod{97}$.

3. 设 p 为质数，求证 $(a+b)^p\equiv a^p+b^p \pmod p$.

提示：用二项式定理展开$(a+b)^p$。

4. 已知1954年10月1日是星期5，设公历n年的第七天是星期s，证明下列求s的公式：

$$s\equiv n-1+\left[\frac{n-1}{4}\right]-\left[\frac{n-1}{100}\right]+\left[\frac{n-1}{400}\right]+1 \pmod 7.$$

注。$[x]$表示数x的整数部分。

§4. 秦九韶定理 Euler函数

引理。 设$m_1,\cdots,m_k$两两互质，若$a\equiv b \pmod{m_i}, i=1,\cdots,k$，则$a\equiv b \pmod{m_1\cdots m_k}$。

证。命$c=a-b$，因为$a\equiv b \pmod{m_i}$，故$m_i \mid c$，因之m_i的分解式中的所有质因数都在c的分解式中出现（而且若某个质因数在m_i中重复出现，则在c中至少出现同样多次），但$m_1,\cdots,m_k$两两互质，所以$i\neq j$时m_i和m_j的分解式中没有公共的质因数，因之，$m_1,\cdots,m_k$的分解式中的所有质因数都在c的分解式中出现，故$m_1\cdots m_k \mid a$，即 $a\equiv b \pmod{m_1\cdots m_k}$。

定理1（秦九韶定理）。设$m_1,\cdots,m_k$两两互质。设对每个m_i指定一个整数a_i，这样，则模$m_1\cdots m_k$恰有一个整数x存在适合下列合同式：

$$\begin{cases} x\equiv a_1 \pmod{m_1}, \\ \cdots, \\ x\equiv a_k \pmod{m_k}. \end{cases} \tag{1}$$

证一，命$m=m_1\cdots m_k$。设$r_1,\cdots,r_m$是模m的一个完全剩余系，$r_{i1},\cdots,r_{im_i}$是模m_i的一个完全剩余系，试看任意r_j，模m_i，r_j合同于某r_{ij_i}，即任意r_j决定一组

$$r_{1j_1},\ \cdots,\ r_{kj_k}. \tag{2}$$

今若$j\neq j'$，则r_j决定的组(2)和$r_{j'}$决定的组(2)必不相同，因否则$r_j\equiv r_{j'} \pmod{m_i}$，$i=1,\cdots,k$。因而由引理将有$r_j\equiv r_{j'} \pmod m$，与$r_1,\cdots,r_m$是模$m$的一个完全剩余系的假定冲突。总之，每个$r_j$决定一个组(2)，不同的$r_j$决定不同的组(2)。但$r_{ij_i}$由$r_{i1},\cdots,r_{im_i}$中选取，共有$m_i$个不同的取法，因而可能的组(2)共有$m_1\cdots m_k=m$个。今$r_1,\cdots,r_m$也有$m$个，所以任取一个组(2)恰有一个$r_j$存在合同于$r_{ij_i}$模$m_i$，定理中所给的一组数$a_1,\cdots,a_k$模$m_1,\cdots,m_k$合同于一个组(2)，故有一个$x$适合(1)。至于模$m$恰有一个这样的$x$由以上的证明已很明显，今再直接说明如下，若$x,x'$都适合(1)，则$x\equiv x' \pmod{m_i}$，故由引理，

$$x\equiv x' \pmod m.$$

证二，先不讨论普遍情形而先求e_i使适合下列特殊的合同式：

$$\begin{aligned} &e_i\equiv 1 \pmod{m_i}, \\ &e_i\equiv 0 \pmod{m_j}, \qquad j\neq i. \end{aligned} \tag{3}$$

今$j\neq i$时m_i和m_j互质，故m_i和$\prod_{j\neq i} m_j$互质，由上节定理，有c_i存在使$c_i\prod_{j\neq i} m_j\equiv$

$1(mod\ m_i)$，取$e_i=c_i\prod_{j\neq i}m_j$，则$c_i$显然适合(3)。今取

$$x=a_1e_1+\cdots+a_ke_k,$$

则模m_i，$x=a_1e_1+\cdots+a_{i-1}e_{i-1}+a_ie_i+a_{i+1}e_{i+1}+\cdots+a_ke_k\equiv a_10+\cdots+a_{i-1}0+a_i1+a_{i+1}0+\cdots+a_k0=a_i$，故$x$适合(1)。唯一性的证明同上，

秦九韶定理（及其推广）在数论上起基本性的作用，证二给出求x的一个简便的方法，这个方法（包括§1求S，T的方法）秦氏称为求一术。

设n是任意正整数，试看模n的任意剩余类A，设$a\in A$。若a和n互质，则A中任意数和n互质。事实上，若$b\equiv a(mod\ n)$，则$a=b+qn$，倘b和n有一个大于1的公因数d，则由上式d也是a的因数，因而d是a和n的公因数，此为矛盾。可见，若A中有一个数和n互质，则所有的数都和n互质，故A中的数或者都和n互质，或者都和n不互质。在第一种情形下，我们说剩余类A和n互质，和n互质的剩余类的个数记为$\varphi(n)$，称为**Euler函数**。显然，$\varphi(n)$等于模n的一个完全剩余系中和n互质的数的个数；因而$\varphi(n)$又等于$\leqslant n$的正数中和n互质的数的个数。

现在我们看怎样计算$\varphi(n)$。

定理2。设$m=m_1\cdots m_k$而$m_1,\cdots,m_k$两两互质，如此，则

$$\varphi(m)=\varphi(m_1)\cdots\varphi(m_k)\tag{4}$$

证。在定理1的证一中，若r_j和m互质，则r_{ij_i}和m_i互质。事实上，因为r_j和m没有大于1的公因数，故r_i和m_i更没有大于1的公因数，因而r_j和m_i互质。但$r_j\equiv r_{ij_i}(mod\ m_i)$故$r_{ij_i}$和$m_i$互质。反之，若$r_{ij_i}$和$m_i$互质，$i=1,\cdots,k$，则$r_j$和$m$互质。事实上，因为$r_{ij_i}$和$m_i$互质故$r_j$和$m_i$互质，因而$m_i$的分解式中的任意质因数不能整除$r_j$，故$m$的分解式的任意质因数不能整除$r_j$，即$r_j$和$m$互质。今和$m$互质的$r_i$共有$\varphi(m)$个而和$m_i$互质的$r_{ij_i}$共有$\varphi(m_i)$个，故得(4)。

定理3。设$n=p_1^{r_1}\cdots p_k^{r_k}$是$n$的质因数分解式，$p_1,\cdots,p_k$都不同，则

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\cdots\left(\frac{1}{p_k}\right).\tag{5}$$

证。先设p为质数而求$\varphi(p^r)$。我们知道一个数a和p互质等于说$p\nmid a$。今在从1到p^r的p^r个数中，是p的倍数的共p^{r-1}个，即$p.2p,3p,\cdots,p^{r-1}p$，因而和p互质的共p^r-p^{r-1}个，即$\varphi(p^r)=p^r\left(1-\frac{1}{p}\right)$。

由定理二有$\varphi(n)=\varphi(p_1^{r_1})\cdots\varphi(p_k^{r_k})=p_1^{r_1}\left(1-\frac{1}{p_1}\right)\cdots p_k^{r_k}\left(1-\frac{1}{p_k}\right)=n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)$。

定理4（**Fermat－Euler定理**）。若a和n互质，则

$$a^{\varphi(n)}\equiv 1(mod\ n).\tag{6}$$

证。设$r_1,\cdots,r_n$是模n的一个完全剩余系，由上节定理的证一，$ar_1,\cdots,ar_n$也是模n的一个完全剩余系，故$ar_1,\cdots,ar_n$按适当次序合同于$r_1,\cdots,r_n$。今若r_i和n互质，则因为a也和n互质，故知ar_i也和n互质。设$r_1,\cdots,r_{\varphi(n)}$是$r_1,\cdots,r_n$中和$n$互质的数，

由上，$ar,\cdots,ar_{\varphi(n)}$是$ar_1,\cdots,ar_n$中和$n$互质的数．但和$n$互质的数只能与和$n$互质的数合同，故$ar_1,\cdots,ar_{\varphi(n)}$按一定次序和$r_1,\cdots,r_{\varphi(n)}$合同，因之，

$$ar_1\cdots ar_{\varphi(n)}\equiv r_1\cdots r_{\varphi(n)}\ (mod\ n).$$

因为$r_1,\cdots,r_{\varphi(n)}$和$n$互质，故这些数可由上式两边消去而得(6)，

若$n=p$是一个质数，则$\varphi(n)=p-1$，故得

推论（Fermat 定理）．若p是质数而$p\nmid a$，则

$$a^{p-1}\equiv 1(mod\ p).$$

习　　题

1．今有物不知数，三三数之剩二，五五数之剩三，七七数之剩二，问至少物几何？（孙子算经）．

2．解合同式 $x^2+6x+15\equiv 0(mod\ 77)$．提示：先模7和模11解此合同式而后用求一术．

3．由实际计算验证$3^{16}\equiv 1(mod\ 17)$．

4．今天是星期一，$10^{10^{10}}$天后是星期几？

5．设$\frac{r}{n}$是一个既约真分数而n不是偶数也不是5的倍数，求证$\frac{r}{n}$展成一个无尽小数必是一个循环小数，其循环节的位数是$\varphi(n)$的因数，而且是一个纯循环小数．

6．纸牌$2n$张（比方$2n=52$），用下列手法洗牌：将牌平分为上下两部，将下部最末一张洗在最下面，上部最末一张洗为倒数第二张，下部倒数第二张洗为倒数第三张，上部倒数第三张洗为倒数第四张，如此间错，求证用这种手法继续洗下去，洗到第$\varphi(2n-1)$次必然还原．提示：用$0,1,\cdots,2n-1$代表由上而下各牌．

7．对于定理一证二中之$e_1,\cdots e_k$，求证模m，

$$e_i^2\equiv 1,$$

$$e_ie_j\equiv 0(i\neq j),$$

$$e_1+\cdots+e_k\equiv 1.$$

第二章　群

§1. 变换及置换

群是近世代数上最基本的概念，群这一个概念概括许多具体的运算系统，而群论的应用也是多方面的，话虽如此，抽象群的最主要的根源却应该说是变换群．因此，本章从变换群讲起，而于§3才进入抽象群的讨论．

设 A, B 是两个集合．如果对于 A 的任意元素规定了 B 的一个确定的元素为它的影象，那么，我们便规定了 A 到 B 的一个**写象**．写象常用希腊字母 σ, τ 等代表．若 σ 是 A 到 B 的一个写象而 $a\in A$，a 在 σ 之下的影象记为 $\sigma(a)$．设 A_1 是 A 的子集，A_1 所有元素的影象的集合称为 A_1 的影象集合，记为 $\sigma(A_1)$．

设 σ 是 A 到 B 的一个写象，A 的影象集合 $\sigma(A)$ 未必等于 B，如果 $\sigma(A)=B$，换句话说，如果 B 的任意元素是 A 的某个元素的影象，则 σ 说是 A 到 B 全部的一个写象．

B 的一个元素可能不是 A 的任何元素的影象，也可能是 A 的不只一个元素的影象，如果 B 的任意元素恰是 A 的一个元素的影象，则 σ 说是 A 到 B 的一个一对一的写象．

设 σ 是 A 到 B 的一个一对一的写象，我们规定 B 到 A 的一个写象 τ 如下：$\tau(b)=a$，如果 $\sigma(a)=b$，这就是说，τ 把 b 变成的元素等于在 σ 之下变成 b 的那个元素，这个写象 τ 称为 σ 的**逆**，记为 σ^{-1}，σ^{-1} 显然也是一对一的．

A 到 A 自己的一个写象叫做 A 的一个**变换**，A 的最简单的变换就是把 A 的每个元素变成自己的变换（或说是使 A 的每个元素都不动的变换），这个变换叫 A 的**同一变换**，记为 I，或为了明确起见记为 I_A，这个变换自然是一对一的而且它的逆就是它自己．

设 σ 写 B 到 C，τ 写 A 到 B，我们规定 A 到 C 的一个写象 ρ 如下：$\rho(a)=\sigma(\tau(a))$，这就是说，先用 τ 写 A 到 B，再用 σ 写 B 到 C，这样连续作两个写象所引起的由 A 到 C 的写象就是 ρ，ρ 称为 σ，τ 的**积**，记为 $\sigma\tau$．由定义，$(\sigma\tau)(a)=\sigma(\tau(a))$．注意 $\sigma\tau$ 表示先用 τ 再用 σ，不是先用 σ 再用 τ．

两个写象不一定可以相乘，但自然 A 的两个变换则永远可以相乘．

设 σ 是 A 到 B 的写象，下列二事实是显然的：

$$\sigma I_A=\sigma,\qquad I_B\sigma=\sigma.$$

如果 σ 是一对一的，则

$$\sigma^{-1}\sigma=I_A,\qquad \sigma\sigma^{-1}=I_B.$$

写象的乘法适合结合律：若 σ 写 C 到 D，τ 写 B 到 C，ρ 写 A 到 B，则

$$\sigma(\tau\rho)=(\sigma\tau)\rho.$$

事实上，对于任意 $a\in A$，

$$(\sigma(\tau\rho))(a)=\sigma((\tau\rho)(a))=\sigma(\tau(\rho(a))),$$
$$((\sigma\tau)\rho)(a)=(\sigma\tau)(\rho(b))=\sigma(\tau(\rho(a))).$$

故 $(\sigma(\tau\rho))(a)=((\sigma\tau)\rho)(a)$，因而 $\sigma(\tau\rho)=(\sigma\tau)\rho$.

对于写象的乘法，交换律不成立，比方，设 σ 写 A 到 B，τ 写 B 到 A，这时 $\sigma\tau$ 和 $\tau\sigma$ 都有意义，但 $\sigma\tau$ 是 B 的变换，$\tau\sigma$ 是 A 的变换. 即使 $A=B$，$\sigma\tau$ 和 $\tau\sigma$ 一般也是不相等的，这样的例子我们在几何上是很熟悉的.

现在我们取一个集合 M 而看 M 的一对一的变换.

M 的一组一对一的变换说是作成一个**变换群** G，如果

1) $\sigma\in G$ 时，σ^{-1} 也 $\in G$，

2) $\sigma\in G$，$\tau\in G$ 时，$\sigma\tau$ 也 $\in G$，

3) G 非空.

M 的任意变换群 G 包含 M 的同一变换 1，因由 3)，G 非空. 设 $\sigma\in G$，由 1)，$\sigma^{-1}\in G$，由 2)，$\sigma\sigma^{-1}\in G$，但 $\sigma\sigma^{-1}=1$，故 $1\in G$.

M 的同一变换自己就作成一个变换群，因为 $1^{-1}=1$，$1\cdot 1=1$，所以显然三个条件都适合.

M 的所有一对一的变换作成一个变换群 G. 事实上，1 是一对一的，故 $1\in G$ 因而 3) 成立，一对一的变换的逆仍是一对一的，故 1) 成立，又因为两个一对一的变换的积显然也是一对一的，所以 2) 也成立，这自然是 M 的最大的变换群. M 的任意变换群都是它的“子群”.

设 M 是一个有限集合. M 的一个一对一的变换叫做 M 的一个**置换**. M 的一个变换群相应地也就叫做一个置换群. 若 M 有 n 个元素，M 的所有置换作成的置换群叫做 n **次对称群**，n 次对称群共有 $n!$ 个元素.

设 σ 是 M 的一个置换，若 $\sigma(a_1)=a_2$，$\sigma(a_2)=a_3$，$\cdots$，$\sigma(a_{r-1})=a_r$，$\sigma(a_r)=a_1$，而 σ 不变 M 的其余的元素，则 σ 称为一个**轮换**，记为 $(a_1a_2\cdots a_r)$. $(a_1a_2\cdots a_r)$ 自然也可以记为 $(a_2\cdots a_ra_1)$，$(a_3\cdots a_ra_1a_2)$，等，例如 $(abc)=(bca)=(cab)$，只包含两个元素的一个轮换，比方 (a_1a_2)，叫作一个**交换**. 只包含一个元素的一个轮换，比方 (a_1)，实际上就代表同一变换.

定理1. 任意置换 σ 恰有一法写成不相杂的轮换的乘积.

证. 两个轮换 $(a_1a_2\cdots a_r)$，$(b_1b_2\cdots b_s)$ 说是不相杂，如果 $a_1,\cdots,a_r$，$b_1,\cdots b_s$ 都不同，注意不相杂的轮换相乘适合交换律：

$$(a_1\cdots a_r)\ (b_1\cdots b_s)=(b_1\cdots b_s)\ (a_1\cdots a_s).$$

先证 σ 可以写成不相杂的轮换的乘积. 取任意 $a_1\in M$. 若 $\sigma(a_1)=a_1$，则 a_1 自己就作成一个轮换. 设 $\sigma(a_1)=a_2$，$\sigma(a_2)=a_3$，$\cdots$，这样下去，由于 M 有限，写到某一个元素必然回到 a_1，例如 $\sigma(a_{r-1})=a_r$，$\sigma(a_r)=a_1$. 于是我们得到一个轮换 $(a_1a_2\cdots a_r)$. 若 M 已经没有另外的元素，则 σ 就等于这个轮换. 设 b_1 不在 $a_1,a_2,\cdots,a_r$ 之内，则同样

作法又可得到一个轮换 $(b,b_2\cdots b_s)$。若M的元素已尽，则 σ 等于这两个轮换的 乘积。若还有另外的元素，则又可得到一个轮换，如此类推，由于M有限，最后必得

$$\sigma=(a_1\cdots a_r)\ (b_1\cdots b_s)\cdots(c_1\cdots c_t)。\qquad(1)$$

上面把 σ 分成轮换的乘积的方法显然是唯一的。因为，无论怎样把 σ 分成轮换的乘积，必有一个轮换包含 a_1，这个轮换既包含 a_1，则按照轮换的定义，必包 含 $a_2,\cdots,a_r$，于是这个轮换就是 $(a_1\cdots a_r)$。同样，包含 b_1 的轮换必然也就是 $(b_1\cdots b_s)$，如此 类推，可见这个写法和 (1) 完全相同，这样我们便证明了定理.

例．四次对称群的二十四个元素可以写成下面的形式：

1，(12)，(13)，(14)，(23)，(24)，(34)，

(123)，(132)，(124)，(142)，(134)，(143)，(234)，(243)，

(1234)，(1243)，(1324)，(1342)，(1423)，(1432)，

(12)(34)，(13)(24)，(14)(23)。

上面写的 1 代表同一变换．M的四个元素用数字 1,2,3,4 代表，只包含一个元素的轮换等于同一变换，所以把一个置换写成轮换的乘积，只包含一个元素的轮换可以删去，例如 (12)(3)(4)=(12)。

定理2. 任意置换可以写成交换的乘积。

证．因为任意置换可以写成轮换的乘积，所以只要证明任意轮换可以写成交换的乘积．但不难说明下列公式成立：

$$(a_1a_2\cdots a_r)=(a_1a_r)(a_1a_{r-1})\cdots(a_1a_3)(a_1a_2)\qquad(2)$$

置换表为交换的乘积，表法不是唯一的，比方 (12)=(12)(12)(13)=(23)(13)(23)。

公式 (2) 说明含 r 个之元素的轮换可以写成 $r-1$ 个交换的乘积．若 σ 表为k个不相杂的轮换的乘积，这些轮换分别含 $r_1,\cdots,r_k$ 个元素，则 σ 可以表为 $\sum_{i=1}^{k}(r_i-1)$个交换的乘积．视 $\sum_{i=1}^{k}(r_i-1)$ 为奇为偶，我们说 σ 是一个**奇置换或偶置换**，并且，我们规定

$$sgn\,\sigma=(-1)^{\sum_{i=1}^{k}(r_i-1)}$$

定理3. $sgn\ \sigma\tau=sgn\,\sigma\ sgn\,\tau$.

证，将 σ 和 τ 分为不相杂的轮换的乘积，设 σ 等于 k 个轮换的乘积，这些轮 换 分别含 $r_1,\cdots,r_k$ 个元素，于是 σ 等 于 $\sum_{i=1}^{k}(r_i-1)$个交换之积．设最后一个交换为 (ab)．以 (ab) 乘 τ 而看其变化，a 和 b 可能在 τ 的两个不同的轮换之内，比方

$$\tau=(a\text{——})(b\sim\sim)\cdots\cdots,$$

这样，则

$$(ab)\tau=(a\text{——}b\sim\sim)\cdots\cdots.$$

可见 $sgn(ab)\tau=(-1)sgn\,\tau$；$a$ 和 b 也可能在同一个轮换之内，比方

$$\tau=(a\text{——}b\sim\sim)\cdots\cdots,$$

这样，则

$$(ab)\tau=)a\text{——})(b\sim\sim)\cdots\cdots,$$

而仍有 $sgn\,(ab)\tau=(-1)\,sgn\,\tau$. 总之，以一个交换乘 τ 即将 $sgn\,\tau$ 变号，今 σ 等于 $\sum_{i=1}^{k}(r_i-1)$ 个交换之积，故以 σ 乘 τ 乃将 $sgn\,\tau$ 变号 $\sum_{i=1}^{k}(r_i-1)$ 次，即

$$\begin{aligned} sgn\,\sigma\tau&=(-1)^{\sum_{i=1}^{k}(r_i-1)}\quad sgn\,\tau\\ &=sgn\,\sigma\ sgn\,\tau. \end{aligned}$$

由定理3，σ,τ 的奇偶与其积的奇偶之关系如下：

偶×偶＝偶，　　奇×奇＝偶，

奇×偶＝奇，　　偶×奇＝奇。

今同一变换1是偶变换，而由定理3，

$sgn\,\sigma\ sgn\,\sigma^{-1}=sgn\,\sigma\,\sigma^{-1}=1$，因而 $sgn\,\sigma^{-1}=sgn\,\sigma$，故偶置换的逆仍为偶置换，由上已知偶置换乘偶置换仍为偶置换，故有

定理4. M 的所有偶置换作成一个置换群.

若 M 有 n 个元素，则偶置换作成的群叫 n 次交代群，n 次交代群自然是 n 次对称群的“子群”.

定理5. 若 $n>1$ 则奇置换的个数和偶置换的个数相等，因之，n 次交代群的元数为 $\frac{n!}{2}$.

证. 用 G 表示次对称群，H 表示 n 次交代群. 取任意奇置换 σ，比方 σ 是一个交换. 用 σH 代表以 σ 乘 H 的所有元素而得的集合. 因为 σ 为奇，H 中的元素为偶，故 σH 中的元素皆为奇. 此外，G 中任意奇置换 τ 必在 σH 之内. 事实上，因为 σ 和 τ 皆为奇，故 $\sigma^{-1}\tau$ 为偶，因而在 H 内，比方 $\sigma^{-1}\tau=h\in H$. 于是 $\tau=\sigma h\in\sigma H$，由此可见 $G=H\cup\sigma H$，H 包含所有偶置换，σH 包含所有奇置换. 但 H 的元数和 σH 的元数相等，因若 $\sigma h_1=\sigma h_2$，则 $h_1=h_2$，故 H 中不同的元素乘以 σ 仍得不同的元素，这便证明了定理.

习　　题

1. 设 σ 和 τ 是 M 的两个变换具有下列性质：$\sigma\tau=1$，$\tau\sigma=1$. 求证 σ 和 τ 都是一对一的变换而且 $\tau=\sigma^{-1}$.

2. 设 σ 是 M 到 N 的写象. 求证对于 M 的任意子集 A,B，$\sigma(A\cap B)\subset\sigma(A)\cap\sigma(B)$. 设 A 是 N 的子集，M 中所有写到 A 中的元素的集合称为 A 的逆影象，记为 $\sigma^{-1}(A)$. 若 A,B 是 N 的任意子集，求证 $\sigma^{-1}(A\cup B)=\sigma^{-1}(A)\cap\sigma^{-1}(B)$.〔提示：证明两个集合相等只要证明它们互相包含.〕举例说明 $\sigma(A\cap B)=\sigma(A)\cap\sigma(B)$ 不成立.

3. 写出四次交代群中的元素，计算(123)(234)(14)(23).

4. 用 $1,2,\cdots,\cdots,n$ 代表 M 中的元素，求证 M 的任意置换可以表为(12)，(13)，

…,(1n)的乘积，又可以表为(12),(23),…(n−1,n)的乘积.

5. 设σ,τ是两个置换，把τ表为不相杂的轮换的乘积，求证计算στσ⁻¹只要用σ变换τ中的文字，例如σ=(123)，τ=(12)(34)，则στσ⁻¹=(23)(14)，即按照σ的变法把τ中之1换成2,2换成3,3换成1，即得στσ⁻¹.

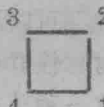
§2. 对 称 性

我们看到一个图案画或到商店看到各种各样的花布觉得很好看，为什么好看呢？颜色鲜艳固然是一个原因，但是一个重要的因素是由于这些花样有对称性，因而使我们发生一种协调之感.

平面图形中，圆是非常对称的，正方形正三角形就不如圆对称，至于斜三角形那就完全没有对称性了. 对称性怎样明确地表示出来呢？对称性的大小以什么为标准呢？

设K是一个图形（平面上或空间的），所有把K变成它自己的刚性运动作成一个变换群G. 因为，首先同一变换把K变成自己；若σ和τ都把K变成自己，则连续施行σ和τ而得的τσ也把K变成自己；最后，若σ把K变成自己，则逆变换σ^{-1}自然也把K变成自己. G叫做K的**对称性群**，G就是K的对称性的正确的数学上的表示.

圆所以非常对称，因为圆的对称性群包括绕圆心的任意转动以及这样的转动加上对于直径的反射.



现在我们研究正方形的对称性. 首先，把正方形正转90°，180°，270°的转动都把正方形变成自己；其次可以绕对角线24转180°，又可以绕13转180°；再，我们可以绕14和23的中分线转180°，又可以绕12和34的中分线转180°. 这样共有七个刚性运动，加上同一变换，共有八个. 现在我们用一种简单的写法把这些运动表示出来. 用σ代表正转90°的转动，则正转180°和270°的转动等于σ^2和σ^3.（注意$\sigma^3=\sigma^{-1}$）. 用τ代表绕13（转180°）的转动，不难说明στ，$\sigma^2\tau$，$\sigma^3\tau$等于绕12和34的中分线，绕24，绕14和23的中分线的转动，所以八个运动可以写成下面的形式：

$$1,\ \sigma,\ \sigma^2,\ \sigma^3,$$
$$\tau,\ \sigma\tau,\ \sigma^2\tau,\ \sigma^3\tau.$$

为了便于计算乘积，我们注意下列关系式：

$$\begin{cases}\sigma^4=1,\\ \tau^2=1,\\ \tau\sigma=\sigma^3\tau.\end{cases}\qquad(1)$$

例如$(\sigma\tau)(\sigma^2\tau)$可以计算如下：$\sigma\tau\sigma^2\tau=\sigma(\tau\sigma)\sigma\tau=\sigma(\sigma^3\tau)=\sigma\tau=\sigma^4(\tau\sigma)\tau=(\sigma^3\tau)\tau=\sigma^3$. 由于群的元素都可以用σ和τ表示而(1)确定了元素间的相乘关系，所以σ和τ叫群的**生成元素**，(1)叫群的**界说关系**.

八个运动又可以用四个顶点的置换表示出来，例如σ相当置换(1234). 这样得到

的八个置换如下：

$$1,\quad (1234),\ (13)(24),\ (1432),$$
$$(24),\ (12)(34),\ (13),\quad (14)(23).$$

运动的乘法自然相当置换的乘法，八个运动既然作成一个群，八个置换也就作成一个群。

空间图形以球为最对称，其对称性群包括绕球心的任意转动以及这样的转动加上对于直径面的反射。空间图形特别有趣的是五个正多面体，本节的一个习题是研究正四面体的对称性群。

不但几何图形有对称性，别的东西也可以有对称性；比方 n 个文字的一个多项式 $f(x_1,\cdots,x_n)$。如果对于置换 σ，

$$f(\sigma(x_1),\ \cdots,\sigma(x_n))=f(x_1,\cdots,\ x_n).$$

则我们说 σ 把 $f(x_1,\cdots,x_n)$ 变成它自己。所有把 $f(x_1,\cdots,x_n)$ 变成它自己的置换作成一个置换群，叫做 $f(x_1,\cdots,x_n)$ 的**对称性群**。若 $f(x_1,\cdots,x_n)$ 的对称性群是 n 次对称群，则 $f(x_1,\cdots,x_n)$ 叫做一个**对称多项式**。若 $f(x_1,\cdots,x_n)$ 的对称性群是 n 次交代群，则 $f(x_1,\cdots,x_n)$ 叫做一个**交代多项式**。

习　　题

1. 研究正四面体的对称群，说明若刚性运动只限于不变空间转向的运动，则正四面体的对称性群可以用四次交代群表示；若刚性运动包括改变空间转向的运动在内，则正四面体的对称性群可以用四次对称群表示。

2. 研究一种花布的对称性群。

3. 说明 n 个文字 $x_1,\cdots,x_n$ 的多项式 $\prod\limits_{i<j}(x_i-x_j)$ 是一个交代多项式。

4. 求多项式 $x_1x_3+x_2x_4$ 的对称性群。

§3. 抽象群的定义

试看下列各种运算系统：

1) 集合 M 的一个变换群。例如有限集合的一个置换群，平面或空间的刚性运动群，向量空间的线性变换群，等。

2) 所有 n 列非奇异方阵的乘法系统。

3) 所有整数的加法系统。

4) 所有非 0 实数的乘法系统。

5) 其他。

比较这些系统，我们看到，它们都有一种算法，根据这种算法由两个元素决定一个元素，它们的算法都适合结合律，它们都有这样一个元素，这个元素运算到其他元素上使之不变，这个元素在 1) 4) 中记为 1，在 2) 中记为 I，在 3) 中记为 0；还有，在这些系统中，每个元素有一个反面的元素：在 1) 2) 4) 中叫逆元素，在 3) 中叫负元素。